Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.31, NO.3, Jun. 2021 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2021.31.3.373

Periodic-and-on-Event 메시지 분석이 가능한 차량용 침입탐지 기술*

이 세 영,[1†] 최 원 석[2‡]
[1]고려대학교 정보보호대학원 (대학원생), [2]한성대학교 (교수)

Periodic-and-on-Event Message-Aware Automotive Intrusion Detection System*

Seyoung Lee,[1†] Wonsuk Choi[2‡]
[1]Korea University (Graduate student), [2]Hansung University (Professor)

요 약

운전자의 안전성 및 편의성을 향상시키기 위하여, 최근 자동차에는 다수의 전자제어장치가 탑재되고 있다. 전자제어장치들은 차량의 상태를 서로 공유하기 위하여 일반적으로 CAN 통신 프로토콜을 이용하여 통신한다. 현대의 자동차는 안전성 및 편의성과 관련된 최첨단 서비스를 제공하고 있지만, 사이버보안 위협에 대한 Attack Surface가 증가하는 문제점이 있다. 자동차 해킹의 경우에는 운전자 생명과 직접적 영향이 있기 때문에, 이에 대응하기 위한 자동차 보안 기술 개발은 매우 중요하다. 차량용 침입탐지 기술은 자동차 해킹에 대응하기 위해 연구되고 있는 가장 대표적인 자동차 보안 기술 중 하나지만, 현재 제품화 가능한 수준의 차량용 침입 탐지 기술은 모두 주기 메시지에 대한 침입 탐지 여부만 분석이 가능하고 주기 메시지와 이벤트 메시지가 혼합된 형태인 PE (Periodic-and-on-Event) 메시지에 대해서는 분석이 어렵다. 본 논문에서는 PE 메시지를 이용하여 자동차 내부 네트워크에 침입하는 공격자 유형을 분류하고 이를 탐지할 수 있는 기법을 제안한다. 그리고 실제 차량에서 제안하는 기법을 우리의 공격자 모델에서 평가한 결과 0%의 FPR과 FNR을 보여준다.

ABSTRACT

To provide convenience and safety of drivers, the recent vehicles are being equipped with a number of electronic control units (ECUs). Multiple ECUs construct a network inside a vehicle to share information related to the vehicle's status; in addition, the CAN protocol is normally applied. As the modern vehicles provide highly convenient and safe services, it provides many types of attack surfaces; as a result, it makes them vulnerable to cyber attacks.

The automotive IDS (Intrusion Detection System) is one of the promising techniques for securing vehicles. However, the existing methods for automotive IDS are able to analyze only periodic messages. If someone attacks on non-periodic messages, the existing methods are not able to properly detect the intrusion. In this paper, we present a method to detect intrusions including an attack using non-periodic messages. Moreover, we evaluate our method on the real vehicles, where we show that our method has 0% of FPR and 0% of FNR under our attack model.

Keywords: CAN (Controller Area Network), In-vehicle Network, Security, Automotive Intrusion Detection System

Received(01. 22. 2021), Modified(04. 14. 2021), Accepted(04. 16. 2021)

* 이 논문은 2021년도 정부(교육부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업(No.NRF-2020R1C1C1007446) 그리고 현대자동차의 지원으로 수행되었음

† 주저자, seyoung0131@korea.ac.kr
‡ 교신저자, wonsuk@hansung.ac.kr(Corresponding author)

I. 서 론

운전자의 운전 편의성 (Convenience) 또는 안정성 (Safety)를 제공하기 위해, ECU (Electronic Control Unit)이라 불리는 전자제어장치가 차량에 탑재되고 있다. 과거 기계적 방식에 의하여 제어되던 차량의 일부 기능을 ECU에 의하여 전자적으로 제어함으로써 운전 편의성과 안정성이 향상될 수 있다. 예를 들어, 운전자가 브레이크를 작동시키지 않았다 하더라도, 전방에 장애물이 감지되어 충돌이 예상되는 경우 자동적으로 차량의 브레이크를 작동시킨다. 고급 차량의 경우 약 70개의 ECU가 탑재되어 있으며, 다수의 ECU가 차량에 탑재되었다는 것은 차량의 여러 기능들이 각각 ECU에 의해 전자적으로 제어되고 있음을 의미한다[1]. 차량에 탑재되어 있는 여러 ECU들은 자동차 내부에서 네트워크를 구성하여 차량의 상태정보를 송·수신한다. 그리고 자동차 내부 네트워크 통신 프로토콜로써 CAN (Controller Area Network)가 사용되고 있다. CAN 프로토콜은 1983년 독일의 Bosch 社에 의하여 개발된 데이터 통신 프로토콜이며, 높은 신뢰성으로 인해 현재까지도 대부분의 자동차 제조회사에서 자신들의 자동차 내부 네트워크에 적용하여 사용하고 있는 사실 표준 (De-facto Standard)이다.

과거 전통적인 자동차와 비교하였을 때, 현대의 자동차들은 ICT (Information and Communications Technology) 기술과 융합하여 자율주행과 같이 최첨단 서비스를 제공할 수 있게 되었다. 하지만, ICT 기술은 운전 편의성이나 안정성 향상과 동시에 사이버보안 위협에 대한 Attack Surface를 증가시킨다. 실제로 2010년 Koscher et al. 연구팀은 운전자가 운전석에 탑승하지 않은 상태에서 CAN 통신 프로토콜이 적용되어 있는 자동차 내부 네트워크에 차량 제어 메시지를 주입함으로써 해당 차량을 제어하는 것이 가능함을 최초로 시연하였다[1]. 2013년과 2015년에는 C. Miller와 C. Valasek이 해킹 분야에서 세계적 컨퍼런스인 DEFCON과 BlackHat US에서 자동차도 컴퓨터 시스템과 마찬가지로 사이버보안 공격으로부터 안전하지 않다는 것을 보여주었다[7,10]. 특히, C. Millier와 C. Valasek가 발표한 보고서에는 실험에 사용한 자동차에 대한 정보뿐만 아니라, 자신들이 사이버보안 취약점을 분석하면서 경험하였던 시행착오까지 모두 공개하였다. C. Miller와 C. Valasek의 연구결과로 인해 학계와 산업계 모두 자동차 보안에 대한 중요성을 인지할 수 있는 기회가 되었다. 특히, 비전문가까지 자동차 해킹 방법에 대하여 이해할 수 있었으며, 이와 함께 자동차 보안 기술에 대한 연구도 함께 발전시킬 수 있는 기회를 제공하였다.

과거에는 자동차와 관련된 사이버보안 기술이 잠재적인 수요였다면, 최근에는 위에서 설명한 것과 같은 실질적 보안 위협으로 인해 자동차 사이버보안과 관련된 현실적 요구사항 및 의무사항이 등장하고 있다. 특히, 유엔유럽경제위원회 (United Nations Economic Commission for Europe, UNECE)의 WP.29의 자동차 사이버 보안 요구사항과 관련된 법규가 채택됨에 따라 2022년 7월 유럽에서 등록되는 모든 차량에 자동차 사이버 보안을 위한 기술적 조치가 의무화되었다. UNECE 법규는 자동차 산업에서 법적 구속력이 있는 최초의 국제 표준 법률이며, 유럽의 54개 협약국뿐만 아니라 자동차 안전기준 국제조화 및 상호인증에 관한 협정에 따라 한국과 일본도 동일한 법규를 채택할 예정이다. 따라서, 대부분의 글로벌 자동차 제조회사들은 자신들의 차량을 판매하기 위해 UNECE 법규를 반드시 만족해야 한다.

