The Journal of The Institute of Internet, Broadcasting and Communication (IIBC)
Vol. 17, No. 6, pp.127-135, Dec. 31, 2017. pISSN 2289-0238, eISSN 2289-0246

https://doi.org/10.7236/JIIBC.2017.17.6.127
JIIBC 2017-6-17

자동차 내부 네트워크를 위한 경량 메시지 인증 코드 사용기법

Usage Techniques of a Truncated Message Authentication Code for In-Vehicle Controller Area Network

우사무엘*, 이상범**

Woo Samuel*, Sang-Bum Lee**

요 약 대부분의 최신 자동차들은 편안하고 안전한 운전 환경을 위해 다양한 종류의 ECU들을 탑재하고 있다. ECU들 사이의 효율적인 통신을 위해 대부분의 자동차 제조사들은 Controller Area Network(CAN) 프로토콜을 사용하고 있다. 그러나 CAN은 데이터 인증을 제공하지 않는다. 이러한 취약점 때문에 CAN은 메시지 재생공격에 취약하다.
본 논문은 자동차 내부 네트워크에 적용 가능한 현실적인 메시지 인증 기법을 제안한다. CAN 데이터 프레임의 제한적인 공간을 고려하여, 데이터와 메시지 인증 코드 (MAC)를 동시에 전송하기 위해서는 짧은 길이의 MAC을 사용하는 것이 가장 적합하다. 그러나 짧은 길이의 MAC은 암호학적 안전성을 충분히 보장하지 않기 때문에 안전성을 보장하기 위한 추가적인 조치가 필요하다. 본 연구에서 제안한 메시지 인증 기술은 CAN의 제한된 데이터 페이로드를 고려하기 때문에 차량 내부의 안전한 네트워크를 설치하는데 유용하게 활용될 수가 있다.

Abstract Recently, the most brand new vehicles contain a lot of ECU for comfortable and safety driving environments. For efficient communication network among ECUs, almost car manufactures use CAN protocol which enables to decrease the number of communication lines dramatically and ensures higher data transmission reliability. However, CAN dose not ensure authentication of CAN data frame. So it is vulnerable to replay-attack on CAN data frame. This paper proposes the practical message authentication technique for In-vehicle CAN. To transmit data and MAC together, it is very useful to use the short length of MAC after considering limited space of CAN data frame. However to ensure safety of MAC, additional technique is required. We suggested a message authentication technique that can be usefully applied to build a safety network inside the vehicle because it considers limited data payload of CAN.

Key Words : In-Vehicle Network, Controller Area Network, HMAC, HOTP

Ⅰ. 서 론

여기에 자동차에는 운전자의 편의와 안전을 위해 다양한 전자제어기능이 탑재되고 있다[1]. 자율주행자동차 관련 기술이 발전하면서 지금보다 더 많은 전자제어기능이 자동차에 탑재될 것으로 전망된다[2].

*준회원, 한국전자통신연구원
**정회원, 단국대학교 컴퓨터과학과
접수일자: 2017년 5월 25일, 수정완료: 2017년 11월 22일
게재확정일자: 2017년 12월 8일

Received: 25 May, 2017 / Revised: 22 November, 2017 / Accepted: 8 December, 2017
**Corresponding Author: sblee@dankook.ac.kr
Dept. of Computer Science in Dankook University, Korea

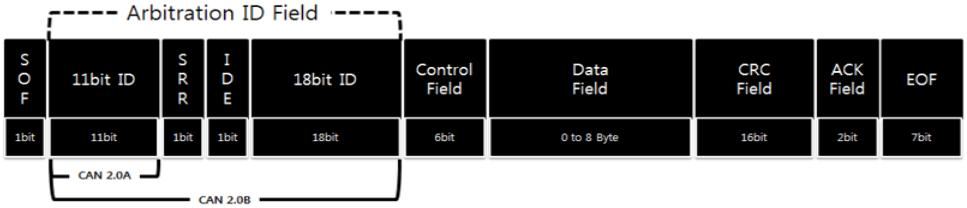

그림 1. CAN 데이터 프레임 포멧
Fig. 1. CAN data frame format

자동차에 전자제어기능을 효율적으로 적용하기 위해서는 보다 많은 자동차 전장부품의 사용이 필수적으로 요구된다. ECU는 이와 같은 자동차 전장부품들 중 가장 핵심이 되는 요소이다[3][4]. 최근에는 각종 편의기능을 탑재하기 위해 ECU의 활용 범위를 넓히고 있다.

자동차에 탑재되는 ECU가 늘어나면서 효율적인 자동차 내부 네트워크를 구축하기 위해 Controller Area Network (CAN), LIN, FlexRay등의 통신 프로토콜들이 개발되었다[5][6]. 그중 CAN은 지난 30년간 자동차 내부 네트워크 구축에 지배적으로 사용되었고, 최근 출시되는 차량에도 CAN이 사용되고 있다[7][8].

