Hybrid anonymous message broadcast for VANETs

Andrea Huszti
University of Debrecen
Debrecen, Hungary
huszti.andrea@inf.unideb.hu

Szabolcs Kovács
University of Debrecen and CCLab Ltd.
Debrecen, Hungary
kovacs.szabolcs@inf.unideb.hu

Norbert Oláh
University of Debrecen
Debrecen, Hungary
olah.norbert@inf.unideb.hu

***Abstract*—At present, the number of cars is increasing rapidly. There is a growing need for participants to be able to communicate with each other in order to increase the efficiency of transport and the safety of vehicles and pedestrians. The Intelligent Transportation System recommends the use of Vehicular Ad-hoc networks for this purpose. A cryptographic protocol is proposed, where eligible vehicles can authentically and anonymously report road conditions (e.g. traffic jams, accidents, etc.). Our proposed solution is hybrid, globally it is PKI-based, locally identity-based cryptography is applied and two lists are handled. It takes advantage of bilinear pairings, the devices do not store the master secret key, provides batch verification of messages, moreover the anonymity of the senders can be revoked. We also demonstrate the security analyses of the protocol in applied pi calculus with the help of the ProVerif tool. We show that the proposed protocol provides mutual authentication for parties and token secrecy during the Communication Setup, moreover anonymous message authentication in phase of Incident Report. We have also implemented the proposed protocol in Python and demonstrated that it is suitable for practice.**

***Index Terms*—Identity-Based Cryptography, Anonymity Revocation, VANET**

I. Introduction

The Vehicle Ad-Hoc Network (VANET) is a system developed for short-range communication with a distance between 100 and 300 meters. This can be Vehicle-to-Vehicle (V2V) or Vehicle-to-Infrastructure (V2I) communication. The main purpose of creating VANET was to prevent accidents. It has a number of applications to increase human safety and assist drivers in downtown transportation. The rate of accidents is increasing day by day in parallel with the number of vehicles, thus it is getting more and more important to provide high security solutions for VANETs. Attackers can intercept, tamper, modify or replay the transmitted messages in the wireless network communication environment, which risks the security and reliability of VANETs [1]. Several solutions have been proposed in the scientific literature. These are based on various security requirements, such as authentication, secrecy or anonymity. Authentication ensures the legitimacy of entities in VANETs. If an incident occurs, the legality of each submitter's identity and the integrity of the incident's data must be verified. Since adversaries can collect any information on the network which are broadcasted by vehicles, they can obtain the route of a vehicle and violate the personal privacy of the driver over time [2]. In order to prevent being tracked, vehicles need to broadcast security messages anonymously. Secure, efficient anonymous authentication and communication factors play a prominent role in the development of adequate VANET systems.

The presented research has been supported by the SETIT Project (no. 2018-1.2.1-NKP-2018-00004), which has been implemented with the support provided by the National Research, Development and Innovation Fund of Hungary, financed under the 2018-1.2.1-NKP funding scheme. Project no. TKP2020-NKA-04 has been implemented with the support provided from the National Research, Development and Innovation Fund of Hungary, financed under the 2020-4.1.1-TKP2020 funding scheme.

A. Related Work

For a traditional PKI, devices must store certificates and revocation lists in addition to keypairs. Lu et al. introduced a PKI system [3] that builds on blockchains. To initialize the system, entities must generate keys and communicate with leading organizations, which requires a secure communication channel. In addition, each device must store three lists (in this case blockchains): the valid certificates, the sent messages, and the revoked public keys lists. Another proposal that is based on a mechanisms similar to PKI is the scheme of Vijayakumar et al. in [4], which contains a trusted authority (TA) who manages keys and vehicle licenses. They apply batch authentication of vehicles, however, the IEEE Standard for Wireless Access in Vehicular Environments [5] recommends to change pseudonyms and certificates frequently for the purpose of privacy protection. Therefore, the vehicles have to communicate with TA, which makes the system inefficient due to high computational overhead and communication costs and it cannot ensure that high-speed vehicles receive new certificates in time. Since certificates must be updated from time to time due to the finite validity period for schemes [3], [4] secure channels and certificate management are necessary.

