An Intrusion Detection System Against Black Hole Attacks on the Communication Network of Self-Driving 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
Colchester, United Kingdom
kdm@essex.ac.uk,contact@annagruebler.com

***Abstract*—The emergence of self-driving and semi self-driving vehicles which form vehicular ad hoc networks (VANETs) has attracted much interest in recent years. However, VANETs have some characteristics that make them more vulnerable to potential attacks when compared to other networks such as wired networks. The characteristics of VANETs are: an open medium, no traditional security infrastructure, high mobility and dynamic topology. In this paper, we build an intelligent intrusion detection system (IDS) for VANETs that uses a Proportional Overlapping Scores (POS) method to reduce the number of features that are extracted from the trace file of VANET behavior and used for classification. These are relevant features that describe the normal or abnormal behavior of vehicles. The IDS uses Artificial Neural Networks (ANNs) and fuzzified data to detect black hole attacks. The IDSs use the features extracted from the trace file as auditable data to detect the attack. In this paper, we propose hybrid detection (misuse and anomaly) to detect black holes.**

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

I. INTRODUCTION

The Federal Communications Commission (FCC) has been recognized vehicular ad hoc networks (VANETs) since October 2002 [1]. VANETs allow self-driving and semi self-driving vehicles to communicate with each other and road side units (RSUs) without traditional trust infrastructures. These vehicles and RSUs can exchange Cooperative Awareness Messages (CAMs), control data and emergency notifications between them within radio coverage [2]. In VANETs, the three types of communication are vehicle to vehicle (V2V), vehicles to infrastructures (V2I) and infrastructures to infrastructure (I2I) [3]. These networks provide security and safety to passengers, drivers and vehicles by exchanging CAMs and emergency messages [4] [5]. They have some characteristics that expose them to different types of attacks at multiple levels of the network such as black hole, gray hole, rushing and DoS attacks. VANETs posses characteristics like high mobility, fast changing network topology, absence of fixed security infrastructures and open communication medium [6]. These characteristics also make security a challenge for these types of vehicles [2].

Self-driving and semi self-driving vehicles are considered a new revolution in the automotive industry and scientific research. These vehicles are equipped with communication devices in the form of On Board Units (OBU) and an array of sensors and embedded systems [7]. These components allow vehicles and RSUs to generate and exchange CAMs to reduce the amount of accidents and traffics jam that occur from human errors. Figure 1 shows vehicles, RSUs and the occurrence of an accident. Once an accident has occurred, CAMs and control data are created and communicated to the RSUs and other vehicles in that zone.

In our research, we simulate an intelligent intrusion detection system that is mounted directly in the vehicles rather than the RSUs, allowing for protection from potential attacks even when no RSUs are in the vicinity.

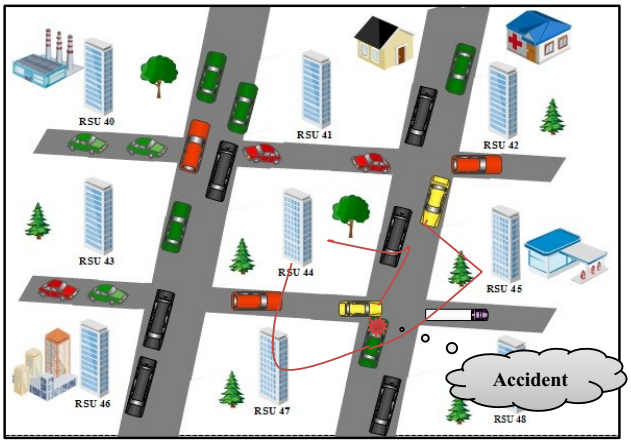

Fig. 1. An example of the process of responding to cases of emergency on the road

In our research, we designed a new intrusion detection system to protect external communication in self-driving and semi self-driving vehicles from black hole attacks. The proposed security system offers real-time detection and isolation of malicious vehicles that have a direct negative impact on other vehicles in the zone. Detection depends on the features that are extracted from the trace file which is generated using network simulator version 2 (NS2) model.

This paper is organized in the following way: Section II explores related works in the domain of attacks on external communication for self-driving and semi self-driving vehicles. Section III describes the methodology and section IV explains the experimental results. Section V discusses the results and outcomes of the scheme. Section VI is a summary of future works.