그러나 CAN은 매우 폐쇄적인 네트워크 환경만 고려하고 개발되었기 때문에 기본적인 정보보호기능도 제공하지 않고 있다[9][10]. CAN은 버스 네트워크 토폴로지를 이용하여 데이터를 브로드캐스트 하는 과정에서 송신 데이터에 대한 인증을 보장하지 않는다. 이 때문에 데이터 재전송공격이 가능하다[11][12].

2010년 워싱턴대학의 연구팀이 실제 자동차를 이용한 CAN 취약점 분석 및 해킹 연구를 발표하면서 자동차 해킹에 대한 심각성이 자동차 업계와 학계에 본격적으로 알려졌다[13][14]. 이후 CAN의 취약점을 보완하기 위한 많은 연구들이 진행되었으나, CAN의 제한적인 데이터 페이로드 때문에 안전성과 가용성을 모두 보장하는 기법은 제안되지 않았다. CAN의 제한적인 데이터 페이로드를 고려하여 보안 기법을 설계할 때는 안전성과 가용성의 적절한 균형을 맞추어 보안 기법을 설계해야 한다. CAN 데이터 프레임의 제한적인 공간을 고려하여, 데이터와 메시지 인증 코드 (Message Authentication Code: MAC)를 동시에 전송하기 위해서는 짧은 길이의 MAC을 사용하는 것이 가장 적합하다. 그러나 짧은 길이의 MAC은 암호학적 안전성을 충분히 보장하지 않기 때문에 안전성을 보장하기 위한 추가적인 조치가 필요하다.

본 논문은 짧은 길이의 MAC과 함께 MAC을 생성할 때 사용하는 인증키의 변경 주기를 빠르게 유지하여 암호학적 안전성을 보장하는 CAN 데이터 프레임 인증 기법을 제안한다. 본 논문의 구체적인 기여도는 다음과 같다.

- 제한적인 CAN 데이터 페이로드에 적용 가능한 truncated MAC 사용방법 제안
- Truncated MAC의 안전성을 보장하기 위한 Session key update 기법 제안
- 제안 기법의 안전성 및 효율성 분석

II. 배경지식

1. Controller Area Network

CAN 프로토콜은 ECU들 간의 효율적인 통신을 지원하기 위해 BOSCH사에서 개발했다. CAN 프로토콜은 버스 네트워크 토폴로지를 지원하는 송신자 ID 기반의 브로드캐스트 통신기법이다. CAN은 버스네트워크 토폴로지를 지원하므로써 자동차 내부 ECU들 사이의 통신 회선의 복잡성과 길이를 획기적으로 감소시켰다. 이러한 이유로 자동차 업계에서는 신속하게 CAN 버스시스템을 도입하였으며 1993년에는 ISO의 국제 표준 규격 (ISO 11898)으로 제정되었다. CAN 버스시스템은 메시지에 있는 ID의 길이에 따라 두 가지 모드로 구분된다.

- 표준 CAN 2.0A (11bit ID)
- 확장 CAN 2.0B (29bit ID)

표준 CAN 2.0A와 확장 CAN 2.0B 의 메시지 구조는 그림 1과 같다. 확장 CAN 2.0B는 29bit의 식별자를 가진다. CAN 2.0A와는 다르게 CAN 2.0B는 ID 필드가 두 곳으로 구분되어 있다. IDE 필드는 두 개의 ID 필드를 구분한다. 제어 필드(Control Field)는 데이터 필드(Data

field)의 바이트 수를 가리키는 Data Length Code(DLC)로 구성된다. 데이터 필드는 다른 노드로 전하고자 하는 데이터를 포함하며 최대 8바이트까지 사용 가능하다. CRC필드는 15bit Cyclic Redundancy Check(CRC)코드와 1-bit CRC 필드 경계필드로 구성된다. ACK 필드는 2bit로 구성된다. CAN은 메시지의 인증이 제공되지 않아 누구나 쉽게 메시지를 위조하거나 재전송하여 자동차를 제어할 수 있다는 점이다. 또한, CAN 버스시스템을 위한 보안 메커니즘 설계 시, CAN 의 데이터 페이로드가 8byte로 매우 협소하기 때문에 충분한 안전성을 보장할 수 있는 MAC을 사용할 수 없다.

Ⅲ. 위협 모델 및 보안 요구사항

1. 위협모델

본 장에서는 자동차 내부 CAN 버스 시스템의 취약점으로 인해 발생 가능한 위협모델을 소개한다. 본 논문에서 제안하는 위협모델은 기존 연구들이 제안하고 실험을 통해 증명한 내용을 기반으로 설계되었다[13][14][15][16][17][18].

● 공격자 능력 (Attacker ability)

공격자는 자동차 내부에 탑재된 ECU들을 강제 구동시킬 수 있는 데이터 프레임을 다음과 같은 방법으로 획득할 수 있다.

