자율주행에서 사용되는 CAN 통신 기술에서의 스푸핑 보안 위협

손석빈, 정소이*, 김중헌

고려대학교, *한림대학교

lydiasb@korea.ac.kr, *sjung@hallym.ac.kr, joongheon@korea.ac.kr

Spoofing Security Threats in CAN Communication Technology used in Autonomous Driving

Seok Bin Son, *Soyi Jung, Joongheon Kim
Korea Univ., *Hallym Univ.

요 약

본 논문은 자율주행 차량 내부 부품에서의 제어를 위해 사용되는 CAN 통신 기술에 대해서 소개하였다. 또한 CAN 통신 기술에서 발생할 수 있는 보안 위협인 스푸핑 공격에 대해서 기술하였다.

Ⅰ. 서 론

자율주행 기술이 발전하면서, 운전자는 운전에서의 부담감이 줄어들어 편리함을 확보할 수 있으며, 정밀한 제어로 교통 사고가 발생할 수 있는 위험을 줄여줄 수 있으므로 안전성을 확보할 수 있다.[1] 이에 따라 자율주행에 관련된 연구들이 많이 진행되었다.[2-6] 자율주행에서 소프트웨어가 사용되면서, 해커들이 차량에 탑재되어 있는 소프트웨어에서의 취약점을 악용하여 보안 공격을 할 가능성이 높아졌다. 특히 최근에는 자동차의 내부 시스템 아키텍처에서의 대표적인 프로토콜인 CAN (Controller Area Networks) 통신에 대해 보안 위협의 가능성이 대두되었다. 이에 본 논문은 자율주행 차량 내의 CAN 통신에 대해서 소개하고, CAN 통신에서 발생할 수 있는 보안 위협에 대해서 소개한다.

Ⅱ. LiDAR 기술에서의 보안 위협

2.1 CAN 통신 기술

자동차 내의 핸들, 브레이크 등의 부품은 전자 제어 장치(ECU; Electronic Control Units)를 사용하여 제어되는데, 이때 CAN 버스는 ECU 간의 통신을 위해 대표적으로 사용되는 프로토콜이다.[7] 따라서 CAN 통신은 자율주행 자동차에서의 CPS(Cyber-Physical Systems) 제어에 주로 사용한다.

2.2 CAN 통신 기술에서의 스푸핑 공격

CAN 통신에서는 스푸핑 공격이 발생할 수 있다.[8] 스푸핑이란 공격자가 타겟을 속임으로써 발생할 수 있는 공격을 말한다. CAN 통신에서의 스푸핑 공격은 공격자가 비정상적인 CAN 메시지를 정상적인 CAN 메시지인 것처럼 속이고 주입하는 것을 말한다. 비정상적인 CAN 통신으로 인해 차량 내부에서는 브레이크가 제대로 작동되지 않도록 하거나, 엔진을 정지시키는 등의 제어를 할 수 있다.[9] 자율 주행 중에서 공격자가 악의적인 목적으로 CAN 통신에서의 스푸핑 공격을 한다면, 차량을 제대로 제어하지 못하게 되므로 충분히 위험한 교통사고가 발생할 가능성이 있다. 그러므로 CAN 통신에서의 스푸핑 공격에 방어할 수 있는 보안 전략이 필요하다.

Ⅲ. 결론

CAN 통신 기술은 차량 내 통신을 위해 필수적으로 사용되는 기술이다. 본 논문에서는 중요한 차량 프로토콜인 CAN 통신에서 발생할 수 있는 스푸핑 보안 위협을 소개하였다.

ACKNOWLEDGMENT

이 논문은 2022 년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임 (No. 2022-0-00907, (2 세부) AI Bots 협업 플랫폼 및 자기조직 인공지능 기술개발).

참 고 문 헌

[1] Cao, Y., Xiao, C., Cyr, B., Zhou, Y., Park, W., Rampazzi, S., et al. “Adversarial sensor attack on lidar-based perception in autonomous driving” Proc. ACM SIGSAC conference on computer and communications security, pp. 2267-2281, Nov. 2019.

[2] Shin, M., and Kim, J., “Randomized adversarial imitation learning for autonomous driving,” Proc. International Joint Conference on Artificial Intelligence (IJCAI'19). AAAI Press, pp. 4590–4596, Aug. 2019.

[3] Yun, W. J., Kwon, D., Choi, M., Kim, J., Caire, G., and Molisch, A. F., “Quality-aware deep reinforcement

learning for streaming in infrastructure-assisted connected vehicles," IEEE Transactions on Vehicular Technology, vol. 71, no. 2, pp. 2002–2017, Feb. 2022.

[4] Lee, G., Yun, W. J., Jung, S., Kim, J., and Kim, J. H., "Visualization of Deep Reinforcement Autonomous Aerial Mobility Learning Simulations," Proc. IEEE Conference on Computer Communications Workshops (INFOCOM Workshops), May 2021.

[5] Yun, W. J., Jung, S., Kim, J., and Kim, J. H., "Distributed Deep Reinforcement Learning for Autonomous Aerial eVTOL Mobility in Drone Taxi Applications," ICT Express, vol. 7, no. 1, pp. 1–4, 2021.

[6] Park, S., Shin, W. Y., Choi, M., and Kim, J., "Joint mobile charging and coverage-time extension for unmanned aerial vehicles," IEEE Access, vol. 9, pp. 94053-94063, 2021.

[7] Hussain, R., and Zeadally, S., "Autonomous Cars: Research Results, Issues, and Future Challenges," IEEE Communications Surveys & Tutorials, vol. 21, no. 2, pp. 1275-1313, 2019.

[8] Cui, J., Sabaliauskaite, G., Liew, L. S., Zhou, F., and Zhang, B., "Collaborative Analysis Framework of Safety and Security for Autonomous Vehicles," IEEE Access, vol. 7, pp. 148672-148683, 2019.

[9] Ren, K., Wang, Q., Wang, C., Qin, Z., and Lin, X., "The Security of Autonomous Driving: Threats, Defenses, and Future Directions," Proc. IEEE, vol. 108, no. 2, pp. 357-372, Feb. 2020.