International Journal of Computer Information Systems and Industrial Management Applications
ISSN 2150-7988 Volume 18(8s) 2026 pp. 263-280
https://doi.org/10.70917/ijcisim-2026-3232

Article

Cryptanalysis of the Authentication Schemes and Enhancement for Digital Twin System

Dheeraj Tiger[1*], Nishu[2], Vinod Kumar[3], Anshu Malhotra[4]

[1]Department of Applied Sciences, The NorthCap University, Gurugram-122017, India
Email: dheerajtiger@gmail.com, 23asd004@ncuindia.edu
[2]Department of Computer Science and Engineering, The NorthCap University, Gurugram-122017, India
Email: sethinishu@gmail.com
[3]Department of Mathematics, Shyam Lal College, University of Delhi, New Delhi 110032, India
Email: vinod.iitkgp13@gmail.com & vkmaths@shyamlal.du.ac.in
[4]Centre of Excellence-Cyber Security, School of Engineering and Technology, K R Mangalam University, Gurugram-122103, India
Email: anshu@krmangalam.edu.in
*: Corresponding author - 23asd004@ncuindia.edu

Abstract: The rapid development of autonomous vehicle technology has generated a plethora of intelligent services and applications. However, real-time perception, computation and communication related challenges often result in increased latency and degraded user experience. To address these problems, a new computing architecture based on Digital Twin technology is proposed in this research that leverages cloud computing to efficiently collect, integrate, and process the information generated by autonomous vehicles.
The proposed framework offers continuous feedback through real-time synchronization between the physical autonomous vehicles and their corresponding digital twins hosted in the cloud. As the data exchange is happening over open communication networks, it is of critical importance to have strong security, privacy preservation and communication reliability. Therefore, this work aims at designing a secure framework to enable trustworthy data sharing between autonomous vehicles and their digital twins.
The proposed scheme is evaluated through a thorough security analysis to determine its effectiveness. The comparative results show that the proposed methodology reduces the computational and communication overheads significantly compared to the existing vehicle communication approaches and it is well suited for digital twin-enabled transportation environments. The framework lowers communication costs, improves security and privacy, thereby enhancing the overall user experience and boosting operational efficiency. The results of this research are expected to provide significant inputs to the progress of autonomous vehicle technologies and help their smooth integration in future intelligent transportation systems and daily life.
Keywords: ECC, Autonomous vehicle, Digital Twin, Security and Privacy

1. Introduction

In the past few years, we have rapidly advanced our research into autonomous driving, thanks to support from industry and academia. Leading automobile manufacturers including Volvo, Toyota, and Tesla have greatly funded the development and research of advancement of intelligent transportation technologies, and many recently introduced vehicles new now support Level 2 autonomous. An autonomous vehicle (AV) integrates multiple sensing devices and computing systems. These components are responsible for sensing and processing environmental factors like traffic rules, road obstacles, other people, as well as weather. An AV is now able to make real-time driving decisions by adjusting its speed and trajectory to avoid congestion and possible hazards and offer passengers a comfortable trip. But real-time perception, information processing and communication may overwhelm the resources of an AV, resulting in mistakes and collisions, or even a poor user experience. In addition, due to restricted communication capability, an AV cannot predict traffic conditions beyond its line of sight.

The proposed Vehicular Digital Twin Authentication and Key Agreement Framework enables secure information fusion, intelligent decision making and efficient computation in Autonomous Vehicles (AVs). As

autonomous transportation systems evolve continuously, vehicles are generating massive amounts of real-time data that need to be processed in a timely manner and communicated securely. To address these challenges, the framework introduces a novel concept of $iTwin$, online virtual representation as the digital twin of a physical autonomous vehicle (Fig. 1 above). The $iTwin$ continuously collects and updates essential data from its connected AV including daily driving routes, destination details, road and traffic situations, vehicle status and driving behavior patterns. The iTwin can also make use of cloud computing resources for computationally intensive tasks and intelligent decision-making processes that would otherwise place a significant burden on the physical vehicle. This cloud assisted approach enables faster processing, efficient utilization of resources and quick responses which can be sent back to the AV in real time. The $iTwin$ can communicate with other digital twins in the transportation ecosystem as well as support its corresponding physical vehicle. These interactions enable the sharing of traffic updates, environmental information, and safety alerts, thus improving cooperative intelligence between autonomous vehicles. $iTwins$ employs cloud-enabled connectivity to enhance communication capabilities beyond the traditional line-of-sight limitations and to facilitate reliable information sharing across large urban environments and city-wide networks. The framework involves strong authentication and key agreement mechanisms and provides a secure and trusted communication channel to protect confidentiality, integrity and privacy of data exchanged in information transmission. This security layer helps to protect not only the physical vehicles but also their digital twins against unauthorized access and cyber threats. The proposed architecture aims to improve the comfort of passengers, the safety of driving and the efficiency of operation, while reducing the computational overhead on autonomous vehicles. The framework leverages digital twin technology, cloud computing and secure communication protocols to offer a scalable and intelligent solution for next generation transportation systems. It is expected to be a major enabler for the development of autonomous driving technologies and the fast deployment of such technologies in future smart cities and intelligent transportation networks.

1.1. Motivation and contribution

An ongoing adoption of AV can be significantly obstructed by the absence of complete solutions to existing security concerns such as privacy and secure communication. This is because of confidential information sharing and open interaction between $iTwins$ and their physical masters. For instance, the identity or location of a legitimate AV can be monitored; neither AV nor iTwin is capable of verifying the received messages. Anonymous authentication can resolve the above-mentioned issues. Unforgeability and conditional traceability, however, are two additional concerns. To overcome the aforementioned problems, we suggest a secure authentication mechanism based on elliptic curve cryptography. The main contributions of this paper are as follows:

- We present a secure authentication framework that reduces overhead for all participants in the digital twin communication networks. The proposed system is mainly based on lightweight operations such as hashing and ECC scalar multiplications. The protocol is designed to work efficiently in resource constrained vehicular environments by eliminating expensive cryptographic computations and minimizing message exchanges. It also offers reliable identity verification between autonomous vehicles and their digital twins, which allows for trustworthy and seamless communication with low latency and high scalability for large-scale intelligent transportation systems.
- We analyse the security of the proposed scheme under the Real -OR-Random (ROR) paradigm and compared it with the existing authentication schemes. Our approach is particularly useful in digital twin vehicular communication scenarios because it meets the required security requirements with a small computational and communication overhead. Formal analysis shows resilience against various adversarial attacks and validates security of session keys. In addition, the comprehensive performance evaluation demonstrates that the proposed framework achieves a good trade-off among the strength of security, computational efficiency, communication cost, and practical deploy ability in next-generation VNs.
- The comparative analysis of the proposed protocol with some recent authentication schemes proposed for digital twin vehicular communication environments. The findings demonstrate that the suggested plan outperforms the comparative approaches in terms of security and operational effectiveness. In particular, the framework reduces the authentication delay, communication bandwidth consumption and computational burden without compromising the security. The comparative analysis proves the protocol's superiority in scalability, robustness, privacy preservation, and applicability for real-time autonomous vehicle applications that need secure and efficient communication.
- An informal security review verifies that the proposed system can withstand several security attacks and is suitable for practical deployment in digital twin vehicular communication systems. The scheme is secure against impersonation attack, replay attack, man in middle attack, session key disclosure attack and many other known threats in the network. Besides, it offers user anonymity, mutual authentication,

forward secrecy and data confidentiality. These security properties build trust between communicating entities, and contribute to build resilient, secure and privacy-preserving intelligent transportation infrastructures.