가) 자동차 정상 운행 중 CAN 통신 모니터링
나) 자동차 정비기기 사용 중 CAN 통신 모니터링
다) 모니터링 과정 중 데이터 프레임 획득
라) 획득된 데이터 프레임을 이용한 전수조사

공격자는 상기 과정을 통해 획득한 ECU 강제 제어 패킷을 이용하여 공격도구를 제작할 수 있다. 대표적인 공격도구는 다음과 같다.

가) 자동차 자가진단용 스마트폰 어플리케이션
나) 자동차에 탑재할 수 있는 악성 모듈
다) 자동차 네비게이션 업데이트용 악성 펌웨어

● 피해자의 행동 (Victim Behaviour)

대표적인 피해자는 운전자일 것이다. 운전자는 운전편의 및 안전을 위해 다양한 소프트웨어와 하드웨어를 사용할 수 있다. 대표적으로 자동차 자가진단용 스마트폰 어플리케이션이 있다. 운전자는 앱 마켓에서 “자동차 자가진단” 또는 “OBD2”라는 키워드로 검색하여 다양한 차량 진단 앱을 다운로드 받을 수 있다. 2016년 기준 google play store에는 약 300여개의 차량용 스마트폰 어플리케이션이 업로드되어 있다. 또한 최근 출시되는 차량은 커넥티드가 환경을 구축하기 위해 네비게이션에 이동통신 기능이 탑재되어 있다. 대표적인 시스템으로는 현대 블루링크, 기아의 유보등이 있다. 자동차 제조사들은 커넥티드카 서비스 업데이트를 위해 정기적으로 시스템 업데이트용 펌웨어를 배포하고 있다. 상기 두 가지 시나리오에서 스마트폰에 다운로드 받아 사용하는 자가진단 앱이 공격자가 배포한 악성 앱일 경우, 또는 커넥티드가 서비스 업데이트를 위해 사용되는 펌웨어를 정상적인 사이트에서 다운로드 받지 않아서 공격자가 배포한 악성 펌웨어를 다운로드 받아서 설치했을 경우 심각한 위협에 노출될 것이다.

앞에서 설명한 공격자의 능력과 피해자의 행동으로 인해 발생되는 자동차 내부 네트워크 공격은 2010년부터 현재까지 보고된 연구를 기반으로 정리된 것이다. 2010년부터 2016년까지 보고된 각종 해킹 실험들의 공통점은 CAN의 취약점을 근본적인 원인으로 이용하여 해킹을 수행했다는 것이다. CAN에는 데이터 인증 기능이 없기 때문에 공격자가 사전에 획득한 ECU강제 제어 패킷을 다양한 방법으로 자동차 내부에 재전송 시켰을 경우 타켓 ECU를 강제 제어 할 수 있다.

2. 보안 요구사항

본 기존 연구들이 공통적으로 지적하고 있는 근본적인 문제는 CAN의 취약점으로 인해 발생한다. 즉 자동차 내부 CAN의 취약점을 제거한다면, 본 논문에서 제안하는 위협 모델로부터 충분한 안전성을 확보할 수 있다. 안전한 자동차 내부 CAN을 구축하기 위해서는 다음과 같은 보안 요구사항을 만족해야 한다.

가. 메시지 인증(Message Authentication)

CAN은 데이터프레임에 대한 인증을 제공하지 않는다. CAN은 도청된 데이터프레임의 재전송 공격이나, 변조 공격에 취약하다. 그러므로 CAN은 데이터프레임 인증을 보장해야 한다.

나. 키 Freshness(Key Freshness)

매 세션에서 사용되는 키는 이전에 사용된 세션 키들

과 향후 사용될 세션 키들과는 독립적이어야 하고, 매 세션 다른 키가 사용되어야 한다.

Ⅳ. CAN 데이터 프레임 인증 기법

본 장에서는 CAN 데이터 프레임 인증을 위한 보안 기법을 제안한다. 본 논문에서는 8byte 크기의 CAN 데이터 페이로드를 고려한 데이터프레임 인증 기법을 제안한다. 본 논문이 제안하는 데이터프레임 인증 기법을 적용하기 위해 다음 4가지 사항을 가정한다. 첫째, 모든 ECU는 자동차가 출고될 때 세션 키 분배에 사용할 대칭키(Long-term symmetric key)를 탑재한다. 둘째, 모든 ECU는 자신이 수신하는 ECU에 대한 카운터(Counter)를 관리한다. 제안하는 기법은 자동차가 생산-출고 될 때 사전에 진행되는 대칭키 등록 단계, 자동차의 시동 시 진행되는 세션 키 분배 단계, 분배된 세션 키로 인증키를 생성하는 단계, 마지막으로 데이터프레임을 인증하는 인증 단계로 나누어진다.