II. RELATED WORKS

In this research, our focus is on one of the most common attacks in VANETs, namely black hole attacks. Black hole vehicles are used to drop all received packets instead of forwarding them to a destination vehicle. It has three different objectives [8]:

1) Inhibit forwarding of packets from one vehicle to its neighbor's "destination node".
2) Inhibiting the reception of packets from other vehicles.
3) Dropping all received packets.

This attack can have a negative impact [9] because the performance of VANETs is directly influenced by internal and external attacks [10]. In this case, we are trying to protect networks against black hole attacks so that the network layer in the VANETs cannot be attacked [11].

Zhang et al. proposed two types of systems to detect attacks: anomaly detection and misuse detection [12]. Both rely on using features of the network to train an intrusion detection system. The proposed security system can then detect intruders and a potential attack on an ad hoc network. Kabiri et al. suggested a new approach of extracting suitable and static features from the trace files which describe the normal and abnormal behavior of vehicles in the network. They were able to infer the weight of the selected features [13]. The different numbers and types of features had a direct impact on the accuracy of the IDS. Singh et al. proposed an intrusion detection system to identify a malicious vehicle in external communication for self-driving [2]. They use cooperative intrusion detection (cross layers) to detect wormhole attacks using a security system that evaluated the decision packets at the destination station. Yan et al. advocated a novel solution by using a combinatorial approach collecting data from three different resources: radar detection, traffic and neighbouring data [14]. Thus, the system would compute the similarities between these sets of data. The authors considered the radar detection to be the trusted part of the system. Kaur et al. devised an intrusion detection system based on an artificial neural network (ANN) [15]. 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 measured the performance of the network in terms of the packets' delivery ratio, dropped packets, the average end-to-end delay and routing overhead. [16].

We can observe from previous studies that popular IDSs are based on a single approach in detection: either misuse or anomaly. In addition, the incumbent security system adopt all extracted features that capture normal and abnormal behavior in VANETs.

The motivation of our research, is to design an intelligent hybrid security system based on misuse and anomaly detection. This will help providing enough protection for self-driving and semi self-driving networks by detecting novel attack. Moreover, the proposed IDS is based on significant features that have been extracted from trace file by using POS method. To increase detection rate and decrease the number of false alarms, we employed the fuzzy set on selected features, i.e. fuzzification.

Here we present a hybrid detection system that was different from the previous security systems by which it has ability to detect a new attack. In addition, we were able to decrease the number of features that have been extracted from the trace file. This is generated from network simulaton that describes normal and abnormal behavior for VANETs in self-driving vehicles. In other words, the number of those features has been distributed by employing fuzzy sets which has a vital role in enhancing detection rate and decreasing the rate of false alarms.

III. METHODOLOGY

In this paper, we propose an IDS that is based on a dataset which was collected from a trace file that was generated utlising NS2 to model the VANET and its environment. We have attempted to identify breaches in security for self-driving and semi self-driving vehicles. The steps below explain the methodology:

A. Simulation of Urban Mobility Model

We utlise simulator systems to evaluate and test the proposed protocols and algorithms in VANETs. The proposed simulator for the security system is NS2. In order to generate a realistic environment of normal and malicious behavior in VANETs. NS2 simulations require two types of inputs traffic and mobility scenarios. We generated them by using two software solutions: Simulation of Urban Mobility Model (SUMO) and MObilty VEhicles (MOVE) [17]. This software allowed the NS2 to successfully simulate VANETs with different scenarios. SUMO is widely known in the field of VANET simulations, it provides efficient computation even in various sizes of scenarios [18]. MOVE receives the files produced by SUMO by converting them to the NS2 format and immediately using in network simulation.

In our research, we used the Manhattan urban mobility model to create a mobility and traffic scenario for vehicles. The reasons for selecting this type of mobility is a flexibility is selection of direction for vehicles and its adoption in research [19].

B. Feature Sets

The two output files of the NS2 are a trace file and a network animator. These files are used for analysis and visualization of the behavior in VANETs. The security system relies on the features in the trace file which describes both normal and malicious behavior in the VANETs.

The trace file generated in NS2 is divided into three groups: "basic trace", "internet protocol trace" and "AODV trace" [18]. The features extracted from the trace file are used to evaluate the performance of the proposed IDS. The number of false alarms and detection rate of IDS depends on the type and the number of features.

C. Feature Extraction

The trace file describes the events of VANETs, it contains many different data features which are used for analysis.

These features describe normal and abnormal/malicious behavior in VANETs. The number and the type of features have a vital direct role in the effective and efficient performance of the proposed IDS.

