Performance Analysis and Comparison of Anomaly-based Intrusion Detection in Vehicular Ad hoc Networks

Erfan A. SHAMS [1], Ali Hakan ULUSOY [2], Ahmet RIZANER [2]

[1] Dept. of Mathematics, Eastern Mediterranean University, Famagusta, North Cyprus, via Mersin 10 Turkey
[2] Dept. of Information Technology, Eastern Mediterranean University, Famagusta, North Cyprus, via Mersin 10 Turkey

{erfan.shams, alihakan.ulusoy, ahmet.rizaner}@emu.edu.tr

Submitted April 20, 2020 / Accepted August 24, 2020

Abstract. *Security and safety applications of Vehicular Ad hoc Networks (VANETs) are developed to improve the traffic flow. While safety applications in VANETs provide warnings and information for the vehicle and other units in the area, malicious behaviors can render this very purpose meaningless. Intrusion Detection Systems (IDSs) are key features for identifying the presence of faulty or malicious behaviors. Support Vector Machine (SVM) is an efficient tool for anomaly detection and it can be employed for intrusion detection based on the metrics of a known attack or normal behavior. Dropping and or delaying network packets are two of the most common variants among other methods in Denial of Service (DoS) attacks. Hence an IDS which can detect both variants can detect similar types of DoS attacks. The result of the study is obtained by designing and implementing an SVM detection module into computer-generated simulation, which depicts a successful outcome in detection of mentioned DoS attack variants.*

Keywords

Vehicular ad hoc networks, support vector machines, denial of service attack, intrusion detection, machine learning

1. Introduction

An essential role of Vehicular Ad hoc Networks (VANETs) is providing critical information regarding the safety of the traffic. These applications use the available wireless network for gathering or sharing vital information from, or to other vehicles, which is known as Vehicle-to-Vehicle (V2V), as well as roadside units that are referred to as Vehicle-to-Infrastructures (V2I). There are both periodic and on-demand messages exchanged with other units in order to keep the application functional. The ability to receive and transmit these messages on time is crucial, especially in case of emergency.

VANET is a subcategory of Mobile Ad hoc Networks (MANETs), specialized for vehicular environments. This means it is inherently benefitting from the flexibility and unique features of MANETs while also suffering mainly from its security issues. On the other hand, vehicular environment brings additionally unique characteristics to the network; predictable movements, almost no restraint in power consumption and more rapid change in the network topology are some examples [1]. The Onboard Unit (OBU) of a VANET node or vehicle utilizes short-range wireless communication using IEEE 802.11p standard, along with suitable routing protocols. The decision for choosing a proper routing algorithm is itself a separate topic, which is debated briefly or thoroughly in various papers [2–4]. Moreover, Ad hoc On Demand Distance Vector (AODV) and other routing protocols that are generally common in MANETs are still viable in VANETs [4].

Wireless networks, unlike their wired counterpart, have the vulnerability of being accessible to any attacker that happens to be in the coverage area. This is a substantial issue in VANETs as well. Although being susceptible to various types of intrusions, having far less power constraint issues means more flexibility in using the computational power of the OBU. This makes room for using machine-learning algorithms such as Support Vector Machine (SVM) more effectively. What makes SVM a suitable choice for this type of intrusion detection is its strong pattern recognition and the ability to transform non-linearly separable data mapped into linearly separable space. SVM is also one of the best methods used in binary classification or anomaly detection. It is also efficient in terms of training and classification time in comparison to methods such as deep learning [5].

Different types of network intrusions carry on different forms and purposes; Denial of Service (DoS) attacks belong to a group of intrusions which target the availability of a network resource by various methods. Two of the commonly used methods in these kinds of attacks are dropping and delaying network packets. However, there are many other variants of DoS attacks such as flooding attack which tries to bottleneck the available network bandwidth of the target with junk data. The combined properties of DoS attacks and VANETs create new challenges for tracking the presence of

such anomalies in the network. The following objectives are the main contribution of this paper:

- We investigated and the required feature space for packet dropping and delaying type DoS attack detection specifically for the receiving end of a VANET connection.
- We used state of the art computer simulation for generating vehicular traffic environment with realistic mobility patterns to generate normal and malicious datasets as well as evaluating the final IDS.
- Using the selected features in the data gathering module of our proposed IDS to train an SVM-based anomaly detection system for VANETs.

After designing and implementing our proposed IDS we compared its performance to other similar methods. The comparison result shows notable improvement over the other classifiers. To establish a robust method against the mentioned type of DoS attacks, we studied the effect of random packet delays and drops in a generic VANET scenario using computer simulation. Afterward, we selected and studied the effect of the most important parameters that we believed are necessary to identify the presence of intruders in the network.

In this study the receiving vehicle examines the packet arrival pattern to detect traces of intrusion in the network. Previously we have studied possibility of intrusion detection on the intermediate vehicles [6], this method, while it is viable puts extra strain in terms of calculation overhead on every packet forwarding vehicles which can be exhaustive in overcrowded situations. Current study is focused on running the intrusion detection task on the target vehicle which in turn reduces the extra resource consumption on the other vehicles. This also means that we require an update for the data gathering module as well as the detection module. The details of the feature selection related to the data gathering module, training of the detection module, and, the simulation environment are explained further in the coming sections.

