Petri Net을 이용한 차량 인증 보안 메커니즘 모델링

송유진*, 이종근*1)
*창원대학교 컴퓨터공학과
e-mail:syj@changwon.ac.kr, jklee@cwnu.ac.kr

A Vehicular Authentication Security Mechanism Modeling using Petri Net

Yu-Jin Song*, Jong-Kun Lee*
*Dept of Computer Engineering, Changwon National University

요 약

차량 애드혹 네트워크(VANET : Vehicular Ad-Hoc Network) 환경에서 차량들은 네트워크 인프라를 바탕으로 한 통신들을 통하여 서로의 안전이나 편리성을 도모하고자 많은 관심을 가지고 지금까지 연구되어 왔으며 앞으로도 활발히 연구될 것이다. 그러나 안전성이나 편리성을 도모하고자 연구되어왔던 여러 부분들이 보안문제에 직면하면서 새로운 국면으로 접어들고 있다. 이에 본 논문에서는 차량 애드혹 네트워크에서 차량 간 통신을 효율적이고 안전하게 전송하기 위해 우선되어야 하는 차량의 인증을 위한 보안 메커니즘을 제안하고 이를 패트리넷 모델링 기법을 통해 검증하고자 한다. 본 논문에서 제안하는 차량 인증 보안 메커니즘(VASM : Vehicular Authentication Security Mechanism)은 차량 인증 기능과 함께 패트리넷으로 모델링 함으로써 차량들의 많은 변화로 복잡할 수밖에 없는 VANET에서의 보안요구들을 정의하여 수행하는데 유연하게 대처할 수 있다.

1. 서론

차량 애드혹 네트워크(VANET : Vehicular Ad-Hoc Network)는 차량 간 통신을 통하여 운전자의 안전을 향상시키는 응용으로 많은 관심을 받고 있다. 차량 애드혹 네트워크 환경에서 차량들은 다양한 서비스를 네트워크 인프라를 통해 제공 받을 수 있으며 정보들을 빈번한 통신으로 상호 교환한다. 따라서 운전자의 안전을 위해 송수신되는 정보들을 안전하게 전송하고자 차량의 인증과 함께 차량 간의 익명성을 보장하고, 메시지에 대한 인증을 통해 무결성, 가용성, 부인봉쇄와 같은 보안 메커니즘을 얼마나 효율적이고 안전하게 구성하느냐는 문제가 최근 활발히 연구되고 있다.

이에 본 논문에서는 차량 애드혹 네트워크에서 차량 간 통신을 효율적이고 안전하게 전송하기 위해 우선되어야 하는 차량의 인증을 위한 보안 메커니즘을 제안하고 이를 패트리넷 모델링 기법을 통해 검증하고자 한다.

본 논문의 구성은 다음과 같은 순서로 구성된다. 1장의 서론에 이어 2장에서 차량 간 통신에 대하여 정리하고 3장에서는 본 연구에서 제안하는 차량 인증 보안 메커니즘(VASM : Vehicular Authentication Security Mechanism)을 설명하고 이를 패트리넷으로 모델링하여 이를 통해 보안 목적에 따라 수시로 변하는 메커니즘을 얼마나 유연하게 적용할 수 있는지를 제시하고자 한다. 그리고 4장에서 본 연구의 결론과 함께 향후 연구 과제에 대해 설명한다.

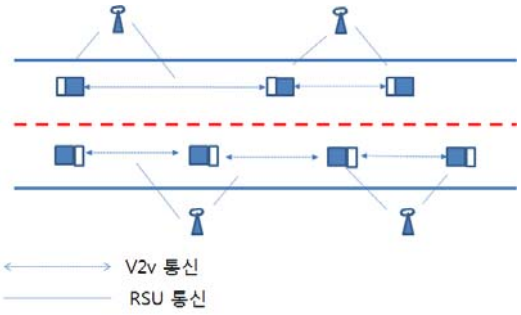
2. 차량간 통신

VANET는 도로의 안전 촉진, 교통량 관리와 운전자와 보행자를 위한 정보시스템의 보급을 위하여 규약 된 네트워크이다. 통신관련 장비로서는 자동차간 통신과 주요 지역에 설치 된 도로 통신장치(RSUs: Roadside units)와의 통신도 포함한다. 특히 VANET에는 차량용 하이패스 단말기(OBUs : Onboard units)에 의하여 차량 위치, 현재시간, 방향, 스피드, 교통량 특이사항, 가속과 감속 등의 자료들이 유통된다. 이러한 데이터에 따라 교통의 흐름 조절이나 사고예방을 위한 조치나 복잡한 교통량 해소와 대체도로의 공고 등을 통하여 도로 교통량을 원할하게 제어하는 역할을 VANET는 담당하고 있다[3,4,5,6]. 본 연구에서는 차량과 차량 간의 통신에서 각 차량에 대한 인증 문제에 초점을 맞추고 있다. 즉 차량과 차량 간에 발생되어지는 통신에서 차량에 대한 인증을 확실히 함으로 사고 예방은 물론 사고후 발생 되어질수 있는 책임 문제 등에 대한 기초 자료로 활용 될 수 있기 때문이다.

