J Inf Process Syst, Vol.21, No.5, pp.555~563, October 2025
https://doi.org/10.3745/JIPS.03.0210

ISSN 2092-805X (Electronic)

JOURNAL OF INFORMATION PROCESSING SYSTEMS JIPS

# V-TRACE: Persistent Tracking Misbehaving Vehicles under Pseudonym Changes in V2X Networks

Juntaek Lee[1], Jiwoo Lee[1], Chanmin Kim[1], and Jiwon Seo[2,*]

**Abstract**

As connected and cooperative intelligent transportation systems (C-ITS) advance with vehicle-to-everything (V2X) communication, the risk of cyber threats such as false data injection and message flooding continues to grow. We present V-TRACE, a lightweight and standard-compliant framework for vehicle tracking and identification that operates effectively even under frequent pseudonym changes. V-TRACE initiates real-time tracking upon detecting anomalous behavior and correlates spatiotemporal patterns across V2X messages to sustain traceability. When identifier rotation occurs, the system seamlessly transitions to an identification phase that maintains persistent monitoring and suppresses further impact. Unlike approaches that require protocol modifications, V-TRACE operates fully within existing V2X standards, ensuring compatibility with current C-ITS deployments. We implement and evaluate V-TRACE using a high-fidelity CANoe.Car2x simulation. Experimental results demonstrate that V-TRACE reliably tracks and re-identifies misbehaving vehicles with minimal overhead, confirming its scalability and practicality in real-world traffic scenarios.

**Keywords**

Cooperative Intelligent Transportation Systems (C-ITS), Misbehaving Vehicle Tracking, V2X

## 1. Introduction

The growing deployment of cooperative intelligent transportation systems (C-ITS) powered by vehicle-to-everything (V2X) communication is fundamentally transforming road safety and mobility. By enabling real-time data exchange among vehicles, roadside units (RSUs), and infrastructure, V2X enhances situational awareness and supports applications such as collision avoidance, traffic incident warnings, and cooperative lane merging. However, the increased connectivity also expands the attack surface for cyber threats that may compromise system integrity and public safety.

Unlike conventional IT systems, cyberattacks in vehicular networks can lead to immediate physical consequences—including traffic collisions, emergency stops, or manipulation of traffic signals—posing significant risks to passengers and public infrastructure [1]. To mitigate such threats, a variety of misbehavior detection techniques have been proposed. Cryptographic approaches focus on signature verification [2], while consistency-based schemes validate message content using spatial and temporal

Manuscript received July 7, 2025; first revision August 13, 2025; accepted September 11, 2025.

* **Corresponding Author:** Jiwon Seo (jwseo@dankook.ac.kr)

[1] Convergence Security Laboratory, Korea Automotive Technology Institute (KATECH), Incheon, Korea (jtlee@katech.re.kr, jwlee3@katech.re.kr, cmkim@katech.re.kr)

[2] Department of Cyber Security, Dankook University, Yongin, Korea (jwseo@dankook.ac.kr)

Juntaek Lee, Jiwoo Lee, and Chanmin Kim contributed equally to this work.

correlation among peers [3]. More recently, machine learning (ML)-based techniques have shown promise in detecting behavioral anomalies through pattern recognition [4]. Despite their effectiveness, these methods are typically limited to passive detection. Once a malicious vehicle is flagged, it may continue to disseminate harmful messages, exacerbating the attack impact. Furthermore, privacy-preserving mechanisms such as frequent pseudonym rotation—designed to prevent vehicle tracking—make it difficult to maintain situational awareness of detected adversaries over time.

