Transport and Telecommunication, 2018, volume 19, no. 4, 325–334
Transport and Telecommunication Institute, Lomonosova 1, Riga, LV-1019, Latvia
DOI 10.2478/ttj-2018-0027

DATA AND CYBER SECURITY IN AUTONOMOUS VEHICLE NETWORKS

Jamal Raiyn

Computer Science Department, Al Qasemi Academic College
Baqa El Gharbia, Israel
raiyn@qsm.ac.il

An autonomous vehicle (AV) is a vehicle that operates and performs tasks under its own power. Some features of autonomous vehicle are sensing the environment, collecting information and managing communication with other vehicles. Many autonomous vehicles in development use a combination of cameras, sensors, GPS, radar, LiDAR, and on-board computers. These technologies work together to map the vehicle's position and its proximity to everything around it. Because of their reliance on these sorts of technologies, which are easily accessible to tampering, a autonomous vehicles are susceptible to cyber attacks if an attacker can discover a weakness in a certain type of vehicle or in a company's electronic system. This lack of information security can lead to criminal and terrorist acts that eventually cost lives. This paper gives an overview of cyber attack scenarios relating to autonomous vehicles. The cyber security concept proposed here uses biometric data for message authentication and communication, and projects stored and new data based on iris recognition. Iris recognition system can provide other knowledge about drivers as well, such as how tired and sleepy they might be while driving, and they are designed to encrypt the vehicle-to-vehicle and vehicle-to-environment communication based on encryption security mechanisms.

Keywords: autonomous vehicle, cyber attack, road safety

1. Introduction

An autonomous vehicle (AV) is a vehicle that can operate under its own power. There are various levels of autonomous vehicles depending on the degree of autonomy. Vehicles with a low degree of autonomy give the driver more control and functionality for managing the vehicle (Broggi *et al*., 2013).

Fully automated vehicles are expected to have full control over all functions; they do not need a driver to be available at all times during a trip and they do not even require a *steering* wheel. In this type of autonomous automation information about the environment is gathered entirely from on-board sensors without any active communication with other vehicles or the infrastructure. Furthermore, automated vehicles can communicate with each other and share information about the environment. Communication is not limited to communication between cars (vehicle-to-vehicle (V2V)), nor to communication between cars and the infrastructure (vehicle-to-infrastructure (V2I)) (Jawhar *et al*., 2013). A cyber attack can start with control technology tools that are embedded in AVs such as electrical window controls, which are now controlled by engine control units (ECUs) as embedded systems. The ECU is one of the most important parts of a vehicle (Petit *et al*., 2014). An attacker can modify the programming code during design and implementation processing. Attackers target code in order to corrupt or degrade hardware performance, or to destroy information. Kems *et al*. (2014) created a virus that could modify the messages delivered by the controller area network (CAN) bus. Upon successful capture of door locking messages, this virus was able to remotely lock a vehicle's doors. Security issues involving the CAN bus, which connects to all the vehicle's components, crate risks for drive safety and privacy. A cyber attacker can configure the settings, modify code, and implant viruses and malware (Uma and Padmavathi, 2013; Petit *et al*., 2014).

Some cyber attacks involve the use of malware like computer viruses, worms, Trojan horses, spyware and adware; there are also denial-of-service attacks, phishing, and man-in-the-middle attacks. Cyber security aims to prevent unauthorized access to digital devices like PCs, laptops, and smart mobile phones, as well as to wireless communication protocols and wireless routers. Most Web browser privacy protocols have default settings that can be affected by malware attacks by allowing communication with cookies and applications that contain information about internet activity. For instance, many smart phones include a GPS system that knows the device's current location. Cyber attacks can use smart phone apps to track online activities and users plans. In global positioning system

(GPS) spoofing an attacker modifies code to report incorrect GPS locations data which misleads drivers to think they are somewhere they are not.