특히 차량간 통신에서 서로 다른 ID를 가져야하며 송수신 매체는 위변조가 불가능 하여야하며 개체간 통신 메시지

1) 교신저자:이종근
메일:jklee@cwnu.ac.kr

는 비인가 된 매체에 대하여 기밀성 보장되어야 한다. 따라서 본 연구에서는 차량간 통신에서의 인증을 위한 보안 메카니즘을 제안하고 그 효율성을 검증한다.



(그림 1) 네트워크 모델

3. 차량 인증을 위한 보안 메커니즘

차량 애드혹 네트워크에서의 통신은 해당 모듈의 통신 상태에 따라 크게 두 가지로 구분된다. 각 차량에 탑재된 OBU(On-Board Unit)들을 통한 차량 간의 통신을 V2V(Vehicle-to-Vehicle) 통신이라 하며, OBU와 도로에 위치한 RSU(Road-Side Unit)를 통한 인프라와의 통신을 V2I(Vehicle-to-Infrastructure) 통신이라고 한다[3]. 두 통신기법은 인프라의 통신 참여 유무에 따라 통신 방법에서도 차이점이 존재하는데 본 연구에서는 일정 그룹에 입력되는 차량의 인증과 함께 그룹 안에 일정시간 존재하는 인증 받은 차량을 이용한 불법적인 공격을 막기 위해 시간 주기별 인증 메커니즘을 제시하고자 하므로 RSU를 통한 V2I 통신을 기반으로 한다.

본 연구에서 제안하는 차량 인증 보안 메커니즘(VASM : Vehicular Authentication Security Mechanism)은 V2I 통신에서 RSU가 자신의 그룹 내에 들어오는 OBU의 인증과정과 인증 받은 OBU의 주기적인 인증 과정을 함께 포함하고 있다. OBU의 주기적인 인증과정이 필요한 이유는 처음 인증 받은 OBU의 상태가 악의적인 해킹으로 인해 불법적인 공격에 노출 될 수도 있으므로, 일정한 시간 주기별로 계속적인 인증과정을 통해 이러한 보안위협에 대비하고자 한 것이다.

다음은 RSU를 통해 OBU의 인증 및 주기적 인증과정에 대해 설명한다.

여기서 RSU는 인증과정을 위해 공개키 알고리즘을 사용하며 OBU는 비밀키 알고리즘을 사용하고 있다:

① 효율적인 OBU들의 인증관리를 위해 RSU는 관리할 수 있는 OBU의 개수를 일정수준으로 정한다.

② OBU가 RSU의 그룹 안으로 들어가면서 OBU는 RSU에게 자신의 UnitNumber를 전달하고, RSU는 OBU에게 받은 UnitNumber를 리스트에서 확인하고 정상적인 UnitNumber일 경우 그 순간의 시간 정보인 TimeStamp가 있는 수 t와 일정시간간격을 나타내는 난수 r을 발생시켜 OBU의 UnitNumber와 함께 RSU의 비밀키로 암호화하여 OBU에게 전달한다.

③ OBU는 정상적인 UnitNumber를 가진 OBU들에게만 공개되는 RSU의 공개키를 이용해 UnitNumber와 t, r을 복호화한 후 그 값들과 자신의 비밀키를 RSU의 공개키로 암호화한 후 RSU에게 보낸다. 이 때 복호화 한 UnitNumber의 값이 자신의 값과 틀리면 RSU를 신뢰할 수 없음을 알 수 있다.

④ RSU는 OBU에게 받은 정보를 자신의 비밀키로 풀어 처음 등록 시 받은 UnitNumber와 t, r이 맞으면 OBU의 비밀키를 저장하여 다음의 주기적 인증과정에서 사용한다.

⑤ 일정시간 후 OBU는 다시 자신의 UnitNumber와 처음 시작 TimeStamp가 있는 수 t와 각 RSU 그룹에서 임의로 미리 정해진 간격시간 i 만큼의 일정 시간 간격 후의 수 r+i를 자신의 비밀키로 암호화하여 OBU의 UnitNumber와 함께 RSU에게 보낸다.

