A Systematic Review on Intelligent Intrusion Detection Systems for VANETs

Fábio Gonçalves[†*], Bruno Ribeiro[†*], Oscar Gama[†*],
Alexandre Santos[‡*], António Costa[‡*], Bruno Dias[‡*], Joaquim Macedo[‡*] and Maria João Nicolau[§*]
[*] Algoritmi Center
Informatics department
University of Minho
Portugal
[†] b7207,b7214,b2583@algoritmi.uminho.pt
[‡] alex,costa,dias,macedo@di.uminho.pt
[§] joao@dsi.uminho.pt

***Abstract*—Vehicular Ad hoc Networks (VANETs) are a growing area that continues to gain interest with an increasing diversity of applications available. These are the underlying network for Intelligent Transportation Systems (ITS), a set of applications and services that aim to provide greater security and comfort to drivers and passengers.**

However, the characteristics and size of a VANET make it a security challenge. It has been a subject of study, with several research works aimed at this problem, usually involving cryptography. There are, however, some attacks that cannot be solved using traditional methodologies. For example, Sybil attack, Denial of Service (DoS), Black Hole, etc. are not preventable using cryptographic tools. Nonetheless, using an Intrusion Detection System (IDS) can help detect malicious behavior, preventing further damage.

This work presents a Systematic Literature Review (SLR) that aims to evaluate the feasibility of this type of solution. Additionally, it should provide information of the most common approaches, allowing the identification of the most used Machine Learning (ML) algorithms, architectures and datasets used.

***Index Terms*—Machine Learning, Intrusion Detection System, Systematic Literature Review, VANETs**

I. Introduction

Vehicular Ad hoc Networks (VANETs) allow vehicles to communicate amongst themselves and with the infrastructural network. These enable several services to be implemented with the main goal to improve road safety, reducing accidents and traffic congestion. The specific characteristics of these types of networks facilitate the existence of vulnerabilities, making them especially attractive for attackers.

There are several studies done on preventing VANET attacks, generally by using cryptographic tools [1] [2] [3] [4] [5]. However, these methods cannot detect or prevent some attacks. Denial of Service (DoS), black hole, grey hole, Sybil, etc. are some examples of attacks that cannot be prevented by traditional methods. The usage of cryptography can even increase the possibility of DoS [6]. If the messages are signed, checking for the signatures on fake ones can overload an entity.

One possible solution for this problem is the usage of an Intrusion Detection System (IDS). These can detect attacks and trigger a response, minimizing the effects on the targeted system [7]. Traditional IDSs assume that an intruder's behavior will be noticeable from normal network operation. Signature detection systems compare the behavior of an attacker with known attacks, assuming no new attacks will happen. Anomaly detection systems focus on detecting significant deviations from normal behavior. However, the definition of these criteria is difficult to attain [8]. The usage of intelligent algorithms enables the IDS to learn previous attacks and discover new ones.

The purpose of this research is to evaluate the feasibility of implementing an IDS for VANETs, focusing on the ones taking advantage of intelligent algorithms. Moreover, this study should identify which types of IDS, Machine Learning (ML) algorithms, datasets and IDS testing methodology are most commonly used.

One of the most accepted ways to conduct an extensive review of the existing literature is using a Systematic Literature Review (SLR). This type of research should have a well-defined methodology allowing the identification of works with relevance to the study being carried out.

The document is organized as follows: Section II describes the SLR methodology, including all the steps taken from the definition of the Research Questions (RQs) to the extraction of the data. Additionally, the literature sources and search string, and the inclusion/exclusion criteria are identified; Section III presents a synthesis of the collected papers. Section IV contains an analysis of the experimental results; Finally, in section V, the conclusions and future work are presented.

II. Methodology

A SLR should follow a strict methodology providing an efficient and exact way to gather and evaluate existing works. It also provides a way for a study to be replicated and peer-reviewed. This research follows the methodology proposed by [9] and it's presented in Figure 1.

The methodology presented is comprised of 6 main steps: define the RQs, specify the literature sources and search string, select relevant studies, assessing the studies collected, extract

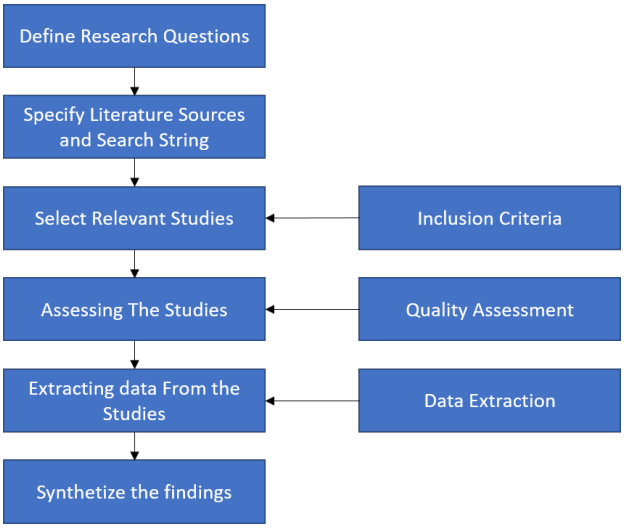

Fig. 1. Methodology

the data from the studies and finally, synthesize the collected data.

A. Research Questions

The goal of this review is to identify the state of the art of IDSs for VANETs, mainly the ones that use ML. The RQ defined are the following:

- **RQ1** How can an attacker target VANETs? This question aims to find which types of attackers exist in a VANET environment and how they can target their nodes.
- **RQ2** Can IDSs detect attacks targeting VANETs? Mainly the ones with no cryptographic solutions. Some IDSs can detect attacks in more traditional networks but, VANETs have a different structure and communication types. The goal of this question is to find if IDSs can be used in these types of networks, with a special interest in attacks not preventable by other tools.
- **RQ3** Which kind of IDS can be use in VANETs? This question aims to find which type of IDS is best suited for this environment.
- **RQ4** Can ML algorithms improve IDSs to detect attacks and which types of ML are the most suited? VANETs have characteristics that can facilitate several vulnerabilities. Thus, there can be a plethora of different types of attacks and attackers. The goal of this question is to find if the usage of ML algorithms can help detect attacks.
- **RQ5** How can an IDS be tested and evaluated?
- **RQ6** Which metrics can be used to evaluate the IDS performance? Question 5 and 6's main goal is to find how an IDS can be tested and evaluated, and which metrics can be used to do so.