To secure the information exchange in autonomous vehicles, a new scheme is proposed here based on biometric data In the interest of simplicity and security users need something to replace traditional procedures based on passwords. The main goal of a message authentication system is to disguise a classified message and render it unreadable to all unauthorized persons. Biometrics can meet this requirement and provide faster and easier access. Biometrics comprises methods of recognizing a person based on physiological or behavioural characteristics. To improve safety in AVs, a new scheme is proposed her that uses iris recognition to authenticate vehicle–to-vehicle communication.

The rest of this paper is organized as follows: Section 2 presents different cyber attack scenarios involving AV networks, section 3 describes a system model for data and cyber security AV networks, section 4 explain the implementation of the secure V2V communications; and section 5concludes the paper.

2. Cyber attack on scenarios in VH

Concerns about cyber attacks play a major role in the development and use of AV technologies (Schmittner *et al.*, 2014). This section will point out which technology tools that are embedded in AVs are of interest to attackers, such as sensors, LiDAR, camera hardware, and GPS\GNSS as illustrated in Figure 1. Increasing the degree of automation of a vehicle increases the possibility of a cyber attack. Cyber attack detection systems monitor data as it is received and processed. Furthermore, they maintain system integrity, confidentiality and privacy, availability, authentication, and authorization.

2.1 Cyber attack on sensor networks

Most of the sensors in AVs are only accessible internally. These applications ensure that the vehicle keeps running. Only a few types of applications are involved in perceiving the environment. *Sensor perception* is the process of converting the physical environment into digital signals for further processing, such as measuring forces or distances (Raiyn, 2013a). Sensor networks are targets of interest to attackers. The work of (Knoll, 2014) examines external attacks, but their focus is limited to gaining entrance via exploitable input and output channels, such as Bluetooth, keyless entry systems and wireless maintenance ports.

2.2 Cyber attack on cameras

A camera is an optical device that can perceive the world as a digital video signal (Raiyn, 2013a). Cameras are frequently found in AVs for many applications; they are used to detect traffic signs and to detect and track objects. They can be attacked in various ways. For instance, attackers can hide or replace the images of traffic signs at important locations or add lines to a road to confound lane detection.

2.3 Cyber attack on GPSs

This section will describe currently available global navigation satellite systems (GNSS) (Toledo-Moreo, 2010). The main task of a GNSS is to provide localization and time synchronization services. Several systems of this type are available, the most famous of this type the global positioning system (GPS) (Zandbergen, 2009). GPS data are transmitted coarse/acquisition (C/A) code. This is unencrypted navigation data. It has it is own PRN codes, but it is on the order of 1012 bits long. When locked onto the signal, a receiver will receive Y code, which is the encrypted signal with an unspecified W code. Only authorized users can decipher this. In later GPS satellites, extra features have been added.

There are several methods for augmenting GNSS data, to get a better estimate of location. Three of these methods are satellite-based augmentation systems (SBASs), assisted-GPS and differential-GPS. SBASs are commonly used in airplanes, for critical phases such as the landing phase. They consist of a few satellites and many ground stations. A SBAS covers only a certain GNSS for a specific area. The accuracy of every GNSS, depends heavily on external factors and can be influenced by them (Velaga *et al.*, 2010). This is true not only of GNSS applications, but also of every other wireless transmission application. (propagation errors and space weather)**.** The satellites involved orbit the earth at a height of approximate 20.000 km. At this height, signals can be affected in many ways. According to Raiyn (2017a), ‘space weather’, greatly influenced by the sun, affects signals too. A GNSS requires exact timing on the order of nanoseconds to determine position. Furthermore, if a satellite signal reaches earth, it can be reflect from buildings and other objects, causing an increase in travel time and influencing measurements (Raiyn, 2017b).

2.4 Cyber attack on Light Detection and Ranging (LiDAR)

Light detection and ranging (LiDAR) involves a type of range-finding sensor. It works by emitting a light pulse and measuring the time it takes to reflect off a distant surface. The time is a measure of the distance. Since LiDAR is the preferred technique for speed measurement devices, jammers are widely available on the (black) market. However, LiDAR can see objects that reflect the signal. If the signal fails to return (due to absorption, transparent objects or range limits), the system concludes there is no object present. The absorption of light by rain or snow can reduce the remission rate drastically. The attack is an extension of a replay attack; it aims to relay the original signal sent from a target vehicle's LiDAR system from another position to create fake echoes (Amar, 2006).

