Intrusion detection method for GPS based on deep learning for autonomous vehicle

Article *in* International Journal of Electronic Security and Digital Forensics · January 2022

DOI: 10.1504/IJESDF.2022.120039

2 authors:

Manale Boughanja
Université Ibn Tofail
11 PUBLICATIONS **16** CITATIONS
SEE PROFILE

Tomader Mazri
Université Ibn Tofail
213 PUBLICATIONS **548** CITATIONS
SEE PROFILE

Intrusion detection method for GPS based on deep learning for autonomous vehicle

Boughanja Manale* and Tomader Mazri

Advanced Systems Engineering, Electrical Engineering,
Networks and Telecommunications System,
Ibn Tofail Science University,
Kenitra, Morocco
Email: Boughnja.manale@gmail.com
Email: tomader20@gmail.com
*Corresponding author

Abstract: Protecting an environment in perpetual motion will be difficult to be secured against attacks, and also challenging to detect threats. The intrusion will result in serious security risks. With the refinement of the attacker's skills, new intrusions pose serious problems. To enhance security measurements must be implemented. The intrusion detection system (IDS) is a relevant innovation, which checks the system's activity to detect any suspicious behaviour that may indicate that the system has been attacked or misused. We outlined the key design of autonomous AV keys and their challenges. Most technology has been used as machine learning techniques but it was only used for the processing of applications based on imagery. In this study, we have proposed a model to secure the GPS sensor. The model implements the deep learning technique to predict vehicle behaviour as a function of location. Our model helps to improve the accuracy and scalability of the vehicle.

Keywords: security; detection; deep learning; algorithms; intrusion detection system.

Reference to this paper should be made as follows: Manale, B. and Mazri, T. (2022) 'Intrusion detection method for GPS based on deep learning for autonomous vehicle', *Int. J. Electronic Security and Digital Forensics*, Vol. 14, No. 1, pp.37–52.

Biographical notes: Boughanja Manale received DUT in Computer Network Administration in Higher School of Technology (EST) Salé in 2014. She received her LP Diploma in network and telecommunication, Science University Rabat (Morocco) in 2015. She received her Master's degree in Information Systems Security from the National School of Applied Sciences in Kenitra, Morocco. Her current work path towards her PhD is at the Faculty of Sciences in Kenitra, Morocco. Her research interests include security and machine learning techniques.

Tomader Mazri is a Professor at ENSA of Kenitra. She is a holder of a Habilitation to Direct Research in Networks and Telecom Systems from Ibn Tofail University and a National Doctorate in Microelectronics and Telecom Systems from Sidi University Mohammed Ben Abdellah and the National Institute of Posts and Telecommunications of Rabat.

1 Introduction

The latest technological innovations are rapidly and radically transforming our daily life. Today, the development has been known on different levels and started from the evolution in the field of mobile networks in the sense, the evolution from 1G to 5G and moving to the evolution of transportation. The vehicular ad hoc network (VANET) is a subset of mobile ad hoc network (MANET), alludes to many smart vehicles utilised on the road. These vehicles give communication services to each other or with the roadside infrastructure (RSU) founded on a wireless local area network (LAN) technologies (Engoulou et al., 2014). Before, vehicles were being composed of mechanical parts and now it is replaced by electronic parts and equipped with wireless connectivity, this new technology is known as the autonomous vehicle (AV). What do we mean by AV? The autonomous vehicle, known also as a self-driving or driverless car is a vehicle that is fit for detecting and exploring its environment without human inputs (Maurer et al., 2016), the vehicles are outfitted with an enormous number of sensors and have network connectivity than the non-autonomous ones. With the advent of any new technology, several challenges and security issues are increasing and the AV is considered as a niche of attackers because the attacks have undoubtedly arisen.

The AV is susceptible to attack, due to several things, such as the increase in communication channels as well as external communication which poses a danger. Moreover, internal communication targets the vehicle's components (Thing and Wu, 2016). Besides, because the technology is in its infancy, the hardware and software have not yet been rigorously tested. The AV contains several sensors, which are responsible for collecting the data from the environment. One of the most relevant sensors is the global positioning system (GPS), it is a device that provides the vehicle's location. The GPS sensor faces many attacks such as spoofing and jamming attacks, and to deal with these attacks, several techniques have been implemented among them we can find deep learning (DL) which is a new concept that was applied to improve safety of the system. In our case, we used the deep neural network (DNN), to enhance security and classify the behaviour of the GPS sensor to detect if the vehicle is considered as an honest node or malicious. For that, our paper is organised as follows: in section two, we will present an overview of the autonomous vehicle, including the AV architecture and taxonomy of attacks. In section three, we will present an in-depth study on intrusion detection system and we will focus on a case study (GPS sensor), then we will present in detail our proposed methodology. Finally, we conclude in section four.