In the identity-based method, each device only needs to store the public parameters, its own ID, and its associated secret key. The public key consists of some of the participant's identification information (e.g. license plate number concatenated with a time stamp). No certificates are required and there is no cost of storing and handling them. The secret key of the participants is generated and distributed by the TA. For VANET systems, the secret key is stored by the On-board Unit (OBU) and can be loaded offline or online. In the latter case, it is necessary to build a secure channel. In our scheme long-time identity-based keys are generated for the participants, if a secret key is compromitted, a new public key with a new timestamp is generated with its secret key loaded offline and the old public key is put on a revocation list.

Debiao He et al. recommended an identity-based authentication scheme [6] that does not include bilinear pairing. The reason for this is that bilinear pairing requires more resources than symmetric cryptographic primitives. Messages are sent with anonymous IDs that each device generates for itself before each message. Verification requires the knowledge of the master's secret key. Unfortunately, when any of the vehicles is compromised it leads to entire system being compromised since they contain all parameters of the system, including the master secret key. Our proposed solution eliminates this problem as vehicles do not have to store the master secret key. Thus, damage to a device does not affect the entire system. The master secret key is stored by TA.

In [7] an identity-based signature scheme (CPAS) is proposed for reducing the computation cost in anonymous authentication. The disadvantage of this proposition is that CPAS does not possess an effective revocation mechanism for illegal vehicles. When the vehicles are compromised, the system of VANET cannot ignore the threats.

Wang and Yao's solution in [8] combines the management of the PKI revocation list and the authentication mechanism of the identity-based environment. They suggest that certificates should be provided for long-term keys which the devices use for mutual authentication for each RSU managed domain that results in certificate management and revocation list verification. Anonymity of the users can be revoked anytime by TA. In our scheme anonymity revocation is accomplished by the TA and the RSU reported the adversarial vehicle, hence even TA alone cannot determine the real identity.

VANETs systems ([9],[10],[11]) which are based on group signatures. An advantage of these solutions that they provide anonymous authentication for group members, they can create signatures without revealing their real identity. Such schemes need to implement an efficient key management mechanism that gives significant computational overhead.

B. Our Contribution

We propose a hybrid pseudonym-based anonymous message broadcast scheme for VANETs. Locally the protocol is based on identity-based cryptography to save certificate management overhead. In our case a public key is the hash of the licence plate (in case of the vehicle) or GPS coordinate for RSUs and the current timestamp. Public keys are long term, a Revocation List is handled by TA to store public keys of compromised secret keys. Our protocol is globally PKI-based, that means public keys of TAs including system parameters are managed by certificates assuming that in practice a network of TAs manages the keypairs. Our scheme protects sender anonymity and message unlinkability for vehicles, hence drivers' traffic habits, routes are kept secret to protect their privacy. Besides Revocation Lists an Anonymized User List is also maintained by the Roadside Units and the Trusted Authorities to be able to revoke vehicles anonymity in case of malicious messaging. Malicious users public key is put on the Revocation List. During the protocol design minimizing computational costs for vehicles is considered to increase communication efficiency. The cost of report message submission is only one hash calculation and one scalar multiplication besides precomputations and OBUs store only one list, the Revocation List. Efficiency of the protocol is increased with the possibility that report messages can be verified in batch. We also provide a security analysis in applied pi calculus using the Proverif tool. We show that the proposed protocol possesses mutual entity authentication during Communication Setup, secrecy of authorized secret values, moreover, we consider sender anonymity, message unlinkability, non-repudiation of malicious messages and anonymity revocation as well. Formal security analysis is given only in [6], none of the other mentioned schemes has.

