Journal of Korea Multimedia Society Vol. 21, No. 12, December 2018(pp. 1448-1458)
https://doi.org/10.9717/kmms.2018.21.12.1448

VANET 환경에서의 협력적 메시지 전달을 위한 블록체인 기반 평판 시스템

이경모†, 이경현††

A Reputation System based on Blockchain for Collaborative Message Delivery over VANETs

Kyeong Mo Lee†, Kyung-Hyune Rhee††

ABSTRACT

Vehicular Ad-Hoc Networks (VANETs) have become one of the active areas of research, standardization, and development because they have tremendous potentials to improve vehicle and road safety, traffic efficiency, and convenience as well as comfort to both drivers and passengers. However, message trustfulness is a challenge because the propagation of false message by malicious vehicles induces unreliable and ineffectiveness of VANETs, Therefore, we need a reliable reputation method to ensure message trustfulness. In this paper, we consider a vulnerability against the Sybil attack of the previous reputation systems based on blockchain and suggest a new reputation system which resists against Sybil attack on the previous system. We propose an initial authentication process as a countermeasure against a Sybil attack and provide a reliable reputation with a cooperative message delivery to cope with message omission. In addition, we use Homomorphic Commitment to protect the privacy breaches in VANETs environment.

Key words: Blockchain, Identity Management, Reputation, Smart Contract

1. 서 론

Vehicular ad hoc Networks(VANETs)은 차량이 차량 간 통신(Vehicle to Vehicle) 혹은 차량과 인프라 간 통신(Vehicle to Infrastructure)등으로 트래픽 혹은 안전메시지를 교환하며 이를 기반으로 지능형 교통 시스템과 같은 어플리케이션을 통해 운전자에게 안전하고 편리한 차량 환경을 제공한다[1]. 하지만 이러한 메시지 교환 과정 중 악의적인 차량에 의한 허위 메시지 전파 및 전송 중 트래픽 변조 등 다양한 공격이 발생하고 있어[2] 메시지 송신자 검증 외 메시지 내용에 대한 신뢰성 보장을 위한 방법이 필요하다[3]. 이러한 메시지 내용에 대한 신뢰성 보장 방법으로써 차량에 대해 주체 및 메시지 내용을 기반으로 평판을 적용하는 연구가 진행되었다[4,15].

차량환경에서 평판은 차량 혹은 차량에 의해 송신

※ Corresponding Author : Kyung-Hyune Rhee, Address: A12-1305, Daeyeon Campus, Pukyong National University, Yongso-ro 45, Nam-gu, Busan, (48513), Republic of Korea, TEL : +82-51-629-6247, FAX : +82-51-626-4887, E-mail : khrhee@pknu.ac.kr
Receipt date : Oct. 1, 2018, Revision date : Dec. 5, 2018
Approval date : Dec. 12, 2018

† Interdisciplinary Program of Information Security, Graduate School, Pukyong National University (E-mail : dlrud2539@pukyong.ac.kr)
†† Department of IT Convergence and Application Engineering, Pukyong National University
※ This research was supported by the MSIT(Ministry of Science, ICT), Korea, under the ITRC(Information Technology Research Center) support program (IITP-2018-2015-0-00403) supervised by the IITP(Institute for Information &communications Technology Promotion)

된 메시지가 신뢰할만한 것인지를 결정하는 지표가 되며, 특정 차량에 대한 보상을 주거나 제재를 가할 수 있는 기준을 제공한다. 보통 특정 차량의 평판은 해당 차량의 과거 행동에 대해 몇 가지 지표를 이용해 계산된다. 초기 평판 시스템은 중앙 집중 방식으로서 모든 평판값은 차량으로부터 중앙 서버로 전달된 센서데이터 값 혹은 차량 운전자의 경험을 토대로 중앙 서버 혹은 클라우드에서 저장 및 처리되었다. 하지만 증가하는 차량의 개체 수 때문에 중앙 처리 기관에서는 평판값 계산의 오버헤드가 발생하였으며 평판값을 저장 및 처리하는 중앙 집중 시스템에 의해 평판값 위변조가 발생할 가능성이 제기되었다[5].

한편 중앙 집중 방식의 병목현상 문제를 해결하기 위해 분산처리 방식의 차량 평판시스템이 제안되었다[4]. 해당 시스템에서는 지리적으로 분산된 차량 혹은 RSU(Road-Side Unit)에 의해 지역적으로 수집되는 차량의 속도와 위치 등과 같은 센서값으로부터 지역별로 메시지에 대한 신뢰성을 계산하여 이로부터 메시지의 신뢰성을 측정하였다. 하지만 분산처리 방식의 평판 시스템에서 공격자는 각 RSU와 차량의 센서 데이터를 위조하거나 허위 신원을 통해 평판 시스템을 무력화할 수 있었으며 또한 지역적으로 계산되는 평판값에 대해 전체 환경에서 평판값을 동기화하여 관리해야 하는 문제가 발생하였다.

이후 언급된 평판값 공유의 문제 및 분산처리 환경에서 발생될 수 있는 공격가능성과, 중앙 집중 시스템에서 평판 값 위변조 문제를 해결하기 위해 블록체인 기반의 차량 평판 관리시스템이 제안되었다[6-7]. 블록체인은 일반적으로 분산된 네트워크에서 모든 참여자간 일관된 분산 데이터베이스를 유지하기 위해 사용하는 기술로서 초기 비트코인이라 불리는 암호화폐 교환의 목적으로 사토시 나카모토에 의해 제안되었다[8].

