Received: 14 January 2021 | Revised: 10 March 2021 | Accepted: 16 March 2021

DOI: 10.1002/ett.4279

RESEARCH ARTICLE

SI-AKAV: Secure integrated authentication and key agreement for cellular-connected IoT devices in vehicular social networks

Alireza Esfahani[1] | Jérémie Decouchant[1] | Marcus Völp[1] | Shahid Mumtaz[2] | Kostromitin Konstantin Igorevich[3]

[1] Interdisciplinary Centre for Security, Reliability and Trust (SnT), University of Luxembourg, Luxembourg City, Luxembourg

[2] Instituto de Telecomunicações - Pólo de Aveiro, Aveiro, Portugal

[3] South Ural State University, Chelyabinsk, Russia

Correspondence
Alireza Esfahani, Interdisciplinary Centre for Security, Reliability and Trust (SnT), University of Luxembourg, Luxembourg City, Luxembourg.
Email:alireza.esfahani@uni.lu

Funding information
Horizon 2020 Framework Programme and Fonds nationale de recherche (FNR) Luxembourg

Abstract

Vehicular social networking (VSN), as a novel communication paradigm, exploits opportunistic encounters among vehicles for mobile social networking, collaborative content dissemination, and to provide a variety of services for users and their vehicles. VSNs promise to solve problems such as the ever-increasing number of road accidents, or traffic congestion, by forming networks of vehicles whose users share common interests. However, in particular in urban regions, VSNs benefit from extending far beyond vehicular networks with their road side units, by integrating all kinds of sensors to provide higher accuracy and additional information in increasingly crowded areas. Integrating such sensors turns VSNs into networks of cellular-connected IoT devices with mobile cells and raises the question how to authenticate all these units in a scalable, efficient, and anonymous manner. In this article, we present SI-AKAV, an efficient group-local authentication scheme for cellular-connected IoT devices, which is specifically tailored to overcome the high computational costs of existing schemes, while improving in all of the above dimensions. For example, compared with the state-of-the-art authentication and key agreement protocol (AKA), SI-AKAV reduces communication volume by 29% and computation overhead by 41%.

1 | INTRODUCTION

The wireless communication capabilities of vehicular ad hoc network (VANET) have been employed in various applications such as vehicular social networks (VSNs) where vehicles with a common interest form overlay networks that are efficient for content sharing, accident avoidance, maneuvering, parking spot identification or other services.[1,2] Drivers, passengers, and vehicles themselves connect to VSNs to obtain additional information and content that they cannot obtain themselves and for sharing valuable information with other vehicles. However, to tap into the full potential of this future intelligent transportation system technology, VSNs must extend far beyond vehicles and road side units, particularly in urban areas. For example, to disentangle complex traffic situations, vehicles benefit from tapping into additional sensors observing critical spots; and to find a nearby free parking spot, they benefit from querying sensors at the parking lot. In such a network, road-side units (RSUs), but sometimes also the on-board communication gateways of vehicles if no such unit is nearby, form cells, by connecting all kinds of sensors in their proximity and by assisting in their authentication towards passing vehicles and other nodes in the network. In other words, what used to be quite limited VANET-based overlays, become networks of cellular-connected IoT devices.

However, before putting the above applications into practice, it will be necessary to solve today's VSNs' security and privacy issues. In particular, message authenticity and integrity must be enforced, which turns key agreement technology into an essential requirement for establishing secure channels between RSUs and sensors in order to protect information flows and, in turn, user privacy.

Unfortunately, existing key management approaches in VANETs (eg, IPSec and SSL) are inadequate to cope with the peculiarities of VSNs[3] for the following reasons: first, the dynamic network feature of VSNs makes mobile-user to request for a frequent operation while it is needed to access to the several RSUs.[4] Second, the bounded computation capability of sensors in extended VSNs makes it challenging to effectively fulfill highly complex algorithms. In particular, abundant but cheap sensors deployed in urban areas come with limited computation and communication capabilities. Third, improperly protected or even open wireless channels make vehicles prone to attacks that aim at revealing the users' private information (such as their identity, motion pattern, or preferences).[4,5]

In the current 4G long-term evolution-advanced networks and in evolved LTE networks, the evolved packet system authentication and key-agreement (EPS-AKA) protocol ensures the authenticity of user equipment towards the serving network (SN) and the home network (HN).[6]

Nevertheless, various security vulnerabilities have been identified in EPS-AKA, including man-in-the-middle attacks (MitM), denial of service attacks,[7] and redirection attacks.[8,9] The 3GPP SA3 group[10] suggest the 5G-AKA protocol to improve over the EPS-AKA protocol, by providing security guarantees, such as identifier hiding to protect privacy against passive attackers. However, formal verification attempts of 5G-AKA[11-13] revealed several security vulnerabilities remain in this improved version, including limited key agreement, shortage of key confirmation, and identity traceability. Along with the security issues stated above, performance issues become a fundamental challenge in the current standard AKA mechanisms, particularly for massive mobile devices.[11] Since the current 3GPP standard[10] mentions that there is no authentication protocol for massive IoT devices, each device requires performing the full AKA protocol to remain standard conform in situations where a multitude of mobile devices connect concurrently to 3GPP networks. Such situations could easily induce severe congestion[14] due to significant signaling and communication costs.[15] In particular, if several devices in a group request access to the network, existing authentication protocols will suffer from high network latency until the authentication completes, mostly when devices roam domains far from their home.

To address the challenges mentioned above and to tackle the raised security issues, we propose SI-AKAV, a secure integrated authentication and key agreement protocol for VSNs. For the first time to the best of our knowledge, the proposed protocol considers an authentication component, as proposed in Reference 13, which assumes the role of a proxy and is responsible for managing devices as a group instead of as individual entities. In VSNs, such authentication components are naturally available in the form of RSUs and on-board communication gateways. In particular, we extend the work from Lai et al,[13] where a similar approach is followed to provide secure and efficient group authentication and key agreement for a group of LTE mobile devices and cellular-connected sensors. The main contributions of this article are as follows.

- First, we review the literature on security approaches for VSNs and give an overview of VSNs with a focus on their security;
- Second, we propose a secure integrated group key-based authentication scheme, in which a lightweight group key agreement (GKA) protocol (based on AKA) ensures both security and practicality. SI-AKAV meets the security requirements defined in EPS-AKA and can resist attacks including MitM attacks, redirection attacks, and impersonation attacks. Our analysis shows further that the transmission and computation overheads of the authentication process is considerably reduced;
- Third, we highlight several open research issues and future research directions in security aspect of VSNs.

The remainder of this article is organized as follows. Section 2 discusses related work. Section 3 introduces the system model and security assumption of our protocol. Sections 4 and 5, describe our secure integrated GKA protocol, respectively, its security analysis in greater detail. Sections 6 and 7 present our performance analysis and some important open research issues, respectively. Section 8 concludes.

2 | RELATED WORK

VSNs appear as a novel and attractive communication paradigm utilizing opportunistic encounters among vehicles, sharing the same interests or goals, thereby forming a communication layer on top of more classical mobile networks[16] (eg, VANETs). Applications of VSNs include cooperative driving, accident/road block evasion, but also collaborative content dissemination[17-20] (see Figure 1). Extending VSNs to not only include vehicles and RSUs, but, in particular in urban regions, also all kinds of sensors, turns them into networks with a massive amount of IoT devices. These networks can be clustered quite naturally by proximity to a RSU or by defining regions if no such unit should be deployed. In the latter case, entering vehicles can assume the role of the head of such a regional cluster.

Many related studies have been reported on GKA protocols for massive IoT devices, which we discuss in the following. They can be divided mainly into the following four categories.

