Hybrid Intrusion Detection in Connected Self-Driving Vehicles

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

Klaus McDonald-Maier
School of Computer Sciences and Electronic Engineering
University of Essex, Colchester, UK
kdm@essex.ac.uk

***Abstract*—Emerging self-driving vehicles are vulnerable to different attacks due to the principle and the type of communication systems that are used in these vehicles. These vehicles are increasingly relying on external communication via vehicular ad hoc networks (VANETs). VANETs add new threats to self-driving vehicles that contribute to substantial challenges in autonomous systems. These communication systems render self-driving vehicles vulnerable to many types of malicious attacks, such as Sybil attacks, Denial of Service (DoS), black hole, grey hole and wormhole attacks. In this paper, we propose an intelligent security system designed to secure external communications for self-driving and semi self-driving cars. The proposed scheme is based on Proportional Overlapping Score (POS) to decrease the number of features found in the Kyoto benchmark dataset. The hybrid detection system relies on the Back Propagation neural networks (BP), to detect a common type of attack in VANETs: Denial-of-Service (DoS). The experimental results show that the proposed BP-IDS is capable of identifying malicious vehicles in self-driving and semi self-driving vehicles.**

***Index Terms*—Self-driving cars, ANNs, IDS, BP.**

I. Introduction

The traditional definition of the internet has expanded to become a ubiquitous network that is now often called the Internet-of-Things (IoTs), featuring Machine to Machine (M2M) communication. This type of connectivity can provide an efficient connectivity for self-driving vehicles.

Self-driving vehicles are considered one of the most important aspects of device to device communication [1]. VANETs are a wireless mobile networks which allow self-driving vehicles to exchange beacons of information, such as Cooperative Awareness Messages (CAMs) with each other and road side units (RSUs) in their communication area. It is aimed to send/receive warning messages between neighboring vehicles, in order to offer road safety and comfort services on busy roads.

In wireless networks, malicious attacks can be launched from any location at any time within the radio area, because they do not have firewall and gateways, while in wired networks the malicious attack needs physical access to make an attack [2]. Each vehicle is very much exposed to being compromised because the car is free to move independently and does not have any physical protection [1]. Self-driving vehicles depend on the cooperative participation of other vehicles within the radio coverage area, this is because external communication has decentralized architecture. In this case, attackers try to break the cooperative protocols between the vehicles and the RSUs. Security systems such as encryption/decryption mechanisms and digital signatures can be used to reduce the amount of potential attacks on VANETs that were considered as the first line of defense. Moreover, these algorithms are unable to protect the system from unknown attacks because they were not designed to secure VANETs from these known attacks. For this reason, self-driving vehicles need a second line of defense in place to detect and identify these novel attacks, i.e. an intrusion detection system (IDS).

A primary approach to detecting the malicious behaviour in vehicle is through the communication between the CAMs, via VANET between self-driving vehicles and with their RSUs. Any intrusion detection scheme proposed to secure the routing protocol of VANETs of self-driving vehicles has two issues: (1) securing transmitted data from a vehicle to another (device to device), (2) securing and monitoring whole CAMs transmitted between vehicles the RSUs. IDS is considered an effective way to detect an intruder in the external communication of self-driving vehicles [2]. The IDS should be captured and examined for each packet that has been transferred or received between vehicles. This process is called audit data. The security system can determine normal and abnormal behaviour based on the audit data that has been collected from VANETs.

An IDS is composed of three phases:

- Data collection phase.
- Analysis data phase.
- Response phase.

In our paper, we propose misuse detection and anomaly detection or hybrid IDS based on Back Propagation artificial neural networks (ANNs) to predict attacks on the external communications of self-driving and semi self-driving vehicles. In other words, the proposed IDS is targeted to detect different types of cyber-attacks such as Distributed Denial of Service (DDoS) and network scanning. We utilized the Kyoto data set to evaluate the performance metrics of the proposed hybrid security system [3]. In this paper, we have two contributions, namely:

1) Reduce the number of features found in the Kyoto benchmark dataset.

2) Design intelligent intrusion detection scheme. It is based on a hierarchical network model.

The figure 1 demonstrates the basic structure of the proposed IDS that has been installed on each vehicle to detect malicious behaviour.

