Online-Journals.org

iJIM International Journal of Interactive Mobile Technologies

iJIM | eISSN: 1865-7923 | Vol. 19 No. 17 (2025) | OPEN ACCESS

https://doi.org/10.3991/ijim.v19i17.56675

PAPER

Privacy-Aware and Efficient Model for Secure Infrastructure in Software-Defined Vehicular Networks

Meryem Chouikik[1], Mariya Ouaissa[2] (✉), Mariyam Ouaissa[3], Zakaria Boulouard[1], Mohamed Kissi[1]

[1]LIM, Hassan II University, Casablanca, Morocco

[2]LISI, Cadi Ayyad University, Marrakech, Morocco

[3]LTI, Chouaib Doukkali University, El Jadida, Morocco

m.ouaissa@uca.ac.ma

ABSTRACT

The rapid advancement of software-defined vehicular networks (SDVN) has transformed transportation systems by introducing programmability, flexibility, and centralized management. By decoupling the control and data planes, SDVN enhances network efficiency and adaptability, thereby enabling real-time traffic management and intelligent decision-making. However, this centralization also presents significant security and privacy risks, exposing networks to threats such as unauthorized access, data breaches, and malware infections. To address these challenges, we propose a secure and privacy-respecting infrastructure for SDVN, integrating advanced cryptographic techniques and lightweight authentication mechanisms. Our model utilizes the Edwards-curve digital signature algorithm (EdDSA) for authentication, elliptic curve Diffie-Hellman (ECDH) for key exchange, and an enhanced certificate revocation list (CRL) to strengthen security. This approach aims to provide low-latency authentication, robust data protection, and improved privacy preservation, while ensuring efficient resource utilization in SDVN. Through verification and analysis, including simulation comparisons showing 20% improvement in authentication time and 15% reduced computation overhead, we demonstrate the effectiveness of our model in securing vehicular communications against emerging cyber threats.

KEYWORDS

software-defined networking (SDN), vehicular ad hoc networks (VANET), software-defined vehicular networks (SDVN), elliptic curve Diffie-Hellman (ECDH), Edwards-curve digital signature algorithm (EdDSA), privacy, security

1 INTRODUCTION

The rapid growth of intelligent transportation systems (ITS) has heightened interest in vehicular ad hoc networks (VANETs) as a critical technology for inter-vehicle communication and data exchange. VANETs, which evolved from mobile ad hoc networks (MANETs), enable automobiles to function as mobile nodes,

Chouikik, M., Ouaissa, M., Ouaissa, M., Boulouard, Z., Kissi, M. (2025). Privacy-Aware and Efficient Model for Secure Infrastructure in Software-Defined Vehicular Networks. *International Journal of Interactive Mobile Technologies (iJIM)*, 19(17), pp. 162–178. https://doi.org/10.3991/ijim.v19i17.56675

Article submitted 2025-05-19. Revision uploaded 2025-07-06. Final acceptance 2025-07-07.

allowing for real-time information transmission that improves road safety, reduces traffic congestion, and enhances the driving experience [1].

Software-defined networking (SDN) [2] is an innovative approach to network management that separates the control and data planes. The inclusion of SDN into VANETs makes it easier to manage communications between vehicles and infrastructure. Integrating SDN with VANETs helps improve traffic control, optimize resource allocation, and allow for more efficient routing [3]. However, the dynamic and distributed nature of software-defined vehicular networks (SDVN) presents serious concerns regarding network administration, security, and privacy risks [4]. With the global push toward connected and autonomous vehicles, securing the SDVN infrastructure becomes increasingly critical. The proliferation of smart mobility solutions, 5G-enabled vehicular environments, and the rise in vehicular cyber-attacks underscore the urgency of research in this area. Traditional VANETs suffer from limited adaptability and weak protection against real-time threats, which SDVN seeks to overcome, albeit at the cost of introducing centralized vulnerabilities.

To address these challenges, it is essential to design a secure and privacy-respecting infrastructure to ensure reliable communication among vehicles, roadside units (RSUs), and the SDN controller. Traditional security mechanisms often struggle to combine strong encryption, robust authentication, and computational efficiency, leading to increased latency and excessive resource consumption in vehicular environments. Additionally, preserving user privacy is crucial, as vehicles continuously exchange sensitive location and identity-related data, exposing them to tracking and profiling risks [5].

In this paper, we propose an efficient and privacy-aware model for a secure infrastructure in SDVN, integrating advanced cryptographic techniques, lightweight authentication mechanisms, and privacy-preserving protocols. Our model relies on the Edwards-curve digital signature algorithm (EdDSA) for secure authentication, encrypted key exchange via elliptic curve Diffie-Hellman (ECDH), and a certificate revocation list (CRL) mechanism to strengthen security and resilience against cyber threats. Furthermore, we analyze the role of blockchain-based trust management and anomaly detection to mitigate potential attacks while maintaining high network performance.

The proposed approach aims to ensure low-latency authentication, robust data protection, and improved privacy preservation, all while ensuring efficient resource utilization in SDVN. Through in-depth analysis and simulations, we demonstrate the effectiveness of our model in securing vehicular communications against emerging cyber threats. This article's remaining content is organized as follows: The system model is shown in section 2, the algorithms employed in our scheme are covered in section 3, the suggested model is explained in section 4, security and performance are examined in part 5, and the conclusion is given in section 6.

2 SYSTEM MODEL

In this section, we will describe VANETs and their evolution towards SDVNs. We will also discuss the integration of SDN into VANETs to improve their management and security, as well as aspects related to the security of SDVN networks.

2.1 Overview of VANET

VANETs are a subset of MANETs designed to provide communication between vehicles and infrastructure. VANETs are crucial for enabling ITS, which improves

road safety, traffic efficiency, and passenger comfort [6]. Communications in a VANET network occur in several ways: V2V, V2I, and V2X.

- **Vehicle-to-vehicle (V2V):** Direct communication between vehicles to share information about the road (e.g., accidents, traffic congestion, weather conditions). Uses protocols such as DSRC (Dedicated Short-Range Communications) and IEEE 802.11p.
- **Vehicle-to-infrastructure (V2I):** Interaction between vehicles and road infrastructures (smart traffic lights, toll stations, and road sensors). Helps improve traffic management and safety.
- **Vehicle-to-everything (V2X):** Extended communication includes Vehicle-to-Pedestrian (V2P), Vehicle-to-Cloud (V2C), and Vehicle-to-Network (V2N) interactions.

A VANET relies on the interconnection of vehicles and fixed infrastructures to ensure efficient communication. It consists of several entities:

- **On-board unit (OBU):** Installed in vehicles, it enables communication with other vehicles and infrastructures.
- **Road-side unit (RSU):** Fixed units placed along roads to facilitate communication between vehicles and centralized servers.
- **Management servers:** Located in the cloud or control centers to process data and optimize traffic.

