Light and Efficient Authentication Mechanism for Connected Vehicles using Unsupervised Detection

†Ramzi Boutahala, †Hacène Fouchal, ‡†Marwane Ayaida, and ††Shiwen Mao
† Université de Reims Champagne Ardenne, CReSTIC EA 3804, 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
ramzi.boutahala@univ-reims.fr, hacene.fouchal@univ-reims.fr, marwane.ayaida@uphf.fr, smao@ieee.org

***Abstract*—Cooperative Intelligent Transport Systems (C-ITS) are very important in our daily lives. They ensure road safety through the exchange of data between vehicles and road side units (RSU). Due to the sensitivity of the exchanged data between different entities, C-ITS systems are vulnerable to Cyber-attacks, they require high protection. In order to guarantee the integrity and the authentication of the exchanged messages, the European Telecommunications Standards Institute (ETSI), has specified specific procedures to manage certificates and signatures of all sent messages. Each vehicle periodically sends signed CAMs. Then, the integration of the signature and certificate in each transmitted CAM has a considerable impact on the communication channel load and bandwidth. In this study, we propose a new lightweight authentication mechanism which considers that vehicles on road are composed of a set of clusters having different sizes. The clusters are dynamic and change continuously. In each cluster, we implement some procedures in order to reach a trusted environment where vehicles communicate with unsigned messages when they trust their neighbours. When the trust is not guaranteed, vehicles switch to the standard communication until trust recovery. In order to reach the trust, each vehicle computes its own prediction of neighbours behavior. based on trajectory, speed. The prediction is performed using an auto-encoder running the LTSM algorithm. We have implemented this mechanisms on the OMNET++ environment and we have concluded that our mechanisms reduce the overhead generated by the authentication algorithms around 34% of the size of exchanged messages.**

***Index Terms*—Clustering, Security, Privacy, Signature, Authentication.**

I. Introduction

In today's world, the number of vehicles continues to grow. There will be more than two billion vehicles on our roads by 2050 [1], resulting in more accidents, traffic jams and environmental pollution. According to the World Health Organization (WHO), the total number of deaths due to road accidents remains unacceptably high at about 1.24 million per year [2]. Cooperative Intelligent Transportation Systems (C-ITS) have the potential to address these issues, as they enable real-time connections between vehicles and infrastructure to alert the driver with the disruptive events. They also provide new services that improve driving through cooperation between road infrastructure, drivers, and vehicles. However, these services use messages to exchange road information (e.g. traffic jams, accidents, etc.), which yields in a vulnerability to various risks of cyber attacks. In order to protect the system, it is very important to ensure the integrity of these information and to authenticate the origin of the exchanged messages.

In Europe, a C-ITS protocol was introduced by the European Telecommunications Standards Institute, under the name ETSI ITS G5. This protocol defines the policies for managing security certificates, the format and fields of the secure CAMs (Cooperative Awareness Messages), as well as the signature and encryption algorithms. According to the ETSI standard, each vehicle must sign its CAMs using these certificates. However, the integration of the signature and the certificate in each sent CAM represents a high impact on the communication channel load and bandwidth.

In this paper, we propose a new lightweight concept for security in C-ITS that aims to reduce the size of the bandwidth consumed by the signatures and the certificates of the CAMs exchanged between vehicles. This is advantageous because it avoids the risk of overloading the communication channel, reduces CAM latency and enhances the security overload. For this issue, we use the concept of clustering to establish trust between neighbors, which allows the vehicles to send unsigned CAMs. We have implemented our architecture on the Artery framework, using the OMNET++ network simulator and the SUMO road traffic simulator, in order to demonstrate the efficiency of our proposal. The paper is structured as follows. Section 2 introduces the related works. Section 3 describes the proposed architecture within this study. Section 4 outlines the simulation tests, which includes the simulation settings and the result analysis, before concluding this work in Section 5.

II. Related work

This section presents some important works about the security for connected vehicles.

