2025 12th International Conference on Wireless Networks and Mobile Communications (WINCOM) | 979-8-3315-9878-5/25/$31.00 ©2025 IEEE | DOI: 10.1109/WINCOM65874.2025.11313388

Trust Verification in Connected Vehicles Using Unsupervised Variational Autoencoder

Ramzi Boutahala[†], Hacène Fouchal[†], Marwane Ayaida[‡†], and Shiwen Mao[§]
[†]Université de Reims Champagne Ardenne, Lab-I*, 51097 Reims, France
[‡]Univ. Polytechnique Hauts-de-France, CNRS, Univ. Lille, UMR 8520 - IEMN, F-59313 Valenciennes, France
[§]Department of Electrical and Computer Engineering, Auburn University, Auburn, AL 36849-5201 USA
Email: ramzi.boutahala@univ-reims.fr, hacene.fouchal@univ-reims.fr, marwane.ayaida@uphf.fr, smao@ieee.org

***Abstract*—Connected and Automated Mobility (CCAM) is undergoing a paradigm shift, with safety and efficiency increasingly dependent on connectivity. Cooperative Intelligent Transport Systems (C-ITS) support this transformation by enabling the exchange of Cooperative Awareness Messages (CAMs) between vehicles and roadside infrastructure. These messages, transmitted periodically at 1–10 Hz, must be digitally signed in compliance with ETSI standards using Pseudonym Certificates (PCs). However, this security process introduces a significant overhead, as the size of the security data can be up to three times larger than the CAM payload, thereby consuming a considerable portion of the communication channel bandwidth. In this paper we propose a new authentication scheme based on deep learning. Instead of exchanging signed CAMs every time, the vehicles will authenticate each other once to establish cluster-based trust relationships, and then they will exchange only unsigned CAMs during the cluster lifetime. To ensure security within the cluster, an unsupervised variational autoencoder analyzes vehicle behavior to detect anomalies and confirm that each vehicle remains the same entity originally authenticated. Through simulations using OMNeT++, SUMO, and Artery, our method achieved a 48.9% reduction in the volume of messages exchanged between vehicles, significantly decreasing communication channel overhead.**

***Index Terms*—Cooperative and Connected Automated Mobility (CCAM); Communication Overhead; Clustering; Cybersecurity; Digital Signature; Authentication; Variational Autoencoder; Deep Learning; Cooperative Intelligent Transport Systems (C-ITS).**

I. Introduction

With global vehicle numbers projected to exceed 2.5 billion by 2050 [1], issues related to road safety, congestion, and environmental pollution are increasingly critical. Each year, road accidents are responsible for nearly 1.35 million fatalities and millions of injuries [2]. To mitigate these challenges, Cooperative Intelligent Transportation Systems (C-ITS) have been introduced, aiming to enhance road safety and mobility efficiency. C-ITS relies on vehicle-to-everything (V2X) communications to enable interaction between vehicles, drivers, and roadside units (RSUs). Within this framework, vehicles exchange standardized message types. According to the European Telecommunications Standards Institute (ETSI), C-ITS communication is organized through a layered protocol that includes Cooperative Awareness Messages (CAMs) and Decentralized Environmental Notification Messages (DENMs), standardized in ETSI EN 302 637-2 [3] and ETSI EN 302 637-3 [4]. Message dissemination is achieved via the GeoNetworking protocol (ETSI EN 302 636-4-1) [5], which supports both direct (single-hop) and relayed (multi-hop) geographic communication. The ITS-G5 framework, which functions over the 5 GHz band [6], supports periodic CAM transmission with frequencies varying from 1 to 10 Hz. According to ETSI TS 103 097 [7], message security—covering privacy, authentication, and integrity—is ensured via pseudonym certificates issued and controlled under a PKI system. In this study, we focus on the CAM standard. CAMs are periodic messages that allow vehicles to share status information, such as GPS coordinates, speed, and heading. CAMs contain payload content along with a pseudonym-based certificate and a signature. They are transmitted regularly by vehicles to neighboring nodes at intervals corresponding to 1–10 Hz. To ensure security, CAMs are signed with the pseudonym certificate. Attaching both a signature and a certificate to each CAM introduces considerable overhead, leading to higher channel utilization and bandwidth demand. In fact, the additional security data (300 bytes) enlarges the payload nearly threefold compared to the original CAM size of 100 bytes.