As we continue, in this paper, we discuss other related works on this issue in Sec. 2, then describe the nature of the problem and both its common and unique specifications in Sec. 3. In Sec. 4, we present the details of the proposed SVM Intrusion Detection Module (IDM) design, followed by its performance analysis in various situations with a comparison to other detection systems in Sec. 5 and finally, in Sec. 6, make our conclusion and discuss future works.

2. Related Work

Security of VANETs is a point of discussion in many computer science journals. Some of the most common security attacks in VANETs are mentioned by Kolandaisamy et al. [7]. Their solution to particularly Distributed DoS (DDoS) attack is to first create a reputation-based system for selecting cluster heads for network routing. Then, the cluster heads will use the proposed Stream Position Performance Analysis to rate the trustworthiness of the data flow coming from other vehicles. Another research by Zhou et al. [8] suggests another reputation-based system using a method called distributed collaborative intrusion detection system of the VANET. This method is an invariant-based anomaly detection that analyzes the behavior of vehicles as well as traffic and communication flow to identify malicious nodes.

A paper by Basant Subba et al. [9] demonstrates an Intrusion Detection System (IDS) based on game theory. The intrusion detection runs in three layers; immediate neighbor level, cluster level, and RSU level. To minimize the network overhead, the researchers used two players non-cooperative game between any two vehicles to detect malicious behavior. The system can detect intrusions with higher accuracy when the number of agents increases in the cluster, however, the false alarm ratio will also increase by introducing more agents. Similarly, Muhammad Mohsin Mehdi et al. [10] proposes a trust model based on game theory for VANETs, which tags nodes as a defender or attacker to determine the safest path available for routing. It shows better performance in a higher density of defender nodes and performs better in longer duration of established connections.

Khattab et al. [11] proposed an intrusion detection for identifying and mitigating DoS attacks in VANET by using discriminant analysis methods. Their proposed system requires fuzzification for pre-processing data to reduce the ambiguity of malicious and non-malicious inputs. Their utilized classifiers are Linear Discriminant Analysis (LDA) and Quadratic Discriminant Analysis (QDA). The researchers obtained high classification ratio with good precision, recall and F-Score. However, the IDS is dependent on a special data pre-processing to be effective.

G. Kumaresan et al. [12], have introduced a group key authentication scheme for security in VANETs by authentication in a cluster-based network. In this scheme, a cluster head acts as an authenticator for the safety of the packets targeting any cluster member. In another paper by Hichem Sedjelmaci et al. [13], which also considers cluster formation, the authors employ collaborative intrusion detection to form a stable cluster with the most trusted node as its head. In another paper, Lee and Jeong proposed a black hole detection method based on mutual authentication scheme in VANET [14]. This method requires authenticating nodes in the area to be effective that makes it more similar to an infrastructure network.

Neeraj Kumar et al. [15] proposed a collaborative trust aware IDS, based on information from the different states of the nodes in the area. The authors used the Markov Chain Model for state transitions and collaborative trust index for generating intrusion alerts. Their system shows about 90% success rate. Gisung Kim et al. proposed a method [16], which uses the C4.5 algorithm for misuse detection to enhance a one-class SVM for pattern recognition. The authors depicted an increase in the performance and reduced time of detection for known attacks, while also noting that the train-

ing and testing time is lower than the conventional methods. Another SVM-based IDS is proposed in [6], which is focused on trust value for every vehicle based on the response from the detection module.

A new approach for intrusion detection in VANET is proposed by Tao Zhang and Quanyan Zhu [17]. In this approach, the authors designed a collaborative intrusion detection system that is also focused on keeping the privacy of the users. The classifiers in this IDS are trained in a decentralized manner to detect malicious vehicles. The authors presented effective methods to minimize the empirical risk related to the privacy of the vehicles in VANET. Data fusion is a process of collecting data from heterogeneous environments, which is a technique used by Uzma Khan et al. [18]. The authors designed an IDS which utilizes information coming from different layers of wireless networks to demonstrate its effectiveness compared to single parameter utilization.

More comprehensive studies of known intrusions in VANET, alongside surveys of different detection methods are available in review articles by various authors [19–24].

3. Problem Definition

To address the main concern of this research in more details, we will be discussing the concept of the problem alongside its characteristics and effects in VANET environments.

Self-organization is one of the main aspects of any ad hoc network and highly depends on routing protocols, which use cooperative path discovery for establishing connections, and VANETs are no exception. This implies that any device with VANET capability can participate in sending, receiving and forwarding data packets in its coverage area. Since ad hoc networks are not moderated by a central infrastructure, as mentioned in the introduction, any malicious or defective network node can affect other nodes in its wireless coverage area. There are varieties of security attacks present in VANET, each targeting a vital functionality of the network. Confidentiality, integrity and availability are three main functionalities which are targeted in DoS attacks [22].

