블록체인을 적용한 VANET 의 위치 정보 보호에 대한 연구 동향

강정환*, 박성환*, 권동현**
*부산대학교 정보융합공학과
**부산대학교 정보컴퓨터공학부
jeonghwan@pusan.ac.kr, starjara@pusan.ac.kr, kwondh@pusan.ac.kr

Research Trends on Location Privacy Protection in VANET using Blockchain

Jeong-Hwan Kang*, Seong-Hwan Park*, Dong-Hyun Kwon**
*Dept. of Information Convergence Engineering, Pusan National University
*Dept. of Computer Science and Engineering, Pusan National University

요 약

지능형 교통 시스템의 주요 인프라 중 하나인 VANET 은 차량과 인프라 간의 통신을 통해 교통을 예측함으로써 도로 상에서의 안전을 보장한다. VANET 은 모든 노드가 네트워크에 가입할 수 있는 개방형 네트워크이기 때문에 개인 정보 보호가 주된 관심사이다. 분산형 신뢰 관리 시스템은 차량 네트워크에서 수신된 메시지가 신뢰할 수 있는 지에 대한 여부를 결정함으로써, 악의적인 공격자로부터 차량을 지킬 수 있다. 분산형 k-익명성 체계와 블록체인을 결합한 신뢰 관리 시스템은 주변 차량들과 협력하여 익명의 은폐 영역을 구축한다. 본 논문에서는 블록체인을 적용한 분산형 신뢰 관리 시스템을 통해 차량의 위치 정보를 보호하는 최근 연구들을 살펴본 뒤에 향후 발전 방향에 대해 논하도록 하겠다.

1. 서론

최근 무선 통신, 빅데이터, AI 와 같은 기술이 발전하면서, 차량과 도로변 장치(RSU), 스마트 기기 간의 통신을 활용한 차량 인터넷(IoV) 기술과 지능형 교통 시스템(ITS)이 빠르게 발전하고 있다. 지능형 교통 시스템의 주요 인프라 중 하나인 VANET(Vehicular Ad-hoc Network)은 MANET(Mobile Ad-hoc Network)의 하위 유형으로, 차량-차량(V2V) 간, 차량-인프라(V2I) 간, 차량-보행자(V2P) 간의 통신을 통해, 운전자와 보행자를 예측하고 지원함으로써 도로 상에서의 안전을 보장한다.

VANET 은 다양한 공격에 저항하고 인증성, 가용성, 기밀성, 무결성 및 부인 방지와 같은 보안 서비스의 목표를 보장할 수 있을 만큼 충분히 안전해야 한다.[1] VANET 은 모든 노드가 네트워크에 가입할 수 있는 개방형 네트워크이며, 이로 인해 신뢰할 수 없는 노드는 VANET 을 통해 다른 운전자의 활동, 습관 및 특정한 패턴을 검출할 수 있다.[2] 따라서, 개인 정보 보호는 VANET 환경에서의 중요한 관심사이다. 만약 사용자의 정보가 노출이 되면 악의적인 행위자에 의해 사용자가 피해를 입을 수 있기 때문이다.[3]

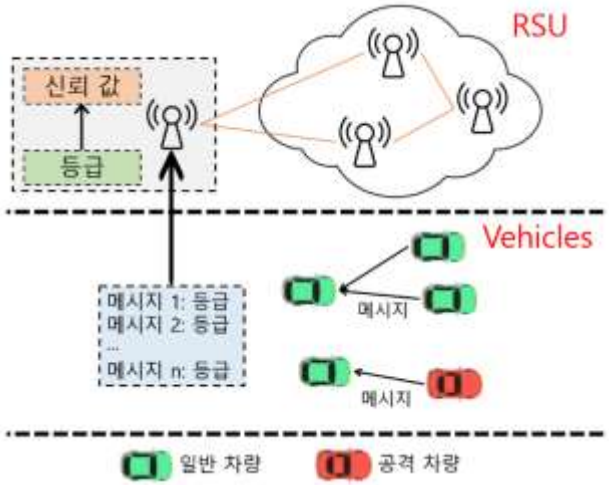
본 연구에서는 VANET 환경에서 사용자의 위치 정보 보호를 블록체인을 통해 구현하는 연구의 동향을 확인하고자 한다. 2 장과 3 장은 관련 연구로서, 2 장에서 블록체인 기반 신뢰 관리 시스템에 대한 연구를 살펴보고, 3 장에서는 분산형 k-익명성 체계를 활용한 위치 정보 보호에 대한 연구를 살펴본다. 그리고, 4 장에서 앞선 관련 연구를 활용한 VANET 환경의 위치 정보 보호에 대한 연구 사례를 제시하고, 이를 비교한다. 마지막으로 5 장에서 결론을 제시하도록 하겠다.