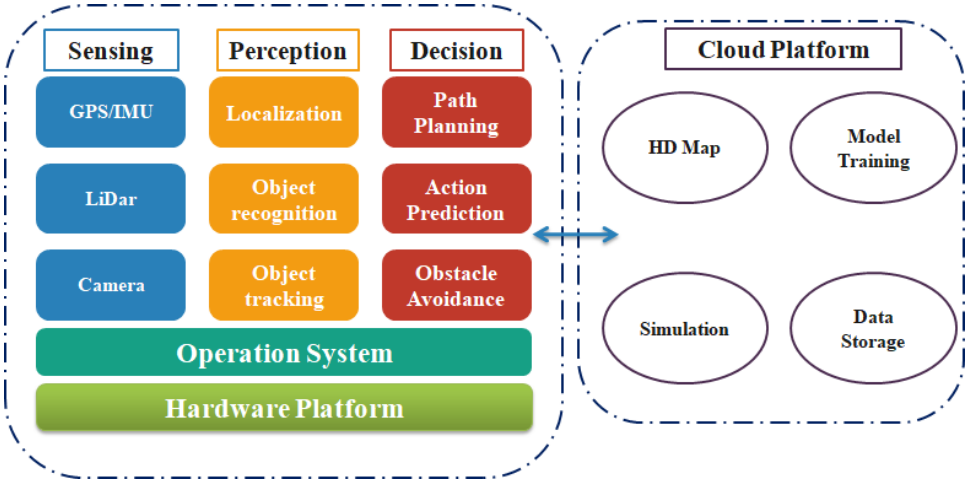
2 Overview of autonomous vehicle

The field of autonomous vehicles is rapidly developing, compared to traditional vehicles (Liu et al., 2018). AV can improve road safety, alleviate traffic congestion, and change driving behaviours.

2.1 Autonomous vehicle architecture

The architecture of the AV is composed of three main components: autonomous driving algorithm, the client system, and cloud platform (Liu et al., 2018). Figure 1 shows the AV system.

Figure 1 Autonomous vehicle system architecture overview (see online version for colours)



The algorithm subsystem extracts meaningful information from sensors to understand their surroundings and to make decisions about their future actions. The client system integrates these algorithms collectively to fulfil real-time and reliability necessities. Concerning the cloud platform, its role is to provide the capability of processing and storage for the autonomous vehicle. Next, we will explain the main components of the AV.

The autonomous driving algorithm: is constituted with the following algorithm:

- Sensing: the AV consists of several sensors, which are aiming to collect data. Indeed, each sensor gives advantages and downsides, the data have to be mixed and generated from a couple of sensors to expand reliability and protection (Kato et al., 2015). They can contain the following:
  - a *GPS/IMU:* or global positioning system/ initial measurement unit that is a system that helps the AV to determine its location by reporting the inertial updates and global positioning. The goal of combining the two systems is to achieve real-time updates for vehicles (Sullivan and Frost, 2018).
  - b *LiDar:* light detection and ranging the system is used for mapping and localisation it helps also to avoid the obstacles for vehicles (Sullivan and Frost, 2018). Besides, it could be used to determine the location of a moving car, to detect the obstacles that can get through it.
  - c *Camera:* are generally used for item recognition and item tracking duties which include lane detection, light detection, and pedestrian detection. The goal of the camera is to catch the surrounding of the vehicle to strengthen its protection (Meyrowitz et al., 1996).
  - d *Radar and sonar:* these two devices are used for obstacle avoidance, both of them generate data representing the distance and the velocity from the nearest object in front of the vehicle path (Heinzelman, 2019).
  - e *TPMS:* tyre pressure monitor systems it is a small device that is placed directly on the vehicle which intends to update the vehicle's control system with specific information (Interface, 2018).

- Perception: in this step, the AV tries to understand its environment via three main tasks (Kato et al., 2015).
  a *The localisation:* considered the most critical step in autonomous driving. Especially in city areas, the localisation precision dominates the reliability of self- sufficient riding (Kato et al., 2015). For example, GPS is used to specify the location of the vehicle.
  b *Object detection and tracking:* for detecting the obstacle that faces the vehicle itself. For example, LiDar is used to avoid obstacles.
- Decision: based on the comprehension of the vehicle's surroundings, this stage can generate a secure and efficient action plan in real-time (Interface, 2018). The decision is made in three stages.
  a *Path planning:* to identify the best path to deliver navigation plans in real-time.
  b *Action prediction:* to make sure that the vehicle travels in a secure environment it critical to predicting the different nearby vehicles. Last and not least, obstacle avoidance; to avoid obstacles.

Autonomous driving vehicle system: the autonomous vehicle client system contains two components:

- The robotic operating system (ROS): this is considered a powerful distributed framework. For example; localisation is hosted in a ROS node that communicates through a topic and services.
- Hardware platform: that can be summarised into the different equipment in the system.

Autonomous driving platform: the autonomous vehicle is a mobile system; therefore, it needs a cloud platform to provide distributed computing and also storage capacity. The cloud platform consists of four components:

- The simulation: to test the entire developed algorithm before it will be implemented in a real vehicle.
- HD map: which involves several stages; raw data processing, point cloud production, point cloud alignment, as well as final map generation.
- The model training: provides data updates to improve the autonomous vehicle system.
- Data storage: to store all processing made in the cloud platform.

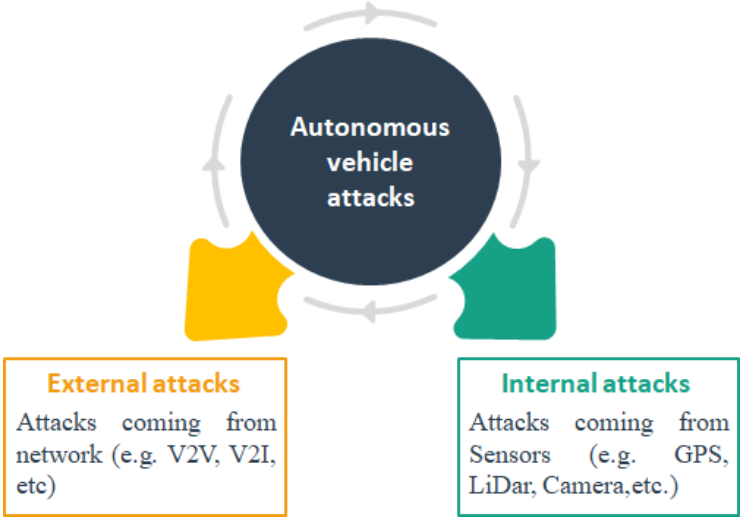
2.2 Taxonomy of attack in autonomous vehicle

With the innovation in smart cities, several attempts have been made to enhance the efficiency in the work environment and standard of living worldwide. One of the fields that have been improved is the transportation infrastructure and system. In this section, we will provide a taxonomy of attacks in AV. The autonomous vehicle can be attacked by an internal or external attack (Plathottam and Ranganathan, 2018).