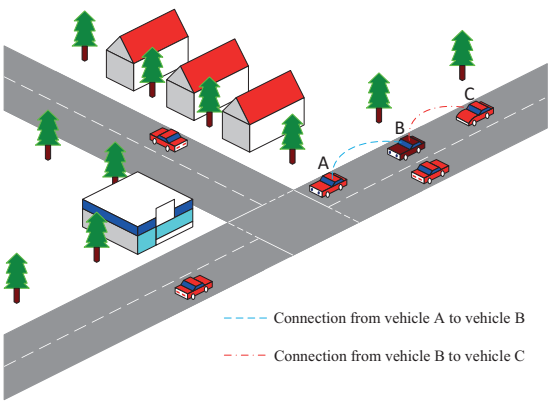

Fig. 1. An arbitrary VANET scenario.

Generally, DoS and Distributed DoS (DDoS) attacks target availability and integrity of the victim. For instance, Jellyfish (JF) attack [25] is a DoS type attack that takes advantage of an ongoing path discovery process in the network to become a Packet Forwarding Node (PFN) and sabotage the connection. For these kinds of attacks, it is important for the malicious node to become part of the packet forwarding route, hence, usually, the attacker is going to perform Rushing Attack [26] in advance to have a higher chance of being selected as a legitimate PFN. When it is selected as a PFN, then one of the three variants of JF attack can be the case here: periodic drop attack, delaying attack and packet reorder attack [25]. Figure 1 illustrates a VANET scenario with a possible malicious node in the area. In this figure, it is assumed that vehicle A is trying to send a message to vehicle C, which is out of its coverage area and needs vehicle B as a PFN. If vehicle B is an attacker, then vehicle C is going to either miss random or all packets from the intended message or receive it with considerable delay. The immediate effect of this type of attack will be reduced packet delivery ratio and increased end-to-end delay. This is a critical issue in VANET when it comes to safety and emergency applications. What makes such types of attacks difficult to detect is their possible periodic behavior, which means at random periods, they are acting exactly as other legitimate nodes. This will help them stay low profile in comparison to attackers that aggressively and consistently affect the performance of a network. Therefore, periodic attackers are able to stay hidden and undetected in various situations.

In this paper, we concentrate on the described types of attack to design an SVM IDM that is able to identify periodic drop and delaying DoS attacks by analyzing the attack pattern on the receiving node. The key to this solution is to find distinctive patterns that appear in presence of an attack, that would help create a well-defined support vector for the best possible classification according to our data inputs. Moreover, since this IDM can detect periodic random packet drops, it can theoretically be able to detect similar types of intrusions that affect packet delivery, such as grey-hole attack [27].

4. SVM Intrusion Detection Module

Any type of IDS generally consists of three different modules, namely, gathering module, detection module and response module [26]. The role of the detection module is identifying the presence of attack and initiating proper alert for the response module. In our proposed IDM, we selected SVM as the classifying algorithm. SVM which is also known as Support Vector Networks has its performance known to be excellent in two-class or binary data classification [28, 29].

4.1 Feature Space

Although SVM is a powerful tool, it is highly dependent on feature selection for the best-drawn support vector. For se-

lecting proper inputs, it is necessary to look at the behavior of the network under attack and in normal state. For instance, in the presence of a malicious node that targets the availability of the network, there are higher number of packet-drops and increased end-to-end delay. Also, for a scenario where the receiving vehicle is analyzing the incoming data, the number of forwarding vehicles between the source and the destination which is known as hop-count can be an additional hint for malicious behavior. It is clear that in a direct communication when the hop-count is defined as 1, there is zero chance of having an attacker that is trying to delay or drop an incoming packet, although more than two hop-counts mean that there are PFNs in between that can potentially be malicious nodes.

Although more features in machine learning methods can help increasing the accuracy of the system, it will also increase the complexity and classification time. Therefore, we started creating our dataset based on the three mentioned features which proved to be enough for our task. All three parameters are calculated as the average value in one second interval, which we used as training data for our SVM IDM by the following procedure.

4.2 The Dataset

We obtained our training and testing dataset by building a computer-generated simulation of the VANET environment. We used a combination of Network Simulator 2 (NS-2) [30], and, MOVE (MObility model generator for VEhicular networks) [31] together with micro-traffic simulator SUMO [32] for simulating the VANET connectivity, and, vehicle mobility in a predefined roadmap respectively. We collected the dataset in real-time during the simulation with the following setup.

Our training scenario involves 10 VANET nodes or vehicles with the configuration that is given in Tab. 1. Only one connection established between two vehicles for normal dataset without attack, and for malicious dataset a single vehicle from the remaining pool selected as the malicious vehicle. The attacker starts its malicious behavior by rushing attack during the path discovery process. This helps the attacker to have a higher chance of being in the packet forwarding route.

Parameters	Values
Simulation Area	1000×1000 m^2
Mac Protocol	IEEE 802.11p
Routing Protocol	AODV
Simulation Time	1000 s
Number of Vehicles	10 / 30 / 50
Vehicle placement / Movement	Random Start / Destination Road (generated by SUMO)
Vehicle Speed	0 Km/h to 50 Km/h
Traffic Model	Constant Bit Rate (CBR)
Traffic Rate	64 Kbps
Packet Size	512 B
Random Noise in CBR	Disabled

Tab. 1. Simulation Parameters (NS-2, SUMO).

