Senior2Local: A Machine Learning Based Intrusion Detection Method for VANETs

Yi Zeng[1], Meikang Qiu[2(✉)], Zhong Ming[2], and Meiqin Liu[3]

[1] College of Electronic and Information Engineering, Xidian University, Xi'an, Shaanxi, China
zengyi_xidian@163.com
[2] College of Computer Science, Shenzhen University, Shenzhen, Guangdong, China
{mqiu,mingz}@szu.edu.cn, qiumeikang@yahoo.com
[3] College of Electrical Engineering, Zhejiang University, Hangzhou, China
liumeiqin@zju.edu.cn

Abstract. Vehicular Ad-hoc Network (VANET) is a heterogeneous network of resource-constrained nodes such as smart vehicles and Road Side Units (RSUs) communicating in a high mobility environment. Concerning the potentially malicious misbehaves in VANETs, real-time and robust intrusion detection methods are required. In this paper, we present a novel Machine Learning (ML) based intrusion detection methods to automatically detect intruders globally and locally in VANETs. Compared to previous Intrusion Detection methods, our method is more robust to the environmental changes that are typical in VANETs, especially when intruders overtake senior units like RSUs and Cluster Heads (CHs). The experimental results show that our approach can outperform previous work significantly when vulnerable RSUs exist.

Keywords: ML · Intrusion detection · VANETs · RSUs
Game theory

1 Introduction

The Vehicular Ad-hoc Network (VANET) is an emerging type of Mobile Ad-hoc Networks (MANETs) with excellent applications in the intelligent traffic system. Despite the promising future of VANETs, they are known to be sensitive to various misbehaves, ranging from malicious attacks to random failures [15]. Considering the safety of vehicles is directly related to human lives, security is one of the main challenges in VANETs. Various detection methods have been proposed in the past decade to detect and mitigate Intrusions in VANETs. Most of these presented methods overlook the security of senior units or just simply rely on a set of predefined and fixed threshold(s) to secure the senior units.

However, senior units, Road Side Units (RSUs) and Cluster Heads (CHs) (see Sect. 2.1), are not guaranteed to be safe in a VANET. Although RSUs are built to be robust, yet intruders can still impair the system through physical

M. Qiu (Ed.): SmartCom 2018, LNCS 11344, pp. 417–426, 2018.
https://doi.org/10.1007/978-3-030-05755-8_41

attacking RSUs or impersonating as an RSU [8]. Not to mention that CHs are easier than RSUs to be impersonated or overtook [10]. The overlook of those senior units' security can lead to serious consequences [10]. Furthermore, considering the highly dynamic nature of VANETs, it is not achievable to find a set of fixed thresholds to detect malicious nodes. In contrast, our online Machine Learning based (ML-based) intrusion detection method can automatically determine whether a node is malicious or not considering all available data from the VANET.

In addition, we argue that RSUs cannot be marked simply as either malicious or cooperative, taken that cooperative RSUs might behave abnormally due to the nature of VANETs. One example is illustrated in Fig. 1. We find that RSU 2 drops packets from all CHs that connected to because different reasons, which will make it be detected as an intruder without further investigation. However, it is actually a cooperative RSU which dops packages out of malicious intent. Meanwhile, RSU 1 pretends to be a normal RSU and answers requests from CH 4 and CH 2, which will be classified as a cooperative RSU by most of the methods presented, yet it is an intruder who might spoof other units in the VANET [3]. Both misclassifications will lead to extra costs and dangerous outcomes. Hence, we clearly see from this example that a trust system, where RSUs are motivated to provide trustworthy information, is required in order to mitigate the influence of vulnerable nodes and fake RSUs.