2. 블록체인 기반 분산형 신뢰 관리 시스템

VANET 환경에서 차량 네트워크는 높은 이동성과 가변성으로 인해 차량 네트워크에 접속된 주변 차량이 신뢰할 수 있는지 판단해야 하며, 악의적인 차량에 의해 공격받기 전에 빠른 판단이 필요하다.[4] 이러한 문제를 해결하는 방법 중 하나로서 신뢰 관리 시스템이 연구되고 있다. 신뢰 관리 시스템은 차량 네트워크에서 수신된 메시지가 신뢰할 수 있는 지에 대한 여부를 결정한다.

Z. Yang 외 4 명[5]은 블록체인 기술을 기반으로 한 차량 네트워크의 분산형 신뢰 관리 시스템을 제안하

였다. 이 시스템에서 차량은 베이지안 추론 모델을 사용하여 주변 차량으로부터 수신된 메시지를 검증한다. 검증 결과를 기반으로 차량은 각 메시지를 송신한 차량에 대한 등급을 생성한다. 해당 등급을 사용하여 도로변 장치(RSU)는 관련된 차량의 신뢰 값 오프셋을 계산하고, 계산된 데이터를 블록으로 압축한다. 그런 다음 각 RSU 는 모든 RSU 가 관리하는 신뢰 블록체인에 블록을 추가한다. 이때 공동 작업 증명 및 지분 증명 합의 메커니즘을 사용하여, 블록에 더 많은 오프셋 값(stake)을 저장하고 이를 통해 RSU 가 해시 함수에 대한 암호화 임시 값을 더 쉽게 찾을 수 있다. 위의 방식으로 모든 RSU 는 업데이트되고 안정적이고 일관된 신뢰 블록체인을 협력적으로 유지한다.



(그림 1) 분산형 신뢰 관리 시스템[5]

3. 분산형 k-익명성 체계

가장 널리 사용되는 위치 정보 보호 방법 중 하나인 k-익명성 체계는 요청한 사용자의 실제 위치 대신, 최소 k-1 명의 협력 사용자가 포함된 익명의 은폐 영역을 활용하여 공격자가 요청한 사용자와 1/k 보다 큰 신뢰도로 쿼리를 연관시킬 수 없게 하는 것이다.[6]

최초의 분산형 k-익명성 체계 중 하나를 제안한 Chow 외 2 명[7]은 중앙 집중형 서버와 같은 제 3 의 기기의 도움 없이, 모바일 사용자의 위치 정보를 공개하지 않고 위치 기반 서비스를 사용할 수 있는 P2P 공간 은폐 알고리즘을 구현하였다. 요청한 모바일 사용자는 그룹을 구성하는 데 필요한 수의 '피어'를 찾은 다음, 개인정보 보호 요구사항을 충족하는 최소의 그리드 영역을 선택한다. 그런 다음 그룹 내에서 임의의 피어를 '에이전트'로 선택한다. 이 에이전트를 매개로 위치 기반 데이터베이스 서버와 통신한다. 이를 통해, 요청한 사용자가 적어도 k-1 개의 주변 사용자와 함께 익명의 은폐 영역을 생성하도록 하였다. 다만, 이를 구현하기 위해서는 요청한 사용자의 주변에 적어도 k-1 개의 다른 사용자가 존재해야 하고, 이러한 조건이 충족되기를 기다려야만 한다.

