electronics

MDPI

Article

Mutual V2I Multifactor Authentication Using PUFs in an Unsecure Multi-Hop Wi-Fi Environment

Mohamed K. Elhadad [1,*] and Fayez Gebali [2,*]

[1] Department of Computer Engineering and Artificial Intelligence, The Military Technical College, Cairo 11766, Egypt
[2] Department of Electrical and Computer Engineering, University of Victoria, Victoria, BC V8W 3P6, Canada
* Correspondence: melhaddad@ieee.org or moh.elhadad@mtc.edu.eg (M.K.E.); fayez@uvic.ca (F.G.)

Abstract

Secure authentication in vehicular ad hoc networks (VANETs) remains a fundamental challenge due to their dynamic topology, susceptibility to attacks, and scalability constraints in multi-hop communication. Existing approaches based on elliptic curve cryptography (ECC), blockchain, and fog computing have achieved partial success but suffer from latency, resource overhead, and limited adaptability, leaving a gap for lightweight and hardware-rooted trust models. To address this, we propose a multi-hop mutual authentication protocol leveraging Physical Unclonable Functions (PUFs), which provide tamper-evident, device-specific responses for cryptographic key generation. Our design introduces a structured sequence of phases, including pre-deployment, registration, login, authentication, key establishment, and session maintenance, with optional multi-hop extension through relay vehicles. Unlike prior schemes, our protocol integrates fuzzy extractors for error tolerance, employs both inductive and game-based proofs for security guarantees, and maps BAN-logic reasoning to specific attack resistances, ensuring robustness against replay, impersonation, and man-in-the-middle attacks. The protocol achieves mutual trust between vehicles and RSUs while preserving anonymity via temporary identifiers and achieving forward secrecy through non-reused CRPs. Conceptual comparison with state-of-the-art PUF-based and non-PUF schemes highlights the potential for reduced latency, lower communication overhead, and improved scalability via cloud-assisted CRP lifecycle management, while pointing to the need for future empirical validation through simulation and prototyping. This work not only provides a secure and efficient solution for VANET authentication but also advances the field by offering the first integrated taxonomy-driven evaluation of PUF-enabled V2X protocols in multi-hop Wi-Fi environments.

Keywords: vehicular area networks; multi-hop communications; physical unclonable functions; mutual authentication

check for updates

Academic Editor: Daniel Gutiérrez Reina

Received: 4 July 2025
Revised: 21 October 2025
Accepted: 22 October 2025
Published: 24 October 2025

Citation: Elhadad, M.K.; Gebali, F. Mutual V2I Multifactor Authentication Using PUFs in an Unsecure Multi-Hop Wi-Fi Environment. *Electronics* **2025**, *14*, 4167. https://doi.org/10.3390/electronics14214167

Copyright: © 2025 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

1. Introduction

Intelligent transportation systems (ITS) are a direct product of advances in information systems and the Internet of Things (IoT). Smart vehicles and vehicle area networks (VANs) are now a reality [1–3]. Vehicle-to-vehicle (V2V) communication allows nearby vehicles to exchange relevant data. Vehicles also communicate with infrastructure such as traffic lights and signs via vehicle-to-infrastructure (V2I) and vehicle-to-everything (V2X) communication modes. This naturally demands securing these interactions ensuring data privacy, and authenticating communicating entities [4,5].

Public key protocols such as elliptic curve cryptography (ECC) and Rivest–Shamir–Adleman (RSA) are very powerful, but they are mainly used for data hiding and digital signatures. The secret key is never shared. On the other hand, the physical unclonable functions (PUFs) used here are used for simple symmetric encryption and are mainly used for mutual authentication and secure key management [6].

Both V2V, V2I and V2X utilize conventional vehicle security and authentication protocols to facilitate this secure exchange in data [7–10]. These protocols face the following challenges:

1. The dynamic nature of the network topology results from the mobility of the vehicles and the need for handover and continually authenticating vehicles that move into the coverage area.
2. Network scalability, where the number of vehicles and the extent of the coverage area vary from limited inside a municipality to very large for a highway. Handover of security certificates becomes necessary in the microscale of a city block, for example.
3. Heterogeneity due to use several types of network infrastructure and manufacturers of vehicles.
4. Identifying priorities and handling the different types of network traffic.
5. Detecting malicious vehicles or the onset of attacks on the infrastructure and the vehicles themselves.
6. Secret keys are typically stored in non-volatile random access memory (NVRAM), which can be attacked to extract the secret keys and duplicate them.
7. Secret keys cannot be static since this opens the doors to several types of attacks. Dynamic session keys are costly unless vehicles are equipped with physical unclonable functions (PUFs) [11].

PUFs have been used earlier for authentication, but the protocols used were simple since the PUF was used only to authenticate the device to the challenger. It was not clear how the challenger knows the expected response. Furthermore, the device typically sends back the expected response to be verified by the challenger. This is a one-time password scheme (OTP) where this challenge-response pair cannot be used again. In our proposed protocol here, the same challenge-response pair can be used as often as desired since the response is never revealed to the challenger.

This PUF technology offers a novel approach for authenticating vehicles by infrastructure and also allows for authenticating the infrastructure by the vehicles themselves (as will be shown in the proposed protocol). Using PUFs also facilitates secure and dynamic session key exchange and immunity to tampering. PUFs harness the inherent physical variations in hardware during the manufacturing process to endow devices with unique identities, which can be pivotal in generating and distributing secure secret keys among vehicles in a network [11]. It is imperative in V2X to be equipped with robust security mechanisms that include PUFs in their design as a hardware-based security mechanism.

This manuscript introduces a novel framework for vehicle authentication in VANs, specifically designed to address the aforementioned limitations by incorporating PUFs and ensuring anonymity in vehicle authentication.

1.1. Contributions

The contributions of this work are summarized as follows:

1. Using PUFs installed on each vehicle helps achieve mutual authentication between the vehicle and roadside unit (RSU), drones, etc.
2. Proposal of secure, anonymous and lightweight mutual authentication and key exchange protocols. The proposed protocol does not require clock synchronization, which is needed for timestamp-based mutual authentication protocols.

3. Proposal of a secure key exchange protocol between several vehicles in the same RSU coverage area to accomplish secure multi-hop packet store-and-forward Wi-Fi network.
4. Incorporation of freshness and presence properties in the proposed protocols to enhance security and prevent several impersonation attacks through context awareness and transaction history.
5. Evaluation of the proposed protocols using informal security analysis.
6. Evaluation of the proposed protocols using formal security analysis.

1.2. Organization of the Paper

The remainder of this paper is structured as follows: Section 2 reviews related work in the field of vehicle authentication protocols, highlighting the gaps our study aims to fill. Section 3 details the proposed mutual authentication and key exchange protocols and mechanisms for ensuring anonymity and security. Section 4 presents the security analysis using informal as well as formal techniques. Section 5 summarizes the main features of the proposed multifactor V2I authentication protocol. Section 6 discusses the advantages of the proposed security protocols. Section 7 discusses some protocol limitations and future research directions.

The notations used in the proposed schemes are alphabetically presented in Table 1.

Table 1. Notations and parameters used in the proposed authentication protocol.

Notation	Definition/Description
V_i	Vehicle node i equipped with an On-Board Unit (OBU).
R	Roadside unit (RSU) serving as a local infrastructure node.
C	Cloud Authority/Trusted Third Party responsible for CRP management.
ID_i	Permanent identity of vehicle i assigned by the authority.
PW_i	Password or secret credential of vehicle i.
k_i	Long-term secret key of vehicle i (shared with C).
$Cert_R$	Short-lived digital certificate issued by C to RSU R.
$PUF(\cdot)$	Physical Unclonable Function producing unique responses from challenges.
CRP	Challenge–Response Pair (c_j, r_j) derived from a PUF.
c_j	PUF challenge j.
r_j	Ideal PUF response corresponding to c_j.
r'_j	Noisy response generated in practice under environmental factors.
$helper_data$	Public data enabling error correction of noisy PUF responses.
$FE(\cdot)$	Fuzzy Extractor algorithm for reconstructing reliable keys from noisy PUFs.
TID_i	Temporary Identifier for V_i used to preserve anonymity.
$nonce_v, nonce_r$	Random nonces generated by vehicle V_i and RSU R, respectively, for freshness.
n_i	Authentication token computed by V_i: $n_i = H(ID_i \parallel k_i \parallel PW_i \parallel nonce_v)$.
$E_{pk_X}(\cdot)$	Asymmetric encryption under the public key of entity X.
$H(\cdot)$	Cryptographic one-way hash function (e.g., SHA-256).
$K_{V_i,R}$	Session key established between vehicle V_i and RSU R.
$LoginReq$	Encrypted login request message from V_i to R.
$AuthCheck$	Authentication request message sent from R to C.
$Resp$	Response from V_i during PUF-based challenge–response authentication.

2. Related Works

Vehicular Ad Hoc Networks (VANETs) represent one of the most challenging environments for secure authentication due to their high mobility, dynamic topology, and stringent latency requirements. Over the past decade, a wide range of solutions have been proposed, which can broadly be classified into four paradigms: (i) conventional cryptography-based schemes, (ii) blockchain-based frameworks, (iii) fog/edge-assisted models, and (iv) hardware-assisted protocols using Physical Unclonable Functions (PUFs). In this section, we critically analyze each paradigm in terms of its motivation, mechanisms, and shortcomings before synthesizing the research gap that motivates our contribution. Our review adopts a systematic mapping approach [12,13], ensuring that we not only catalog prior work but also identify structural limitations across categories.

