SecVanet: provably secure authentication protocol for sending emergency events in VANET

2023 14th International Conference on Information and Knowledge Technology (IKT) | 979-8-3503-4941-2/23/$31.00 ©2023 IEEE | DOI: 10.1109/IKT62039.2023.10433027

Seyed Amir Mousavi
Department of Computer
Ferdowsi University of Mashhad
Mashhad, Iran
amirmousavi@mail.um.ac.ir

Mohammad Sadegh Sirjani
Department of Computer
Ferdowsi University of Mashhad
Mashhad, Iran
mohammadsadegh.sirjani@mail.um.ac.ir

Seyyed Javad Bozorg Zadeh Razavi
Department of Computer
Ferdowsi University of Mashhad
Mashhad, Iran
s.j.bozorgzadehrazavi@mail.um.ac.ir

Morteza Nikooghadam
Department of Computer Engineering, Imam Reza International University,
Mashhad, Iran
m.nikooghadam@imamreza.ac.ir

***Abstract*— Recently, the number of accidents resulting in irreparable damages like death has risen due to the increased number of vehicles worldwide. Vehicular ad hoc network (VANET) is a new technology for enhancing road safety, reducing traffic load, and providing emergency services. Vehicles can send warnings in a network to announce accidents and seek help from emergency vehicles. Security and privacy are now significant concerns in developing vehicular ad hoc networks despite the many advantages of VANET. The communication channel in this network is public and insecure, so there is concern about eavesdropping, message manipulation, and impersonation, which creates significant risks. For this reason, a safe and efficient protocol is proposed in this article to ensure data security in VANET. The security of the proposed protocol has been proven by the Scyther tool. The security analysis performed on the protocol also shows that the proposed protocol is resistant to many attacks and meets various security requirements. We also evaluated the performance of the proposed protocol in terms of computational complexity and showed that the proposed scheme has less computational complexity than similar schemes.**

Keywords*— Authentication, Privacy, Key agreement, VANET, Scyther Tool

I. INTRODUCTION

With the continuous urban development and economic progress, intercity road transportation is constantly evolving and creating new challenges [5]. The rapid growth of the transportation industry has increased the number of vehicles. It significantly increases the efficiency of people's travel. Technologies such as 5G are discussed to facilitate communication in vehicular ad hoc networks (VANET) [6]. During this time, some impatient people may violate the traffic rules, leading to an accident.

As can be seen in Figure 1, When accidents occur, drivers may be injured, and people's property may be at risk. It is critical at this point that emergency vehicles (EVs) must be dispatched to the scene. The law authorizes Emergency vehicles to pass quickly to perform specific tasks under certain conditions. Examples of such vehicles include ambulances, fire trucks, and police cars.

In recent years, there have been numerous reports of emergency vehicles being delayed in arriving at the scene of an accident due to incorrect information, leading to loss of life due to lack of timely treatment. In addition, some traffic accidents are caused by the theft of electric vehicles by thieves or illegal use, which leads to harmful social effects [3][4]. In general, VANETs present several security challenges, which prompt many researchers to focus on securing the data exchanged in this network [1][2].

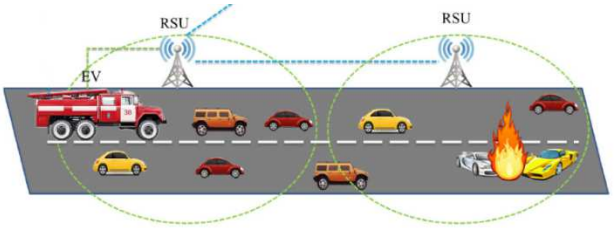

Fig. 1. System architecture.

Due to the vulnerability of the public channel (Internet), the information transmitted through it can be intercepted, eavesdropped on, and manipulated by attackers. For example, a malicious attacker may impersonate ordinary vehicles and falsely report an accident, causing emergency vehicles to be dispatched to the scene. This causes chaos in assisting these vehicles, which have had an accident.

