computers

MDPI

Article

PUFGuard: Vehicle-to-Everything Authentication Protocol for Secure Multihop Mobile Communication

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

[1] Department of Electrical and Computer Engineering, University of Victoria, Victoria, BC V8W 3P6, Canada; fayez@uvic.ca

[2] Department of Computer Engineering and Artificial Intelligence, The Military Technical College, Cairo 11766, Egypt

[*] Correspondence: melhaddad@ieee.org or moh.elhadad@mtc.edu.eg

[†] These authors contributed equally to this work.

Abstract: Vehicle area networks (VANs) encompass a spectrum of communication modes, including point-to-point visible light communication, 5G/6G cellular wireless communication, and Wi-Fi ad hoc multihop communication. The main focus of this paper is the introduction and application of physically unclonable functions (PUFs) as a pivotal element in secure key generation, authentication processes, and trust metric definition for neighboring vehicles. The multifaceted protocols proposed herein encompass comprehensive security considerations, ranging from authentication and anonymity to the imperative aspects of the proof of presence, freshness, and ephemeral session key exchanges. This paper provides a systematic and comprehensive framework for enhancing security in VANs, which is of paramount importance in the context of modern smart transportation systems. The contributions of this work are multifarious and can be summarized as follows: (1) Presenting an innovative and robust approach to secure key generation based on PUFs, ensuring the dynamic nature of the authentication. (2) Defining trust metrics reliant on PUFs to ascertain the authenticity and integrity of proximate vehicles. (3) Using the proposed framework to enable seamless transitions between different communication protocols, such as the migration from 5G/6G to Wi-Fi, by introducing the concept of multimodal authentication, which accommodates a wide spectrum of vehicle capabilities. Furthermore, upholding privacy through the encryption and concealment of PUF responses safeguards the identity of vehicles during communication.

Keywords: V2X; V2V; V2I; IoV; PUF; authentication; VAN

check for updates

Citation: Gebali, F.; Elhadad, M.K. PUFGuard: Vehicle-to-Everything Authentication Protocol for Secure Multihop Mobile Communication. *Computers* **2023**, *12*, 233. https://doi.org/10.3390/computers12110233

Academic Editor: Paolo Bellavista

Received: 15 October 2023
Revised: 2 November 2023
Accepted: 9 November 2023
Published: 14 November 2023

1. Introduction

In vehicle area networks (VANs), vehicles have three possible modes of communication: point-to-point visible light communications (VLCs) between infrastructure components, 5G/6G cellular wireless communications, and IEEE 802.11 Wi-Fi ad hoc multihop communications. The first two modes are point-to-point communication between a vehicle and infrastructure, such as antennas located at traffic lights, light posts, mobile unmanned areal vehicles (drones), and blimps or dirigibles. The third mode is the most vulnerable to attacks since it involves the collaboration of many intermediate vehicles (nodes) to establish a communication path between a vehicle and an intended destination.

The multihop and dynamic nature of Wi-Fi ad hoc connectivity for VANs essentially requires an efficient routing protocol and zero-trust multifactor authentication. In order for a node to participate in the ad hoc system connectivity (routing and authentication), the node must be able to register in the system using multifactor authentication and satisfy freshness, presence, and context awareness [1–3]. The requirements for secure VAN communication include authentication, anonymity, a proof of presence, ensuring freshness, and the exchange of ephemeral session keys between any two entities.

The main contributions of this work are summarized as follows:

1. Providing a physically unclonable function (PUF)-based secure key generation and dynamic key exchange between the communicating vehicles.
2. Defining PUF-based trust metrics to assess the authenticity and integrity of neighboring vehicles.
3. PUF-backed seamless handover and transition between protocols, such as transitioning between 5G/6G and Wi-Fi.
4. Multimodal authentication to handle diverse vehicle capabilities.
5. Privacy-preserving PUF use by encrypting and hiding PUF responses. This protects vehicles' identities during communications.

