computers

MDPI

Article

Intelligent Intrusion Detection of Grey Hole and Rushing Attacks in Self-Driving Vehicular Networks

Khattab M. Ali Alheeti [1,2,*], Anna Gruebler [1] and Klaus McDonald-Maier [1]

[1] Embedded and Intelligent Systems Research Laboratory, School of Computer Science and Electronic Engineering, University of Essex, Wivenhoe Park, Colchester CO4 3SQ, UK; contact@annagruebler.com (A.G.); kdm@essex.ac.uk (K.M.-M.)

[2] College of Computer Science and Information Technology, University of Anbar, Anbar 31001, Iraq

* Correspondence: kmali@essex.ac.uk; Tel.: +44-1206-872770

Academic Editor: Thomas Strang

Received: 27 May 2016; Accepted: 14 July 2016; Published: 22 July 2016

Abstract: Vehicular ad hoc networks (VANETs) play a vital role in the success of self-driving and semi self-driving vehicles, where they improve safety and comfort. Such vehicles depend heavily on external communication with the surrounding environment via data control and Cooperative Awareness Messages (CAMs) exchanges. VANETs are potentially exposed to a number of attacks, such as grey hole, black hole, wormhole and rushing attacks. This work presents an intelligent Intrusion Detection System (IDS) that relies on anomaly detection to protect the external communication system from grey hole and rushing attacks. These attacks aim to disrupt the transmission between vehicles and roadside units. The IDS uses features obtained from a trace file generated in a network simulator and consists of a feed-forward neural network and a support vector machine. Additionally, the paper studies the use of a novel systematic response, employed to protect the vehicle when it encounters malicious behaviour. Our simulations of the proposed detection system show that the proposed schemes possess outstanding detection rates with a reduction in false alarms. This safe mode response system has been evaluated using four performance metrics, namely, received packets, packet delivery ratio, dropped packets and the average end to end delay, under both normal and abnormal conditions.

Keywords: security; vehicular ad hoc networks; intrusion detection system; self-driving car; semi self-driving car

1. Introduction

Vehicular ad hoc networks (VANETs) play a vital role in the growth and the use of self-driving and semi self-driving vehicles [1]. Internal and external communication systems are considered important components in autonomous and semi-autonomous cars. VANETs represent the communication between vehicles (V2R) and their Road Side Units (RSUs) or intra vehicular communication (V2V) in radio coverage areas, as shown in Figure 1.

External communication between self-driving vehicles and roadside equipment in Intelligent Transportation System (ITS) depend primarily on IEEE 802.11p wireless transmission [2]. In autonomous and semi-autonomous vehicles, the communication utilises Cooperative Awareness Messages (CAMs) or Basic Safety Message (BSM), which are transferred between RSUs and vehicles or just between vehicles in that zone [3]. The major objective of ITS communication is to enable traffic and passengers' safety. VANETs [4] are mobile nodes that facilitate communication in a particular zone as well as with RSUs in the absence of a fixed security infrastructure, which is used in conventional networks like wired networks [5]. Many researches consider VANETs a subclass or subtype of Mobile Ad hoc Networks (MANETs) [3]. They directly affect the ITS through the provision of comfort

services and safety applications to drivers and passengers. The major goal of VANETs is to guarantee safety of road users and also the vehicles themselves. As indicated above, through the exchange of warning message and control data, these networks can achieve their goals and provide emergency and comfort notifications to passengers and drivers, such as messages concerning emergency braking or accidents [6].

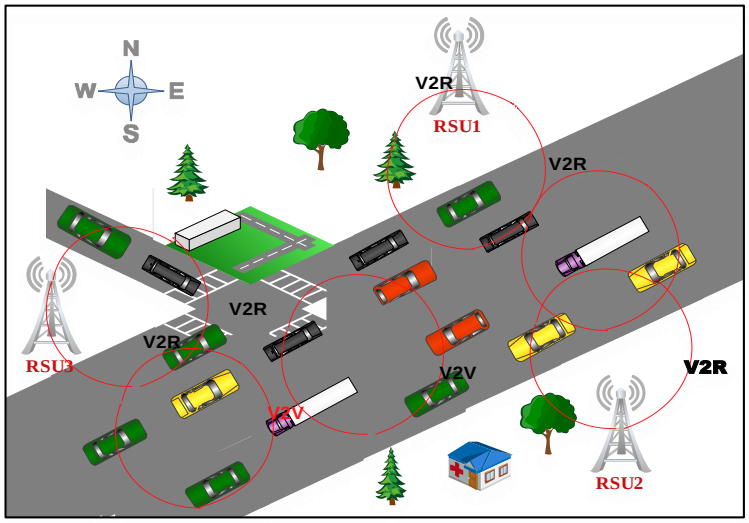

Figure 1. A basic structure of Vehicular ad hoc networks.

In ad hoc networks, three types of routing approaches are utilised: (1) the proactive approach; (2) the reactive approach; and (3) the hybrid approach [7]. One of the reactive protocols that is generally applied in external communication for autonomous vehicles is the routing protocol utilising the demand vector. High rate of throughput, low rate of delay and sequence numbering are key factors for the selection of the Ad hoc On-Demand Distance Vector (AODV) routing protocol [7]. The usage of sequence numbers enables AODV to perform more proficiently when compared with other routing protocols.

Authentication of messages and vehicles in cooperative vehicular ad hoc networks safety, warning messages, control data, and notification messages is needed in self-driving and semi self-driving vehicles. Traditional security systems like encryption/decryption methods may be able to prevent external attacks from achieving their goal of hacking sensitive information and data control between RSUs and self-driving vehicles. However, these vehicles do not possess the ability to secure external communication from internal attacks. In addition, every layer of the VANETs is vulnerable to attacks [8,9], and this makes its security one of the greatest challenges [9]. This paper focuses on protecting the external communication system from internal/external attacks on the network layer, such as Denial of Service (DoS), black hole, grey hole, wormhole and rushing attacks [10]. Grey hole and rushing attacks can stop cooperation, which results in disconnection between the vehicles and the road side units (RSUs) [10]. Creation of a suitable security system for the routing protocols is required, as the network layers work directly with routing protocols. Instead of forwarding packets to the correct destination node, malicious nodes displace or drop packets. For such attacks, most received packets are dropped and are not moved to their destination node. Other problems can arise in such an attack, for instance an overhead increase and Packet Delivery Rate (PDR) decrease on the network [10]. The attack detection is a difficult task owing to selective dropping of data packets [11]. A network suffering from grey hole attacks either forwards packets to the destination node in the period of process discovery as "true" behaviour, and then, when the network behaves maliciously, be made to drop almost every received packet [11].

Rushing attacks or sudden attacks are seen as an emerging type of Denial of Service (DoS) attacks that have a direct and negative effect on the action of the routing protocols, particularly on AODV and Dynamic Source Route [10]. The source vehicle floods road requests (RREQ) to the destination vehicle, via VANETs in the road discovery phase. The rushed vehicle receives at this point the RREQ and moves the packet directly to destination vehicles without delay, i.e., a zero delay [12]. The original packet will automatically be removed by the destination node as a copy packet, because the node has already accepted the packet from the rushing attack. Such attacks are particularity effective when they are near the source or destination vehicles [12].