Authors of [3] proposed an authentication protocols for connected vehicles. This protocol uses the signature messages for the authentication without needing a central authority. The proposed protocol reduces the authentication time and overhead. However, it will increase rapidly the size of the revocation list in case of an attack since each vehicle uses

978-1-5386-7462-8/23/$31.00 ©2023 IEEE

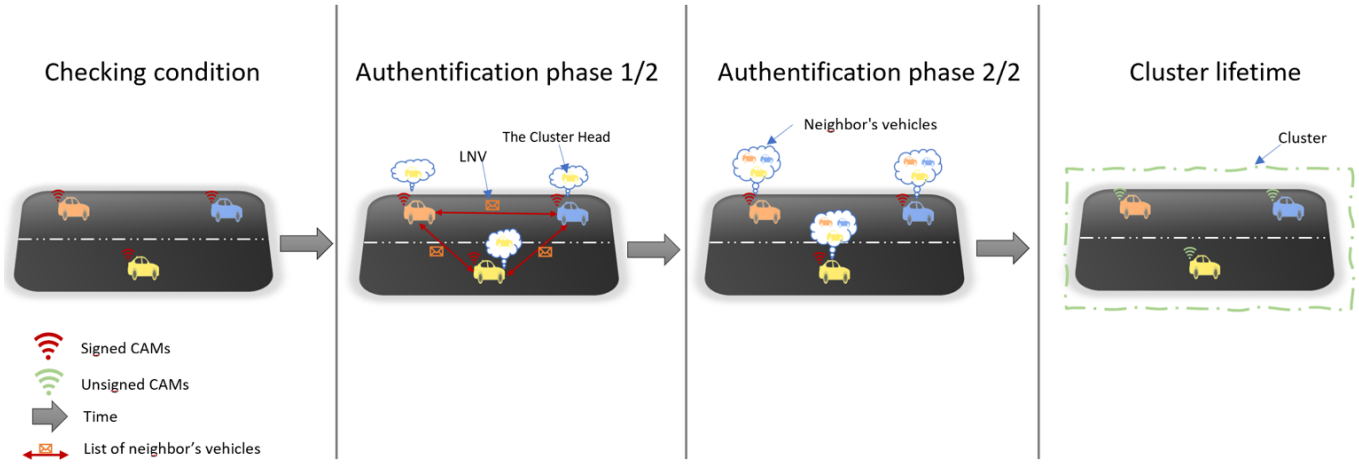

Fig. 1. Cluster construction steps

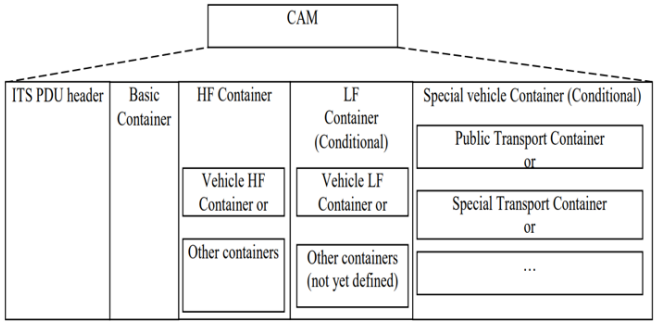

Fig. 2. General structure of a CAM [7]

multiple pseudonyms that need to be revoked all if the vehicle is corrupted.

The work in [4] designed another authentication technique, denoted Trust Based Authentication Technique (TBAT). TBAT uses the trust degrees in order to select the more convenient cluster-heads. All the messages are digitally signed and they are encrypted by the sender using the cryptographic concept of public-private keys. This technique reduces the authentication time, but increases drastically the latency, in an open cooperative world, where the messages need to be shared without any encryption.

In [5], authors present an authentication scheme based on signature that preserves the privacy. For this issue, authors proposed to divide the network into different domains to facilitate the management of the certificates. They proposed also the usage of a Hash Message Authentication Code (HMAC) to replace the usage of the certificate revocation list, which is known to be time consuming. Doing such, they reduce, in one hand, the time to verify the message integrity, and in the other hand the number of invalid messages. As a consequence, this reduces authentication overhead and cost.

The authors of [6] suggested an authentication mechanism using clustering in order to resolve the problem of usage of cryptography in VANETs since the frequently change in the vehicles' positions. It aims at creating stable clusters and trustworthy in all the network. They propose also to detect malicious vehicles and the cluster heads are selected among the most trusted ones. The routing efficiency will be ensured using the network stability and these trusted cluster heads. To increase, even more, the security of the network, few vehicles are selected to monitor their neighbouring ones. In this work also, the signature and asymmetric cryptography is used. So, the same drawbacks than the work in [4].

