자율주행에서 사용되는 LiDAR 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 LiDAR Technology Used in Autonomous Driving

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

요 약

본 논문은 자율주행에서 주로 사용되는 환경 인식 기술인 LiDAR 기술에 대해서 소개하였다. 또한 LiDAR 기술에서 발생할 수 있는 보안 위협인 LiDAR 스푸핑 공격에 대해서 기술하였다.

Ⅰ. 서 론

자율주행 기술이란 사람이 자동차를 직접 제어하지 않아도 주변 환경과의 상호 작용을 환경을 파악하고, 스스로 운전을 제어할 수 있는 기술을 의미한다.[1] 최근에는 자율주행을 보다 효율적이고 안전하게 하기 위해 다양한 연구들이 수행되어왔다.[2-6]

다양한 자율주행 기술 중에서도 주변 환경을 감지하여 충돌 회피를 실현시켜주는 기술인 LiDAR (Light Detection and Ranging)이 보편적으로 사용되고 있다. 이러한 LiDAR 기술에서의 공격자는 스푸핑 보안 공격을 할 가능성이 있다. 이에 본 논문은 LiDAR 기술을 소개하고, 해당 기술에서 발생할 수 있는 스푸핑 보안 위협에 대해서 소개한다.

Ⅱ. LiDAR 기술에서의 보안 위협

2.1 LiDAR 기술

자율주행 자동차에서는 교통사고를 예방하기 위해, 주변 환경을 감지하여 정보를 전달해주는 센서의 역할이 중요하다. 자율주행 자동차에서 대표적으로 사용되는 센서는 LiDAR 이다. LiDAR 은 레이저 신호를 보내고 반사되는 신호를 감지하는 방법으로 동작한다. 이 방법으로 주변 장애물 및 객체를 감지하고, 객체까지의 거리를 계산할 수 있으며, 자율주행에서의 충돌을 회피할 수 있다.[7]

2.2 LiDAR 기술에서의 스푸핑 공격

LiDAR 은 스푸핑(Spoofing) 공격의 타깃이 될 수 있다. 스푸핑 공격이란 일반적으로 공격자가 합법적인 접근자인 것처럼 속이고 정보를 해킹하고 조작하는 것을 말한다. LiDAR 기술에서는 스푸핑 공격의 일종인 공격자가 악의적인 목적으로 중간에서 신호를 가로채어 조작하는 중간자 공격(Man In The Middle)이 실행될 수 있다. 중간에서 LiDAR 신호를 가로채어 실제 장애물의 위치가 아닌 더 멀거나 가까운 다른 위치에서 레이저를 반사하고, 실제인 것처럼 속일 수 있다는 것이다. 즉, LiDAR 스푸핑 공격이란 가짜 장애물 감지 신호를 보내거나 장애물까지의 거리를 조작하는 공격을 의미한다.[7-8] 이처럼 실제 주행 중에 LiDAR 기술에 스푸핑 보안 위협이 발생한다면, 장애물을 제대로 인식하지 못하게 되므로, 치명적인 교통사고가 발생할 수 있다. 그러므로 LiDAR 에서의 스푸핑 공격에 대응할 수 있는 보안 전략이 시급하다.

Ⅲ. 결론

LiDAR 기술은 자율주행에서 환경 및 상황 인식을 위해 주로 사용되는 기술이다. 본 논문에서는 이러한 LiDAR 기술에서 발생할 수 있는 보안 위협인 스푸핑 공격에 대해서 소개하고 보안 사고의 심각성을 시사하였다.

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] 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.

[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] 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.

[8] Cao, Y., 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.