Vehicle Diagnostics Over Internet Protocol and Over-the-Air Updates

**M. Kathiresh, R. Neelaveni, M. Adwin Benny,
and B. Jeffrin Samuel Moses**

Connected Cars

In the last two decades, the revolutionary progress in the field of automotive electronics and wireless technology and the ever-augmenting demands of the customers result in the automotive industry coming up with vehicles designed to sketch an incomparable driving experience from the traditional vehicles. By assisting this progress of meeting the demands of the clients like ensuring comfort, entertainment, connectivity, and other parameters during travel better than that of the pre-existing versions, cars of the recent times have truly taken the act of representing one's own individualism. Technologies like vehicle-to-vehicle communication (V2V) and vehicle-to-infrastructrue (V2I) communication, which enable communication between the automobiles and the environment through information exchange, not only come to aid in meeting the above said requirements but also enhance the user experience. This concept of vehicle interaction with the user and the surrounding environment is known as connected vehicles.

As shown in Fig. 1, the connected cars are automobiles that deploy several communication technologies to interact with the driver of the vehicle or with the other vehicles on the road or with the outside infrastructure. This vehicle interaction with the external world, resulting in the benefits of comfort, safety, connectivity, and entertainment, can be achieved using techniques like telematics, mechatronics, and artificial intelligence.

M. Kathiresh (✉) · R. Neelaveni
PSG College of Technology, Coimbatore, India

M. A. Benny
Infosys Limited, Bengaluru, India

B. J. S. Moses
Volvo Groups Private Limited, Bengaluru, India

M. Kathiresh, R. Neelaveni (eds.), *Automotive Embedded Systems*,
EAI/Springer Innovations in Communication and Computing,
https://doi.org/10.1007/978-3-030-59897-6_5

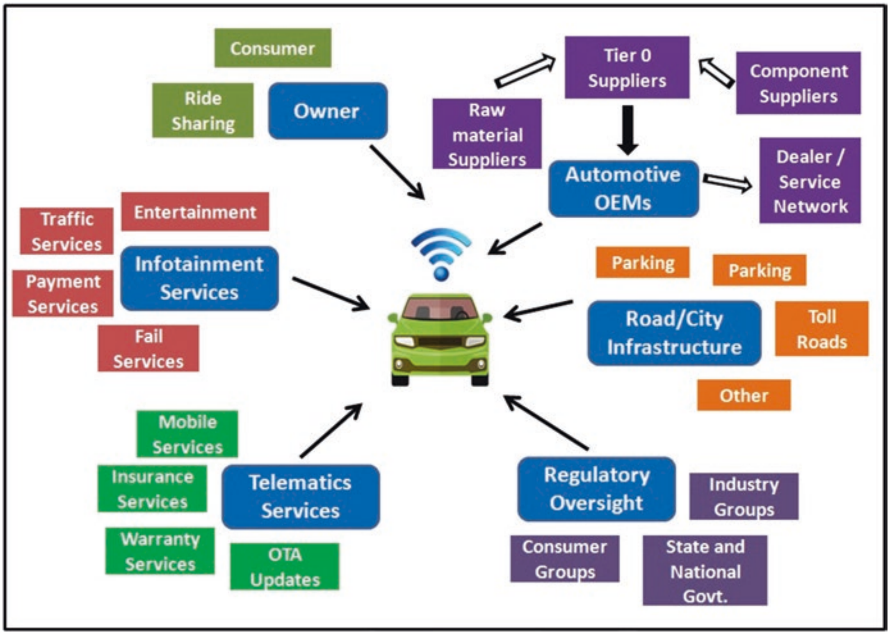

Fig. 1 Use cases of connected car technology

A typical connected car is built with intelligent features like muting the music on sensing the arrival of phone calls, so that the driver could indulge in without any disturbance; generating a signal of caution on the blockades or barricades or any obstructions that come in the way of the vehicle; stipulating information on an accident; providing the location of a nearby hospital or an emergency unit; transferring the vehicle status to the service providers enabling their access to remote monitoring; and many more additional features. Thus, cars of the recent times embedded with intelligence, enhanced versions of themselves with the aid of numerous sensors and actuators, have gained the ability to adapt themselves according to the current demands.