기존의 블록체인과 결합한 차량 평판 관리 모델에서[6-7]는 차량 클러스터(Vehicle Cluster) 단위에서 센서 데이터 값이나 평판값에 대한 합의를 수행하여 차량에 대한 평판점수를 산출하는 방법을 제시하였으나, 평판 계산의 주체가 차량일 때 비트코인의 PoW(Proof of Work)와 같은 합의 알고리즘을 수행하는 것은 적합하지 않았다. 또한 저장된 정보는 차량 클러스터(Vehicle Cluster)간에서만 유지되어 해당 클러스터가 소멸되면 평판에 관한 정보가 소멸되는 문제점이 있었다.

최근에는 스마트 컨트랙트를 활용한 블록체인 기반의 개체 중심의 차량 평판 시스템에 관한 연구가 진행되었다. 이 시스템에서는 차량의 실제 신원과 블록체인 주소를 연결시켜 차량이 수행한 행위에 대해 차량 운전자가 주관적으로 이를 평가하고 평가 과정의 전반적인 처리를 스마트컨트랙트를 통해 투명하고 무결하게 처리하는 시스템이다. 하지만 이 시스템에서는 차량의 신원과 블록체인의 주소를 연결하여 악의적인 차량의 경우 해당 블록체인 주소를 블랙리스팅 시킬 수 있지만 블록체인의 주소는 비용없이 생성될 수 있어 악의적인 공격자는 주소를 무작위로 생성하여 공격을 하는 시빌 공격(Sybil Attack)이 가능한 문제가 있었다. 또한 V2V(Vehicle-to-Vehicle) 환경에서 메시지 누락 및 위변조 공격에 대한 방어 기법 혹은 부적절한 행위 방지를 위한 동기부여 방안 없이 메시지의 신뢰성만을 지표로 평판을 산출한 제한점이 있었다. 이를 개선하기 위해 본 논문에서는 시빌 공격에 대한 대응방안으로 스마트 컨트랙트와 OTP(One-Time Password)를 활용한 초기 신원 인증방법을 제시한다. 또한 V2V 환경에서 전달되는 메시지의 신뢰성 뿐 아니라 협력적으로 메시지를 전달하는 행위에 대해서도 블록체인 상 신원과 연관하여 평판을 기록 및 저장하고, 협력적 행위에 대한 좋은 평판을 부여하는 시스템을 제안한다. 제안 시스템은 암호학적 기법인 Homomorphic Commitment[9]을 사용하여 평판 과정에서 발생할 수 있는 차량의 신원 노출문제에 대해 익명성을 보장한다. 또한 성능 평가를 위해 제안 평판 시스템의 안전성을 분석한다.

본 논문의 구성은 다음과 같다. 2장에서 평판시스템 및 블록체인 기반의 신원 관리에 대해 소개하며 3장에서 보안 요구사항과 시스템 모델을 제시하고 4장에서는 제안 시스템의 알고리즘을 기술하고 이에 대한 안전성을 분석하며 5장에서는 결론을 맺는다.

2. 사전연구

2.1 평판 시스템

Zhang[10]은 차량에서 평판 시스템을 크게 개체 중심, 데이터 중심, 혼합 형태로 분류하였으며 개체 중심의 경우 차량의 이전 행위에 대한 정보를 피드백

하여 차량의 평판을 산출하는 형태이며 데이터 중심은 차량에 의해 발생하는 데이터/이벤트 자체에 대한 신뢰성을 평가하는 모델이다. 혼합형은 이 두 가지 모델을 결합한 것을 말한다. 평판의 수집원과 관련하여서는 1)사용자에 의해 제출된 평판 2) 센서데이터 기반의 수집으로 구분되며 1)의 경우 사용자간 상호 평판을 부여하는 방법을 사용해 주관이 개입되는 시스템이며 2)의 경우 사람의 주관적 판단에 의한 평판의 오류를 줄이기 위해 센서 장비로부터 수집된 정보를 기준으로 평판을 산출하는 시스템이다.

평판 데이터의 수집기간은 VANET 환경에서 차량의 이동성과 정보의 시·공간적 유효성[2,4] 때문에 단기적으로 수집되는 것이 적합하다. 제안 시스템에서는 개체중심의 평판시스템과 사용자에 의해 제출된 평판을 활용한 시스템을 구성한다.

2.2 블록체인 스마트 컨트랙트

기존 중앙 집중 방식 네트워크 구조와 달리 블록체인 네트워크에서는 중앙 관리 주체 없이 네트워크의 모든 구성원은 해시함수, 합의 알고리즘 등을 통해 분산된 환경에서 무결하고 일관된 데이터베이스를 유지하며 채굴과정에서 생성되는 블록에 정보를 저장한다. 참여 노드는 블록들의 암호학적 연결 구조인 블록체인의 동일한 복사본을 저장하여 동기화 하며 한번 블록체인에 기록된 정보는 위변조가 어렵다. 블록체인의 높은 무결성과 안전성 때문에 블록체인은 다양한 응용에서 적용되었으며 범용적 목적의 사용을 위해 이더리움 스마트컨트랙트가 제안되었다. 블록체인의 경우 분산합의 절차를 통해 분산 환경에서도 하나의 신뢰되는 결과를 생성할 수 있으며 이와 같은 성질은 기존의 평판시스템의 문제를 효율적으로 개선시킬 수 있어 평판 시스템과 잘 결합된다[11]. 특히 스마트컨트랙트에서는 각 트랜잭션의 송신자를 개개인이 소유한 개인키로부터 생성된 서명을 메시지와 함께 검증함으로써 식별할 수 있다.

