Digital Communications and Networks 3 (2017) 180–187

HOSTED BY

Contents lists available at ScienceDirect

Digital Communications and Networks

journal homepage: www.elsevier.com/locate/dcan

Using discriminant analysis to detect intrusions in external communication for self-driving vehicles☆

Khattab M.Ali Alheeti[a,b,*], Anna Gruebler[c], Klaus McDonald-Maier[d]

[a] Embedded and Intelligent Systems Research Laboratory, School of Computer Science and Electronic Engineering, University of Essex Wivenhoe Park, Colchester CO4 3SQ, UK
[b] University of Anbar, College of Computer Science and Information Technology, Anbar-Iraq
[c] Data Science at AltViz in London - Data Scientist, UK
[d] School of Computer Science and Electronic Engineering, University of Essex, Colchester CO4 3SQ, UK

ARTICLE INFO

Keywords:
Secure communication
Vehicle ad hoc networks
IDS
Self-driving vehicles
Linear and quadratic discriminant analysis

ABSTRACT

Security systems are a necessity for the deployment of smart vehicles in our society. Security in vehicular ad hoc networks is crucial to the reliable exchange of information and control data. In this paper, we propose an intelligent Intrusion Detection System (IDS) to protect the external communication of self-driving and semi self-driving vehicles. This technology has the ability to detect Denial of Service (DoS) and black hole attacks on vehicular ad hoc networks (VANETs). The advantage of the proposed IDS over existing security systems is that it detects attacks before they causes significant damage. The intrusion prediction technique is based on Linear Discriminant Analysis (LDA) and Quadratic Discriminant Analysis (QDA) which are used to predict attacks based on observed vehicle behavior. We perform simulations using Network Simulator 2 to demonstrate that the IDS achieves a low rate of false alarms and high accuracy in detection.

1. Introduction

Self-driving and semi self-driving vehicles are attracting increased attention from both industrial and research communities due to their potential positive societal and economic effects [1]. These vehicles depend heavily on internal and external communications systems to achieve goals, such as traffic safety, ideal exploitation of resources, reduction of human error and reduction in the number of injuries and fatalities from traffic accidents [2]. In other words, autonomous and semi-autonomous vehicles operate without drivers and have the ability to improve traffic flow for vehicles and reduce human errors [3].

VANETs are external communication systems that support intelligent transportation systems for vehicles [4]. VANETs play an important role in establishing a secure and safe environment for self-driving and semi self-driving vehicles [5]. VANETs applications can be classified into safety and non-safety applications [6]. Real-time safety applications, fleet management services, and traffic management and monitoring are the most important uses for these networks [7]. Additionally, security systems are very important for the safe operation of these vehicles [7]. Strong and reliable security mechanisms are needed to protect information and controller data as it is transferred between vehicles and their Road Side Units (RSUs) in areas with radio coverage [8].

The IDS can be used as an effective tool to know when unauthorised users are trying to gain access, already have access or have compromised the network. However, when IDS is implemented for wired networks, there are additional challenges in setting up IDS due to the dynamic topolopies of ad hoc networks. Traditional security systems are sometime unable to provide a safe environment and sufficient protection for sensitive data [1]. Traditional methods can only identify external attacks and they are unable to detect and block internal malicious agents. In order to detect internal attacks, an intelligent security system is proposed based on and trail data. This data is collected from the trace file used to monitor normal and abnormal behaviors in automobile vehicles. VANETs are a subclass of mobile ad hoc networks (MANETs) [9]. There have been a few previous attempts to secure MANETs routing protocols. For example, the Secure Efficient Ad hoc Distance vector routing protocol (SEAD) [10], the secure on-demand routing protocol - Ariadne [11], Authenticated Routing for Ad hoc Networks (ARAN) [12], and Security-Aware Ad hoc Routing (SAAR) [13], Resiliency Oriented Secure (ROS) [14], Secure Routing Protocol (SRP) [15], Secure AODV (SAODV) [16], Secure Link-State Protocol (SLSP) [17], and Cooperative Security-Enforcement Routing (CSER) [18]. These routing schemes cannot completely eliminate all internal attacks, even when they are implemented correctly. This is due

☆ Peer review under responsibility of Chongqing University of Posts and Telecommunication.

* Corresponding author.
E-mail addresses: kmali@essex.ac.uk (K.M.A. Alheeti), contact@annagruebler.com (A. Gruebler), kdm@essex.ac.uk (K. McDonald-Maier).

http://dx.doi.org/10.1016/j.dcan.2017.03.001
Received 25 September 2016; Received in revised form 26 February 2017; Accepted 7 March 2017
Available online 09 March 2017

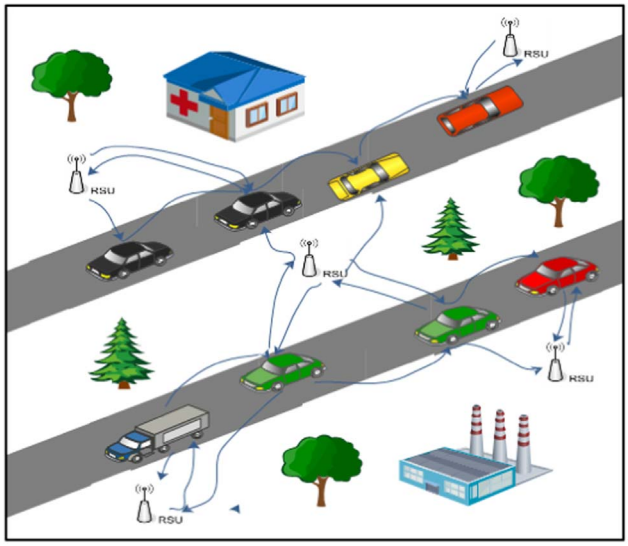

Fig. 1. VANETs Architecture.

to attacker presence inside the network with adequate credentials. For instance, a compromised mobility node holds all of the vital cryptographic keys and can easily launch several types of attacks, such as grey hole attacks, routing loop attacks and black hole attacks. Thus, it is important to develop responsive detection techniques for VANETs that are applicable to the aforementioned attacks. Fig. 1 illustrates how communications take place between vehicles and RSUs in a single zone, VANETs allow mobile vehicles to communicate with other vehicles (V2V) and with infrastructures on the roadside (V2R).