979-8-3315-9878-5/25/$31.00 © 2025 IEEE

This study introduces an innovative method that combines deep learning with trust clustering to minimize the cost generated by continuous CAM authentication. Our method enables nearby vehicles to authenticate once and establish mutual trust, forming a trust cluster valid for a defined period. During this interval, vehicles stop sending signed CAMs and instead send only unsigned CAMs, significantly reducing the communication load. To ensure message reliability during this trust period, we integrate an unsupervised deep learning model—specifically, an LSTM based variational autoencoder (VAE) to monitor the behavior of neighboring vehicles and detect any inconsistencies that could indicate compromised vehicles. The proposed approach was assessed through simulations conducted with OMNeT++, SUMO, and Artery under various scenarios on the A4 highway (Paris–Reims, France). The structure of the paper is as follows: Section II discusses existing literature, Section III presents the developed architecture, Section IV reports the simulation environment together with the results, and Section V summarizes the conclusions.

II. Related Work

The following section reviews significant contributions in the field of security mechanisms for connected vehicles. The authors in [8] introduced a trust-based mechanism in which cluster-heads are chosen according to their reliability scores. The approach secures communication by applying public–private key encryption, compelling each sender to sign and encrypt its messages. While effective in ensuring integrity, the scheme suffers from high latency in collaborative environments where fast, and sometimes plaintext, exchanges are necessary.

The study in [9] proposed two privacy-preserving cryptographic solutions. The first relies on zone-based encryption combined with anonymous authentication to prevent eavesdropping and restrict communication to authorized vehicles. Its main weakness is the 224-byte overhead added to each message, which increases bandwidth usage and delays transmission. The second scheme, better adapted to vehicular environments, allows nodes to distribute keys among themselves. The use of compact group signatures reduces demand on network bandwidth and memory resources, while maintaining robust privacy. However, the revocation procedure remains complex during attacks and does not fully provide non-repudiation.

In [10], the authors proposed a privacy-preserving scheme built on digital signatures. To address the burden of certificate handling, the network is divided into multiple domains. The design also integrates a Hash Message Authentication Code (HMAC) to optimize the management of certificate revocation lists. This addition enhances the efficiency of integrity verification and reduces the number of rejected messages, thereby decreasing both computational load and communication overhead.

The authors in [11] presented a clustering-based authentication framework intended to overcome the drawbacks of conventional cryptographic solutions in highly dynamic VANET environments. The method builds stable groups of vehicles to preserve trust across the network and designates cluster heads from nodes considered the most reliable. Additional mechanisms were suggested to detect malicious participants, while a few vehicles were tasked with monitoring the behavior of their neighbors. Although this strategy leverages signatures and asymmetric cryptography to enhance protection, it still suffers from limitations similar to those identified in [8].

In [12], a decentralized authentication method was proposed, where message signatures replace the need for a central authority. This design reduces verification time and communication overhead. However, its main weakness lies in the revocation process: if a vehicle is compromised, every pseudonym linked to it needs to be revoked together, which rapidly enlarges the revocation list.

The work in [14] proposed an identity-based authentication approach that also incorporates ring signatures, but its efficiency is limited due to high computational costs during signing and verification.

In a related study, [15] suggested a variant that couples ring signatures with bilinear pairings and adds batch verification to lower the computational load. Despite these improvements, the scheme remains inefficient for single signature operations.

Similarly, [16] introduced a certificateless aggregate authentication method. This construction combines ring signatures with bilinear pairings on elliptic curves to enhance privacy and reduce verification delays. Overall, these contributions share the objective of minimizing resource consumption through lightweight authentication, but none explores adaptive or on-demand activation of security services as a means of conserving bandwidth.