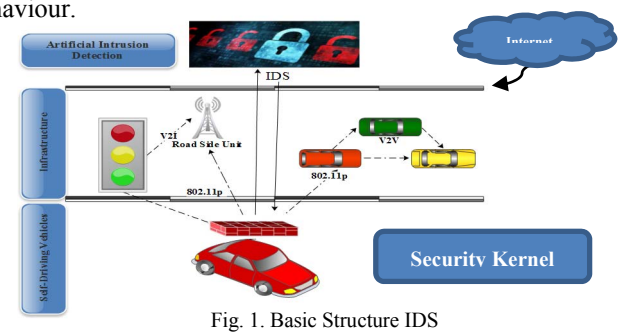

Fig. 1. Basic Structure IDS

The rest of the research paper is organized as follows: Section II: Literature reviews. Section III: Benchmark data set collection. Section IV: The proposed security system. Section V: Experimental evaluation and results. Section VI: Discussion and section VII: Conclusion.

II. Literature Reviews

In the next five years, it is projected that more than 250milion vehicles will be connected together with RSUs [4]. Self-driving and semi self-driving vehicles will be a major element in the IoT domain, with one in five vehicles having wireless communication by 2020 [4]. Petit et al. have investigated potential cyber-attacks and threats on automation and cooperative automated vehicles [5]. Their research demonstrates that these vehicles will be associated with many different types of such attacks. In addition, these vehicles need to be built with the awareness of these threats in mind, and thus incorporated into the early stage development of self-driving vehicles. Zhang et al. have presented surveys for defense schemes and attacks such as Sybil in the related area of the IoT [1]. The authors define three as a serious type of Sybil attacks: SA-1, SA-2 and SA-3, these have a direct and negative impact on performance and privacy data of smart objects in IoT. Ali et al. have proposed intelligent security systems to secure external communication of self-driving vehicles [6]. These systems have the ability to detect two types of attacks such as a grey hole and rushing attacks. The authors noted that IDS can be built based on two technologies which are Feed-Forward Neural Network (FFNN) and Support Vector Machine (SVM). They also compared the two technologies to identify which one is more accurate. Tahir et al. have presented a security scheme for the networked sensor systems [7]. Their system is based on using the inherent features of a device to generate a secure identity for devices in their environment. Petit et al. have compared the different ways that reflect the current case of identification and standardization of open challenges of security and privacy of automotive vehicles [8]. In other words, they created a survey of the requirements and challenges of principle security in self-driving vehicles. In practice, this survey focused on pseudonym approaches which relied on keys of cryptography mechanisms.

Our previous work had researched IDS systems that focused either on detecting abnormal behaviour [9] or misuse [10], here we propose a first system that addresses the detection of both through a hybrid IDS. However, we proposed a hybrid security system to secure and identify attacks in external communication of self-driving and semi self-driving vehicles.

III. Benchmark Data set Collection

The dataset utilised is considered one of the most important factors in evaluating the efficiency of any proposed system. Most of the previous researches used the KDD Cup 99' data set for evaluating performance of the proposed security system [11]. However, we cannot use this data in the research work presented here, as it suffers from a major problem of not covering current and recent network topologies and latest attack trends. This data is outdated it was extracted and created by system simulation more than 10 years ago [3]. We used the Kyoto benchmark in testing and evaluating performance of the proposed IDS. It is built from the real traffic data on a network. This honeypot data was collected over a 3-year period [11]. The Kyoto data set consists of two types of data:

1) *Kyoto data set with Internet Protocol (IP) source and IP destination.*
2) *Kyoto data set without IP.*

We used the first option as it utilises a label field of normal and abnormal connection. This type of the Kyoto data set consists of 24 factors that reflect normal and abnormal behaviour of a network. The first 14 features were derived from KDD Cup 99' data set, as well as the remainder of the features generated from a real network. Table 1 shows the types of features.

Table 1 Features of Kyoto Data set

Feature Name	Feature Source
Duration, Service, Source bytes, Destination bytes, Count, Same srv rate, Serror rate, Srv serror rate, Dst host count, Dst host srv count, Dst host same src port rate, Dst host serror rate, Dst host srv serror rate and Flag	KDD Cup 99'
IDS_detection, Malware_detection, Ashula_detction, Label, Source IP Address, Source Port Number, Destination IP Address, Destination Port Number, Start Time and Duration	Real Network

IDS researchers recommended the use of this data set in any new proposed IDS because it gives a more practical and accurate evaluation and results [3].