자동차 보안 분야에서는 관련된 기술 개발의 시급성으로 인해 학계와 산업계 모두 상용화 수준의 기술 개발을 목표로 연구가 진행되고 있다. 특히, 자동차 내부 네트워크의 비정상 트래픽을 탐지하는 차량용 침입탐지 기술인 Automotive IDS (Intrusion Detection System)에 대한 연구가 활발히 진행되고 있다[2,3,4,5,6,12,13,15]. Automotive IDS는 자동차 내부 네트워크에서 송·수신되는 메시지들을 분석하여 정상 또는 비정상 상태 여부를 판단함으로써, 차량 해킹으로 인해 악의적으로 주입되는 메시지를 탐지한다. 앞에서 언급한 자동차 해킹 방법들은 모두 차량 제어를 위한 메시지를 자동차 내부 네트워크에 주입하기 때문에, Automotive IDS에 의하여 탐지될 수 있다. 게다가, Automotive IDS는 현재 자동차 내부 네트워크 구조에서 시스템 변경 없이 적용이 가능한 장점을 갖기 때문에 자동차 제조회사로부터 더욱 많은 관심을 받고 있다. 그러나 안타깝게도 지금까지 제안된 Automotive IDS는 자동차 내부 네트워크에서 주기 메시지만 분석이 가능할 뿐, 주기 및 비주기가 혼합된 형태의 메시지를 대상으로는 정상 또는 비정상 여부를 판단할 수 없다. 주기적으로 전송되는 메시지 중 차량의 상태가 변경되는 특정 이벤트가 발생 시에 추가적인 메시지가 비주기적

으로 전송된다. 우리는 이러한 메시지를 PE (Periodic- and-on-Event) 메시지라 부른다. 이는 PE 메시지를 이용하여 차량 제어를 시도하는 차량 해킹에 대하여, 지금까지 제안된 Automotive IDS 기술로는 탐지가 어렵다는 것을 의미한다.

본 논문에서는 실제 차량에서 PE 메시지가 전송될 때, 메시지의 주기성을 분류하여 제시한다. 그리고 이를 바탕으로 PE 메시지 중 이벤트 (On-Event) 메시지가 전송되었을 때 해당 메시지가 정상 또는 비정상 여부를 탐지할 수 있는 기법을 제안한다. 마지막으로, 실제 차량을 이용하여 여러 가지 상황에서 수집된 데이터를 이용하여 우리가 제안하는 기법이 PE 메시지 CAN ID를 이용하여 악의적으로 주입되는 메시지를 올바르게 탐지할 수 있음을 보여주도록 하겠다.

II. 관련연구

2.1 자동차 해킹

2010년 Koscher et al. 은 자동차의 내부 CAN 통신을 분석할 수 있는 CARShark 도구를 제작하여 전송되는 CAN 메시지를 분석하였으며 분석된 CAN 메시지를 CAN Bus에 주입하여 자동차의 일부 기능을 임의로 제어할 수 있음을 처음으로 입증하였다[1]. 2013년 C. Miller와 C. Valasek은 공격자가 자동차의 CAN 네트워크에 물리적으로 접근한다는 가정하에 Toyota와 Ford 자동차를 대상으로 도어락 해제, 브레이크, 가속 등 자동차를 강제 제어하는 CAN 메시지 주입 공격을 발표하였다[7]. 자동차 내 CAN Bus에 전송되는 메시지들은 암호화와 인증 등의 보안 메커니즘이 적용되지 않았기 때문에 CAN Bus에 전송되는 메시지 분석과 임의의 CAN 메시지 주입이 가능하였다. 이후 공격자가 자동차의 CAN Bus에 물리적인 접근 없이 CAN 네트워크에 접근하여 공격 CAN 메시지를 주입하는 방법과 관련한 연구가 수행되었다[8,9,10]. C. Miller와 C. Valasek은 공격자가 CAN Bus로 접근 가능한 다양한 유무선 Attack Surface에 대해 조사하고 접근 방법과 통신 거리에 따라 분류를 수행하였다. 예를 들어, 공격자는 CAN Bus와 연결되어 있는 자동차의 인포테인먼트 시스템을 타겟으로 해당 시스템에서 지원하는 CD Player나 USB 포트를 통해 악성 프로그램을 실행시켜 CAN Bus 상으로 공격 CAN 메시지 주입이 가능함을 시사하였다. Foster et al. 연구팀은 자동차의 진단을 위해 사용되는 OBD-Ⅱ (On-Board Diagnostic version Ⅱ) 포트를 악용한 공격 방법을 제시하였다[9]. 해당 포트는 CAN 버스와 연결되어 있으므로 공격자가 악의적인 텔레매틱장치를 애프터마켓에 판매하여 해당 장치가 연결된 자동차를 대상으로 원격에서 공격 CAN 메시지 주입이 가능함을 시연하였다. C. Miller와 C. Vlasek은 공격자가 사전에 OBD-Ⅱ에 공격 장치를 연결하여야 한다는 가정 없이 원격에서 자동차 해킹이 가능함을 시연하였다[10]. Jeep Cherokee 자동차에서 외부 네트워크 통신을 제공하는 텔레메틱스 시스템의 취약점을 분석하여 해당 장치를 악의적으로 업데이트 이후 원격에서 자동차에 접근하여 악의적인 CAN 메시지를 주입함으로써 가속, 핸들 조향, 브레이크 등 강제 제어 공격이 가능함을 발표하였다. [11]은 Tesla model S 자동차를 대상으로 웹 브라우저 취약점을 분석하였으며 해당 취약점을 통해 CAN 네트워크에 접근하여 자동차의 강제 제어 공격을 보였다.

2.2 Automotive IDS

CAN Bus에 주입되는 공격 CAN 메시지를 탐지하기 위해 Automotive IDS 연구가 꾸준히 연구되고 왔다. Automotive IDS 기법은 CAN 표준 프로토콜을 위배하지 않으며 현재 자동차에 바로 적용 가능하다는 장점이 있으며 CAN Bus 상에 발생 되는 다양한 패턴 및 특성을 분석하여 정상 또는 공격 CAN 메시지를 탐지한다. Automotive IDS 기법들은 CAN Bus 상에 전송되는 메시지의 통계적 특성을 이용하는 접근법과 ECU의 고유한 하드웨어 특성을 이용하는 접근법으로 분류할 수 있다.