The problem of anomaly detection has recently drawn significant focus, with machine learning providing the means to identify complex abnormal patterns. A considerable body of research highlights the use of LSTM architectures for detecting irregularities in multiple scenarios. The study in [17] introduced a cluster-driven framework that deploys a small fraction of nodes as monitoring agents, strategically placed within the network. Operating in promiscuous mode, these agents use statistical evaluation to reveal irregularities in routing misbehavior. In [18], a recurrent variational autoencoder was developed to capture respiratory dynamics. By calculating the KL divergence between original and reconstructed signals, the framework identified apnea occurrences through signal amplitude fluctuations combined with threshold-based detection.

III. Proposed Methodology

The frequent transmission of signed CAMs, each including a certificate and a signature, introduces significant communication overhead and increases channel load. The security information alone can triple the size of a standard CAM, which typically has a payload of around 100 bytes. To overcome this limitation, we introduce a trust-based strategy whereby vehicles, after a single authentication step, may broadcast unsigned CAMs for the duration of a predefined trust window. The details of this mechanism, which enables one-time authentication followed by lightweight message exchange, are presented in the following, along with the overall procedure of our approach.

A. Cluster Dynamics in Trust-Based Approach

1) Cluster Construction: In the proposed method, nearby vehicles form a cluster, assuming that all are within mutual communication range. To initiate this process, vehicles synchronize to verify their eligibility for cluster formation. If no new neighbor information is received within a predefined time period, the vehicles proceed to elect a Cluster Head (CH). Each vehicle then calculates the cluster's geographic center using latitude and longitude data extracted from neighboring vehicles' CAM messages (as illustrated in Figure 1). This involves converting the geographic coordinates into Cartesian coordinates (X_i, Y_i, Z_i), averaging these values $(X_{\text{mean}}, Y_{\text{mean}}, Z_{\text{mean}})$, and transforming the averages back into geographic coordinates $(\text{Lon}_G, \text{Lat}_G)$ to define the cluster center. Once selected, the Cluster Head (CH) initiates authentication with neighboring vehicles by sending a certificate request along with its List of Neighboring Vehicles (LNV).

In response, the vehicles send back their own certificates and LNVs, allowing each vehicle to verify the CH's identity and to check for consistency across neighbor lists. If verification succeeds, the vehicles temporarily form a cluster. If verification fails, vehicles pause briefly before retrying the process. This authentication and cluster formation cycle repeats periodically.

2) Cluster Update:: Once a cluster is formed, vehicles trust each other and communicate using unsigned CAM messages. To ensure security and guard against malicious alterations, every node continuously observes the behavior of its neighbors with the help of a deep learning–based anomaly detection model, explained later in this section. If an anomaly is detected, the vehicle sends a certificate request to re-authenticate the suspicious node. When a new vehicle joins the cluster, the first vehicle that detects it initiates a certificate request. Conversely, if a vehicle leaves the cluster, it is removed from the list of authenticated neighbors.

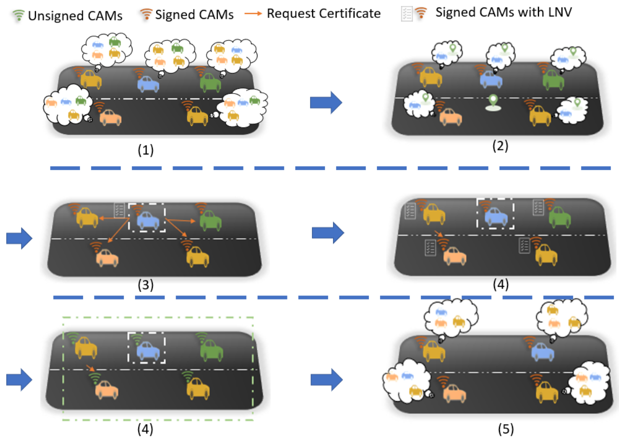

Fig. 1. The procedure for cluster construction.

B. Trust Management

In this section, we describe how our approach maintains a high level of security, while reducing the security overhead. The dynamics of a cluster is related to managing the trust of each vehicle towards all other cluster members. During this phase, each vehicle frequently checks the behaviors and the trajectories of its neighbors. To do so, each vehicle uses the content of the CAMs that are received from its neighbors as parameters to detect unsound CAMs. The key idea is that a vehicle continues to trust the sender and accepts its unsigned CAMs as long as the sender's behavior remains consistent. In order to assess the consistency of a vehicle's behavior, a detection system is proposed. The model functions as an approximation tool for complex estimations that are otherwise difficult to compute directly. It is trained on calibrated data to estimate relevant parameters and improve accuracy. Building on this, we propose an *unsupervised deep learning strategy* that tracks changes in the behavior of surrounding vehicles. When the observed deviation goes beyond a set threshold, the system flags the sender as potentially compromised and requests certificate renewal for validation. The details of this mechanism are outlined below.