표 1. Notation
Table 1. Notation

item	value
ECU_j	ID가 j인 일반 ECU
GECU	게이트웨이 ECU
ECU_S	송신 ECU
ECU_R	수신 ECU
C_i	i 번째 세션에서 사용하는 카운터
AK_ij	i 번째 세션에서 j번째 데이터 프레임에 대한 인증 코드를 생성할 때 사용하는 인증키
KGK_i	i 번째 세션에서 AK_ij를 생성할 때 사용하는 키 생성키
M_ij	i 번째 세션에서 j 번째로 송신하는 데이터 프레임
MAC_ij	i 번째 세션에서 j 번째로 송신하는 데이터 프레임의 인증 코드
SK_i	ECU_i가 사전에 저장하고 있는 인증키
SK_G	모든 ECU가 공유하고 있는 키 생성키
$H_X(\ )$	"X"를 키로 사용하는 일 방향 해쉬 함수
$KDF_X(\ )$	"X"를 키로 사용하는 키 생성 함수

1. 대칭키 등록 단계

GECU를 포함한 모든 ECU들은 안전한 환경에서 SK_i (인증용 대칭키)와 SK_G (키 생성용 대칭키)를 공유한다. 본 논문에서 대칭키 등록단계는 큰 기여도가 없으므로 자세한 설명을 생략한다. ECU의 수리 또는 교체 작업이 필요할 경우 지정된 정비소에서 대칭키 업데이트 작업을 수행한다. GECU와 모든 ECU들은 대칭키를 안전하게 저장하기 위해 Secure storage를 사용한다고 가정한다. 그림 2는 GECU를 포함하여 총 5개의 ECU가 서브네트워크를 형성한 환경에서 대칭키가 공유된 모습을 보여주고 있다.

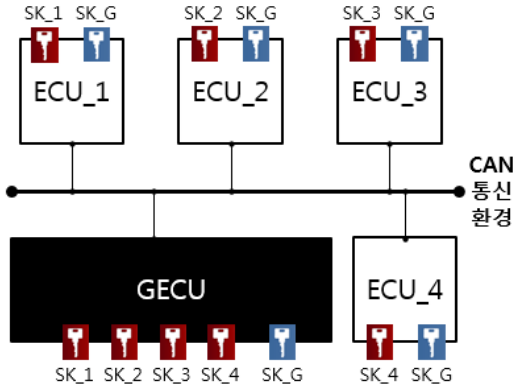

그림 2. Long-Term 대칭키 저장
Fig. 2. Long-Term Symmetric key loading

2. 키 생성키 (KGK_i) 생성단계

GECU를 포함한 모든 ECU들은 i 번째 세션에서 통신을 시작하기 전에 i 번째 세션에서 사용 할 키 생성키(KGK_i) 생성 단계를 수행한다. KGK_i 생성 과정은 GECU를 중심으로 모든 ECU가 순차적으로 진행한다. KGK_i 생성과정은 AKEP2(Authentication and Key Exchange Protocol Version2)프로토콜을 이용한다. GECU와 ECU_j는 그림 3과 같이 KGK_i 생성 과정을 진행한다.

가) GECU는 난수 RA를 생성하여 ECU_j에게 전송한다.
나) i 번째 세션에서 GECU는 모든 ECU들과 키 생성키 생성 단계를 진행하는 동안 동일한 난수 RA를 사용한다.
다) 난수 RA를 수신한 ECU_j는 난수 RB를 생성한다.
라) ECU_j는 식 1 과 같이 제 1 인증 값(MAC1)을 생성한다. MAC1은 SK_j를 키로 사용하는 일 방향 해쉬 함수 HSK_j( )에 GECU의 ID와 자신의 ID와 난수 RA와 난수 RB를 입력하여 생성한다.

