Machine Learning Approach for Multiple Misbehavior Detection in VANET

Jyoti Grover, Nitesh Kumar Prajapati, Vijay Laxmi, and Manoj Singh Gaur

Department of Computer Engineering
Malaviya National Institute of Technology, Jaipur, India
{jyoti.grover,prajapati5nitesh,vlgaur,gaurms}@gmail.com

Abstract. The motivation behind Vehicular Ad Hoc Networks (VANETs) is to improve traffic safety and driving efficiency. VANET applications operate on the principle of periodic exchange of messages between nodes. However, a malicious node may transmit inaccurate messages to trigger inevitable situations. Each transmitted packet contains the status of sender like its identity, position and time of sending the packet in addition to safety message. A misbehaving node may tamper with any information present in the propagated packet. Fake messages may be created by attacker node itself or it may force another node to create fake messages. In this paper, we present a machine learning approach to classify multiple misbehaviors in VANET using concrete and behavioral features of each node that sends safety packets. A security framework is designed to differentiate a malicious node from legitimate node. We implement various types of misbehaviors in VANET by tampering information present in the propagated packet. These misbehaviors are classified based upon multifarious features like speed-deviation of node, received signal strength (RSS), number of packets delivered, dropped packets etc. Two types of classification accuracies are measured : Binary and Multi-Class. In Binary classification, all types of misbehaviors are considered to be in a single "misbehavior" class whereas, Multi-class classification is able to categorize misbehaviors into particular misbehaving classes. Features of packet sending nodes are extracted by performing experiments in NCTUns-5.0 simulator with different simulation scenario (varying the number of legitimate and misbehaving nodes). Proposed framework for classification of misbehavior is evaluated using WEKA. Our approach is efficient in classifying multiple misbehaviors present in VANET scenario. Experiment result shows that Random Forest and J-48 classifiers perform better compared to other classifiers.

1 Introduction

Vehicular Ad Hoc Networks (VANETs) applications are based upon the frequent exchange of safety messages by vehicles. This is also required to facilitate route planning, road safety and e-commerce applications. VANET security is an essential component for each of these applications. VANET is a typical kind of Mobile Ad Hoc Network (MANET). High mobility, large scale and frequent topology changes are the main characteristics of vehicular networks. Vehicle passenger safety can be improved by means of inter-vehicle communication. For example, in case of an accident, VANET communication can be used to warn other vehicles approaching the site.

A. Abraham et al. (Eds.): ACC 2011, Part III, CCIS 192, pp. 644–653, 2011.

VANETs are facing a number of security threats [1] which may degrade the performance of VANET and even life safety. For example, an attacker node may create an illusion of traffic congestion by pretendig multiple vehicles simultaneously and launch Denial of Service (DoS) attack by impairing the normal data dissemination operation.

In this paper, we introduce different kind of attacks based upon the physical properties and safety packet distribution behavior of nodes in VANET. Usually, a node observing a critical event triggers safety warning packets. All the nodes receiving this message forward it to other nodes in their transmission range. In this manner, it is the responsibility of honest nodes to forward each received safety packet to other nodes in its neighborhood. Terms *attackers, malicious node, misbehaving node, illegitimate node* are used interchangeably in this paper.

We perform a series of experiments with different number and type of misbehaviors and derive features from physical and packet transmission characteristics of honest and misbehaving nodes. We construct various instances of honest and misbehaving nodes. Machine learning method is used to classify the behavior as `honest` or `malicious`. Our classification algorithms are able to differentiate different kinds of misbehaviors during classification phase. Features used for classification are speed deviation, distance, received signal strength (RSS), number of packets generated, delivered, dropped, collided. These features are calculated by nearby observer nodes. All observer nodes exchange their observation with other nodes in its vicinity. The experiments are evaluated using Naive Bayes, IBK, J-48, Random Forest and Ada Boost1 classifiers [15] supported by Waikato Environment for Knowledge Analysis (WEKA) [2], which is a data mining tool. As per our knowledge, machine learning method has not been previously applied to distinguish different misbehaviors in VANET. Specifically, the major contributions of our paper are:

1. Implementation of variants of misbehaviors in VANET.
2. Extract the features that may be used in differentiating misbehavior instances.
3. Classification of misbehaviors using machine learning method.

The rest of this paper is organized as follows. Section 2 discusses related work on misbehaviors in VANET and their detection methodologies. Section 3 provides overview of VANET and attacker model. In Section 4, a brief outline of proposed methodology is introduced. It discusses different features, feature extraction module used in classification of misbehaviors in VANET. Experimental setup and results are discussed in Section 5 and 6 respectively. Concluding remarks with future work are covered in Section 7.