IV. The Proposed Security System

The detection system and reducing process of the number of features are considered a significant contribution made in this paper. It consists of five phases which are:

1) *The preprocessing phase.*
2) *The features selection phase.*
3) *The Fuzzification phase.*
4) *The training and testing phases.*

The proposed intelligent IDS is a utilised MPL that is comprised of four layers: an input layer, a two hidden layers and an output layer. The fuzzification data is considered input data for the first layer that consists of 65 neurons. The number of hidden layers and neurons based on the accuracy of the training phase. In other words, we designed IDS with two hidden layers; the first hidden layer consists of 12 neurons while the second hidden layer consists of five neurons. The proposed security system has three values in the output layer which are: normal, abnormal and unknown. The detection phase is considered the second contribution of proposed IDS.

The steps below explain the methodology of the proposed IDS and how we were able to reduce the number of features and maintaining the detection accuracy with fuzzification. Figure 3 shows the overall IDS architecture.

A. Preprocessing Data Set Phase

We utilize the Kyoto benchmark data set to evaluate performance of the proposed security system. This data set needed preprocessing stages such as: encoding, uniform

distribution and normalization.

1) Encoding stage: Some features were represented by symbols such as a flag feature with symbols: “SO”, “REJ”, “RSTO”, “SF”. We needed to convert symbol features to numerical values before making any changes to the data set. This process is considered important because the feature vector fed to the input layer of BP and had to be numerical.

2) Uniform distribution stage: This is very important to BP. Without it, the system training would not be accurate. We prepared 60,000 data set records to simulate the proposed security system. It is divided into three subsets with each of them having different number of normal and abnormal records that were generated randomly from the original dataset. They had the following property: if the sample number of normal pattern is T subset and the original dataset has D samples, then there is a probability of finding a sample of class normal in the first subset D/T samples of the final data. Hence, each subset of the final data set has almost the same distribution and ratio of record type of the full data set.

3) Normalization of numerical attributes stage: In the normalization, each numerical is value set between 0.0 and 1.0 according to Equation 1. As a result, neural network training is often more efficient with normalized data, it is used as the preferable predictor.

$$X = \frac{x - MIN}{MAX - MIN} \quad (1)$$

Where X is the normalized value with a range between 1 and 0, x is the original value, max and min are maximum and minimum values of the original variable. These values are used to match the upper and lower limits of the activation Function-Sigmoid that have been used in the ANN models.

In the training phase, we set some data set of validation to overcome one common problem in ANN which is over-fitting that usually occurs during the training phase. The training process is stopped when validation errors increase for a specified number of iterations.

B. Extract The Impact of Features Input Phase

Feature selection and the ranking process for significant features are considered important issues in design of the detection systems [12]. Thus, the effective and efficient performance of the IDS heavily depends on the number and type of Kyoto features. In other words, the elimination of useless features improves the detection rate, decreasing the computation time and memory, hence enhancing the overall performance of an IDS.

The most important features are selected to increase the accuracy of the detection and reducing the amount of the false alarms. In this paper, a statistical approach is utilised to select significant features that have a high weight value and a critical effect, namely the Proportional Overlapping Score (POS) technique [13].

The POS is calculated for each feature in Kyoto benchmark to avoid from the outlier’s effect. In this case, relevant features selection depends on the measure for the overlap value. The designer can set the dataset size of the selected features [14]. The POS is considered the most efficient and suitable method with common types of dataset [13]. Furthermore, it is effective, even with a dataset that has classification problems. These problems are examples such as outliers and high-dimensional binary [14]. The POS is employed to calculate the overlapping rate in the dataset. The recognition features are picked up by measuring the overlap between feature values in the Kyoto dataset across two classes. It yields a perfect performance on all types of dataset with different classifiers approach [13]. We used the statistical R language for programming the POS method that pseudocode is shown below:

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[1:23,] # define the features matrix 23.
12. G <- jitter(G). # to avoid the noise in data
13. class <- as.factor(data[24,]) #define class labels.
14. set.seed(1234).
15. selection <- Sel.Features(G, Class, K=23,Verbose=TRUE)
    # the main function.
16. selection$Features. # extract the number of features
17. selection$Measures. # extract name of features.
```

Now, each feature is tagged with overlap value, we then start removing the features which had the lowest weight. The principle of trial-and-error is used to determine the optimal number of extracted features based on accuracy detection in the training phase for ANN [15]. In other words, we started with 23 features and after each round of training we calculated the training accuracy and deleted features that had less influence in the detection process. This process will be repeated several times until we get to the criteria which is: the optimal number of the features that is based on the training accuracy.

In this paper, we can achieve 99.18% training accuracy with 13 features, that describes normal and abnormal behaviour in the Kyoto benchmark. Reducing the number of features is the first contribution in this paper. The proposed IDS examined with all features and 13 selected features. These features are shown in table 2.

TABLE 2 SIGNIFICANT FEATURES

Signaficant Feature Name	Feature Source
Duration, Service, Source bytes, Destination bytes, Count, Dst host count, Dst host srv count, and Flag	KDD Cup 99’
Label, Source IP Address, Source Port Number, Destination IP Address, Destination Port Number and Duration	Real Network

C. The Fuzzification Phase

Fuzzy set is considered an optimal solution for a dataset that suffered from the classification problems [16]. The significant features are selected from the Kyoto benchmark dataset and had a direct and positive impact on the performance of the proposed IDS [17]. In this paper, we reduce the number of features that made the name of classes for normal and malicious behavior, as it is not very well separated. In this case, the detection rate is declined and increases the number of false alarms.

The fuzzification process has the ability to establish a clear border within significant features to fix classification problems [16]. In Table 2, we have illustrated the role of the fuzzification in changing the results for the better.

$$f(x,a,b,c) = max(min({}^{x-a}/_{b-a}, {}^{c-x}/_{c-b}),0) \qquad (2)$$

Where, x is the normal value of the dataset before fuzzification while a, b and c values represent the fuzzy domain values. The proposed security system is to ultimately be more efficient with fuzzification data [15]. In other words, it has the ability to fix the confusion or ambiguity through redistributing each feature value with new five values. Equation 2 allows each value from the selected features to take five values from the fuzzy domain with interval range is [0, 1].

TABLE 3 PERFORMANCE METRICS

IDS with all Features		IDS with 13 Features	IDS with 13 Fuzzification Features
Misuse Detection Normal	97.5%	99.79%	99.23%
Misuse Detection Abnormal	99.2%	64.34%	99.05%
Anomaly Detection Normal	92.04%	60.35%	99.04%
Anomaly Detection Abnormal	99.85%	98.45%	99.06%
Unknown Rate	28.5	0%	0.03
Average FP Alarm	2.27%	23.61%	1.82%
Average FN Alarm	1.01%	7.38%	0.4%
Average Error Rate	1.9%	19.32%	0.88%
Training Para.Epochs	115	75	27

According to table 3, we can easily notice the important role of the fuzzification dataset in enhancing detection rate, reducing the amount of false alarms and error rate. In addition, fuzzification features have a positive reflect on the training phase for ANN reducing the number of epochs.

D. The Training and Testing Phase

In our IDS, we employ a popular supervised learning of neural network architecture called multi-layer perceptron (MLP) with back-propagation gradient-descent in the designed security system [17]. The collection of non-linear neurons is connected to each other to form a feed-forward multi-layer in MLP [18]. This technique is known to be robust for prediction and classification problems. Figure 2 demonstrates the graphical representation of the original MLP used in this research. Cross-validation is used to determine the "optimal" number of hidden layers and neurons that were based on the experimental design of the IDS. Specifically, MLPs started from a small number of neurons, and with one hidden layer, that measures the error ratio of the trained BP on holdout samples, steadily increasing the number of neurons at a hidden layer where the performance of the trained phase on holdout samples has started to decline due to overtraining problem. In this case, we determine an optimal number of neurons for the hidden layer of the ANN.