In this paper, we present V-TRACE, a scalable and lightweight framework for misbehavior-aware “vehicle tracking” and “identification” in V2X environments. V-TRACE augments existing detection logic with persistent tracking and targeted mitigation, even in the presence of pseudonym changes. Upon detection of anomalous behavior, V-TRACE initiates real-time tracking using basic safety messages (BSMs), and transitions to an identification phase using probe vehicle data (PVD) when vehicle identifiers change. This design enables continuity in monitoring adversarial vehicles, by relying solely on standard-compliant V2X messages without requiring protocol modifications. In addition, the tracking and identification components in V-TRACE are orthogonal to the underlying detection logic, supporting integration with cryptographic, consistency-based, or ML-based misbehavior detectors. To validate the effectiveness of our framework, we implement and evaluate V-TRACE in a high-fidelity simulation using CANoe.Car2x. Experimental results demonstrate that V-TRACE achieves reliable re-identification and real-time tracking with minimal overhead, while suppressing the propagation of malicious messages

## 2. Related Work

Vehicle tracking and identification have long been studied in the context of ITS [5-15], primarily with a focus on vision-based and sensor-based approaches. Early works relied on sensor-based techniques and signature cues such as license plate features or physical shape models. Subsequently, research shifted toward computer vision methods using roadside cameras and CCTV infrastructure, enabling vehicle re-identification across non-overlapping camera views [5]. These systems have been further enhanced by deep learning, which leverages convolutional neural networks (CNNs) and recurrent structures to extract robust appearance features from images captured by ground-based or unmanned aerial vehicle (UAV)-mounted cameras. More recent trends explore cross-domain vehicle re-identification [8,9], integrating data from heterogeneous sources to improve robustness across lighting, weather, and perspective variations. Despite their high accuracy in controlled settings, vision-based tracking and re-identification approaches suffer from practical limitations [10]: they require costly infrastructure deployment, are sensitive to occlusion and adverse weather, and lack privacy-preserving mechanisms. Moreover, these methods are not compatible with pseudonym-based privacy models in V2X environments, where vehicles periodically change their identifiers. Pseudonym rotation has been widely adopted in V2X networks to protect driver privacy, mitigating threats such as linkability attacks—where adversaries associate successive messages to re-identify a vehicle—and trajectory inference attacks, which reconstruct spatiotemporal traces to reveal a driver’s route or habits [11]. While effective for privacy preservation, these mechanisms also fragment identifiers across multiple pseudonyms, allowing misbehaving vehicles to conceal their tracks and complicating accountability for malicious actions. Several studies have explored message-based detection and tracking methods [12-15]. However, Masuda et al. [12] proposed a framework that matches camera-based perception with CAM/CPM messages to extract vehicle IDs, focusing on optimizing collective perception. Some works [13,14] primarily focused on anomaly detection using ML over broadcast messages and did not consider identifier changes. Because these approaches were not designed to track a specific vehicle across pseudonym rotations, they do not address the continuity problem that arises in misbehavior-targeted tracking scenarios like ours. Moreover, most of these systems rely solely on BSMs, which—are prone to global positioning system (GPS) noise, packet loss, and limited behavioral context, and they typically attempt to track all vehicles indiscriminately, leading to high computational overhead.

V-TRACE differs from prior models by adopting a selective tracking strategy that reduces computational overhead and scales effectively in dense traffic. In addition to BSMs, it leverages PVD for time-stamped behavioral snapshots, improving trajectory continuity and resilience to pseudonym changes. Operating fully within the V2X protocol suite, V-TRACE requires no visual sensors or learning-based identifiers and is readily compatible with real-world deployments.

