A Lightweight Seamless Authentication Scheme for Edge-Assisted IoV networks

Seunghwan Son
School of Electronic and Electrical Engineering
Kyungpook National University
Daegu, Korea
sonshawn@knu.ac.kr

Myeonghyun Kim
School of Electronic and Electrical Engineering
Kyungpook National University
Daegu, Korea
kimmyeong123@knu.ac.kr

Youngho Park
School of Electronic and Electrical Engineering
Kyungpook National University
Daegu, Korea
parkyh@knu.ac.kr (Corresponding author)

***Abstract*—Internet of vehicles (IoV) is an expanded concept of vehicular ad-hoc networks (VANET), and it is more scalable and can be combined with the latest mobile communication technology such as 5G and 6G. The IoV environment aims to realize autonomous driving through communication such as vehicle-to-infrastructure (V2I), vehicle-to-vehicle (V2V), and vehicle-to-person (V2P). Among them, V2I interaction is the most basic communication. In IoV environments, vehicles have mobility, and it is very frequent to authenticate with the same RSU or another RSU after authenticating with a RSU in its first region. If the authentication process is repeated in re-authentication situations, it can put a burden on the vehicle and RSU and have negatively the performance of the network. In this paper, we proposed authentication protocols considering three situations: Initial authentication, re-authentication, and handover authentication. We demonstrate that our scheme has resistance to various attack scenarios, and compared the performance of the proposed scheme with existing schemes.**

***Index Terms*—Internet of vehicle, re-authentication, handover authentication, chaotic-map, edge computing**

I. Introduction

Compared to the vehicular ad-hoc networks (VANET), internet of vehicles (IoV) is easier to integrate with network architectures such as cloud computing and edge computing because communication technology or bandwidth is more scalable [1], [2]. In IoV networks, V2I, V2V, V2P, and V2X interactions occur to provide services to users. However, These communication is conducted through a public channel, which is vulnerable to various attacks such as replay, man-in-the-middle (MITM), and impersonation attacks [3]–[7], [9]. Therefore, it is necessary to construct a secure authentication scheme IoV networks.

Many researchers have attempted to design a mutual authentication protocol to ensure secure communication in the IoV networks [8], [10], [11]. However, vehicular networks must consider the following two additional considerations in addition to security. First, vehicles have limited computing power [12]. If bilinear pairing or elliptic curve cryptosystems are used in the authentication process, it takes a lot of time in the vehicle and may cause network delay. Second, vehicles have mobility and it is frequent to re-authenticate with the same edge server or another edge server. If a vehicle performs the first authentication process occurs in re-authentication and handover authentication situations, it is inefficient to both vehicles and edge servers. Therefore, in this paper, we design a lightweight seamless authentication scheme for IoV networks. The main contributions are as follows:

- We propose authentication schemes for three situations: Initial authentication, re-authentication, and handover authentication. Compared to the initial authentication situation, the computational cost in re-authentication and handover situations has been significantly reduced.
- We used Chebyshev chaotic map [13] in the proposed initial authentication phase to reduce the computational cost. Through the information generated in the initial authentication process, vehicle can re-authenticate with an edge server using only hash and exclusive-OR operations.
- We show the efficiency of our scheme through comparison with other papers. The proposed scheme has significantly lower lower computational cost than other schemes.

This study was supported by the BK21 Four project funded by the Ministry of Education, Korea (4199990113966).

II. Network Model

The proposed edge-assisted IoV network consists of three entities: Cloud server (CS), edge server (ES), and vehicle. Fig. 1 shows the proposed model and the detailed descriptions are as follows.

- **CS**: A CS initiates the system, deploys edge servers, and registers vehicles. We assume that cloud server is fully trusted.
- **ES**: An ES provides services to vehicles after authenticating within its region. When a vehicle is moved to other region, the ES that was communicating with the vehicle send information to other ES to help the other ES authenticate the vehicle quickly. Furthermore, an ES stores expiration time of vehicle after initial authentication, the ES can quickly re-authenticate the previously authenticated vehicles. We assume that ESs are honest-but-curious entities. Therefore, an edge server do not have information about vehicles that is not in their region.