2 Related Work

Various types of attacks on an inter-vehicle communication system are presented by Aijaz *et al* [1]. They analyze how an attacker may manipulate the input of an OBU and sensor readings. The authors proposed plausibility checks using constant system examinations. However, this paper does not discuss how to apply plausibility checks in detail.

M. Raya and J.P. Hubaux [3] discuss a number of unique challenges in VANETs. They describe how adversaries use safety applications to create various attacks and

security problems. However, they have not analyzed how to achieve these attacks and do not provide solutions to address these security threats.

Golle *et al* [4] propose an approach for detecting and correcting malicious data in VANET. In this approach, every vehicle builds a model of VANET in which specific rules and statistical properties of VANET environment are implemented and stored. When a node receives a message, it compares the received message with the VANET model. If the received message does not comply with the VANET model, it is considered to be an invalid message. The VANET model used in this paper is predefined and does not provide the flexibility to switch to a new one. Ghosh *et al* [5][6] present a misbehavior detection scheme (MDS) for post crash notification (PCN) applications. They consider various parameters such as tuning and impact of mobility on performance of MDS. In their work, OBUs determine the presence of bogus safety message by analyzing how the driver behaves in response to an event.

Raya *et al* [7] have formulated a misbehavior detection system to exclude malicious vehicles from the communication system. It is based on the deviation of attacker node from normal behavior. Cryptographic keys belonging to a malicious node are revoked upon its detection. Normal and abnormal behavior is differentiated by using a clustering algorithm. Yan *et al* have proposed a position verification approach for detection of position related misbehaviors in [8]. Xiao *et al* [9] illustrate a localized and distributed scheme to detect ID spoofing attack in VANETs. This approach takes advantage of VANET traffic patterns and road side base stations. Their detection approach uses statistical analysis of signal strength distribution.

Raya *et al* [10] present their work on "data centric trust" in VANETs. They confirms the occurrence of an event based upon the messages received from multiple vehicles. They propose that vehicles use a decision logic system like Dempster-Shafer, Bayesian inference in their framework. However, their work assume that vehicles leave their radio range rapidly. Hence, it removes the use of reputation and ignores information from local sensors. Schmidt *et al* [11] construct reputation models for other vehicles based on the claims from sending vehicles. In this way, they create a model for normal behavior of nodes in VANET. If the behavior of a node differs from the normal behavior, it is marked as suspicious.

Kim *et al* [12] have introduced a message filtering model that leverages multiple complementary sources of information. They constructed a multi-source detection model so that drivers are alerted after multiple sources prove the existence of a certain event. Our framework is somewhat similar to the above with an exception that we are also able to classify different types of misbehaviors apart from just being able to identify them.

3 System and Attacker Model

VANET consists of two basic components: (1) Road Side Unit (RSU) and (2) On Board Unit (OBU). RSU is a fixed unit while OBUs are installed in vehicles and hence these are mobile. Each node in VANET consists of an Event Data Recorder (EDR), Global Positioning System (GPS) receiver, computing platform and a radar. A conceptual architecture of VANET is shown in Figure 1. There is a hierarchy of central authorities (CA) that is responsible for managing vehicles identities registered in its respective

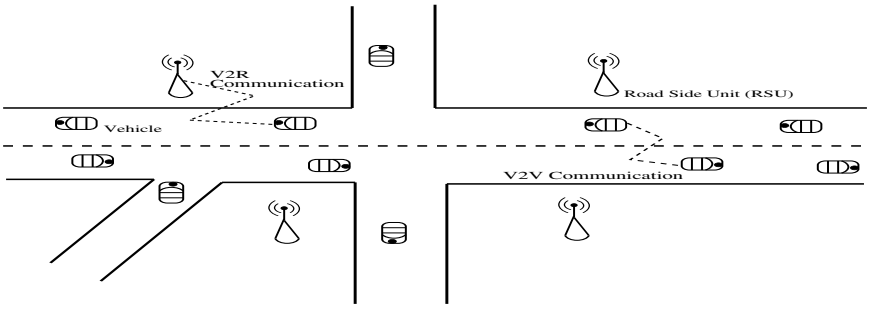

Fig. 1. Architecture of Vehicular Ad Hoc Network

geographic region. As communication framework, dedicated short range communication (DSRC) protocol [13], currently being standardized as IEEE 802.11p is used at data link layer. This protocol provides transmission range of 250 to 1000m and data rates in the 6-27Mbps range.