## 3. Design of V-TRACE

V-TRACE is a system designed to enable persistent tracking of anomalous vehicles C-ITS, even in the presence of frequent pseudonym changes—a key feature of privacy-preserving V2X communication. The system comprises two tightly integrated components: a “tracking mechanism” for real-time observation of flagged entities, and an “identification mechanism” for re-associating new pseudonyms with previously tracked vehicles. V-TRACE operates within a standard-compliant C-ITS environment and leverages a periodic broadcast message, such as BSMs, defined in the SAE J2735 specification. Each vehicle periodically transmits BSMs containing its current speed, position, heading, and timestamp, which are received by nearby vehicles and RSUs to enable cooperative awareness and safety-critical applications. In addition to BSMs, V-TRACE selectively leverages PVD messages—which provide time-stamped historical records of a vehicle’s recent movement—for trajectory reconstruction and behavior correlation. This is particularly useful in scenarios where misbehavior is not immediately apparent or where identifier changes obscure behavioral patterns. One of the main challenges in vehicle tracking arises from the pseudonym rotation policy adopted in V2X systems, where temporary identifiers such as VIDs are periodically changed to protect driver privacy. This policy, enforced by security architectures like the Security Credential Management System (SCMS), ensures anonymity by rotating identifiers such as MAC addresses and digital certificates. While effective in preserving privacy, it makes subsequent messages from the same physical vehicle appear unlinkable over time, complicating efforts to maintain behavioral continuity. V-TRACE addresses this challenge by maintaining continuous observation of suspicious entities through its tracking module and re-establishing linkage after pseudonym changes via its identification module.

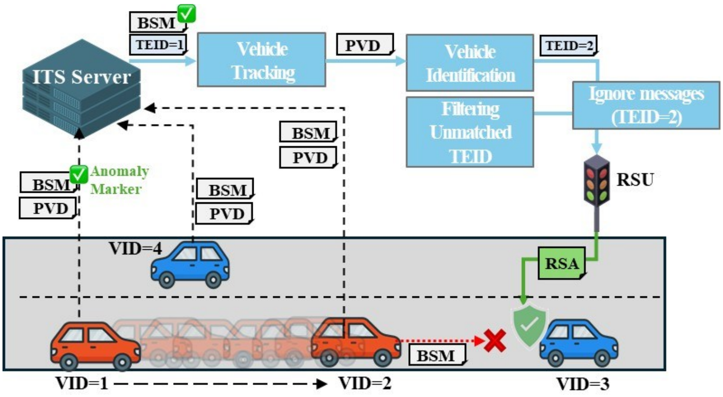


**Fig. 1.** System overview of V-TRACE.

## 3.1 Tracking Mechanism

The tracking mechanism is triggered upon reception of a BSM containing an Anomaly Marker, which signals that the transmitting vehicle has locally detected suspicious behavior—typically targeting itself—based on its internal misbehavior detection logic. We assume that such logic is already embedded within each vehicle, operating independently of the V-TRACE system. Once activated, the Anomaly Marker is automatically embedded into the vehicle's outgoing BSMs via an extension field, without modifying the standard BSM structure. Each vehicle may adopt its own detection policies—ranging from simple rule-based heuristics to advanced ML models—enabling flexible and deployment-specific integration. Upon receiving an Anomaly Marker, as illustrated in Fig. 1, the ITS center elevates the associated VID to a temporary entity identifier (TEID) and initiates the tracking process. From that point on, V-TRACE continuously collects and analyzes all BSMs associated with the TEID, enabling real-time monitoring of the vehicle's mobility patterns and behavioral anomalies.

$$\begin{aligned} new\_lat &= asin(sin(radian(\varphi)) * cos\, R\, /\, \delta + cos(radian(\varphi)) \\ &\quad * sin\, R\, /\, \delta * cos\, \theta) \\ new\_lon &= radian(\lambda) + atan2(\sin\, \theta * \sin\, R\, /\, \delta * \cos\, (radian(\varphi)), \cos\, R\, /\, \delta \\ &\quad - sin(radian(\varphi)) * sin(new\_lat)) \end{aligned} \tag{1}$$

To maintain tracking robustness under conditions such as network delay or packet loss, V-TRACE applies a motion model to predict the vehicle's next likely position. Using the Spherical Law of Cosines [16], the system computes an estimated location based on the vehicle's most recent heading, speed, and coordinates. In this formula, $new\_lat$ and $new\_lon$ denote the predicted latitude and longitude, $\varphi$ and $\lambda$ are the current latitude and longitude, $\theta$ is the heading, $\delta$ is the traveled distance derived from speed and prediction interval, and $R$ is the Earth's radius (6,371 km).

