자율주행 자동차 V2V 통신을 위한 DID 활용 메시지 전송 및 검증

정기연, 정승욱
건양대학교 사이버보안공학과
ions@kakao.com, swjung@konyang.ac.kr

DID based V2V Communication for Verifying Vehicle

Ki-Yeon Jeong, Seung Wook Jung
Dept. of Cyber Security Engineering, Konyang University

요 약

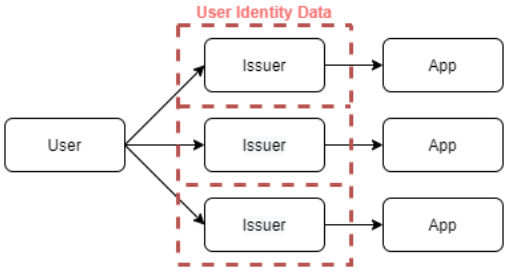
자율주행 자동차는 최근 들어 비약적인 발전을 거듭하고 있지만, 동시에 V2V, V2I 등 차량의 네트워킹에 따른 보안 문제에 대한 중요도 또한 함께 올라가고 있다. 이에 대비책으로 SCMS 를 중심으로 보안 기술이 발전하고 있지만, 중앙 데이터베이스에 대한 의존도는 여전히 높아 한 번의 보안 사고에도 심각한 피해가 우려되는 상황이다. 본 논문은 이러한 상황을 방지하기 위해 블록체인의 DID(Decentralized Identify, 탈중앙화 신원증명) 기술을 적용하는 방안을 설명하고, 그 예시로 긴급 차량에서의 DID 활용 방안을 제안한다.

1. 서론

최근 자율주행 자동차는 비약적인 발전을 거듭해 SAE Level 4 이상의 완전 자동화를 향후 5 년 이내 개발을 목표로 달려가고 있다 [1]. Level 4 이상의 발전을 위해서는 ITS(Intelligent Transport System)를 요구하게 되었고, 이에 발맞춰 IEEE 802.11p, Wave, LTE V2X 등 V2X(Vehicle to Everything) 통신 기술 개발이 활발하게 이뤄지고 있다. 하지만 발전을 거듭할수록 네트워크에 대한 의존은 필수불가결한 요소가 되었고, 보안의 중요성 또한 꾸준히 제기되고 있다. 현재는 보안 사고를 예방하기 위해 PKI 기반의 SCMS(Security Credential Management System)를 중심으로 보안 기술이 발전하고 있지만, SCMS 또한 중앙데이터베이스의 의존도가 높고 많은 인증기관을 보유하고 있다는 단점을 가지고 있다. 이를 개선하기 위해 본 논문에서는 블록체인을 활용한 DID(Decentralized Identity, 탈중앙화 신원증명) 기술로 차량 인증의 방법을 긴급차량에 적용하는 예시를 통해 제안한다.

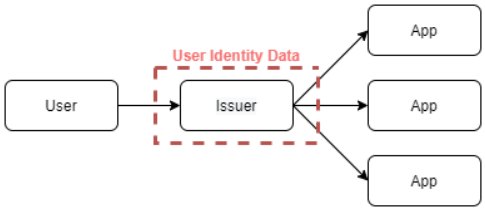
2. DID 개요

전 세계적으로 많은 사람들이 인터넷 활동 등의 다양한 작업을 처리하기 위해 (그림 1)과 같이 고유한 식별자를 만들어 사용했다(전화번호, 이메일, 사이트 ID 등). 하지만 고유한 식별자의 대다수는 외부 기관에서 관리와 사용이 이루어지기 때문에, 자신의 정보를 직접 통제할 수 없을 뿐더러, 인터넷의 경우 각 사이트마다 아이디와 패스워드의 생성이 필수로 자리 매김하여 사용자에게 부담 또한 커지게 되었다.



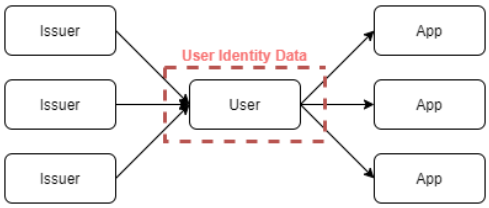
(그림 1) Traditional Identity Management [2]

이를 해결하기 위해 (그림 2)와 같이 SNS 나 포털사이트의 대표 계정을 이용하여 다른 웹 서비스 사용을 지원했으나, 기업/기관에서 사용자의 신원 데이터를 관리하는 것은 동일하기 때문에 해킹과 같은 피해를 입을 경우 모든 사용자의 데이터가 탈취될 수 있다는 단점은 해결되지 않았다.