The rest of this paper is organized as follows. Section 2 summarizes the notations and terms used. Section 3 discusses background and related works. Section 4 defines the VAN under consideration emphasizing the different communication protocols used, such as Wi-Fi and 5G/6G cellular communication. Section 5 discusses the communication modes of VANs from the point of view of security and vulnerability to attacks. Section 6 provides a brief introduction to physically unclonable functions (PUFs). Section 7 discusses the proposed PUF-based authentication protocols. Section 8 explains the proposed protocol for vehicle-to-infrastructure authentication. Section 9 explains the proposed protocol for vehicle-to-vehicle authentication. Section 10 discusses the immunity of our proposed protocols to several types of attacks. Section 11 provides the conclusion of the presented work.

2. Notation and Terms Used

Table 1 lists the notations and terms used in this work.

Table 1. Abbreviations and terms used in this work.

$A \rightarrow B$	A sends a message to B through an insecure communication channel
C	Certification authority
$D_k(m)$	Decryption of message m with secret key k
$E_k(m)$	Encryption of message m with secret key k
$h = H(m)$	Collision-resistant hash of message m
k_{px}	RSA public key for vehicle x
k_{sx}	RSA secret key for vehicle x
k_{xy}	Symmetric secret ephemeral key shared between entities x and y
$m_1 \vert\vert m_2$	Concatenation of messages m_1 and m_2
N	Nonce
R_x	Identity and label of any remote road-side unit (RSU)
$\{CRP_x\}$	Set of challenge-response pair for PUF of V_x
RoT	Root of trust
V_x	Identity and label of vehicle x
$I2I$	Infrastructure-to-infrastructure communication
$V2I$	Vehicle-to-infrastructure communication
$V2V$	Vehicle-to-vehicle communication

3. Related Works

There was early work on authenticating nodes in a multihop system. Badetia and Hussain [4] considered the case of a distributed mechanism for node authentication in wireless sensor networks (WSNs). Their work was limited since they assumed the nodes to be stationary and have limited power, data storage, and processing capabilities.

Node authentication could be based on an identity-based signature where each node uses its IP or email as the public key and a trusted authority issues the private node or secret key [5]. An implicit assumption here is that each WSN node is capable of securely storing its secret key and performing the encryption/decryption operation required for public key infrastructure (PKI) field arithmetic.

Fakroon et al. [1–3] developed a multifactor authentication scheme using physically unclonable functions. The scheme ensures secure and anonymous communication between several entities comprising a healthcare IoT system.

4. Vehicle Area Networks (VANs)

In an intelligent transportation system, both vehicles and transportation infrastructure have undergone complete digitization. This includes entities such as vehicles, traffic lights, light posts, the hierarchical structure of 5G/6G base stations, and IEEE 802.11 Wi-Fi communication.

Figure 1 shows the primary communication modes within a VAN.

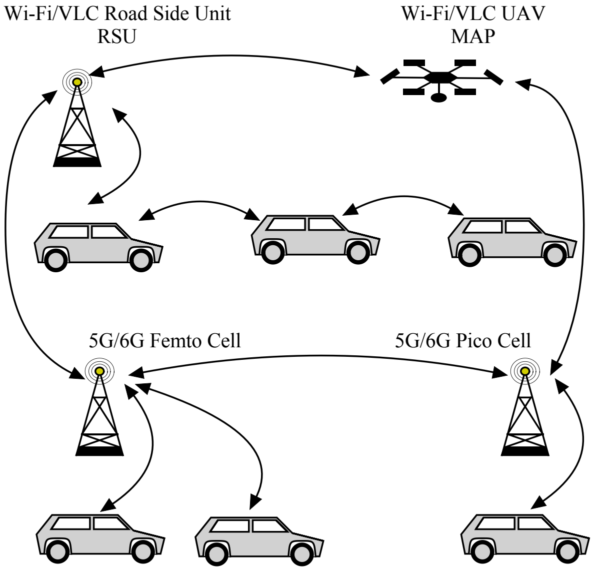

Figure 1. VAN system operating in 5G/6G cellular system model as well as an IEEE 802.11 Wi-Fi model. MAP: mobile access point, RSU: road-side unit, UAV: unmanned aerial vehicle, VLC: visible light communications.