II. Preliminaries

In 1984, Shamir formulated the properties of an identity-based encryption system [12]. An identity-based encryption scheme is specified by four randomized algorithms: *setup, extract, encrypt* and *decrypt*:

- **Setup**: takes a security parameter, then returns the master secret key and the system parameters ($params$). The system parameters are publicly known but only the Private Key Generator (PKG) will know the master secret key.
- **Extract**: takes as input the $params$ and the master secret key, and an arbitrary $ID \in 0, 1^*$ then returns a private key *d*. The ID, the public key, is a unique information about the user and the *d* is the corresponding private key extracted from the public key.
- **Encrypt**: takes as input $params, ID$, and $M \in \mathbb{M}$, the finite message space and returns a ciphertext $C \in \mathbb{C}$, the finite ciphertext space.
- **Decrypt**: takes as input $params, ID, C \in \mathbb{C}$, and a private key d and returns $M \in \mathbb{M}$.

These algorithms must satisfy the standard consistency constraint, namely when d is the private key generated by algorithm $Extract$ when it is given ID as the public key, then $\forall M \in \mathbb{M} : Decrypt(params, ID, C, d) = M$, where $C = Encrypt(params, ID, M)$.

An important building block of identity-based cryptography is the bilinear pairing. Let us review the definition of the admissible bilinear map [13]. Let G_1 and G_2 be two groups of order q for some large prime q. A map $e : G_1 \times G_1 \rightarrow G_2$ is an admissible bilinear map if satisfies the following properties:

1) Bilinear: We say that a map $e : G_1 \times G_1 \rightarrow G_2$ is bilinear if $e(aP, bQ) = e(P, Q)^{ab}$ for all $P, Q \in G_1$ and all $a, b \in Z$.
2) Non-degenerate: The map does not send all pairs in $G_1 \times G_1$ to the identity in G_2. Since G_1, G_2 are groups of prime order, if P is a generator of G_1 then $e(P, P)$ is a generator of G_2.
3) Computable: There is an efficient algorithm to compute $e(P, Q)$ for any $P, Q \in G_1$.

We should mention that bilinearity can be restated to for all $P, Q, R \in G_1$ $e(P + Q, R) = e(P, R)e(Q, R)$ and $e(P, Q + R) = e(P, Q)e(P, R)$. We can find G_1 and G_2 where these properties hold. The Weil and Tate pairings prove the existence

of such constructions. Typically, G_1 is an elliptic-curve group and G_2 is the multiplicative group of a finite field.

III. Protocol

A. Participants

Trusted Authority is the trusted third-party with high computing resources and responsible for defining system parameters, the public and secret keys in the initialization phase. It loads the data offline into the On-board Units (OBU). The TA is the only authority that stores all the valid, public keys.

Roadside Units (RSU) are devices along the road that receive messages and transmit them when needed. Every RSU has its own domain to supervise. They are responsible inter alia for the Communication Setup, i.e. for the authentication of the incoming OBUs.

On-board Units (OBU) are tamper-proof devices built in the vehicles. Through them the vehicles are able to communicate in the network.

B. Phases

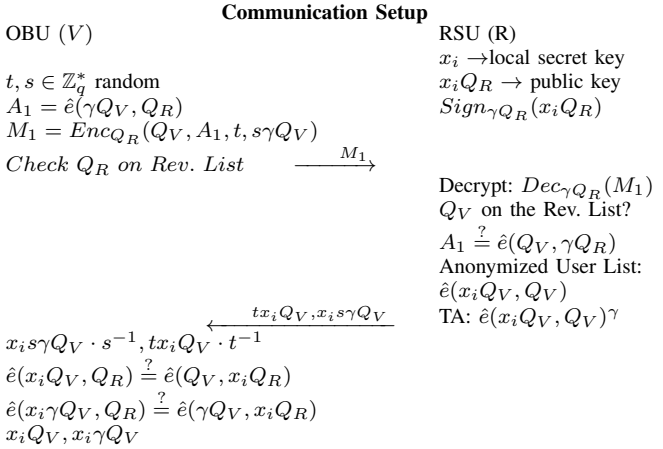
The protocol consists of four parts. The first part is Initialization, during which system parameters, public IDs, secret keys are generated and assigned to participants. The second part is Communication Setup, where vehicles arriving to the domain of the given RSU register, i.e. they are given their authorized ID and authorized secret key. A value generated from the OBU's real identifier is also added to the Anonymized User List, which is later used for the anonymity revocation. The third phase of the protocol is the report of road conditions, accidents, traffic jams, and so on., which is called Incident Report. In this phase vehicles broadcast their announcements to surrounding participants, which can be vehicles or the RSU of the given domain. The fourth part is the Malicious User Management phase. The anonymity of the malicious messengers is revoked and their ID is added to the Revocation List.

