On the Detection of Grey hole and Rushing Attacks in Self-Driving Vehicular Networks

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*—Vehicular ad hoc networks play an important role in the success of a new class of vehicles, i.e. self-driving and semi self-driving vehicles. These networks provide safety and comfort to passengers, drivers and vehicles themselves. These vehicles depend heavily on external communication to predicate the surrounding environment through the exchange of cooperative awareness messages (CAMs) and control data. VANETs are exposed to many types of attacks such as black hole, grey hole and rushing attacks. In this paper, we present an intelligent Intrusion Detection System (IDS) which relies on anomaly detection to protect external communications from grey hole and rushing attacks. Many researchers agree that grey hole attacks in VANETs are a substantial challenge due to them having their distinct types of behaviour: normal and abnormal. These attacks try to prevent transmission between vehicles and roadside units and have a direct and negative impact on the wide acceptance of this new class of vehicles. The proposed IDS is based on features that have been extracted from a trace file generated in a network simulator. In our paper, we used a feed-forward neural network and a support vector machine for the design of the intelligent IDS. The proposed system uses only significant features extracted from the trace file. Our research, concludes that a reduction in the number of features leads to a higher detection rate and a decrease in false alarms.**

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

I. INTRODUCTION

Vehicular ad hoc networks (VANETs) play a significant role in the development and the deployment of self-driving and semi self-driving vehicles which makes them a field of great interest. All layers of the VANETs are exposed to many types of attacks. Security is one of the biggest challenges in vehicular ad hoc networks [1]. In this paper, we focus on attacks on the network layer, for instance denial of service (DoS), black hole, grey hole, wormhole and rushing attacks [2]. In our research, we have designed an intrusion detection system (IDS) to secure the network layer in VANETs from potential attacks. Because the network layer deals directly with routing protocols, the design of a security system for the routing protocols is needed.

Three types of routing approaches are used in ad hoc networks: proactive approach, reactive approach and hybrid approach [3]. A routing protocol such as on demand vector (AODV) is considered one of the reactive routing protocols that has been commonly used in external communication for autonomous vehicles. The motivation to select the AODV protocol is a high rate of throughput, low rate of delay, and sequence numbering [3]. The sequence numbers make AODV more efficient in terms of performance, when compared with other routing protocols. Self-driving and semi self-driving vehicles rely heavily on external communication for transferring and receiving notification messages and control messages. Attacks like grey hole and rushing attacks can contribute to thwart cooperation for the purpose of creating a disconnect between the vehicles and the road side units (RSUs) [2]. The basic principle of VANETs is to allow mobile nodes and infrastructures on the roadside to exchange packets from the source node to the destination node, but malicious nodes create disorder or drop packets rather than forward these to the appropriate destination node. Grey hole attacks are considered a possible attack which targets the network layer in a communication system for autonomous vehicles. In the case of an attack, all or some received packets are dropped and not forwarded to the destination node. Additionally, in an attack other problems can be created such as an increase in overhead and a decrease of the packet delivery rate (PDR) on the network [2]. Many researchers consider the detection of the grey hole attacks in AODV a difficult task because it has two types of behaviours (normal and malicious) [4]. In other words, the network can forward all packets to the destination node during the discovery process just like in honest behaviours, but the network can then maliciously be made to gradually drop some or all received packets [4].

Rushing attacks or sudden attacks are considered a new type of DoS attacks that have a direct and negative impact on the performance of routing protocol, especially on demand ad hoc network routing protocols such as AODV and dynamic source route (DSR) [2]. In the road discovery phase, the source vehicle floods road requests (RREQ) to destination vehicle through VANETs. In this case, the rushing vehicle will receive RREQ and directly forward the packet to destination vehicles without any delay (zero delay) for this reason named rushing [5]. The destination will discard the original packet as a duplicate packet because the node already received the packet from rushing attacks. This type of attack is more effective when it is close to the source or destination vehicles [5].

In self-driving and semi self-driving vehicles, external and internal communication systems are considered one of the essential components. Grey hole attacks can create many problems for vehicles in these networks like preventing vehicles from receiving important messages from other nodes in that zone. Figure 1 shows how VANET's operate.