In this paper, we propose an IDS to protect external communication in autonomous and semi-autonomous vehicles from grey hole and rushing attacks. This security system is capable of detecting malicious behaviour in real time, thereby preventing the malicious vehicle from communicating with other vehicles. In addition, we propose a novel response system to switch infected vehicles into a "safe mode" without delay to protect passengers'/drivers' lives and even the vehicles themselves.

This work is presented in the following sequence: Section 2 discusses similar research in the area of protection for attacks on VANETs. Next, Sections 3 and 4 explore the methodology while Section 5 gives details of the experimental results. Section 6 discusses these experimental results. Finally, Section 7 gives the conclusions and directions on future research on this topic area.

2. Related Works

Traffic accidents are a major cause of death and serious injuries [13]. In the field of self-driving cars, VANETs are developed to enhance the safety of passengers/drivers and vehicles. Their aim is to ensure the safety of the users on the road through enhanced traffic systems that achieve a reduction in the number of accidents arising from human errors. Self-driving vehicles require access to essential information like signs/warning messages and CAMs that are exchanged between vehicles and RSUs in real-time.

The performance of VANETs is improved by strengthening their defences against malicious attacks. Alheeti et al. have enhanced detection rate and reduced the number of false alarms that was generated by IDS [14] based on a Defense Advanced Research Projects Agency (DARPA) dataset utilising a hybrid IDS to secure host/network from the potential attacks. In [15], statistical techniques are used in building intrusion detection systems for vehicular ad hoc networks to identify rogue nodes. The authors can improve the IDS application layer that was based on CAMs for efficient detection malicious of behaviour for high change dynamic. Banerjee proposes a security system to discover and eliminate the grey hole and black hole attacks on the VANETs [16], where data are divided into equal blocks, and these blocks are then sent to the destination node by different routes instead of sending every data along the same route. The destination node examines the size of the sent data block; if the system detects differences in the size of the received data, it can identify the malicious route. At this point, the source node will be used to prevent data from being sent via the malicious route [16]. Vuong et al. developed traditional IDS for detecting cyber-attacks on robotic vehicles [17]. Their IDS is based on a decision tree method that relies on physical features and cyber in detecting malware codes. The system is evaluated by injecting two types of malicious codes in different scenarios including DoS. Sedjelmaci et al. designed an accurate and lightweight intrusion detection framework called AECFV [18]. It has the ability to detect the most dangerous attacks such as black hole, packet duplication wormhole, selective forwarding, Sybile and resource exhaustion attacks on VANETs. Their security system is based on a clustering approach to provide sufficient protection for VNETs. The vehicle's trust-level and nodes' mobility were used in elected Cluster-Heads (CHs), the authors also used various performance metrics in evaluating the proposed system. Alheei et al. proposed an intelligent IDS to identify malicious behaviour to secure the external communication for self-driving and semi self-driving vehicles [1]. Fuzzy Petri Nets were employed in this system that is particularly suited for dropping attack detection. Packet delivery rate, end-to-end delay and throughput were utilised to measure the performance of the proposed security system.

Bouali et al. propose a prevention and detection system to identify abnormal behaviour of vehicles [19]. This security system has the ability to predict the vehicle's future behaviour and is based on Kalman filters that have the ability to predict vehicles' behaviour. Assila et al. created a new security scheme to protect VANETs from possible attacks [8], which is based on the verification of the CAMs. This scheme helps researchers to decrease the number of attacks and tackle threats. Zhang et al. proposed two systems to detect intruders: anomaly based detection and misuse based detection [20]. Both rely on using features of the network to train an IDS that can identify intruders and a potential attacks on an ad hoc network. Reddy et al. propose Cross Layer Intrusion Detection (CLID) to protect wireless mesh networks (WMNs) from rushing attacks [12]. CLID was created at the network layer and the MAC layer to decrease the false alarm rate. This cooperative intrusion system assessed the proposed security system with network simulator. Pavani et al. created an IDS to protect the VANETs against the grey hole and black hole attacks [21]; they employed several machine learning approaches: Decision Tree (C-4.5), Multi-Layer Perceptron (MLP), K-Nearest Neighbourhood (KNN) and Support Vector Machines (SVM). This method was simulated via the popular network simulator version 2 (ns-2) [22]. MLPs discovered intrusions more accurately and with less false error rates.

In summary, there are two kinds of detection methods: (1) anomaly detection; and (2) misuse detection [23]. The work presented here proposes a security system that makes use of anomaly detection. Signature or misuse based detection which relies on the features of the known attacks is highly accurate and has a lower false alarm rate; however, it cannot consistently identify novel attacks. Behaviour or anomaly detection is based on the vehicle's normal behaviour which classifies several actions that deviate significantly from normal behaviour thus indicating an attack. Anomaly detection systems conversely suffer from a high rate of false alarms, have complications in handling regular misbehaviour and are often computationally expensive. We have used the ns-2 in designing the proposed IDS here. There are many characteristics inherent in ns-2 that have encouraged various researchers to make use of it, such as low cost, high speed of simulation, open source and a rich library.

3. The Proposed Intrusion Detection System

We propose a security system that determines the vehicle's behaviour as normal or malicious based on data that are collected through a trace file. The IDS uses trace files produced by a simulation that includes both normal and abnormal behaviour in VANETs [24]. The types and quantity of features play an important role in increasing the rate of detection and decreasing false alarms in such a system. Based on a prior study [25] we focus on highly relevant features extracted from a trace file [25]. We use both Support Vector Machines (SVM) and Feed Forward Neural Networks (FFNN) in the design of the IDS as both techniques have been successfully applied in self-driving vehicles [26].

The proposed IDS attempts to offer sufficient protection against grey hole attacks and rushing attacks of the external communication system in self-driving vehicles. The following details the methodology of the proposed security system:

3.1. Simulation of Traffic and Mobility Scenarios

We utilised two software tools to generate a real-world traffic of abnormal/normal behaviour for self-driving and semi self-driving vehicles: Simulation of Urban Mobility Model (SUMO) and MObilty VEhicles (MOVE) [27]. The output files of these tools are used as input to ns-2 [28]. The reasons for employing SUMO to generate mobility scenarios are that it is open source, widely used in VANETs, microscopic and facilitates multi-model traffic simulation [29]. In addition, it is computationally efficient and straightforward to adapt with various numbers of vehicles as well as the MOVE model designed on SUMO [30,31].

The mobility models are divided into three types: urban, highway and rural models [32]. The urban mobility model includes many types of models, such as the Random Way Point (RWM) model, the Manhattan mobility model and the Rice University Model (RUM) [32]. In this paper, we use the Manhattan mobility model because it is widely used in the research field and it allows vehicles

to move in different directions [32]. The Simulation of Urban Mobility Model (SUMO) and MObilty VEhicles (MOVE) are shown in Figure 2.