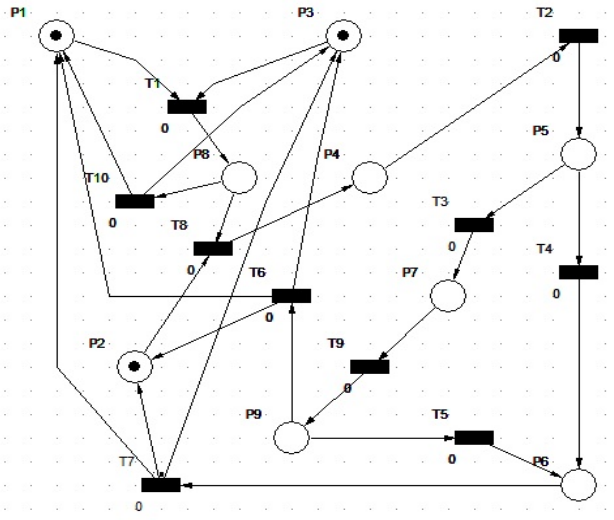
⑥ RSU는 OBU의 UnitNumber를 확인하고 해당 OBU의 비밀키를 이용해 t와 r+i, 그리고 UnitNumber를 복호화하여 OBU의 처음 시작시간인 t와 미리 정해진 일정시간 간격을 적용한 r+i의 값이 맞으면 OBU가 외부 공격에 노출되지 않고 그룹 내에서 운행되고 있음을 알 수 있다.

⑦ OBU가 그룹을 빠져 나갈 때까지 위의 ⑤ ⑥ 과정이 반복된다.

⑧ 마지막으로 ② ④ ⑥의 단계에서 값이 틀리면 해당 OBU가 보안위협에 노출된 것이므로 RSU 그룹에서 제거한다.

제안된 VASM을 패트리넷을 이용해 모델링 하면 다음(그림 1)과 같다.

(그림 1)에서 P1에 마킹된 토큰의 수는 RSU가 관리할 수 있는 차량들의 수를 정의하는 것이다. 즉 해당 RSU가 자신의 그룹에 얼마나 많은 차량들을 인증 관리할 수 있는가를 토큰의 개수로 정의하여 모델링 할 수 있으며 P3에 마킹된 토큰은 OBU 하나의 인증을 위한 것으로서 이 토큰의 유무를 통해 OBU의 존재와 OBU의 제거를 알 수 있다.



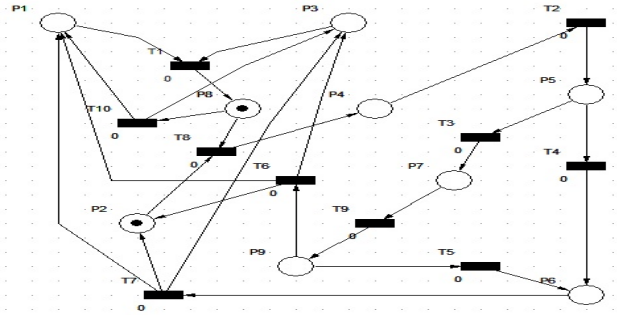
(그림 2) VASM의 초기 패트리넷 모델

다음에 기술되어 있는 <표 1>은 (그림 2)에 있는 place와 transition의 각각의 역할에 대해 기술한 것이다.

<표 1> VASM 패트리넷 모델의 Place와 Transition의 내용

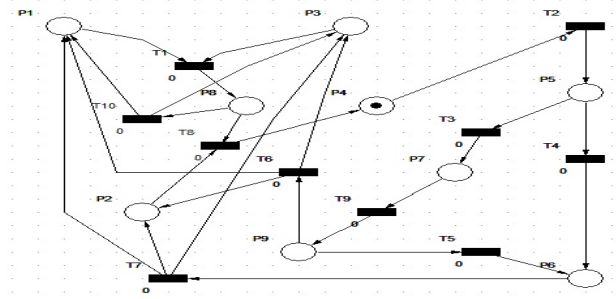
Place	내용
P1	RSU(관리가능한 OBU의 개수 설정)
P2	RSU(t와 r값 생성)
P3	OBU(UnitNumber)
P4	OBU(UnitNumber, t, r) OBU 비밀키
P5	RSU(OBU의 비밀키 저장)
P6	RSU(OBU제거)
P7	OBU(t, 일정시간 후의 시간간격값 r+i)
P8	RSU(OBU의 UnitNumber가 정상인지 확인)
P9	RSU(OBU의 비밀키로 t, r+i, UnitNumber확인)
Transition	내용
T1	OBU의 UnitNumber를 RSU에 보낸다
T2	RSU의 공개키로 UnitNumber, t, r, OBU 비밀키를 암호화한다.
T3	OBU 인증
T4	OBU 제거
T5	OBU 제거
T6	OBU 인증
T7	OBU 제거
T8	RSU의 비밀키로 UnitNumber, t, r을 암호화하여 OBU로 보낸다
T9	OBU의 UnitNumber와 t, r+i를 OBU비밀키로 암호화하여 OBU UnitNumber와 함께 RSU로 보낸다
T10	OBU 제거