2.1. Cryptography-Based Protocols

Traditional VANET authentication mechanisms have primarily relied on public-key cryptography. Elliptic Curve Cryptography (ECC) [14] has been widely used because of its reduced key size and efficiency compared to RSA. Identity-Based Cryptography (IBC) [15] was introduced to eliminate certificate overhead, while group signature schemes [16] were designed to ensure conditional anonymity of vehicles with traceability for accountability.

While these schemes represent significant progress, several issues persist. First, they assume secure storage of long-term private keyswithin On-Board Units (OBUs), but real vehicles remain vulnerable to physical tampering. Compromised OBUs enable large-scale impersonation attacks, invalidating cryptographic guarantees. Second, certificate revocation is a major bottleneck: large Certificate Revocation Lists (CRLs) [17] must be distributed frequently, leading to bandwidth overhead. This is particularly critical in multi-hop Wi-Fi environments, where latency accumulates at each hop, often exceeding the 100 ms threshold mandated for safety-critical messages. Furthermore, most studies evaluate these approaches under idealized conditions rather than at an urban scale, meaning the true scalability of cryptography-based VANET authentication remains questionable.

2.2. Blockchain-Based Frameworks

To overcome centralized trust anchors, blockchain has been proposed as an alternative for vehicular identity and message verification [18,19]. By leveraging a tamper-evident distributed ledger, blockchain promises transparency, accountability, and resilience against single points of failure. Several models rely on RSUs or fog nodes as consensus participants, theoretically ensuring decentralized validation of vehicles.

However, the practicality of blockchain for real-time VANET security is limited. Consensus algorithms such as Proof-of-Work (PoW) and Proof-of-Stake (PoS) impose computational and time overheads on the order of seconds, which is incompatible with the millisecond-scale requirements of vehicular safety applications. Even consortium or PBFT-based blockchains suffer from excessive message complexity when scaled to thousands of participants. Moreover, the obligation to store and synchronize a continuously growing ledger is unrealistic for OBUs with limited resources. Consequently, blockchain approaches, while attractive for post-incident forensics or liability attribution, are fundamentally misaligned with the ultra-low latency demands of V2X authentication.

2.3. Fog and Edge-Assisted Protocols

The fog/edge paradigm [20,21] seeks to reduce end-to-end latency by moving authentication closer to vehicles. Fog nodes deployed at RSUs perform lightweight authentication and manage session keys locally, thereby alleviating the reliance on distant cloud servers.

Several studies demonstrate that this approach reduces average authentication delay and improves throughput for time-sensitive vehicular communication.

Despite these advantages, fog-based approaches face multiple unresolved issues. First, they typically rely on static symmetric or asymmetric keys, making them vulnerable once a fog node is compromised. Unlike cloud infrastructures, fog nodes are geographically distributed and more susceptible to physical capture by adversaries. Second, their security guarantees are bounded by the trustworthiness of fog infrastructure, which may vary by operator and jurisdiction. Third, most performance studies evaluate only small-scale topologies with simplified channel assumptions, overlooking the complex dynamics of multi-hop Wi-Fi relays and high-density urban mobility. Finally, fog solutions fail to leverage hardware-level unclonability, which is vital for ensuring that compromised software does not lead to unrestricted impersonation.

2.4. PUF-Based Authentication Protocols

Physical Unclonable Functions (PUFs) [22,23] represent a promising alternative to key-storage-based models. PUFs exploit intrinsic manufacturing randomness to generate unique challenge–response pairs (CRPs), eliminating the need for permanently stored cryptographic keys. This property makes them highly resistant to invasive attacks, as no secret exists until the PUF is challenged.

PUFs have been integrated into vehicular protocols to provide lightweight authentication with minimal computational load. However, current PUF-based VANET schemes exhibit significant limitations. Many only enable unidirectional authentication, verifying vehicles to RSUs but not vice versa, leaving vehicles exposed to rogue RSUs. Most assume direct communication between vehicles and RSUs, neglecting the reality of multi-hop Wi-Fi forwarding where relay vehicles are necessary. Additionally, the scalability problem of CRP management remains unresolved: large fleets require millions of CRPs to be generated, distributed, and refreshed, which is impractical without centralized orchestration. Finally, PUF outputs are inherently noisy; without mechanisms such as fuzzy extractors or helper data [24], error rates can render authentication unreliable under environmental variations such as temperature or voltage changes.

2.5. Comparative Analysis and Research Gap

Taken together, prior works highlight the difficulty of balancing performance, scalability, and security in VANET authentication. Cryptographic schemes provide strong theoretical security but suffer from latency and revocation bottlenecks. Blockchain approaches deliver tamper resistance but introduce prohibitive consensus delays. Fog-assisted methods reduce latency but inherit vulnerabilities from their infrastructure. PUF-based schemes offer unclonability and lightweight computation but are restricted to unidirectional, single-hop contexts with unresolved scalability challenges.

Research Gap: To date, no existing approach simultaneously achieves the following: (i) bi-directional trust between vehicles and infrastructure, (ii) seamless multi-hop Wi-Fi forwarding, (iii) freshness and presence guarantees resistant to replay and desynchronization attacks, and (iv) scalable CRP lifecycle management integrated with cloud resources. Addressing this multi-dimensional gap requires rethinking how hardware trust primitives are combined with scalable architectures.

Table 2 provides a comparison matrix for the different authentication approaches, showing the relative strengths and weaknesses across latency, scalability, trust, and unclonability.

Table 2. Comparative feature matrix of authentication approaches, showing the relative strengths and weaknesses across latency, scalability, trust, and unclonability.

Approach	Latency	Scalability	Bi-Directional Trust	Unclonability	CRP Lifecycle Managment
Cryptography-Based	High	Poor	Yes	No	Not Supported
Blockchain-Based	High	Poor	Yes	No	Not Feasible
Fog/Edge-Assisted	Low	Moderate	Parital	No	Not Addressed
PUF-Based	Low	Poor	Unidirectional	Yes	Not Scalable
Proposed Work	Low	High	Yes	Yes	Full Support

In the context of VANET authentication, high latency refers to delays exceeding roughly 100 ms, which would not meet the stringent requirements of safety-critical V2X applications [25]. Conversely, low latency implies end-to-end delays on the order of a few tens of milliseconds (e.g., <50 ms), suitable for real-time communication. A moderate latency rating lies between these extremes (approximately 50–100 ms). Similarly, we qualify scalability in terms of the number of vehicles an RSU or domain can handle. High scalability denotes support for on the order of hundreds of nodes (around > 500 vehicles per RSU) without significant performance degradation [26]. A poor scalability rating implies the scheme can only manage on the order of mere tens of vehicles (e.g., <50 per RSU) before encountering bottlenecks. Ratings like "moderate scalability" fall in between (handling a few dozen up to a few hundred vehicles). These threshold values are grounded in ranges commonly reported in VANET studies; for example, safety message latencies around 100 ms are considered low-latency requirements [25], and recent high-density V2X experiments scale to 500-node networks as a stress test for authentication protocols [26]. By basing our qualitative terms on such established figures, Table 2's comparative analysis is made more concrete and transparent. This ensures that descriptors like "high" or "low" latency, "good" or "poor" scalability, etc., are interpreted consistently against typical benchmarks in the literature, rather than as subjective labels.

Figure 1 provides a taxonomy of the different authentication approaches in VANETs. Cryptographic, blockchain, fog/edge, and PUF paradigms are contrasted with the proposed framework.

2.6. Our Contribution

This work advances the state of the art by proposing the first integrated PUF-based authentication framework that achieves the following:

1. Provides bi-directional authentication,securing both vehicles and RSUs against impersonation.
2. Natively supports multi-hop Wi-Fi forwarding, addressing the realities of vehicular connectivity.
3. Incorporates freshness and presence guarantees using nonces, temporary identifiers, and inductive proofs.
4. Introduces cloud-assisted CRP management to ensure scalability for large fleets.

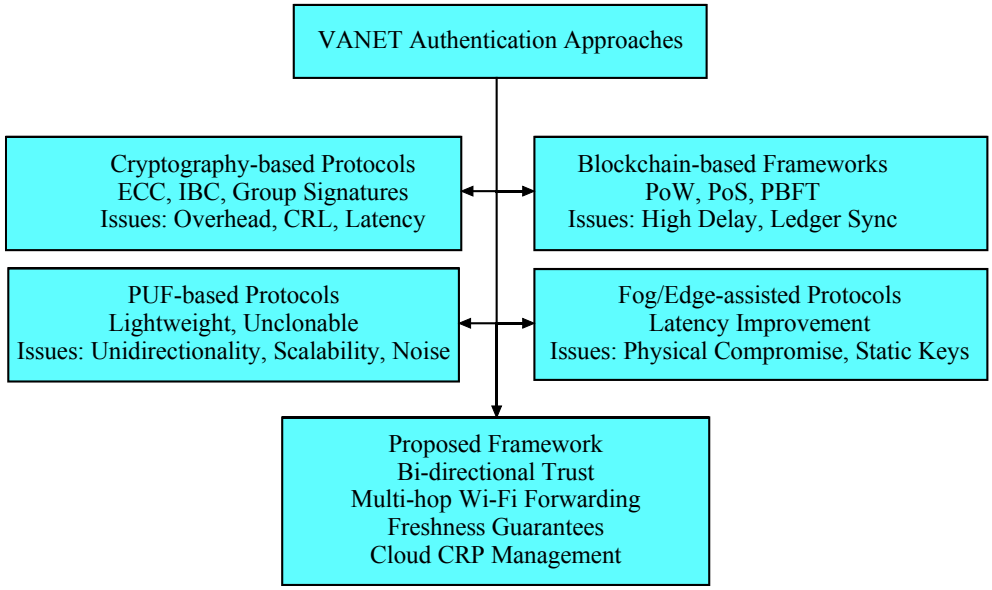


Figure 1. Taxonomy of authentication approaches in VANETs. Cryptographic, blockchain, fog/edge, and PUF paradigms are contrasted with the proposed framework.