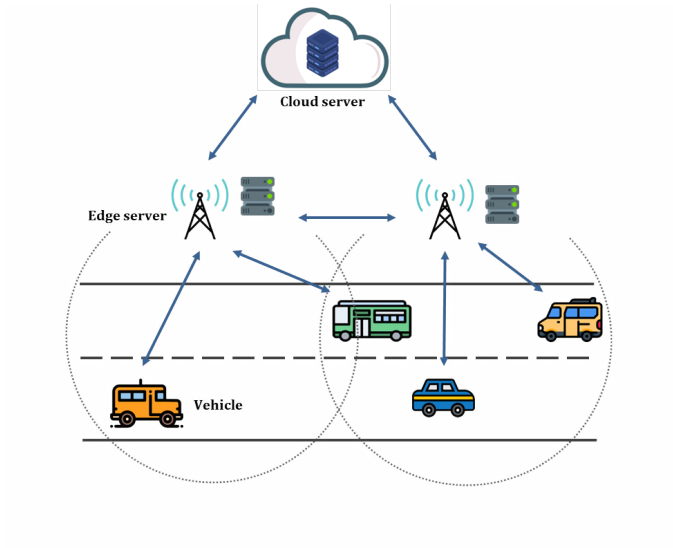

Fig. 1. The edge-assisted IoV network model.

- **Vehicle**: A vehicle registers to CS, authenticates with an ES, and can be provided services. Vehicles often move to edge servers in other regions, and re-authentication is often performed. Vehicles have limited computing power and an adversary can steal a memory in the vehicle and attempt power analysis attack [14]. Furthermore, an adversary can attempt various attacks after registering as a legitimate vehicle on the network.

III. Proposed Scheme

The proposed scheme consists of six phases: Initialization, vehicle registration, vehicle login, initial authentication, re-authentication, and handover authentication. The notations and their meanings are as shown in Table I, and the detailed description of each phase is as follows.

TABLE I
Notations and Meanings

Notation	Meaning
V_i	i-th vehicle
ES_j	j-th edge server
s_j	secret key of ES_j
ET_i	expiration time of V_i
$T_k (k = 1, 2, ..)$	timestamps
RID_i	pseudo identity of V_i
SID_i	secret identity of V_i
PID_i^j	pseudo identity of V_i agreed upon between ES_j and V_i

A. Initialization

The system is initiated by CS. CS chooses a Chebyshev polynomial function $T_n(x)$ with $x \in (-\infty, +\infty)$, cryptographic one-way hash function $h(.)$, a large prime number p, and a time threshold of the network $\triangle T$. CS chooses a random number $s < n$, computes $P = T_s(x)\ mod\ p$. Then, the system public parameters are $\{x, T_n(x), p, h(.), P, \triangle T\}$ and CS keeps s secretly. After that, CS chooses ID_j and s_j, computes $SID_j = h(ID_j||s)$, and sends (ID_j, SID_j, s_j) to ES_j. ES_j computes $P_j = T_{s_j}(x)$, publishes (ID_j, P_j), and stores (SID_j, s_j) securely.

B. Vehicle Registration

A user chooses ID_i and PW_i and inputs it to V_i. Then, V_i computes $HIP_i = h(ID_i||PW_i)$ and $HID_i = ID_i \oplus h(R_{i-TA})$, and sends $(HID_i, T_{HIP_i(x)})$ to CS. Then, CS computes $R_{i-TA} = T_s(T_{HIP_i}(x))$ and $ID_i = HID_i \oplus h(R_{i-TA})$ and checks whether ID_i is registered. CS chooses a random number a_{CS} and computes $RID_i = h(ID_i||a_{CS})$, $SID_i = h(RID_i||s)$, and $M_i = (RID_i||SID_i) \oplus h(R_{i-TA}||HID_i)$. Then, CS sends M_i to V_i. V_i computes $(RID_i||SID_i) = M_i \oplus h(R_{i-TA}||HID_i)$, chooses a random number a_i, computes $X_i = a_i \oplus HIP_i$, $Y_i = (RID_i||SID_i) \oplus h(ID_i||PW_i||a_i)$, and $Auth_i = h(ID_i||PW_i||RID_i||SID_i)$, and stores $X_i, Y_i, Auth_i$.

C. Vehicle login

A user can login to V_i using ID_i and PW_i. The user inputs ID_i and PW_i to V_i, and then V_i computes $a_i = X_i \oplus h(ID_i||PW_i)$, $(RID_i||SID_i) = Y_i \oplus h(ID_i||PW_i||a_i)$, and $Auth_i^* \stackrel{?}{=} h(ID_i||PW_i||RID_i||SID_i)$. If $Auth_i^* = Auth_i$, the user log in to V_i.

