www.revistageintec.net
ISSN: 2237-0722
revista GEINTEC Gestão, Inovação e Tecnologias

Securing the Communication between Automotive Grade Processors

Rudrappa B Gujanatti[1]; Suhasini Kharka[2]; Arsiya Peerzade[3]; Sushant S Jadhav[4]; Shridevi Mallayyanavarmath[5]

[1]Department of ECE, KLE Dr. M.S. Sheshgiri College of Engineeringand Technology, *(VTU)*, Belagavi, India.
[1]arsiyapeerzade1999@gmail.com@gmail.com

[2]Department of ECE, KLE Dr. M.S. Sheshgiri College of Engineeringand Technology, *(VTU)*, Belagavi, India.
[2]rudraguj@gmail.com

[3]Department of ECE, KLE Dr. M.S. Sheshgiri College of Engineeringand Technology *(VTU)*, Belagavi, India.
[3]shridevimallayyanavarmath@gmail.com

[4]Department of ECE, KLE Dr. MS Sheshgiri College of Engineeringand Technology, *(VTU)*, Belagavi, India.
[4]23sushant@gmail.com

[5]Department of ECE, KLE Dr. M.S. Sheshgiri College of Engineeringand Technology, *(VTU)*, Belagavi, India.
[5]suhasinitiger1203@gmail.com@yahoo.com

Abstract

The project proposes about securing communication between Electronic Control Units (ECUs) in vehicles. ECUs are the microprocessors which are used in the vehicles/automobiles and these processors are also termed as automotive grade processors. Few of the automotive grade processors are "Renesas Processors", "Raspberry Pi Processors", "Freescale Processors", etc. The goal of the project is to incorporate secure data encryption and decryption measures and its impact on the system hardware along with the increase in communication latency. A danger that has been insulant tended to in existing vehicle security assaults, in which the enemy compromises the program of ECUs. In most cases, the assailants overseen to remotely abuse vulnerabilities found on web empowered ECUs such as the media transmission unit or the infotainment framework and from there along the side move through the in vehicle organize and take over security basic components such as the brake, steering wheel and the motor control ECUs. Due to the criticality of such occurrences and the expanding level of security dangers against vehicles, there's a critical got to address the security concerns of inner and outside vehicular communication to ensure the security of travelers. Hence it is vital to maintain safe and secured transmission of data in mobiles.

Key-words: ECU, Encryption, Decryption, Vehicle Security.

1. Introduction

Automobiles were never broader and more comprehensive composed of machine systems with inadequate electrical control operations. In terms of consumer experiences and experience, technology innovations in electronics have led to the growth of the automotive industries in general enhancing the overall driving dynamics of a vehicle and vital operations. Electronic Control Units are digital assets that are connected to on-board systems (ECUs). As they work in collaboration with one another, they must interact their state of the system to one another. Rather than using specialized signal wires for exchanging information, which could involve a lot of electrical connections and skills for the benefit of the technology company, the automotive industry has shifted to data communication.

Different communications buses connect the vehicle ECUs internally. As a result, if any of the other ECUs is compromised, the assailant will be able to receive and manipulate data from other important ECUs. The key reason for this is the inadequacy of confidential information. Furthermore, communication systems seem to be more highly susceptible when data security and credibility are lacking. It has recently been demonstrated that if an assailant can take control of a vehicle by utilizing CIA's inadequacy (Confidentiality, integrity and Authenticity). Furthermore, if a significant ECU is jeopardized, an assailant could even reconfigure the encrypted data.

Symmetric Key Cryptography

A symmetric cryptosystem encrypts and transmits data using only one key. The secret key is the key which is used for encryption and decryption, and is only regarded by those who are approved to use it. The encrypted message is sent over without any unencrypted passwords attached in a cryptographic system. To specify few of the advantages of this method are that the system operates at higher speed, less time consumption; this is because it makes use of only single key for encryption and decryption. Few examples of symmetric cryptography are “Caesar CIpher”, “Hill Cipher”, “Data Encryption Standard”, etc.