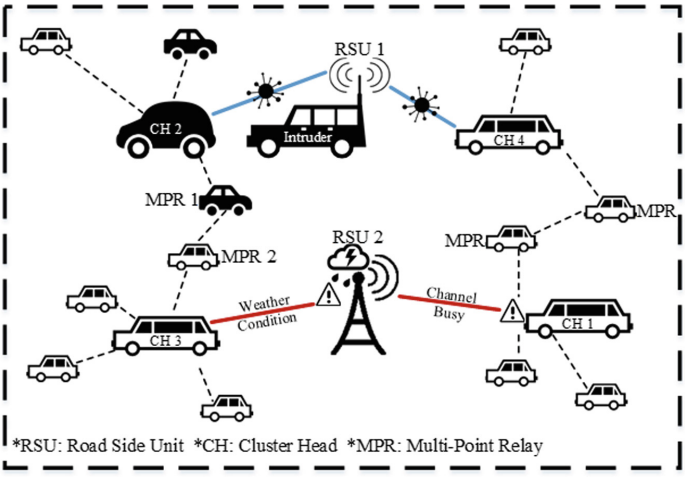

Fig. 1. Trust system is required for RSUs

In this paper, we proposed an Intrusion Detection method based on Machine Learning (ML) and game theory for VANETs. Our method securing the VANET ranging from senior units (RSUs and CHs) to local vehicles level to level. A trust system is built to credit RSUs. Then, Artificial Neural Network (ANN) is

presented in RSUs to detect malicious CHs. Finally, in local scale, online Support Vector Machine (SVM) is trained and implemented to detect malicious vehicles inside clusters.

This paper's contribution can be summarized as follows: **(1)** We apply game theory to secure senior units which proved to be more reliable than presented works under the dramatically changing environment in VANETs. **(2)** ANN is implemented in our methods in RSUs, which is known to be more precise than most presented classification methods in VANETs. **(3)** We apply simplified SVM in vehicles, which is a light-weight detection method that suits the resource-constrained nature of vehicles. **(4)** To our best knowledge, this is the first through intrusion detection method that concerning each level of nodes in detail. This presented method is proved to outperform presented methods dramatically when senior level nodes are damaged.

The rest of this article is divided into five sections. Section 2 presented background information and problem statements. The Senior2Local detection method is elaborated in Sect. 3. The experimental result is shown in Sect. 4. Finally, Sect. 5 gives the concluding remark of this paper.

2 Problem Statement

2.1 Backgrounds of VANETs

A VANET as a whole consists of RSUs, CHs, Multi-Point Relays (MPRs), and normal vehicles. Each vehicle, including CH and MPR, is equipped with technologies that allow communications between each point possible.

Globally, RSUs are capable of communicating with other RSUs via physical networks, e.g., data center network [6]. This character also empowers RSUs to use cloud computing and regardless of the resource constraint. An RSU can connect to every vehicle in the area that covered by its wireless network directly. All those RSU-based connections together build up the global view of a VANET.

From the local perspective, this connection between RSU and its correlative cars usually including several vehicular clusters. These clusters follow Vehicular Ad-Hoc Network Quality of Service Optimized Link State Routing (VANET QoS-OLSR) [13], which is a clustering protocol that considers a trade-off between the QoS requirements and the high mobility metrics in VANET. For every cluster concerned, a CH is selected to facilitate the management of each cluster. Then, these heads are responsible for selecting a set of specific vehicles charged of transmitting the network topology information through messages called Topology Control (TC) and forwarding the packets. Such nodes are called MPRs.

Problems can arise no matter globally or locally to impair the VANET due to the vulnerability of RSUs and vehicles.

2.2 Problems and Challenges in VANET

Globally, RSUs can be physically damaged by malicious actions or accidents [8]. In this scenario, the accuracy of analyzing CHs can be dampened. If there is

a specific RSU which is physically vulnerable, then, there are chances that the data transmitted through this RSU is not trust-worthy. Another issue is the impersonation [8]. Intruders can impersonate as RSUs, spoofing service advertisements or safety messages. Those two major issues with RSUs are illustrated in Fig. 2.

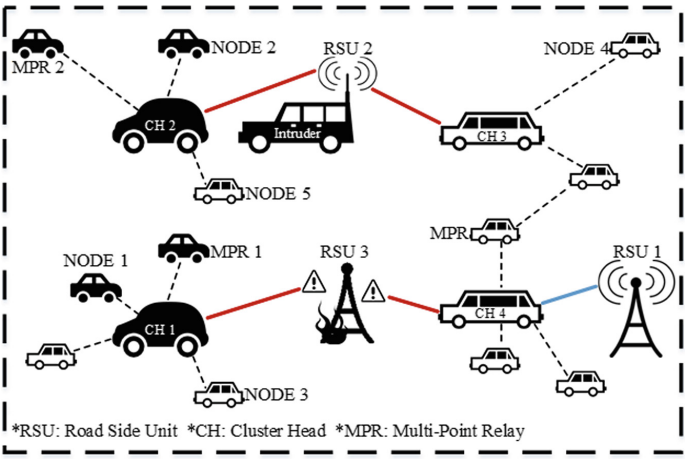

Fig. 2. Global intrusion examples in VANETs

In Fig. 1, only RSU 1 is working properly. RSU 1 can exchange data with CH 4 and oversees the related cars in the cluster continuously. Hence security actions can take place as expected, a high security of this area can be ensured.