2. Related Work

The development of Digital Twin (DT) technology in the Internet of Vehicles (IoV) has attracted a lot of attention from the research community due to its capability of enhancing the intelligent transportation systems by means of real-time monitoring, decision making, and secure communication. Zhang et al. [5] proposed a dynamic simulation framework to model mobile electric vehicles (EVs) and charging infrastructures to evaluate the efficiency of different IoV navigation strategies via DTs and mobility models. Their work showed how DT technology can enhance route planning, energy management and overall transportation efficiency by offering a virtual representation of physical vehicular environments. Similarly, Bhatti et al. [6] presented an advanced DT framework for electric vehicles to enhance the transportation services in IoV ecosystems. Their framework allowed efficient data collection, analysis and predictive maintenance, helping intelligent vehicle operation. However, IoV communication is still suffering from security threats. The confidentiality and integrity of the transmitted information can be compromised by intermediate entities and malicious attackers, which poses great challenges for secure data exchange among connected vehicles and infrastructure. These security issues have been addressed by using the symmetric and asymmetric cryptographic techniques. Symmetric encryption algorithms like Data Encryption Standard (DES) and Advanced Encryption Standard (AES) are widely employed in IoV communications due to their high processing speed, low computational complexity and suitability for large-scale real-time applications. On the other hand, asymmetric encryption protocols such as ElGamal and ECC provide greater security guarantees by utilizing public-key mechanisms that enable secure communication without revealing private keys. Many researchers proposed advanced cryptographic schemes for improving the vehicular communications. Sellami and Alaya [7] introduce a hybrid key management framework by merging symmetric and asymmetric encryption techniques to speed up information disseminating in Ad Hoc Vehicular Networks. “La Manna et al. [8] improved the security of automotive wireless software updates by applying an attribute-based encryption mechanism embedded in vehicle software and hardware platforms”. Furthermore, Xu et al. [9] scheme an authentication and key agreement protocol for vehicular DT communications with bilinear pairing techniques. However, the research on the specific technical requirements of DT modelling and secure communication in IoV-enabled Cyber-Physical Systems is scarce. Therefore, in this work, we propose dedicated DT modelling strategies and security mechanisms based on asymmetric encryption for improving data confidentiality, reducing encryption and decryption delays, and for improving the overall security of the vehicular digital twin communications.

3. System Model

Fig. 1. Architecture of the proposed vehicular digital twin framework The architecture of the proposed vehicular digital twin framework includes Autonomous Vehicles (AVs), a Trusted Central Authority (CA), and associated Intelligent Twins ($iTwins$). The following section describes the main characteristics and security requirements of each participant.

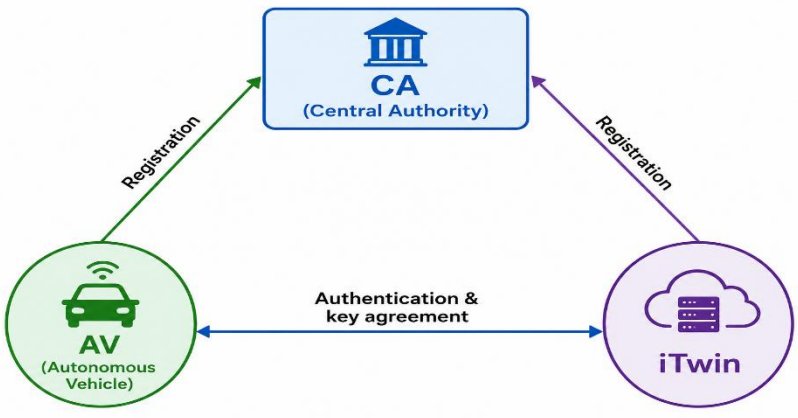

Figure 1: System model

- **Central Authority (CA):** CA generates and distributes pseudonyms to all AVs and $iTwins$ in the framework. It also generates group certificates for each $iTwins$. This allows communication with other iTwins after the corresponding AV has been successfully authenticated. The CA should also trace the real identity of $iTwins$ whenever a malicious message is sent or a security violation occurs.

- **Autonomous Vehicle (AV):** The AV talks to its associated $iTwin$, gathering information via onboard sensors to improve the quality of service and operational efficiency. Before any communication with an iTwin is established, the AV has to authenticate itself to the CA and establish a secure communication channel to ensure the confidentiality, integrity and authenticity of the transmitted data.
- ***iTwins* (ith Digital Twin):** The $iTwins$ provides computational and decision-making services based on information collected from its physical counterpart, thus improving passenger experience and service quality. To protect the exchanged information, the iTwin authenticates itself to the CA first, and then establishes a secure channel to communicate with the AV.

To ensure the security and reliability of the proposed framework, reliable authentication and secure communication between all the participating entities are required. To reduce impersonation attacks, the CA creates secure pseudonyms and secret credentials for each AV and $iTwins$ All communication links between the AVs, $iTwins$ and the CA should be secured using appropriate symmetric or asymmetric encryption mechanisms, based on sensitivity and urgency of transmitted information. Furthermore, the CA should be able to verify the authenticity of the identities created by $iTwins$ and detect any malicious or illicit activities within the network. It provides trust, accountability, and secure information sharing in the vehicular digital twin ecosystem.

3.1. Attacker Model

Due to the high-risk nature of the DT network, possible security risks and vulnerabilities should be considered. In this work, we study mutual authentication and session key formation technique using the Dolev-Yao (DY) threat model [10]. This model assumes that an opponent has full control of the communication channel, i.e., the adversary can intercept, change, replay or inject messages. We also investigate the adversary model suggested by CKM [11]. The CKM framework empowers the advisory with enhanced capabilities, since it allows access to temporary session-specific credentials which may lead to a disclosure of the negotiated session key between communication entities. Furthermore, the model allows for the evaluation of protocol robustness against assaults involving session exposure, key compromise, and other sophisticated threats that may arise in dynamic digital twin communication settings.

This model provides a more comprehensive examination of the possible capabilities that an adversary may possess within the system. The security of the mutual authentication and session key negotiation process within the DT network may be comprehensively assessed against a variety of threats and hostile entities by integrating the DY threat model with the CKM adversary architecture.

3.2 Notation Table: The major notations employed throughout the proposed authentication framework are summarised in Table 1.