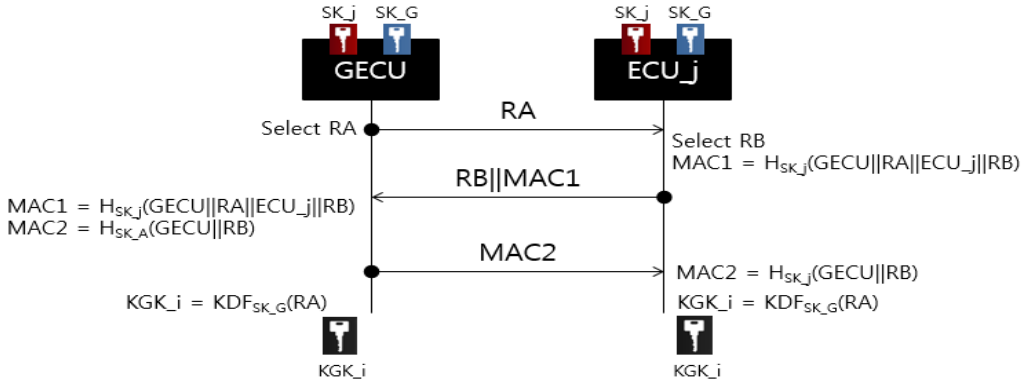

그림 3. 키 생성 키 도출 단계
Fig. 3. Key generation key derivation phase

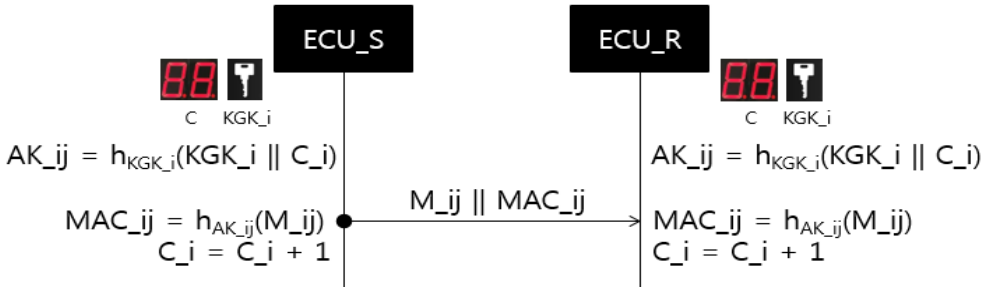

그림 4. 인증키와 HMAC 생성 단계
Fig. 4. Authentication key and HMAC generation phase

마) ECU_j는 MAC1과 RB를 GECU에게 전송한다.

바) MAC1과 RB를 수신한 GECU는 식 (1) 을 이용하여 MAC1을 검증한다.

$$MAC1 = H_{SK\_j}(GECU \parallel ECU\_j \parallel RA \parallel RB) \quad (1)$$

사) MAC1 검증이 정상적으로 종료되면 GECU는 식 2와 같이 제 2 인증 값(MAC2)를 생성한다. MAC2는 SK_A를 키로 사용하는 일 방향 해쉬 함수 HSK_A( )에 GECU의 ID와 난수 RB를 입력하여 생성한다.

$$MAC2 = H_{SK\_j}(GECU \parallel RB) \quad (2)$$

아) MAC2생성 후 GECU는 식 3과 같이 KGK_i를 생성한다. KGK_i는 SK_G를 키로 사용하는 키 생성함수 KDFSK_G( )에 난수 RA를 입력하여 생성한다.

$$KGK\_i = KDF_{SK\_G}(RA) \quad (3)$$

자) GECU는 MAC2를 ECU_j에게 전송한다.

차) ECU_j는 식 (2)를 이용하여 MAC2를 검증한다.

카) MAC2 검증이 정상적으로 종료되면 ECU_j는 식 (3)과 같이 KGK_i를 생성한다.

3. CAN 데이터 프레임 인증 과정

데이터 프레임 인증 과정은 데이터 프레임 인증코드 생성단계와 데이터 프레임 인증코드 검증단계로 나뉜다. 데이터 프레임 인증코드 생성단계는 송신자 측에서 수행된다. 데이터 프레임 인증코드 검증단계는 수신자 측에서 수행된다. CAN 데이터 프레임의 데이터 페이로드는 8byte로 매우 제한적이기 때문에 64bit 이하의 짧은 메시지인증코드(MAC)을 사용한다. 그림 4은 일반적인 CAN 데이터 프레임 포맷에서 8byte 데이터 필드에 짧은 MAC을 저장하는 예를 보이고 있다. 본 논문에서는

8byte 데이터 필드 중 16bit 데이터필드를 MAC 저장에 사용하는 방법을 제안한다. 짧은 MAC을 사용할 경우 암호학적 안전성을 보장할 수 없다. 본 논문에서는 16bit MAC의 암호학적 안전성을 보장하기 위해 일회성 인증키를 이용한 데이터 프레임 인증 기법을 제안한다. i 번째 세션에서 j 번째 메시지를 송-수신할 때 일회성 인증키를 이용한 CAN 데이터 프레임 인증과정은 그림 5와 같다.

가) 송신자 ECU(ECU_S)와 수신자 ECU(ECU_R)은 KGK_i 생성 단계를 통해 i 번째 세션에서 사용할 KGK_i를 공유하고 있다.

나) ECU_S와 ECU_R은 ECU_S가 i 번째 세션에서 송신한 데이터 프레임의 송신횟수(C_i)를 관리하고 있다. ECU_S 와 ECU_R이 관리하고 있는 C_i는 동기화된 값이다.

다) ECU_S와 ECU_R은 i 번째 세션에서 j 번째로 송-수신하는 데이터 프레임 M_ij를 송-수신하기 전에 식 (4)와 같이 일회성 인증키 AK_ij를 생성한다.

$$AK\_ij = H_{KGK\_i}(KGK\_i \parallel C\_i) \qquad (4)$$

라) AK_ij를 생성한 ECU_S는 M_ij를 송신하기 전에 식 (5)와 같이 M_ij에 대한 데이터 프레임 인증코드(MAC_ij)를 생성한다.

$$MAC\_ij = H_{AK\_ij}(M\_ij) \qquad (5)$$

마) MAC_ij를 생성한 후 M_ij와 함께 MAC_ij를 ECU_R에서 전송한다.

바) M_ij와 MAC_ij를 수신한 ECU_R은 기 생성한 AK_ij와 식 5를 이용하여 M_ij에 대한 MAC_ij를 검증한다.

