VANET 환경에서 차분 프라이버시 기술을 이용한 시스템 모델 설계

권덕규, 손승환, 오지현, 박영호
경북대학교, 경북대학교
kdk145@knu.ac.kr, sonshawn@knu.ac.kr, j2hnoh@knu.ac.kr, parkyh@knu.ac.kr

Design of a network model using differential privacy technology for VANET environments

Kwon Deok Kyu, Seung Hwan Son, Oh Ji Hyeon, Young Ho Park
Kyungpook National Univ.

요 약

차분 프라이버시 (Differential Privacy)는 비식별화 정도를 측정하는 기술로, 데이터에 노이즈를 첨가함으로써 원본 데이터의 통계적 성질을 유지함과 동시에 각 데이터에 대한 식별력을 낮추어 사용자 프라이버시를 보호한다. 이러한 차분 프라이버시 기술은 실시간으로 데이터를 생성 및 분석하는 차량 네트워크 환경에 적합하다. 본 논문에서는 차분 프라이버시를 이용하여 VANET(Vehicular Ad-hoc Network) 환경을 위한 시스템 모델을 제안하고 이를 이용한 데이터 흐름을 설명한다.

Ⅰ. 서 론

VANET (Vehicular Ad-hoc Network)은 지능형 차량과 인프라 간에 무선 네트워크를 구축하여 노면 상황, 사고 회피, 멀티미디어 등 다양한 서비스를 제공할 수 있는 네트워크 환경이다 [1]. VANET 환경은 RSU 등의 인프라와 차량 간에 무선으로 통신해야 하는 특성으로 인해 데이터 보호의 측면에서 보안성 확보가 필수적이다. 또한, 이러한 보안성 확보에는 차량의 제한된 컴퓨팅 리소스와 고속 이동성을 고려해야 한다. 따라서, 상기 언급한 VANET 환경의 특성을 고려하여 안전한 데이터 통신을 위한 보안 프로토콜 및 알고리즘은 필수적이라 할 수 있다 [2]-[4].

VANET 환경은 기본적으로 TA (Trusted Authority), RSU (Roadside Unit) 및 차량으로 구성된다. 차량은 중앙에서 네트워크를 제어하는 TA와 통신을 위해 노변 기지국인 RSU에 데이터를 전송한다. 이 과정에서, 대규모의 차량과 TA가 통신할 경우, TA에 과도한 부하가 생겨 병목현상, 단일 장애점 문제 등 다양한 네트워크 문제를 초래할 수 있다. 따라서, 최근에는 VANET 환경에 엣지 컴퓨팅 기술을 적용하여 중앙 서버의 부하를 줄이고 서비스 실시간성을 보장하기 위한 연구가 진행되고 있다.

차분 프라이버시는 프라이버시의 기준을 정량적으로 표기하여 사용자 및 데이터의 프라이버시 정도를 측정하는 기술이다. 따라서, 차분 프라이버시를 데이터에 적용하였을 경우, 각 데이터 비식별화 달성이 가능함과 동시에 전체 데이터의 통계적 특성을 보존할 수 있는 특징을 가진다. 이러한 특징은 대규모의 데이터가 교환되며 각 데이터가 사용자의 민감한 정보를 담고있는 VANET 환경에 적합하다.

본 논문에서는 차분 프라이버시 기술을 이용하여 안전한 사용자 인증 및 데이터 업로드 방식을 지원하는 시스템 모델을 제안한다. 또한, 제안한 시스템 모델의 각 참여자가 수행하는 역할을 기술하고 이를 통한 데이터 흐름을 설명한다.

Ⅱ. 제안하는 시스템 모델

제안하는 차분 프라이버시 기반 VANET 시스템 모델은 TA, 클라우드 서버, 엣지 노드 및 차량으로 구성된다. 그림 1은 본 논문에서 제안한 시스템 모델에며 자세한 내용은 다음과 같다.