In VANET, all information is publicly available as safety messages are meant for each vehicle. Safety communication system of VANET differs from the usual approach in information systems where restrictions can be applied to access the system. VANET vulnerabilities originate from openness of wireless communication channel (can be accessed by anyone) and unencrypted exchange of information.

We consider active attackers only and they posses capability to compromise the integrity of messages. Each node transmitting a safety/alert packet dispatch its identity, position and time-stamp with the packet. However, a misbehaving node may tamper with any of the information sent in the packet. For example, attackers may create bogus alerts or suppress legitimate messages. Malicious nodes may generate wrong traffic warning message and propagate it to other vehicles in the network. These active attackers may force legitimate drivers to change their driving behavior. For example, honest vehicles may slow down or take alternate routes if fake messages regarding harmful events are distributed in the network. As a result, malicious nodes succeed in disruption of normal driving behavior of vehicles. Attackers may also suppress valid messages of critical safety information by dropping or capturing them. Malicious node may generate fake packets in place of forwarding valid packets. We briefly discuss different types of VANET misbehaviors implemented in this paper:

1. **Packet Suppression Attack:** In this attack, whenever a vehicle receives safety packets from a neighboring node, it does not forward these packets unlike the normal functionality of VANET. All the legitimate nodes in VANET forward every received safety packet, but malicious nodes do not follow this approach. Misbehaving nodes can also insert fake safety packets in the network.
2. **Packet Replay Attack:** Replay attack is a form of attack in which a normal data transmission is fraudulently repeated or delayed. This operation is carried out by a malicious node that intercepts the safety packet and retransmits it. Replay attack is usually performed by malicious or unauthorized node to impersonate a legitimate vehicle or RSU. It creates an illusion of apparently valid though non-existing events.

3. **Packet Detention Attack:** This attack is a subset of the packet replay attack. In this attack, a vehicle delays the packet forwarding process by certain time duration in the network. It is more dangerous than replay attack, as vehicles do not get enough time to respond to a particular emergency situation. For example, a honest vehicle $V1$ may broadcast *TRAFFIC JAM* safety packet at time-stamp t_0 to its neighboring nodes. This message is sent after some delay by a malicious vehicle. After receiving another *TRAFFIC JAM* packet, vehicles may change their path to nearby road-segment thereby leading to real congestion on this route even though the jam may have cleared by this time.
4. **Identity Spoofing Attack:** This attack is a impersonation or spoofing attack where an attacker spoofs the identity of another node in the network and hence, all the messages directed to the victimized node are received by the attacker. The attacker can feign safety message by using multiple identities simultaneously to create illusion of non-existing events.
5. **Position Forging Attack:** In this attack, an attacker broadcasts timely coordinated wrong traffic warning messages with forged positions, leading to illusion of a car accident, a traffic jam or an emergency braking.
6. **Combination of Identity and Position Forging Attack:** In this attack, attacker may use multiple identities while launching position forging attacks.

We have created variants of these attacks. First three misbehaviors are temporal, i.e. related to *time* of sending the packets, which plays a key role for VANET applications. Invalid value of *Position* and *Identity* fields in packet is also responsible for creating illusion of non-existing events.

In all attacks, the main objective of malicious node is to distrupt VANET traffic and part thereof. By assuming false identity or spoofing identities, malicious node's aim is to evade detection. The main contribution of this paper is detection of misbehavior instances, detecting node responsible for this misbehavior is beyond the current scope of the paper.

We assume that vehicles communicate using the Dedicated Short Range Communication (DSRC) technology. Majority of vehicles are honest. In our case, only up to a 25% of vehicles are assumed to be illegitimate. In our model, it is assumed that RSUs are always honest. All the vehicles trust the message generated by RSUs.

4 Proposed Methodology

Our proposed methodology uses classification algorithms supported by WEKA [2]. It is used to train and test malicious and legitimate instances. Figure 2 describes our detection approach. It shows different steps involved in classification of samples (either as legitimate or particular type of misbehavior).