Following a successful rushing attack, the malicious vehicle starts to periodically drops or delays the incoming packets. The delays are between 200 milliseconds to 1 second; this enables the attacker to cover its presence and stay indistinct. After running the simulations, we collected the normal and malicious datasets containing the average drop rate, average end-to-end delay, and, average hop-counts. We eliminated the first 200 seconds of simulation to ensure the traffic and data flow are established.

We split the dataset into training and test datasets by choosing the latter to be 25% of the collected pool of 800 samples. This test data is used only for evaluating the trained IDM and is not taken into account for the final evaluation. It is worth noting that the training data may seem small, however, our performance analysis shows that the SVM IDM can generalize the intrusion patterns very well on the collected dataset. We carried out the performance analysis in real-time simulations with 15 different scenarios (see Tab. 2) each of which has 50 different mobility patterns. Hence, a total of 750 simulations are run for the final evaluation.

4.3 Training the SVM IDM

For the SVM itself, like any other machine learning technique requires parameter tuning. The main parameter of an SVM is its kernel, which is the function that finds similarity scores in given data in higher dimensions, or simply as mentioned before, makes the data linearly separable without transforming the data. There are different kernels for SVM and each has its hyperparameter. Another important parameter in SVM is the regularization or penalty parameter (C); this parameter controls the margin of the hyperplane between classes. Higher C parameter helps to classify the training data with more precision, however, it also leads to overfitting. In our study, we trained the network using polynomial and Gaussian kernels with different degrees. The best result obtained by using the polynomial kernel with degree 2 and the regularization parameter (C) set to 100. In each training iteration, the program randomly selects normalized input data from the available training pool until the best result is achieved. After the training is done, the SVM is tested against the test data to see the final result.

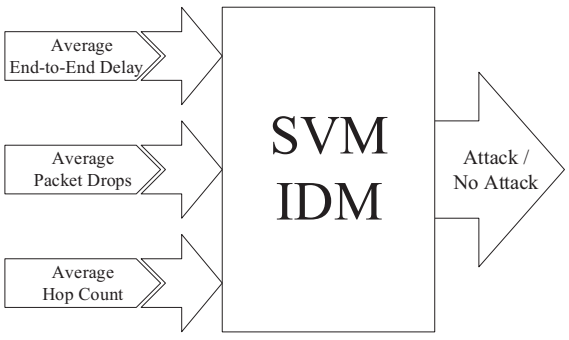

Fig. 2. SVM IDM block diagram.

The training process for a small dataset such as ours is less than a second on a notebook PC with Intel Core i7 7700HK CPU. This allows us to repeat the training with random inputs from the entire pool as many times as needed to get our desired performance which is about 99% on the initial test data. To further test the performance of the obtained SVM, we integrated it into NS-2 for real-time performance analysis in different setups which are presented in Sec. 5. Figure 2 illustrates a simplified diagram of the designed SVM IDM.

5. Performance Analysis

To evaluate the functionality of our proposed SVM detection module, we prepared different scenarios, which carried out with the same tools that are mentioned in the previous section. The malicious vehicle does periodic drops and delays from 200 milliseconds to 1 second randomly. The performance is measured in terms of average Precision (PR), Recall (RC) and Matthew's Correlation Coefficient (MCC) [33] for general binary classification measurements. During the classification process, the IDM either detects the presence of attack correctly, known as True Positive (TP) or sends a false alarm out when there is actually no intrusion which is known as False Positive (FP). In normal situations when there is no intrusion, the system should not trigger any alarm, known as True Negative (TN), hence, any other negative output where there is an active intrusion in the network is considered to be False Negative (FN). The mentioned performance measures are calculated as shown in (1), (2) and (3):

$$PR = \frac{TP}{TP + FP}, \tag{1}$$

$$RC = \frac{TP}{TP + FN}, \tag{2}$$

$$MCC = \frac{TP \times TN - FP \times FN}{\sqrt{(TP + FN)(TP + FP)(TN + FP)(TN + FN)}}. \tag{3}$$

The remaining performance metrics are Detection Rate (DR) and False Alarm Rate (FAR) which are more important for evaluating performance of intrusion detection in general, and are calculated as shown below in (4) and (5):

$$DR = \frac{TN}{TN + FP}, \tag{4}$$

$$FAR = \frac{FN}{FN + TP}. \tag{5}$$

Additionally, to compare the result of our proposed system, we performed a separate simulation to depict the performance comparison between our proposed system and other available methods in the same environment.

The average measure is obtained by evaluating SVM output in every one second for the entire duration of the simulation. We repeated every setup 50 times with each having different vehicle traffic flow on the roads of the same map. We decided to use a generic setup for the network simulation parameters which are more commonly used in other similar studies. A complete list of configurations is available in Tab. 1. In general, we designed three main scenarios with different number of vehicles: 10, 30 and 50. Each of these scenarios have five different setups with a varying number of attackers. The number of malicious vehicles changes from one to five, which are distributed randomly in the map. An extra scenario with 30 vehicles and 6 RSUs are used to compare our proposed IDM with the LDA and QDA detection systems proposed by Alheeti et al. [11].