3. Proposed Multihop Wi-Fi Authentication Scheme

Before discussing the proposed protocol, we provide a brief account of how a PUF is used to establish mutual authentication and a reliable key exchange mechanism through a helper data algorithm. The steps to use the PUF to enable the server to authenticate the client and exchange the same key are as follows 10:

1. The server obtains the challenge/response of a certain PUF from the device manufacturere (CRP).
2. The server selects a challenge c and its associated response r.
3. The server generates the helper data w, which is similar to forward error correction coding:
$$w = \mathrm{FEC}(r).$$
4. The server generates a hash using r to obtain a one-time password and a secret key
$$[h, k] = \mathrm{H}(r,\ w).$$
5. The server sends c and w to the client. Note that this does not reveal any secret information.
6. The client uses its PUF to obtain a noisy response $r' = \mathrm{PUF}(c)$.
7. The client removes the noise from the response using received w,
$$r'' = \mathrm{FEC}(r', w)$$
8. The client uses the noise-free response to generate the secret key and has a pair
$$[h', k'] = \mathrm{H}(r'',\ w).$$
9. The client sends h'' to server to complete the authentication and key exchange.
10. The server compares its h with the received h''. If both match, then authentication and secret key exchange are deemed successful.

We discuss here our proposed secure and anonymous vehicle authentication protocols. The protocols use PUFs, context awareness and transaction history to achieve higher security levels.

Our mutual authentication schemes has the following phases:

1. Pre-deployment phase;
2. Registration phase;
3. Vehicle login phase;
4. Multi-hop mutual authentication phase;
5. Multi-hop communication phase.

Figure 2 shows the system under consideration.

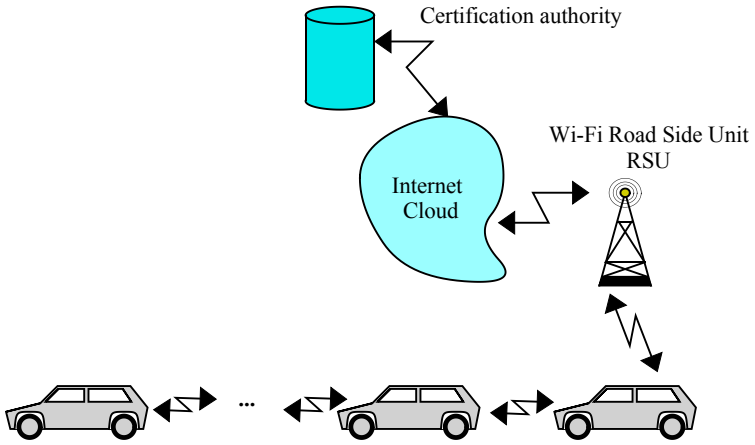


Figure 2. The multi-hop Wi-Fi VAN system under consideration.

The main entities are certification authority (C), roadside units (RSU or R) and smart vehicles (V_i) containing Wi-Fi gateways and attached IoT sensor and actuator devices. Each vehicle is registered at the certification authority using the fabrication information supplied by the vehicle manufacturer. The vehicle gateway is responsible for establishing and monitoring communication between the vehicle and other vehicles or RSUs.

Wi-Fi communication is established by roadside units (RSU). The RSU is able to contact certification authorities to obtain information about vehicles in its coverage area. The figure shows at least one vehicle can directly connect to the RSU. However, most of the vehicles in the given geographical area are not in direct contact with the RSU.

To reach the RSU, these vehicles must depend on collaborative multi-hop communication as shown.

We state some basic assumptions for our analysis as follows:

1. A coverage area is one that is served by an infrastructure device, e.g., an RSU, that can be considered a root-of-trust (RoT).
2. Not all vehicles have direct access to the infrastructure and must rely on a cooperative multi-hop message store-and-forward strategy.
3. Not all vehicles are trusted since some malicious vehicles might be present in the system
4. All trusted vehicles must have a PUF, or an equivalent synthetic $\{CRP\}$ set, to facilitate creation of a unique ID, generation of a secret key exchange, and mutual authentication between vehicles and the RSU.

3.1. Pre-Deployment Phase

The two main players here are the roadside unit (RSU or R) and vehicles (V).

3.1.1. Roadside Unit (RSU or R)

The roadside units are considered a root-of-trust (RoT) and are responsible for establishing secure communication and mutual authentication with the certification authority (C). A symmetric secret key k_{rc} is established between R and the certification authority C. Communication between R and C could be direct or via an RSU hierarchy to reduce and enhance the cost of communication.

3.1.2. Pre-Deployment for Vehicles (V)

The pre-deployment phase is conducted by the vehicle manufacturer, or more specifically the PUF fabricator, prior to selling the vehicle. A vehicle V_i is given the following three unique parameters:

1. Identity (ID_i);
2. Password (PWD_i);
3. Symmetric key k_i.

In addition, a vehicle could be supplied with a PUF that can generate its unique set of challenge/response pair set ($\{CRP\}$). If a PUF is not chosen, then the manufacturer assigns a unique secret key k to be used between the roadside unit and the vehicle.

The vehicle manufacturer supplies the vehicle parameters (ID_i, PWD_i, k_i, $\{CRP\}_i$) to the certification authority C to be used for the login and authentication phases of vehicles. Listing 1 summarizes the steps needed to construct the PUF challenge response set $\{CRP\}$ to complete the vehicle pre-deployment phase.

Listing 1. Vehicle pre-deployment phase.

1	*Fab*	:	$ID_i = \text{Assign_ID}(V_i)$	
2		:	$\{PWD\}_i = \text{Assign_PWD}(V_i)$	
3		:	$k_i = \text{Assign_key}(V_i)$	
4		:	$\{CRP\}_i = \phi$	% Initialize $\{CRP\}$
5		:	**FOR** $j = 1 : n$ **DO**	
6		:	$r_j = \text{PUF}_j(c_j)$	
7		:	$\{CRP\}_i = \text{Concatenate}(\{CRP\}_{i-1} \| \| c_j r_j)$	% Build CRP
8		:	**END FOR**	
9	$Fab \rightarrow C$	:	$PKI(ID_i \| \| PWD_i \| \| k_i \| \| \{CRP\}_i)$	Public key communication

The protocol in Listing 1 allows the device fabricator (Fab) to characterize the PUF after its fabrication to extract its challenge-response pair set $\{CRP\}$. Further, the device fabricator shares this set with a trusted certification authority (C) for sharing with other trusted entities.

3.2. Registration Phase

The main goal of the registration phase is to have the main players exchange public key infrastructure (PKI) credentials as follows:

1. C will share its public key K_c with the RSUs that register with it;
2. RSU will share its public key K_r with C;

3. *RSU* will keep broadcasting a `HELLO`(K_r) message over its coverage area so that incoming vehicles are aware of the RSU public key to use when they desire to login, as discussed in Section 3.3.

3.3. Vehicle Login Phase

Listing 2 shows the vehicle login to an RSU. Login starts by the vehicle contacting the RSU using the latter's public key k_r. Using public key infrastructure (PKI) ensures the vehicle's anonymity. The vehicle supplies its ID and a secret session parameter ϕ_i.

Listing 2. Vehicle login to a roadside unit phase.

1	V_i	:	$n_i = h(ID_i \| \| PWD_i \| \| k_i)$	% Generate a secret parameter
2	$V_i \rightarrow R$	:	$(\mathrm{ID}_i \| \| n_i)$	% Request registration
3	$R \rightarrow C$	:	$E_{k_c}(ID_r \| \| \mathrm{ID}_i)$	% Request V_i parameters
4	$C \rightarrow R$	:	$E_{k_r}(\{CRP\}_i)$	
5	R	:	$n_i' = h(ID_i \| \| PWD_i \| \| k_i)$	
6	R	:	**IF** $n_i = n_i'$	
7		:	Admit V_i	% V_i joins R's coverage area
8		:	**END IF**	

Step 1 : The vehicle prepares a unique hash (ϕ_i) for multifactor authentication, ensuring freshness and presence.
Step 2: The vehicle sends an encrypted message to R using the RSU public key that it obtained from R's `Hello`(k_r) broadcast message.
Step 3: The RSU encrypts a message to request vehicle V_i credentials from C using C's public key k_c.
Step 4: C sends vehicle V_i credentials to R using RSU public key k_r.
Step 5: R independently calculates the hash (ϕ_i').
Steps 6–8: R checks the has values to complete the login phase.

3.4. Multi-Hop Mutual Authentication Phase

The mutual authentication phase is performed between an RSU (R) and a vehicle (V_i) when the vehicle is located within R's coverage area and is already registered. The unique feature in the protocol proposed in this subsection is that both the server R and vehicle V_i execute mutual authentication using the PUF present in the vehicle. This is the first time in the literature, as far as the authors are concerned, that a PUF is used not only to authenticate the device to the server but also to authenticate the server to the device.

3.5. Communication Phase

In the multi-hop communication phase, data routing between an RSU and a certain vehicle is accomplished through collaborative store-and-forward data exchange.

3.5.1. Direct Link Between Vehicle and RSU

We encounter two situations in this phase. The first situation is when the transmitting vehicle V_0 has a direct link with the RSU. At this stage and following the login and mutual authentication phases, the following information is shared:

1. Shared secret session key k_0;
2. Vehicle V_0 uses its temporary ID (TID_0) to preserve its anonymity;
3. A nonce n_0 is shared during the login phase to ensure freshness and presence.