B. Literature Sources and Search String

Using the previously defined RQs, a search string was created using the following method [9] [10]. First, the main search terms are derived from the RQs. Then, using documents already analyzed, more search terms are collected. The next step is to find synonyms and alternative spelling for the major terms already found. Finally, the string is built by joining the terms found. Boolean ORs are used to join alternative spellings and synonyms and ANDs to join major search terms. These can be found in Table I.

TABLE I
SEARCH TERMS

Search Terms	Synonyms and Alternatives
VANET	VANETs; Vehicular ad-hoc network;
IDS	Intrusion Detection System; Anomaly Detection
Machine Learning	Intelligent Algorithms
Attack	Attackers; Intrusions; Intruders

The search terms found were used to build a Search Query (SQ) and perform a preliminary search using some of the major databases, namely, IEEE, Science Direct and ACM. The documents obtained were filtered keeping only those mentioning VANET and IDS. the studies resulting from this research were:

- IEEE - 6 Papers
- Science Direct - 6 Papers
- ACM - 2 Papers

Due to the small volume of results obtained, it was decided to increase the number of databases. And thus, the research for new databases was started.

However, two issues were encountered: the query language is not the same across all platforms; the number of studies resulting from some surveys was too large to be manually analyzed. During this process, an aggregator platform was found, Crossref [11]. This is a non-profit organization that provides a free to use platform. It contains studies from the most well-known databases. Crossref provides an easy-to-use REST API that allows to search documents based on their titles and metadata. Moreover, there are some well-documented libraries available implemented in several languages.

The main issue with this platform is the lack of support of Boolean AND, performing an OR operation with all terms. Thus, any study that contains only one of the search terms is returned. Therefore, some of the previously defined terms may not make sense in this paradigm. For example, using the acronym for Intelligent Transportation System, ITS, would return all documents containing "its" in their metadata.

To accommodate this new perspective, a new SQ was built, **"vanets vanet vehicular ad hoc networks network intrusion detection system systems anomaly anomalies intelligent"**. Although simple, this search string includes all the terms that should be present in all the resulting studies.

C. Studies selection

As Crossref only performs Boolean OR, using the SQ 6,239,042 studies were returned. In this search, no filters were used and all the supported databases were searched. As the volume of the returned studies was too large to be manually analyzed, an automatic tool was built. Using the

”habanero” library [12], a well-documented library that allows easy Crossref access, a python application was built.

This automated tool receives a SQ and uses it to execute multiple requests to the Crossref platform until all the results are returned. To reduce the volume of returned studies, a filter was implemented. Its purpose was to provide a boolean AND that Crossref does not have. So, two sets of terms were built. These will be used to perform boolean OR inside each group and boolean AND with the terms of the other group.

The first group contains the following terms:

- vanet;
- vanets;
- vehicular ad hoc network;
- vehicular ad hoc networks;
- vehicular ad-hoc network;
- vehicular ad-hoc networks;
- intelligent transportation system;
- intelligent transportation systems.

The second groups, terms are as follows:

- ids
- idss
- intrusion detection system
- intrusion detection systems
- intrusion detection
- intrusions detection
- anomaly detection
- anomalies detection
- intelligent detection

After filtering the obtained terms, 41 papers remained. All the returned results are stored in a Mongo Database to provide easy access and manipulation of the results.

D. Inclusion/Exclusion Criteria

Using as an example the parameter defined by the authors in [10], the following inclusion criteria were defined:

- If a study has a journal and a conference version available, only the journal version is kept;
- If a study has several version published, only the most recent is kept;
- If a study exists in more that one source, only one of its copies is included;

In addition to inclusion criteria, excluding criteria is also defined to exclude ineligible studies. The defined exclusion criteria are the following:

- Only papers available to download are kept. Some papers have restricted access and so, will not be included;
- Only studies from conferences or journals that are indexed in Scopus are included. This criteria is meant to only use studies from reliable sources;
- Studies that do not consider VANETs
- Studies that do not consider MLs

The inclusion and exclusion criteria were applied to the 22 studies. 12 of the documents filled the criteria and were kept. Two of the documents found were reviews on IDSs, ”A Survey on Intrusion Detection Systems and Honeypot based proactive security mechanisms in VANETs and VANET Cloud” [13] and ”A review and classification of various VANET Intrusion Detection Systems” [14]. Of these two papers, only the first was considered. In this study, an in-depth SLR of IDSs for VANETs is made. Therefore, its relevant studies were collected and used to enrich the SLR. Since the second document does not apply any methodology to the review it makes, it was discarded.

After using the same criteria on the survey papers and removing the repeated papers, 22 papers remained in total. Figure 2 shows how the papers are distributed by year. It is noticeable an increase in studies from 2013 with a drop in the last two years.

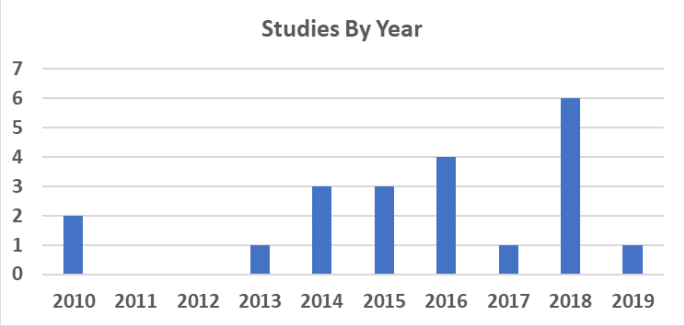

Fig. 2. Studies by year

E. Data Extraction

At this stage, the objective was to extract specific information about the gathered studies. So, to be as precise as possible, a table with parameters to be collected from the studies was distributed to other reviewers. These parameters are network simulator, traffic simulator, type of IDS, detection type, ML algorithm, which attacks were targeted, which datasets were used and where the IDSs were located.

In Figure 3 the network simulators used are presented. The most commonly used network simulator is Network Simulator 2 (ns-2), followed by Network Simulator 3 (ns-3). These are two of the most popular network simulators. They provide the majority of the network implementations, including WAVE and ITS-G5, which are open-source and highly customizable. Some studies use Matlab or their own simulator, and others just use the data directly from the datasets (usually from datasets publicly accessible). Unfortunately, some of the papers do not specify which simulator was used.