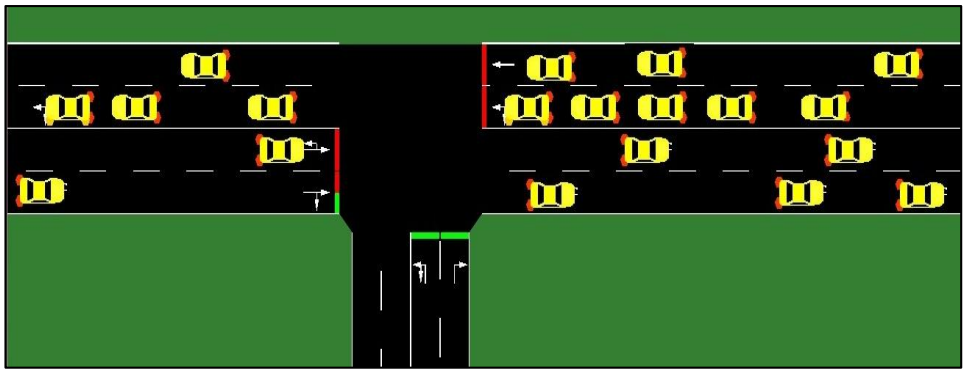

Figure 2. Screenshot of Simulation of Urban Mobility Model (SUMO) and MObilty VEhicles (MOVE).

The self-driving communication simulation is carried out using ns-2 and employs four abnormal vehicles: two rushing attacks and two grey hole attacks on the system. Figure 3 shows the system simulation designed in ns-2.

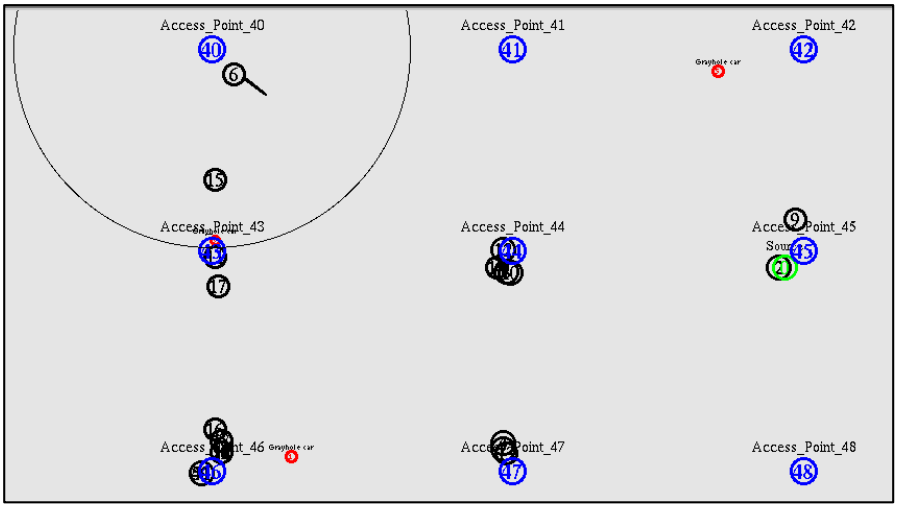

Figure 3. Screenshot of network simulator.

A vital problem in simulation systems are the parameters employed during the initial stages because they have an important role in identifying the mobility, behaviour and traffic type of vehicles. Table 1 details initial parameters like the Radio Propagation Model (Two Ray Ground), Type of Traffic (CBR), and Routing protocol (greyholeaodv) [33].

Table 1. Simulator Environmental and Parameters.

Parameter	Value
Simulator	ns-2.35RC7
Simulation time	499 s
Number of nodes	40 Vehicles
Number of RSUs	9 RSUs
Type of Traffic	Constant Bit Rate (CBR)
Topology	600 × 600 (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 802.11p
Speed	30 m/s
Interface queue type	Priority Queue
Network Interface type	Physical Wireless
Mobility Models	Manhattan Mobility Model

3.2. Feature Sets and Extraction

As indicated above, the IDS is based on a trace file which was extracted from ns-2. The IDS deduces from the features whether the behaviour of vehicles is normal or malicious. Overall, extracting features from a trace file for the purpose of an IDS could be difficult as it involves large and overlapping data. We made use of the AWK language to obtain features that define the actions of vehicles in VANETs [34]. They define five events: receive (r), send (s), drop (D), movement (m), and forward (f) [35].

The detection system rate and false alarms numbers and the features were obtained from the trace file as follows:

1. Generate the trace file from ns-2.
2. Use the AWK language to evaluate the output file from ns-2. The trace file is processed using the AWK language to determine the packet delivery rate (PDR), end-to-end delay and throughput.
3. Produce 21 features that define normal and malicious behaviour.
4. Choose 15 features that, based on our previous study [25], accurately reflect the behaviour of self-driving vehicles. Proportional Overlapping Score (POS) were used to extract significant features from the trace files.

Table 2 shows the 15 selected features from the entire features space extracted from the trace file that are generated in ns-2.

Table 2. Features Selection.

Basic Trace	IP Trace	AODV Trace
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 Source IP with Sequence number

POS is considered the most suitable and efficient scheme with a dataset that has common classification problems such as outliers and high-dimensional binary [36,37]. It was employed to calculate the overlapping rate in the features extracted. The R code the POS method using the following pseudocode [36]:

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").
6.  library(propOverlap).
7.  ?propOverlap.
8.  getwd().
9.  data <- read.csv("data1.csv",header=T).
10. str(data).
11. data <- t(data).
12. G <- data[1:23,] # define the features matrix 23.
13. G <- jitter(G). # to avoid the noise in data
14. class <- as.factor(data[24,]) #define class labels.
15. set.seed(1234).
16. selection <- Sel.Features(G, Class, K = 23,Verbose = TRUE) # the main function.
17. selection$Features. # extract the number of features.
18. selection$Measures. # extract name of features.
```

All extracted features were tagged with the repetition value, and then the features with the lowest weight were removed.

3.3. Fuzzification of the Dataset

The features that were extracted have some issues, which may have direct impact on the average rate of detection and number of false alarms of the system; for instance, if the normal or abnormal behaviour is not obvious from the features, or if they do not classify as well-defined normal and abnormal behaviours. In this case, we have to design a mathematical model that can be employed to redistribute the features and cope with ambiguity. Fuzzy sets are increasingly popular to tackle such problems efficiently [38] and will thus be employed to address the problem of classification using a fuzzification of the features that were obtained from the ns-2 trace file. Our previous work [39] did not employ fuzzy sets and we obtained a false alarm rate of 12.24%. After incorporating fuzzy sets, we obtain a false alarm rate of 0.17% [25].

In Equation (1), each value was distributed in five values of fuzzy with a range in [0,1]: low, medium low, medium, medium high and high.

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

where x is the feature value while a, b and c represent the values of the fuzzy domain. By using fuzzification data, we attempt to increase the detection rate of the proposed IDS while reducing the number of false alarms at the same time.

3.4. Intelligent Detection System

In this section, we detail an intelligent IDS that utilises SVM and FFNN to identify the vehicles performing rushing attacks and grey hole attack in VANETs. Our proposed IDS makes use of a data set of 30,000 records to define the normal and malicious behaviours in VANETs. The data set, obtained from the trace file, was split into three subsets: (1) the validation set; (2) the test set; and (3) the training set. This is in order to manage a common problem with neural networks Artificial Neural Network (ANN), i.e., the over-fitting of training data.

The FFNN includes one or more hidden layer, the input layer and the output layer. The input layer is made up of 75 neurons, which equals the number of fuzzified features obtained from the trace

file after using a fuzzy set. We utilise two hidden layers to raise the accuracy of detection of the system and to reduce the amount of false alarms. There are five neurons in the first hidden layer while the second hidden layer contains 11 neurons. There are two neurons (normal and abnormal) in the output layer. In order to determine the optimal FFNN configuration in terms of hidden neurons and layers, we made use of the trial and error method in order to configure and choose the best ratio of training based on the situation selected that have been created in the proposed system. The parameters in the initial stages have a vital role to play in the performance of the FFNN, which has a direct effect on the performance of detection. We show in Figure 4 below the optimal structure of the FFNN that was thus determined.

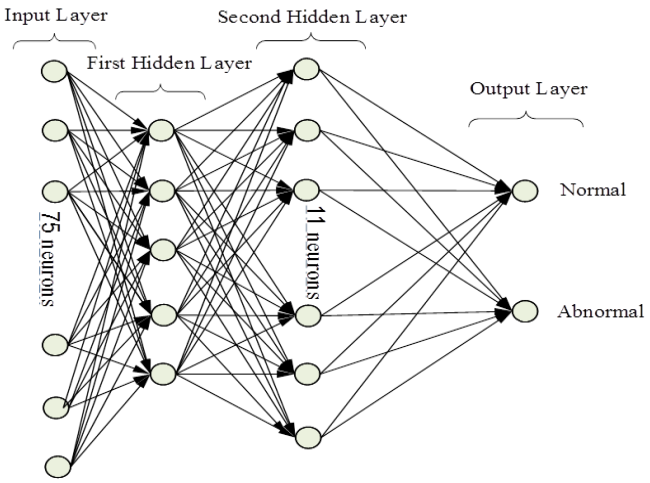

Figure 4. Structure of the Artificial Neural Network (ANN).

The formal mathematical formula for the parameters for SVM and FFNN are detailed as follows. Equation (2) is the learning function for the SVM with C data training:

$$C = \left\{ (x_i, y_i) \middle| x_i \in R^P \right\} \tag{2}$$

where the range value of $y_i \in \{-1, 1\}$, i = 1, 2, 3, 4, . . . , n. The value of x_i indicates the class. In FFNN, the training phase ends when the least-square-error E value between the desired d_i and actual output y_i is less than $E_{max} = 1 \times 10^{-5}$.

$$E = \frac{1}{2p} \sum_{p=1}^{P} \sum_{i=1}^{m} (y_i - d_i)^2 \tag{3}$$

where p is the total number of training patterns, and

$$d_i = \begin{bmatrix} 1 \; If \; the \; training \; pattern \; \in i^{th} \; texture \\ -1 \; otherwise \end{bmatrix}$$

As indicated above, the initial parameters play a vital role in the FFNN performance, which has a direct effect on the performance of detection. These parameters form the basis of our study, and they influence the detection rate in the training phase of the simulation. The parameters of the training phase used in the FFNN are shown in the Table 3 below:

Table 3. Feed Forward Neural Networks (FFNN) Parameters.

Parameter	Value
Train Param. Epochs	46
Train Param. Lr	1×10^{-8}
Train Param. Goal	0
Train Param. min_grad	1×10^{-13}
Gaussian Radial Basis Function	1
BoxConstraint	1×10^{5}

The simulation is executed on a PC with an Intel 5744 core i3-380M processor and 4GB RAM memory.

3.5. Generate Grey Hole and Rushing Attacks

In order to analyse the security system performance, we designed two types of scenarios identified in the previous stage, i.e., the normal and abnormal behaviours. Numerous researches consider that creating grey hole attacks is hard [11] in VANETs due to the fact that these attacks exhibit two behaviours. Thus, the vehicle may be considered normal at time t = 0 and become abnormal at t = n.

This condition makes creating grey hole attacks a difficult challenge in ad hoc networks. The abnormal behaviour that caused the dropping of some or sometimes all received packets was implemented in ns-2 using the Object-oriented programming and Object Tool Command Language (OTCL) script. However, we were required to create a new routing protocol in order to generate grey hole attacks in VANETs. Additionally, we need to adapt the AODV routing protocol so as to create rushing attacks. Two functions were incorporated into the standard AODV routing protocol to simulate selective packet dropping. There are 40 vehicles and nine RSUS [33] in our simulation environment, with two rushing vehicles and two grey hole vehicles. Detection is focused on identifying which vehicle drops packets received from RSU or vehicles in coverage radio area.

3.6. Methodolgy

This section details the methodology for proposed IDS that has the ability to provide sufficient security of the external communication of self-driving and semi self-driving vehicles.

The general structure of the proposed security system is shown in Figure 5. There are the following eight stages in the IDS:

1st Stage (generation of the realistic world): Obtain the mobility and traffic model which shows the actual movement of vehicles in VANETs. The ns-2 in this stage made use of the output file from MOVE and SUMO as input to obtain a trace file that defines both normal and abnormal.

