VANET에서의 위치 프라이버시 보호 기술 분석

김영민*, 정두훈*, 임헌정**, 이준호**, 정태명*
*성균관대학교 정보통신공학부
**성균관대학교 전자전기통신공학과
e-mail: imyomi45@hanmail.net, euler07@naver.com,
{hjlim99, jhlee83}@imtl.skku.ac.kr, tmchung@ece.skku.ac.kr

The Analysis of Location Privacy Preserving Technology in VANET

Young-Min Kim*, Doo-Hun Jeong*, Hun-Jung Lim**, Jun-Ho Lee**, and Tai-Myoung Chung*
*School of Information Communication Engineering, Sungkyunkwan Univ
**Dept of Electrical and Computer Engineering, Sungkyunkwan Univ

요 약

인간의 가장 큰 욕구인 편의와 안전을 위해 우리의 곁에서 떨어질 수 없는 것이 차량이다. 그러므로 차량을 이용하면서 겪게 되는 안전과 편의 또한 떼어놓을 수 없는 문제 중에 하나다. 그 편의와 안전을 위해 VANET이 활발히 개발 중이다. VANET은 차량에서 사용되는 근거리/중거리 통신용 무선 프로토콜로써 차량 간 통신인 V2V, 차량과 네트워크 기반구조 간의 통신인 V2I를 지원하는 네트워크로써 다양한 서비스를 제공한다. 이에 학문적, 상업적으로 많은 관심을 받고 있다. 그러나 네트워크 기반의 기술인만큼 사용자의 프라이버시 침해가 큰 문제로 대두되고 있다. 이 중에서도 사용자의 익명성, 추적성, 객체인증에 관한 Location Privacy는 개발과정에서 큰 걸림돌이 되고 있다. 이에 본 논문에서는 VANET에서의 Location Privacy 보호에 대한 기술들의 개략적인 내용을 서술하고, 장단점을 분석하였다. Location Privacy 보호를 위한 기술에는 해쉬통합을 이용한 보호기술, MAC-체인을 이용한 보호기술, 그리고 세션 키 교환을 이용한 보호기술이 있다. 세 가지 기술 중에서 MAC-체인을 이용한 기술이 Location Privacy 보호에 가장 적합하다.

1. 서론

VANET(Vehicular Ad hoc Network)은 크게 차량 간 통신인 V2V(Vehicle To Vehicle), 차량과 각 도로에 설치되어 있는 *RSU*(Road Side Unit)간의 통신인 V2I(Vehicle To Infrastructure)로 나뉜다. 사용자는 V2V를 통해 차량 간의 안전주행메시지를 교환하여 차량 간 사고를 예방함으로써 안전을 보장받을 수 있고, V2I를 통해 주변 편의시설정보 및 멀티미디어 서비스를 제공받음으로써 사용자의 편의를 극대화 할 수 있다. 그러나 그와 함께 대두되고 있는 것이 보안문제이다. 본 논문에서는 보안문제 중에서 Location Privacy를 위협하는 요소를 중요 문제로 인식하여 익명성 보장을 위한 Location Privacy 보호에 관한 세 가지 기술들의 장단점을 분석한다.

본 논문의 구성은 다음과 같다. 2장에서는 VANET 환경에서 보안 위협에 관련된 보안 요소를 알아본다. 3장에서는 Location Privacy 보호를 위한 세 가지 기술에 대해서 분석한다. 4장에서는 세 가지 기술의 장단점을 정리한다. 마지막으로 5장에서는 결론을 맺는다.

2. 보안 요소

본 장에서는 VANET 환경에서의 보안 위협에 관련된 보안 요소 중 Location Privacy에 대한 위험요소에 대해 파악하고, 그에 필요한 보안요소를 정의한다. V2V와 V2I를 통한 통신에는 다음과 같은 위험요소가 있다. 첫 번째로 V2V통신 상황에서 사용자의 위치 정보를 변조하여 다른 사용자에게 전달하게 되면 정보를 받은 사용자들이 잘못된 위치정보로 인해 사고를 당하거나 길을 혼잡하게 만들 수 있는 위험요소가 있다. 두 번째로 V2I통신 상황에서는 공격자가 네트워크를 통해 무선채널 방해신호(DoS 공격)를 보냄으로써, 네트워크 동작이 중단되고 차량 간 안전메시지 교환이 불가능해져 사고를 유발 할 수 있다. 이러한 위험요소를 방지하기 위한 보안요소는 다음과 같다[1,2,3,4,5].