- The internal attacks: are considered as the attacks that are coming from the vehicle itself (Tyagi and Dembla, 2014). The AV contains several sensors and interfaces which cause a lack of security.
- The external attacks: are the attacks that come from the network (Tyagi and Dembla, 2014). We can divide these attacks into three types (Thing and Wu, 2016): the vehicle to vehicle communication (V2V); caused by the communication between vehicles, the vehicle to infrastructure (V2I); caused by the communication between vehicle and its surroundings like the RSU and so on, the vehicle to everything communication (V2X); this type of attack is considered the most critical because it cases a huge lack of security in AV.

Figure 2 shows the taxonomy of attacks in AV.

Figure 2 Taxonomy of attacks in autonomous vehicle (see online version for colours)



3 Intrusion detection in autonomous vehicle

3.1 Localisation and navigation in autonomous vehicle

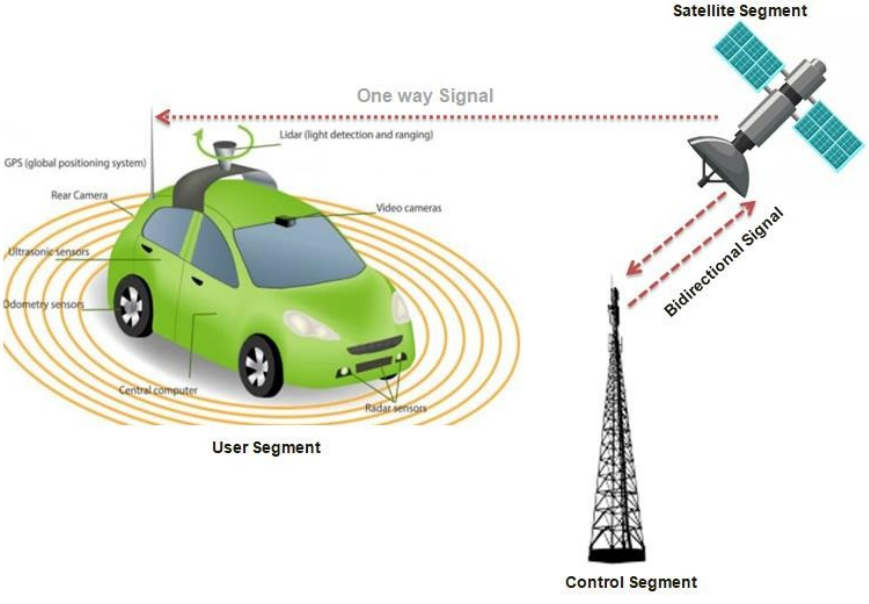
Typically, an autonomous vehicle compromises significant sensors. Since each sensor presents advantages and disadvantages, the data in the AV coming from numerous sensors must be consolidated for expanded increased efficiency, trustworthiness, and security. In the previous section, we have presented the different sensors that make up the AV. In this section, we will focus on the most critical task. For AV, the most basic assignments are the geographical position, which means, the precision and ongoing assurance of the unit's position. The position of a vehicle usually depends on the global navigation satellite system (GNSS) and it aims to provide the location. This section will provide details of the GNSS technologies and understand the advantages and

disadvantages as it applies to autonomous driving. GNSS is composed of several satellites system (GPS, GLONASS, GALILEO, and BEIDOU).

3.2 Case study: GPS sensor

All GPS receivers operate on the same fundamental concepts to calculate a 3D space and time navigation solution. The navigation solution is computed through trilateration whereby the receiver calculates its distance to four (or even more) satellites (Liu et al., 2018).

Figure 3 Core segment of global positioning system (GPS) (see online version for colours)



Every satellite produces and broadcasts a unique public stream of pseudo-random numbers (PRN) known as a coarse acquisition code (C/A), repeating every 1ms. Then, the GPS receivers produce their local copy of each satellite's C/A code and estimate the time offset required to adjust the local copy too much the received copy. The GPS constituted of three main components as shown in Figure 3:

- The space segment: This is composed of numerous satellites. Every satellite carries various atomic timers to maintain a precise time.
- The control segment: includes tracking stations, which monitor satellite navigation signals and transfer data continuously.
- The user segment: that consists of the end-user (military or civilian users) and their GPS equipment. In our case, we focus on the GPS sensor in the AV.

3.3 Attack on GPS

Some of the AV characteristics cause vulnerabilities in the communication layers (Nashashibi et al., 2018). In other terms, the external communication system has some properties that cause security issues such as mobility, velocity, etc. In this case, attackers can initiate their attack without physical access. Traditional systems cannot protect sensitive information. Earlier work has focused on a couple of attacks targeting GPS: jamming and spoofing. Indeed, the jamming attack is launched to prevent the vehicle to receive the signal. On the other hand, the spoofing attack is carried out to mislead the system. With this reasoning, we can deduce that there are two levels of attack that target the GPS sensor.

