International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 03 Issue: 04 | Apr-2016 www.irjet.net p-ISSN: 2395-0072

Improving the Security for In-Vehicle CAN using Hash Algorithm

K.NANDHINI[1], S.VASANTHI[2]

[1]PG scholar department of IT, Sona College of Technology,Tamilnadu,India.
nandhuakil93@gmail.com

[2]Associate professor department of IT, Sona College of Technology,Tamilnadu,India.

vasanthi_sv@yahoo.com

ABSTRACT- The modern vehicle is dependent on software to manage their functionalities. In automotive industry for updating and maintaining the in-vehicle of software process, it is a costly method. So to produce wireless communication to vehicles, vehicular to maintain many new applications to the vehicles. The vehicle contain an electronic control units and controller area network. An electronic control unit is used to control the electrical system of vehicle (ECU) and CAN is commonly used to build an efficient network of ECU. Unfortunately, some security issued are allowed in CAN, so whole in-vehicle network could be critical. In-vehicle networks connected to the external device, key management technique is used for secure communication between vehicle and external network using AES algorithm. In this paper, we improve a security protocol for in-vehicle CAN using MD5 algorithm which helps to communicate between vehicle and driver's smart phone. This MD5 algorithm is a one way hash function, which provides security to original message and message is more secured.

Key word: controller area network, key management technique, ECU, MD5 algorithm, in-vehicle network

1 INTRODUCTION

This survey paper present research in surveying the in-vehicle network of the connected car. It aim to highlight current research within the place, so that difference directions can be taken in the future.

Today's more functionalities are implemented in software. The modern vehicle have Electronic Control Units (ECU). It handles different tasks, such as mirror adjustment, engine control and anti-spin system. Vehicles have dependent on software, update is more important in vehicle's software and procedure to maintain the vehicle efficiency are important.

To apply modern IT technology to vehicles, so this technology to provide security for drivers as well as passengers[11]. Modern vehicle contain more number of automotive application components. These components ECU is most necessary component that controls one or more electrical system of the vehicles. Vehicular on board architecture can consist of different communication network such as local internet network, controller area network and so on.

The in-vehicle networks are represented by controller area network, CAN has de facto standard because it automatically decrease and number of communication lines and it secure data communication reliability[7]. In today's vehicle have lack of security issues are involved. By connecting the OBD2 scan tool, they were able to provide security issue commands while driving. Sometime these attacks are performed through the diagnostic interface, so far requires physical access to the vehicle we expert these attack will possible to wireless connection in a future version of a connected car.

Vehicular security have been achieved by European funded project (e.g., SELCOM, PRECLOSA, EVITA and so on)[8]. EVITA project is specifically developed proper solution for vehicular network and security requirement. It develop a secure connection environment among ECUs, but it does not provide a particular security architecture for a specific connection protocol.

In our existing method to provide the security between driver's smart phone and in-vehicle CAN. Here we can use key management technique for secure communication using AES algorithm. In this paper, we improve the security of in-vehicle CAN. Here we can use hash algorithm for secure communication, it is a one way hash function and it is irreversible method. So original message can't be retrieved from hash.

The rest of this paper is outlined as follows. Section II presents the related work within the area. In Section III, we give a background to the vehicle settings. Section IV presents the existing and proposed solution of this paper. The paper concludes with a discussion in Section V.

2. RELATED WORK

H.Schweppe et al[10] they proposed securing one-to-one as well as one-to-many communication between ECUs, and secure the honest of information and the in-vehicle data aggregation process of data sent to other vehicles. The car 2x communication is strongly faith in received data. The vehicular communication architecture has been designed for functional requirements, such as error recovery, low latency, and high capacity to electromagnetic interference. Our security solution instead ensures an open yet symmetric based trust between ECUs. Some Limitations are Wireless link is limited, Data cannot to multiple receivers, Security-configuration within the on-board network.

T. Hoppe et al[4] they proposed improvement of CAN to control system security, an algorithm for detection of malicious CAN messages is specified, and it has been implemented in the simulation environment of CANoe. The result shows that this algorithm has strong detection function and worth practice signification. CAN control systems have long been used in places like automobile, industrial automation, industrial equipment, aerospace, medical equipment, etc. In general protocols, hardware and software have been the dominant parts of CAN control systems. Features of CAN protocol and design an algorithm for detection of malicious CAN messages. Some Limitations are Error bit cannot destroy, Network problem is raised, Data length is limited.