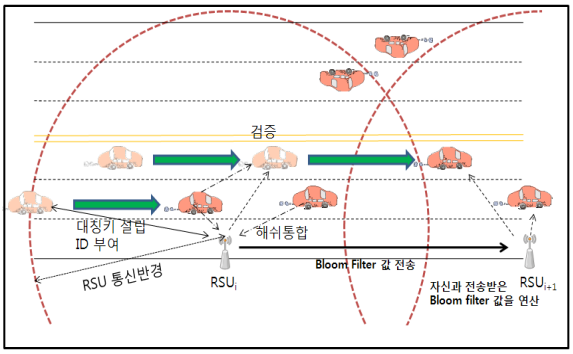
- 객체인증(Entity Authentication): 객체인증은 프로토콜의 구성자가 다른 구성자의 특정정보 또는 증거를 확인함으로써 실제 네트워크 노드임을 확인해야 한다.
- 추적성(Traceability): 필요 시 인증 가능한 제 3의 기관이 개입하여 차량에 대한 추적을 가능하게 해야 하며, 실제 사고 발생 차량의 실제 아이디를 알 수 있어야 한다.
- 익명성(Anonymity): 사용자의 개인정보는 사용자의 프라이버시 위협을 보호하기 위해, 네트워크 내부의 메시지로부터 노출되지 않아야 한다.

본 논문에서는 위의 세 가지 보안 요소 중 익명성과 추적성에 초점을 맞춘다.

3. Location Privacy 보호 기술

3.1 해쉬통합을 이용한 보호 기술

차량 밀집환경에서 익명성을 보장하고 효율적인 V2V 통신을 위해 (그림 1)과 같이 *RSU*와 각 차량이 대칭키를 교환한 후, 각 차량의 메시지를 *RSU*가 통합하여 해쉬통합 값을 Bloom Filter로 처리하고 각 차량이 이를 받아 수신한 메시지를 검증할 수 있게 하는 기술이 제안되었다 [6].



(그림 1) 해쉬통합 기술의 메시지 검증

이 기술에서는 VANET의 두 계층구조인 AAA와 *RSU* 사이의 통신은 항상 신뢰받는다고 가정한다. 차량이 자신의 통신반경 안에서 *RSU*를 감지하면 둘 사이에 대칭키를 공유하게 된다. 이 과정은 공개키 기반의 Diffie-Hellman 키 교환 프로토콜을 적용하여 이루어진다. 신뢰된 기관과 k개의 노드가 통신할 때, 각 노드는 똑같은 ID를 사용하여 서로간의 익명성을 보장하면서 기관은 각각의 노드를 구분할 수 있는 k-anonymity기술을 적용시키고, RSU_i가 k개의 차량에게 똑같은 ID를 할당하여 ID-Key 테이블에 저장한다.

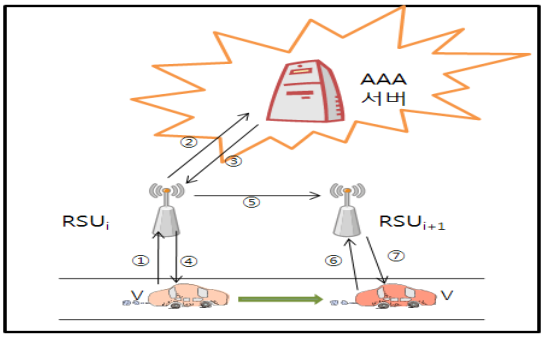
메시지 송신차량은 공유한 키로 메시지에 대한 메시지 인증코드(HMAC)값을 계산하여 RSU_i와 주변차량에게 전송한다. RSU_i는 받은 ID값이 ID-Key 테이블에 있는지 확인하고 공유한 키를 이용해 HMAC값이 유효한 값인지 확인한다. ID나 HMAC가 유효하지 않으면 해당 메시지는 폐기한다. 그 후 RSU_i는 임계 시간 안에 수신한 모든 메시지 값을 해쉬하여 Bloom Filter에 삽입하고 타임스탬프를 붙여 주변 차량들에게 전송한다.