In vehicular ad hoc networks, the reliability of the messages sent between the vehicles involved in the accident and the rescue vehicles is of great importance because sending invalid messages can endanger the security of the vehicles in the network.

Therefore, to prevent such attacks, verifying the vehicle sending the message's identity is a suitable solution to reduce these risks. For this reason, many researchers have recently tried to provide protocols that meet the security needs of automotive contingency networks and are also resistant to various attacks such as impersonation attack, replay attack, password guessing attack, insider attack, and stolen verifier attack.

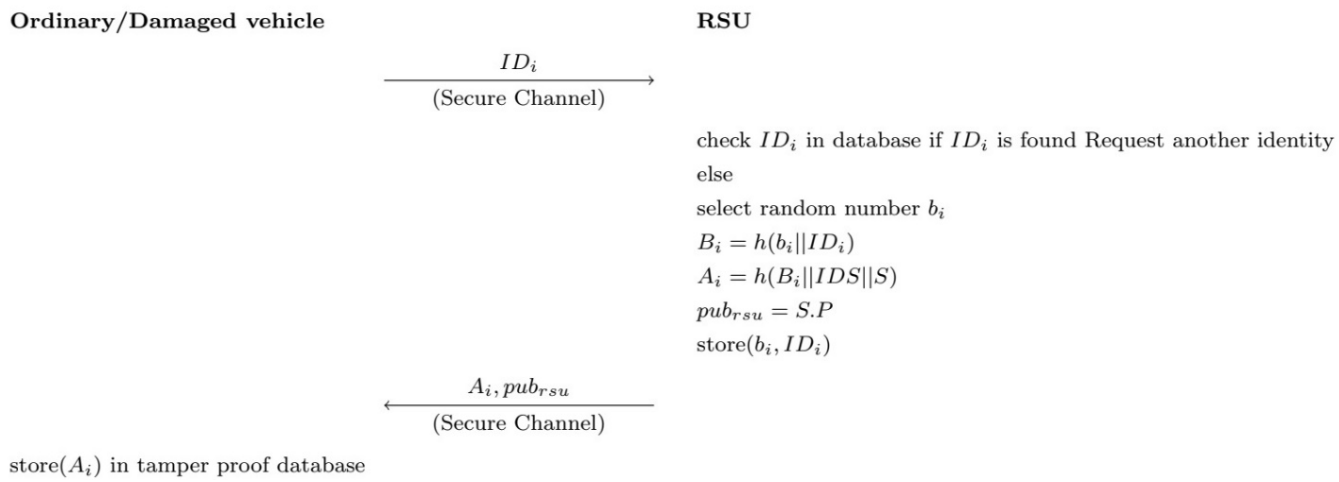

Fig 2. Ordinary/Damaged vehicles registration phase

Shao et al. presented an authentication and key agreement scheme for VANETs [7]. After some time in the article [8], it was proved that the scheme of Shao et al. could not provide the security requirement of forward and backward security, and the proposed scheme of Shao et al. could only provide some security aspects.

Song et al. [9] presented a three-party authentication and key agreement scheme based on bilinear pairing, which aimed to Privacy-Preserving in vehicular ad hoc network. In 2018, Wang et al., after reviewing Song et al.'s scheme, claimed that their scheme was not secure and presented an improved scheme with much overhead [10]. Chen et al. suggested a scheme of sharing information between vehicles, with the condition that each vehicle in the network must be reliable [11].

As far as we know, there is still no authentication and key agreement scheme at the time of the incident in VANET that can consider all security aspects and perform well. Therefore, in this paper, an authentication and key agreement protocol presented such a scenario that can consider all aspects of an emergency vehicular ad hoc network.

II. OUR PROPOSED SCHEME

In this section, we will introduce the proposed protocol. The proposed protocol includes two phases of registration, authentication and key agreement, which will be explained in detail below. Table 1 shows the symbols used in the proposed protocol.