1) Background of Variational Autoencoder: An autoencoder is defined as an unsupervised neural model aimed at extracting compact encoding–decoding patterns from data [20]. A Variational Autoencoder (VAE) is a generative probabilistic framework that integrates Bayesian inference with the autoencoder structure [23]. It establishes a relation between the observed input x, latent variables z, and model parameters θ. The prior distribution of z is noted as $p(z)$, and the likelihood of observing x given z is written as $p_\theta(x|z)$. Consequently, the marginal distribution of x is expressed as:

$$p(x) = \int p_\theta(x|z)\, p(z)\, dz. \tag{1}$$

Since this integral is usually intractable, the VAE introduces an approximation of the posterior distribution, denoted $q_\phi(z|x)$. In this formulation, the encoder with parameters ϕ estimates $q_\phi(z|x)$, whereas the decoder with parameters θ reconstructs x from z. Applying Jensen's inequality shows that optimizing this approximate posterior corresponds to maximizing a tractable lower bound of the log-likelihood, known as the *Evidence Lower Bound (ELBO)* [24]:

$$\mathcal{L} = -D_{KL}(q_\phi(z|x)\,\|\,p(z)) + \mathbb{E}_{z\sim q_\phi(z|x)}\big[\log p_\theta(x|z)\big]. \tag{2}$$

Here, D_{KL} denotes the Kullback–Leibler divergence, which encourages the latent distribution to remain close to the prior. To make training feasible with gradient descent, the *reparameterization trick* is applied:

$$z = \mu_\phi(x) + \sigma_\phi(x)\varepsilon, \quad \varepsilon \sim \mathcal{N}(0, 1). \tag{3}$$

Under Gaussian assumptions, the ELBO can be expanded as:

$$\begin{aligned}\mathcal{L} \approx 0.5 \sum_j &\Big(1 + \log \sigma_j^2(x) - \mu_j^2(x) - \sigma_j^2(x)\Big)\\ &+ \frac{1}{M} \sum_l \log p_\theta(x|z_l).\end{aligned} \tag{4}$$

where M is the number of Monte Carlo samples from the latent space and J is the latent dimensionality. The final objective combines a reconstruction error with a regularization term, leading to the following loss:

$$\text{Loss} = \text{MSE} + \text{KL}, \tag{5}$$

where the reconstruction term is measured by the mean squared error (MSE):

$$\text{MSE} = \frac{1}{N} \sum (x - x')^2, \tag{6}$$

with x denoting the original input, x' the reconstruction, and N the total number of samples.

2) Offline Variational Autoencoder Training Phase: The variational autoencoder operates under an unsupervised learning paradigm, meaning that no labeled datasets are required for distinguishing between normal and abnormal driving patterns. In the context of C-ITS, we generated a dataset of 40 million CAM messages generated by simulating one thousand vehicles driving on the A4 highway between Reims and Paris in France. Each vehicle sends a CAM every 100 ms. We then pre-processed these CAMs to extract two key parameters that characterize vehicle behavior. To do so, we calculated the distance between each pair of consecutive CAMs sent by the same vehicle, using Vincenty's formula to compute the three-dimensional geodesic distance based on latitude, longitude, and altitude. The resulting dataset includes the following input variables: heading and distance. The dataset was segmented into groups of 10 consecutive CAMs, corresponding to an interval of one second. These segments were provided as input to a long short-term memory (LSTM) architecture. The encoder LSTM transformed each sequence into feature vectors, which were then mapped onto the mean $\mu_\phi(x)$ and variance $\sigma^2_\phi(x)$ using separate linear layers. From this representation, a latent variable z was sampled and passed through a decoder LSTM tasked with reconstructing the original sequence. Model training was guided by a composite loss that integrates the mean squared error (MSE) with the Kullback–Leibler (KL) divergence, encouraging the reconstructions to remain consistent with the input data. Once the model was trained, the limit for anomaly detection was set by identifying the highest mean absolute error (MAE) obtained from the training data. During evaluation, whenever the reconstruction error of a given time segment surpasses this limit, the corresponding CAM sequence is marked as anomalous; otherwise, it is treated as valid.