2.2.1 통계적 특성

Taylor et al. 과 Song et al. 은 CAN Bus에 전송되는 CAN 메시지의 주기성을 이용하여 공격을 탐지하는 IDS 기술을 제안하였다[4,12]. 대부분의 CAN 메시지는 정상 상황에서 일정 주기로 Bus에 전송되기 때문에 정상 시간 인터벌보다 짧은 인터벌로 전송되는 CAN 메시지에 대해 공격으로 탐지한다. Muter et al. 은 정상과 공격 상황에서 CAN Bus에 전송되는 CAN ID들의 엔트로피를

분석하여 공격을 탐지하였다[13]. 정상 상황에서 주기적으로 전송되는 CAN ID 메시지에 의해 측정된 엔트로피와 달리 특정 CAN ID 메시지가 다수 주입되는 공격 상황에서는 해당 CAN ID의 엔트로피 값이 증가하므로 공격 탐지가 가능하다. 그러나 주기적으로 전송되는 CAN 메시지와 달리 PE 메시지는 특정 이벤트 발생 시에 주기성이 유지되지 않으므로 주기성을 이용한 통계적인 방법을 사용하여 공격을 탐지할 수 없다.

2.2.2 하드웨어 특성

Cho, K, T et al. 은 ECU를 구성하는 clock source의 하드웨어 특성을 반영하는 clock skew를 이용하여 공격을 탐지하고 ECU를 식별하는 기법을 제안하였다[2]. 동일한 주기로 메시지를 전송하는 ECU라 할지라도 하드웨어의 clock source의 특성으로 인해 서로 다른 고유한 clock skew를 가진다. 따라서 CAN 메시지의 clock skew가 특정 값 이상으로 변동될 경우 이를 공격으로 탐지하는 기술을 설계하였다. 그러나 최근 ECU의 clock skew를 알고 있는 공격자는 clock skew를 모방하여 공격 CAN 메시지 주입이 가능하다는 연구 결과가 발표되었다[14]. 또한, ECU의 하드웨어 특성인 전압(Voltage) 신호를 이용하여 공격을 탐지하고 공격 ECU를 식별하는 연구도 수행되었다[3,6,15]. 각 ECU에 공급되는 전압 차이로 인해 ECU가 생성하는 CAN 신호는 ECU마다 유일하다. 즉, 동일한 CAN 메시지를 전송하더라도 ECU의 특성에 따라 아날로그 전압 신호는 서로 다른 형태를 가진다는 점을 이용하여 공격을 탐지한다. 해당 방법은 CAN Bus에 전압 레벨 측정을 위한 추가적인 하드웨어가 필요하다는 한계점이 있다.

III. 배경지식

3.1 전자제어장치 (ECU)

과거 기계적으로 자동차가 조작됨과 다르게 최신 자동차는 운전자 편의성과 안전성을 위해 전자적으로 내부 시스템을 제어하는 ECU가 발전되었다. ECU는 CAN 컨트롤러, CAN 트랜시버, MCU (Micro Controller)로 구성되어 있다. CAN 컨트롤러는 내부 버퍼를 가지고 있으며 트랜시버로부터 전달된 메시지에 대한 수신 여부를 메시지 ID를 확인하여 판별하고 수신한 메시지를 MCU로 전달한다. 반대로 MCU에서 전송하는 메시지는 CAN 컨트롤러를 통해 트랜시버로 전달된다. CAN 트랜시버는 컨트롤러에서 송신 요청된 메시지를 전기적인 신호르 바꾸어 CAN Bus로 전송하거나 CAN Bus로부터 전기 신호를 읽고 이를 디지털로 변환하여 컨트롤러에게 메시지를 전달한다. MCU는 ECU의 제어를 담당하며 CAN 메시지를 해석하여 처리하거나 CAN Bus로 CAN 메시지 전송을 요청한다.

3.2 CAN 프로토콜

자동차 내부에 탑재되는 ECU가 증가 되고 그에 따라 ECU 간의 효율적인 통신을 위해 제안된 Bus형 통신 구조이다. CAN은 멀티 마스터 통신 방식으로 CAN Bus에 연결된 모든 ECU가 Bus가 유후인 경우 언제든지 메시지 전송이 가능하다. CAN Bus는 전기적인 신호로 통신하기 위해 꼬인 2선(twisted-pair wire) 형태로 CAN_H (CAN High)와 CAN_L (CAN Low)로 구성되어 있으며 잡음 (noise)에 견고하기 위해 두 라인의 전압 차이를 이용하여 통신을 수행한다. CAN_H와 CAN_L에 각각 3.5V와 1.5V의 전압을 전송한 경우, 전압 차이는 2V이며 디지털 0 (dominant) bit를 의미한다. CAN_H와 CAN_L 모두 2.5V 전압을 전송하는 경우, 전압 차이가 0V이며 디지털 1 (recessive) bit를 의미한다.

3.3 데이터 프레임

CAN 프로토콜의 표준 데이터 프레임은 Fig. 1과 같이 SOF (Start Of Frame), Arbitration ID, Control, Data, CRC (Cyclic Redundancy Check), ACK (Acknowledge), EOF (End Of Frame) 7개의 영역(Field)으로 구성되어 있다. 표준 CAN 2.0A 형식은

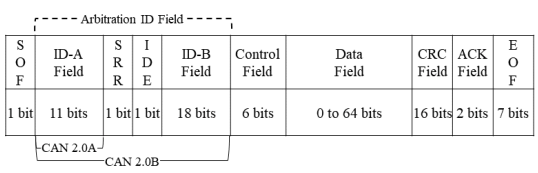

Fig. 1. CAN Data Frame

Arbitration ID 영역 내 11bit ID를 사용하고 확장 CAN 2.0B 형식은 29bit ID를 사용한다.

3.4 Arbitration

CAN은 CSMA/BA (Carrier Sense Multiple Access/Bitwise Arbitration) 기법이 적용된 브로드캐스트 통신 방식으로 송신 ECU의 Arbitration ID field를 바탕으로 CAN Bus에서의 통신 우선순위를 결정한다. 낮은 Arbitration ID field를 가지는 메시지가 더 높은 우선순위를 가진다. 즉, 두 ECU가 동시에 CAN Bus에 데이터 프레임 전송 시 우선순위가 높은 CAN 메시지가 통신 경합에서 이기게 되며 메시지 전송을 수행하고 우선순위가 늦은 CAN 메시지는 전송이 중지된다. 통신 경합에서 진 ECU는 다음 Bus Idel 상태에서 메시지 전송을 재시도 한다.