제안하는 시스템에서 각 차량은 블록체인 상 정의되는 인증된 주소를 가지며 이에 대해 평판값을 하나의 속성으로 보고 메시지를 협력적으로 전달하는 차량이 전달과정에 참여했다는 증명으로 암호학적 Commitment를 전달하고 이는 이후 블록체인의 스마트 컨트랙트에서 처리 과정을 거쳐 평판 값으로 반환된다.

2.3 준동형 Commitment (Homomorphic Commitment)

Commitment는 커미터(Committer)가 선택한 메시지의 값을 다른 사람에게 비공개한 상태에서 이를 상대방에게 전달하고 전달한 값을 차후에 공개할 수 있도록 하는 암호학적 기술을 의미한다. 최근 익명성과 프라이버시가 강조된 암호화폐[12]의 경우 Pederson commitment[9]를 사용하고 있으며 이는 준동형 성질을 만족한다. 이는 특정조건에서 숨기고자 하는 메시지 m에 대해서 랜덤한 숫자 r을 $(g^m \cdot h^r)$와 같이 구성하여 전달하고 이후 공개할 때에는 메시지 m과 랜덤값 r을 함께 공개한다. 이때 전달한 값 $C=(g^m \cdot h^r)$을 만족시키는 m, r과 또 다른 $C' = (g^{m'} \cdot h^{r'})$을 만족시키는 m', r'이 있을 때 이는 $C \times C' = (g^{m+m'} \cdot h^{r+r'})$을 만족시키며 이러한 성질을 준동형 성질이라고 한다. 이후 $Statement = (g^m \cdot h^r)$을 만족시키는 비밀값$(m,r)$을 공개하는 절차를 de-commit으로 정의한다. 본 논문에서는 다수의 참여자간 협력적 메시지에 관한 증명으로 스마트 컨트랙트에 전달될 개별적인 Commitment[10]를 구성하여 환경에 전파하고 이후 환경에서 전달되는 메시지에 대해 신뢰성을 사용자가 판단하여 이후 메시지를 전파할 때 새로운 Commitment로 구성하여 전달하는 모델을 제시한다.

3. 시스템 모델

3.1 평판 시스템 요구사항

• 메시지의 진위성 : 전달되는 메시지의 무결성과 메시지 내용의 진위성이 검증되어야 한다.

• 공정성 : 올바른 메시지 전달에 협력적인 차량과 올바르지 않은 메시지 전파를 차단한 차량은 좋은 평판을 얻어야하며, 악의적인 공격자 및 공모 공격자는 어떠한 이득도 얻을 수 없어야 하고 이후 고발될 수 있어야 한다. 참여 없이 메시지를 누락시키는 노드는 아무것도 얻을 수 없다.

3.2 보안 요구사항

• 익명성 : 협력적 메시지 전달 과정에서 Commitment 값으로부터 공격자는 어떠한 차량에 관한 신원정보도 획득할 수 없어야 한다.

• 공모 공격에 안전 : 공모공격에 대해 저항하거나 고발 할 수 있는 절차가 설계되어야 한다.

• 평판값의 무결성 및 투명성 : 평판값은 무결한 방법으로 계산되고 기록되어야 한다.

• 시빌 공격 대한 안전 : 시빌(Sybil) 공격자[13]에 대한 안전성이 확보되어야 한다.

• DoS 공격에 대한 안전 : 악의적으로 시스템의 취약점을 이용하는 DoS 공격에 대한 안전성이 확보되어야 한다.

3.3 시스템 모델

시스템은 다음의 6개 프로세스로 구성된다. 1)스마트 컨트랙트 초기화 2)OTP 인증 3)메시지 전파 및 참여증명 생성 4)메시지 검증 및 전달 5)참여증명 검증 6)고발절차 및 평판 재조정으로 진행되며 다음은 시스템에서의 표기법을 나타낸다.

• 가정 사항

초기 차량의 신원 식별 및 OTP 인증을 위해 기존 운용중인 V-PKI(Vehicular Public Key Infrastructure)가 존재하며 차량의 신원에 대한 검증을 담당하는 차량 관리국을 DoT(Department of Transport)로 두고 DoT와 각 노변 장치(Road Side Unit)들은 컨소시엄 형태의 블록체인을 구성하며 스마트 컨트랙트 구동을 위한 블록체인을 구성하였다고 가정한다. 차량의 신원과 블록체인 주소를 연결하는 OTP 인증 과정 전 DoT는 실제 차량의 소유주와 차량의 정보를 검증하고 VPKI 로부터 얻은 공개키를 통해 차량에게 OTP를 안전한 채널을 통해 전송할 수 있다고 가정한다.

또한 차량은 충분한 양의 센싱 능력을 갖추었으며 차량의 운전자는 메시지 전달과정 중에 메시지 내용의 신뢰성을 주관적으로 판단하여 평가할 수 있다고 한다. 이때 차량의 운전자는 좋은 평판을 얻기 위해 이성적으로 행동한다고 가정한다. 각 표(표 2-7)에서는 6개의 프로세스의 알고리즘을 기술한다.

1) 스마트 컨트랙트 초기화 단계

차량은 평판을 관리하는 블록체인 네트워크에 참여를 위해 블록체인 주소와 관련된 키 쌍을 생성하고 이더리움 블록체인 주소를 생성한다. DoT는 사전에 확인된 차량의 정보를 토대로 블록체인 노드로 참여하는 차량의 속성을 다음과 같이 스마트 컨트랙트 상 정의한다.