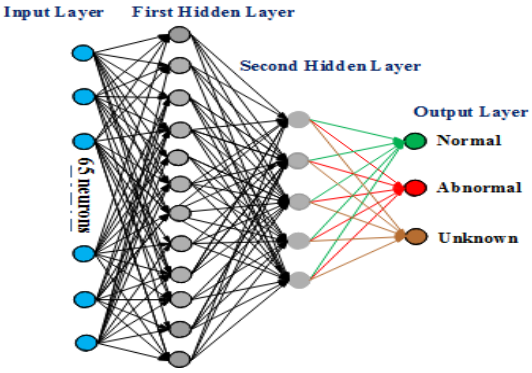

Fig. 2. Graphical representation of our MLP neural network model

We used a 100-fold cross-validation to decrease the bias related with the process of random splitting of the Kyoto data set into training phase and testing phase. The network training ends when the Least-square-error E between the desired d_i and actual output y_i is less than Emax or when the number of sweeps equal 500. We define $E_{\max= 1*10^{-7}}$.

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

Where p is the total number of training patterns, and:

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

For all experiments, the learning rate α was fixed to 1*10-7 for each training yielding difference, of which the best result is selected. In our research, we used trial-and-error attempts to configure the best ratio of training depending on the condition put on the second phase of the proposal. Table 4 shows some of the configuration parameters used in the ANN.

TABLE 4 ANN PARAMETERS

Parameter	Value
Train Parameter epochs	81
Train Parameter ln.	$1*10^{-7}$
Train Parameter goal	0
Train Parameter Minimum Gradient	$1*10^{-11}$

In the detection phase, we tested the detection system with significant features that selected from the Kyoto benchmark data set. The behaviours are analyzed and then the IDS generates four types of alarms: true positive, true negative, false positive and false negative [6]. These alarms and the detection accuracy rate are used to measure the IDS performance. The detection phase has three outputs which are: normal, abnormal and unknown. We design the simulation on a system with an Intel core i3 processor "2.53GHZ" and 4GB RAM memory.

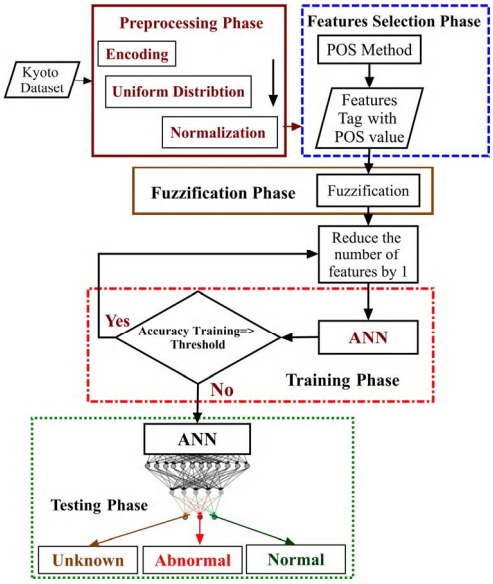

Fig. 3. Overall IDS Architecture

The misuse and anomaly detection systems are utilised so ANN can efficiently learn the benign and malicious behaviours through the iterative operation [19]. In addition, it has the ability to improve real-time responsiveness and reducing the costs.

V. Experimental Evaluation And Results

The proposed IDS used a dataset of 60,000 records to describe the normal, abnormal and unknown behaviour in networks. The data set used in our evaluations come from the Kyoto University as indicated above [20]. The accuracy training algorithm is = 99.18%. The accuracy of the detection is calculated based on Equation 4 below [17] [21]:

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

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

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

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

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

The data set was divided into three subsets: the test set (25%), the validation set (25%) and the training set (50%). We tried to avoid one of the most common problems of an ANN which was the over fitting by specific parts of the data used to validate.

A. Training and Testing IDS with Misuse Detection

We used a misuse detection technique in designing the IDS. This system has two features: high detection rate and low false alarms. These characteristics are made more interactive when building any IDS. The accuracy of the detection rate and the number of records that were used in our proposed IDS is shown in Table 5.

TABLE 5 Classification Rate

Class	Original No.	Neural No.	Accuracy
Normal	6895	6829	99.04%
Abnormal	3105	3076	99.06%
Unknown	0	4	0.04%

Table 6 shows the rate of alarm and error rate that generated in our proposal based on Equations 5, 6, 7 and 8.

TABLE 6 Alarm and Error Rates

Alarm Rates			
True positive	99.59%	**False negative**	0.40%
True negative	97.99%	**False positive**	2.00%
Error Rate	0.95%		

B. Training and Testing IDS with Anomaly Detection