It is necessary to create an intelligent anomaly IDS to secure routing protocols on the network layer from potential internal and external attacks. Thus, the intrusion detection forms secondary defense. The IDS can be used as an effective tool for identifying when unauthorized users are trying to gain access, already have access or have compromised the network. However, when IDS is implemented on wired networks, there are additional challenges in setting up the IDS due to the dynamic topologies of ad hoc networks. An IDS has recently been used in external vehicle communications to identify and block any attacks that target the communication systems. Decisions made in the detection frameworks are based on the current normal and abnormal behaviors of the monitored self-driving vehicles [8,19,20]. The contributions of this paper are summarized as follows:

- An intelligent IDS using Linear Discriminant Analysis (LDA) and Quadratic Discriminant Analysis (QDA) to detect anomalies and malicious behaviors for self-driving and semi self-driving vehicles.
- The proposed security system is not dependent on expensive external hardware such as Radar, Lidar, computer vision, or any RSUs.

Section two discusses related work in the domain of security systems in ad hoc networks. Section three discusses intrusion detection systems. Section four describes the simulation system and section five describes the simulation results. Section six discusses generalized results. Section seven contains our conclusion and outlines future works.

2. Related works

Autonomous vehicles are becoming increasingly open and connected to the external environment. This development increases the possibility for attacks as it enables intruders to launch various types of attacks on vehicles [6]. These vulnerabilities have direct negative effects not only on passengers, but also on pedestrians around them. The external communications system used for self-driving and semi self-driving vehicles face many security issues in their wireless communications. The role of an IDS is to collect traffic data from the communications system, analyze it and then identify/blocking any malicious behaviour in the VANETs.

Wireless communications systems in autonomous vehicles helps to prevent common problem such as drivers errors. Additionallly, VANETs supply critical information emergency cases, such as warning and notification messages. Thus, security and privacy are considered very important issues for VANETs. Although many previous studies address the problems in VANETs, many security issues that remain still need to be addressed. Studies such as that by Ozgur et al. have employed cognitive techniques to enhance communication performance in wireless sensor networks [21].

2.1. Packet drop intrusion detection

Alheeti et al. [22] designed an intelligent IDS for securing controller data and information as it is transferred between self-driving vehicles and their infrastructure. Malicious agents were detected and blocked by an IDS in a radio zone. The detection system used Fuzzy Petri Nets to enable sufficient protection. In [23], Uyyala designed an IDS in secure MANETs which aimed at black hole and grey hole attacks. It could detect and isolate malicious behavior in nodes. As a result, the authors noticed improved network performance. In [24], the authors developed an IDS to secure MANETs from potential attacks. It used a Fuzzy Interface System (FIS) to detect abnormal behavior in MANETs. The IDS was capable of identifying packet-drop attacks with high accuracy and a low false positive rates. In [25], an adaptive detection threshold was used to design an IDS capable of identifying intelligent abnormal activities in VANETs. The proposed system can immediately identify any malicious behavior in VANETs as data is extracted from mobile vehicles. Additionally, it has the ability to detect malicious behaviors while maintaining a high rate of packet delivery during the detection process.

2.2. Routing protocols

Zaidi [26] presented an IDS using a statistical technique to detect false information attacks. Traffic models were used to detect rogue nodes in VANETs. The authors used different types of parameters, such as transmission intervals for a large number of vehicles, to distinguish between normal and abnormal behavior. Ali et al. designed an IDS to protect external communications for driverless and semi-driverless vehicles [27]. The proposed IDS relied heavily on features extracted from the trace file of Network Simulator v2(ns-2). Support Vector Machines (SVMs) and Feed-Forward Neural Networks (FFNNs) were used to build an intelligent IDS with the ability to detect and block two common types of attacks: grey hole attacks and rushing attacks.

Coussement et al. designed an IDS to identify abnormal behaviors that may have negative impact on the external communications systems of mobile vehicles [28]. The proposed system examines incoming and outgoing communication packets to detect attacks. It uses a decision making mechanism to secure sensitive information of VANETs. Two approaches to security are configured: one for vehicles and one for RSUs. These systems work together to establish groups of mobile nodes based on vehicle speed. The proposed security system is based on a combination of two IDS schemes and the clustering of mobile nodes.

2.3. Cross-layer intrusion detection

In [29], the authors proposed a cooperative IDS to identify black hole attacks. It was based on a cross-layer architecture called MAC and a network layer detection system using information from VANETs and vehicle conditions data to determine vehicle behavior. The cross-layer security system reduced the number of false alarms and enhanced

detection accuracy.

Marve et al. proposed an IDS based on a cross-layer architecture to detect Denial of Service(DoS) and Distributed Denial of Service (DDoS) attacks on various layers in the transfer protocol stack [30]. The authors were able to design a security system that provides sufficient protection for nodes in MANETs while reducing the number of false alarms.

In [31], the authors propose a cross-layer architecture IDS that had the ability to detect malicious nodes and different types of DoS attacks. Additionally, the proposed IDS could detect various kinds of sink hole attacks and flooding attacks in an efficient manner.

Akyildiz et al. proposed a novel technology, called xG networks, to fix common problems in existing wireless networks. The proposed system has the ability to improve communication performance by increasing the available communication bandwidth and improving efficiency in bandwidth consumption [32].