In *Feature extraction module*, we extracted features from different attack cases which are able to differentiate various types of misbehaviors. Different inputs of feature extraction module are: (1) VANET model, (2) Attack model and (3) VANET application which is affected by attack. A series of experiments are performed in NCTUns-5.0 [14] by mutation of varied number of legitimate and misbehaving nodes to extract the indiscriminated features. These extracted features are applied to the classification algorithms

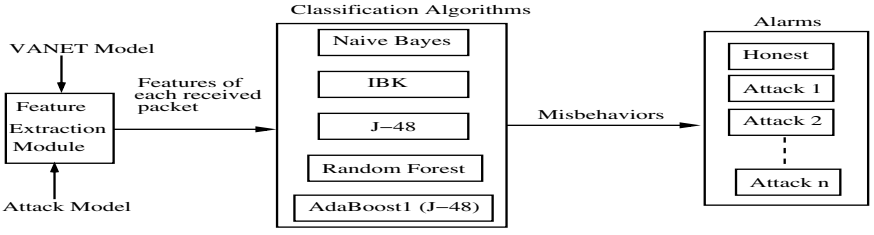

Fig. 2. Proposed Design for classification of legitimate and misbehaving nodes

like Naive Bayes, IBK, AdaBoost1 (with J-48 as base classifier), J-48 and Random Forest (RF) algorithms [15] in WEKA [2]. Finally, various misbehaviors are differentiated based upon these features. We briefly describe features used for classification.

Features are the attributes used to classify different types of misbehavior in VANET. Classifications are performed on relevant attributes or patterns existing with higher frequency to classify a sample as legitimate node or misbehaving node. We derive following features after performing sequence of experiments with different combinations of above defined attacks in VANET scenario. These features are normalized after their node-wise extraction at each interval of time.

- **Geographical Position validation:** Nodes receiving the safety messages verify whether the message is generated by the node located within the area of critical situation or not.
- **Acceptance Range Verification w.r.t observing RSUs:** Uniformly deployed RSUs in VANET scenario verify the acceptance range of each received packet. This operation is performed by measuring the difference between the sending vehicle and RSU position at each time interval. If this difference is greater than the acceptance range, the received message is discarded.
- **Speed Deviation verification:** Consistency in speed at consecutive time interval is verified for each vehicle. This is required to verify fake position broadcasts in the network.
- **Received Signal Strength (RSS):** This parameter is required to verify ID spoofing attacks. RSS value of attacker vehicle and spoofed vehicles is same for the attack duration.

Features related to verification of geographical position, acceptance range, speed and RSS are required to classify position and identity spoofing (Sybil) attacks. Features related to safety packet distribution behavior (Number of packets transmitted, received, dropped, captured) are responsible to classify temporal attacks. These features may be difficult to estimate accurately in the real scenario of VANET. It is assumed that nodes transmit information about packet transmitted/received and packet delivery ratio (PDR) periodically to RSUs within range. All RSUs exchange this information to estimate these features. Though malicious nodes may falsify this information, it is assumed that low number of such nodes in a large network like VANET may not have much impact on the performance of network.

Though we collected legitimate and malicious samples through simulations, it must be noted that features related to delivery time of packets can't be accurately determined in realistic VANET scenario. The features used to detect ID and position spoofing attacks are equally applicable in realistic scenarios. Following are the features used to detect temporal attacks in VANET.

- **Packets Transmitted:** It is the total number of packets generated by each node.
- **Packets Received:** It is the total number of packets received by each node.
- **Packet Delivery Ratio:** It is defined as the ratio of number of packets received and number of packets transmitted. This parameter is required to determine the probability of presence of temporal attacks (packet detention, replay and suppression attacks).
- **Packet Drop Ratio:** It is defined as the ratio of number of packets dropped and number of packets transmitted.
- **Packet Capture Ratio:** It is the ratio of number of captured packets and transmitted packets.
- **Packet Collision Ratio:** It is the ratio of number of packet collisions and transmitted packets.
- **Packet Retransmission Error Ratio:** It is the ratio of number of packet retransmission errors and transmitted packets.

5 Experimental Setup

We conducted our experiments using NCTUns-5.0 simulator [14], an integrated network and traffic simulation platform. This platform provides multiple features including road network simulation, communication and network protocol simulation, vehicular traffic simulation and feedback loop among vehicles. In our experiments, we simulated a two–direction 6 km highway with multi lanes in each direction. Simulation time is varied between (20–2000 seconds). Varying number of Vehicles are randomly deployed and have different behavior including speed (10–50 m/s), acceleration and deceleration. Inter vehicle distance is also varied for each experiment i.e. density is also a variable factor. Traffic arrival rate is 500 vehicles/hour and transmission range is 250 meters. Each experiment is run 5-10 times with different seed values. Average of these results is calculated. We vary different parameters for deriving multiple samples used in classification. We applied a widely used radio propagation model – 'shadowing model' – to consider the multi–path propagation effects of the real world communication system.