2.1 | Pseudonym certificate authentication protocols

For pseudonym certification schemes, trust authority must generate many pseudonyms and certificates. As a legal identity, each vehicle requires randomly selecting the pseudonym and the corresponding certificate since participating in the authentication process. Nevertheless, each vehicle must hold many pseudonyms and certificates to provide privacy requirements, leading to tremendous efforts on vehicles with inadequate computing and storage resources. Furthermore, in the case of revocation, the vehicle should add all pseudonyms and certificates to the certificate revocation list (CRL), which is further a significant challenge for CRL's management.[21] Raya and Hubaux[22] proposed an authentication scheme that each vehicle needs to preload a large number of anonymous public and private key pairs mutually with the corresponding public key certificates. In order to sign the messages, they have leveraged a public-key-based scheme. Furthermore, a pseudo ID is generated in each public key certificate in order to achieve privacy. However, this protocol needs a considerable storage space to collect this security data.[23-25]

2.2 | Signature-based group authentication protocols

The signature-based group is broadly utilized for anonymous authentication in VSNs due to its anonymity and traceability features. During the authentication process, a signature belongs to each group can prove the reliability of

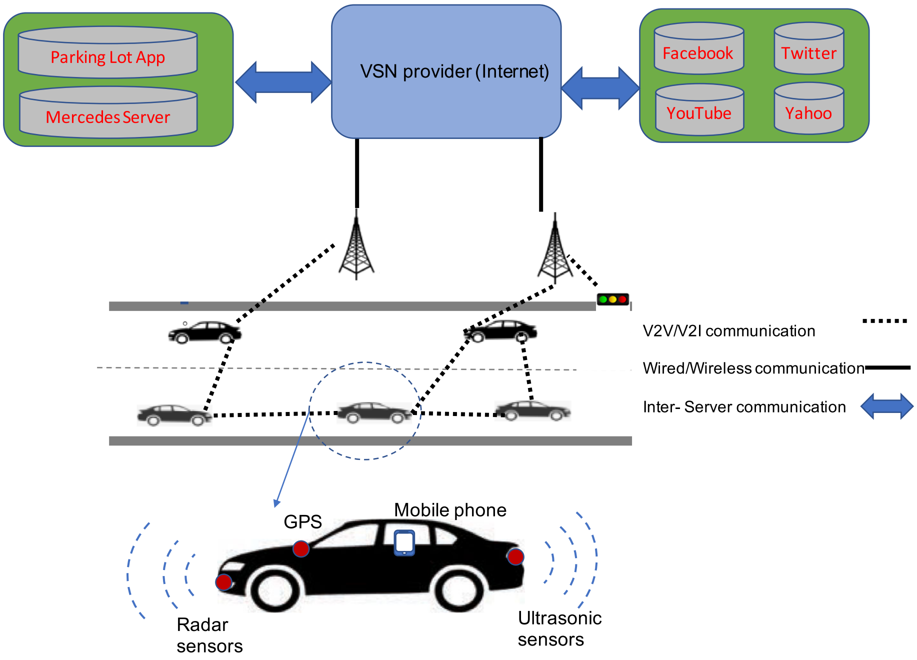

FIGURE 1 Vehicle social networks overview where vehicles establish social ties based on mobility and common interests (eg, Facebook, Twitter, Parking lot app, and so on)

vehicles without revealing their identities. Meantime, the group leader assures vehicle's traceability. The group leader can withdraw the signature once the vehicle is found not to be illegible. Nevertheless, to obtain some particular services, the vehicle needs to show its identity information which signature-based group scheme can hardly achieve this goal.[26] Lin et al[27] proposed a group signature-based scheme, where it signs each message before broadcasting it. Considering there is noidentity information involved in messages, it can also gain identity privacy preservation. Furthermore, Calandriello et al[28] have shown that the group-signature-based scheme can benefit from the reduction of key pairs' storage cost and bandwidth consumption. They also presented a related scheme, where a vehicle can generate public and private key pairs by using a group key to reduce the group signature-based scheme's overhead. The proposed scheme can reach a tradeoff between the signature-based group scheme and the public key infrastructure-based scheme. Xi et al[29] proposed a random key-set-based authentication protocol to improve the vehicles' privacy. An RSU is takes care of issuing an anonymous certificate to vehicles. Besides, for intervehicle communications, a vehicle's identity is anonymous to other vehicles. However, this scheme essentially faces certificate revocation issues.[30]

2.3 | Aggregation-based group authentication protocols

In this category of protocols, each group selects a group leader who can aggregate many access request messages from all group members into an aggregation access request message. Then the group leader can authenticate all the group's members simultaneously by monitoring the aggregate information. Lai et al[31] have first designed a lightweight group authentication protocol (LGTH) by using the aggregation message authentication code (AMAC) technique. By the LGTH protocol, the home subscriber server (HSS) can achieve access authentication with the mobile devices in a group simultaneously by verifying the AMAC. Cao et al[32] have shown that the LGTH protocol[31] cannot resist the interior forgery attack, and it lacks identity privacy protection. They also presented a group-based authentication scheme for mobile devices in LTE networks.[32] In this protocol, the group leader aggregates all of the signatures from the group members, and consequently, the mobility management entity (MME) can simultaneously trust the MTC group by verifying the aggregate signature generated by the group leader. Use of the aggregation method can reduce the communication cost.[8,31,32]

2.4 | Secure context transmission-based group authentication protocols

A large number of vehicles belonging to the same HN can create a group. Since the first vehicle in the group makes the complete access authentication process, all security setting data is stored securely at the SN, which can be used further for other group members. Afterward, each group member can join and be authenticated by the SN without reaching the HN.[13] Huang et al[33] propose a secure AKA (S-AKA) protocol that can provide a group authentication keys and resist the typical attacks. The authors gave a formal proof of the S-AKA protocol to guarantee its robustness. However, similarly to other existing schemes, this scheme is not fit for group-based communications due to the loss of group authentication mechanism. The first group-based authentication and key-agreement scheme for mobile devices was proposed by Chen et al.[34] The proposed scheme optimizes the performance of authentication of group communications. Nevertheless, it also cannot provide enough security and has vulnerability to redirection, MitM, and so on.[13] A lightweight group authentication scheme (GLARM) for resource-constrained Machine-to-Machine (M2M) is proposed by Lai et al.[35] They show that GLARM can achieve efficient and secure group authentication. All devices can be authenticated simultaneously while the authentication overhead is minimized. However, GLARM cannot achieve privacy-protection and key backward secrecy/key forward secrecy. Secure and efficient AKA (SE-AKA) was proposed by Lai et al[13] to enhance group authentication scenarios in LTE networks. SE-AKA provides strong security properties, including privacy and key forward/backward secrecy. An extensive security analysis has shown that SE-AKA is secure against various malicious attacks. The performance evaluation in terms of communication, computational and storage overheads demonstrates that the whole authentication process's transmission overhead is considerably decreased. However, SE-AKA employs elliptic curve Diffie-Hellman to achieve forward and backward secrecy, which is hugely costly for resource constraint cellular-connected IoT devices.

Table 1 summarizes the properties of state-of-the-art authentication and key management protocols and related those to our protocol SI-AKAV.

TABLE 1 Comparison of security goals and overheads among the most relevant AKA protocols

Feature	SE-AKA[13]	GLARM[35]	G-AKA[34]	*SI-AKAV* (this article)
Type of cryptosystem	Hybrid	Symmetric	Symmetric	Symmetric
Key fwd/backwd secrecy	✓	×	×	✓
Resistance to attacks	Replay, MITM, and Redirection	MITM, and Redirection	Redirection	Replay, MITM, and Redirection
Privacy-preservation	×	✓	×	✓
Communication overhead	Small	Small	Medium	Small
Computation overhead	Medium	Small	Large	Small

3 | SYSTEM MODEL AND SECURITY ASSUMPTION OF OUR SCHEME

3.1 | System model

As shown in Figure 1, VSNs[36] are a particular category of VANETs that provide multiple services (eg, based on social interests or relationships) to users. VSNs can afford related vehicular applications and services according to the interests and desires of vehicle users. Precisely, the vehicle can join around a social network and gain useful information, with RSU cooperation.[37] VSNs includes two layers. At the top layer, secure channels, such as the transport layer security protocol, can connect the VSN provider and RSUs. The VSNs grant application data to RSUs and RSUs work as gateways to deliver data to the vehicles. In the lower layer, vehicles include cellular-connected IoT devices (eg, sensors and gateways) which can interact with each other and with RSUs. This article focuses on addressing the security issues in the lower layer where sensors/gateways communicate with each other or RSUs.

Our system model, shown in Figure 2, considers the following entities in an LTE scenario.

Massive IoT deployment. Our system consists of a large number of vehicles including IoT devices (eg, sensors/smartphones) that form groups ($G_1, \dots, G_m$) based on their similarity (eg, type of application, type of device, proximity). For each group of vehicles, one leader (eg, gateway)—the cluster head (CH)—is selected. Communication between group members and the CH is performed through direct links and the group authentication process is performed for each group with its gateway (eg, the smartphone) through the respective CH.