사) M_ij와 MAC_ij의 송-수신 및 검증과정이 모두 종료되면 ECU_S와 ECU_R은 C_i를 1만큼 증가시킨다.

4. 키 생성키(KGK_i) 업데이트 단계

i 번째 세션에서 ECU_S와 ECU_R이 관리하는 C_i는 유한한 크기이다. ECU_S의 C_i가 표현할 수 있는 범위보다 많은 데이터 프레임을 ECU_R에게 전송할 경우 C_i는 초기화 되고 0부터 다시 관리될 것이다. i 번째 세션에서 동일한 C_i가 발생할 경우 메시지 재생공격으로부터 안전성을 보장할 수 없다. 본 논문은 메시지 재생공격으로부터 안전성을 보장하기 위해, 키 생성키 업데이트 단계를 제안한다. i 번째 세션에서 C_i가 최대 표현 수치에 다다르기 전에 GECU와 모든 ECU들은 키 생성키 업데이트 과정을 수행한다. 키 생성키 업데이트 과정은 기 수행했던 키 생성키 생성 단계와 동일하다. i 번째 세션에서 키 생성키 생성 단계를 수행하면 KGK_i+1을 생성하게 되고 i+1 번째 세션이 시작된다.

V. 안전성 분석

안전성 분석은 3.2절의 보안요구사항에 입각하여 제안 메커니즘을 분석한다. 효율성 분석은 데이터 오버헤드 발생량을 분석한다.

1. 안전성 분석

● **메시지 인증 (Message Authentication)**

제안하는 메시지인증 기법은 16bit 의 메시지인증코드를 사용한다. 일반적인 Hash의 경우 16bit 출력값은 “생일 공격 이론”에 따라 28번의 시도로 충돌쌍 공격(Collision Resistance Attack)에 성공할 수 있다. 그러나 대칭키 기반의 HMAC의 경우 Key가 노출되지 않는다면 공격자는 자신이 원하는 메시지에 대한 HMAC을 생성할 수 없기 때문에 “생일 공격 이론”을 사용하지 못하고 전수조사 공격을 수행해야 한다[19][20].

16bit HMAC을 사용하는 시스템에서 인증코드를 생성하는 키를 교체하지 않는 다는 조건하에 공격자가 전수조사를 수행할 경우 2^{16}번의 공격을 수행하면 충돌쌍 공격에 성공할 것이다. 그러나 우리가 제안하는 메시지 인증 기법은 메시지 인증 코드를 생성할 때마다 새로운 인증키를 생성하여 사용하기 때문에 공격자가 전수 조사 공격을 수행하더라도 전수조사를 이용한 충돌쌍 공격으로부터 안전한 시스템을 유지할 수 있다. 즉 16bit 크기의 HMAC을 사용하는 우리 시스템은 매번 새로운 키를 사용하여 HMAC을 생성하기 때문에 전송하는 메시지와 메시지인증코드를 대상으로 충돌쌍 공격에 성공할 확률은 매번 동일한 확률을 가질 것이다(2^{16}).

● **키 freshness (Key freshness)**

본 논문이 제안하는 메시지 인증 방식에서는 두 가지 종류의 세션 키가 사용된다. 첫 번째는 일회성 세션 키

생성에 사용되는 키 생성키(KGK)이며 두 번째는 메시지 송신시 마다 새롭게 생성되는 일회성 메시지 인증키(AK)이다. 매 세션에서 사용되는 KGK는 각 세션마다 랜덤하게 생성된 값(RA)으로부터 유도되므로 서로 연관성이 없다. 메시지 전송 시 마다 생성되는 인증키(AK)는 송신자와 수신자만이 유지하고 있는 메시지 카운터와 KGK를 이용하여 생성된다. 즉 KGK와 AK는 매번 새로운 랜덤 또는 카운터를 이용하여 생성되기 때문에 키 Freshness를 보장한다.

2. 가용성과 효율성

CAN의 제한적인 데이터 페이로드를 고려한다면 안전성과 가용성(효율성)사이의 트레이드오프는 필수적으로 발생 할 수밖에 없다. 이를 최소화하는 것이 가장 효율적인 보안 기법일 것이다. 본 논문이 제안하는 메시지 인증 기법은16bit길이의 작은 메시지 인증코드를 사용하면서도 안전성을 고르게 유지시키는 키 사용방법과 메시지 인증코드 사용방법을 제안했다. 우리가 제안하는 메시지 인증코드 사용방법을 사용할 경우 필연적으로 통신 오버헤드는 발생한다. [표 2]는 우리가 제안하는 기법을 사용했을 때 발생하는 통신오버헤드를 나타낸다. 우리가 제안하는 기법을 사용하지 않을 경우 64bit 데이터를 전송할 때 하나의 데이터 프레임만 전송하면 된다. 이때 데이터를 제외한 오버헤드는 56bit이다(Controller 필드, ID필드 등 통신을 위해 필수적으로 사용되는 bit). 우리가 제안하는 기법을 사용할 경우 64bit 데이터를 전송하려면 두 개의 데이터 프레임을 전송해야 할것이고 이때 데이터 오버헤드는 56bit*2이다. 데이터 오버헤드는 기존의 2배가 되는 것을 아니다. 6400bit의 데이터를 전송하는 경우 양 33개의 데이터 프레임만 추가적으로 발생하기 때문에 전체 오버헤드는 데이터 전송 량에 때라 결정된다.

