A design solution to reduce electrical/electronic complexity with secured CAN architecture for an automotive power system

Shrihari Saraf
Dept. Of Electrical Engineering
National Institute Of Technology
Warangal, INDIA
sarafshrihari11@gmail.com

A V Giridhar
Dept. Of Electrical Engineering
National Institute Of Technology
Warangal, INDIA
giridhar@nitw.ac.in

Shweta Jahagirdar
Electronic Division ERC
TATA MOTORS Limited
Pune, INDIA
shweta.jahagirdar@tatamotors.com

***Abstract*—The word automotive at present scenario drives everybody's attention to exponentially emerging technology that is electric vehicles (EV). EV's are the combinations of drive train and various electrical and electronic systems. These large E/E systems in EVs are controlled by various control units, sensors and actuators Making the In-vehicle architecture complex. This paper mainly deals with this problem and provides a design approach to reduce the in-vehicle architecture complexity by making use of the CAN and if necessary, CAN-FD. This paper is divided into three sections, the section I shows the proposed gateway architecture using CAN. Section II is the electrical node simulation part for completing the offline architecture. Section III deals with the security of the proposed design solution. This paper work will be clearly be helpful for in-vehicle architecture design and control for the next generation vehicles. The simulation part makes use of MATLAB software and the feasibility of the solution is tested using the VECTOR CANOE software. This paper also covers some aspects of the battery modelling for offline analysis of the Li-Ion batteries in order to improve the efficiency of the battery and the battery management system used therein.**

Keywords—EV (Electric Vehicle), CAN (Controller Area Network), AES (Advanced Encryption Standard), ECU (Electronic Control Unit), OCV (Open Circuit Voltage), SOC (State of Charge), SOH (State of Health)

I. INTRODUCTION

In electrical as far as the Power system is considered it is majorly molded into three parts mainly generation, transmission and distribution of electrical energy.

The recent need of the hour is to automate the entire power system. Emphasis is mainly on automating the distribution system. Along with the word automation comes the transfer of data and secure communication and a control authority controlling all these scenarios. In distribution system automation, the master distribution system automation system needs to communicate with the peripherals that are electrical systems and sub systems at the end user side's in order to make a desired move. Hence the Proper design solution with reduced complexity of the communication with security is necessary as far the automation is concerned.

In the similar way the automotive also is a combination of chassis, engine, transmission and driveshaft with remaining system and subsystem all this forms the automotive power system. Modern automobile along with the engine, Chassis, body and wheels also are equipped with the sensors and electronic devices which assist the smooth functioning and driving of the automotive. Due to all this advancement and improvement various electrical and electronic circuits are to be added which further increases the complexity of the vehicle. To coordinate these electrical and electronic systems and subsystems introduction of the control units is done. Though the in-vehicle network was so called as an isolated network but the few years has changed the concept.

Today's vehicles not only transport people but also provide entertainment and other services that is infotainment (Information and entertainment). For example, the TCU that Telematics control unit inside the vehicle connects the user of the automobile to the World Wide Web through in-vehicle architecture. All these are very complex process. Hence keeping all these in mind and in order to reduce the in-vehicle architecture complexity and increase the power management and thereby shouldering the vehicle efficiency this design solution becomes a great motivation for all.

II. SECTION I

A. Controller Area network

The Controller area network [2] that is the CAN bus is the robust serial communication bus for control applications in an automotive in real time. CAN bus operate at a speed of up to 1Mbps with excellent other features too. The main purpose is to establish communication between the systems and subsystems present in the automobile for smooth functioning of it.

With CAN based network bus system would significantly reduce the amount of discrete wiring complexity and thereby making the data management easier. CAN is a serial communication protocol and is designed for high speed and reliable data transmission in complex environments.

Below Fig. 1(a) and (b) shows the importance of CAN in this design approach.