먼저, 여기에 사용된 Bloom Filter는 어떤 원소가 어떤 집합에 속해있는지를 확인하는데 쓰이는 확률적인 자료구조로서, 많은 양의 데이터를 입력해도 자료구조의 크기가 늘어나지 않게 유지할 수 있으며 데이터의 포함여부를 빠르게 확인할 수 있다. 이 통합 과정은 주기적으로 이루어지기 때문에 이전 통신에서의 주변차량 정보가 누적되지 않게 된다. 타임스탬프를 붙이는 이유는 송신차량이 타임스탬프를 붙여 메시지를 전송하면 수신차량은 타임스탬프 값을 확인하여 주어진 임계치의 시간보다 크게 되면 메시지를 버려 재생공격을 방지할 수 있기 때문이다.

차량이 RSU_i에서 RUS_{i+1}로 이동하는 경우 RSU_i는 Bloom Filter 값과 함께 이동하는 차량과의 Key 정보를 주위 *RSU*의 공개키로 암호화 하여 보낸다. 주위 *RSU*는 자신의 Bloom Filter 값에 받은 Bloom Filter 값을 Bitwise-OR 연산하여 두 정보를 모두 포함하도록 한다. *RSU*는 이렇게 생성된 값을 임계 시간이 지나면 버리고, 자신의 통신반경에서 생성되는 Bloom Filter 값을 마찬가지 방법으로 주위의 *RSU*들에게 전송한다. 이때 사용되는 Bloom Filter 값은 주기적으로 생성되는 값이기 때문에 각 차량정보는 누적되지 않는다. 이러한 과정으로 차량이 다른 *RSU*의 통신반경으로 이동하는 경우에도 메시지 인증이 가능하다.

3.2 MAC-체인을 이용한 보호 기술

차량의 프라이버시를 보호하면서 추적성을 제공하기 위하여 차량 네트워크 환경에서 차량과 *RSU* 간 상호인증 프로토콜을 수행할 때 익명 아이디(Pseudonym)와 MAC-체인 (Massage Authentication Code chain)을 이용한 (그림 2)와 같은 상호 인증 프로토콜이 제안됐다[7].



(그림 2) MAC-체인 기술의 상호인증 과정

각 차량 V와 *RSU*에는 AAA의 공개키가 들어있는 인증서가 저장되어 있다. AAA는 대칭키를 생성하고 프로토콜을 시행하기 이전에 안전한 방법으로 V와 *RSU*에게 분배한다. KDC(Key Distribution Center)는 대칭키 K_i, K_{i+1}를 생성하고 RSU_i, RSU_{i+1}가 대칭키 K_i, K_{i+1}를 공유할 수 있도록 안전한 방법으로 분배한다. 차량이 시동을 거는 시점에서 V는 차량의 시작점에 위치한 RSU_i를 통해 AAA와 상호인증을 한다. ①~④단계는 RSU_i, AAA, V가 각각 상호인증을 수행하는 단계이다. 이후 V와 RSU_i는 V가 생성한 난수값으로, 세션 키 K를 생성하고 이 키를 이용하여 안전하게 암호화 통신한다. 이후 차량이 운행되기 시작하면 ⑤~⑥단계와 같이 상호인증과정을 수행한다. 프로토콜의 세부는 아래와 같다.

① V가 RSU_i에게 MAC-체인으로 생성되는 ID의 1번째 익명 아이디ps_1와 V가 생성한 난수값 r_0을 보내고 RSU_i는 그 메시지를 개인키로 복호화하여 ps_1, r_0에 저장한다.

② AAA와 V의 상호인증 단계: RSU_i가 정보를 AAA에게 전달하여 AAA는 메시지를 대칭키 K로 복호화하고,

이 메시지를 AAA의 개인키로 복호화하고 계산한 ps_1와 RSU_i로부터 받은 ps_1가 같은지 확인한다.

③ RSU_i와 AAA의 상호인증 단계: RSU_i에 저장된 ps_1와 AAA로부터 받은 ps_1가 같은지 확인한다.

④ RSU_i와 V의 상호인증 단계: RSU_i가 V에게 메시지를 전달하고 V는 그 메시지가 인증이 된 것을 확인하고 ps_1을 계산하고 r_1을 선택한다.

⑤ RSU_i는 RSU_{i+1}에게 메시지를 주고 RSU_{i+1}은 인증을 한 후에 ps_1에 저장한다.