If no BSMs matching the TEID are received within a predefined timeout window, V-TRACE assumes that the vehicle has changed its identifier—a typical evasion strategy under privacy-preserving V2X protocols. A BSM is considered valid only if it falls within a 0.5-m spatial tolerance, reflecting typical global navigation satellite system (GNSS) errors; for example, the global average user range error (URE) was ≤0.643 m (95%). In such cases, the system transitions to the identification phase. To support this handover, V-TRACE maintains a sliding window of the target vehicle's recent trajectory, including time-stamped positions, speed, and heading. This trajectory log serves as a behavioral fingerprint and is used to compare against candidate VIDs appearing in subsequent BSMs. By leveraging this contextual history, V-TRACE improves the chances of correctly re-identifying the same physical entity, even under identity obfuscation. This seamless switch from tracking to identification enables persistent situational awareness against adversarial vehicles attempting to escape detection through simple identifier manipulation.

## 3.2 Identification Mechanism

After the tracking mechanism transitions to the identification phase, V-TRACE initiates a candidate search procedure to re-establish continuity under a new identifier. Fig. 2 illustrates this process. During this phase, BSMs previously marked as anomalous are retained and serve as anchors for evaluating behavioral consistency. To enhance re-identification accuracy, V-TRACE also collects PVD messages from nearby vehicles, which contain time-stamped snapshots of position, speed, and heading. These PVD records are grouped by VID and MAC address, allowing the system to construct per-vehicle behavior logs for comparison. This data collection is only triggered upon TEID timeout, thereby minimizing overhead while focusing on relevant re-identification targets.

The identification process consists of three sequential stages—Candidate Preselection, Trajectory Alignment Check, and Snapshot Continuity Check—each designed to progressively filter out irrelevant or implausible matches. In the Candidate Preselection stage, V-TRACE filters out VIDs that are already active TEIDs, then considers only candidates whose positions—derived from recent PVD snapshots—fall within a configurable distance from the predicted location of the missing vehicle. This prediction is computed from the last known state (position, heading, speed) using the Spherical Law of Cosines, while the Haversine formula [17] is used to calculate the great-circle distance between the predicted and observed positions. $\varphi_1$ and $\lambda_1$ represent the latitude and longitude of the predicted location, while $\varphi_2$ and $\lambda_2$ correspond to the latitude and longitude of the candidate location. $R$ denotes the 6,371 km. If the resulting distance falls within a spatial threshold, the candidate proceeds to the next step.

$$\begin{aligned} d = 2 * R * atan2(&\sqrt{}[sin^2((\varphi_2 - \varphi_1)/2) + \cos(\varphi_1) * \cos(\varphi_2) * sin^2((\lambda_2 - \lambda_1)/2)], \\ &\sqrt{}[1 - (sin^2((\varphi_2 - \varphi_1)/2) + cos(\varphi_1) * cos(\varphi_2) * sin^2((\lambda_2 - \lambda_1)/2))]) \end{aligned} \tag{2}$$