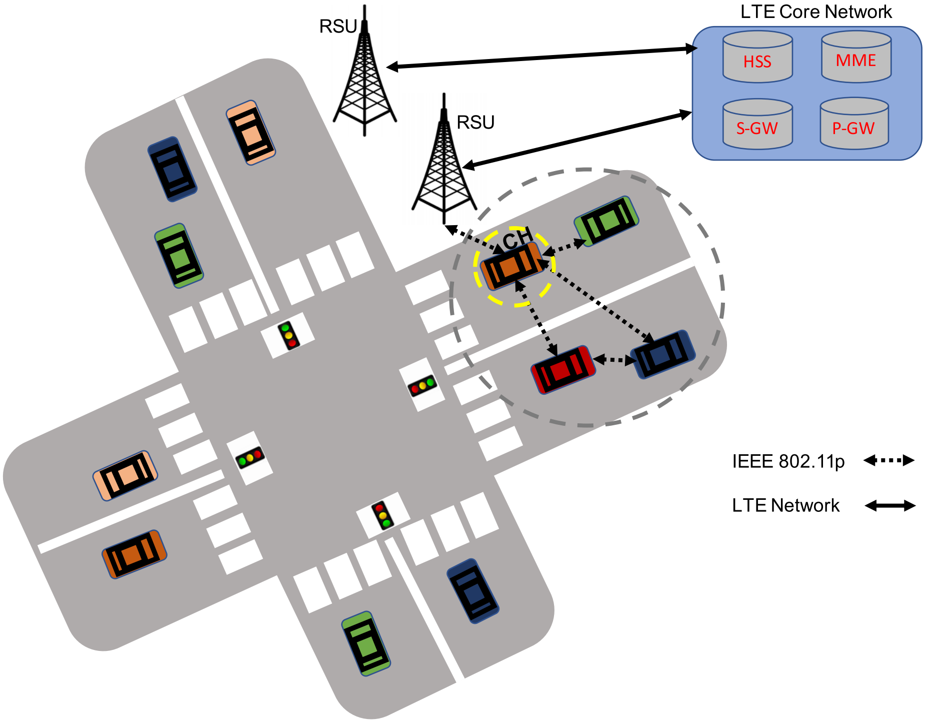

FIGURE 2 Network architecture where vehicles including sensors and/or smartphones form a group. In each group, a cluster head communicates to other members of the group and the nearest road-side unit

Road-side units RSUs play the role of a proxy. Leveraging the role of these gateways in the authentication phase of the IoT devices avoids bottlenecks at the network operator side and allows for a more efficient authentication, in terms of achievable delays and reduced overheads. The gateway needs to be present during the whole authentication phase and when establishing session keys. Otherwise, any device with the computational power of a normal smartphone suffices.

LTE core network. Each LTE core network includes several entities. MME is responsible for all the functions related to the users' devices and the control plane session management.[34] HSS is located in each HN and provides authentication and management services for the each entity. In addition, in our system model, we assume that HSSs are also responsible for providing authentication and management services for the massive IoT devices of their respective HNs. Differently from Huang et al,[33] our assumption is that the HSS is also responsible for the group management service. Thus, in our system model, we do not need to have any other server (eg, group management server), nor do we have to establish a secure channel between that server and the HSS.

3.2 | Security assumption

We assume that an adversary cannot compromise the HSS of the HN, and thus is trusted by all entities in our system. It is secure to preestablish the reliable channel for each cellular-connected IoT device (eg, vehicles including sensor or gateway) using traditional security protocols, for example, using the third generation partnership project authentication and key agreement. Other malicious adversaries can impersonate RSUs in the system, and then they will deceive other RSUs to provide access services for illegal users. Besides, we assume that the adversary can modify or inject messages, interrupt messages propagation over the air, and corrupt the proposed protocol.

4 | SI-AKAV: LIGHTWEIGHT AUTHENTICATION AND KEY AGREEMENT PROTOCOL

In this section, we propose a secure integrated authentication key agreement scheme called SI-AKAV. With SI-AKAV, when a vehicle detects a nearby RSU it tries to associate with the RSU. Our assumption is to choose a gateway (eg, a smartphone available at a vehicle) as the CH. The vehicles, including sensors/gateways, create several groups based on particular principles. These principles included using the same application, belonging within the same region, or having the same behavior. Then, the RSU and CH, by using the group identity (eg, ID_{G_i}), can provide a message authentication code (MAC) to each group for authentication of the rest member of each group. In order to manage the information of each group, a group information management list (GIML) is created (As shown in Table 3). The GIML contains group identity, CH temporary identity $\mathrm{TID}_{\mathrm{CH}_i}$. The detailed implementation of SI-AKAV will be presented in the following sections. For clarity of presentation, Table 2 lists the notations we use to describe SI-AKAV.

4.1 | Initialization

SI-AKAV initially associates a mobile node to a HN through a subscription procedure. It then allows the mobile node to roam from network to network. We assume devices are prepared as follows:

- Each sensor/gateway and HSS preshare a secret key.
- A group key is known by all sensors/gateway in the same group as well as by the HSS.
- Function $f_x^1$is used to calculate the MAC, which is known by every sensor/gateway.

TABLE 2 Group information list

Group	Group ID	Temporary CH ID
G_1	ID_{G_1}	$\mathrm{TID}_{\mathrm{CH}_{G_1}}$
⋮	⋮	⋮
G_m	ID_{G_m}	$\mathrm{TID}_{\mathrm{CH}_{Gm}}$

TABLE 3 Notations

Symbol	Description
R_i	A random number generated by i
MAC_x	The message authentication code computed by x
ID_x	The identity of x
key_x	The key known by x
TK_x	The temporary key calculated by x
KG_x	The session key calculated by x
f_k^1	MAC generation function using k
f_k^2	A one way hash function which is used to calculate a temporary key by using k
f_k^3	A one way hash function which is used to generate a session key between two entities by using k

- Function f_x^2 is a one way hash function used to calculate the group temporary key. This function is run once for each CH.
- Function f_x^3 is similar to f_x^2 and used to calculate the session key (more details in Table 3)

We assume CH and sensors/gateways are already identified, for example, by their $\mathrm{ID}_{\mathrm{CH}_{G_i}}$ and $\mathrm{ID}_{S_{G_i}}$, respectively. CH and sensors/gateways provide their identities when they visit a SN. The SN checks whether the CH contains the authentication request from an active group and if any sensor/gateway of this group has already completed full authentication. If not, the CH takes care of the authentication process. Initially, the CH belongs to a specific group. It provides its identity to the HSS in the SN through the RSU. Then, the HSS in the HN will verify the validity of the claimed identity of the CH and that it belongs to the claimed group. The RSU completes a full authentication process for the CH and obtains, as a result, an authentication token $\mathrm{AUTH}_{\mathrm{HSS}}$, derived from the HSS. SI-AKAV consists of two processes: (i) the CH gateway authentication process; and (ii) the sensors/gateway authentication process.

4.2 | CH gateway authentication process

We now detail the authentication process for the CH gateway CH_{G_1}, which is the CH of group G_i and therefore initiates the authentication process for the group. The description naturally generalizes to any other group of vehicles. We consider that the communication between RSU and HSS is secure.[13] The following steps (1-8) describe how the CH gateway is authenticated through the RSU and HSS. The CH gateway authentication process is also shown in Figure 3.

- **Step-1: Access request**
  $\mathrm{CH}_{G_i} \rightarrow \mathrm{RSU}_{G_i}$
- **Step-2: Identity request**
  $\mathrm{RSU}_{G_i} \rightarrow \mathrm{CH}_{G_i}$
- **Step-3: Identity response (**$\mathrm{AUTH}_{\mathrm{CH}_{G_i}}$**)**
  $\mathrm{CH}_{G_i} \rightarrow \mathrm{RSU}_{G_1}$
  CH_{G_i} generates $\mathrm{AUTH}_{\mathrm{CH}_{G_i}} = (\mathrm{ID}_{\mathrm{CH}_{G_i}} \| \mathrm{ID}_{G_i} \| R_{\mathrm{CH}_{G_i}} \| \mathrm{MAC}_{G_i})$, where $\mathrm{MAC}_{G_i} = f^1_{\mathrm{key}_{\mathrm{CH}_{G_i}}}(\mathrm{ID}_{\mathrm{CH}_{G_i}} \| \mathrm{ID}_{G_i} \| R_{\mathrm{CH}_{G_i}})$.
- **Step-4: Authentication data request (**$\mathrm{AUTH}_{\mathrm{CH}_{G_i}}$, LAI**)**
  $\mathrm{RSU}_{G_i} \rightarrow \mathrm{HSS}$
  RSU_{G_i} sends the concatenation of $\mathrm{AUTH}_{\mathrm{CH}_{G_i}}$ and LAI to the HSS.
- **Step-5: Authentication data response (**$\mathrm{AUTH}_{\mathrm{HSS}}$**)**
  $\mathrm{HSS} \rightarrow \mathrm{RSU}_{G_i}$
  After verifying AUTH_{G_i} and LAI, HSS generates $\mathrm{AUTH}_{\mathrm{HSS}} = (R_{\mathrm{HSS}} \| R_{\mathrm{CH}_{G_i}} \| \mathrm{LAI} \| \mathrm{TK}_{G_i})$ and sends it to the RSU. TK_{G_i} is the temporary key for the group which is calculated as: $\mathrm{TK}_{G_i} = f^2_{\mathrm{key}_{G_i}}(\mathrm{ID}_{G_i} \| R_{\mathrm{HSS}})$.

