An enhanced authentication solution for infrastructureless vehicle environments

1st Marwa Slimene
Inria
Villeneuve d'Ascq, France
marwa.slimene@inria.fr

2nd Nathalie Mitton
Inria
Villeneuve d'Ascq, France
0000-0002-8817-6275

3rd Patrick Sondi
Center for Digital Systems
IMT Nord Europe
Villeneuve-d'Ascq, France
0000-0001-9484-7357

4th Ahmed Meddahi
Center for Digital Systems
IMT Nord Europe
Villeneuve-d'Ascq, France
0000-0002-9255-2114

***Abstract*—Robust vehicle authentication is essential in order to ensure an effective audit of vehicle-to-vehicle (V2V) communications. However, most existing approaches rely on a centralized infrastructure to access both authorities' certificates andrevocation lists, thus making them ineffective in dynamic and infrastructureless environments. In this paper, we highlight this critical limitation, and propose a method which enables the vehicles to update their local authentication databases independently from infrastructure availability. Our approach aim to allow vehicles to perform V2V authentication using locally stored data, in order to ensure continuity of secure communications even when disconnected from the Infrastructure. We further analyze the probability of successful authentication under two scenarios, which are the first with up-to-date databases, and the second with outdated ones. The analytical results show that the authentication probability decreases to below 75% after 30 hours of disconnection with long-lived certificates, while updates keep it above 90% in highway scenarios, even with short-lived certificates.These findings demonstrate the feasibility of maintaining reliable V2V authentication outside the infrastructure coverage, and point out the necessary improvements for evolving towards secure and auditable V2V communications.**

***Index Terms*—V2V communication, Authentication, infrastructureless environments, Local database management.**

I. Introduction

Ensuring trust and security in vehicular networks is a critical prerequisite for the safe deployment of cooperative and autonomous driving systems. Among the various security mechanisms, authentication plays a central role in verifying the legitimacy of communicating entities and preventing malicious intrusion or falsification of messages. Authentication is a cornerstone of secure vehicular communication systems. It ensures that only legitimate entities participate in message exchanges, thereby preserving message integrity, establishing trust among peers, and enabling traceability for misbehavior detection or post-incident audit. Nowaday, most solutions rely on mechanisms based on public key infrastructure (PKI), which involve digital certificates, certificate authorities (CA), and regular access to certificate revocation lists (CRL). These systems are effective when vehicles remain connected to infrastructure, such as Edge or Cloud services through roadside units (RSUs) or base stations.

However, in infrastructureless environments, such as rural areas, vehicles may not be able to access up-to-date revocation lists or CA certificates of some other vehicles' certificate. Such situations could severely compromise their ability to authenticate other entities, rendering traditional PKI-based solutions ineffective. Some proposals suggest relying on relay vehicles or different types of lead nodes to supply disconnected authentication, but these approaches still maintain a partial dependency on infrastructure and fail to guarantee full autonomy in infrastructureless contexts.

This paper addresses the following question: *how can authentication remain reliable when vehicles solely rely on potentially outdated local data*? Through a combination of analytical modeling and distributed protocol design, our contribution draws a thorough evaluation of authentication in infrastructureless environments, complemented by a distributed solution that mitigates the effects of data obsolescence through peer-to-peer updates. Specifically, we:

- Propose an analytical model to estimate the probability of successful authentication over time, considering certificate validity, revocation rate, and the freshness of local authentication databases;
- Develop an opportunistic and distributed update protocol enabling vehicles to synchronize their authentication data when encountering other vehicles;
- Evaluate the effectiveness of our approach through simulations, in order to draw potential improvements in authentication reliability under disconnection conditions;
- Discuss deployment implications, protocol limitations, and integration of proposals into V2X architecture.

The remainder of this paper is structured as follows. Section II presents related work and outlines the limitations of existing solutions. Section III introduces the analytical model used to evaluate authentication reliability in infrastructureless vehicular environments. Section IV describes the proposed distributed protocol designed to improve authentication reliability outside infrastructure coverage and presents the corresponding results and analyses. Finally, Section V concludes the paper and outlines future research directions.