D. Initial authentication

V_i generates a timestamp T_1 and a random number b_i and computes $B_i = T_{b_i}(x)$, $B_{ij} = T_{b_i}(P_j)$, $M_{i1} = RID_i \oplus h(B_{ij}|T_1)$, and $D_{i1} = h(SID_i||RID_i)$. Then, V_i transmits $(B_i, M_{i1}, D_{i1}, T_1)$ to a nearby ES_j. ES_j checks whether $|T_1^{'} - T_1| \leq \triangle T$. If it satisfies, ES_j generates a random number b_j and a timestamp T_2, computes $RID_i = M_{i1} \oplus h(B_{ij}||T_1)$, $B_j = T_{b_j}(x)$, $M_{j1} = RID_i \oplus h(T_{b_j}(P)||T_2)$, and $D_{j1} = h(D_{i1}||SID_j||T_2)$, and transmits $(B_j, M_{j1}, D_{j1}, T_2)$ to CS. CS checks $|T_2^{'} - T_2| \leq \triangle T$, computes $RID_i = M_{j1} \oplus h(T_s(P_j)||T_2)$, $SID_j = h(RID_i||s)$, $D_{i1} = h(SID_i||RID_i)$, and $SID_j = h(ID_j||s)$, and checks $D_{j1} \stackrel{?}{=} h(D_{i1}||SID_j||T_2)$. If it is not equal, CS rejects the message. Otherwise, CS generates a timestamp T_3 and random numbers b_{cs} and r_{cs}, computes $RID_i^{new} = h(RID_i||r_{cs})$, $SID_i^{new} = h(RID_i^{new}||s)$, $B_{CS} = T_{b_{CS}}(x)$, $M_{CS1} = (RID_i^{new}||SID_i) \oplus h(T_{b_{CS}}(B_j)||T_s(P_j))$, $M_{CS2} = SID_i^{new} \oplus h(SID_i||RID_i^{new})$, and $D_{CS} = h(SID_i^{new}||RID_i^{new})$, and sends $(B_{CS}, M_{CS1}, M_{CS2}, D_{CS}, T_3)$ to ES_j. ES_j checks T_3, and generates a timestamp T_4, a random number r_j and a expiration time ET_i. Then, ES_j computes $(RID_i^{new}||SID_i) = M_{CS1} \oplus h(T_{b_j}(B_{CS})||T_{s_j}(P))$, $R_j = T_{r_j}(x)$, $M_{j2} = RID_i^{new} \oplus h(T_{r_j}(B_i)||T_4)$, $PID_i^j = h(RID_i^{new}||s_j)$, $M_{j3} = (M_{CS2}||PID_i^j||ET_i) \oplus h(RID_i||RID_i^{new})$, $SK = h(PID_i^j||SID_i||RID_i^{new}||T_{r_j}(B_i)$, and $D_{j2} = h(D_{CS}||SK||T_4)$. Then, ES_j sends $(R_j, M_{j2}, M_{j3}, D_{j2}, T_4)$ to V_i and stores RID_i^{new} and ET_i. V_i receives the message, checks T_4, computes $RID_i^{new} = M_{j2} \oplus h(T_{r_j}(B_i)||T_4)$, $M_{CS2}||PID_i^j||ET_i) = M_{j3} \oplus$

