Securing Perception System of Autonomous Vehicle

Mariam Faied, Kevin Daimi, Samar Bayan
Department of Electrical and Computer Engineering, and Computer Science
University of Detroit Mercy
Detroit, Michigan, USA
Email: {faiedma, daimikj, bayansa}@udmercy.edu

***Abstract*—The sophisticated internal communication of the autonomous vehicle together with the various external communications will greatly increase the attack surface and widely open the door for even more security threats as compared to the non-autonomous vehicle. This requires further strict security measures and protection. This paper attempts to secure the communications within the Perception System. It aims to protect both the Environment and Location Perception modules. Both symmetric and asymmetric cryptography will be used depending on the size of the exchanged messages. Cryptographic protocols will be provided.**

Keywords*— *Autonomous vehicle; Cryptography; Perception system security; Security protocol.

I. INTRODUCTION

Vehicle accident statistics showed about six million average car accidents per year occurring in the United States [1]. Those that resulted in death were caused by driver's faults, such as alcohol drinking (40 %), speeding (30 %) and reckless driving (33 %). According to the National Highway Traffic Safety Administration (NHTSA), the financial cost of crashes reached 242 billion dollars in 2010 [2]. For this reason, scientists nowadays are more oriented towards how to minimize the role of the driver. As a result, it should be no surprise that the autonomous vehicle idea became a reality. The autonomous vehicles are divided into five levels of autonomy ranging from level 1 (low level driver assistance) to level 5 (full automation) [3]. The autonomous vehicle provides various benefits including reduced human stress, improved productivity and mobility, traffic safety, and reduced accidents costs [4]. In 2007, about six autonomous vehicles (level 3) completed 90 Km test drives [5]. The improvements resulting from these tests will definitely contribute to having even more autonomous vehicles on the roads during the years to come.

Autonomous vehicles are anticipated to provide safer transportation with well-planned techniques to avoid these large numbers of accidents. Undoubtedly, they will improve human safety and reduce the accident costs. The way that the autonomous vehicle functions could be compared to the way humans analyse the environmental signals. In other words, humans possess an action-perception reaction to the environment. This process is handled by three systems: the perception system (sensing the environment), the cognition system (analysing the data and making decisions) and finally the action system (implementing the decisions resulted from the cognitive system) [6]. An autonomous vehicle is supposed to function in a similar pattern.

The work of the autonomous vehicle is basically dependent on three technologies: the embedded processors, the sensors, and the communication systems [7]. The communication technologies can be categorized into inter- and intra-vehicle. The first category allows for outside communications and the second is defined by different communication techniques allowing data transmission within the vehicle [8]. These increased levels of communications of the autonomous vehicle make it more vulnerable to security attacks [9].

In the past, vehicles were initially made to be isolated mechanical devices [10]. This means that the attacks were targeted to a specific vehicle because every vehicle was operating independently. However, with the introduction of connected and autonomous vehicles, inter-vehicle communication increases the risk over multiple vehicles. Hence, part of autonomous vehicle safety relies in providing deterministic techniques to improve cybersecurity and prevent cyber-attacks. Physical safety is the other part of the autonomous vehicle's security which ensures that pedestrians and people in the vehicle are safe [11]. This is achieved through well-designed navigation algorithms.

The use of various processors and networks by autonomous vehicles opened the door wide for several possible vulnerabilities. These include spoofing, sender/receiver related errors, segmented network related errors, and communication corruption [12] – [15]. Weaknesses of the Control Area Network (CAN), such as the susceptibility to Denial of Service attacks (DoS), and the absence of authentication, contribute to the majority of these vulnerabilities. To avoid security attacks based on these vulnerabilities, security requirements should have been enforced prior to the actual design of these vehicles [16]. Message encryption techniques alone do not impose data integrity and confidentiality [17]. To help with the protection efforts, researchers have introduced a number of tools to enrich the security of data transmission in both inter-vehicle and intra-vehicle communications [18]. To this end, Schlatowe et al. [19] suggested relying on trust management and control. In a similar fashion, the use of polices to govern the access to these resources was proposed in [20]. Further attempts to enrich the security of the autonomous vehicles included relying on the tamper proof microkernel, proxy, and network stack to augment the security of the vehicle networks [21]. Others suggested adding more sensors to the autonomous vehicle to monitor the chips' performance to provide integrity and availability [22].