Because the autonomous technology is a relatively new concept, additional research and proposals must be performed in order to prove its effectiveness and applicability. Security and privacy must be taken into consideration to ensure the success of self-driving and semi-self-driving vehicles. In our research, we propose a security system to protect external vehicle networks from common attacks such as DoS, black hole, and grey hole attacks. It is based on features from the trace files generated by ns-2.

3. Intrusion Detection Systems (IDS) overview

Typically, VANETs have two security layers [33]. They are used to protect the internal and external communications systems of autonomous and semi-autonomous vehicles.The two layers are an Intrusion Prevention Systems (IPS) and an IDS [34]. Security measures are a serious topic in automotive systems because the first layer alone typically does not provide adequate security [35].

Additionally, the external communications of these vehicles can provide a variety of safety and non-safety services, which aid in increasing research efforts and the growing interest in security systems. An IDS is seen as one way of protecting VANETs, as it can detect malicious or abnormal activities in the host or network [36]. An IDS has the ability to provide adequate security and privacy for systems and networks because it plays a vital role in identifying and preventing internal attacks, which cannot be identified or blocked by other security methods. Furthermore, certain studies have confirmed that an IDS is effective at detecting any unauthorized access [37].

3.1. IDS categories

IDS can be categorized in various ways. However, the major classification is: misuse, anomaly, and specifications detection systems [38]. Each detection method has certain qualities that separate it from the others. These qualities can be positive or negative. However, all these methods attempt to provide adequate security, prevent unauthorized access, and detect all unauthorized access by malicious agents or nodes [38].

- Signature-based system – This type of detection technique involves a security system containing a database of the behaviors of possible attacks. This data-set can be compared to the behavior of the system and attacks are detected when there is a match.
- Anomaly-based system – This detection system depends on known behaviors. There is an attack if the system detects any deviation from regular behavior. Additionally, the system depends on a profile developed from the regular behavior of the network.
- Specifications-based system – This detection system works based on a set of conditions whose availability in the protocol or program is necessary. An attack can be detected when these conditions are not met.

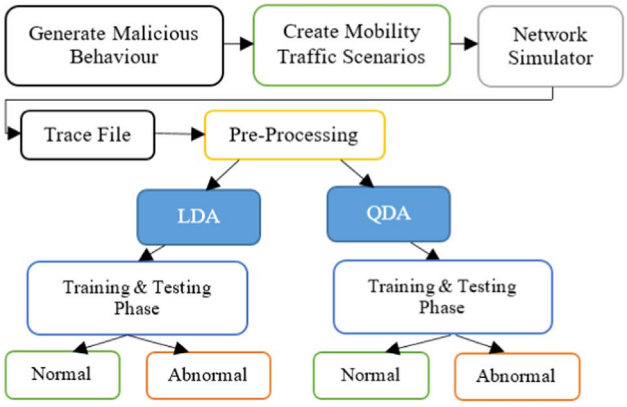

Fig. 2. VANETs Architecture.

There are many mechanisms that can be used for the protection of the communications systems in self-driving and semi-self-driving vehicles. We have chosen to use an IDS because they are designed to detect internal attacks, which is an advantage over conventional security mechanisms such as cryptographic methods which cannot detect internal attacks. We propose an intelligent IDS that uses the behaviors of vehicles, which are collected from the trace file generated by ns-2.

The proposed IDS is deployed on each vehicle that plays an important role in detecting internal or external attacks on the VANETs of self-driving and semi-self-driving vehicles without the need for additional hardware.

4. The proposed scheme

The proposed intelligent IDS first simulates malicious behaviors for self-driving vehicles. The network simulator uses various tools to establish a realistic model of abnormal and normal behaviors for autonomous vehicles. In other words, mobility and traffic models are generated in the early stages of the proposed IDS. An overview of the architecture of the proposed IDS is shown in Fig. 2. The security system requires a series of processing steps that are explained below.

The proposed IDS is largely based on behaviors features extracted from the trace file generated by ns-2. These features indicate either normal or malicious vehicle behavior. The extracted features require pre-processing phase to prepare them for the training phase of LDA and QDA. This preprocessing includes encoding, normalization and uniform distribution. After preprocessing is complete, the extracted dataset is ready for the training and testing phases of LDA and QDA.

4.1. Establish abnormal behavior

Here, a malicious agent behavior is added to ns-2 by using the VANETs – Ad hoc On-Demand Distance Vector Routing (AODV) protocol protocol. This protocol is used to evaluate the performance of the proposed IDS. The generated behavior of a mobility node is called a DoS agent when it makes network resources unavailable to the proper users in the VANETs.

In order to generate DoS behavior in the VANETs, we must modify some internal parameters for the two files in the routing protocol. In other words, two files in the AODV-VANET must be modified to establish the malicious behavior. These files are VANETs – AODV.cc and VANETs – AODV.h. Additionally, the TCL scenario for VANET requires a few lines of extra code for simulating this behavior under specific conditions. The malicious agent is an abnormal entity that causes dropped router packets. Furthermore, the malicious scenario must update some functions in the TCL program in reder to run the DoS functions that were established in the VANET – AODV files.

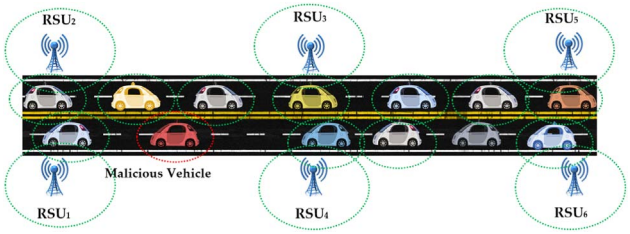

Fig. 3. Traffic and mobility Scenario.