3) Processing Phase: During dynamic clustering, vehicles periodically activate the VAE within a reserved time slot to evaluate the CAM messages exchanged with neighbors, as depicted in Fig. 2. Each vehicle processes the most recent 10 CAMs obtained from surrounding nodes. The pre-processing is identical to what was done during training. Afterward, the VAE reconstructs the time-window input and compares the reconstruction error against the threshold defined in the training phase. If the error for a given sample surpasses this threshold, that message is classified as inconsistent. If an anomaly is detected, the vehicle issues a certificate request to the suspected neighbor. In the absence of a response, it halts the exchange of unsigned CAMs and withdraws from the cluster.

IV. Performance Evaluation

To evaluate the proposed approach in a simulation environment that closely reflects real-world conditions, we used several simulators and frameworks. First, we employed the OMNeT++ network simulator [26], which is developed as a set of independent modules that can be combined to form complex systems. OMNeT++ is designed to model communication systems, networks, multiprocessors, and other distributed systems. It is based on the C++ programming language and uses NED (Network Description Language) to define network topology. The simulator relies on discrete event scheduling rather than continuous-time simulation. We also used the Artery framework [25], Artery provides support for V2X communications and extends the simulator with modular and event-driven capabilities. Each simulated vehicle was equipped with the full C-ITS protocol stack, including security mechanisms. The exchange of messages was performed through the IEEE 802.11p physical layer as provided by the VEINS framework. Traffic mobility was simulated using SUMO [27], which generates realistic vehicle movements and traffic flows. Artery was coupled with SUMO to achieve synchronization between mobility and communication in real time. This setup enabled a quantitative assessment of the effectiveness of the proposed scheme in reducing communication overhead within C-ITS. To assess the efficiency of the proposed scheme, simulations were conducted under realistic traffic conditions. The A4 highway (Paris-Reims, France), was used as the reference environment. The road infrastructure was reconstructed from OpenStreetMap data and imported into SUMO to emulate actual driving conditions. Traffic density was varied by generating scenarios with 10, 20, and 30 vehicles traveling unidirectionally from Reims toward Paris. Vehicle mobility included controlled randomness, introduced through a Gaussian noise parameter ($\sigma = 0.5$), to reproduce fluctuations in speed and trajectory observed in real traffic. During the simulation, each vehicle checks the last 10 CAMs received from its neighbors every 5 seconds, using extracted heading and position data for anomaly detection. Figure 3 shows the cumulative number

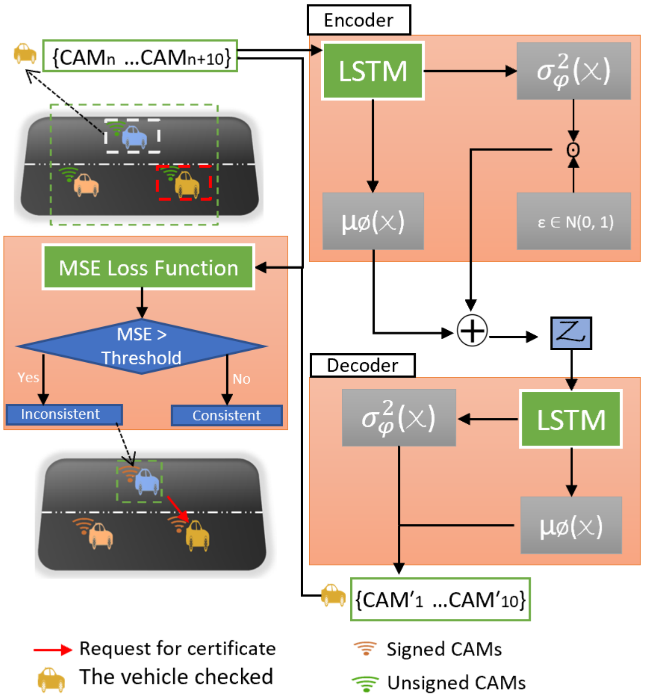

Fig. 2. Overview of the proposed VAE-driven method for detecting inconsistencies.