- GPS data level spoofing: which can be summarised and emits fake GPS signals to tamper with a timely solution of victim receivers without altering its position. The spoofer accomplishes this by changing several settings in the navigation data.
- GPS signal-level spoofing: a signal level-spoofing device synthesises and sends out forged GPS signals that transport the same navigation data as that transmitted simultaneously by the GPS satellites. By carefully controlling the timing delay of each code. The spoofer can manipulate the time solution of the target without affecting its position.
- Message falsification attack: This aims to upload plenty of false messages to upgrade the HD map in real-time.
- GPS replay attack: intends to destroy the encryption and authentication security of GPS signals. It is primarily carried out by permanently forwarding legitimate GPS signals, which are received from the GPS and recorded earlier by attackers. As a result of this attack, opponents can reach the objective of misleading and interfering with the target navigation system.
- Sybil attack: refers to the attack where the opponents leverage a malicious car to exploit multiple vehicle identities to deliver multiple location metrics with different identities to legal vehicles that create a location request, to influence autonomous driving decisions.
- Rogue updates: that intend to block the functionality of the device.

3.5 Related works

Vehicular communication has plenty of security necessities as it manages applications for a sheltered driving environment, for example, traffic data, climate condition, street crisis, navigation, and so forth. A large portion of the application mentioned depends on the location information. On the off chance that the location information of vehicles is compromised, at that point, the compromised application will not work correctly. Besides, bogus or deluded location information could lead to serious problems such as an accident that could potentially result in financial damages and even risk to the drivers' lives (Lim and Manivannan, 2016).

Location is considered essential and crucial information in AV, so a harmful node or malicious attacker may try to diffuse the wrong location information to profit from finding short routes or to launch malicious attacks. To deal with the location-based

attack, various researches have been developed. In Xiaonan et al. (2007), they proposed a cryptographic scheme to detect and remove malicious nodes. The proposed solution use pseudonyms that are connected to a couple of keys public and private employed by the certificate authority (CA). Kohlweiss et al. (2008) proposed a solution to detects and notify from location spoofing attacks by self-certified pseudonyms.

In Feng et al. (2017), they proposed a defending method against multiple-source Sybil attacks. The proposed method utilises the RSU to validate the certificate for each vehicle. If the proposed method finds two vehicles, use the same certificate it will be declared as a malicious node. Similarly, the location of the vehicle is tracked by collecting the GPS node and the position from active nearby nodes via the TS signature (Chen et al., 2009). In Ruj et al. (2011), they provide a data- centric misbehaviour detection algorithm that detects false alert messages from a specific location by monitoring behaviour after the alert messages are sent.

Another solution is presented based on the regular alert messages sent to the vehicle so that the position of the neighbours is observed over time and the mismatching of the vehicle's position will be marked the message as a flag (Montgomery et al., 2009). In Magiera and Katulski (2015), they proposed a method that aims to deduce and detect the spoofing attack. It is based on the presence of encryption that is transmitted on the same frequency band. Montgomery et al. (2009) proposed a technique that uses an application of spatial processing method for detecting the GPS spoofing attack. Another method that uses the information provided by an authentic RSU to detect spoofing attacks was presented in Anouar et al. (2016). In Ranganathan et al. (2016), they create an RF device to connect the GPS antenna and the GPS receiver. On the other hand, Liu et al. (2019) and Tippenhauer et al. (2011) proposed a technique that can predict the minimal signal to launch a spoofing attack on the receiver. To enhance the accuracy of the system, Jwo et al. (2013) proposed a method to improve the GPS precision. In Panice et al. (2017), they present a novel solution to detect anomaly in the vehicle based on the support vector machine (SVM). Optimising the GPS signal was implemented in Panice et al. (2017).

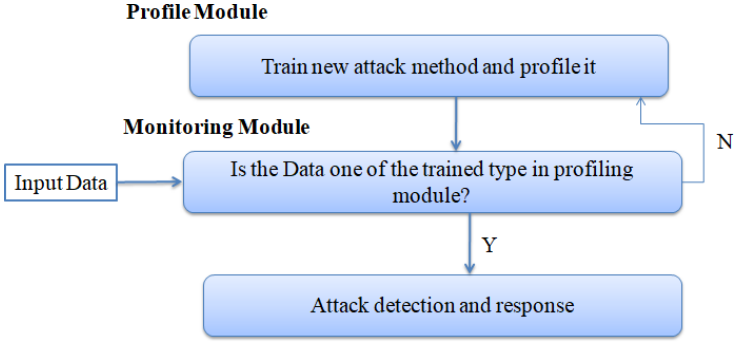
Zeng et al. (2018) improved the GPS terminal's resiliency to interference. In Behfarnia and Eslami (2018), they proposed a model based on the Bayesian network (BN) to analyse the GPS spoofing attack. Sukkarieh et al. (1999) presented a high integrity IMU/GPS navigation for an AV to enhance the integrity of the information provided by the sensor. Similarly, Milanés et al. (2008) provided a solution based on the cooperation of the GPS and inertial navigation system (INS), to enhance the vehicle guidance and detect incorrect information. In Manale and Tomader (2020), the authors present a detailed study of the intrusion detection system. From the study carried out, we were able to differentiate between three types of detection: machine learning detection, behaviour detection, and malware detection. The security of the GPS sensor in AV should be taken seriously because any loss or altering in the localisation information may have serious consequences

The researchers made several techniques to enhance the security of this component, and more work to strengthen the security of the GPS to deal with all sorts of attacks will be beneficial. For this reason, it is necessary to optimise the GPS signal and implement strong methods such as encryption methods at the level of data collection. The data should be verified to ensure the accuracy of the collected data from the HD map to prevent HD maps from being replaced or contaminated. Also, system security must include system control and monitoring through the preparation of redundant equipment to replace the compromised ones to avoid system downtime.