IV. 공격자 모델

이번 장에서는 자동차 내부 네트워크에 악성 메시지를 주입하여 차량을 악의적으로 제어하는 공격자 모델에 대하여 설명하겠다. 지금까지 소개된 자동차 해킹관련 연구는 대부분 자동차 내부 네트워크에 악성 메시지를 주입함으로써 차량을 임의로 제어하였다. 따라서, 자동차 내부 네트워크의 트래픽을 분석하여 악성 메시지 주입을 탐지하는 Automotive IDS 기술에 대한 연구가 활발히 진행되고 있다. 하지만, 메시지의 전송 주기 분석 결과를 기반으로 악성 메시지 주입을 탐지하는 Automotive IDS는 PE 메시지의 이벤트 메시지를 이용하여 주입하는 경우에는 제대로 탐지하지 못한다. 본 논문에서는 기존 Automotive IDS들이 제대로 탐지하지 못하는 공격 유형을 공격자 모델로 정의한다. 또한, 공격자 모델은 이벤트 메시지를 주입하는 방법에 따라 2가지 유형으로 구분한다. Type I 공격자는 PE 메시지 CAN ID를 이용하여 이벤트 메시지를 주기적으로 전송하는 공격자를 의미한다. 일반적으로는 공격자가 자동차 내부 네트워크를 장악하기 위해 매우 짧은 주기로 악성 메시지를 주입하는 것이 일반적이다. 게다가, 딜레이 없이 계속해서 메시지를 주입할 수도 있다. Type II 공격자는 정상 이벤트 메시지가 전송될 때 메시지의 개수와 이벤트 메시지 간의 시간 간격을 정상적인 이벤트 메시지 전송과 똑같이 하여 주입하는 공격자를 의미한다. Type II 공격의 경우에는 사전에 공격 대상이 되는 PE 메시지의 이벤트 메시지의 개수와 전송주기를 알고 있어야 한다.

V. CAN 메시지 전송 유형

자동차의 여러 기능을 전자적으로 제어하기 위하여, 여러 개의 ECU들이 자동차에 탑재되어 동작하고 있다. 이러한 전자제어장치는 자동차 내부에서 네트워크를 구성하여 차량의 상태 정보나 제어 메시지를 공유하고, 네트워크 구성을 위하여 일반적으로 CAN 프로토콜이 사용되고 있다. 따라서, ECU들은 CAN 프로토콜에서 정의되어 있는 데이터 프레임을 이용하여 CAN 메시지를 자동차 내부 네트워크에 브로드캐스트 전송한다. CAN 메시지의 내용에 따라, ECU는 CAN 메시지를 주기적 또는 비주기적으로 전송한다. 그리고 일부 메시지의 경우에는 주기적으로 전송되는 과정에서 차량의 상태가 변경되는 이벤트가 발생되는 경우 비주기 메시지가 추가적으로 전송되는 혼합된 형태로 메시지를 전송한다. Fig. 2는 실제 차량의 내부 네트워크에서 전송되는 CAN 메시지들의 전송 유형 3가지를 보여주고 있다. Fig. 2-(a)는 일정한 시간 간격을 갖고 주기적으로 전송되는 메시지의 전송시간을 보여주고 있다. Fig. 2-(b)는 자동차의 상태가 변경되는 이벤트가 발생할 때에만 전송되는 메시지의 전송시간을 보여주고 있다. 예를 들어 자동차의 엔진이 켜질 때, 현재 차량의 상태를 확인하기 위해 CAN ID 0x7D0를 이용하는 진단 (Diagnostic) 메시지가 전송된다. 이러한 진단 메시지는 엔진이 켜지는 이벤트가 발생할 때에만 전송된다. 마지막으로, 주기 메시지와 이벤트 메시지가 혼합된 형태로 전송되는 PE 메시지가 있다. Fig. 2-(c)는 일정한 시간 간격을 갖고 전송되는 주기 메시지의 전송시간과 이벤트 메시지의 전송시간을 혼합하여 보여주고 있다. 본 논문에서 CAN 메시지 수집을 위해 사용한 차량의 경우, PE 메시지 전송 유형 중 차량의 상태가 변경되는 이벤트가 발생하는 경우 연속된 3개의 이벤트 메시지가 전송되는 것을 확인하였다. 이는 자동차 제조회사마다 조금씩 차이가 있는 것으로 알려져 있다.

우리가 제안하는 기법은 PE 메시지 전송 유형 중 이벤트 메시지가 전송될 때 정상 또는 비정상 여부를 판단하는 방법이기 때문에, PE 메시지의 전송 유형에 대하여 자세히 설명하도록 하겠다. PE 메시지 전

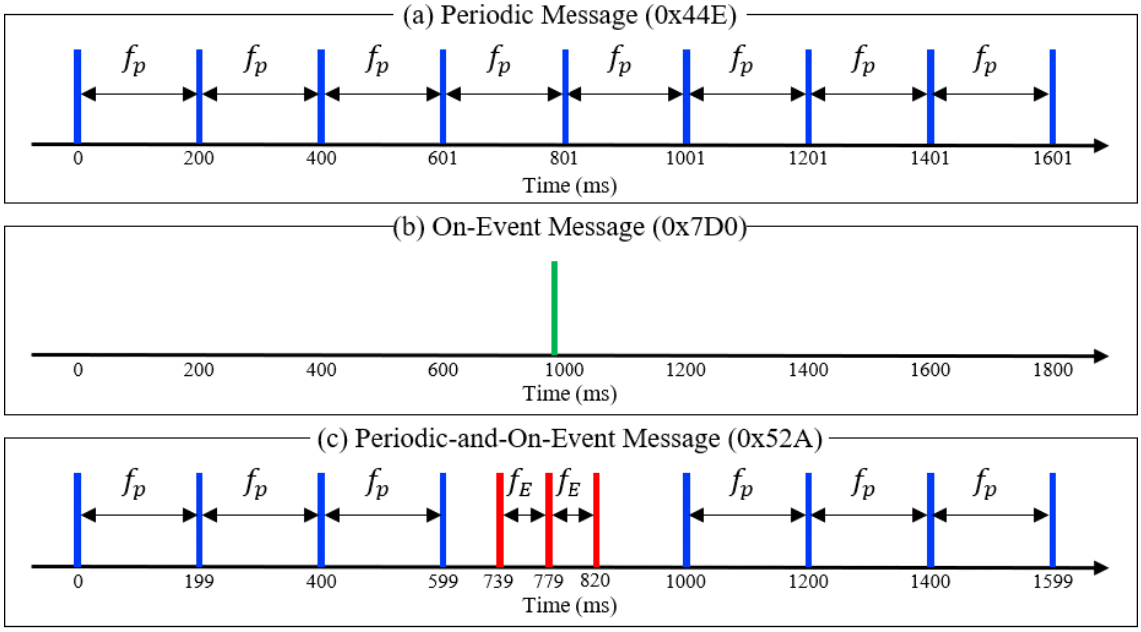

Fig. 2. Three different message transmission types (a) Top: Periodic message, (b) Middle: On-event message, (c) Bottom: PE message

송 유형은 차량의 상태정보를 주기적으로 알리기 위해 주기 메시지가 일정 주기로 전송된다. 그리고 차량의 상태정보가 변경되는 이벤트가 발생하였을 때, Fig. 3에서 보여주는 것처럼 연속된 3개의 이벤트 메시지가 전송된다. 이벤트가 한번 발생하게 되면 그에 대응되는 이벤트 메시지는 3개를 하나의 쌍으로 하여 전송된다. 그리고 3개의 이벤트는 서로 40ms의 시간 간격을 갖고 있어 3개 이벤트 메시지가 모두 전송되는 80ms의 시간이 필요하다. 3개의 이벤트 메시지가 전송되는 시간과 주기 메시지가 전송되는 시간이 겹치는지 여부에 따라서 PE 메시지의 전송 유형은 2가지로 구분된다. Fig. 3-(a)는 2개의 주기 메시지 사이에 3개의 이벤트 메시지가 전송되는 경우를 보여주고 있으며, Fig. 3-(b)는 3개의 이벤트 메시지가 전송되는 시간과 주기 메시지가 전송되는 시간이 겹치는 경우를 보여주고 있다. 이렇게 시간이 겹치는 경우에는 한번의 주기 메시지 전송이 생략되게 된다.