Initialization

During initialization, participants' identity-based key pairs and system parameters are generated. In the first step, TA generates system parameters: groups G_1, G_2, bilinear map $e : G_1 \times G_1 \rightarrow G_2$, generator element P of G_1, hash function $H : \{0,1\}^* \rightarrow G_1$. All parameters are made public. TA randomly selects a master secret key $\gamma \in Z_q^*$ that is kept secret, then calculates and publishes the public parameters $(P, \gamma P)$ via PKI certificates. In addition to system parameters and the master secret key, TA also generates an identity-based key pair for every participant. It creates an ID $(Q_V = H(ID_V||T), Q_R = H(ID_R||T))$ for each vehicle and RSU, which is the hash of the license plate for vehicles, GPS coordinate for RSUs, and the current timestamp. This ID will be their public key. The secret keys $(\gamma Q_V, \gamma Q_R)$ are calculated with the master secret key. System parameters and their private key are loaded offline into the OBUs. The two lists, one for the revoked identifiers, the Revocation List, and one for the authenticated users, the Anonymized User List, are initialized here as well.

Communication Setup

In this phase, eligible vehicles are given the authorized ID required for communication and a value required to revoke anonymity.RSU needs to check the authenticity of the sender, i.e., the secret key received from the TA. The OBU and the RSU also need to check whether the real identifier is missing from the Revocation Lists. The OBUs store a Revocation List which contains the corrupted RSUs and the Revocation List of RSUs contains the corrupted OBUs. If these conditions above hold, then the vehicle Q_V is eligible for sending messages, hence will have an authorized ID: $x_i Q_V$ and an authorized secret key: $x_i \gamma Q_V$. In the case of message broadcast, the receivers (vehicles or RSU) verify the existence of a valid authorization ID of the sender.



After the successful authentication the RSU and the TA add the user to the Anonymized User List. RSU sends $e(x_i Q_V, Q_V)$ to the list, and TA modifies it to $e(x_i Q_V, Q_V)^\gamma$. Since TA stores the list of vehicle IDs, RSU and TA together are able to revoke the anonymity of the senders via exhaustive search. The OBU generates two random values $t, s \in \mathbb{Z}_q^*$ that are required to assure confidentiality of the authorized ID and authorized secret key to avoid active attacks (e.g. impersonation and replay attacks). The message sent contains its own ID (Q_V), A_1, the random value *t*, and $s\gamma Q_V$ concatenated and encrypted with Boneh and Franklin encryption using the RSU public key. The RSU decrypts the message with its own secret key (γQ_R), verifies the authenticity of the OBU, i.e. whether $A_1 = \hat{e}(Q_V, \gamma Q_R)$ and whether it is on the Revocation List. It then calculates and returns $tx_i Q_V$ and $x_i s\gamma Q_V$. The OBU verifies the authenticity of the values obtained and then stores the authorized ID and the authorized secret key.