3.6 Intrusion detection with machine learning

The intrusion detection techniques have been created to deal with security issues and to prevent any sort of attack. The implementation of the machine learning (ML) technique improves the detection of malicious attacks. Ftaimi and Mazri (2020) presented a detailed classification for ML techniques, which help us to understand the efficiency of these techniques to improve the performance of the system. Figure 4 shows the common architecture of IDS based on ML.

Figure 4 Architecture of intrusion detection system based on the ML technique (see online version for colours)

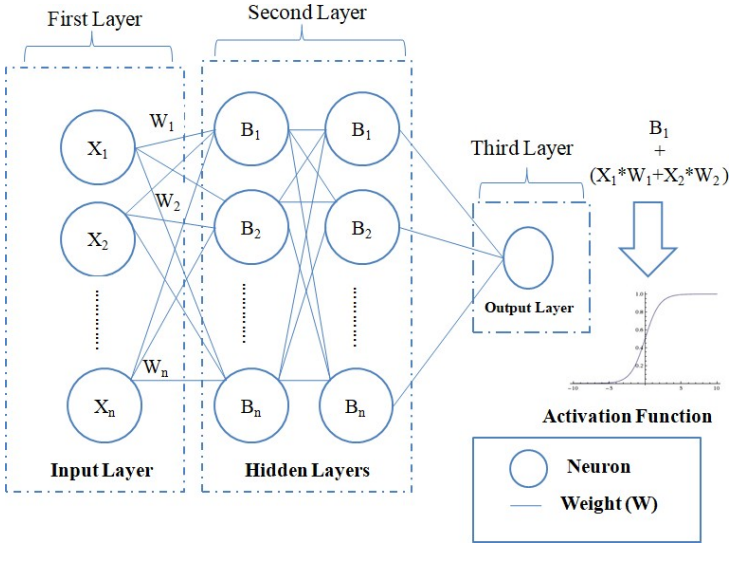


Source: Kang and Kang (2016)

The architecture contains two main modules:

- the monitoring module: this detects the type of entering data
- the profiling module: responsible for the update of the database.

Figure 5 Deep neural network structure (see online version for colours)



Deep learning (DL) is a type of ML inspired by the structure of the human brain in terms of DL this structure is called an artificial neural network (ANN). Figure 5 shows the structure of a neural network (NN).

3.7 The functioning of deep learning

The structure of DL is constituted of three main layers. Every layer is composed of neurons, which are the core entity of a neural network. In the NN the information process takes place, where each neuron is fed to a neuron in the first layer of the network which formed the first layer called also the input layer at the other end the output layer with a neuron that deduces the result, depending on the chosen methodology with the hidden layers existing between them. The information is transmitted from one layer to another over connecting channels, each of these has a value attached to it and hence is called a weighted (W) channel all neurons have a unique number associated with called bias (B).

This bias is added to the weighted sum of the inputs reaching the neuron which is applied to an activation function. This function determines if a neuron is activated or not, every activated neuron passes on information to the following layer up till the last layer.

3.8 Proposed methodology

The growth of the AV is greatly prompted by the need to develop vehicles that are faster, more reliable, and secure. However, it still has many unsolved issues concerning security and safety due to the number of sensors, and the communication channel. Understanding the behaviour and separate between normal and abnormal conduct starts to be difficult. For this reason, the interest in using a system capable of detecting and preventing any sort of attack will be beneficial. Therefore, it is important to monitor and detect anomalies from the first step to the end. In AV, data can be generated from several locations (e.g., sensor or network). This collected data is very challenging in this type of environment and the detection must be implemented at all levels of the communication. The planned system must be able to distinguish between normal and abnormal behaviours. Our study aims to propose a detection system able to secure the data coming from the sensor and more precisely the data generated by the GPS sensor. As we have already explained the GPS, provide coordinates to locate the vehicle.

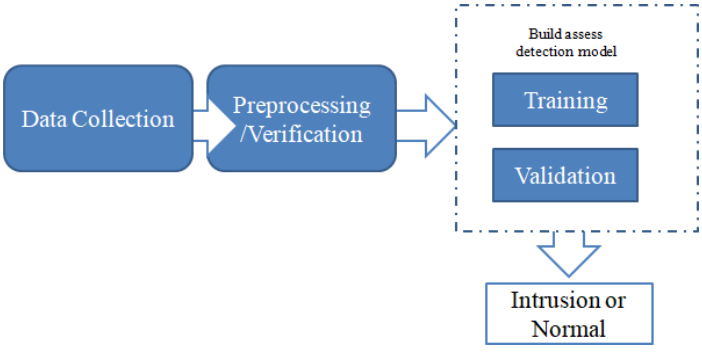
Once the vehicle is fixed with wrong coordinates, it will lose its path or even have greater consequences on human lives. The intrusion detection system is composed essentially of three components:

- Sensors: responsible for collecting data (in our case we talk about the GPS data). This latter contains the GPS coordinates and the speed of the vehicle at a specific time.
- Analyser: receives all information from the sensors and responsible for analysing this information and indicates whether an attack takes place, if so, what response should be taken.
- User interface: allows IDS user's to view and/or define the system behaviour.