II. Related Work

PKI forms the foundational pillar of authentication in vehicular networks, enabling vehicles to mutually verify identities

979-8-3503-9281-4/25/$31.00 ©2025 IEEE

through certificates issued by trusted CAs. While PKI mechanisms have demonstrated their effectiveness in connected environments, they face critical limitations in infrastructureless contexts—i.e., scenarios lacking RSU, cellular networks (5G), or any other Internet access. In such disconnected situations, authentication must be performed locally, without relying on external connectivity for certificate issuance, verification, or revocation. Recent studies attempted to address this challenge by proposing cooperative or decentralized mechanisms to preserve PKI-based authentication under isolated conditions.

The solution proposed in [1] introduces a self-organized security framework based on dynamic vehicle clustering, where cluster heads locally manage authentication. The scheme operates entirely without infrastructure and relies solely on V2V communications. However, it depends on stable cluster formation and sustained cooperation among vehicles, which are difficult to maintain in low-density or highly dynamic environments. In [2], the authors present an aggregate authentication mechanism based on elliptic curve cryptography and certificateless signatures, aiming to improve verification efficiency. Although designed for infrastructureless settings, this scheme presupposes a trusted authority for key generation, introducing an implicit dependency on infrastructure. Moreover, it does not address certificate revocation in disconnected scenarios. The work in [3] proposes a blockchain-based certificate revocation scheme where revoked credentials are propagated via a distributed ledger. While this approach ensures fast and transparent revocation dissemination, it requires vehicles to access the blockchain network, thus relying on at least intermittent Internet connectivity. As such, it remains unsuitable for fully disconnected vehicular environments. Combining blockchain technology with cryptographic accumulators and zero-knowledge proofs (ZKP) [4] allows a vehicle to verify the revocation status of a certificate without downloading the entire Certificate Revocation List (CRL). However, the accumulators must be regularly updated, which again introduces a dependency on periodic access to the blockchain. The certificate revocation scheme proposed in [5] also leverages blockchain and accumulators to reduce storage and improve verification efficiency. However, it requires synchronization with a distributed ledger, making it impractical for purely infrastructureless scenarios. A fully decentralized certificate management system is presented in [6], using a private blockchain and a voting mechanism among vehicles to handle certificate issuance and revocation. Although this design eliminates reliance on centralized authorities, it depends on high node participation and robust consensus protocols, which are difficult to guarantee in sparse or intermittently connected networks.

In summary, while all these approaches aim to minimize reliance on infrastructure, most of them depend on implicit assumptions such as intermittent Internet access, the ability to synchronize distributed ledgers, or sustained cooperation among nodes. These assumptions do not hold in disconnected situations, such as rural highways or post-disaster areas.

III. Authentication reliability in infrastructureless environments

Ensuring secure and reliable authentication in vehicular networks is paramount, particularly in scenarios where access to infrastructure such as 5G networks, Edge/Cloud services, or RSUs is intermittent or nonexistent. While numerous studies have addressed authentication mechanisms within infrastructure coverage, the challenges posed by infrastructureless settings remain less explored. To bridge this gap, we develop an analytical model to evaluate the probability of successful authentication between vehicles operating without consistent access to the network infrastructure.

A. Analytical model

In our scenario illustrated in figure 1, we consider a vehicle initially traveling on a highway within an infrastructure-covered area. The vehicle is connected to the infrastructure via RSUs, allowing it to access a global authentication database containing up-to-date certificates issued by authentication authorities, as well as the corresponding revocation lists. Once the vehicle leaves the coverage area and enters a rural zone, it loses access to this infrastructure, including any 5G gNB, RSU, Edge or Cloud-based connectivity. At the moment of disconnection t_0, the vehicle stores a complete local copy of the authentication databases available just before leaving the covered area. From that point onward, the vehicle relies exclusively on this local copy to authenticate other vehicles encountered through V2V communications. Over time, these databases become increasingly obsolete, which directly impacts the reliability of the authentication process. The objective is to evaluate the reliability of the authentication process in uncovered areas. We develop an analytical model to compute the probability a vehicle can authenticate another, based on its potentially outdated local databases, at a given time t_i after leaving the coverage area, denoted as $P_{\text{auth}}(t_i)$. The study is carried out in a simplified highway scenario, where vehicles move along a straight road. The model accounts for vehicle mobility, encounter probability (modeled as a Poisson process), and key factors such as certificate expiration, revocation rate, and the freshness of local databases. These aspects are represented using exponential laws to capture their time-dependent behavior under disconnected conditions. Probability of successful authentication at time t_i is :

