Support Vector Machine (SVM) Based Sybil Attack Detection in Vehicular Networks

Pengwenlong Gu, Rida Khatoun, Youcef Begriche, Ahmed Serhrouchni
LTCI, CNRS, TELECOM ParisTech, Université Paris-Saclay, 75013, Paris, France

***Abstract*—Vehicular networks have been drawing special attention in recent years, due to its importance in enhancing driving experience and improving road safety in future smart city. In past few years, several security services, based on cryptography, PKI and pseudonymous, have been standardized by IEEE and ETSI. However, vehicular networks are still vulnerable to various attacks, especially Sybil attack. In this paper, a Support Vector Machine (SVM) based Sybil attack detection method is proposed. We present three SVM kernel functions based classifiers to distinguish the malicious nodes from benign ones via evaluating the variance in their Driving Pattern Matrices (DPMs). The effectiveness of our proposed solution is evaluated through extensive simulations based on SUMO simulator and MATLAB. The results show that the proposed detection method can achieve a high detection rate with low error rate even under a dynamic traffic environment.**

***Index Terms*—Vehicular Networking, Machine Learning, Sybil Attack, Vehicle Driving Pattern, Intrusion detection.**

I. Introduction

The integration of motor vehicles and information technology has become increasingly popular with the evolution of roadway safety and efficiency requirements. Specifically, vehicular networks could have diverse applications associated with safety, traffic grid efficiency, and infotainment [1]. Since driving safety is relevant with most vehicular applications, it is of high importance to implement appropriate security mechanisms. Due to its dynamic and infrastructure-independent nature, vehicular networks are vulnerable to various attacks compared to conventional networks. In order to ensure the safety and security in vehicular networks, security mechanisms have been proposed over the past few years and several of them are standardized by IEEE [2] and ETSI [3].

In general, the proposed security services are based on three major mechanisms: Encryption algorithms, Public Key Infrastructure (PKI) and Pseudonymous. These services can protect the privacy of ITS stations, the authenticity and integrity of messages in vehicular communication environments. However, vehicular networks are still vulnerable to Sybil attacks. Sybil attacks happen when different pseudonyms are used by one malicious node at the same time. Each pseudonym acts as a vehicle in communicating with other ITS stations.

In vehicular networks, Sybil attacks can cause damage in both Networking layer and Application layer. Since the CSMA/CA is implemented in Networking layer, the cooperation among virtual nodes leads to the possibility of using more channel resource than other benign nodes. In Application layer, the virtual nodes also take part in communicating with other ITS stations. Under this circumstance, when a malicious node uses multiple pseudonyms at the same time, the virtual nodes, generated based on the usage of pseudonymous, can help to increase the influence of fake safety messages by broadcasting them to other benign nodes. In addition, several proposed driving safety and traffic efficiency services are based on voting scheme [4]. With the help of virtual nodes, the malicious node can easily take advantage in voting.

Machine learning is a process in which a set of threshold parameters is trained to classify an unknown behaviour [5]. Support Vector Machine (SVM) [6], [7] is a classification and regression prediction tool that uses machine learning theory to maximize predictive accuracy. It leverages a flexible representation of the class boundaries and implements automatic complexity control to reduce overfitting [8]. Furthermore, it often has good generalization performance and the same algorithm solves a variety of problems with little tuning, which makes SVM suitable for dynamic environment [9].

In this paper, we measure vehicles' driving patterns in near capacity road traffic situations, and consider the possibility to detect Sybil attacks based on the variation of their driving patterns.The main idea is to evaluate the similarity of vehicle driving patterns, then use SVM classifiers to distinguish the malicious nodes from the benign ones. The major contributions of this work are listed as follows:

- Relying on beacon information, we designed a data format - Driving Pattern Matrix (DPM) - to describe vehicle driving pattern within a time period.
- Using Machine Learning techniques, we extended the detection method into more dynamic environment.

The remainder of this paper is organized as follows. Section II is literature review on the studies that have been done on the Sybil attack detection in wireless environments especially in vehicular networks. Then attack model of Sybil nodes is defined in Section III. In Section IV, our vehicle driving pattern similarity measurement method is introduced. The simulation results and conclusion are presented in Section V and Section VI, respectively.