Packet replay, suppression and detention attacks are basically related to delivery time of packets. If the packets are not delivered in time, it can lead to serious mishappenings. Packet may contain some important information like traffic jam ahead or any information related to road blockage due to accidents or any other natural calamities like landslides. In a packet suppression attack, the number of packets which are to be delivered get reduced. There may be some other reason for the delay in the delivery of packets such as collision and congestion in the network. For the above reason, we calculated a threshold value of the packet delivery ratio by running a number of experiments and training these results using Weka.

ID and position spoofing attacks are implemented as follows. Whenever a misbehaving node is about to send a beacon packet to announce its present ID and position, it selects an ID randomly on the field and applies it to the beacon packet (rather than applying its real ID and position). Whenever a malicious node receives any safety message, it drops this packet. Number of fake identities bounded with illegitimate node is varied in each experiment.

6 Results and Analysis

In this section, we analyze the results produced after classification. All classifiers use 10-fold cross-validation for training and testing samples. Our experimental results are evaluated using the following evaluation metrics [16]. True positive (TP) is the number of malicious vehicles correctly identified as malicious. False positive (FP) is the number of legitimate nodes incorrectly identified as malicious vehicle. True negative (TN) is the number of legitimate nodes correctly identified as a legitimate vehicle. False negative (FN) is the number of malicious nodes incorrectly identified as legitimate. The performance of classifiers can be measured by analysing the following parameters.

- **True Positive Rate (TPR):** It is the ratio of malicious vehicles correctly classified as malicious. It is defined as $TPR = TP/(TP+FN)$
- **False Positive Rate (FPR):** It is the proportion of legitimate vehicles incorrectly classified as malicious. It is also called `false alarm rate` and defined as $FPR = FP/(FP+TN)$.
- **True Negative Rate (TNR):** It is the proportion of legitimate vehicles identified as legitimate. It is defined by the expression $TNR = TN/(TN+FP)$.
- **False Negative Rate (FNR):** It is defined as the proportion of malicious nodes incorrectly identified as legitimate. It is evaluated as $FNR = FN/(FN+TP)$.

The classifiers are trained with various features consisting of 3101 legitimate and 1427 malicious samples (184 packet detention + 200 replay + 370 suppression + 300 Identity forging + 373 Position forging samples). Table 1 shows the binary-class and multi-class classification accuracy using attributes of legitimate and misbehaving vehicles. In binary-class classification, all types of misbehaviors are considered to in a single "misbehavior" class. Multiclass classification is a special case of statistical classification. It is used to assign one of several misbehaving class labels to an instance. Multiclass classification is more complex as compared to binary classification. We observe from this table that `Random Forest` (RF) and `J-48` classifier outperform rest of the classifiers in terms of high values of TPR, TNR and small values of FPR, FNR. The reason for better classification is the *bagging* and *boosting* properties of these classifiers. Whereas, `Naive Bayes` classifier shows poor results as compared to other classifiers. Improved multi-class classification accuracies can also be seen in Table 1.

We have shown through simulations that our proposed approach shows promising results on legitimate and malicious instances gathered from the simulation process. However, in a realistic VANET scenario, the proposed approach may be unsuitable to detect temporal attacks because of unavailability of packet transmit/receive information by individual node.

Table 1. Classification accuracy using various attributes of legitimate and misbehaving vehicles

Classifiers	Binary-Class				Multi-Class			
	TPR	FPR	TNR	FNR	TPR	FPR	TNR	FNR
Naive Bayes	0.42	0.03	0.96	0.57	0.32	0.01	0.98	0.67
IBK	0.56	0.11	0.88	0.43	0.58	0.04	0.95	0.41
J-48	**0.92**	**0.01**	**0.98**	**0.07**	**0.93**	**0.004**	**0.99**	**0.06**
RF	**0.92**	**0.01**	**0.98**	**0.07**	**0.93**	**0.005**	**0.99**	**0.06**
AdaBoost1	0.92	0.02	0.97	0.07	0.93	0.008	0.99	0.06

A distributed approach in realistic scenario can be used to evaluate the parameters required for temporal attacks detection. In this approach, all VANET nodes (vehicles and RSUs) observe the functionality of their neighboring nodes (nodes present in their vicinity). Each node that generates a safety packet overhears the further forwarding of that packet by all receiving nodes. Features of VANET like mobility, presence of RSUs in the form of traffic and road lights and traffic pattern can be used in this approach. RSUs can record the trajectories of vehicles moving across them and exchange it with others RSUs or vehicles. In this manner, all nodes exchange observations regarding the send and receive time of each packet, thereby contributing to generation of parameters required to detect temporal attacks in VANET. We use the benefit of availability of this information in the simulator for temporal attack detection in our implemented approach.