TABLE 1. Notations of Proposed Scheme

Symbol	Explain of Symbols
ID_i	Identity of Ordinary vehicle (Damaged vehicles)
ID_s	Identity of emergency vehicle
IDS	Identity of RSU
s	Secret key of RSU
$pub_{rsu}=s.P$	Public key of RSU
x	Secret key of emergency vehicle
$pub_{EMV}=x.P$	Public key of emergency vehicle
LOC_s	Realm of emergency vehicle
LOC_i	location of Ordinary vehicle
T_1, T_2, T_3, T_4	Timestamps used in protocol

A. Ordinary/Damaged vehicles registration phase

As seen in Figure 2, First, every ordinary vehicle sends its *ID* or license plate to RSU for registration; the RSU checks whether this *ID* is duplicated or not; if it is not duplicated, the RSU selects a random number b_i and the parameters A_i, B_i will be obtained from the (1) and (2) equations.

$$B_i = h(b_i \,||ID_i) \tag{1}$$

$$A_i = h(B_i||IDS||S) \tag{2}$$

Next, the b_i and ID_i parameters are stored in the memory of RSU. Finally, the A_i parameter and pub_{rsu} are sent to the Ordinary vehicle through the secure channel, and the A_i parameter is stored in the Ordinary/ Damaged vehicle.

B. Emergency vehicle registration phase

As seen in Figure 3, In this phase, each Emergency vehicle sends ID_s as well as LOC_s and pub_{EMV} to RSU through the secure channel. RSU selects the random number d_i and obtains the parameter D_i from $D_i = h(ID_s||d_i)$, and finally, the parameters ID_s and d_i and LOC_s Emergency vehicle are stored in the RSU memory and the parameter RSU sends D_i It through the secure channel for Emergency vehicle.

C. Authentication and key agreement phase

In this phase, when the driver of the damaged vehicle sends a warning, the car's automatic system will select two random numbers s_i and q_i as well as the time stamp T_1. Because all entities have the RSU public key, Damaged vehicles can calculate Q_i and $key1_i$ parameters through equations $Q_i = q_i.p$ and $key1_i = q_i.pub_{rsu}$. Then it will encrypt the ID_i and LOC_i parameters and the time stamp T_1 with the *key1* parameter, and as you can see in Figure 4, the parameters A_i, Q_i, $s_i.p, T_1$, $E1_i$ through public channel will send for RSU.

When the RSU receives the message, the freshness of the message is checked. The parameter $key1'_i$ is created through $key1'_i = s.Q_i$, and because $key1'_i = key1_i$ can decrypt the $E1_i$ parameter and compare the timestamp sent with the $E1_i$ parameter and compare the timestamp sent with the timestamp obtained from the decryption.

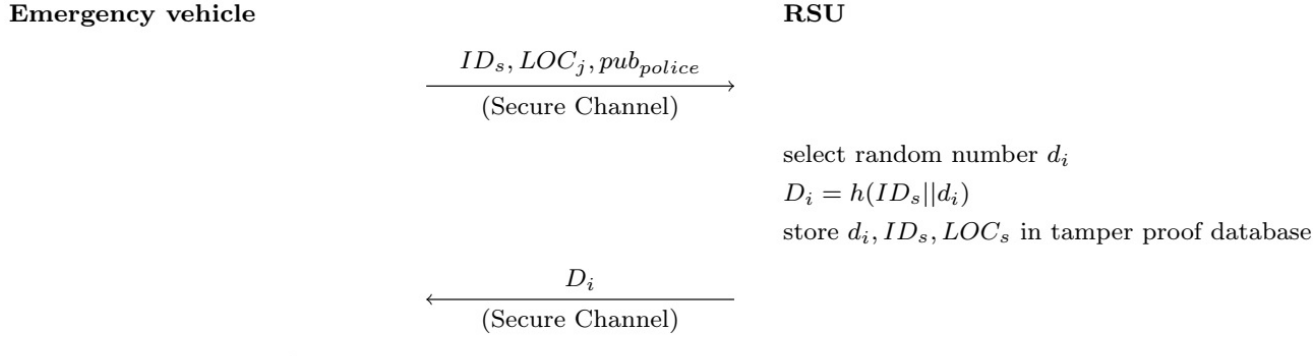

Fig 3. Emergency vehicle registration phase

Then, according to ID_i , it will obtain the parameter b_i which corresponds to this ID_i stored in the memory, and $B_i = h(b_i \,||ID_i)$, $A_i^* = h(B_i||IDS||S)$ and after , A_i^* compares it with A_i received and if correct, it is determined that the received message has not been tampered with on the way.