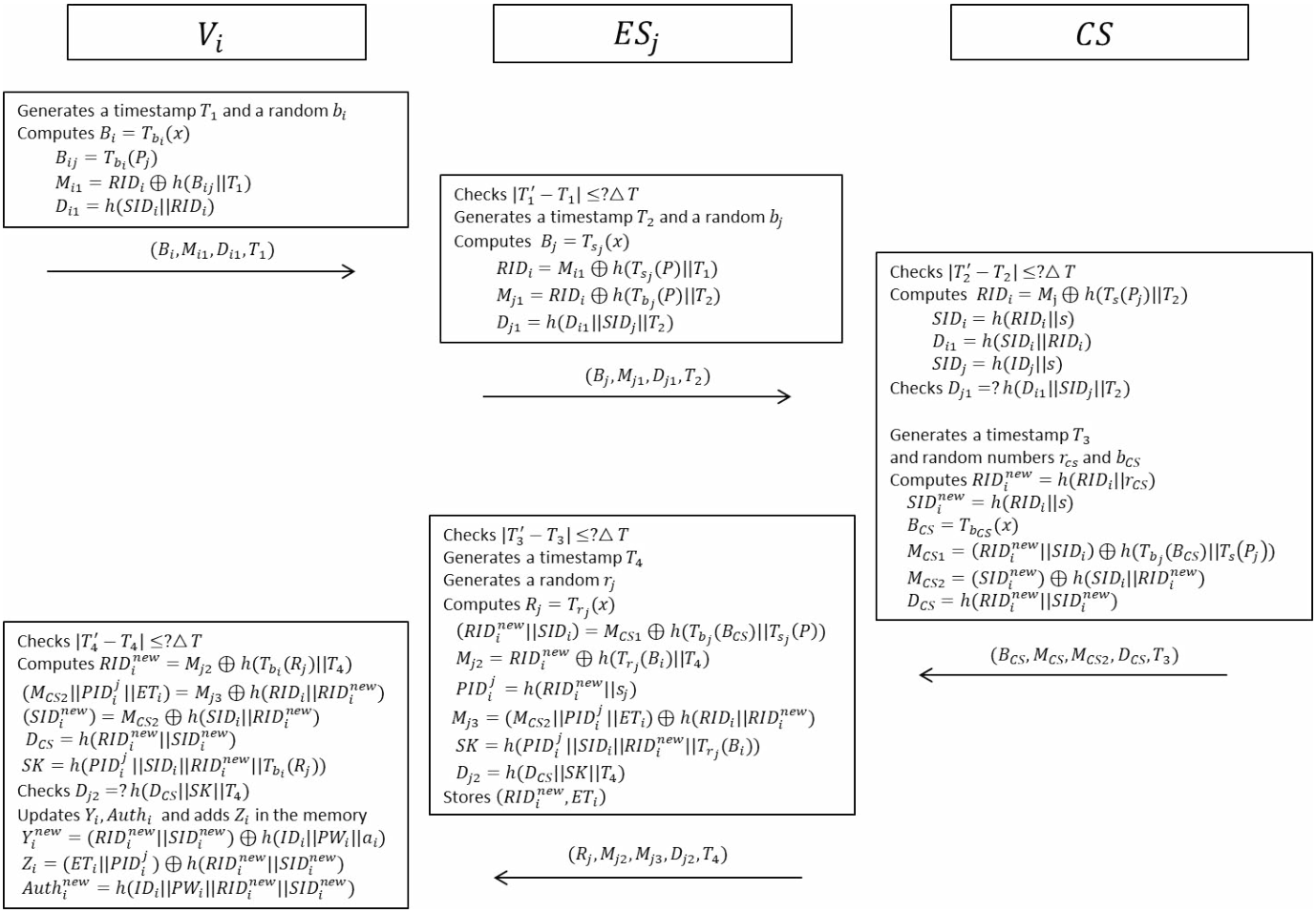

Fig. 2. The proposed initial authentication phase.

$h(RID_i||RID_i^{new})$, $SID_i^{new} = M_{CS2} \oplus h(SID_i||RID_i^{new})$, $D_{CS} = h(RID_i^{new}||SID_i^{new})$, and $SK = h(PID_i^j||SID_i||RID_i^{new}||T_{r_j}(B_i)$, and checks $D_{j2} \stackrel{?}{==} h(D_{CS}||SK||T_4)$. If it is equal, V_i computes $Y_i^{new} = (RID_i^{new}|SID_i^{new}) \oplus h(ID_i||PW_i||a_i)$, $Z_i = (ET_i||PID_i^j) \oplus h(RID_i^{new}||SID_i^{new})$, and $Auth_i^{new} = h(ID_i||PW_i||RID_i^{new}||SID_i^{new})$ and updated Y_i and $Auth_i$ to Y_i^{new} and $Auth_i^{new}$ and adds Z_i in the memory. The proposed initial authentication phase is summarized in Fig. 2.

E. Re-authentication

In the re-authentication phase, V_i can quickly reconnect to ES_j. V_i generates a timestamp T_5, computes $N_i = h(RID_i^{new}||PID_i^j||T_5)$, sends (N_i, ET_i, T_5) to ES_j. Then, ES_j checks T_5 and retrieves RID_i^{new} using ET_i, computes $PID_i^j = h(RID_i^{new}||s_j)$, and checks $N_i \stackrel{?}{=} h(RID_i^{new}||PID_i^j||T_5)$. If it is equal, ES_j generates a timestamp T_6, computes $SK = h(RID_i^{new}||PID_i^j||T_5||T_6)$ and $N_j = h(SK||T_5||T_6)$, and sends (N_j, T_6) to V_i. V_i checks T_6 and computes $SK = h(RID_i^{new}||PID_i^j||T_5||T_6)$. Then, V_i verifies that $N_j \stackrel{?}{=} h(SK||T_5||T_6)$, and if it is equal, V_i succeeds to reconnect to ES_j. The proposed re-authenticaiton phase is summarized in Fig. 3.

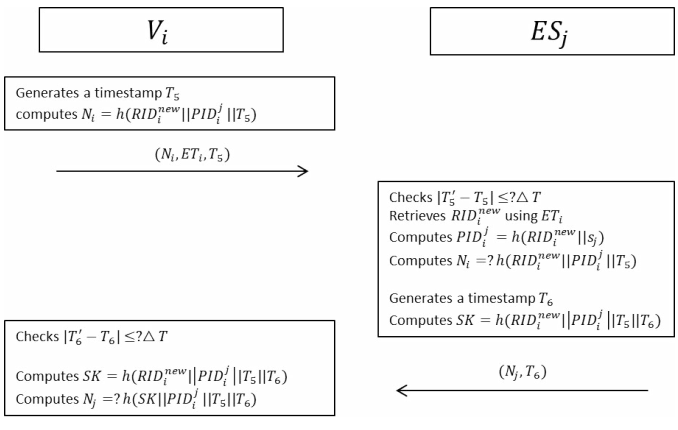

Fig. 3. The proposed re-authentication phase.