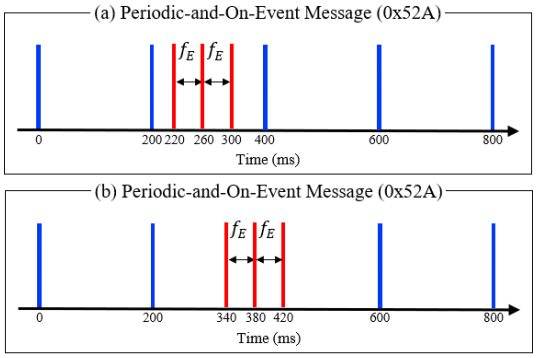

Fig. 3. PE message transmission types

VI. 제안기법

이번 장에서는 주기 메시지와 이벤트 메시지가 함께 혼합되어 전송되는 형태인 PE 메시지를 분석하는 기법을 제안한다. 제안하는 기법에 대한 이해를 쉽게 하기 위해, 제안하는 기법을 i) 주기 메시지 분석, ii) 이벤트 메시지 분석, iii) 침입 탐지로 구분하여 설명하겠다.

6.1 주기 메시지 분석

PE 메시지는 주기 메시지와 이벤트 메시지로 구별할 수 있으며, 주기 메시지는 일정한 시간 간격으로 주기적으로 전송되는 메시지를 의미한다. PE 메

시지를 전송하는 ECU는 사전에 정해진 주기로 주기 메시지 전송을 요청하지만, 실제 네트워크에 해당 메시지가 전송되는 것은 조금의 Delay가 발생한다. Delay가 발생되는 주요 원인 중 하나는 CAN Bus에 연결된 여러 개의 ECU가 동시에 메시지 전송을 시도할 때, arbitration 과정을 수행하고 우선순위가 낮은 메시지의 경우 우선순위가 높은 메시지들이 모두 전송이 완료될 때까지 기다리기 때문에 발생한다. 따라서, 주기 메시지의 주기성을 분석할 때 해당 Delay를 고려하여야 한다. Fig. 4.는 실제 차량에서 주기 메시지들이 전송되는 시간 간격의 분포를 보여주고 있다. 예를 들어, 10ms의 주기로 전송되는 CAN ID 0x316의 경우 시간 간격이 일정하지 않음을 알 수 있다. 그리고 10ms 보다 더 짧은 시간 간격이 있음을 알 수 있다. 이는 Delay로 인해 시간 간격이 길어졌다, 다시 정상 간격으로 메시지가 전송되면 상대적으로 시간 간격이 짧아진 것으로 보이기 때문이다. 따라서, 사전에 설정된 주기 메시지의 주기 f_P로 연속적으로 전송되는 주기 메시지의 시간 간격 t는 하한 값 lb_P와 상한 값 ub_P를 갖는 일정 구간 안에 들어가게 되며 이를 식으로 표현하면 아래와 같다.

$$f_P - lb_P \leqq t \leqq f_P + ub_P \quad (1)$$

본 기법에서는 PE 메시지 중 주기 메시지의 주기성

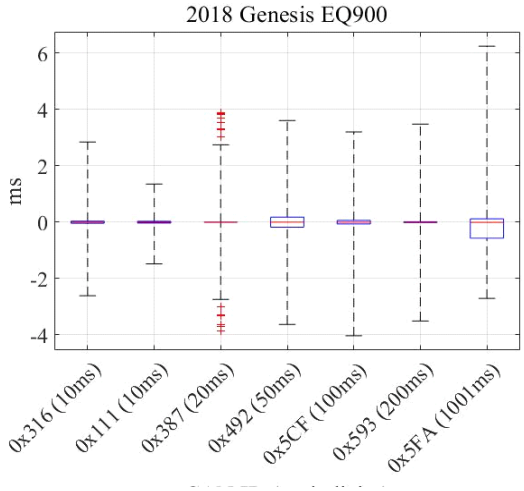

Fig. 4. Distribution of time intervals as a function of CAN IDs

을 위반하는지 판단하기 위하여 위 식 (1)을 이용한다. 만약, 주기 메시지 분석 결과가 주기 위반을 하는 경우 제안하는 기법에서는 공격 메시지 또는 이벤트 메시지로 간주하게 된다. 다음에 설명할 이벤트 메시지 분석 방법을 이용하여 해당 메시지가 정상 또는 악성 여부를 결정한다.

6.2 이벤트 메시지 분석

PE 메시지 중 이벤트 메시지가 전송되면, 주기 메시지의 주기성이 유지되지 않는다. 앞서 설명한 주기 메시지 분석 과정에서 이벤트 메시지가 전송되었을 때, 해당 메시지가 정상적인 이벤트 메시지 전송된 것인지 악성 메시지가 주입된 것인지 추가적인 분석이 필요하다. 5장에서 설명한 것처럼, 차량의 상태가 변경되는 이벤트가 변경되었을 때, PE 메시지 중 이벤트 메시지는 n번 전송된다. 우리가 실험한 실제 차량의 경우에는 항상 3개의 이벤트 메시지가 전송되었다. 그리고 n개의 이벤트 메시지는 일정한 주기를 갖고 전송된다. 우리가 실험한 차량의 경우에는 40ms의 주기로 전송되었다.

주기 메시지의 주기를 위반한 메시지에 대하여, 우리는 이벤트 메시지 여부를 식 (2)와 같이 확인한다. 이는 주기 메시지의 주기성 위반 여부를 확인하기 위한 방법과 매우 유사하다. f_E는 이벤트 메시지들의 전송 주기이며, lb_E와 ub_E는 연속적으로 전송되는 이벤트 메시지의 시간 간격 하한 값과 상한 값을 나타낸다.

$$f_E - lb_E \leqq t \leqq f_E + ub_E \quad (2)$$

주기 메시지를 분석하는 방법과의 차이점은 3개의 연속된 메시지를 확인하는 것이다. 다시 말해, 주기 메시지의 주기를 위반한 메시지가 발견되었을 때, 연속된 3개의 메시지가 이벤트 메시지의 주기성을 확인함으로써 이벤트 메시지 여부를 판단한다.

6.3 침입 탐지

앞서 설명한 것처럼 주기 메시지의 주기성을 위반한 메시지의 경우 이벤트 메시지 분석 과정을 거쳐, 이벤트 메시지의 주기성을 위반한 경우 우리의 기법은 해당 메시지를 악성 메시지로 판단하고 자동차 내

부 네트워크의 침입이 발생하였다고 탐지한다.