As detailed in Section II, the autonomous vehicle relies on three major components: Perception, Planning and Control Systems. This paper aims at securing the Location and Environment Perception subsystems of the Perception System. Both symmetric and asymmetric cryptography will be employed. The proposed security protocols will be discussed. The reminder of the paper is organized as follows. Section II briefly presents an overview of the autonomous vehicle. Section III introduces the proposed Perception

 ISBN: 978-1-61208-727-6

System Security (PSS), and Section IV gives the security requirements of the proposed protocol. Finally, the paper is concluded in Section V.

II. AUTONOMOUS VEHICLE OVERVIEW

Autonomous vehicles are intended to transport passengers to their destinations without any human interference. The function of an autonomous vehicle is modelled by three major systems: Perception, Planning and Control [8] [23]-[26]. These components are illustrated in Figure 1.

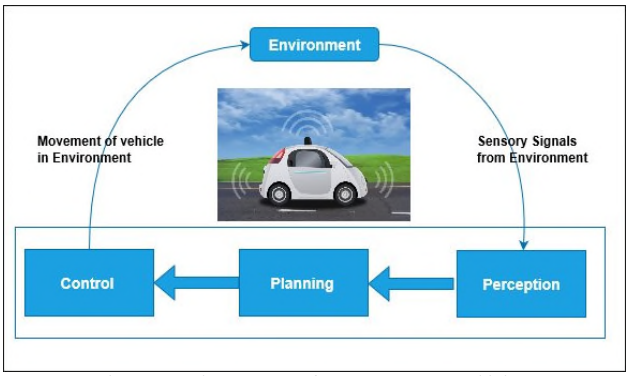

Figure 1. Major Systems of an Autonomous Vehicle.

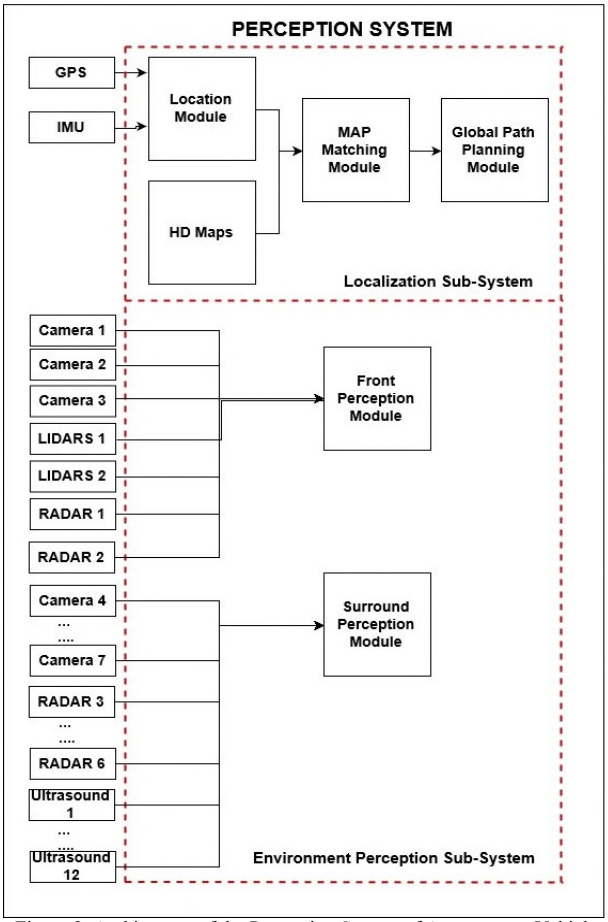

Figure 2. Architecture of the Perception System of Autonomous Vehicle.

The Perception System consists of the Localization and Environmental Perception Subsystems. The Environment Perception Subsystem collects information from the external environment to pilot the detection and identification of the vehicle surroundings. Its function is aided by four types of smart sensors: Camera, Light Detection and Ranging Device (LIDAR), Radio Detection and Ranging Device (Radar), and Ultrasound. Cameras execute detections of lane lines marking, road surface, and on-road objects. The LIDAR constructs a map of the environment to discover obstacles, and the Radar employs radio waves to detect obstacles. Together, LIDAR and Radar grant more accurate positioning of the obstacles on the road than each functioning alone. The Ultrasound Sensor perceives objects through ultrasound acoustic waves. The main purpose of the Perception Module is to blend data coming from the four sensors and prepare them for the next phase [24] [26].

