M2M에서 지능형 자동차기반의 종단간 인증 프로토콜

이근호*

요약

미래의 기계와 장비 도구들은 IT기술을 이용하여 스마트 장치 기반으로 지식 발전의 형태로 발전되어 질것이다. 스마트한 기계 도구들은 다른 기계들과 함께 새로운 결정을 만들고, 지식을 이해하고 지식을 생산하기 위해 자동으로 지식을 축적할 것으로 기대된다. 본 논문에서는 M2M(Machine to Machine)에서의 지능형 자동차 기반의 종단간 인증 프로토콜을 제공하여 안전한 인증기법을 제안하였다. M2M에서의 지능형 자동차 클러스터 구조에 대한 보안 위협을 살펴보았다.

End-to-End Authentication Protocol based on Intelligent Vehicle in M2M

Keun-Ho Lee*

ABSTRACT

In the future, machine and device tools will be more improved in the form of a knowledge evolution based smart device using IT(Information Technology). The intelligent machine tools is expected to gather knowledge autonomously by producing knowledge, understanding knowledge and making a new decision with other machine. In this paper, we propose a secure authentication scheme that provides end-to-end authentication protocol based on intelligent vehicle in M2M. We present detailed security threats against intelligent vehicle cluster architecture in M2M.

Key Words :M2M(Machine to Machine), Authentication, Intelligent Vehicle, Threshold

* 백석대학교 정보통신학부(✉root1004@bu.ac.kr)
· 제1저자(First Author) : 이근호 · 교신저자(Correspondent Author) : 이근호
· 접수일(2011년 7월 20일), 수정일(1차 : 2011년 8월 17일), 게재확정일(2011년 8월 22일)

Ⅰ. 서 론

IT분야의 급격한 발전은 개인용 PC에서 스마트폰으로의 변화와 스마트폰을 기반으로 다양한 주변 기기들과의 융합을 통한 새로운 서비스 환경을 만들어가면서 급속도로 사회의 변화를 주도하고 있다. 언제 어디서나 쉽게 정보를 얻거나 주변의 장치와 기계간의 통신을 위한 M2M (Machine to Machine)은 이동통신 사업자와 연구자들간의 주요기술 연구분야로서 다양한 서비스 환경을 만들어가면서 새로운 기술을 적용하고 있다.

M2M 통신은 기기의 장비들간의 다양한 통신 환경을 이용하여 다양한 정보 전송이 이뤄지도록 연구가 되고 있으며, 그 분야중 다양한 기기들이 자동차와 연결하여 다양한 정보 전송이 가능하도록 하는 지능형 자동차의 연구가 IT와의 연계를 통하여 융합 연구가 이뤄지고 있다.

최근 융합기술이 생활에 다양한 영향을 미치고 있으며, 융합기술을 주도하는 국가가 세계를 주도할 정도로 중요한 기술이다. 융합의 중심에는 정보통신 기술이 있으며, IT기반의 융합이 필요하다. IT기반의 융합발전에는 수많은 문제점이 존재하고 있으며, 그중에서도 가장 중요한 요소가 각 기계간의 통신이 안전성을 보장하는 보안이다.

본 논문에서는 M2M에서의 보안요소와 지능형 자동차에 대한 보안 위협요소를 살펴보고, 임계치 인증기법을 통한 종단간 인증프로토콜을 제안한다.

Ⅱ. 관련연구

2.1 M2M 보안요소

M2M(사물통신) 서비스는 Machine to Machine, Machine to Man, Man to Machine의 개념으로 정의를 내릴 수 있으며, 주변의 사물이나 기기에 정보를 수집하고 통신을 가능하게 하는 장치를 설치하여 사람과 주변 기기에게 다양한 정보를 제공하는 정보 서비스의 개념이다. M2M의 활용 분야로는 Sensor Network, Tracking, Car Telemetics, Emerging Device에서 이용되어지고 있다[2]. M2M에서의 기술은 식별기술, 정보수집기술, 통신기술, 지능화 기술, 소형화 기술이 필수 기술요소로서 사물간 정보 교환과 제어를 통해 모든 기기와 시스템을 자율적으로 안전하게 관리 해야 한다[1].