Incident Report

In this phase, the vehicles anonymously notify the surrounding vehicles and the RSU whenever an incident occurs. The authenticity of the message, the sender's eligibility and the revocability of sender anonymity are checked. To achieve anonymity and unlinkability vehicles attach a self-generated anonymous ID, a pseudonym (A_{ID}), to the message. The pseudonym is the product of the vehicle ID (Q_V) and a random scalar $a \in Z_q^*$ generated by the vehicle. The anonymity can

only be revoked by the Roadside Units together with the TA. The following figure shows the details of the message sent to the RSU. During messaging, every participant in the domain will receive the message, and they can verify it using their own public and authorized secret keys.

The receiver first checks the timestamp T, then calculates bilinear maps and verifies if the sender has a valid authorized pseudonym and whether the message is altered. Taking advantage of the bilinearity of the bilinear map, the integrity of the message M is verified and the source of the message A_2 is checked whether it is the owner of A_{ID}. Due to bilinear maps the same standardized messages from several vehicles sent in the same hour can be batched and verified. The RSU also checks if bilinear map of values of A_3 and A_{ID} are listed in the Anonymized User List, ensuring that anonymity can be revoked to exclude malicious attackers. In the case of the last check is not met, the RSU sends a signed message to the other OBUs.

Incident report

OBU (V)	RSU (R)
$a, b \in \mathbb{Z}_q^*$ random	
$A_{ID} = aQ_V$	
$A_1 = ax_iQ_V$	
$A_2 = bH(M\|\|T) + a\gamma Q_V$	
$A_3 = a^{-1}x_i\gamma Q_V$	
$\xrightarrow{A_{ID},A_1,A_2,A_3,bP,M,T}$	
	Check: T
	$\hat{e}(A_{ID}, x_iQ_R) \stackrel{?}{=} \hat{e}(A_1, Q_R)$
	$\hat{e}(A_2, P) \stackrel{?}{=} \hat{e}(A_{ID}, \gamma P) *$
	$\hat{e}(H(M\|\|T), bP)$
	$\hat{e}(A_3, A_{ID})$ on the An. User List?

Malicious User Management Users are able to report if they become aware of suspicious behaviour. In such cases, the RSU decide the fate of the reported user. OBU sends A_{ID}, A_1, A_2, A_3 to the RSU. The RSU checks the validity of A_3 in the phase of the Incident report. In the case of a malicious user message, RSU and TA applying their secret values x_i and respectively calculate $\hat{e}(A_{ID}, A_3)^{x_i^{-1}\gamma^{-1}}$, that is $\hat{e}(Q_v, Q_v)$. TA determines Q_V by an exhaustive search and it is added to the Revocation List. The Revocation List is shared by the RSUs and OBUs, sending an update to each other in the event of a change.

IV. Security Analysis

During the security analysis the fulfilment of the security requirements are examined. In the various phases of the protocol several messages (reports and setup requests) are sent. In the case of message broadcast it is of crucial importance to ensure that both the senders and the content of the messages are reliable, since there are several relevant attacks (e.g. impersonation attack) that can pose a security threat to the systems. In this section we demonstrate the security analysis of the Communication Setup and the Incident report phases of the proposed protocol. After defining the security requirements (mutual authentication, message integrity, validity of the source of the message, etc.) and the adversarial model, we provide the analysis in applied pi calculus with the help of the Proverif tool.

A. Security Requirements

Firstly, we collect and define the relevant security requirements. The requirements include basic properties such as secrecy, and entity authentication. Moreover, we consider sender anonymity, message unlinkability, non-repudiation of malicious messages, anonymity revocation as well.

In both phases the anonymity of vehicles should be assured.

1) Sender anonymity, message unlinkability
The protocol must provide the sender's anonimity (e.g. GDPR requirements for data anonymization), the senders and their messages should not be linked. Moreover, the messages should not reveal any information about the submitters. The adversary should not be able to link messages from the same sender, either. Traffic habits and routes could provide information about the submitter.

We require the following properties for the Communication Setup.