The most used traffic simulator was Simulation of Urban Mobility (SUMO), which in some studies is used in combination with MObility VEhicles (MOVE), as can be seen in Figure 4. From the information collected, only one more traffic simulator was used, VANET Mobisim. The remaining studies used data from a dataset or did not specify which one was used.

One of the key aspects of this research was to find which datasets were used in each study. These are shown in Figure

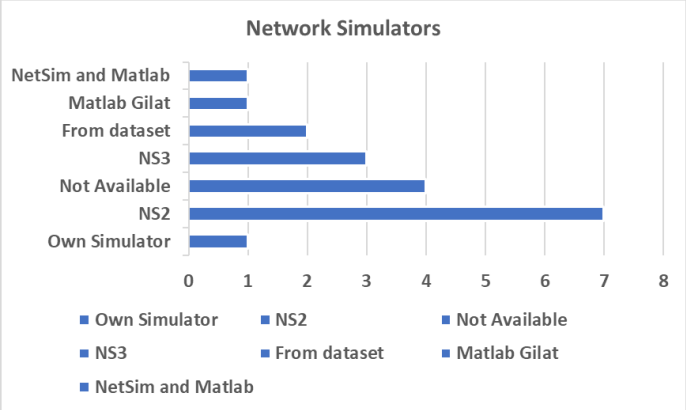

Fig. 3. Network Simulators

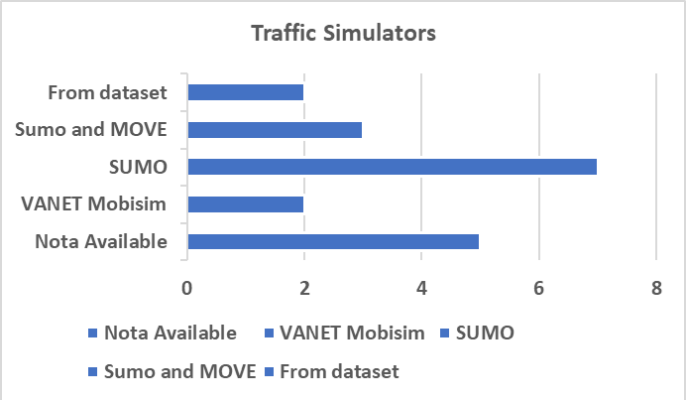

Fig. 4. Traffic Simulators

5. Most of the studies collected their datasets from the simulations. Some of them were obtained from the tracefile generated by the network simulator (ns-2 and ns-3) and others from values extracted during the simulation. Some of the studies used the existing datasets, Kyoto dataset [15] and NSL-KDD [16].

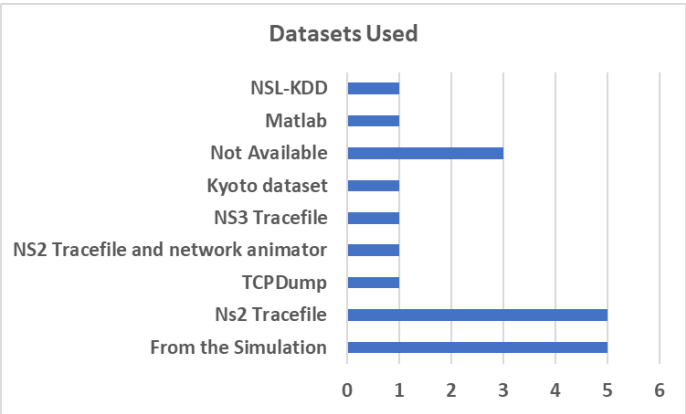

Fig. 5. Datasets

Figure 6, shows which ML algorithms were more used in the studies. The most common was Neural Networks (NN) followed by Support Vector Machine (SVM). Some of the studies also combine more than one machine learning algorithm.

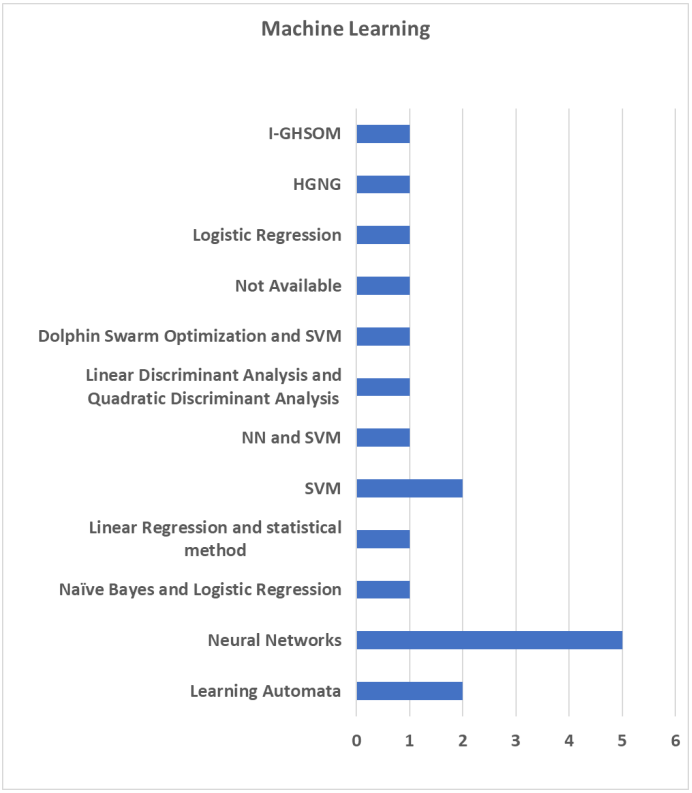

Fig. 6. Machine Learning Algorithms

III. Synthesis Of Collected Data

Misra et al. [17]: In this work, the authors propose a Learning Automata (LA) based solution for IDS in VANET. The proposed model is privacy conscious assigning a dynamic ID to each vehicle making it untraceable.

In the proposed solution, a VANET management system is built. Each route has a base station and all vehicles are equipped with transmitting devices required to communicate with the base stations. Each attacker will create malicious packets to divert traffic.

Both the attackers and the system have a budget based system. The bigger the budget for the attacker, the more packets it will be able to generate. For the IDS, the budget increases the sampling rate of VANET packets.

The attackers are detected using only their dynamically attributed IDs. If only un-allocated IDs are attributed and if more than one vehicle possesses the same ID, one of them is malicious. The learning automata is used to attribute the budget for under attack grids and re-calculating the sampling rate.