2.5 Cyber attacks on wireless communication

Attacks on AVs' radio communication are also possible. The attacker uses a decreasing signal- to-noise ratio, or high latency between the sender and receiver to damage the packet during data transmission before it can be received. In this way, the attacker can delay the communication between the sender and the receiver for a long period of time (Raiyn, 2013b).

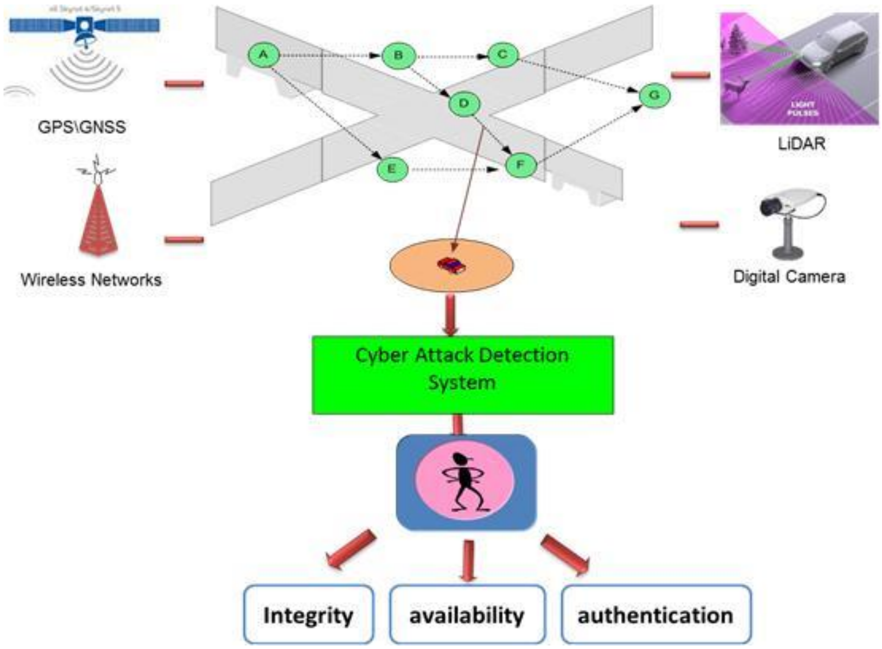

Figure 1. Information cyber security

3. System Model

AVs are sometimes referred to as *driverless* or *self-driving vehicles*. They offer many advantages and are expected to appear on the commercial market by 2030. Comfort is an obvious advantage, but in the current society, the practical advantages of AVs become clearer every day. When roads are congested productivity decreases and money is wasted on fuel and time. Cooperative AVs enhance traffic flow. With regard to road safety, smart vehicles are likely to decrease the number of injuries and fatalities. Current research focuses on the autonomous technologies related to vehicle localization. AVs collect information from the environment as they lack security, as is illustrated in Figure 2. These autonomous technologies consider malicious input. From a security-by-design perspective this is wrong, because a decision made by an AV is only as good as its sensors can perceive. A faulty observation can lead to a dangerous situation. To save the AV from being controlled by terrorists or thieves, we propose here a cyber attack defense model to secure information and to ensured that the vehicle cannot be attacked.