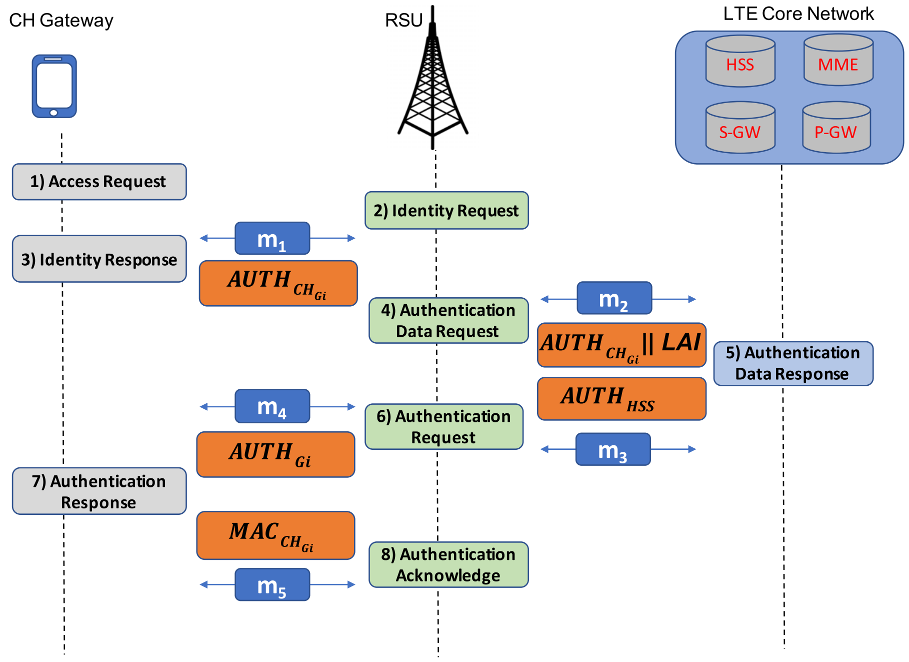

FIGURE 3 Cluster head gateway authentication process

- **Step-6: Authentication request** (AUTH_{G_i})

  $\mathrm{RSU}_{G_i} \rightarrow \mathrm{CH}_{G_i}$

  RSU_{G_i} stores $\mathrm{AUTH}_{\mathrm{HSS}}$, generates $\mathrm{AUTH}_{G_i} = (\mathrm{ID}_{\mathrm{RSU}}\|\mathrm{ID}_{G_i}\|\mathrm{AUTH}_{\mathrm{HSS}}\|R_{\mathrm{RSU}}\|\mathrm{MAC}_{\mathrm{RSU}}\|\mathrm{LAI})$ and sends it to CH_{G_i}, where $\mathrm{MAC}_{\mathrm{RSU}} = f^1_{\mathrm{TK}_{G_i}}(\mathrm{ID}_{\mathrm{RSU}}\|\mathrm{ID}_{G_i}\|R_{\mathrm{RSU}}\|\mathrm{TID}_{\mathrm{CH}_{G_i}})$ and $\mathrm{TID}_{\mathrm{CH}_{G_i}}$ is available through Table 3.
- **Step-7: Authentication response** ($\mathrm{MAC}_{\mathrm{CH}_{G_i}}$)

  $\mathrm{CH}_{G_i} \rightarrow \mathrm{RSU}_{G_i}$

  After verifying AUTH_{G_i}, CH_{G_i} generates $\mathrm{MAC}_{\mathrm{CH}_{G_i}} = f^1_{\mathrm{key}_{\mathrm{CH}_{G_i}}}(\mathrm{ID}_{\mathrm{CH}_{G_i}}\|\mathrm{ID}_{G_i}\|\mathrm{TID}_{\mathrm{CH}_{G_i}})$, where $\mathrm{KG}_{\mathrm{CH}_{G_i}} = f^3_{\mathrm{key}_{\mathrm{CH}_{G_i}}}(R_{\mathrm{CH}_{G_i}}\|R_{\mathrm{RSU}}\|\mathrm{LAI})$ is a session key. The calculated $\mathrm{MAC}_{\mathrm{CH}_{G_i}}$ is sent back to RSU.
- **Step-8: Authentication acknowledgement (success/fail)**

  $\mathrm{RSU}_{G_i} \rightarrow \mathrm{CH}_{G_i}$

  When the *RSU* receives an authentication response message, carrying $\mathrm{MAC}_{\mathrm{CH}_{G_i}}$, it checks if it has received the correct response as follows:

  (1) CH_{G_i} calculates $\mathrm{KG}_{\mathrm{CH}_{G_i}} = f^3_{\mathrm{key}_{\mathrm{CH}_{G_i}}}(R_{\mathrm{CH}_{G_i}}\|R_{\mathrm{RSU}}\|\mathrm{LAI})$;

  (2) Then CH_{G_i} calculate $\mathrm{MAC}'_{\mathrm{CH}_{G_i}} = f^1_{\mathrm{key}_{\mathrm{CH}_{G_i}}}(\mathrm{ID}_{\mathrm{CH}_{G_i}}\|\mathrm{ID}_{G_i}\|\mathrm{TID}_{\mathrm{CH}_{G_i}})$;

  (3) The CH_{G_i} verifies whether $\mathrm{MAC}'_{\mathrm{CH}_{G_i}}$ equals the received $\mathrm{MAC}_{\mathrm{CH}_{G_i}}$ or not.

  If $\mathrm{MAC}'_{\mathrm{CH}_{G_i}}$ is not the same as $\mathrm{MAC}_{\mathrm{CH}_{G_i}}$, the RSU_{G_i}terminates the procedure. However, If $\mathrm{MAC}'_{\mathrm{CH}_{G_i}}$ equals $\mathrm{MAC}_{\mathrm{CH}_{G_i}}$, the RSU_{G_i} sends the authentication acknowledgment message to CH_{G_i}, which completes the authentication and key agreement procedure for the CH smartphone. $\mathrm{KG}_{\mathrm{CH}_{G_i}}$ can then be used in subsequent sessions between the CH smartphone and RSU.

4.3 | Sensors/gateways authentication process

We define $S_{G_{i,j}}$ as the *j*th sensor/gateway initiating the authentication process in group G_i. CH_{G_i}, which locally stores the existing AUTH_{G_i}, performs mutual authentication and key agreement with $S_{G_{i,j}}$. After a CH gateway has been authenticated, the group authentication data distribution (ie, steps 4-6 of the CH gateway authentication process) does not need to be performed to authenticate the remaining sensors/gateway. This procedure is shown in Figure 4, and we describe in the following how SI-AKAV authenticates the remaining sensors/gateways of a given group through the CH gateway.