Now, according to the realm that was sent to RSU through Damaged vehicles, RSU will search for the saved ID_s and d_i parameters of emergency vehicles present in that realm and finally calculate the equations (3) to (7), it will send the parameters $E2_i, s_i.p, T_2, w_i$ and F_i to the emergency vehicle through the public channel.

$$D_i = h(ID_s||d_i) \tag{3}$$

$$w_i = h(D_i||ID_i||LOC_i) \tag{4}$$

$$F_i = f_i.p \tag{5}$$

$$key2_i = f_i.pub_{EMV} \tag{6}$$

$$E2_i = ENC_{key2_i} = \left(ID_i\middle||LOC_i\middle||T_2\right) \tag{7}$$

As seen in Figure 4, when the emergency vehicle receives the message sent by the RSU, it checks the freshness of the message. It calculates the parameter w_i^* according to equations (8) to (10) and receives it with the parameter w_i from the RSU, which will be compared to ensure that the message has not been tampered with on the way.

$$key2_i' = x.F_i \tag{8}$$

$$DEC(E2)_{key2_i'} = (ID_i^*, LOC_i^*, T_2^*) \tag{9}$$

$$w_i = h(D_i||ID_i||LOC_i^*) \tag{10}$$

Then the emergency vehicle selects a random number z_i and from the relationship $sk_i = h\left(z_i.s_i.p\middle||LOC_i\middle||ID_i\right)$ and $Auth_i = h(sk_i||ID_i||LOC_i)$ will calculate the session key and $Auth_i$. Next, the emergency vehicle will send the $z_i.p, Auth_i, T_3$ parameters to the damaged vehicle.

When the message sent by the emergency vehicle reaches the damaged vehicle, the damaged vehicle will first check the freshness of the message. The affected vehicle obtains the session key from the equation $sk_i = h\left(s_i.z_i.p\middle||LOC_i\middle||ID_i\right)$ and the parameter $Auth_i^*$ from the equation $Auth_i^* = h(sk_i||ID_i||LOC_i)$, compares the $Auth_i^*$ parameter with the $Auth_i$ parameter sent by the emergency vehicle. If these two parameters are equal, it is determined that the received message has not been forged or tampered with.

III. SECURITY ANALYSIS

In this section, we informally examine the security of the suggested scheme and demonstrate its resilience to typical attacks. Next, we utilize the Scyther tool to validate the security and accuracy of the proposed scheme formally.

A. Informal Security Analysis

In this section, we provide the informal security proof for the proposed scheme and show its robustness against attacks and its ability to provide major security requirements.

1) Perfect Forward Secrecy

In this security requirement, it is assumed that if the long-term parameters, such as the RSU secret key or emergency vehicle secret key, are leaked, the attacker has access to it. In this case, the attacker should not be able to obtain the session key. Since the session key of the proposed protocol $sk_i = h\left(s_i.z_i.p\middle||LOC_i\middle||ID_i\right)$ has parameters s_i and z_i which are random numbers, based on Elliptic-curve Diffie–Hellman theorem (ECDH) The attacker cannot obtain the $s_i.z_i.p$ or $z_i.s_i.p$ parameters and generate the session key.

2) Mutual Authentication

In the proposed protocol, the mutual authentication requirement is met by checking the equality of parameters such as $Auth_i^* = Auth_i$, $A_i^* = A_i$ and $w_2^* = w_2$ at each stage. Therefore, our proposed protocol meets this security requirement.