(그림 2) Federated Identity Management [2]

DID(Decentralized Identity, 탈중앙화 신원증명)는 이 같은 현상을 해결하기 위해 나온 새로운 모델이자 식별자로 (그림 3)과 같다. 데이터에 대한 주권을 개개인이 가지고 필요할 때 그 데이터를 중앙화 된 시스템을 거치지 않고 증명할 수 있는 기술이다. 사용자는 목적에 따라 정보를 선택하여 제공함으로써 신원 확인이 가능하고, 동시에 자격 검증이 가능하게 된다.



(그림 3) User-Centric Identity Management [2]

2.1. DID 기술 설명

간단한 예시로 DID 는 세가지의 문자열 집합으로 구분된다. 1) DID URI scheme 식별자, 2) DID method, 3) DID method 에서 정의된 식별자. 각각의 문자열은 ':' 문자로 구분되며 그 예시는 (그림 4)와 같다.

(그림 4) A simple example of a DID [3]

이러한 문자열은 DID document 에 기초하여 해석되며, DID document 는 (그림 5)의 예시처럼 구성되어 있다.

```
{
  "@context": [
    "https://www.w3.org/ns/did/v1",
    "https://w3id.org/security/suites/ed25519-2020/v1"
  ]
  "id": "did:example:123456789abcdefghi",
  "authentication": [{
    // used to authenticate as did:...fghi
    "id": "did:example:123456789abcdefghi#keys-1",
    "type": "Ed25519VerificationKey2020",
    "controller": "did:example:123456789abcdefghi",
    "publicKeyMultibase": "zH3C2AVvLMv6gmMNam3uVAjZpfkcJCwDwnZn6z3wXmqPV"
  }]
}
```

(그림 5) EXAMPLE: A simple DID document [3]

2.2. DID 디자인 목표

DID 는 다음 <표 1>을 디자인 목표로 한다.

3. 긴급 차량 DID 적용 시나리오

DID 는 일반 차량에도 적용이 가능하지만, 특수한 상황에서 더욱 효과적으로 활용할 수 있다. 이번 장에서는 긴급 차량에 DID 를 적용한 V2X 환경의 시나리오를 구상하여 DID 의 효용성과 효율성을 검증한다. 앰뷸런스 등의 긴급 차량은 특정한 목적을 위해 긴급 상황 시 차량 등 장애물에 구애받지 않고 주행해야 한다. 이를 위해 긴급 차량에 대해서 DID 를 발급하고 (DID Document 를 블록체인에 기록) 긴급 차량임을 나타내는 VC(Verifiable Credential)를 긴급 차량에 발급한다. 긴급 차량은 긴급 상황 시 막힘없는 주행을 위해 VC 를 가지고 VP(Verifiable Presentation)를 생성하여 주변 차량들에게 다른 차선으로 이동하도록 VP 를 제공한다. 주변 차량들은 VP 를 검증하고, 긴급 차량이 맞는 경우에 차선을 이동하게 된다.

<표 1> DID Design Goals [3]

Goal	Description
Decentralization	Eliminate the requirement for centralized authorities or single point failure in identifier management, including the registration of globally unique identifiers, public verification keys, services, and other information.
Control	Give entities, both human and non-human, the power to directly control their digital identifiers without the need to rely on external authorities.
Privacy	Enable entities to control the privacy of their information, including minimal, selective, and progressive disclosure of attributes or other data.
Security	Enable sufficient security for requesting parties to depend on DID documents for their required level of assurance.
Proof-based	Enable DID controllers to provide cryptographic proof when interacting with other entities.
Discoverability	Make it possible for entities to discover DIDs for other entities, to learn more about or interact with those entities.
Interoperability	Use interoperable standards so DID infrastructure can make use of existing tools and software libraries designed for interoperability.
Portability	Be system- and network-independent and enable entities to use their digital identifiers with any system that supports DIDs and DID methods.
Simplicity	Favor a reduced set of simple features to make the technology easier to understand, implement, and deploy.
Extensibility	Where possible, enable extensibility provided it does not greatly hinder interoperability, portability, or simplicity.