Table 1. Notation

Notation	Description
$V_{r_n}^{cmt}(ID, r_n)$	The commitment scheme is used as a proof of participation that the correct message is delivered to another vehicle during the message delivery process. The secret value is composed of the identity value ID and the random value of the vehicle r_n.
$Proof_{seq}, Proof_{len}$	$Proof_{len}$ means the total number of vehicles that cooperatively delivered the message, and $Proof_{seq}$ is incremented whenever messages are passed. Since the highest $Proof_{len}$ is the most reliable, each participant who delivers the message with highest $Proof_{len}$ has a good reputation.
$Contract_{function}$	It represents the function of the smart contract, which is composed of the following function set. $function\ set := < announce, gather, submit, renew >$
	$Announce$: It receives a proof of participation value for Mid(Message-ID).
	$Gather$: It gathers r_n for the message which is evaluated as a reliability by a vehicle and calculates a reputation of the participants.
	$Submit$: It is used to report the fact that a message corresponding to Mid is forged. It is designed to resist against a collusion attack.
	$Renew$: It is used to re-adjust the reputation value by considering the number of vehicles participating in the correct or incorrect message delivery process.
$Vehicle_{key}^{action}$	$key\ set := < sk, pk >, action\ set := < sig, ver >$ The private key sk and public key pk are respectively used to make blockchain address. sig is used to sign a blockchain transaction, and ver is used to sign a blockchain transaction.

<Unique ID, SensorAccuracy, RepValue, acting Coverage>

이후 차량의 ID를 발급하기 전에 DoT는 별도 차량에 대한 신원인증 과정을 거친 뒤 차량과 연관된 인증서를 통해 발급할 ID에 관련된 OTP 인증값과 해당 ID에 관한 속성이 정의된 스마트 컨트랙트의 주소를 암호화하여 차량에게 전달하고 이후 책임 추적성을 위해 차량의 실제신원과 스마트컨트랙트 상의 ID을 매핑하여 기록한다.

2) OTP 인증단계

차량은 DoT로부터 전달받은 암호화된 메시지를 통해 OTP 정보를 얻은 후 스마트컨트랙트 주소에서 정의된 인증함수로 OTP값을 전송하여 인증을 시도한다. 인증과정에서 OTP 인증에 성공하면 해당 ID 및 관련정보는 해당 차량이 소유하게 된다.

3) 메시지 전파 및 참여증명 생성

Commitment 스킴 사용을 위한 초기화 단계로써 전역 파라미터를 초기 글로벌 매개변수 절차와 같이 정의한다.

Mid 생성단계에서는 메시지와 식별과 무결성의 확인을 위해 Mid setup 알고리즘과 같이 해시함수를 적용하여 Mid를 생성한다.

Proof setup단계에서는 이성적인 차량이 메시지의 무결성 및 신뢰성을 확인 후 전달과정에 참여했다는 증명을 Pederson Commitment의 형태로 생성하며 이때 $<ID, r_n>$ 값은 비공개로 한 뒤 이후 $Contract_{gather}$함수를 통해 r_n값을 공개한다. 이 때 $Proof_{seq}$는 참여자가 참여증명을 생성할 때마다 1씩 증가시켜 함께 브로드캐스팅 한다.

이후 Broadcast 단계에서는 <Mid, Msg, V_n^{cmt}, $Proof_{seq}$>를 브로드 캐스팅한다.

4) 메시지 검증 및 전달 단계

차량 간 통신(V2V) 혹은 브로드캐스팅을 통해 전달받은 튜플 <Mid, Msg, $V_{r_n}^{cmt}$, $Proof_{seq}$>을 받으면 3

Table 2. Setup(Smart Contract Construct)

Algorithm 1. Setup(Smart Contract Construct)	
Input : Unique ID, Output : ID which owned by vehicle(Depart of Transport) address owner; set owner= msg.sender; set generator= msg.sender; onlyOnwer() condition is defined as below; <msg.sender is only DoT>	onlyOwner() condition; set vehicleInfo{ Vehicle[owner].ID Vehicle[owner].sensorAccuracy, Vehicle[owner].repValue Vehicle[owner].actingCovarage Vehicle[owner].otp Vehicle[owner].signer } mapping(string => address) reporter; mapping(string => address) submitter; mapping(address => vehicleInfo) Vehicle;

Table 3. Setup(OTP Authentication)

Algorithm 2. Setup(OTP Authentication)	
onlyOwner() Condition; //generate OTP and save OTP value OTP = generated random number by DoT function setHash(OTP) { return hashed otp } Vehicle[owner].otp = hashed otp	//receive OTP and Authenticate OTP Value _otp = it received by vehicle function authentication(_otp) { require(Vehicle[owner].otp == keccak256(_otp); Vehicle[owner] = Msg.Sender; submitter[ID]= Vehicle[owner].ID delete Vehicle[owner].otp; }

Table 4. Propagating messages and generating proof of participation

Algorithm 3. Propagating messages and generating proof of participation	
Input : <Msg, Global Parameter> Output : <Mid, Msg, V_n^{cmt}, $Proof_{seq}$> Secret : <ID, r_n>	
//Initialization Global Parameter(Commitment Setup) *Let* $q, p \in P$ *be primes* that $p = r \cdot q + 1$ for some $r \in N$ *Let* q be the order of a subgroup of $Z_P^*(G_q)$ *Let* $g, h \in G_q$ //Mid setup function setMid(Msg){ Mid= hash(Msg) }	//Proof setup to prove the fact vehicle cooperate with others function set proofOfParticipate(ID){ r <– *Uniformly Random* V_r^{cmt} <– $(g^{ID} \cdot h^r)$ Return $V_r^{cmt}(ID_r, r)$; //Broadcast <Mid, Msg, V_n^{cmt}, $Proof_{seq}$> }