2.2 SDN based VANET

Software-defined networking is a cutting-edge method that divides the control plane from the data plane to centralize network management. In the context of VANETs, the integration of SDN facilitates the management of communications between vehicles and infrastructure [7]. By centralizing network control, SDN enhances routing efficiency and enables dynamic resource management, which is essential in high-mobility environments. This flexible and programmable architecture allows the network to quickly adapt based on traffic needs and conditions, while also strengthening security by ensuring real-time monitoring and a rapid response to incidents. SDN-based VANETs thus offer a more efficient and secure way to manage intelligent transportation networks [8].

- **Control and data plane separation:**
  - Control plane: Choosing how to manage traffic is the responsibility of the control plane.
  - In an SDN-based VANET, the control plane is centralized and managed by an SDN controller.
  - Data plane: In response to the control plane's choices, the data plane is in charge of forwarding traffic. In VANETs, the data plane consists of vehicles and RSUs that forward data packets.
- **SDN controller:**
  - The network's brain is the SDN controller. It can make well-informed judgments on resource allocation, routing, and network management since it has a comprehensive perspective of the network.

- In an SDN-based VANET, the controller can dynamically adjust routing paths, manage network resources, and implement policies to optimize network performance.
- The primary SDN controller oversees assigning global rules to sub-SDN controllers; these controllers define the routing parameters, disseminate the policy rules, and explain network behavior.

- **OpenFlow protocol:**
  - A popular protocol in SDN, OpenFlow enables communication between the data plane devices and the SDN controller.
  - (e.g., switches, routers, and in this case, vehicles and RSUs).
  - In VANETs, OpenFlow can be used to program the behavior of vehicles and RSUs, enabling flexible and adaptive network management.

Figure 1 illustrates an SDN-based architecture applied to vehicular networks. It depicts a main SDN controller overseeing multiple local SDN controllers, each responsible for managing a specific network zone. Each zone consists of a base station (BS) connected to multiple RSUs, which facilitate communication between vehicles and infrastructure [9]. Additionally, vehicles can also interact with each other through vehicle-to-vehicle communications. This architecture enables centralized and optimized network management through SDN, enhancing the flexibility and adaptability of vehicular communications. Finally, a trusted authority is integrated into the infrastructure to oversee security and manage sensitive information, ensuring reliable and secure communication between different network components.

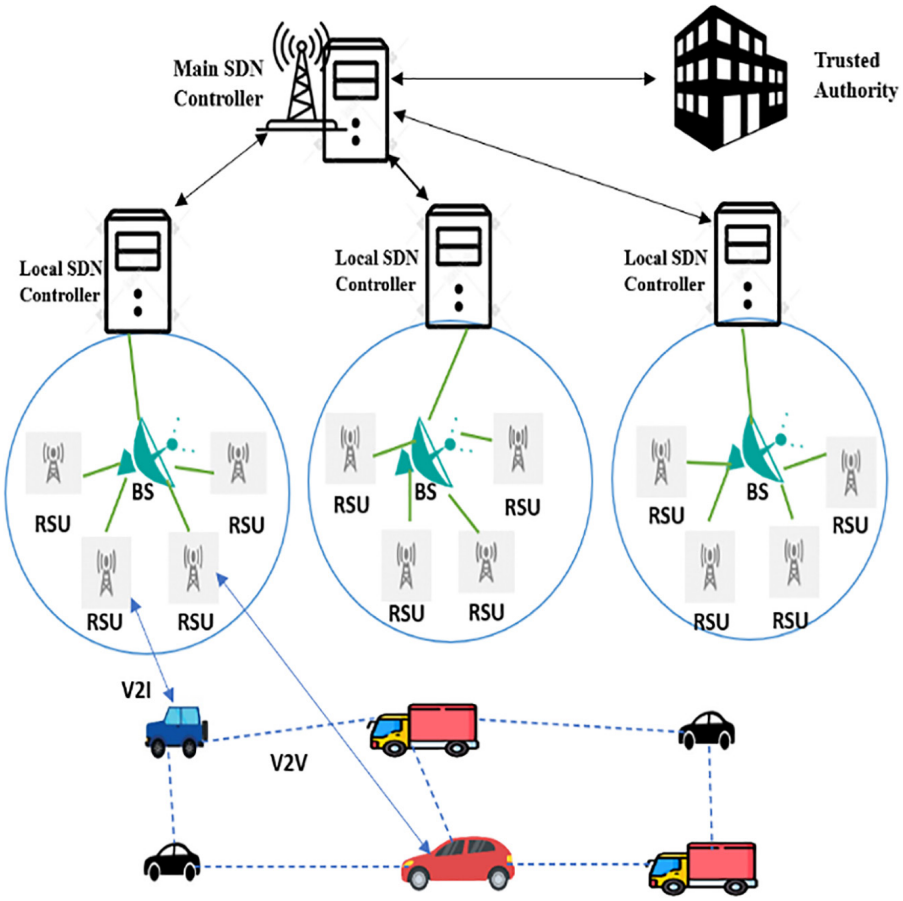

Fig. 1. SDN-based architecture for managing VANET networks

2.3 IoT smart home vulnerabilities

Security in SDVN is crucial due to their dynamic and distributed nature. Unlike traditional VANETs, SDVN centralizes control through an SDN controller, enhancing flexibility and scalability but also introducing vulnerabilities such as distributed denial-of-service (DDoS) attacks, controller compromise, and single points of failure. Ensuring security requires real-time authentication, encrypted communication, and data integrity mechanisms, supported by intrusion detection systems (IDS), cryptographic techniques, and multi-controller architectures [10].

To build a resilient SDVN infrastructure, additional mechanisms such as blockchain-based trust management and multi-controller architectures can strengthen network defense. Given the potential risks of SDVN attacks, including traffic disruptions and privacy breaches, adopting a multi-layered security approach is essential. As SDVN evolves with 5G, edge computing, and quantum cryptography, advanced security frameworks must anticipate emerging cyber threats, ensuring safe and reliable vehicular communications [11].

Figures 2 and 3 highlight the main threats to an SDVN network by distinguishing between two fundamental planes: the control plane, managed by the SDN controller, and the data plane, which includes RSUs and vehicles. Several attack vectors are identified: (1) attacks where an attacker intercepts communications between vehicles and the infrastructure; (2) falsified traffic flows, which disrupt the proper functioning of the network by injecting false data; (3) vulnerabilities in RSUs, which can be exploited to compromise communication; (4) attacks targeting communication between SDN controllers and the network, potentially leading to critical malfunctions; and (5–6) security vulnerabilities in the controllers themselves, which are prime targets for attackers seeking to take control of the network. This analysis highlights the risks associated with SDN integration in vehicular networks and underscores the importance of adopting appropriate cybersecurity solutions [12].