Fig. 1(a) In-vehicle architecture without CAN

978-1-7281-8873-7/20/$31.00 ©2020 IEEE

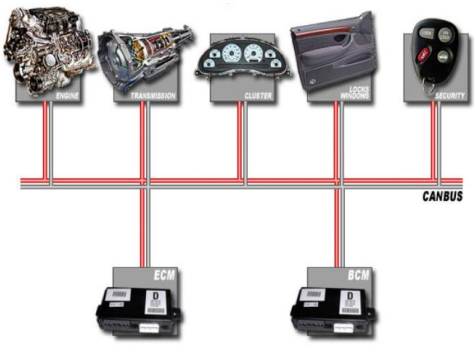


Fig. 1(b) In-Vehicle architecture with CAN

B. *Proposed Design solution*

Concerning to the above issue a design solution is been proposed to reduce the in-vehicle architecture complexity. This project is distributed into two phases. Firstly, the secured

Communication buses are the one through which the data is transported inside the vehicles. There are many types of communication buses such as CAN (Controller area network), LIN (Local Interconnect network), Ethernet, Flex Ray etc. In this project the design solution is implemented using the CAN bus protocol.

Proposed design solution consists of the VECU as a secured gateway with advanced encryption standard connected to various nodes present through available CAN1, CAN2, CAN3, K-line/Lin circuits. The nodes blocks shown below in the design model indicate the various electrical/electronic system and subsystem present in the vehicle.

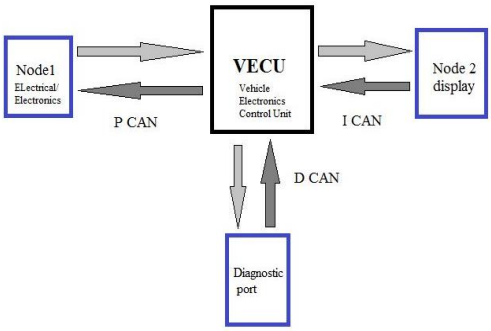


Fig. 2 Basic Block diagram of the proposed design approach

C. *The Gateway Feature*

In order to introduce a security feature this, control unit shown in Fig. 1 is used as a gateway to establish communication between the various nodes connected to CAN of which one node is simulation is shown in this paper which mathematical model of Li-Ion battery for SOC estimation in order to improve the BMS of EV. The feasibility of this proposed architecture is tested using the Vector Canoe software. This mainly helps to check whether proper communication is being established in between the nodes present. This work is evaluated with the help of logging data. The performance evaluation environment in [1] is taken as reference for this work. Considering the Fig.2 this setup in Fig.3 is formed.

Fig. 3 Performance evaluation test setup for gateway ECU

Above Fig.3 shows the performance evaluation environment in which the gateway feature is introduced in the proposed architecture.

Below Table 1 shows the specifications of the equipment's used in the performance evaluation.

Table. 1 Evaluation Tools

Sr. no.	***Tool***	***Note***
1.	Vehicle ECU	Clock freq.: - 8MHz – 40 MHz
2.	CANOE (Identified tool)	Baud rate variation from 250k to 500Kbps
3.	Display	For feasibility check (data logging)
4.	AUTO-COM tool (attack model)	In order to check the security of the proposed model
5.	ECU	Used as a node

III. SECTION II

Electrical Node Simulation

As discussed, nodes are to be simulated for offline analysis purpose, taking this as an opportunity node is been simulated using MATLAB. This part of project includes the simple mathematical modeling of battery for offline analysis using the data samples mainly the charging and discharging voltage and current samples. This part models the battery into a mathematical polynomial with certain parameters considering the linear and nonlinear constraints.

A Thevenin's equivalent model of a battery is considered with OCV in series with an internal resistance, and RC branch. The main objective of this work is the parameter identification after formulating the battery into a polynomial form with relevant coefficients. An optimization problem is formed and the parameters are identifies using the weighted least square curve fit method. This method provides us with the range of the coefficients necessary for exactly matching the battery characteristics. An evaluation is done based on actual characteristics of the battery and proper values of the coefficients are tabulated.

This modeling work included in this paper as a node simulation part will also be helpful in Dynamic SOC estimation, series resistance estimation contributing to Sate of health SOH estimation of battery. The reference data is taken from [9] and the results are nothing but comparison with this offline data in from [9].