3) Resistance to the Replay Attack

An attacker can record a legitimate network transmission and retransmit it at a later time using a replay attack. The primary goal is to deceive the system into believing that the data being retransmitted is authentic. In the proposed protocol, there is no chance of an attack

Ordinary/Damaged vehicle	**RSU**	**Emergency vehicle**
When the alarm system is activated		
select random numbers s_i, q_i		
select time stamp T_1		
$Q_i = q_i.p$		
$key1_i = q_i.pub_{rsu}$		
$E1_i = ENC_{key1_i}(ID_i, LOC_i, T_1)$		
	$\xrightarrow{E_1, A_i, s_i.p, Q_i, T_1}$	
	Select Time Stamp T_2	
	$\lvert T_2 - T_1 \rvert < \Delta T$	
	$key1_i^{'} = S.Q_i$	
	$Dec(E1_i)_{key1_i^{'}} = (ID_i^*, LOC_i^*, T_1^*)$	
	$T_1 =^? T_1^*$	
	$b_i^* = search(ID_i^*)$	
	$B_i^* = h(b_i^* \lvert\lvert ID_i^*)$	
	$A_i^* = h(B_i^* \lvert\lvert IDS \lvert\lvert S)$	
	$A_i =^? A_i^*$	
	$LOC_s, ID_s, d_i = search(LOC_i)$	
	$D_i = h(ID_s \lvert\lvert d_i \lvert\lvert T_2)$	
	$w_i = h(D_i \lvert\lvert ID_i \lvert\lvert LOC_i)$	
	select random number f_i	
	$F_i = f_i.p$	
	$key2_i = f_i.pub_{EMV}$	
	$E2_i = ENC_{key2_i}(ID_i, LOC_i, T_2)$	
		$\xrightarrow{E2, s_i.p, T_2, w_i, F_i}$
		Select Time Stamp T_3
		$\lvert T_3 - T_2 \rvert < \Delta T$
		$key2_i^{'} = F_i.x$
		$DEC(E2)_{key2_i^{'}} = (ID_i^*, LOC_i^*, T_2^*)$
		$T_2 =? T_2^*$
		$w_i^* = h(D_i \lvert\lvert ID_i^* \lvert\lvert LOC_i^*)$
		$w_i =? w_i^*$
		select random number z_i
		$sk_i = h(z_i.s_i.p \lvert\lvert LOC_i \lvert\lvert ID_i)$
		$Auth_i = h(sk_i \lvert\lvert ID_i \lvert\lvert LOC_i)$
	$\xleftarrow{z_i.p, Auth_i, T_3}$	
Select Time Stamp T_4		
$\lvert T_4 - T_3 \rvert < \Delta T$		
$sk_i = h(s_i.z_i.p \lvert\lvert LOC_i \lvert\lvert ID_i)$		
$Auth_i^* = h(sk_i \lvert\lvert ID_i \lvert\lvert LOC_i)$		
$Auth_i =? Auth_i^*$		

Fig 4. Authentication and key agreement phase

because time stamps are used and checked for freshness at each stage.

4) Resistance to the Stolen Verifier Attack

This attack assumes the attacker cannot obtain the session key if they can access the RSU memory or the vehicles involved in the protocol. In proposed protocol, due to the use of elliptic curve encryption ECDH theorem, since in $sk_i = h(s_i.z_i.p||LOC_i||ID_i)$ the parameters of s_i and z_i which are random numbers, the attacker will not be able to generate the session key.

5) Resistance to the Impersonation Attack

In the proposed protocol, when any entity receives a message, the integrity of the received message and the sender's identity is checked through the three equalities of $Auth_i^* = Auth_i$, $w_2^* = w_2$ and $A_i^* = A_i$. If these parameters are not equal and these equalities are not established, the connection will be disconnected if the entities are not authenticated. Considering that our proposed protocol uses a strict mutual authentication mechanism. As a result, there is no possibility of an impersonation attack by the attacker.

6) Resistance to the Known-session-specific Temporary Information Attack

In this attack, it is assumed that if the random parameters in the protocol are leaked, and the attacker can get the random parameters, it should not be possible for the attacker to get the session key. In the proposed protocol, because there is a long-term ID_i parameter in $sk_i = h(s_i.z_i.p||LOC_i||ID_i)$, this attack will not be possible even if random parameters are leaked.

