정 보 보 호 학 회 지
제29권 제1호, 2019. 2

# Toward Automotive Ethernet Security

김 휘 강*

요 약

지난 5년동안 전통적인 차량에 적용된 CAN 버스 상에서의 침입탐지시스템에 대한 연구가 활발히 진행되고 있다. 초기에 rule-base 로 탐지하거나, 단순한 경량 알고리즘을 통해 침입탐지를 하는 알고리즘이 주를 이루었다면, 최근에는 machine learning을 적용한 탐지 알고리즘들 역시 많이 개발되고 있다. CAN 용 침입탐지시스템이 그간 학계에서 주로 연구가 이루어졌었다면 2019년 이후에는 상용차량들에 침입탐지시스템을 실제 탑재하여 출시될 예정에 있기 때문에, 이제는 산업계 주도적인 개발과 적용이 이루어질 것으로 보여진다. 다만, CAN 버스의 설계 구조상 공격 노드를 특정하기 어렵다는 한계와 전송량 대역폭의 제한으로 인해 기술적인 한계가 있어 왔기 때문에, 최근에는 IP 체계가 적용되고 automotive ethernet 기반으로 차량 네트워크가 빠르게 적용될 예정에 있다. 이에, 본 기고문에서는 automotive ethernet 의 보안기술에 대해 살펴보고, automotive ethernet 상에서 침입탐지시스템을 개발하기 위해 필요한 사항들은 어떤 것들이 있을지 살펴보고자 한다.

## Ⅰ. 서 론

CAN (Controller Area Network) 은 범용성과 효율성으로 인해 대부분의 전통적인 차량의 통신 백본으로서 널리 활용되어왔다. 하지만 차량 내 탑재되는 ECU 의 개수가 증가하고 점차 차량제어가 복잡다단해 짐에 따라 CAN을 기능면에서, 전송량 대역폭 면에서 개선할 필요가 꾸준히 제기되어 왔다.

이에, CAN-FD, LIN, FlexRay, MOST 와 같은 다양한 네트워크 체계가 제시되었으나 아직 CAN 의 범용성을 완전히 대체하지 못하고 있으며, 일부 기술은 소수의 OEM 에 의해서만 채택되어 과도기적 기술로 되어가고 있다.

기존의 CAN 도 hybrid 네트워크 형태로 수용하면서 기존의 TCP/IP 체계 및 확장된 대역폭을 지원할 수 있는 새로운 차량의 통신 네트워크 기반기술로 automotive ethernet 이 각광받고 있다.

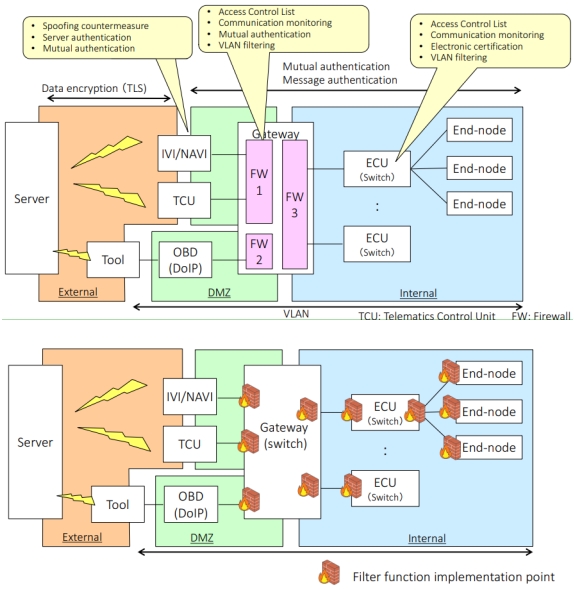
Automotive ethernet는 diagnostics over IP 나 전기차 충전에 일부 쓰이고 있으며, 추후 그 적용범위가 확대될 것으로 예상되고 있다.

추후 5G와의 연결, 자율주행기술의 적용이 확대 적용되면, 각 ECU 및 actuator 간 통신을 automotive ethernet을 통해 처리하게 될 가능성이 높은데, 이에 대한 보안 설계 역시 중요해지고 있다. 그간 CAN 상에서는 차량용 Firewall을 통한 CAN 인터페이스간 접근제어나 CAN 기반 차량용 침입탐지시스템이 네트워크 단 보안을 위해 구현되어 왔다. 하지만 아직 automotive ethernet을 위한 네트워크 보안체계는 산발적으로 차량 보안벤더에 의해 제시되고 있는 단계로 명확한 위협이나 대응 기술이 제시되지 않고 있다. 이에 automotive ethernet 과 IP 체계가 준비 없이 차량에 탑재될 경우 기존에 전통적인 차량에 있던 보안 취약점과 더불어 일반 ethernet 환경 및 IP 체계가 가지고 있던 취약점이 모두 상속되어 더 보안상 취약한 상황이 되지 않을까라는 우려 역시 증가하고 있다.