As mentioned in Sec. 3, each of the attacking vehicles need to have a chance to be in the packet forwarding route to be able to affect the transmission. For instance, in a scenario with five malicious vehicles, when there is an ongoing attack during the data transfer, it can be the effect of one or up to five, attackers present in packet forwarding. When there is such a condition, with one or more malicious vehicles affecting the transmission, we expect positive output from our proposed SVM IDM.

Apparently, due to the random mobility of VANET nodes in the area, there are times when the two communicating vehicles are within range of each other and do not need any PFN in between; or times when there are no malicious vehicles in the area to fit into the routing table. In these cases, there is no attack and therefore the output of the SVM IDM should be negative. Therefore, in every simulation run, there are both cases of the network being under attack or performing normally.

The obtained average attack uptime in every setup is shown in Tab. 2. As it is depicted, with an increase in the number of vehicles, the average attack uptime decreases from 344 seconds for 10 vehicles to 271 seconds for 30 vehicles and 247 seconds for 50 vehicles. It is due to the larger proportion of the number of malicious vehicles to normal vehicles, therefore, attackers have a better chance of affecting the network, hence increasing the average attack uptime. In addition, the increase in the number of attackers in every category with a different number of vehicles, increases the average attack uptime by letting malicious vehicles to have a greater chance to be in the transmission area.

For analyzing the classification performance of our SVM IDM, the proposed module takes normalized data in every second and uses it as the input for the module. We have the average results for PR, RC, and MCC from different scenarios presented in Tab. 3. As it is visible, the average PR and RC for all setups are depicting an excellent performance above 99 %, with the only exception being the average PR of 50 vehicles. MCC on average is observed to be close to 1, which means the classification results are consistent. The average PR and RC values are around 98 to 99 % for the

Number of Vehicles	Number of Attackers					Average
	1	2	3	4	5	
10	228.18	324.20	360.26	390.62	415.9	343.83
30	165.78	260.08	291.04	315.54	325.1	271.51
50	145.86	241.02	262.42	283.48	304.1	247.38

Tab. 2. Average time (seconds) of JF nodes actively affecting the network in 1000 seconds simulations.

different number of vehicles. This shows that the SVM IDM is scarcely affected by the number of vehicles in our study. In term of the number of attackers in the simulation area, with respect to the number of vehicles, the changes in both PR and RC stay very much the same. Although it can be seen that in presence of only one attacker in the system, PR and RC are marginally lower than the other number of attackers. All of the values are again between 98 % to slightly below 100 %.

The results for DR and FAR calculations are available in Tab. 4. By looking at the average DR in the table, it is apparent that the proposed IDM can precisely identify the intruders with 99 % success rate. False alarm found to be as low as under 1 %. This will greatly reduce the chance of identifying genuine VANET nodes as intruders and ensures their availability for consistent network packet routing.

To conclude the performance analysis, we compared the SVM IDM to QDA and LDA methods to observe the performance of detecting malicious vehicles with network packet dropping behavior under different detection systems. Figure 3 and Figure 4 provide the results of the comparison between the mentioned systems. The performance measures are in terms of DR, PR, and F-Score (6); the latter measure is also known as F-Measure or the harmonic mean of PR and RC.

$$\text{F-Score} = 2\frac{PR \times RC}{PR + RC}. \tag{6}$$

We can observe that the proposed SVM IDM method with the select features can detect malicious vehicles much more efficiently than the other two methods. It is followed by LDA which provides better performance compared to the more similar method, namely QDA. All of the mentioned methods present PR above 90 % which means FP ratio is low.

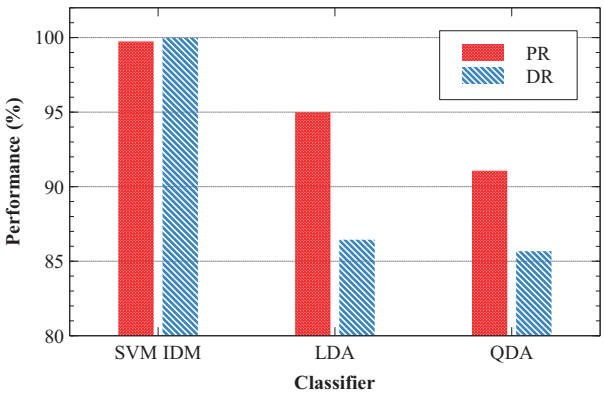

Fig. 3. PR and DR performance comparison between SVM IDM, LDA and QDA.

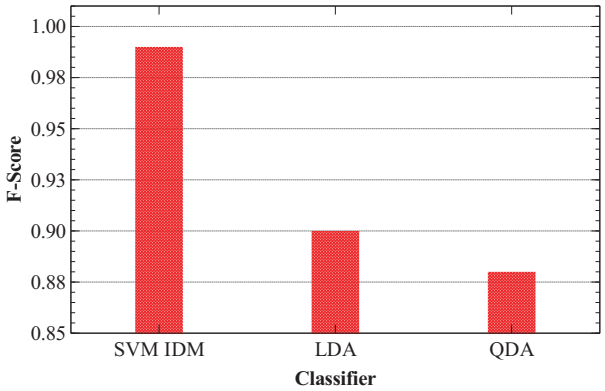

Fig. 4. F-Score performance comparison between SVM IDM, LDA and QDA.