Here we propose an IDS to protect external communication in autonomous and semi-autonomous vehicles from grey hole and rushing attacks. The proposed security system has the ability to detect abnormal/malicious behavior in real time thus preventing a malicious vehicle from communicating with other vehicles.

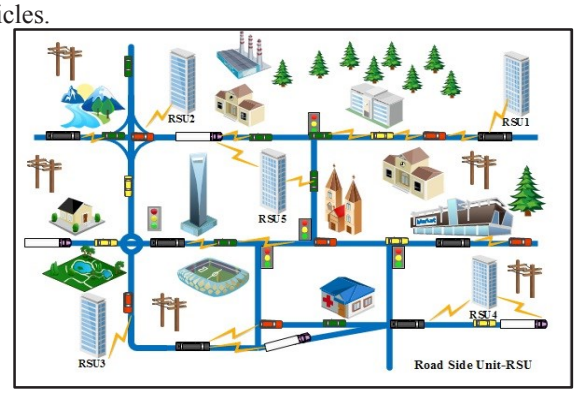

Fig.1 An example of the process of responding to cases of emergency on the road

The IDS utilises trace files generated from the simulator; it contains features that describe normal and abnormal behavior in VANETs. The type and the number of features have an important role in increasing the detection rate and decreasing false alarms in the proposed security system. We selected a significant feature extracted from the trace file based on our previous study [6]. Support vector machine (SVM) and feed forward neural networks (FFNN) are used in the design of our proposed IDS. The main reason for using these artificial intelligent networks is that significant number of research attests to the efficiency of these networks, particularly in self-driving vehicles [7].

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 discussion. Section VI provides conclusions and future directions of research.

II. Related Works

Traffic accidents have caused the deaths of thousands of people over the world [8]. Researchers in the field of VANETs for intelligent transport system (ITS) are developing networks to increase the safety of passengers and vehicles. Their target is to provide safety to the users on the road through enhanced traffic systems that lead to a decrease in the number of accidents that occur from human errors. In real-time applications, self-driving vehicles need access to important information such as warning messages and cooperative awareness messages (CAMs) between vehicles and RSUs. Therefore, security and safety becomes a very important issue in VANETs developments.

Some research seeks to improve the performance of VANETs by enhancing their defense systems against malicious attacks. Assila et al. present a new security scheme to protect VANETs from the potential attacks. They present a new design based on the verification of cooperative awareness messages. This scheme helps researchers to reduce the number of attacks and address the threats. Banerjee proposed a security system to detect and remove both grey hole and black hole attacks on the MANETs [9]. The main idea is that the data is divided into equal blocks, then the blocks are sent to the destination node by a different route rather than sending all the data in the same route. The destination node checks the size of the sent data; when the system is found to differ in the size of the received data, it can detect the malicious route. In this case, the source node was asked to send the data again and avoid the malicious route and the malicious nodes therein [9]. Reddy et al. proposed a cross layer intrusion detection (CLID) to secure Wireless Mesh Networks (WMNs) against rushing attacks [5]. The CLID was built at the network layer and the MAC layer to reduce the false alarm rate. The cooperative intrusion system evaluated the proposed security system with network simulator. Al Shahrani, proposed two approaches to handling overhead and time in security dynamic source router (SDSR) based on all neighbours nodes are safe [10]. Pavani et al. designed an intrusion detection system to secure MANETs against both black hole and grey hole attacks [11]. Their research used four types of machine learning approaches: Decision Tree (C–4.5), Multi-Layer Perceptron (MLP), K-Nearest Neighborhood (KNN) and Support Vector Machine (SVM). The proposed method was applied by using the network simulator version 2 (NS2). It can be observed from the experimental results that MLP detected the intrusions with more precision and with less false error rates than the other approaches. Kaur et al. Devised an intrusion detection system based on the Backpropagation neural network [12]. The main aim of this security system was to secure MANETs against black hole attacks. The researchers were able to prove the efficiency of the ANN in their research and they used different types of performance metrics to calculate the effectiveness of the IDS in MANETs.