<표 2> SAE J2735 17messages [4]

주요 Messages	사용 범위	내용
BSM (Basic Safety Message)	V2V	전체적인 안전 관련 정보 제공, 100ms 주기의 브로드캐스팅 통신
PVD (Probe Vehicle Data)	V2I	차량에 수집된 'prove data'(차량 운행상태)를 RSU에 전달
MapData	I2V	교차로 및 도로 지형 데이터에 대한 정보 제공
SPaT (SinglePhaseAndTiming)	I2V	교차로에서 현재의 신호위상 및 시간 동기화에 대한 정보를 제공(MapData 와 연동하여 사용)
RTCMCorrections (Real-Time Differential Correction Maritime)	I2V	RTCM 보정정보를 제공하기 위한 메시지
PSM (PersonalSafetyMessage)	V2P	위험 범위에 있는 보행자에 관한 정보 제공
PDM (ProveDataManagement)	I2V	I2V, PVD메시지를 관리하기 위한 메시지
RSA (RoadSideAlert)	V2X	공공 안전 차량 및 RSU로부터 ad-hoc 메시지 생성 지원
SSM (SignalStatusMessage)	I2V	설비동작 상태 요청에 대한 response 용도 사용
SRM (SignalRequestMessage)	V2I	교차로 진입차량이 신호 컨트롤러로부터 서비스 정보를 얻기 위한 메시지
TIM (Traveler Information Message)	I2V	다양한 교통정보, 돌발상황, 사전 도로작업 등에 대한 정보 전달 메시지
CSR (CommonSafetyRequest)	V2V	안전정보교환 데이터 지원에 대한 요청 메시지
EVA (EmergencyVehicleAlert)	V2X	긴급차량에 대한 정보를 전달
ICA (Intersection VehicleAlert)	V2X	교차로 부근 차량 위험조건에 대한 정보를 전달
NMEACorrections	I2V	초기 GPS 데이터 포맷의 메시지를 DSRC 채널을 통해 전송하기 위한 용도로 사용
testMessages00-15	N/A	사용 지역별 맞춤형 메시지 형태로 사용
Not Assigned	N/A	새로운 메시지 내용 추가시 할당

3.1. SAE J2735 표준

시나리오에 앞서, 자율주행 차량은 상호간의 통신에 대하여 표준 규격이 요구된다. SAE(Society of Autonomous Engineers, 미국 자동차 공학회)는 J2735 을 통해 IEEE 가 제시한 WAVE 통신에 대하여 V2V/V2I

통신을 위한 메시지, 데이터 프레임, 요소 형식 및 구조 등 신호 규격에 대한 정의를 진행하였다. 2017 년 기준으로 Message 17 개, Data Frame 156 개, 데이터 요소 230 개, 외부 정의 참조 데이터 요소 58 개로 구성되어 있고, 개체들은 ASN 방식으로 정의되어 있다. SAE 2735 표준의 메시지는 <표 2>와 같다 [4].

그리고 긴급 차량에게 이용되는 주된 메시지와 사용 목적은 <표 3>과 같다.

<표 3> 긴급 차량 운용에 필요한 메시지

BSM	차량 상태와 관련된 safety data를 교환하는 데 사용하는 메시지
TIM	다양한 타입의 정보를 전송하기 위한 메시지 (예, 도로 표지판 정보 등)
RSA	차량에게 도로 상의 위험을 알리기 위한 메시지
EVA	응급차량이 주변 차량에게 응급상황 경고를 알리는 메시지 (응급차량은 경찰차, 구급차, 소방차 등이 될 수 있다.)
SPAT	기지국이 차량에게 현시 상태를 알리기 위한 메시지

3.2. 메시지 전송

SAE J2735 규격의 모든 메시지(M)을 전송할 때 VP + T + M + Sign(M||T), 또는 VP = VC + T + M + Sign(VC||M||T)로 전송할 수 있다. 여기서 T 는 재전송 공격 (Replay attack)을 막기 위한 시점 정보, 또는 Sequence number 또는 Challenge-Response 방식에서 Response 정보일 수 있다. Challenge 는 random number 이고 response 는 random number 일수도 random number + 1 등 일 수 있다. 여기서 || 은 concatenation 이며 M 은 긴급상황을 알리는 메시지이며 Sign(M)은 메시지 M 을 서명한 서명값이다.

3.3. DID 등록 및 VC 발급 절차

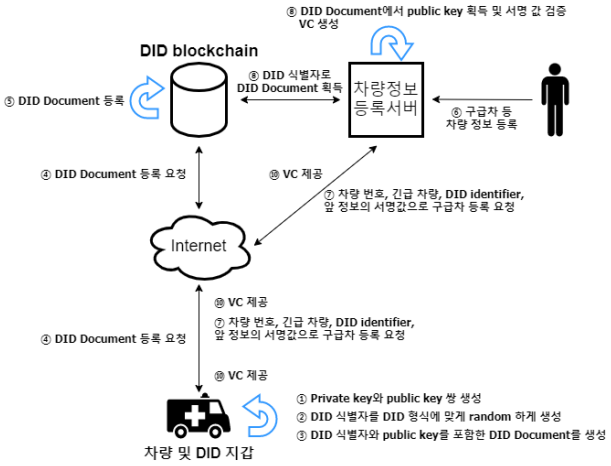
DID 환경을 구축하고 VP 위해서는 모든 차량이 차령 정보를 등록해야 한다. 먼저, 차량은 VP 검증을 위한 private key 와 public key 쌍을 생성하며, DID 식별자를 DID 형식에 맞게 random 하게 생성하고 DID 식별자와 public key 를 포함한 DID Document 를 생성한다. 이후 인터넷을 통해 생성된 DID Document 는 DID blockchain 에 등록 요청이 수행되게 된다.