In terms of F-Score, SVM IDM and LDA provide scores more or equal to 0.9; and in the case of DR, only the SVM IDM has a score above 90 %.

Another important issue when comparing classification tools is computational complexity. As mentioned before, SVM is highly efficient in terms of both training and prediction or classification time. In terms of Big-O notation, the training time has the time complexity of $O(n \times m^2 + m^3)$ in the worst case, and, $O(s \times n)$ for the classification time, where m is the number of samples, n is the number of features, and, s is the number of support vectors [34]. LDA has similar time complexity which is $O(m \times n^2 + n^3)$ for training when $n < m$ [35], and, $O(n)$ for prediction. The computational complexity of QDA is similar to LDA, however, it is less efficient when the feature count is high. Hence, in terms of computational efficiency all mentioned algorithms are relatively lightweight and for a small dataset with small feature space similar to this research the difference is negligible.

6. Conclusions and Future Works

A delayed or dropped message in critical situations is a potential accident in VANET environments. Safety applications in VANETs can become much more efficient if the OBU is able to identify the presence of such malicious behaviors in the network and isolate the culprit. SVM is a potent machine-learning tool with suitable classification abilities and low resource consumption. In this paper, we used a polynomial kernel of degree 2 for training our SVM IDM for packet dropping and delaying DoS attack detection in the VANET environment. The proposed system is then verified by implementing the SVM IDM in the receiving VANET node, which examines the average number of packet

Number of Vehicles		Number of Attackers					Average
		1	2	3	4	5	
10	PR (%)	99.76	99.73	99.75	99.77	99.74	99.75
	RC (%)	99.00	99.12	99.25	99.20	99.20	99.15
	MCC	0.9920	0.9915	0.9922	0.9916	0.9909	0.99
30	PR (%)	99.14	99.34	99.37	99.47	99.29	99.32
	RC (%)	98.91	99.14	99.15	99.11	99.11	99.09
	MCC	0.9883	0.9897	0.9896	0.9896	0.9881	0.99
50	PR (%)	98.27	99.15	99.03	99.12	99.24	98.96
	RC (%)	98.89	99.25	99.15	99.30	99.34	99.19
	MCC	0.9834	0.9895	0.9877	0.9890	0.9898	0.99

Tab. 3. Performance of SVM IDM in terms of PR, RC and MCC.

Number of Vehicles		Number of Attackers					Average
		1	2	3	4	5	
10	DR (%)	99.93	99.87	99.86	99.86	99.82	99.87
	FAR (%)	1.00	0.88	0.75	0.80	0.80	0.85
30	DR (%)	99.83	99.77	99.74	99.75	99.66	99.75
	FAR (%)	1.09	0.86	0.85	0.89	0.89	0.91
50	DR (%)	99.70	99.73	99.66	99.65	99.67	99.68
	FAR (%)	1.11	0.75	0.85	0.70	0.66	0.81

Tab. 4. Performance of SVM IDM in terms of DR and FAR.

drops, end-to-end delay, and hop-counts in every one second interval to identify the possible intrusion. We observed that in every different VANET scenario the system is able to classify the presence or absence of DoS attackers with high PR and RC, averaging to 99 %. MCC is also very close to 1, which means our trained SVM is very consistent with the classification. Furthermore, the detection module has a low FAR to prevent harming the availability of the network by false alarms and potentially eliminating genuine VANET nodes. To further evaluate the performance of the SVM IDM, we compared the proposed system with QDA and LDA methods. This comparison depicted a better performance in comparison to the other two methods in every criterion. This proves a simple SVM with proper features and parameters can be an effective tool as the core of the detection module in an intrusion detection system. In our future works on VANET security, we plan to expand our research to create an IDS which is effective against more varieties of security attacks in VANET.

References

[1] AL-SULTAN, S., AL-DOORI, M. M., AL-BAYATTI, A. H., et al. A comprehensive survey on vehicular ad hoc network. *Journal of Network and Computer Applications*, 2014, vol. 37, no. 1, p. 380–392. DOI: 10.1016/j.jnca.2013.02.036

[2] LI, F., WANG, Y. Routing in vehicular ad hoc networks: a survey. *IEEE Vehicular Technology Magazine*, 2007, vol. 2, no. 2, p. 12–22. DOI: 10.1109/MVT.2007.912927

[3] EZE, E. C., ZHANG, S., LIU, E. Vehicular ad hoc networks (VANETs): current state, challenges, potentials and way forward. In *ICAC 2014 - Proceedings of the 20th International Conference on Automation and Computing: Future Automation, Computing and Manufacturing*. Cranfield (UK), 2014, p. 176–181. DOI: 10.1109/IConAC.2014.6935482

[4] UR-REHMAN, S., KHAN, M. A., ZIA, T. A., et al. Vehicular ad-hoc networks (VANETs)-an overview and challenges. *Journal of Wireless Networking and Communications*, 2013, vol. 3, no. 3, p. 29–38. DOI: 10.5923/j.jwnc.20130303.02