F. Handover authentication

In the handover situation, before V_i sends message to ES_{j+1}, ES_j generates a timestamp T_7 and a random number

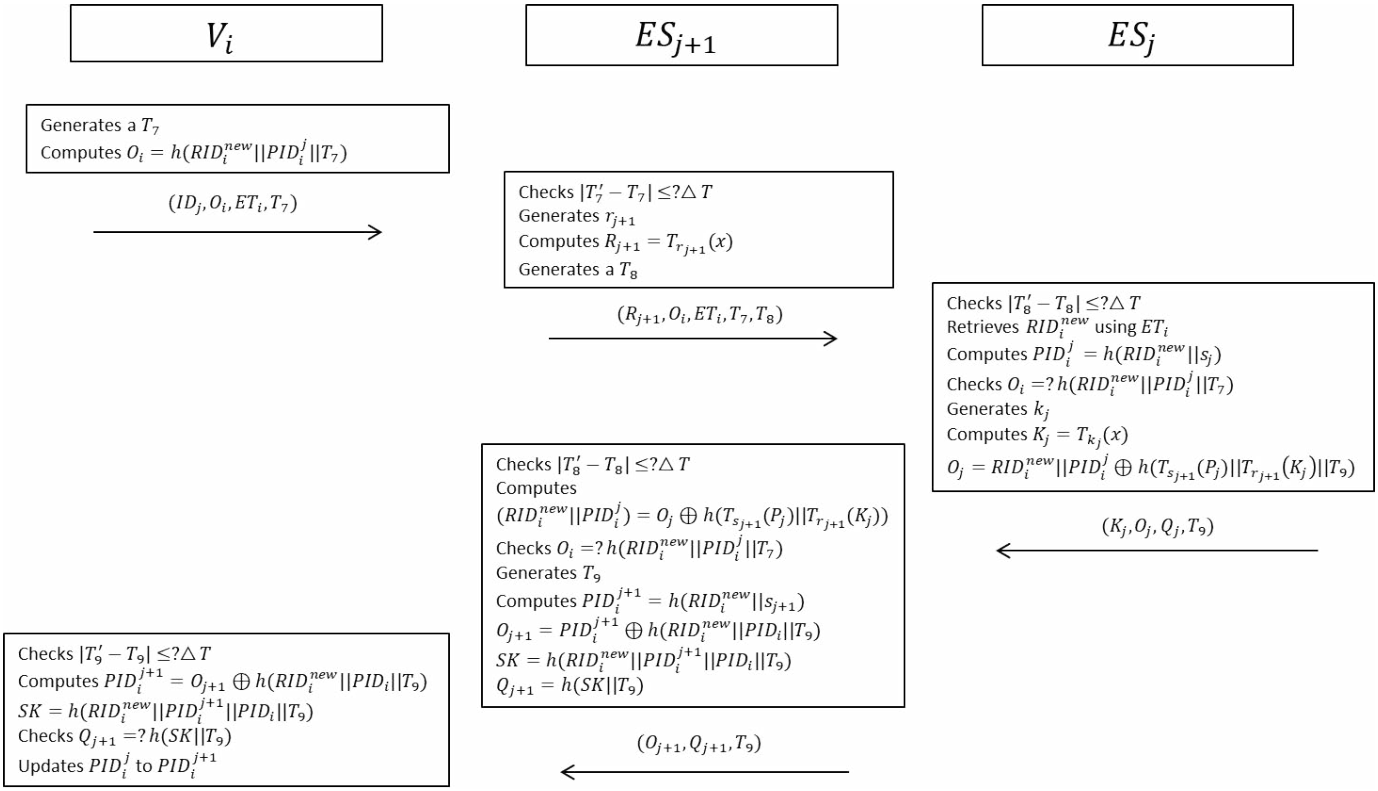

Fig. 4. The proposed handover authentication phase.