Generally, IDSs have two types of detection methods. These methods are misuse and anomaly detection [13]. In our paper, we propose a security system that uses anomaly detection. Misuse or signature detection systems rely on the features of known attacks, are highly accurate and have a low rate of false alarms, but they cannot consistently identify novel attacks. Anomaly or behavior detection is based on the normal behavior of nodes. It classifies any action that considerably deviates from the normal behavior an attack. However, anomaly detection systems have a high rate of false alarms, difficulty in handling gradual misbehavior and are computationally expensive.

III. Methodology

In our paper, we propose a security system based on the behaviour of vehicles, whether normal or abnormal that is collected from the trace file. The proposed IDS can provide sufficient protection against grey hole attacks and rushing of the external communication in self-driving vehicles. The steps below explain the methodology of the proposed security system:

A. Simulation of Traffic and Mobility Scenarios

We selected an efficient network simulator NS2 to evaluate and measure the performance of the proposed security system [14]. NS2 uses two software solutions to create a real scenario of normal and/ or abnormal behavior in VANETs. These are: Simulation of Urban Mobility Model (SUMO) and MObilty VEhicles (MOVE) [14]. The SUMO is computationally efficient

and it is widely used in different sizes of scenarios in VANETs [15] [16] and the MOVE model is built on SUMO. The urban and highway mobility model is commonly used in NS2. We employed the urban mobility model of Manhattan because it flexible and is widely used in this research field [17].

B. Feature Sets and Extraction

The proposed IDS relies on a trace file that was generated from NS2. The IDS infers from features whether the behaviour of vehicles is normal or abnormal. Generally, researchers consider extracting features from a trace file difficult because it consists of large and overlapping data. We used the AWK language to extract features that capture the events of vehicles in VANETs. They describe five events: send (s), receive (r), drop (D), forward (f) and movement (M) [18].

The rate of the detection system and number of false alarms based on the number and the type of features that were extracted from the trace file. The steps below explain how the features were extracted:

1. Generate the trace file from NS2.
2. Use AWK language to analyse the output file from NS2.
3. Produce 21 features that describe normal and abnormal behaviour.
4. Select fifteen features based on our previous study that accurately reflect the behaviour of self-driving vehicles [6].

Table 1 shows the 15 selected features from whole features that were used in the proposed security system.

Table 1 Features Selection

Basic Trace	IP Trace	AODV Trace
Packet ID, Payload Size and Type, Source and Destination MAC, and Ethernet	IP Source and Destination	Packet Tagged, Hop Counts, Broadcast ID, Destination IP with Sequence number, Source IP with Sequence number

C. Fuzzification of the Dataset

The extracted features can have some problems that have a direct impact on the average detection rate and number of false alarms of the system, such as the distribution of the features or if the name of the classes is not well defined or ambiguous between the normal and malicious behavior. In this situation, we need a mathematical model to redistribute the features and develop solutions to ambiguity such as a fuzzy set. We use the fuzzy set well-known and widely used in scientific fields for a number of reasons, including efficiency [19]. Fuzzy sets are considered a good solution of the classification problem by applying a fuzzification on the features that were extracted from the trace file "NS2". 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% [6]. We can clearly notice the important role of fuzzification in enhancing the detection rate and reduction of false alarms.

According to equation 1, each value is distributed in four values of fuzzy with a range in [0, 1].

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

Where x is the feature value while a, b and c represent the values of the fuzzy domain. Employing fuzzification data increase the detection rate of IDS as well as decreasing the number of false alarms that are generated from IDS.

D. Simulation Parameters and Mobility Scenarios

Self-driving communication are created on the NS2 as shown in figure 2, this shows four malicious vehicles, two perpetrating grey hole and two rushing attacks. NS2 has many characteristics that have encouraged many researchers to use it, such as speed of simulation, low cost and a rich library. Moreover, it is open source and object-oriented [20].