The Localization Subsystem is in charge of determining the autonomous vehicle's position and planning the global path to the destination. An autonomous vehicle's location can be relative, absolute, or hybrid [23]. Relative location represents the location of the autonomous vehicle in relative to its initial position and the absolute location is determined by the Global Positioning System (GPS). The hybrid location refers to the combination of both relative and absolute locations for a more accurate position determination. This is the technique currently pursued in autonomous vehicles testing [23]. Once the hybrid location is identified by the Location Module, the Map Matching Module intermixes it with High Definition Mapping (HD). The HD map is a high resolution map [27] acting as a storage space within the Location Subsystem that saves various types of information including information about roads, traffic conditions, and traffic signs. This map is updated constantly by the manufacturers. Note that this reliance on high accurate maps stems from the fact that an autonomous vehicle operates precisely in 3D space [28]. The final step in the Localization Subsystem is carrying out global planning to the vehicle's final destination. The architecture of the overall perception system is illustrated in Figure 2.

The Planning System employs artificial intelligence to merge and analyse the data from the Environmental Perception Subsystem, Location Subsystem and the outer environment. It is similar to the way the cognitive system of human beings functions. Planning is divided into three stages: Mission Planning, Behavioural Planning, and Motion Planning. The mission planning is accomplished by implementing a search over the roads network connectivity. Behavioural planning deals with the behaviour of the autonomous vehicle based on road signs and traffic conditions, and the motion planning stamps the most important role that artificial intelligence plays in studying the local positioning and making decisions on driving the autonomous vehicle [26]. The control system of the autonomous vehicle receives decisions made by the planning system and implements them through many Electronic Control Units (ECUs) [8] [23]. An overall architecture of the autonomous vehicle is presented in Figure 3.

 ISBN: 978-1-61208-727-6

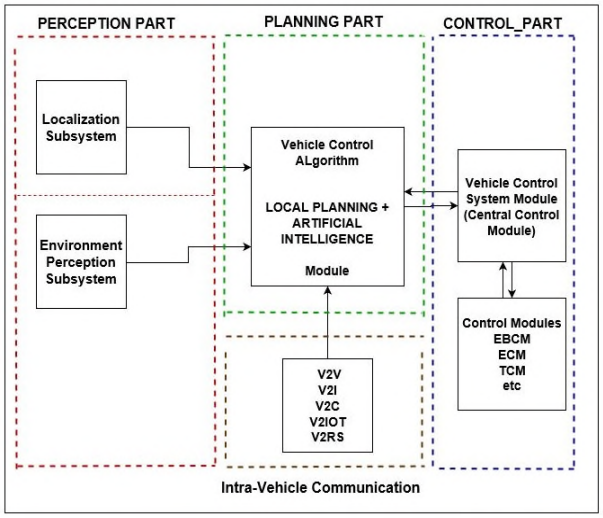

Figure 3. Overall Internal Architecture of Autonomous Vehicle.

III. PROPOSED PSS SECURITY APPROACH

The proposed security protocol will handle the communication between the components of the perception system in the autonomous vehicle. The perception system is made up of two subsystems: Location Subsystem and Environment Perception Subsystem. The parties involved in this protocol and the notations used are illustrated in Tables I and II. As mentioned above, the Environment Perception Subsystem includes the Camera, LIDAR, Radar, and Ultrasound sensors.

TABLE I. COMMUNICATION PARTIES

Party	Meaning
S_i	Environment Perception Sensors
GPS	Global Positioning System Module
IMU	Inertial Measurement Unit
iPM	Front/ Surround Perception Module
MMM	Map matching Module
LM	Location Module

TABLE II. NOTATION USED IN PROTOCOLS

Party	Meaning
PU_S, PR_S	Public and private keys of sender
PU_R, PR_R	Public and private keys of receiver
$PU_{S\text{-}old}$, $PR_{S\text{-}old}$	Old public/private key of sender
$PUR_{\text{-}old}$, $PRR_{\text{-}old}$	Old public/private key of receiver
K_{Old}	Old symmetric master key
K	Master key (symmetric)
K_{Sn}	Session key (symmetric)
$K_{Sn\text{-}old}$	Old session key (symmetric)
H	Hash
MAC	Message Authentication Code
K_{MAC}	MAC key
E	Encryption
D	Decryption
TS_i, where i=1 to 5	Time stamps
N_i	Nonce generated by sensor i
M_i	Message generated by sensor i
C	Cipher text