4.2. Create mobility and traffic scenarios

In this research, ns-2 is employed to evaluate the overall performance of the proposed system and calculate the number of false alarms. ns-2 uses software tools to generate a realistic environment of malicious and normal behaviors for self-driving vehicles by providing two types of inputs traffic and mobility scenarios. The tools are the Simulation of Urban Mobility Model (SUMO) and MObilty VEhicles (MOVE) [39,40]. These tools allow ns-2 to simulate the external communications of vehicles in different scenarios.

SUMO is an efficient mobility program that has been used to generate real environments in VANETs [41]. Additionally, SUMO provides efficient computation, even in congedted city scenarios with large numbers of vehicles [41]. MOVE is an extension of SUMO [41]. It takes the output files generated in SUMO and converts them into ns-2 files. Bushra et al. presented a comprehensive survey of wireless communications in urban areas. The authors classify all urban application scenarios employed in design mobility systems in urban areas [42]. The Manhattan urban mobility model is used to design mobility and traffic scenarios for self-driving vehicles, and has been widely adopted in scientific research [43]. Fig. 3 illustrates a traffic and mobility scenario for driverless vehicles.

It shows the communications between vehicles and RSUs in a radio coverage area. The Manhattan mobility model is used in design for various reasons, such as flexibility and its common use in VANETs.

4.3. Features from the trace file

A trace file describes all events and actions of vehicle communication in a VANET. The proposed security system is based on features that have been extracted from a trace file generated by ns-2 [44]. Typically, a trace file is divided into three subfiles: basic trace, internet protocol trace and VANETs - AODV trace [41]. However, the performance and efficiency of the detection system depend on the type and number of extracted features. In order to evaluate the efficiency of the detection system, we used all 21 features from the trace file that reflect behaviors of a mobility node on the street [1].

The proposed IDS is based on LDA and QDA which have the ability to learn normal and malicious behaviors through a training phase. Cost reduction and real-time detection enhancement are the major motivations for utilizing using artificial intelligence to build the intelligent IDS [45].

4.4. LDA and QDA

Discriminant methods, whether linear or quadratic, are efficient and mathematically robust and they often create classification systems whose precision is comparable to more complex methods [46]. The core idea of LDA is based on a Bayes' optimal classifier and a linear separation hyper-plane is the basic class separator [47]. Eq. 1 is the linear discriminant function [47]:

$$d_k(\chi) = 2\mu_k^T \sum_k^{1-} \chi - \mu_k^{-1}\mu_k - 2\log\pi(k) \tag{1}$$

where k representes normal and abnormal classes, π_k is the prior probability, χ is the set of measurements, $\sum_k$ is the covariance matrix, and μ_k is the mean vector. QDA is a generalized version of LDA that can only discriminate between two classes of points [48]. The discriminant function of LDA is used for QDA after beingmultiplied by −2, as shown in Eq. 2 [49]:

$$d_k(\chi) = (\chi - \mu_k)^T \sum_k^{-1} (\chi - \mu_k) + \log|\sum_k| - 2\log\pi_k \tag{2}$$

The discriminant rule for QDA is shown in Eq. 3 [50]:

$$d_k(\chi) = \min_{1\le k\le k} d_k(\chi) \Leftrightarrow \max_{1\le k\le k} p^{(\chi/k)} \tag{3}$$

where $p^{(\chi/k)}$ is the posterior distribution. The training and testing phases are applied are used in the experimental section.

4.5. Fuzzification of the data

The extracted features have a direct impact on the performance of the proposed security system. In other words, the number and type of features have a strong influence on the detection rate and the number of false alarms. The dataset for the security system suffers from common classification problems, such as normal and malicious agents being non-obvious in the extracted features and an unclear border between normal and abnormal behaviors. In this case, the optimal solution is to use a fuzzification model on the dataset extracted from ns-2. We design a mathematical model is to redistribute features and cope with the ambiguity.

However, the mathematical model is proposed to address the classification problem [51]. In a previous study, the security system was designed without fuzzification model and had a false alarm rate of 12.24. After incorporating fuzzifcation, we obtain a false alarm rate of only 0.17 [52]. Each feature value is distributed across the five values in Eq. 4 with a range of [0.1] corresponding to: low, medium low, medium, medium high and high.

$$f(x, a, b, c) = \max(\min((x-a)/(b-a), (c-x)/(c-b)), 0) \tag{4}$$

Where x is the feature value and a,b and$c$ represent the values of the fuzzy domain. Fuzzification increases the detection rate of the proposed IDS while reducing the number of false alarms.

4.6. Network simulator parameters and environment

In this paper, the communication system for self-driving vehicles is built based on ns-2. ns-2 was designed to simulate wired and wireless networks [39]. However, the designers faced problems in simulating the external communications of self-driving vehicles with ns-2. A major reason for this is that the basic ns-2 simulator was not designed to support the simulation of VANETs. It was problematic for the designers to simulate the VANETs of self-driving vehicles with ns-2 due to unavailability issues. We use extra tools in conjunction with ns-2 for simulating the VANETs of self-driving and semi-self-driving vehicles. The tools used are SUMO and MOVE [53]. ns-2 combined with these traffic and mobility systems is used to create and intelligent IDS for external communications systems in the real world. In this proposal, the communication environment is composed of 30 cars and six RSUs [39].