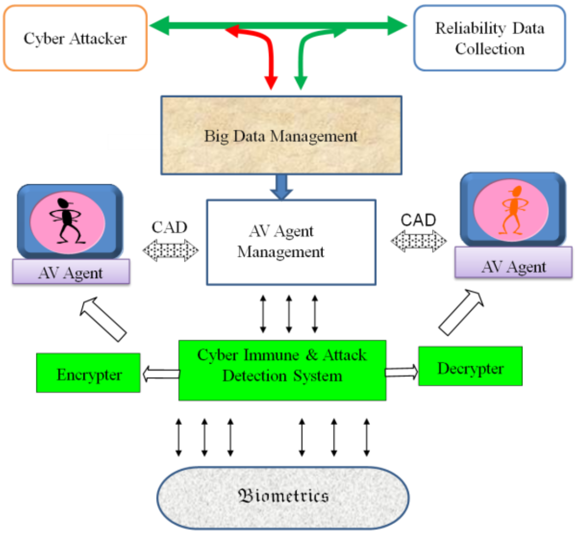

Figure 2. System model

In general, to protect information from unauthorized access, various algorithms have been introduced. These algorithms address the integrity, confidentiality, privacy, availability, authentication, and authorization of information at the servers, including information in files and databases and information in transit between servers, and between servers and clients. The security of information can be ensured in a number of ways. The most common is the use of cryptography in information transmission based on message protocols and authentication. For outside communication, encryption algorithms have been used.

3.1 Communication in AV networks

In some types of autonomous automation, information about the environment is gathered entirely from on-board sensors, without any active communication with other vehicles or the infrastructure. Furthermore, AVs can communicate with each other and share information about the environment. Communication is not limited to communication between (V2V), nor to that between cars and the infrastructure (V2I). Autonomous vehicles used vehicle –to-vehicle communication for lane changes, intersection crossing, and cooperative merging on highways (see Fig. 3 and 4).

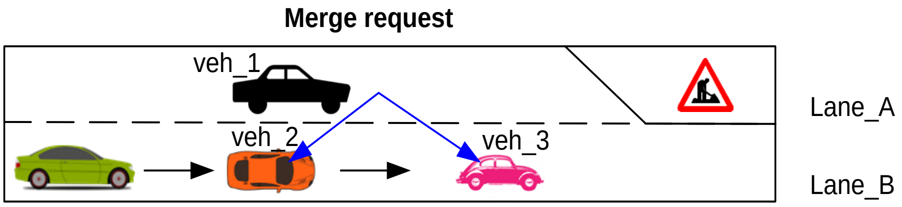

Figure 3. Road lane change

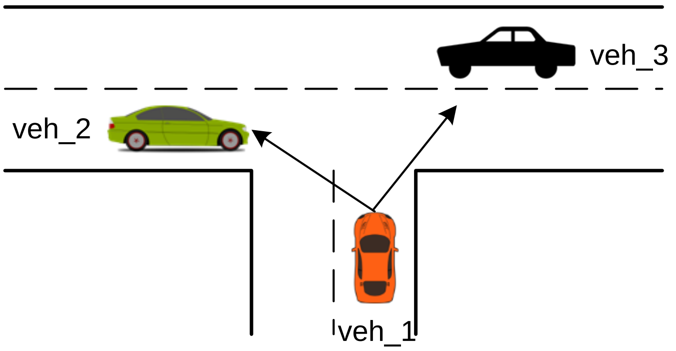

Figure 4. Intersection crossing

3.2 Algorithm description

- An AV-agent is created, by operating the VA.
- The AV agent sends a notification to central control unit (CCU).
- The CCU builds an augmented trip for the AV.
- Data transmission between the CCU and the AV is secured by a biometric identification system.
- The biometric data (DNA of the AV) is presented in a sequence of machine language.

$$\left[\underset{\text{head}}{\overset{1}{\overleftrightarrow{001}}},\ \overset{2}{\overleftrightarrow{111}},\ \overset{3}{\overleftrightarrow{001}},\dots,\underset{\text{tail}}{\overset{n}{\overleftrightarrow{N}}}\right]$$

- The first part (head) of the biometric sequence is allocated to the CCU.
- The last part (tail) of the sequence is allocated to the AV.
- For data transmission only the body of the biometric sequence is sent randomly.
- The biometric identification system orders the sequence using a key.