A. Localization Subsystem Communication

The communications between the modules in the Localization Subsystem of the Perception System (LSPS) are unidirectional (one-way communication). These include communication between GPS/IMU modules and the Location Module (LM), communication between the Location Module (LM) and the Map Matching Module (MMM), and communication between the Map Matching Module (MMM) and the Global Path Module (GPM).

In the GPS/IMU and LM communication, the GPS module sends the coordinates of the autonomous vehicle, known as GPS coordinates, to the Location Module. GPS coordinates represent unique identification of the location of the vehicle. They are expressed as a combination of latitude and longitude. GPS coordinates embody the absolute location of the autonomous vehicle. The IMU unit sends the velocity, altitude and the position of the vehicle. However, these represent the relative location of the autonomous vehicle. The LM will then calculate the hybrid location of the autonomous vehicle, which is the most accurate location based on the absolute and the relative locations. LM sends this hybrid location to the MMM. The MMM will match the location of the autonomous vehicle with the electronic map EM data. This matched location is sent to the GPM. The GPM is responsible for planning the global path from the starting point to the destination point. Hence, the message transmitted within the above three communications is converted into the real-time location of the autonomous vehicle. Table III lists the different types of messages that are exchanged between various components of the Location Subsystem in the Perception System. The exchanged messages, as represented in Table III, are small. This justifies the use of asymmetric encryption. In other words, since these messages are small, the communications within the Location Subsystem lead themselves efficiently to public key cryptography.

TABLE III. MESSAGES WITHIN LOCALIZATION SYSTEM

Operation	Message Type
GPS to LM	GPS coordinates (Absolute location)
IMU to LM	Altitude, Velocity (Relative location)
LM to MMM	Hybrid location
MMM to GPM	Hybrid location

Since the approach is similar for all of the above communications, this protocol will adopt S for sender and R for receiver. If LM is sending data to MMM, S is LM, and R is MMM, and if MMM is sending data to GPM, S is MMM, and R is GPM. The details of this protocol are presented below.

1) Initialization and Key Distribution Stage

Each component in the Location Subsystem has its own built-in public and private keys. In addition, components also have built-in public keys of the receivers. To clarify this, Figure 4 depicts the initialization phase once the vehicle starts. The built-in keys will be referred to as old keys because they will be replaced immediately with fresh new keys for security purposes. Therefore, ‘old” will be added to suffix to denote that.

 ISBN: 978-1-61208-727-6

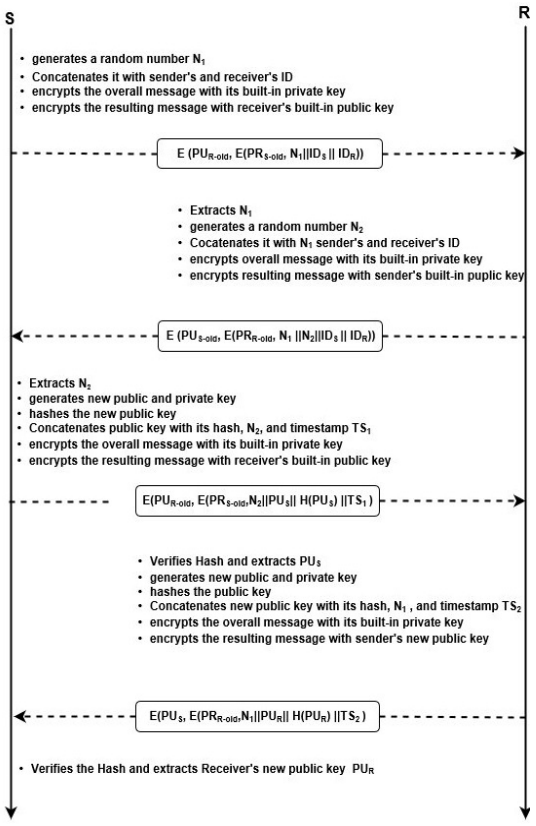

Figure 4. Initialization Stage of LSPS

The sender first generates a random number N_1, concatenates it with the ID of the receiver and its ID, encrypts the concatenated message with the built-in private key and then with the receiver's public key. This represents a request for communication. Note that || stands for concatenation.

