AES Security Protocol Implementation for Automobile Remote Keyless System

[1]*BAKDEVI SARANGI, Gandhi Institute of Excellent Technocrats, Bhubaneswar, India*

[2]*SNIGDHARANI DASH, Gurukula Institute of Technology, Bhubaneswar, Odisha, India*

***Abstract*—The remote keyless system is widely used in automobile industry to lock or unlock the automobile's door, trunk, and start the ignition. It comprises a handheld key fob to be held by the driver and a set of radio transceiver devices located in the automobile. Operation commands are represented by strings of wireless signal transmitted between the key fob and the radio transceiver to realize various car operations. Because the radio signal is transmitted in proximity of open area, the remote keyless system has the possibility of exposing the key secret commands to a car thief. The operation commands which are denoted by plaintexts or even cipher texts cannot overcome this security problem. This paper proposes a new approach in which encryption of the operation commands is realized by a model of AES algorithm computed with a fixed key and a variable key. In the newly designed AES security protocol, the key fob and radio device will be engaged in the protocol interrogation after the key fob initiates a connection. The fixed key can be defined by car manufacturer or car dealer, and it is used for the encryption of handshake message and a pseudo random number (PRN). This PRN is proposed by the key fob, and will serve as the variable key. This method can effectively defeat today's common attack tricks such as brute-force key guess attack, statistics attack, masquerade attack, etc.**

Keywords-AES security algorithm; encryption (decryption) key; remote keyless system

I. INTRODUCTION

The remote keyless system is widely used to remotely perform operations such as locking or unlocking an automobile's door, trunk or glove compartment, starting the ignition, etc. It duplicates the features of a car key with added operating convenience that allows the car owner to manipulate the key operations at a distance. A remote keyless system can include both a remote keyless entry system (RKE) and a remote keyless ignition system (RKI). It consists of a handheld radio key fob which is attached on a keychain and a radio transceiver which is located at the automobile. This system works on the principle of sending pulses of radio frequency energy between the key fob and the automobile on a particular frequency. These pulses are then received and interpreted by the transceiver in the automobile, which in turn performs the appropriate function.

Since the radio signal is transmitted in a proximity open area around the automobile, security is a very critical concern. Car thief can use an inexpensive radio scanner to receive theradio signal between the automoile and key fob. A tech-savvy car thief can then analyze the intercepted radio pattern and deduce certain security characteristics to crack the remote keyless system. Conventionally, the remote keyless system works on a relatively straightforward way in which the settings of a DIP switch component in a circuitry specify the intended communication source and target. Typically, there is no cryptographic measure taken. The car thief can simply intercept the radio pattern, and then masquerade as the car owner to spoof the car receiver. This kind of the remote keyless system provides a poor security capability to the automobile.

The Texas Instruments (TI) has designed a Digital Signature Transponder (DST) tag [1] which is cryptographically enabled and has Advanced Encryption Standard (AES) [2] encryption deployed with a 40-bit-length cryptographic key. This tag is applied in the automobile immobilizer system. A DST sends a 24-bit factory-set identifier, and then authenticates itself by engaging in a challenge-response protocol. The reader initiates the protocol by sending a 40-bit challenge. The DST encrypts this challenge under its key and returns a 24-bit response. Therefore, it is the secrecy of the key that ultimately protects the DST against cloning and simulation. However, a 40-bit key is relatively short according to today's cryptographic standard, and is vulnerable to brute-force key guessing attack. Steve Bono, M. Green, et al., claim they have cracked the DST by observing DST responses when presented with a large amount of specially chosen challenges [3]. In addition, a fixed key algorithm is easily attacked by an eavesdrop-and-masquerade attack because the radio pattern is always consistent with respect to time, especially for the automobile remote keyless system which has a relatively small set of radio patterns.