M2M에서의 Device의 위협에는 기기간의 도청, 가로채기, 부인과 관련된 프라이버시 및 변조 위협요소가 있으며, Gateway에서는 불법 도용 및 접근을 통한 권한 위배, 물리적 침입, 재사용 공격, 중간자 공격의 위협요소가 존재한다. M2M 네트워크에서는 불법침투, 서비스 거부를 통한 마비, 바이러스, 웜, 트로이목마, 자원고갈 등의 보안 위협 요소가 있다[1].

2.2 지능형 자동차 보안요소

지능형 자동차는 융합분야 기술의 발전으로 인하여 홈네트워크, 텔레매틱스, 지능형 로봇 등이 접목되어 생활의 편리성을 제공하기 위한 다양한 형태의 서비스로 진화되고 있다. 지능형 자동차의 서비스 모델은 Car to Enterprise(C2E), Car to Car(C2C), Car to Home(C2H) 간의 다양한 모델을 제시하고 있다. 그림 1과 같이 지능형 자동차 통신 환경은 차량간 통신과 차량과 RSU(Road Side Unit)과 같은 인프라 장비와의 통신 상태로 구분할 수 있다.

지능형 자동차 서비스에서의 주요 역기능으로 개인정보 및 프라이버시 침해, 차량정보, 차량간 통신 메시지, 통신트래픽 정보 등의 위변조 등의 위협 요소로부터 안전한 메시지 전송이 필요하다. 안전한 차량 서비스 및 통신을 위한 지능형 자동차의 보안 프레임워크에는 Secure Positioning, Vehicle-to-Infrastructure

Secure Communication, Vehicle-to-Vehicle Secure Communication, User Access Control, VPKI(Vechicle PKI) 등을 포함하고 있다.

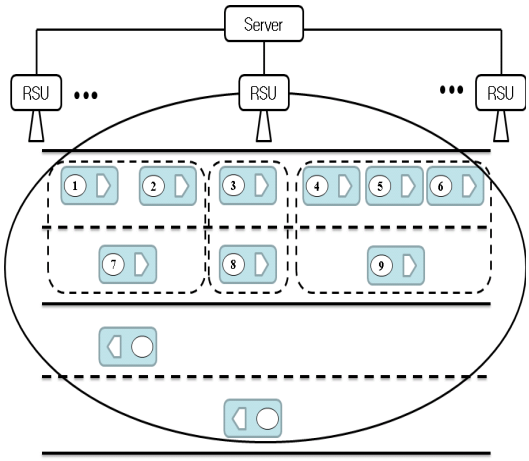

그림 1. 지능형 자동차 환경
Fig 1. Environment in Intelligent Vehicle

지능형 자동차에서의 보안 위협 요소로는 네트워크 측면에서 많은 위협이 발생할 수 있다. 거짓 정보를 발생시키는 공격 차량에 의해 일정 네트워크 영역안에 있는 다른 차량들에게 거짓 정보를 보내는 Forgery 위협과 일정 네트워크 영역안에서 다른 차량의 통신에 장애를 가하는 신호를 발생시키는 Jamming공격이 존재한다. 주행중에 메시지 또는 정보의 전달 과정에서 drop, corrupt, 또는 modify를 통한 정보의 위변조 공격하는 In-transit Traffic Tampering과 차량의 상태 정보를 변경하여 다른 차량으로 하여금 오인하도록 하는 공격하는 Impersonation 공격이 있다. 시간, 위치, 차량 ID, 이동 정보 등의 차량과 관련된 개인 프라이버시 정보에 대한 침해하는 Privacy Violation과 차량 내부의 정보인 속도, 위치, 차량 전장 부분의 상태, 각종 센싱 정보 등에 대한 위변조의 공격이 가능한 On-board Tampering이 위협요소이다[2,4].