II. Related Work

The Sybil attack was firstly mentioned in the year of 2002. In [10] Douceur mentioned that in peer-to-peer system [11] with no logically central, trusted authority to vouch for a one-to-one correspondence between entity and identity, it is possible for an unfamiliar entity to present more than one identity. The proposed Sybil detection methods can be divided into

978-1-5090-4183-1/17/$31.00 ©2017 IEEE

secure key based methods, resource testing based methods, reputation based methods and position based methods.

a) Secure Key-based Techniques: The secure key-based techniques rely on using trusted certification in order to establish trust between entities. Several works based on wireless sensor networks [12], mobile ad-hoc [13] networks and also in vehicular networks [14] have been published in past a few years. This type of system needs a trusted third party or a centralized authority. The authority only provides valid keys to the honest nodes. However, the main drawbacks of this type solution are: firstly, the generation and management of a huge number of keys is costly. Therefore, it may cause a performance bottleneck in large-scale systems; secondly, it is hard to construct an central authority, which can be trusted by all participants. Furthermore, in vehicular scenarios, malicious nodes can easily get several legal identities (e.g., Pseudonymous), then the trusted certification based prevention methods would not work in this case.

b) Resource Testing-based Techniques: The goal of resource testing is to attempt to determine if a number of identities possess fewer resources than would be expected if they were independent [12]. One example in wireless environment is the collision rate in MAC layer. In 802.11 wireless networks, CSMA/CA is used as multiple access method. The transmitters retransmit data after a back off prior when collision occurred in transmission channel. In this case, one hypothesis is that due to the cooperativeness among the Sybil identities configured on the same physical device, the local collision rate would be lower than in normal cases. However, one of the main drawbacks is that this abnormal state can be easily discovered by the monitoring system using some statistical methods, but the Sybil identities cannot be distinguished from normal users.

c) Reputation System: In recent years, reputation systems have received a significant amount of attention as a solution for mitigating the affects of malicious nodes in peer-to-peer systems and also in ad-hoc networks or Online Social Networks(OSN). In [15], the reputation functions have been evaluated into symmetric and asymmetric function. The results show that symmetric functions cannot distinguish normal users from malicious while nodes can improve their own reputation score. And asymmetric functions employs the notion of transitive trust, which force malicious nodes to build up trust before launching attacks. However, based on the permitted services in vehicular networks, like the traffic condition announcement service, malicious nodes only need to launch the attack during rush hour in order to maximize the profit that is earned by obstructing some vehicles from their paths. In this case, they still have time to get good reputations.

d) Position Verification: In ad-hoc networks, position verification is considered as a promising approach for the detection of Sybil attacks in recent years. In this approach, networks verify the physical position of each node. The Sybil nodes are expected to be detected by using this approach because they are at the same position where the malicious node generates them.

Several methods have been proposed in the past few years. Most of them are based on the beaconing mechanism in vehicular communication. In [16]–[18], vehicles estimate the position of their neighbours based on the Received Signal Strength Indication (RSSI), compare it with the geographic position they claimed in beacons and calculate the mean square error. If the mean square error is greater than a threshold, the transmitter is considered as a Sybil node. In [19], the detection is improved by using multiple node observers in order to get better detection rate. And in [20] the detection system is developed based on an information-thoeretic framework. Some base stations are implemented in this method and the Received Signal Strength are collected by the base stations.

As we have seen above, position verification relies on witness and verification by the neighbour nodes. In this case, every node is required to estimate neighbours' position by using RSSI or other information, and compare it with the position that neighbours announced. However, this type of methods are costly while the traffic density is high, and the motivation of users is also questionable.

In [21] a footprint detection scheme is proposed which can reconstruct the trajectory of a vehicle based on the signed message it received from different RSUs it passes by. And in [22] Rabieh *et al.* also proposed a scheme to detect virtual nodes based on their claimed location. A challenge packet is sent to the vehicle's claimed location by using directional antenna from RSUs. The exist Sybil attacks detection methods are briefly presented in Table I.

III. Attack Model

While one vehicle is using several pseudonyms together during the same time period, each pseudonym is an individual vehicle in the view of other ITS stations (include OBUs and RSUs) because each valid pseudonym has its own key pair for signing. Based on the analysis of defending methods and messages implemented, we can confirm that it is possible for one vehicle to use different pseudonyms together during the same time period to launch Sybil attacks.

Sybil attacks in vehicular communication environment can be summarized in two procedures in general: virtual nodes generation procedure and launch attack procedure. Based on the standards of ETSI [23] [24], Cooperative Awareness Messages (CAMs) can be used in virtual nodes generation procedure in order to make the virtual nodes known by other ITS stations. The launch attack procedure relies on using Decentralized Environmental Notification Message (DENM)s to report fake road traffic condition to the RSU.