2) Authentication of both parties
   - Authentication of OBU: Adversaries should not be able to impersonate a legal OBU. Without secure authentication attackers are able to gain legal OBUs' authorized IDs from the RSU.
   - Authentication of RSU: Adversaries should not be able to impersonate a legal RSU. Impersonating an RSU the adversary is able to issue authorized IDs to illegal OBUs.
3) Secrecy of the authorized ID and authorized secret keys
The authorized ID is a confidential datum, it is issued only for eligible participants. An adversary should not have any information about it. Adversaries with valid authorized IDs are able to submit incident reports successfully. Since the local secret of RSU is changed every day, the generated authorized ID of the on board units is also changed regularly.

The Incident Report provides the following properties.

4) Authenticity and data integrity of messages
The receiver participants must be sure that the source of a message is valid, *i.e. the sender vehicle is eligible for report submission*, moreover the attackers must not able to modify or forge messages.
5) Anonymity revocation, non-repudiation of malicious messages
Anonymous messaging allows malicious behaviour of authorized vehicles. To limit possible abuses of anonymity, authorized participants should be able to revoke vehicles anonymity if it is necessary. The sender vehicle must not be able to deny its malicious incident reports.

B. Adversarial model

In our security analysis we consider passive and active attackers, which listen to the channels and try to impersonate legal participants and forge valid messages. Consequently, the Dolev-Yao model is considered. In the Dolev-Yao model an adversary posseses the following properties:

1) The adversary has complete control over the entire network.
2) He acts as a legitimate user, can intercept and compose any message and is limited by the constraints of the used cryptographic methods.
3) The adversary can initiate the protocol with any party, and can be a receiver to any party.

We also defined the trust model, we assume that participants do not reveal their secret keys and RSU does not reveal the real identity of the vehicles during the communication.

C. Applied π Calculus

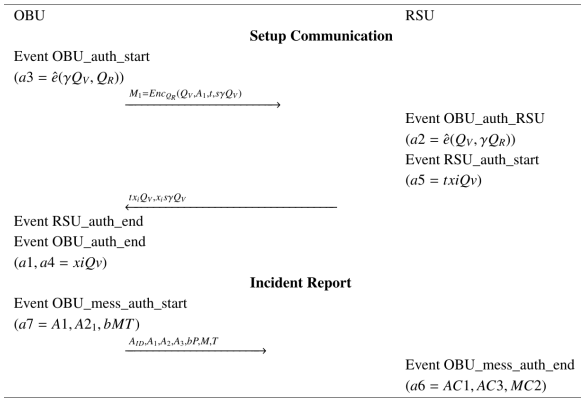
We applied the applied π calculus ([14]) and the ProVerif tool for security analysis. ProVerif handles input files encoded in a variant of the applied π calculus which supports types. We give the formalization for operations and cryptographic primitives. For details please check [15]. We formalize two phases of the protocol and differentiate three processes as follows. In the main process of the protocol, identification numbers, secret keys, public keys are generated for the participants and other parameters are given. Two sub-processes represent the OBU's and the RSU's protocol steps in the Communication Setup and the Incident Report phases. We consider an unbounded number of sub-processes running in parallel and model the interactions between the OBU and the RSU.

D. Security Properties

ProVerif applies queries for security evaluations which can be a correspondence or a fact. When we use *reachability*, we query whether a term remains secret for the attacker ($query\ attacker : m$). A *correspondence* is a form of $F \Longrightarrow H$, which means if F holds, then H also holds. In the model we define events constituting important stages in our protocol and test whether event b had been previously executed if event a was executed. The $query\ evinj\ :\ a(x,y) \Longrightarrow evinj\ :\ b(y,z)$. means that for each occurrence of the event $a(x,y)$, there is a *distinct* earlier occurrence of the event $b(y,z)$ for some z. Further information can be found in [16]. In order to run the security queries, six events are defined. In the Communication Setup we apply injective correspondences for the mutual authentication of the OBU and the RSU. We prove OBU authentication with the nested correspondence:

query a1:nonce,a2:E, a3:nonce;
inj-event(OBU_auth_end(a1)) ==>
(inj-event(OBU_auth_RSU(a2)) ==>
inj-event(OBU_auth_start(a3))).