제안된 VASM을 패트리넷으로 모델링하여 이를 패트리넷 시뮬레이션 도구로 시뮬레이션 한 결과를 다음 그림에서 단계별로 나타내었다.



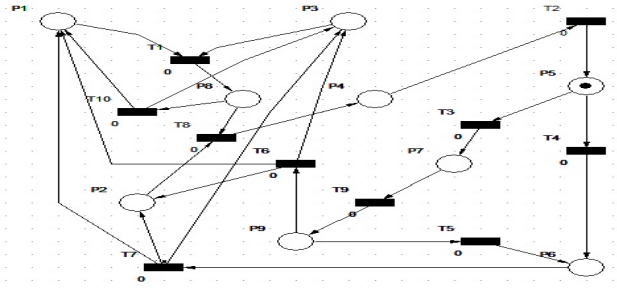
(그림 3) 트랜지션 t1 점화 후

[P8은 OBU의 UnitNumber가 정상값이면 t8 점화, 비정상값이면 t10 이 점화된다.]



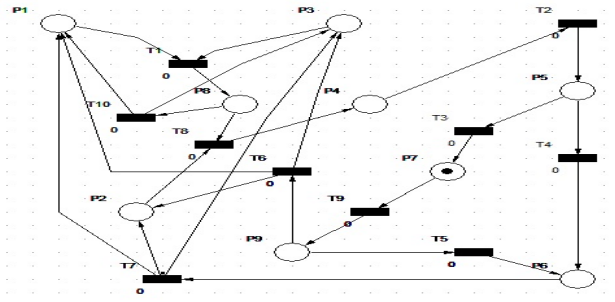
(그림 4) 트랜지션 t8 점화 후

[P4는 OBU가 RSU의 공개키로 UnitNumber,t,r을 암호화한 값과 OBU의 비밀키를 전송한다.]



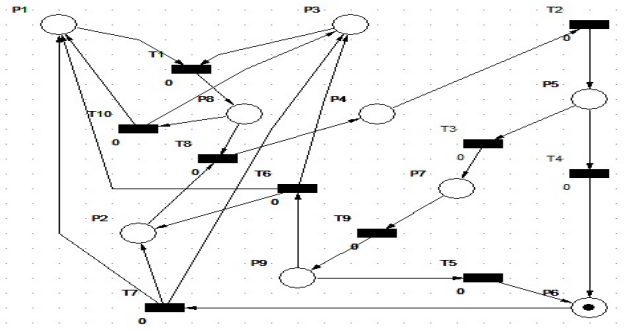
(그림 5) 트랜지션 t2 점화 후

[P5는 RSU가 자신의 개인키로 복호화하여 정상값이면 OBU의 비밀키를 저장하고 t3을 점화, 아니면 t4를 점화한다.]



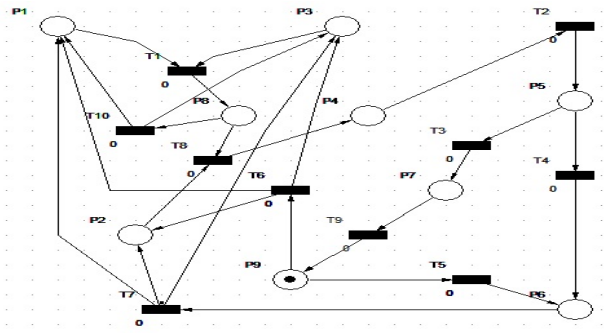
(그림 6) 트랜지션 t3 점화 후

[P7은 일정시간후 OBU가 UnitNmber, t, r+i 값을 OBU의 비밀키로 암호화하여 RSU에 보낸다.]