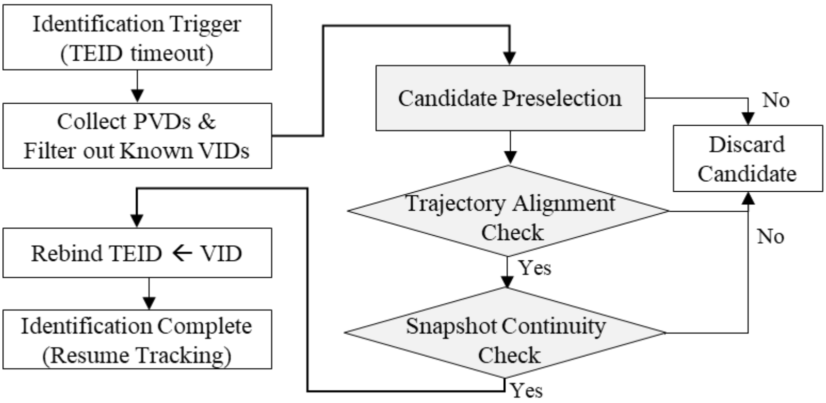

Identification Trigger (TEID timeout)
Collect PVDs & Filter out Known VIDs
Candidate Preselection
No
Discard Candidate
Trajectory Alignment Check
No
Yes
Rebind TEID ← VID
Identification Complete (Resume Tracking)
Snapshot Continuity Check
Yes

**Fig. 2.** Flow diagram of the vehicle re-identification process in V-TRACE.

The Trajectory Alignment Check stage examines whether the candidate's movement pattern is consistent with the expected trajectory of the original TEID. This involves verifying both displacement and directionality over multiple timestamps to ensure that the candidate is not only nearby but also plausibly continuing along the same path. Heading deviations and movement vectors are compared against the projected trajectory, and candidates falling outside acceptable distance or angular thresholds (e.g., ±15°) are filtered out. These values were chosen based on typical urban driving behavior, where vehicles within 100 m and ±15° are likely to follow similar paths. The distance threshold accounts for vehicle spacing and GPS noise, while the directional threshold tolerates minor lane changes. Finally, in the Snapshot Continuity Check stage, V-TRACE compares the candidate's historical PVD vector—comprised of time-stamped position, speed, and heading records—with the stored behavioral log of the missing vehicle. At each timestamp, the system computes spatial deviations using the Haversine formula and assesses whether the candidate maintains sufficient overlap with the original trajectory. If a majority of points fall within the noise-tolerant threshold, the candidate is accepted. Once a match is confirmed, the candidate's VID is promoted to a new TEID, and tracking resumes seamlessly under the updated identifier. V-TRACE immediately resumes message filtering and mitigation, suppressing anomalous activity from the re-identified node. This tightly coupled pipeline between re-identification and tracking ensures that malicious vehicles cannot escape accountability through simple identifier rotation, preserving situational awareness and enabling timely response.

# 4. Evaluation

To evaluate the performance of V-TRACE, we implemented a closed-loop V2X simulation environment using CANoe.Car2x [18], which supports SAE J2735 and IEEE 1609.2 standards. CANoe.Car2x is a simulation and testing tool for V2X communication, offering integrated support for protocol stacks, security, and HIL/SIL-based emulation of vehicle and RSUs. The evaluation was conducted with Program Version 15.4.35 (64-bit), DLL Version 22.10.20, and Driver Version 11.2.30 on a Windows-x86 configured RT Kernel. The simulation includes multiple vehicle nodes, an RSU node, and a central ITS server. To simulate anomaly-triggering conditions, a vehicle node is configured to intermittently transmit abnormal messages—such as location-speed mismatches—thereby activating the embedded misbehavior detector and generating an Anomaly Marker. All nodes operate within an isolated simulation environment, ensuring that message propagation, tracking, and re-identification are carried out under controlled and reproducible conditions. Vehicle and RSU nodes are configured to generate BSM and PVD messages following predefined mobility patterns and communication intervals.