## Ⅱ. Automotive ethernet 관련 표준화 현황

Automotive ethernet 관련하여 다양한 기관들에서 표준화 및 기술제정을 위해 노력하고 있으며, 대표적으로는 OPEN Alliance SIG, AUTOSAR, JASPAR, IEEE-SA 등이 두각을 보이고 있다. 특히 JASPAR 에서는 automotive ethernet 용 보안체계 및 적용 방안을 실용적으로 제시하고 있는데, 차량의 ethernet 스위치에서 ACL (Access Control List; 접근제어목록)을 적용하여 보안성을 높이고, VLAN별 접근제어, 인증을 강화하는

* 고려대학교 정보보호대학원 (cenda@korea.ac.kr)




〔그림 1〕 Automotive Ethernet use case (by JASPAR)

use case를 예시적으로 제시한 바 있다.[1]

[그림 1]에서 보는 것처럼 네트워크 단에서 VLAN을 이용한 네트워크 구분 및 제어를 (port-based VLAN, Tagged VLAN, Private VLAN, VLAN ACL) 하여 기본적인 망분리를 하고, 유입 또는 연계되어 확대될 수 있는 attack surface를 줄이는 것을 1차로 제시하고 있다.

그리고 차량용 Firewall을 통해 IP filtering을 할 것을 제안하고 있으며, 네트워크 내에 연결된 ECU 및 통신노드들이 compromise 된 상황에 대비하여 IEEE 802.1x 기반의 MAC filtering, port security, MAC authentication, Dynamic ARP inspection을 하도록 가이드하고 있다.

일부 제안한 내용 (예: DDoS 에 대한 대응)은 필요한 부분이긴 하지만 현재 automotive ethernet 스위치의 성능상 아직은 적용이 쉽지 않은 부분 역시 존재한다.

## Ⅲ. Automotive ethernet 용 침입탐지시스템

그간 국내 차량들에 대해 CAN traffic 분석 중심의 침입탐지시스템이 다수 연구개발 되어 왔다.

Kang 등의 논문 [3]에서 볼 수 있듯이 대부분의 초기 차량용 침입탐지시스템은 CAN traffic 분석을 통해 차량 고유의 arbitration ID를 식별하고, 비정상 트래픽이 유입시 traffic 이 어떻게 변화하는가를 주로 역공학을 통해 관찰한 결과를 토대로 개발이 되었다.

| 적용방법론 | reference |
|---|---|
| survival analysis | [2] |
| IDS 개발 시 CAN 트래픽 분석을 위한 역공학 지원도구 | [3] |
| GAN (Generative Adversarial Networks | [4] |
| CAN's remote frame monitoring | [5] |
| Driver profiling (by Data mining) | [6] |
| Interval analysis | [7] |
| RNN (Recurrent Neural Network) | [8] |
| source identification by signal analysis and machine learning | [9], [10], [11], [12] |

CAN traffic 분석이 이루어진 경우에는 차량의 computation power를 고려하여 경량화된 알고리즘을 통해서도 차량 내 이상징후를 손쉽게 탐지할 수 있는 범용알고리즘들이 국내 차량 트래픽을 분석하여 개발되었다 [2,5,7].

최근 2년간은 보다 정교한 탐지와 robustness 확보를 위해 Deep learning 기술이 차량용 침입탐지시스템에 적극 고려되기 시작하였으며 [4, 8], 그리고 공격 데이터를 확보하기 어렵다는 점을 고려하여 GAN를 이용하여 정상트래픽을 기준으로 비정상 트래픽을 생성하여 탐지력을 높이는 방안 역시 고려되었다 [4].

다만, CAN이 broadcasting 방식이어서 침입을 탐지한다 하더라도 공격의 source를 특정하기 어렵다는 점에 착안하여 최근에는 공격자 source를 오류 없이 식별하는 방안이 hardware signal analysis를 통해 새로이 제시되고 있다 [9,10].