표 2. 통신 오버헤드
Table 2. Communication overhead

Data (bit)	MAC (each message)	Message	Overhead
64	16	2	56bit*2
6400	16	133	56bit*133

Ⅵ. 관련 연구

자동차-IT 융합기술의 발전과 함께 자동차 내부 네트워크 안전성에 대한 다양한 연구들이 진행되고 있다. 대다수의 기존 연구들은 자동차 내부 네트워크 중 가장 중요한 CAN 버스시스템의 취약점을 분석하고 이를 해결하기 위한 방안을 제안하고 있다.

M. Wolf와 T. Hoppe등은 [3][10][11]에서 CAN 통신에 참여하는 ECU에 대한 접근제어와 브로드캐스트 되는 메시지에 대한 비 암호화/인증으로 인해 발생할 수 있는 문제점들을 지적하고 있다. 이들은 CANoe 시뮬레이터 기반의 실험을 통해 CAN에서 메시지 재전송공격이 가능함을 증명하였다. 또한 이러한 문제점을 해결하기 위해 기기인증서 기반의 ECU 인증과정과 대칭키 기반의 메시지 암호화 기법을 제안하였다. 그러나 이들이 제안한 보안 메커니즘은 ECU의 연산능력과 CAN 데이터 페이로드를 고려하지 않고 설계되었기 때문에 실제 차량 환경에는 적용하는 것은 불가능하다.

D. K. Nilsson등은 [12]에서 ECU의 연산능력과 제한적인 CAN 메시지 구조를 고려한 DDA(Delayed Data Authentication)기법을 제안하였다. DDA기법은 메시지 재전송공격을 막기 위해 Message Authentication Code(MAC)사용한다. 이때 CAN 메시지 구조에서 가용할 수 있는 영역이 부족함을 지적하고 CRC필드를 사용하는 기법을 제안했다. 또한 DDA는 4개의 메시지를 그룹으로 묶어서 인증하는 기법을 제안했다. 그러나 CAN에서 CRC 필드는 동적으로 사용이 불가능하다. 또한 보통 수 ms이내로 전송 받은 CAN 메시지에 대한 처리가 필요한 자동차 내부 네트워크에서 DDA기법을 사용할 경우 최소 80ms이상의 인증지연 시간이 발생하기 때문에 자동차환경에 DDA기법을 적용하는 것은 사실상 불가능하다.

기존 연구들의 경우 CAN 버스 시스템의 암호학적 안전성 결여 문제를 지적하고 CANoe등의 시뮬레이션 툴로만 공격 가능성을 실험한 반면, K. Koscher등은 [26]에서 다양한 방식의 분석방법을 통해 실제 양산 자동차를 이용하여 자동차 내부 네트워크의 문제점을 지적하였다. 특히 이들은 자동차 내부 네트워크에서 ECU간 주고 받는 메시지의 의미를 분석하기 위해 리버스 엔지니어링과 퍼징 등의 기법을 사용하여 메시지를 분석하고 메시지 재전송 공격 및 차량 내부 네트워크에 대한 다양한 공격

가능성을 실제 차량환경의 실험으로 증명하였다. 그러나 ECU Firmware에 대한 리버스 엔지니어링과 CAN 메시지의 퍼징을 통한 CAN 메시지 분석은 상당히 많은 시간을 필요로 한다. 그리고 이들이 수행한 공격은 ECU를 탈거하여 펌웨어를 수정 후 다시 장착하는 방법을 사용하고 있어서 공격의 실효성이 낮고, 공격을 위해서는 공격대상이 되는 자동차를 장시간 점거해야 한다는 공격자의 능력이 요구되어 현실적인 공격방법으로는 부적합하다.

Ⅶ. 결론

최신 자동차들은 각종 전자제어 시스템을 운영하기 위해 CAN을 사용한다. 하지만 차량 내부의 CAN은 어떠한 정보보호 기법도 적용되어 있지 않기 때문에 메시지 재생공격을 이용한 해킹에 무방비 상태로 노출되어있다. 악의적인 공격자는 이런 특성을 이용하여 차량에 제어 데이터를 다양한 방법으로 주입하여 차량을 임의로 제어할 수 있다. 본 논문이 제안한 메시지인증 기법은 CAN의 제한적인 데이터 페이로드를 고려한 보안기법으로써 안전한 차량 내부 네트워크 구축에 활용될 수 있다.

References

[1] A. Saad and U. Weinmann, “Automotive software engineering and concepts,” in GI Jahrestagung, pp. 318 - 319, Frankfurt, Germany, September-October 2003.