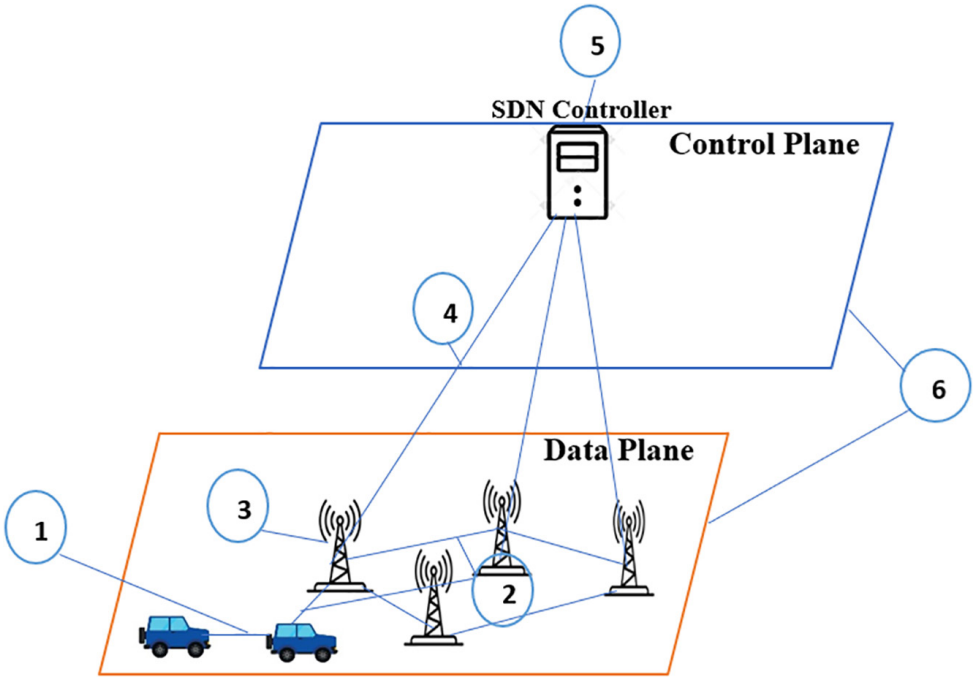

Fig. 2. Issues and vulnerabilities in SDVN

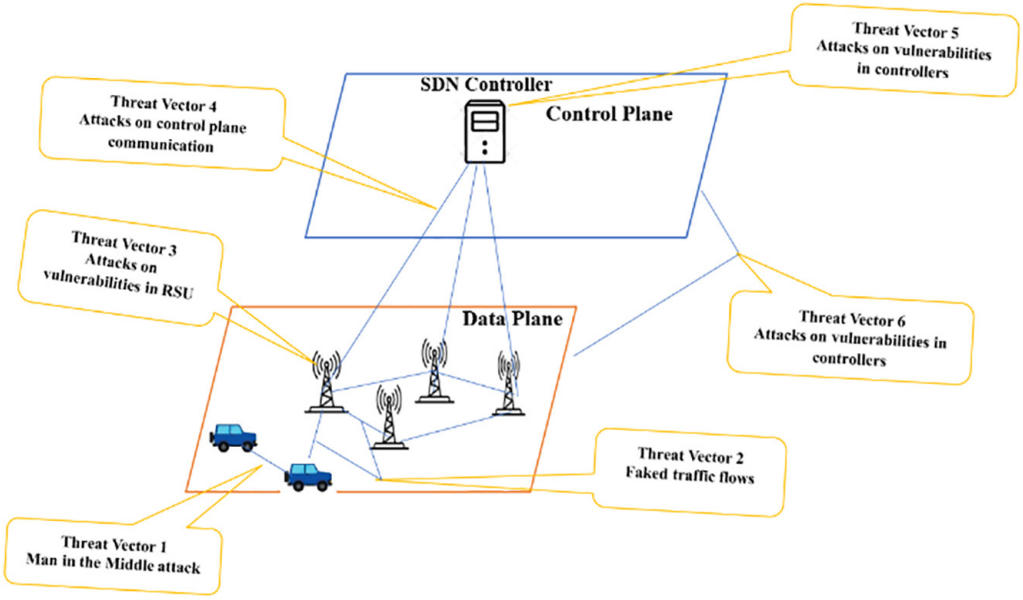

Fig. 3. Issues and threats in SDVN

3 PRELIMINARIES

Among cryptographic solutions, EdDSA and ECDH play a key role. EdDSA ensures fast and secure authentication, preventing unauthorized access, while ECDH facilitates encrypted key exchange, protecting communication from eavesdropping and Man-in-the-Middle (MitM) attacks. Their combination significantly enhances SDVN security, reducing risks associated with compromised authentication and communication. In this section, we will describe the ECDH algorithm and the EdDSA. We will cover the basic principles of these cryptographic techniques and their security benefits [13].

3.1 Elliptic curve Diffie-Hellman (ECDH)

A key agreement system called ECDH enables two parties to create a shared secret across an unprotected channel. It is a variation on the classical Diffie-Hellman (DH) key exchange, except instead of using modular arithmetic, it makes use of Elliptic Curve Cryptography (ECC). ECDH with reduced key sizes is more bandwidth and computationally efficient while providing the same security advantages as DH [14].

1. **Elliptic curve cryptography (ECC)**
   - Elliptic curves over finite fields have an algebraic structure, which forms the basis of the ECC public-key cryptography technology.
   - The Elliptic Curve Discrete Logarithm Problem (ECDLP) is computationally intractable with current technology, and its complexity is the foundation for ECC's security.
2. **Elliptic curve Diffie-Hellman (ECDH)**
   - ECDH is a key exchange protocol that uses elliptic curves to generate a shared secret between two parties.
   - The shared secret can then be used to derive a symmetric key for encrypting subsequent communications.

3. **Security of ECDH**
   - **Elliptic curve discrete logarithm problem (ECDLP):**
     - The security of ECDH relies on the difficulty of solving the ECDLP, which is the problem of finding "dA" given the Eq. (1):

$$QA = dA \times GQA = dA \times G \tag{1}$$

     - With the current technology, solving the ECDLP for well-chosen elliptic curves is computationally infeasible.
   - **Smaller key sizes:**
     - Though key sizes are significantly smaller, ECDH offers the same degree of security as regular DH. For instance, the security of a 3072-bit RSA key is comparable to that of a 256-bit ECC key.
     - Smaller key sizes result in reduced computational overhead and bandwidth usage, making ECDH more efficient.
   - **Forward secrecy:**
     - ECDH provides forward secrecy, meaning that even if an attacker compromises one of the private keys in the future, they cannot decrypt past communications.
     - This is because the shared secret is ephemeral and not stored after the session ends.
4. **Applications of ECDH**
   - **Secure communication:** ECDH is widely used in secure communication protocols such as TLS (Transport Layer Security) and SSH (Secure Shell) to establish a shared secret for encrypting data.
   - **Wireless security:** ECDH is used in wireless security protocols like WPA3 (Wi-Fi Protected Access 3) to provide secure key exchange between devices.
   - **IoT security:** ECDH is suitable for securing communications in IoT (Internet of Things) devices due to its efficiency and strong security.
   - **Cryptographic protocols:** ECDH is used in various cryptographic protocols, including Signal, WhatsApp, and other end-to-end encrypted messaging apps.