The main idea behind our proposal is to create a system that detects the GPS attack. For this reason, our study was started by understanding how GPS sensors work, and then how the three parameters: position, speed and time can be related to each other to detect

misbehaviour at the vehicle's level. We can summarise the process of our proposal as follows:

Figure 6 Process of our proposal (see online version for colours)



As presented in the figure above, the process of our proposal passes through several stages: data collection, processing and verification, and the response phase.

The proposed model is parameterised as follows:

- Activation function: in our model, we use the sigmoid activation function. The input of the function is converted to a value ranging from 0.0 to 1.0. Entries that are significantly higher than 1.0 are converted to a value of 1.0, likewise, values that are significantly lower than 0.0 are snapped into The sigmoid function takes the weighted (w) sum of the input features (x) as an input and outputs the probability value of the outcome as given by equations (1) and (2).

$$h_j = \sum_i^n \left(w_{ij} x_i + b_j \right) \tag{1}$$

$$a_j = \text{sigmoid}\left(h_j \right) \tag{2}$$

- Loss function: is used to optimise the algorithm. The loss is calculated on training and validation and its interpretation is based on the performance of the model in these two sets. In our case, we use binary cross-entropy since we have a binary classification.
- Accuracy metric: is used to measure the performance of the algorithm in an interpretable way. The accuracy of a model is usually specified after the model parameters and is calculated as a percentage. It is a measure of the accuracy of your model's prediction relative to the actual data.

  Optimiser: is utilised to minimise the error rate, there are two important metrics to determine the efficiency of an optimiser the first one is the speed of convergence and the second is the generalisation. In our case, we used RMSProp.

3.8.1 Data collection

The on-board unit (OBU) collects data from embedded sensors in the vehicle [e.g., global positioning system (GPS)] and obtains incoming power from battery-powered vehicles.

The data is composed of the following fields: OBU-ID, timestamp, position, speed. Table 1 explains each field.

Table 1 Data fields in AV

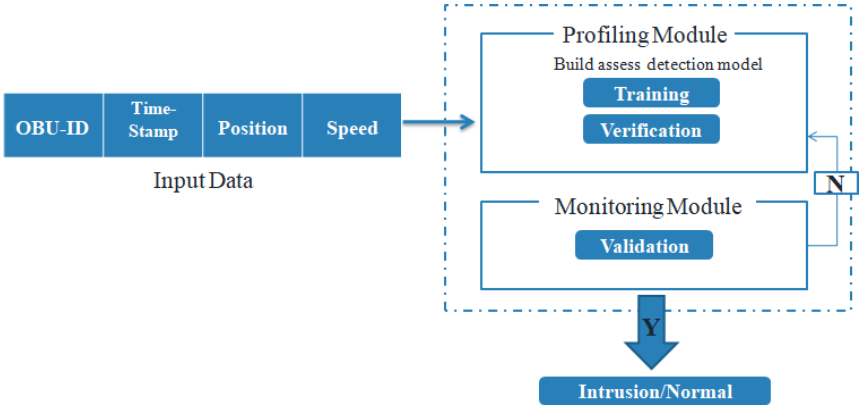
Fields	*Explanation*
OBU-ID	The vehicle ID
Time-stamp	The current time of the vehicle
Position	Is the position given by the GPS sensor in the current time
Speed	The vehicle velocity

The collected data includes two different levels. First GPS data-trace where we get the exact coordinates of the vehicle (longitude, latitude). Then, this data is verified using the time-stamp and the speed of the vehicle to verify its position. The second step is to feed the NN with the collected data.

3.8.2 Processing and verification

The principle is quite simple as already explained in Figure 3 the DL process goes through two main steps: Profiling, in this step for our proposal the model divides the collected data into two categories; the data for training, and the data for validation. Then, goes to the monitoring step in which we check if the data have already passed through the first step of profiling or not. After the verification, the model can then define the data collected as much as an intrusion or legitimate data. Figure 7 shows the proposed model in details.

Figure 7 Proposed methodology (see online version for colours)



3.8.3 Respond phase

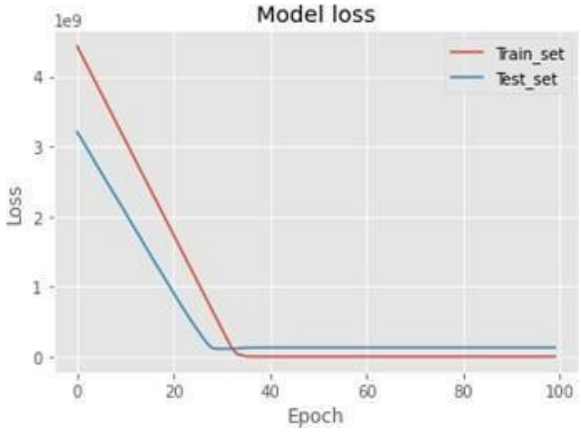
At this level, the system deduces either the vehicle behaves well or not. This means, that the system should provide a way that controls all the systems to prevent any attack from an insider or outsider attacker. After our system deduces the real behaviour of the vehicle the next step is the activation of the protection technique. In this case, we divide it into two types of defence:

- Passive defence: that provides another layer of defence against adversaries by implementing the intrusion detection system which intends to identify internal and external attacks. This defence can be made by implementing such an encryption technique to reinforce the security level in the AV. The encryption technique can be added to the GPS signal via a private key or even encrypt the telemetry and communication links to improve data transmission security
- Active defence: as a continuous process that does not react with the attacker's network. It focuses on defending threat scenarios and on the continuous 'hunt' for attackers who have penetrated the network. This technique can be implemented to ensure for example the accuracy of the data collection to verify deeply the collected data (in our case to generate an HD map).