RSU 2 is actually a vehicular intruder impersonating as a normal RSU. Firstly, this leads CH 3 and other cooperative cars in the area covered by RSU 2, e.g., NODE 4 and NODE 5, try to exchange important data with this intruder, hence important information of cars can be leaked, and extra transporting consumption is required. Secondly, this intruder can take cover for CH 2, which is a malicious CH performing malicious actions. This directly leads MPR 2 and NODE 2, which all are malicious vehicles, take malicious actions barbarically, which might even cost massive death.

RSU 3 is an RSU which is physically damaged which cannot receive packages from CH 1 or CH 4. Despite the driving experience in the related area is dampened, the malicious CH 1 will remain undetected. This failure of detecting CH 1 leads NODE 1 and MPR 1 continuously perform malicious actions barbarically, which surely will damage the whole VANET.

Locally, if intruders remain undetected, especially when intruders play a roll in the cluster, serious consequences can happen [9]. One dangerous scenario is when the head of the cluster is malicious. As a CH, it can perform malicious actions without being detected by other vehicles. Malicious CHs can send fake data or spam to other members in the cluster. More dangerously, a malicious CH

can take cover for other malicious nodes in the cluster. It can choose a malicious node as an MPR, which can perform Denial of Service (DoS) or inject fake data to other clusters. If the CH is not malicious, however, malicious nodes in the cluster can be isolated and a trust-worthy node can be chosen as MPR. Hence, the guarantee of CH is trust-worthy is important for the whole cluster.

As RSUs are not guaranteed to be cooperative constantly, we assume RSUs can be intruders or real RSUs which have chances to perform packages drop, like examples mentioned in [8]. As for CHs, different from other presented methods which regard them as trust-worthy all the time, we treat them same as other normal vehicles, which can be overtaken by intruders.

3 The Senior2Local Intrusion Detection Method

In this section, we will illustrate the details of our proposed ML-based intrusion detection method for VANETs. Senior2Local Intrusion Detection method is divided into two functional modules: *Global Intrusion Detection and Propagation*, *Local Intrusion Detection and Propagation*.

3.1 Global Intrusion Detection and Propagation

In this process, our presented model will firstly analyze all the CHs in the cluster based on pre-trained ANN that is implemented in RSUs. Although ANNs can detect intruders effectively, they normally require a high computational resource to train and implement. In a VANET, only RSUs are concerned as unlimited in the resource, which is suitable to use ANN to detect malicious CHs. The ANN in our proposed method is firstly trained and tested on a fuzzification dataset which was collected from a trace file that was generated utilizing GloMoSim 2.03 [14] to model the VANET and its environment. This fuzzification ANN-based detector is inspired by the work [1], yet we will only use this ANN in RSUs to detect malicious CHs. Furthermore, we trained our ANN to output a real number ranging from -1 to 1, which denotes the belief of the CH being cooperative or malicious. If the number is positive, then the CH is marked as cooperative, otherwise, it is marked as malicious. The absolute value of the number $BasBili$, denotes the basic belief of CH being that way. The total accuracy of the training process is 99.97%. The true positive rate on testing data is 99.91%, and the true negative rate on testing data is 99.84%.

After we implement this well-trained ANN, RSUs are able to detect malicious CHs that connected directly to themselves individually. Then, a trust system is built up to evaluate each RSU's credit. Trust is constructed by exchanging detection belief about CHs based on their previous interactions. Practically, fake RSUs may be tempted to collusion with each other to provide fake detection results over CHs, which may lead to misleading results. To overcome scenarios that most multiple RSUs are imprisoned by intruders, we adopt the credibility update function and a belief function transplanted from [11] with the aim of

encouraging RSUs, even fake ones, to participate in the trust establishment process and provide truthful analyze results over CHs.