[5] LIU, P., CHOO, K. K. R., WANG, L., et al. SVM or deep learning? A comparative study on remote sensing image classification. *Soft Computing*, 2017, vol. 21, no. 23, p. 7053–7065. DOI: 10.1007/s00500-016-2247-2

[6] SHAMS, E. A., RIZANER, A., ULUSOY, A. H. Trust aware support vector machine intrusion detection and prevention system in vehicular ad hoc networks. *Computers and Security*, Sep. 2018, vol. 78, p. 245–254. DOI: 10.1016/j.cose.2018.06.008

[7] KOLANDAISAMY, R., NOOR, R. M., KOLANDAISAMY, I., et al. A stream position performance analysis model based on DDoS attack detection for cluster-based routing in VANET. *Journal of Ambient Intelligence and Humanized Computing*, 2020. DOI: 10.1007/s12652-020-02279-2

[8] ZHOU, M., HAN, L., LU, H., et al. Distributed collaborative intrusion detection system for vehicular ad hoc networks based on invariant. *Computer Networks*, 2020, vol. 172, p. 1–14. DOI: 10.1016/j.comnet.2020.107174

[9] SUBBA, B., BISWAS, S., KARMAKAR, S. A game theory based multi layered intrusion detection framework for wireless sensor networks. *International Journal of Wireless Information Networks*, 2018, vol. 25, no. 4, p. 399–421. DOI: 10.1007/s10776-018-0403-6

[10] MEHDI, M. M., RAZA, I., HUSSAIN, S. A. A game theory based trust model for vehicular ad hoc networks (VANETs). *Computer Networks*, 2017, vol. 121, p. 152–172. DOI: 10.1016/j.comnet.2017.04.024

[11] ALHEETI, K. M. A., GRUEBLER, A., MCDONALD-MAIER, K. Using discriminant analysis to detect intrusions in external communication for self-driving vehicles. *Digital Communications and Networks*, 2017, vol. 3, no. 3, p. 180–187. DOI: 10.1016/j.dcan.2017.03.001

[12] KUMARESAN, G., ADILINE MACRIGA, T. Group key authentication scheme for vanet intrusion detection (GKAVIN). *Wireless Networks*, 2017, vol. 23, no. 3, p. 935–945. DOI: 10.1007/s11276-016-1197-z

[13] SEDJELMACI, H., SENOUCI, S. M. An accurate and efficient collaborative intrusion detection framework to secure vehicular networks. *Computers and Electrical Engineering*, 2015, vol. 43, p. 33–47. DOI: 10.1016/j.compeleceng.2015.02.018

[14] LEE, B. K., JEONG, E. H. A black hole detection protocol design based on a mutual authentication scheme on VANET. *KSII Transactions on Internet and Information Systems*, 2016, vol. 10, no. 3, p. 1467-1480. DOI: 10.3837/tiis.2016.03.032

[15] KUMAR, N., CHILAMKURTI, N. Collaborative trust aware intelligent intrusion detection in VANETs. *Computers and Electrical Engineering*, 2014, vol. 40, no. 6, p. 1981–1996. DOI: 10.1016/j.compeleceng.2014.01.009

[16] KIM, G., LEE, S., KIM, S. A novel hybrid intrusion detection method integrating anomaly detection with misuse detection. *Expert Systems with Applications*, 2014, vol. 41, no. 4, p. 1690–1700. DOI: 10.1016/j.eswa.2013.08.066

[17] ZHANG, T., ZHU, Q. Distributed privacy-preserving collaborative intrusion detection systems for VANETs. *IEEE Transactions on Signal and Information Processing over Networks*, 2018, vol. 4, no. 1, p. 148–161. DOI: 10.1109/TSIPN.2018.2801622

[18] KYRIAKOPOULOS, K. G., APARICIO-NAVARRO, F. J., PARISH, D. J. Manual and automatic assigned thresholds in multilayer data fusion intrusion detection system for 802.11 attacks. *IET Information Security*, 2014, vol. 8, no. 1, p. 42–50. DOI: 10.1049/iet-ifs.2012.0302

[19] KHAN, U., AGRAWAL, S., SILAKARI, S. Detection of malicious nodes (DMN) in vehicular ad-hoc networks. *Procedia Computer Science*, 2015, vol. 46, p. 965–972. DOI: 10.1016/j.procs.2015.01.006

[20] HORTELANO, J., RUIZ, J. C., MANZONI, P. Evaluating the usefulness of watchdogs for intrusion detection in VANETs. In *2010 IEEE International Conference on Communications Workshops, ICC 2010*. Capetown (SA), 2010, p. 1–5. DOI: 10.1109/ICCW.2010.5503946

[21] RAJKUMAR, M. N., NITHYA, M., HEMALATHA, P. *Overview of VANET with Its Feature and Security Attacks*. 6 pages. [Online] Cited 2020-03-23. Available at: https://www.irjet.net/archives/V3/i1/IRJET-V3I124.pdf