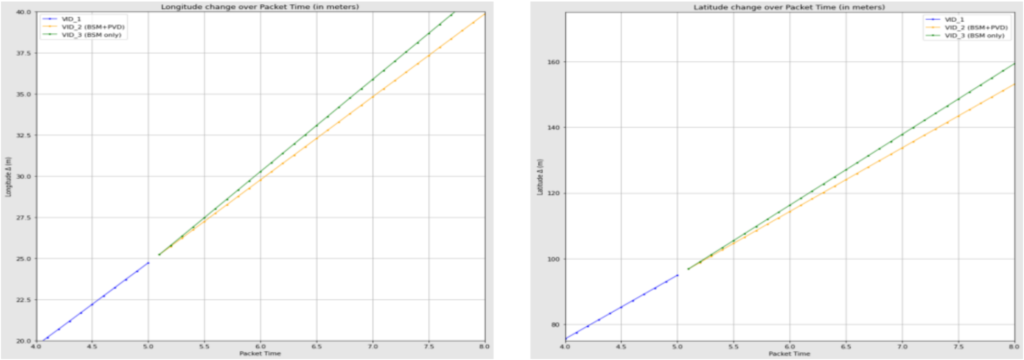
We evaluated the performance of V-TRACE by measuring execution time, memory usage, and spatial accuracy of both the tracking and identification mechanisms. Simulations were conducted with 1 to 20 vehicles over a 10-second window, with each mechanism invoked every 100 ms, consistent with the broadcast interval of standard BSM messages (10 Hz, per SAE J2735). This setup allowed us to assess how well V-TRACE maintains real-time responsiveness under increasing traffic density. The tracking mechanism showed near-linear growth in execution time as the number of vehicles increased. The overhead rose from 0.8 ms with a single vehicle to 22.5 ms with 20 vehicles—an increase of approximately 21 ms overall. This corresponds to an average per-vehicle increase of approximately 1.1 ms, or about 2.7% of the 100-ms time budget. Crucially, all executions remained well within the real-time constraint defined by the BSM transmission rate. These results confirm that V-TRACE's tracking process scales efficiently with minimal computational cost. The identification mechanism was evaluated under the same simulation settings. To trigger frequent re-identification events, all vehicle VIDs were randomized every 5 seconds, representing a more aggressive scenario than typical pseudonym change intervals. This stress-test setting was designed to evaluate the robustness of the identification mechanism under worst-case conditions while reflecting the dynamic nature of real-world traffic. Table 1 summarizes the measured execution time and latency under increasing vehicle density, alongside reference limits drawn from domain standards.

**Table 1.** Real-time performance of V-TRACE Tracking and Identification

| Number of vehicles | Tracking time (ms) | Identification latency (ms) |
|---|---|---|
| 2 | 0.8 | 2.0 |
| 5 | 3.5 | 40 |
| 10 | 6.5 | 95 |
| 15 | 13 | 160 |
| 20 | 22.5 | 210 |

To further examine scalability, we conducted an additional large-scale experiment with 100 vehicles. Specifically, 80 vehicles were processed through the tracking pipeline only, while 20 vehicles underwent both tracking and re-identification to emulate a more congested and complex environment. The choice of 100 vehicles reflects a realistic V2X communication range of 500 m per direction, as specified in the 5GAA test procedures and 3GPP TR 36.885/22.885. Under the assumptions of a straight four-lane road, a speed of 60 km/h, a 2-second safety gap, and a vehicle length of 4.7 m, the maximum number of vehicles simultaneously within the ±500 m range is approximately 105, making 100 a representative limit for large-scale testing. This test yielded worst-case latencies of approximately 145 ms for tracking and 907 ms for identification, confirming that V-TRACE remains stable even under extremely dense traffic conditions. In the same experiment, memory usage was continuously profiled using the memory-profile Python library to capture the peak additional memory required by each processing pipeline. The maximum overhead was measured at only 0.0898 MB for both tracking and re-identification. Such a small footprint is negligible compared to the memory budgets typically available on modern on-board units (OBUs) and embedded vehicular controllers, underscoring the suitability of V-TRACE for deployment in resource-constrained platforms without impacting concurrent in-vehicle functions.