To increase the efficiency and the accuracy of the detection system, we need to extract the most effective features upon which to base the IDS. In our research, we used a statistical approach to extract features that have a high weight value, namely the Proportional Overlapping Scores (POS) method [20].

The distinguishing extracted features are singled out by analyzing the overlap among the expression values across two classes. We have been used package included function for calculate the proportional overlapping score for each feature in trace file avoiding the outliers effect. Relevant features selection are based on the measure for the overlap is the one defined in the POS technique. The dataset size of the selected features might be set by users [21].

POS is considered suitable and efficient even with data that has classification problems such as the high-dimensional binary and outliers [21]. The identification features are picked by evaluating the overlap between feature values across both classes "normal or abnormal".

The POS is used to measure the overlapping rate between the features in the trace file [21], shown below is the POS algorithm pseudo code.

Algorithm POS Method	
1.	Inputs: "data1.csv".
2.	Output: Sequence of the selected features.
3.	install.packages("propOverlap").
4.	source("http://bioconductor.org/biocLite.R").
5.	biocLite("Biobase").
5.	library(propOverlap).
6.	?propOverlap.
7.	getwd().
8.	data <- read.csv("data1.csv",header=T).
9.	str(data).
10.	data <- t(data).
11.	G <- data[1:21,] # define the features matrix 21.
12.	G <- jitter(G). # to avoid the noise in data
13.	Class <- as.factor(data[22,]) #define the observations' class labels.
14.	set.seed(1234).
15.	Selection <- Sel.Features(G, Class, K=21,Verbose=TRUE) # the main function.
16.	Selection$Features. # extract the number of features
17.	Selection$Measures. # extract name of features.

We extracted 21 features from the trace file and used the statistical R language to apply the POS pseudo code. These features are: Packet ID, Payload Size and Type, Source and Destination MAC, Ethernet, IP Source and Destination, Packet Tagged, Hop Counts, Broadcast ID, Destination IP with Sequence number and Source IP with Sequence number.

The number and the type of features have a vital direct role in effective and efficient performance of the proposed IDS. The motivation behind the reduction in the number of features is computation time, memory and accuracy. We used the principle of trial-and-error to choose the best number of features based on the training rate. In our work, we started with the entire set of features. After each round of training we removed the feature which had the lowest weight. This process is repeated until we are left with a set comprising of only 15 features. This set of 15 features is used for the classification of normal and abnormal behavior. Table 1 compares our IDS and previous studies where they authors employed all extracted features from trace file [22].

Table 1 Performance Metrics

	IDS with all Features	IDS with 15 Features
Training Rate	98.97%	99.86%
Average False Alarm	6.21%	0.53%
Error Rate	2.05%	0.15%
TrainParam.Epochs	68	15

D. Fuzzy Membership

According to previous studies, many researchers utilised fuzzy set in order to avoid the classification problems [23]. The nature of the dataset that is extracted from the trace file "features" has a direct impact on the performance of IDS [24]. When the name of the classes for normal and abnormal behavior is not well separated the detection rate is decreased and the number of false alarms increases.

Fuzzification is considered a suitable approach that classifies problems by creating clear border within extracted features [23].

$$f(x,a,b,c) = max(min({}^{x-a}/_{b-a}, {}^{c-x}/_{c-b}),0) \quad (1)$$

Where a, b and c represent the fuzzy domain values while x is the normal value of the dataset before fuzzification. The main motives of applying fuzzification data is to increase the detection rate of IDS as well as decrease the number of false alarms generated from IDS. It resolves ambiguity and confusion through adding five new values for each previous value of the features. According to equation 1 each value from the dataset takes five values from the fuzzy domain and the range of the interval is [0,1].

E. Simulation Environmental and Parameters

A VANET is created on the NS2 as shown in figure 4. In our simulation, we designed two malicious vehicles that represente black hole attacks. A common problem that is exposed when simulating the VANETs with NS2 is a realistic mobility model and traffic model because the NS2 is designed for wired and wireless networks [19]. To overcome this problem, we used the SUMO and MOVE tools to create realstic mobility and traffic model for VANETs [25].

A screenshot of NS2 utilizing a NAM trace file is shown in figure 2. Figure 2 shows Manhattan mobility model that consists of 9 RSUs and 40 vehicles (38 normal vehicles and 2 black hole vehicles).