The protocol in Listing 3 illustrates the case when V_0 needs to send a message to the RSU when a direct link is available.

Listing 3. Vehicle V_0 communicates with a roadside unit (RSU) when a direct link is available.

1	V_0	:	$n_0 = \text{Generate_Nonce}()$
2		:	$h = H([TID_0 \| \| n_0])$
3	$V_0 \rightarrow R$	:	$m_0 = E_{k_i}([Data \| \| n_0 \| \| h])]$
4	R	:	$[Data \| \| n_0 \| \| h])] = D_{k_i}(m_0)$
5		:	$h' = H([TID_0 \| \| n_0])$
6		:	$\text{Authenticate}(h, h')$

At the end of the protocol in Listing 3 transmitting vehicle V_0 succeeds in securely transmitting the message to RSU while maintaining its anonymity using temporary ID (TID_0)), privacy using encryption, and proof of presence and freshness using nonce n_0.

3.5.2. Indirect Link Between Vehicle and RSU

The second situation is when there is no direct link between the vehicle and the RSU. In that case, seeking the aid of authenticated other vehicles is needed to properly establish a link between the vehicle V_0 and RSU. Figure 3 illustrates this situation.

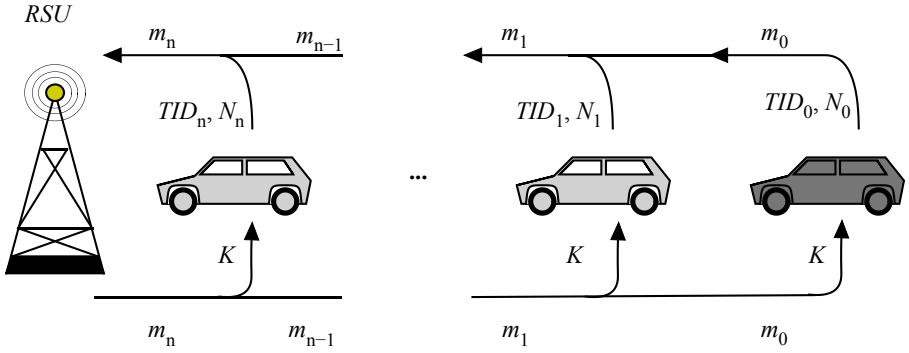


Figure 3. Communication between vehicle V_0 and an RSU when a direct link is not available. n intermediate vehicles V_1 to V_n execute a multi-hop store-and-forward system. A symmetric shared key K is defined for the RSU and vehicles V_0 to V_n.

The figure shows vehicle V_0 is attempting to communicate with R but requires the services of n intermediate vehicles (TID_i), where some of these vehicles might not have been authenticated and should not be trusted. A secret shared key K will be generated between R and V_0 and also involve the n other intermediate vehicles V_i with $1 \leq i \leq n$.

This situation is challenging since there is no authentication or shared secret key between the source vehicle V_0 and the intermediate vehicles. The protocol in Listing 4 illustrates the case when V_0 needs to establish communication with the RSU when a direct link is not available and a multi-hop packet store-and-forward is used. We assume the case of n intermediate vehicles V_1 to V_n.

Notice in the protocol in Listing 4, Line 1, that transmitting vehicle V_0 sends its location GPS_0 to help establish the best routing path to the destination RSU.

Listing 4. Vehicle communication with a roadside unit (RSU) when a direct link is not available and the vehicle requests to transmit to the RSU via n intermediate nodes.

1	V_0	:	Req_XMT(TID_0, R, GPS_0)	% $V_0 \rightarrow R$
2	$V_1 \rightarrow V_0$	:	ACK(TID_1, TID_0)	% V_1 near V_0
3	$V_0 \rightarrow V_1$	:	$m_0 = E_{k_0}(TID_0 \| \| N_0)$	
4.a		:	**FOR** $i = 1 : n - 1$ **DO**	
4.b	V_i	:	Req_XMT(TID_i, R, GPS_i)	
4.c	V_{i+1}	:	ACK(TID_{i+1}, TID_i)	
4.b	$V_i \rightarrow V_{i+1}$	:	$m_i = \left[E_{k_i}(TID_i \| \| N_i) \| \| m_{i-1}\right]$	
4.c		:	**END FOR**	
5	$V_n \rightarrow R$	:	Req_XMT(TID_n, R, GPS_n)	
7	R	:	ACK(R, TID_n)	
8	$V_n \rightarrow R$	:	$m_n = [E_{k_n}(TID_n \| \| N_n) \| \| m_{n-1}]$	
9.a	R	:	$K =$ Generate_secret_key$(\cdots)$	
1	R	:	Req_XMT(R, V_n)	
2	$V_n \rightarrow R$	:	ACK(TID_n, R)	
9.b	$R \rightarrow V_n$	:	$m_n = E_{k_n}(K)$	
9.c		:	**FOR** $i = 1 : n$ **DO**	
9.d	R	:	$m_i = E_{k_i}[K \,\|\| \, m_{i-1}]$	% augmented message
9.e		:	**END FOR**	
10	$R \rightarrow V_n$	:	m_n	
11.a		:	**FOR** $i = n : -1 : 1$ **DO**	
11.a	$V_i \rightarrow V_{i-1}$	:	$E_{k_i}(m_i)$	
11.b	V_{i-1}	:	$m_{i-1} = \text{DEC}_{k_{i-1}}(m_i)$	
11.a		:	**END FOR**	

3.6. Overall Protocol: Putting It All Together

Algorithm 1 summarizes all the operations discussed in Listings 1 to 4. The algorithms shows all the phases necessary to achieve mutual authentication using PUFs. There are six essential phases in the algorithm starting with pre-deployment at the PUF manufacturer and exchange of secret PUF data with trusted certification authorities that communicate with associated infrastructure such as roadside units.

Figure 4 provides a flowchart for the steps performed in Algorithm 1. The main players involved in execution of the algorithm are the vehicles, and any multi-hop relay vehicles, roadside units infrastructure, certification authorities and the PUF manufacturer or fabricator. It should be mentioned here that vehicles only communicate among themselves or the roadside units. There is no direct communication between vehicles and certification authorities.

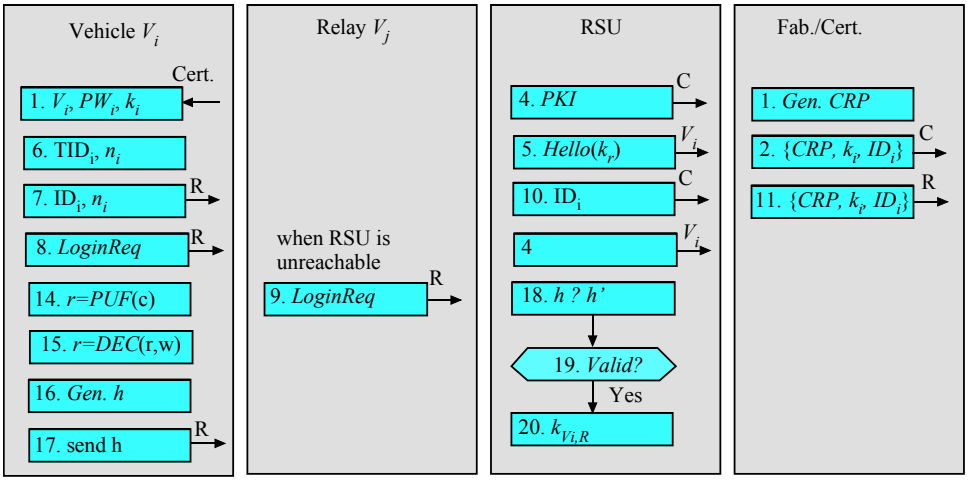


Figure 4. Summarizing the main steps done by the protocol main players for performing Algorithm 1.

Algorithm 1: Multi-hop mutual authentication protocol using PUFs

Input: Vehicle V_i with identity ID_i, password PW_i, secret k_i, and PUF-generated CRPs $\{(c_j, r_j)\}_i$; RSU R; cloud authority C.

Output: Secure session key $K_{V_i,R}$ established between V_i and R, extendable to multi-hop forwarding.

Phase 1: Pre-deployment (manufacturing/initialization) ;

1. Fab house generates CRP set $\{(c_j, r_j)\}_i$ for V_i via its PUF.
2. Fab house sends to cloud authority C vehicles' (ID_i, PW_i, k_i).
3. C stores $\{(c_j, r_j)\}_i$ in its CRP database, indexed by ID_i.

Phase 2: Registration ;

4. RSU R establishes a TLS/PKI-secured link with C.
5. R broadcasts a HELLO and its public key to nearby vehicles.

Phase 3: Login (vehicle $\rightarrow$ RSU) ;

6. V_i generates TID_i and computes nonce n_i.
7. V_i sends (ID_i, n_i) to R
8. V_i sends $LoginReq = E_{pk_R}(ID_i, TID_i, \phi_i, nonce_v)$ to RSU R.
9. If R is unreachable, $LoginReq$ is forwarded by neighboring authenticated vehicles (multi-hop).
10. R contacts C with the vehicle identity (ID_i)
11. C sends to R the authentication dataset of vehicle V_i

Phase 4: Authentication and Key Establishment ;

12. R validates ϕ_i and selects a fresh challenge c_j from $\{c_j, r_j\}_i$.
13. R sends $(c_j, helper_data)$ to V_i over the secure channel.
14. V_i generates a noisy response $r'_j = PUF(c_j)$.
15. Using $helper_data$, V_i corrects r'_j to recover r_j.
16. V_i computes $h = H(r_j \parallel nonce_v \parallel TID_i)$.
17. V_i sends $Resp = h$ back to R.
18. R verifies h against the expected hash using r_j from C.
19. If valid, mutual authentication is successful. Otherwise, abort.
20. Both parties derive a session key $K_{V_i,R} = H(r_j \parallel nonce_v \parallel ID_i \parallel TID_i)$.