This paper proposes a new wireless protocol, named AES Security Protocol (ASP), which has an enhanced security mechanism for the remote keyless system. It uses AES cryptographic algorithm with fixed key and variable key combined model. Both the fixed and the variable key are 124bit-length, and should be long enough to defeat current commonly-seen attacks such as statistics and brute-force attack. The fixed key encryption is used for protection of handshake message and distribution of a pseudo random number produced by the key fob after the handshake is confirmed. PRN will act as the variable key after both the car transceiver and the key fob are key-synchronized. Since cipher texts encrypted from a message by the variable keys are different in every time of operation, this model can effectively defend it from a masquerade attack.

II. THE ADVANCED ENCRYPTION STANDARD IN BRIEF

The Advanced Encryption Standard (AES) is a block cipher encryption standard. It is derived from the Data Encryption Standard (DES). AES algorithm requires small memory and can be easily implemented in both software and hardware platform. It is also fast to execute.

With every time of encryption or decryption, AES operates on a 4×4 square matrix of bytes, termed the state (shown in Fig. 1). In Fig.1, every cell represents one byte in the state.

S0	S4	S8	S12
S1	S5	S9	S13
S2	S6	S10	S14
S3	S7	S11	S15

igure 1. AES Data Structure

Thus, the whole state is a 128-bit block. The AES key is also 128-bit long. The states will be computed and modified at four stages during the process of encryption and decryption. The four stages are called Add_Round_Key, Substitute_Bytes, Shift_Rows and Mix_Columns.

In Add_Round_Key stage, the 128 bits of state are straightforwardly XORed with the 128 bits of round key. The round key is a kind of transformation of the cipher key.

Substitute_Bytes stage is the modification of byte replacement. AES defines a 16x16 matrix of byte, which is called S-box. The S-box contains all possible 256 8-bit values. Every byte in the AES state will be replaced by a byte in the Sbox according to the following mapping way: The leftmost of 4-bit value of each state cell serves as row reference index to the S-box, and the rightmost 4-bit value of that state cell serves as column reference index to the S-box. The selected byte of the S-box replaces the byte of the state cell.

The Shift_Rows transformation stage is a row level shift operation in which the first row of state is not modified. For the second row, a 1-byte circular left shift is performed. According to the same way, a 2-byte circular left shift and a 3-byte circular left shift are performed to the second and the third row respectively.

Contrary to the Shift_Rows transformation, Mix_Columns is a column operation. In the Mix_Columns stage, each byte of a column is replaced by a new value which is a function of all four bytes in the same column. The function is depicted in Equation 1, where S is the original value, and S' represents a new value which is used to replace the original value.

□02 03 01 01□ □S0.0 S0.1 S0.2 S0.3□ □S'0.0 S'0.1 S'0.2 S'0.3□
□ □ □ □ □

□01 02 03 01□×□□SS12..00 SS12..11 SS12..22 SS12..33□□□=□□□SS"12..00 SS"12..11 SS"12..22 SS"12..33□□□

□01 01 02 03□

□ □ □
□□03 01 01 02□□ □□S3.0 S3.1 S3.2 S3.3□□ □□S'3.0 S'3.1 S'3.2 S'3.3□□

(1)

Fig.2. depicts the AES encryption and decryption process. Encryption (decryption) runs through 10 rounds of state computation and modification. Each round includes four stages mentioned above, except the tenth round. Finally, the result of the state is copied out and served as the output matrix.