A. Problem Formulation

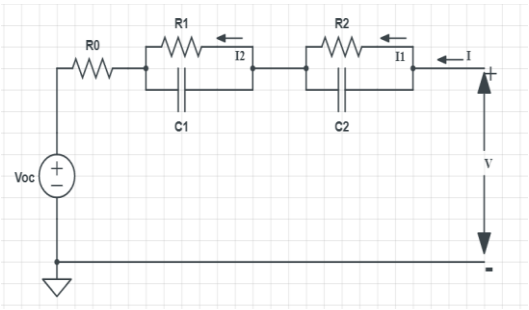


Fig.4 2-RC Equivalent circuit model

The above circuit is the Thevenin's equivalent model. An illustration with one open circuit voltage source in series with resistance and two RC branches in series is shown.

From [3] analysis of the 2-RC equivalent model of battery is considered for modeling purpose. There were some shortcomings observed in 1-RC model hence 2-RC equivalent is considered in this paper. To predict the run time characteristics of a battery mathematical model with certain empirical formulae are required also, mathematical model as compared to electrochemical models are easy to compute.

To capture the behavior of the Li-Ion battery the Thevenin's equivalent circuit of battery is considered. To mathematically model the above circuit an extensive relationship between the battery parameters and the Li-Ion terminal voltage is considered thereby providing the foundation of the problem.

The OCV changes with change in SOC in a nonlinear manner. Based on Fig. 5 the above circuit is formulated into 9th order polynomial and the equations are aforementioned.

Applying KVL in the above mesh of Fig.5 we get,

$$Voc = V - I * R_0 - \frac{1}{C1}\int(I - I_1)dt - \frac{1}{C2}\int(I - I_2)dt \quad (1)$$

Where, Voc = OCV that is the open circuit voltage

V = Terminal voltage

R_0 = Internal resistance of the battery

For the above RC branches,

$$V_1(t) = IR_1\,(1 - e^{(-\frac{t}{R1*C1})}) \quad (2)$$

$$V_2(t) = IR_2(1-e^{(-\frac{t}{R2*C2})}) \quad (3)$$

$$R_0(t) = \beta o + \beta 1 * e^{(\beta 2*SoC(t))} \quad (4)$$

The OCV changes with change in SOC in a non-linear manner during charging and discharging. Aforementioned that the OCV is dependent on SOC, following this it is parameterized into a 9th order polynomial equation which is as follows,

Thus Voc = F(SoC) {Polynomial function}

Now, using this equation (2), (3) and (4) in (1) we get the polynomial representation of OCV as follows,

$$Voc\,(t) = \alpha o + \alpha 1*SoC(t) + \alpha 2*SoC^2\,(t) + \alpha 3*SoC^3\,(t) + \alpha 4*SoC^4\,(t) + \alpha 5*SoC^5\,(t) + \alpha 6*SoC^6\,(t) + \alpha 7*SoC^7\,(t) + \alpha 8*SoC^8\,(t) + \alpha 9*SoC^9\,(t) + IR_1\,(1 - e^{(-\frac{t}{R1*C1})}) + IR_2(1-e^{(-\frac{t}{R2*C2})}) + I(\beta o + \beta 1 * e^{(\beta 2*SoC(t))}) \quad (5)$$

Where, R_0= Internal resistance, Voc = Open circuit voltage of the battery to be modelled, SoC = state of charge of the battery

αi for i= 0,1,2,----,9 are the coefficients of the polynomial

βi for i=1,2 are the coefficients defining the change in the internal resistance of the Li-ion battery.

B. Parameter Identification and extracrtion

The main aspect of this modelling is nothing but the estimation of the coefficients which are used to emulate the OCV of the batteries and with the help of curve fir process check the feasibility and reduce the error using the weighted least square method.

If a model structure is determined from and input and output then it is said to be identifiable. Two sets of parameters under the same input generating different output sequence of parameters so that they can be distinguished.

Now, consider the battery is idled for long and equation (2) and (3) are zero and the capacitors from the RC are uncharged then the changes in $V_1(t)$ and $V_2(t)$ are governed and the terminal voltage becomes

$$V\,(t) = \alpha o + \alpha 1*SoC(t) + \alpha 2*SoC^2\,(t) + \alpha 3*SoC^3\,(t) + \alpha 4*SoC^4\,(t) + \alpha 5*SoC^5\,(t) + \alpha 6*SoC^6\,(t) + \alpha 7*SoC^7\,(t) + \alpha 8*SoC^8\,(t) + \alpha 9*SoC^9\,(t) + IR_1\,(1 - e^{(-\frac{t}{R1*C1})}) + IR_2(1-e^{(-\frac{t}{R2*C2})}) + I(\beta o + \beta 1 * e^{(\beta 2*SoC(t))}) \quad (6)$$

In rest of the period after full discharge $V_1(t)$ and $V_2(t)$ approaches zero and V(t) becomes the OCV. This tells that OCV at SOC = 0 is nothing but the αo.