We show with a simple injective correspondence the authentication of the RSU



query a4:E,a5:E; inj-event(RSU_auth_end(a4)) ==> inj-event(RSU_auth_start(a5)).

In the Incident Report phase we use the following basic correspondence assertion for the OBU's message authentication in the incident report:

query a6:E,a7:E; event(OBU_mess_auth_end(a6)) ==> event(OBU_mess_auth_start(a7)).

Furthermore, secrecy of the exchanged authorized IDs are also evaluated with the query *query attacker(xiQv). query attacker(xiγQv).* by testing whether the x_iQ_v, $x_i\gamma Q_v$ can be accessed by the adversary. All the queries above return with the value true, therefore the mutual authentication of OBU and RSU and secrecy of the authorized ID and the authorized secret key hold in our model, moreover all the verifications hold in the Incident Report. Consequently, the report message is not altered.

E. Sender anonymity, message unlinkability, non-repudiation of malicious messages, anonymity revocation

In the Communication Setup phase an adversary listening to the channel should not be able to determine the ID of the OBU, otherwise the location of the vehicle is revealed. Messages $M_1, tx_iQ_V, x_is\gamma Q_V$ do not give information about Q_V. M_1 is a Boneh-Franklin ciphertext. An attacker is not able to distinguish this encrypted message from a random value [17]. To provide sender anonymity in the Incident Report phase pseudonyms (aQ_V) and authorized pseudonyms (ax_iQ_V) are sent. Since for each report message a fresh, secret random value $a \in Z_q^*$ is generated, the pseudonyms and authorized pseudonyms are different and not linkable. After reporting the incident, the RSU checks whether the anonymity of the OBU can be revoked, *i.e.* whether $e(A_3, A_{ID})$ is on the Anonymized User List. Value $e(Q_V, Q_V)$ calculated by RSU and TA is uniquely mapped to Q_V, hence non-repudiation of malicious messages holds.

V. Performance Evaluation

The parameters used for the performance evaluation could be found in [15]. The additional parameters were generated at runtime, and in each case we used a random number generator,

their specified size was 128 bits for the PC and Raspberry Pi. To select the devices, we must first define the environment in which they will operate and their primary role. From an automotive perspective, we distinguish two main directions: autonomous and connected vehicles and also we can also talk about downtown and out-of-town (highway) traffic. For out-of-town traffic, we need devices that can send and receive messages in a fraction of a second. During development, we analysed the code on a personal computer (3.4-3.9 GHz single-core speed). The results obtained here approximate the assumed performance of an RSU. In the automotive industry Raspberry Pi is often chosen for IoT projects, and it also has a higher computing capacity. The Raspberry Pi 4 already has a 1.5 GHz processor, up to 8GB of RAM and fully functional operating systems. With this performance, it would already hold its own, even for autonomous vehicles. In the event of an emergency, it is able to send a message in a fraction of a second to inform other vehicles, and it can also process and respond to the information received in a few tenths of a second. In the Incident Report phase a lot of computation could be done as precomputation to make the sending even faster. The Malicious User Management processing part includes the verification of the exposure message, then the exhaustive search in the Anonymized User List. The size of the list affects the computational time.

	PC	RasPi 4
Comm. setup - Authorized ID request (OBU)	0.0199 s	0.1453 s
Comm. setup - User authentication (RSU)	0.0297 s	0.1949 s
Comm. setup - Authorized ID confirmation (OBU)	0.0179 s	0.1333 s
Incident report - send	0.0086 s	0.0593 s
Incident report - receive	0.0281 s	0.2076 s

VI. Conclusion

In this paper we propose a new hybrid anonymous broadcast message scheme based on identity-based cryptography for VANETs. Our protocol takes advantage of bilinear pairings, the devices do not store the master secret key, only the revocation lists is downloaded on OBUs, moreover, the anonymity of the sender can be revoked. We show with formal analysis that the protocol is secure. It is implemented in Python and the performance analysis shows that the proposed scheme is robust and efficient. However, some improvements needs to made in the future, such as using blockchains for the revocation and anonymity lists.