Table 5. Message verification and delivery

Algorithm 4. Message verification and delivery	
Global Input : <Mid, Msg, $V_{r_n}^{cmt}$, $Proof_{seq}$> **Case1)** Contents is not trustworthy or contaminated" **Output1)** $Contract_{anounce}(Mid, false)$ **Case2-a)** Contents is trustworthy and impossible to report to blockchain"	**Output2-a)** Broadcast <Mid, Msg, $V_{r_{new}}^{cmt}$, $Proof_{seq}$>, Secret : <ID, r_n> **Case2-b)** Contents is trustworthy and possible to report to blockchain" **Output2-b)** $Contract_{anounce}(Mid, V_{r_{new}}^{cmt}, Proof_{len})$, Secret : <$ID, r_n$>
Case1) if Mid =! Hash(msg) { <Drop the Message> and then if it is untrustworthy called $Contract_{anounce}(Mid, false, Proof_{len})$ <$v_{n_{sk}}^{sig}$ is used to sign blockchain transaction> } **Case2-a)** $Proof_{seq}$= $Proof_{seq}$+1 function set proofOfParticipate(ID){ r_{now} <– *Uniformly Random* $V_{r_{new}}^{cmt}$ <– $V_{r_n}^{cmt} \cdot (g^{ID_{r_{new}}} \cdot h^{r_{new}})$	//Broadcast Proof <Mid, Msg, V_{new}^{cmt}, $Proof_{seq}$> **Case2-b)** $Proof_{len} = Proof_{seq}$ send transaction called $Contract_{anounce}(Mid, V_{r_{new}}^{cmt}, Proof_{len})$ <$v_{n_{sk}}^{sig}$ is used to sign blockchain transaction>

가지 경우에 따라 다르게 동작한다.

• **Case 1)** 튜플에 포함된 메시지 및 Mid가 해시 함수의 연산을 통해 무결성이 확인되고 난 후 메시지 내용이 올바르지 않거나 허위정보일 경우 $Contract_{anounce}(Mid, false, Proof_{len})$ 트랜잭션을 통해 해당 메시지를 스마트 컨트랙트에 보고하게 된다. 만약 무결성이 손상되었다면 메시지를 전파하지 않고 버린다. 이후 보고를 한 차량은 $Contract_{renew}$에서 조건을 만족하면 좋은 평판을 얻을 수 있으며, "**Case2-a**" 혹은 "**Case2-b**"와 같이 거짓메시지를 전달한 경우에는 $Contract_{gather}$에서 평판 부여에 관한 조건을 만족시키지 못하거나 $Contract_{submit}$에서 이성적인 차

Table 6. SmartContract(Proof Verification)

Algorithm 5 SmartContract(Proof Verification)

Input : $Contract_{anounce}(Mid, V_{r_n}^{cmt}, Proof_{len})$ transaction

$Contract_{anounce}(Mid, V_{r_n}^{cmt}, Proof_{len})$ {
//Mid duplication checking and Proof length checking
if (same Mid is exist) and ($V_{r_n}^{cmt}$ =! 0) and ($Proof_{len_n} > Proof_{len_{new}}$) then **maintain a** $V_{r_n}^{cmt}$
else
replace $V_{r_{new}}^{cmt}$
<Event : request for submitting proof for mid and proof length> }
if (same Mid is not exist)
Mid = *Mid*
<Event : request for submitting proof for Mid and proof length>
inner call $Contract_{gather}(V_{r_{new}}^{cmt}, mid, Proof_{len_n})$
// this releases the secret value of participant that has been delivered to de-commit the proof

// Target proof setup
$Contract_{gather}(V_{r_{new}}^{cmt}, mid, Proof_{len_n})${
Target Proof = $V_{r_{new}}^{cmt}$
Proof length = $Proof_{len_n}$

// Start de-committing
call $Contract_{submit}(mid, r_n)$ {
reporter= msg.sender;
Reporting(reporter, r_n, Mid)

//DoS Defense(delayed-response)
Set deadlineTimer : T(now time + n Interval) for mid
if T<block.now then
return false

// de-committer setup and de-commit
Event Submitting(submitter, r_n, Mid)
for (i=0, i=<proof length, i++)
if submitter =! reporter;
submitter= msg.sender;
accumulator[i] = ($g^{submitter.id} \cdot h^{r_n}$)
deadlineTimer check
"Continue"
for (j=0, j<proof length-1. j++)
temp = accumulator[0]
temp = temp * accumulator[j+1]

// if de-commit result is true
if Target Proof = temp
<extract "submitter" form Event "Submitting">
Vehicle[submitter].repValue=
Vehicle[submitter].repValue + 1

<extract "reporter" from Event "Reporting">
Vehicle[reporter].repValue=
Vehicle[reporter].repValue + 2
// if de-commit result is false
}For for (j=0, j<proof length. j++)
Event fail(submitter.ID[j])||reporter.ID)

량들에 의해 고발되어 평판이 감소한다.