$$P_{\text{auth}}(t_i) = P_r \cdot P_{\text{val}}(t_i)$$

with:

- P_r: Probability of encountering a vehicle.
- $P_{\text{val}}(t_i)$: Probability a certificate is valid at time t_i.

Probability of encountering a vehicle follows a Poisson model:

$$P_r(t_i) = \int_0^{t_i} \lambda_v v e^{-\lambda_v v t}\, dt = 1 - e^{-\lambda_v v t_i}$$

with:

- λ: Density of vehicles (vehicles/km).
- v: Average speed of vehicles (km/h).

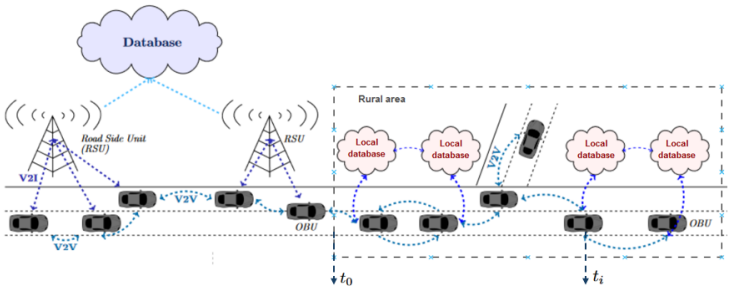

Fig. 1. V2I and V2V Authentication System.

- $\Delta t = t_i - t_0$: duration since disconnection.

A certificate is considered valid if:

1) The vehicle is not revoked $(1 - P_{\text{rev}})$ and local databases are up-to-date.
2) Or the vehicle is revoked but ignores it $(P_{\text{rev}} \cdot P_{\text{unk}})$.
3) And the certificate has not expired $(1 - P_{\text{exp}})$.

Therefore:

$$P_{\text{val}}(t_i) = [(1 - P_{\text{rev}}) + P_{\text{rev}} \cdot P_{\text{unk}}] \cdot (1 - P_{\text{exp}})$$

Probability of having a vehicle revoked at time t_i depends on the revocation rate λ_R:

$$P_{\text{rev}}(t_i) = \int_0^{t_i} \lambda_R e^{-\lambda_R t}\, dt = 1 - e^{-\lambda_R t_i}$$

Probability that a certificate has expired depends on the time elapsed since it was issued $(t_i - t_{\text{émis}})$ and follows an exponential decrease:

$$P_{\text{exp}}(t_i) = \int_0^{t_i} \lambda_{\text{exp}} e^{-\lambda_{\text{exp}}(t - t_{\text{émis}})} dt = 1 - e^{-\lambda_{\text{exp}} \cdot (t_i - t_{\text{émis}})}$$

Probability that a certificate is revoked without notification:

$$P_{\text{unk}}(t_i) = P_{\text{not\_meeting}}(t_i) \cdot P_{\text{deconnection}}(t_i)$$

with:

- $P_{\text{not\_meeting}}(t_i)$: Probability of not finding a vehicle with up-to-date databases.
- $P_{\text{deconnection}}(t_i)$: Probability that the vehicle has been offline for a time $t_i - t_{\text{update}}$.

$$\begin{aligned} P_{\text{not\_meeting}}(t_i) &= \int_0^{t_i} \lambda v p_{\text{comm}} f \cdot e^{-\lambda v p_{\text{comm}} f (t - t_{\text{update}})} dt \\ &= e^{-\lambda v p_{\text{comm}} f (t_i - t_{\text{update}})} \end{aligned}$$

with:

- λ: Density of vehicles (vehicles/km).
- v: Average speed of vehicles (km/h).
- p_{comm}: Successful communication between 2 vehicles.
- f: Fraction of vehicles with an up-to-date database.
- T_{obsolete}: Time after which data becomes obsolete.
- t_{update}: Time of last update.

$$P_{\text{unk}}(t_i) = \begin{cases} e^{-\lambda v p_{\text{comm}} f (t_i - t_{\text{update}})}, & \text{if } t_i - t_{\text{update}} > T_{\text{obsolete}}, \\ 0, & \text{otherwise.} \end{cases}$$

Hence the final equation:

$$P_{\text{auth}}(t_i) = (1 - e^{-\lambda_v v t_i}) \cdot [(1 - P_{\text{rev}}(t_i)) + P_{\text{rev}}(t_i) \cdot P_{\text{unk}}(t_i)] \cdot (1 - P_{\text{exp}}(t_i))$$

$$= (1 - e^{-\lambda_v v t_i}) \cdot (e^{-\lambda_R t_i} + (1 - e^{-\lambda_R t_i}) P_{\text{unk}}(t_i)) \cdot e^{-\lambda_{\text{exp}} \cdot (t_i - t_{\text{émis}})}$$

Finally, by replacing $P_{\text{unk}}(t_i)$:

$$P_{\text{auth}}(t_i) = \begin{cases} (1 - e^{-\lambda_v v t_i}) \cdot \left(e^{-\lambda_R t_i} + (1 - e^{-\lambda_R t_i}) e^{-\lambda_v p_{\text{comm}} f (t_i - t_{\text{update}})}\right) \\ \quad \cdot e^{-\lambda_{\text{exp}} (t_i - t_{\text{émis}})}, \quad \text{if } t_i - t_{\text{update}} > T_{\text{obsolete}} \\ (1 - e^{-\lambda_v v t_i}) \cdot e^{-\lambda_R t_i} \cdot e^{-\lambda_{\text{exp}} (t_i - t_{\text{émis}})}, \quad \text{otherwise} \end{cases}$$

To realistically estimate this probability, we referred to the scientific literature and existing standards to identify typical values for key parameters. These include, among others, certificate lifetime, the time after which a local database becomes obsolete, average vehicle speed, as well as revocation and communication rates. The selected values are summarized in Table 1. We first define the set of parameters used to compute the authentication probabilities. All values are derived from current state-of-the-art methodologies and empirical studies:

- Certificate revocation rate: $\lambda_R = 0.005$ /per hour.
- Data obsolescence threshold: $T_{\text{obsolete}} = 0.5$ hour .
- Vehicle density: $\lambda_v = 20$ vehicles/km.
- Average vehicle speed: $v = 100$ km/h.
- Average certificate lifetime: $T_{\text{cert}} = \{5min, 24h, 168h\}$
- Certificate expiration rate: $\lambda_{\text{exp}} = \frac{1}{T_{\text{cert}}}$ /hour.
- Initial update time: $t_{\text{update}} = 0$.
- Initial assumption of no meeting: $P_{\text{not\_meeting}}(t_i) = 1$.

B. Results and discussion

To evaluate the reliability of vehicle-to-vehicle authentication in infrastructureless environments, we simulate the analytical model for three different certificate lifetimes: 168 hours, 24 hours, and 5 minutes. The latter reflects the constraints imposed by privacy-preserving systems, where short-lived pseudonyms are frequently rotated to mitigate vehicle tracking. Such designs necessitate frequent certificate renewal.

Figure 2 illustrates the evolution of the authentication probability $P_{\text{auth}}(t)$ as a function of the time elapsed since

Parameters	Typical Values	Sources and Justifications
Root CA certificate lifetime	5–10 years	[7]–[10] Root certificates are rarely renewed to maintain the stability of the trust chain.
Short-lived certificates	1 day, 1 month or 1 certificate per message	[11] Short validity helps protect privacy and reduces impact in case of key compromise.
Certificate revocation rate	0.1% to 1% per hour	[12]–[15] Rate varies by scenario, typically low under normal operating conditions.
BSM message frequency	Every 100 ms	[11], [16] For safety-critical messages.
Event or cancellation messages	1 message every 1–5 seconds	[11] Sent upon specific events; frequency depends on context and urgency.
CRL update requirement	Every 30 min to 1 hour	[17], [18] Frequent updates quickly reflect certificate status changes.