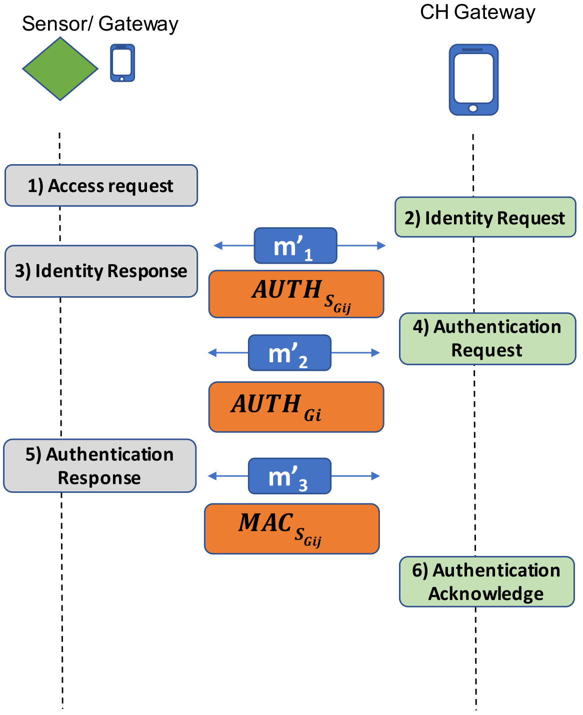

FIGURE 4 Sensors/gateways authentication process

- **Step-1: Access request**
  $S_{G_{i,j}} \rightarrow \mathrm{CH}_{G_i}$
- **Step-2: Identity request**
  $\mathrm{CH}_{G_i} \rightarrow S_{G_{i,j}}$
- **Step-3: Identity response** $(\mathrm{AUTH}_{S_{G_{i,j}}})$
  $S_{G_{i,j}} \rightarrow \mathrm{CH}_{G_i}$
  $S_{G_{i,j}}$ generates $\mathrm{AUTH}_{S_{G_{i,j}}} = (\mathrm{ID}_{S_{G_{i,j}}} \| \mathrm{ID}_{G_i} \| R_{S_{G_{i,j}}})$ and sends it to CH_{G_i}.
- **Step-4: Authentication request** (AUTH_{G_i})
  $\mathrm{CH}_{G_i} \rightarrow S_{G_{i,j}}$
  CH_{G_i} uses the previously stored values AUTH_{G_i} and sends it to $S_{G_{i,j}}$.
- **Step-5: Authentication response** $(\mathrm{MAC}_{S_{G_{i,j}}})$
  $S_{G_{i,j}} \rightarrow \mathrm{CH}_{G_i}$
  After verifying the received $\mathrm{MAC}_{\mathrm{RSU}}$ through AUTH_{G_i}, $S_{G_{i,j}}$ generates $\mathrm{MAC}_{S_{G_{i,j}}}$ and sends it to CH_{G_i}. The generated $\mathrm{MAC}_{S_{G_{i,j}}}$ is calculated such as: $\mathrm{MAC}_{S_{G_{i,j}}} = f^1_{\mathrm{KG}_{S_{G_{i,j}}}}(\mathrm{ID}_{S_{G_{i,j}}} \| \mathrm{ID}_{G_i} \| \mathrm{TID}_{S_{G_{i,j}}})$, where $\mathrm{KG}_{S_{G_{i,j}}} = f^3_{\mathrm{key}_{S_{G_{i,j}}}}(R_{\mathrm{CH}_{G_i}} \| R_{S_{G_{i,j}}} \| \mathrm{LAI})$.
- **Step-6: Authentication acknowledgment (success/fail)**
  $\mathrm{CH}_{G_i} \rightarrow S_{G_{i,j}}$
  After verifying the $\mathrm{MAC}_{S_{G_{i,j}}}$, CH_{G_i} sends the authentication acknowledgment. In addition, the $\mathrm{KG}_{S_{G_{i,j}}}$ can be used for the subsequent session between the sensor/gateways and CH gateways.

4.4 | Vehicle joining and leaving the group

The group that is formed by vehicles (including sensors/gateways) requires backward and forward secrecy. Backward secrecy means a new vehicle cannot exchange messages before it joins the group. By contrast, forward secrecy considers that a leaving or dismissed vehicle cannot maintain reaching the group's communication. When a vehicle leaves the group, the CH must cancel the necessary relationship between the sensor/smartphone and the group. Therefore, the vehicle cannot continue communication with the RSUs as the group member. In addition, it is necessary to update the group key, when a vehicle leaves the group, to prevent the old vehicle from decrypting the group's new packets. A new group key must be generated and shared among the group members while the old vehicle leaves the group. Furthermore, when a vehicle requests to join the group, it does not need to perform a full AKA authentication procedure with the SN. Updating the group key is a problem which is out of the scope of this article.

5 | SECURITY EVALUATION

We now present a security analysis that demonstrates that SI-AKAV can provide the required security properties and resist attacks.

5.1 | Security analysis

The following lemmas show that SI-AKAV has the same security properties, namely, the mutual authentication, confidentiality, and independent session key properties, as the protocol proposed by Lai et al.[13]

Lemma 1. *(Mutual authentication) Given two received messages either*$\mathrm{MAC}_{\mathrm{CH}_{G_i}}$ *or* $\mathrm{MAC}_{S_{G_{i,j}}}$*, respectively, SI-AKAV mutually authenticates CH gateway or sensor/gateway.*

Proof. Upon reception of $\mathrm{MAC}_{\mathrm{CH}_{G_i}}$, the RSU checks whether the received $\mathrm{MAC}_{\mathrm{CH}_{G_i}}$ is equal to the calculated $\mathrm{MAC}'_{\mathrm{CH}_{G_i}}$. The CH gateway is considered authenticated if the equality holds. In addition, upon receipt of $\mathrm{MAC}_{S_{G_{i,j}}}$, the CH gateway checks whether the received $\mathrm{MAC}_{S_{G_{i,j}}}$ is equal to the calculated $\mathrm{MAC}'_{S_{G_{i,j}}}$. The sensor/gateway is considered authenticated if the equality holds. ■

Lemma 2. *(Confidentiality) SI-AKAV provides confidentiality.*

Proof. By contradiction, we assume that SI-AKAV cannot provide confidentiality. If this is the case, an adversary should be able to get the CH gateway or sensor's/gateway's identity (eg, $ID_{\mathrm{CH}_{G_i}}$ or $\mathrm{ID}_{S_{G_{i,j}}}$) through $\mathrm{MAC}_{\mathrm{CH}_{G_i}} = f^1_{\mathrm{key}_{\mathrm{CH}_{G_i}}}(\mathrm{ID}_{\mathrm{CH}_{G_i}}\|\mathrm{ID}_{G_i}\|\mathrm{TID}_{\mathrm{CH}_{G_i}})$ or $\mathrm{MAC}_{S_{G_{i,j}}} = f^1_{\mathrm{KG}_{S_{G_{i,j}}}}(\mathrm{ID}_{S_{G_{i,j}}}\|\mathrm{ID}_{G_i}\|\mathrm{TID}_{S_{G_{i,j}}})$, for the CH gateway or sensors/gateway, respectively. However, without knowing the $\mathrm{KG}_{\mathrm{CH}_{G_i}}$ or $\mathrm{KG}_{S_{G_{i,j}}}$, the identity of the CH gateway $\mathrm{ID}_{\mathrm{CH}_{G_i}}$ or of a sensor/gateway $\mathrm{ID}_{S_{G_{i,j}}}$, which are based on a hash value, cannot be obtained. ■

Lemma 3. *(Independent session key) Given the session key* KG_x*, SI-AKAV gives an independent session key property.*

Proof. If the session key KG_x is compromised by an adversary, the mobile device can detect the compromised key session. This is because the generation of the session key KG_x in the proposed authentication mechanism is hashed based on the key that belongs to each entity. ■

Lemma 4. *(Perfect forward/backward secrecy (PFS/PBS)) While PFS emphasizes the protection of past communications, PBS assures reestablishing secure communication channels for further communications.*

Proof. PFS feature confirms that if a new car, including sensor/gateway, wants to join the group, the group's access control is mandatory. The temporary group key must also be updated when the new car joins a group; so that even if the new sensor/gateway can sniff the old messages transmitted over the group, it cannot decrypt them. PBS ensures that if an old car leaves the group, the CH gateway will cancel the necessary relationship between the car and the group, consequently, the sensor/smartphone belongs to the car cannot continue communication with the CH gateway or RSU as the group member. ■

5.2 | Resistance to attacks

Besides the security properties mentioned above, SI-AKAV can resist the following attacks.

5.2.1 | Man-in-the-middle (MITM)

After having obtained any entity's identity (ie, $\mathrm{ID}_{\mathrm{CH}_{G_i}}$ or $\mathrm{ID}_{S_{G_{i,j}}}$), an adversary is not able to launch a MITM attack between the sensor/gateway and a CH gateway and computes the keys $\mathrm{KG}_{\mathrm{CH}_{G_i}}$ or $\mathrm{KG}_{S_{G_{i,j}}}$, because it is not able to obtain the secret keys that are only known to the sensors/gateway or the CH gateway. In addition, $\text{key}_{\text{CH}_{G_i}}$ and $\text{key}_{S_{G_i,j}}$ are securely stored in the CH or any sensor/gateway, respectively, and are never transmitted to any other entity.