k_j, computes $K_j = T_{k_j}(x)$, $O_j = (RID_i^{new}||PID_i^j||ET_i) \oplus h(T_{k_j}(P_{j+1}))$, and $Q_j = h(RID_i^{new}||PID_i^j||h(T_{s_j}(P_{j+1})))$, and sends (K_j, O_j, Q_j, T_7) to ES_{j+1}. Then, ES_{j+1} checks T_7, computes $(RID_i^{new}||PID_i^j||ET_i) = O_j \oplus h(T_{s_{j+1}}(K_j))$, checks $Q_j \stackrel{?}{==} h(RID_i^{new}||PID_i^j||h(T_{s_j}(P_{j+1})))$, and stores $(RID_i^{new}, PID_i^j, RID_i^{new} \oplus PID_i^j, ET_i)$. After that, when V_i moves into the coverage of ES_{j+1}, V_i generates a timestamp T_8 and computes $O_i = RID_i^{new} \oplus PID_i^j$ and $Q_i = h(RID_i^{new}||PID_i^j||T_8)$ and sends (O_i, Q_i, T_8) to ES_{j+1}. ES_{j+1} checks T_8 and retrieves RID_i^{new} and PID_i^j using O_i and checks $Q_i \stackrel{?}{=} h(RID_i^{new}||PID_i^j||T_8)$. If it is equal, ES_{j+1} generates T_9, computes $PID_i^{j+1} = h(RID_i^{new}||s_{j+1})$, $O_{j+1} = PID_i^{j+1} \oplus h(RID_i^{new}||PID_i^j||T_9)$, $SK = h(RID_i^{new}||PID_i^{j+1}||PID_i||T_9)$, and $Q_{j+1} = h(SK||T_9)$, and sends (O_{j+1}, Q_{j+1}, T_9) to V_i. Then, V_i checks T_9, computes $PID_i^{j+1} = O_{j+1} \oplus h(RID_i^{new}||PID_i^j||T_9)$ and $SK = h(RID_i^{new}||PID_i^{j+1}||PID_i||T_9)$, and checks $Q_{j+1} \stackrel{?}{=} h(SK||T_9)$. If it is equal, V_i updates PID_i^j to PID_i^{j+1} as we described in 3. The proposed handover authentication phase is summarized in Fig. 4.

IV. Security analysis

We demonstrate that the proposed protocol is secure against various attacks performed by an adversary A and can guarantee security features.

1) Replay and MITM attakcs: Each message of our scheme include a timestamp, and therefore, if A intercept a transmitted message, modify it, and resends it to the other party, the time threshold of the message would be exceeded, and the message must be rejected. Furthermore, each message incldue message hash value, and therefore, if A generates a new timestamp and sends it to the other party, the message would be considered invalid. Therefore, the proposed protocol is secure against replay and MITM attacks.

2) Stolen memory attack: A can hijack a memory of V_i and can obtain the stored data $(X_i, Y_i, Auth_i)$, and Z_i if V_i is initially authenticated. Then, A can attempt disguising as V_i to authenticate with ES_j. However, A cannot obtain RID_i, SID_i, and PID_i^j, which are essential to authenticate with a nearby edge server without knowing ID_i and PW_i. In this attack scenario, A must succeed to guess ID_i and PW_i simultaneously, and it is virtually impossible. Therefore, the proposed scheme secure against vehicle memory stolen attacks.

3) Insider attack: A registers as a legitimate user and try to obtain the session key of other V_i. In the proposed scheme, $SK = h(PID_i^j||SID_i||RID_i^{new}||T_{b_i}(R_j)$. A cannot obtain any of these values, and it is impossible to guess the values simultaneously. Therefore, the proposed protocol is secure against insider attacks.

4) Impersonation attack: A can disguise as V_i or ES_j and try to agree a session key. To impersonate V_i, A must be able to generate a legitimate $(B_i, M_{i1}, D_{i1}, T_1)$. However,

TABLE III
THE COMPARISON RESULTS.

	Scenario 1			Scenario 2			Scenario 3	
	V_i	RSU_j/ES_j	TA/CS	V_i	RSU_j/ES_j	RSU_{j+1}/ES_{j+1}	V_i	RSU_j/ES_j
Wang *et al.*	$T_p + T_{mul} + 4T_{mod} + T_h$ $\cong 23.4393\,ms$	$T_p + T_{mul} + 6T_{mod} + T_h$ $\cong 31.1393\,ms$	-	$T_p + T_{mul} + T_{mod} + T_h$ $\cong 11.8893\,ms$	$2T_{mod}$ $\cong 7.7\,ms$	$T_p + T_{mul} + 3T_{mod}$ $\cong 19.587\,ms$	-	-
Xi *et al.*	$3T_{mod} + 2T_{mul} + T_{add}$ $\cong 16.0308\,ms$	$6T_{mod} + 2T_{mul} + T_{add}$ $\cong 27.5808\,ms$	-	-	-	-	$2T_{mul} + T_{add}$ $\cong 4.4808\,ms$	$2T_{mul} + T_{add} + T_h$ $\cong 4.4831\,ms$
Proposed	$3T_c + 10T_h$ $\cong 2.249\,ms$	$7T_c + 9T_h$ $\cong 5.2147\,ms$	$4T_c + 10T_h$ $\cong 2.9887\,ms$	$4T_h$ $\cong 0.0092\,ms$	$3T_c + 3T_h$ $\cong 2.2329\,ms$	$3T_c + 6T_h$ $\cong 2.2398\,ms$	$3T_h$ $\cong 0.0069\,ms$	$3T_h$ $\cong 0.0069\,ms$

A cannot generate the message without knowing RID_i and SID_i, which are unknown. In a similar way, A cannot disguise as without knowing s_j and SID_j. Therefore, A fails to impersonate a legitimate entity of the network. In the re-authentication and handover authentication phases, A must know RID_i^{new} and PID_i^j to impersonate V_i. However, A cannot obtain or calculate the above values, and therefore, the proposed scheme is secure against impersonation attacks.