III. Threshold 기반의 종단간 인증 프로토콜

3.1 가정

제안하는 프로토콜의 환경은 다음의 가정을 따른다. 모든 차들이 같은 환경에서의 이동을 기반으로 한다. 각 차들은 그림 2의 노드로 표시하여 가중치를 기준으로 표시한다. 첫째, 이동 자동차들은 RSU를 통하여 서버로부터의 인증을 받는다. 실제 네트워크의 물리계층에서는 DoS(Denial-of-Service)의 공격이 가능하다. 물리계층에서의 DoS공격에 대해서는 고려하지 않는다. 둘째, 클러스터를 구성했을 경우 각각의 자동차는 RSU나 주변 노드들로부터 자신의 클러스터 정보를 알고 있어야 한다. RSU는 인증서버와 CH(Cluster Head)간의 통신시 안전한 연결을 수행한다. CH(Cluster Head)가 클러스터내의 노드들의 ID를 관리하고, 각 CH는 항상 신뢰할수 있어야 한다. CH는 클러스터내의 서버의 역할을 한다고 가정한다. 각 노드들은 CH 선출 기준에 따라 그림 2와 같이 각 노드별로 가중치를 임의적으로 구성하였다.

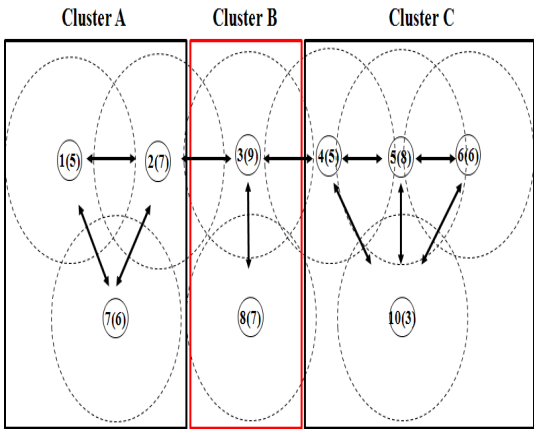

그림 2. 클러스터 구성
Fig 2. Cluster Configuration

가중치의 기준은 자동차에 속성(차량의 속도, 거리, 차량의 연산기능 등) 들을 기반으로 구성한다고 가정한다. CH는 노드들의 인증서의 기한이 초과되면 바로 폐기처리하며 새로운 인증서를 받도록 한다. CH를 통한 인증서는 인증서버로부터 각 노드의 키를 이용하여 재발급한다.

각 클러스터의 구성은 그림 1의 내용을 기초로하여 Cluster A, B, C로 구성한다. Cluster 구성시 이웃 노드들과의 관계와 가중치를 기반으로 Cluster를 구성한다. Cluster A에서의 CH는 노드 2가 가중치가 7로 제일 높으므로 클러스터 헤드의 역할을 수행한다. Cluster B는 노드 3, Cluster C는 노드 5가 CH의 역할을 수행한다고 가정한다. 각 클러스터간의 연결을 위해서는 클러스터내에 인접한 노드가 게이트웨이의 역할을 수행한다.

3.2 사용 기호 표시

본 논문에서 사용되는 표기법은 아래와 같은 표기법을 사용한다.