For attack strategy [25], malicious nodes can be divided into rational and irrational attackers based on their profiles. Rational attackers have a specific target and irrational ones do not seek a specific outcome. In the scenarios that we describe, only rational attackers are being taken into consideration since they are more dangerous and more predictable. One assumption is that the rational Sybil attackers only launch attacks when traffic density is high. They report fake traffic condition information with the help of virtual nodes created by themselves, in order to mislead other ITS stations into

TABLE I: SYBIL ATTACKS DETECTION METHODS

Method	References	Advantage	Disadvantage
Secure Key-based	[12]–[14]	Can prevent the generation of fake identities	The generation and management of a huge number of keys is costly and it is hard to construct an central authority, which can be trusted by all participants
Resource Testing-based	[12]	No add extra overhead	Sybil identities can be hardly distinguished and located
Reputation System	[15]	Low extra overhead and low error rate	Malicious nodes can still get good reputations if the attack period is only a small percentage of time
Position Verification	[16]–[20]	High detection rate	The location estimation based on RSSI is not accurate enough

making wrong decisions. In this way, the traffic density would be potentially decreased after the next intersection, and the attackers can reduce their travel time.

In [26], Hao *et al.* proposed two Sybil attack strategies: "Regular Attack"and "Smarter Attack". In Regular Attacks, malicious node broadcasts beacons for the virtual vehicles using the regular power. In Smarter Attacks, malicious node may reduce his communication range to make the virtual vehicles' behaviour looks reasonable. We only consider the V2I communication, therefore, regular attack strategy is chosen.

In this work, only rational attackers are taken into consideration, who launches the attacks in Near-capacity conditions (26-42 vehicles per kilometre [27]). Malicious nodes' strategy depends the received CAMs, calculating the reasonable location for virtual nodes in next time slot, then forging CAMs for the virtual nodes and broadcast them.

IV. Driving Pattern Evaluation

As mentioned above, we hypothesized that when the traffic density is high, the similarity of vehicle driving pattern would be obvious. In this section, we present a method that mainly represent vehicles' driving patterns by using eigenvalues of their driving pattern matrix and the classification procedure based on several SVM classifiers. A brief description of the proposed algorithm is illustrated in Fig. 1.

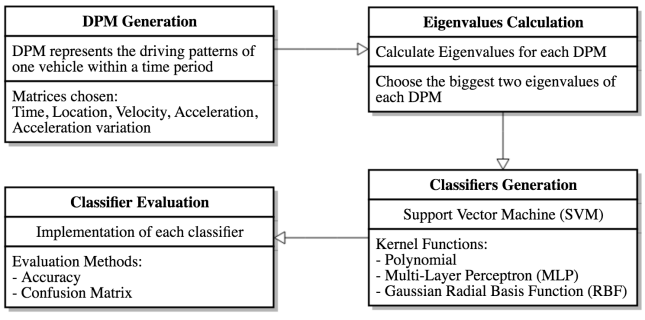


Fig. 1: Diagram of the proposed algorithm

A. Vehicle Driving Pattern Description

In our method, we use the Driving Pattern Matrix (DPM) to describe vehicles' driving patterns within a time period and the similarity measurement is based on the right eigenvectors of their DPM. The driving pattern of a vehicle at certain time is described by using a five elements vector. For example, $\vec{V_1} = (x_{11}, x_{12}, x_{13}, x_{14}, x_{15})$ represents the driving pattern of a vehicle at time t_1. Where

- x_{11} represents time at time t_1
- x_{12} represents location of vehicle at time t_1
- x_{13} represents velocity of vehicle at time t_1
- x_{14} represents acceleration of vehicle at time t_1
- x_{15} represents vehicle's acceleration variation at time t_1

Therefore, the DPM of a vehicle within time period (t_1, t_n) can be represented as:

$$A = \begin{bmatrix} x_{11} & x_{12} & x_{13} & x_{14} & x_{15} \\ x_{21} & x_{22} & x_{23} & x_{24} & x_{25} \\ x_{31} & x_{32} & x_{33} & x_{34} & x_{35} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ x_{n1} & x_{n2} & x_{n3} & x_{n4} & x_{n5} \end{bmatrix} \quad (1)$$

B. Reference Matrix

An symmetric matrix A has an eigenvector $\vec{x}$ and corresponding eigenvalue λ if:

$$A \cdot \vec{x} = \lambda \cdot \vec{x} \quad (2)$$

In our scenarios, for the DPM V_i of each vehicle v_i within time period (t_1, t_n), we construct matrix $V_i^T \cdot V_i$, where exists:

$$(V_i^T \cdot V_i)^T = V_i^T \cdot (V_i^T)^T = V_i^T \cdot V_i \quad (3)$$

The matrix $V_i^T \cdot V_i$ is symmetric, and there exists an orthogonal matrix C has:

$$C^{-1}(V_i^T \cdot V_i)C = C^T(V_i^T \cdot V_i)C = diag(\lambda_{i1}, \lambda_{i2}, \lambda_{i3}, \lambda_{i4}, \lambda_{i5}) \quad (4)$$

where $(V_i^T \cdot V_i)u_j = \lambda_{ij}u_j (1 \leq j \leq 5)$. $\lambda_{ij}(respu_{ij})$ are the eigenvalue (resp eigenvector) of matrix $V_i^T \cdot V_i$.

