An Intrusion Detection System Against Malicious Attacks on the Communication Network of Driverless Cars

Khattab M. Ali Alheeti
School of Computer Sciences and Electronic Engineering
University of Essex, Colchester, UK
University of Anbar, College of computer - Anbar, Iraq
kmali@essex.ac.uk

Anna Gruebler, Klaus D. McDonald-Maier
School of Computer Sciences and Electronic Engineering
University of Essex
UK Colchester
contact@annagruebler.com, kdm@essex.ac.uk

***Abstract*—Vehicular ad hoc networking (VANET) have become a significant technology in the current years because of the emerging generation of self-driving cars such as Google driverless cars. VANET have more vulnerabilities compared to other networks such as wired networks, because these networks are an autonomous collection of mobile vehicles and there is no fixed security infrastructure, no high dynamic topology and the open wireless medium makes them more vulnerable to attacks. It is important to design new approaches and mechanisms to rise the security these networks and protect them from attacks. In this paper, we design an intrusion detection mechanism for the VANETs using Artificial Neural Networks (ANNs) to detect Denial of Service (DoS) attacks. The main role of IDS is to detect the attack using a data generated from the network behavior such as a trace file. The IDSs use the features extracted from the trace file as auditable data. In this paper, we propose anomaly and misuse detection to detect the malicious attack.**

Keywords—security; vehicular ad hoc networks; intrusion detection system; driverless car.

I. Introduction

A vehicular ad hoc network (VANET) is a self-configuring and self- adaptive network of wireless links that connect mobile vehicles. It is a group of wireless mobile vehicles that cooperate by sending or receiving packets of data, to or from each other's nodes allowing them to communicate beyond the direct wireless transmission possible in the individual vehicle radio range [1]. Each vehicle in the vehicular ad hoc network can act as a router or a host [1]. The VANETs allow vehicles to communicate directly with each other (V2V), stations (V2I) and roadside units (RSUs) in the absence of a fixed infrastructure [2]. VANETs can be used on Intelligent Transportation System (ITS) to ensure the safety and comfort for road users [3]. The main objective of VANETs is to protect the passengers, drivers and the vehicle itself. These networks provide security and achieve their goals by exchanging cooperative awareness messages (CAMs) [4]. Furthermore, these networks play a main and vital role in self-driving cars because they eliminate time and space constraints and make information available to the vehicle when required. However, certain characteristics of these networks have resulted in vulnerabilities at all levels. These characteristics are: the open wireless medium, the highly dynamic network topology and the absence of traditional security infrastructure [5]. In addition, there are other concerns which have increased their vulnerability, namely the routing mechanism and the auto-configuration [5]. VANETs have unique features that distinguish them from conventional networks, such as high-speed, mobility and density of vehicles on the road. These features make procuring network security a challenging and threat prone task [1].

A new generation of vehicles being researched are called self-driving vehicles. These vehicles are considered a revolution in the automotive industry as these vehicles did not officially appear as vehicles in markets until recently. Vehicle manufacturers used to collaborate with communication companies before the advent of self-driving vehicles. Vehicles have started being equipped with communication devices On Board Units (OBU), which consist of omni directional antennas, at least one processor, a Global Position System (GPS), and an array of sensors for V2V and V2I communications [6]. In addition, these devices are able to generate emergency messages such messages to notify of emergent braking, traffic jams or accidents. These early messages send to the vehicles enable them to avoid congestion and accidents through detours or changing lanes. Figure 1 shows RSUs, vehicles and the occurrence of an accident. Once an accident has occurred, CAMs are generated and communicated to the RSUs and other vehicles in that zone.