On-Board Diagnostics

From the earliest days of the commercial sale of the car, it has been obvious that maintenance and diagnosis are required to the proper working of the automobile. Until the primary 1970s, an honest deal of the routine maintenance and repair was done by car owners themselves, using inexpensive tools and equipment. Car owners cannot, as a matter in any case, do their own maintenance and repairs on certain automotive subsystems (particularly the engine). In fact, the quality shop manual used for years by technicians for repairing cars is rapidly becoming obsolete and is

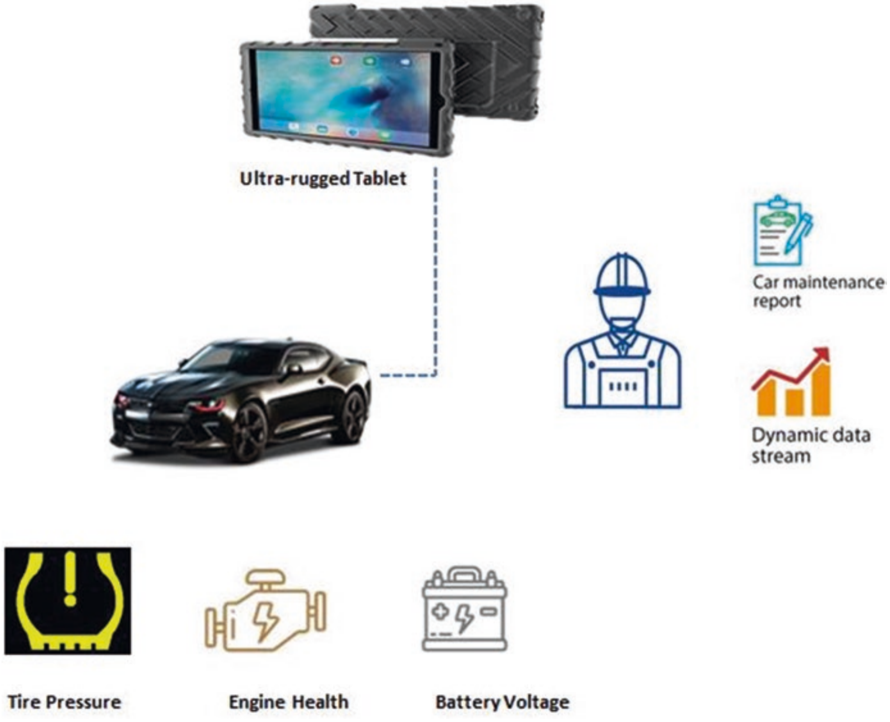

Fig. 2 Conventional vehicle diagnostics

being replaced by electronic technician aids. In the past two decades, the concept of on-board diagnostics (OBD) is used in vehicles. The OBD system has a malfunction indicator light present in the dashboard of the car to indicate any failure in vehicle parameters. The status of the vehicle is determined through various sensors, and in case of any issues, a unique code called Diagnostic Trouble Codes (DTC) is stored in the memory and later recovered by the technician using the scan tool to identify the cause of failure. Each of the DTCs has a letter and three numbers associated with it. The first letter is used to indicate the system related to the error, for example, “P” stands for powertrain which covers functions that include engine, transmission, and associated drivetrain accessories. “U” codes for network and vehicle integration which covers functions that are shared among computers and systems on the vehicle, etc. The numbers are manufacturer specific. The process of conventional vehicle diagnostics is shown in Fig. 2.

Diagnostics Over Internet Protocol (DoIP)

Even though the on-board diagnostics are useful to detect the errors, it requires the physical presence of the vehicle at the service center. The repair technicians can start the diagnostic analysis, only if the vehicle arrives at the workshop. The process performed by the repair technician to carry out analysis of the state of vehicle and fix the issues is very time-consuming. This in turn makes the vehicle owner inconvenienced. The remedy to these problems is to perform vehicle diagnostics remotely using the Internet. This reduces the overall downtime of the vehicle owner to fix the issues in the vehicle.

DoIP facilitates obtaining the data trouble codes and other status parameters from a vehicle remotely with the gateway module present inside automobiles [1, 2]. Using the gathered diagnostic information, the service person can do the major part of the repair work well in advance before bringing the vehicle to the service center. This helps the process of fixing the problems very quickly as the service technician can start the work immediately on getting the vehicle to the service center. DoIP can be used to continuously monitor the status of a vehicle to detect the faults present in it. This reduces the time for the detection of issues as well as the cost for the OEMs and also reduces the need to visit the service center. The process of conventional vehicle diagnostics is shown in Fig. 3.