Table 1: Symbol and their descriptions

Symbol	Description
AV_i	The ith autonomous vehicle
d_i	The ith virtual representation of digital twin
CA	Central authority
AID_i	Identities of AV_i
$RAID_i$	pseudonym of AV_i
DID_i	Identities of d_i
$RDID_i$	pseudonym of d_i
u_{CA}	The secret key of CA
u_{AV_i}	The secret key of AV_i
s_{AV_i}	The public key of AV_i
u_{d_i}	The secret key of d_i
s_{d_i}	The public key of d_i
AST_i, DST	The secret point on AID_i and DID_i
SK	Session key
C_i	The ith ciphertext
r_i	The ith random number
n_i	The ith random number
N_j	The jth random number
N_k	The kth random number
$E_k(x)$	Encrypt x with k
$H(\cdot)$	Hash function
$e(\cdot)$	Bilinear map function
$\|$	Concatenate operation

4. Details of Chen et.al Protocol [18]

The proposed contains the following parts as below:

4.1 Setup Phase

CA selects three cyclic multiplicative groups, G_1, G^2 and $G_3$with the same order q; two randomly selected elements g and ĝ where g ∈ G₁, ĝ ∈ G₂; a bilinear map e: $G_1 \times G_2 \rightarrow G_3$ where the following equation holds: $e(g^a, \hat{g}^b) = e(g, \hat{g})^{ab} = e(g^b, \hat{g}^a)$ and three one-way secure hash functions H_1: $\{0,1\}^* \rightarrow Z_q^*$, H_2: $\{0,1\}^* \rightarrow G_1$ and H_3: $\{0,1\}^* \rightarrow G_2$.

a. Digital Twin registration phase

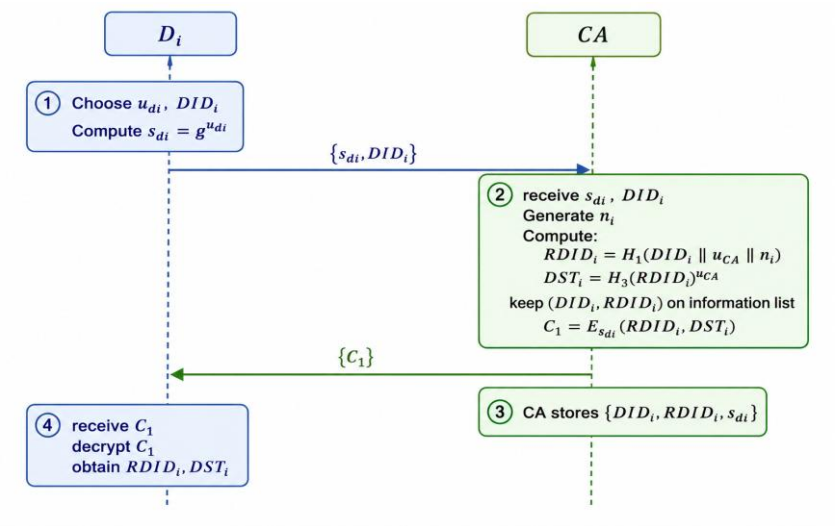

Figure 4.2: DT registration of [18]

All the virtual entities or digital twin representations are enrolled with the CA during this phase. The following procedure are executed when a virtual representation dt_i initiates a registration request with CA. The details of the phase in the following flowchart:

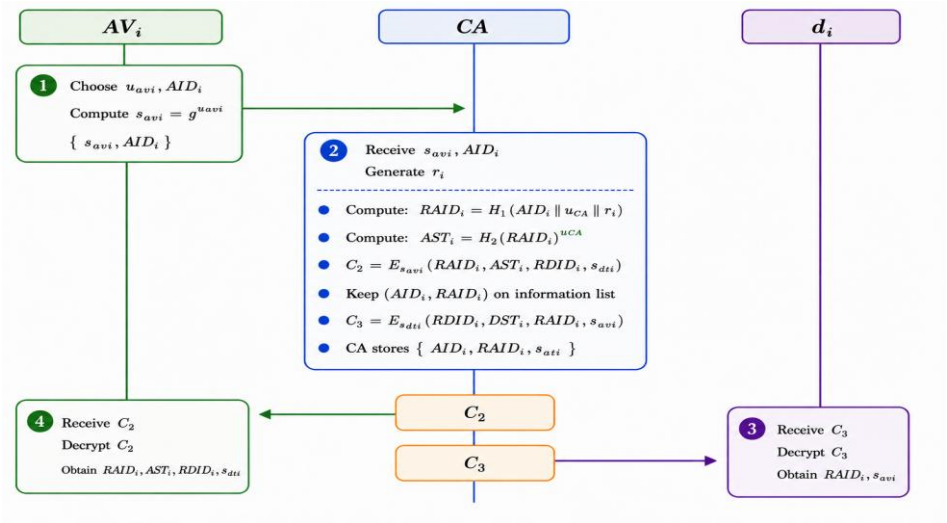

Figure 4.3: AV_i Registration of [18]

4.3 AV Registration phase

In this phase, if an AV requests registration with CA and a virtual identity to join the network, the following process is performed. If an autonomous vehicle AV_i intends to register with the

CA, the below steps are executed. The fig 4.3 discusses the flowchart of the phase:

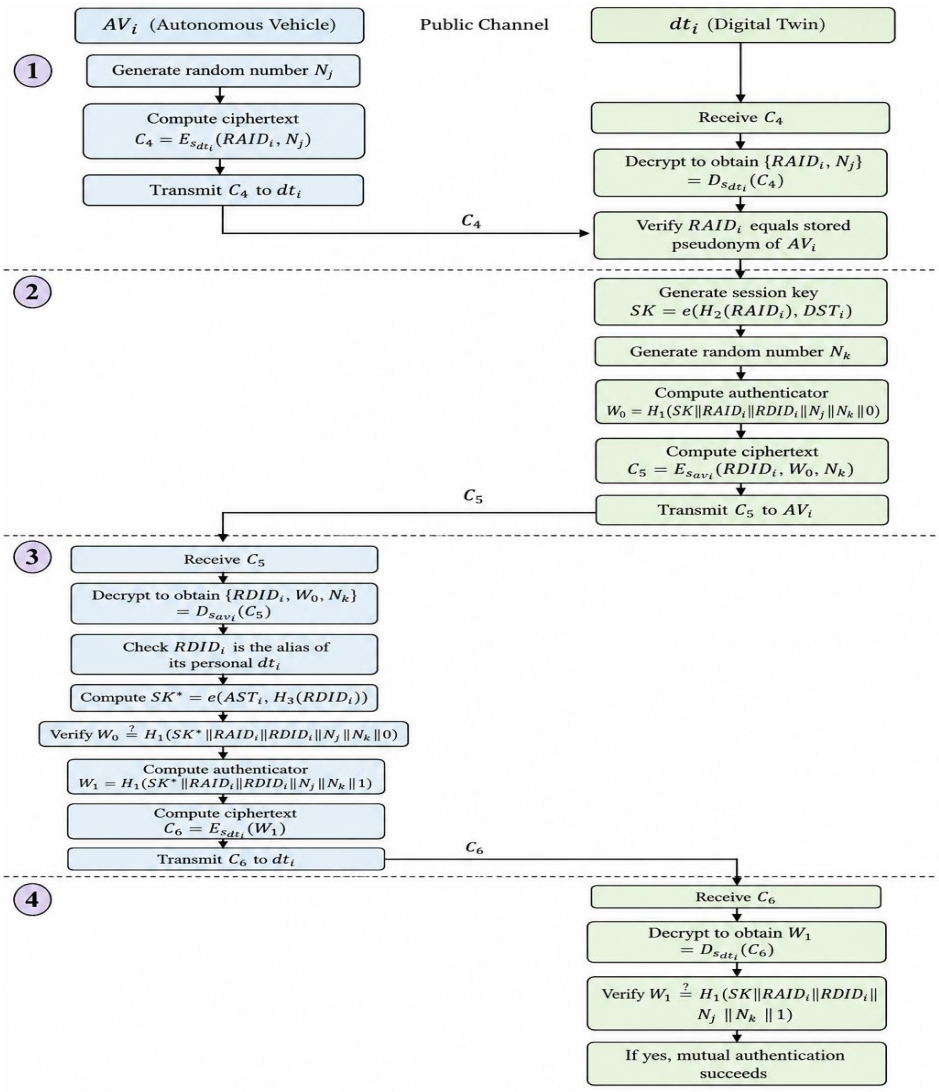

Figure 4.4: Login and authentication phase [18]

b. Login and authentication phase

The fig 4.4 discusses the login and authentication phase of the chen t al's protocol[18].