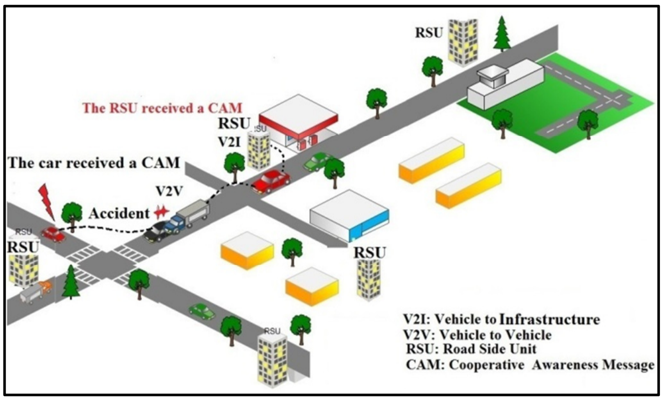

Fig. 1. An example of the process of responding to cases of emergency on the road

We propose a new approach to secure external communication in self-driving and semi self-driving vehicles from potential attacks. The main motivation for this security system is the real-time detection of malicious vehicles in the VANET's environment. The intelligent intrusion detection system (IDS) has the ability to detect abnormal or malicious behavior and isolate a malicious vehicle from communicating with the system. The detection system relies only on data collected from the network in the form of a trace file.

This paper is organized in the following way: Section II explores related work in the research area of attacks on VANETs. Section III describes the methodology and section IV explains the experimental results. Section V shows the dissection. Section VI is conclusions and future work.

II. Related works

VANETs face many security problems in the communication system. The role of the security system is collecting traffic data from the VANETs, analyzing it, and then detecting and predicting any abnormal behavior in the network.

VANETs provide critical information for emergency real-time applications, therefore, security and privacy become a very important issue. The VANETs enable self-driving and semi self-driving vehicles to avoid or reduce problems such as drivers' error by either making desired decisions or by sending CAMs to other vehicles, one of the most significant requirements for VANETs is security.

VANETs face many types of attacks, we have chosen to focus on the attack. As we know, self-driving vehicles rely heavily on communication with their external environment in order to make decisions. DoS attacks can have two different objectives [7]:

1) Control of a vehicles' resources.

2) Jamming the communication channels.

In this case, we can infer that the DoS attacks have direct negative impact on the life of passengers and on the vehicles themselves, when it prevents the arrival of warning messages from and to other vehicles [8]. Therefore, they are internal or external attacks that have a direct impact on the network by denying users the available resources [9]. The main motivation of selecting the DoS attack is that it can be launched against any layer in the network [10] and is therefore a high priority to defend against.

Yan et al. proposed a novel solution to this security problem, namely; a combinatorial approach to collect data from three different resources: radar detection, traffic and neighboring data. Thus, the system computed the similarity between these data [11]. Liu et al. designed a system to secure the communications system for the vehicles depending on roadside units. Their infrastructure contained a Certification Authority (CA) based cluster distributed in different regions. The aim was to show that IDS using a CA database provided more protection against malicious vehicles with legal certificates [12]. Al-Mutaz et al. presented a new protocol for the detection of Sybil attacks in vehicular networks. The proposed technique was based on reports periodically collected by the road side units regarding the status of their physical neighborhood. This new technology was based on the platoon model, through which the protocol could identify abnormal vehicle behaviors. The platoon is considered one of the features generated by the vehicles through their communication across networks. This takes place through periodic messages, which the attacker tries to jam. It is this jamming that affects the vehicles' ability to achieve the platoon [13]. Lyamin et al., proposed an algorithm for detecting denial of service attacks in real-time based on some performance metrics such as the percentage of false alarms for any jamming channel and the average beacon time for vehicular ad hoc networks [14]. Lakshmi et al., focused on the importance of protecting VANETs by isolating malicious vehicles that were designed to damage the performance of the network. To identify a malicious vehicle they measure the performance of the network in terms of a packet's delivery ratio, dropped packets, the average end-to-end delay and routing overhead. [15]. Thajeal, discussed the vulnerabilities in ad hoc wireless networks, and described an IDS using ANN. Researchers have shown the possibility of the application of cooperative statistical anomaly detection models to protect against attacks on routing protocols, on wireless MAC protocols or on wireless applications and services [16]. Singh et al., proposed a detection system to detect malicious nodes based on data mining in MANETs. The security system uses three stages: collect the dataset, analysis and detection. The core of detection was based on the data extracted from the trace file that was generated by using Network Simulation version 2 (NS2) [17].