C. Classification

Due to the reality that the eigenvalues decrease quickly, we can sort them in decrease order and take the top k $(k < 5)$ instead of all 5 eigenvalues to represent the characteristics of the original DPM in classification. In this work, the two biggest eigenvalues are chosen. We note $\lambda_{i1}^{ma} = max\{\lambda_{i1}, \lambda_{i2}, \lambda_{i3}, \lambda_{i4}, \lambda_{i5}\}$ and $\lambda_{i2}^{ma} = max\{\{\lambda_{i1}, \lambda_{i2}, \lambda_{i3}, \lambda_{i4}, \lambda_{i5}\} - \{\lambda_{i1}^{ma}\}\}$ the two biggest eigenvalues values of each DPM.

We note $\mathcal{V} = \{\vec{v}_i, u_i\}_{1 \leq i \leq n}$ a set with n vehicles where vector $\vec{v}_i = (\lambda_{i1}^{ma}, \lambda_{i2}^{ma})$ represents the driving patterns of vehicle v_i, and $u_i \in \{-1, 1\}$ gives the label of $\vec{v}_i$. The label -1 means $\vec{v}_i$ is malicious and otherwise $\vec{v}_i$ is benign.

Normally if data is linear, a separating hyperplane can be used to divide the data. However, due to the erraticness of virtual nodes' movement, it is often the case that the data is far from linear and the datasets are not linearly separable. Under this circumstance, the dataset $\mathcal{V}$ needs to be projected into feature space where the new dataset $\mathcal{V}'$ is linearly separable:

$$\psi : \mathcal{V} \longrightarrow \mathcal{V}'$$
$$\vec{v} \longrightarrow \psi(\vec{v}) = \begin{pmatrix} \psi_1(\vec{v}) \\ \psi_2(\vec{v}) \end{pmatrix} \tag{5}$$

Then, we have $\mathcal{V}' = \{(\psi(\vec{v}), u_i)\}_{1 \leq i \leq n}$ with $u_i \in \{-1, 1\}$. We then define a kernel function k:

$$k(\vec{v}_i, \vec{v}_j) = < \psi(\vec{v}_i), \psi(\vec{v}_j) > \tag{6}$$

Where $< \cdot, \cdot >$ is the scalar product between two vectors. And the objective is to find out the suitable classifier:

$$f_{\vec{w},b}(\vec{v}) = k(\vec{w}, \vec{v}) + b \tag{7}$$

This classifier depends on parameters $\vec{w}, b, e$ to minimize:

$$\frac{1}{2} k(\vec{w}, \vec{w}) + c \sum_l e_l \tag{8}$$

Under the following constraints:

$$\begin{cases} u_l[k(\vec{w}, \vec{v}_l) + b] \geqslant 1 - e_l, \forall (\vec{v}_l, u_l) \in V \\ e_l \geqslant 0, \forall l \end{cases} \tag{9}$$

Its Lagrange multiplier is:

$$\begin{aligned} L(\vec{w}, b, \vec{e}, \vec{\alpha}, \vec{y}) &= \frac{1}{2} k(\vec{w}, \vec{w}) + c \sum_l e_l \\ &\quad - \sum_l \alpha_l [y_l (k(\vec{w}, \vec{v}_l) + b) + e_l - 1] - \sum_l y_l e_l \\ &= \frac{1}{2} k(\vec{w}, \vec{w}) + \sum_l e_l (c - \alpha_l - y_l) \\ &\quad + \sum_l \alpha_l - \sum_l \alpha_l y_l (k(\vec{w}, \vec{v}_l) + b) \end{aligned} \tag{10}$$

Where the Karush Kuhn Tucker conditions must be satisfied:

$$\begin{cases} \forall l; \alpha_l, y_l, e_l \geqslant 0 \\ \forall l; n_l[k(\vec{w}, \vec{v}_l) + b)] \geqslant 1 - e_l \\ \forall l; y_l \cdot e_l = 0 \\ \forall l; \alpha_l [y_l (k(\vec{w}, \vec{v}_l) + b) + e_l - 1] = 0 \end{cases} \tag{11}$$

Under this circumstance, the question above can be considered as to maximize the following function:

$$\sum_l \alpha_l - \frac{1}{2} \sum_k \sum_l \alpha_k \alpha_l u_k u_l k(\vec{v}_k, \vec{v}_l) \tag{12}$$

Where $\forall l$, $\sum_l \alpha_l [u_l = 0$ and $0 \leq \alpha_l \leq c$.