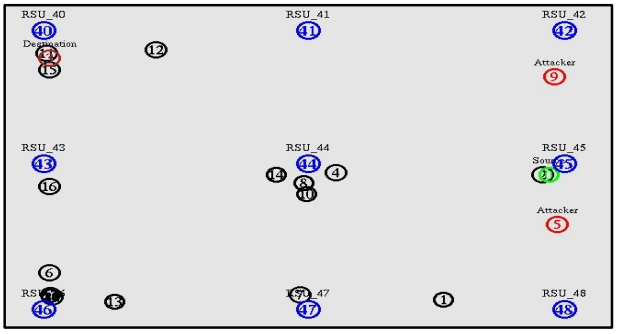

Fig. 2 Simulation in NS2 NAM

The initial parameters determine the behavior and the performance of the proposed system in NS2. These parameters are: simulation time, channel type, speed, number of vehicles and RSU, routing protocol and mobility model [19].

F. Intelligent Intrusion Detection System

The proposed intelligent IDS uses a feed forward neural network (FFNN) to detect black hole vehicles from normal vehicles in VANETs. In our research, we prepared 60000 dataset records to simulate the proposed security system. This data describes normal and abnormal behavior on the VANETs. The collected data are divided into three subsets: 1) a training (50%), 2) a testing (25%) and 3) a validation (25%) subset.

We used the principle of trial-and-error to select the best structure of FFNN employed in the proposed security system. Table 4 shows some of the parameters of the training phase of the FFNN. The value parameters which have been used in training phase are TrainParam. Epochs=15, TrainParam.lr=$1*10^{-7}$, TrainParam.goal=0 and TrainParam.min_grad = $1*10^{-12}$.

We simulated the system the Intel 5744 core i3-380M processor based PC operating at 2.53GHz and 4 GB RAM memory.

G. Generating Malicious behavior

Here, we generated two types of scenarios: normal and abnormal behavior to evaluate the performance of proposed security system. A mobility node is called black hole vehicle when it drops the received packets from other vehicles. To generate black hole behavior in VANETs, modification were made to some files of the routing protocol such as AODV. In other words, the black hole vehicles are used to drop all received packets rather than forward them to a destination vehicle. The VANET environment used in our proposal consists of 40 vehicles and 9 RSUs on a simulator system [19].

H. The Proposed IDS

The proposed security system used FFNN that consists of three layers: an input layer, a hidden layer, and an output layer. The first layer consists of 75 neurons equal to the number of fuzzified features. Our research utilizes the training rate for determining the number of neurons in the hidden layer. In other words, we found that the best training rate is utilizing 8 neurons. The output layer consists of 3 neurons ("normal, abnormal and unknown"), figure 3 shows the overall architecture of the proposed security system, namely:

1. The first stage (Generate the mobility and the traffic model): At this stage, we used both " SUMO and MOVE" to generate the suitable scenarios for NS2. These files are considered input files for the simulation system.
2. The second stage (NS2): The normal and malicious behavior for vehicles is generated. We get two output files: trace and NAM files. The dataset is extracted from the trace file generated from the NS2.
3. The third stage (Data collection and Pre-processing): The features are extracted from the data in the trace file. The features are preprocessed by converting them to numeric values and the values were normalized to values between 0 and 1 according to the equation 2:

$$X = \frac{X - MIN}{MAX - MIN} \qquad (2)$$

Normalising data often permits to increase the detection rate and enhance the performance of ANN [24].

4. The fourth stage (Extracting the main features): In this stage, we extracted the main features from the trace file. OPS is one of the efficient statistical methods that used to calculating the overlapping between features [20]. It was used to extract features that have high priority value.
5. The fifth stage (Fuzzy set): We used the fuzzy set to convert the selected features to their fuzzified counterparts to fix the huge dataset overlap.
6. The sixth stage (Training phase): We trained the ANN with the extracted dataset (main features). We created a repeat condition at this stage to get the best ratio of training. We divided the raw dataset that we extracted from the trace file into six subsets, each subset containing ten thousand records. For each iteration of the training cycle, we used a different subset for training. Hence we used three subsets (30000 records), which resulted in a training rate of 99.86%.