The proposed trust system for RSUs works as follow. The belief function represents the total analyze belief results globally considering all RSUs. We let RSU_x be the x^{th} RSU of the VANET, $Clus^i$ be the Custer i, and CH^i be the CH of $Clus^i$. For example, $Beli_x^i(H)$ is a belief function, whihc will indicate the belief from RSU_x over a hypothesis, e.g., CH^i is H (H is a hypothesis, cooperative, malicious, or uncertain). This belief is a real number ranging from 0 to 1. Let $LRes_x^i = \{Co, Ma, Un\}$ denote the local analyze results over CH^i by RSU_x. Co denotes the possibility of CH^i being cooperative; Ma is the possibility of CH^i being malicious, and Un is an expression of uncertainty. Primarily, $LRes_x^i$ is acquired from the out put of aforementioned ANN. For instance, the ANN output a negative number 0.78, then we set $BasBili$ as 0.78, Co as 0, Ma as 0.78, and Un is equal to $1 - BasBeli$, which is 0.22. The belief function of RSU_x in CH^i will be updated according to the belief updat function presented in [11] after consulting two other RSUs, RSU_1 and RSU_2.

Thus, the problem of establishing the common belief over CHs in the VANET can be achieved after computing, consulting, and combining all the believes. This purposed technique is proved in [11] that it can overcome the problem where malicious RSUs are the majority.

Primarily, we set the credits of each RSU to 1. and now, we can reset the credits of each RSU_x after judging CH^i in favor of RSU_s based on the credibility update function from [11]. After conducting this iteration globally with all the RSUs in the VANET, a reward for consistency and a punishment for inconsistency can be achieved.

The last step is the global propagation process. And more details of this function model as a whole is explained in Algorithm 1. After conducting this model, senior units, e.g., RSUs and CHs, are motivated to perform cooperatively. This can facilitate future local detection since detected malicious CHs are no longer participate in the VANET.

3.2 Local Intrusion Detection and Propagation

Taken that vehicles are resource constrained [4], an intelligent trigger for vehicles to detect the intruder in the local cluster is required. In our presented model, the trigger would go off when package dropping is detected in the cluster. In this trigger detecting process, each vehicle in the cluster would be designed as watchdogs [7] to constantly monitoring and analyzing the behavior of MPRs that within their transmission range. Hence, we are capable to monitor the number of packages that an MPR to send and the number of packages that an MPR actually sent. When a mismatch of those two number happens, we will mark such a MPR as malicious primarily. After every vehicle has its own observation about MPRs in its vicinity, we will let each vehicle in the cluster to exchange and integrate those observations to generate a dataset to train our light-weight SVM in the following process. After this process, a basic perspective over malicious nodes in the cluster is acquired.

Algorithm 1. Global Intrusion Detection and Propagation

Input:
Pre-trained ANN classifier.
Extracted features' data of every CH.
Output:
A updated trust system of RSUs.
A secured set of CHs where acknowledged malicious CHs are banned.
Procedure:

for each RSU_j in the VANET **do**
  for each CH^i that directly connects to RSU_j **do**
    Transmit Behavioral Data to RSU_j
    Transmit Contextual Data to RSU_j
    Apply pre-trained ANN classifier to analyze CH^i
    Save analyze result to $LRes_x$
  end for
end for
Computing, consulting, and comparing classification believes of CH^i globally according to the belief updat function from [11]
for each RSU_j in the VANET **do**
  Reward or Punish the RSU according to the credibility update function from [11]
end for
Broadcast the trust credit of each RSU globally
based on common belief, mark every acknowledged malicious CH
for every acknowledged malicious CH^m **do**
  Ban node CH^m from the network
  Select a new CH^m from $Clus^m$ randomly
end for

After a trigger, a dropping of packages is detected in the previous process, the *Local Intrusion Detection and Propagation* process will initiate. In this part, similar to [12], we integrate the support vectors from the previous training process and the observation from other vehicles in the cluster except the vehicle that running this detection as training data, and the observation of this vehicle is set as the testing dataset. Notice that Gaussian Radial Basis Function kernel is selected in our model, taken that it was experimental proved to be best fitting scenarios in VANETs [12]. In order to conduct a high accuracy in detection, our model will work in an online fashion, which means it will be trained incrementally. Considering the resource constraint in vehicles, the online training process will only keep the support vectors from the previous iteration. Each testing process works as a detection from an individual vehicle, and the final results from all the nodes in the cluster will be integrated after all the detection is done. This integrated list of vehicles can be divided into two parts, the $MaliSet$, which is a list of malicious nodes, and the $CoopSet$, which is a list of cooperative nodes. Those two sets will be stored in the CH of the cluster. In order to reach a regional security, those two sets will be exchanged and integrated between CHs

only when two CHs contacts. This exchange of the *MaliSet* and the *CoopSet* can prevent malicious vehicles run away from a cluster to a new cluster without being noticed. After the detection and propagation, further monitoring will only concern those cooperative nodes, and malicious nodes will be banned from cluster to cluster for security reasons.