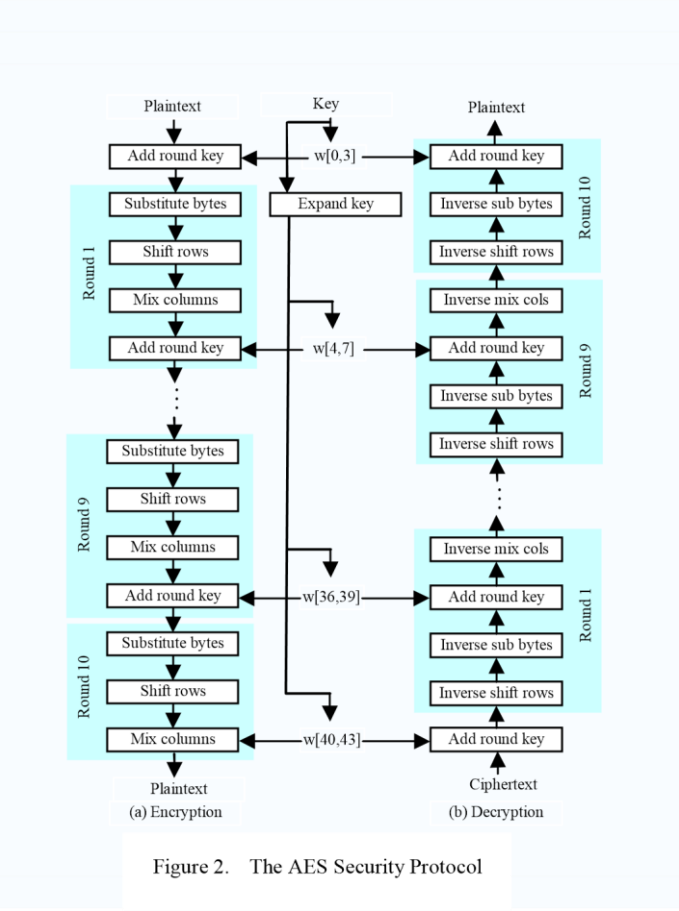

Figure 2. The AES Security Protocol

III. AESSECURITY PROTOCOL

A.ASP Sequence

As the wireless medium for transmitting signal is not reliable and data loss is common, ASP adopts a connectionoriented communication style, i.e. after sending out a packet, the sender will not send another packet until a positive response for the previous packet is received. If a negative response is received, the sender will send the previous packet again. The connection-oriented communication increases transmitting reliability at the cost of more overhead data transferring.

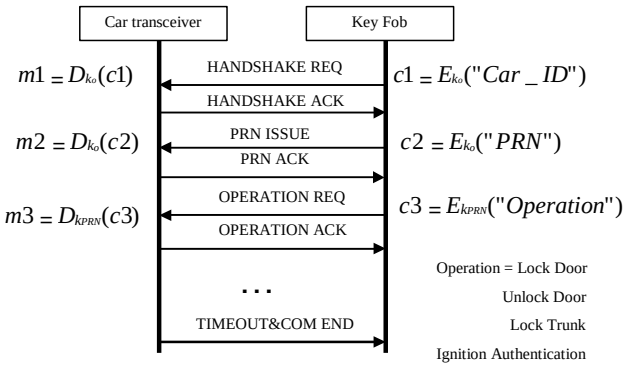

Figure 3. The AES Security Protocol

In ASP, AES is introduced to serve as cryptographic algorithm. In a complete round of protocol interrogation, the cryptographical procedure is divided into two stages which feature a fixed key encryption at the early stage and a variable key encryption at the late stage respectively. The 128-bitlength fixed key is set in both the car transceiver and the key fob by the automobile dealer or the car manufacturer. It varies with different cars. In order to enhance the protection capability to prevent masquerade attack, a 128-bit-length pseudo random number is created by the key fob and distributed to the car transceiver to work as the variable key later on.

The ASP sequence is illustrated in Fig.3. Firstly, the key fob sends a handshake request to the car transceiver. Equation $c1 = E_{ko}("Car\ \_\ ID")$ means cipher text c1 is the result of encryption calculation performed on the car ID with the original fixed key ko. Equation $m1 = D_{ko}(c1)$ means plain message m1 is the function of the decryption calculation performed on c1 with the key ko. Obviously m1 is the car ID. After the car ID is authenticated, the car transceiver sends a positive acknowledgement to the key fob. All the acknowledgement messages are in plaintext form. The key fob then creates a 128-bit-length pseudo random number and encrypts it with ko. This process is denoted by the equation $c2 = E_{ko}("PRN")$. If the car transceiver correctly receives and decrypts c2, it sends out an acknowledgement packet. When the car fob receives this acknowledgement, PRN working as the variable key in both the car transceiver and the key fob will be synchronized. Thereafter the protocol steps into an operation iteration which includes commands: “unlock (or lock) door”, “open trunk”, “authenticate immobilizer”, etc. Equation $c3 = E_{kPRN}("Operation")$ means the operation is encrypted by the variable key k_{PRN}. The number of operations is optional, but a specified timeout counter is set for counting time elapse from the point of the last operation. The key fob will issue a disconnection command after the timeout counter is expired.