To proceed forward we go for least square curve fit method. From above equation (10) we have

$$V\,(t) = g\,(\lambda, t_i) \quad (7)$$

Where λ = parameter set

λ = [αo, α1, α2, α3, α4, α5, α6, α7, α8, α9, β0, β1, β2];

Curve fit method uses the weighted least square method while fitting the data. This process mainly requires a parametric model that relates the response data to the prediction data with more than one coefficient. The result is nothing but the designed model coefficients. In this part the estimation of λ is a data fitting perspective, as it is achieved by minimizing the residual between the exact terminal voltage data and the prediction done. Also, the non-linearity due to the internal resistance should be considered. Now if optimization is unconstrained it will thus lead to a local optimum which is not feasible though exact estimation is obtained. Hence confining the search in a constrained region will be feasible. To obtain the coefficients this method minimizes the summed squared of the residual as discussed above.

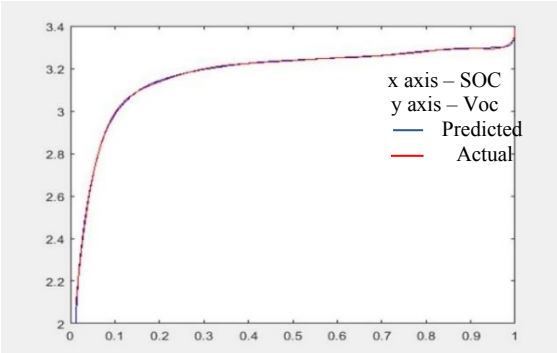
The residual is nothing but the difference between the observed response and the fitted response and is also called as error.

Now in MATLAB to solve the above optimization problem we make use of the *lsqcurvefit* which is leveraged for parameter search in confined trust regions. This makes use of the weighted least square method for the estimation of the coefficients of the polynomial.

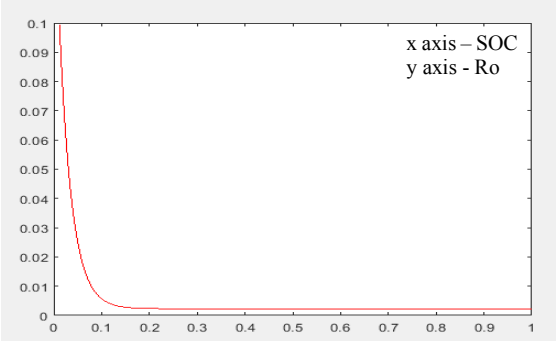
The key question in defining the trust region is minimizing the function and choosing and computing the approximation and thereby modifying the trust region.

This problem is then solved iteratively to estimate the parameter set λ. Thus, the least square curve fit method is

used in the parameter estimation of the battery which is to modeled.



(a)



(b)

Fig. 5(a) Estimated SOC-OCV curves showing actual/predicted terminal voltage comparison, (b) Dependence of R0 on SoC for battery

From Fig. 5(a) we can observe the blue color trace is the scope is the prediction and the red color shows the actual characteristics and with Voc minimum of 2.2V and Maximum of 3.5 V Thus here the node for the proposed model is properly simulated. This node thus will send control signal with SOC, SOH and temperature values over the CAN bus through the gateway which further can be used for making the BMS more efficient in EV.

Below table 2 shows the estimated values of the coefficient for charging scenario of the battery with the constrained trust regions and the results are verified by characteristics comparison shown in Fig. 5(a). After this node simulation part, the third part is the security of the proposed architecture.