- TA : TA는 신뢰할 수 있는 제 3자로서 네트워크를 초기화하고 클라우드 서버, 엣지 노드 및 차량을 등록하는 역할을 수행한다 [5],[6]. 또한, 등록한 데이터를 안전하게 보관함과 동시에 악의적인 차량을 감지하였을 경우 등록을 해제하는 철회(Revocation) 권한을 가진다. 제안한 모델에서 TA는 높은 컴퓨팅 및 저장 리소스를 가진다.
- 클라우드 서버 : 클라우드 서버는 차량 및 엣지 노드의 데이터를 받아 글로벌 AI 모델 생성, 데이터 통계적 활용 등 중앙 서비스를 구축하고 제공하는 역할을 수행한다. 따라서, 클라우드 서버 역시 높은 컴퓨팅 및 저장 리소스를 가진다.
- 엣지 노드 : 엣지 노드는 특정 지역에 배치되어 지역의 RSU를 관리하고 차량에게 네비게이션, 인포테인먼트, 사고 예측 등 직접적인 서비스를 제공한다. 또한, 엣지 노드는 충분한 컴퓨팅 및 저장 리소스를 기반으로 지역 AI 모델을 생성 및 업데이트하기 위해 운행 기록을 비롯한 각 차량의 데이터를 수집한다.
- 차량 : 차량은 부착된 센서 및 카메라를 기반으로 주변 데이터를 수집하고 차량 사용자의 운행 기록, 운전 습관, 사고 데이터 등을 기록한다. 이러한 데이터는 차분 프라이버시 기술을 이용하여 비식별화 과정을 거친 후 RSU를 통해 엣지 노드에 전송된다.

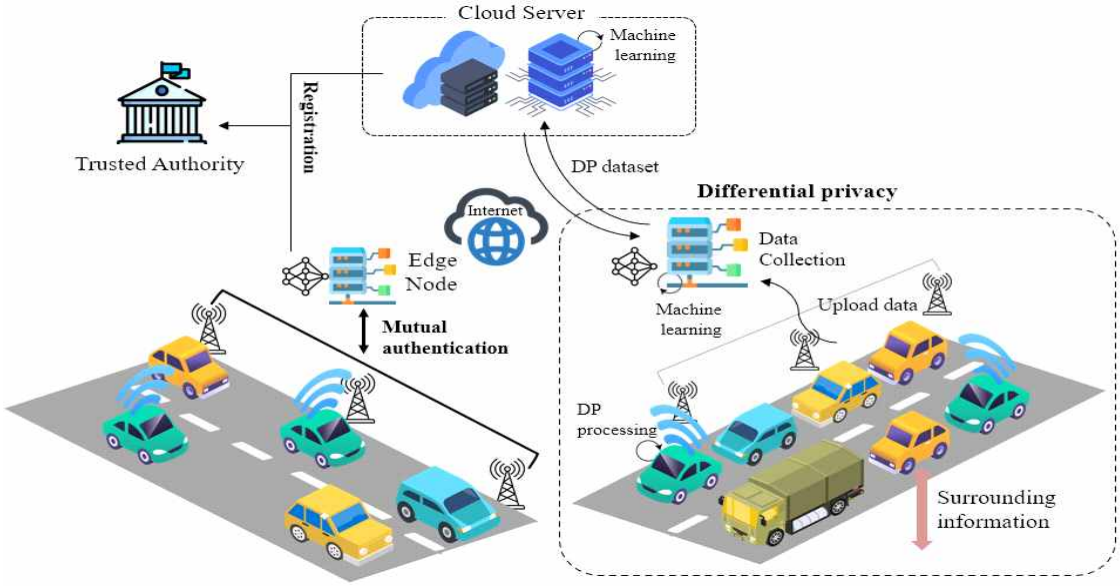

그림 1. 제안하는 시스템 모델.

Ⅲ. 데이터 흐름도

본 장에서는 제안하는 시스템 모델의 데이터 흐름도를 설명한다. 먼저, 차량, 엣지 노드, 클라우드 서버는 TA에 자신의 정보를 전송하여 네트워크에 참여하는 등록 절차를 거친다. 이후, 차량은 엣지 노드와 인증 과정을 통해 자신의 신원 정보를 증명하고 데이터 통신을 시작한다. 또한, 차분 프라이버시 기반 데이터 수집 단계에서 차량은 차분 프라이버시 기술을 이용하여 전송 데이터를 비식별화하고 암호화하여 해당 정보를 엣지 노드에 전송한다. 엣지 노드는 비식별화 정보를 이용하여 AI 모델 업데이트 및 서비스 개선에 이용하게 된다. 또한, 일부 데이터는 클라우드 서버에 업로드하여 글로벌 서비스 개선에 활용한다.