2nd Stage (ns-2): We made use of the output file extracted from the former stage as input files for the ns-2 in this stage. We replicate normal, rushing attacks and grey holes to create two files: Network Animator (NAM) file and trace file.

3rd Stage (data extraction): Here we revisit stage two to extract all the features that were found in the trace file. Nonetheless, our proposed system can, however, work with a reduced feature set of just fifteen important features selected from all of the features [19]. Decreasing the number of features has an important effect in escalating the rate of detection and reducing the rate of false alarms.

4th Stage (pre-processing): Here, we convert some letters and symbols to numerical values using the selected features that were pre-processed. We also want to use these selected features to generate a homogenous distribution to balance the various types of classes in the data collection so as to increase the efficiency of the rate of detection and normalization process to turn all the values of the features between 0 and 1 according to Equation (4):

$$X = \frac{x - MIN}{MAX - MIN} \tag{4}$$

Normalising data often allows an increase in the detection rate and enhances the performance of FFNN [12].

5th Stage (fuzzy set): In this stage, we convert the ordinary data that were generated in Stage 4 into fuzzified data. The process here can be used in solving some common problems that usually occur in the data set like the lack of clarity and overlap.

6th Stage (training and testing phase—FFNN): Stage 5 data are used to train and test the FFNN. We also obtain the rate of detection for both normal and abnormal behaviour in this stage and then determine the four alarm types.

7th Stage (training and testing phase—SVM): Here, in parallel to Stage 6, the training and testing of the SVM is carried out with fuzzified data, which was obtained in Stage 5 in order to identify the efficiency of the security system in the identification of rushing vehicles and grey hole in comparison to normal vehicles.

8th Stage (Comparison): Here, we compare both of the proposed intrusion detection systems that are based on categories, the number of false alarms, rate of detection, standard deviation and rate of error.

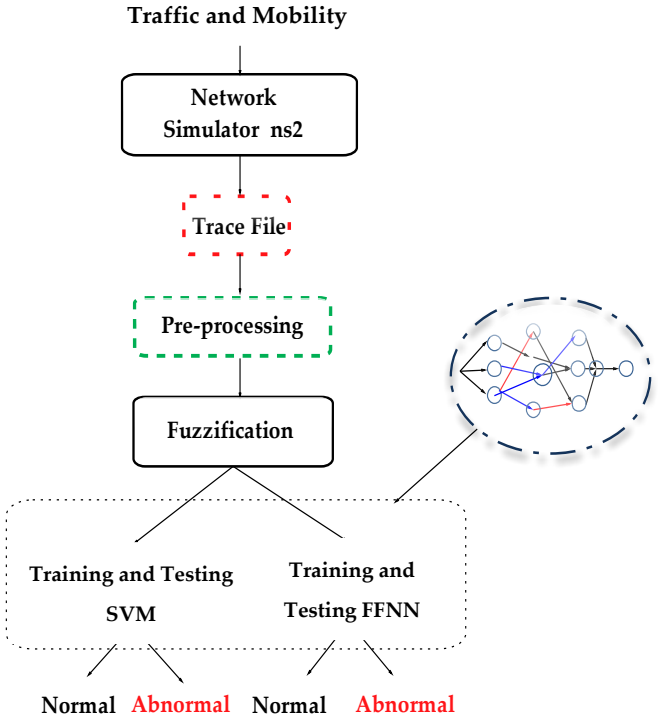

Figure 5. Intrusion Detection System (IDS) Architecture.

4. Response Mechanism

A novel rapid response reaction mechanism for autonomous and semi-autonomous vehicles is introduced on the data link layer of the network, which switches affected vehicles into a safe mode; this protects vehicles by preventing direct communication with the nearby RSUs without mediator. This response mechanism is based on the communication infrastructure provided in a typical mobility scenario, such as the Manhattan urban mobility model [26]. Typical external communication of self-driving vehicle includes three main places in Manhattan scenarios: mobile On-Board Units (OBUs), a Trust Authority (TA) equipped on each vehicle and immobile RSUs at the roadside every 250 m as shown in Figure 6 [40]:

- TAs are responsible for authorization communication between RSUs and vehicles. They contain all vital information about traffic statistics and streets. The Certificate Revocation List (CRL) is

published periodically by the TAs to their RSUs and it has the capability of detecting, receiving and communicating messages to TAs. The TAs and RSU are the building blocks of the system and are considered trusted entities of the system.

- RSUs provide the backbone communication of self-driving vehicles. These vehicles depend heavily on these vital units in VANETs. The wired communication between immobile infrastructures on the road site with TAs is an authentication feature [40].
- Every vehicle is equipped with an Identification On-Board Unit (ID-OBU), which allows it to share local traffic data and control information between vehicles in their radio zone.

The data link layer provides continuous monitoring for malicious situations to manage potential risk/hazards. Thus, when malicious behaviour is detected the system is put into. Our system relies on RSUs in emergency because it possesses the following qualities [40]:

- trusted element because of its wired connection to TAs;
- low delay;
- low bit error rates; and
- high bandwidth.

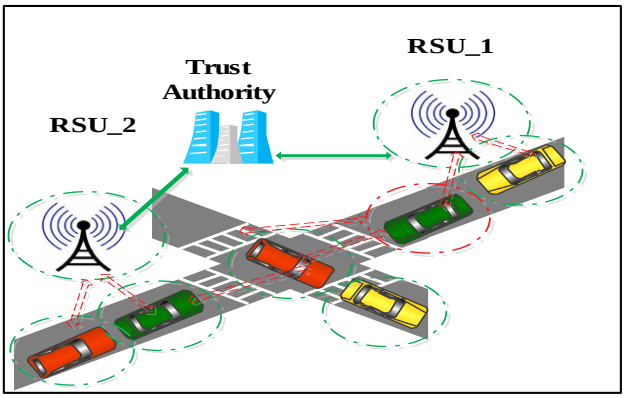

Figure 6. System model.

The basic addressing and access control to the physical layer are core factors to target the response system on the datalink layer. For malicious behaviour, the response system will configure the communication on point-to-point protocol to allow the infected vehicle to communicate with nearby RSUs. In other words, the response system can partially isolate infected vehicles from other vehicles, and restrict their communication to trust points such as RSUs in that radio coverage area.

The IEEE 802.11p protocol provides wireless access in vehicular environments. The Protocol is an enhancement to the IEEE 802.11 standard but it is known to have an issue in scalability rate [41]. It cannot offer the required time-probabilistic characteristics in dense road scenarios because it was originally designed for low mobility networks. Thus, the IEEE 802.11p protocol does not operate efficiently for high density and mobility scenarios in VANETs [41]. Alternatively, it has a minimal scalability capability when there are many self-driving vehicles in the same vicinity [42,43]. Thus, we need to employ the RSU end-points to facilitate in emergency or critical situations.

4.1. Data Link Layer

The response system to switch infected vehicles into safe mode without delay was introduced on the data link layer. It is responsible for transferring control data and information between VANETs entities and has the ability to identify and correct physical layer errors. There are many factors in the data link layer that facilitate this [44]:

- The data link layer provides basic addressing and access control to the physical layer on VANETs of self-driving and semi self-driving vehicles.

- It facilitates vehicle communication among the subnet, which is done through a reconfiguration requirement.

These factors are often seen as crucial for choosing this layer amongst others on VANETs. Various kinds of communication protocol are used in this layer, such as the point-to-point protocol (PPP), Advanced Data Communication Control and High-Level Data Link Control (HDLC) [45]. Our suggested reaction system depends on PPP.

4.2. Safe Mode

The safe mode is a response system that is activated when a self-driving vehicle has been infected. Thus, the proposed system allows a compromised vehicle to communicate only with the closest RSUs in the same coverage area. The safe mode thus establishes a partial isolation policy: the functionality of the mobility node could be fully restored through communication with the RSU. In the absence of a safe mode for vehicular networks, a compromised vehicle may pose a risk to passengers and other road users. Our proposed safe mode provides increased safety and reliability in the event a vehicle is compromised in any way.

5. Experimental Results