Phase 5: Multi-hop Extension (if R unreachable) ;

21. $LoginReq$ is relayed via authenticated neighbors V_{relay} until an RSU is reachable.
22. Each V_{relay} signs the forwarded packet with its session key to prevent tampering.
23. R issues acknowledgments along the reverse multi-hop path, establishing $K_{V_i,R}$.

Phase 6: Session Maintenance ;

24. Both V_i and R periodically refresh session keys using new CRPs.

Error Handling and Security Guarantees ;

25. Replay protection ensured via nonces and TIDs.
26. Forward secrecy is provided since CRPs are never reused.
27. Scalability achieved via cloud-managed CRP lifecycle.
28. Mutual trust guaranteed (vehicle $\leftrightarrow$ RSU), extended to multi-hop.

4. Security Analysis

We develop in this section several security analysis techniques for the proposed VANET mutual authentication protocols. Table 3 provides a roadmap and summary of the protocols discussed here.

This section provides a comprehensive informal and formal verification of the security protocol using a variety of methods. For the informal verification, we discuss some attacks that target VANs and show how the proposed protocol guards against them. For the formal verification, we employed a variety of methods, including Inductive Proof and Game-Based Proof. Each of these approaches verifies the protocol's ability to uphold key security properties such as confidentiality, mutual authentication, anonymity, replay protection, freshness, presence, and impersonation resistance. We structure this section to not only

verify these properties but also to describe in detail the mechanism and reasoning behind each proof.

Table 3. Mapping of formal proof techniques to validated security properties.

Proof Technique	Validated Security Property	Section
Inductive Proof	- Confidentiality of messages - Replay attack resistance - Freshness guarantees via nonces and TIDs - Preservation of secrecy under multi-hop relaying	Section 4.4
Game-based Model	- Indistinguishability of session keys from random values - Adversary advantage bounded by negligible ϵ - Robustness against chosen-message and impersonation attacks	Section 4.5
BAN Logic	- Correctness of authentication beliefs - Mutual agreement on session key between V_i and R - Resistance against impersonation	Section 4.6

4.1. Threat Model

To model anticipated threats, we assume that the adversary initiates the attacks via the embedded edge device present in the vehicles or by intercepting the communication across the network and the cloud. The vehicle, and its edge devices, represent the weakest link. These devices have limited compute resources and do not typically receive prompt software updates. The Dolev–Yao model for the adversary is assumed [27]. In addition, we assume the adversary can do the following actions:

1. Obtain the vehicle ID through eavesdropping or guessing the car model and ID sequence assignment.
2. Gain physical access to the vehicle in the field and extract any secret information from the memory.
3. Access the secret keys through reading the flash or solid-state drive (SSD).
4. Perform any side-channel attacks on the vehicle's edge devices.
5. Corrupt the vehicle's edge device contents to run malicious software.

4.2. Informal Verification

Informal verification was thoroughly discussed in a related publication [11]. We provide here a brief summary as it applies to the protocol of this paper, which is as follows:

1. Tampering attack: Device tampering modifies the chip encapsulation layers. This modifies the PUF response and results in authentication failure.
2. Replay attack: The algorithm in Listing 3 uses nonces that change for each session. Using nonces ensures actual device presence and freshness.
3. Eavesdropping attack: Listings 3 and 4 of the proposed algorithms show that almost all messages are encrypted using dynamic secret keys. In addition, the algorithms in Listings 3 and 4 use encrypted messages using secret keys that change with every session.
4. Impersonation attack: According to the mutual authentication algorithm in Listings 3 and 4, vehicle authentication requires the vehicle to give the correct PUF CRP responses. An impersonating device cannot simply create its own PUF since the

CRP set of this counterfeit PUF would not be registered by the device manufacturer, and no RSU would accept the counterfeit vehicle.

5. Man-in-the-midddle attack: Our communication is protected by at least four layers as follows:
   (a) Insisting that all vehicles are first authenticated via RSUs.
   (b) Using nonces.
   (c) Using dynamic secret keys where each communication session.
   (d) Extensive use of hashing.

   A malicious vehicle will not be able to register with an RSU and will not be able to participate in any activity.
6. Forward/backward secrecy: The secret keys for V2I and V2V modes rely on using nonces and change at the start of each session and after handover between femtocells. Thus, an attacker cannot learn past or future keys.
7. Session key guessing attack: In our protocols there are two session keys: k_i between an RSU and vehicle ID$_i$ $k_{i,j}$ between vehicle ID$_i$ and ID$_j$. These keys can not be inferred since they are not stored in non-volatile random access memories (NVRAMs) and dynamically change through use of nonces.
8. Cloning attack: As was explained in Section 2.4, using a PUF gives the device a unique ID, and a challenge generates a unique ID.
9. Physical attack: Using PUFs eliminates the need to store secret keys in NVRAM. The PUF response is never revealed but is used to generate secret keys and hash values.

4.3. Formal Verification Using Inductive and Game-Based Proofs

In this subsection, we delve into the formal verification of the proposed security protocol, expanding upon the earlier informal analysis. Formal verification is crucial for establishing strong, mathematical assurances about the protocol's ability to uphold critical security properties. In contrast to informal methods, which rely on practical demonstrations and hypothetical attacks, formal techniques offer rigorous, systematic proofs that ensure robustness against even the most sophisticated threats.

For this analysis, we employed two powerful formal methods: Inductive Proof and Game-Based Proof, each serving a distinct purpose in validating the security guarantees of the protocol. These approaches allow us to mathematically verify that the protocol maintains key security properties such as confidentiality, mutual authentication, anonymity, replay protection, freshness, and impersonation resistance. We structure this subsection to not only verify these properties but also to describe in detail the mechanism and reasoning behind each proof.

In the first part of the formal verification, we use Inductive Proof, systematically proving the correctness of each property through a base case and an inductive step. This method ensures that the protocol remains secure under all possible conditions. The second part involves a Game-Based Proof, where we model the adversary's interaction with the protocol as a game. Here, we analyze the likelihood of an adversary successfully breaching the protocol's defenses, demonstrating that the adversary's advantage remains negligible across all properties.

4.4. Inductive Proof

An Inductive Proof method establishes the security properties by proving that each property holds in the base case and continues to hold at every subsequent step of the protocol. This part presents inductive proofs for confidentiality, mutual authentication, anonymity, replay protection, and impersonation resistance as follows:

1. *Confidentiality*

   Base Case:

   Before any communication, the adversary has no knowledge of the session key. Let $\mathcal{K}_A$ represent the adversary's knowledge,

   $$\mathcal{K}_A = \emptyset \quad \text{(no knowledge of } K_{session}\text{)}. \tag{1}$$

   Inductive Step:

   Assume confidentiality holds at step n, i.e., $K_{session} \notin \mathcal{K}_A$. At step $n+1$, the RSU sends the encrypted session key $E_K(K_{session})$ to the vehicle,

   $$R \rightarrow V_i : E_K(K_{session}). \tag{2}$$

   By the semantic security of encryption and the unclonability of the PUF, the adversary cannot learn $K_{session}$, so

   $$K_{session} \notin \mathcal{K}_A \quad \forall n \in \mathbb{N}. \tag{3}$$

   Conclusion:

   By induction, confidentiality is preserved throughout the protocol.

2. *Mutual Authentication*

   Base Case:

   Initially, neither the vehicle nor the RSU has authenticated the other,

   $$\text{Authenticated}(V_i, R) = \text{false}, \quad \text{Authenticated}(R, V_i) = \text{false}. \tag{4}$$

   Inductive Step:

   Assume that mutual authentication holds at step n. At step $n+1$, the vehicle sends $H(PUF(c_V))$ to the RSU. The RSU verifies the PUF response,

   $$\text{If} H(PUF(c_V)) = H(\text{expected} PUF(c_V)), \text{then} \text{Authenticated}(R, V_i) = \text{true}. \tag{5}$$

   Similarly, the vehicle authenticates the RSU,

   $$\text{If } H(PUF(c_R)) = H(\text{expected} PUF(c_R)), \text{then} \text{Authenticated}(V_i, R) = \text{true}. \tag{6}$$

   Conclusion:

   Mutual authentication is preserved by induction,

   $$\text{Authenticated}(V_i, R) = \text{true} \quad \forall n \in \mathbb{N}. \tag{7}$$

3. *Anonymity*

   Base Case:

   Initially, the adversary has no knowledge of the vehicle's identity,

   $$\mathcal{K}_A = \emptyset \quad \text{(no knowledge of the vehicle's identity)}. \tag{8}$$

   Inductive Step:

   Assume anonymity holds at step n, i.e., the adversary cannot link the temporary ID (TID) to the real identity. In the next step, the vehicle uses a new TID, unlinkable to the real identity, so

$$P(\text{Adversary links} TID \text{to real identity}) = 0 \quad \forall n \in \mathbb{N}. \tag{9}$$

4. *Replay Protection and Impersonation Resistance*

   Replay Protection:

   The use of fresh nonces N_V and N_R at each step ensures that replay attacks are impossible, i.e., the adversary cannot replay an old message successfully,

$$P(\text{Replay attack succeeds}) = 0 \quad \forall n \in \mathbb{N}. \tag{10}$$

   Impersonation Resistance:

   PUF responses are unclonable, meaning the adversary cannot impersonate the vehicle or RSU,

$$P(\text{Impersonation attack succeeds}) = 0 \quad \forall n \in \mathbb{N}. \tag{11}$$

4.5. Game-Based Proof

In the College of Computer Science, in Game-Based Proofs, the adversary interacts with the protocol as part of a formal game. Unterweger et al. [28] used game-based privacy proofs for aggregation protocols in the smart grid. The two parties of the game were the challenger and the adversary. We formulate the problem such that the adversary's advantage in winning the game (breaking the security property) is negligible.