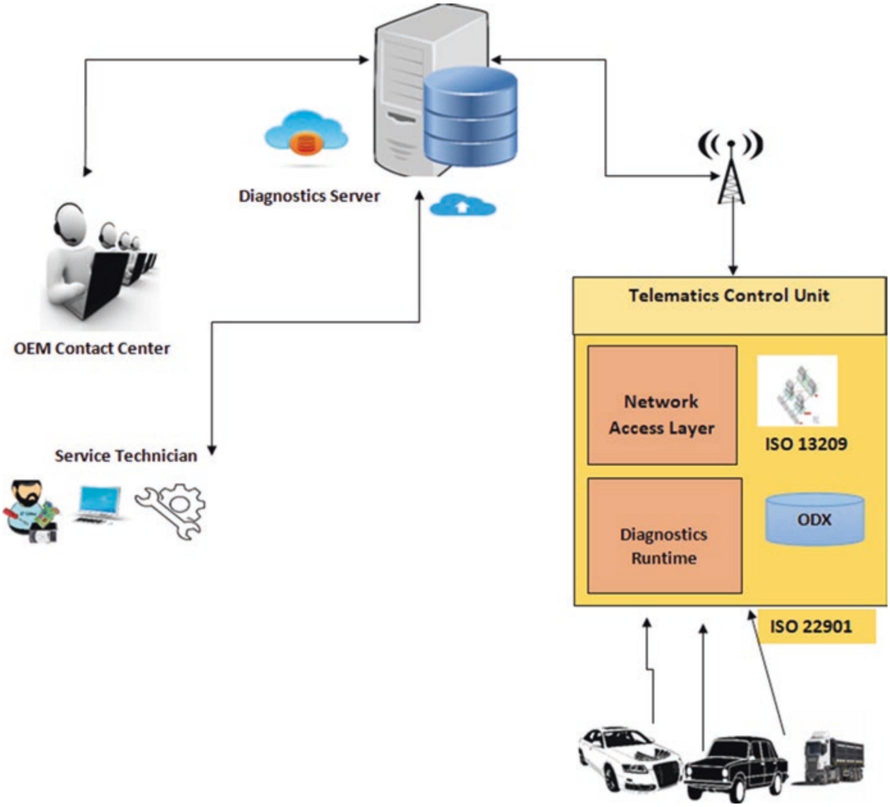

Fig. 3 Vehicle diagnostics over Internet protocol

Software Architecture in Automotive Electronic Control Units

The aspects of safety and comfort of the drivers are the important parameters under consideration. In order to ensure the appropriate levels of these parameters, numerous dedicated ECUs for anti-lock braking and engine management are deployed in today's cars. Sophisticated software application determines the overall functions that a typical ECU handles in a vehicle. Thus, the software of an ECU plays a vital role in determining the function of the system and facilitating installation of the software with the help of Gateway ECU present in vehicles. As shown in Fig. 4, the program memory for every ECU has two sections, namely, Bootloader and Application Area. The application section contains the programs which determine the tasks that the ECU needs to perform. On reset of ECU, the bootloader module executes, and the processor starts executing the application program. A bootloader module has got the following software components:

- Initialization module for hardware after power-ON and reset of the ECU
- Data download manager that facilitates programming flash memory blocks
- Unified Diagnostic Services (UDS) protocol stack for communication between the Target ECU and Gateway ECU
- Data Decryption Module based on a cryptography algorithm as an optional feature
- Data Decompression Module
- Application Layer

Functional domains in automobiles like powertrain, vehicle safety, infotainment, and chassis have many Electronic Control Units. Depending on the speed of data transfer required, different networking protocols like FlexRay, Media Oriented Systems Transport (MOST), Fast Controller Area Network (CAN), Local Interconnect Network (LIN), etc. are used to interconnect various ECUs. The Telematics Control Unit of a vehicle usually acts as a Gateway that facilitates interaction with external infrastructure and interactions among other ECUs.