The model evaluation is performed by simulation, using their own simulator. Several simulations are done varying the number of attackers, attacker and IDS budget. The results vary from 40 to almost 100% of malicious packets caught

TABLE II
PAPER DATA

Paper	Net Sim	Traffic Sim	Attacks	IDS Type	Detection Type	ML	Dataset	Placement
[17]	Own	Own	Malicious packets	Hierarchical	Anomaly	Learning Automata	From Simulation	Base Station
[18]	NS2	N.A.	DoS	Hierarchical	Anomaly	Neural Networks	NS2 Tracefile	Access Points
[19]	N.A.	VANET Mobisim	Abnormal behaviors	Colaborative	Anomaly	Learning Automata	From Simulation	Vehicles
[20]	NS3	SUMO	DoS, R2L, U2R, Probing	Hierarchical	Anomaly	Naive Bayes and Logistic Regression	TCPdump	Each cell and vehicle
[21]	NS3	SUMO	Greedy Behavior	N.A.	Watchdog	Linear Regression	From simulation	N.A.
[22]	NS2	SUMO and MOVE	DoS	N.A.	Anomaly and Misuse	Neural Network	NS2 Tracefile	Any Node
[23]	NS2	SUMO	Black Hole	N.A.	Anomaly and Misuse	Neural Network	NS2 Tracefile and Animator	N.A.
[24]	NS3	SUMO	Selective Forwarding, Black Hole, Packet duplication, Resource Exhaustion and Sybil attack	Hierarchical	Rule Based and Anomaly	SVM	NS3 Tracefile	Vehicles and RSUs
[25]	—	—	DoS	Hierarchical	Misuse and Anomaly	Neural Networks	Kyoto Dataset	N.A.
[26]	N.A.	N.A.	Malicious behavior	N.A.	Watchdog	Bayesian Filter	N.A.	Every Node
[27]	NS2	SUMO and MOVE	Grey Hole and Rushing	N.A.	Anomaly	Neural Networks and SVM	NS2 Tracefile	N.A.
[28]	Matlab	VANET Mobisim	packet dropping	Hierarchical	Watchdog and Anomaly	SVML	From Simulation	Vehicles
[29]	NS2	SUMO and MOVE	DoS and Black Hole	Standalone	Anomaly	Linear and Quadratic Discriminant Analysis	NS2 Tracefile	Vehicles
[30]	NetSim and Matlab	SUMO	Wormhole, Selective Forwarding, Packet Drop	Hierarchical	Anomaly	SVM	NS2 Tracefile	Vehicles
[31]	N.A.	N.A.	Traffic Anomalies	N.A.	Anomaly	Neural Networks	N.A.	N.A.
[6]	N.A.	N.A.	DoS	Hierarchical	N.A.	N.A.	N.A.	N.A.
[32]	-	-	Network Anomalies	Hierarchical	Anomaly	Logistic Regression	NSL-KDD	Vehicles
[33]	NS2	SUMO	Network Anomalies	Hierarchical	N.A.	HGNG	From Simulation	Vehicles
[34]	NS2	SUMO	Network Anomalies	N.A.	Anomaly	I-GHSOM	From Simulation	Vehicles

N.A.: Not Available

depending on the system budget, number of attackers and number of vehicles. In the proposed solution the IDS is in each of the bases stations and seems to have full visibility of the network packets.

Tian et al [18]: Presents a VANET IDS based on the BUSNet. This is a virtual mobile backbone infrastructure constructed using public buses. In this solution, the buses act as cluster-heads gathering the data packets transmitted by all vehicles and transmitting it to the access points along the roadsides. Then, this information is classified using a NN based algorithm and used to detect DoS attacks.

The presented solution is tested through simulation using the ns-2 network simulator. The authors do not indicate how the traffic is modeled or which traffic simulator is used. In the simulation, 50 vehicles transmit data with a Constant Bit Rate (CBR) and a packet size of 512 bytes. The sending period is of 4 seconds. The attacks are performed by two of the vehicles that transmit data with smaller time intervals, 0.01 seconds, at 4 time points during 10 seconds each attack. The authors define a threshold value from which they consider an attack. This value is varied from 0.05 to 0.7 making the results vary. The optimal value for the threshold is 0.2.

Kumar et al [19]: This work proposes an IDS based on a trust aware collaborative learning automata. Each vehicle has a data collection, detection and alert generation module operated by automatons. These modules are used in conjunction to collect information from the data sent between vehicles, according to their position and movement. Then, it is processed to detect attacks and generate attacks.

The solution is tested through simulation using Vanet MobiSim, with a total number of 500 vehicles with speeds between 20 and 50 km/h. Unfortunately, the authors do not indicate which network simulator is used. The authors then vary the number and speed of the nodes to evaluate their solution. The detection rate varies from 95% to 82%, depending on the number of nodes and their speed. The results have a more accentuated descent with the speed increase. Finally, the solution is compared with similar works.

Liu et al [20]: Authors in [20] propose applying data mining methodology to detect known attacks and discover other unknown attacks in VANETs. The solution presented has three main contributions: a decentralized vehicle network with scalable communication and data available about the network; using two data mining models to show feasibility for an IDS in VANETs; and finding new patterns of unknown intrusions.

In the proposed system, the network is divided into a cell grid. Each cell has a transmission tower that enables communication with other cells and the Internet. Each one will run its own data mining models and rules, detecting new attacks. Thus, this allows the IDS to create new rules to be transmitted for each subnetwork. The data exchanged in the network is collected by both vehicles and the tower cell. The authors apply Naive Bayes and Logistic Regression classifiers to the collected data.

The authors first test the network performance of their method using simulation. First, SUMO is used to generate a mobility trace file. This is fed into ns-2 to simulate the wireless network. This scenario is comprised of 150 vehicles that make random turning decisions at intersections, follow the speed limits (from 5 to 20 m/s) and randomly placed traffic lights.

The IDS was tested by loading 5 vehicles with Linux running several network applications. Then, TCPdump was used for 9 months to build the dataset. 4 attack categories with 39 attack types were recorded. These are then classified using WEKA. The evaluation of the models was made using the metrics recall, F-measure and MCC.