We trained and tested the proposed security system with the Kyoto data set [11]. The performance of the proposed IDS is directly related to anomaly detection algorithm. If the anomalies are detected correctly from the data set, it provides a high detection rate and less false alarms. The anomaly detection has the ability to detect novel attacks. Our experiment showed that the performance of the IDS is largely influenced by the type of training data.

The system calculated the classification rate and generated four types of alarms for the proposed IDS as shown in Table 7.

TABLE 7 Classification Rate

Class	Original No.	Neural No.	Accuracy
Normal	6640	6887	99.23%
Abnormal	3060	3031	99.05%
Unknown	0	3	0.03%

Table 8 shows the rate of four alarms and error rate of detection system of communication of self-driving vehicles that were calculated based on Equation 5, 6, 7 and 8.

TABLE 8 Alarm and Error Rates

Alarm Rates			
True positive	99.60%	False negative	0.40%
True negative	98.34%	False positive	1.65%
Error Rate	0.82%		

VI. Discussion

Conventional security systems are not able to protect the external communication of self-driving and semi self-driving vehicles. In this case, we need to identify new security methods or modify the current protection schemes in order to provide efficient functionality in protecting these types of networks.

In our paper, the alarm rate fluctuates between 97.99% and 99.60%. This enables an efficient detection rate with an average rate error of 0.88% while the previous best achieved average error rate was 8.68% [22]. In [22], the average rate of false alarm is 4.86%, while we achieved 1.64% with the IDS presented here. Thus, our results confirm that the performance of hybrid IDS is efficient in detecting DoS of communicating self-driving vehicles. According to the simulator results, we can easily distinguish the role of reducing the number of features and fuzzification data in improving the performance of the security system. The proposed IDS can overcome overlapping problems by employing the POS method in order to select the significant features and applying fuzzy set "fuzzification" to the extracted features. Intelligent IDS can secure the VANETs of self-driving

vehicles by detecting and blocking malicious behaviours in its external communication. The proposed security system is mainly suitable for detecting abnormal behaviours that target vehicles disturbing the communication between self-driving and semi self-driving vehicles. From the experiment, we can observe the important role of the IDS in improving the external security of communication vehicles under different conditions.

The IDS has a direct impact on the performance of the network by improving the detection rate, as well as decreasing the number of false alarms and the error rate. In future work, we need to utilize the IDS on VANETs based on a virtual layer, and we expect to propose a better intrusion behavior category for self-driving vehicles.

VII. Conclusion

In this research, we have designed a hybrid BP-IDS based on the behaviour of connected communicating vehicles. The proposed intrusion detection scheme uses an intelligent anomaly and misuse detection approach in detecting malicious behaviour in VANETs of self-driving vehicles which adapt to the heterogeneous communicating environment. The proposed system has the ability to detect the malicious vehicle which is a source of an attack. The proposed security system can provide sufficient security for VANETs of self-driving cars. This system has been built for the training phase and testing phase of two system scenarios: normal and abnormal that have been based on the Kyoto data set. The IDS is used to analyze the behaviour of each vehicle in the IoT to detect if it is a DoS vehicle or a normal vehicle. If the car is trying to prevent the access to the resources of the network and make these unavailable at any time, this is indicated as a DoS vehicle. The hybrid proposed BP-IDS has the ability to distinguish between both existing, novel or new attacks.

The experiment reflects the performance of IDS in detecting and isolating DoS. It is good for securing the external communication of self-driving vehicles. The proposed BP-IDS can well suited for deployment in heterogeneous environment. This system is flexible and extensive. It has the ability to detect external and internal attacks launched at any time on the network. Our proposed IDS can also isolate malicious self-driving vehicles with high detection rate and can guarantee low false alarm. The process of decreasing the features by POS technology plays important role in enhancing the detection rate of the proposed IDS. Furthermore, the fuzzification data help declining the number of false alarms and error rate when compared with our previous publication.