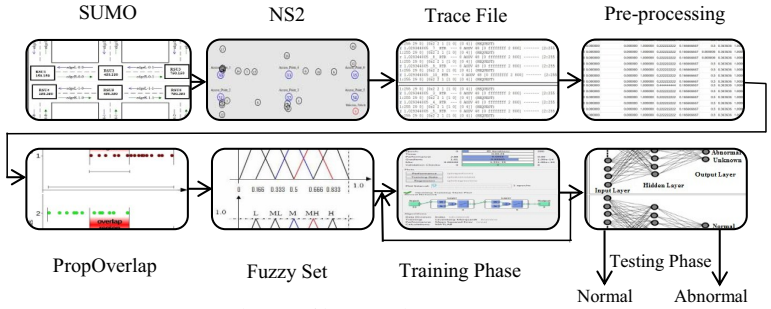

Fig. 3 Architecture of IDS

The hybrid "anomaly and misuse" detection methods are applied to an ANN that can learn the normal or abnormal behavior through the iterative process. The main motivation for using the ANN is to reduce costs, efficiency and to improve real-time responsiveness [26].

IV. Experimental results

The proposed security system can detect two different behaviors: normal or abnormal/ malicious through the IDS. In this subsection, we demonstrate the efficiency of the detection system. The error rate is used as a performance metric to evaluate the IDS.

Anomaly detection or behavior detection systems are employed to identify behavior that describes normal or abnormal for self-driving vehicles while misuse detection systems or database detection are based on the characteristics of known attacks that are generated from VANETs. The behavior detection possesses a positive detection error, difficulty handling gradual misbehavior and expensive computation. The database detection has a low rate of false alarms, but they cannot detect novel types of attacks [24].

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

The training and testing phase uses the fuzzification dataset in both phases (signature), to calculate the total accuracy of the IDS, true positive, false positive, true negative, false negative. The total accuracy of the training classification was 99.8%. We used one subset (10000 records) in the testing phase. Table 2 shows the performance of the classification system and number of records of features used in the IDS.

Table 2 Classification Rate

IDS					
Class	Original Records	ANN	Match Records	Miss Records	Accuracy
Normal	6382	6381	6375	6	99.89%
Abnormal	3618	3617	3611	6	99.80%
Unknown	0	0	0	2	NaN

In our research, we calculated four types of alarms: True Positive (TP), False Positive (FP), True Negative (TN) and False Negative (FN) to measure and evaluate the performance of IDSs. Table 3 shows the rates of four alarms.

Table 3 Alarms Rate

Alarm Type	**Accuracy**
True positive	99.90%
True negative	99.83%
False negative	0.09%
False positive	0.16%

B. Training and Testing Neural Network (Anomaly Detection)

The testing phase used a fuzzified data set that differs from the data set used in the training phase (anomaly). We calculated the total accuracy to evaluate the proposed IDS. The anomaly detection system must be able to identify novel attacks, therefore we used three subsets (30000 records) in the testing phase, table 4 shows the performance of classification and number of records used in the proposed system:

Table 4 Classification Rate

IDS					
Class	Original Records	ANN	Match Records	Miss Records	Accuracy
Normal	19285	19288	19261	27	99.87%
Abnormal	10715	10698	10685	13	99.72%
Unknown	0	14	0	14	NaN

Table 5 shows the rates of four alarms.

Table 5 Alarms Rate

Alarm Type	**Accuracy**
True positive	99.86%
True negative	99.87%
False negative	0.14%
False positive	0.12%

V. Discussion

We designed an IDS to secure external communication of self-driving and semi self-driving cars by detecting black hole vehicles in the VANETs environment. The proposed security system is implemented in seven phases: generate the mobility and the traffic model, network simulation version 2, data collection and pre-processing phase, extracting the main features, fuzzification of the data, training phase and testing phase.

Our experiments confirm that the performance of the IDS is efficiently detecting black hole vehicles with a low false alarm rate. The results indicated a high accuracy of detection rate whether normal or abnormal that fluctuated between 99.89% and 99.72% with a low error rate of only 0.15%. Furthermore, the anomaly detection system also has a low false alarm rate of 0.14%.

In our research, the detection rate ranges between 99.72% and 99.98%. When comparing these results with our previous research where fuzzy sets were not used we obtained a detection rate that ranges from 85.02% to 99.12% [22]. The percentage of false alarms ranges between 0.9% and 0.16%, when comparing these results with our previous research where fuzzy sets were not used, we obtained a false alarm rate ranging from 0.17% to 12.24% [22]. According to the results, we can notice differences between the ratio of detection and false alarms. The use of fuzzy set increases the detection rate while decreasing the number of false alarms. We can notice compared to the previous studies that the proposed system has improved detection and overcome the dataset problems such as overlapping and interference by applying the POS in order to extract the main features and performing a fuzzy set "fuzzification" on the dataset which was extracted from the trace file. This approach has a direct positive impact on the result by increasing the detection rate, decreasing the false alarm rate and error rate. However, the main drawback is that the system needs extra memory resources to store data and the approach is more computationally heavy. A low error rate indicates that the IDS is effective and efficient in identifying anomaly and misuse "hybrid detection" with a high accuracy

and a low false positive alarm rate. Our proposed work can be extracted to build IDS which can detect other types of attacks such as gray and wormhole attacks.