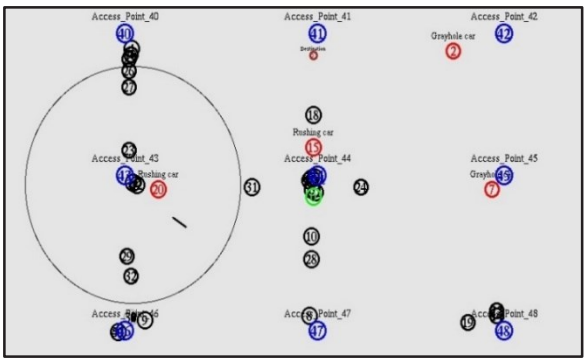

Fig. 2 Screenshot of NS2

In figure 2, we notice the type of mobility model, number of malicious attacks and infrastructure communication based on road side every 250m RSUs (Access_Point$_{1, 2, 3, n}$).

An important issue in simulation systems are the initial parameters because they have a vital role in determining behaviour, mobility and traffic type of vehicles. These include parameters such as Type of Traffic (CBR), Radio Propagation Model (Two Ray Ground) and Routing protocol (greyholeaodv) [17].

E. Intelligent Intrusion Detection System

Here, we designed an intelligent IDS based on an FFNN and SVM to detect vehicles doing a grey hole and rushing attacks in VANETs. Many recent studies have focused on ANN as the most efficient tool in building internal and external systems for self-driving and semi self-driving vehicles [7]. The proposed IDS used a data set of 30,000 records to describe the normal and abnormal behaviour in VANETs. The data set collected from the trace file was divided into three subsets: the test set, the validation set and the training set. We tried to avoid one of the most common problems of an ANN which is the over fitting employing parts of the data used to validate the network performance.

To select the best configuration of the ANN, we used the principle of trial and error to configure and select the best ratio of training depending on the condition select that have been established in the proposed system. The initial parameters play an important role in the performance of the FFNN that have a direct impact on the performance of detection. Figure 3 shows the best structure of the FFNN that was selected in our proposal.

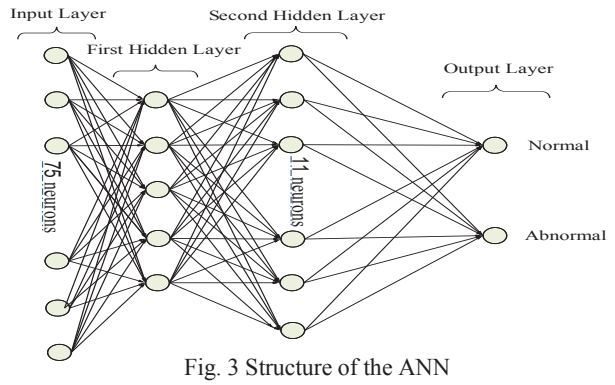

Fig. 3 Structure of the ANN

We explain some the parameters that were used in our research such as learning parameter and TrainParam. goal. In this case, we describe the formal mathematical formula for this parameter for FFNN and SVM. Equation 2 is the learning function for the SVM, C data training:

$$C = \{(x_i, y_i) | x_i \in R^P\} \qquad (2)$$

Where the range value of $y_i \in \{-1, 1\}$, $i = 1, 2, 3, 4, \ldots, n$. The value of xi 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 $E_{\max = 1*10^{-5}}$.

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

Where p is the total number of training patterns, and

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

The initial parameters play an important role in the performance of the FFNN that have a direct impact on the performance of detection. Table 2 shows the parameters of the training phase used in the FFNN.

Table 2 ANN Parameters

Parameter	Value
TrainParam. epochs	46
TrainParam. lr	$1*10^{-8}$
TrainParam. goal	0
TrainParam. min_grad	$1*10^{-13}$
Gaussian Radial Basis Function	1
BoxConstraint	1e5

The simulation is based on the system with an Intel 5744 core i3-380M processor "2.53GHZ" and 4GB RAM memory.

F. Generate Grey hole and Rushing attacks

To evaluate performance of security system, we need to create two types of scenarios previously identified: normal and abnormal behavior. Many researchers consider that creating grey hole attacks is difficult [4] in VANETs because these attacks have two types of behavior normal and abnormal. In other words, the vehicle may be normal at time t=0 and become malicious at time t=n. This makes creating grey hole attacks a big challenge in ad hoc networks. The malicious behaviour that leads to dropping some or all received packets, it is created in NS2 using the Object Tool Command Language (OTCL) script and Object-oriented programming. However, we need to create a new routing protocol (grey hole aodv) to generate grey hole attacks in VANETs. In addition, we need to modify some files in the AODV routing protocol to create rushing attacks. The simulation environment consists of 40 vehicles and 9 RSUs [17]. It has two grey hole vehicles and two rushing vehicles in our scenario. The principle of detection is based on vehicle that drop packets that it received from vehicles or RSU in that zone.