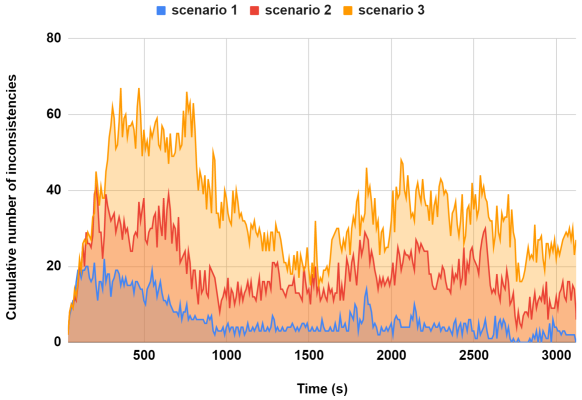

Fig. 3. The cumulative number of inconsistencies every 10s in the three scenarios.

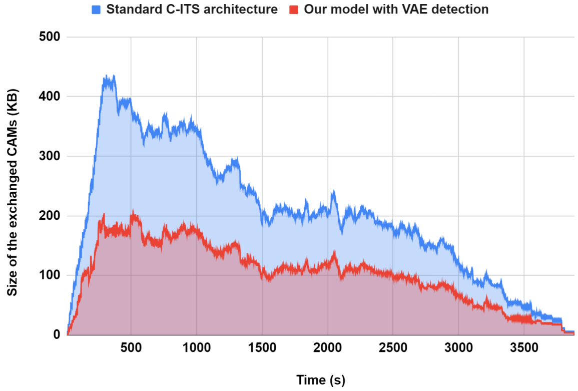

Fig. 4. Volume of exchanged data in Scenario 3, measured each second.

TABLE I
THE PERCENTAGE OF INCONSISTENCIES DETECTED BY THE VEHICLES AND THE NUMBER OF INCONSISTENT EVENTS COMPARED TO THE NORMAL CAM

2*S	Real Anomaly		Anomaly Detected		Sound Cams	
	Number	%	Number	%	Number	%
1	1940	0.41%	2187	0.46%	470227	%99.59
2	6199	0.42%	7741	0.51%	1495743	%99.58
3	12018	0.45%	15531	0.58%	2662441	%99.55

of inconsistent behaviors detected by vehicles based on CAM messages received from neighbors, cumulated every 10 seconds for the three tested scenarios. As illustrated, the number of detected inconsistencies rises proportionally with vehicle density. A larger fleet leads to more simultaneous detections of the same anomaly by neighboring vehicles, thereby amplifying the anomaly count. In the initial simulation phase (0–1000 s), there is a noticeable peak in inconsistencies across all scenarios. This behavior occurs due to the initial proximity and frequent exchanges among vehicles, resulting in multiple simultaneous detections by neighboring vehicles. During the intermediate phase (1000–1800 s), the number of detections decreases significantly, indicating fewer vehicle interactions as the distances between vehicles increase, limiting the formation of clusters and thus reducing anomaly detection activity. In the final simulation phase (1800–3000 s), the number of detected inconsistencies increases again, particularly in scenario 3 (30 vehicles). This is due to more stable vehicle trajectories, resulting in frequent cluster formations and consequently activating the anomaly detection mechanism more regularly.

Table I presents the percentage of inconsistencies detected by the vehicles and the number of inconsistent events relative to the total CAM messages exchanged during the simulation. In all scenarios, more than 99.5% of the CAM messages were consistent. Our model detected only a small fraction of anomalies in vehicle behavior, demonstrating its effectiveness in identifying real-time inconsistencies in the CAM data. The VAE recorded significantly lower rates of detected inconsistencies—0.46%, 0.51%, and 0.58% in the three scenarios—showing how our deep learning-based approach accurately distinguishes normal data and minimizes false detections.