⑥ RSU_{i+1}와 V의 상호인증 단계: V는 RSU_{i+1}에게 ps_1을 전달하고 RSU_{i+1}은 저장된 ps_1과 같음을 확인한다. RSU_{i+1}는 V에게 메시지를 주고 V는 받은 정보와 저장된 정보가 같은지 확인하고 ps_2를 계산하고 r_2를 선택한다.

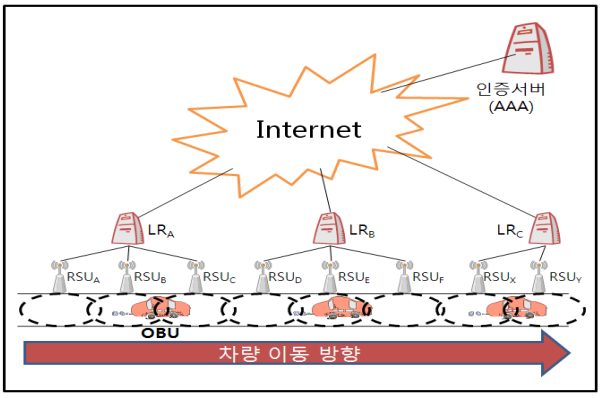
⑦ 이후 V가 목적지에 도착할 때까지 ⑤~⑥단계를 반복한다.

MAC-체인을 이용한 기술은 프로토콜에서 사용되는 MAC함수가 암호학적으로 안전하다고 가정하면, i일 때에 AAA를 제외한 누구도 ps_i에 대응하는 ID를 계산할 수 없으므로 익명성이 보장된다. 또한 수사기관에서 AAA에게 차량의 ID에 대한 추적을 의뢰하면 AAA는 ps_1를 계산하고 RSU_1를 검색한다. 그 후 RSU_1에서는 ps_1을 계산하고 RSU_1는 RSU_2의 위치와 RSU_2에서는 ps_2을 검색한다. 이후 사고발생 위치에 있는 RSU_n까지 계속적으로 ps_i를 검색한다. 그러므로 AAA와 모든 n개의 RSU_i가 협력할 때 Location Privacy를 보호하면서 추적성을 제공한다.

이러한 MAC-체인 기술사용은 네트워크에 추가적인 통신량이 발생하진 않지만 프로토콜 초기단계에서 AAA에 인증을 받아야 한다.

3.3 세션 키 교환을 이용한 보호 기술

OBU(On Board Unit)와 *RSU* 간의 세션 키 교환횟수를 줄이고, 안전한 차량 통신을 위해 (그림 3)과 같은 다수의 *RSU*를 관리하는 *LR*(Local Router)을 포함한 계층적 구조가 제안됐다[8].



(그림 3) 차량 간 세션 키 교환기술의 계층적 구조

OBU는 초기 부팅 시에 인증 구조 제공으로 보안을 강화한 무선 랜의 표준인 IEEE802.1x를 사용하여 *RSU* 와의 세션 키를 공유한다. 그 후 OBU는 *RSU*를 통해 자신이 속한 LR_A에 등록 및 세션 키 생성을 위해 암호화한 값인 TEK(Temporary Encryption Key)를 LR_A에게 전송한다. LR_A은 새로운 세션 키를 생성하여 OBU에게 전송함으로써 OBU와의 일대일 세션 키 생성이 이루어진다. OBU는 동일한 *LR*의 영역에 속한 *RSU*를 이동할 경우 사전에 생성된 OBU와 *RSU* 간의 세션 키를 사용하여 안전한 통신을 할 수 있다. 또한 LR_A와 LR_B 간의 통신으로 인해 LR_B은 OBU가 자신의 영역으로 온다는 것을 사전에 알 수 있다. 마찬가지로 OBU는 주기적으로 전송되는 *RSU*의 비콘 신호에 포함된 메시지를 통하여 LR_B의 영역으로 이동한 것임을 알 수 있다. 이러한 방법으로 OBU가 *LR*과 *RSU* 간, LR_A과 LR_B 간의 핸드오버 시, *LR*과 *RSU*는 이동한 OBU에 대해 사전에 등록된 OBU인지 확인할 수 있다. 따라서 악의적인 공격자가 정상적인 OBU의 정보를 사용하여 새로운 *RSU*를 통해 불법적으로 네트워크에 접속을 시도할 경우 *RSU*는 OBU에 대해 사전에 등록된 OBU 인지를 확인을 위한 액세스 인증을 수행하고, 인증된 OBU에 대해서만 네트워크 접근을 허가하여 악의적인 공격자의 접근을 차단할 수 있다.