G. The Intrusion Detection System

In our research, the ANN consists of an input layer, a hidden layer and an output layer. The input layer comprised 75 neurons equal to the fuzzified features that were extracted from the trace file after applying a fuzzy set to them. We designed two hidden layers to increase the accuracy of detection of the system and to decrease the number of false alarms. The first hidden layer consisted of 5 neurons, the second hidden layer consisted of 11 neurons and the output layer consisted of 2 neurons ("normal" and "abnormal").

The proposed IDS has eight stages, and the overall architecture of the proposed security system is shown in Figure 4, namely:

- The first stage (generate the realistic world) - in this stage, we used two software programs to generate the mobility and traffic model that reflected the real movement of vehicles in VANETs. NS2 used the output files from SUMO and MOVE as input to generate a trace file that describes normal and abnormal.
- The second stages (NS2) - we used the output files from the previous stage as input files for the NS2. We simulated normal, grey hole and rushing attacks to generate two files. These files are the trace file and the NAM file.
- The third stage (data extraction) - In this stage, we extracted all the features from the trace file that were generated in the previous stage. However, the proposed system only used 15 significant features from all the features [6]. Reducing the number of features has a vital role in increasing the detection rate and decreasing the false alarms.
- The fourth stage (pre-processing): in this stage, the selected features were pre-processed to convert some letters and symbols to numbers, and to generate a uniform distribution to balance the different types of classes in collecting the data to increase the efficiency of the detection rate and normalisation process to convert all the values of the features between zero and one.
- The fifth stage (fuzzy set): we needed to convert the normal data that was generated in the previous stage into fuzzified data. This process can solve some common problems that occur in the data set such as overlap and a lack of clarity.
- The sixth stage (training and testing phase – FFNN): we trained and tested the FFNN with the extracted data that was produced in the previous stage. In this stage, we obtained the detection rate for normal and abnormal behaviour, and we calculated four types of alarm.
- The seventh stage (training and testing phase – SVM): we trained and tested the SVM with fuzzified data that was extracted in the fifth stage to check the efficiency of the

proposed security system in the detection of grey hole and rushing vehicles in comparison to normal vehicles.

- The eighth stage (comparison): in this stage, we compared the two proposed intrusion detection systems based on the four criteria, detection rate, the number of false alarms, error rate and standard deviation.

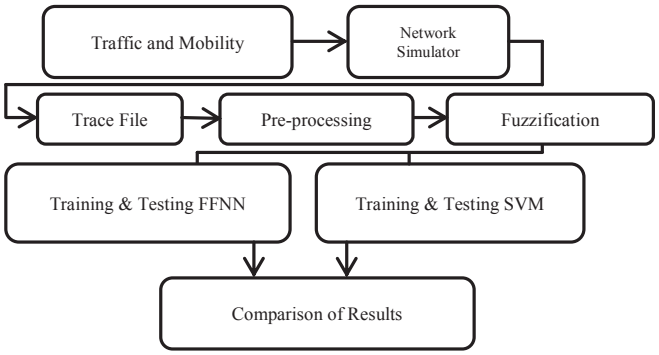

Fig. 4 IDS Architecture

IV. Experimental Results

We generated two types of scenarios and simulated these under actual conditions in order to obtain real data. This data was processed to extract the significant features with some pre-processing of the data. In this case, we have ready data for training and testing to measure the performance of the proposed intelligent detection system. The total accuracy of the training algorithm is 99.71% in training phase. We calculated four types of alarms: true positive (TP), false positive (FP), true negative (TN) and false negative (FN) According to the equation 4, we can calculate the accuracy of the detection system [13]:

$$Accuracy = \frac{Number\ of\ correctly\ classified\ patterns}{Total\ number\ of\ patterns} \quad (4)$$