5. Cryptoanalysis of Chen et al. protocol [18]

The Chen et al. protocol [18] is fail in the many ways as below:

5.1 Session key establishment failure:

In the Section 4.4 mutual Authentication and Key establishment phase, In step 2, dt_i computes Session key $SK = e(H2(RAiDi), DSTi))$. Further, In step, AV_i computes session key $SK* = e(ASTi, H3(RDIDi))$. Here, $H_2: \{0,1\}^* \rightarrow G_1$ and $H_3: \{0,1\}^* \rightarrow G_2$ *and* $e: G_1 \times G_2 \rightarrow G_3$.

The inputs used in both computations are different, there is no mathematical proof demonstrating that $SK = SK^*$. Furthermore, the protocol does not establish the equality $DST_i \neq AST_i$, which is necessary for deriving an identical session key. Consequently, both entities generate different session keys, resulting in authentication failure.

This inconsistency prevents successful secure communication, invalidates mutual authentication, and demonstrates that the protocol cannot guarantee a reliable session key $SK^* \neq SK$ agreement between dt_i and AV_i. The flowchart of the section as:

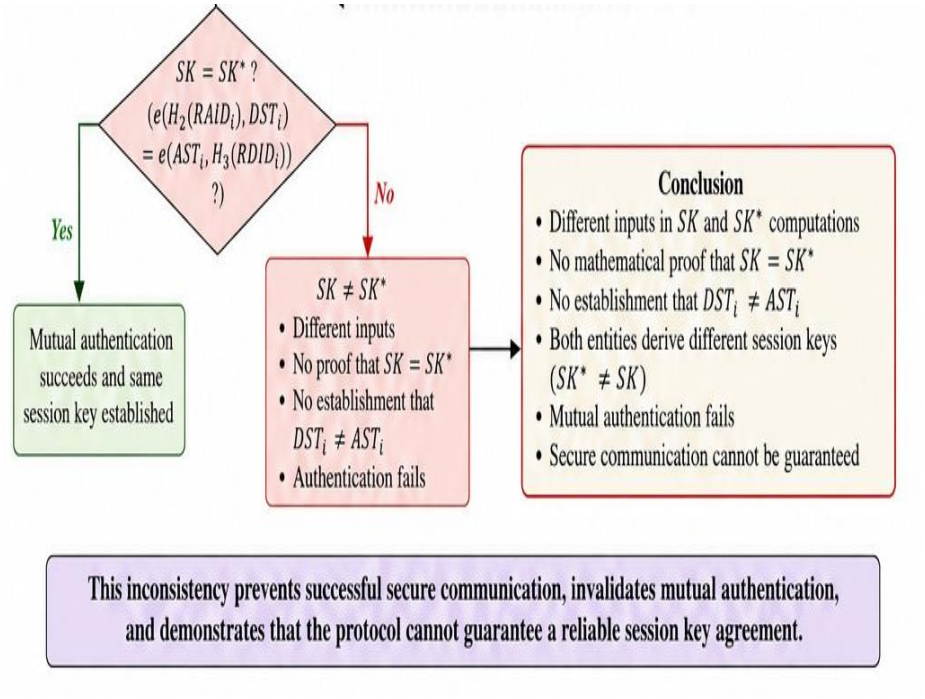

Figure 4.4 Session key establishment failure

5.2 Dependence on CA

The scheme heavily depends on the trusted central authority. Compromise of CA secret key may break the entire system security.

5.3 Replay attack possibility

Although random numbers N_j and N_k are used, absence of timestamp or session expiration mechanisms may permit replay attacks.

5.4 Key escrow problem

Since CA generates or manages keys, it may derive users' session keys, reducing privacy and true end-to-end security.

5.5 Synchronization dependency

The protocol assumes proper synchronization and secure storage of pseudonyms $(RAID_i, RDID_i)$. Desynchronization may cause authentication failure.

5.6 Potential denial-of-service (DoS) attack

Attackers may flood the system with fake authentication requests, exhausting computational resources of AVs or servers.

6. The suggested protocol

The proposed scheme in the paper has the following phases: system initialization, registration, authentication and session key establishment:

6.1. Initialization phase

The operations carried out during the initialization phase are as follows:

– CA selects the non-singular EC as E.

– CA Selects g as the generator element of the cyclic group G. It chooses a random value c which is maintained as the secret key and sets the public key $PK_c = cg$.

– Next, defines a strong cryptographic hash function to ensure secure authentication and integrity verification.

– AV chooses a value x and considers it as confidential private key and computes X = xg as associated public key.

– Intelligent twin ($iTwin$) selects a random value k, considers it as a private key and sets the public key PK_{iT} = kg.

6.2. Registration phase

AV and $iTwin$ are registered through the CA to get the information required to communicate with the VDTNs. An important contract between AV and $iTwin$ and CA is indispensable. The AV and $iTwin$ registration phase is a detailed description of the operation using secure channel:

Step 1. AV takes identity ID_A and password PW_A and calculates $H_{R1} = h(PW_A \parallel ID_A)$, sends $\{ID_A, PW_A, H_{R1}\}$ to CA.

Step 2. When CA is fed with the information above $C_T \in Z_q^*$ is produced. Next CA transfers $\{ID_A, PW_A, H_{R1}, C_T\}$ to $iTwin$.

Step 3. Upon eventual reception of the above message, $iTwin$ inputs own identity ID_T, $iTwin$ computes $H_{R2} = H_{R1} \oplus h(ID_T \parallel ID_A)$ and sends $\{H_{R2}, ID_T\}$ to CA.

Step 4. Upon being received information by $iTwin, CA$ generates $C_A \in Z_q^*$. Then sends out $\{H_{R2}, ID_T\}$ to AV.

Step 5. On collected $\{H_{R2}, C_A\}$, AV executes $H_{R3} = H_{R2} \oplus h(ID_T \| ID_A)$. Finally, AV stores H_{R3} in database.