• **Case 2) "Case 1"**의 메시지 무결성 및 진위성이 만족되는 경우, 이때 블록체인 네트워크에 접근할 수 없을 경우 알고리즘3과 같이 자신의 ID를 사용하여 새로운 Commitment인 <Mid, Msg, V_{new}^{cmt}, $Proof_{seq}$>를 브로드 캐스팅한다.

• **Case 3) "Case 1"**의 메시지 무결성 및 진위성이 만족되는 경우, 이때 블록체인 네트워크에 접근할 수 있을 경우 Mid별로 생성된 참여증명인 V_{new}^{cmt}을 포함하는 블록체인 트랜잭션 $Contract_{anounce}(Mid, V_{r_{new}}^{cmt}, Proof_{len})$을 전송한다. 이때 $Proof_{len}$의 경우 메시지 전달에 참여한 차량의 총 숫자를 의미한다. 이후 동일한 Mid에 대해 값이 보고되는 경우 $Proof_{len}$의 값이 큰 쪽이 평판을 얻기 위한 절차로 진행된다.

5) 참여증명 검증 단계

참여증명 검증 단계에서는 "4) 메시지 검증 및 전달 단계"에서 전달된 참여증명 값인 $V_{r_n}^{cmt}$의 값과 Mid에 대해 이 함수를 구독하는 차량의 경우 Event-Caching Protocol[14]을 통해 참여 증명인 각각의 r_n을 제출해야함을 알린다. 이후 차량의 r_n의 값이 $Contract_{submit}(mid, r_n)$을 통해 각각 스마트 컨트랙트로 전달되면 먼저 이들의 송신 블록체인 주소로부터 ID를 추출하고 이후 전달한 r_n값을 Accumulator 함수를 통해 누적시켜가며 연산하여 De-commit(비밀값의 공개)절차를 수행한다. 이후 최초 $Contract_{anounce}(Mid, V_{r_n}^{cmt}, Proof_{len})$를 전달한 차량은

Table 7. SmartContract(Accusing and Renew)

Algorithm 6 SmartContract(Accusing and Renew)	
Input : $Contract_{anounce}(Mid, V_{r_n}^{cmt}, Proof_{len})$ transaction	
$Contract_{anounce}(Mid, V_{r_n}^{cmt}, Proof_{len})$ **//Mid duplication and false message checking** if (same Mid is exist) and ($V_{r_n}^{cmt}$ = false) and ($Proof_{len}$ = null) then accuser= msg.sender; Event Accusing(Mid, accuser, false) **//this function runs by only DoT** $Contract_{renew}(Mid)${	tempA =count(Accusing Event) for Mid tempB =count(Submitting Event) for Mid if temp A > temp B <extract "submitter" form Event "Submitting"> Vehicle[submitter].repValue= Vehicle[submitter].repValue- 2 <extract "reporter" from Event "Reporting"> Vehicle[reporter].repValue= Vehicle[reporter].repValue - 3 <extract "accuser" from Event "Accusing"> Vehicle[accuser].repValue = Vehicle[reporter].repValue + 1 }

"Reporter"가 되며 내부함수 $Contract_{gather}(V_{r_{new}}^{cmt}, mid, Proof_{len_n})$의 호출을 통해 Target Proof 값인 $V_{r_{new}}^{cmt}$와 개개의 차량의 전달한 차량의 ID 및 각각의 r_n 값으로부터 도출된 temp값이 같은지 검증 후 일치하면 참여증명이 신뢰할 수 있는 것이므로 참여하는 모든 사람들에게 평판을 부여하고 Reporter의 경우 추가적인 평점을 얻는다. 만약 검증에 실패할 경우 참여자들은 아무것도 얻을 수 없다.

6) 고발절차 및 평판 재조정 단계

알고리즘 4의 1번 출력으로 $Contract_{anounce}(Mid, false)$을 발생시킨 차량은 전파되는 메시지가 위변조 되었거나 메시지의 진위성이 없음을 확인하고 보고한 경우이므로 이에 대해 올바른 메시지라고 판단한 차량의 수 $Proof_{len}$와 현재 과정에서 보고된 이벤트의 숫자를 판단하여 만약 잘못된 메시지라고 보고된 경우가 많다면 이를 보고한 "Accuser"에게 평판을 부여한다.

4. 안전성 분석

4.1 평판 시스템의 안전성

메시지 진위성 및 공정성 : 전달되는 메시지의 경우 메시지와 Mid에 의해 각 전파단계마다 해시함수 및 차량 운전자의 주관에 의해 검증될 수 있다. 전달되는 메시지 내용의 진위성은 각 차량이 올바른 것과 올바르지 않은 경우를 구분하여 전달하며 정직한 차량의 경우 높은 평판을 얻기 위해 차량의 센싱 능력 등에 기초하여 메시지의 진위성을 판별하고 메시지의 진위성이 있을 경우 참여증명을 보내거나 그렇지 않다면 폐기한다. 악의적인 차량의 경우 허위 메시지를 생성하거나 공모하여 허위메시지를 생성 및 전파할 수 있으나, 알고리즘 6번과 같은 고발 절차를 통해 다수에 의해 평판값이 감소될 수 있다. 모든 메시지에 대해서는 브로드캐스팅 환경을 가정하며 악의적인 노드가 분산된 환경에서 브로드 캐스팅되는 메시지를 전체를 차단하는 것은 매우 어려우며 메시지 누락 등의 공격에 영향을 받지 않는다. 이후 전달되는 메시지에 대한 신뢰성을 보장하기 위해 참여증명으로 Commitment 스킴을 사용하여 다수에 의해 메시지의 신뢰성 및 진위성을 보장받는다.