3.2 Edwards-curve digital signature (EdDSA)

The EdDSA is a modern, efficient, and secure digital signature scheme based on twisted Edwards curves, a specific form of elliptic curves. It was introduced by Daniel J. Bernstein et al. in 2011 [15]. EdDSA is designed to provide high performance, strong security, and simplicity of implementation, making it a popular choice for cryptographic applications.

- **Twisted Edwards curves:**
  - EdDSA operates on twisted Edwards curves, which are elliptic curves defined by the Eq. (2):

$$ax^2 + y^2 = 1 + dx^2y^2 \tag{2}$$

    where "a" and "d" are the curve parameters.
  - These curves offer efficient arithmetic operations, making them suitable for high-performance cryptographic applications.
- **Deterministic signing:**
  - EdDSA uses a deterministic nonce generation process, meaning the same message and private key will always produce the same signature.

  - This eliminates the need for a high-quality random number generator during signing, reducing the risk of implementation errors (e.g., as seen in ECDSA, where poor randomness can lead to private key exposure).
- **Compact signatures:** EdDSA produces compact signatures. For example, Ed25519 (a widely used EdDSA variant) generates 64-byte signatures for 32-byte private keys.
- **Strong security:** EdDSA is designed to be resistant to common cryptographic attacks, including side-channel attacks and fault injection attacks. It provides 128-bit security for Ed25519, making it suitable for long-term use.
- **Efficiency:** EdDSA is highly efficient in terms of both computation and memory usage, making it ideal for resource-constrained environments like embedded systems or IoT devices.

4 PROPOSED SCHEME

This section outlines the steps of our secure infrastructure scheme in SDVN.

4.1 Protocol sescription

Our scheme is structured into five phases:

1. In order for VANET entities to authenticate with the Certificate Authority (CA) and obtain a public key certificate for communication, a symmetrical approach is utilized to secure the authentication packets that are exchanged during the primary authentication phase between the various network entities. Additionally, a message's signature is generated, verified, and the public/private key pair is generated using the EdDSA approach.
2. The second stage involves communication and authentication between OBUs and RSUs. During this phase, OBUs authenticate with RSUs a second time with the intention of using two distinct keys: one is a shared secret key for V2V or I2V communication, and the other is used for V2V communication.
3. In the next step, controllers exchange public keys. The sub-SDN controller sends an encrypted message and after decryption by the central SDN, both controllers generate a session key for secure communication.
4. The communications sent during the message exchange phase between OBUs or V2V communication are encrypted using the K_{Gi} group key that RSUs issue. To guarantee integrity and non-repudiation, the message hash is then signed using the private key. Using a certificate also makes it possible to authenticate and verify the sender's identity.
5. The revocation phase involves the CA sending a list of revoked certificates to OBUs. Certificates are revoked if a vehicle reports a lost or stolen private key, or if an RSU and SDN controllers detect suspicious behavior. To improve response time, we propose dividing the main revoked certificates list into sublists based on vehicle type (e.g., professional, private, personal), which is specified in the certificate. This allows vehicles to search only for the relevant sublist rather than the entire main list to check the validity of a sender's certificate.

4.2 Registration phase

In the registration phase, the CA and OBU_i authenticate through a series of cryptographic exchanges. The OBU_i first sends a cookie (C_{OBUi}) and supported

cryptographic algorithms (SA_{OBUi}) to the CA, which responds with its own cookie (C_{CA}), chosen algorithm (SA_{CA}), and session ID (ID_{OBUi}). They then agree on an elliptical curve and exchange points (I_{OBUi}.P and I_{CA}.P) to derive secret keys (K_{OBUi} and K_{CA}). The OBU_i encrypts and sends its real identifier (IDr_{OBUi}) and a hash of prior exchanges using AES-128. The CA verifies, retrieves IDr_{OBUi}, and issues an encrypted response containing its public key ($KPUB_{CA}$) and a hash for integrity checking. After validation, the OBU_i requests a certificate, and the CA generates a key pair, signs it, and sends an encrypted message with the key pair, signature, and certificate ($Cert_{OBUi}$). The process concludes with mutual confirmation, and the CA stores registration details for future tracking. The certificate format is: $Cert_{OBUi}$: ID_{OBUi}, $KPUB_{OBUi}$, $Type_{OBUi}$, T_{exp}, ID_{CA}, Sig_{CA}.

In this paper, we examine how CA→RSUs and CA→OBU mutually authenticate using the same registration and authentication procedure. The following actions must be taken by the vehicle to authenticate and obtain a public key certificate.

The many communications sent and received throughout the authentication process are depicted in Figure 4.