$$S \rightarrow R: E\ (PU_{R\text{-}old}, E\ (PR_{S\text{-}old}, N_1||ID_S\ ||\ ID_R)) \quad (1)$$
$$\text{Let } X = E\ (PU_{R\text{-}old}, E\ (PR_{S\text{-}old}, N_1||ID_S\ ||\ ID_R)) \quad (2)$$

The receiver decrypts X with its private key. It then decrypts the resulting message with the sender's public key. This is done to extract the nonce N_1.

$$R: D\ (PU_{S\text{-}old}, D\ (PR_{R\text{-}old}, X)) = N_1\ ||\ ID_S\ ||\ ID_R \quad (3)$$

The receiver generates its random number N_2 and concatenates it with N_1, ID_S, and ID_R. The resulting message is encrypted with its private key, then with the sender's public key to confirm the request received.

$$R \rightarrow S: E\ (PU_{S\text{-}old}, E\ (PR_{R\text{-}old}, N_1\ ||N_2||ID_S\ ||\ ID_R)) \quad (4)$$

Upon receiving the message, the sender decrypts it with its private key. The resulting message is then decrypted with the receiver's public key to get the concatenated nonce. The sender extracts the second nonce N_2 and generates its new public key (PU_S) and private key (PR_S). Furthermore, it concatenates the public key, hash of the public key, the time stamp TS_1, and the nonce N_2. The concatenated message is encrypted with its private key and then with the receiver's public key. Note that time stamp is used because S and R are synchronized.

$$S \rightarrow R: E\ (PU_{R\text{-}old}, E\ (PR_{S\text{-}old}, N_2||\ PU_S\ ||\ H(PU_S)||TS_1)) \quad (5)$$

The receiver decrypts the received message with its private key. It then decrypts it with the sender's public key. R then verifies the hash, ensure the time of the message is still valid, and extracts the sender's new public key (PU_S). The receiver follows the same procedure as the sender did to create its public (PU_R) and private (PR_R) and sends its new public key (PU_R) to the sender. It uses new time stamp TS_2.

$$R \rightarrow S: E\ (PU_S, E\ (PR_{R\text{-}old}, N_1\ ||\ PU_R||\ H(PU_R)\ ||TS_2)) \quad (6)$$

The sender follows similar decryption steps to extract the receiver's new public key (PU_R).

2) LSPS Message Exchange

The sender first encrypts a message (Table III) with the receiver's public key and applies the hash function to the resulting message. Then, it encrypts it with its private key.

$$S \rightarrow R: E\ (PU_R, E\ (PR_S, M\ ||\ H(M)\ ||TS_3))) \quad (7)$$

The receiver, R, decrypts the received message with its private key. What is left from the original message is then decrypted with the sender's public key. The receiver, R, verifies the hash and the time, and extracts the message M. M could be the absolute location, relative location or hybrid location of the autonomous vehicle.

3) LSPS Keys Update

After exchanging a fixed number of messages or after a certain time, both parties will update their keys in a fashion similar to (1) above. The current key will be the old key.

B. Environment Perception Subsystem Communication

The protocol for the Environment Perception Subsystem of the Perception System (EPSPS) below is applied to the messages sent by perception sensors (Camera, LIDAR, Radar and Ultrasound) to the Perception Modules. There are two types of perception modules: Front Perception Module (FPM) and Surround Perception Module (SPM). The encryption details will be similar for both. For this reason, iPM will be used to refer to both.

The type of messages that are transmitted within the Environment Perception Subsystem depends on the smart sensor (LIDAR, Radar, Ultrasound or Camera) that sends the message. Table IV identifies the messages transmitted within this subsystem.

TABLE IV. MESSAGES WITHIN ENVIRONMENT PERCEPTION

Source	Message Type
Camera	Images
LIDAR, Radar, US	Vector of Distances to Obstacles

Since these messages are large, the communications within the Environment Perception Subsystem demands symmetric encryption. The protocol for these communications is as follows.