4.2 시스템 보안성 분석

• 익명성 : 전달되는 과정에서 공개되는 참여증명(Commitment)의 경우 암호화되어 있으며 이로부터 관련된 차량의 ID를 알아내는 것은 이산대수의 어려움에 근간하여 다항시간 내 불가능하다. 또한 참여증명에 대한 검증과정(알고리즘 5)에서도 단순히 블록체인 주소에 대한 r_n 값만을 전달하며 이와 연관된 ID를 스마트컨트랙트 내부에서 추출하여 이후 트랜잭션의 발생 순서에 관계없이 통합되어 검증되므

로 익명성 및 시간 기반의 추론 공격[17]에 대해 저항성을 가진다.

• 악의적인 공격 및 공모에 대한 안전성 : 전파되는 메시지에 대해 참여증명의 값 중 값이 큰 것을 신뢰된 것으로 판단하며 지역적인 공모공격에서 50% 이상의 이성적인 차량만 있다면 악의적인 메시지는 이성적인 차량에 의해 전달되지 않는다. 또한 이후 보고절차를 통해 특정 메시지와 Mid가 거짓 메시지라는 사실이 보고될 때 지역적으로 50% 공모에 성공하여 평판을 얻더라도 전체 차량 환경에서 메시지의 오용보고 건수(Accusing Event)가 알고리즘 6의 Submitting Event의 수보다 크면 기존의 악의적으로 얻은 평판값보다 더 큰 평판값을 감소시켜 공격자 혹은 공모자는 어떠한 좋은 평판도 얻을 수 없다.

• 평판값의 무결성 및 투명성 : 평판값은 블록체인 상 신원과 연결되어 계산되며 투명성 및 무결성이 확보된다. 모든 절차에 있어서 스마트컨트랙트의 Event 함수를 통해 발생한 이벤트를 이를 구독하는 차량에게 알리고 평판에 관한 재조정 절차를 진행하며 만약 DoT에 의해 임의로 평판이 부여될 경우 이는 이벤트 함수로써 모든 차량이 알 수 있게 되어 중앙 기관에 의한 평판위변조에 대해서도 확인 할 수 있다. 또한 평판값의 증가 및 감소는 스마트컨트랙트의 특성에 따라 모두 규칙에 의해 통제되므로 이를 조작하는 것은 불가능하다.

• 시빌공격에 대한 안전성 : 최초 신원 인증 과정에서 OTP의 값은 차량의 인증서 및 공개키를 통해 암호화되고 전달되므로 공격자는 알 수 없으며, 만약 OTP값을 추측하더라도 접근할 수 있는 인터페이스 주소인 스마트컨트랙트 주소를 모르면 신원을 위조할 수 없다. 또한 인증된 블록체인 주소인지의 여부를 최종 평판 산출 과정 전에 검증함으로써 악의적인 참여는 참여증명의 값을 제시할 수 없으므로 평판값을 얻을 수 없다.

• DoS : 악의적인 공격자는 프로토콜의 취약점을 이용하여 참여증명의 값을 제시하지 않는 방식으로 DoS 공격을 수행한다. 이 때 악의적인 차량이 참여증명의 비밀값 r_n을 제출하는 과정에서 응답을 지연시키는 것을 방지하기 위해 타이머를 두어 특정 시간 내 응답이 제출되지 않으면 해당 함수가 종료되도록 하여 DoS 공격을 방어한다.

4.3 시스템 평가

1) 항목의 경우 차량으로부터 발생한 메시지의 평판 계산 방법에 대한 비교분석이며, 모델마다 상이한 방법론을 사용한다. 이 경우 제안하는 모델에서는 스마트 컨트랙트 코드의 무결성과 투명성을 통해 평판 산출의 신뢰성이 보장되며 모듈식 설계와 함수의 구현을 통해 유연한 평판 산출 방법을 적용 할 수 있다.

2) 항목의 경우 언급한 Sybil Attack과 관련된 안전성 보장 항목이며, 제안하는 모델에서는 기존 모델을 개선하여 스마트 컨트랙트 기반의 OTP 인증을

Item / Reference Model	Proposed Model	Zhan et al.[6]	Zhe Yang et al.[7]
1) Message Evaluation Method	Smart Contract Functionality (Algorithm)	Bayesian Inference Model	Local-sensor based Consensus and Parameters
2) Sybil-resistance	Smart Contract OTP Authentication	No Support	No Support
3) Privacy	Pedersen Commitment Scheme	No Support	No Support
4) System Security Model against Attacker	- Message Integrity & Reliability (Rational Participants Model) - Fairness (Smart Contract Algorithm) - Sybil-resistance (Authentication) - Dos-resistance(Timer)	- Message Integrity & Reliability (Rational Participants Model) - Fairness (Vehicle-level Consensus)	- Message Integrity & Reliability (Local-sensor based Consensus) - Fairness (Vehicle-level Consensus)

통해 Sybil Attack에 대한 보호 기능을 제공한다.

3) Privacy의 경우 평판을 계산하는 차량에 대한 프라이버시 보호에 관한 항목으로써, 구체적으로 익명성 혹은 비연계성 등을 통해 보장될 수 있는 특성이다. 이러한 특성은 기존 모델에서는 제공하지 않으며, 제안 모델에서는 Pedersen Commitment를 통해 차량의 식별자를 숨기고, 평판 산출 과정에서 스마트 컨트랙트 내부 EVM 처리 연산을 통해 외부로부터 평판자에 대한 정보를 누출시키지 않기 때문에 평판 산출 과정에서 익명성 및 프라이버시 보호가 가능하다.