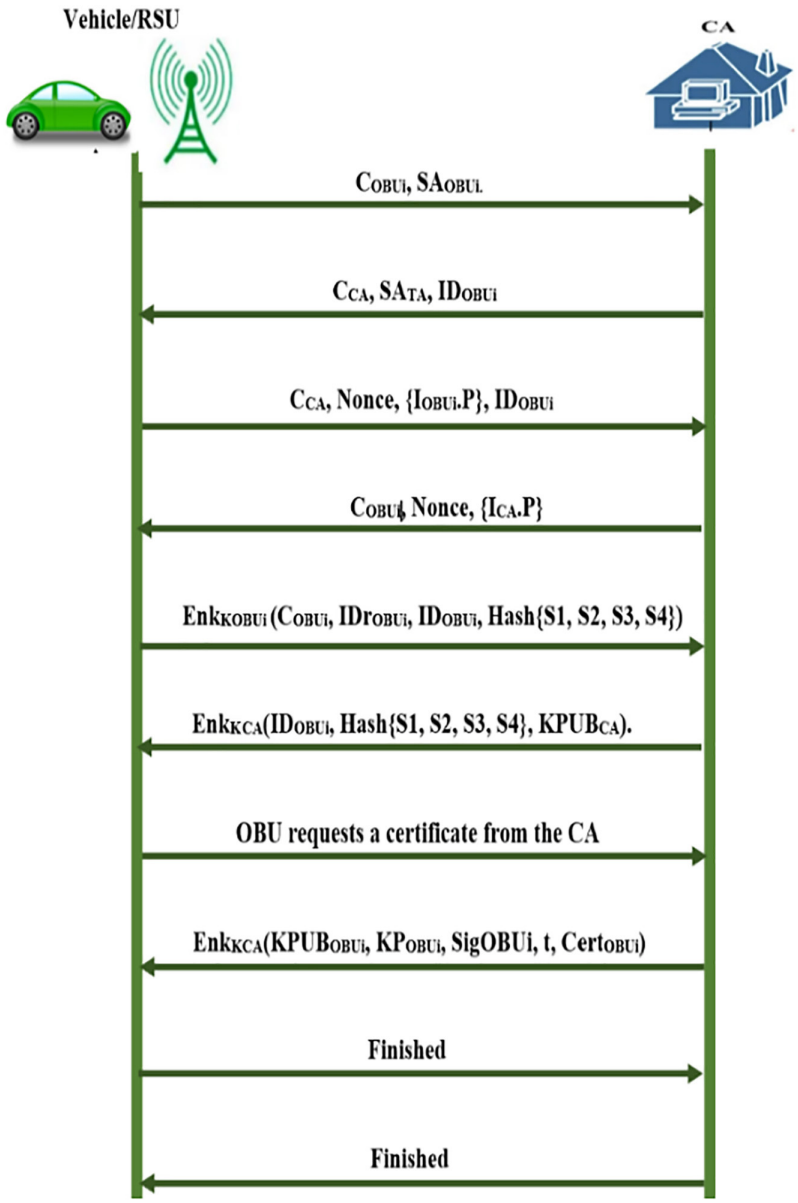

Fig. 4. Registration phase

4.3 Authentication and communication between OBU_i and RSU_i

OBU_i and RSU_i authenticate through mutual verification of certificates and encrypted key exchanges using ECDH. RSU_i broadcasts its ID, public key, and certificate, while OBU_i responds with its encrypted credentials. RSU_i verifies and replies with a signed message, which OBU_i validates before finalizing authentication. Both generate a shared secret key (K_S) for secure communication. RSU_i also provides a group key (K_{Gi}) for V2V communication, ensuring confidentiality by using separate keys for I2V and V2V exchanges (see Figure 5).

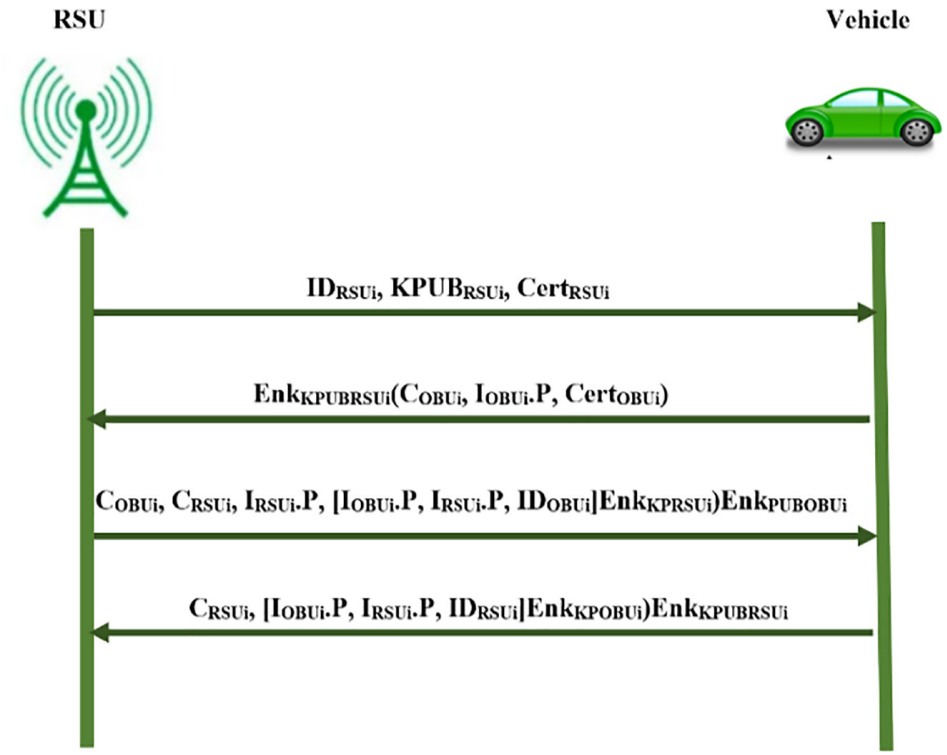

Fig. 5. Authentication and communication between OBU_i and RSU_i

4.4 Secure communication between SDN controllers

The following actions must be taken before initiating secure communication whenever controllers must speak with one another, as illustrated in Figure 6.

1. Public keys are exchanged publicly.
2. Using the public key of the main SDN controller, the sub SDN controller transmits an encrypted message with ID_{Sub}, a nonce N, and a timestamp to the main SDN controller.
3. The main SDN controller decrypts the message, retrieves the contents, and responds with ID_{Main}, a timestamp, and N + 1, encrypted using the sub SDN controller's public key.
4. The sub SDN controller decrypts the message, verifying ID_{Main}, timestamp, and N + 1.
5. Both controllers use N and N + 1 to perform an XOR operation, generating a secret session key for secure communication.

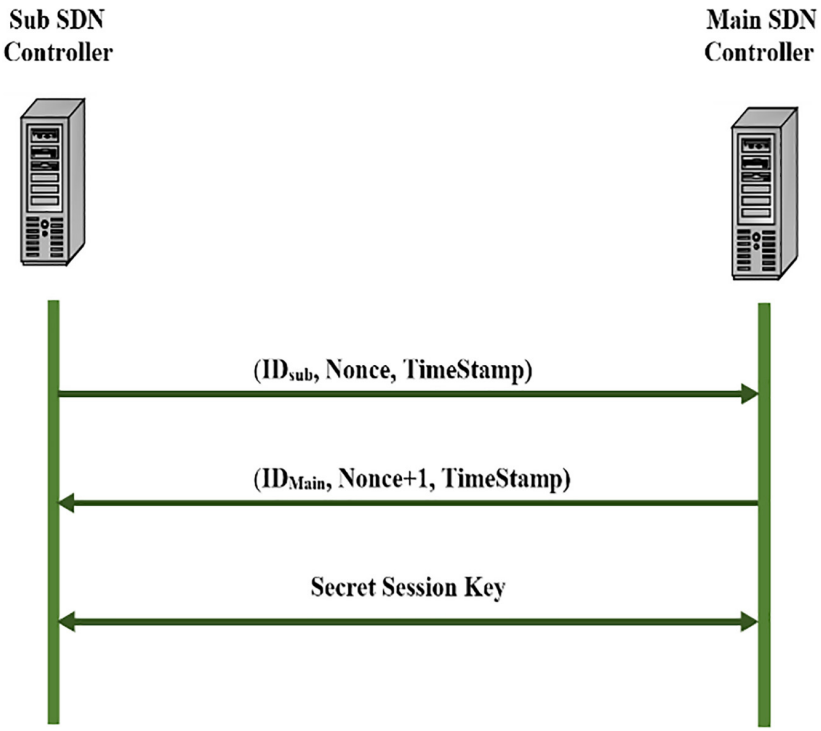

Fig. 6. Mechanism of communication between sub and main SDN controller

4.5 Communication between vehicles

For vehicle-to-vehicle communication, OBU_i encrypts the message with the group key (K_{Gi}) from its RSUi, signs it using EdDSA, and includes its certificate and a timestamp for freshness. Upon receiving the message, OBU_j checks the RSU_i ID, retrieves the corresponding key, decrypts the message, and verifies the sender's signature, timestamp (≤ 300ms), and certificate validity. To prevent replay attacks, the sender's current position can be included, allowing receivers to verify its authenticity (see Figure 7).