In scenario 3, the evaluation focused on communication overhead by assigning standard payload sizes defined in the C-ITS specifications: 300 bytes for authenticated CAMs and 100 bytes for unauthenticated ones. Based on these values, the total data volume exchanged over the course of the simulation was derived, allowing a comparison between transmissions with signed and unsigned messages. The temporal evolution of transmitted data is illustrated in Figure 4, which highlights a clear distinction between the standard C-ITS protocol and the proposed variational framework. Unlike the baseline, where all CAMs are authenticated, our strategy reduces the amount of information exchanged by transmitting unsigned CAMs once trust is established. This substitution translates into a measurable gain, with message sizes reduced by 48.9%. Such a reduction directly impacts network reliability, since the communication channel is less prone to congestion. The underlying reason for this efficiency lies in the trust-cluster paradigm: vehicles avoid redundant signatures while anomaly detection is ensured by the VAE-based monitoring process.

V. CONCLUSIONS

In this study, we introduced a cluster-based trust strategy combined with variational autoencoders to address communication efficiency in C-ITS. Instead of authenticating every transmitted message, vehicles authenticate once and can subsequently exchange unsigned CAMs within a controlled trust window. This significantly reduces the size of the CAMs, alleviates channel congestion, and improves the scalability of the system. Through simulations, our method achieved a 48.9% reduction in message load compared to the conventional C-ITS standard, while preserving reliability in anomaly detection. The proposed framework therefore balances security and efficiency by leveraging unsupervised learning for real-time monitoring of vehicle behavior. Future work will focus on strengthening the resilience of this approach against diverse cyber threats and extending its validation to more heterogeneous traffic environments.

Acknowledgment

This work was supported in part by EC Grant No. 2018-FR-TM-0097-S from the INEA Agency for the InDiD project. The statements made herein are solely the responsibility of the authors. S. Mao's work is supported by the NSF Grant CNS-2415208.

References

[1] International Energy Agency, "How Many Cars Will Be on the Planet in the Future?" [online] Available: http://www.iea.org/aboutus/faqs/transport/ (accessed on Nov. 15, 2022)

[2] World Health Organization (WHO), "Global Status Report on Road Safety 2013," *WHO Technical Report*, Geneva, Switzerland, 2013.

[3] ETSI, T. (2011). Intelligent transport systems (its); vehicular communications; basic set of applications; part 2: Specification of cooperative awareness basic service. Draft ETSI TS, 20(2011), 448-51

[4] ETSI, E. (2014). 302 637–3; Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Application; Part 3: Specifications of Decentralized Environmental Notification Basic Service. European Standard. ETSI.

[5] ETSI, E. (2020). 302 636-4-1 V1. 4.1; Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 4: Geographical Addressing and Forwarding for Point-to-Point and Point-to-Multipoint Communications; Sub-Part 1: Media-Independent Functionality. European Telecommunications Standards Institute: Sophia Antipolis, France.

[6] ETSI, E. (2019). ETSI EN 302 663 v. 1.2. 0-Intelligent Transport Systems (ITS); Access layer specification for Intelligent Transport Systems operating in the 5 GHz frequency band. ETSI, May.

[7] ETSI, T. (2017). 103 097 v1. 3.1-Intelligent Transport Systems (ITS); Security; Security header and certificate formats. Technical specification, European Telecommunications Standards Institute..

[8] R. Sugumar, A. Rengarajan, and C. Jayakumar, "Trust based authentication technique for cluster based vehicular ad hoc networks (VANET)," *Springer Wireless Networks*, vol.24, pp.373–382, Feb. 2018.

[9] J. Camenisch, M. Drijvers, A. Lehmann, G. Neven, and P. Towa, "Zone encryption with anonymous authentication for V2V communication," in *Proc. 2020 IEEE European Symposium on Security and Privacy (EuroS&P)*, Virtual Conference, Sept. 2020, pp.405–424.

[10] X. Zhu, S. Jiang, L. Wang, and H. Li, "Efficient privacy-preserving authentication for vehicular ad hoc networks," *IEEE Transactions on Vehicular Technology*, vol.63, no.2, pp.907–919, Feb. 2013.

[11] F. Mirsadeghi, M. K. Rafsanjani, and B. B. Gupta, "A trust infrastructure based authentication method for clustered vehicular ad hoc networks," *Springer Peer-to-Peer Networking and Applications*, vol.14, pp.2537–2553, July 2021.

