자율주행 차량 OBU의 DoS 공격에 대한 보안성 평가 기법 연구[1)]

이상일,[1†] 이주현,[1] 지청민,[2] 고태형,[2] 엄성욱,[4] 조성우,[4] 홍만표[3‡]

[1]아주대학교 (학부생), [2]아주대학교 (대학원생), [3]아주대학교 (교수),
[4]자동차 안전 연구원 (연구원)

A Study on the Security Evaluation Techniques for DoS Attacks on Autonomous Vehicle OBU

Sangil Lee,[1†] Juhyun Lee,[1] Cheongmin Ji,[2] TaeHyoung Go,[2] Sungwook Eom,[4] Seungwoo Jo,[4] Manpyo Hong[3‡]

[1]Ajou University (Under graduate student), [2]Ajou University (Graduate student), [3]Ajou University (Professor), [4]KATRI (Researcher)

요 약

자율주행 자동차의 자율주행 구현은 차량에 탑재된 임베디드 장비(On Board Unit, OBU)를 통해 이루어진다. OBU는 외부 혹은 차량과의 통신을 통해 차량의 안전과 상태에 관한 메시지(Basic Safety Message, BSM)를 교환하는 역할을 한다. 이러한 환경에서 차량의 OBU에 대한 보안 위협은 자율주행 시스템의 안전에 영향을 미칠 수 있고, 이는 인명피해로 이어질 수 있으므로 OBU에 대한 보안 위협에 대비하는 것이 매우 중요하다. 본 논문에서는 자율주행 차량 OBU의 자원 고갈로 인한 성능 저하를 유발해 BSM을 전송하는 기능에 문제를 일으킬 수 있는 DoS(Denial of Service) 공격에 대비해 OBU를 대상으로 보안성을 평가하는 방법을 제시한다.

I. 서론

Gartner.Inc에 의하면 전 세계적으로 인간의 감독 없이 자율주행을 구현하는 하드웨어가 탑재된 차량은 2018년 13만 7,000대에서 2023년 74만 6,000대로 증가할 것으로 보이며 현재 자율주행차 지각 알고리즘은 운전자보다 성능이 약간 떨어지므로 앞으로 해결해야 할 가장 큰 과제 중 하나는 자율주행차가 도로 주행에 충분히 안전한지 결정하는 것이다[1]. 자율주행차의 안전은 탑승자의 생명과 직결된 중요한 문제이므로 V2X(Vehicle to Everything) 통신의 보안은 매우 중요하다.

V2X 통신의 차량 간 통신은 단거리 전용 통신(Dedicated Short-range Radio Communication, DSRC)을 통해 BSM을 주고받는 것으로 안전을 보장한다. SAE J2735 표준에 따르면 혼잡 제어 알고리즘이 전송률의 감소 속도를 규정하지 않은 경우 OBU는 초당 10개의 BSM을 브로드캐스팅 형태로 전송해야 한다[2]. 자율주행 차량에서 BSM의 전송과 외부와의 통신은 차량의 OBU를 통해 이루어지기 때문에 OBU에 대한 여러 보안 위협이 존재할 수 있다. OBU에 대한 보안 위협 중 하나로, OBU 대상 DoS 공격으로 인한 OBU의 BSM 전송 능력 저하가 있다. DoS 공격은 대상 시스템에 네트워크와 통신의 기능을 마비시킬 목적으로 막대한 양의 요청을 전송하는 것으로 OBU에 대한 DoS 공격은 BSM 전송 능력에 악영향을 미칠 수 있어 V2X 환경에서 위협적인 공격이 될 수 있다[3]. 따라서 본 논문에서는 자체 설계한 보안성 평가 시스템을 사용해 IUT(Implementation Under Test)에 DoS 공격

1) 본 연구는 국토교통부 및 국토교통과학기술진흥원의 연구비지원(21PQOW-B152473-03)으로 수행된 연구임.

을 가하는 동시에 IUT의 BSM 전송률을 측정해 V2X 환경에서 OBU의 DoS 공격에 대한 보안성을 평가하는 방법을 제시한다.

II. 보안성 평가 시스템

2.1 시스템 개요

본 연구에서 설계한 보안성 평가 시스템은 그림 1과 같으며 IUT, TCI(Task Control Interface), 공격 OBU, 모니터링 OBU로 구성된다. IUT는 DoS 공격에 대한 보안성 평가 대상 OBU이다. TCI는 공격 OBU에 공격 명령을 전달하는 역할을 한다. 공격 OBU는 유효한 BSM을 생성해 IUT에 공격을 수행한다. 모니터링 OBU는 IUT가 공격을 받는 동안 초당 전송하는 BSM의 개수를 측정한다.