Table 2: Estimated polynomial coefficients and the extracted parameters

Battery Discharging Scenario					
Sr. no.	***Coefficients***	***Estimated values***	***Sr. no.***	***Coefficients***	***Estimated values***
1	α1	5.1887	9	α9	-262.58
2	α2	-9.8805	10	R1	0.005
3	α3	-82.68	11	1/R1C1	0.012831
4	α4	594.21	12	R2	0.0065
5	α5	-1743.1	13	1/R2C2	0.024059
6	α6	2810.2	14	βo	0.0022949
7	α7	-2588.7	15	β1	0.1526
8	α8	1278	16	β2	38.05

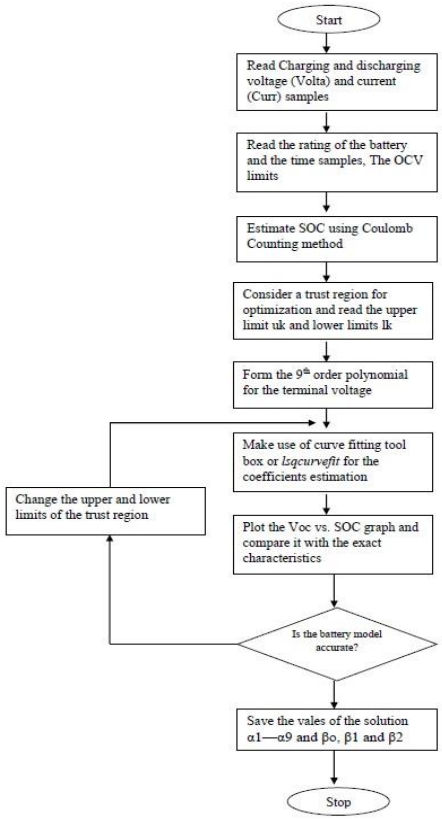


Fig. 6 Flowchart for parameter extraction and SOC estimation

IV. SECTION III

Security of the proposed architecture

After lot of research is been carried and it is observed that CAN bus is more vulnerable to attacks. Along with CAN CAN-FD also fails to provide security as far the communication is concerned. The three main vulnerabilities in CAN are: poor access control, lack of encryption, and lack of message authentication. To make the proposed architecture secured these three vulnerabilities should be eliminated. The requirements mainly include confidentiality, authenticity, access control and Round key management.

A. Advanced Encryption Standard

The National Institute of Standards and Technology has chosen the AES as encryption algorithm. Thus, for symmetric key cryptography The AES is one the most popular algorithm used. Symmetric means encryption and decryption done with the help of same key. The AES is included in the design solution in order to make the architecture a secured one. Below Fig. 8 shows the block diagram of AES. The message to be encrypted is called as plain text. The transformation of plain text to cipher text is done through the encryption. AES is a 128-bit symmetric block cipher. It takes 128 bit of message and encrypts it into 128 bit of cipher text with some key called as round key. The key can be of 128-bit, 192-bit, 256-bit which gives high amount of security. The key size decides the number of rounds or iterations for carrying the

encryption. Instead of stacking 128 bit of message in a single line AES arranges it to a state matrix.

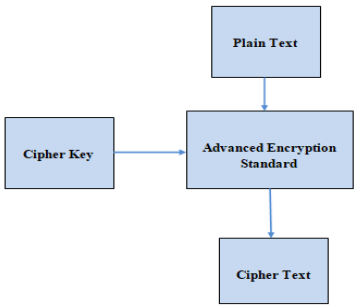


Fig. 7 AES Block diagram

After State matrix formation to go on with encryption series of steps are which includes adding round key, Sub-byte, shift rows and mixing columns. These all four-step process forms one round and number of round executions depends on the length of the round key used.

B. Security Analyis

In the proposed design solution, we assume the following. First, the gateway VECUs pre-share the long-term symmetric keys also called as the round keys. This uploading of keys into the VECU is done through the secured channel Second, ECUs use the data frame filtering which clearly ensures that a receiver ECU can selectively receive the desired data frame (among data frames broadcasted on the in-vehicle CAN bus) using the sender ID. Third Data frame counter is managed by the sender node and receiver node connected to the CAN bus. Fourth, the gateway VECU has more computing power as compared to the other node ECUs. Fifth, a device certificate is uploaded on the gateway VECU and external devices, authenticated by the OEM

- *Encryption*

The best solution to this so far seems to be cryptography [7]. It plays a vital role in providing authentication, security and integrity of the benchmark data. Symmetric and asymmetric cryptography are two types of cryptography. In asymmetric cryptography the public keys are used. In asymmetric encryption the third part encryption is valid but this encryption can be decrypted using the private key which reduces the security level of the asymmetric encryption. However same private key is used for encryption and decryption in symmetric encryption.