In the work [8], the authors have presented two proposals using the cryptography in order to ensure the privacy. the first one aims to fight against the eavesdropping using the zone-encryption. They suggested to combine it with a scheme that ensure the anonymous authentication to allow only the non malicious vehicles to send messages. The main drawback of this proposal is that it introduces an overhead of 224 bytes for the cryptography within each message, which will limit the bandwidth and increase the latency. The second proposal is better adapted to the vehicular environment. It allows the vehicles, them selves, to distribute the keys. This proposal is using compact group signatures and allows to reduce the security overhead in the bandwidth with a limited impact on the cost of storage, while ensuring a high level of privacy. However, the revocation process could be complex, when an attack occurs since it does not guarantee the non-repudiation.

The authors of [9] propose a new authentication mechanism, denoted Certificate less Aggregate scheme based Traceable Ring Signature (CLA-TRS). This mechanism uses the ring signature combined with bi-linear matching on elliptic curve. Thus, it allows to ensure the privacy, while reducing the time for signature verification.

In [10], authors designed an authentication message approach combining the identity-based signature with the ring signature. The non efficiency of this approach is due to the time consuming in message signing and their verification.

Finally, the authors of [11] also use the ring signature

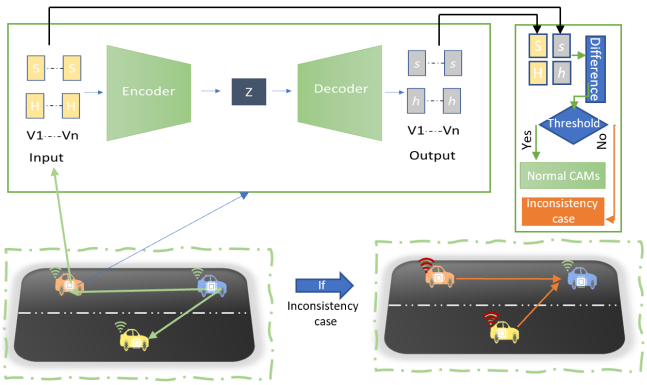

Fig. 3. Architecture of the proposed autoencoder-based process for unsupervised inconsistency detection.

and bi-linear pairing. They also added the batch signature to reduce the verification overhead. However, it is still not enough sufficient in terms of single signature and verification.

All the proposed approaches try to reduce the security fingerprint by proposing lightweight securing mechanisms. However, any one of them propose to alternatively activate and switch off the security mechanism to save the bandwidth.

Machine learning approaches have been intensively studied in recent years. An effective anomaly detection concept is required to represent the anomalous behavior of processes. Several works have proposed LSTM methods for detecting various types of anomalies. The authors of [14] used recurrent variational AE to model breathing and Kullback divergence to compare the output with the input, acting as an apnea detector. This model detects sleep apnea using the amplitude of a breathing signal and a threshold. Clustering is used in [16] to choose a single layer of sparsely placed promiscuous monitors. These monitors utilize statistical anomaly detection to assess routing misbehavior.

III. Our proposal

In our study, we suppose that a set of vehicles are driving close to each other. This assumption is quite realistic and could be enhanced for larger number of vehicles.

This set of vehicles will be considered as a cluster where all members share the same list of neighbors. The dissemination of this list is done through the beacon message (or the CAM message). For this issue, we extended these messages with a new field containing the list of all neighbors in the containers as shown on the Fig. 2. A cluster is built dynamically, at the beginning, each vehicle sends its own list of neighbors and each neighbour updates its current list. These mechanisms have been proposed in [15].

A. Cluster head management

When a cluster is already built, its cluster head is dynamic. Indeed the cluster head changes after a fixed period of time for all vehicles. In our example, this value is 10s. When a vehicle becomes cluster head it requests to each neighbour its certificate. This request is sent to all neighbours in the same time. Since it is a cluster head, its request is supposed to reach all cluster members.

Upon receiving this request, vehicles first check if the sender is really the cluster head, then it checks its neighbor list. Then each vehicle broadcasts its signed CAM with its own neighbor list *LNV* to all vehicles. In this step, the vehicles wait for a period of time Tw (A fixed threshold) to receive all possible CAMs from their neighbors as depicted by Fig. 1. Then, it checks that the condition that all members share the same neighbors is satisfied. The main steps of the whole authentication phase can be illustrated as follows:

- The CH requests for a certificate of each neighbour using a standardized procedure defined in the ETSI CAM standard.
- After receiving this request, vehicles send their CAMs with their effective *LNV*.
- If the *LNVs* are the same on all vehicles, the CH resumes its authentication step.
- Otherwise, all vehicles restart building their cluster.