Asymmetric Key Cryptography

Asymmetric cryptography also known as public-key cryptography, could be a handle that employments a combine of related keys one is open key and one private key which is used to scramble and decode a message and ensure it from unauthorized access or utilize. A open key could

be a cryptographic key that can be utilized by any individual to scramble a message so that it can as it were be deciphered by the expecting beneficiary with their private key. A private key is known as a mystery key is shared as it were with key's initiator. The system which makes use of this method may consume more amount of time for its execution and also it may affect the speed of execution. These methods are slighter complex as compared to the symmetric methods. Few examples of asymmetric cryptography methods are “RSA”, “Elliptic Curve Cryptography”, etc.

When ever we need to decide on which type of cryptography method that has to be used for securing the communication between the ECUs which are the automotive grade processors we need to consider following factors.

- Memory space requirement.
- Power consumption.
- Execution speed.
- Intra/inter vehicle security.

Above factors become important as the different automotive grade processors have different factors associated with them in terms of memory availability, power consumption limitations, and execution speed limitations.

2. Literature Survey

M. Han et al [1] proposed that ECU gets a control of a component for an Intelligent Control Vehicle(ICV) which is designed to archive the quality disconnected among all the ECUs.The results are appeared as the normal memory utilization with 120 ECUs and 100 messages is underneath 40 Mb. In this future work, ICV will confront driveless situation.

M.S.U. Al et al [2] published a paper work stating the utilization of symmetric key cryptography and elliptic curve based open key encryption for guaranteeing keenness and realness. In case a Mother ECU comes up with no work or an foe compromises the get to control of a Mother ECU at that point the communication of that space can be impended. Future scope recommended is to integrate Interruption Location Framework in Mother ECUs, Every information is scrambled and marked with advanced signature. As a result, the measure of data has extended and it needs more transmission capacity.

F. Kohnhäuser, et al [3] proposed a paper predicting approximately two diverse authentication procedures that empowers the straightforward ECUs such as essential sensors, more complex ECUs like sender combination systems. The utilization of authentication conspire is based on excellent car organize that consolidates CAN and Ethernet. It lacks security highlights that can be found in typical car equipment such as lockstep mode, Ecc memory. Long-term improvement can be an approach that as it were the ace ought to guarantee that all the security basic ECUs are in believe commendable computer program state, at that point the ace permits the vehicle motor to dispatch, this way The security of the vehicle is expected to be negatively affected by ECUs.

Ali Shuja Siddiqui et al[4] published a paper portraying information security dangers in car, display a equipment based security system that gives genuine time for the usage of lightweight cryptographic primitives which proposes a hardware-based confirmation protocol for secure communication. In case if there's any damaged portion within the equipment at that point the total framework may collapse. It is focused on equipment based security arrangement for the asset limitations and time basic applications are practical for the car industry.

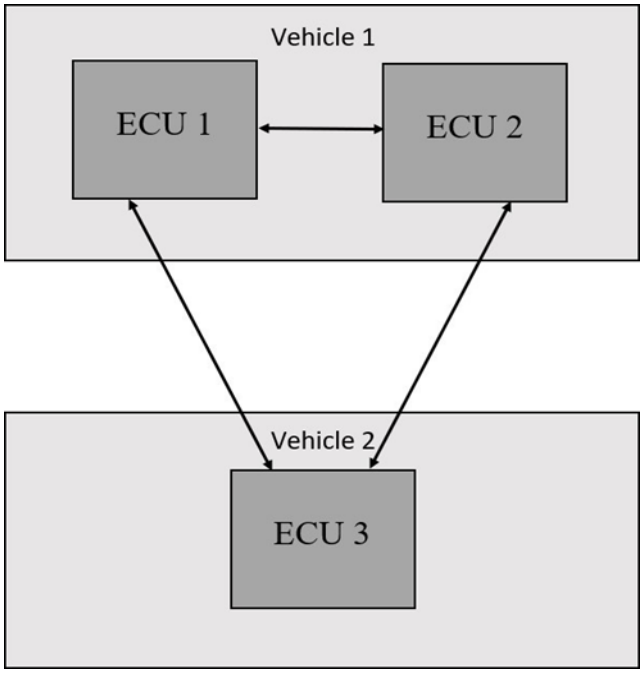
A.S. Siddiqui et al [5] proposed a work on a equipment based secure and trusted system that executes lightweight PUF based common verification and secure encryption over the unreliable communication channel. It fizzled to execute communication over CAN transport in inter-vehicle arrange interfacing ECUs. The future work can be the proposed equipment based security improved system can be coordinates with existing asset implanted gadgets with genuine time reaction prerequisites.