4.7. The proposed IDS

The proposed security system uses LDA and QDA to protect the external communications systems of self-driving and semi self-driving vehicles. It has the ability to distinguish between normal and malicious communications between vehicles and RSUs. The proposed IDS operates in the following six stages:

- Stage I (Generate the traffic and mobility model): At this stage, SUMO and MOVE are employed to generate suitable scenarios for ns-2. The SUMO and MOVE output files are considered as input files for the next step.
- Stage II (Network simulator): The behavior for vehicles, whether normal or abnormal is generated for simulation. Two output files are obtained at this stage, a trace file and a Network Animator (NAM) file. Features are extracted from the trace file generated by ns-2.
- Stage III (Data collection and pre-processing): At this stage, the trace file is used to extract communication features for vehicles. Additionally, the extracted features are pre-processed by transforming them into numeric values, and the values are normalized between 0 and 1 using Eq. 5:

$$X = \frac{X - min}{max - min} \tag{5}$$

Normalizing data often increases the efficiency of LDA and QDA while also increasing detection rate.

- Stage IV (Fuzzification): A fuzzy set is employed to convert the extracted features into their fuzzified counterparts in order to fix classification problem and dataset overlap.
- Stage V (Training phase): LDA and QDA are trained on the extracted dataset. The raw dataset is divided into six subsets, each containing ten thousand records. For each iteration of the training cycle, the proposed system uses a different subset.
- Stage VI (Testing phase): At this stage, the proposed IDS is tested on different subsets to calculate the detection rate and number of false alarms. The testing phase has the ability to record performance metrics for the system.

5. Experimental results

The detection system can identify normal or abnormal/malicious behavior by using the proposed security system. We require real data that reflects normal and abnormal behavior between vehicles and their RSUs, to evaluate performance of the proposed IDS. In order to obtain real data, we need to generate two kinds of scenarios and simulate them under specific conditions. Raw data is generated from the trace file generated by ns-2. These features describe the normal and abnormal behaviors of self-driving and semi self-driving vehicles. The performance of ns-2 is heavily dependent on these features. Table 1 lists the features used in our security system.

Table 1
Simulator environment and parameters.

Parameter	Value
Simulator	ns–2.35
Simulation time	250 s
Number of nodes	30 Vehicles
Number of RSUs	6RS s
Type of Traffic	Constant Bit Rate (CBR)
Topology	600×400 (m)
Transport Protocol	UDP
Packet Size	512
Routing Protocol	VANETs- 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	50 m/s
Interface queue Type	Priority Queue
Network Interface type	Physical Wireless
Mobility Models	Manhattan Mobility Model

5.1. Performance metrics

In order to measure the efficiency and effectiveness of the proposed IDS, we need to calculate performance metrics. The metrics we use are divided into three classes [54]:

- Ranking metric: For this metric, we calculate four types of measures: True Positive*TP*, False Positive*FPk*, True Negative*TN* and False Negative*FN*. Additionally, Precision Rate*PR* and Detection Rate*DR* are calculated for this metric. The accuracy of the system can be calculated as follows [27]:

$$Accuracy = \frac{\text{Number of correctly classified patterns}}{\text{Total number of patterns}} \tag{6}$$

The aforementioned the measures are calculated as follows [55]: Let *TP*=normal connection record classified as normal. *TN*=attack connection record classified as attack. *FP*=normal connection record classified as attack and *FN*=attack connection record classified as normal. The metrics are calculated in the following equations.

$$TP_{Rate\,(sensitivty)} = \frac{TP}{TP + FN} \tag{7}$$

$$TN_{Rate\,(specificity)} = \frac{TN}{TN + FP} \tag{8}$$

$$FN_{Rate} = (1 - sensitivty) = \frac{FN}{FN + TP} \tag{9}$$

$$FP_{Rate} = (1 - specificity) = \frac{FP}{FP + TN} \tag{10}$$

$$DR = \frac{\text{Correctly detected attacks}}{\text{Total number of attacks}} \tag{11}$$

$$DR = \frac{TP + TN}{TP + TN + FP + FN} PR = \frac{TP}{TP + FP} \tag{12}$$

- Threshold metric: Classification Rate*CR* and F-Measure*FM* are calculated in this metric. The*FM* value falls in the range 0 to 1. It is used to as a threshold and is the average of *PR* and Recall. Additionally, Recall is the missing portion of *PR* meaning it is equivalent to *DR*.

$$CR = \frac{\text{Correctly classified instances}}{\text{Total number of instances}} \tag{13}$$

$$CR = \frac{TP}{TP + FN} FM = \frac{2}{\frac{1}{PR} + \frac{1}{Recall}} \tag{14}$$

- Probability metric: This is Root Mean Squared Error *RMSE*. The best way to describe classification results is through creating a confusion matrix by evaluating the performance of the proposed intelligent IDS [27].
- Packet Delivery Rate (PDR): The PDR value is a ratio of received packets at the destination vehicle over sent packets from the source vehicle.

$$PDR = \frac{\sum Number\ \ of\ \ packets\ \ received}{\sum Number\ \ of\ \ packets\ \ Sent} \tag{15}$$

- Throughput: The total number of packets exchanged in the VANET. This is used to measure the effectiveness of the routing protocol.

$$Throughput = \frac{\text{Number of received* packets size}}{\text{Simulation Time}} \quad (16)$$

- End-to-end Delay. This is the calculated average packet delay based on time. In other words, this metric is the average time required for packets to get from the source node to the destination node.

$$End - to - end\ Delay = \frac{\sum \text{End Time} - \text{Start Time}}{\sum \text{Number of connections}} \quad (17)$$

5.2. Training and testing LDA-IDS and QDA-IDS to detect malicious behavior

The extracted features are used in the training and testing phase of the proposed IDS. We used 100-fold cross-validation to decrease biases related to the random splitting of the data set between the training and testing phases. The security system must be able to detect both new and existing attacks. The obtained classification rate for LDA and QDA, as well as the time and error rates are shown in Table 2:

In Table 3, we display four types of measures:*TP, FP, TN and FN* for the proposed security system.