- *Confidentiality*

The proposed security architecture makes use of AES-128 algorithms to secure the CAN data frames from the attackers. When a vehicle is started, every node 1 ECU installed in the subnetwork on one CAN e. g PCAN performs a session key derivation process with VECU (Gateway) using the long-term symmetric keys which are pre shared keys and these keys are also present with legitimate node 2 ECU present on another CAN bus e.g. ICAN storing the long-term symmetric keys are also able to compute the session key but an attacker cannot obtain it. This means that an attacker is neither able to decrypt the key nor able to derive it from the seed. Because the security of the AES-128 algorithms has been proven in [4], it is clear that the attacker cannot obtain CAN data without an encryption key.

- Authentication

Our proposed security architecture uses a 128-bit AES to ensure authentication of the CAN data frame.

- Access Control

As we are clear about the thing that the attackers cannot get the keys for getting access of the architecture. Thereby restricting the attacker to modify the data frame. In This project work the attack model used is an offline wired connection that is utilization of a diagnostic tool. The various E/E system control is done by different ECUs. The diagnosis of these ECUs for research is necessary. The diagnosis is mainly done by the OBD connector which can be an attack model. Hence access control through pre shared keys is done thereby protecting the architecture from unidentified tool attack.

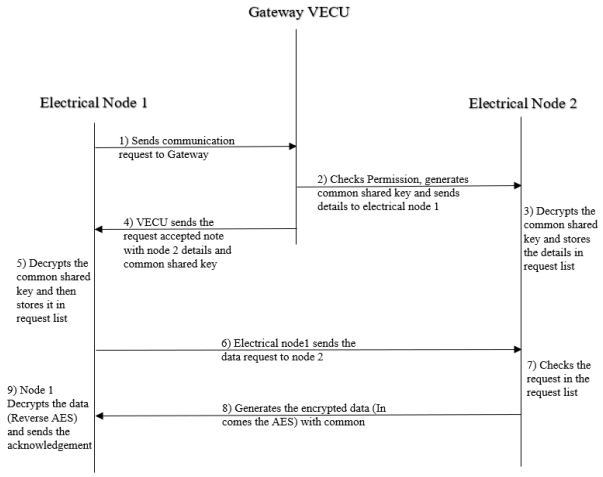


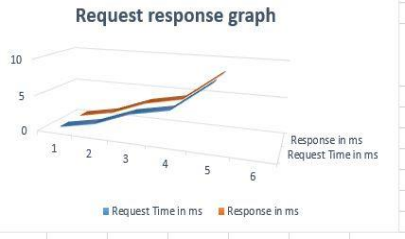
Fig. 8 The Secured communication Scenario

The Above Fig. 8 shows the steps involved in the secured communication between the nodes through the Gateway.

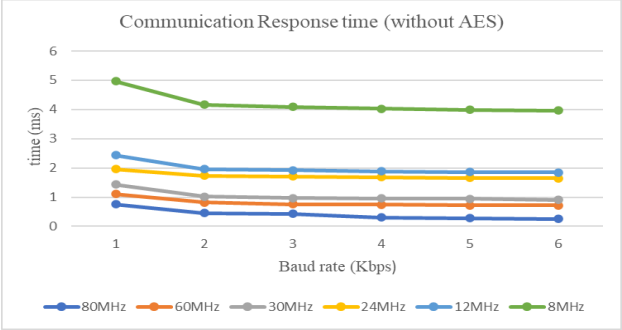
C. Performance Evaluation

The performance evaluation is mainly done in the form communication response time graphs. In this case the execution time and handshaking time is measured with and without AES. This is done by changing the CPU clock rates using PLL setting and the baud rate that is 250kbps or 500kbps. The Processor clock rates are changed from 8Mhz to 80 MHz and the response time graphs are plotted in excel