1) Initialization Stage

The components of the Environment Perception Subsystem have built-in master keys. They are preinstalled at manufacturing time. This means that the Front and Surround Perception Modules will have N built-in master keys, where N is the number of smart sensors connected to the Perception Module, whether front or surround perception module. Once the system becomes in service, the master keys need to be updated and the session keys need to be generated.

2) Master Key Management

The approach begins with a handshake procedure followed by key exchange. The detailed steps are represented in Figure 5.

Each smart sensor generates a nonce, N_1. This nonce with ID_{Si} and ID_{iPM} are encrypted with the old master key and sent to the corresponding perception module. Note that, initially, the old master key is the built in key. Once the new keys are created, the current keys will be old.

$S_i \rightarrow$ iPM: E (K_{old}, N_1|| ID_{Si}||ID_{iPM}) (8)

The iPM confirms the request for communication. It generates another nonce, N_2, and concatenates it with N_1. The resulting value is encrypted with its master key.

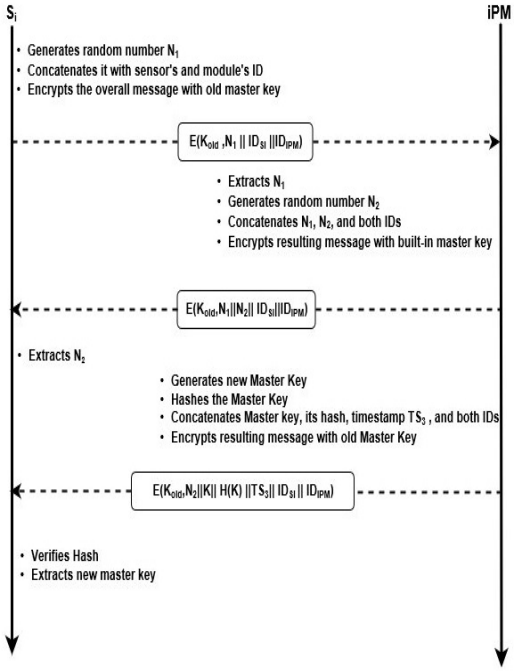

Figure 5. Initialization Stage of EPSPS

iPM → S_i: E (K_{old}, N_1|| N_2|| ID_{Si}||ID_{iPM}) (9)

The smart sensor extracts the second nonce by decrypting the received message with the old master key. iPM then generates a new master key and concatenates it with the hash of this key, its nonce, N_2, and a time stamp. The resulting expression is encrypted its old master key.

iPM → S_i: E (K_{old}, K|| H(K) || N_2 || TS_3|| ID_{Si} || ID_{iPM}) (10)

The smart sensor decrypts the received message with the old master key, verifies the hash and time, and then extracts the new master key. The master key is changed periodically.

3) Session Key Generation

Once the master key is generated, the Perception Modules (whether front or surround) will generate the session key, concatenate it with its hash and time stamp, all encrypted with the old session key. The resulting message is encrypted with the master key.

iPM → S_i: E (K, E (K_{Sn-old}, K_{Sn}|| H(K_{Sn}) ||TS_4)) (11)

The message is decrypted by the smart sensor using the master key. The resulting message is decrypted using the current session key. Having done that, the smart sensor then verifies the hash and extracts the new session key. The iPM then generates the MAC key, K_{MAC}.

4) EPSPS Message Exchange

The smart sensor generates the MAC of the message. It then concatenates the message, MAC of the message and the timestamp. The resulting message is encrypted with the session key and sent to the Perception Module.

X = E (K_{Sn}, M_i || MAC (K_{MAC}, M_i) || TS_5|| ID_{Si} || ID_{iPM}) (12)
$S_i \rightarrow$ iPM: X (13)

The received message (cipher text C) is decrypted using K_S. The result of this decryption represents the concatenation of the message, M_i, and its MAC, timestamp, ID_{Si}, and ID_{iPM}. The time stamp is checked to ensure that the message is current. The IDs are verified and the MAC of the message M_i is found and compared to the received MAC. If they are the same, the message will be considered by the Perception Module.