5.2.2 | Replay attack

In SI-AKAV, random numbers $R_{\text{CH}_{G_i}}$, $R_{S_{G_{i,j}}}$, and R_{HSS} generated by CH_{G_i}, $S_{G_{i,j}}$, and HSS used in generating challenge messages toward the opposite side, respectively. Considering these random numbers used in each authentication procedure are changed frequently if an adversary obtains a random number in an authentication procedure, it cannot reuse the random number in a new authentication procedure. Therefore, SI-AKAV can prevent replay attacks.

5.2.3 | Redirection attack

The redirection attack succeeds if the adversary obtains a car information (sensors/smartphone) by impersonating a CH smartphone. Without the car information, the adversary cannot impersonate any sensor/gateway and connect to a legitimate CH gateway.

6 | PERFORMANCE EVALUATION

In this section, we evaluate the bandwidth consumption and computational overhead of SI-AKAV, and compare them with those of existing schemes.

6.1 | Communication overhead

In order to calculate the bandwidth consumption, our assumption is that the HSS can successfully authenticate the CH gateway when x Authentication Vectors (AVs) are transmitted, and there are $n$sensors/gateway forming p groups. Furthermore, to better comparison the SI-AKAV communication overhead with the existing protocols, the relevant parameters used in these protocols is given in Table 4.

The size of each authentication process (CH gateway and sensors/gateway) in SI-AKAV is calculated as follows.

- CH gateway overhead (bw_{CH}): Five AVs are transmitted during the authentication procedure of the CH gateway ($m_1, \dots, m_5$).

  The size of each m_i is calculated as follows.

1. $|m_1| = |\text{AUTH}_{\text{CH}_{Gi}}| = 2|\text{ID}| + |R| + |\text{MAC}|= 448$ bits
2. $|m_2| = |\text{AUTH}_{\text{CH}_{Gi}}| + |\text{LAI}|= 488$ bits
3. $|m_3| = |\text{AUTH}_{\text{HSS}}| = 2|R| + |\text{LAI}| + |\text{TK}|= 424$ bits
4. $|m_4| = |\text{AUTH}_{Gi}| = 2|\text{ID}| + |m_3| + |R| + |\text{MAC}| + |\text{LAI}|= 912$ bits
5. $|m_5| = |\text{MAC}|= 64$ bits

TABLE 4 Parameter settings

Parameters	Value (bits)
ID_i	128
Random number (R)	128
f_k^1 and MAC	64
f_k^2 and f_k^3	128
LAI	40
TK	128

Therefore, $\mathrm{bw}_{\mathrm{CH}}$ is finally calculated as follows.

$$\mathrm{bw}_{\mathrm{CH}} = \sum_{i=1}^{5} |m_i| = 2336\, bits. \tag{1}$$

- Sensor/gateway overhead ($\mathrm{bw}_{\mathrm{remaining}}$): after the CH has been authenticated, authenticating another node requires three AVs: $m'_1 = \mathrm{AUTH}_{S_{Gi,j}}$, $m'_2 = \mathrm{AUTH}_{Gi}$, and $m'_3 = \mathrm{MAC}_{S_{Gi,j}}$ (See Figure 4). The size of each AVs is calculated as follows.

1. $|m'_1| = 2|\mathrm{ID}| + |R| = 448$ bits
2. $|m'_2| = 2\,|\mathrm{ID}| + |m_3| + |R| + |\mathrm{MAC}| + |\mathrm{LAI}| = 912$ bits
3. $|m'_3| = |\mathrm{MAC}| = 64$ bits

Equation (2) gives the bandwidth consumption for $\mathrm{bw}_{\mathrm{remaining}}$.

$$\mathrm{bw}_{\mathrm{remaining}} = \sum_{i=1}^{3} |m'_i| = 1424\, bits. \tag{2}$$

The overall bandwidth consumption of SI-AKAV, for n sensors and p groups, is then equal to

$$\mathrm{bw}_{\mathrm{total}} = p * \mathrm{bw}_{\mathrm{CH}} + (n - p) * \mathrm{bw}_{\mathrm{remaining}}. \tag{3}$$

Here, $\mathrm{bw}_{\mathrm{CH}}$ and $\mathrm{bw}_{\mathrm{remaining}}$ represent the bandwidth consumed when authenticating the CH gateway and each sensor/gateway, respectively.

We compare the bandwidth overhead of SI-AKAV and the existing AKA protocols in Figures 5 and 6. The results show that the communication overhead of SI-AKAV is much lower than that in SE-AKA[13] and GLARM[35] and is close to G-AKA.[34] In particular, the communication overhead comparison shows that SI-AKAV reduces the communication overhead by 29% (in average).

6.2 | Computation costs

Following the assumption in Reference 38, we measured the time used by the primitive cryptography operations by using the C/C++ OPENSSL library on a Celeron 1.1 GHz processor, which represent a smartphone, and a Dual-Core 2.6 GHz as an MMU/RSU and an HSS. $C_h^S = 0.0356$ ms and $C_h^M = 0.0121$ ms denote the cost of computing the one-way hash function (eg, f_1,f_2, and f_3) used by sensor/smartphones and RSU/MME/HSS, respectively. We assume C_{ran}, which represents the cost of generating a random number, is equal to 0.02 ms for all the entities (the cost of a concatenation

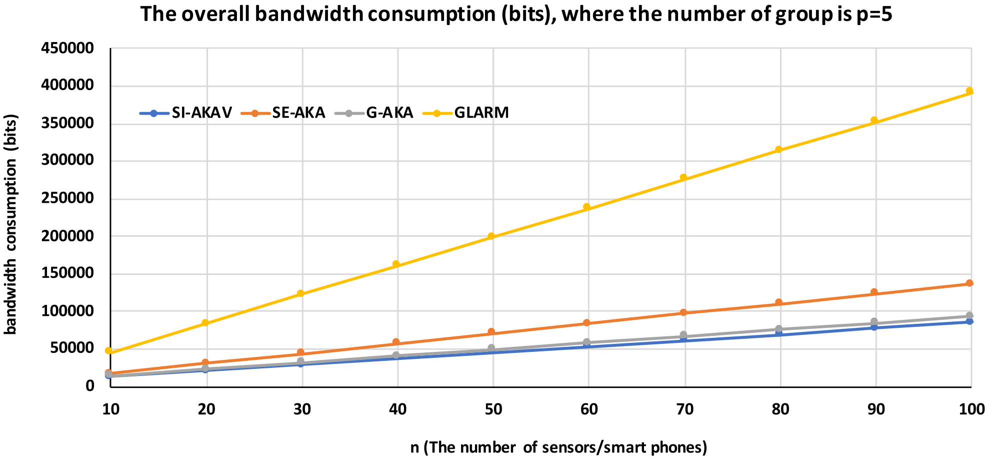

FIGURE 5 Overall bandwidth overhead of SE-AKA,[13] G-AKA,[34] GLARM,[35] and SI-AKAV with $p = 5$ groups

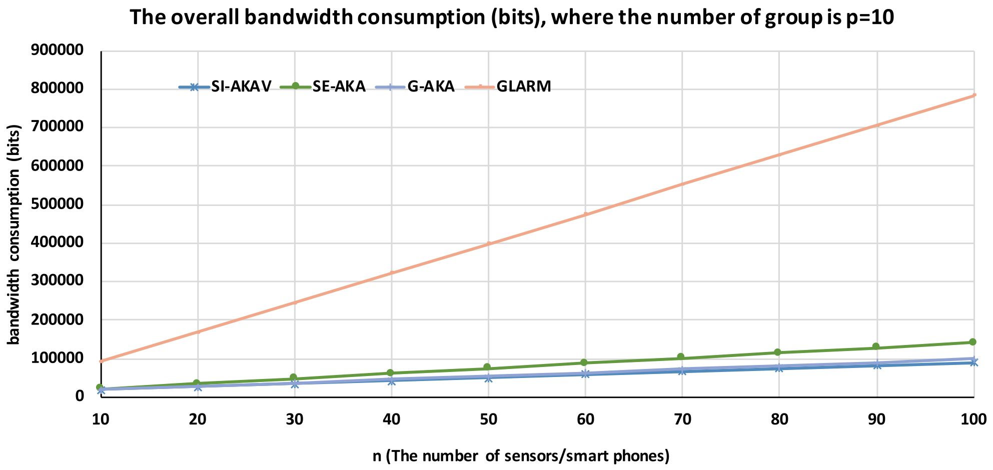

FIGURE 6 Overall bandwidth overhead of SE-AKA,[13] G-AKA,[34] GLARM,[35] and SI-AKAV with $p = 10$ groups