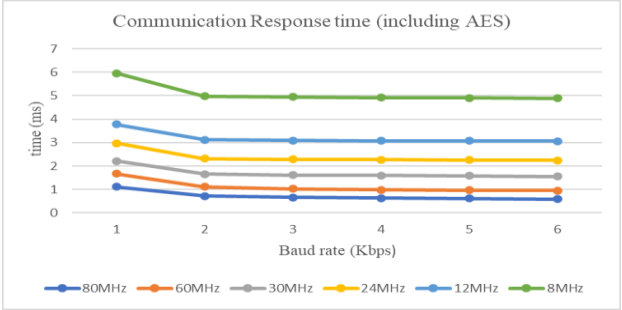
signal Id	Request Time in ms	Respons e time in ms
18EAFFF9x	0.386575	0.387958
	1.41528	1.416759
	3.372296	3.374772
	4.434726	4.443381
	8.33423	8.338054



(a)



(b)



(c)

Fig. 9 (a) Handshaking time during Communication
9 (b) Communication response time without AES
9 (c) Communication response time with AES

The communication response time is mainly divided as follows

1) The Sender node ECU transmits a request message
2) The receiver ECU node receives it.
3) Receiver ECU nodes generates a response message
4) Receiver node ECU transmits response message
5) The Received message is then decrypted by reverse AES

This all communication is encrypted by AES in order to avoid manipulation of data frames and theft of benchmark data in between. Thus, is the communication process

V. Conclusion

The design solution proposed in here to minimize the in-vehicle electrical and electronic complexity with VECU as secured gateway is implemented. This work provides us with the mathematical modeling of Li-ion battery. This modeling part is nothing but offline electrical node simulation for completing the proposed gateway architecture. This electrical node simulation is helpful mainly in Electric vehicle domain as offline analysis of the Li-ion battery helps in improving the efficiency of the batteries and also will be helpful in an efficient battery management system as far the SOC estimation is concerned. Moving towards the security of the design solution, the AES implemented in here considers only the software aspect the hardware design is not part of this work. This work also helps in understanding the power train communication standards and protocols involved and their efficient use. Thus, this work gives a practical security architecture after analyzing the automotive electrical/electronic systems and subsystems and can extensively be helpful in having better BMS and pointing out the performance level of the vehicle ECU for vehicles in which secured communication is of great concern

References

[1] Samuel Woo, Hyo Jin Jo, In Seok Kim, and Dong Hoon Lee, "A Practical Security Architecture for In-Vehicle CAN-FD," *IEEE Transactions on Intelligent Transportation Systems* 2016

[2] Robert Bosch GmbH, Postfach 50, D-7000 Stuttgart 1, "CAN Specifications version 2.0," Mannual On controller area network 1991

[3] Kannan Thirugnanam, Student Member, IEEE, Ezhil Reena Joy T. P., Student Member, IEEE, Mukesh Singh, Student Member, IEEE, and Praveen Kumar, Member, "Mathematical Modelling of Li-Ion Battery Using Genetic Algorithm Approach for V2G Applications," *IEEE Transactions on Energy Conversion, Vol. 29, No. 2, June 2014*

[4] A. Hodjat and I. Verbauwhede, "Minimum area cost for a 30 to 70 Gbits/s AES processor," in *Proc. IEEE/VLSI Comput. Soc. Annu. Symp.*, 2004, pp. 83–88..

[5] Tata Motors Mannual," Gateway Requirements for TML CVBU/EV Platforms," *Version 1.1 TML, Pune*

[6] Tian, N.; Wang, Y.; Chen, J.; Fang, H,"On Parameter Identification of an Equivalent Circuit Model for Lithium-Ion Batteries," Mitsubishi Electric Research Laboratories TR2017-123 August 2017

[7] Coron, J. S. (2006), "What is cryptography? IEEE Security & Privacy Magazine," 70-73. Daemen, J., & Rijmen, V. (2002). The design of Rijndael. Springer, Berlin

[8] Mohammad Haris Shamsi, "Analysis of an electric Equivalent Circuit Model of a Li-Ion battery to develop algorithms for battery states estimation," UPPSALA UNIVERSITET MSc ET 16003Examensarbete 30 hp June 2016

[9] Li-ion Battery Aging Datasets | NASA Open Data Portaldata.nasa.gov › dataset › Li-ion-Battery-Aging-Datasets