Mejri et al [21]: The proposed solution in [21] is comprised of a detection algorithm based on a statistical method, linear regression and watchdog to, in a passive way, be able to detect greedy behavior in the MAC layer. The proposed solution uses a watchdog to monitor the correlation of access times of active nodes. The algorithm considers the network to be under attack if the correlation coefficient is not close to 1 or the correlation coefficient is close to 1 and the slope of the linear regression straight is not close to 1. To do so, the implemented software monitors the following metrics: duration between two successive transmissions, transmission time and connection attempts of a node.

The performance evaluation of the solutions is made using the tracefile generated by SUMO directly in ns-3. The scenario used in SUMO is based on a real city map with signs and traffic lights. Firstly the network is simulated with normal behaved nodes to confirm the application of the linear regression method. Then, there are injected greedy nodes, one by one to a total of four greedy vehicles.

The solution can detect the greedy behavior in 1.3, 1.9, 3.1 and 7.9 seconds for 1, 2, 3 and 4 nodes, respectively.

Alheeti et al [22]: The solution in [22] is an Artificial Neural Networks (ANN) based misuse and anomaly IDS to detect DoS attacks.

To design the solution, firstly, the authors generated a mobility scenario using SUMO. The files generated by SUMO were converted using MOVE to be recognizable by ns-2. Finally, ns-2 was used to simulate communications between the vehicles. The authors used the Manhattan urban mobility to create the mobility and traffic scenario.

The simulation scenario is comprised of 30 vehicles and 6 Road Side Units (RSUs) and runs for 250 seconds. The vehicles run a CBR application that sends User Datagram Protocol (UDP) packets. Only one of the vehicles is malicious. It will drop the packets instead of forwarding them.

The designed solution was able to classify normal and abnormal behaviors with 98.45% and 85.02% accuracy, respectively.

Alheeti et al [23]: Authors in [23] propose to use a Proportional Overlapping Scores (POS) method to reduce the number of features that are extracted from the tracefile. These are used to train an ANN for classification.

The first step of the solution, the generation of the mobility scenario and tracefile, is similar to the one presented in [22]

The generated ns-2 tracefiles were then used in their POS algorithms to extract the more relevant features. Finally, the data from the dataset is then fuzzified to avoid classification problems.

The IDS designed in this solution uses Feed Forward Neural Network (FFNN) to classify the dataset. 60000 dataset records were used, divided into training (50%), testing (25%) and validation(25%). This dataset contains both normal and malicious behavior. The malicious behavior crafted was Black Hole attack, in which the malicious vehicle will drop all the received packets instead of forwarding them.

Finally, the IDS was tested using both anomaly and misuse detection. In misuse detection, it obtained a classification of 99.89% for the normal behavior and 99.80% for the abnormal. For anomaly detection, the results for the normal and abnormal behaviors were 99.87% and 99.72% respectively.

Sedjelmaci et al [24]: In [24], authors propose a cluster-based IDS that aims to protect the network against selective forwarding, black hole, wormhole, packet duplication, resource exhaustion and Sybil attack. The proposed approach applies several detection agents that run at three levels - Cluster member, cluster-head and RSU.

The vehicles are grouped in clusters according to their velocities. The parameters used to select the cluster heads are cluster connectivity and assuring security. Connectivity within a cluster is improved introducing a social behavior.

The IDS architecture is composed of two main detection systems and a decision system. The detection systems are the Local IDS and Global IDS, that runs at cluster member and cluster heads, respectively. The decision system is called Global Decision System and runs at the RSUs. This allows the system to detect attacks at different levels an monitor the several entities. Also, each level can execute different algorithms and detection techniques, evaluating different features. The Global Decision System will receive the aggregate reputation of each vehicle forwarded by the cluster head and computes their trust level.

The evaluation of the solution was made using ns-3 as the network simulator and SUMO to simulate the vehicle's mobility. The IDS evaluation was made in terms of detection rate, false positive rate and detection time. The several attacks were tested with a different number of vehicles. The number of attackers is fixed at 45%. The results presented vary from 92% to 100%, depending on the number of vehicles and the attack tested.

Alheeti et al. [25]: In [25], a hierarchical intelligent IDS to secure communication for self-driving and semi self-driving cars is proposed. The authors use the Kyoto dataset and apply the POS algorithm to decrease the number of features. Then, this data is classified using Back Propagation Neural Network (BPNN).

The designed solution goes through five phases: preprocessing, feature selection, fuzzification and training and testing.

To test the IDS, a dataset of 60000 records extracted from the Kyoto dataset is used. This, is divided into three subsets: test (25%), validation(25%) and training(50%). The results obtained are 99.23% accuracy for normal behavior and 99.05% for abnormal.

Alheeti et al. [27]: In this work, a FFNN and SVM based IDS is proposed. Also, a systematic response is proposed to protect vehicles when malicious behavior is detected.

The IDS is trained by using a dataset built from SUMO and ns-2, using the features from the tracefile. These features are reduced from 21 to 15 using the POS algorithm.

The dataset is comprised of 30000 records that define normal and malicious behavior. This dataset is fuzzified before being used for classification. The authors subdivide the dataset in validation, test and training dataset.

Grey hole attacks are generated by selecting malicious vehicles that will drop packets at random times. To perform the rushing attack, the Ad hoc On-Demand Distance Vector (AODV) protocol needed to be adapted.

The accuracy results obtained in simulation were 99.93% for normal behavior and 99.64% for abnormal behavior in the case of SVM. Using FFNN, the results were 99.82% and 98.86% accuracy for normal and abnormal behavior, respectively.

Wahab et al [28]: In this work, an intelligent IDS is proposed. It is composed of a cooperative monitor, able to collect messages exchanged by vehicles, and uses SVM in an on-line and incremental fashion to classify the vehicles. The protocol overhead is reduced by decreasing the training dataset. This is done by restricting the data collection storage and analysis to only a set of specialized nodes and migrating only a few tuples from one detection iteration to other. Also, a propagation algorithm is proposed that enables the dissemination of only the final decisions among clusters.

The data is collected by all cluster members that are designated as watchdogs. These will continuously monitor and analyze the vehicles of the MultiPoint Relay (MPR) that are serving them, detecting if any packet was dropped. Then, all the watchdogs in each cluster share their collected evidence. Afterward, each watchdog classifies the collected data. To do so, they use their own collected data as the test dataset and the observations of the other watchdogs as the training dataset.