S. Woo et al [6] published a paper on the demonstration of a practical remote assault utilizing real vehicle in a associated car environment in which a driver's smartphone is associated to the in-vehicle CAN. In remote areas this technique cannot be used because it uses CAN which requires internet. Plan the progress the execution security convention through an assessment based on both Secure ECU and CANoe.

I. Studnia et al [7] proposed the diverse conventions being utilized within the implanted systems of current vehicles. At that point examine the potential threats targeting the systems conjointly depicts how the attackers' openings can be improved by the modern communication capacities of advanced cars. Lack of security mechanisms in the current automotive network architecture. In this paper there's need of existing security component within the current car arrange design has become a serious issue with the expansion of remote communication capacities to the present day cars.

3. Methodology

Fig. 1- Block Diagram Representing Inter and Intra Vehicle Communication



Above Fig. 1 shows the possible communication between inter and intra vehicle.

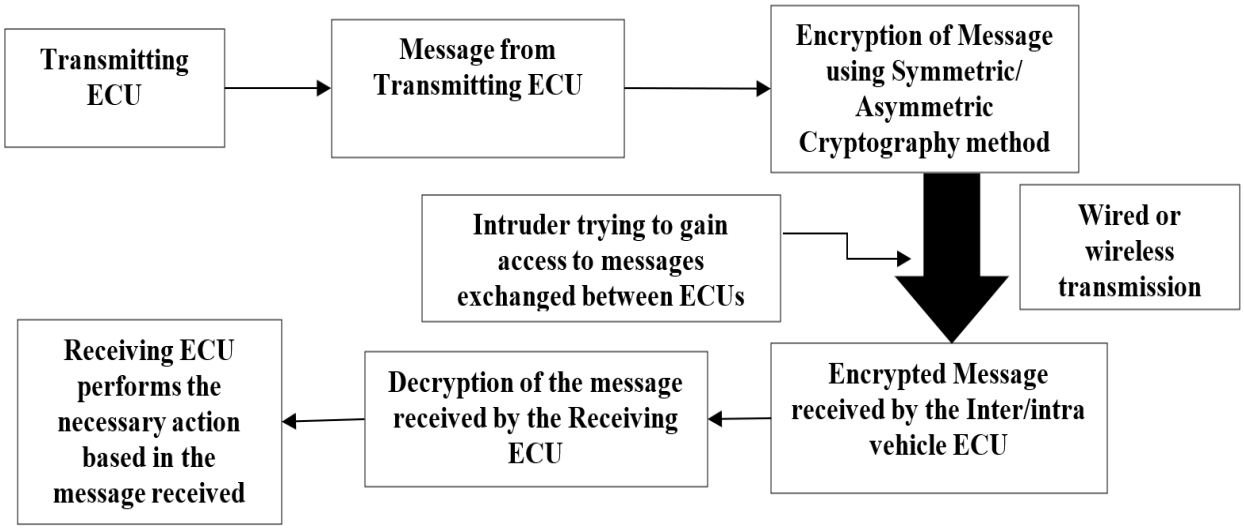
Intra Vehicle Communication

ECU1 and ECU2 which are present within vehicle1 gives rise to intra vehicle communication which is achieved with the help of communication buses. ECU1 connected to bus can read or send to ECU2 and vice versa. With this there comes the aspect of security. If an assailant can breach either of the ECUs, the assailant would also be able to retrieve and modify data of other essential ECUs. If an assailant can breach either of the ECUs, the assailant would also be able to retrieve and modify data of other essential ECUs.

Inter Vehicle Communication

In inter vehicle communication, there are two vehicles involved in the communication as shown in Fig. 1. ECU1 and ECU2 of Vehicle 1 can communicate with ECU3 of vehicle2 and vice versa. If one of the ECUs is compromised, the compromised ECU can monitor the other ECUs. As a result, the security is increased.

Fig. 2- Block Diagram Representing Communication between ECUs



The communication between ECUX and ECUY needs to the encrypted to avoid the ECUs being compromised by the intruder who wants to hack the ECU and take control of various operations of the vehicle. From the transmitting ECU the message needs to be encrypted either using symmetric or asymmetric cryptography method. While choosing the method we need to consider the factors mentioned above in section I. Decision of the method is again based on the criticality of the messages that are to be encrypted, for example, if the message is pertaining to life critical operations such as steering control, power brake, etc., then such encryption method chosen should be such that it should provide more security to the messages exchanged and at the same time they should be decrypted as soon as possible. At the receiver ECU these aspects play a vital role.