따라서 Ghaffari 외 3 명[8]은 새로운 분산형 익명화 프로토콜을 제안하였다. 이들은 각 모바일 노드가 특정 영역을 익명화 하게 하였다. 모바일 노드들은 서로에 대한 정보에 액세스 할 필요 없이 쿼리를 익명화 시킨다. 제안된 프로토콜에서의 각 요청은 무작위로 선택된 티켓과 함께 전송되는데, 서버에서 생성된 암호화된 응답은 이 티켓의 해시 값을 기반으로 특정 모바일 노드(브로커 노드)로 전송된다. 요청한 사용자는 브로커 노드에 쿼리하여 응답을 받는데, 이를 통해 익명의 요청한 사용자와 브로커 노드에 필요한 필드를 제외한 모든 메시지가 암호화된다.

4. 연구 사례

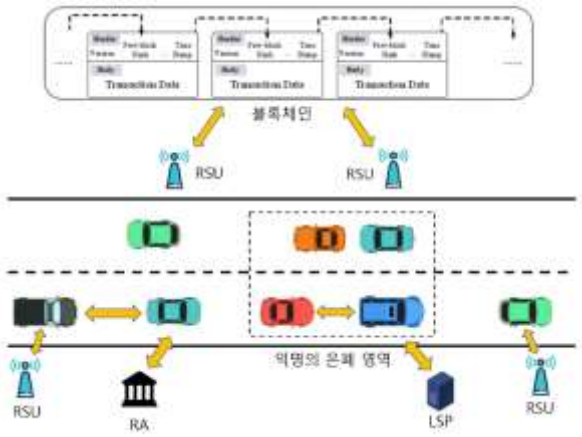
4.1. 단일 블록체인 기반 위치 정보 보호 체계

B. Luo 외 4 명[9]은 기존의 분산형 k-익명성 체계에 대한 연구[7][8]가 익명의 은폐 영역을 생성할 때 협력하는 사용자들의 신뢰도를 고려하지 못한다는 점을 지적하였다. 예를 들자면, 위치 기반 서비스(LBS)의 쿼리를 생성하는 요청 차량 자체가 악의적인 경우, 악의적인 차량은 주변의 협력 차량으로부터 받은 정보를 노출시킬 수 있다. 또는, 협력 차량이 악의적인 경우, 민감한 지역에 위치를 노출하거나 위치 기반 서비스 제공 업체와 결탁함으로써 부적절한 위치를 제공하여 익명의 은폐 영역을 교란시킬 수 있다. [9]는 이러한 문제로 인해 기존의 분산형 k-익명성 체계 연구는 VANET 에 적용될 수 없다고 지적하였다.

위의 문제를 해결하기 위해서 [9]는 차량에 대한 신뢰 관리 방법을 새롭게 고안하였고, 이를 적용한 분산형 신뢰 관리 시스템을 구축하기 위해 데이터 일관성, 변조 방지 등의 특성을 가진 블록체인 기술을 채택하여 차량의 '과거 신뢰 정보'를 기록하였다.