The proposed solution was tested by simulation. Matlab Gilat has been used to implement the network related algorithms and VanetMobiSim to simulate the road traffic. The simulations are made with several vehicles varying from a total of 100 to 500. The number of malicious vehicles varies from 10% to 50%. The solution has a detection rate of 98.1%.

Alheeti et al [29]: Authors in [29], propose an intelligent IDS to protect against attacks, mainly DoS and Black Hole attack using Linear and Quadratic Discriminant Analysis.

Firstly, malicious behaviors are simulated. To generate the DoS attack, the authors modify the AODV protocol. In this case, the DoS attacks are performed by dropping packets.

Then, the mobility and traffic scenarios are created. SUMO and MOVE are used to generate a realistic environment of malicious and normal behaviors. Additionally, ns-2 is used to simulate communications. The dataset is extracted from the ns-2 tracefile and all the 21 features are maintained. Before being used for the test and train, the data is fuzzified.

The obtained detection rate results are 86.44% for the Linear Discriminant Analysis and 85.67% for the Quadratic Discriminant Analysis.

Sharma et al [30]: Authors in [30], propose a new method for the selection of a stable Cluster Head, using Hybrid Fuzzy Multi-criteria. Then, a machine learning based IDS using SVM is used to detect malicious behavior. The SVM based IDS detection capabilities are improved by using a Dolphin Swarm Algorithm. This algorithm uses the dolphin swarm behavior of hunting and praying to detect and isolate malicious nodes in the network.

The proposed scheme is tested using simulation. NetSim and Matlab are used as the network simulators and SUMO for the traffic. In the simulation, several node densities are tested from 50 to 300 and a maximum of 45% of the vehicles are attackers.

The detection rate of the proposed IDS varies depending on the number of vehicles and is more than 98% for packet drop and selective forwarding and wormhole attack.

Nie et al [31]: In [31], an anomaly detection algorithm is proposed using the network traffic estimation made using the spatio-temporal feature of the network traffic. The convolutional NN is used to extract features of the traffic matrix.

To detect the anomalies, first, the traffic is estimated based on the convolutional network. The anomaly detection is done based on a threshold identification approach.

There were 3000 tests carried and the results indicate that there is a high true positive rate mainly compared with previous works.

Tan et al [6]: This work main goal is to propose a certificateless authentication scheme with Chinese remainder theory for efficient group key distribution. However, as several anomaly messages need to be authenticated during a relatively short period, there is the possibility of DoS attacks. So, an unsupervised anomaly detection scheme is proposed. This applies time warping for distance measurement. In this scheme, vehicles need to maintain communication with the RSUs as they perform part of the work.

The built IDS is a multilevel hierarchy with the clusters at one level are joined as clusters at the next level.

The proposed scheme is tested experimentally using python and the pypbc library. The authors do not indicate any network or traffic simulator

Zhang et al [32]: Authors in [32] propose a privacy preserving machine learning based collaborative IDS. With that goal, a collaborative IDS architecture is proposed, enabling information and knowledge sharing. Then, an alternating direction method of multipliers algorithm is used to capture the distributed nature of the network and construct a collaborative learning algorithm over a VANET on a regularized empirical risk minimization algorithm. The privacy of collaborative learning is achieved by using the dual variable perturbation before minimizing the augmented Larange function. The goal

of the classifier is to detect if the network is under attack using logistic regression.

The proposal is tested using the well known NSL-KDD dataset evaluating the impact of the VANET size and topology.

Ayoob et al [33]: In [33], authors propose using an IDS with a Hierarchical Growing Gas Network (HGNG) based classifier. Also, a semi-cooperative feature extraction method is used to collect the current location information, the location features and the historical information.

The IDS is trained in a non-attack situation so the IDS can detect anomalies in the VANET. Each vehicle calculates measurements as, for example, average traffic and location information .

Simulation is used to test the designed IDS. SUMO is used as the traffic simulator and ns-2 the network simulator. The evaluation is done by inserting 50% of malicious vehicles and verify the network changes.

Liang et al [34]: The authors in [34] propose a feature extraction algorithm and a classifier based on an Improved Growing Hierarchical Self-Organized Map (I-GHSOM). The proposed algorithm extracts two key features: the differences of traffic flow and position.

The proposed IDS consists of three modules: feature extraction, classifier and response. The feature extraction module quickly translates the measurements in the messages to features. The traffic flow extracted is the difference in flows between two adjacent vehicles. The difference in position is the difference between the claimed and detected position.

The classifier module has been trained and can check if there are any deviations in the messages according to the features extracted. Finally, the response module takes action to assure the security of the network.

The performance of the scheme is evaluated using simulation. ns-2 is used to simulate network communications and SUMO to simulate the vehicle's mobility. The rate of rogue vehicles is varied from 10% to 40%. The IDS has a better performance with a lower number of vehicles. The false positive rate increases with the increment in rogue vehicle rate and the true positives decrease. The values for the true positive rate vary from a little over 98% to 86.5%. The false positives rate is between 0.4% and less than 1.2%.

IV. Analysis of Experimental Results

The most common approach for an IDS for VANETs uses the tools shown in Table III. That solution is comprised of a hybrid detection, that performs misuse and anomaly detection. The simulation is performed using ns-2 as the network simulator and SUMO to simulate the vehicle's mobility. In most of the solutions, the dataset is obtained directly from the network simulator tracefile.

Unfortunately, a number of studies did not specify which network and traffic simulator was used. The same happened for the dataset used to train and test the IDS.

Most of the used studies use their own datasets, either from collected events from the simulation or directly from the network simulator tracefile. The ones that use more reliable datasets choose the known NSL-KDD and Kyoto datasets. These are publicly available datasets with a high reputation and used by many works. However, they are not obtained from VANET networks and thus may produce biased results.

TABLE III
IDs tools used

Network Simulator	NS-2
Traffic Simulator	SUMO
Dataset	Net Simulator Tracefile
ML algorithm	NN
IDS Type	Hierarchical

The studies that use their own datasets do not make them publicly available compromising the validity of their results. This combined with the lack of explanation on how the datasets are constructed and the clear explanation on how to build the attacks (ratio between normal and abnormal messages, etc.), complicates the verification of the results. Moreover, the great majority of the results presented indicate a very high value of the detection rate. This value may indicate overfitting of the model. Also, most of the studies do not present the configuration used in the algorithms.