The main entities involved in the VAN system include the following:

1. Vehicles that can communicate with other vehicles and infrastructure components using Wi-Fi or 5G/6G cellular communications. Vehicles have unique identities (ID) and PUFs [6] and sensors such as GPS, radar, LIDAR, acoustic, infrared, video cameras, etc. Vehicles also have actuators to activate brakes, accelerators, lights, etc.
2. Pico/femtocell base stations, or servers, which are considered the hardware root-of-trust (HRoT) since they contain layered security protocols and tamper resistance. These base stations could be located at traffic lights, light posts, buildings, etc.
3. Wi-Fi wireless access points (WAP) These WAPs could be located at traffic lights, light posts, buildings, etc.
4. Remote road-side infrastructure units (RSUs) that provide connectivity between IEEE 802.11 Wi-Fi and 5G/6G pico/femtocells.
5. The Internet cloud or virtual private network (VPNs) that provide connectivity between the base stations and ensure an increased throughput and reduced latency.
6. The certification authority (CA), which keeps a database of the vehicles and their associated IDs and challenge response pairs (CRPs).

Figure 2 shows the communications modes for smart vehicles. Each vehicle has a gateway to facilitate connectivity with 5G/6G cellular systems as well as IEEE 802.11 Wi-Fi ad hoc multihop systems.

The gateway is the hub for connecting the various sensors and actuators onboard the vehicle and the infrastructure systems (V2I) and other vehicles (V2V). Inserting a PUF in the gateway enables it to be treated as an HRoT at a low cost.

Communication between vehicles could be indirect using multihop ad hoc IEEE 802.11 Wi-Fi. In this scenario, mutual authentication becomes essential for ensuring the security of the interaction. Alternatively, another communication approach could involve the direct utilization of the 5G/6G infrastructure cellular network. In such instances, the vehicles engaged in communication must authenticate themselves to the base station or stations that oversee the cells in which they are situated.

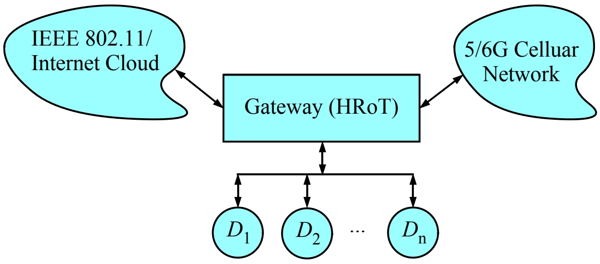

Figure 2. Basic communication model for a vehicle in VAN system.

5. VAN Security Considerations

From the observations of Section 4, we see that 5G/6G cellular communications are based on a point-to-point communication mode where each vehicle talks directly to the parent pico/femtocell closest to the vehicle. In contrast, Wi-Fi communications are based on a multihop mode of communications where routing algorithms select a path between the vehicle and the wireless access point (WAP). This path typically involves a collaboration of intermediate vehicles to complete the connection.

From this observation, we note that there is a need to create ephemeral secret session keys between any two entities that need to communicate. These two entities are dynamic in the sense that new vehicles arrive or leave an RSU, and secure communication can only be established after a secret key has been generated and exchanged in a secure manner. Attacks on Wi-Fi access are more diverse compared to attacks on 5G/6G cellular access. Examples of attacks targeting Wi-Fi access include the man in the middle, denial of service, blackhole routing, etc.