TABLE I
SUMMARY OF KEY PARAMETER VALUES FOR V2X

the vehicle lost connectivity to the infrastructure. The x-axis represents time in hours, while the y-axis denotes the corresponding probability of successful authentication based solely on the local, potentially outdated, certificate database.

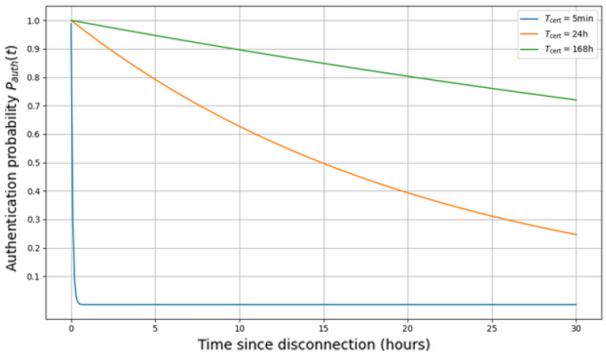

Fig. 2. Evolution of authentication probability over time depending on certificate lifetime duration.

As expected, longer certificate lifetimes result in a slower decline in authentication reliability. When $T_{\text{cert}} = 168$ hours, the authentication probability remains above 0.65 even after 40 hours of disconnection. In contrast, for $T_{\text{cert}} = 24$ hours, the degradation is more pronounced, with $P_{\text{auth}}(t)$ dropping below 0.2 over the same period, significantly reducing the chance of successful peer authentication. The most critical scenario arises with the shortest certificate duration, $T_{\text{cert}} = 5$ minutes. In this case, the probability drops sharply—falling below 0.3 in less than one hour and approaching zero shortly thereafter. This rapid decline is explained by the high expiration rate $\lambda_{\text{exp}} = 1/T_{\text{cert}}$, which causes most locally stored certificates to become invalid within a short time frame. Such conditions are typical in anonymity-focused systems, where pseudonym changes are frequent and aggressive.

These findings reveal a fundamental trade-off between privacy and robustness. While short-lived certificates enhance anonymity and reduce long-term linkability, they also narrow the time window during which effective authentication can occur—especially in disconnected scenarios. If peer-to-peer updates are infrequent, due to low vehicle density or unreliable communication, the authentication process deteriorates quickly. This underscores the need to balance privacy-oriented mechanisms (e.g., frequent pseudonym rotation) with operational resilience. A potential solution, outlined in Section IV, is to enable opportunistic synchronization of authentication data among vehicles. Such a distributed protocol could significantly extend the practical validity of short-term certificates by propagating fresh authentication information even in the absence of infrastructure.

IV. Our Contribution for Peer-Based Authentication Data Synchronization

A. Proposed protocol

In disconnected vehicular environments, the success of V2V authentication depends heavily on the freshness of each vehicle's local authentication database. To counter the natural degradation of trust over time, we propose a decentralized update protocol that allows vehicles to opportunistically refresh their databases through encounters with peers. The protocol differentiates between two types of vehicles:

- Trusted vehicles: These include emergency services (e.g., police, ambulance, fire trucks), fleet vehicles from certified manufacturers, or any entity officially recognized as trustworthy.
- Standard vehicles: All other vehicles without formal trust status. They can participate in data exchange but are subject to stricter conditions for updates.

This distinction is essential to prioritize trust and prevent the propagation of outdated or malicious data.

Trusted Vehicle (TV) Behavior

As shown in Fig.3, TVs start checking the freshness of their database as soon as they leave infrastructure. They can only update from the infrastructure or another trusted vehicle. If the database is still valid, they operate normally and periodically broadcast their presence so that nearby standard vehicles can update from them. If the database is outdated, they attempt to update via a trusted peer.