그리고 정상적인 이벤트 메시지로 분석된 경우, 해당 이벤트 메시지를 제외하고 나머지 메시지들이 다시 주기 메시지의 주기성 위반 여부를 판단한다. 5장에서 설명한 것과 같이, PE 메시지에서 3개의 이벤트 메시지가 전송된 이후 전송되는 주기 메시지는 이벤트 메시지 전송 타이밍과 주기 메시지가 전송되는 타이밍이 겹치지 않는 경우와 겹치는 경우로 발생 가능하다. 겹치는 경우에는 해당 타이밍의 주기 메시지의 전송을 생략하게 된다. 따라서, 이벤트 메시지를 제외한 상태에서 주기 메시지의 주기성 위반 여부를 판단할 때에는 주기 또는 주기의 2배의 되는 경우가 존재한다는 사실을 반영하여야 한다. Fig. 5는 제안하는 기법을 알고리즘으로 표현하여 설명하고 있다.

Algorithm 1 Intrusion Detection for PE Message

```
Inputs:
    ID: Target CAN ID
    f_P: Frequency of periodic message
    f_E: Frequency of event message
Initialize:
    t_init ← first time ID is monitored
    event ← False
    N ← Number of event messages
while message with ID arrives do
    t ← time − t_init
    if event then
        t ← time − t_temp
        if (f_P − lb_P ≤ t ≤ f_P + ub_P) or
                (2 * f_P − lb_P ≤ t ≤ 2 * f_P + ub_P) then
            event, t_init ← false, time
            continue            /* Normal periodic message */
        else
            break               /* Attack message */
    if f_P − lb_P ≤ t ≤ f_P + ub_P then
        t_init ← time           /* Normal periodic message */
    else
        t_temp, n, t_Einit ← t_init, 1, time
        while message with ID arrives do
            t ← time − t_Einit
            if f_E − lb_E ≤ t ≤ f_E + ub_E then
                n, t_Einit ← n + 1, time
                if n==N then
                    event ← True
                    break       /* Normal event message */
            else
                break           /* Attack message */
```

Fig. 5. Algorithm for intrusion detection

VII. 평가

7.1 실험환경

우리가 제안하는 기법을 평가하기 위하여, 우리는 실제 차량의 내부 네트워크에서 데이터를 수집하였다. Fig. 6은 평가를 위해 사용된 차량인 2018년식 Genesis EQ900과 자동차 내부 네트워크에 접근하여 데이터 수집을 위한 실험 환경을 보여주고 있다. 차량의 내부 네트워크에서 송·수신되는 메시지 중 PE 메시지들을 차량에서 이벤트를 직접 발생시켜가면서 확인을 하였다. Table 1은 자동차 내부 네트워크에 존재하는 PE 메시지 CAN ID와 주기 메시지의 주기, 자동차의 상태가 변경될 때 발생하는 이벤트 메시지의 개수와 그 메시지들 간의 간격을 보여주고 있다.

제안하는 기법을 평가하기 위한 평가지표로써, 우리는 FPR (False Positive Rate)와 FNR (False Negative Rate)를 다음과 같이 정의하여 평가에 사용한다.

- **FPR**: 정상 이벤트 메시지를 악성 메시지로 오탐하는 경우의 비율
- **FNR**: 주입된 악성 메시지를 정상 이벤트 메시지로 미탐하는 경우의 비율

FPR과 FNR을 평가하기 위해서는 주기 메시지의 주기 위반 여부를 확인하여야 한다. 사전에 정해진 주기로 ECU에서 주기 메시지 전송이 요청되지만 CAN Bus 상 Arbitration 과정, ECU의 Process delay 등으로 인해 정확히 정해진 주기대로 CAN Bus에 나타나지 않는다. 우리는 Fig. 4와 같이 실험적으로 대다수의 주기 메시지가 정해진 주기의 ±5ms 범위 이내의 오차를 두고 CAN Bus에 주기적으로 전송됨을 확인하였다. 따라서 주기성 위반 여부를 확인하기 위해, Fig. 4에서 보여주었던

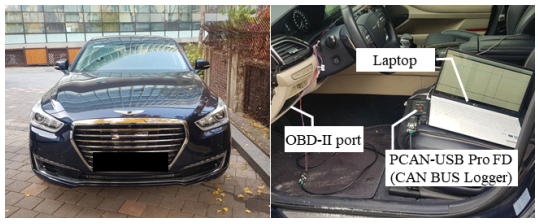

Fig. 6. Evaluation setup

결과 값을 활용하여 ±5ms의 Threshold를 사용한다.

7.2 정상 이벤트 메시지

이번 소절에서는 제안하는 기법의 FPR을 평가하기 위하여, 차량의 상태를 변경하면서 PE 메시지에서 이벤트 메시지가 전송되도록 하였다. 이렇게 발생하는 이벤트 메시지는 정상 메시지로써 제안하는 기법이 정상으로 판단해야 하고, 악성으로 판단하는 경우에는 FPR의 비율이 높아지게 된다. 자동차 내부 네트워크에 이벤트 메시지가 전송되게끔 하기 위해, 우리는 차량의 문을 열거나 닫고, 차량이 후진할 때 차량 뒤쪽에 장애물을 놓는 등의 행위를 하였다. Table 2는 정상 이벤트 메시지에 대하여 제안하는 기법의 FPR을 보여주고 있다.

위 결과로부터 제안하는 기법은 모든 CAN ID에 대하여 FPR의 0%인 것을 확인할 수 있다. CAN ID 0x55B인 PE 메시지의 경우 총 139번의 차량의 상태 변화 이벤트 (서라운드 뷰 변경) 발생 시 14번의 이벤트에서 상태 변화를 한번 시켰음에도 불구하고 그에 대한 3개의 이벤트 메시지가 연속적으로 2회 전송되는 현상을 확인하였다. 연속적으로 전송된 이벤트 메시지로 인해 이벤트 메시지를 제외한 주기 메시지의 간의 주기가 정상 주기를 벗어나게 되었으며, 이로 인해 14번의 오탐이 발생하게 되었다. 해당 오탐을 없애기 위해 연속적 이벤트 메시지 전송이 확인된 경우, 주기 오차를 추가로 반영 (±5ms) 하여 모든 정상 이벤트 메시지 전송 후에도 오탐이 발생하지 않도록 하였다.