At this point, we have the opportunity to devise two distinct vehicle authentication algorithms: one for communication between vehicles and infrastructure RSU networks and another for communication between two vehicles via Wi-Fi wireless networks. The former necessitates the capability to authenticate vehicles during handover processes between RSUs, while the latter entails the engagement and authentication of intermediary vehicles, some of which may have malicious intentions

VAN Threat Model

The adversary possesses multiple avenues for targeting VAN Infrastructure, which include potential attack vectors via vehicles, the Wi-Fi infrastructure, the 5G/6G cellular system, or the direct targeting of the vehicles themselves. The most vulnerable aspect of this IoT transportation system is the vehicles themselves, primarily because they may not receive regular software/firmware updates and are susceptible to tampering. The analysis adopts the Dolev–Yao model to represent the adversary's capabilities, alongside other potential adversary actions, such as the following:

1. Obtaining the vehicle ID, PUF manufacturer, or the types of sensors installed.
2. Gaining physical access to the vehicle electronics.
3. Attacking storage devices on the vehicle to gain access to any stored secret keys whether in non-volatile random access memories (NVRAMs), read-only memories (ROMs), etc.
4. Gaining access to secret keys via side-channel attacks (SCAs).
5. Contaminating remote firmware updates to install malicious software.
6. Adding malicious vehicles to launch denial-of-service attacks (DoS) or launch blackhole attacks that disrupt the multihop routing of data among the vehicles.

6. Physically Unclonable Functions

Physically unclonable functions (PUFs) are now becoming an important and practical addition to smart devices to provide unique biometrics and labels. The recent Biden–Harris initiative on the cybersecurity labeling of smart devices certainly validates this trend [7].

A silicon PUF is an electronic circuit that produces a unique response vector r to a given challenge vector c

$$r = \mathrm{PUF}(c) \tag{1}$$

The uniqueness of the challenge/response pair (CRP) stems from the inevitable random processing variations (RPV) in the circuit response incurred during device manufacturing. There is also the inevitable measurement noise sources associated with silicon devices, such as shot noise, flicker noise, and thermal noise [8].

We notice that CRPs are very similar to the normal authentication process for the case of humans, where the user ID is considered the challenge and the secret password or passphrase is the response. Therefore, we must ensure that the response vector r in Equation (1) is never be shared.

The noise sources corrupt the response r and introduce difficulties in both the authentication process and secret key generation that require a consistent and stable CRP. The most common approach to remove the noise from the response is to use forward error correction techniques [9–11]. In this approach, the server sends the challenge but also appends helper data vector w, which represents redundancy information, to be able to remove the noise from the client response [12].

7. Proposed PUF-Based VAN Authentication Protocols

Several protocols are required to establish secure communication in VANs. These authentication protocols include the following:

1. I2I communication.
2. V2I communication.
3. V2V communication.

This work assumes that I2I communication is already secure since infrastructure is considered an RoT and employs layered security protocols. Therefore, the focus in this work is on V2I and V2V communication.

A source vehicle V_s and a destination vehicle V_d and some intermediate nodes/vehicles are involved. The broad tasks to be performed in our proposed protocol are the following:

1. V2I authentication.
2. A secret key generation and exchange between a RSU and a vehicle.
3. V2V authentication and a secure key exchange.

The following sections illustrate how these three steps are accomplished.

Predeployment

The vehicle manufacturer registers with the certification authority (C) servers. The details stored at C for each vehicle are necessary to facilitate authentication. The data to be registered include the vehicle identity ID_x and the set of CRPs ({ CRP }) pertinent to the PUF used in the vehicle.

8. V2I Authentication Protocol

Assume that we have a vehicle V_x that needs to communicate with smart transportation infrastructure RSUs as well as other vehicles. It has already been stated that each RSU is considered an RoT.

Algorithm 1 Line 1: The vehicle broadcasts its ID_v to the infrastructure system RSUs. The nearest RSU will pick the vehicle identity ID_v.

