VANET 환경에서 Distance-Bounding 기반의 안전한 상호인증 프로토콜

김민진*, 김범용*, 이상현**, 전문석*
*숭실대학교 일반대학원 컴퓨터학과
**숭실대학교 정보과학대학원 정보보안학과
e-mail : minjini57@ssu.ac.kr
gflawer@ssu.ac.kr
drizzle0118@naver.com
mjun@ssu.ac.kr

Design of Authentication Protocol Based on Distance-Bounding in VANET

Minjin Kim*, Bumryong Kim*, Sanghyun Lee **, Moon-Soeg Jun *
*Dept. of Computer Science & Engineering, Soongsil University
** Graduate School of Information Sciences

요 약

VANET 은 차량간 통신 네트워크로 사고나 교통정보를 차량간 전달하거나 인프라를 통해 교통시스템 등의 서비스를 가능하게 한다. 사용자의 편의와 교통시스템의 효율을 위해 확산이 기대된다. 이에 다수의 차량 과 인프라 간, 차량과 차량간 통신에서 악의적인 해커의 공격에 대비할 수 있는 보다 안전한 인증 프로토콜이 필요하다. 본 논문에서는 VANET 환경에서 Distance-Bounding Protocol 과 Diffie-Hellman 을 이용한 상호 인증 및 키 교환 프로토콜을 제안한다. 제안하는 프로토콜은 보안성평가를 통해 안전성을 검증하였으며, 이를 통해 VANET 환경에서 불법적인 RSU 나 해커의 공격으로부터 안전한 통신을 가능하게 할 것으로 예상된다.

1. 서론

통신기술의 발달로 모든 사물간의 통신인 IoT(Internet of Things)시스템이 보급되었고, 이에 따라 차량간의 통신도 가능해졌다. 차량 네트워크로는 Vehicular ad hoc network 가 있다.

VANET(Vehicular ad hoc network)은 차량간, 차량과 인프라간의 통신을 지원한다. 차량은 이동성이 가장 큰 특징으로 도로를 지나며 다수의 인증을 받아야 할 필요가 있다. 그렇다면 필연적으로 악의적인 RSU(Road Side Unit)이나 해커의 중간자 공격에 위협이 있다.

악의적인 정보는 교통체계의 혼란이나 운전자 안전에 심각한 위협이 된다. 때문에 VANET 에서는 지속적으로 신뢰할 수 있는 방법과 차량이 지나면서 각 RSU 들을 만날 때 마다 인증을 받아야 하는 점이 중요하다.

본 논문에서는 차량이 안전하게 RSU 를 거쳐 SP(Service Provider)의 인증을 받고 또 도로를 지나면서 각 RSU 에게 인증 받을 수 있는 방법 제안한다. Distance-Bounding Protocol(이하 DBP) 을 기반인 고속의 통신으로 신뢰성을 보장하는 인증프로토콜을 설계한다.

해당 프로토콜로 안전인증과 함께 RSU 와 Car 간 Diffie-Hellman Key Exchange(이하 DH)를 사용함으로 인증 후의 신뢰 통신 또한 보장할 수 있다.

2. 관련연구

2.1 VANET

VANET 은 운전자의 안전, 편의와 교통시스템의 활용을 제공한다. 무선통신이 가능하도록 OBU(On Board Unit)을 탑재한 차량과 도로에 설치되어 인프라와의 유무선 링크를 제공하는 RSU, 서비스 제공자 SP 로 이뤄진다. VANET 은 차량끼리의 통신이나 차량의 무선을 이용해 ITS(Intelligent Transportation System)과 통신을 지원한다. 즉 두 가지 통신방법 V2I(Vehicle-to-Infrastructure) 와 V2V(Vehicle-to-Vehicle) 이 있다 [1].