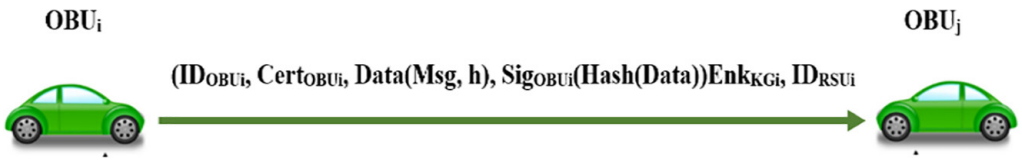

Fig. 7. Communication between vehicles

4.6 Revocation

In the revocation phase as shown in Figure 8, RSUs detect and report malicious vehicles to the CA, which decides whether to revoke their certificates. Certificates are also revoked if a vehicle's private key is lost or stolen. Revoked certificates are added to the CRL to inform RSUs and VANET vehicles. To improve verification efficiency, the CRL is divided into sub-CRLs based on vehicle type (e.g., professional or private), allowing faster certificate validation by limiting searches to relevant sub-lists.

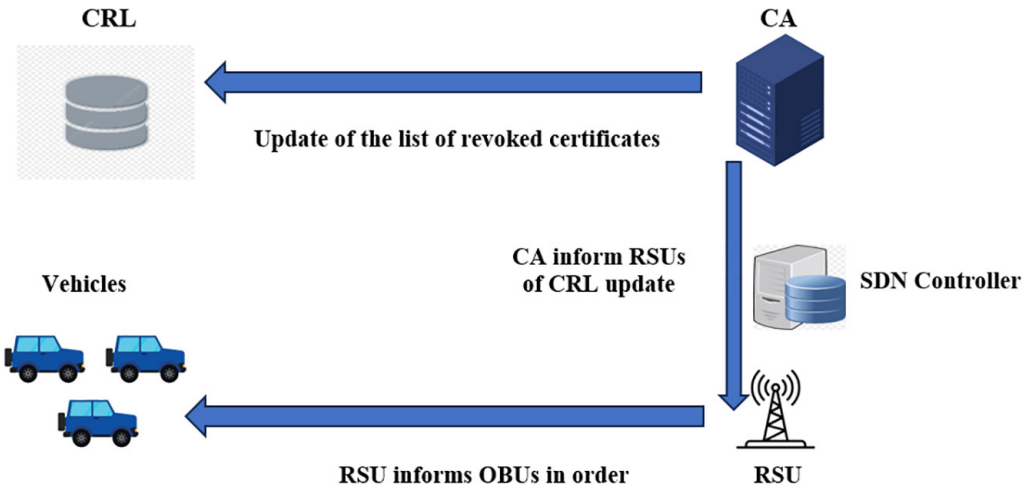

Fig. 8. The different steps of the evocation phase

5 SECURITY ANALYSIS

To demonstrate that our model can meet the security objectives and requirements, we examine the security analysis and the formal verification in this part.

5.1 Analysis of security requirements

Mutual authentication. To issue a public key certificate to an OBU, an authentication procedure is carried out in which the OBU and the CA mutually authenticate each other. Cookies are used in this process to verify that each entity is indeed who it claims to be. In the second phase of the solution, OBUs and RSUs exchange a series of messages to mutually authenticate and establish a secret key. The ECDH algorithm is used for this secret sharing. To facilitate V2V communication, the RSU also creates a group key (K_{Gi}) for each OBU inside its zone. For SDN side both the sub and main controllers generate a session key for secure communication.

Confidentiality. By encrypting authentication packets with the secret key that OBUs and CA share, our method guarantees their confidentiality.

Non-repudiation. Since each message sent over the VANET needs to be signed using the sender's private key, the signature allows the sender's identity to be confirmed. Following successful authentication, the CA and OBUs generate this key. The EdDSA technique and the sender's public key are used to verify this signature. By signing, a message's recipient can verify the sender's identity and guarantee non-repudiation.

Privacy preservation. By sending messages anonymously, individuals can protect their privacy by using genuine vehicle identification or pseudonyms. During the authentication procedure, the CA issues these pseudo-identifiers.

Availability. DoS attacks are designed to deplete a server's resources and render it unavailable; using cookies enables countering these assaults and, thus, ensuring server availability.

Integrity. In our system, the hash of the four messages transmitted in steps five and six allows us to confirm the integrity of these exchanges. The hash functions guarantee data integrity.

5.2 Formal verification

Using a formal, modular, and expressive language made available by the AVISPA (Automatic Validation of Internet Security Protocols and Applications) [16] software, we defined the protocols and their security features. SAT-based Model-Checker (SATMC), Tree-Automata-based Protocol Analyzer (TA4SP), CL-based Attack Searcher (CL-AtSe), and On-the-fly Model-Checker (OFMC) are some of the back-ends that use a variety of automatic machine analysis techniques. Our suggested approach's main objective is to confirm that it can offer a trustworthy key exchange across the different VANET organizations in order to safeguard the back-end server-based registration, authentication, and data transfer stages.

We can conclude that the suggested system can achieve our objective and withstand malicious attacks, including replay attacks, secrecy attacks, and DoS attacks, after testing this specification with the OFMC and CLAtSe backends. Figure 9 displays the outcomes of the model checking results.

```
% OFMC
% Version of 2006/02/13
SUMMARY
  SAFE
DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
  /home/span/span/testsuite/results/proposed-final.if
GOAL
  as_specified
BACKEND
  OFMC
COMMENTS
STATISTICS
  parseTime: 0.00s
  searchTime: 0.47s
  visitedNodes: 131 nodes
  depth: 10 plies
```

```
SUMMARY
  SAFE

DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
  TYPED_MODEL

PROTOCOL
  /home/span/span/testsuite/results/proposed-final.if

GOAL
  As Specified

BACKEND
  CL-AtSe

STATISTICS

  Analysed   : 1 states
  Reachable  : 1 states
  Translation: 0.09 seconds
  Computation: 0.00 seconds
```

Fig. 9. Results reported by the OFMC and CL-AtSe Back-ends

6 PERFORMANCE EVALUATION

This section compares our authentication protocol's performance to other protocols currently in use based on computation overhead and security.

6.1 Comparison of security performance

We have contrasted our protocol's security protocol performance with that of other authentication methods. The proposal may check the security level and offer the most comprehensive security performance, as indicated in Table 1.

We have evaluated our protocol against the security protocols of other authentication systems. The proposal may offer the most thorough security performance and verify the security level, as indicated in Table 1.