Therefore, the classifier can be considered as:

$$f(\vec{v}) = \sum_l \alpha_l u_l f_{\vec{w},b}(\vec{v}) = k(\vec{v}_l, \vec{v}) + b \tag{13}$$

In this work, three kernel functions are taken into consideration: Polynomial, Gaussian Radial Basis Function (RBF) and Multi-Layer Perceptron (MLP).

- Polynomial: $k(\vec{v}_i, \vec{v}_j) = (< \vec{v}_i, \vec{v}_j > + h)^d$ where h is a constant value.
- RBF: $k(\vec{v}_i, \vec{v}_j) = exp(-\frac{\|\vec{v}_i - \vec{v}_j\|^2}{2\sigma^2})$
- MLP: $k(\vec{v}_i, \vec{v}_j) = tanh(\rho < \vec{v}_i, \vec{v}_j > + \varrho)$

Their performance will be evaluated in the next section based on the simulation results.

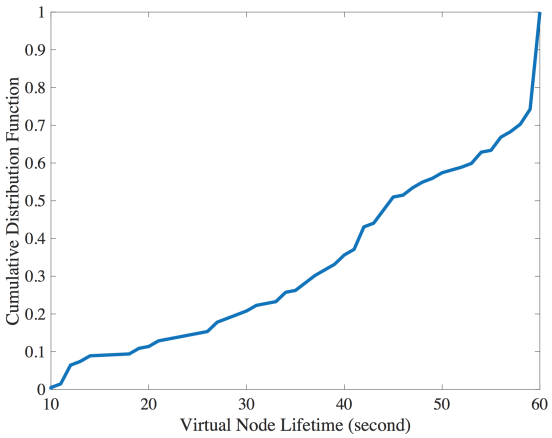


Fig. 2: Lifetime of virtual nodes

V. Experimental Results

In the following simulations, SUMO simulator is chosen to simulate traffic flows in urban scenario, where parameters are set based on real-time urban traffic. The Sybil nodes generation procedure follows the strategy defined in Section III. The detection method is implemented on the RSU, and vehicles are demanded to periodically communicate their driving patterns with the RSU via CAM message. we choose a window size of 60 seconds and vehicles within 10 second before and after the target vehicle. More details are presented in Table II:

TABLE II: PARAMETERS USED IN SIMULATION

Parameter	Value
Simulation Scenario	Urban Scenario
Simulation Time	300s
Window Distance	1 km
Street Width	2 Lanes
Vehicle Velocity	40 - 60 km/h
Number of Vehicles Simulated	350 - 800
Communication Range	300m

A. Virtual Nodes' Characteristics

As illustrated in Fig. 3, the driving patterns of benign nodes have obvious similarity and the driving patterns of Sybil nodes show erraticness. This result is caused by two reasons:

- The variation of virtual nodes' lifetime: We measured the lifetime for more than 200 virtual nodes, the CDF is illustrated in Fig. 2. We can find out that more than 70% of the virtual nodes do not have the same length of lifetime as the benign ones (60 seconds).
- The erraticness of virtual nodes' movement: Virtual nodes should not be set to the positions that are captured by the benign ones.

Both these issues cannot be figured out by Sybil nodes, because they cannot control the components of other road users. They can only adjust their own strategies and make their driving patterns as reasonable as possible. Our detection system is directed against this weak point of Sybil nodes, making it possible to separate virtual nodes from benign ones.

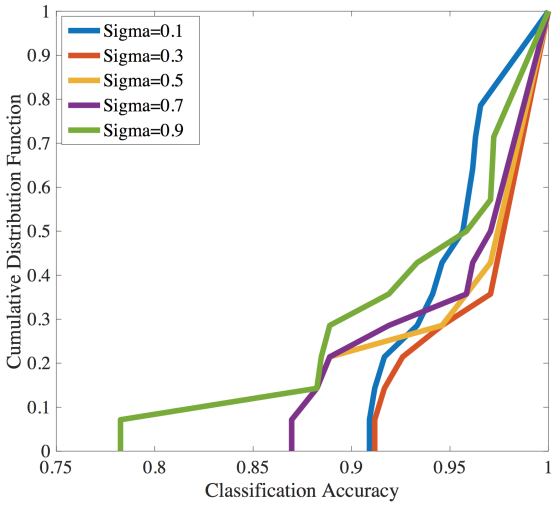


Fig. 4: RBF Classifier with $sigma$ values from 0.1 to 0.9.