Separately, we evaluated the accuracy of re-identification in a controlled experiment simulating frequent pseudonym changes. Each vehicle was assigned a constant but distinct speed (e.g., 70 km/h, 80 km/h), and VIDs were rotated every 5 seconds to represent a challenging re-identification scenario. We measured the rate of positional change (in m/s) along both latitude and longitude axes before and after the VID change. As shown in Fig. 3, both V-TRACE and the BSM-only configuration exhibited similar motion patterns prior to the identifier change. However, after rotation, V-TRACE preserved trajectory consistency (e.g., 19.3757 m/s in latitude), while the BSM-only baseline deviated significantly (e.g., 21.5267 m/s), indicating incorrect re-identification. These results confirm that V-TRACE's use of PVD snapshots significantly improves re-identification accuracy compared to BSM-only methods



(a) (b)

**Fig. 3.** Longitude (a) and latitude (b) trajectories: V-TRACE vs. BSM-only after re-identification.

# 5. Conclusion

In this work, we presented V-TRACE, a misbehavior-aware vehicle identification and tracking framework that persistently monitors suspicious vehicles despite frequent pseudonym changes. It triggers real-time tracking upon anomaly detection and maintains traceability through spatiotemporal analysis of BSM and PVD data, seamlessly handling pseudonym rotations via re-identification. Our evaluation shows that V-TRACE operates within real-time constraints and is suitable for deployment in resource-constrained C-ITS environments. By bridging misbehavior detection and persistent monitoring, V-TRACE offers a scalable, privacy-preserving solution for future V2X ecosystems. Future work will focus on large-scale field evaluations and integration with cooperative perception and edge-based C-ITS.

## Conflict of Interest

The authors declare that they have no competing interests.

## Funding

None.

## References

[1] A. Gorine and C. Agboile, “Securing V2X communication: DDoS attack implementation and mitigation via VEINS simulation,” *International Journal of Multidisciplinary Research and Publications*, vol. 7, no. 3, pp. 61–68, 2024.

[2] J. Whitefield, L. Chen, F. Kargl, A. Paverd, S. Schneider, H. Treharne, and S. Wesemeyer, “Formal analysis of V2X revocation protocols,” in *Security and Trust Management*. Cham, Switzerland: Springer, 2017, pp. 147-163. https://doi.org/10.1007/978-3-319-68063-7_10

[3] A. Kaiser, “White paper on misbehaviour detection and reporting to misbehaviour authority,” CAR 2 CAR Communication Consortium, 2021 [Online]. Available: https://hal.science/hal-04447506/.

[4] O. Ajibuwa, B. Hamdaoui, and A. A. Yavuz, “A survey on AI/ML-driven intrusion and misbehavior detection in networked autonomous systems: techniques, challenges and opportunities,” 2023 [Online]. Available: https://arxiv.org/abs/2305.05040.

[5] A. Holla, M. M. M. Pai, U. Verma, and R. M. Pai, “Vehicle re-identification and tracking: algorithmic approach, challenges and future directions,” *IEEE Open Journal of Intelligent Transportation Systems*, vol. 6, pp. 155-183, 2025. https://doi.org/10.1109/OJITS.2025.3538037

[6] S. D. Khan and H. Ullah, “A survey of advances in vision-based vehicle re-identification,” *Computer Vision and Image Understanding*, vol. 182, pp. 50-63, 2019. https://doi.org/10.1016/j.cviu.2019.03.001

[7] S. Abizada, “CNN based deep learning for vehicle re-identification,” in *12th World Conference “Intelligent System for Industrial Automation” (WCIS-2022)*. Cham, Switzerland: Springer, 2022, pp. 215-223. https://doi.org/10.1007/978-3-031-53488-1_26

[8] J. Peng, H. Wang, F. Xu, and X. Fu, “Cross domain knowledge learning with dual-branch adversarial network for vehicle re-identification,” *Neurocomputing*, vol. 401, pp. 133-144, 2020. https://doi.org/10.1016/j.neucom.2020.02.112

[9] K. Zhou, Y. Yang, Y. Qiao, and T. Xiang, “Domain generalization with mixstyle,” 2021 [Online]. Available: https://arxiv.org/abs/2104.02008.