6.3. Authentication and key agreement phase

Following registration, AV creates a secure shared session key by mutually authenticating with its matching ($iTwin$). After that, all subsequent communications between the entities are secured using this session key. The login and authentication phase provides confidentiality, integrity, authenticity and resistance to various security attacks. The phase contains the following phases:

Step 1. AV login with identity ID_A^* and password PW_A^* and computes $H_{R1}^* = h(PW_A^* \parallel ID_A^*)$. AV verifies $H_{R3} ?= H_{R1}^*$ if yes then AV generates a $\in Z_q^*$. AV computes $W_1 = h(ID_A \parallel C_A \parallel ID_T)$ and $K_1 = h(PW_A \parallel ID_T)$. Then, AV encrypts (ag, W_1, C_A) with K_1as $E_1 = E_{K_1}(ag, W_1, C_A)$. Finally, AV sends $M_1 = \{E_1, T_1\}$ to $iTwin$.

Step 2. As $M_1 = \{E_1, T_1\}$ is received from AV, first $iTwin$ verifies timestamp $t_2 - t_1 \leq \triangle t$ if the time-stamp validation. fails, the request is immediately discarded. Otherwise, the $iTwin$ proceeds with the process, calculates $K_1^* = h(PW_A \parallel ID_T)$ and decrypts E_1 using K_1^* as $(ag, W_1, C_A) = D_{K_1^*}(E_1)$. Calculates $W_1^* = h(ID_A \parallel C_A \parallel ID_T)$ and verifies $W_1^* ?= W_1$. If the verification condition holds successfully, the $iTwin$ randomly generates a value $b \in Z_q^*$ is generated and calculates session key as $SK_T = h(ID_A \parallel ID_T \parallel C_A \parallel C_T \parallel bag \parallel t_3)$. Further, AV computes $W_2 = h(C_A \parallel C_T \parallel t_3)$ and $K_2 = h(C_A \parallel ID_T)$. Finally, $E_2 = E_{K_2}(W_2, bg, t_3)$is encrypted by $iTwin$ and sends $M_2 = \{E_2, t_3\}$ to AV.

Step 3. Now, $M_2 = \{E_2, t_3\}$, is received thereafter AV first verifies $t_3 - t_2 \leq \triangle t$ if yes then calculates the key $K_2^* = h(C_A \parallel ID_T)$ and decrypts $(W_2, bg, t_3) = D_{K_2^*}(E_2)$ with K_2^*. AV also calculates $W_2^* = h(C_A \parallel C_T \parallel t_3)$ and verifies $W_2^* ?= W_2$. If yes then, AV computes the session key $SK_A = h(ID_A \parallel ID_T \parallel C_A \parallel C_T \parallel bag \parallel t_3)$ is calculated by AV.

After that AV and $iTwin$ agree the session key $SK = SK_A = SK_T$.

7. Security Assessment

We have done both formal and informal evaluations to verify its robustness against potential threats. The technique ensures the secrecy and the authenticity of both parties involved.

7.1 Informal security analysis

The proposed protocol is secure in informal ways:

7.1.1 Security of Private Keys

User selects a private key $k \in Z_q^*$ where $Z_q^*$is the set of non-zero integers mod q. The public key is $P_{pubk} = k.g$. There are a number of procedures that an attacker A would have to conduct in order to undermine the security of the system. First the attacker must learn the private key from publicly available sources. However, it is very challenging for the attacker to retrieve the private key because the ECC discrete logarithm problem is

computationally difficult to solve and the private key is derived using a master key g. Consequently, the attacker is unable to recreate the private key from the public information provided and the security of the whole system is maintained.

7.1.2. Impersonation Attack

An impersonation attack is one in which an adversary pretends to be an authenticated user in order to gain access to information or privileges. To initiate such an attack, the information used during the secret key establishment process must be abused to demonstrate the impersonator's legitimacy.

We consider two different forms of the attacks:

– **Autonomous Vehicle:** In this attack, the adversary attempts to gather information or gain unauthorized advantages by impersonating the AV entity. For secret key establishment, the AV transmits $M_1 = \{E_1, t_1\}$ to the $iTwin$. The encryption process using a private key together with the ECC based DLP makes it nearly impossible for the advisory to recover E_1 and the private key. Therefore, the attacker fails in impersonating the legitimate AV entity.

– ***iTwin* -IA:** In this scenario, the attacker attempts to imitate an $iTwin$ entity using the information exchanged during the secret key establishment stage. This authentication phase involves the $iTwin$ and the AV transmitting the messages $M_1 = \{E_1, t_1\}$ and $M_2 = \{E_2, t_2\}$ through a public channel. However, because of the computational hardness of the ECC based DLP, it becomes difficult for the eves to compute the private keys K_1 and K_2. Thus, the attacker cannot successfully impersonate a legitimate $iTwin$ entity.

7.1.3. Authentication Mutual

In our scheme, the secret key agreement phase involves three entities: the $iTwin$, the CA and the AV. During the registration phase, a unique key is generated by each iTwin and AV node. However, prior to accepting the key, a mutual authentication process must be carried out to authenticate the identities. The verification process ensures that the communication session is participated only by the authorized entities to prevent the unauthorized access, impersonation attempts and malicious nodes from creating the secure connections in the digital twin vehicular network.

7.1.4 Session Key Disclosure Attacks

In the proposed scheme, the $iTwin$ and AV agree on a secret key in the session key agreement phase. They then use this key to calculate the session key (SK_A). Note that all other parameters needed to compute the session key are public except (a) and (b). Both iTwin and AV randomly generate (a) and (b). In this case, an attacker cannot find these random values in polynomial time to derive (a) and (b). Thus, even if the attacker knows the secret key K_1, K_2, he/she cannot get the session key (SK_T). Moreover, the proposed scheme employs a secure hash function to secure communication; as there is no invertible hash function, the attacker cannot determine (SK_T) from the transmitted parameters. Thus, the proposed methodology is resilient to key disclosure attacks. Also, the use of fresh random values for each session significantly raises the resistance against cryptanalytic attacks and prevents attackers from correlating several communication sessions to disclose sensitive information.

7.1.5. Eavesdropper Attack

The capacity to collect and interrupt communications over an unsecure route is known as an eavesdropping attack. In order to circumvent this issue, we compute all other parameters using a secure hash function and introduce a new random integer in every authentication cycle. This method prevents the attacker from obtaining user identities or sensitive parameters. Therefore, the security of our proposed approach is highly robust against the eavesdropping attacks. Furthermore, the dynamic generation of authentication parameters ensures that intercepted messages cannot be re-used or analyzed effectively, thus preserving the confidentiality and privacy of all communicating entities.

7.1.6 Forward Secrecy Perfect

The scheme proposed supports the provisions of Perfect Forward Secrecy (PFS) and it prevents the attacker to retrieve the session key ($SK = SK_A = SK_T$). This is because, with the current session key, there is no information to derive about previous session keys. Furthermore, it is computationally infeasible for an attacker to compute the fresh random values generated by the $iTwin$ and AV, which makes it very hard to compute the values $(abg)\ or\ (bag)$. Thus, even if a long-term private secret key is compromised, the scheme still achieves perfect forward secrecy and protects the previously established session keys. In addition, the randomness parameters in each communication session are generated independently and thus compromise of one session does not compromise the confidentiality of previous or future sessions. This feature greatly increases the overall security and resilience of the protocol.