Table 1. A list of PE messages from Genesis EQ900

PE Message list			
CAN ID	Frequency of periodic messages	Number of event messages	Frequency of event messages
Changing unit of temperature (°C -〉 °F)			
0x043	1000ms	3	40ms
Changing gears (e.g., P-〉R, P-〉D)			
0x52A	200ms	3	40ms
Opening and closing front doors			
0x541	100ms	3	40ms
Turning on and off head light			
0x553	200ms	3	40ms
Changing states of parking assist camera			
0x55B	600ms	3	40ms

Table 2. False positive rate on normal event messages

CAN ID	# of normal events	# of detections	FPR (%)
0x043 (1000ms)	100	0	0.00
0x52A (200ms)	105	0	0.00
0x541 (100ms)	104	0	0.00
0x553 (200ms)	100	0	0.00
*0x55B (600ms)	139	0	0.00

*0x55B의 경우 다른 CAN ID 들과 달리 3개의 이벤트 메시지가 연속적으로 2회 전송되는 경우가 발견되었으며 (139번 중 14번), 추가 분석을 통해 연속적으로 전송된 이벤트 메시지가 확인된 경우에도 오탐이 발생하지 않도록 한 결과를 표시하였음

7.3 Type I 공격자 탐지

Type I 공격자는 PE 메시지 중 이벤트 메시지를 주기적으로 주입함으로써 차량의 오작동을 유발하는 공격 방법이다. Type I 공격 유형에 대하여 제안하는 기법을 평가하기 위하여, 우리는 실제 차량에서 PE 메시지 CAN ID를 이용하여 메시지를 주기적으로 주입하였다. 이 때, PE 메시지 중 주기 메시지는 계속해서 일정한 시간 간격으로 전송되고 있는 상태이며 주입한 공격 메시지의 패킷은 정상 메시지와 동일하게 주입하였다. 전송 주기를 기반으로 제안된 기존 Automotive IDS의 경우에는 PE 메시지 CAN ID를 이용하여 메시지를 주입하면, 해당 메시지가 정상적인 이벤트 메시지인지 공격 메시지를 제대로 판단하지 못 한다[2, 4, 12]. Table 3은 메시지 주입 주기별 제안하는 기법의 FPR을 보여주고 있다. 이 수치를 얻기 위하여, 우리는 주입 시간 간격을 1ms, 10ms, 50ms 3가지 경우로 각각 100회 수행하였다.

위 결과에서 우리는 PE 메시지 CAN ID를 대상으로 주입된 모든 공격 메시지를 0%의 FNR로 탐지할 수 있는 것을 확인할 수 있다. 하지만, 주입되는 메시지로 인하여 정상적으로 전송되는 주기 메시

지를 제안하는 기법이 오탐하는 경우가 발생하여 0이 아닌 FPR이 계산되었다.

7.4 Type II 공격자 탐지

Type II 공격자는 차량의 상태가 변경되는 이벤트가 발생하였을 때, 전송되는 연속되는 이벤트 메시지의 개수와 메시지들 간의 시간 간격을 동일하게 하여 주입하는 공격자를 의미한다. 따라서, Type II 공격 유형에 대하여 제안하는 기법을 평가하기 위해 우리는 실제 차량에서 PE 메시지 CAN ID를 이용하여 메시지를 주입하였고, 주입하는 메시지의 개수와 시간 간격을 실제 이벤트 메시지가 전송될 때와 동일하게 하였다. Type I과 동일하게, 주입한 공격 메시지의 패킷은 정상 메시지와 동일한 값으로 주입하였다. 우리의 실험 차량인 제네시스 EQ900의 경우 연속된 3개의 이벤트 메시지가 전송되었고 시간 간격은 40ms 이였다. Table 4는 PE 메시지 CAN ID별 제안하는 기법의 FNR을 보여주고 있다. 이 수치를 얻기 위하 여, 우리는 CAN ID별 40ms 주기로 3번의 이벤트 메시지 주입을 100회를 수행하였다.

우리가 제안하는 기법은 PE 메시지에 이벤트 발생 시 전송되는 이벤트 메시지 개수와 전송 주기를 분석하여 정상 및 비정상 메시지를 판단한다. 따라서 Type II 공격 실험에서 주입한 공격 이벤트 메시지와 정상 주기 메시지 전송 시점이 겹치는 경우, 두 메시지 모두 CAN Bus에 모니터링 되기 때문에 우리가 제안하는 기법은 이를 공격 메시지로 판단한다. 그러나 주입한 공격 이벤트 메시지와 정상 주기 메시지 전송이 겹치지 않는 경우 주입한 주입한 이벤트 메시지와 정상 이벤트 메시지의 전송 주기가 동일하기 때문에 이를 정상 이벤트 메시지로 판단한다. 대부분의 PE 메시지 CAN ID가 200ms 이상의 주기를 가지기 때문에 높은 FNR을 보였다. 다만, CAN ID 0x541의 경우 주기가 100ms로 더 짧은 주기를 가지기 때문에 주입한 공격 이벤트 메시지와 높은 확률로 주기 메시지 전송 시점이 겹치게 되어 더 낮은 FNR 31.67%를 보였다. 즉, 공격 이벤트 메시지 주입 시점과 정상 주기 메시지 전송 시점이 겹치는 경우 우리는 이를 공격 메시지로 올바르게 판단할 수 있다.

Type II 공격 유형에 대한 높은 FNR 에러율을 줄이기 위하여, 우리는 제안하는 기법에서 추가적으로 메시지 패킷의 data 값을 함께 분석하였다. Fig. 7은 CAN ID 0x043의 주기적인 메시지(파란색) 전송과 이벤트 발생 이후 전송되는 이벤트 메시지와 주기 메시지(주황색)의 패킷 data를 보여준다. 즉, 우리가 분석한 PE 메시지들은 고정된 패킷 data로 주기 메시지 전송 중에 이벤트 발생 시, 이벤트 발생을 나타내기 위해 주기 메시지와는 다른 패킷 data 값으로 전송된다. 따라서 이벤트 메시지 전송의 주기성 분석과 패킷 data 필드의 변화를 함께

Table 3. FPRs and FNRs of intrusion detection for Type I attack

CAN ID	Attack Frequency	FPR (%)	FNR (%)
0x043 (1000ms)	1ms	0.00	0.00
	10ms	0.00	0.00
	50ms	0.00	0.00
0x52A (200ms)	1ms	0.00	0.00
	10ms	0.19	0.00
	50ms	0.00	0.00
0x541 (100ms)	1ms	0.00	0.00
	10ms	0.00	0.00
	50ms	0.00	0.00
0x553 (200ms)	1ms	0.00	0.00
	10ms	0.00	0.00
	50ms	1.65	0.00
0x55B (600ms)	1ms	0.00	0.00
	10ms	0.00	0.00
	50ms	0.00	0.00

Table 4. FPRs and FNRs for of intrusion detection for Type II attack

CAN ID	# of attack events	FPR (%)	FNR (%)
0x043 (1000ms)	100	0.00	98.00
0x52A (200ms)	100	0.00	63.00
0x541 (100ms)	100	0.00	31.67
0x553 (200ms)	100	0.00	68.00
0x55B (600ms)	100	0.00	83.00

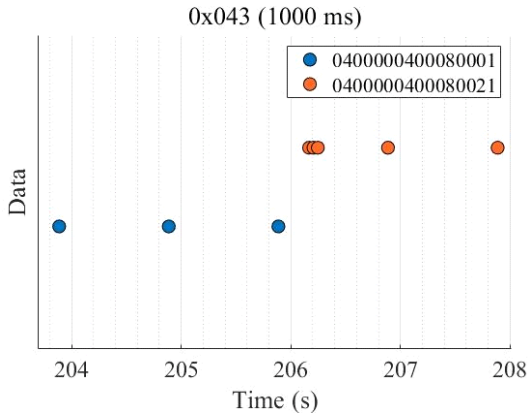

Fig. 7. CAN ID 0x043 messages data

Table 5. FPRs and FNRs of enhanced intrusion detection for Type II attack

CAN ID	# of attack events	FPR (%)	FNR (%)
0x043 (1000ms)	100	0.00	0.00
0x52A (200ms)	100	0.00	0.00
0x541 (100ms)	100	0.00	0.00
0x553 (200ms)	100	0.00	0.00
0x55B (600ms)	100	0.00	0.00

분석하면 정상 메시지와 비정상 메시지를 정확하게 판단할 수 있다. Table 5는 data 필드를 함께 분석하도록 제안하는 기법을 수정하였을 때의 Type II 공격 유형의 탐지 정확도를 보여주고 있다. 따라서 이벤트 메시지 전송의 주기성과 data 필드 변화를 함께 분석하면 Type II 공격 유형에 대해 0%의 FPR과 FNR을 얻을 수 있다.