Over-the-Air Updates

As there is a large number of Electronic Control Units present in a vehicle, the size of software application in a modern luxury vehicle can go beyond 100 million lines of program. It is quite obvious that the process of maintaining and updating such a complex software application for several thousand vehicles which are in production and millions which are in use is a tedious task. As shown in Fig. 5, in the conventional way of software update, the improvisations to the vehicles with the current software are provided by recalling them to the dealership either for the rectification of any problems in the software or in the circumstances of the addition of new features to the software, in order to enhance the performance of the vehicles. This

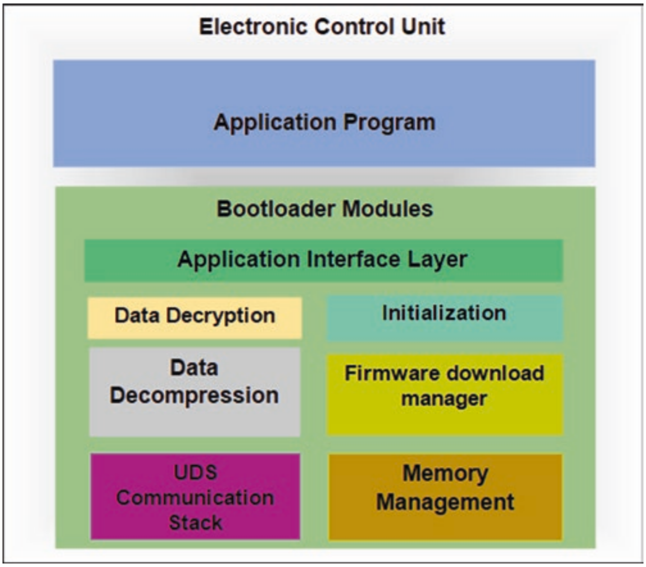

Fig. 4 Software architecture of an electronic control unit in vehicles

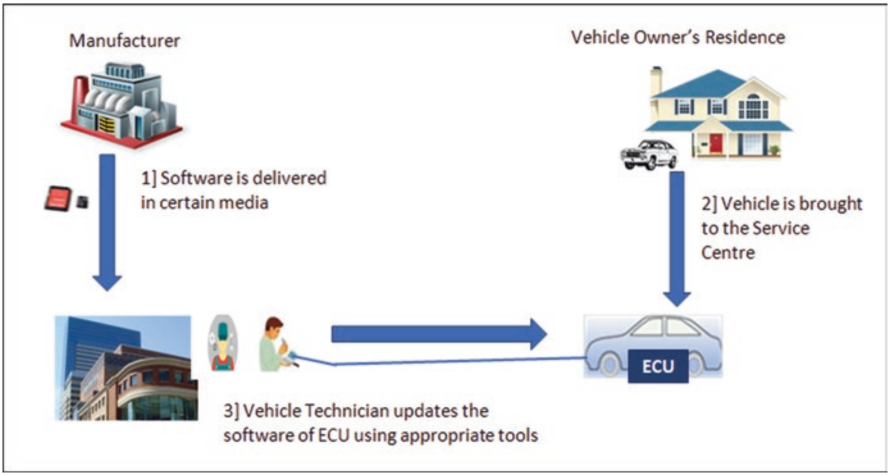
Manufacturer
Vehicle Owner's Residence
1] Software is delivered in certain media
2] Vehicle is brought to the Service Centre
ECU
3] Vehicle Technician updates the software of ECU using appropriate tools

Fig. 5 Conventional Software Update Process for Automotive ECUs

process which demands the time and energy of the user may incur losses to the OEM gradually resulting in their downfall. So to prevent this, over-the-air update which enables the automatic update of the firmware of the ECUs emerges as a solution. Besides that, it also is an error-free and a faster mechanism that aids both programming and updating a car's firmware within its life cycle.

Over-the-air software updates refer to the practice of remotely updating the code on an embedded device [3]. The embedded hardware must be built with OTA functionality for this mechanism to work. As of now, OTA is a well-established concept for cellular phones, and its application to the automotive domain helps to handle sophisticated automotive systems. OTA uses a wireless medium to establish communication between OTA software server situated in the cloud and the telematics unit of a vehicle which acts a client. With the help of OTA process, it is possible to update software of vehicle ECUs at any location whether it is an assembly shop, location of a dealer, a service station, or the owner's parking area. It also does this software download as a background activity even when the vehicle is running, and once the download is done, it tells the service person or the user that it is ready for the installation of the updated software.