등록이 된 이후 관리자는 차량 정보 등록 서버에 긴급차량 등의 차량 정보를 등록하고, 긴급차량은 차량 번호, 긴급 차량, DID Identifier 등을 이에 대한 서명값과 함께 차량정보 등록서버에 긴급 차량 등록을 요청한다. 차량정보 등록서버는 DID 식별자를 이용해 DID Document 를 획득하고, 차량 정보 등록 서버의 DID Document 에서 public key 획득과 서명 값 검증이 이뤄진다. 그리고 서명이 맞으면 VC 를 생성하여 긴급 차량에 전달되게 된다. (그림 6)은 이 과정을 나타낸다.

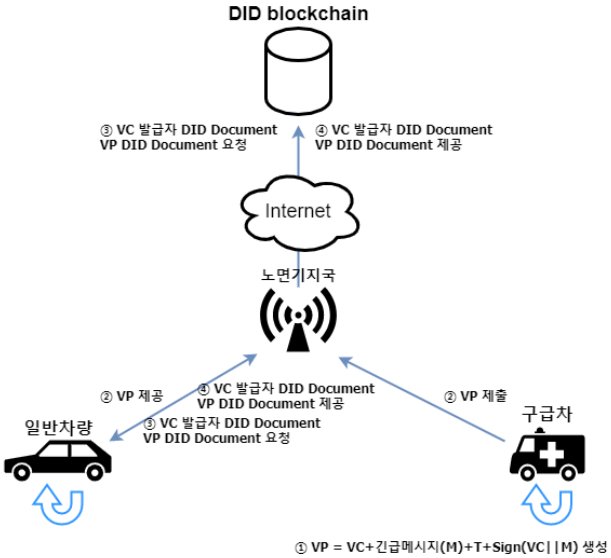
3.1. 긴급 차량 알림 절차

VC 생성 이후, 긴급한 상황이 발생하였을 경우 구급차는 VC + 긴급메시지(M) + T + Sign(VC||M||T)이 담긴 VP 를 생성하여 노면 기지국으로 전송하여 근처의 일반 차량에게 제공하게 된다. 이후 일반 차량은 VC 발급자에 대한 DID Document 와 VP 생성자 DID Document 요청 정보를 다시 노면 기지국으로 전송하고, 인터넷을 통해 DID blockchain 에 전송된다. 이후 VC 발급자 DID Document 와 VP 생성자 DID Document 을 수신하게 된다.

수신한 VC 발급자 DID Document 와 VP 생성자 DID Document 를 이용하여 VC 검증, VP 검증을 마친 뒤 차선 변경을 시도한다. (긴급 차량 알림에 대한 시나리오는 노면 기지국을 통하여 데이터를 전송하는 용도로 삼았으나, V2I 등의 기술이 발전하면, 노면 기지국이 아닌 가로등, 도보 등 사물 또한 사용할 수 있다.)



(그림 6) DID 등록 및 VC 발급 절차



(그림 7) 긴급 차량 알림 절차

4. 결론

자율주행 차량이 발전을 거듭할수록, 사용자의 측면에서는 더욱 편리한 생활을 영위할 수 있지만, 한 번의 사고 또한 생명을 위협하는 피해를 발생시킬 수 있다. 때문에 완전무결한 Level 5 자율주행을 위해서는 V2X 간 신뢰성 높은 통신 방식이 필수적이다. 본 논

문에서는 DID 기술을 이용하여 안전하고 Single Point of Failure 가 없는 높은 수준의 보안을 제공하는 방안을 제안하였다.

참고문헌

[1] NHTSA, Automated Vehicles for Safety, 2020, https://www.nhtsa.gov/technology-innovation/automated-vehicles-safety

[2] Loïc Lesavre el al. “A Taxonomic Approach to Understanding Emerging Blockchain Identity Management Systems”, NIST, 2020, pp. 1-2.

[3] W3C, Decentralized Identifiers v1.0, 2021. 8.

[4] 박준연, 2019, 『스마트 팩토리와 실 도로 주행환경에서의 WAVE V2X 통신 전파 모델 연구』, 한양대학교 공학대학원 석사학위 논문