Table 1. Security performance comparison

Security Features	[17]	[18]	[19]	Proposed Scheme
Mutual Authentication	Yes	Yes	Yes	Yes
Confidentiality	Yes	Yes	Yes	Yes
Integrity	Yes	Yes	Yes	Yes
Non-repudiation	Yes	No	No	Yes
Privacy Preservation	No	Yes	Yes	Yes
Availability	No	No	No	Yes

6.2 Computation overhead

The computing cost required by our method and accompanying protocols is evaluated in this section. To determine the execution time of such single operations using existing and proposed protocols, the rational arithmetic C/C++ library (MIRACL) [20] is run on a computer with a 2.10 GHz CPU and 32G of memory [21].

The total amount of time spent by the vehicle, RSU and SDN controllers is known as the overheads that equal to PM + 2MTP + 5BP + 2BP + 4MTP in our proposed with PM (Point Multiplication), BP (Bilinear Pairing) and the Hash Function MTP (Map-to-Point). Table 2 illustrates the operations and their computation overheads.

Table 3 indicates the operation numbers of the computation overheads for the existing protocols and the proposed protocol. We exhibit the computation cost for OBU, RSU and SDN of the proposed protocol and the current protocols [17–19] in Figure 10.

Because the suggested protocol uses lightweight operations to perform mutual authentication, it is found to be faster than the protocols used in [17–19].

Table 2. Computation overhead of single operation

Operations	Description	Time (ms)
PM	Point Multiplication	2.258
BP	Bilinear Pairing	6.443
H	Hash (SHA-256)	0.021
EXP	Exponentiation in Bilinear Group	3.212
ENC	AES-128 Encryption	0.902
DEC	AES-128 Decryption	7.357
MM	Modular Multiplication	1.657
MP	Modular Square Root	2.942
MTP	Map-to-Point Hash Function	2.258
SING/VER	Signature/Verification EdDSA	3.21

Table 3. Comparison of computation overheads

Protocols	Operation Numbers		
	Vehicle's Side	RSU's Side	Total (ms)
[17]	PM + 2MTP + 5BP	2BP + 4MTP	48.352
[18]	4PM + 5H + 2EXP	3BP + 5H + 2EXP	41.419

(Continued)

Table 3. Comparison of computation overheads *(Continued)*

Protocols	Operation Numbers		
	Vehicle's Side	RSU's Side	Total (ms)
[19]	7PM	7PM	30.95
Our	2ENC + DEC + SING/VER + 2PM	ENC + 2DEC + SING/VER + PM	27.971

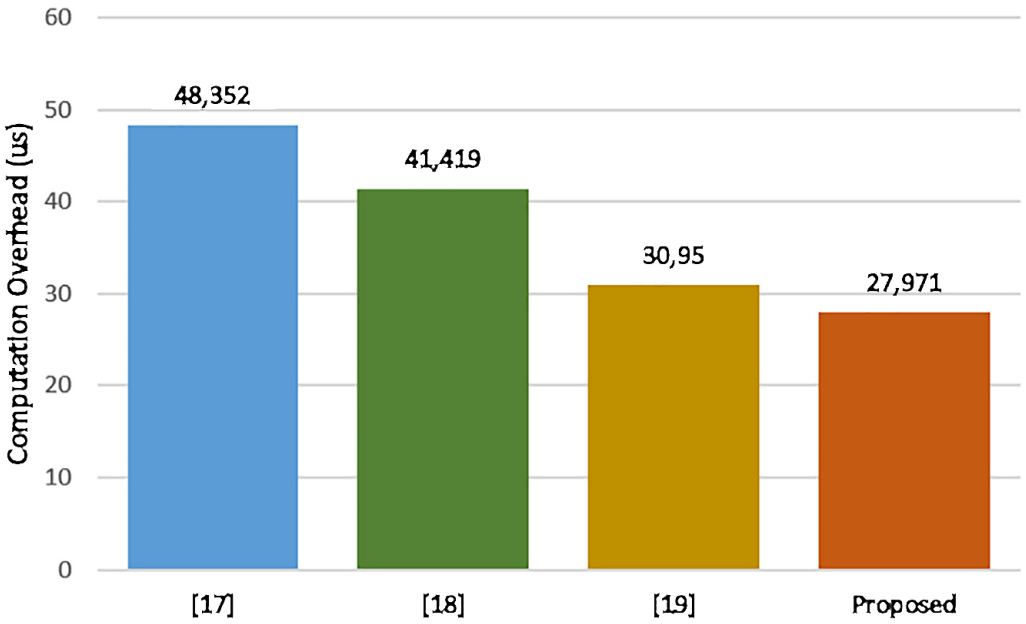

Fig. 10. Computation cost of different schemes

The proposed security infrastructure is designed with real-world deployment feasibility in mind. Its compatibility with 5G-V2X standards, particularly those defined by 3GPP for ultra-reliable low-latency communication (URLLC), ensures seamless integration into emerging vehicular networks. The lightweight cryptographic operations (EdDSA and ECDH) are well-suited for resource-constrained OBUs and RSUs, making them ideal for deployment in embedded vehicular systems. Furthermore, the optimized CRL structure—divided by vehicle type (e.g., professional, private, emergency services)—can significantly reduce verification latency, a crucial requirement for real-time vehicular communication. This modular CRL approach also facilitates prioritization of emergency vehicles in urban traffic scenarios. The overall framework is adaptable to both edge- and cloud-assisted architectures, enabling scalable integration in modern ITS infrastructures.

7 CONCLUSION

In this paper, we presented a privacy-aware and efficient model for secure infrastructure, which addresses important security and privacy concerns faced by centralized control in SDVN systems. Our proposed system incorporates sophisticated cryptographic techniques such as EdDSA for quick and secure authentication, ECDH for safe key exchange, and an upgraded CRL for effective management of compromised credentials. This combination offers low-latency connectivity, strong data protection, and better privacy preservation while maximizing resource efficiency. The results and analysis show that our strategy effectively mitigates common cyber dangers like unauthorized access

and data breaches while maintaining scalability and operational efficiency. Our method is ideal for real-time vehicle communications because it improves security and privacy while imposing minimal computational overhead. Future work will aim to integrate post-quantum cryptography, enhance trust management, and apply AI-based anomaly detection to improve security. We also plan to optimize the model for high-mobility scenarios and ensure compatibility with 5G-V2X and ETSI standards, while exploring edge and fog deployments for better scalability and low-latency performance.