B. Formal Security Analysis using the Scyther Tool

Scyther is a formal automated instrument for the examination, refutation, and authentication of the security characteristics of protocols [13]. Scyther offers the verification of user-defined and automatically generated claims, each representing a security property. Claim *Alive* guarantees the execution of a set of events by communication party *R*. *Nisynch* ensures the successful sending and receiving of all exchanged messages bythe sender and receiver. *claim (R; secret; rt)* implies that *R* claims that *rt* should be unknown to the attacker. *weakagree* ensures protocol robustness against impersonation attack. The analysis in Figure 5 shows that the protocol meets all security requirements.

Scyther results : autoverify

Claim				Status		Comments
SecVanet	Damagedvehicles	SecVanet,Damagedvehicles1	Secret _Hidden_ 1	Ok	Verified	No attacks.
		SecVanet,Damagedvehicles2	Secret authi	Ok	Verified	No attacks.
		SecVanet,Damagedvehicles3	Alive	Ok	Verified	No attacks.
		SecVanet,Damagedvehicles4	Weakagree	Ok	Verified	No attacks.
		SecVanet,Damagedvehicles5	Niagree	Ok	Verified	No attacks.
		SecVanet,Damagedvehicles6	Nisynch	Ok	Verified	No attacks.
	RSU	SecVanet,RSU1	Secret _Hidden_ 3	Ok	Verified	No attacks.
		SecVanet,RSU2	Secret _Hidden_ 2	Ok	Verified	No attacks.
		SecVanet,RSU3	Alive	Ok	Verified	No attacks.
		SecVanet,RSU4	Weakagree	Ok	Verified	No attacks.
		SecVanet,RSU5	Niagree	Ok	Verified	No attacks.
		SecVanet,RSU6	Nisynch	Ok	Verified	No attacks.
	emergencyvehicle	SecVanet,emergencyvehicle1	Secret _Hidden_ 5	Ok	Verified	No attacks.
		SecVanet,emergencyvehicle2	Secret _Hidden_ 4	Ok	Verified	No attacks.
		SecVanet,emergencyvehicle3	Alive	Ok	Verified	No attacks.
		SecVanet,emergencyvehicle4	Weakagree	Ok	Verified	No attacks.
		SecVanet,emergencyvehicle5	Niagree	Ok	Verified	No attacks.
		SecVanet,emergencyvehicle6	Nisynch	Ok	Verified	No attacks.

Done.

Fig 5. Formal Security Analysis of the Proposed Scheme

IV. PERFORMANCE ANALYSIS

To assess and compare the effectiveness of the proposed system in relation to the complexity of computation, we take into consideration the durations presented in the scheme of Abbasinezhad-Mood et al. [14], where TM (Time of performing ECC point multiplication), TA (Time of performing ECC point addition), TE (Time of performing modular exponentiation), TH (Time of computing a hash function),TP (Time for a bilinear pairing), TS (Time for a sign operation),TC(Time for a Chebyshev map operation) and TSE (Time of computing a symmetric encryption/decryption) are 2.2265 ms, 0.0288 ms, 3.85 ms, 0.0023 ms, 5.811 ms, 3.85 ms, 1.113 ms and 0.0046 ms, respectively. Table 2 shows the cost of the proposed scheme and other schemes.

TABLE 2. THE COMPARISON OF COMPUTATION COST

Scheme	Total Computation	Time(ms)
[12]	5TS +6TH+2TSE	19.273
[15]	25TC + 29TE	139.475
SecVanet	7TM + 9TH + 4TSE	15.623

V. CONCLUSION AND FUTURE WORK

This article introduced an authentication protocol for Secure communication in vehicular ad hoc networks, enabling lightweight authentication between EVs and Damaged vehicles. Prior to starting the EV, the driver's identity is verified. Once the initial authentication with the first Damaged vehicle is finished, the EV only needs to calculate a few essential parameters for subsequent authentication with the driver's Damaged vehicles. Finally, we proved that the proposed protocol could meet various security requirements and resist well-known attacks such as replay attacks, stolen verifier attacks, and known-session-specific temporary information attacks. We also analyzed and proved the security of the proposed scheme through the Scyther tool.