TABLE 5 Computational cost (total over n sensor forming p groups)

Device (ms)	SI-AKAV	SE-AKA[13]	G-AKA[34]	GLARM[35]
CH gateway	$3C_h + C_{\text{ran}} = 0.1268$	$4C_h + 2C_{\text{mul}} = 0.7424$	$4C_h = 0.1424$	$5C_h = 0.1825$
Sensors/gateways	$C_{\text{ran}} + 2C_h = 0.0912$	$3C_h + 2C_{\text{mul}} = 3.2608$	$4C_h = 0.1424$	$4C_h = 0.1424$
RSU/MMU	$C_{\text{ran}} + 2C_h = 0.0912$	$3C_h + 2C_{\text{mul}} = 0.963$	$3C_h = 0.0363$	$C_h = 0.0121$
HSS	$C_{\text{ran}} + C_h = 0.0556$	$2C_h = 0.0712$	$2C_h = 0.0242$	$C_h = 0.0121$
Total	$0.2736p + 0.0912(n - 1)$	$0.0242p + 4.2471n$	$0.0242p + 0.1787n$	$0.14n + 0.06$

Abbreviations: HSS, home subscriber server; RSU, road-side unit; SE-AKA, secure and efficient AKA.

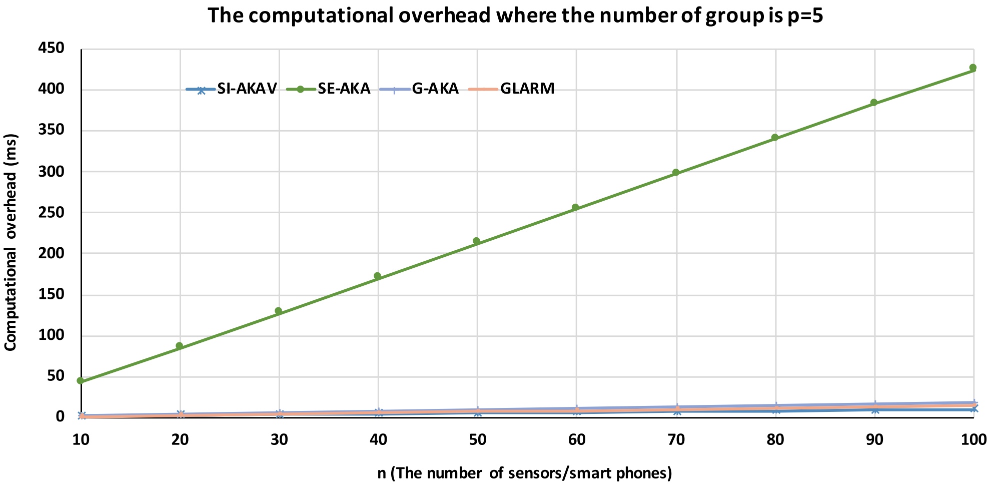

FIGURE 7 Overall bandwidth overhead of SE-AKA,[13] G-AKA,[34] GLARM,[35] and SI-AKAV with $p = 5$ groups

operation is omitted). In the case of SE-AKA, $C_{\text{mul}} = 0.6$ ms denotes the cost of a multiplication operation. Moreover, n represents the number of sensors/smartphones, p stands for the number of groups. We illustrate the total computational cost of SI-AKAV, SE-AKA,[13] G-AKA,[34] and GLARM[35] in Table 5. In addition, we illustrate the computational overhead of SI-AKAV and the existing AKA protocols in Figures 7 and 8. More precisely, SI-AKAV reduces the computation overhead by 41%, 9%, and 8% compared with SE-AKA[13] G-AKA,[34] and GLARM,[35] respectively.

7 | FUTURE RESEARCH DIRECTION

VSN is a recent communication networks paradigm that exploits users' social benefits, which has brought interests not only to academic domain but also to the industry domain for different applications classifying nonsafety-related applications to safety-based applications (eg, collision warning and entertainment). Furthermore, using these applications rely

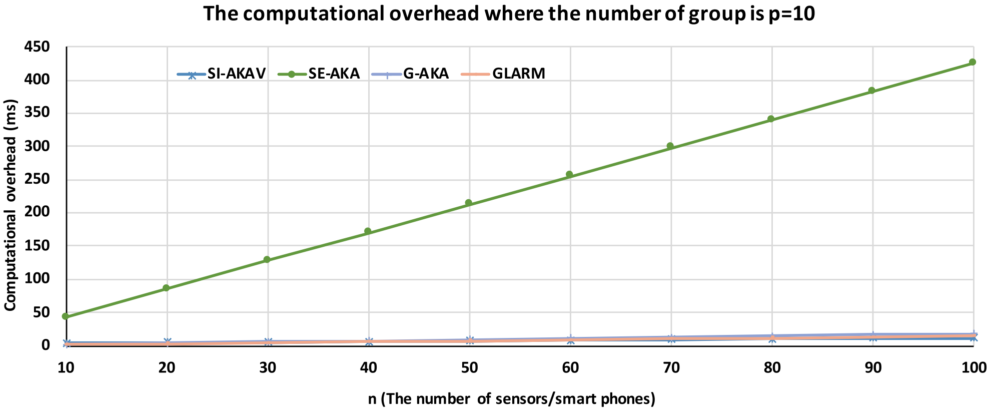

FIGURE 8 Overall bandwidth overhead of SE-AKA,[13] G-AKA,[34] GLARM,[35] and SI-AKAV with $p = 10$ groups

on drivers' information. In this context, if VSNs publish personal information of drivers to other entities, it might be a big concern in terms of privacy. Therefore, privacy, authentication, data integrity, and security are key issues in AKA protocols over VSNs that need to be addressed before VSNs are publicly accepted. In addition, social trust in VSNs is vital to encourage the participants to participate in different applications. After reviewing the recent efforts done in this direction and based on our analysis, we highlight a few future research issues.

- ***Mutual authentication:*** To assure that just a legitimate user is permitted to access resources in AKA protocol over VSNs, the users' identity must be presented. RSUs also need to be authenticated by users to prevent rogue services. In doing so, the users can have secure access to HS services with strong security guarantees.
- ***Key agreement:*** The confidentiality and integrity of transmitted data are guaranteed by creating session keys. This makes an adversary unable to privacy leakage and data corruption during communications.
- ***User anonymity:*** The AKA structure should be able to protect users' original identities in order to prevent users from being recognized by an adversary.

8 | CONCLUSION

In this article, we proposed SI-AKAV, a secure integrated authentication and key agreement protocol for cellular-connected IoT devices in VSNs. SI-AKAV is based on the AKA protocol, which we have enhanced to support group-based authentication of the massive IoT applications. Furthermore, to the best of our knowledge, SI-AKAV considers for the first time an authentication component, as proposed in Reference 13, that plays the role of a proxy and is responsible to manage devices as a group instead of individual entities. In particular, we considered the user's mobile phone (ie, smartphone) as the authentication component that manages the vehicles as a group and facilitate the whole proposed authentication and key agreement protocol. The security analysis shows that SI-AKAV can provide security guarantees, and prevent the various security threats. In addition, our performance evaluation demonstrates its efficiency in terms of computation complexity as well as communication overhead. We can conclude that despite VSNs still being in their infancy, SI-AKAV can enhance the authentication of group vehicles where the research community, automotive industry, and social application providers have a substantial interest in developing them. As future work, we plan to provide an extensive security analysis by using formal verification tools (eg, ProVerif). In addition, we will investigate the group member joining and leaving processes in detail.

ACKNOWLEDGMENT

This work was supported by the European Union's Horizon 2020 Research and Innovation Programme under grant agreement No 830892, project SPARTA, and by the Fonds nationale de recherche (FNR) Luxembourg through the FNR Core Project ByzRT (C19/IS/13691843).

DATA AVAILABILITY STATEMENT

Data sharing not applicable to this article as no datasets were generated or analyzed during the current study.