8 REFERENCES

[1] M. Houmer, M. Ouaissa, M. Ouaissa, and M. L. Hasnaoui, "SE-GPSR: Secured and enhanced greedy perimeter stateless routing protocol for vehicular ad hoc networks," *International Journal of Interactive Mobile Technologies (iJIM)*, vol. 14, no. 13, pp. 48–64, 2020. https://doi.org/10.3991/ijim.v14i13.14537

[2] K. Nisar *et al.*, "A survey on the architecture, application, and security of software defined networking: Challenges and open issues," *Internet of Things*, vol. 12, p. 100289, 2020. https://doi.org/10.1016/j.iot.2020.100289

[3] M. Chouikik, M. Ouaissa, M. Ouaissa, Z. Boulouard, and M. Kissi, "The role of software-defined vehicular networks in society 5.0," in *Emerging Disruptive Technologies for Society 5.0 in Developing Countries*, in Advances in Science, Technology & Innovation, S. Arezki, M. Ouaissa, M. Ouaissa, M. Krichen, and A. Nayyar, Eds., Springer, Cham, 2025, pp. 237–242. https://doi.org/10.1007/978-3-031-63701-8_20

[4] M. Arif *et al.*, "SDN-based VANETs, security attacks, applications, and challenges," *Applied Sciences*, vol. 10, no. 9, p. 3217, 2020. https://doi.org/10.3390/app10093217

[5] R. Kumar and N. Agrawal, "A survey on software-defined vehicular networks (SDVNs): A security perspective," *The Journal of Supercomputing*, vol. 79, pp. 8368–8400, 2023. https://doi.org/10.1007/s11227-022-05008-y

[6] N. H. Hussein, C. T. Yaw, S. P. Koh, S. K. Tiong, and K. H. Chong, "A comprehensive survey on vehicular networking: Communications, applications, challenges, and upcoming research directions," *IEEE Access*, vol. 10, pp. 86127–86180, 2022. https://doi.org/10.1109/ACCESS.2022.3198656

[7] M. Chouikik, M. Ouaissa, M. Ouaissa, Z. Boulouard, and M. Kissi, "Detection and mitigation of DDoS attacks in SDN based intrusion detection system," *Bulletin of Electrical Engineering and Informatics*, vol. 13, no. 4, pp. 2750–2757, 2024. https://doi.org/10.11591/eei.v13i4.7570

[8] S. Kumar, B. Ben Sujin, K. Bhavani, D. Srilatha, and K. Anand, "Software defined network based next generation mobile communication network architecture," *International Journal of Interactive Mobile Technologies (iJIM)*, vol. 18, no. 23, pp. 138–148, 2024. https://doi.org/10.3991/ijim.v18i23.51337

[9] Y. Fan and N. Zhang, "A survey on software-defined vehicular networks," *J. Comput.*, vol. 28, no. 4, pp. 236–244, 2017.

[10] R. Sultana, J. Grover, and M. Tripathi, "Security of SDN-based vehicular ad hoc networks: State-of-the-art and challenges," *Vehicular Communications*, vol. 27, p. 100284, 2021. https://doi.org/10.1016/j.vehcom.2020.100284

[11] K. M. Ali Alheeti, A. Alzahrani, M. Alamri, A. Khairi Kareem, and D. Al_Dosary, "A comparative study for SDN security based on machine learning," *International Journal of Interactive Mobile Technologies (iJIM)*, vol. 17, no. 11, pp. 131–140, 2023. https://doi.org/10.3991/ijim.v17i11.39065

[12] W. B. Jaballah, M. Conti, and C. Lal, "Security and design requirements for software-defined VANETs," *Computer Networks*, vol. 169, p. 107099, 2020. https://doi.org/10.1016/j.comnet.2020.107099

[13] M. Ouaissa and A. Rhattoy, "A new scheme of group-based AKA for machine type communication over LTE networks," *International Journal of Electrical & Computer Engineering*, vol. 8, no. 2, pp. 1169–1181, 2018. https://doi.org/10.11591/ijece.v8i2.pp1169-1181

[14] A. P. Fournaris, I. Zafeirakis, C. Koulamas, N. Sklavos, and O. Koufopavlou, "Designing efficient elliptic curve Diffie-Hellman accelerators for embedded systems," in *2015 IEEE International Symposium on Circuits and Systems (ISCAS)*, 2015, pp. 2025–2028. https://doi.org/10.1109/ISCAS.2015.7169074

[15] D. J. Bernstein, S. Josefsson, T. Lange, P. Schwabe, and B. Y. Yang, "EdDSA for more curves," *Cryptology ePrint Archive*, 2015.

[16] AVISPA Project, https://avispa-project.org/main

[17] M. Han, L. Hua, and S. Ma, "A self-authentication and deniable efficient group key agreement protocol for VANET," *KSII Transactions on Internet and Information Systems*, vol. 11, no. 7, pp. 3678–3698, 2017. https://doi.org/10.3837/tiis.2017.07.021

[18] D. He, D. Wang, Q. Xie, and K. Chen, "Anonymous handover authentication protocol for mobile wireless networks with conditional privacy preservation," *Science China Information Sciences*, vol. 60, 2017. https://doi.org/10.1007/s11432-016-0161-2

[19] X. Li, Y. Han, J. Gao, and J. Niu, "Secure hierarchical authentication protocol in VANET," *IET Information Security*, vol. 14, no. 1, pp. 99–110, 2019. https://doi.org/10.1049/iet-ifs.2019.0249

[20] MIRACL Library, https://miracl.com/

[21] P. Wang, Y. Liu, and S. Lv, "An improved lightweight identity authentication protocol for VANET," *Journal of Internet Technology*, vol. 20, no. 5, pp. 1491–1504, 2019.

9 AUTHORS

Meryem Chouikik received her engineer's degree in Network and Telecommunications in 2021. She is currently a PhD student at FST Mohammedia, Morocco. Her research interests include Network, Telecommunications, Internet of Things, SDN and Communication Vehiculaire.

Mariya Ouaissa is a Professor in Cybersecurity and Networks at FSSM, Cadi Ayyad University, Marrakech, Morocco. She is a Ph.D. graduated in 2019 in Computer Science and Network from ENSAM, Moulay Ismail University, Meknes, Morocco. Her main research topics are Cybersecurity, IoT, M2M, D2D, WSN, Cellular Networks, and Vehicular Networks (E-mail: m.ouaissa@uca.ac.ma).

Mariyam Ouaissa is currently an Assistant Professor in Networks and Systems at ENSA, Chouaib Doukkali University El Jadida, Morocco. She has a Ph.D. in Computer Science and Networks graduated in 2019 from Moulay Ismail University, ENSAM, Meknes, Morocco. Her main research topics are IoT, M2M, WSN, Vehicular Networks, and Cellular Networks. She is mainly working on M2M congestion overload problem, security and the resource allocation.

Zakaria Boulouard is currently a Professor at Department of Computer Sciences at the Faculty of Sciences and Techniques Mohammedia, Hassan II University, Casablanca, Morocco. He received his PhD degree in 2018 from Ibn Zohr University, Morocco and his research interests include Artificial Intelligence, Big Data Visualization and Analytics, Optimization and Competitive Intelligence.

Mohamed Kissi received his PhD degree from the UPMC, France in 2004 in Computer Science. He is currently a Professor in Department of Computer Science, University Hassan II Casablanca, Faculty of Sciences and Technology, Mohammedia, Morocco. His current research interests include machine learning, data, and text mining (Arabic).