3.9 Discussion and result

As presented before the GPS sensor faces several security issues. Therefore, implementing a solution that could prevent any suspicious third party to penetrate the system is curial. In our case, we have presented a solution that permits us to avoid any attempt to disturb the good behaviour of the AV concerning the GPS sensor. We present our result concerning the implementation of our proposal work; Figure 8 shows the representation of the loss model which permits us to deduce the way to measure how well a specific algorithm models the given data. Concerning Figure 9, it represents the accuracy of our model which presents the precision of the result that was given. Our model gives us the following result.

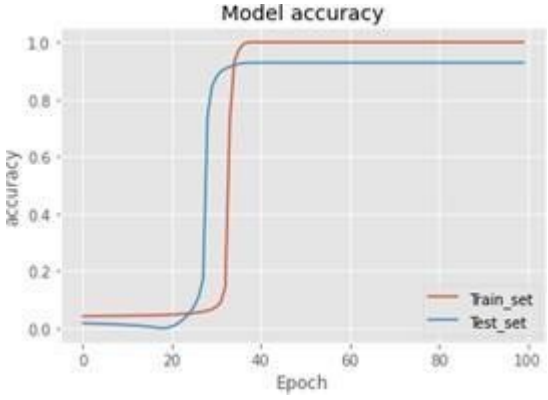
Figure 8 Loss model (see online version for colours)



One of the most commonly used plots for debugging a neural network is a loss curve during training. It gives insight into the training process and the direction in which the network is learning. During an epoch, the loss function is computed for each data element and it is ensured to provide the quantitative loss measure at the given epoch. In our example, we used 100 epochs that represent the number of times the learning algorithm will run on the set of training and test datasets. The loss pattern indicates how bad the model prediction was in an example signal. As shown in Figure 8 an instantiation of the

training and testing process in the direction of our network learns. The loss of our model will almost always be lower on the training dataset than on the test dataset. This means that we should expect some discrepancy between the training and test loss curves. As we can see in our model, the prediction gives almost a result close to zero, which means that the model gives a good fit which is identified by the training and test loss decreasing to a point of stability. The two datasets are correlated with each other, which as we explained gives stability to our model and also allows us to behave appropriately and give good results.

Figure 9 Accuracy model (see online version for colours)



Accuracy is one of the criteria for evaluating classification models. In a non-formal way, accuracy refers to the proportion of correct predictions made by the model and it is used to understand the progress of neural networks. The accuracy is usually calculated after the model settings and represented as a percentage model concerning the actual data. As shown in Figure 9, the plot of accuracy model as we can see for each epoch we are getting increased accuracy, initially, for the first epoch we have received accuracy close to 0.1 for the training and the testing datasets. While, in the 100 epoch we have arrived up to 92% more than 0.92. The evolution of our accuracy of our model increases up the epoch, which shows that our model gives a good result.

4 Conclusions

In this paper, we presented a proposed method to improve the security of a GPS sensor. Each vehicle node can perform an attack detection on the GPS based on the vehicle behaviour. The proposed method uses the concept of deep learning because of the advantages of learning quickly from previous experience. We clearly explained our concept and presented the experimental result we found and showed the effectiveness of our model. We expect that the results will motivate practical defence systems to protect massive GPS users and GPS-enabled autonomous vehicles. Our perspective is to continue along this path to propose an intrusion detection system that will be able to handle all the sensors in the autonomous vehicle to protect it from any threat from either internal or external sources.

References

Anouar, B. et al. (2016) 'Vehicular navigation spoofing detection based on V2I calibration', *Colloq. Inf. Sci. Technol. Cist.*, October, pp.847–849, 2016, doi: 10.1109/CIST.2016.7805006.

AV Interface (2018) *Tai virtul unelmatini*, p.2.

Behfarnia, A. and Eslami, A. (2018) 'Risk assessment of autonomous vehicles using Bayesian defense graphs', *IEEE Veh. Technol. Conf. 2018*, August, pp.1–5, doi: 10.1109/VTCFall.2018.8690732.

Chen, C., Wang, X., Han, W. and Zang, B. (2009) 'A robust detection of the sybil attack in urban VANETs', *29th IEEE International Conference on Distributed Computing Systems Workshops*, July, pp.270–276.

Engoulou, R.G. et al. (2014) 'VANET security surveys', *Comput. Commun.*, Vol. 44, pp.1–13, doi: 10.1016/j.comcom.2014.02.020.

Feng, X. et al. (2017) 'A method for defensing against multi-source Sybil attacks in VANET', *Peer-to-Peer Netw. Appl.*, Vol. 10, No. 2, pp.305–314, doi: 10.1007/s12083-016-0431-x.

Ftaimi, S. and Mazri, T. (2020) 'A comparative study of Machine learning algorithms for VANET networks', *ACM Int. Conf. Proceeding Ser.*, doi: 10.1145/3386723.3387829.

Heinzelman, G. (2019) 'Autonomous vehicles, ethics of progress autonomous vehicles, ethics of progress', *2019 TMC 592 – Research, Ethical Issues in Technology*, April, Prof. Jason Bronowitz Arizona State University, April, doi: 10.13140/RG.2.2.28046.31048.

Jwo, D.J. et al. (2013) 'GPS/INS integration accuracy enhancement using the interacting multiple model nonlinear filters', *J. Appl. Res. Technol.*, Vol. 11, No. 4, pp.496–509, doi: 10.1016/S1665-6423(13)71557-8.