Additionally, we display some performance metrics for each of the proposed IDS. LDA-IDS and QDA-IDS, for evaluation their performance individually. The Classification Rate *CR*, Detection Rate *DR*, Precision Rate *PR*, F-Measure *FM*,*P-value* and mean error are provided in Table 4.

The*P-value* is calculated to measure the difference between the LDA and QDA methods. This value indicates that there is a significant difference between the errors of the two methods.

The Packet Delivery Rate (PDR) and End-to-end delay are displayed in Table 5.

6. Discussion

The goal of our research was to design an intelligent IDS that provides a secure environment for autonomous and semi-autonomous vehicles. The IDS has the ability to detect abnormal behavior and take actions to prevent attacks on the network, vehicles or passengers. In the absence of an IDS, the security of the system cannot be guaranteed. The proposed security system was implemented in six phases: generation of the mobility and traffic model, ns-2, generation of the trace file, data collection and pre-processing, training and testing for LDA and QDA, and a comparison of the performances of the two types of proposed intelligent security systems.

In order to evaluate the performance of the proposed security systems, we compared our proposed IDS with previous systems that achieved error rates of 2.05 [1], 10 [28] and 19 [25], while our new security system achieved an error rate of 0.58. The average false alarm rate of the system in [1] is 12.24, while we have achieved a rate of 9.91 with the proposed system.

Fig. 4 shows a performance comparison between the LDA and QDA methods. The error rate for LDA-IDS was 0.385 and the *TP* and *TN* measures fluctuated between 86.44 and 92.73 with excellent efficiency. The *FN* alarm rate was approximately 7.27, which is a good indicator of the feasibility of the design.

The error rate for QDA-IDS was 0.397. The *TP* and *TN* measures fluctuated between 84.55 and 87.44 with excellent efficiency. However, the *FN* alarm rate was relatively high at approximately 12.56. We could enhance the detection rate of the proposed security system by switching between LDA and QDA dynamically based on different conditions.

Based on the experimental results, we can confidently say that LDA-IDS is more efficient and effective at detecting abnormal vehicle

Table 2
Classification rate.

IDS			
Class	Accuracy – Test Phase	Time/s	Error Rate-Train Phase
LDA-Normal	99.94%	8.79s	0.385
LDA-Abnormal	81.09%		
Class	Accuracy– Test Phase	Time/s	Error Rate-Train Phase
QDA-Normal	91.07%	14.27s	0.397
QDA-Abnormal	78.87%		

Table 3
Alarm rate.

Alarm Type	LDA	QDA
True positive	86.44%	84.55%
True negative	92.73%	87.44%
False positive	7.27%	12.56%
False negative	13.56%	15.45%

Table 4
Performance metrics.

Performance Metrics						
Class	CR	DR	PR	FM	P-value	Mean Error
LDA	88.87%	86.44%	94.99%	0.9	8.7E-08	0.385%
QDA	84.55%	85.67%	91.07%	0.88		0.397%

Table 5
Comparison performance.

Performance Metrics	VANETs without IDS	VANETs with IDS
Packet Delivery Ratio	43.59	96.67
Average End-to-End Delay	1.5442ms	1.4835ms
Average Throughput	34.21kbps	81.47kbps

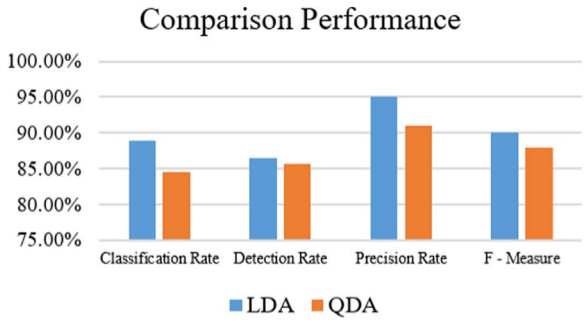

Fig. 4. performance compare between LDA and QDA.

behavior than QDA-IDS, and has a lower false negative alarm rate.

7. Conclusion and future work

We have proposed a reliable IDS to detect malicious behavior in the communications systems for self-driving and semi self-driving vehicles. The proposed IDS can detect abnormal behavior and take actions to prevent attacks on the network, vehicles and passengers. It uses a prediction scheme to secure the external communications systems for autonomous vehicles. The proposed LDA-IDS has the ability to identify the actions of a malicious agent. It is considered a novel protection system for external communications because it is the first work utilizing abnormal behavior prediction for securing VANETs.

The proposed IDS can identify and prevent DoS and black hole attacks by monitoring routing tables and analyzing trace files generated by ns-2. The generated trace files defines the behaviors in VANETs based on the controller data and information that is sent, received, forwarded and dropped in packets. The QDA method has a higher error rate than LDA. Thus, we conclude that the simpler LDA algorithm will generally achieve better performance than the more complicated QDA algorithm. LDA and QDA can both make the proposed IDS more efficient at securing VANETs.

A possible future extension of the security system is to enhance RSUs with intelligent an IDS and to enhance vehicles with AI techniques such as the k-Nearest Neighbors algorithm.