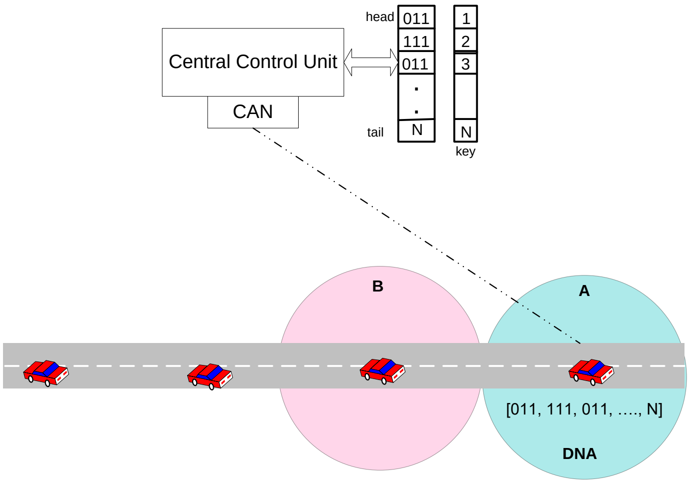

Figure 5. Encryption scheme

Biometric data are used to increase information security levels in message communication. To secure data communication between the AV and serves provider a mobile agent is created; it includes the biometric data (in our case Iris detection information) and is responsible for communication security in mobility, as illustrated in Figure 6. The biometric data is located in a pool.

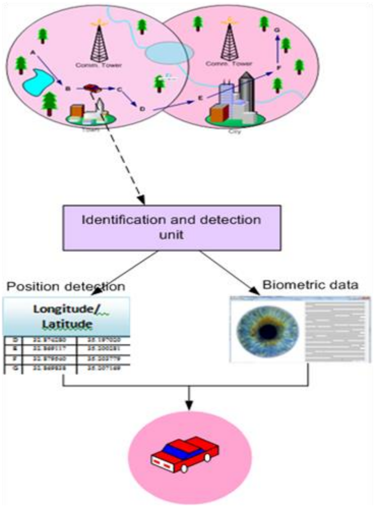

Figure 6. Biometric authentication process

3.3 Iris recognition

Security is an important aspect of fully autonomous vehicles. Security schemes should be accurate and cost-effective alternatives to traditional protocols using passwords or personal identification numbers. To secure the communication between AVs, we propose biometrics; by referring specific physiological or behavioural characteristics, biometrics provides the capability to distinguish between authorized users and cyber attackers. The advantages of using biometrics authentication are the facts that passwords cannot be lost or forgotten, and that it is more reliable and efficient than traditional authentication. The commonly used biometric data include fingerprint, iris, voice, face, and retina identification, and hand geometry (Kade Mahesh *et al*., 2017). The right biometric method for securing data communication in AVs is iris identification. Iris recognition methodology works in two phases, a training and a testing phase. In the training phase, the system learns the features of the iris and improves its rules. In the testing phase, system is tested with images from databases. Figure 7 illustrates the steps in the iris recognition algorithm: segmentation, which used to detect the upper and the lower eyelids, the iris and pupil boundaries; feature extraction which registers some unique attributes of the iris; the matching of the obtained vector in binary code based on the minimum Hamming distance algorithm. The result is expressed as accepted or as rejected if the comparison is mismatched. The binary code derived from the iris is used secure the V2X communication in AVs with the application of encryption keys**.**

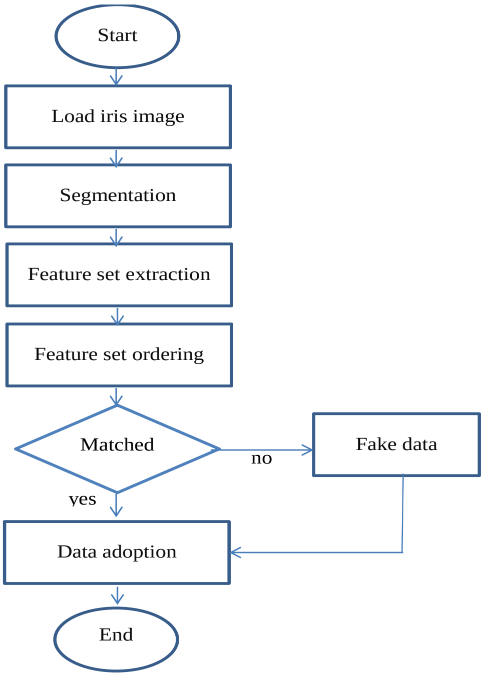

Figure 7. Iris recognition methodology

3.4 Identification and detection unit (IDU)

As in other prediction methods, the identification and detection unit (IDU) uses a data base of images that are known (i.e. the sequence of the pixels of these images is known, and for each pixel in the database it is known whether or not the pixel belongs to a certain sequence). The database is divided into two separate sets of pixels – the training set and the test set. In both sets there are pixels that belong to a certain family (of attributes) and sequence, and pixel that do not.