[22] HOA LA, V., CAVALLI, A. Security attacks and solutions in vehicular ad hoc networks: a survey. *International Journal on Ad Hoc Networking Systems*, 2014, vol. 4, no. 2, p. 1–20. DOI: 10.5121/ijans.2014.4201

[23] SHARMA, S., KAUL, A. A survey on intrusion detection systems and honeypot based proactive security mechanisms in VANETs and VANET cloud. *Vehicular Communications*, 2018, vol. 12, p. 138–164. DOI: 10.1016/j.vehcom.2018.04.005

[24] MALHI, A. K., BATRA, S., PANNU, H. S. Security of vehicular ad-hoc networks: a comprehensive survey. *Computers and Security*, 2020, vol. 89, p. 1–30. DOI: 10.1016/j.cose.2019.101664

[25] KAUR, S., KAUR, R., VERMA, A. K. Jellyfish attack in MANETs: a review. In *Proceedings of 2015 IEEE International Conference on Electrical, Computer and Communication Technologies, ICECCT 2015*. Coimbatore (India), 2015, p. 1–5. DOI: 10.1109/ICECCT.2015.7226168

[26] SHAMS, E. A., RIZANER, A. A novel support vector machine based intrusion detection system for mobile ad hoc networks. *Wireless Networks*, 2018, vol. 24, no. 5, p. 1821–1829. DOI: 10.1007/s11276-016-1439-0

[27] TYAGI, P., DEMBLA, D. Investigating the security threats in vehicular ad hoc networks (VANETs): towards security engineering for safer on-road transportation. In *Proceedings of the 2014 International Conference on Advances in Computing, Communications and Informatics, ICACCI 2014*. New Delhi (India), 2014, p. 2084–2090. DOI: 10.1109/ICACCI.2014.6968313

[28] CORTES, C., VAPNIK, V. Support-vector networks. *Machine Learning*, Sep. 1995, vol. 20, no. 3, p. 273–297. DOI: 10.1007/bf00994018

[29] PENG, S., HU, Q., CHEN, Y., et al. Improved support vector machine algorithm for heterogeneous data. *Pattern Recognition*, 2015, vol. 48, no. 6, p. 2072–2083. DOI: 10.1016/j.patcog.2014.12.015.

[30] *The Network Simulator 2 - ns-2*. [Online] Cited 2020-03-24. Available at: http://www.isi.edu/nsnam/ns/

[31] KARNADI, F. K., MO, Z. H., LAN, K. C. Rapid generation of realistic mobility models for VANET. In *IEEE Wireless Communications and Networking Conference, WCNC*. Kowloon (China), 2007, p. 2508–2513. DOI: 10.1109/WCNC.2007.467

[32] KRAJZEWICZ, D., ERDMANN, J., BEHRISCH, M., et al. *Recent Development and Applications of SUMO - Simulation of Urban Mobility*. 10 pages. [Online] Cited 2020-03-26. Available at: http://elib.dlr.de/80483/

[33] MATTHEWS, B. W. Comparison of the predicted and observed secondary structure of t4 phage lysozyme. *BBA - Protein Structure*, 1975, vol. 405, no. 2, p. 442–451. DOI: 10.1016/0005-2795(75)90109-9

[34] CLAESEN, M., DE SMET, F., SUYKENS, J. A. K., et al. *Fast Prediction with SVM Models Containing RBF Kernels*. [Online] Cited 2020-03-26. Available at: http://arxiv.org/abs/1403.0736

[35] CAI, D., HE, X., HAN, J. Training linear discriminant analysis in linear time. In *Proceedings - International Conference on Data Engineering*, 2008, p. 209–217. DOI: 10.1109/ICDE.2008.4497429

About the Authors . . .

Erfan A. SHAMS received B.S. degree in Agriculture Engineering from Hormozgan University, Bandar-Abbas, Iran, in 2009 and the M.S. degree in Information Technology from Eastern Mediterranean University (EMU), Famagusta, North Cyprus, in 2015. He is currently a Ph.D. candidate in Applied Mathematics and Computer Science at EMU. His research interest includes security and machine learning in wireless and vehicular ad hoc networks, studying under the supervision of Professor Ahmet Rizaner and Professor Ali Hakan Ulusoy.

Ali Hakan ULUSOY was born in Eskisehir, Turkey, on June 3, 1974. He graduated from the double major program of the Department of Electrical and Electronic Engineering (EEE) and Department of Physics in Eastern Mediterranean University (EMU), Famagusta, North Cyprus in 1996. He received his M.S. and Ph.D. degrees in EEE in EMU in 1998 and 2004, respectively. He joined Information Technology Department, EMU, in 2004. His current research interests include wireless communications, receiver design, channel estimation, fuzzy systems, wireless networks, cloud computing, and millimeter wave communications.

Ahmet RİZANER received the B.S., M.S. and Ph.D. degrees in Electrical and Electronics Engineering from the Eastern Mediterranean University (EMU), Famagusta, North Cyprus, in 1996, 1998 and 2004, respectively. He joined the Department of Information Technology, EMU, in 2004. His main research interests include wireless communication, adaptive channel estimation, fuzzy channel estimation, multiuser detection techniques, digital video broadcasting, millimeter Wave communication and intrusion detection in mobile ad hoc networks.