Algorithm 1: V2I authentication protocol.

```
1  $V$ : broadcast_request_connect($\mathrm{ID}_v$);
2  $R$ : handover($\mathrm{ID}_v$); % Nearest RSU receiving connection request
3  if $ID_v \in R_i$ then
4      $R \rightarrow R_i$ : get_CRP($\mathrm{ID}_v$);
5  else
6      $R \rightarrow C$ : get_CRP($\mathrm{ID}_v$);
7  end
8  $C : m_1 = (\{CRP_v\})$;
9  $C \rightarrow R : m_3$;
10 $R : (c, w) =$ choose_CRP;
11 $R : N =$ generate_nonce( );
12 $R : k = H(c, r)$; % session key between $R$ and $V$
13 $R : h = H(N, c, r)$; % $h$ is used for authentication and freshness
14 $R : m_2 = E_k(N)$;
15 $R : m_3 = (m_2 || c, w)$;
16 $R \rightarrow V : m_3$;
17 $V : r = \mathrm{PUF}(c, w)$;
18 $V : k = H(c, r)$;
19 $V : N = D_k(m_2)$;
20 $V : h' = H(N, c, r)$;
21 $V \rightarrow R : h'$;
22 if $h = h'$ then
23     move to V2V authentication
24 else
25     failed authentication
26 end
```

Algorithm 1 Line 2: The RSU interrogates adjacent RSUs to see if any of them were serving the vehicle in question. If the vehicle just left RSU R_i, it will copy the CRP associated with the vehicle ID_v, (Line 4). If the vehicle just arrived and was not handed over, the RSU will contact C and ask to receive the CRP associated with the vehicle ID_v (Line 7).

Algorithm 1 Line 9: C will prepare a message m_1 containing the requested CRP associated with ID_v.

Algorithm 1 Line 10: C sends the message m_1 to R. The channel between RSUs and RSUs and C are secure since all these resources are RoTs.

Algorithm 1 Line 11: R selects a particular challenge c and its associated response r. R then calculates the helper data w using forward error correction coding:

$$w = \mathrm{FEC}(r);$$

Algorithm 1 Line 12: R will generate a nonce N to help check the presence and freshness of V.

Algorithm 1 Line 13: R will generate a symmetric secret session key to be used between R and V.

Algorithm 1 Line 14: R will generate a hash based on N, c, and r. This will help with the authentication, presence, and freshness properties.

Algorithm 1 Line 15: R will encrypt the nonce N using the secret session key k.

Algorithm 1 Line 16: R will generate concatenated message m_3.

Algorithm 1 Line 17: R sends m_3 to the vehicle.

Algorithm 1 Line 18: Upon receiving m_3, V will exercise its PUF and use the helper data w to obtain the desired correct response r.

Algorithm 1 Line 19: V will use c and r to generate its local version of the secret session key k.

Algorithm 1 Line 20: V will use the secret key to decode m_2 and obtain the nonce N.
Algorithm 1 Line 21: V will generate the authentication hash value h' using N, c, and r.
Algorithm 1 Line 22: V sends its hash h' to R.
Algorithm 1 Line 23: R compares h and h'.

9. V2V Authentication Protocol

Algorithm 2 is performed to establish authentication and a symmetric session key exchange between two vehicles that desire to communicate. These two vehicles could be intermediate nodes in a multihop Wi-Fi system transmitting data between a source vehicle V_s and a destination vehicle V_d. The two nodes are assumed to be V_1 and V_2, and the general situation is when the two vehicles have been authenticated by two different RSUs: R_1 and R_2, respectively.