Standard vehicle behavior

As soon as a standard vehicle leaves the infrastructure, it begins monitoring the age of its local authentication database. If the database becomes outdated (i.e., exceeds the obsolescence threshold), the vehicle enters a cautious operating mode: it limits sensitive data exchanges and starts broadcasting update requests to nearby vehicles.

When encountering other vehicles, the update process follows these rules:

- If a trusted vehicle responds, the update is performed immediately using its database.

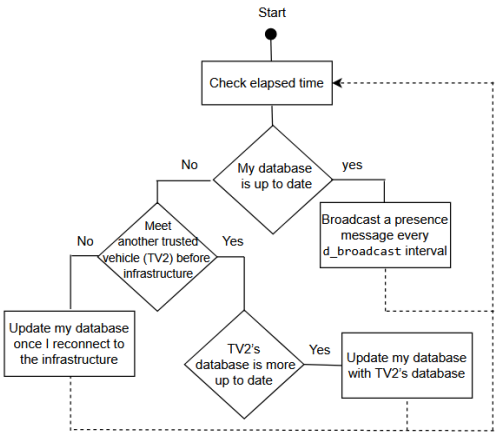

Fig. 3. Behavior of a trusted vehicle in infrastructureless environments.

- If another standard vehicle is encountered, the update is only accepted if the peer's database is more recent and still within the acceptable obsolescence window.
- In case multiple candidates are present:
  - A trusted vehicle is always prioritized.
  - Otherwise, the standard vehicle selects the most recent valid database version available.

This process is iterative, enabling the standard vehicle to progressively improve the freshness of its authentication data as it continues its movement outside infrastructure coverage.

B. Evaluation of the proposed protocol

To evaluate the effectiveness of the proposed protocol, we studied the most favorable case for database freshness renewal, aiming to observe the maximum possible improvement in authentication probability.

We consider a highway scenario where vehicle V1, after downloading a fresh authentication database from infrastructure, enters a disconnected segment while driving at a moderate speed of 100 km/h. The goal is to identify the best possible encounter that allows V1 to opportunistically reset its authentication freshness parameter (t_{update}). This scenario is illustrated in figure 4, which shows vehicle V1 crossing an uncovered highway segment and updating its authentication database by interacting with other vehicles, depending on their respective positions.

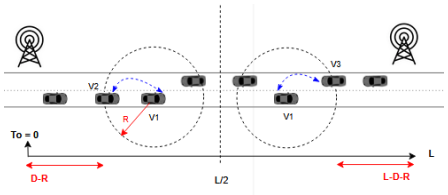

Fig. 4. Strategic update opportunities based on vehicle position and direction.

Two optimal cases are considered:

- If V1 is in the first half of the uncovered segment, the most favorable case is meeting a faster vehicle V2, traveling in the same direction at the maximum highway speed of 130 km/h, located within V1's communication range and as close as possible to the left-side infrastructure.
- If V1 is in the 2^{nd} half, the best case is met when a vehicle V3 comes from the opposite direction, also at 130 km/h, having recently exited the infrastructure zone.

In both situations, the encountered vehicle is assumed to hold a fresher database. The value of t_{update} is then dynamically adjusted based on the estimated time since the peer's last infrastructure contact, computed using V1's current position D along the highway and the communication range R.

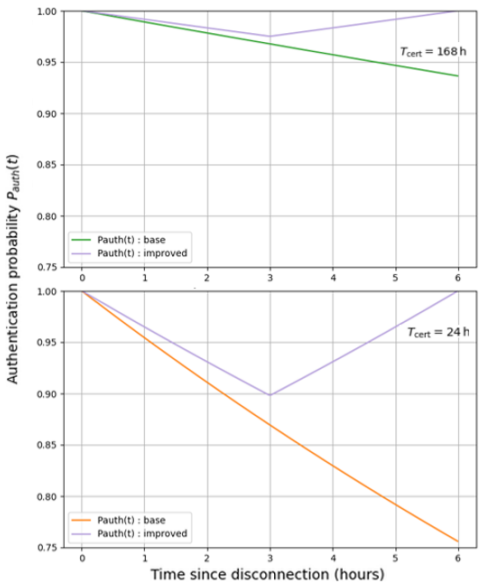

Fig. 5. Improved P_{auth} on a $L = 600$ km highway segment.