Figure 6 illustrates the process of updating the software in a typical vehicle ECU. OTA implementation is a three-step process as follows:

- Development of software updates to enhance the features of the automobile and storage of the newly developed software update files in the cloud database servers which is accessible to all the stakeholders
- Downloading of the newly received software update file into the memory module present in the Telematics Control Unit through the Internet
- Installation of the software update in vehicle ECUs

OTA is a collaborative process which requires participation from various stakeholders to give lifetime support to automobiles. The major stakeholders in the process of OTA are as follows:

- Tier 1 and Tier 2 suppliers who are responsible for development and supply of various automotive components
- The dealers who are responsible for the sales of vehicles
- Service stations for fixing faults and doing maintenance of vehicles

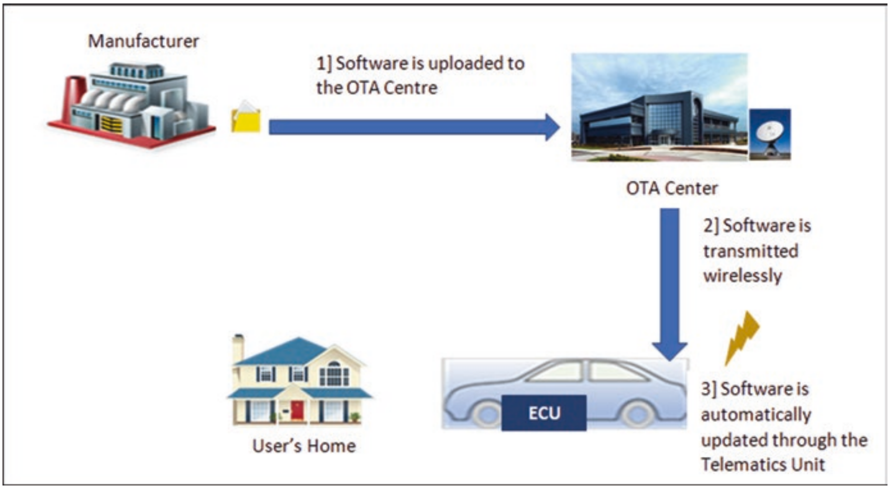
Manufacturer
1] Software is uploaded to the OTA Centre
OTA Center
2] Software is transmitted wirelessly
User's Home
ECU
3] Software is automatically updated through the Telematics Unit

Fig. 6 Over-the-air software update process in automotive ECUs

- Owners of vehicles

Is the Process of DoIP and OTA Safe?

Anyone with a wireless communication interface can intercept critical data, which is a threat resulting due to the addition of these new features in the name of providing comfort to the users. This critical data when fallen into the wrong hands can be misused, thereby posing a potential threat. The resulting possibilities are that one can get hold of the code flashed into the ECU; tap into the vehicle's OBD interface; and potentially alter the transmitted code illicitly. By doing so, they can gain control over the car and cause catastrophes harming lives and the environment [4]. Therefore, it is significantly important enough to ensure the confidentiality, integrity, and authenticity of the data during the process of sharing over DoIP and OTA.

AUTomotive Open System Architecture (AUTOSAR) is an open community that provides software standards for automotive applications. For securing over-the-air updates, AUTOSAR suggests cryptographic algorithms [5]. Any cryptographic standard is considered vulnerable to brute force attacks. Cryptography alone will not be able to provide data security at the highest level; therefore an improved data security method which involves a combination of both cryptography and steganography is preferred to provide maximum security for over-the-air updates in automobiles [6].

The following are the preferred data security mechanisms that can be used to have reliable and safe vehicle diagnostics and software update through the Internet.

Cryptography

Cryptography is the art of encrypting sensitive information. Cryptography is based on mathematical theory and computer science practice. Cryptographic algorithms are designed with computational hardness assumptions, making such algorithms hard to break. Cryptography basically requires two steps: encryption and decryption. The encryption process uses a cipher in order to encrypt plaintext and turn it into cipher text. Decryption applies that same cipher to turn the cipher text back into plaintext. Cryptography is the development and creation of the mathematical algorithms used to encrypt and decrypt messages, and cryptanalysis is the science of analyzing and breaking encryption schemes. Cryptology is the term referring to the broad study of secret writing and bounds both cryptography and cryptanalysis.