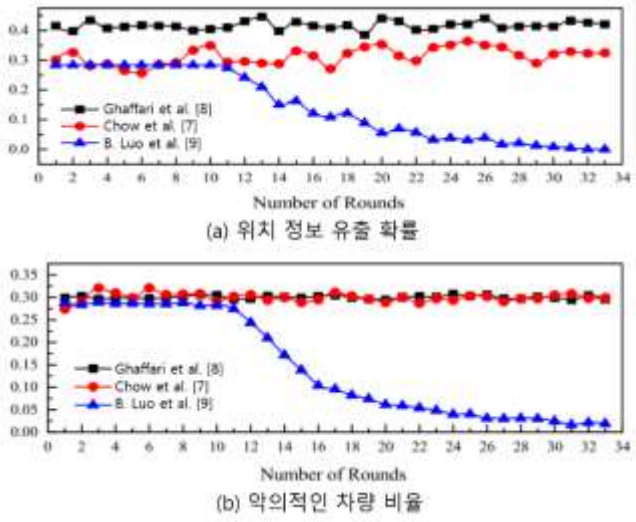
[9]는 익명의 은폐 영역 생성을 일종의 거래로 간주하고 블록체인에 이러한 신뢰 정보를 기록함으로써 주변의 더 높은 신뢰도를 가진 협력 차량을 선택할 수 있게 하였다. 또한, 차량이 고속으로 주행하면서 많은 양의 데이터를 처리해야 하는 것은 차량에 부담을 주고, 블록체인을 위한 합의 알고리즘을 실행하고 실시간으로 블록체인을 업데이트 및 유지하는 것 또한 차량에 많은 부담을 준다. 따라서 [9]는 RSU 를 사용하여 시스템을 위의 기능을 구현하였는데, 이는 앞선 관련 연구 [5]와 유사하다고 볼 수 있다.

[그림 2]는 [9]에서 구현한 분산형 신뢰 관리 시스템의 아키텍처이다. RSU 는 신뢰 관리를 위한 연산을 수행하며, 블록체인에 차량의 신뢰 정보를 저장한다. 이때, RSU 만이 블록체인에 트랜잭션을 기록할 수 있고, 차량은 해당 데이터를 쿼리하기 때문에 컨소시엄 블록체인을 채택하였다. 이는 퍼블릭, 프라이빗 블록체인에 비해 제한된 액세스, 높은 효율성 및 우수한 확장성이라는 해당 시스템에 적합한 특성을 가지고 있다.



(그림 2) 블록체인을 적용한 분산형 신뢰 관리 시스템[9]

앞선 [7], [8]의 연구의 실험 결과와 [9]의 실험 결과를 비교했을 때[그림 3], 라운드가 진행될수록 [9]는 [7], [8]에 비해 악의적인 차량의 참여 비율과 위치 정보 유출에 대한 확률이 크게 감소하였다. 익명의 은폐 영역을 구성하는 데 필요한 시간 지연은 [8]이 가장 적고, [7]과 유사한 정도로 발생하였다.

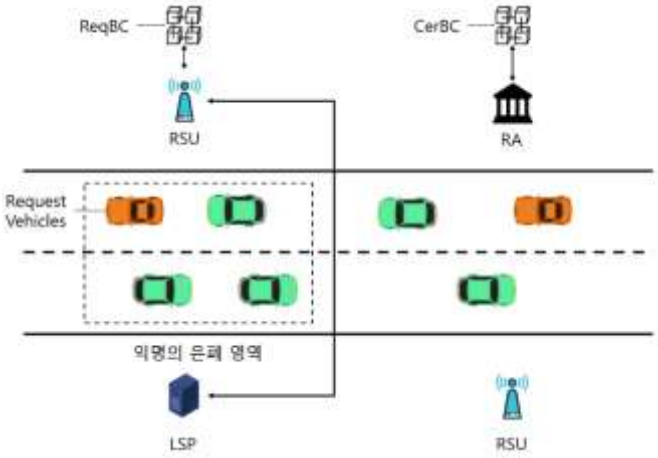


(그림 3) 위치 정보 유출 확률과 악의적인 차량 비율[9]