There are two types of IDSs, misuse and anomaly detection systems [18]. Anomaly detection systems are based on the normal behavior of a subject and any action that significantly deviates from the normal behavior is considered intrusive. However, this type of systems has a high positive detection error, difficulty handling gradual misbehavior and expensive computation. The misuse detection systems are based on the characteristics of known attacks or system vulnerabilities, which makes them highly effective, but they cannot detect novel types of attacks. In our research, we propose a system that uses both types of IDSs

III. Methodology

In this paper, we propose a security system for external communication for self-driving and semi-self-driving vehicles that depends on intelligent IDS. The security system is based on data collected from the network. The steps below explain the methodology:

A. *Mobility model*

We used two tools to generate a real-world traffic of normal and malicious behavior and mobility models for vehicle's ad hoc networks. These tools are Simulation of Urban Mobility Model (SUMO) and MObilty VEhicles (MOVE) [19]. MOVE is designed on SUMO. The output file of these tools is a mobility file for the vehicles that is an image of the real world; these files are used as input to NS2 [20]. The files of the map (file name.net.xml) and route (file name.rou.xml) were used to produce SUMO trace files (file name.sumo.tr) that were then imported to MOVE and converted to the NS2 format for the VANETs' analysis. Generally, mobility models are divided into two types: urban mobility models and highway mobility models [21]. The urban mobility model includes many types of models such as the Random Way Point (RWM) model, Manhattan mobility model and Rice University Model (RUM). In this paper, we use the Manhattan model because it allows vehicles to move in vertical or horizontal direction. Another reason for the use of this model is widely used in the research field [21].

B. Simulation environment

We created a VANET's environment on the NS2 simulator as shown in figure 2 and selected one of the vehicles as a malicious vehicle. The NS2 is designed to simulate different networks such as wired and wireless networks [22]. However, we face a problem in simulating the VANETs with NS2 because the simulator is not designed specifically for VANETs. In this case, we need extra tools to achieve the simulation: SUMO, MOVE and City Mob (generate mobility model) [23]. We use the network simulation version 2 (NS2.35) [22] and mobility system to achieve the IDS for VANETs in the real world.

A screenshot of NS-2 utilizing Network the Animator (NAM) trace file is shown in figure 2.

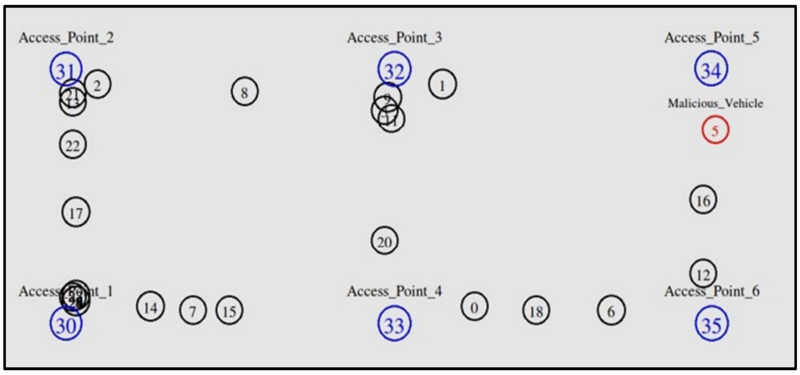

Fig. 2 Screenshot of Simulation in NS-2 NAM

One of the important issues in the simulation system is the initial parameters. They specify the performance and the behavior in NS2. Some parameters used in simulating the VANETs are: Constant Bit Rate (CBR) application that sends constant packets through the transport protocol such as (UDP), Radio Propagation Model (Two Ray Ground) in table 1 [22].