표1. 기호
Table1. Symbol

- CH_A : Cluster Head A
- ID_X : Identification X
- $K_{S,CH}$: 세션키 S와 CH or S와 CH 비밀키 공유
- Time : 현재시간
- S : CH_A 멤버노드
- X : CH_B 멤버노드
- K_{A+} : 노드 A의 공개키
- K_{A-} : 노드 A의 개인키
- $cert_A$: 노드 A의 인증서
- e : 인증서 유효기간
- $Nonce_A$: 노드 A 난수 생성

3.3 Threshold를 이용한 서명

그림 3은 그림 2의 클러스터 구성을 기반으로 세개의 클러스터 서비스는 K/k 공개키/개인키 쌍으로 구성되어져 있다. 임계치 키 구성 기법을 이용하면 각 CH_i는 개인키 k에 의해서 s_i를 공유한다. 메시지 m은 CH_i는 공유하는 s_i를 이용하여 $PS(m,s_i)$ 을 통하여 부분 서명을 한다. 올바른 CH_A와 CH_B는 부분 서명을 생성하고, c의 결합에 의해서 서명을 전달한다. 비록 CH_C는 부분 서명에는 실패해도 c는 개인키 k를 이용하여 CH 에 의해 메시지 m을 통해 서명되어 $(m)k$ 서명을 생성한다.

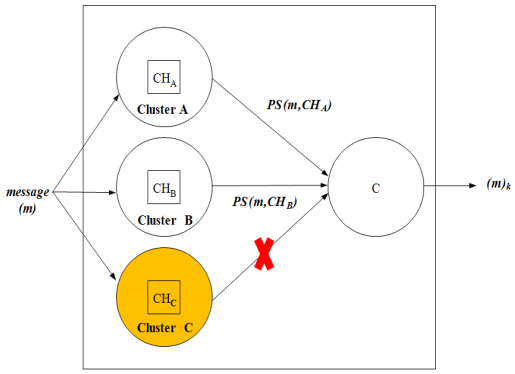

그림 3. 임계치 서명 구성
Fig 3. Threshold Signature Configuration

3.4 종단간 인증 프로토콜

그림 4는 그림 2의 클러스터 구성을 통한 다른 RSU를 이용한 CH간의 인증 프로토콜이다. 다른 RSU를 통해 인증을 하기 위해서는 인증 서버로부터 서버의 키를 이용하여 인증서를 받아 인증서버에 등록이 된 CH인지를 확인할 수 있다.

지능형 자동차에서 상황이 수시로 변경되는 상황에서 각 노드들의 변화를 체크하는 것을 클러스터 단위로 진행함으로써 관리의 효율화가 발생한다. 그림 2의

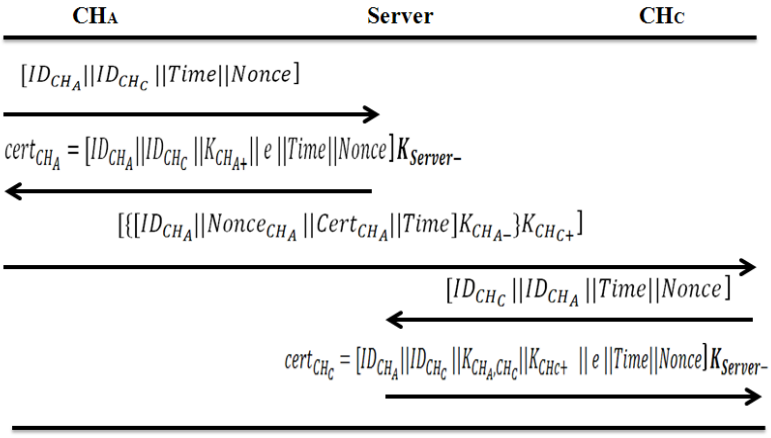

그림 4. 종단간 인증 프로토콜
Fig 4. End-to-End Authentication Protocol

노드 1이 빠른 속도로 이동하여 클러스터 다른 RSU지역의 ClusterC지역으로 이동했을 경우 노드에 대한 인증 작업을 하기 위해서 CH_C는 인증서버로부터 노드 1을 관리했던 CH_A와의 교신을 통해 이 가지고 있던 정당한 노드인지를 확인할 수 있다.