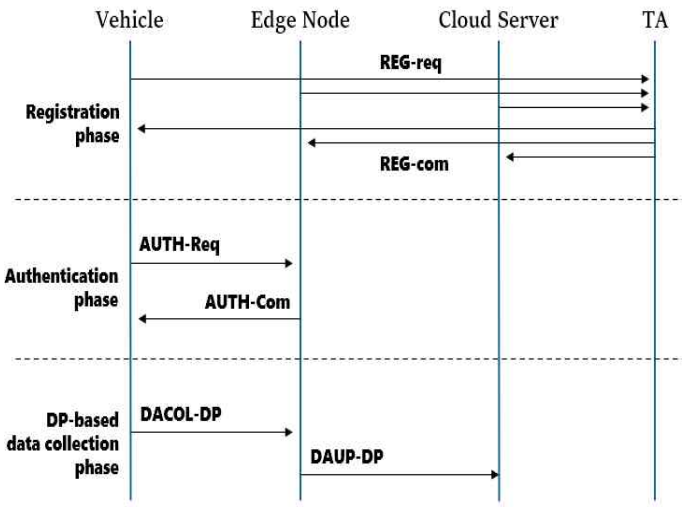

그림 2. 제안하는 시스템 모델의 데이터 흐름도.

Ⅳ. 결론

본 논문에서는 VANET 환경에서 차분 프라이버시를 기반하여 사용자 프라이버시를 보호하는 시스템 모델 및 데이터 흐름도를 제안하였다. 제안한 시스템 모델은 엣지 노드를 활용하여 클라우드 서버의 부하를 낮추고 높은 실시간성을 보장할 수 있다. 또한, 차량은 엣지 노드의 지역성을 기반으로 다양한 서비스를 제공받을 수 있다. 향후, 제안한 시스템 모델 및 데이터 흐름도를 기반으로 ECC(Elliptic Curve Cryptography), Laplace 기반 차분 프라이버시, PUF(Physically Unclonable Function) 등 최신 암호 기술을 이용하여 프로토콜을 제안할 계획이다.

ACKNOWLEDGMENT

This work was supported by Institute of Information & communications Technology Planning & Evaluation (IITP) grant funded by the Korea government(MSIT) (No.RS-2024-00396797, Development of core technology for intelligent O-RAN security platform)

참 고 문 헌

[1] Lee, M., and Atkison, T. "VANET applications: Past, present, and future," Vehicular Communications, pp. 100310-100323, Mar. 2021.

[2] Son, S., Lee, J., Park, Y., Park, Y., and Das, A. K. "Design of blockchain-based lightweight V2I handover authentication protocol for VANET," IEEE Transactions on Network Science and Engineering, pp. 1346-1358, Jan. 2022.

[3] Lee, J., Kim, G., Das, A. K., and Park, Y. "Secure and efficient honey list-based authentication protocol for vehicular ad hoc networks," IEEE Transactions on Network Science and Engineering, pp. 2412-2425, Jun. 2021.

[4] Kim, M., Lee, J., Oh, J., Park, K., Park, Y., and Park, K. "Blockchain based energy trading scheme for vehicle-to-vehicle using decentralized identifiers," Applied Energy, pp. 119445-119453, Sep. 2022.

[5] Yu, S., and Park, Y. "A robust authentication protocol for wireless medical sensor networks using blockchain and physically unclonable functions," IEEE Internet of Things Journal, pp. 20214-20228, May 2022.

[6] Son, S., Oh, J., Kwon, D., Kim, M., Park, K., and Park, Y. "A privacy-preserving authentication scheme for a blockchain-based energy trading system," Mathematics, pp. 4653-4671, Nov. 2023.