Table 1 Simulator Environmental and Parameters

Parameter	Value
Simulation time	250s
Number of nodes	30 Vehicles
Number of RSUs	6 RSUs
Type of Traffic	Constant Bit Rate (CBR)
Topology	600 x 400 (m)
Transport Protocol	UDP
Packet Size	512
Routing Protocol	AODV
Channel type	Wireless
Queue Length	50 packets
Number of Road Lanes	2
Radio Propagation Model	Two Ray Ground
MAC protocol	IEEE 802.11
Speed	50 m/s
Interface queue type	Priority Queue
Network Interface type	Physical Wireless
Mobility Models	Manhattan Mobility Model

C. Malicious behavior

To measure and evaluate the performance of IDSs, we need to generate two types of behavior: normal and malicious. A vehicle is called malicious when it drops the packets. The malicious behavior is created in NS2 using the Tools Command Language (TCL) script and the database extracted from the trace file. In this case, we need to modify some files of the routing protocol to generate the abnormal behavior (select which vehicles are to drop packets rather than forward them to the a destination vehicle). In our work, we add a malicious vehicle to the AODV routing protocol. Because of the change in behavior, the trace file generated from the malicious vehicles has different characteristics than the trace file generated from the normal behavior.

The VANETs environment consists of 30 vehicles and 6 RSUs on an NS2 simulator [22]. We create one malicious vehicle in our scenario.

D. Feature sets

The IDS relies on features that describe the events in the VANET. We can extract behavior from the trace file as it contains many different data (features) that can be used for analysis. These features describe normal and abnormal or malicious behavior.

A trace file is used to evaluate the performance of the proposed IDS. Trace files capture the events of the network that can be used for performance evaluation, e.g. the amount of packets transferred between two vehicles, the delay in the transfer of the packets, packet drop. In this case, the type and the number of the features are very important for IDS. In our research, we train and test the IDS with all features of trace file that describe the normal and malicious behavior.

We can get five types of events feature from a trace file, these events are: send (s), receive (r), drop (D), forward (f) extracted and movement (M) [23]. The trace file is divided into three parts that are “basic trace”, “IP trace” and “AODV trace” information. It contains twenty five fields which are shown in the below table 2 [23].

Table 2 features of trace file

Basic Trace	IP Trace	AODV Trace
Event, Time, Trace level, Node Number, Packet ID, Payload Size and Type, Delay, Source and Destination MAC, and IP Packet	IP Source and Destination, Port Source and Destination, Time to Live and next Hope Node	Packet Tagged, Hope Counts, Broadcast ID, Destinatio IP with Sequence number, Source IP with Sequence number and Label of Record

E. Intelligent detection system

The intelligent detection system uses an ANN to identify malicious vehicles in VANETs. Current studies in the field of self-driving vehicles, confirm that ANN (Feed Forward) is the most efficient and convenient in design of internal and external systems for these vehicles [24]. The IDS (more than 32000 records) describe the behavior on the network whether normal or malicious. The dataset is divided into different groups, also it is again divided into three subsets, the first subset is the training set (50%), the second subset is the validation set (25%) and the third subset test set (25%).

The network training ends when the least-square-error E between the desired d_i and actual output y_i is less than Emax or when the number of sweeps equal 500, we define $E_{\max= 1*10^{-5}}$. For all experiments, the learning rate α was fixed to $1*10^{-6}$ for each training yielding difference, of which the best result is selected.

In our research, we used trial-and-error attempts to configure the best ratio of training depending on the condition put on the second phase of the proposal. Table 3 shows some of the configuration parameters used in the ANN.

Table 3 ANN Parameters

Parameter	Value
TrainParam. epochs	68
TrainParam.lr	$1*10^{-5}$
TrainParam. goal	0
TrainParam. min_grad	$1*10^{-14}$

We design the simulation on system with an Intel core i3 processor (2.53GHZ) and RAM memory (4GB).