The improved authentication probability is expressed as:

$$P_{\text{auth-improved}}(t_i) = P_{\text{auth}}(t_x)$$
$$\text{with} \quad t_x = \begin{cases} \frac{D-R}{v_x}, & \text{if } D < \frac{L}{2} \\ \frac{L-D-R}{v_x}, & \text{if } D > \frac{L}{2} \end{cases}$$

To quantify the benefits of the proposed protocol, we evaluate its impact on the authentication probability in two realistic highway configurations: $L = 600$ km and $L = 100$ km. In both scenarios, the road is delimited at each end by RSUs, and each vehicle initially receives a complete authentication database before leaving coverage. The observed vehicle travels at a constant speed of $v_{\text{node}} = 100$ km/h, while encountered vehicles travel at $v_X = 130$ km/h. The communication range is set to $R = 0.5$ km, and two certificate lifetimes are considered: $T_{\text{cert}} = 168$ h and $T_{\text{cert}} = 24$ h.

In each case, we compare the evolution of the authentication probability over time for:

- The base case where the database remains static throughout the trip.
- The improved case where opportunistic updates are enabled via encounters with fresher peers.

Figures 5 and 6 illustrate the enhancement of the authentication probability at each instant $t_x > 0$ after the vehicle

departs from infrastructure. Over the entire segment of length L between two RSUs, the improved curve highlights the effect of mid-trip updates that refresh the database and help maintain high authentication success.

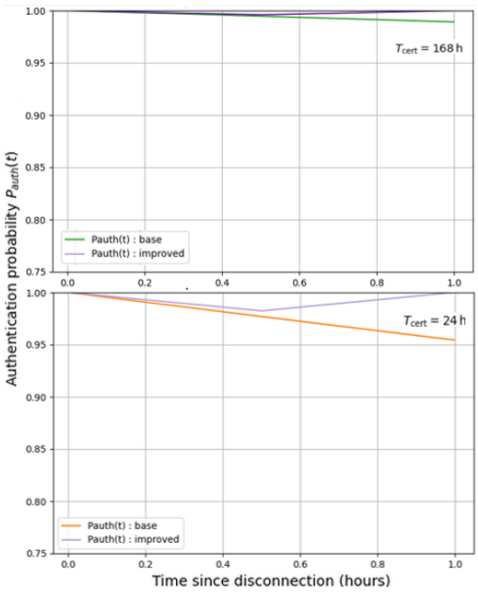

Fig. 6. Improved P_{auth} on a $L = 100$ km highway segment.

- On a longer highway 600 km, we observe a significant improvement in authentication when V1 is allowed to update its database through encounters. This is especially noticeable when certificate lifetimes are short 2h, as updates help counteract the rapid trust decay.
- On a shorter highway 100 km,update opportunities are naturally more frequent due to higher vehicle density in the covered areas. The gap between P_{auth} and P_{improved} is smaller but remains non-negligible, particularly when the certificate validity period is short.

The authentication model raises several practical implications for deployment. It significantly improves authentication reliability outside infrastructure coverage by enabling opportunistic updates of local databases. However, its effectiveness depends on the presence of nearby vehicles, particularly trusted ones, which is guaranteed in low-density areas.

V. Conclusion and Perspectives

This paper addresses the challenge of maintaining reliable authentication in V2V communications without the support of a centralized infrastructure. Based on the existing authentication solutions of the literature, we propose a way to ensure authentication continuity both within and outside infrastructure coverage. Our main contribution is an analytical model that captures the evolution of authentication probability over time, considering certificates' expiration, revocations, and databases' freshness. The analyzes reveal the limitations of static credentials and the rapid degradation of trust in disconnected scenario. To mitigate these challenges, we introduce a decentralized update protocol that enables vehicles to opportunistically refresh their authentication databases through encounters with other peers. The protocol is designed for being integrated seamlessly into hybrid V2X architectures, where it could complement centralized authentication mechanisms in order to maintain reliability during infrastructure outages.