Acknowledgements

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

References

[1] K.M.A. Alheeti, A. Gruebler, K. D. McDonald-Maier, An intrusion detection system against malicious attacks on the communication network of driverless cars, in: 2015 Proceedings of the 12th Annual IEEE Consumer Communications and Networking Conference (CCNC), IEEE, 2015, pp. 916–921.
[2] M.O. Cherif, Optimization of v2v and v2i communications in an operated vehicular network, France (2010) (Ph.D. thesis).
[3] Y. Saleem, M.H. Rehmani, S. Zeadally, Integration of cognitive radio technology with unmanned aerial vehicles: issues, opportunities, and future research challenges, J. Netw. Comput. Appl. 50 (2015) 15–31.
[4] M.O. Cherif, S.-M. Senouci, B. Ducourthial, Efficient data dissemination in cooperative vehicular networks, Wirel. Commun. Mob. Comput. 13 (12) (2013) 1150–1160.
[5] T. Umer, M. Amjad, N. Shah, Z. Ding, Modeling vehicles mobility for connectivity analysis in vanet, in: Intelligent Transportation Systems, Springer, 2016, pp. 221–239.
[6] H. Sedjelmaci, T. Bouali, S.M. Senouci, Detection and prevention from misbehaving intruders in vehicular networks, in: 2014 IEEE Global Communications Conference, IEEE, 2014, pp. 39–44.
[7] H. Sedjelmaci, S.M. Senouci, A new intrusion detection framework for vehicular networks, in: 2014 IEEE International Conference on Communications (ICC), IEEE, 2014, pp. 538–543.
[8] H. Sedjelmaci, S.M. Senouci, M. Feham, An efficient intrusion detection framework in cluster-based wireless sensor networks, Secur. Commun. Netw. 6 (10) (2013) 1211–1224.
[9] S. Yousefi, M.S. Mousavi, M. Fathy, Vehicular ad hoc networks (vanets): challenges and perspectives, in: 2006 Proceedings of the 6th International Conference on ITS Telecommunications, IEEE, 2006, pp. 761–766.
[10] Y.-C. Hu, D.B. Johnson, A. Perrig, Sead: secure efficient distance vector routing for mobile wireless ad hoc networks, Ad hoc Netw. 1 (1) (2003) 175–192.
[11] Y.-C. Hu, A. Perrig, D.B. Johnson, Ariadne: a secure on-demand routing protocol for ad hoc networks, Wirel. Netw. 11 (1–2) (2005) 21–38.
[12] K. Sanzgiri, B. Dahill, B.N. Levine, C. Shields, E.M. Belding-Royer, A secure routing protocol for ad hoc networks, in: Network Protocols, 2002. Proceedings. in: Proceedings of the 10th IEEE International Conference on, IEEE, 2002, pp. 78–87.
[13] S. Yi, P. Naldurg, R. Kravets, Security-aware ad hoc routing for wireless networks, in: Proceedings of the 2nd ACM international symposium on Mobile ad hoc networking & computing, ACM, 2001, pp. 299–302.
[14] A. A. Pirzada, C. McDonald, Secure routing protocols for mobile ad hoc wireless networks, Advanced Wired and Wireless Networks.
[15] P. Papadimitratos, Z. J. Haas, Secure routing for mobile ad hoc networks, in: the SCS Commnication Networks and Distributed Systems Modeling and Simulation Conference (CNDS), San Antonio, TX, January 27-31, 2002, 2002, pp. 193–204.
[16] M.G. Zapata, Secure ad hoc on-demand distance vector routing, ACM SIGMOBILE Mob. Comput. Commun. Rev. 6 (3) (2002) 106–107.
[17] P. Papadimitratos, Z.J. Haas, Secure link state routing for mobile ad hoc networks, in: Proceedings of the IEEE Symposium on Applications and the Internet Workshops, 2003, pp. 379–383.
[18] B. Lu, U. W. Pooch, Cooperative security-enforcement routingin mobile ad hoc networks, in: IEEE 4th International Workshop on Mobile andWireless Communications Network, 2002, pp. 157–161.
[19] S.S. Doumit, D.P. Agrawal, Self-organized criticality and stochastic learning based intrusion detection system for wireless sensor networks, in: IEEE Military Communications Conference, MILCOM'03, 2003, vol. 1, 2003, pp. 609–614.
[20] S. Shin, T. Kwon, G.-Y. Jo, Y. Park, H. Rhy, An experimental study of hierarchical intrusion detection for wireless industrial sensor networks, IEEE Trans. Ind. Inform. 6 (4) (2010) 744–757.
[21] O.B. Akan, O.B. Karli, O. Ergul, Cognitive radio sensor networks, IEEE Netw. 23 (4) (2009) 34–40.
[22] K.M.A. Alheeti, A. Gruebler, K.D. McDonald-Maier, A. Fernando, Prediction of dos attacks in external communication for self-driving vehicles using a fuzzy petri net model, in: 2016 IEEE International Conference on Consumer Electronics (ICCE), 2016, pp. 502–503.
[23] A. Mitrokotsa, R. Mavropodi, C. Douligeris, Intrusion detection of packet dropping attacks in mobile ad hoc networks, in: Proceedings of the International Conference on Intelligent Systems And Computing: Theory And Applications, 2006, pp. 111–118.
[24] A. Chaudhary, V. Tiwari, A. Kumar, Design an anomaly based fuzzy intrusion detection system for packet dropping attack in mobile ad hoc networks, in: IEEE International Advance Computing Conference (IACC), 2014, pp. 256–261.
[25] C. A. Kerrache, A. Lakas, N. Lagraa, Detection of intelligent malicious and selfish nodes in vanet using threshold adaptive control, in: Electronic Devices, Systems and Applications (ICEDSA), 2016 Proceedings of the 5th International Conference on, IEEE, 2016, pp. 1–4.
[26] K. Zaidi, M. Milojevic, V. Rakocevic, A. Nallanathan, M. Rajarajan, Host based intrusion detection for vanets: A statistical approach to rogue node detection.
[27] K.M.A. Alheeti, A. Gruebler, K.D. McDonald-Maier, On the detection of grey hole and rushing attacks in self-driving vehicular networks, in: 7th IEEE Computer Science and Electronic Engineering Conference (CEEC), 2015, pp. 231–236.
[28] R. Coussement, B. Amar Bensaber, I. Biskri, Decision support protocol for intrusion detection in vanets, in: Proceedings of the third ACM international symposium on Design and analysis of intelligent vehicular networks and applications, ACM, 2013, pp. 31–38.
[29] R. Baiad, H. Otrok, S. Muhaidat, J. Bentahar, Cooperative cross layer detection for blackhole attack in vanet-olsr, in: 2014 International Wireless Communications and Mobile Computing Conference (IWCMC), IEEE, 2014, pp. 863–868.
[30] T.K. Marve, N.U. Sambhe, A review on cross layer intrusion detection system in wireless ad hoc network, in: 2015 IEEE International Conference on Electrical, Computer and Communication Technologies (ICECCT), 2015, pp. 1–4.
[31] R. Shrestha, K.-H. Han, D.-Y. Choi, S.-J. Han, A novel cross layer intrusion detection system in manet, in: Proceedings of the 24th IEEE International Conference on Advanced Information Networking and Applications, 2010, pp. 647–654.
[32] I.F. Akyildiz, W.-Y. Lee, M.C. Vuran, S. Mohanty, Next generation/dynamic spectrum access/cognitive radio wireless networks: a survey, Comput. Netw. 50 (13) (2006) 2127–2159.
[33] R.H.S. driving Car Sensors, Researcher Hacks Self-driving Car Sensors, ⟨http://spectrum.ieee.org/cars-that-think/transportation/self-driving/researcher-hacks-selfdriving-car-sensors⟩, March 2015.
[34] G. Samara, W.A. Al-Salihy, R. Sures, Security issues and challenges of vehicular ad hoc networks (vanet), in: Proceedings of the 4th International Conference on New Trends in Information Science and Service Science (NISS), 2010, pp. 393–398.
[35] M.N. Mejri, J. Ben-Othman, M. Hamdi, Survey on vanet security challenges and possible cryptographic solutions, Veh. Commun. 1 (2) (2014) 53–66.
[36] D. Tian, Y. Wang, G. Lu, G. Yu, A vehicular ad hoc networks intrusion detection system based on busnet, in: Proceedings of the 2nd International Conference on Future Computer and Communication (ICFCC), vol. 1, 2010, pp. V1-225.
[37] R. Bronte, H. Shahriar, H.M. Haddad, A signature-based intrusion detection system for web applications based on genetic algorithm, in: Proceedings of the 9th International Conference on Security of Information and Networks, ACM, 2016, pp. 32–39.
[38] Y. Ping, J. Xinghao, W. Yue, L. Ning, Distributed intrusion detection for mobile ad hoc networks, J. Syst. Eng. Electron. 19 (4) (2008) 851–859.
[39] T.N.S. ns 2, The network Simulator - ns-2, www.isi.edu/nsnam/ns (June 2014).
[40] J. Harri, F. Filali, C. Bonnet, Mobility models for vehicular ad hoc networks: a survey and taxonomy, IEEE Commun. Surv. Tutor. 11 (4) (2009) 19–41.
[41] C..C.C. Consortium, Car 2 car communication consortium, www.car-2-car.org/index.php?Id=5 (June 2011).
[42] B. Rashid, M.H. Rehmani, Applications of wireless sensor networks for urban areas: a survey, J. Netw. Comput. Appl. 60 (2016) 192–219.
[43] J. Breu, A. Brakemeier, M. Menth, Analysis of cooperative awareness message rates in vanets, in: Proceedings of the 13th International Conference on ITS Telecommunications (ITST), 2013, pp. 8–13.
[44] S. Chettibi, Y. Labeni, A. Boulkour, Trace file analyzer for ad hoc routing protocols simulation with ns2, in: 2015 Proceedings of the First International Conference on New Technologies of Information and Communication (NTIC), 2015, pp. 1–6.
[45] Using artificial intelligence to create a low cost self-driving car, ⟨http://budisteanu.net/Download/ISEF20220Autonomous20car20Doc20particle.pdf⟩ (Jule 2015).