4.2. 다중 블록체인 기반 위치 정보 보호 체계

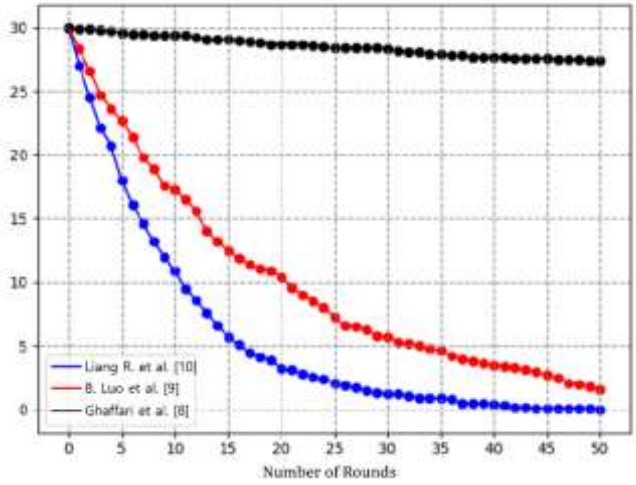
Liang R. 외 2 명[10]은 블록체인 기반 위치 정보 보호 신뢰 모델을 제안하였다. [9]와 마찬가지로 요청 차량은 가까운 RSU 로 위치 조회 요청을 전송하고, RSU 는 익명의 은폐 영역을 만들기 위해 협력 차량을 수집한다. 그런 다음 쿼리 결과가 요청 차량으로 반환된다. [그림 4]는 [10]에서 구현한 두 가지 블록체인이 적용된 분산형 신뢰 관리 시스템이다.

[10]에서는 차량 간의 직접적인 통신을 피하고, 개인 정보 공개 확률을 줄이기 위해 가명의 인증서를 사용한다. 이를 위해, 인증서용 블록체인(CerBC)과 요청 정보용 블록체인(InfBC)의 두 가지 블록체인으로 나누어 관리한다. CerBC 는 RSU 에서 모든 인증서 등록, 업데이트 및 해지에 관한 트랜잭션이 저장된다. InfBC 는 LBS 에서 모든 쿼리 요청이 기록되며, 요청 차량과 협력 차량 모두 가명을 사용한다.



(그림 4) 블록체인 기반 위치 정보 보호 체계[10]

새롭게 부상하는 HotStuff 는 통신 부담과 시스템 관성의 단점을 가지고 있다. 기존의 PoW 합의 메커니즘은 차단 속도가 느리고 자원이 많이 사용된다. 이를 보완한 방식인 HotStuff + PoW 의 하이브리드 합의 모델을 제안하였다. 이를 통해 자원의 낭비를 줄이며 PoX 합의 메커니즘에 비해 계산 효율을 향상시켰다.



(그림 5) 위치 정보 유출 확률(%)[10]

앞선 [8], [9]의 실험 결과와 [10]의 실험 결과를 비교했을 때[그림 5], 블록체인을 사용한 [9]에 비해 악의적인 차량을 더 빨리 제거하기 때문에, 라운드가 진행될 수록 위치 정보 유출 확률이 더 빠르게 줄어든 것을 확인할 수 있다. [9]는 블록체인을 사용하지 않고 각 차량의 신뢰 값을 개별적으로 유지하는 시스템이기 때문에 위치 정보 유출에 취약하다.

[9]와 [10]의 성능을 비교했을 때, 차량 수에 따른 인증서 존재 증명에 대한 스토리지 오버헤드는 [10]에서 약 45% 감소했으며, 소요 시간(ms)은 약 46% 소

하였다. 하지만 익명의 은폐 영역을 구성하는데 걸리는 시간은 [8]과 [9]에 비해 [10]에서 다소 증가하는 경향을 보였다.

5. 결론

본 논문에서는 블록체인을 적용한 VANET 의 위치 정보 보호에 대한 연구 동향을 확인하였다. 분산형 신뢰 관리 시스템은 VANET 에서 발생하는 다양한 유형의 보안 문제를 효과적으로 예방할 수 있다. 또한, 4 장에서 제시한 연구 사례를 통해 기존의 관련 연구를 VANET 에 적용했을 시에 발생했던 보안 문제를 블록체인을 적용함으로써 보다 효율적으로 해결할 수 있는 것을 확인하였다.