4) 공격자에 대한 시스템 보안 모델의 경우 시스템에서 만족하는 공격자에 대한 보호 수준으로 정의되며, 기존모델에서도 1) 차량 메시지의 무결성 및 진위성, 2) 공정성(부당한 평판을 얻을 수 없음)을 제시하고 있으나, 제안하는 모델에서는 추가적으로 DoS와 Sybil 공격에 대한 추가적인 안전성을 제공한다.

5. 결 론

본 논문에서는 차량환경에서 전달되는 메시지 내용의 신뢰성 확보를 위해 제안되었던 블록체인 기반의 차량 평판시스템에서 발생할 수 있는 시빌 공격에 대한 대응방안으로 스마트 컨트랙트와 연계한 초기 신원 인증 방법을 제시하였다. 또한 차량환경에서 비협력적인 메시지 전달 및 메시지 위변조 공격에 대한 대응방안으로 메시지 전달 과정에서 메시지의 신뢰성을 판단하여 협력적으로 전파하는 차량에게 좋은 평판을 부여하는 시스템을 제안하였다. 추가적으로 제안 시스템에서는 차량의 프라이버시 보호를 위해 Commitment 스킴을 사용하였으며 이에 대한 전체 과정을 알고리즘으로 구현 및 안전성을 분석하였다. 향후 제안된 시스템을 통해 획득한 평판을 기반으로 메시지 신뢰성이 요구되는 다양한 차량 어플리케이션에 활용할 수 있을 것으로 기대된다.

REFERENCE

[1] K. Zhang, J. Ni, K. Yang, X. Liang, J. Ren, and X.S. Shen, "Security and Privacy in Smart City Applications: Challenges and Solutions," *IEEE Communications Magazine*, Vol. 55, No. 1, pp. 122-129, 2017.

[2] M. Raya, P. Papadimitratos, and J.P. Hubaux, "Securing Vehicular Communications," *IEEE Wireless Communications*, Vol. 13, No. 5, pp. 8-15, 2006.

[3] Q. Li, A. Malip, K.M. Martin, S.L. Ng, and J. Zhang, "A Reputation-based Announcement Scheme for VANETs," *IEEE Transactions on Vehicular Technology*, Vol. 61, No. 9, pp. 4095-4108, 2012.

[4] Soleymani, Abdullah, Hassan, Anisi, Goudarzi, Baee et al., "Trust Management in Vehicular Ad Hoc Network: A Systematic Review," *EURASIP Journal on Wireless Communications and Networking*, Vol. 2015, No. 1, pp. 1-146, 2015.

[5] A. Schaub, R. Bazin, O. Hasan, and L. Brunie, "A Trustless Privacy-preserving Reputation System," *Proceeding of IFIP International Information Security and Privacy Conference*, Vol. 471, pp. 398-411, 2016.

[6] Z. Yang, K. Yang, L. Lei, K. Zheng, and V.C. Leung, "Blockchain-based Decentralized Trust Management in Vehicular Networks," *IEEE Internet of Things Journal*, p. 1, 2018.

[7] Z. Yang, K. Zheng, K. Yang, and V.C. Leung, "A Blockchain-based Reputation System For Data Credibility Assessment in Vehicular Networks," *Proceeding of Personal, Indoor, and Mobile Radio Communications*, pp. 1-5, 2017.

[8] S. Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System, Whitepaper*, 2008.

[9] T.P. Pedersen, "Non-Interactive and Information-theoretic Secure Verifiable Secret Sharing," *Proceeding of Annual International Cryptology Conference*, pp. 129-140, 1991.

[10] J. Zhang, "Trust Management for VANETs: Challenges, Desired Properties and Future Directions," *International Journal of Distributed Systems and Technologies*, Vol. 3, No. 1, pp. 48-62, 2012.

[11] V. Buterin, *A Next-generation Smart Con-*

tract and Decentralized Application Platform, *Ethereum White Paper*, 2014.

[12] D. Yang, G. Jack, and Z. Wilcox-O'Hearn, *Survey of Confidentiality and Privacy Preserving Technologies for Blockchains; R3*, *Zcash Company*, 2016.

[13] J.R. Douceur, "The Sybil Attack," *Proceeding of International Workshop on Peer-to-peer Systems*, pp. 251-260, 2002.

[14] Ethereum Contract ABI, https:// github.com/ethereum/wiki/wiki/Ethereum-Contract-ABI (accessed Sept., 21, 2018).

[15] J.H. Shin, T.H. Kim, and S.W. Tak, "A Reputation Management Scheme Improving the Trustworthiness of Multi-peers and Shared Resources in P2P Networks," Journal of Korea Multimedia Society Vol. 11, No. 5, pp. 1409-1419, 2008.

이 경 모

2016년 2월 국가 평생 교육 진흥원 학사 졸업
2017년 9월~현재 부경대학교 대학원 정보보호학(협) 석사과정
관심분야 : 정보보호, 블록체인, 보안 관리, 인프라 보안, 네트워크 보안

이 경 현

1982년 2월 경북대학교 수학교육과 졸업
1985년 2월 한국과학기술원 응용수학과 석사
1992년 8월 한국과학기술원 수학과 박사
1985년 2월~1993년 2월: 한국전자통신연구원 연구원, 선임연구원
1993년 3월~현재: 부경대학 IT융합응용공학과 교수
관심분야 : 정보보호, 암호이론, 암호 프로토콜, 통신보안, 블록체인