References

[1] K. Zhang, L. Xiaohui, L. Rongxing, and S. Xuemin, "Sybil Attacks and Their Defenses in the Internet of Things," Internet of Things Journal IEEE, no. 5, pp.372-383, 2014.

[2] M. Erritali, b. El Ouahidi, "A review and classification of various VANET Intrusion Detection Systems," IEEE Security Days (JNS3), 2013 National,pp. 1- 6, 2013.

[3] J. Song, T. Hiroki, O. Yasuo, E. Masashi, I. Daisuke, and N. Koji, "Statistical analysis of honeypot data and building of Kyoto 2006+ dataset for NIDS evaluation," In Proceedings of the First Workshop on Building Analysis Datasets and Gathering Experience Returns for Security, pp. 29-36. ACM, 2011.

[4] Internet of Things & Smart Cities (2016, January). Available online: http://Downloads/151102_insights_capitalising_on_internet_of_things.

[5] J. Petit and E. Steven Shladover, "Potential Cyberattacks on Automated Vehicles," Intelligent Transportation Systems, IEEE Transactions on 16, no. 2, pp.546-556, 2015.

[6] K. M. Alheeti, A. Gruebler, K. McDonald-Maier, "On the detection of grey hole and rushing attacks in self-driving vehicular networks," In Computer Science and Electronic Engineering Conference (CEEC), 7th 2015 Sep 24 (pp. 231-236), 2015.

[7] H. Tahir, R. Tahir, K. McDonald-Maier, "Securing MEMS Based Sensor Nodes in the Internet of Things," In 2015 IEEE Sixth International Conference on Emerging Security Technologies (EST), (pp. 44-49).

[8] J. Petit, S. Florian, F. Michael and K. Frank, "Pseudonym schemes in vehicular networks: a survey," Communications Surveys & Tutorials, IEEE 17, no. 1, pp: 228-255, 2015.

[9] M. Sato, H. Yamaki, H. Takakura, "Unknown attacks detection using feature extraction from anomaly-based ids alerts," In Applications and the Internet (SAINT), 2012 IEEE/IPSJ 12th International Symposium on pp. 273-277, 2012.

[10] B. Ahmed, "Link analysis approach to improve detection of fragmentation attacks in Misuse IDS," In 2009 First International Conference on Communications and Networking, pp. 1-8, 2009.

[11] The third international knowledge discovery and data mining tools competition dataset KDD99-Cup http://kdd.ics.uc

i.edu/databases/kddcup99/kddcup99.html.

[12] K. M. Alheeti, L. Al-Jobouri, K. McDonald-Maier, "Increasing the rate of intrusion detection based on a hybrid technique," 5th In Computer Science and Electronic Engineering Conference, pp. 179-182, 2013.

[13] 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.

[14] Official site for PropOverlap package (2016, April). Available online: http://cran.r-project.org/web/packages/propOverlap/index.html.

[15] 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. In 2015 Sixth International Conference on Emerging Security Technologies (EST) 2015 Sep 3 (pp. 86-91).

[16] 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.

[17] K. M. Alheeti, W. Venus, and M. Suleiman Al Rababaa, "The affect of fuzzification on neural networks intrusion detection system," In Industrial Electronics and Applications, ICIEA 2009. 4th IEEE Conference on 2009 May 25 (pp. 1236-1241), 2009.

[18] D. Delen, S. Ramesh, and B. Max, "Identifying significant predictors of injury severity in traffic accidents using a series of artificial neural networks,"Elsevier Accident Analysis & Prevention-no.3,434-444,2006.

[19] Using Artificial Intelligence to create a low cost self-driving car. Pdf (2016, April). Available online.

[20] Koyoto dataset (2016, April). Available online: http://www.takakura.com/kyoto_data/BenchmarkData-Description-v5.pdf.

[21] S. M. Al-Naqshabandi, "Simulation system for computer network intrusion detection," A thesis submitted in partial fulfillment of there quirements for the degree of doctor of philosophy in computer science, Al-Nahrain University, Baghdad, Iraq, pp.61-66, 2007.

[22] K. Ali Alheeti, A. Gruebler, K. D. McDonald-Maier, "An Intrusion Detection System Against Malicious Attacks on the Communication Network of Driverless Cars," In IEEE Consumer Communications and Networking Conference (CCNC), 12th Annual 2015 (pp. 916-921).