1. *Confidentiality*

   Game Definition:

   The adversary wins if they can correctly guess the session key $K_{session}$ after intercepting the ciphertext $E_K(K_{session})$.

   Adversary's Advantage:

   The adversary's advantage Adv_A is the probability of guessing $K_{session}$ given the ciphertext

$$Adv_A = P(A\text{guesses } K_{session}). \tag{12}$$

   By the semantic security of encryption and the unclonability of the PUF, this probability is negligible,

$$Adv_A = \text{negligible}. \tag{13}$$

2. *Mutual Authentication*

   Game Definition:

   The adversary wins if they can impersonate either the vehicle or RSU and fool the other party into authenticating them.

   Adversary's Advantage:

   The adversary's advantage is the probability of generating a valid PUF response,

$$Adv_A = P(A\text{generates valid } H(PUF(c_V))). \tag{14}$$

   Since PUF responses are unclonable, this probability is negligible,

$$Adv_A = \text{negligible}. \tag{15}$$

3. *Anonymity*

Game Definition:

The adversary wins if they can link the temporary ID (TID) to the vehicle's real identity.

Adversary's Advantage:

The adversary's advantage is the probability of linking the TID to the real identity,

$$Adv_A = P(A \text{ links } TID \text{ to real identity}). \quad (16)$$

Since the TID is unlinkable without the trusted mapping, this probability is negligible,

$$Adv_A = \text{negligible}. \quad (17)$$

4. *Replay Protection and Impersonation Resistance*

Replay Protection:

The adversary's advantage in performing a replay attack is negligible due to the use of fresh nonces,

$$Adv_A = P(\text{Replay attack succeeds}) = \text{negligible}. \quad (18)$$

Impersonation Resistance:

Since PUF responses are unclonable, the adversary cannot impersonate the vehicle or RSU,

$$Adv_A = P(A \text{ generates valid PUF response}) = \text{negligible}. \quad (19)$$

Summary of Formal Verification

Table 4 shows the summary of obtained resistance results of the proposed protocol against all the tested attacks.

Moreover, through the use of Inductive Proof and Game-Based Proof, we verified that the protocol satisfies the following security properties as follows:

- Confidentiality: The session key remains confidential.
- Mutual Authentication: Both the vehicle and RSU authenticate each other correctly.
- Anonymity: The vehicle's real identity is protected through the use of temporary IDs.
- Replay Protection: Replay attacks are prevented by using fresh nonces.
- Impersonation Resistance: Adversaries cannot impersonate the vehicle or RSU.

This comprehensive analysis demonstrates that the protocol is secure against the most common attack vectors under standard cryptographic assumptions.

Table 4. Summary of resistance against attacks.

Attack Type	Description	Resistance Mechanism	Status
Tampering Attacks	Physical tampering with the device.	PUF sensitivity to hardware changes.	Resistant
Replay Attacks	Reusing old messages to gain access.	Use of nonces for freshness.	Resistant
Impersonation Attacks	Impersonating the vehicle or RSU.	PUF challenge-response pairs prevent impersonation.	Resistant

Table 4. *Cont.*

Attack Type	Description	Resistance Mechanism	Status
Eavesdropping Attacks	Intercepting messages to gather sensitive information.	Encryption based on PUF-generated keys.	Resistant
MITM Attacks	Intercepting and altering communication between vehicle and RSU.	Mutual authentication and encryption prevent unauthorized modifications.	Resistant
Forward/Backward Secrecy	Ensuring past or future sessions remain secure even if the session key is compromised.	A new session key is generated for each session.	Resistant
Session Key Guessing Attacks	Brute-force attempts to guess the session key.	The session key is derived from PUF and cryptographic hash, making guessing infeasible.	Resistant
Cloning Attacks	Attempting to clone the vehicle's PUF to impersonate it.	PUF is unclonable and unique to each device.	Resistant
Physical Attacks	Direct physical attacks on the device to extract cryptographic keys or disable the PUF.	PUF is highly sensitive to physical tampering, rendering the device unusable.	Resistant

4.6. Formal Proof Using BAN Logic

Michael Burrows, Martin Abadi, and Roger Needham introduced BAN logic as a formal validation of authentication protocols [29]. Ahmad et al. [30] used BAN logic for mutual authentication and secure key exchange. Yang et al. [31] used BAN logic to validate authentication protocol for VANET traffic emergency message broadcasting.

We start here by providing a summary of the symbols used in BAN formal protocol verification formalism [29]. The notation of BAN rules are given in Table 5.

The following BAN rules verify that our multi-hop authentication protocol supports secure authentication and key exchange:

- Message meaning: If R believes that key k is shared with V and R receives m encrypted under k, then R believes that V once sent m.

$$\frac{R| \equiv V \overset{k}{\longleftrightarrow} V \lhd (X)_k}{R| \equiv V| \sim X}.$$

- Nonce verification: If R believes m is fresh and R believes V once sent m, then R trusts m,

$$\frac{R| \equiv \#(m), R| \equiv V| \sim m}{R| \equiv V| \equiv m}.$$

- Jurisdiction: If R believes V has jurisdiction over m and R trusts V trusts m, then R trusts m,

$$\frac{R| \equiv V| \Rightarrow m, R| \equiv V| \equiv m}{R| \equiv m}.$$

- Freshness concatenation: If part of a message is fresh, then the entire message is fresh too. In other words, if R trusts that m_1 is fresh, then R trusts that m_1 and m_2 are fresh,

$$\frac{R| \equiv \#(m_1)}{R| \equiv \#(m_1, m_2)}.$$

- Trust rule: If R trusts m_1 and m_2, then R trusts m,

$$\frac{R| \equiv (m_1, m_2)}{R| \equiv m_1}.$$

- Session key:

$$\frac{R| \equiv \#(m), R| \equiv V| \equiv m}{R| \equiv S \overset{k}{\longleftrightarrow} V}.$$

Our proposed multi-hop authentication protocol should achieve the following goals:

- Goal 1:

$$R| \equiv V| \equiv V \overset{k}{\longleftrightarrow} R.$$

- Goal 2:

$$V| \equiv R| \equiv R \overset{k}{\longleftrightarrow} V.$$

- Goal 3:

$$R| \equiv V \overset{k}{\longleftrightarrow} R.$$

- Goal 4:

$$V| \equiv R \overset{k}{\longleftrightarrow} V.$$

- Goal 5:

$$V_i| \equiv V_{i-1}| \equiv V_i \overset{k}{\longleftrightarrow} V_{i-1}.$$

- Goal 6:

$$V_i| \equiv V_{i+1}| \equiv V_i \overset{k}{\longleftrightarrow} V_{i+1}.$$

- Goal 7:

$$V_i| \equiv V_i \overset{k}{\longleftrightarrow} V_{i-1}.$$

- Goal 8:

$$V_i| \equiv V_i \overset{k}{\longleftrightarrow} V_{i+1}.$$

Basic assumptions of the multi-hop authentication protocol are as follows:

- A1:

$$R| \equiv \#(N).$$

- A2:

$$V_0| \equiv \#(N).$$

- A3:

$$V_{i+1}| \equiv V_i \Rightarrow m_i.$$

- A4:

$$V_i| \equiv V_{i+1} \Rightarrow m_{i+1}.$$

- A5:

$$R| \equiv V_n \Rightarrow m_n.$$

- A6:
$$V_n| \equiv R \Rightarrow m_n.$$
- A7:
$$V_1| \equiv V_0 \overset{m_0}{\longleftrightarrow} V_1.$$
- A8:
$$R| \equiv V_n \overset{m_n}{\longleftrightarrow} R.$$

Following are the messages transferred in the multi-hop authentication protocol:

- Message 1:
$$V_0 \rightarrow V_1 : E_{k_0}(TID_0||N_0).$$
- Message 2:
$$V_i \rightarrow V_{i+1} : \left[E_{k_i}(TID_i||N_i)||m_{i-1}\right].$$
- Message 3:
$$V_n \rightarrow R : [E_{k_n}(TID_n||N_n)||m_{n-1}].$$
- Message 4:
$$R \rightarrow V_n : E_{k_n}(K).$$
- Message 5:
$$V_i \rightarrow V_{i-1} : E_{k_i}(m_i).$$

BAN analysis of our multi-hop authentication scheme returns the following:

- S1: According to Msg 1, we can write
$$V_1 \lhd E_{k_0}(TID_0||N_0).$$
- S2: Based on Assumption A3, S1 and message-meaning rule, we have
$$\frac{V_1| \equiv V_0 \overset{k_i}{\longleftrightarrow} V_1, V_1 \lhd E_{k_0}(TID_0||N_0)}{V_1| \equiv V_0 \sim E_{k_0}(TID_0||N_0)}.$$
- S3: According to Msg 2, we can write
$$V_{i+1} \lhd E_{k_i}(TID_i||N_i).$$
- S4: Based on Assumption A4, S3 and message-meaning rule, we have
$$\frac{V_{i+1}| \equiv V_i \overset{k_i}{\longleftrightarrow} V_{i+1}, V_i \lhd E_{k_i}(TID_i||N_i)}{V_{i+1}| \equiv V_i \sim E_{k_i}(TID_i||N_i)}.$$

The previous BAN logic analysis illustrates that the proposed V2V multi-hop protocol achieves multifactor authentication through an insecure Wi-Fi environment.