[10] A. Ayala-Acevedo, A. Devgun, S. Zahir, and S. Askary, “Vehicle re-identification: pushing the limits of re-identification,” in *Proceedings of IEEE Conference on Computer Vision and Pattern Recognition (CVPR) Workshops*, Long Beach, CA, USA, 2019, pp. 291-296.

[11] L. Benarous, S. Zeadally, S. Boudjit, and A. Mellouk, “A review of pseudonym change strategies for location privacy preservation schemes in vehicular networks,” *ACM Computing Surveys*, vol. 57, no. 8, article no. 204, 2025. https://doi.org/10.1145/3718736

[12] H. Masuda, O. El Marai, M. Tsukada, T. Taleb, and H. Esaki, “Feature-based vehicle identification framework for optimization of collective perception messages in vehicular networks,” *IEEE Transactions on Vehicular Technology*, vol. 72, no. 2, pp. 2120-2129, 2023. https://doi.org/10.1109/TVT.2022.3211852

[13] A. Sharma and A. Jaekel, “Machine learning based misbehaviour detection in VANET using consecutive BSM approach,” *IEEE Open Journal of Vehicular Technology*, vol. 3, pp. 1-14, 2021. https://doi.org/10.1109/OJVT.2021.3138354

[14] A. Uprety, D. B. Rawat, and J. Li, “Privacy preserving misbehavior detection in IoV using federated machine learning,” in *Proceedings of 2021 IEEE 18th Annual Consumer Communications & Networking Conference (CCNC)*, Las Vegas, NV, USA, 2021, pp. 1-6. https://doi.org/10.1109/CCNC49032.2021.9369513

[15] M. Khajeh Hosseini, A. Talebpour, and S. Shakkottai, “Privacy risk of connected vehicles in relation to vehicle tracking when transmitting basic safety message type 1 data,” *Transportation Research Record*, vol. 2673, no. 12, pp. 636-643, 2019. https://doi.org/10.1177/0361198119875433

[16] I. Todhunter, *Spherical Trigonometry*. London, UK: Macmillan, 1886, pp. 29-31.

[17] N. R. Chopde and M. Nichat, “Landmark based shortest path detection by using A* and Haversine formula,” *International Journal of Innovative Research in Computer and Communication Engineering*, vol. 1, no. 2, pp. 298-302, 2013.

[18] Vector Informatik GmbH, “CANoe.Car2x,” c2025 [Online]. Available: https://www.vector.com/int/en/products/products-a-z/software/canoe/option-car2x/.

**Juntaek Lee** **https://orcid.org/0009-0004-3971-0816**

He received the B.S. degree in Information Security Engineering from Soonchunhyang University, South Korea, in 2019. He is currently a researcher with the Convergence Security Laboratory at the Korea Automotive Technology Institute. His research interests include embedded system security, and V2X communication security.

**Jiwoo Lee** **https://orcid.org/0009-0006-6858-0437**

He received the M.S. degree in Information and Communication Engineering from Incheon National University, South Korea, in 2023. He is currently a researcher with the Convergence Security Laboratory at the Korea Automotive Technology Institute. His research interests include spiking neural networks and security for AI.

**Chanmin Kim** **https://orcid.org/0009-0003-9384-1553**

He received the M.S. degree in Information Security from Soonchunhyang University, South Korea, in 2022. He works as a researcher at the Convergence Security Laboratory of the Korea Automotive Technology Institute. His areas of expertise include threat analysis and risk assessment (TARA) and V2X communication security.

**Jiwon Seo** **https://orcid.org/0000-0003-1848-750X**

She received the Ph.D. degree in Electrical and Computer Engineering from Seoul National University, South Korea, in 2023. She is currently an assistant professor with the Department of Cyber Security at Dankook University. Her research interests include system security and cybersecurity for cyber-physical systems.