In order to obtain realistic data, we generated two kinds of outcomes and simulated these outcomes under real conditions. We processed these data to obtain important features with various pre-processing of the data. In this situation, we used pre-determined data for training and testing in order to carry out the measurement of the IDS. Overall, the accuracy of the training reached 99.71%. We also carried out calculation of four kinds of alarms: false positive (FP), true positive (TP), false negative (FN) and true negative (TN). We are able to calculate the detection accuracy of the system using Equation (5) [23]:

$$Accuracy = \frac{Number\ of\ correctly\ classified\ patterns}{Total\ number\ of\ patterns} \tag{5}$$

$$TP_{Rate(sensitivty)} = \frac{TP}{TP + FN} \tag{6}$$

$$TN_{Rate(specificity)} = \frac{TN}{TN + FP} \tag{7}$$

$$FN_{Rate} = (1 - sensitivity) = \frac{FN}{FN + TP} \tag{8}$$

$$FP_{Rate} = (1 - specificity) = \frac{FP}{FP + TN} \tag{9}$$

5.1. Detection System Phase

5.1.1. Testing Neural Network to Detect Grey Hole Attacks

We used the fuzzified data obtained from the trace file in testing the IDS to detect grey hole attacks in external communication for self-driving vehicles. In this section, we utilised measurement of the rate of detection and the calculation of the alarms. We also made use of cross validation for SVM and FFNN to analyse the performance of the security system. In this instance, we split the dataset into twenty datasets (k = 20), of which five per cent were employed in the testing phase and ninety per cent for the training dataset. We replicated this process in the measurement of the performance for the IDS through the calculation of the rate of detection for normal and abnormal standard deviation (SD) and alarms. We show the rate of detection accuracy and the number of records that were utilised in our suggested security system in Table 4.

Table 4. Classification Rate.

IDS				
Class	**Accuracy**	**Time/s**	**Error Rate**	**SD**
SVM-Normal SVM-Abnormal	99.93% 99.64%	0.12	0.21	0.429
Class	**Accuracy**	**Time/s**	**Error Rate**	**SD**
FFNN-Normal FFNN-Abnormal	99.82% 99.86%	0.99	0.15	0.102

Table 5 shows the rate of four alarms for grey holes.

Table 5. Alarm Rate.

Alarm Type	**FFNN**	**SVM**
True positive	99.92%	99.88%
True negative	99.75%	99.89%
False negative	0.08%	0.11%
False positive	0.25%	0.12%

5.1.2. Testing Neural Network to Detect Rushing Attack

There was a difference in the type and numbers of records that we made use of in the training phase from the data set we used in the testing phase. In this phase, the IDS is supposed to be able to identify rushing attacks, which have a direct and negative effect on VANETs. We created an IDS with differences in the both security systems. It has the capability to identify novel attacks. In Table 6, the rate of detection accuracy, time, error rate and standard deviation utilised are detailed.

Table 6. Classification Rate.

IDS				
Class	**Accuracy**	**Time/s**	**Error Rate**	**SD**
SVM-Normal SVM-Abnormal	99.79% 99.80%	0.23	0.18%	0.139
Class	**Accuracy**	**Time/s**	**Error Rate**	**SD**
FFNN-Normal FFNN-Abnormal	99.80% 99.75%	1.01	0.19%	0.127

Table 7 shows the rate of four alarms for rushing attacks.

Table 7. Alarm Rate.

Alarm Type	**FFNN**	**SVM**
True positive	99.86%	99.70%
True negative	99.78%	99.92%
False negative	0.12%	0.30%
False positive	0.22%	0.07%

In addition, we need to calculate additional performance metrics for the both proposed IDS based on FFNN (FFNN-IDS) and SVM (SVM-IDS) for evaluation of their performance individually, including their Precision Rate (PR), Detection Rate (DR), Classification Rate (CR) and Mean Squared Error (MSE).

5.2. Response Mechanism Protocol Phase

This section evaluates the normal and abnormal behaviour of self-driving and semi self-driving vehicles identified above.

5.2.1. Normal Behaviour

To identify the effect of the proposed response system, we evaluated this under normal conditions. We made use of the novel response system to program one of the self-driving vehicles. Performance metrics of vehicles in two instances under similar conditions were determined and are shown in Table 8.

Table 8. Performance metrics.

Class	PR	DR	CR	MSE
FFNN-IDS	99.76%	99.83%	99.89%	0.167%
SVM-IDS	99.90%	99.84%	99.79%	0.150%

Table 9 provides the performance metric of the proposed response system, which is used to protect self-driving vehicles. We calculated performance metrics such as PDR, total dropped packets and average end-to-end delay for VANETs, with and without the presence of a response system.

Table 9. Performance metrics of normal behaviour.

Performance Metrics	Without Response System	With Response System
Generated Packets	8226	8226
Received Packets	5769	8153
Packet Delivery Ratio	70.13%	99.11%
Totally Dropped Packets	3074	74
Average End-to-End Delay	202.17 ms	22.63 ms

5.2.2. Abnormal Behaviour

After evaluating normal behaviour, we also subjected the response system to malicious/abnormal behaviour, from which we obtained the performance metrics in Table 10. The table below allows differentiating between the active role of the proposed response system in two cases of self-driving vehicles.

Table 10. Performance metrics of abnormal behaviour.

Performance Metrics	Without Response System	With Response System
Generated Packets	8226	8226
Received Packets	3555	6216
Packet Delivery Ratio	43.21%	75.56%
Totally Dropped Packets	4878	2010
Average End-to-End Delay	72.90 ms	44.65 ms

6. Discussion

The core objective of this research was to create an IDS that provides a secure environment for self-driving and semi self-driving vehicles. We implemented the methodology of this IDS in eight phases, which lead to generating the mobility and traffic model, the trace file, the ns-2, fuzzification, data collection and pre-processing, training and testing for the SVM, and training and testing for the FFNN, and compared the results we generated from the two types of IDS. In Figure 7, two IDS are compared; we found that the IDS based on the FFNN was more effective and efficient in determining

abnormal vehicles with a smaller false negative alarm rate than the IDS using SVM; however, we can observe that SVM performance is much higher that of the FFNN. SVM is faster than FFNN because the SVM automatically computes the number of hidden layers in an optimised way [46]. Figure 7 also shows the difference in the performance of FFNN and SVM. The IDS system based on SVM had an error rate of 0.19%. However, in this particular system, there was fluctuation of alarm rates between 99.92% and 99.70% with high rate and efficient accuracy. Alternatively, the average false negative rate of alarm recorded was low, around 0.20%, which is a good indicator of the performance of the results.

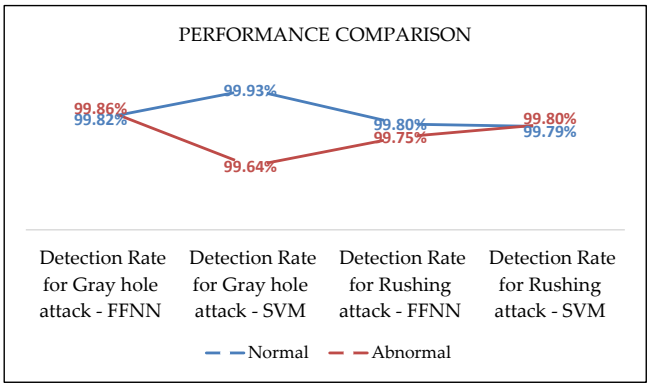

Figure 7. Performance Comparison.