여기에서의 Server는 신뢰할 수 있는 공인인증 서버로서 각 RSU를 통해서 CH를 관리한다. CH를 통해서 새롭게 RSU에 진입하는 노드와 떠나가는 노드에 대한 정보를 Server로 실시간으로 정보를 전달함으로써 각 노드에 대한 악의적인 공격에 대응할 수 있다. 모든 CH는 항상 Server로부터 신뢰할 수 있는 인증서를 받아서 인증 작업을 진행할 수 있다. 그림 3에서 처럼 임계치 구성을 통해서 CH가 노드의 메시지를 놓친 경우 Threshold를 통해서 정확한 메시지를 전달 할 수 있도록 구성하였다. 서버의 공개키를 CH들이 알고 있으며 각 CH의 개인키를 통해서 안정성을 확보할 수 있다.

각 CH간의 통신을 위한 요청시 CH의 ID와 현재시간과 Nonce를 생성하여 보내고, 서버는 유효기간을 포함한 인증서를 보내줌으로써 CH간의 상호 인증을 해준다.

Ⅳ. 결론

지능형 자동차 발전과 융합 발전에 따른 수많은 보안 이슈들이 예상이 되고 있다. 자동차 산업에서의 향후 보안 이슈는 상당히 치명적인 위협요소들을 내재하고 있어 이에 대한 보안연구가 상당히 중요하다. 본 연구에서는 수많은 보안 위협요소중 자동차의 다양한 변화에 대응할 수 있도록 클러스터 기반으로 종단간에 인증 프로토콜을 제안하였다. 제안된 프로토콜은 고속도로 상황에서 확장성이 넓은 지역에서 효율적인 인증을 통해 안전성을 높일 수 있다. 향후 연구로는 클러스터를 구성함에 있어 다양한 변화의 내용을 효율적으로 구성할 수 있는 알고리즘의 연구와 수많은 변화속에서도 리소스의 낭비를 줄이면서 안정성을 높일 수 있는 연구의 진행이 필요하다.

참고문헌

[1] 장용, “M2M표준화 동향”, 제 13회 정보통신표준화 워크숍, 한국통신학회 통신표준화연구회, pp. 227~240, 2011년, 8월 26일.

[2] 최병철, 한승완, 정병호, 김정녀, “지능형 차량 보안 기술 동향”, 전자통신동향분석 제22권 제1호, pp.114-118], 2007년, 2월.

[3] Maxim Raya, Panos Papadimitratos, and Jean-Pierre Hubaux, “Securing Vehicular Communications,” In Magazine of IEEE Wireless Communications - IVC Specials, EPFL, pp.8-15, Oct. 2006.

[4] Dong-Hoon Kim, Jun-Yeob Song and Seuk-Keun Cha, “Introduction of Case Study for M2M Intelligent Machine Tools”, Proceedings of 2009 IEEE International Symposium on Assembly and Manufacturing, pp. 17-20, November, 2009

[5] Inhyok Cha, Yogendra Shah, Andreas U. Schmidt, Andreas Leicher, and Michael Victor (Mike) Meyerstein, "Trust in M2M Communication", IEEE VEHICULAR TECHNOLOGY MAGAZINE, pp. 69-75, SEPTEMBER, 2009

Acknowledgement

본 논문은 한국정보과학회 논문지 정보통신 제 33권 제 4호, 310-323쪽(2006년 8월) “이동 Ad Hoc망을 위한 다중계층 클러스터링기반의 인증 프로토콜”의 내용을 바탕으로 M2M에서의 지능형 자동차 기반으로 재구성한 논문임을 밝힙니다.

저자소개

이근호(Keun-Ho Lee)

2006년 고려대학교 컴퓨터학과(이학박사)
2006년~2010년 (주)삼성전자 DMC연구소
2010년~현재 백석대학교 콤인성개발원 팀장
2010년~현재 백석대학교 정보통신학부 전임강사
※ 관심분야 : M2M 보안, 이동통신보안, 융합 보안, 개인정보보호