본 논문에서 제시한 연구 사례는 모두 RSU 에 의존하여 익명의 은폐 영역을 구성한다. 이는 도심을 벗어난 지역에서는 RSU 의 부족이나 부재로 인해 실현될 수 없거나, RSU 를 설치해야 하는 문제점을 발생시킨다. 따라서 RSU 에 의존하지 않는 신뢰 관리 시스템의 구현 방안을 후속 연구로 제시할 수 있다. 또한, 익명의 은폐 영역을 생성하는 데 소요되는 시간이 늘어나는 양상을 보였는데, 이를 개선하는 것 또한 후속 연구가 될 수 있다. 마지막으로, 블록체인이 지속적으로 발전하고 있으므로 분산형 신뢰 관리 시스템에 필요한 블록체인을 향후 개선하는 방법 또한 후속 연구로 제시할 수 있다.

Acknowledgement

본 연구는 과학기술정보통신부 및 정보통신기획평가원의 대학 ICT 연구센터지원사업의 연구결과로 수행되었음. (IITP-2020-0-01797)

참고문헌

[1] F. Azam, S. K. Yadav, N. Priyadarshi, S. Padmanaban and R. C. Bansal, "A Comprehensive Review of Authentication Schemes in Vehicular Ad-Hoc Network," in IEEE Access, vol. 9, pp. 31309-31321, 2021.

[2] Ravi Tomar, Manish Prateek, G. H. Sastry. Vehicular Adhoc Network (VANET) - An Introduction. International Journal of Control Theory and Applications, International Science Press 2016, 9 (18), pp.8883-8888.

[3] R. Hussain, J. Lee and S. Zeadally, "Trust in VANET: A Survey of Current Solutions and Future Research Opportunities," in IEEE Transactions on Intelligent Transportation Systems, doi: 10.1109/TITS.2020.2973715.

[4] S. Li and X. Wang, "Quickest Attack Detection in Multi-Agent Reputation Systems," in IEEE Journal of Selected Topics in Signal Processing, vol. 8, no. 4, pp. 653-666, Aug. 2014, doi: 10.1109/JSTSP.2014.2309943.

[5] Z. Yang, K. Yang, L. Lei, K. Zheng and V. C. M. Leung, "Blockchain-Based Decentralized Trust Management in Vehicular Networks," in IEEE Internet of Things Journal, vol. 6, no. 2, pp. 1495-1505, April 2019, doi: 10.1109/JIOT.2018.2836144.

[6] C.-Y. Chow, M. F. Mokbel, and X. Liu, “A peer-to-peer spatial cloaking algorithm for anonymous location-based service,” in Proc. 14th Annu. ACM Int. Symp. Adv. Geographic Inf. Syst, 2006, pp. 171–178

[7] Chow, C.-Y., Mokbel, M.F., Liu, X.: A peer-to-peer spatial cloaking algorithm for anonymous location-based service. In: Proceedings of 14th Annual ACM International Symposium Advance Geographic Information System, pp. 171–178 (2006)

[8] M. Ghaffari, N. Ghadiri, M. H. Manshaei and M. S. Lahijani, "P^4QS: A Peer-to-Peer Privacy Preserving Query Service for Location-Based Mobile Applications," in IEEE Transactions on Vehicular Technology, vol. 66, no. 10, pp. 9458-9469, Oct. 2017, doi: 10.1109/TVT.2017.2703631.

[9] B. Luo, X. Li, J. Weng, J. Guo and J. Ma, "Blockchain Enabled Trust-Based Location Privacy Protection Scheme in VANET," in IEEE Transactions on Vehicular Technology, vol. 69, no. 2, pp. 2034-2048, Feb. 2020, doi: 10.1109/TVT.2019.2957744.

[10] Liang R., Li B., Song X. (2020) Blockchain-Based Privacy Preserving Trust Management Model in VANET. In: Yang X., Wang CD., Islam M.S., Zhang Z. (eds) Advanced Data Mining and Applications. ADMA 2020. Lecture Notes in Computer Science, vol 12447. Springer, Cham.