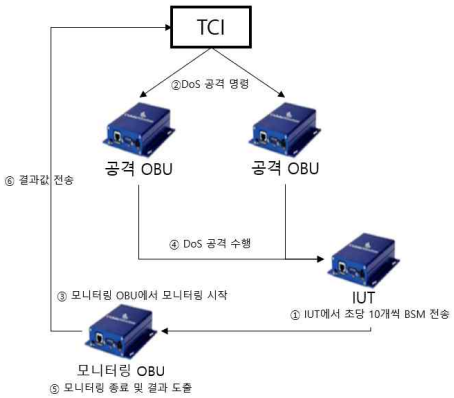

그림 1. 보안성 평가 시스템

2.2 BSM 생성

WAVE(Wireless Access for Vehicle Environment)란 IEEE 802.11 무선 LAN 기술을 차량 환경에 맞도록 개량한 DSRC 통신 기술의 일종이며 이 중 IEEE 1609.2는 인증과 보안 서비스를 제공한다. IEEE 1609.2는 차량 간 전송되는 BSM의 위/변조 방지 및 메시지 송신자가 적합한 송신자인지를 식별하기 위한 공개키 기반 전자 서명 기술을 포함한다. BSM 서명 알고리즘은 ECDSA(Elliptic Curve Digital Signature Algorithm)로 IEEE 1609.2에 명시되어 있다[4]. 본 연구에서는 사전에 수집한 BSM을 IEEE 1609.2 표준에 따라 generationTime, certificate, signature 필드를 변경해 DoS 공격을 위한 BSM을 생성한다. generationTime은 공격 BSM을 만드는 시점으로 변경하며 certificate는 유효한 인증서 값으로 변경한다. signature는 IEEE 1609.2에 명시된 Hash(Hash(*Data input*) || Hash(*Signer Identifier input*))를 유효한 키를 사용해 서명한 값으로 변경한다. Data input은 서명하고자 하는 메시지, Signer Identifier input은 유효한 인증서 값이다.

2.3 공격

TCI가 공격 OBU에 공격 명령을 전달하면 공격 OBU는 IUT에 공격을 수행한다. 공격 시 2.2절의 방법으로 생성한 BSM을 사용한다. Federal Motor Vehicle Safety Standards에 의하면 DSRC 장비는 초당 최소 5,500개 이상의 BSM에 대한 신뢰성 검사를 수행할 수 있는 능력이 있어야 한다[5]. 따라서 IUT는 초당 최소 5,500개 이상의 BSM을 수신할 수 있어야 한다. 그러나 본 연구에서 공격 OBU로 사용한 Cohda MK5가 초당 전송할 수 있는 BSM의 최대 개수는 약 4,000개 미만이기 때문에 공격 OBU 2대를 사용하여 IUT에 공격을 수행한다.

2.4 모니터링

모니터링 OBU는 공격 전후 IUT가 전송하는 BSM을 PCAP 파일로 저장한다. 저장한 파일로부터 IUT의 초당 BSM 전송률을 계산한 결과를 TCI에 전송한다.

2.5 보안성 평가

TCI는 모니터링 OBU로부터 전송받은 결과를 통해 IUT가 DoS 공격을 받는 중에도 초당 10개의 BSM 전송률을 유지하는지 확인한다.

III. 실험 결과

본 연구에서 설계한 보안성 평가 시스템을 이용하여 A사와 B사의 OBU에 대한 보안성 평가를 진행하였다. 공격 OBU의 초당 전송률을 변경하며 IUT에 공격을 수행하는 동시에 IUT는 초당 10개의 BSM을 전송한다. 공격 OBU의 전송률에 따른 IUT의 초당 BSM 전송률을 모

니터링 OBU를 통해 측정하였다. 공격 OBU의 BSM 전송률에 관계없이 공격 시간은 10초이며, 이 시간 동안 IUT가 전송하는 평균 BSM 전송률은 표 1, 2와 같다.