7.1.7. Replay Attack

The scheme we propose is secure against replay attacks, in which an adversary attempts to retransmit messages it has previously intercepted in order to gain unauthorized access or to disrupt communication. The scheme provides a number of security mechanisms against such attacks, e.g., use of secure hash function, checking conditions (W1) and (W2), generating new timestamps and random integers for each authentication session . These mechanisms provide immediate detection and rejection of messages which are out of date or duplicates. Moreover, timestamp validation procedure guarantees freshness of the message and random nonces eliminate message reuse. Therefore, replayed authentication requests cannot be accepted by legitimate communicating entities in any case.

7.1.8. Denial of Service (DoS) Attack

In order to resist to DoS attacks, the proposed scheme provides an effective preventive mechanism to limit the login and authentication attempts to three consecutive requests. When an AV tries to login and authenticate three times without presenting valid credentials, its login and authentication features are temporarily disabled. This limitation prevents an attacker from flooding the system with authentication requests and thus exhausting resources or disturbing the system. Moreover, the temporary lockout mechanism reduces redundant computational burden on network entities, reserves processing resources for legitimate users and enhances availability, reliability and stability of the vehicular digital twin communication environment.

7.1.9. Offline User Identity Prediction Attack

It is an offline attack on the identity of the user where an adversary attempts to predict his/her identity by analyzing messages transmitted through an open channel. The proposed solution utilizes the user identifier IDA to generate a password and a secret key that are highly resistant against facilitating this attack. This safeguard significantly enhances the resistance of the proposed system against offline user identity prediction attacks.

7.1.10 Insider Attacks

An insider attack is a hostile activity in which an unauthorized individual obtains access to a system in order to steal passwords or other personal data and attempt unauthorized logins on several different systems. Encrypted communication between the AV and $iTwin$ utilizing private keys—which are safely maintained and only accessible by authorized users mitigates this kind of attack. This method successfully stops unauthorized users from gaining access to private data by utilizing credentials that have been stolen. Therefore, the proposed architecture provides resistance against insider attack. Moreover, strong credential management and identity verification further lowers the chances that insiders will misuse their privileges.

7.1.11. Man-in-the-Middle Attack

In a Man-in-the-Middle (MITM) attack, the attacker can utilize the intercepted messages from server side in the login phase. The proposed scheme mitigates this attack by using fresh random numbers and pseudonymous identities, which prevents the attacker from successfully interacting with the communicating entities. The proposed scheme also effectively resists this attack since messages M_1 and M_2 are encrypted by private keys and secret keys respectively and are additionally protected by a secure hash function. Furthermore, mutual authentication guarantees that only legitimate entities can establish trusted communication sessions within the network.

7.2 Formal security analysis using Real-oracle random (ROR) model

A common model used to demonstrate the security of an authentication scheme is the Real-Or-Random (ROR) model. Security of an authentication scheme in the ROR model is considered as strong evidence for the security and reliability of the scheme. This model provides a rigorous formal framework for the evaluation of session key indistinguishability and the quantification of an adversary's success probability, thereby allowing complete security analysis against a wide range of cryptographic attacks and threat models [18].

The proposed scheme considers three types of players: autonomous vehicles, digital twins and central authority. The xth instance of AV, yth instance of dt and CA are represented as Π_{AV}^{x}, Π_{dt}^{y}, and Π_{CA} and Π_{CA}, respectively.

Note that $Z = \{\Pi_{AV}^{x}, \Pi_{dt}^{y}, \Pi_{CA}\}$

. We also define an attacker, $\mathcal{A}$ to have the following query capabilities.

- **Execute(Z):** $\mathcal{A}$ can listen in on communications between AV, dt, and CA sent over a public channel.

- **Hash(string):** $\mathcal{A}$ can use a string to determine the output of a hash function.
- **Send (Z, M):** $\mathcal{A}$ can transmit M to Z and obtain Z's answer.
- **Corrupt(Z):** $\mathcal{A}$ can obtain a party's secret information, such as certain smart card values, permanent keys, or temporary data.
- **Corrupt(Z):** $\mathcal{A}$ can learn secret information of a party, e.g. some values of smart cards, permanent keys or temporary data.
- **Test(Z):** c is the result of a coin flip by $\mathcal{A}$. If c=1, $\mathcal{A}$ can correctly determine the session key; if c=0, $\mathcal{A}$ can determine a random string of the same length as the session key.

Theorem: The proposed authentication scheme is secure under the Real-Or-Random model if the adversary A performs Execute, Send, Reveal, Corrupt, and Test queries. The advantage of A in deriving the session key is negligible.

Mathematically,

$$Adv_A^P(\xi) \leq \frac{q_{send}}{2^{l-1}} + \frac{3q_{hash}^2}{2^l} + 2\max\left\{C' \cdot q_{send}^{s'}, \frac{q_{send}}{2^l}\right\} + \frac{(q_{exe} + q_{send})^2}{p}$$

Since l and p are large, the above probability is negligible.

Therefore,

$$Adv_A^P(\xi) \approx 0$$

Proof: Let the final session key be:

$$SK = SK_A = SK_T = h(ID_A \parallel ID_T \parallel C_A \parallel C_T \parallel bag \parallel t_3)$$

where $bag = abg$, generated from random values $a, b \in Z_q^*$.

The proof contains the following games as below:

- **Game G_0: Real Attack**

This is the real execution of the proposed protocol. The adversary A tries to distinguish the real session key from a random key.

$$Adv_A^P(\xi) = |2Pr[Succ_0] - 1|$$

- **Game G_1: Execute Query**

In this game, A can eavesdrop the public messages:

$M_1 = \{E_1, T_1\}$ $M_2 = \{E_2, t_3\}$, where

$E_1 = E_{K_1}(ag, H_1, C_A)$ and $E_2 = E_{K_2}(H_2, bg, t_3)$

Since ag and bg are encrypted, A cannot obtain a, b, or $bag = abg$. Therefore, eavesdropping does not help.

$$Pr[Succ_1] = Pr[Succ_0]$$

- **Game G_2: Send Query**

Here, A actively sends forged messages to AV or iTwin. However, timestamp verification is performed:

$t_2 - t_1 \leq \Delta t$ and $t_3 - t_2 \leq \Delta$

Also, the verification values must satisfy:

$H_1^* = H_1$ and $H_2^* = H_2$

Since H_1 and H_2 are protected by secure hash functions, forging them is computationally infeasible. Thus,

$$|Pr[Succ_2] - Pr[Succ_1]| \leq \frac{q_{send}}{2^l}$$

- **Game G_3: Hash Query**

The adversary may query the hash oracle to find:

$$SK = h(ID_A \parallel ID_T \parallel C_A \parallel C_T \parallel bag \parallel t_3)$$

But $bag = abg$ is unknown to A. To compute bag, A must solve the Elliptic Curve Diffie-Hellman Problem, which is hard. Therefore,

$$|Pr[Succ_3] - Pr[Succ_2]| \leq \frac{q_{hash}^2}{2^{l+1}}$$

- **Game G_4: Reveal Query**

If A performs a Reveal query on an accepted session, the session is no longer fresh. According to the ROR model, the Test query is only allowed for fresh sessions.