B. Groza and S. Murvay[2] they proposed data authentication could be help to detect and recover from injection and alternative attacks in the in-vehicle network. Controller Area Network is a bus commonly used by controllers inside vehicles and in various industrial applications. Here we implement a broadcast authentication protocol based on key based and time synchronization, a commonly used method of wireless sensor networks, which allows us to take benefit from the use of symmetric primitives without need secret keys during broadcast.

D. K. Nilsson,et al[6] they proposed Modern vehicles contain an in-vehicle network contain more number of ECUs. These electronic control units are responsible for vehicle, including vehicle control. To date, no security features exist in this network. In upcoming trend among automobile manufacturers is to found a wireless connection to the vehicle to provide remote diagnostics and software update is more important. As a consequence, the in-vehicle network is open to external communication, and a potential entry point for attackers is present. Messages sent on the in-vehicle network lack integrity protection and data authentication; thus, the network is dangerous to injection and changing attacks. Some Limitations are No security for the data, Message transmit to node is delay.

3.BACKGROUND

3.1 Connected car

The connected car contain three domain

1. The vehicle consisting of in-vehicle network and ECUs
2. The portal provide various services of vehicle
3. Communication link to provide communicate with the vehicle and portal

The in-vehicle network can be divided into different sub category 1.controller area network (CAN) 2.local area network (LIN) and so on. In generally, a connected car vehicle is always connected to the external device.

3.2 Controller area network

Controller area network is used for communication purpose between different electronic devices such as gear control, engine management system, lighting control, air conditioning and so on. CAN to provide a mechanism for hardware and software by which various electronic modules can communicate with each other. Communication between different electronic modules which was first released by Robert Bosch in 1986. CAN is a multi-master serial bus that connected to the ECUs inside vehicle. CAN contain four types of frame

1. Data frame that is used for data transfer
2. Remote frame contain no data and it is used for request the data frame with the same identifier
3. Error frame that is used when an error is catches in the destination frame
4. Overload frame is node transmit it delay the next time data frame transmission

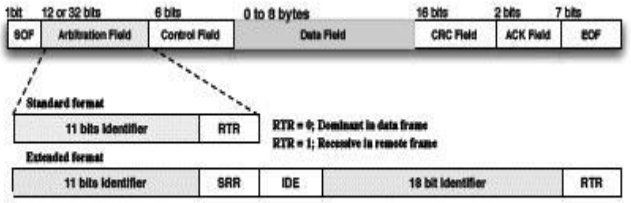


Figure 1: CAN frame format

CAN data frame contain 8 byte data field as shown fig 1: this frame format allows 11-bit identifier (ID) and extendent frame format allows 29-bit identifier. Since controller area network is a multi-master protocol, the priority of transmission is recover through bus contension called arbitration; a broadcasting process is one bit at a time and it is comparing with broadcast using other ECUs. CRC 16-bit field is provided to check the identity of each receiver frame.

3.3 Security features

In this chapter we present a number of security features proposed for in-vehicle network for communication purpose.

Nilsson et al [6] to propose the use of MAC data authentication in CAN communication and data integrity. Here to achive 128-bit key distribute with two communicating ECUs.

Wolf et al[12] to improve the security of communication by authentication and encryption. Each and every authentication can produce the certificate. Another authentication to receive the symmetric key that is shared between Driver's smartphone and in-vehicle CAN.

Chavez et al[1] to secure the CAN protocol. They are proposed to higher layer protocol, integrity could be enforced by hash algorithm, and the confidentiality could be enforced by RC4 algorithm of CAN data frames.

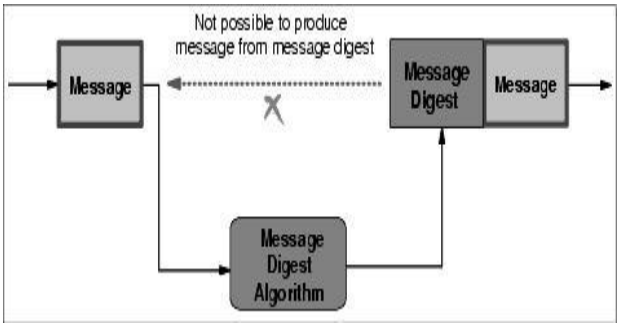
Confident-iality	Integrity	Authentication	Communi-cation	Timing
✓			–	Real-Time
	✓	✓	End-to-End	Delayed
✓		✓[1]	Group	Real-Time
✓	✓	✓	End-to-End	Real-Time
	✓	✓	Group	Delayed[2]