A. Fostering Result comparison

To assess the influence, or even the dependency, that datasets put on the derived results, a simulation setup has been made. This does not try to show how good the classifier is, but how it can produce biased results depending on the dataset.

So, using SUMO, a scenario has been built comprised of a 4x4 grid where vehicles follow 10 specific routes. The normal behavior vehicles will broadcast messages in 1 second intervals.

To decide if a vehicle is an attacker, a random number between 0 and 100 is generated. If its smaller than 10, the vehicles is selected as an attacker. If it is chosen as an attacker, it will randomly start DoS attacks. To do so, it will send the same messages as the normal vehicles but with a small time interval, that will be randomly chosen from 0 to 40% of the normal period. The attacks will be made at random times during a random interval until a max of 60 seconds. The ML algorithms test and training will be done using Weka.

All messages received by the vehicles will be stored in the same dataset and are marked as attack or normal. From the dataset, the top 200000 messages were chosen to train a classifier. These were divided into training (80%) and test (20%). This division is made randomly using the Weka tool. Multilayer Perceptron was used to classify the collected training set using 10 fold cross-validation. The algorithm configuration is the default.

During the model training phase, the results indicate 100% of accuracy, which is indicative of possible overfitting. The trained model is then used to classify the test dataset. The accuracy of the classifier for this dataset is 100%, with all messages well classified.

Then, to test how much the results may be biased datasets, the same scenario has been run again creating a completely

new dataset. As the chosen attacker will be random and the attack intervals too, this dataset will have completely different attacker vehicles with different DoS attacks. Using the previously trained model in this dataset the detection rate is much smaller decreasing to 67%. The true positive rate for the abnormal messages is only 55% meaning that almost half of the attacks considered as normal messages.

This does not mean that the studies results are biased but, without the datasets that were used to train and test the models, it is not possible to verify the results obtained.

V. Conclusions

In this paper, an extensive SLR on the usage of intelligent IDS in VANET is presented. 22 papers were obtained and evaluated, allowing the identification of the most common solutions in this area. The most common combination of network and traffic simulator found in the studies is ns-2 with SUMO. As for the most common ML algorithm, NN seems to be the preferred one (its several variants). The used datasets are generally created for each study, either from the simulation or from the network simulator tracefile. Finding highly reputable and publicly available datasets was one of the goals of the SLR. Unfortunately, it seems that this is not the case.

The evaluation of the studies showed that most of them do not clearly identify how their datasets and attacks are created. Additionally, none of them makes their datasets publicly available for peer review. Some of them use widely reputed datasets that are publicly available, such as the Kyoto dataset and the NSL-KDD. However, these are not obtained from VANETs and can skew the final results.

As a future work, the main goal will be to create an architecture for intelligent attack detection. One focus of this work should be the creation of datasets large enough to allow the efficient training of a ML algorithm. Also, an extensive description of how the dataset was created, attacks and normal messages, should be made. Moreover, it must be made publicly available for peer review.

Acknowledgment

This work has been sponsored by the Portugal Incentive System for Research and Technological Development. Project in co-promotion 002797/2015 (INNOVCAR 2015-2018), and also by COMPETE: POCI-01-0145-FEDER-007043 and FCT - Fundação para a Ciência e Tecnologia within the Project Scope: UID/CEC/00319/2019.

References

[1] F. Gonçalves, A. Santos, A. Costa, B. Dias, B. Ribeiro, J. Macedo, M. J. N. Nicolau, S. Sousa, O. Gama, S. Barros, and V. Hapanchak, "Hybrid Model for Secure Communications and Identity Management in Vehicular Ad Hoc Networks," *9th International Congress on Ultra Modern Telecommunications and Control Systems (ICUMT'2017)*, pp. 414–422, 2017.

[2] F. Gonçalves, B. Ribeiro, V. Hapanchak, S. Barros, O. Gama, P. Araújo, M. J. Nicolau, B. Dias, J. Macedo, A. Costa, and A. Santos, "Secure Management of Autonomous Vehicle Platooning," in *Proceedings of the 14th ACM International Symposium on QoS and Security for Wireless and Mobile Networks*, ser. Q2SWinet'18. New York, NY, USA: ACM, 2018, pp. 15–22. [Online]. Available: http://doi.acm.org/10.1145/3267129.3267146

[3] ETSI, "ETSI TS 102 940 V1.1.1 Intelligent Transport Systems (ITS); Security; ITS communications security architecture and security management," 2012.

[4] B. Bellur, "Certificate Assignment Strategies for a PKI-Based Security Architecture in a Vehicular Network," in *IEEE GLOBECOM 2008 - 2008 IEEE Global Telecommunications Conference*, nov 2008, pp. 1–6.

[5] A. Hesham, A. Abdel-Hamid, and M. A. El-Nasr, "A dynamic key distribution protocol for PKI-based VANETs," in *IFIP Wireless Days*, vol. 1, no. 1, oct 2011, pp. 1–3. [Online]. Available: http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6098221

[6] H. Tan, Z. Gui, and I. Chung, "A Secure and Efficient Certificateless Authentication Scheme With Unsupervised Anomaly Detection in VANETs," *IEEE Access*, vol. 6, pp. 74 260–74 276, 2018.

[7] M. Erritali and B. E. Ouahidi, "A review and classification of various VANET Intrusion Detection Systems," in *2013 National Security Days (JNS3)*, apr 2013, pp. 1–6.

[8] L. Anyanwu, J. Keengwe, and G. Arome, "Scalable Intrusion Detection with Recurrent Neural Networks," *Information Technology: New Generations (ITNG), 2010 Seventh International Conference on*, vol. 6, no. 1, pp. 21–28, 2010.

[9] B. Kitchenham and S. Charters, "Guidelines for performing Systematic Literature Reviews in Software Engineering," *Engineering*, vol. 2, p. 1051, 2007.

[10] S. Amara, J. Macedo, F. Bendella, A. Santos, S. Journal, S. Amara, J. Macedo, F. Bendella, and A. Santos, "Group formation in mobile computer supported collaborative learning contexts: a systematic literature review," vol. 19, no. 2, pp. 258–273, 2015.

[11] "Crossref." [Online]. Available: https://www.crossref.org/

[12] "Habanero." [Online]. Available: https://github.com/sckott/habanero

[13] D. Singelee and B. Preneel, "Location verification using secure distance bounding protocols," in *IEEE International Conference on Mobile Adhoc and Sensor Systems Conference, 2005.*, nov 2005, pp. 7 pp.–840.