$$TP = X = \{X_1, X_2, ..., X_n\} \tag{1}$$

$$TN = Y = \{Y_1, Y_2, ..., Y_n\} \tag{2}$$

Each image is then divided into frames, a frame being a subset of pixel from the sequence. The number of pixel in each frame is a variable and is dynamically set to obtain optimal results.

$$\begin{aligned}
X_1 &= \left\{x_1^1, x_2^1, \ldots, x_n^1\right\} \\
X_2 &= \left\{x_1^2, x_2^2, \ldots, x_n^2\right\} \\
&\ldots\ldots \\
X_n^m &= \left\{x_1^m, x_2^m, \ldots, x_n^m\right\}
\end{aligned} \tag{3}$$

If for example a certain frame is composed of 200 segments, the frames might consist of pixels 1 to 10, 2 to 11, 3 to 12, etc. Statistical methods are then applied to find correlation between certain properties of the frame. The basic logic of the statistical differentiation of pixels is known and is widely used by many prediction systems.

$$J = X \oplus Y \tag{4}$$

$$J = \begin{cases} 1 & \text{if } \ x \neq y \\ 0 & \text{otherwise} \end{cases} \tag{5}$$

A large number of correlating factors is defined by the identification and detection unit (IDU) and grouped into sets. A number is linked with each correlating factor, which is then turned into a single number that represents the strength of the correlation factors for each frame with respect to the probability that this frame belongs to a certain family or not. As a result, we have a large number of frames, and for each pair of a frame we have a number that is correlated to the probability that this frame belongs to a certain attribute (e.g. colour similarity) or not.

$$J = \left\{J_1^1, J_2^2, J_3^3, J_4^4 \ldots\ldots\ldots\ldots\right\}. \tag{6}$$

Optimization of J:

$$J_{\mathrm{Pr}\,ediction}(J_1^*) = J_{demand} + k * (\Delta J)\,. \tag{7}$$

In addition to the statistical method an innovative method for the logical XOR multiplication of matrices is applied to enrich the number of frames, which potentially contributes to the prediction model.

4. Implementation and Results

In this section, we present the results of the implemented IDU Algorithm. The IDU is used for the colour detection of eye image in both analog and digital formats. Automatic object detection divides the image into frames, which consist of sets of pixels. In next phase, we use the logical XOR multiplication of frame matrices. This is an enrichment mechanism not currently used in any of the known prediction methods. The columns of each vector in the matrix consist of 0 and 1 values for all of the known 20 pixels in each position of the segment. Position 1 in the first vector indicates whether the attribute is present (=1) or not (=0) in the first position of the first segment. In a similar way, position 20 in the vector will indicate whether or not attribute 16 is present in the third position of the first frame. The other vectors in the matrix are related to the other frames of the set. The values of the vector, which are obtained through logical XOR operations, are related to the non-similarities of the attribute in terms of the positions of the attribute in the sequence of frames.

$$\begin{pmatrix} \underbrace{\begin{matrix} 1 & 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 \end{matrix}}_{segements} \end{pmatrix} \mathbf{\mathit{XOR}} \underbrace{\begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 0 \\ 0 \end{pmatrix}}_{\text{Data Set}}$$

Figure 8 illustrates the segments of pixels. Each pixel's colour matches a certain number between 1 and 255. Figure 9 illustrates the clustering method, which is based on levels of colour.