Therefore, Reveal query does not help A to distinguish the real session key.

$$Pr[Succ_4] = Pr[Succ_3]$$

- **Game G_5: Corrupt Query**

Even if A obtains stored or long-term values, A cannot compute the session key because the session key depends on fresh random secrets:

$a, b \in Z_q^*$ and $bag = abg$

These random values are generated freshly in each session. Hence, old secret leakage cannot derive the current session key.

$$|Pr[Succ_5] - Pr[Succ_4]| \leq \frac{q_{exe} + q_{send}}{p}$$

- **Final Advantage**

Combining all games:

$$Adv_A^P(\xi) \leq \frac{q_{send}}{2^{l-1}} + \frac{3q_{hash}^2}{2^l} + 2\max\left\{C' \cdot q_{send}^{s'}, \frac{q_{send}}{2^l}\right\} + \frac{(q_{exe} + q_{send})^2}{p}$$

Since l and p are large, the above probability is negligible.

Therefore,

$$Adv_A^P(\xi) \approx 0$$

Hence, the proposed authentication scheme is secure under the ROR model.

Note: We proved in Theorem 1 that the proposed login and authentication protocol is semantically secure and securely establishes session keys under the Real-Or-Random (ROR) model, provided that Secure symmetric encryption, Collision-resistant one-way hash functions, Elliptic Curve Computational Diffie–Hellman (ECCDH) problem hardness. Also, the proposed protocol provides security in the following attacks :

- Mutual authentication
- Session key agreement
- Resistant to replay attacks
- Protection from impersonation attacks
- Resistance to man-in-the-middle attacks
- Confidentiality of the exchanged messages.
- Hence, the proposed protocol is provably secure in the ROR model.

Detailed Explanation of Each Term

The inequality consists of four attack probabilities.

1. Password Guessing Attack Probability

$$\frac{q_{send}}{2^{l-1}}$$

This term represents the probability of successfully performing an **online password guessing attack**.

Where:

q_{send}: Number of active Send queries issued by attacker

l: Bit-length of password/hash output

The attacker tries multiple login attempts.

For one guess:

$$Pr = \frac{1}{2^{l-1}}$$

After q_{send}attempts:

$$Pr = \frac{q_{send}}{2^{l-1}}$$

Interpretation

Suppose:

$$l = 128$$

$$q_{send} = 2^{20}$$

Then:

$$\frac{2^{20}}{2^{127}} = 2^{-107}$$

which is extremely small.

Hence brute-force password guessing becomes infeasible.

2. Hash Collision Probability

$$\frac{3q_{hash}^2}{2^l}$$

This term comes from the **Birthday Paradox** and represents the probability of finding collisions in hash outputs.

The protocol uses secure hash computations such as:

$$\Psi_1 = h(ID_A \parallel C_A \parallel ID_T)$$

and

$$\Psi_2 = h(C_A \parallel C_T \parallel t_3)$$

If the attacker finds two inputs producing same hash:

$$h(x) = h(y)$$

authentication may fail.

Birthday Bound

The collision probability for q_{hash}hash queries is approximately:

$$\frac{q_{hash}^2}{2^l}$$

The constant 3 appears because multiple hash functions/checks are used.

Interpretation

Suppose:

- $q_{hash} = 2^{30}$
- $l = 256$

Then:

$$\frac{3(2^{30})^2}{2^{256}} = \frac{3 \cdot 2^{60}}{2^{256}} = 3 \cdot 2^{-196}$$

which is negligible.

Thus, collision attacks are practically impossible.

3. Cryptanalytic Attack Probability

$$2\max\left\{C' \cdot q_{send}^{s'}, \frac{q_{send}}{2^l}\right\}$$

This term models advanced cryptographic attacks.

First Part

$$C' \cdot q_{send}^{s'}$$

This denotes the probability of breaking the encryption/hash system using sophisticated attacks.

Where:

- C': Small constant
- s': Security exponent

If the cryptographic primitives are secure:

$$C' \cdot q_{send}^{s'} \approx 0$$

Second Part

$$\frac{q_{send}}{2^l}$$

Again, represents brute-force probability.

The proof takes:

$$\max\{\cdot\}$$

because attacker will use the stronger attack strategy.

The factor 2 accounts for two protocol phases/messages.

Interpretation

Even if attacker performs many queries, the probability remains negligible due to exponential denominator 2^l.

4. Elliptic Curve Diffie–Hellman Attack Probability

$$\frac{(q_{exe} + q_{send})^2}{p}$$

This term models attacks against ECC Diffie–Hellman computations.

The session key depends on:

$$abg$$

derived from:

$$ag, bg$$

The attacker attempts to solve the ECCDH problem.

Parameters

- q_{exe}: Execute queries (passive attacks)
- q_{send}: Active attacks
- p: Large prime order of elliptic curve group

ECC Security

Breaking ECCDH requires solving discrete logarithm problem.

The success probability is bounded by:

$$\frac{(q_{exe} + q_{send})^2}{p}$$

Interpretation

Suppose:

- $p \approx 2^{256}$
- $q_{exe} = q_{send} = 2^{30}$

Then:

$$\frac{(2^{30} + 2^{30})^2}{2^{256}} = \frac{2^{62}}{2^{256}} = 2^{-194}$$

which is negligible. Thus, ECCDH attacks are computationally infeasible.

Combined Security Bound

Adding all attack probabilities:

$$Adv_A^P(\xi) \leq \frac{q_{send}}{2^{l-1}} + \frac{3q_{hash}^2}{2^l} + 2\max\left\{C' q_{send}^{s'}, \frac{q_{send}}{2^l}\right\} + \frac{(q_{exe} + q_{send})^2}{p}$$

Each term is negligible because:

- $2^l$is extremely large,
- $p$is a large prime,
- ECCDH is computationally hard,
- Hash functions are collision resistant,
- Encryption is semantically secure.

Final Conclusion

Since all probabilities are negligible:

$$Adv_A^P(\xi) \approx 0$$

8. Performance analysis

We have tested our proposed scheme with proposed schemes by Yao et al. [1], Wu et al. [2], Kumar et al. [3] and Nandy et al. [4] and compared our proposed scheme with them. We also analyze and prove the variation of some important performance parameters: communication cost and computation cost. We have evaluated it on Intel Pentium® CPU 2020 Model 240 GHz and 64-bit core Ubuntu 18.04 OS. The proposed protocols were also developed in a strong powerful language, Python 3.6, like the existing protocols. The proposed authentication scheme is implemented and evaluated using the most widely used network simulator (NS3) platform. In the subsections below, we provide our performance and quantitative measures analysis for each scheme.

8.1. Computation cost

In order to evaluate our approach, in comparison with those of earlier papers, we performed a careful comparative analysis of the computing costs of the approach we employ. We defined the execution times of various operations (that we used) in our calculations as $t_{\mathrm{h}}, t_{\mathrm{e}} c_{\mathrm{m}}, t_{\mathrm{s}}\, y_{\mathrm{m}}$ and t_{fe}. This involves one-way hash which is a hash algorithm under SHA2, point multiplication algorithm of an elliptic curve cryptography (EC),

cryptography symmetric operations and operations under fuzzy extractor respectively. Previous studies [15] show that the timings for EC point and fuzzy extractor are the same. We could determine when the XOR operation would occur hence we left it out. But these were the precise execution timings that were found: t_h = 0.01975 ms, $t_e c_m$ = 0.103156 ms, $t_s y_m$ = 0.063332 ms, and t_{fe} = 0.103156 ms. For our comparisons we concentrate on the authentication, and, communication stages as our vehicles are only registered once. According to our research, the technique recommended by " et al. [2] calls for $34t_h + 2t_e c_m$ = 0.877812 ms, but Yao et al. [1] call for $22t_h + 7t_s y_m + 4t_e c_m$ = 1.290448 ms. Kumar et al. [3] also achieve execution time of $10t_h + 5t_e c_m$ = 0.69353 ms. Nandy et al. [4] state that the need is $13t_h + 2t_s y_m + 1t_{f_e}$ = 0.48657 ms". However, in practice our recommended protocol just requires $11t_h + 4t_s y_m$ = 0.470578 ms. With these calculations we can conclude that our proposed protocol is more efficient.