F. The Proposed Model of IDS

The ANN used in this paper consists of three layers, an input, a hidden, and an output layer. An input layer consists of 25 neurons equal to the number of features in the features vector. The hidden layer consists of 5 neurons which the output layer consists of 3 neurons.

The proposed system has three stages, figure 3 shows the overall architecture of the proposed IDS, namely:

- The first stage (Data collection and Pre-processing)- The normal and malicious behavior for vehicles is built into the NS2, and a dataset is generated from the trace file. We extract the features from the data in the trace file. The features are preprocessed using normalization, transformation and uniform distribution.
- The second stage (Training)- In this we train the ANN with the extracted dataset (features).
- The third stage (Testing)- In this step, we test ANN with data features that describe malicious and normal behavior. After the trained ANN is stable, it can surveil the VANETs security by identifying the network control messages and data packets in real time and generating an alarm immediately if there is malicious behavior.

The malicious vehicles can perform many types of attacks such as DoS attacks [25] and we build a detection system for detecting the DoS attack. We detect the DoS attack by its behavior, such as flooding and dropping packets [26].

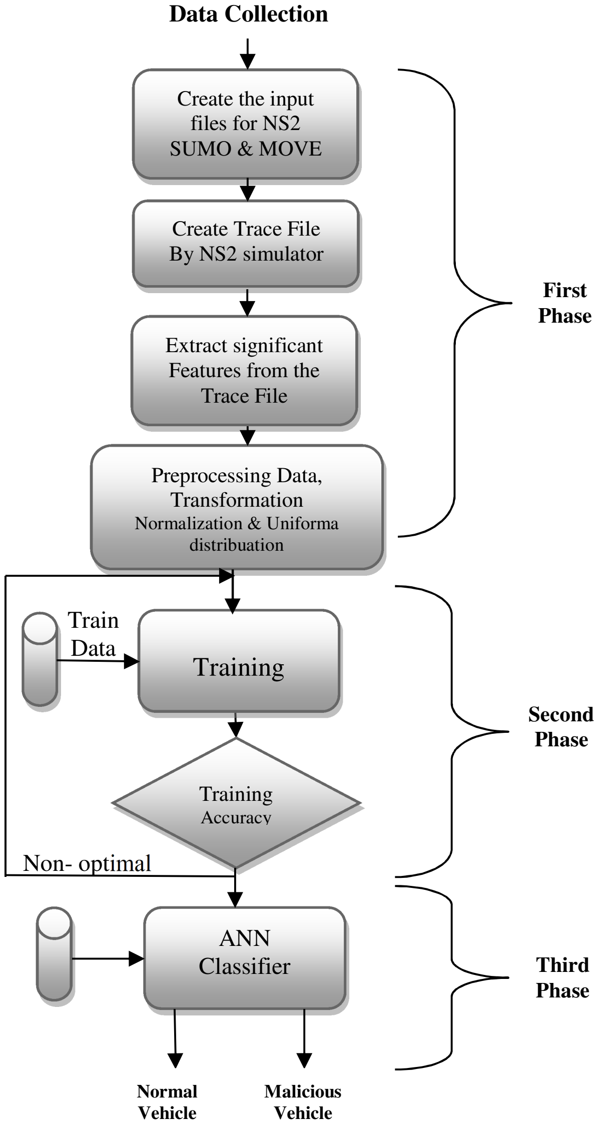
Data Collection
Create the input files for NS2 SUMO & MOVE
Create Trace File By NS2 simulator
Extract significant Features from the Trace File
Preprocessing Data, Transformation Normalization & Uniforma distribution
First Phase
Train Data
Training
Training Accuracy
Non- optimal
Second Phase
ANN Classifier
Third Phase
Normal Vehicle
Malicious Vehicle

Fig. 3 Architecture of IDS

The anomaly and misuse detection methods are based on an ANN that can learn the normal or abnormal behavior through the iterative process. The main reason for using the ANN is to reduce the cost, achieve real-time responsiveness and to be efficient [18].