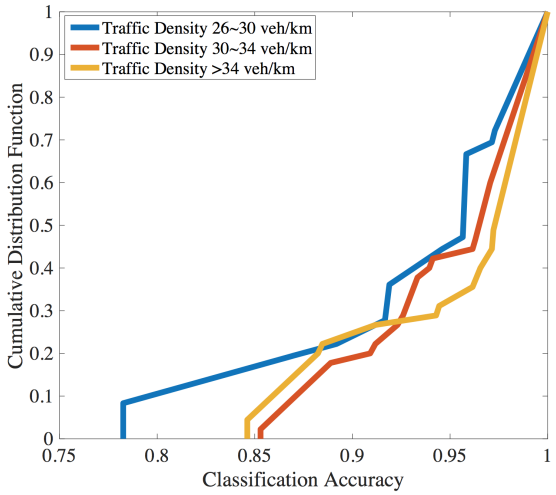


Fig. 5: Testing groups classification accuracy in three different traffic densities.

B. Classification Accuracy

We launched 15 times Sybil attacks under 3 different traffic densities. The first group is chosen as the training group and the other 14 groups are testing groups. As illustrated in Table III, the classification accuracy in all testing groups, and Fig. 3 shows the training group classification results. In this work, all three kernel functions are implemented with different parameters. Generally speaking, due to the reality that benign nodes show strong similarity in their driving patterns, the classifiers which cover less surface reach higher accuracies.

In more detail, as illustrated in Fig. 4, the performance of RBF classifier with different $sigma$ values, which can be noticed is that with the increase of the $sigma$ value, from 0.1 to 0.9, the classifier reaches its best accuracy at the point $sigma = 0.3$, then its performance decreases with the increase of the $sigma$ value. In SVM, a very small value of $sigma$ means a large margin is necessary which may leads to misclassified training group. On the other hand, with a very large $sigma$ value, the training group can be well classified, however, the classifier would not reach high classification accuracy in testing groups.

As shown in Fig. 5, testing groups classification accuracy with different traffic density. As we expected, when the traffic density is high (> 34 vehicles per kilometre), the classifiers reach higher classification accuracy. That because when the traffic density is high, the average distance between two adjacent vehicles are small, their driving patterns would show stronger similarity compare to the low traffic density scenarios. Otherwise, when the distance between vehicles is small, the erraticness of virtual nodes' driving patterns would also be obvious. Because they should not be set to the positions that are captured by the benign ones.

C. Classification Error Rate

In this work, the confusion matrix is also chosen to evaluate the performance of classifiers, which is considered as a comprehensive and visually attractive way to summarise the error rate. Normally a confusion reports the number of False Positives (FP), False Negatives (FN), True Positives (TP), and True Negatives (TN). The error rate of a classifier corresponds three metrics: True Positive Rate (TPR) which means the well detected ratio, False Positive Rate (FPR) which represents the percentage of benign nodes that are reported as malicious and False Negative Rate (FNR) which means the percentage of malicious nodes are reported as benign.

TABLE IV: CONFUSION MATRIX

	TP	TN	FP	FN	TPR	FPR	FNR
rbf $\sigma = 0.3$	325	94	2	8	97.6%	2%	2.4%
Poly $d = 2$	326	74	1	28	92.1%	1.3%	7.9 %
MLP [-2 2]	326	90	1	12	96.5%	1.1%	3.6%

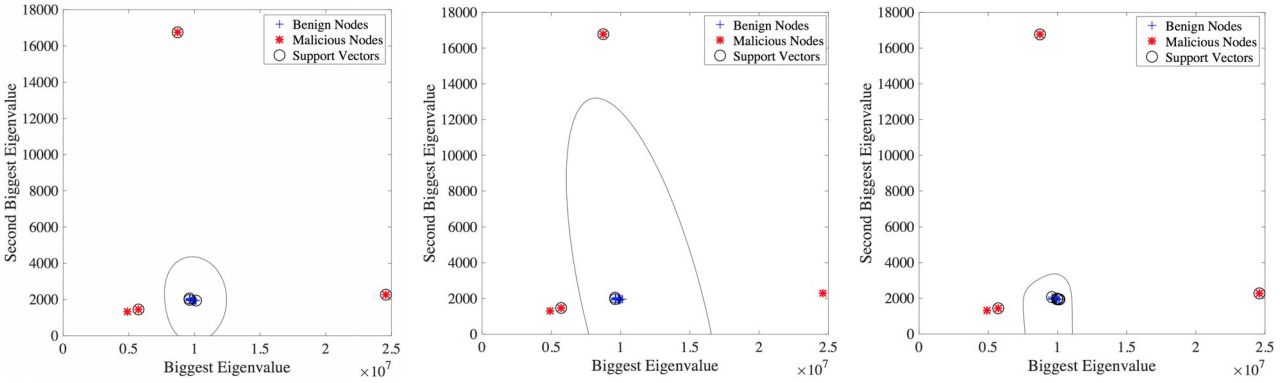
As shown in Table IV the summary of these three classifiers' confusion matrices. Generally speaking, these classifiers all reached high detection rate with low error rate. When we go into more detail, which can be noticed is that the FNR of polynomial classifier is about 8%, but the FPR is low. As we have seen above in Fig. 3, the polynomial classifiers covered more surface than the other two classifiers. In this case, benign nodes can be hardly reported as malicious, but malicious nodes could be reported as benign.