ORCID

Alireza Esfahani https://orcid.org/0000-0002-2100-1569

REFERENCES

1. Neyja M, Mumtaz S, Huq KM, Busari SA, Rodriguez J, Zhou Z. An IoT-based e-health monitoring system using ECG signal. Paper presented at: Proceedings of the GLOBECOM 2017-2017 IEEE Global Communications Conference, Marina Bay Sands Singapore, Singapore: IEEE; December 4, 2017:1-6.
2. Meneses F, Silva R, Santos D, Corujo D, Aguiar RL. An integration of slicing, NFV, and SDN for mobility management in corporate environments. *Trans Emerg Telecommun Technol*. 2020;31(1):e3615.
3. Xue K, Meng W, Zhou H, Wei DSL, Guizani M. A lightweight and secure group key based handover authentication protocol for the software-defined space information network. *IEEE Trans Wirel Commun*. 2020;19(6):3673-3684.
4. Li J, Xue K, Liu J, Zhang Y, Fang Y. An ICN/SDN-based network architecture and efficient content retrieval for future satellite-terrestrial integrated networks. *IEEE Netw*. 2019;34(1):188-195.
5. Li J, Xue K, Wei DSL, Liu J, Zhang Y. Energy efficiency and traffic offloading optimization in integrated satellite/terrestrial radio access networks. *IEEE Trans Wirel Commun*. 2020;19(4):2367-2381.
6. Standard 3GPP 3rd generation partnership project. technical specification group service and system aspects, 3GPP system architecture evolution (SAE); security architecture; 2019. (Rel 16), V16.1.0.
7. Dahiya A, Gupta BB. A reputation score policy and Bayesian game theory based incentivized mechanism for DDoS attacks mitigation and cyber defense. *Future Generat Comput Syst*. 2021;117:193-204.
8. Cao J, Ma M, Li H, et al. A survey on security aspects for 3GPP 5G networks. *IEEE Commun Surv Tutor*. 2019;22(1):170-195.
9. Parne BL, Gupta S, Chaudhari NS. PSE-AKA: performance and security enhanced authentication key agreement protocol for IoT enabled LTE/LTE-A networks. *Peer Peer Netw Appl*. 2019;12(5):1156-1177.
10. Standard 3GPP 3rd generation partnership project. technical specification group service and system aspects, security architecture and procedures for 5G system; 2018. (Rel. 15), V15.3.1.
11. Dehnel-Wild M, Cremers C. Security Vulnerability in 5G-AKA Draft. Technical Report. . Oxford, UK: Department of Computer Science, University of Oxford; 2018:14-37.
12. Hussain SR, Echeverria M, Chowdhury O, Li N, Bertino E. Privacy attacks to the 4G and 5G cellular paging protocols using side channel information. Paper presented at: Proceedings of the Network and Distributed Systems Security (NDSS) Symposium, California, United States; 2019:24-27.
13. Lai C, Li H, Lu R, Shen XS. SE-AKA: a secure and efficient group authentication and key agreement protocol for LTE networks. *Comput Netw*. 2013;57(17):3492-3510.
14. Cao J, Ma M, Li H. LPPA: lightweight privacy-preservation access authentication scheme for massive devices in fifth generation (5G) cellular networks. *Int J Commun Syst*. 2019;32(3):e3860.
15. Altaf I, Arslan AM, Mahmood K, Kumari S, Xiong H, Khurram KM. A novel authentication and key-agreement scheme for satellite communication network. *Trans Emerg Telecommun Technol*. 2020;e3894.
16. Chen P, Xie Z, Fang Y, Chen Z, Mumtaz S, Rodrigues JJPC. Physical-layer network coding: an efficient technique for wireless communications. *IEEE Netw*. 2019;34(2):270-276.
17. Mishra Anupama, Gupta Neena, Gupta BB. Defense mechanisms against DDoS attack based on entropy in SDN-cloud using POX controller. *Telecommun Syst*. 2021;1–16.
18. Khan S, Muhammad K, Mumtaz S, Baik SW, Albuquerque VHC. Energy-efficient deep CNN for smoke detection in foggy IoT environment. *IEEE Internet Things J*. 2019;6(6):9237-9245.
19. Wang H, Li Z, Li Y, Gupta BB, Choi C. Visual saliency guided complex image retrieval. *Pattern Recogn Lett*. 2020;130:64-72.
20. Yu C, Li J, Li X, Ren X, Gupta BB. Four-image encryption scheme based on quaternion Fresnel transform, chaos and computer generated hologram. *Multimed Tools Appl*. 2018;77(4):4585-4608.
21. Huang D, Misra S, Verma M, Xue G. PACP: an efficient pseudonymous authentication-based conditional privacy protocol for VANETs. *IEEE Trans Intell Transp Syst*. 2011;12(3):736-746.
22. Raya M, Hubaux J-P. Securing vehicular ad hoc networks. *J Comput Secur*. 2007;15(1):39-68.
23. Zeng S, Huang Y, Liu X. Privacy-preserving communication for VANETs with conditionally anonymous ring signature. *Int J Netw Secur*. 2015;17(2):135-141.
24. Zhang J, Zhen W, Xu M. An efficient privacy-preserving authentication protocol in VANETs. Paper presented at: Proceedings of the 2013 IEEE 9th International Conference on Mobile Ad-hoc and Sensor Networks, Dalian, China: IEEE; 2013:272-277.
25. Petit J, Schaub F, Feiri M, Kargl F. Pseudonym schemes in vehicular networks: a survey. *IEEE Commun Surv Tutor*. 2014;17(1):228-255.
26. Sun Y, Feng Z, Hu Q, Su J. An efficient distributed key management scheme for group-signature based anonymous authentication in VANET. *Secur Commun Netw*. 2012;5(1):79-86.
27. Lin X, Sun X, Ho P-H, Shen X. GSIS: a secure and privacy-preserving protocol for vehicular communications. *IEEE Trans Veh Technol*. 2007;56(6):3442-3456.
28. Calandriello G, Papadimitratos P, Hubaux JP, Lioy A. Efficient and robust pseudonymous authentication in VANET. Paper presented at: Proceedings of the 4th ACM International Workshop on Vehicular Ad hoc Networks, Montreal, Quebec Canada: ACM, New York, NY; 2007:19-28.

29. Xi Y, Sha K, Shi W, Schwiebert L, Zhang T. Enforcing privacy using symmetric random key-set in vehicular networks. Paper presented at: Proceedings of the 8th International Symposium on Autonomous Decentralized Systems (ISADS'07), Sedona, AZ: IEEE; 2007:344-351.
30. Zhang C, Lin X, Lu R, Ho P-H, Shen X. An efficient message authentication scheme for vehicular communications. *IEEE Trans Veh Technol*. 2008;57(6):3357-3368.
31. Lai C, Li H, Lu R, Jiang R, Shen X. LGTH: a lightweight group authentication protocol for machine-type communication in LTE networks. Paper presented at: Proceedings of the 2013 IEEE Global Communications Conference (GLOBECOM), Atlanta, GA: IEEE; 2013:832-837.
32. Cao J, Ma M, Li H. GBAAM: group-based access authentication for MTC in LTE networks. *Secur Commun Netw*. 2015;8(17):3282-3299.
33. Huang Y-L, Shen C-Y, Shieh SW. S-AKA: a provable and secure authentication key agreement protocol for UMTS networks. *IEEE Trans Veh Technol*. 2011;60(9):4509-4519.
34. Chen Y-W, Wang J-T, Chi K-H, Tseng C-C. Group-based authentication and key agreement. *Wirel Personal Commun*. 2012;62(4):965-979.
35. Lai C, Lu R, Zheng D, Li H, Shen XS. GLARM: group-based lightweight authentication scheme for resource-constrained machine to machine communications. *Comput Netw*. 2016;99:66-81.
36. Vegni AM, Loscri V. A survey on vehicular social networks. *IEEE Commun Surv Tutor*. 2015;17(4):2397-2419.
37. Yu R, Kang J, Huang X, Xie S, Zhang Y, Gjessing S. MixGroup: accumulative pseudonym exchanging for location privacy enhancement in vehicular social networks. *IEEE Trans Depend Secure Comput*. 2015;13(1):93-105.
38. Cao J, Li H, Ma M, Zhang Y, Lai C. A simple and robust handover authentication between HeNB and eNB in LTE networks. *Comput Netw*. 2012;56(8):2119-2131.

How to cite this article: Esfahani A, Decouchant J, Völp M, Mumtaz S, Konstantin Igorevich K. SI-AKAV: Secure integrated authentication and key agreement for cellular-connected IoT devices in vehicular social networks. *Trans Emerging Tel Tech*. 2021;e4279. https://doi.org/10.1002/ett.4279