IV. Experimental results

The detection system may be installed in three configurations: vehicles, RSU or both on the vehicles and RSU. In our study, we selected to install the detection system in vehicles. The security system can identify among two different behaviors: normal or abnormal/ malicious through IDS. In this section, we show the performance of the detection system. Detection accuracy is used as a performance metric to evaluate the IDS.

To measure and evaluate the performance of IDSs, we need to calculate four: True Positive (TP), False Positive (FP), True Negative (TN) and False Negative (FN). The accuracy of the system result should be calculated as follows [27]:

$$Accuracy = \frac{Number\ of\ correctly\ classified\ patterns}{Total\ number\ of\ patterns} \quad (1)$$

In addition, the measures will be calculated as follows [45]: Let

$TP =\neq normal\ connection\ record\ classified\ as\ normal$

$TN =\neq attack\ connection\ record\ classified\ as\ attack$

$FP =\neq normal\ connection\ record\ classified\ as\ attack$

$FN =\neq attack\ connection\ record\ classified\ as\ normal:$

$then$

$$TP_{Rate(sensitivty)} = \frac{TP}{TP + FN} \quad (2)$$

$$TN_{Rate(specificity)} = \frac{TN}{TN + FP} \quad (3)$$

$$FN_{Rate} = (1 - sensitivity) = \frac{FN}{FN + TP} \quad (4)$$

$$FP_{Rate} = (1 - specificity) = \frac{FP}{FP + TN} \quad (5)$$

A. Result of Training and Testing Neural Network with (Misuse Detection)

During the training and testing phase, we used the same dataset in both phases (signature), to calculate the total accuracy, true positive, false positive, true negative, false negative. Total accuracy of train = 98.97

The performance of classification and number of records used in the proposed system is shown in table 4.

Table 4 Accuracy of Classification

Attack Class	IDS				
	Real Record	ANN	Match Records	Miss Records	Accuracy
Normal	14533	14404	14379	25	98.94%
Abnormal	2868	2997	2843	154	99.12%
Unknown	0	0	0	0	NaN

The rates are calculated by equations (2,3,4 and 5) as shown table 5.

Table 5 Recognition Rate

Alarm Type	Accuracy
True positive	**99.82%**
True negative	**94.86%**
False negative	**0.17%**
False positive	**5.13%**

B. Result of Training and Testing Neural Network (Anomaly Detection)

During the training and testing phase, the data set used in the testing phase differs from the data set used in the training phase (anomaly). We calculate the total accuracy to evaluate the performance of the IDS. In this case, the IDS must be able to detect novel attacks, the performance of classification and number of records used in the proposed system is shown in table 6:

Table 6 Accuracy of Classification

Attack Class	IDS				
	Real Record	ANN	Match Records	Miss Records	Accuracy
Normal	28676	28790	28234	556	98.45%
Abnormal	3725	3609	3167	442	85.02%
Unknown	0	2	0	2	NaN

The rates are calculated by equations (2,3,4 and 5) as shown table 7.

Table 7 Recognition Rate

Alarm Type	Accuracy
True positive	**98.06%**
True negative	**87.75%**
False negative	**1.93%**
False positive	**12.248%**

V. Discussion

The main motivation of the proposed system is to implement a secure communication of self-driving cars by identifying malicious cars in VANETs. This system is implemented via three phases: data collection and pre-processing phase, training phase and testing phase.

This approach is characterized in that it integrates different techniques to get the best results in addition that a comparison with the expected theoretical results to ensure the effectiveness of the system.