8.2. Communication cost

The communication cost can be estimated by looking at the size of the messages transmitted across different stages of the protocol. This section will compare the communication cost of the proposed protocols with previous techniques. The data on communication parameters result is taken from [15]. The cost of all variable and function used in the suggested schema is presented. Four bytes in particular represent r and eight bytes represent T and 16 bytes for an identity number. For our proposed protocol, we have used the SHA2 one-way hash method with a message digest of 32 bytes and the ECC symmetric key of 16 bytes. The elliptic curve scalar multiplication is legal and it has a 20-byte representation [6, 7] as stated in previous studies. The proposed protocol has two messages, $M_1 = \{E_1, T_1\}$ and $M_2 = \{E_2, T_2\}$, transmitted during the communication phase, where M_1 is a communication request that is sent from AV to $iTwin$, and M_2 is a response to the communication request from iTwin to AV. Each of these messages necessitate 24 bytes (16 + 8 bytes). As a result, our protocol is efficient in terms of digital communication in $iTwin$, the feature makes the proposed protocol very suitable and has the best fit.

9. Conclusion and future scope

This paper presented a secure authentication and key agreement framework for digital twin-enabled vehicular communication. The proposed architecture maintains synchronization between an autonomous vehicle and its corresponding digital twin, allowing real-time data collection, cloud-based processing, and information exchange. To secure communications among participating entities, authentication mechanisms were designed for both intra-twin and inter-twin interactions. The security analysis showed that the proposed protocol can withstand several common attacks, including replay, eavesdropping, impersonation, session key disclosure, and man-in-the-middle attacks. In addition, the formal security verification confirmed the robustness of the protocol in establishing secure session keys between communicating entities. Performance comparisons with existing vehicular authentication schemes demonstrated that the proposed method requires lower computational and communication costs while providing comparable or stronger security guarantees. These characteristics make the scheme suitable for deployment in digital twin-based vehicular environments where both security and efficiency are important requirements.

Future work may focus on extending the proposed framework to support large-scale vehicular networks with increased numbers of digital twins and connected vehicles. The integration of edge computing and distributed architectures can further reduce communication latency and improve service availability. Moreover, the application of post-quantum cryptographic techniques may strengthen the protocol against future quantum computing threats. Additional research can also investigate secure data sharing, privacy preservation, trust management, and interoperability among heterogeneous digital twin platforms. Such developments will enhance the practicality and applicability of digital twin technology in intelligent transportation systems and smart mobility environments.

References

1. L. Yao, C. Lin, J. Deng, F. Deng, J. Miao, K. Yim, G. Wu, Biometrics-based data link layer anonymous authentication in vanets, in: 2013 Seventh International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, IEEE, 2013, pp. 182–187.
2. L. Wu, Q. Sun, X. Wang, J. Wang, S. Yu, Y. Zou, B. Liu, Z. Zhu, An efficient privacy-preserving mutual authentication scheme for secure V2V communication in vehicular ad hoc network, IEEE Access 7 (2019) 55050–55063.
3. V. Kumar, M. Ahmad, D. Mishra, S. Kumari, M. K. Khan, RSEAP: RFID based secure and efficient authentication protocol for vehicular cloud computing, Vehicular Communications 22 (2020) 100213.
4. T. Nandy, M. Y. I. Idris, R. M. Noor, A. K. Das, X. Li, N. A. Ghani, S. Bhattacharyya, An enhanced lightweight and secured authentication protocol for vehicular ad-hoc network, Computer Communications 177 (2021) 57–76.
5. T. Zhang, X. Liu, Z. Luo, F. Dong, Y. Jiang, Time series behavior modeling with digital twin for internet of vehicles (2019).

6. G. Bhatti, H. Mohan, R. R. Singh, Towards the future of smart electric vehicles: Digital twin technology, Renewable and Sustainable Energy Reviews 141 (2021) 110801.
7. B. Alaya, L. Sellami, Clustering method and symmetric/asymmetric cryptography scheme adapted to securing urban VANET networks, Journal of Information Security and Applications 58 (2021) 102779.
8. M. La Manna, L. Treccozzi, P. Perazzo, S. Saponara, G. Dini, Performance evaluation of attribute-based encryption in automotive embedded platform for secure software over-the-air update, Sensors 21 (2) (2021) 515. URL https://www.mdpi.com/1424-8220/21/2/515
9. J. Xu, C. He, T. H. Luan, Efficient authentication for vehicular digital twin communications, in: 2021 IEEE 94th Vehicular Technology Conference (VTC2021-Fall), IEEE, 2021, pp. 1–5.
10. D. Dolev, A. Yao, On the security of public key protocols, IEEE Transactions on information theory 29 (2) (1983) 198–208.
11. R. Canetti, H. Krawczyk, Universally composable notions of key exchange and secure channels, in: International Conference on the Theory and Applications of Cryptographic Techniques, Springer, 2002, pp. 337–351.
12. S. Itoo, M. Ahmad, V. Kumar, A. Alkhayyat, RKMIS: robust key management protocol for industrial sensor network system, The Journal of Supercomputing (2023) 1–29.
13. V. Kumar, A. M. A. Al-Tameemi, A. Kumari, M. Ahmad, M. W. Falah, A. A. Abd El-Latif, PSEBVC: Provably secure ecc and biometric based authentication framework using smartphone for vehicular cloud environment, IEEE Access 10 (2022) 84776–84789.
14. V. Kumar, RSFVC: Robust biometric-based secure framework for vehicular cloud networking, IEEE Transactions on Intelligent Trans- portation Systems, IEEE, 2023.
15. M. Wazid, A. K. Das, N. Kumar, A. V. Vasilakos, Design of secure key management and user authentication scheme for fog computing services, Future Generation Computer Systems 91 (2019) 475–492.
16. K. Kumar, V. Kumar, Seema, Robust Authentication Protocol for Autonomous Vehicle using Digital Twin Networks, Tuijin Jishu/Journal of Propulsion Technology, 2632 – 2645, 45(1), 2024.
17. Guanjie Li, Tom H. Luan, Jinkai Zheng, Dihao Hu, Jie Cao, Yalun Wu, A secure and lightweight data sharing scheme in vehicular digital twin network, Peer-to-Peer Networking and Applications (2025) 18-37.
18. Chien-Ming Chen, Qingkai Miao, Sachin Kumar,Tsu-Yang Wu, Privacy-preserving authentication scheme for digital twin-enabled autonomous vehicle environments, Trans. Emerging Tel Tech,.2023,34