해외의 연구동향 역시 차량 트래픽 분석을 통해 침입탐지를 하는 추세에서 이제는 어떻게 공격자를 정확히 식별해 낼 것인지로 이슈가 옮겨가고 있다[11,12].

## Ⅳ. Automotive Ethernet 적용 시 고려사항

Automotive Ethernet을 적용 시에 고려해야 할 보안사항을 정리하면 다음과 같다.

첫째, automotive ethernet 에서는 기본적으로 TCP/IP 체계가 함께 적용될 예정에 있으므로, 기존의 TCP/IP 상에 존재하는 취약점, 특히 공격자 식별에 문

제를 일으키는 IP spoofing 에 대비하여 기존의 CAN 환경에서 연구된 [9,10,11,12] 및 MAC security 적용을 고려하여야 한다. 상용 automotive ethernet switch 에 기본적인 port security 등은 구현이 되어 있으나 내부 차량 네트워크에서 다량의 공격이 발생하는 것을 상정하고 있지 않으므로 성능상의 제약이 발생할 수 밖에 없어서 현재로서는 차량 내 automotive ethernet switch 의 이중화 구성을 통해 차량 내 가용성을 최대한 확보하는 전략이 필요할 것으로 예상된다.

둘째, 차량이 출고될 때에 탑재된 automotive ethernet switch 상에 VLAN 기반의 접근제어 및 IP 기반의 접근제어가 기본 기능으로 탑재되겠지만, factory setting 으로 탑재된 접근제어를 공격자가 우회할 경우, 또는 기존에 허용된 통신에 대해 공격자가 트래픽을 조작할 경우에는 대응이 어렵다. 더불어 차량 운전자가 직접 보안설정을 관리하는 것은 불가능에 가까우므로 동적으로 접근제어를 업데이트 하고 즉시 대응이 가능하도록 SDN (Software Defined Network) 개념을 적용하되, 관리를 차량 외부의 모니터링 서비스와 연계하여 대응할 수 있도록 하는 것이 필수적이다. 특히 automotive ethernet 이 적용된 차량이 ITS (Intelligent Transportation System) 과 연계하여 동작하거나 5G서비스와 연계된 자율주행차량에 적용될 경우를 고려한다면, 유연한 원격 차량보안관리가 이루어질 수 있도록 차량내부와 외부간 보안통신을 지원하고 SDN을 통해 유연한 정책 적용과 관리가 이루어질 수 있도록 고려하는 것이 필요하다.

셋째, [4]에서 볼 수 있듯이, 차량과 관련된 공격은 아직 샘플이 수집되거나 공격 사례가 수집된 예가 적어서 signature based detection을 하기가 쉽지 않다. 그러므로 원격에서 차량 트래픽을 모니터링하여 차량보안 관제 서비스를 하는 주체가 공격 signature를 생성할 수 있도록 하거나, GAN을 이용하여 발생가능한 비정상 트래픽에 미리 대응할 수 있는 이상징후 탐지 시스템을 같이 적용하는 것이 필요하다. 요컨대, 차량이 주행하면서 발생시키는 트래픽 및 이상 징후 탐지 로그를 ITS의 Cloud 로 전송하여 분석과 대응 지원을 받는 기술 역시 필요하다.

## Ⅴ. Toward intrusion detection to intrusion response

네트워크 단에서의 보안은 일반 ethernet 기반의 네트워크 상에서는 (1) Firewall을 통한 접근제어, (2) contents 분석을 통한 Intrusion detection, (3) detection 된 결과를 토대로 즉시 차단 (Intrusion prevention) 으로 진화되어 왔다.

반면에, 차량용 네트워크에서는 공격으로 의심되는 CAN packet을 차단할 경우, 혹시 모를 오탐 (false positive)으로 인해 차량의 오동작을 유발하고 이로 인해 발생할 수 있는 차량안전문제에 대한 우려 때문에 “intrusion detection”을 한 뒤에도 “intrusion prevention” 으로 이어지는 것이 불가능에 가까웠다. 물론 오탐을 일으킬 가능성이 없는 알고리즘이 개발되었다 하더라도 CAN의 broadcasting network 이라는 특성 때문에 공격과 동시에 차단이 이루어지기 어려우며, attack source를 정확히 식별하기 어려운 문제는 여전히 난제로 남아 있어 왔다.