[14] M. Erritali and B. El Ouahidi, "A review and classification of various VANET Intrusion Detection Systems," *2013 National Security Days - 3eme Edition Des Journees Nationales de Securite, JNS3*, pp. 1–6, 2013.

[15] J. Song, H. Takakura, Y. Okabe, M. Eto, D. Inoue, and K. Nakao, "Statistical analysis of honeypot data and building of Kyoto 2006+ dataset for NIDS evaluation," *Proceedings of the First Workshop on Building Analysis Datasets and Gathering Experience Returns for Security - BADGERS '11*, pp. 29–36, 2011. [Online]. Available: http://portal.acm.org/citation.cfm?doid=1978672.1978676

[16] M. Rummel and M. Rummel, "Der Social Entrepreneurship-Diskurs. Eine Einführung in die Thematik," *Wer sind Social Entrepreneurs in Deutschland?*, no. Cisda, pp. 21–38, 2011.

[17] S. Misra, P. V. Krishna, and K. I. Abraham, "A stochastic learning automata-based solution for intrusion detection in vehicular ad hoc networks," *Security and Communication Networks*, vol. 4, no. 6, pp. 666–677, jun 2011. [Online]. Available: http://doi.wiley.com/10.1002/sec.200

[18] D. Tian, Y. Wang, G. Lu, and G. Yu, "A vehicular ad hoc networks intrusion detection system based on BUSNet," *Proceedings of the 2010 2nd International Conference on Future Computer and Communication, ICFCC 2010*, vol. 1, pp. V1–225–V1–229, 2010.

[19] N. Kumar and N. Chilamkurti, "Collaborative trust aware intelligent intrusion detection in VANETs," *Computers and Electrical Engineering*, vol. 40, no. 6, pp. 1981–1996, 2014. [Online]. Available: http://dx.doi.org/10.1016/j.compeleceng.2014.01.009

[20] X. Liu, G. Yan, D. B. Rawat, and S. Deng, "Data mining intrusion detection in vehicular ad hoc network," *IEICE Transactions on Information and Systems*, vol. E97-D, no. 7, pp. 1719–1726, 2014.

[21] M. N. Mejri and J. Ben-Othman, "Detecting greedy behavior by linear regression and watchdog in vehicular ad hoc networks," *2014 IEEE Global Communications Conference, GLOBECOM 2014*, no. ii, pp. 5032–5037, 2014.

[22] K. M. Alheeti, A. Gruebler, and K. D. McDonald-Maier, "An intrusion detection system against malicious attacks on the communication network of driverless cars," *2015 12th Annual IEEE Consumer Communications and Networking Conference, CCNC 2015*, pp. 916–921, 2015.

[23] K. M. A. Alheeti, A. Gruebler, and K. D. McDonald-Maier, "An Intrusion Detection System against Black Hole Attacks on the Communication Network of Self-Driving Cars," *2015 Sixth International Conference on Emerging Security Technologies (EST)*, pp. 86–91, 2015. [Online]. Available: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=7429276

[24] H. Sedjelmaci and S. M. Senouci, "An accurate and efficient collaborative intrusion detection framework to secure vehicular networks," *Computers and Electrical Engineering*, vol. 43, pp. 33–47, 2015. [Online]. Available: http://dx.doi.org/10.1016/j.compeleceng.2015.02.018

[25] K. M. Ali Alheeti and K. McDonald-Maier, "Hybrid intrusion detection in connected self-driving vehicles," *2016 22nd International Conference on Automation and Computing, ICAC 2016: Tackling the New Challenges in Automation and Computing*, pp. 456–461, 2016.

[26] J. Rupareliya, S. Vithlani, and C. Gohel, "Securing VANET by Preventing Attacker Node Using Watchdog and Bayesian Network Theory," *Procedia Computer Science*, vol. 79, pp. 649–656, 2016. [Online]. Available: http://dx.doi.org/10.1016/j.procs.2016.03.082

[27] K. Ali Alheeti, A. Gruebler, and K. McDonald-Maier, "Intelligent Intrusion Detection of Grey Hole and Rushing Attacks in Self-Driving Vehicular Networks," *Computers*, vol. 5, no. 3, p. 16, 2016.

[28] O. A. Wahab, A. Mourad, H. Otrok, and J. Bentahar, "CEAP: SVM-based intelligent detection model for clustered vehicular ad hoc networks," *Expert Systems with Applications*, vol. 50, pp. 40–54, 2016.

[29] K. M. Alheeti, A. Gruebler, and K. McDonald-Maier, "Using discriminant analysis to detect intrusions in external communication for self-driving vehicles," *Digital Communications and Networks*, vol. 3, no. 3, pp. 180–187, 2017. [Online]. Available: http://dx.doi.org/10.1016/j.dcan.2017.03.001

[30] S. Sharma and A. Kaul, "Hybrid fuzzy multi-criteria decision making based multi cluster head dolphin swarm optimized IDS for VANET," *Vehicular Communications*, vol. 12, pp. 23–38, 2018. [Online]. Available: https://doi.org/10.1016/j.vehcom.2017.12.003

[31] L. Nie, Y. Li, and X. Kong, "Spatio-Temporal Network Traffic Estimation and Anomaly Detection Based on Convolutional Neural Network in Vehicular Ad-Hoc Networks," *IEEE Access*, vol. 6, pp. 40 168–40 176, 2018.

[32] T. Zhang and Q. Zhu, "Distributed Privacy-Preserving Collaborative Intrusion Detection Systems for VANETs," *IEEE Transactions on Signal and Information Processing over Networks*, vol. 4, no. 1, pp. 148–161, 2018.

[33] A. Ayoob, G. Su, and G. Al, "Hierarchical Growing Neural Gas Network (HGNG)-Based Semicooperative Feature Classifier for IDS in Vehicular Ad Hoc Network (VANET)," *Journal of Sensor and Actuator Networks*, vol. 7, no. 3, p. 41, 2018.

[34] J. Liang, J. Chen, Y. Zhu, and R. Yu, "A novel Intrusion Detection System for Vehicular Ad Hoc Networks (VANETs) based on differences of traffic flow and position," *Applied Soft Computing Journal*, vol. 75, pp. 712–727, 2019. [Online]. Available: https://doi.org/10.1016/j.asoc.2018.12.001