VI. CONCLUSION

Self-driving and semi self-driving vehicles are heavily based on the external communication to exchange and broadcast CAMs, emergence notification and control data. In addition, these vehicles cannot predict the external environment without VANETs. In this case, the security of these networks is crucial for deployment and development of these types of vehicles.

The identification and isolation of black hole vehicles in VANETs can be achieved through an intelligent IDS guarding awareness messages and control data being communicated. Black hole vehicle prevents the transmission of CAMs and notification messages from vehicle to vehicle or infrastructure by dropping each received packet in that zone. In this case, a reliable detection system is necessary to provide the required security for external communication for these vehicles. An open environment that permits different types of attacks that can have negative impact on the emergence of these vehicles. In our research, we have built an intelligent detection system to secure external communication to self-driving and semi self-driving cars. This approach has been designed for training and testing of two system scenarios: normal and malicious that have been created on the NS2. Our approach is to analysis the behavior of each mobility vehicle in the VANETs to identify if it is a black hole vehicle or normal vehicle. If a vehicle drops all received data from closed vehicle, this is detected as a black hole vehicle. One of the important aspects for the proposed IDS is the capability of identifying both existing and novel attacks. Based on this experiment, our hybrid IDS has demonstrated good performance in detecting and isolating black hole attacks in external communication of self-driving vehicles. The process of reducing the extracted features by POS method had a significant role in improving the performance of the security system. In addition, the fuzzy set help reducing the error rate and the number of false alarms when compared with our previous research.

REFERENCES

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

[2] 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 - December 2012.

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

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

[5] S. Khalfallah, M. Jerbi, M. Oussama Cherif, S. Mohammed Senouci, B. Ducourthial, Expérimentations descommunications intervéhicules, Colloque Francophone surl'Ingénierie des Protocoles, 2008.

[6] 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].

[7] 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.

[8] 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.

[9] M. Raya, P. Papadimitratos, J. Hubaux, "Securing Vehicular Communications", IEEE Wireless Communications, Vol 13, 2006.

[10] 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.

[11] 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.

[12] I Aad, JP Hubaux, EW Knightly, "Impact of Denial of Service Attacks on Ad Hoc Networks", Networking,IEEE/ACM Transactions on Volume 16, August, 2008.

[13] P. Kabiri, M. Aghaei, " Feature Analysis for Intrusion Detection in Mobile Ad-hoc Networks", International Journal of Network Security, Vol. 12, no. 1, pp. 42-49, 2011.

[14] YAN G., OLARIU S., WEIGLE M.: "Providing VANET security through active position detection", Comput.Commun., 31, (12), pp. 2883–2897, 2008.

[15] R. Kaur, A. Kaur, " Blackhole Detection In Manets Using Artificial Neural Networks," International Journal For Technological Research In Engineering, Vol. 1, no. 9, pp. 959-962, 2014.

[16] V. Lakshmi 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.

[17] The Network Simulator - ns-2; www.isi.edu/nsnam/ns. [Accessed 7 June 2014].

[18] Car 2 Car Communication Consortium, "The Handbook for Vehicle-to-X Cooperative Systems Simulation," 2011.

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

[20] O. Mahmoud, et al. "A feature selection method for classification within functional genomics experiments based on the proportional overlapping score," BMC Bioinformatics 15.1:274, pp, 1-20, 2014.

[21] Official site for PropOverlap package: " http://cran.r-project.org/web/packages/propOverlap/index.html" [Access: 14 December 2014].

[22] K. Ali Alheeti, A. Gruebler, K. D. McDonald-Maier, " An Intrusion Detection System Against Malicious Attacks on the Communication Network of Driverless Cars", published in 12th Annual IEEE Consumer Communications Networking Conference, Las Vegas, Nevada – USA, 2015.

[23] J. Ramkumar, R. Murugeswari, " Fuzzy Logic Approach for Detecting Black Hole Attack in Hybrid Wireless Mesh Network," 2014 IEEE International Conf. on Innovations in Engineering and Technology (ICIET'14), Vol. 2347 - 6710, pp. 877-882, 2014.

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

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

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