7.5 기존 Automotive IDS와의 비교

Table 6은 제안된 Automotive IDS 기법과 우리가 제안한 기법의 비교를 나타낸다. [2,4,12]는 추가적인 하드웨어 장비가 필요하지 않지만 주기 메시지에 대해서만 설계된 기법이며 [3,6,15]은 Voltage 신호에 기반하여 ECU를 식별하는 기법이므로 악의적으로 전송된 PE 메시지를 탐지할 수 있으나 Voltage 신호 측정을 위한 추가적인 하드웨어 장비가 필요하다는 한계점이 있다. 우리가 제안하는 기법은 추가적인 하드웨어 장비가 필요 없으며 주기 메시지뿐만 아니라 PE 메시지에 대해서도 고려한 Automotive IDS 기법이다.

VIII. 결 론

본 논문에서 우리는 PE 메시지 분석이 가능한 차량용 침입탐지 기술을 제안하였다. PE 메시지의 경우, 주기 메시지가 일정한 시간 간격으로 전송되면서 차량의 상태가 변경될 때마다 이에 대응되는 이벤트 메시지가 함께 전송된다. PE 메시지는 주기 메시지와 이벤트 메시지 유형이 혼재되어 전송되기 때문에 기존 차량용 침입탐지 기술들은 PE 메시지를 이용하여 자동차 내부 네트워크에 악성 메시지를 전송하는 경우 이를 제대로 탐지하지 못한다. 우리는 PE 메시지를 대상으로 2가지 공격 유형을 정의하고 우리의 기법이 실제 차량에서 효과적으로 탐지하는 것을 보여주었다. 특히, Type II 공격 방법의 경우에는 전송 주기만을 분석하여서는 높은 FNR을 보여주었지만, 패킷 data 필드를 함께 분석하면 0%의 FNR을 보여주었다. 본 기법이 PE 메시지를 제대로 분석하지 못하는 기존 차량용 침입 탐지 기술과

Table 6. Comparison of the automotive IDS methods

Methods	[4], [12]	[2]	[3], [6], [15]	Our method
Approach	Frequency-based	Clock-skew-based	Voltage-based	Frequency-based and Data payload-based
Additional hardware	Not need	Not need	Need	Not need
Type of detected messages	Periodic	Periodic	Periodic and Periodic-and-on-Event	Periodic and Periodic-and-on-Event

함께 동작하여 공격 탐지 정확도를 향상시키고 결과적으로 상용화 수준의 기술 개발을 앞당길 것으로 기대 할 수 있다.

References

[1] Koscher, Karl, et al, "Experimental security analysis of a modern automobile," IEEE Symposium on Security and Privacy, pp. 447-462, Jul. 2010

[2] Cho, Kyong-Tak, and Kang G. Shin. "Fingerprinting electronic control units for vehicle intrusion detection," 25th USENIX Security Symposium, pp. 911-927, Aug. 2016

[3] Choi, Wonsuk, et al. "Voltageids: Low-level communication characteristics for automotive intrusion detection system," IEEE Transactions on Information Forensics and Security, 13(8), pp. 2114-2129, Aug. 2018

[4] Song, Hyun Min, Ha Rang Kim, and Huy Kang Kim. "Intrusion detection system based on the analysis of time intervals of CAN messages for in-vehicle network," 2016 international conference on information networking (ICOIN), pp. 63-68, Mar. 2016

[5] Seo, Eunbi, Hyun Min Song, and Huy Kang Kim. "Gids: Gan based intrusion detection system for in-vehicle network." 16th Annual Conference on Privacy, Security and Trust (PST), pp. 1-6, Nov. 2018

[6] Choi, Wonsuk, et al. "Identifying ecus using inimitable characteristics of signals in controller area networks," IEEE Transactions on Vehicular Technology, 67(6), pp. 4757-4770, Feb. 2018

[7] Miller, Charlie, and Chris Valasek. "Adventures in automotive networks and control units," Def Con 21, 2013

[8] Checkoway, Stephen, et al. "Comprehensive experimental analyses of automotive attack surfaces," in Proceedings of the 20th USENIX Security Symposium, pp. 447-462, Aug. 2011

[9] Foster, Ian, et al. "Fast and vulnerable: A story of telematic failures." 9th USENIX Workshop on Offensive Technologies, Aug. 2015.

[10] Miller, Charlie, and Chris Valasek. "Remote exploitation of an unaltered passenger vehicle," Black Hat USA, Aug. 2015

[11] Lv, Samuel, Sen Nie, and Ling Liu. "Car Hacking Research: Remote Attack Tesla Motors," Keen Security lab of Tencent, Sep. 2016

[12] Taylor, Adrian, Nathalie Japkowicz, and Sylvain Leblanc. "Frequency-based anomaly detection for the automotive CAN bus," IEEE World Congress on Industrial Control Systems Security (WCICSS), pp. 45-49, Dec. 2015

[13] Müter, Michael, and Naim Asaj. "Entropy-based anomaly detection for in-vehicle networks." IEEE Intelligent Vehicles Symposium (IV), pp. 1110-1115, Jun. 2011

[14] Sagong, Sang Uk, et al. "Cloaking the clock: emulating clock skew in controller area networks," ACM/IEEE 9th International Conference on Cyber-Physical Systems (ICCPS), pp. 32-42, Apr. 2018

[15] Foruhandeh, Mahsa. et al. "SIMPLE: Single-frame based physical layer identification for intrusion detection and prevention on in-vehicle networks,", In Proceedings of the 35th Annual Computer Security Applications Conference, pp. 229-244, Dec. 2019

〈저자소개〉

이 세 영 (Seyoung Lee) 학생회원
2014년 2월: 서울시립대학교 수학과 졸업
2016년 2월: 고려대학교 정보보호대학원 석사 졸업
2016년 3월~현재: 고려대학교 정보보호대학원 박사과정
〈관심분야〉 자동차 보안, IoT/CPS 보안

최 원 석 (Wonsuk Choi) 종신회원
2008년 2월: 서울시립대 수학과 졸업
2013년 2월: 고려대학교 정보보호대학원 석사 졸업
2018년 8월: 고려대학교 정보보호대학원 박사 졸업
2018년 9월~2020년 2월: 고려대학교 정보보호연구원 연구교수
2020년 3월~현재: 한성대학교 IT융합공학부 조교수
〈관심분야〉 센서 보안, 자동차 보안, 암호 프로토콜