IV. AUTONOMOUS VEHICLE SECURITY REQUIREMENTS

Within the LSPS, the message integrity is ensured through hashing the message. The hash typically provides integrity of the exchanged data. If the data is changed by even one bit, the hash will be invalid. This makes it hard for an attacker to disturb the data. To ensure that only the receiver will recover the exchanged message, messages are encrypted by the public key of the receiver to achieve confidentiality so that no one except the receiver can decrypt it. Message authentication is ensured by encrypting the overall result with the sender's private key. This authenticates the sender.

For the EPSPS, the message integrity and the authentication are enforced by applying the message authentication code. The use of the MAC confirms that the message received is coming from the sender without being

 ISBN: 978-1-61208-727-6

modified [20]. Through this part of the protocol, symmetric key encryption guarantees the confidentiality of the message since no one, but the sender and receiver, know the symmetric key used within each session. Moreover, the use of the master key enhances the security level.

V. CONCLUSION

Autonomous vehicles are no more just ideas but are finding their way to implementation. The autonomous vehicle should be secured so that people can trust the use of these technologies. The autonomous vehicle is considered part of the Internet of Things (IoT). It works in a similar way to the human being, but with much more focus. Enforcing the security of the Perception System of the autonomous vehicle was the focus of this paper. Both Environmental Perception and Localization Subsystems were protected via cryptographical protocols to secure the data transmission within both subsystems of the perception system. The first subsystem, the Localization Module, consisted of short messages that caused the employment of public key cryptography, while the long messages of the Environment Perception Module necessitated private key cryptography.

This work concentrated on the security of the Perception System. Future work will include securing the Planning and Control Systems in addition to securing the communication between the three systems.

REFERENCES

[1] Driver Knowledge, "Car Accidents in the United States," [Online]. Available: https://www.driverknowledge.com/car-accident-statistics/. Retrieved June 2019.

[2] N. H. T. S. Administration, "Traffic Safety Facts," Department of Transportation, United States, 2016, [online]. Available: https://cdan.nhtsa.gov/tsftables/tsfar.htm. Retreived June 2019.

[3] SAE, "Taxonomy and definitions for term related to on-road motor vehicle automated driving systems," Standard J3016, 2014, [online]. Available: https://www.sae.org/standards/content/j3016_201401/. Retreived June 2019.

[4] T. Litman,Victoria Transport Policy Institute, "Autonomous Vehicle Implementation Predictions: Implications for Transport Planning," Victoria Transport Policy Institute, March 2019. [Online]. Available: http://www.vtpi.org/avip.pdf, Retreived May 2019.

[5] A. Hars, "Autonomous cars: The next revolution looms," inventivio Innovative Briefs, 2010. [Online]. Available: http://www.inventivio.com/innovationbriefs/2010-01/index.html. Retreived June 2019.

[6] R. Shiffrar and M. Blake, "Perception of Human Motion," Annu. Rev. Psychol, 2007, [online]. Available: http://psych.annualreviews.org. Retreived June 2019.

[7] A. M. Wyglinski, X. Huang, T. Padir, L. Lai, T. R. Elsenbarth, and K. Venkatasbramanian, "Security of Autonomous Systems Employing Embedded Computing and Sensors," in Proc. IEEE Computer Society, 2013, pp 80-86.

[8] J. Wang, J. Liu, and N. Kato, "Networking and Communications in Autonomous Driving, A Survey," in Proc. IEEE Communication Surveys and Tutorials, Dec. 2018, pp. 1-1.

[9] V. L. L. Thing and J. Wu, "Autonomous Vehicle Security: A taxonomy of Attacks and Defences.," in IEEE International Conference on Internet of Things (iThings); IEEE Green Computing and Communications (GreenCom); IEEE Cyber, Physical and Social Computing (CPSCom), IEEE SmartData (SmartData), 2016, pp. 534-539.

[10] S. Abuelsamid, " Autonomous Vehicle Cybersecurity, The Need to Protect Automated and Connected Vehicles", 2016, https://www.karambasecurity.com/static/pdf/Autonomous-Automotive-Cybersecurity-Report.pdf. Retrieved June 2019.

[11] S. Brame, "The safety and Security of Autonomous Cars", August 2018, https://restechtoday.com/safety-security-autonomous-cars/. Retrieved June 2019.

[12] M. Gerla and P. Reiher, "Securing the Futurre Autonomous Vehicles: A Cyber-Physical Systems Approach," in Securing Cyber-Physical Systems, Ed. K. P. Al-Sakib, London, CRC Press, 2015, pp. 197-217.