Our experiments in NS2 show that the detection system is effective and efficient for identifying anomalies with a low false negative alarm rate, the error rate is 2.05%. The obtained results indicated that the calculated rate of alarms fluctuated between 94.86 and 99.82, which deal with good efficient accuracy. On the other hand, the anomaly detection system has a low false negative alarm rate of about 2% that is a good indicator of the results. However, the main problem is the high rate of false positives in anomaly detection because of the different records that describe both normal and abnormal behavior.

VI. Conclusion

Security and safety are a serious issue and a crucial requirement for self-driving and semi self-driving vehicles. The development of self-driving vehicles is in its initial phases and formal deployment of the technology is heavily dependent upon security and integrity of the systems involved. The detection of malicious vehicles in vehicular ad hoc networks can be achieved through the intelligent classification of messages and data being communicated. DoS attacks can have a direct impact on the life of passengers and on the vehicles themselves. This form of attack prevents the reception of CMA from vehicle to vehicle or infrastructure in that zone. In this case, IDS has become a very important solution to provide the required protection for VANETs. In our research, we have designed and implemented an intelligent detection system. The system has been designed for training and testing of two system scenarios that have been generated from the network. Our concept is to investigate the behavior of each vehicle in the network to determine if it is malicious or not. If a node drops all received data, this is identified as a vehicle that is malicious. The detection system should be capable of detecting both existing and new intruders who are related to packet drop. Although the error rate of our proposed system is 2.05%, still the IDS is effective and efficient in detecting anomaly and misuse with a high accuracy and a low false positive alarm rate. Our proposed work can be extended to use a fuzzy data set to reduce the rate of error and false positives incurred in the system.

References

[1] P. Sivaranjanadevi, M. Geetanjali, S. Balaganesh and T. Poongothai, “An Effective Intrusion System for Mobile Ad Hoc Networks using Rough Set Theory and Support Vector Machine”, IJCA Proceedings on EGovernance and Cloud Computing Services - 2012 EGOV(2) 1-7, December 2012.

[2] G. Chandrasekaran, “VANETs: The Networking Platform for Future Vehicular Application”. Rutgers University, pp. 45-51, 2007.

[3] Y. Saleem Yaseen, “Enhanced a Routing Protocol for Vehicular Ad hoc Networks (VANETs) ”, Master dissertation, 2011.

[4] S. Khalfallah, M. Jerbi, M. Oussama Cherif, S. Mohammed Senouci, B. Ducourthial, Expérimentations descommunications inter-véhicules, Colloque Francophone surl’Ingénierie des Protocoles (CFIP), Les Arcs : France, 2008.

[5] Surles intersections. Thèse, France (2008).U.S. Dept. of Transportation, “National Highway Traffic Safety Administration, Vehicle Safety Communications Project Final Report”, apr. 2006, http://wwwnrd. nhtsa.dot.gov/pdf/nrd-12/060419-0843/PDFTOC.htm. [Accessed 10 June 2014].

[6] M. Saeed Al-kahtani, “Survey on security attacks in Vehicular Ad hoc Networks (VANETs)”, Signal Processing and Communication Systems (ICSPCS), 2012 6th International Conference on IEEE, no. 978-1-4673-2391-8, pp. 1 - 9 , 2012.

[7] G. Samara, W. A.H. Al-Salihy and R. Sures, “ Security Issues and Challenges of Vehicular Ad Hoc Networks (VANET)”, New Trends in Information Science and Service Science (NISS), 2010 4th International Conference on IEEE, no. 978-89-88678-17-6, pp. 393-398, 2010.

[8] M. Raya, P. Papadimitratos, J. Hubaux, “Securing Vehicular Communications”, IEEE Wireless Communications, Vol 13, 2006.

[9] S. Zeadally, R. Hunt, Y.Shyan Chen, A. Irwin and A. Hassan, “ Vehicular ad hoc networks (VANETS): status, results, and challenges”, Springer Science Business Media, LLC, 2010.

[10] M. Singh, G. Mehta, C. Vaid, “ Detection of Malicious Node in Wireless Sensor Network based on Data Mining”, International Conference on Computing Sciences, IEEE, no. 978-0-7695-4817-3/12, pp. 291-294, 2012.