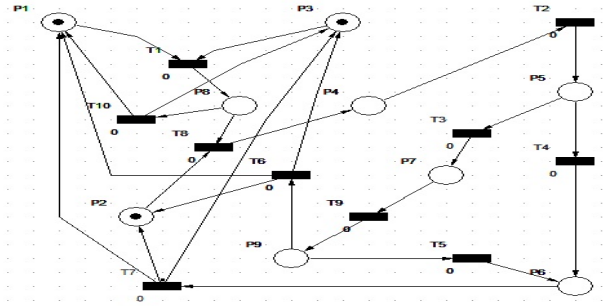
(그림 7) 트랜지션 t4 or t5 점화 후

[P6은 P5, P7에서 보내는 값이 비정상적인 값이므로 OBU를 제거한다.]



(그림 8) 트랜지션 t9 점화 후

[P9는 RSU가 OBU의 비밀키로 UnitNumber,t,r+i를 복호화하여 확인하고 정상값이면 t6 점화 비정상값이면 t5 점화한다.]



(그림 9) 트랜지션, t6, t7, t10 점화 후

[정상값 인증 후 t6 점화하며 다시 인증 작업을 하기 위해 초기 모델로 돌아간다. 비정상값일 경우 t7, t10 점화하며 OBU제거하고 다시 인증작업을 하기 위해 초기 모델로 돌아간다.]

위의 시뮬레이션 결과에서 나타난 것과 같이 최초 차량 OBU가 RSU 그룹 내 진입 시 OBU 인증 과정과 주기적인 OBU 인증과정이 원활하게 수행됨을 알 수 있었다. 또한 인증과정에 문제가 되는 여러 상황 즉, OBU 제거를 수행하는 t4, t5, t7, t10의 점화 상태의 빈도를 통해 차량 애드혹 네트워크 내에서의 차량 인증에 대한 보안 강도를 알 수 있다.

4. 결론

본 논문에서 제안한 V2I 통신에서의 차량 인증 보안 메커니즘 VASM은 RSU와 OBU 사이에서 서로의 인증을 위해 암호화 알고리즘과 시간 난수들을 사용하는데 OBU 입장에서의 RSU의 인증이 필요하고, 또한 RSU에서 그룹 내에 진입하는 OBU의 인증이 필요하므로 이를 위한 알고리즘을 위해 공개키 알고리즘과 비밀키 알고리즘을 적절히 혼용하여 사용함으로써 서로간의 인증이 모두 가능하도록 하였다. 즉, RSU에서는 공개키 알고리즘을 사용하여 OBU에게 자신이 정당한 RSU임을 인증 받고, OBU 에서는 비밀키 알고리즘을 사용하여 RSU에게 자신의 정당함을 인증 받도록 하였다.

그리고 패트리넷의 모델링 특성상 RSU 그룹의 제한 차량 숫자들을 토큰의 개수로 마킹함으로써 적절히 시뮬레이션 할 수 있으며, 트랜지션 점화의 빈도를 통해 보안 강도를 측정할 수 있다는 장점이 있다. 이와 같이 패트리넷으로 모델링 함으로써 차량들의 많은 변화로 복잡할 수 밖에 없는 VANET에서의 보안요구들을 정의하여 수행하는데 유연하게 대처할 수 있다.

향후 연구에서는 제안한 메커니즘을 여러 대의 OBU들로 확장하여 모델링한 후 시뮬레이션 해보고, 또한 인증 메커니즘 외에 메시지 무결성이나 부인봉쇄와 같은 보안 요구들에 대한 메커니즘을 정의하여 패트리넷을 이용해 모델링함으로써 각각의 환경에 맞는 보안 메커니즘을 제안하는 것이 필요하다.

참고문헌

[1] J.L.Peterson, “Petri Net Theory and Modeling of Systems” Englewood Cliffs, NJ: Prentice Hall, 1981.

[2] T. Murata, “Petri Nets: Properties, analysis and applications” Proc. IEEE, vol. 77, pp. 541-580, 1989.

[3] C. Zhang, X. Lin, R. Lu, P.H. Ho and X. Shen, ″An Efficient Message Authentication Scheme for Vehicular Communications″ IEEE Trans, on Vehicular Technology, vol. 57, no. 6, pp. 3357-3368, Nov, 2008.

[4] N-W Wang etc.el., “A novel secure communication schemd in vehicular ad hoc networks”, Computer communication, vol.31, pp.2827-2837,2008

[5] X.Sun, X.Lin,P-H. Ho, “Secure Vehicular Communications Based on Group Signature and ID-based Signature Scheme”, Proc. ICC 2007, 2007, pp.1539-1545

[6] C-T Li,M-S Hwang,Y-P Chu, “A secure and efficient communication scheme with authenticated key establishment and privacy preserving for vehicular ad hoc networks”, Computer communication, vol.31, pp.2803-2814,2008