4 Experimental Results and Analysis

In this section, we evaluate the performance of the Senior2Local intrusion detection method using network simulation and the performance is compared with two novel ML-based intrusion detection methods. The first baseline mechanism is the SVM-based Context-Aware Security Framework (SVM-CASE) that proposed in [5], which is a well-known ML-based method for intrusion detection in VANET. The other based line is CEAP (Collection, Exchange, Analysis, and Propagation) that proposed in [12], which is another ML-based detection method for VANETs.

4.1 Simulation Setup

The experimental platform we use is GloMoSim 2.03 [14]. We set the simulation area as 600 m × 600 m. The total number of nodes we used is 50, 100, 150, and 200 for each iteration. The total number of RSUs in our simulation is 6. For each iteration, we set 10%, 20%, 30%, and 40% nodes as intruders. The transmission range we used is 120 m. The moving speed is set from 5 m/s to 30 m/s randomly for each vehicle. The total simulation time was set to 900 s.

The parameters used to evaluate the performance of the different methods are the accuracy rate and attack detection rate. Accuracy Rate is the number that results when the number of correctly detected malicious nodes is divided by the total number of detected malicious nodes. The attack detection rate is the number results when the total number of correctly detected malicious nodes is divided by the total number of malicious nodes.

$$\text{Accuracy Rate} = 100\% \times \frac{\text{Number of Correctly Detected Malicious Nodes}}{\text{Total Number of Detected Malicious Nodes}} \tag{1}$$

$$\text{Attack Detection Rate} = 100\% \times \frac{\text{Total Number of Correctly Detected Malicious Nodes}}{\text{Total Number of Malicious Nodes}} \tag{2}$$

We compare different parameters under one possible scenario in the VANET. In this case, half of the RSUs are fake RSUs collude together to provide fake data in order to interfere with the detection process [2]. Futhermore, one of the RSU is physically broken (denying all the detection requests), which is a possible scenario chould happened in VANETs [8]. In our simulation, one of the RSU from the six RSUs is selected randomly and start to denying all the detection requests as a simulation of the physically broken scenario. Then, we selected 3 RSUs randomly from the other 5 RSUs and let them transmit some

similar fake data with others. The fake data is actually generated from the real detection results, yet we let those fake RSUs report malicious when they detect cooperative nodes, and vice versa.

4.2 Experimental Results

Firstly, we can learn from Fig. 3 that the Senior2Local method can outperform the SVM-CASE method and CEAP method dramatically when RSUs are not trustworthy. We can see a dramatic decline in the accuracy performance of SVM-CASE [5] and CEAP [12] in our experimental scenario comparing to their original experimental result, which was at least 98.7% and 98.9% respectively. Yet, the Senior2Local's accuracy is more robust, the average accuracy is 98.37% even when most of the functional RSUs are fake. From Fig. 4, we can observe a higher ability to detect attacks of the Senior2Local method. This ability is much higher than SVM-CASE and CEAP in the same environment. The average attack detection rate of the Senior2Local method is 98.25%, which means even most of the RSUs cannot provide trustworthy detection data, Senior2Local still can secure the VANET. Those two results can reflect the ability of Senior2Local to overcome impersonation and physical vulnerability, which can be a more suitable detection method to implement in the VANET.