차량들간의 통신을 위해 RSU 에게로부터 키를 할당받고 해당 키를 가지고 다른 차량이나 infrastructure 와 통신 한다. 통신에 앞서 진정한 차량, RSU 인지를 판별할 수 있는 인증이 필요하다. 인증은 SP 라는 백 본 네트워크와 차량, RSU 세 개의

※ 본 논문은 미래창조과학부의 2015 년 고용계약형 SW 석사과정 지원사업을 지원받아 수행한 결과임

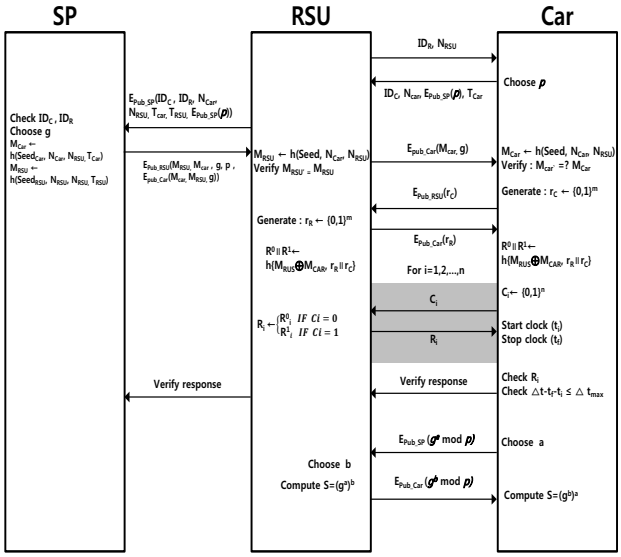
구성요소가 상호간에 이루어져야 한다. RSU 는 도로마다 일정한 간격으로 배치가 된다. 많은 수의 RSU 가 존재함에 따라 악의적은 RSU 를 설치할 경우에도 적절한 검증 없이 차량과 통신을 하게 되면 치명적인 보안 위협이 된다.

2.2 Distance-Bounding Protocol

무선환경의 중계공격에 저항 하기 위해, 1993 년 Brand 와 Chaum 에 의해서 제안되었다 [2]. 다양한 DBP 변형 프로토콜이 제안되었지만 기본 모델은 저속→고속→저속으로 사전 난수 값들을 공유하고 고속으로 0, 1 bit 를 전송한다. 이 비트 스트림을 통해서 상호 인증과 시간을 측정한다. 시도 값에 따른 응답은 한 비트씩 고속으로 전달되고 이 응답은 Upper-Bound 이내에 이루어져야 한다. 마지막 저속통신에서 검증 자는 해당 과정이 적정 시간 안에 이루어졌는지 판단하고 시간차 확인을 통해 대략적으로 가까운 거리에 있음을 확인할 수 있다 [3][4].

3. 제안

제안하는 프로토콜의 기본 가정은 다음과 같다. 첫째, SP 와 Car, SP 와 RSU 는 고유 Seed 값을 공유하고 있다. 둘째, SP, RSU, Car 의 공개키는 공개되어 모두 알고 있다.



(그림 1) 제안하는 인증 프로토콜

제안하는 인증 프로토콜은 (그림 1)과 같이 진행된다.

RSU 는 지속적으로 본인의 반경에 신호를 보내고 있다가 반경에 들어온 차량에게 아이디와 난수 값을 전송한다. 통신을 원하는 Car 는 자신의 아이디, 난수 값, 타임스탬프 값, DH 을 위한 소수 P 값을 전달한다.

Car 로부터 정보를 받은 RS 는 난수를 생성하여 SP 에게로 자신의 정보와 Car 의 정보를 함께 전달한다. 데이터를 수신한 SP 는 아이디를 확인하고 DH 을 위한 소수 g 값을 선택한 후, Seed 값, 두 난수 값, 타임스탬프를 이용해 각각 해쉬 값을 생성하여 RSU 와 Car 에게 전송한다.