$$TP_{Rate(sensitivty)} = \frac{TP}{TP + FN} \quad (5)$$

$$TN_{Rate(specificity)} = \frac{TN}{TN + FP} \quad (6)$$

$$FN_{Rate} = (1 - sensitivity) = \frac{FN}{FN + TP} \quad (7)$$

$$FP_{Rate} = (1 - specificity) = \frac{FP}{FP + TN} \quad (8)$$

A. Testing Neural Network to detect Grey hole Attacks

We tested the IDS with the fuzzified data that was generated from the trace file to detect grey hole attacks in external communication for self-driving vehicles. In this phase, we measured the detection rate and to calculate of the alarms. We employed cross validation for FFNN and SVM to evaluate the performance of the proposed security system. In this case, the datasets are divided into 20 datasets (k=20) that have been used 90% from datasets in the training phase and 5% in testing phase. We repeated this process to measure the performance for IDS by calculating the detection rate for normal and abnormal, alarms and standard deviation (SD). Table 3 shows the detection accuracy rate and the number of records that were used in our proposed security system.

Table 3 Classification Rate

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

Table 4 shows the rate of four alarms for grey hole and rushing attacks.

Table 4: 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%

B. Testing Neural Network to detect Rushing Attack

The type and number of records that was used in the training phase differs from the data set that was used in the testing phase. The IDS should be able to detect rushing attacks that have a direct and negative impact on VANETs. In both proposed security systems, we designed IDS with anomaly detection. It has the ability to detect novel attacks. Table 5 shows the accuracy of the detection rate and the number of records that were used in our proposed security system.

Table 5: Classification Rate

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

Table 6 shows the rate of four alarms for grey hole and rushing attacks.

Table 6 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%

V. Discussion

The motivation of this research is to provide an intelligent security system that creates a safe environment for self-driving and semi self-driving vehicles. The methodology of the proposed IDS was implemented in eight phases: generating the mobility and traffic model, the NS-2, the trace file, data collection and pre-processing, fuzzification of the data, training and testing for the FFNN, training and testing for the SVM and comparing the results that were generated in the two types of intelligent IDS. When we compare the two types of IDS, we can observe that the IDS was based on the FFNN was more effective and efficient in detecting malicious vehicles with a low false negative alarm rate than the IDS based on the SVM but we can notice SVM performance much faster the FFNN. The comparison

performance between the FFNN and SVM is as shown in figure 5. The error rate for the IDS based on the SVM was 0.19%. In this system, the alarm rate fluctuated between 99.92% and 99.70% with excellent and efficient accuracy. On the other hand, the average false negative alarm rate was low at about 0.20% which is a good indicator of the results.

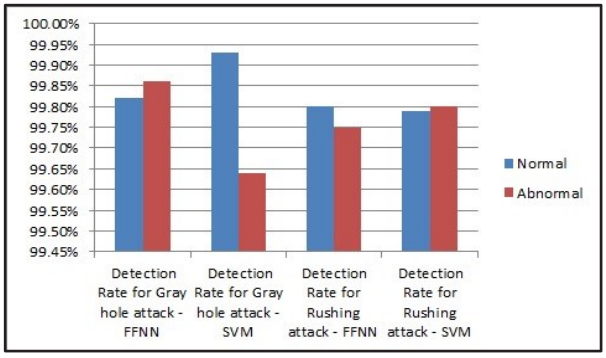

Fig. 5: Performance Comparsion

Meanwhile, the error rate for the IDS based on the FFNN was 0.17%. The alarm rate fluctuated between 99.92% and 99.75% with good and efficient accuracy. On the other hand, the average false negative alarm rate was low at about 0.1% which is an excellent indicator of the results. We could improve the detection rate by using fuzzified data with FFNN and SVM that create flexibility in selecting the system that is more efficiently with different conditions. In addition, in our proposal, we selected the significant features based on the previous study [6]. All these factors make the proposed security system more efficient in securing the external communication systems of self-driving and semi self-driving vehicles.