[13] U. E. Larson and D. K. Nilsson, "Securing Vehicles Against Cyber Attacks", in Proc. The 4th Annual Workshop on Cyber Security and Information Intelligence Research CSIIRW'08, New York, USA, 2008, pp. 1-3.

[14] P. Thom and C. MacCarley, "A Spy Under the Hood: Controlling Risk and Automotive EDR". Risk Management Magazine, Feb. 2008; pp. 22–25.

[15] M. Wolf, M. Weimerskirch, and C. Paar, "Security in Automotive Bus Systems," in: Proc. the Workshop on Embedded Security in Cars, Bochum, Germany, 2004, pp. 1-13.

[16] E. Yagdereli, C. Gemci, and A. Z. Aktas, "A Study on Cyber-Security of Autonomous and Unmanned Vehicles," in Proc. Journal of Defense Modeling and Simulation: Applications, Methodology, Technology, 2015, Vol. 12, pp. 369-381.

[17] J. Yoshida, EE Times, "CAN Bus Can Be Encrypted, Says Trillium," [online]. Available: http: //www.eetimes.com/document.asp?doc id=1328081, Oct. 2015. Retrieved: May 2019.

[18] A. Lima, F. Rocha, M. Volp, and P. Esteves-Verissimo, "Towards Safe and Secure Autonomous and Cooperative Vehicle Ecosystems", in Proc. the 2nd ACM Workshop on Cyber-Physical Systems Security and Privacy CPS-SPC'16, Vienna, Austria, Oct. 2016, pp. 59-70.

[19] J. Schlatow, M. Moestl, and R. Ernst, "An Extensible Autonomous Reconfiguration Framework for Complex Component-Based Embedded Systems," in Proc. 12th International Conference on Autonomic Computing (ICAC), Grenoble, France, July 2015, pp. 239–242.

[20] V. Prevelakis and M. Hammad, "A Policy-Based Communications Architecture for Vehicles,' in Proc. International Conference on Information Systems Security and Privacy, Angers, France, 2015, pp. 155-162.

[21] M. Hamad, J. Schlatow, V. Prevelakis, and R. Ernst, "A Communication Framework for Distributed Access Control in Microkernel-Based Systems." In Proc. the 12th Annual Workshop on Operating Systems Platforms for Embedded Real-Time Applications (OSPERT16), Toulouse, France, July 2016, pp. 11–16.

[22] E. Villani, N. Fathollahnejad, R. Pathan, R. Barbosa, and J. Karlsson, "Reliability Analysis of Consensus in Cooperative Transport Systems," In Proc. 32nd International Conference on Computer Safety, Reliability and Security, SAFECOMP 2013 - Workshop ASCoMS (Architecting Safety in Collaborative Mobile Systems) of the, Toulouse, France, Sept. 2013, pp. 1-8.

[23] J. Zhao, B. Liang, and Q. Chen, "The key Technology toward the self-driving car," in Proc. The International Journal of Intelligent Unmanned Systems, vol. 6, issue 1, pp. 2-20, 2018.

[24] M. Mody et al., "Understanding Vehicle E/E Architecture Topologies for Automated Driving: System Partitioning and Trade-off Parameters," in Proc. Autonomous Vehicles and Machine Conference, 2018, pp. 358-1-358-5(5).

[25] S. Behere and N. Torngren, "A Functional Architecture for Autonomous Driving," in Proc. WASA'15, Montereal, Canada, 2015, pp. 1-7.

[26] S. D. Pendleton, H. Andersen, X. Du, X. Shen, M. Meghjani, Y. H. Eng, D. Rus, and M. H. Ang, "Perception, Planning, Control, and Coordination for Autonomous Vehicles," Machines, Vol. 5, issue 1, 2017, pp. 1-54.

[27] Nanalyze, "5 Startups Doing HD Mapping for Autonomous Vehile", November 2018, https://www.nanalyze.com/2018/11/hd-mapping-autonomous-vehicles/. Retrieved June 2019.

[28] H. Verdhan, "HD Maps: New age maps powering the autonomous vehicles", September 2017,[online]. Available: https://www.geospatialworld.net/article/hd-maps-autonomous-vehicles/. Retrieved June 2019.

 ISBN: 978-1-61208-727-6