VI. Conclusion

In this paper, a vehicle driving pattern similarity measurement method in near capacity traffic scenario was introduced. This method was developed to measure the benign vehicles' similarity in driving patterns and detect the variation between benign vehicles and Sybil nodes in their driving patterns. This variation can be reflected in their Driving Pattern Matrices. Vehicle driving patterns are mainly represented using the eigenvalues of its DPM in this proposed detection method. The SVM methods are then used to classify the vehicles and distinguish the virtual nodes from benign ones. Simulation results show that in all events, the majority benign vehicles have similar driving patterns, and the Sybil nodes show erraticness in their driving patterns. All the three kernel functions are reached high detection rate with low error rate.

TABLE III: Testing Groups Classification Accuracy

Traffic Density	26-30	26-30	26-30	26-30	30-34	30-34	30-34	30-34	30-34	> 34	> 34	> 34	> 34	> 34
rbf $\sigma = 0.1$	0.917	0.956	0.945	1	0.909	0.941	0.961	0.933	0.963	0.961	0.912	1	0.965	1
rbf $\sigma = 0.3$	0.917	1	0.945	1	1	0.971	1	1	0.926	1	0.912	1	1	1
rbf $\sigma = 0.5$	0.958	0.870	0.946	1	1	0.971	1	1	0.889	1	0.882	1	1	1
rbf $\sigma = 0.7$	0.958	0.870	0.919	1	1	0.971	1	1	0.889	0.962	0.882	1	1	1
rbf $\sigma = 0.9$	0.958	0.782	0.919	1	1	0.971	1	0.933	0.889	0.884	0.882	0.971	1	0.972
Polynomial $d = 2$	0.958	0.783	0.919	1	1	0.912	0.923	0.933	0.889	0.846	0.882	0.971	1	0.972
Polynomial $d = 4$	0.958	0.782	0.892	0.971	0.939	0.853	0.923	0.933	0.889	0.846	0.882	0.943	0.966	0.944
mlp [-1 1]	0.958	0.826	0.973	1	1	0.971	1	1	0.889	1	0.882	1	1	1
mlp [-2 2]	0.958	0.826	1	1	1	0.971	1	1	0.889	1	0.882	1	1	1



(a) RBF Sigma=0.5 (b) Polynomial d=2 (c) MLP

Fig. 3: Training group classification results with all three kernel functions

REFERENCES

[1] R. Khatoun and S. Zeadally, "Smart Cities: Concepts, Architectures, Research Opportunities," *Commun. ACM*, vol. 59, no. 8, Jul. 2016.

[2] "IEEE Standard for Wireless Access in Vehicular Environments Security Services for Applications and Management Messages," *IEEE Std 1609.2-2013 (Revision of IEEE Std 1609.2-2006)*, pp. 1–289, April 2013.

[3] "Intelligent Transport Systems (ITS); Security; Trust and Privacy Management," *ETSI TS 102 941 V1.1.1*, pp. 1–30, Juin 2012.

[4] B. Ostermaier, F. Dotzer, and M. Strassberger, "Enhancing the Security of Local DangerWarnings in VANETs - A Simulative Analysis of Voting Schemes," in *Availability, Reliability and Security, 2007. ARES 2007. The Second International Conference on*, April 2007, pp. 422–431.

[5] J. F. C. Joseph, B. S. Lee, A. Das, and B. C. Seet, "Cross-Layer Detection of Sinking Behavior in Wireless Ad Hoc Networks Using SVM and FDA," *IEEE Transactions on Dependable and Secure Computing*, vol. 8, no. 2, pp. 233–245, March 2011.

[6] B. E. Boser, I. M. Guyon, and V. N. Vapnik, "A Training Algorithm for Optimal Margin Classifiers," in *Proceedings of the Fifth Annual Workshop on Computational Learning Theory*, ser. COLT '92. New York, NY, USA: ACM, 1992, pp. 144–152.

[7] C. J. C. Burges, "A Tutorial on Support Vector Machines for Pattern Recognition," *Data Min. Knowl. Discov.*, vol. 2, no. 2, Jun. 1998.