VI. Conclusion

Intelligent intrusion detection systems have become an important security application in modern systems such as self-driving and semi self-driving vehicles. The networks, vehicles and devices are exposed to many types of attacks that have a direct impact on the development and deployment of self-driving vehicles. Our proposed intelligent IDS can detect grey hole and rushing attacks in VANETs. These networks can provide safety to self-driving and semi self-driving by CAMs and data control that were exchanged between the vehicles in that zone. Grey hole and rushing attacks try to drop some or all received messages which can have a direct impact on the passenger's life, drivers and vehicles themselves. In other words, self-driving and semi self-driving vehicles without security cannot achieve their task in providing comfort and safety while in operation. In our paper, we designed an intelligent security system to secure external communication for self-driving vehicles. The IDS has been designed for training and testing with fuzzified data by using FFNN and SVM. This system deals with two system scenarios that have been generated and simulated in NS2. The behavior of all vehicles is investigated to identify the normal behavior and abnormal behavior in VANETs. We can detect grey hole and rushing attacks by monitoring or analyzing the trace file generated in network simulator. The trace file describes the behaviour of the network through send, receive, move, forward and drop. A possible further extension of the system is to these attacks with different AI techniques such as fuzzy petri nets (FPNs).

References

[1] C. Bhushan, "Security framework for VANET for privacy preservation," ICCCNT, Fourth International Conference on Computing, Communications and Networking Technologies (ICCCNT) 2013, pp. 1-6, doi:10.1109/ICCCNT.2013.6726601, 2013

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

[3] S. Surmukh, P. Kumari, and S. Agrawal, "Comparative Analysis of Various Routing Protocols in VANET," Advanced Computing & Communication Technologies (ACCT), 2015 Fifth International Conference on. IEEE, no. 978-1-4799-8487-9, pp. 21-22, 2015.

[4] G. Usha, and S. Bose, "Impact of Gray hole attack on adhoc networks," Information Communication and Embedded Systems (ICICES), International Conference on. IEEE, no. 978-1-4673-5786-9, pp. 404-409, 2013.

[5] K. Ganesh Reddy, P. Santhi Thilagam and B. Nageswara Rao, " Cross-Layer IDS for Rushing Attack in Wireless Mesh Networks," CCSEIT-12, pp. 396-400, 2012.

[6] K. Ali Alheeti, A. Gruebler, K. D. McDonald-Maier, " An Intrusion Detection System Against Black Hole Attacks on the Communication Network of Self-Driving Cars," Sixth internantional Conference on Emerging Security Technologies EST-2015 IEEE, Germany.

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

[8] A. Assila, I. Jabri and A. Ltifi, "Secure Architecture Dedicated for VANET Alarm Messages Authentication through Semantic Verification," Sciences of Electronics, 6th Technologies of Information and Telecommunications Technologies of Information and Telecommunications (SETIT) IEEE, no. 978-1-4673-1657-6, pp. 652-657, 2012.

[9] S. Banerjee, " Detection/Removal of Cooperative Black and Gray Hole Attack in Mobile Ad-Hoc Networksm," Proceedings of the World Congress on Engineering and Computer Science (WCECS), USA, no. 978-988-98671-0-2, PP. 22-24, 2008.

[10] K. Ganesh Reddy, P. Santhi Thilagam, B. Nageswara Rao, " Cross-Layer IDS for Rushing Attack in Wireless Mesh Networks," CCSEIT-12, pp. 396-400, 2012.

[11] K. Pavani, A. Damodaram, " Anomaly Detection System for Routing Attacks in Mobile Ad Hoc Networks," Int. J. Of Network Security, Vol. 6, pp. 13-24 , 2014.

[12] R. Kaur and 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.

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

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

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

[16] "TAPAS Cologne " Scenario," http://sumo.sourceforge.net/doc/current/docs/userdoc/Data/Scenarios/TAPASCologne.html,2011. [Access 20 Oct. 2014].

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

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

[19] C. Guanrong, Introduction to Fuzzy Sets, "Fuzzy Logic and Fuzzy Control Systems, " 2nd ed., Houston, Texas: CRC Press, ISBN 0-8493-1658-8, 2001.

[20] T. Issariyakul and E. Hossain , "Introduction to Network Simulator NS2," 2nd ed., New York Dordrecht Heidelberg London: Springer Press, 2012.