RSU 는 $\mathbf{M_{RSU}}$ 검증을 위해 $\mathbf{M_{RSU}}'$ 를 생성하여 검증하며, Car 에게 암호화된 $\mathbf{M_{Car}}$ 을 전송한다. Car 는 $\mathbf{M_{Car}}'$ 을 생성하여 $\mathbf{M_{Car}}$ 를 검증한다. 검증이 완료되면 DBP 를 위한 난수 $\mathbf{r_R}$, $\mathbf{r_C}$에 0,1 bit 를 랜덤적으로 선택해서 저장하고, 이 난수를 RSU 와 Car 는 서로 교환한다.

이후 RSU 와 Car 는 서로 h{$\mathbf{M_{RSU}} \oplus \mathbf{M_{Car}}$, $\mathbf{r_R} \parallel \mathbf{r_C}$} 연산으로 동일한 $\boldsymbol{R^0}$, $\boldsymbol{R^1}$ 를 공유하게 되며, 이 값을 이용하여 다음과 같이 DBP 과정을 진행한다. 먼저 Car 에서 0,1 bit 의 랜덤 값 $\mathbf{C_i}$ 을 요청하면 해당하는 RSU 가 $\mathbf{R_i}$ 값으로 응답한다. Car 는 응답 bit, 시간차를 확인하고 RSU 와 SP 에게 확인응답을 보낸다.

인증과정이 완료되면 Car 는 키 교환을 위해 Car 의 비밀 값 a 를 선택하고 $\boldsymbol{g^a \bmod p}$값을 RSU 에게 전송한다. RSU 도 동일한 과정으로 비밀 값 b 를 선택하여 $\boldsymbol{g^b \bmod p}$ 을 Car 에게 전송하면 RSU 와 Car 간의 비밀 키를 공유하게 된다.

4. 보안 평가

본 논문에서 제안한 프로토콜은 다음과 같은 특성을 가진다.

첫째, Relay 공격에 저항성을 지닌다. DBP 를 통해 유효시간 내 비트를 주고 받음으로 두 노드가 물리적으로 가까이에 있음을 확인할 수 있다. 또한 유효시간 검증을 하므로 Relay 공격에 안전하다. 둘째, Replay 공격에 저항성을 지닌다. RSU 와 Car 에서 만든 타임스탬프 값을 상호인증 과 DBP 과정에서 사용하기 때문에 재전송 공격으로부터 안전하다. 셋째, Forward security & Error Detection 이 가능하다. DBP 과정중 생성된 비트 배열R_i^0, R_i^1 랜덤 값 C 에 대한 응답 값으로 약속된 R_i^0, R_i^1 주고 받는 과정에서 비트에 대한 응답비트 중 1 bit 의 위치만 잘못되어도 Error Detection 이 가능하며, 이를 통해 Forward Security 와 상호인증이 가능하다.

5. 결론

VANET 에서 악의적인 RSU 로 발생할 수 있는 보안 취약점이 있다. 이에 따라 상호인증을 제공하는 프로토콜을 제안했다. 제안한 프로토콜은 Relay Attack, Replay Attack, Forward security & Error Detection 에 안전성을 보안분석을 통해 확인하였다. 향 후 VANET 에서 보다 안전한 인증을 제공하는 프로토콜로 사용될 것으로 기대된다.

참고문헌

[1] Paul, Bijan, et al. "Vanet routing protocols: Pros and cons." arXiv preprint arXiv:1204.1201, 2012.

[2] Sou, Sok-Ian, and Ozan K. Tonguz. "Enhancing VANET connectivity through roadside units on highways." Vehicular Technology, IEEE Transactions on 60.8, pp.3586-3602, 2011.

[3] Cremers, Cas, et al. "Distance hijacking attacks on distance bounding protocols" Security and Privacy (SP), 2012 IEEE Symposium on. IEEE, 2012.
[4] Avoine Gildas, Chong Hee Kim, “Mutual Distance Bounding Protocols”, Mobile Computing, IEEE Transactions on Vol.12 , 2013.