There are five primary functions of cryptography:

- *Privacy/confidentiality*: Ensuring that no one can read the message except the intended receiver
- *Authentication*: The process of proving one's identity

- *Integrity*: Assuring the receiver that the received message has not been altered in any way from the original
- *Non-repudiation*: A mechanism to prove that the sender really sent this message
- *Key exchange*: The method by which crypto keys are shared between the sender and receiver

There are several ways of classifying cryptographic algorithms. They are categorized based on the number of keys that are employed for encryption and decryption and further defined by their application [7]:

- *Private key cryptography*: Private key cryptography or symmetric cryptography is the form of cryptography where only a single private key is used to encrypt and decrypt information as shown in Fig. 7. Using one common key creates a key management issue. It is possible that the private key may be stolen or leaked. Key management involves prevention of these risks by changing the encryption key often and appropriately distributing the key. Private key cryptography schemes are generally categorized as either stream ciphers or block ciphers. The most widely used private key cryptographic algorithms are Advanced Encryption Standard, Rivest Ciphers (RC1, RC2, RC3, RC4, RC5, and RC6), Data Encryption Standard, Twofish, Blowfish, and ChaCha.
- *Public key cryptography*: Public key cryptography or asymmetric cryptography is an encryption scheme that uses two mathematically related, but not identical keys—a public key and private key for encryption and decryption process. As shown in Fig. 8, the public key is used to encrypt, and the private key is used to decrypt. It is computationally infeasible to compute the private key based on the public key because of the one-way functions. Using this property the public key is shared freely, thereby facilitating the users to have easy and convenient encryption methods. Private keys have to be kept secret to ensure that only the owners of the private keys can decrypt the cipher text.

Public key cryptography ensures both confidentiality and integration of the original message. The one-way function can be realized using multiplication and factorization or by using exponentiation and logarithms. The ease of multiplication and exponentiation versus the relative difficulty of factoring and calculating logarithms,

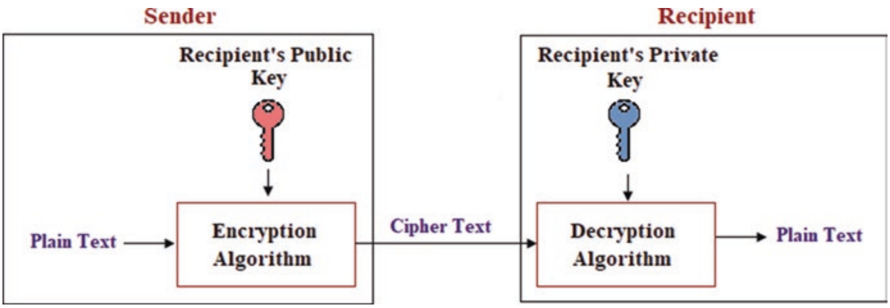

Fig. 7 Private key cryptography

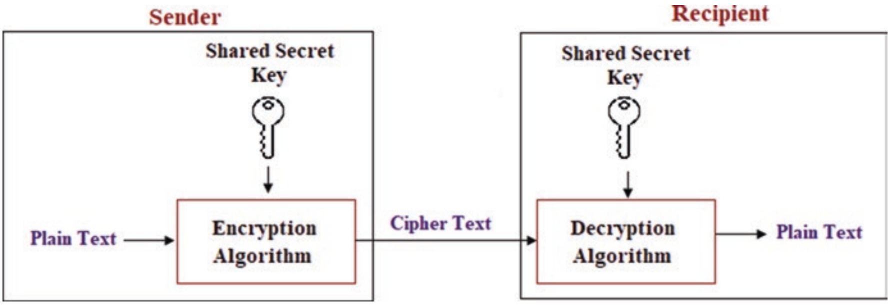

Fig. 8 Public key cryptography

respectively, create the one-way functions. The mathematical infeasibility in public key cryptography is brought by using a trapdoor in the one-way function so that the inverse calculation becomes easy with some prior information. Since public key cryptography is mathematically linked, the key generation process can be done locally at the receiver end. The most widely used public key cryptographic algorithms are Ronald Rivest, Adi Shamir, and Leonard Adleman (RSA) algorithm, Digital Signature Algorithm (DSA), Diffie-Hellman key exchange, ElGamal encryption, and Elliptic Curve Cryptography (ECC). Each of these algorithms has their own pros and cons; based on the application, a suitable algorithm is implemented for the cryptosystem.

Digital Signatures

A digital signature is the public key message authentication within the physical world. It is common to use handwritten signatures on handwritten or typed messages. They are wont to bind signatory to the message. Similarly, a digital signature could be a technique that binds an entity to the digital data. This binding will be independently verified by the receiver additionally as any third party. Digital signatures could be a cryptographic value that is calculated from the information and a secret key known only by the signer. The receiver of the messages needs assurance that the message received is the original message sent by the sender. This requirement is extremely crucial in business applications, since the likelihood of a dispute over exchanged data is extremely high. The most commonly used digital signature algorithms are RSA, ElGamal, DSA, ECDSA, EdDSA, Schnorr signature algorithm, and rapid digital signature. Each of these algorithms has their own pros and cons, based on the application.