When the transmitting ECU sends the encrypted message to the receiving ECU the intruder may attempt to access the encrypted message. The main intention of the intruder is to gain access to the original message in the process of which intruder tries to understand the key used for communication. Our encryption should be such that the intruder should not be able to guess the key used for encryption and decryption by use of frequency analysis, or birthday attack, etc. Here we propose to use symmetric encryption methods for critical application which need quick response or necessary action to be taken by the receiving ECU as it will consume less amount of time for its decryption and consumes less power. For other non-critical applications, we can look forward for using symmetric or asymmetric methods for encryption. Here we propose to use multiple encryption algorithms to provide more security to the communication between the ECUs. Apart from the securing the messages we need to look at the integrity if the messages that being exchanged between the ECUs and also look for authenticity of the messages.

In the proposed system we look forward to implements the security aspect for communication between the ECUs and also look forward for the authentication of the messages to keep check on whether the message was sent by an authentic ECU or whether it was sent by compromised ECU.

To measure the system performance we look forward to use the metrics such as timing analysis, memory analysis and power consumption details for a the encryption and decryption methods proposed to be used in the given framework.

4. Conclusion

The project propose to use a secure framework for encryption and decryption of the messages that will be exchanged between the ECU for communication. Within the plot, a trusted ace ECU confirms the computer program keenness of all safety -basic ECUs within the vehicle. Tests is to display confidentiality, integrity, authenticity. The observing of the ECU information guarantees the security of the information. Filtering a non-compromised ECU from a compromised ECU is more difficult with secure in-vehicle communications. As a future scope the implementation will look forward for keeping track of the compromised ECUs and the method by which the ECUs were compromised which will help to enhance the security aspects of the ECU communication. In expansion, the ensured ECU information can be utilized to analyze post-accident scenarios, driving behaviors, vehicle conditions, etc. The coordinate's watcher can screen the ECU information and create an alarm, in case the ECU information is conflicting.

References

M. Han, A. Wan, F. Zhang and S. Ma, "An Attribute-Isolated Secure Communication Architecture for Intelligent Connected Vehicles," *in IEEE Transactions on Intelligent Vehicles, 5*(4), 545-555, 2020, doi: 10.1109/TIV.2020.3027717

M.S.U. Alam, S. Iqbal, M. Zulkernine and C. Liem, "Securing Vehicle ECU Communications and Stored Data," ICC 2019 - 2019 *IEEE International Conference on Communications (ICC),* Shanghai, China, 2019, 1-6, doi: 10.1109/ICC.2019.8762043.

F. Kohnhäuser, D. Püllen and S. Katzenbeisser, "Ensuring the Safe and Secure Operation of Electronic Control Units in Road Vehicles," 2019 *IEEE Security and Privacy Workshops (SPW), San Francisco, CA, USA, 2019,* 126-131, doi: 10.1109/SPW.2019.00032

Ali Shuja Siddiqui, Yutian Gui, Jim Plusquellic, Fareena Saqib. "A Secure Communication Framework for ECUs", *Adv. Sci. Technol. Eng. Syst. J. 2*(3), 1307-1313 (2017).
DOI: 10.25046/aj0203165

A.S. Siddiqui, Y. Gui, J. Plusquellic and F. Saqib, "Secure communication over CANBus," 2017 *IEEE 60th International Midwest Symposium on Circuits and Systems (MWSCAS), Boston, MA,* 2017, 1264-1267.

S. Woo, H.J. Jo and D.H. Lee, "A Practical Wireless Attack on the Connected Car and Security Protocol for In-Vehicle CAN," in *IEEE Transactions on Intelligent Transportation Systems,* 16(2), 993-1006, April 2015, doi: 10.1109/TITS.2014.2351612.

I. Studnia, V. Nicomette, E. Alata, Y. Deswarte, M. Kaâniche and Y. Laarouchi, "Survey on security threats and protection mechanisms in embedded automotive networks," *2013 43rd Annual IEEE/IFIP Conference on Dependable Systems and Networks Workshop (DSN-W),* Budapest, 2013, 1-12. doi: 10.1109/DSNW.2013.6615528