그러나 공격자에게 기존의 *LR*에서 사용된 세션 키가 노출 될 경우 추가적으로 생성되는 세션 키의 유추가 가능한 문제점이 있고, 기존의 시설에 *LR*을 추가적으로 설치해야 한다는 단점이 있다.

4. Location Privacy 보호 기술 분석

본 논문에서 기술한 VANET에서의 Location Privacy 보호 기술은 <표 1>과 같다.

<표 1> Location Privacy 보호 기술 분석

	해쉬통합을 이용한 보호 기술	MAC-체인을 이용한 보호 기술	세션 키 교환을 이용한 보호 기술
장점	익명성	익명성, 추적성	익명성
단점	-	추가적인 통신량 요구	세션 키 노출 시 위험

차량 밀집환경에서의 해쉬통합을 이용한 보호 기술은 *RSU*가 반경 내의 모든 차량에 같은 ID를 할당함으로써 익명성을 만족한다. 그러나 밀집환경에서만 효율적이라는 한계가 있다. MAC-체인을 이용한 보호 기술은 초기 부팅 시에 익명의 아이디를 생성하고 차량에서 생성한 난수값

을 이용해 RSU를 지날 때마다 새로운 ps_i를 생성하여 익명성과 추적성을 보장한다. 하지만 초기단계에서의 AAA의 인증을 받아야 하는 추가적인 통신량이 요구된다는 단점이 있다. 세션 키 교환을 이용한 보호 기술은 RSU가 OBU에 대해 사전에 등록이 됐는지 확인하여 인증된 OBU에 대해서만 접근을 허가하여 공격자의 접근을 차단함으로써 익명성을 보장할 수 있다. 그러나 기존 LR을 통해 세션 키의 유추가 가능하기 때문에 공격의 위험성이 있다.

5. 결론

본 논문에서는 VANET에서의 Location Privacy 보호를 위한 보안요소들을 제시하고, 그 해결방안이 될 수 있는 기술들을 비교 분석하였다. 그 결과, 추가적인 통신량이 요구되나 익명성과 추적성을 모두 제공하는 MAC-체인 기술이 Location Privacy 보호를 위한 가장 적합한 기술인 것으로 나타났다. 그러나 이는 Location Privacy에 관련된 두 요소만을 고려한 결과이며, 이 두 요소를 포함한 VANET에서의 보안 요소 모두를 만족하는 기술개발에 대한 연구가 필요하다.

참고문헌

[1] Florian Dötzer, “Privacy Issues in Vehicular Ad Hoc Networks", in Proc. of the 2nd ACM International Workshop on Vehicular Ad Hoc Networks, Sep. 2005.

[2] M. Mauve, J. Widmer, H. Hartenstein, "A Survey on Position-Based Routing in Mobile Ad Hoc Networks", IEEE Network, 2001.

[3] K. Sha, Y. Xi, W. Shi, L. Schwiebert, T. Zhang, "Adaptive Privacy-Preserving Authentication in Vehicular Networks", in Proc. of the International Workshop on Vehicle Communication and Applications, Oct, 2006.

[4] "Event data recorder applications for highway and traffic safety", [Online]. Available : http://www-nrd.nhtsa.dot.gov/edr-site/

[5] "INter-Vehiclar Network Technologies (INVENT) home" [Online]. Available : http://web.njit.edu/borcea/invent/

[6] 정석재, 유영준, 백정하, 이동훈, “차량 밀집환경에서 안전하고 효율적인 V2V 메시지 인증기법”, 정보보호학회 논문지 제20권 제4호 pp. 41 ~ 52, Aug, 2010.

[7] 김성훈, 김범한, 이동훈, “VANET 환경에서 프라이버시를 보호하면서 사고 발생 시 추적 가능한 인증 프로토콜”, 정보보호학회논문지 제18권 제5호 pp. 115 ~ 124, Oct, 2008.

[8] 유승호, 정수환, “V2I 기반의 VANET 환경에서 안전한 차량 통신을 위한 세션 키 교환 기법”, 정보과학회논문지: 정보통신 제35권 제4호 pp. 311 ~ 317, Aug, 2008.