Hash Functions

Hash functions use no key for encryption. Instead, a fixed-length hash value is computed based upon the plaintext that makes it impossible to retrieve the contents or length of the plaintext from the message digest. Hash algorithms are typically used to provide a digital fingerprint of a file's contents. Hash algorithms ensure integrity of the encrypted file. Hash functions are also commonly employed by many operating systems to encrypt passwords. Since hash functions produce a fixed-length value, there are a finite number of hashes for each type of algorithm. This makes collisions possible. A collision occurs when two different data (plaintext) produce the exact same hash. It's extremely rare for this to happen, but older hashing algorithms have encountered this problem. To overcome this problem, the hash value size has been increased for the same hashing algorithms. Some of the widely used hash algorithms are Message Digest (MD) algorithm which has different version like MD4 and MD5 with variable hash length, Secure Hash Algorithm (SHA), RACE Integrity Primitives Evaluation (RIPEMD), and Whirlpool.

Steganography

Steganography is the process of hiding secret data inside an ordinary, non-secret file or message to avoid detection [8]. Steganography can be used to conceal almost any type of digital content, including text, image, video, or audio content. The content to be concealed through steganography is often encrypted before being incorporated into the cover file. The use of steganography can be combined with encryption as an extra step for hiding or protecting data. Steganography is generally used to convey a secret message or code. There are many legitimate uses for steganography, but malware developers have also been using steganography to obscure the transmission of malicious code. Image steganography is the most commonly used steganography method to embed the secret data. In image steganography, the input message is inserted into the cover medium using special algorithms. Based upon the domain type, image steganography techniques are classified as spatial domain and transform domain techniques.

Summary

Tremendous growth in the field of automotive electronics, wireless communication, and information technology has made the processes of diagnostics over Internet protocol and software update over the Internet possible. As these processes use the Internet, an unreliable channel for information exchange, this involves lots of risks in terms of security of the data. AUTOSAR specifies cryptographic algorithms to have secured data transmission in automotive applications. It is also true that the cryptographic algorithms when combined with the art of steganography provide an additional security for the data being over the Internet during the process of DoIP and OTA.

References

1. M. Johanson, P. Dahle, A. Söderberg, Remote vehicle diagnostics over the Internet using the DoIP protocol, in *Proceedings of the Sixth International Conference on Systems and Networks Communications*, (IARIA, Barcelona, Spain, 2011), pp. 226–231
2. J. Lee, E. Lee, S. Park, Extended communication interface for remote vehicle diagnosis using Internet protocol, in *Proceedings of the 19th Asia-Pacific Conference on Communications (APCC)*, (Denpasar, 2013), pp. 421–426
3. M. Shavit, A. Gryc, R. Miucic, Firmware update over the air (FOTA) for automotive industry. SAE Technical Paper, in *Proc. of Asia Pacific Automotive Engineering Conference*, vol. 14, (2007)
4. H. Yu, C.-W. Lin, Security concerns for automotive communication and software architecture, in *Proceedings of IEEE Conference on Computer Communications Workshops*, (San Francisco, CA, 2016), pp. 600–603
5. AUTOSAR. Specification of crypto interface for adaptive platform AUTOSAR AP release 17-10. Document ID 883, October 27 (2017)
6. K. Mayilsamy, N. Ramachandran, V.S. Raj, An integrated approach for data security in vehicle diagnostics over IP and software update over the air. Comp. Elect. Eng. **71**, 578–593 (2018)
7. N.B.F. Silva, D.F. Pigatto, P.S. Martins, K.R.L.J.C. Branco, Case studies of performance evaluation of asymmetric and symmetric cryptographic algorithms for embedded systems. J. Netw. Comp. Appl. **60**, 130–143 (2016)
8. M. Hussain, A.W.A. Wahab, N.B. Anuar, R. Salleh, R.M. Noor, Pixel value differencing steganography techniques: Analysis and open challenge, in *Proc. of IEEE International Conference on Consumer Electronics-Taiwan (ICCE-TW)*, (2015), pp. 978–979