[2] Dongwon Kim, “Traffic Information Service, Inter-Vehicle Communication,” The International Journal of Internet, Broadcasting and Communication VOL. 12 No. 3, June, 2012.

[3] M. Wolf, A. Weimerskirch, and C. Paar, “Security in Automotive Bus Systems,” in Proceedings of ESCAR 04, 2004.

[4] R. Charette, “This car runs on code,” Online: http://www.spectrum.ieee.org/feb09/7649, Feb. 2009.

[5] T. Nolte, H. Hansson and L.L. Bello, "Automotive communications-past, current and future," in Proceedings of ETFA(Emerging Technologies and Factory Automation), 2005.
DOI: 10.1109/ETFA.2005.1612631

[6] K.H. Johansson, M. Törngren, L. Nielsen, “Vehicle applications of controller area network,” D. Hristu-Varsakelis, W.S. Levine (Eds.), Handbook of Networked and Embedded Control Systems, Springer (2005) ISBN: 0-8176-3239-5

[7] CAN in Automation. Webpage, 2004. www.can-cia.org.

[8] BOSCH CAN. Webpage, 2004. www.can.bosch.com.

[9] Tobias Hoppe and Jana Dittman. “Sniffing/Replay Attacks on CAN Buses: A simulated attack on the electric window lift classified using an adapted CERT taxonomy”. In Proceedings of the 2nd Workshop on Embedded Systems Security (WESS), Salzburg, Austria, 2007.

[10] Hoppe T, Kiltz S, Dittmann J. “Security threats to automotive CAN networks—practical examples and selected short-term countermeasures,” Reliability Engineering & System Safety, Accepted Manuscript, Available online 5 July 2010, in press
DOI: 10.1016/j.ress.2010.06.026

[11] Nilsson, D.K., Larson, U.E., Jonsson, E.: Efficient In-Vehicle Delayed Data Authentication based on Compound Message Authentication Codes. In: Proceedings of the IEEE 68th Vehicular Technology Conference (VTC2008-Fall) (2008)
DOI: 10.1109/VETECF.2008.259

[12] D. K. Nilsson and U. E. Larson, "Secure Firmware Updates over the Air in Intelligent Vehicles," in Proceedings of the First IEEE Vehicular Networking & Applications Workshop (Vehi-Mobi). IEEE, 2008, pp. 380-384.
DOI: 10.1109/ICCW.2008.78

[13] K. Koscher, A. Czeskis, F. Roesner, S. Patel, T. Kohno, S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, and S. Savage. Experimental security analysis of a modern automobile. The IEEE Symposium on Security and Privacy, Oakland, CA, May 16-19, 2010.
DOI: 10.1109/SP.2010.34

[14] S. Checkoway, D. McCoy, D. Anderson, B. Kantor, [15] H. Shacham, S. Savage, K. Koscher, A. Czeskis, F. Roesner, and T. Kohno. “Comprehensive experimental analyses of automotive attack surfaces.” In D. Wagner, ed., Proceedings of USENIX Security 2011. USENIX, Aug. 2011.

[15] Sun Jin Oh “An Anomaly Detection Method for the Security of VANETs”, The International Journal of Internet, Broadcasting and Communication, vol. 10, no. 2, pp 77-83, April. 2010.

[16] W. Samuel, J. HyoJin, and L. DongHoon “A Practical Wireless Attack on the Connected Car and Security Protocol for In-vehicle CAN”, IEEE Trans, Intelligent Transportation Systems, vol. 16, no. 2, pp 993-1006,IEEE, 2015.
DOI: 10.1109/TITS.2014.2351612

[17] D. K. Nilsson and Larson, U.E.: “Conducting Forensic Investigations of Cyber Attacks on Automobile In-Vehicle Networks. In: Proceedings of the First ACM International Conference on Forensic Applications and Techniques in Telecommunications, Information and Multimedia (e-Forensics). ACM Press, New York (2008)

[18] S. You, M. Krage, and L. Jalics, “Overview of Remote Diagnosis and Maintenance for Automotive Systems”, in 2005 SAE World Congress, Detroit, MI, USA, 2005.
DOI: 10.4271/2005-01-1428

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

[20] Black, J., Cochran, M. “MAC Reforgeability”, FSE 2009. LNCS, vol. 5665, pp. 345 - 362. Springer, Heidelberg

[21] Yasuda, K.: Multilane HMAC- security beyond the birthday limit. INDOCRYPT 2007. LNCS, vol. 4859, pp. 18 - 32. 2007

저자 소개

우사무엘(준회원)

- 2010년 : 단국대학교 컴퓨터과학과 석사
- 2016년 : 고려대학교 정보보호대학원 박사
- 2016년~현재 : 한국전자통신연구원 선임연구원

이 상 범(정회원)

- 1989년: LOUISIANA STATE UNIV 컴퓨터 과학 석사
- 1992년: LOUISIANA STATE UNIV 컴퓨터 과학 박사
- 1993년~현재: 단국대학교 컴퓨터과학과 교수