B.Date Link layer

ASP’s data link layer, in particular, provides sufficient information to describe how the key fob and the car transceiver should implement the data transmission mechanism in order to provide reliable communications of data. The packet structure is shown in Fig.4.

Length	Car ID	Direction	Type	Command	Data	Checksum

Figure 4. ASP Packet Structure

where

- Length - Total number of bytes in a packet.
- Car ID - The car unique ID.
- Direction – There are two possibilities. Packet is sent from the key fob (0x00). Packet is sent from the car transceiver (0x01).
- Type - Command type: commands are categorized into Request (0x00) and Acknowledgment (0x01).
- Command - Command codes which are defined as: Handshake (0x00), PRN Issue (0x01), Car Operation option (0x02), Disconnection (0x03).
- Data – Its contents may vary depending on command type. For example, in the case of command “handshake”, there is no such field in the request packet. However, in its response packet, there is one byte which is 0x00 to mean positive acknowledgment and 0x01 to mean negative acknowledgment. For command “Operation request”, this field is filled with a door operation option in request packet, and a positive (or negative) acknowledgment in the response packet respectively. In the case of pseudo random number issue, the data field is the 128 bits pseudo random number in the issuing packet, and the same acknowledgment byte as in the handshake case in the response packet.
- Checksum – CRC16

The ASP packet will be encrypted with the right cipher key in transmission except the fields Length and Checksum. During the connection stage, if a radio device (could be either the key fob or the car transceiver) receives a packet, it first checks the packet’s checksum. If successful, it then decrypts the cipher text and compares the car ID. If the car ID is its own, it will perform the operations according to the fields of the packet.

C.ASP State Machine

In ASP, 3 states are defined for the radio devices. As shown in Fig.5, it consists of the Disconnected State, PRN Distribution State and Door Operation State. The later two pertain to connected state category. One state can transfer to another state if a pre-specified positive acknowledgement packet is received. For example, when the key fob receives the positive acknowledgement of handshake request, the key fob shifts into the PRN Distribution State. In order to avoid cases in which the communication accidentally breaks out, timers are defined for the two connected states to guarantee them returning back to the Disconnected State after the timer expires.

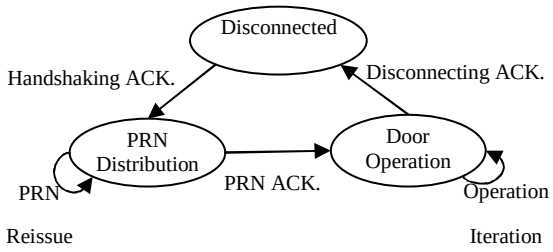

Figure 5. ASP State Machine

D.Security Analysis

One of the most important principles in cryptographic design is that the security of a system should be based on the secrecy of the keys, not on the secrecy of the algorithm and the encryption procedures. Car thief intercepts the cipher and the plain messages transmitted between the car and the key fob in the close proximity, and then use these messages to try to deduce the cryptographic key or simulate the message. Typically a car thief cracks the automobile keyless system by three attack methods: brute-force key guessing attack, statistics attack, and masquerade attack.

1)Brute-force key guessing attack

With the brute-force key guessing attack, the method to guess the key is by continuously trying to send a large amount of different key-encrypted-ciphers until the system gives an appropriate response, and thus the secret key is reached. In ASP, the variable key is a pseudo random number and it differs with each time of operation. Thus, only guessing the fixed key for the attacker is meaningful. But the fixed key has 128-bitlength with which gives $2^{128} \approx 3.4\times e^{38}$ possible variants. Such a large number actually makes the attack impossible.