The rate of error for the IDS based on the FFNN was found to be 0.17% and the fluctuation of the alarm rate was between 99.92% and 99.75% with a high and efficient rate of accuracy. Alternatively, the average false negative rate of alarm was minimal, at about 0.1. Making use of fuzzified data with FFNN and SVM create flexibility in selecting the system that is very efficient with various conditions, thus allowing improving the rate of detection. Additionally, 15 significant features were incorporated, such as payload ID, MAC Ethernet, IP, Packet Tagged and Hop Counts, into the IDS. Thus, the features selected help in making the proposed security system more efficient in securing the external communication systems of self-driving and semi self-driving vehicles.

In the experimental result of the response mechanism protocol phase, we note the efficient role of the safe mode protocol in providing and establishing the safety environment for self-driving and semi self-driving vehicles. This protocol can adapt with these vehicles under different conditions, i.e., normal and abnormal behaviours. It has the ability to isolate the communication of the infected vehicles from the surrounding mobility and immobility nodes but keep connection with the closest RSU to introduce this victim vehicle in the safe mode communication.

In order to evaluate the performance of the IDS, we need to compare it with the previous best achieved average error rate, which is 2.05% [39], while we have achieved an 0.18% error rate with the IDS presented here. In [39], the average of false alarm is 4.68%, while we have achieved 0.15% with this IDS.

The response model that is proposed in this paper plays an important role in enhancing the overall performance for the external communication for self-driving and semi self-driving vehicles. Tables 8 and 9 reflect a vital performance of the proposed approach that was evaluated under normal and abnormal conditions. In the two scenarios, the number of generated packets is 8226. On the one hand, the number of received and dropped packets under normal condition without the response system is 5769 and 2457, respectively. On the other hand, the number of received packets is 8153 and the number of dropped packets is 73 under normal conditions with the response system. However, under abnormal or malicious conditions with and without the response system, the number of received packets is 3555 under the abnormal scenario without response system and 4671 is the number of dropped packets. Under the same condition with the response system, the number of received packets is 6216, while 2010 is the number of dropped packets.

7. Conclusions

In modern systems such as self-driving and semi self-driving vehicles, intelligent intrusion detection systems have become a vital security application. These vehicles, networks and devices are subjected to different types of attacks that have a direct effect on the development and use of self-driving vehicles. The intelligent IDS introduced here has the capability to detect grey hole and rushing attacks in VANETs. These network types can assure secure self-driving and semi self-driving by CAMs and control data that are swapped between the different vehicles in a zone. Rushing attacks and grey hole attacks attempting to bring about a drop in some or all incoming messages, which can lead to a direct consequence to the lives of passengers, vehicles and drivers. In addition, without security, self-driving and semi self-driving vehicles will not be able to achieve their function in providing safety and comfort when being operated.

We created an intelligent security system that can secure external communication system for self-driving vehicles. We designed the IDS to be used for training and testing with fuzzified data through the use of SVM and FFNN. This system can produce two system outcomes, which we have been able to generate and simulate in ns-2. We also studied the behaviour of all vehicles to detect normal and abnormal behaviour in VANETs. We applied monitoring and analysis of the trace files that were generated in network simulator to detect grey hole and rushing attacks. The trace file defines the behaviour of the network using receive, send, forward, move and drop. A possible additional extension of this system is to study these attacks with different AI techniques like Fuzzy Petri Nets (FPNs).

Acknowledgments: This research has been supported by the Engineering and Physical Sciences Research Council (EPSRC) Grant EP/K004638/1 (project named RoBoSAS).

Author Contributions: Khattab M. Ali Alheeti designed the proposed system and simulated it within different conditions for measuring the efficiency of the security system and response system for Automatic driving cars. Anna Gruebler had a substantial role in improving the proposed system throughout the scientific notes. Klaus McDonald-Maier had the essential and distinct role in writing and designing and simulating the system throughout his continuous feedback and scientific guidance and advice. All authors have read and approved the final manuscript.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Alheeti, K.A.; Gruebler, A.; McDonald-Maier, K.D.; Fernando, A. Prediction of DoS Attacks in External Communication for Self-driving. In Proceedings of the IEEE International Conference on Consumer Electronic (ICCE), Las Vegas, NV, USA, 7–11 January 2016.
2. Wyglinski, M.; Huang, X.; Padir, T.; Lai, L.; Eisenbarth, T.; Enkatasubramanian, K. Security of Autonomous Systems Employing Embedded Computing and Sensors. *Micro IEEE* **2013**, *33*, 80–86. [CrossRef]
3. Breu, J.; Brakemeier, A.; Menth, M. A quantitative study of Cooperative Awareness Messages in production VANETs. *EURASIP J. Wirel. Commun. Netw.* **2014**, *1*, 1–8. [CrossRef]
4. Koscher, K.; Czeskis, A.; Roesner, F.; Patel, S.; Kohno, T.; Checkoway, S.; McCoy, D.; Kantor, B.; Anderson, D.; Shacham, H.; et al. Experimental security analysis of a modern automobile. In Proceedings of the IEEE Symposium on Security and Privacy, Oakland, CA, USA, 16–19 May 2010.
5. Alheeti, K.A.; Gruebler, A.; McDonald-Maier, K.D. On the Detection of Grey hole and Rushing Attacks in Self-Driving Vehicular Networks. In Proceedings of 7th Computer Science and Electronic Engineering Conference (CEEC), Colchester, UK, 24–25 September 2015.
6. Nzouonta, J.; Rajgure, N.; Wang, G.; Borcea, C. VANET routing on city roads using real-time vehicular traffic information. *IEEE Trans. Veh. Technol.* **2009**, *58*, 3609–3626. [CrossRef]
7. Surmukh, S.; Kumari, P.; Agrawal, S. Comparative Analysis of Various Routing Protocols in VANET. In Proceedings of 5th IEEE International Conference on Advanced Computing & Communication Technologies, Haryana, India, 21–22 February 2015.
8. Kenney, J. Dedicated Short-Range Communications (DSRC) Standards in the United States. *Proc. IEEE.* **2011**, *99*, 1162–1182. [CrossRef]

9. Chetan, V.S.; Benni, N.S.; Bhushan, C. Security framework for VANET for privacy preservation. In Proceedings of the 2013 Fourth International Conference on Computing, Communications and Networking Technologies (ICCCNT), Tiruchengode, India, 4–6 July 2013.
10. Raya, M.; Papadimitratos, P.; Hubaux, J. Securing vehicular communications. *IEEE Wirel. Commun. Mag.* **2006**, *13*, 8–15. [CrossRef]
11. Usha, G.; Bose, S. Impact of Gray hole attack on ad hoc networks. In Proceedings of the International Conference on IEEE, Information Communication and Embedded Systems (ICICES), Chennai, India, 21–22 February 2013.