TABLE 1: Security features of communication

4.PROPOSED WORK

4.1 MD5 algorithm

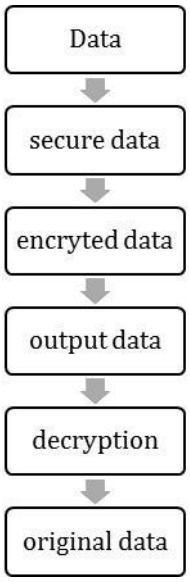
In this paper we can propose message digest algorithm 5 based on NS2, it widely used for cryptography hash algorithm. In this section we can compare AES and MD5 algorithm. Security mechanisms of the vehicle. This MD5 format as a 32 bit hexadecimal number. MD 5 algorithm is used commonly used to verify data integrity. Message digist algorithm is developed by Ronald Rivest of MIT in 1992. MD5 was like to be an in secure, MD5 is replaced by Rivest in 1991 for security purpose.



MD5 is a variable length message into s fixed length output of 128 bits. The input message is separated into 512 bits block (sixteen 32 bit words); the message is padded so that length is divisible by 512, the padding work as given below: first as single bit, 1 as depended on end of the message. This is followed by many zeros that are required to bring the length of the message up to 64 bit. Other bits are filled up to 64 bits, it is representing the original message modulo 2^{64}. The md5algorithm is a bit state, it is divide into four 32-bit words denoted A,B,C and D. the processing of a message block is consist of four similar stages, termed rounds. Each round is non-linear function F, modular addition, and left rotation. Each round is represented by XOR, AND, OR and NOT respectively.

FLOW DIAGRAM

Flow diagram describes how the security provided by the MD5 algorithm. MD5 is applied to the input data. MD5 to generate the secure data. Secure data is divided in two that are encrypted data and also provide the output user. User send this output data to receiver, then encrypted output data receiver applied the decryption technique to the original message.



Flow diagram of MD5

4.1.1 key generation

RC4 algorithm is used for key generation. RC4 is a symmetric stream cipher developed by Ron Rivest of RSA data security. This algorithm was trade secret of RSA but it was reverse engineered and published to internet in 1994. This algorithm is a pseudo random number generator with the output of PRNG being xored with the plaintext stream. In this paper, we can use multiple array list based on this technique. Here all the datas are processed using list based method. Pop the nth element off a list used in option processing.

4.1.2 Encryption

Message digist algorithm used for both encryption and decryption purpose only. Here MD5 is used for security purpose. It is a one way hash function, so can't get the original message.MD5 operates 128-bit state, divided into four 32-bit words and denote A,B,C and D. these are initialized to contain fixed constant. In this method, we can use some concept. First we can create and initialize the data

MD5 initialize:

First we create and initialize a MD5 state variable. This will be cleaned up when we call MD5 final.

MD5 update:

Hash function to maintain the array based technique. Here one or more data into the hash. We can passing the "ABC" is equivalent to passing these letters in a separate calls.

MD5 final:

It is used to close the current hash and returns the hash data.128-bits represented as binary data. Finally we can sent the message using encryption, so the message is securely sent to vehicle CAN.

4.1.3 Decryption

The message can securely receive from vehicle CAN. Here we can't get the original message, so it is more secure than AES algorithm. Finally we can compare the AES and MD5 algorithm, md5 is secure because it is a one way function, not easily get the original message. It is a irreversible method. So securely communicate between vehicle's smart phone and in-vehicle CAN. Here we can send text message from A, receiver can receive the message decrypted by B. The md5 algorithm is a bit state, it is divide into four 32-bit words denoted A,B,C and D. the processing of a message block is consist of four similar stages, termed rounds. Each round is non-linear function F, modular addition, and left rotation. Each round is represented by XOR, AND, OR and NOT respectively.