Kang, M.J. and Kang, J.W. (2016) 'Intrusion detection system using deep neural network for in-vehicle network security', *PLoS One*, Vol. 11, No. 6, pp.1–17, doi: 10.1371/journal.pone.0155781.

Kato, S et al. (2015) 'An open approach to autonomous vehicles', *IEEE Micro.*, Vol. 35, No. 6, pp.60–68, doi: 10.1109/MM.2015.133.

Kohlweiss, M., Andersson, C. and Panchenko, A. (2008) 'Self-certified Sybil-free pseudonyms', *Conference: Proceedings of the First ACM Conference on Wireless Network Security, WISEC 2008*, Alexandria, VA, USA, 31 March to 2 April.

Lim, K and Manivannan, D. (2016) 'An efficient protocol for authenticated and secure message delivery in vehicular ad hoc networks', *Veh. Commun.*, April, Vol. 4, pp.30–37, doi: 10.1016/j.vehcom.2016.03.001.

Liu, Q. et al. (2019) 'Secure pose estimation for autonomous vehicles under cyber attacks', *IEEE Intell. Veh. Symp. Proc. 2019*, June, No. 4, pp.1583–1588, doi: 10.1109/IVS.2019.8814161.

Liu, S., Li, L., Tang, J. and Wu, S. (2018) *Creating Atonoumous Vehicle Systems*, The Morgan.

Magiera, J. and Katulski, R. (2015) 'Detection and mitigation of GPS spoofing based on antenna array processing', *J. Appl. Res. Technol.*, Vol. 13, No. 1, pp.45–57, doi: 10.1016/S1665-6423(15)30004-3.

Manale, B and Tomader, M. (2020) 'A survey of intrusion detection algorithm in VANET', *ACM International Conference Proceeding Series*.

Maurer, M. et al. (2016) *Autonomous Driving: Technical, Legal and Social Aspects*, pp.1–706, doi: 10.1007/978-3-662- 48847-8.

Meyrowitz, A.L. et al. (1996) 'Autonomous vehicles', *Proc. IEEE*, Vol. 84, No. 8, pp.1147–1163, doi: 10.1109/5.533960.

Milanés, V. et al. (2008) 'Autonomous vehicle based in cooperative GPS and inertial systems', *Robotica*, September, Vol. 26, No. 5, pp.627–633, doi: 10.1017/S0263574708004232.

Montgomery, P.Y., Humphreys, T.E. and Ledvina, B.M. (2009) *Receiver-Autonomous Spoofing Detection: Experimental Results of a Multi-Antenna Receiver Defense against a Portable Civil GPS Spoofer*, p.7.

Nashashibi, F. et al. (2018) *Véhicules autonomes et connectés, les défis actuels et les voies de recherché*, Inria.

Panice, G. et al. (2017) 'A SVM-based detection approach for GPS spoofing attacks to UAV', *ICAC 2017 – 2017 23rd IEEE Int. Conf. Autom. Comput. Addressing Glob. Challenges through Autom. Comput.*, September, pp.7–8, doi: 10.23919/IConAC.2017.8081999.

Plathottam, S.J. and Ranganathan, P. (2018) 'Next generation distributed and networked autonomous vehicles: review', *2018 10th Int. Conf. Commun. Syst. Networks, COMSNETS 2018*, January, pp.577–582, doi: 10.1109/COMSNETS.2018.8328277.

Ranganathan, A. et al. (2016) 'SPREE: a spoofing resistant GPS receiver', *Proc. Annu. Int. Conf. Mob. Comput. Networking, MOBICOM*, Vol. 0, No. 1, pp.348–360, doi: 10.1145/2973750.2973753.

Ruj, S et al. (2011) 'On data-centric misbehavior detection in VANETs', *IEEE Veh. Technol. Conf. 2011*, doi: 10.1109/VETECF.2011.6093096.

Sukkarieh, S. et al. (1999) 'A high integrity IMU/GPS navigation loop for autonomous land vehicle applications', *IEEE Trans. Robot. Autom.*, Vol. 15, No. 3, pp.572–578, doi: 10.1109/70.768189.

Sullivan, L. and Frost, L.A. (2018) *Global Autonomous Driving", Global Automotive & Transportation Research Team at Frost & Sullivan*, p.82, March.

Thing, V.L.L. and Wu, J. (2016) 'Autonomous vehicle security: a taxonomy of attacks and defences', *Proc. - 2016 IEEE Int. Conf. Internet Things; IEEE Green Comput. Commun. IEEE Cyber, Phys. Soc. Comput. IEEE Smart Data, iThings-GreenCom-CPSCom-Smart Data 2016*, pp.164–170, doi: 10.1109/iThings-GreenCom-CPSCom-SmartData.2016.52.

Tippenhauer, N.O. et al. (2011) 'On the requirements for successful GPS spoofing attacks', *Proc. ACM Conf. Comput. Commun. Secur.*, pp.75–85, doi: 10.1145/2046707.2046719.

Tyagi, P. and Dembla, D. (2014) 'A taxonomy of security attacks and issues in vehicular ad-hoc networks (VANETs)', *Int. J. Comput. Appl.*, Vol. 91, No. 7, pp.22–29, doi: 10.5120/15893-5040.

Xiaonan, L et al. (2007) 'Securing vehicular ad hoc networks', *2007 2nd International Conference on Pervasive Computing and Applications, ICPCA'07*, pp.424–429.

Zeng, K. et al. (2018) 'All your GPS are belong to us: towards stealthy manipulation of road navigation systems', *Proc. 27th USENIX Secur. Symp.*