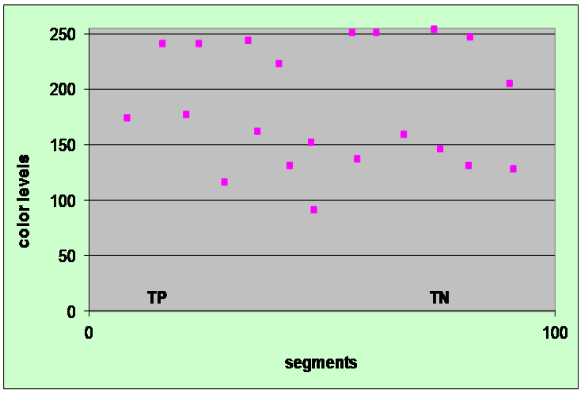

Figure 8. Colour levels

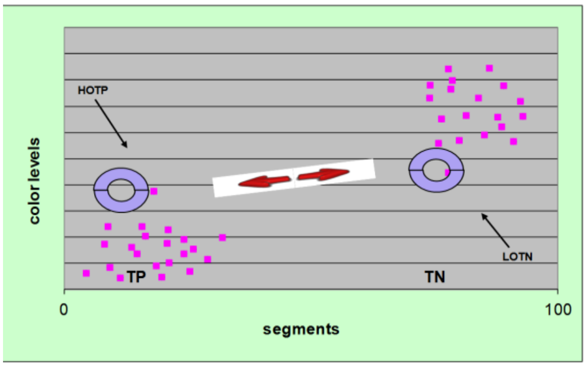

Figure 9. Colour classification

The automatic object detection strategy was implemented in WEKA (Waikato Environment for Knowledge Analysis), which implements many machine learning and data mining algorithms. We have converted the objects in image to 0, 1. The binary symbols are divided into frames and each frame contains a sequence of 0, 1. The classification is based on colour levels as illustrated in Figure 10. Figure 11 shows the clustering of the colours.

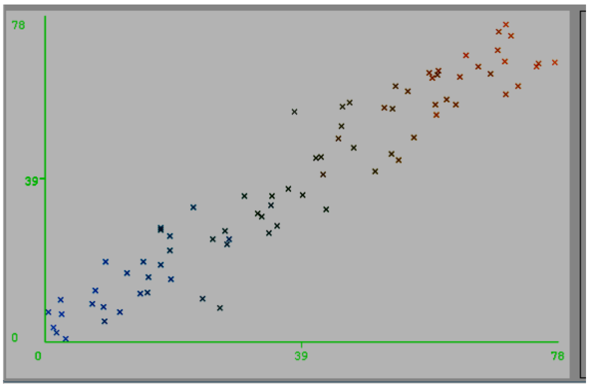

Figure 10. Colour levels in images

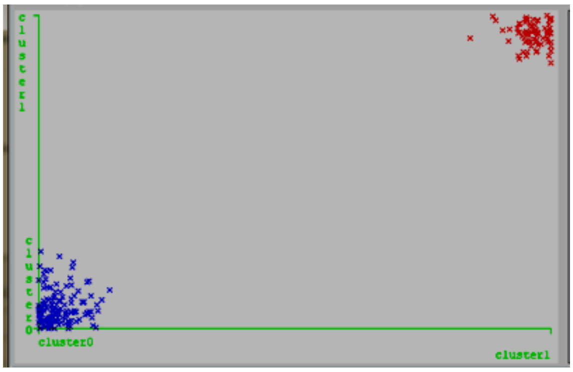

Figure 11. Colour clustering in images

5. Conclusion and future work

This paper gives an overview of the cyber security in AV. Cyber security involves new collected data based on sensors, GNSSs, and LiDAR. To secure the data communication in AVs, we have proposed an authentication method based on biometric data. Biometrics provides a reliable authentication of individual humans identities by their using data associated with idiosyncratic characteristics of physiology and behaviour type (Chirchi *et al.*, 2011). The physiological data consist of fingerprint, iris, voice, face, and retinal characteristics, and hand geometry (Parwin and Verma, 2016). Biometrics data compared to traditional authentication mechanisms such as ID cards and passwords are more accurate and cost - effective. In this paper, we chose iris recognition to secure the data communication in AV networks.