2)Statistics attack

The statistics attack is the way that a few words of cipher texts and their corresponding plain texts are presumed to be known. The attacker analyzes the relationship between them and finally concludes out the secret key. The more texts known, the more likelihood the key will be cracked. ASP has only the car ID encrypted by the fixed key. Even though the attacker is assumed to know the car ID and its cipher, it is unlikely to deduce the key just from this single plain-cipher text pair.

3)Masquerade attack

The masquerade attack is the way that the car thief intercepts the wireless signals which are sent from the car owner to accomplish the car door operations. The car thief does not try to analyze these signal patterns to reach the plaintext; rather, he will pretend to be the car owner to gain access to the car. Obviously the variable key is effective to defeat the masquerade attack because its value is only valid for that time of operation, and not correlated with the next time.

E.Hardware Implementation

In the hardware design, there are several factors to take into consideration such as lifespan of the key fob's battery, key fob size, system cost, customer-acceptable protocol execution time, radio coverage range, etc.

We adopt a low-cost 8-bit ATMega128L microprocessor and CC2420 RF transceiver chip for both the car transceiver and the key fob. The two components are typically used in Wireless Sensor Network (WSN) [4]. ATMega128L operates on 7.37MHz frequency, and CC2420 works on 2.4 GHz unlicensed ISM band with max 250 kbits/sec data transmission rate. With an antenna length of one-quarter wavelength of 2.4 GHz, the transmission range is around 50 meters. The key fob has a similar size of a coin, and is powered by 3V button cell. Statistically, one cell can sustain around 3800 times of operation. Assuming 1 operation lasts for three seconds and 5 operations are conducted per day, 3800 operations is equivalent to 2 years battery lifespan.

IV. CONCLUSION AND ONGOING WORKS

This paper proposes a wireless protocol with a fixed and a variable key in AES for confidentiality protection of messages transmitted in the automobile keyless system. The protocol can effectively defeat today's common attack tricks. In the implementation, several practical factors are considered so that ASP can be widely adopted. Lastly, we also try to make the car transceiver as a general wireless hardware platform in which more function modules could be deployed.

REFERENCES

[1] TI product datasheet http://www.ti.com/rfid/docs/manuals/pdfSpecs/RITRP-V9WK_ds.pdf.

[2] William Stallings, "Cryptography and Network Security Principle and Practice", third edition, chapter 5.

[3] Steve Bono, Matthew Green, Adam Stubblefield, and Avi Rubin, "Analysis of the Texas Instruments DST RFID" Johns Hopkins University from http://rfid-analysis.org/.

[4] Crossbow sensor network manufacturer http://www.xbow.com/.

[5] Open SSL http://www.openssl.org.

[6] Wireless medium access control and physical layer specifications for low-rate wireless personal area network. IEEE Standard, 802.15.4-2003, May 2003.

[7] AES Wikipedia web site: http://en.wikipedia.org/wiki/AES.

[8] Ansaf Ibrahem Alrabady, "Analysis of Attacks Against the Security of Keyless-Entry Systems for Vehicles and Suggestions for Improved Designs," IEEE transactions on vehicular technology, vol. 54, No. 1, January 2005.

[9] A. I. Alrabady and S. M. M, "Some attacks against vehicles' passive entry security systems and their solutions," IEEE Transactions. Veh. Technol., vol. 52, no. 2, pp. 431–439, Mar. 2003.

[10] "Microchip Inc., data sheet for HCS412," in KeeLoq Code Hopping Encoder and Transponder. Chandler, AZ: Microchip Technol., Inc., 2000.

[11] Daniel J. B., "Cache-timing attacks on AES,"The University of Illinois.

[12] Secure hash standard, Federal Information Processing Standard 180-2, National Institute of Standards and Technology, Washington. URL: http://csrc.nist.gov/publications/fips/.

[13] David B., Remote timing attacks are practical (2003). URL: http://crypto.stanford.edu/~dabo/papers/ssl-timing.pdf.