5) Session key disclosure attack: A can directly try to calculate the session key using transmitted messages in a public channel. In the three authentication situations, A cannot obtain any of values that is necessary to calculate the session key. For example, in the initial authentication phase, the session key is calculated by $SK = h(PID_i^j||SID_i||RID_i^{new}||T_{b_i}(R_j))$. All the values are transmitted after being masked and are not exposed to other parties. Similarly, the session key of the re-authentication and handover situations are cannot be calculated by A. Therefore, the proposed scheme has resistance to session key disclosure attacks.

6) Anonymity and untraceability: The identity of vehicle is not transmitted through a public channel, and therefore, anonymity of V_i is guaranteed in the proposed scheme. Instead, A can try to trace V_i if a same message is transmitted repeatedly. However, the pseudo identity RID_i and updated after the initial authentication phase, and A cannot trace V_i. Furthermore, ET_i is updated at certain times, A cannot obtain any meaningful value of V_i. Therefore, the proposed scheme can guarantee untraceability of V_i.

7) Denial-of-service (DoS) attack: A can randomly generate and transmit messages to paralyze the network. If A sends a message B_A, M_{A1}, D_{A1}, T_A to ES_j. Then ES_j relays the message and CS checks the validity of the message through checking $D_{j1} \stackrel{=}{?} h(D_{i1}||SID_j||T_2)$. If it is not equal, the message is immediately rejected, and if messages are continuously sent from the same entity, the entity will be revoked. Furthermore, in the re-authentication and handover authentication situations, A must know RID_i^{new} and PID_i^j which is matching to transmitted ET_i. However, the above values are veiled to other parties except V_i and ES_j. Therefore, the proposed scheme has resistance to DoS attack.

V. PERFORMANCE ANALYSIS

In this section, we compared the proposed scheme with the cutting edge schemes [15], [16] in IoV networks. The comparison is based on the simulation results by Kilinc and Yanik's report [17]. We do not consider the time cost of exclusive-OR operation because it generates negligible computational cost. We describe the notations and their meanings in the below and the simulation results are shown as Table II.

- T_{bp}: Bilinear pairing operation
- T_{mul}: Scalar multiplication on a elliptic curve-based group
- T_{mod}: Modular exponentiation
- T_{add}: Point addition on a elliptic curve-based group
- T_c: Chebyshev polynomial computation
- T_h: Hash function

TABLE II
TIME COST OF EACH OPERATION

Operation	Computational cost
T_{mul}	2.226 ms
T_{add}	0.0288 ms
T_{mod}	3.85 ms
T_c	0.742
T_p	5.811 ms
T_h	0.0023 ms

The comparison results are summarized in Table III. Scenario 1 means an initial authentication, Scenario 2 means a handover authentication, and Scenario 3 means a re-authentication situations, respectively. In the first scenario, in the schemes of [15], [16], only V_i and ES_j participate in the communication. Thus, our scheme can raise a more communication cost than [15], [16]. However, their schemes are using operations with high time cost such as blinear pairing, ecc multiplication, and modular exponentiation, and raise much more computational cost than the proposed scheme. The results of second and third scenarios clearly show the superiority of the proposed scheme. In the second scenario, in our scheme, V_i only performs four hash operations in vehicle side, and it takes $0.0092ms$. On the other side, V_i should perform a bilinear pairing operation, ecc multiplication, modular exponentation, and hash operation and it takes $11.8893ms$ in the scheme of

[15]. Furthermore, ES_j and ES_{j+1} also conducts significantly lower computations in our scheme compared to the scheme of [15]. In the third scenario, V_i takes $4.4808ms$ in the scheme of [16] and takes $0.0069ms$ in our scheme, and our scheme has notably lower computational cost. As a results, we show that the proposed scheme has superior performance than the existing schemes [15], [16].

VI. Conclusions

In this paper, we propose a seamless authentication protocols for edge-assisted IoV networks. The proposed scheme includes initial authentication, re-authentication, and handover authentication. In the initial authentication phase, V_i and ES_j can autheticate each other using a chaotic-map, and generates an expiration time. Then, V_i can quickly authenticates to the same RSU or the other RSU using the expiration time. We informally demonstrates the security of our scheme, and compared computaional cost and communication cost with existing schemes. As a result, the proposed scheme has superior performance than other schemes. In the future work, we analyze the proposed protocol in formal methods such as BAN logic and RoR model, and improve the security and efficiency of the proposed protocol. Furthermore, we simulate it using network simulator 3 to show the practicality.