[12] X. Lin and X. Li, "Achieving efficient cooperative message authentication in vehicular ad hoc networks," *IEEE Transactions on Vehicular Technology*, vol.62, no.7, pp.3339–3348, Sept. 2013.

[13] The European Telecommunications Standards Institute (ETSI), "E.N. 302 637-2 v1. 3.1-intelligent transport systems (its); Vehicular communications; Basic set of applications; part 2: Specification of cooperative awareness basic service," European Standard, Sept. 2014.

[14] J. Li, Y. Liu, Z. Zhang, B. Li, H, Liu, and J. Cheng, "Efficient ID-based message authentication with enhanced privacy in wireless ad-hoc networks," in *Proc. 2018 International Conference on Computing, Networking and Communications (ICNC)*, Maui, HI, Mar. 2018, pp.322–326.

[15] S. Bouakkaz and F. Semchedine, "New efficient certificateless scheme-based conditional privacy preservation authentication for applications in VANET," *Elsevier Vehicular Communications*, vol.34, pp.100414, Apr. 2022,

[16] F. Liu and Q. Wang, "IBRS: An efficient identity-based batch verification scheme for VANETs based on ring signature," in *Proc. 2019 IEEE Vehicular Networking Conference (VNC)*, Los Angeles, CA, Dec. 2019, pp.1–8.

[17] Y. Huang and W. Lee, "A cooperative intrusion detection system for ad hoc networks," in *Proc. 1st ACM workshop on Security of Ad Hoc and Sensor Networks*, Fairfax, VA, Oct. 2003, pp.135–147.

[18] C. Yang, X. Wang, and S. Mao, "Unsupervised detection of apnea using commodity RFID tags with a recurrent variational autoencoder," *IEEE Access Journal*, vol.7, pp.67526–67538, May 2019.

[19] H.D. Nguyen, K.P. Tran, S. Thomassey, and M. Hamad, "Forecasting and anomaly detection approaches using LSTM and LSTM autoencoder techniques with the applications in supply chain management," *Elsevier International Journal of Information Management*, vol.57, pp.102282, Apr. 2021.

[20] D.P. Kingma, and M. Welling, "Auto-encoding variational bayes," arXiv:1312.6114, May 2014. [Online]. Available: https://arxiv.org/abs/1312.6114.

[21] R. Boutahala, M. Ayaida, and H. Fouchal, "Reducing security overhead in the context of connected Vehicles," in *Proc. IEEE GLOBECOM 2022*, Rio de Janeiro, Brazil, Dec. 2022, pp. 1–6.

[22] R. Boutahala, H. Fouchal, and M. Ayaida, "An efficient approach to reduce the security messages overload on C-ITS," in *Proc. IEEE ICC 2022*, Seoul, South Korea, May 2022, pp.1500–1505.

[23] Y. Guo, W. Liao, Q. Wang, et al., "Multidimensional time series anomaly detection: A GRU-based Gaussian mixture variational autoencoder approach," in *Proc. Asian Conference on Machine Learning*, Beijing, China, Nov. 2018, pp.97–112.

[24] D.P. Kingma and M. Welling, "Auto-encoding variational bayes," *arXiv preprint arXiv:1312.6114*, Dec. 2013, [online] Available: https://arxiv.org/abs/1312.6114.

[25] R. Riebl, H. Günther, C. Facchi, and L. Wolf, "Artery: Extending veins for VANET applications," in *Proc. 2015 International Conference on Models and Technologies for Intelligent Transportation Systems* (MT-ITS), Budapest, Hungary, June 2015, pp.450–456.

[26] A. Varga, "The omnet++ discrete event simulation system," in *Proc. the European Simulation Multiconference*, Prague, Czech Republic, June 2001, pp.319–324, 2001.

[27] D. Krajzewicz, G. Hertkorn, C. Rössel, and P. Wagner, "Sumo (simulation of urban mobility) - An open-source traffic simulation," in *Proc. 4th Middle East Symposium on Simulation and Modelling*, Dubai, UAE, Sept. 2002, pp.183–187.