[8] J. Yang, Y. Chen, W. Trappe, and J. Cheng, "Detection and Localization of Multiple Spoofing Attackers in Wireless Networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 24, no. 1, Jan 2013.

[9] W. Hu, J. Gao, Y. Wang, O. Wu, and S. Maybank, "Online Adaboost-Based Parameterized Methods for Dynamic Distributed Network Intrusion Detection," *IEEE Transactions on Cybernetics*, vol. 44, Jan 2014.

[10] J. R. Douceur, "The Sybil Attack," in *Proceedings of 1st International Workshop on Peer-to-Peer Systems (IPTPS)*, 2002.

[11] R. Khatoun, G. Doyen, D. Gaiti, R. Saad, and A. Serhrouchni, "Decentralized alerts correlation approach for ddos intrusion detection," in *2008 New Technologies, Mobility and Security*, Nov 2008, pp. 1–5.

[12] J. Newsome, E. Shi, D. Song, and A. Perrig, "The Sybil attack in sensor networks: analysis defenses," in *Information Processing in Sensor Networks, Third International Symposium on*, April 2004.

[13] S. Capkun, L. Buttyan, and J. P. Hubaux, "Self-organized public-key management for mobile ad hoc networks," *IEEE Transactions on Mobile Computing*, vol. 2, no. 1, pp. 52–64, Jan 2003.

[14] T. Zhou, R. R. Choudhury, P. Ning, and K. Chakrabarty, "P2DAP - Sybil Attacks Detection in Vehicular Ad Hoc Networks," *IEEE Journal on Selected Areas in Communications*, vol. 29, no. 3, pp. 582–594, 2011.

[15] A. Cheng and E. Friedman, "Sybilproof Reputation Mechanisms," in *Proceedings of the 2005 ACM SIGCOMM Workshop on Economics of Peer-to-peer Systems*. New York, NY, USA: ACM, 2005, pp. 128–132.

[16] B. Xiao, B. Yu, and C. Gao, "Detection and Localization of Sybil Nodes in VANETs," in *Proceedings of the 2006 Workshop on Dependability Issues in Wireless Ad Hoc Networks and Sensor Networks*, ser. DIWANS '06. New York, NY, USA: ACM, 2006, pp. 1–8.

[17] B. Yu, C.-Z. Xu, and B. Xiao, "Detecting Sybil attacks in VANETs," *Journal of Parallel and Distributed Computing*, vol. 73, no. 6, 2013.

[18] Y. Chen, J. Yang, W. Trappe, and R. P. Martin, "Detecting and Localizing Identity-Based Attacks in Wireless and Sensor Networks," *IEEE Transactions on Vehicular Technology*, vol. 59, no. 5, Jun 2010.

[19] C. Piro, C. Shields, and B. N. Levine, "Detecting the Sybil Attack in Mobile Ad hoc Networks," in *Securecomm and Workshops*, Aug 2006.

[20] S. Yan, R. Malaney, I. Nevat, and G. W. Peters, "Optimal Information-Theoretic Wireless Location Verification," *IEEE Transactions on Vehicular Technology*, vol. 63, no. 7, pp. 3410–3422, Sept 2014.

[21] S. Chang, Y. Qi, H. Zhu, J. Zhao, and X. Shen, "Footprint: Detecting Sybil Attacks in Urban Vehicular Networks," *IEEE Trans. on Parallel and Distributed Systems*, vol. 23, no. 6, pp. 1103–1114, June 2012.

[22] K. Rabieh, M. M. E. Mahmoud, T. N. Guo, and M. Younis, "Cross-layer scheme for detecting large-scale colluding Sybil attack in VANETs," in *2015 IEEE International Conference on Communications (ICC)*.

[23] "Intelligent Transport Systems (ITS);Vehicular Communications; Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service," *ETSI EN 302 637-2 V1.3.1*, pp. 1–44, Spt 2014.

[24] "Intelligent Transport Systems (ITS);Vehicular Communications; Basic Set of Applications; Part 3: Specifications of Decentralized Environmental Notification Basic Service," *ETSI EN 302 637-3 V1.2.1*, Spt 2014.

[25] R. G. Engoulou, M. Bellache, S. Pierre, and A. Quintero, "VANET security surveys ," *Computer Communications*, vol. 44, pp. 1 – 13, 2014.

[26] Y. Hao, J. Tang, and Y. Cheng, "Cooperative Sybil Attack Detection for Position Based Applications in Privacy Preserved VANETs," in *Global Telecommunications Conference, 2011 IEEE*, Dec 2011, pp. 1–5.

[27] K. Abboud and W. Zhuang, "Stochastic analysis of a single-hop communication link in vehicular ad hoc networks," *IEEE Transactions on Intelligent Transportation Systems*, vol. 15, no. 5, Oct 2014.