Table 5. Basic notations of BAN logic.

Notation	Description
R and V	Principal actors
$R\mid\equiv m$	R trusts message m
$R\lhd m$	R receives message m
$R\mid\Rightarrow m$	R has jurisdiction over m
$R\mid\sim m$	R once sent m
(m_1, m_2)	Messages m_1 or m_2 are one part of the message (m_1, m_2)
$< m >_k$	Message m is encrypted with key k
$(m)_k$	Message m is hashed with key k
$R \overset{k}{\longleftrightarrow} V$	k is a secret variable between R and V
$R \overset{k}{\rightleftharpoons} V$	m is secret and known only to R and V and parties trusted by them
$\#(m)$	Message m is fresh

5. Discussion

The proposed work introduces a novel mutual V2I multifactor authentication protocol tailored for vehicular networks, offering several distinctive contributions that advance current security frameworks for VANETs. These contributions are as follows:

1. Bi-directional Multi-hop Authentication: The protocol enables bi-directional authentication using PUF hardware tokens over unsecured multi-hop Wi-Fi links. This feature ensures that both the vehicle and the roadside unit (RSU) authenticate each other, even when communication occurs via intermediate relay vehicles. Previous V2I authentication schemes typically assumed direct, single-hop connectivity; our multi-hop extension fills this critical gap by enabling cooperative forwarding with maintained trust guarantees.
2. Cloud-based CRP Lifecycle Management: A cloud authority is integrated to manage the Challenge–Response Pair (CRP) lifecycle. This entity issues fresh challenges, prevents reuse, and coordinates revocation or renewal, eliminating finite CRP storage constraints on vehicles. Cloud-assisted oversight ensures centralized monitoring and scalability, supporting large fleets without sacrificing security continuity.
3. Formal Security Verification: We provide a formal security analysis based on established cryptographic verification tools. The model confirms resistance to replay, man-in-the-middle, impersonation, and PUF cloning attacks under realistic adversarial assumptions. Collectively, these contributions—multi-hop mutual authentication, cloud-assisted CRP management, and verified robustness—establish a new benchmark for lightweight, scalable V2I authentication frameworks.
4. Comparative Advantages: Relative to prior studies, the proposed protocol offers the following clear performance and design improvements:
    - *Lightweight Operation:* By relying on symmetric primitives and PUF responses rather than PKI-based digital signatures, the protocol minimizes computational and latency overhead. While RSA-based methods incur hundreds of

milliseconds of delay, the PUF-based challenge–response mechanism achieves sub-50 ms authentication.

- *Mutual Trust Establishment:* Both the vehicle and the RSU verify each other's legitimacy, preventing impersonation in multi-hop environments where intermediate relays may be untrusted.
- *Multi-hop Robustness:* Unlike earlier PUF-Guard and similar frameworks [11], the proposed system explicitly supports relay-based multi-hop trust propagation.
- *Multifactor Integration:* Beyond the PUF, vehicle-specific identifiers or biometric traits can be fused to reinforce authentication strength.
- *Cloud Oversight:* The centralized cloud authority enables efficient CRP lifecycle management and scalability beyond localized trust zones.

Overall, this scheme achieves low latency, high scalability, and mutual trust in complex, multi-hop vehicular topologies, addressing limitations observed in earlier PUF-based and PKI-based designs.

6. Conclusions

In conclusion, this paper establishes a robust, comprehensive framework that enhances the security of Vehicular Ad Hoc Networks (VANETs). The proposed PUF-based mutual authentication protocol supports diverse modes of vehicular communication, visible light, 5G/6G, and Wi-Fi multi-hop, while providing end-to-end protection against tampering, replay, eavesdropping, and impersonation.

Our framework leverages PUF technology as a hardware root of trust for secure key generation, exchange, and verification without relying on non-volatile key storage. The integration of one-time passwords and ephemeral keys preserves forward and backward secrecy, mitigating man-in-the-middle threats. These design features collectively fortify confidentiality, integrity, and trust within smart transportation infrastructures.

The implications of this work are substantial: by ensuring resilient, unclonable, and efficient authentication mechanisms, the framework lays the groundwork for the next generation of intelligent transportation systems. It establishes an adaptable foundation that unites hardware-level security with system-wide trust management across dynamic vehicular environments.

Nevertheless, certain assumptions and constraints remain. The proposed framework presumes the availability of stable, vendor-consistent PUF modules across vehicles and RSUs. Vehicles without PUF hardware can still participate through multifactor authentication, but at a reduced trust level, as their secret keys must be stored in NVRAM. The overall system security remains bounded by the weakest non-PUF node. Therefore, achieving full-scale deployment requires careful interoperability design across heterogeneous hardware ecosystems.

7. Future Work

Future research will focus on validating the framework's empirical feasibility, addressing interoperability challenges, and extending its resilience against real-world conditions. These efforts are structured as follows.

1. Implementation Roadmap. While the proposed protocol's security has been formally proven, its practical performance must be demonstrated through simulation and prototyping. The planned implementation roadmap includes:
    - *Vehicle Nodes:* Modeled as Mininet-WiFi stations representing vehicular OBUs with software-based PUF modules.

- *RSUs:* Simulated as Mininet access points using cloud-issued short-lived certificates.
- *Cloud Authority:* Operated as a Mininet controller responsible for CRP lifecycle management and challenge validation.
- *PUF Simulation:* Realized via software fuzzy extractors to emulate noise-resilient CRP generation [24].

2. Simulation Environment. We will employ Mininet-WiFi [32] integrated with SUMO [33] to emulate dynamic vehicular mobility and multi-hop wireless propagation. This setup enables realistic performance assessment under variable traffic densities, hop distances, and network loads. Mininet-WiFi is a widely used network emulator that extends the well-known Mininet environment to support wireless stations and access points with full mobility and multi-hop capabilities [32,34]. This makes it particularly well-suited for emulating vehicular ad hoc networks (VANETs) in software. Crucially, Mininet-WiFi can realistically model multi-hop Wi-Fi topologies akin to our scenario—for example, vehicles forwarding packets over multiple wireless hops to reach an RSU—while running real network protocols and applications. The platform also integrates with the SUMO traffic mobility simulator, allowing us to import realistic vehicle movement traces and road network layouts [35].
This integration means we can recreate dynamic VANET scenarios (with vehicles joining, leaving, and moving between RSU coverage areas) and evaluate our authentication protocol under realistic mobility patterns. Another advantage is that Mininet-WiFi enables fine-grained measurement of network metrics. We will be able to measure latency (end-to-end and per-hop communication delay), authentication delay (time to complete our handshake), and system throughput under varying loads, all within a controlled, reproducible environment. It also scales to a significant number of virtual nodes, which will let us assess scalability (e.g., testing hundreds of simulated vehicles per RSU) before moving to real hardware. In summary, Mininet-WiFi offers an ideal balance of realism and flexibility—it has been employed in prior vehicular network research for prototyping V2X protocols. [32], and it provides the tools (mobility modeling, wireless channel emulation, etc.) needed to evaluate our multi-hop authentication scheme rigorously. We emphasize that this simulation-based evaluation is part of our future work plan, to be conducted in the next phase of the project, laying the groundwork for subsequent field testing. The implementation in Mininet-WiFi will not only validate the feasibility of our protocol in a complex network setting but also guide any optimizations before we proceed to hardware prototyping.
3. Evaluation Metrics. Performance will be evaluated using the following:
    - *Authentication Latency:* End-to-end handshake delay, per hop and aggregate.
    - *Key Generation Time:* Average CRP evaluation and validation duration.
    - *Communication Overhead:* Number of messages and data exchanged.
    - *Scalability:* Performance degradation with increasing node count.
    - *Robustness:* Authentication success under packet loss, noise, or adversarial interference.

    Preliminary projections indicate an authentication latency below 10 ms per hop, satisfying the sub-100 ms safety requirement for real-time VANET applications.
4. Hardware Prototyping. Subsequent stages will involve deploying a hardware-in-the-loop prototype using FPGA-based PUF modules integrated into vehicular OBUs and RSUs (e.g., Raspberry Pi or Jetson Nano boards). This will enable the evaluation of end-to-end handshake efficiency, interoperability with IEEE 802.11p/C-V2X standards, and resilience to environmental perturbations.

5. Long-term Research Directions. The following open challenges remain to be addressed:
   - *Legacy Integration:* Develop hybrid authentication modes for vehicles lacking PUF hardware.
   - *Standardization:* Define cross-vendor CRP formats and lifecycle management protocols.
   - *Hardware Optimization:* Explore cost-efficient, automotive-grade PUF designs resilient to modeling and side-channel attacks [36].
   - *Environmental Calibration:* Investigate adaptive fuzzy extractors to stabilize CRPs under variable temperature and voltage conditions.
   - *Decentralized Trust:* Incorporate distributed ledger technologies to reduce single-point dependence on cloud authorities.

In summary, the proposed framework represents a major step toward scalable, bidirectional, and hardware-rooted authentication for vehicular networks. Continued empirical validation and hardware deployment will ensure the practicality, reliability, and standardization necessary for real-world adoption in intelligent transportation systems.

Author Contributions: Conceptualization, F.G. and M.K.E.; methodology, F.G. and M.K.E.; analysis, M.K.E. and F.G. All authors have read and agreed to the published version of the manuscript.

Funding: No funding was received for conducting this study.

Data Availability Statement: The original contributions presented in this study are included in the article. Further inquiries can be directed to the corresponding author.

Conflicts of Interest: The authors have no relevant financial or non-financial interests to disclose.