7 Conclusion

Misbehaving vehicles are disastrous for any VANET application. Misbehavior detection mechanisms are becoming prominent area of research in VANET. In this paper, we implemented various forms of misbehaviors in VANET. Features of each form of misbehavior is extracted. These experiments are performed using various combinations of misbehaviors. We have designed a framework for binary and multi-class classification to differentiate between (legitimate and malicious behavior) and (legitimate and particular class of misbehavior) respectively. The results are validated using evaluation metrics computed by various classifiers. We observe that `Random forest` and `J-48` classifiers signify the perfect classification of malicious vehicles with high values of TPR, TNR and small values of FPR and FNR. The basic framework proposed in this paper can be made compatible with any type of misbehaviors induced in a particular application. As a part of future work, we would like to implement detection approach for temporal attacks in realistic scenario.

References

1. Aijaz, A., Bochow, B., Dtzer, F., Festag, A., Gerlach, M., Kroh, R., Leinmller, T.: Attacks on Inter Vehicle Communication Systems - an Analysis. In: Proc. WIT, pp. 189–194 (2006)
2. University of Waikato: Open Source Machine Learning Software Weka, `http://www.cs.waikato.ac.nz/ml/weka`

3. Raya, M., Hubaux, J.P.: Securing Vehicular Ad Hoc Networks. Journal of Computer Security 15(1), 39–68 (2007)
4. Golle, P., Greene, D., Staddon, J.: Detecting and Correcting Malicious Data in VANETs. In: Proceedings of the 1st ACM International Workshop on Vehicular Ad Hoc Networks (VANET 2004), pp. 29–37. ACM, New York (2004)
5. Ghosh, M., Varghese, A., Kherani, A.A., Gupta, A.: Distributed Misbehavior Detection in VANETs. In: Proceedings of the 2009 IEEE Conference on Wireless Communications and Networking Conference, pp. 2909–2914. IEEE, Los Alamitos (2009)
6. Ghosh, M., Varghese, A., Kherani, A.A., Gupta, A., Muthaiah, S.N.: Detecting Misbehaviors in VANET with Integrated Root-cause Analysis. Ad Hoc Netw. 8, 778–790 (2010)
7. Raya, M., Papadimitratos, P., Aad, I., Jungels, D., Hubaux, J.P.: Eviction of Misbehaving and Faulty nodes in Vehicular Networks. IEEE Journal on Selected Areas in Communications, Special Issue on Vehicular Networks 25(8), 1557–1568 (2007)
8. Yan, G., Olariu, S., Weigle, M.C.: Providing VANET Security Through Active Position Detection. Comput. Commun. 31(12), 2883–2897 (2008)
9. Xiao, B., Yu, B., Gao, C.: 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 (DIWANS 2006), pp. 1–8. ACM, New York (2006)
10. Raya, M., Papadimitratos, P., Gligor, V.D., Hubaux, J.P.: On data centric trust establishment in ephemeral ad hoc networks. In: IEEE INFOCOM (2008)
11. Schmidt, R.K., Leinmuller, T., Schoch, E., Held, A., Schafer, G.: Vehicle Behavior Analysis to Enhance Security in VANETs. In: Vehicle to Vehicle Communication, V2VCOM (2008)
12. Kim, T.H., Studer, H., Dubey, R., Zhang, X., Perrig, A., Bai, F., Bellur, B., Iyer, A.: VANET Alert Endorsement Using Multi-Source Filters. In: Proceedings of the Seventh ACM International Workshop on VehiculAr InterNETworking, pp. 51–60. ACM, New York (2010)
13. Jiang, D., Delgrossi, L.: IEEE 802.11p: Towards an International Standard for Wireless Access in Vehicular Environments. In: Vehicular Technology Conference (VTC-2008), pp. 2036–2040. IEEE, Los Alamitos (2008)
14. NCTUns 5.0, Network Simulator and Emulator, `http://NSL.csie.nctu.edu.tw/nctuns.html`
15. Witten, I.H., Frank, E.: Data Mining: Practical Machine Learning Tools and Techniques with Java Implementations. Morgan Kaufmann, San Francisco (1999)
16. Fawcett, T.: An introduction to ROC analysis. Pattern Recogn. Lett. 27(8), 861–874 (2006)