SIMULATION AND RESULT

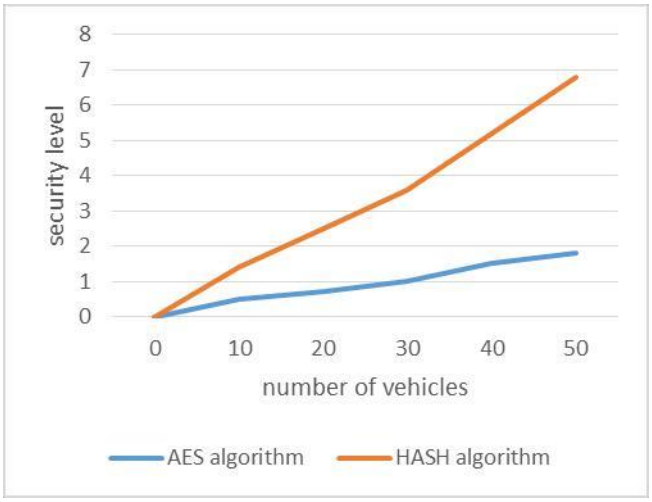


Figure 2: comparison of AES and MD5 algorithm

This figure2 we propose the security of in-vehicle CAN. Here number of vehicles are connected to the in-vehicle network. Here we can increase the security level using MD5 algorithm. We can compare AES and MD5 algorithm, finally MD5 algorithm is secured. MD5 is a one way hash function, can't get the original data. So it is a secure method of in-vehicle CAN.

V CONCLUSION

Routing is one of the most important parameter in inter-vehicle communication (IVC) and vehicles to infrastructure communications (V2I). Thus this paper has presented an

overview about the security protocols of vehicle CAN. In this paper also introduce the secure communication between driver's smart phone and in-vehicle CAN. We plan to improve the performance of the proposed security protocol with an implementation of the MD5 algorithms on software to optimize our security technology. Many new services are expected to be introduced in the vehicle and since the vehicle is safety-critical, it is vital that the vehicle is secured, so that these new services cannot violate with the safety and security mechanisms of the vehicle. Finally MD5 algorithm is best because AES is a symmetric key method. MD5 is a one way hash, can't easily get the original message.

REFERENCES

[1]M. L. Ch´avez, C. H. Rosete, and F. R. Henr´ıguez, "Achieving Confidentiality
Security Service for CAN," in Proc. of the 15th International Conference on Electronics, Communications and Computers, 2005. CONIELECOMP 2005.Feb. 2005.

[2]Groza and S. Murvay, "Efficient protocols for secure broadcast in controller area networks," IEEE Trans. Ind. Informa., vol. 9, no. 4, pp. 2034–2042, Nov. 2013.

[3].Göteborg, Sweden 2012" A Structured Approach to Securing the Connected Car" Division of Networks and Systems Department of Computer Science and Engineering.

[4]T. Hoppe, S. Kiltz, and J. Dittmann, "Security threats to automotive CAN networks—Practical examples and selected short-term countermeasures," Rel. Eng. Syst.

[5]S. Mangard, M. Aigner, and S.Dominikus, "A highly regular and scalable AES hardware architecture," IEEE Trans. Comput., vol. 52, no. 4, pp. 483–491, Apr. 2003.

[6]D. K. Nilsson,et al "Efficient in-vehicle delayed data authentication based on compound message authentication code"ieee transaction on intelligent system vol.16 2012.

[7]Pierre Kleberger, Tomas Olovsson, and Erland Jonsson" Security Aspects of the In-Vehicle Network in the Connected Car" 2011 IEEE Intelligent Vehicles Symposium (IV) Baden-Baden, Germany, June 5-9, 2011.

[8]Rakesh Kumar and Mayank Dave "A Review of Various VANET Data Dissemination Protocols" International Journal of u- and e- Service, Science and Technology Vol. 5, No. 3, September, 2012.

[9]Rukaiya Shaikh1, Disha Deotale2"A Survey on VANET Security using ECC, RSA & MD5"International Journal of Advanced Research in Computer and Communication EngineeringVol. 4, Issue 6, June 2015.

[10]H. Schweppe et al., "Securing Car2X applications with effective hardware software codesign for vehicular on-board networks,".Safety, vol. 96, no. 1, pp. 11–25, Jan. 2011.

[11]Samuel Woo, Hyo Jin Jo, and Dong Hoon Lee, Fellow, IEEE" A Practical Wireless Attack on the Connected Car and Security Protocol for In-Vehicle CAN" IEEE transactions on intelligent transportation systems, vol. 16, no. 2, april 2015.

[12]M. Wolf, A. Weimerskirch, and C. Paar, "Security in Automotive Bus Systems," in Workshop on Embedded IT-Security in Cars, Bochum, Germany, Nov. 2004.