12. Reddy, K.G.; Thilagam, P.S.; Rao, B.N. Cross-layer IDS for rushing attack in wireless mesh networks. In Proceedings of the Second International Conference on Computational Science, Engineering and Information Technology, Coimbatore, India, 26–28 October 2012.
13. Assila, A.; Jabri, I.; Ltifi, A. Secure Architecture Dedicated for VANET Alarm Messages Authentication through Semantic Verification. In Proceedings of the 6th International Conference on IEEE Sciences of Electronics, Technologies of Information and Telecommunications (SETIT), Sousse, Tunisia, 21–24 March 2012.
14. Alheeti, K.A.; Al-Jabouri, L.; McDonald-Maier, K.D. Increasing the Rate of Intrusion Detection based on a Hybrid Technique. In Proceedings of the 5th IEEE International Conference on Computer Science and Electronic Engineering (CEEC'13), Colchester, UK, 17–18 September 2013.
15. Zaidi, K.; Milojevic, M.; Rakocevic, V.; Nallanathan, A.; Rajarajan, M. Host Based Intrusion Detection for VANETs: A Statistical Approach to Rogue Node Detection. *IEEE Trans. Veh. Technol.* **2015**, *99*, 1–6. [CrossRef]
16. Banerjee, S. Detection/Removal of Cooperative Black and Gray Hole Attack in Mobile Ad-Hoc Networks. In Proceedings of the World Congress on Engineering and Computer Science (WCECS), San Francisco, CA, USA, 22–24 October 2008.
17. Vuong, T.; Loukas, G.; Gan, D. Performance evaluation of cyber-physical intrusion detection on a robotic vehicle. In Proceedings of the IEEE Computer and Information Technology, Ubiquitous Computing and Communications, Dependable, Autonomic and Secure Computing, Pervasive Intelligence and Computing (CIT/IUCC/DASC/PICOM), Liverpool, UK, 26–28 October 2015.
18. Sedjelmaci, H.; Senouci, S.M. An accurate and efficient collaborative intrusion detection framework to secure vehicular networks. *Comput. Electr. Eng.* **2015**, *43*, 33–47. [CrossRef]
19. Bouali, T.; Senuci, S.; Sedjelmaci, H. A distributed detection and prevention scheme from malicious nodes in vehicular networks. *Int. J. Commun. Syst.* **2016**, *49*, 1683–1704. [CrossRef]
20. Zhang, Y.; Lee, W. Intrusion detection in wireless ad-hoc networks. In Proceedings of the 6th annual International Conference on Mobile Computing and Networking, Boston, MA, USA, 6–11 August 2000.
21. Pavani, K.; Damodaram, A. Anomaly Detection System for Routing Attacks in Mobile Ad Hoc Networks. *Int. J. Netw. Secur.* **2014**, *6*, 13–26.
22. Issariyakul, T.; Hossain, E. *Introduction to Network Simulator ns-2*, 2nd ed.; Springer: New York, NY, USA; Dordrecht, The Netherlands; Heidelberg, Germany; London, UK, 2012.
23. Alheeti, K.A.; Venus, W.; Suleiman, M. The Affect of Fuzzification on Neural Networks Intrusion Detection System. In Proceedings of the IEEE Computer Society, Xi'an, China, 25–27 May 2009.
24. Selvamani, K.; Anbuchelian, S.; Kanimozhi, S.; Elakkiya, R.; Bose, S.; Kannan, A. A hybrid framework of intrusion detection system for resource consumption based attacks in wireless ad-hoc networks. In Proceedings of the IEEE International Conference Systems and informatics (ICSAI), Yantai, China, 19–20 May 2012.
25. Alheeti, K.A.; Gruebler, A.; McDonald-Maier, K.D. An Intrusion Detection System against Black Hole Attacks on the Communication Network of Self-Driving Cars. In Proceedings of the IEEE Sixth International Conference on Emerging Security Technologies (EST), Braunschweig, Germany, 3–5 September 2015.
26. Using Artificial Intelligence to Create a Low Cost Self-Driving car. Available online: http://budisteanu.net/Download/ISEF%202%20Autonomous%20car%20Doc%20particle.pdf (accessed on 7 November 2015).
27. The Network Simulator- ns-2. Available online: http://www.isi.edu/nsnam/ns (accessed on 12 April 2016).
28. Danquah, W.; Altilar, D. Hybrist Mobility Model—A Novel Hybrid Mobility Model for VANET Simulations. *Int. J. Comput. Appl.* **2014**, *86*, 15–21.
29. Pandey, A. Simulation of Traffic Movement in VANETs Using Sumo. Ph.D. Thesis, National Institute of Technology, Rourkela, India, 2013.

30. Car 2 Car Communication Consortium. The Handbook for Vehicle-to X Cooperative Systems Simulation. Available online: https://www.car-2-car.org/index.php?id=5 (accessed on 10 June 2015).
31. DLR—Institute of Transportation Systems, SUMO—Simulation of Urban MObility. Available online: http://sumo.sourceforge.net/doc/current/docs/userdoc/Data/Scenarios/TAPASCologne.html,2011 (accessed on 15 March 2016).
32. Dean, A. Neural Network Vision for Robot Driving. Available online: https://www.ri.cmu.edu/pub_files/pub2/pomerleau_dean_1995_1/pomerleau_dean_1995_1.pdf (accessed on 8 April 2016).
33. Study of Network Simulator 2. Available online: http://www.isi.edu/nsnam/ns/ns-documentation.html (accessed on 10 September 2015).
34. Khan, N.; Usmani, Z. *Performance Analysis of Modelling Wireless Network in Campus Environment*; Topology Elsevier: Amsterdam, The Netherlands, 2008.
35. Zhou, L.; Hass, Z. Security Ad hoc Networks. *IEEE Netw. Mag.* **1999**, *13*, 24–30. [CrossRef]
36. Mahmoud, O.; Harrison, A.; Perperoglou, A.; Gul, A.; Khan, Z.; Metodiev, M.V.; Lausen, B. A feature selection method for classification within functional genomics experiments based on the proportional overlapping score. *BMC Bioinform.* **2014**, *15*, 1–20. [CrossRef] [PubMed]
37. Official Site for PropOverlap Package. Available online: http://cran.r-project.org/web/packages/propOverlap/index.html (accessed on 7 April 2016).
38. Guanrong, C. *Introduction to Fuzzy Sets, Fuzzy Logic and Fuzzy Control Systems*, 2nd ed.; CRC Press: Houston, TX, USA, 2001; ISBN: 0-8493-1658-8.
39. Alheeti, K.A.; Gruebler, A.; McDonald-Maier, K.D. An intrusion detection system against malicious attacks on the communication network of driverless cars. In Proceedings of the 12th Annual IEEE Consumer Communications and Networking Conference (CCNC), Las Vegas, NV, USA, 9–12 January 2015.
40. Peng, Y.; Abichar, Z.; Chang, J. Roadside-aided routing (RAR) in vehicular networks. In Proceedings of the IEEE International Conference on Communications ICC 2006, Istanbul, Turkey, 11–15 June 2006.
41. Alasmary, W.; Zhuang, W. Mobility impact in IEEE 802.11 p infrastructure less vehicular networks. *Ad Hoc Netw.* **2012**, *10*, 222–230. [CrossRef]
42. Van, E.; Klein, W.; Karagiannis, G.; Heijenk, G. Exploring the Solution Space of Beaconing in VANETs. In Proceedings of the First IEEE Vehicular Networking Conference, VNC2009, Tokyo, Japan, 28–30 October 2009.
43. Campolo, C.; Vinel, A.; Molinaro, A.; Koucheryavy, Y. Modeling broadcasting in IEEE 802.11p/WAVE vehicular networks. *IEEE Commun. Lett.* **2011**, *15*, 199–201. [CrossRef]
44. Whitehouse, R.; Scott, M. *Implementation of Data link Layer Protocols for a Network Simulator*; Computer Science Tripos Part II; Homerton College, University of Cambridge: Cambridge, UK, 2011.
45. Holma, H.; Antti, T. *Wcdma for Umts*, 3rd ed.; Wiley: Chichester, UK, 2000.
46. Camps-Valls, G., Bruzzone, L. (Eds.) *Kernel Methods for remote Sensing Data Analysis*; Section 5.64; Wiley: New York, NY, USA, 2009; pp. 78–79.