REFERENCES

[1] Hussain, R., Lee, J., & Zeadally, S. (2020). Trust in VANET: A survey of current solutions and future research opportunities. *IEEE transactions on intelligent transportation systems*, *22*(5), 2553-2571.

[2] Lai, C., Lu, R., Zheng, D., & Shen, X. (2020). Security and privacy challenges in 5G-enabled vehicular networks. *IEEE Network*, *34*(2), 37-45.

[3] Cui, J., Wei, L., Zhong, H., Zhang, J., Xu, Y., & Liu, L. (2020). Edge computing in VANETs-an efficient and privacy-preserving cooperative downloading scheme. *IEEE Journal on Selected Areas in Communications*, *38*(6), 1191-1204.

[4] Raja, G., Anbalagan, S., Vijayaraghavan, G., Dhanasekaran, P., Al-Otaibi, Y. D., & Bashir, A. K. (2020). Energy-efficient end-to-end security for software-defined vehicular networks. *IEEE Transactions on Industrial Informatics*, *17*(8), 5730-5737.

[5] Hussain, R., Kim, D., Son, J., Lee, J., Kerrache, C. A., Benslimane, A., & Oh, H. (2018). Secure and privacy-aware incentives-based witness service in social internet of vehicles clouds. *IEEE Internet of Things Journal*, *5*(4), 2441-2448.

[6] Yahiatene, Y., Rachedi, A., Riahla, M. A., Menacer, D. E., & Nait-Abdesselam, F. (2019). A blockchain-based framework to secure vehicular social networks. *Transactions on emerging telecommunications technologies*, *30*(8), e3650.

[7] Shao, J., Lin, X., Lu, R., & Zuo, C. (2015). A threshold anonymous authentication protocol for VANETs. *IEEE Transactions on vehicular technology*, *65*(3), 1711-1720.

[8] Zhao, Z., Chen, J., Zhang, Y., & Dang, L. (2015). An Efficient Revocable Group Signature Scheme in Vehicular Ad Hoc Networks. *KSII Transactions on Internet & Information Systems*, *9*(10).

[9] Song, C., Zhang, M. Y., Peng, W. P., Jia, Z. P., Liu, Z. Z., & Yan, X. X. (2017). Research on batch anonymous authentication scheme for VANET based on bilinear pairing. *Journal on Communications*, *38*(6), 49-57.

[10] Wang, Z. (2018). A privacy-preserving and accountable authentication protocol for IoT end-devices with weaker identity. *Future Generation Computer Systems*, *82*, 342-348.

[11] Chen, C. L., Chiang, M. L., Peng, C. C., Chang, C. H., & Sui, Q. R. (2017). A secure mutual authentication scheme with non-repudiation for vehicular ad hoc networks. *International Journal of Communication Systems*, *30*(6), e3081.

[12] Chen, C. L., Chen, Y. X., Lee, C. F., Deng, Y. Y., & Chen, C. H. (2019). An efficient and secure key agreement protocol for sharing emergency events in VANET systems. *Ieee Access*, *7*, 148472-148484.

[13] Cremers C. Scyther, Semantics and Verification of Security Protocols [Ph.D. dissertation]. Eindhoven University of Technology; https://pure.tue.nl/ws/files/2425555/200612074.pdf, (2006)

[14] Abbasinezhad-Mood, D., Ostad-Sharif, A., & Nikooghadam, M. (2019). Novel anonymous key establishment protocol for isolated smart meters. IEEE Transactions on Industrial Electronics, 67(4), 2844-2851.

[15] Abdelfatah, R. I., Abdal-Ghafour, N. M., & Nasr, M. E. (2021). Secure VANET authentication protocol (SVAP) using Chebyshev chaotic maps for emergency conditions. IEEE Access, 10, 1096-1115.