다만, 차량용 네트워크가 automotive ethernet 으로 진화하고 차량 외부와의 연결이 5G와 같은 delay를 최소화한 네트워크로 연결될 경우, 차량 내에서 정밀한 탐지가 어려운 경우, 차량의 상태정보 및 캡쳐된 이상 packet을 인접한 Cloud 로 전송하여 공격여부를 원격에서 탐지된 뒤 결과를 받아 response를 하는 체계로 발전시켜 나갈 수 있다. 또한 차량 외부로부터 유입되는 공격의 경우 SDN 기술을 적용하여 차량 외부로부터 유입되는 공격을 동적으로 차단하는 것이 가능해 질 것으로 예상하고 있다.

## Ⅵ. 결 론

근 미래의 차량 네트워크 보안은 Automotive ethernet을 통해 차량 내부통신 및 외부와의 통신 속도가 향상된 점을 십분 활용하여 보다 능동적인 대응이 가능할 것으로 예상된다. 요컨대, automotive ethernet 은 기존 차량 네트워크 보안의 한계를 뛰어넘어, 침입탐지시스템에서 침입대응시스템으로 진화해 나갈 수 있도록 하는 security enabler 가 될 것으로 예상된다.

현재 automotive ethernet 환경에서의 침입탐지시스템 개발 및 침입대응시스템 개발은 아직 초기단계이므

로, 이 분야의 연구에 본격적으로 투자해 나갈 경우 차량보안 미래기술을 선도해 나갈 수 있을 것으로 예상된다.

## 참 고 문 헌


[1] Mikio Kataoka, “Cyber Security Study for AutomotiveEthernet in Japan Automotive Industry”, 7th IEEE-SA Ethernet & IP Automotive Technology Day, San Jose, CA, USA, Nov. 2017

[2] Han, Mee Lan, Byung Il Kwak, and Huy Kang Kim. “Anomaly intrusion detection method for vehicular networks based on survival analysis.” Vehicular communications 14 (2018): 52-63.

[3] Kang, Tae Un, Hyun Min Song, Seonghoon Jeong, Huy Kang Kim, “Automated Reverse Engineering and Attack for CAN using OBD-II”, IEEE VTC2018-Fall, Aug. 2018

[4] Seo, Eunbi, Hyun Min Song, and Huy Kang Kim. “GIDS: GAN based Intrusion Detection System for In-Vehicle Network.” 2018 16th Annual Conference on Privacy, Security and Trust (PST). IEEE, 2018.

[5] Lee, Hyunsung, Seong Hoon Jeong, and Huy Kang Kim. “Otids: A novel intrusion detection system for in-vehicle network by using remote frame.” 2017 15th Annual Conference on Privacy, Security and Trust (PST). IEEE, 2017.

[6] Kwak, Byung Il, JiYoung Woo, and Huy Kang Kim. “Know your master: Driver profiling-based anti-theft method.” 2016 14th Annual Conference on Privacy, Security and Trust (PST). IEEE, 2016.

[7] 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). IEEE, 2016.

[8] Tariq, Shahroz, et al. “Detecting In-vehicle CAN Message Attacks Using Heuristics and RNNs.” International Workshop on Information and Operational Technology Security Systems. Springer, Cham, 2018.

[9] Choi, Wonsuk, et al. “Voltageids: Low-level communication characteristics for automotive intrusion detection system.” IEEE Transactions on Information Forensics and Security 13.8 (2018): 2114-2129.

[10] Choi, Wonsuk, et al. “Identifying ecus using inimitable characteristics of signals in controller area networks.” IEEE Transactions on Vehicular Technology 67.6 (2018): 4757-4770.

[11] Cho, Kyong-Tak, and Kang G. Shin. “Viden: Attacker identification on in-vehicle networks.” Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security. ACM, 2017.

[12] Kneib, Marcel, and Christopher Huth. “Scission: Signal Characteristic-Based Sender Identification and Intrusion Detection in Automotive Networks.” Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security. ACM, 2018.


## 〈저 자 소 개〉


**김 휘 강 (Huy Kang Kim)**
종신회원

1998년 2월 : KAIST 산업경영학과 학사
2000년 2월 : KAIST 산업공학과 석사
2009년 2월 : KAIST 산업 및 시스템공학과 박사
2004년 5월~2010년 2월 : 엔씨소프트 정보보안실장. Technical Director
2010년 3월~2014년 12월 : 고려대학교 정보보호대학원 조교수
2015년 1월~현재 : 고려대학교 정보보호대학원 부교수
관심분야 : 온라인게임 보안, 네트워크 보안, 네트워크 포렌식