References

[1] J. Feng, N. Liu, J. Cao, Y. Zhang, and G. Lu, "Securing traffic-related messages exchange against inside-and-outside collusive attack in vehicular networks," *IEEE Internet of Things Journal*, pp. 9979–9992, 2019.

[2] A. Boualouache, S.-M. Senouci, and S. Moussaoui, "A survey on pseudonym changing strategies for vehicular ad-hoc networks," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 1, pp. 770–790, 2017.

[3] Z. Lu, W. Liu, Q. Wang, G. Qu, and Z. Liu, "A privacy-preserving trust model based on blockchain for vanets," *IEEE Access*, vol. 6, pp. 45 655–45 664, 2018.

[4] P. Vijayakumar, V. Chang, L. J. Deborah, B. Balusamy, and P. Shynu, "Computationally efficient privacy preserving anonymous mutual and batch authentication schemes for vehicular ad hoc networks," *Future generation computer systems*, vol. 78, pp. 943–955, 2018.

[5] "Ieee standard for wireless access in vehicular environments–security services for applications and management messages," *IEEE Std 1609.2-2016 (Revision of IEEE Std 1609.2-2013)*, pp. 1–240, 2016.

[6] D. He, S. Zeadally, B. Xu, and X. Huang, "An efficient identity-based conditional privacy-preserving authentication scheme for vehicular ad hoc networks," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 12, pp. 2681–2691, 2015.

[7] K.-A. Shim, "\cal cpas: an efficient conditional privacy-preserving authentication scheme for vehicular sensor networks," *IEEE Transactions on Vehicular Technology*, vol. 61, no. 4, pp. 1874–1883, 2012.

[8] S. Wang and N. Yao, "Liap: A local identity-based anonymous message authentication protocol in vanets," *Computer Communications*, vol. 112, pp. 154 – 164, 2017.

[9] D. Boneh and H. Shacham, "Group signatures with verifier-local revocation," in *Proceedings of the 11th ACM conference on Computer and communications security*, 2004, pp. 168–177.

[10] Y. Jiang, S. Ge, and X. Shen, "Aaas: An anonymous authentication scheme based on group signature in vanets," *IEEE Access*, vol. 8, pp. 98 986–98 998, 2020.

[11] B. K. Chaurasia and S. Verma, "Conditional privacy through ring signature in vehicular ad-hoc networks," in *Transactions on computational science XIII*. Springer, 2011, pp. 147–156.

[12] A. Shamir, "Identity-based cryptosystems and signature schemes," in *Advances in Cryptology*, G. R. Blakley and D. Chaum, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 1985, pp. 47–53.

[13] D. Boneh and M. Franklin, "Identity-based encryption from the weil pairing," in *Advances in Cryptology — CRYPTO 2001*, J. Kilian, Ed. Berlin, Heidelberg: Springer Berlin Heidelberg, 2001, pp. 213–229.

[14] M. Abadi and C. Fournet, "Mobile values, new names, and secure communication," *Acm Sigplan Notices*, vol. 36, no. 3, pp. 104–115, 2001.

[15] "Github source," https://github.com/kovacssz94/VANET/tree/main/.

[16] B. Blanchet, "Proverif: automatic cryptographic protocol verifier user manual for untyped inputs," 2012.

[17] R. Canetti, S. Halevi, and J. Katz, "Chosen-ciphertext security from identity-based encryption," in *Advances in Cryptology - EUROCRYPT 2004*. Springer Berlin Heidelberg, 2004, pp. 207–222.