Algorithm 2: V2V authentication protocol between two vehicles V_1 and V_2.

```
1  $V_1 \rightarrow R_1$ : request_pairing(ID$_1$, ID$_2$);
2  $R_1$ : get_RSU_ID(ID$_2$);
3  $R_2 \rightarrow R_1$ : acknowledge($ID_2$);
4  $R_1 \rightarrow V_1$ : safe_to_communicate(ID$_2$);
5  $R_2 \rightarrow V_2$ : safe_to_communicate(ID$_1$);
6  $R_1 : N_1 =$ generate_nonce( );
7  $R_1 \rightarrow R_2 : (N_1, \mathrm{ID}_1, \mathrm{ID}_2)$;
8  $R_2 : N_2 =$ generate_nonce( );
9  $R_2 : k_{2,1} = H(N_1, N_2, \mathrm{ID}_1, \mathrm{ID}_2)$;
10 $R_2 : h_{2,1} = H(N_1, N_2, \mathrm{ID}_1, \mathrm{ID}_2)$;
11 $R_2 \rightarrow R_1 : (N_2)$;
12 $R_1 : k_{1,2} = H(N_1, N_2, \mathrm{ID}_1, \mathrm{ID}_2)$;
13 $R_1 : h_{1,2} = H(N_1, N_2, \mathrm{ID}_1, \mathrm{ID}_2)$;
14 $R_1 : m_1 = E_{k_1}(k_{1,2}, h_{1,2})$;
15 $R_2 : m_2 = E_{k_2}(k_{2,1}, h_{2,1})$;
16 $R_1 \rightarrow V_1 : m_1$;
17 $R_2 \rightarrow V_2 : m_2$;
18 $V_1 : m_3 = D_{k_1}(m_1)$;
19 $V_2 : m_4 = D_{k_2}(m_2)$;
20 $V_1 \rightarrow V_2 : h_{1,2}$;
21 $V_2 \rightarrow V_1 : h_{2,1}$;
22 if $h1, 2 = h_{2,1}$ then
23     move to V2V communication
24 else
25     failed authentication at $V_1$
26 end
27 if $h_{2,1} = h_{1,2}$ then
28     move to V2V communication
29 else
30     failed authentication at $V_2$
31 end
```

It is required that V_1 and V_2 establish mutual authentication and exchange a session key before starting to communicate.

Algorithm 2 Line 1: Vehicle V_1 contacts RSU R_1 requesting to be paired with vehicle V_2 to establish one hop of the multihop connection.

Algorithm 2 Line 2: R_1 broadcasts a message to all the adjacent RSUs inquiring which RSU has authenticated V_2 with identity ID$_2$.

Algorithm 2 Line 3: R_2 informs R_1 that it is the RSU that authenticated V_2.

Algorithm 2 Line 4: R_1 informs V_1 that is safe to communicate with V_2 since it has already been authenticated.

Algorithm 2 Line 5: R_2 informs V_2 that is safe to communicate with V_1 since it has already been authenticated.

Algorithm 2 Line 6: R_1 generates nonce N_1 to help with ensuring the freshness and presence properties of V_1.

Algorithm 2 Line 7: R_1 now sends a message to R_2 containing the generated nonce and the IDs of the two communicating vehicles.

Algorithm 2 Line 8: R_2 generates a nonce N_2 to ensure the presence and freshness of the connection.

Algorithm 2 Line 9: R_2 now generates the secret session key $k_{2,1}$ that will be used by V_1 and V_2.

Algorithm 2 Line 10: R_2 generates an authentication hash function $h_{2,1}$ to help prove the authenticity of V_1 and V_2 and ensure their freshness and presence.

Algorithm 2 Line 11: R_2 sends the secret data $k_{1,2}$ and $h_{1,2}$ to R_1.

Algorithm 2 Line 12: R_1 generates the secret session key $k_{1,2}$ that will be used by V_1 and V_2.

Algorithm 2 Line 13: R_1 generates an authentication hash function $h_{1,2}$ to help prove the authenticity of V_1 and V_2 and ensure their freshness and presence.

Algorithm 2 Line 14: R_1 encrypts message m_1 using the local secret key k_1. The message contains the secret data $k_{1,2}$ and $h_{1,2}$ to R_1.

Algorithm 2 Line 15: R_2 encrypts message m_2 using the local secret key k_1. The message contains the secret data $k_{1,2}$ and $h_{1,2}$ to R_2.

Algorithm 2 Line 16: R_1 sends the message m_1 to V_1.

Algorithm 2 Line 17: R_2 sends the message m_2 to V_2.

Algorithm 2 Line 18: V_1 decodes m_1 using its local secret key k_1. Now V_1 has knowledge of the secret key $k_{1,2}$ to use for communication with V_2. The message also contains the hash value $h_{1,2}$.