References

[1] F. Sakiz and S. Sen, "A survey of attacks and detection mechanisms on intelligent transportation systems: VANETs and IoV," *Ad Hoc Netw*., vol. 61, pp. 33–50, Jun. 2017.

[2] R. Gasmi and M. Aliouat, "Vehicular ad hoc networks versus Internet of Vehicles—A comparative view," in Proc. *IEEE Int. Conf. Netw. Adv. Syst. (ICNAS),* 2019, pp. 1–6.

[3] S. Son, J. Lee, Y. Park, Y. Park, and A. K. Das, "Design of blockchain-based lightweight V2I handover authentication protocol for VANET," *IEEE Trans. Netw. Sci. Eng*., vol. 9, no. 3, pp. 1346–1358, May 2022.

[4] D. Kwon, S. Son, Y. Park, H. Kim, Y. Park, S. Lee, and Y. Jeon, "Design of secure handover authentication scheme for urban air mobility environments," *IEEE Access*, vol. 10, pp. 42529–42541, 2022.

[5] D. Chattaraj, B. Bera, A. K. Das, J. J. P. C. Rodrigues, and Y. Park, "Designing fine-grained access control for software-defined networks using private blockchain," *IEEE Internet Things J*., vol. 9, no. 2, pp. 1542–1559, Jan. 2022.

[6] J. Lee, S. Yu, M. Kim, Y. Park, and A. K. Das, "On the design of secure and efficient three-factor authentication protocol using honey list for wireless sensor networks," *IEEE Access*, vol. 8, pp. 107046-107062, 2020.

[7] J. Oh, J. Lee, M. Kim, Y. Park, K. Park, and S. Noh, "A secure data sharing based on key aggregate searchable encryption in fog-enabled IoT environment,"*IEEE Trans. Netw. Sci. Eng*., vol. 9, no. 6, pp. 4468-4481. May 2022.

[8] M. Wazid, P. Bagga, A. K. Das, S. Shetty, J. J. P. C. Rodrigues, and Y. Park, "AKM-IoV: Authenticated key management protocol in fog computing-based internet of vehicles deployment," *IEEE Internet of Things J.,* vol. 6, no. 5, pp. 8804-8817, Oct. 2019.

[9] S. Yu and Y. Park, "A robust authentication protocol for wireless medical sensor networks using blockchain and physically unclonable functions," *IEEE Internet Things J*., vol. 9, no. 20, pp. 20214-20228, May 2022.

[10] T. Alladi, S. Chakravarty, V. Chamola, and M. Guizani, "A lightweight authentication and attestation scheme for in-transit vehicles in IoV scenario," *IEEE Trans. Veh. Technol*., vol. 69, no. 12, pp. 14188–14197, Dec. 2020.

[11] B. Farahani, F. Firouzi, V. Chang, M. Badaroglu, N. Constant, and K. Mankodiya, "Towards fog-driven IoT eHealth: Promises and challenges of IoT in medicine and healthcare," *Future Gener. Comput. Syst*., vol. 78, pp. 659–676, Jan. 2018.

[12] M. Kim, K. Park, S. Yu, J. Lee, Y. Park, S.-W. Lee, and B. Chung, "A secure charging system for electric vehicles based on blockchain," *Sensors*, vol. 19, no. 13, p. 3028, Jul. 2019.

[13] L. Zhang, "Cryptanalysis of the public key encryption based on multiple chaotic systems," *Chaos Solitons Fract*., vol. 37, no. 3, pp. 669–674, 2008.

[14] P. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," in *Proc. Annu. Int. Cryptol. Conf.,* 1999, pp. 388–397.

[15] C. Wang, J. Shen, J.-F. Lai, and J. Liu, "B-TSCA: blockchain assisted trustworthiness scalable computation for V2I authentication in VANETs," *IEEE Trans. Emerg. Topics Comput*., vol. 9, no. 3, pp. 1386–1396, Jul.–Sep. 2021.

[16] N. Xi, W. Li, L. Jing, and J. Ma, "ZAMA: A ZKP-Based Anonymous Mutual Authentication Scheme for the IoV," *IEEE Internet of Things J*., vol. 9, no. 22, pp. 22903-22913. Jun. 2022.

[17] H. H. Kilinc and T. Yanik, "A survey of SIP authentication and key agreement schemes," *IEEE Commun. Surveys Tuts*., vol. 16, no. 2, pp. 1005-1023, 2nd Quart., 2014.