B. Cluster dynamics

When the authentication setup from the cluster head has been achieved, the communications between vehicles are done using unsigned CAM messages. Indeed, the trust established earlier allows to all cluster members to have confidence. In order to guarantee a trusted environment between all neighbours during the cluster lifetime, vehicles periodically predict the behavior of each other. Here are the main steps of this part:

- Vehicles start transmitting their CAMs without signature or certificate.
- Vehicles predict the path of all other vehicles periodically.

C. Cluster update

As shown in Fig. 1, each cluster has a lifetime, at the end of this period, all vehicles return to their initial state sending signed CAMs, they start a new authentication process again.

If a cluster receives a signed CAM from a new vehicle that has just joined the cluster, the vehicles immediately stop forming a cluster and revert to the encrypted communication based on signed CAMs. This starts directly without waiting for the end of the cluster time period.

To do this, the first vehicle in the cluster that receives the new vehicle message broadcasts a signed CAM to inform all its neighbors that a new vehicle is within communication range and is not a current cluster member. Then, all other cluster members restart the authentication process with the updated list of neighbors.

D. Trust management

The dynamics of a cluster is based on how trust is managed by each vehicle regarding all other neighbours. The main idea is that each vehicle will watch the behavior of each neighbour by checking its received messages. The content of a message is used to understand the behavior of a vehicle and mainly

its trajectory. When a vehicle considers that the behavior of a sender is sound, then it maintains its confidence regarding the sender. It will continue accept unsigned messages from the sender.

In order to measure the soundness of a vehicle behavior, we propose to use a machine learning based mechanism which continuously measures the variation of the neighbour behavior. When this variation reaches an unacceptable level, then we think that the sender may be compromised, so we request its certificate to authenticate it.

This mechanism is detailed in the next section.

E. Unsupervised vehicle behavior prediction

For the purpose of detecting unsound CAMs in the trusted clusters, we introduce a new mechanism based on deep learning method in order to detect lack of soundness automatically. Auto-encoder is an unsupervised neural network that attempts to learn the optimum encoding-decoding technique from data [13]. This mechanism has the advantage to not require labeled consistent data, which is another difficult challenge since anomalous data are not always available. The auto-encoder consists of two layers: an encoder neural network that compresses the data into the latent space, while the decoder neural network decompresses the encoded representation into the output layer [12]. The main idea of our unsound process is to incorporate an LSTM auto-encoder to compute the difference between the input data of CAMs and the expected data within a time window. Fig. 3 shows our methodology which is detailed below:

F. Offline training phase

- We have first trained the LSTM auto-encoder model by considering speed and heading as input data for training, inputting the data as time series.
- Then we calculate the maximum mean absolute error loss value on the training samples. This will be the threshold for detecting unsoundness.

G. Implementation phase

- Each vehicle is provided with a model that will be activated during the dynamic phase of the clusters.

H. Processing phase

- Periodically, each vehicle tests the incoming data from its neighbors to detect if there is any inconsistency between the CAMs using this model.
- Each vehicle calculates the mean absolute error loss value on the testing samples.
- If the reconstruction loss for a sample exceeds this threshold, vehicles will label these samples as inconsistent.

I. Re-authentication phase

- After detecting an inconsistency, the vehicle sends a request certificate to the suspected vehicle.
- If there is no answer, the vehicles end the cluster and start building a new one.