Algorithm 2 Line 19: V_2 decodes m_2 using its local secret key k_2. Now V_2 has knowledge of the secret key $k_{2,1}$ to use for communication with V_1. The message also contains the hash value $h_{2,1}$.

Algorithm 2 Line 20: V_1 sends to V_1 its version $h_{1,2}$ to establish mutual authentication.

Algorithm 2 Line 21: V_2 sends to V_1 its version $h_{2,1}$ to establish mutual authentication.

Algorithm 2 Lines 22–27: V_1 checks that $h_{1,2}$ equals $h_{2,1}$.

Algorithm 2 Lines 28–33: V_2 checks that $h_{2,1}$ equals $h_{1,2}$.

10. Informal Security Analysis of the Proposed Protocols

We discuss here some attacks and how the proposed protocols counter them.

10.1. Tampering Attack

A tampering attack relies on gaining access to the physical devices to modify memory content or obtain information about the construction of PUF circuits. The PUF circuit is very sensitive to any changes in the integrated circuit environment. The response of the PUF will be drastically changed and the vehicle will not be able to gain access to the system since its biometric has been irreversibly damaged.

10.2. Replay Attack

A replay attacker intercepts authentication challenge/response messages and resends a delayed or repeated response when a challenge is received. However, Algorithms 1 and 2 abundantly use nonces that change for each session or change on a regular basis. Thus, the responses to the same challenge will be totally different, and repeating a response does not offer any hope of gaining access to the system.

10.3. Eavesdropping Attack

In our proposed algorithms, almost all messages are encrypted using dynamic and oft-changing secret keys. In our proposed Algorithms 1 and 2, all messages are encrypted and not sent as plain text. There is one exception in Algorithm 1 on Line 16, which shows sending messages in the clear. The message contains the challenge c destined to a vehicle and the associated helper data w. These data do not help the attacker gain any information about the expected response. Algorithm 2 does not send any messages in the clear.

10.4. Impersonation Attack

A vehicle trying to impersonate another vehicle must mimic its PUF CRP set to gain access to the system resources and participate in the system activities and services. This is necessary since our proposed protocols rely heavily on PUFs to establish unique and unclonable vehicle biometrics. A PUF can not be duplicated. An impersonating device can not 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.

10.5. Man-in-the-Midddle Attack

In a VAN, a man-in-the-middle attack is accomplished with a malicious vehicle inserting itself into the multihop chain to replace another vehicle. However, this mode of communication is protected by at least four layers: insisting that all vehicles are first authenticated via RSUs, using nonces, using dynamic secret keys, and the extensive use of hashing. A malicious vehicle will not be be able to register with an RSU and will not be able to participate in any activity.

10.6. 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 femto cells. Thus, an attacker can not learn past or future keys.

10.7. Session Key Guessing Attack

In our protocols there are two session keys: the secret key k_i between an RSU and vehicle ID_i via $V2I$ and the secret key $k_{i,j}$ between vehicle ID_i and ID_j via $V2V$. These keys can not be inferred since they are not stored in NVRAMs and dynamically change through the extensive use of nonces. Thus, the attacker has to randomly guess two keys, and not just one, go obtain any hope of communicating.

10.8. Cloning Attack

A cloning attack attempts to replicate the credentials of the vehicle. We explained that PUFs are mainly used to authenticate the vehicle and provide a means of generating dynamic secret keys. In addition, a PUF can not be cloned since its response will be inherently different.

10.9. Physical Attack

Physical attacks try to infer the vehicle secret keys by checking the content of NVRAMs. Using PUFs, there is no need to store secret keys in NVRAMs since they are generated dynamically at the start of each session. Algorithms 1 and 2 show that the PUF response is never revealed but is used to generate secret keys and hash values.