[11] G. Yan, S. Olariu, M. Weigle, “Providing VANET security through active position detection”, computer communication, 31, (12), pp. 2883–2897, 2008.

[12] W. Liu, H. Zhang, W. Zhang, “An autonomous roadside infrastructure based system in secure VANETs”, Wireless Communications, Networking and Mobile Computing, 2009. WiCom '09. 5th International Conference on IEEE, no. 978-1-4244-3693-4, pp. 1-6, 2009.

[13] M. Al-Mutaz, L. Malott, S. Chellappan, “Detecting Sybil attacks in vehicular networks”, Journal of Trust Management 2014 1:4 Springer, pp. 2-19, 2014.

[14] N. Lyamin, A. Vinel, M. Jonsson, and Jonathan Loo, “ Real-Time Detection of Denial-of-Service Attacks in IEEE 802.11p Vehicular Networks”, IEEE Communications Letters, Vol. 18, no. 1, pp. 110-113, 2014.

[15] V. L. Praba, A. Ranichitra, “ Detecting Malicious Vehicles and Regulating Traffic in VANET using RAODV Protocol”, International Journal of Computer Applications (0975 – 8887), Vol. 84, no. 1, pp. 36-41, 2013.

[16] S. A. Thajeal, “ Intrusion Detection in Wireless Ad-Hoc Networks”, Al-Rafidain University College for Seciences, no. 24, pp. 133-147, 2009.

[17] M. Singh, G. Mehta, C. Vaid, “ Detection of Malicious Node in Wireless Sensor Network based on Data Mining”, International Conference on Computing Sciences, IEEE, no. 978-0-7695-4817-3/12, pp. 291-294, 2012.

[18] Technical Report: Using Artificial Intelligence to create a low cost self-driving car. Pdf [Accessed 10 Jul 2014].

[19] N. R. Vaza, B. Amit Parmar, M. Trupti kodinariya, " Implementing Current Traffic Signal Control Scenario in VANET Using Sumo”, International Journal of Advance Engineering and Research Development (IJAERD), no. 2348 - 4470, pp. 1-4, 2014.

[20] W. Danquah, D. Altilar, “ Hybrist Mobility Model - A Novel Hybrid Mobility Model for VANET Simulations”, International Journal of Computer Applications (0975–8887), Vol. 86, no. 14, pp. 15-21, 2014.

[21] Technical Report: Using Artificial Intelligence to create a low cost self-driving car. Pdf [Accessed 10 Jul 2014].

[22] Study of Network simulator 2 http://www.isi.edu/nsnam/ns/ns-documentation.html. [Accessed 10 September 2014].

[23] L. Zhou and Z. Hass, “ Security Ad hoc Networks”, IEEE Network Magazine, Vol. 13, No. 6, pages 24-30, 1999.

[24] N. R. Vaza, B. Amit parmar, M. Trupti kodinariya, “ Implementing Current Traffic Signal Control Scenario in VANET Using Sumo”, International Journal of Advance Engineering and Research Development (IJAERD), no. 2348 - 4470, pp. 1-4, 2014.

[25] S. Shirke, V. Ghorpade , “ Intrusion Detection System for AODV Protocol in MANET”, International Journal of Engineering Research & Technology (IJERT), Vol. 2, no. 2278-0181, pp. 235-240, 2013.

[26] G. Samara, W. A.H. Al-Salihy and R. Sures, “ Security Issues and Challenges of Vehicular Ad Hoc Networks (VANET)”, New Trends in Information Science and Service Science (NISS), 2010 4th International Conference on IEEE, no. 978-89-88678-17-6, pp. 393-398, 2010.

[27] M. Khattab Ali, W. Venus, and M. Suleiman Al Rababaa, “The Affect of Fuzzification on Neural Networks Intrusion Detection System", IEEE computer society.2009.