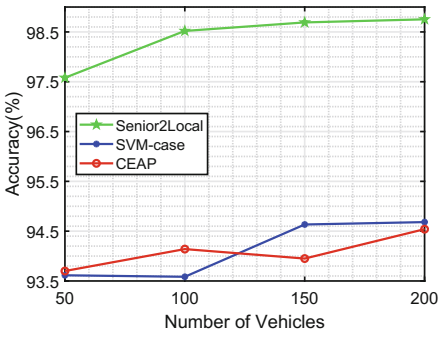

Fig. 3. Accuracy rate comparison

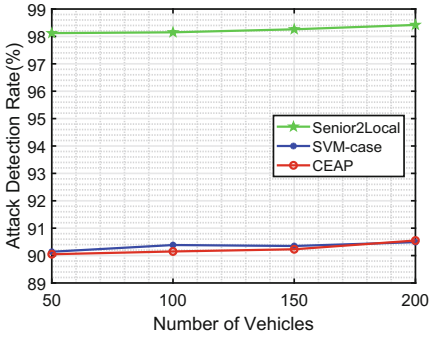

Fig. 4. Attack detection rate comparison

5 Conclusion

In this paper, we presented Senior2Local, a novel ML-based intrusion detection method for VANETs. We used game theory to build a trust system for RSUs. ANN is implemented in our model based on trust-worthy RSUs to securing CHs. After removing malicious CHs, a light-weight SVM is used to detect malicious MPRs cluster to cluster locally. The experimental result shows that Senior2Local is more robust and trust-worthy comparing to presented ML-based detection methods.

Acknowledgement. This work is supported by China NSFC 61836005 and 61672358; China NSFC 61728303 and the Open Research Project of the State Key Laboratory of Industrial Control Technology, Zhejiang University, China (ICT1800417).

References

1. Alheeti, K.M.A., Gruebler, A., McDonald-Maier, K.D.: An intrusion detection system against black hole attacks on the communication network of self-driving cars. In: 2015 Sixth International Conference on Emerging Security Technologies (EST), pp. 86–91. IEEE (2015)
2. Chim, T.W., Yiu, S., Hui, L.C., Li, V.O.: Security and privacy issues for inter-vehicle communications in vanets. In: 6th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks Workshops, 2009, SECON Workshops 2009, pp. 1–3. IEEE (2009)
3. Gai, K., Qiu, M., Ming, Z., Zhao, H., Qiu, L.: Spoofing-jamming attack strategy using optimal power distributions in wireless smart grid networks. IEEE Trans. Smart Grid **8**(5), 2431–2439 (2017)
4. Kumar, N., Chilamkurti, N.: Collaborative trust aware intelligent intrusion detection in vanets. Comput. Electr. Eng. **40**(6), 1981–1996 (2014)
5. Li, W., Joshi, A., Finin, T.: SVM-case: an SVM-based context aware security framework for vehicular ad-hoc networks. In: 2015 IEEE 82nd Vehicular Technology Conference (VTC Fall), pp. 1–5. IEEE (2015)
6. Liu, J., Wan, J., Zeng, B., Wang, Q., Song, H., Qiu, M.: A scalable and quick-response software defined vehicular network assisted by mobile edge computing. IEEE Commun. Mag. **55**(7), 94–100 (2017)
7. Marti, S., Giuli, T.J., Lai, K., Baker, M.: Mitigating routing misbehavior in mobile adhoc networks. In: Proceedings of the 6th Annual International Conference on Mobilecomputing and Networking, pp. 255–265. ACM (2000)
8. Qian, Y., Moayeri, N.: Design of secure and application-oriented VANETs. In: 2008 IEEE Vehicular Technology Conference, VTC Spring 2008, pp. 2794–2799. IEEE (2008)
9. Qiu, M., Gai, K., Thuraisingham, B., Tao, L., Zhao, H.: Proactive user-centric secure data scheme using attribute-based semantic access controls for mobile clouds in financial industry. Futur. Gener. Comput. Syst. **80**, 421–429 (2018)
10. Sharma, S., Kaul, A.: A survey on intrusion detection systems and honeypot based proactive security mechanisms in VANETs and VANET cloud. Vehic. Commun. (2018)
11. Wahab, O.A., Bentahar, J., Otrok, H., Mourad, A.: Towards trustworthy multi-cloud services communities: a trust-based hedonic coalitional game. IEEE Trans. Serv. Comput. **11**(1), 184–201 (2018)
12. Wahab, O.A., Mourad, A., Otrok, H., Bentahar, J.: CEAP: SVM-based intelligent detection model for clustered vehicular ad hoc networks. Expert. Syst. Appl. **50**, 40–54 (2016)
13. Wahab, O.A., Otrok, H., Mourad, A.: Vanet QoS-OLSR: QoS-based clustering protocol for vehicular ad hoc networks. Comput. Commun. **36**(13), 1422–1435 (2013)
14. Zeng, X., Bagrodia, R., Gerla, M.: GloMoSim: a library for parallel simulation of large-scale wireless networks. In: ACM SIGSIM Simulation Digest, vol. 28, pp. 154–161. IEEE Computer Society (1998)
15. Zhu, M., et al.: Public vehicles for future urban transportation. IEEE Trans. Intell. Transp. Syst. **17**(12), 3344–3353 (2016)