[46] T. Rasymas, V. Rudžionis, Evaluation of methods to combine different speech recognizers, in: Federated Conference on Computer Science and Information Systems (FedCSIS), 2015, pp. 1043–1047.
[47] D.S., Statistical data mining and machine learning, Tech. rep., Department of Statistics Oxford (2016).
[48] S. Bhattacharyya, A. Khasnobish, S. Chatterjee, A. Konar, D. Tibarewala, Performance analysis of lda, qda and knn algorithms in left-right limb movement classification from eeg data, in: 2010 International Conference on Systems in Medicine and Biology (ICSMB), 2010, pp. 126–131.
[49] S.H. Baek, D.-H. Park, H. Bozdogan, Hybrid kernel density estimation for discriminant analysis with information complexity and genetic algorithm, Knowl.-Based Syst. 99 (2016) 79–91.
[50] J.H. Friedman, Regularized discriminant analysis, J. Am. Stat. Assoc. 84 (405) (1989) 165–175.
[51] G. Chen, T.T. Pham, Introduction to fuzzy sets, fuzzy logic, and fuzzy control systems, CRC Press, 2000.
[52] K.M.A. 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 Proceedings of the Sixth International Conference on Emerging Security Technologies (EST), 2015, pp. 86–91.
[53] K.-c. Lan, C.-M. Chou, Realistic mobility models for vehicular ad hoc network (vanet) simulations, in: . in: Proceedings of the 8th International Conference on ITS Telecommunications, ITST, 2008, pp. 362–366.
[54] R. Caruana, A. Niculescu-Mizil, Data mining in metric space: an empirical analysis of supervised learning performance criteria, in: Proceedings of the Tenth ACM SIGKDD International Conference on Knowledge discovery and Data Mining, ACM, 2004, pp. 69–78.
[55] G. Creech, J. Hu, A semantic approach to host-based intrusion detection systems using contiguousand discontiguous system call patterns, IEEE Trans. Comput. 63 (4) (2014) 807–819.