표 1. A사 OBU에 대한 보안성 평가 실험 결과

BSM 전송률 (BSM/s) (공격 OBU 1,2합산)	IUT 평균 BSM 전송률 (BSM/s)
1,600	10.0
2,000	9.9
3,000	10.0
4,000	10.0
5,000	9.9
6,000	10.0

표 2. B사 OBU에 대한 보안성 평가 실험 결과

BSM 전송률 (BSM/s) (공격 OBU 1,2합산)	IUT 평균 BSM 전송률 (BSM/s)
1,600	9.9
2,000	9.6
3,000	9.6
4,000	8.8
5,000	8.9
6,000	8.3

A사 OBU의 보안성 평가를 진행한 결과, 공격 OBU의 초당 BSM 전송률이 6,000 인 경우에도 IUT는 초당 평균 10개의 BSM을 전송한다. 그러나 B사의 경우, 공격 OBU의 초당 BSM 전송률이 2,000 이상일 경우 IUT의 초당 평균 BSM 전송률이 감소했고, 4,000 이상일 경우 9 미만으로 감소했다. B사 OBU는 초당 공격받는 메시지가 증가함에 따라 BSM 전송 능력이 감소하는 경향을 보인다.

A사와 B사의 OBU는 비공개로 개발 중이며 Cohda MK5 OBU도 일정 수준 이상의 DoS 공격을 받으면 BSM 전송률이 감소하는 것을 확인했다. 따라서 BSM 전송률 감소의 원인을 분석하기 위해 Cohda MK5를 IUT로 동일한 보안성 평가 절차를 수행하였다.

IUT가 DoS 공격을 받기 전후의 프로세스별 CPU 점유율을 비교하여 IUT의 BSM 전송 능력 감소 원인을 분석했다.

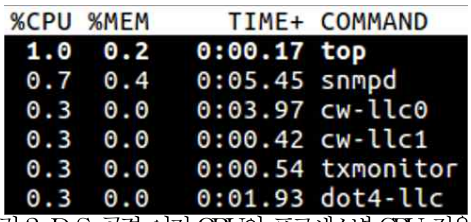

그림 2. DoS 공격 이전 OBU의 프로세스별 CPU 점유율

IUT가 DoS 공격을 받기 전 초당 10개의 BSM을 전송할 때 프로세스별 CPU 점유율을 보면 cw-llc0, dot4-llc의 점유율이 매우 낮은 것을 확인했다.

그림 3. DoS 공격 중 OBU의 프로세스별 CPU 점유율

IUT가 DoS 공격을 받는 도중 초당 10개의 BSM을 전송할 때 cw-llc0, dot4-llc의 점유율이 매우 증가한 것을 확인했다. 즉, DoS 공격 BSM 수신을 위한 프로세스를 수행하기 위해 OBU에서 CPU 자원을 사용한다. 이로 인해 IUT의 자원 고갈로 인한 성능 저하로 BSM을 전송하는 기능에 문제가 발생한다.

IV. 결론

본 논문에서는 자체 설계한 보안성 평가 시스템을 통한 OBU의 DoS 공격에 대한 보안성 평가 방법을 제시했다. SAE J2735 표준에 따르면 혼잡 제어 알고리즘이 전송률의 감소 속도를 규정하지 않은 경우 OBU는 초당 10개의 BSM을 브로드캐스팅 형태로 전송해야 한다[2]. 따라서 제시한 평가 방법을 활용해 자율주행 차량에 탑재될 OBU에 대해 해당 표준 준수 여부를 판단한다. A사와 B사의 OBU에 대한 보안

성 평가 결과 A사의 OBU는 DoS 공격을 받는 동안에도 초당 10개의 BSM을 전송할 수 있었지만, B사의 경우 일정 수준 이상의 전송률로 DoS 공격을 받으면 BSM 전송 능력에 문제가 발생했다. 향후 다른 OBU에 대해서도 본 논문에서 제시한 방법으로 DoS 공격에 대한 보안성 평가를 진행할 수 있을 것으로 기대된다.

[참고문헌]

[1] Gartner Forecasts More Than 740,000 Autonomous-Ready Vehicles to Be Added to Global Market in 2023′ , Gartner, 2019. 11. 14

[2] SAE. “Dedicated Short Range Communications (DSRC) Message Set Dictionary”. SAE J2735. 2016

[3] Hakima Khelifi, Senlin Luo, Boubakr Nour, Sayed Chhattan Shah, "Security and Privacy Issues in Vehicular Named Data Networks: An Overview", Mobile Information Systems, vol. 2018, Article ID 5672154, 11 pages, 2018. https://doi.org/10.1155/2018/5672154

[4] IEEE. “IEEE Standard for Wireless Access in vehicular Environments -Security Services for Applications and Management Messages” . IEEE 1609.2. 2016

[5] Federal Motor Vehicle Safety Standards; V2V Communications, https://www.federalregister.gov/d/2016-31059/p-2218

[6] J. Straub et al., "CyberSecurity considerations for an interconnected self-driving car system of systems," 2017 12th System of Systems Engineering Conference (SoSE), 2017, pp. 1-6, doi: 10.1109/SYSOSE.2017.7994973.