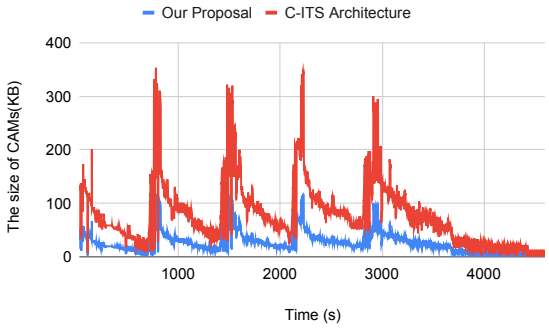

Fig. 4. The size of the exchanged CAMs

IV. Evaluation

In order to evaluate the performances of our proposal, we have used the Artery environment [13]. It is an open-source framework for the OMNET++ network simulator [14]. It is plugged to Simulator of Urban Mobility (SUMO) [15], which will be used to simulate the road traffic. Artery provides each vehicle with the standard C-ITS protocol stack with its security mechanisms. Artery also uses the IEEE 802.11 physical layer implemented by the framework VEINS to exchange CAMs over networks. We have launched our simulation in a portion of the A4 motorway between Paris and Reims in France. During an hour and a half of simulation time, we collected data from vehicles on the Highway. We applied the first part of our proposal to see the effectiveness of establishing trust between vehicles on the channel communication overload. Then, we took these CAMs data to train our LSTM auto-encoder. Fig. 4 shows the number of signed and unsigned CAMs exchanged in our simulation. We notice that our architecture has reduced the number of signed messages compared to the standard C-ITS. The presence of unsigned CAMs here is significant; our approach has replaced a major part of the signed CAMs with small-sized unsigned CAMs. The size of the CAMs exchanged throughout the simulation was then calculated. According to the C-ITS standard, the signed CAM size is 300 bytes, while the unsigned CAM size is 100 bytes. Fig. 5 show the comparisons of the size of the CAMs exchanged during the simulation of our proposal and the C-ITS architecture. In fact, our proposal reduced the size to 34% of that of the normal C-ITS protocol. This is due to the use of unsigned CAMs.

Fig. 6 show the lack of soundness detected by our LSTM auto-encoder in the speed data of the CAMs. After the training phase, we tested a sample of CAMs to detect if there is any inconsistency between CAMs using this model. To do this, we tested the data provided by the CAMs of one vehicle that are collected for 200s in our simulation. The LSTM auto-encoder detected a few cases of inconsistency which are represented by the red point in the figure. This case of inconsistency is due to the use of the mean absolute error loss value as a threshold.

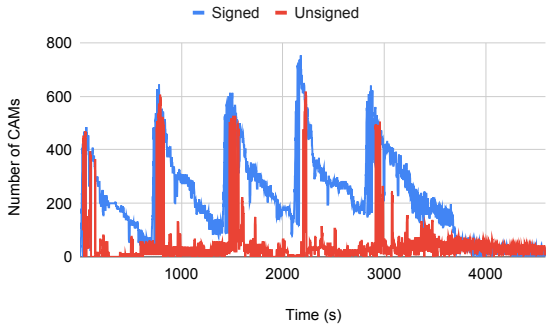

Fig. 5. The number of Signed/Unsigned CAMs

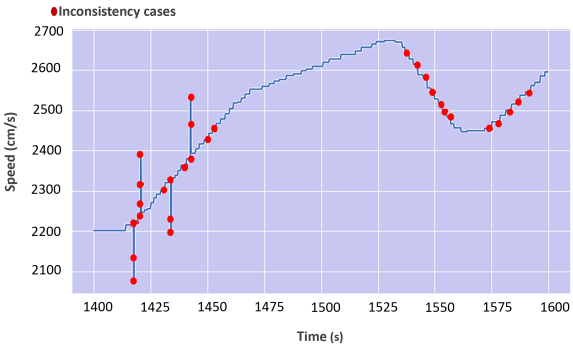

Fig. 6. Detection of inconsistencies from tested data

V. Conclusion

In this work, we proposed a solution to avoid the risk of communication channel overload in C-ITS. Contrary to the ETSI protocols, which define the security standards for C-ITS, which consider an exhaustive strategy. Our approach exploits the intelligent potential that arises when vehicles coordinate as a group rather than as a pair of individuals to leverage these standards in a selective protocol. We show that using this strategy, it is possible to significantly reduce the number of authentications required while ensuring security with real-time consistency checking using deep learning detection. Vehicles in our proposal have a model based on LSTM auto-encoder in order to measure the soundness of a vehicle behavior. We evaluated and compared our approach using several settings with the C-ITS architecture. For this purpose, Our approach effectively reduces network overhead. The results show that the resource utilization of our approach is better optimized, reducing the size of message exchanges between vehicles by 34%. Our approach is a robust solution that provides a high level of security through a real-time Unsupervised Detection. We intend to evaluate our proposal's resistance to various types of cyber attacks.

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 in part by the NSF under Grant ECCS-1923717 and CNS-2107190.

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] 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.

[4] 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.

[5] 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.

[6] 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.

[7] 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.

[8] 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.

[9] 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,

[10] 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.

[11] 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.

[12] 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.

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

[14] 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.

[15] 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.

[16] 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.

[17] 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.

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

[19] 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.