11. Conclusions

In summation, our paper's endeavors have culminated in the establishment of a robust and comprehensive framework designed to fortify security within the intricate milieu of VANs. These systems encompass a diverse array of communication modes, including point-to-point visible light communication, 5G/6G cellular wireless communication, and Wi-Fi ad hoc multihop communication. The fulcrum of our work lies in the pioneering utilization of physically unclonable functions (PUFs), which serve as a linchpin for secure key generation, authentication, and the articulation of trust metrics for neighboring vehicles. Our protocols are multifaceted and address a spectrum of security considerations, from the bedrock of authentication and anonymity to the pivotal tenets of the proof of presence, freshness, and the dynamic exchange of ephemeral session keys. We have delved into the complex fabric of VAN security, contending with challenges ranging from tampering and replay attacks to eavesdropping and impersonation. Moreover, our meticulous design ensures resilience against man-in-the-middle attacks and forward/backward secrecy, safeguarding the integrity and confidentiality of VAN communications. A noteworthy feature of our approach is its immunity to cloning and physical attacks, as the PUF-based security mechanism obviates the need to store secret keys in non-volatile memories (NVRAMs). The implications of our contributions are profound, serving as a cornerstone for fortified trust, privacy, and security in the era of smart transportation systems. As VANs continue to evolve, our paper offers a dependable foundation upon which the pillars of secure communication can be erected, ultimately enhancing the reliability and safety of modern transportation systems.

Author Contributions: Conceptualization, M.K.E.; methodology, F.G. and M.K.E.; writing—original draft preparation, F.G.; writing—review and editing, M.K.E. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: Data are contained within the article.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Fakroon, M.; Alshahrani, M.; Gebali, F.; Traorè, I. Secure remote anonymous user authentication scheme for smart home environment. *Internet Things* **2020**, *9*, 100–158. [CrossRef]
2. Fakroon, M.; Gebali, F.; Mamun, M. Multifactor authentication scheme using physically unclonable functions. *Internet Things* **2021**, *9*, 1–28. [CrossRef]
3. Hu, H.; Han, Y.; Yao, M.; Song, X. Trust Based Secure and Energy Efficient Routing Protocol for Wireless Sensor Networks. *IEEE Access* **2022**, *10*, 10585–10596. [CrossRef]
4. Badetia, N.; Hussain, M. Distributed Mechanism For Authentication of Nodes In Wireless Sensor Networks. In Proceedings of the International Conference for Convergence in Technology (I2CT), Mumbai, India, 7–9 April 2017.
5. Al-Mahmud, A.; Akhtar, R. Secure sensor node authentication in wireless sensor networks. *Int. J. Comput. Appl.* **2012**, *46*, 10–17.
6. Tuylis, P. Securing the New Chiplet Era of Semiconductor Design. 2023. Available online: https://www.designing-electronics.com/securing-the-new-chiplet-era-of-semiconductor-design-2/ (accessed on 1 October 2023).
7. The White House. Cybersecurity Labeling Program for Smart Devices. 2023. Available online: https://www.whitehouse.gov/briefing-room/statements-releases/2023/07/18/biden-harris-administration-announces-cybersecurity-labeling-program-for-smart-devices-to-protect-american-consumers/ (accessed on 1 October 2023).
8. 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.
9. Gebali, F. IoT Hardware Security: Using Physically Unclonable Functions (PUFs) for Authentication and Secure Key Exchange. In Proceedings of the International Scientific Conference of the Military Technical College (ICEENG), Cairo, Egypt, 29–31 March 2023.
10. Cui, Y.; Wang, C.; Liu, W.; Yu, Y.; O'Neill, M.; Lombardi, F. Low-Cost Configurable Ring Oscillator PUF with Improved Uniqueness. In Proceedings of the International Symposium on Circucits and Systems (ISCAS), Montreal, QC, Canada, 22–25 May 2016; pp. 558–561.
11. Gassend, B.; Lim, D.; Clarke, D.; van Dijk, M.; Devadas, S. Identification and authentication of integrated circuits. *Concurr. Comput. Pract. Exp.* **2004**, *6*, 1077–1098. [CrossRef]
12. Tuyls, P.; Skoric, B.; Kevenaar, T. *Security with Noisy Data*; Springer: Berlin/Heidelberg, Germany, 2007.