References

1. Siegel, J.E.; Erb, D.C.; Sarma, S.E. A Survey of the Connected Vehicle Landscape—Architectures, Enabling Technologies, Applications, and Development Areas. *IEEE Trans. Intell. Transp. Syst.* **2018**, *19*, 2391–2406. [CrossRef]
2. Arena, F.; Pau, G.; Severino, A. An Overview on the Current Status and Future Perspectives of Smart Cars. *Infrastructures* **2020**, *5*, 53. [CrossRef]
3. Lee, R. Intelligent Transportation. In *Artificial Intelligence in Daily Life*; Springer: Berlin/Heidelberg, Germany, 2020; pp. 265–282. [CrossRef]
4. Lu, Z.; Qu, G.; Liu, Z. A survey on recent advances in vehicular network security, trust, and privacy. *IEEE Trans. Intell. Transp. Syst.* **2018**, *20*, 760–776. [CrossRef]
5. Farsimadan, E.; Palmieri, F.; Moradi, L.; Conte, D.; Paternoster, B. Vehicle-to-everything (V2X) communication scenarios for vehicular ad-hoc networking (VANET): An overview. In Proceedings of the International Conference on Computational Science and Its Applications (ICCSA), Cagliari, Italy, 13–16 September 2021; pp. 15–30. [CrossRef]
6. Gebali, F.; Mamun, M. SRAM Physically Unclonable Functions for Smart Home IoT Telehealth Environments. In *Cybersecurity in Smart Homes: Architectures, Solutions and Technologies*; Khatoun, R., Ed.; Wiley-iSTE: Hoboken, NJ, USA, 2022; pp. 125–151.
7. Ghosal, A.; Conti, M. Security issues and challenges in V2X: A survey. *Comput. Netw.* **2020**, *169*, 107093. [CrossRef]
8. Hasan, M.; Mohan, S.; Shimizu, T.; Lu, H. Securing vehicle-to-everything (V2X) communication platforms. *IEEE Trans. Intell. Veh.* **2020**, *5*, 693–713. [CrossRef]
9. Rathore, R.S.; Hewage, C.; Kaiwartya, O.; Lloret, J. In-Vehicle Communication Cyber Security: Challenges and Solutions. *Sensors* **2022**, *22*, 6679. [CrossRef]
10. Wang, Z.; Zhou, Y.; Qiao, Z.; Yang, B.; Gu, C.; Xu, Y. An Anonymous and Revocable Authentication Protocol for Vehicle-to-Vehicle Communications. *IEEE Internet Things J.* **2022**, *10*, 5114–5127. [CrossRef]
11. Gebali, F.; Elhadad, M. PUFGuard: Vehicle-to-Everything Authentication Protocol for Secure Multihop Mobile Communication. *Computers* **2023**, *12*, 233. [CrossRef]
12. Kitchenham, B.; Charters, S. *Guidelines for Performing Systematic Literature Reviews in Software Engineering*; Technical report, EBSE Technical Report EBSE-2007-001; Keele University:Keele, UK; Durham University: Durham, UK, 2007.
13. Petersen, K.; Feldt, R.; Mujtaba, S.; Mattsson, M. Systematic Mapping Studies in Software Engineering. In Proceedings of the 12th Int'l Conference on Evaluation and Assessment in Software Engineering (EASE), Bari, Italy, 26–27 June 2008; BCS: Swindon, UK, 2008. [CrossRef]

14. Ullah, S.; Zheng, J.; Din, N.; Hussain, M.T.; Ullah, F.; Yousaf, M. Elliptic Curve Cryptography; Applications, challenges, recent advances, and future trends: A comprehensive survey. *Comput. Sci. Rev.* **2023**, *47*, 100530. [CrossRef]
15. Groza, B.; Andreica, T.; Berdich, A.; Murvay, P.S.; Gurban, H. PRESTvO: PRivacy Enabled Smartphone-based Access to vehicle On-board units. *IEEE Access* **2020**, *8*, 119105–119122. [CrossRef]
16. Perera, M.N.S.; Nakamura, T.; Hashimoto, M.; Yokoyama, H.; Cheng, C.M.; Sakurai, K. A Survey on Group Signatures and Ring Signatures: Traceability vs. Anonymity. *Cryptography* **2022**, *6*, 3. [CrossRef]
17. Alrawais, A.; Alhothaily, A.; Mei, B.; Song, T.; Cheng, X. An Efficient Revocation Scheme for Vehicular Ad-Hoc Networks. In Proceedings of the13th Int'l Conference on Future Networks and Communications (FNC 2018)–Procedia Computer Science, Gran Canaria, Spain, 13–15 July 2018; Volume 129, pp. 312–318. [CrossRef]
18. Dwivedi, S.K.; Amin, R.; Das, A.K.; Leung, M.T.; Choo, K.K.R.; Vollala, S. Blockchain-based vehicular ad-hoc networks: A comprehensive survey. *Ad Hoc Netw.* **2022**, *137*, 102980. [CrossRef]
19. Wang, C.; Cheng, X.; Li, J.; He, Y.; Xiao, K. A survey: Applications of blockchain in the Internet of Vehicles. *EURASIP J. Wirel. Commun. Netw.* **2021**, *2021*, 77. [CrossRef]
20. Keshari, N.; Singh, D.; Maurya, A.K.; Gupta, D.; Khare, A. A survey on Vehicular Fog Computing: Current state-of-the-art and future directions. *Veh. Commun.* **2022**, *38*, 100512. [CrossRef]
21. Alrawais, A.; Alhothaily, A.; Hu, C.; Cheng, X. Fog Computing for the Internet of Things: Security and Privacy Issues. *IEEE Internet Comput.* **2017**, *21*, 34–42. [CrossRef]
22. Shamsoshoara, A.; Korenda, A.R.; Afghah, F.; Zeadally, S. A survey on physical unclonable function (PUF)-based security solutions for Internet of Things. *Comput. Netw.* **2020**, *183*, 107593. [CrossRef]
23. Umar, M.; Islam, S.H.; Mahmood, K.; Ahmed, S.; Ghaffar, Z.; Saleem, M.A. Provable Secure Identity-Based Anonymous and Privacy-Preserving Inter-Vehicular Authentication Protocol for VANETs Using PUF. *IEEE Trans. Veh. Technol.* **2021**, *70*, 12158–12167. [CrossRef]
24. Delvaux, J.; Gu, D.; Schellekens, D.; Verbauwhede, I. Helper Data Algorithms for PUF-Based Key Generation: Overview and Analysis. *IEEE Trans. Comput.* **2014**, *34*, 889–902. [CrossRef]
25. Rezazadeh Baee, M.A.; Simpson, L.; Boyen, X.; Foo, E.; Pieprzyk, J. Authentication strategies in vehicular communications: A taxonomy and framework. *EURASIP J. Wirel. Commun. Netw.* **2021**, *2021*, 129. [CrossRef]
26. Afshar, M.A.; Benchoubane, N.; Cayoren, B.; Kurt, G.K.; Ozdemir, E. Privacy-Preserving and Simultaneous Authentication in High-Density V2X Networks. *arXiv***2025**, arXiv:2501.06087.
27. Rakotonirina, I.; Barthe, G.; Schneidewind, C. Decision and Complexity of Dolev-Yao Hyperproperties. *Proc. ACM Program. Lang.* **2024**, *8*, 1913–1944. [CrossRef]
28. Unterweger, A.; Taheri-Boshrooyeh, S.; Eibl, G.; Knirsch, F.; Küpçü, A.; Engel, D. Understanding Game-Based Privacy Proofs for Energy Consumption Aggregation Protocols. *IEEE Trans. Smart Grid* **2019**, *10*, 5514–5523. [CrossRef]
29. Burrows, M.; Abadi, M.; Needham, R. A Logic of Authentication. *ACM Trans. Comput. Syst.* **1990**, *8*, 18–36. [CrossRef]
30. Ahmad, K.; Ginting, J.G.A.; Damarjati, C.; Cahyadi, E.F. Analyzing MORNeS Protocol for Secure Key Exchange with BAN Logic. In Proceedings of the 2025 International Electronics Symposium (IES), Surabaya, Indonesia, 5–7 August 2025.
31. Yang, A.; Yao, J.; Wei, W. A Lightweight Security Authentication Protocol for VANET Traffic Emergency Message Broadcasting. In Proceedings of the 10th International Symposium on Advances in Electrical, Electronics and Computer Engineering (ISAEECE), Xi'an, China, 20–22 June 2025; pp. 293–304.
32. Fontes, R.R.; Rothenberg, C.E.; Afzal, S.; Hessel, F. Mininet-WiFi: Emulating Software-Defined Wireless Networks. In Proceedings of the 2015 11th International Conference on Network and Service Management (CNSM),Barcelona, Spain, 9–13 November 2015; pp. 348–353. [CrossRef]
33. Krajzewicz, D.; Erdmann, J.; Behrisch, M.; Bieker, L. Recent Development and Applications of SUMO—Simulation of Urban MObility. *Int. J. Adv. Syst. Meas.* **2012**, *5*, 128–138.
34. Fontes, R.R.; Rothenberg, C.E. Mininet-WiFi: Emulation Platform for Software-Defined Wireless Networks. 2025. Available online: https://mininet-wifi.github.io/ (accessed on 21 October 2025).
35. Fontes, R.R.; Rothenberg, C.E. Mininet-WiFi + SUMO Emulation Platform. 2025. Available online: https://mininet-wifi.github.io/sumo/ (accessed on 21 October 2025).
36. Maes, R. *Physically Unclonable Functions: Constructions, Properties and Applications*; Springer: Berlin/Heidelberg, Germany, 2016.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.