Iris recognition systems use a segmentation method to detect the shape of the iris and pupil and to extract features, such as visual and statistical features using a normalized iris image and matching approach. They use encryption methods to secure vehicle-to-vehicle and vehicle-to-environment communication and they are also capable of providing advanced knowledge about drives, such as their levels of fatigue and sleepiness while driving.

Acknowledgements

The author wishes to thank the Centre for Innovation in Transportation at the University of Tel Aviv for funding this research.

References

1. Amar, N., (2006) LIDAR technology overview. *ETI–US Geological Survey*, Retrieved August 17.
2. Broggi, A. *et al*. (2013) Extensive Tests of Autonomous Driving Technologies. *IEEE Transactions on Intelligent Transportation Systems*, 14.3. 1403–1415.
3. Chirchi, V.R.E *et al*. (2011) Iris Biometric Recognition for Person Identification in Security Systems, *International Journal of Computer Application*, 24, 9. 0975-8887.
4. Jawhar, I, Mohamed, N. and Usmani, H. (2013) An Overview of Inter-Vehicular Communication Systems, Protocols and Middleware. *Journal of Networks*, 8, 12. 2749–2761.
5. Kade Mahesh, K. Kishore, P.V.V. and Karande Kailash, J. (2017) Survey on Iris Image Analysis, *Indian Journal of Science and Technology*, 10(19),1-15.
6. Kastner, R. and Michalke, T. (2010) Attention-based traffic sign recognition with an array of weak classifiers. (IV), 2010 *IEEE* (June 2010). 333–339.
7. Kerns, A.J., Wesson, K.D. and Humphreys T.E. (2014) A blueprint for civil GPS navigation message authentication. *Position, Location and Navigation Symposium* - PLANS 2014 (May 2014), 262–269.
8. Knoll, A. (2014) *Environmental Sensing and Data Processing*.
9. Parwin, R. and Verma, S. (2016) Iris Recognition Using Dual tree complex transform, *International Journal of Engineering Development and Research*, 4, 4. 2321-9939.
10. Petit, J., Feiri, M. and Kargl, (2014) Revisiting attacker model for smart vehicles. *Wireless Vehicular Communications* (WiVeC), IEEE 6th International Symposium. pp. 1–5.
11. Raiyn, J, (2013a) Detection of Objects in Motion - A Survey of Video Surveillance, *Advances in Internet of Things*, 3: 73-78.

12. Raiyn, J. (2013b) Handoff self-management based on SNR in mobile communication networks, *Int. J. Wireless and Mobile Computing*, 2013; 6(1): 39-48.
13. Raiyn, J. (2016) Speed Adaptation in Urban Road Network Management, *Transport and Telecommunication*, 17, 2. 11-121
14. Raiyn, J. (2017a) Road traffic congestion management based on search allocation approach, *Transport and Telecommunication*. 18. (1).25-33.
15. Raiyn, J. (2017b) Developing Vehicle Locations Strategy on Urban Road, *Transport and Telecommunication*, 18. (4). 253–262.
16. Schmittner, C. *et al*. (2014) Security Application of Failure Mode and Effect Analysis. *Computer Safety, Reliability and Security*. pp. 310–325.
17. Toledo-Moreo, R. (2010) Lane-level integrity provision for navigation and map matching with GNSS, dead reckoning and enhanced maps. *IEEE Transactions on Intelligent Transportation Systems*, 11, 1. 100–112.
18. Uma, M. and Padmavathi, G. (2013) A Survey on Various Cyber Attacks and their Classification, *International Journal of Network Security*, 15, 6. 391-397.
19. Velaga, N.R., Quddus, M.A. and Bristow A.L. (2010) Detecting and Correcting Map Matching Error in Location-Based Intelligent Transport Systems, *12th WCTR*, 2010 July, Lisbon, Portugal.
20. Zandbergen, A.P. (2009) Accuracy of iPhone Locations: A Comparison of Assisted GPS, WiFi and Cellular Positioning, *Transactions in GIS*, 13(1). 5-16.