In our future work, we intend to implement the proposed protocol in a vehicular simulation environment to evaluate its performance under varying road configurations, traffic densities and mobility patterns. Ultimately, our goal is to use the proposed protocol in order to develop a fully auditable V2V authentication system which will remain operational regardless of infrastructure availability, and guarantee auditability.

Acknowledgment

This work was supported by the French national research program PEPR Future Intelligent Networks for Trusted and Sustainable Systems (FITNESS).

References

[1] F. M. Salem and A. S. Ali, "Sos: Self-organized secure framework for VANET," *Int. Journal of Com. Systems*, vol. 33, no. 7, p. 4317, 2020.
[2] H. Tan, W. Zheng, P. Vijayakumar, K. Sakurai, and N. Kumar, "An efficient vehicle-assisted aggregate authentication scheme for infrastructureless vehicular networks," *IEEE Trans. on Intelligent Transportation Systems*, vol. 24, no. 12, pp. 15 590–15 600, 2023.
[3] J. K. Shahrouz and M. Analoui, "Privacy-aware revocation in VANETs with a blockchain using accumulator," *Vehicular Communications*, vol. 53, p. 100918, 2025.
[4] A. Tesei, D. Lattuca, M. Luise, P. Pagano, J. Ferreira, and P. C. Bartolomeu, "A transparent distributed ledger-based certificate revocation scheme for VANETs," *Journal of Network and Computer Applications*, vol. 212, p. 103569, 2023.
[5] J. Xie, J. Leng *et al.*, "Cr-ba: Public key infrastructure certificate revocation scheme based on blockchain and accumulator," *Security and Communication Networks*, vol. 2022, p. 2069195, 2022.
[6] M. N. S. Perera, T. Nakamura, M. Hashimoto, H. Yokoyama, C. Cheng, and K. Sakurai, "Certificate management scheme for VANETs using blockchain structure," *Cryptography*, vol. 6, no. 2, p. 20, 2022.
[7] H. U. Team, "Accountable de-anonymization in v2x communication," *Vehicular Communication Journal*, 2023.
[8] *C2C-CC (Car2Car Communication Consortium) Security Standards*, Car2Car Communication Consortium Std., 2019.
[9] A. Haidar, "Validation platform for secure v2x communications," *PhD Thesis, Politecnico di Torino*, 2020.
[10] J. Smith and A. Doe, "Post-quantum impacts on v2x certificates," *IEEE Vehicular Communications*, 2023.
[11] *ETSI ITS-G5 - European ITS Communication Standards*, European Telecommunications Standards Institute Std., 2016.
[12] G. Scopelliti, C. Baumann, F. Alder, and E. Truyen, "Efficient and timely revocation of v2x credentials," in *Proc. of Int. Conf. on Vehicular Communication Systems*. Falder Publishing, 2024.
[13] B. Brecht, D. Therriault, A. Weimerskirch, W. Whyte, V. Kumar, T. Hehn, and R. Goudy, "A security credential management system for v2x communications," *IEEE Transactions on Intelligent Transportation Systems*, vol. 19, no. 12, pp. 3850–3871, 2018.
[14] T. Wang and Y. Lee, "Survey on certificate revocation schemes," *IEEE Access*, 2020.
[15] M. A. Simplicio and C. B. Margi, "Revocation in vehicular public key infrastructures," *Vehicular Networking Conference*, 2021.
[16] *IEEE 802.11p - Wireless Access in Vehicular Environments*, IEEE Standards Association Std., 2010.
[17] *IEEE 1609.2 - IEEE Standard for Wireless Access in Vehicular Environments (WAVE)–Security Services for Applications and Management Messages*, IEEE Standards Association Std., 2016.
[18] *ETSI TS 103 097 - Intelligent Transport Systems (ITS); Security; Security header and certificate formats*, European Telecommunications Standards Institute (ETSI) Std., 2016.