M2M에서 텔레매틱스 기반의 차량과 기기간 인증 기법

이근호*

요약

정보기술의 발전으로 기기와 장치간 통신을 이용하는 컨버전스 기반의 M2M(Machine to Machine) 시장이 급성장하고 있다. 이동통신 사업자 중심의 많은 글로벌 기업들이 M2M 사업에 참여하고 있다. 이에 본 논문에서는 지능형 자동차 기반의 텔레매틱스 개념과 보안의 취약성을 알아보았다. 지능형자동차와 IT 기술의 융합과 이동통신망 기술의 발전은 사용자에게 제공되는 다양한 서비스의 질은 향상 시켰지만 이로 인한 보안 위협요소는 증가하였다. 본 연구에서는 텔레매틱스 사업에 이동통신사업자의 참여로 생성될 수 있는 새로운 클러스터 기반의 서비스 모델을 제시하였다. 제시한 새로운 클러스터 모델에서 새롭게 생성된 환경에서 발생 될 수 있는 차량 이동통신망 보안의 취약성을 분석하였다. 분석한 보안 위협요소 중 발생할 수 있는 취약성을 해결하기 위한 방법으로 M2M 기기와 스마트폰을 통한 차량 상호 인증 기법을 제시하였다.

M2V(Machine to Vehicle) Authentication Scheme based on Telematics in M2M

Keun-Ho Lee*

ABSTRACT

As the developing of the information technology, M2M market of the global telecommunication companies are using communication between devices and machines. New M2M business model is growing rapidly of the many companies. In this paper, the concept of telematics and vulnerabilities of vehicle network security are discussed. The convergence of vehicle and information technology provided to user that the development of mobile communication technology have improved quality of service but as a result security threats became diverse. In this research, we proposed new business model that be occurred to the participation of mobile carriers in telematics business. We analyzed mobile radio communication network security vulnerabilities. We proposed smart phone and vehicle authentication scheme with M2M device as a way to solve vulnerabilities.

Key Words : Telematics, Vehicle, Authentication, M2M

* 백석대학교 정보통신학부(✉root1004@bu.ac.kr)
· 제1저자(First Author) : 이근호 · 교신저자(Correspondent Author) : 이근호
· 접수일(2012년 1월 18일), 수정일(1차 : 2012년 2월 16일), 게재확정일(2012년 2월 17일)

Ⅰ. 서 론

정보기술 및 이동통신 기술의 발전으로 많은 분야에서 기기와 장치간의 융합에 의한 새로운 서비스가 만들어지고 있다. 급속도로 증가하는 스마트폰 보급률과 다른 기기와의 융합을 통한 새로운 연구 영역인 M2M (Machine-to-Machine)분야에 대한 관심과 개발이 활발하게 이루어지고 있다. M2M 통신에서 수많은 다양한 업체의 참여로 인하여 보안에 대한 큰 연구가 이루어지고 있다[1].

M2M 통신은 사용자와 각 기기와 장치들간의 연동이 가능하며, 주변 기기를 통한 다양한 정보를 수집하여 분석하고 분류하여 사용자나 시스템과 다른 주변 기기에게 정보를 제공해준다. M2M 새로운 사업모델의 확장을 통해 많은 기업의 참여와 연구가 활발히 진행되고 있다. M2M 통신은 사람과 기기간의 정보 전달을 통해 사용자가 실시간으로 정보를 확인하는 서비스 수준까지 이르렀다. 이러한 서비스 환경으로 사용자는 신속하고 정확한 정보를 제공 받을 수 있지만, 기기와의 데이터 전송 시 많은 보안 위협의 문제가 발생한다.

본 논문에서는 M2M의 응용분야인 지능형 자동차의 한분야인 텔레매틱스의 기술에 대해서 살펴보고, 발생할 수 있는 보안 위협요소와 취약성에 대해 분석하고, 차량 내의 M2M 기기와 스마트폰의 상호 인증에 대한 기법을 제안한다.

Ⅱ. 관련연구

2.1 M2M 보안

M2M에서는 잦은 네트워크의 변화와 무선채널의 위험에 따른 정보 수집의 어려움과 안정적인 관리와 효과적인 인증의 방법이 요구된다. M2M 은 기존 유.무선 통신보안의 특성을 이용하여 보안 위협요소로부터 안전한 정보수집 등의 서비스를 제공해야 한다. M2M 통신 환경에서는 데이터 노출로 인한 위치, 개인정보, 과금 데이터 등의 민감한 정보를 전송을 하기 때문에 네트워크 어느 곳에서나 도청에 의해 수집되는 데이터 유출을 예방하기 위해 데이터의 기밀성을 보장해야 한다. 중간자(man-in-the-middle) 공격을 통한 데이터의 불법 변경 및 삭제, 위조된 데이터의 삽입 등에 대응하기 위한 무결성 보장이 필요하다. 서비스 거부공격(DoS)은 시스템의 가용성 및 생산성을 훼손함으로써 시스템 자원과 정보에 대한 접근 능력을 감소시킬 수 있다. 따라서 M2M 통신 환경에서도 주체 또는 디바이스들의 정보 접근 능력을 침해하지 않도록 시스템 가용성을 보장 할 수 있는 보안 메커니즘이 필요하다. 이동성을 제공을 위한 위치추적의 경우 M2M 디바이스는 디바이스의 위치정보 노출로 인해 디바이스 및 디바이스 소유자의 위치나 이동 경로가 노출될 가능성이 존재한다. 따라서 이동성을 제공하면서 추적 불가능성을 제공할 수 있는 보안 메커니즘이 필요하다[2,3].

2.2 텔레메틱스 보안

M2M의 주요 응용분야로는 텔레매틱스, 물류관리, 지능 검침 시스템, 원격 자산 관리 시스템, 판매 관리 시스템(POS) 및 보안 관련 분야가 있다[4].

텔레매틱스(Telematics)는 차량의 위치파악기술, 양방향 통신이 가능한 무선 통신망과 차량 내 단말기를 통해 차량, 운전자, 탑승자에게 다양한 정보 및 서비스를 제공한다. 텔레매틱스 시장은 다수의 하부 업체들이 각각의 독립 분야를 맡아서 참여하는 구조로 되어 있다. End-User에게 서비스가 제공되는 과정에 있어서 텔레매틱스 서비스 사업자, 칩셋 공급업체, 모듈업체, 단말제조업체, 이동통신사업자, 서비스업체, 솔루션업체 등으로 구성되어 있으며, 이외에도 다양한 업체의 참여가 이루어지고 있다. 이동통신 사업자가 텔레매틱스 사업에 참여함으로써 차량 이동간 새

로운 보안 취약성이 존재 할 수 있다[1].

지능형 자동차에서 사용하는 대표적인 네트워크로는 Ad Hoc 망 기반의 VANET (Vehicular Ad-hoc Networks)이 알려져 있으며, 차량 중심으로 차량 간 통신망(V2V Vehicle-To-Vehicle)과 차량과 인프라 통신망(V2I Vehicle-To-Infrastructure)으로 분류된다[5].

VANET도 기존의 무선 네트워크 환경이 가지고 있는 보안 취약성을 그대로 가지고 있으며 내용은 다음과 같다[6]. 한명의 공격자가 네트워크상에서 여러 개의 환영 노드들로 나타나서 혼란을 가중시키는 The Sybil Attack과 공격 차량에 의해 차량 간 네트워크 영역 내에서 다른 차량들을 거짓 정보로 오염시키는 위조 공격, 차량 네트워크 영역 내에서 다른 차량의 통신에 장애를 유발하는 신호를 발생시켜 네트워크 통신을 마비시키는 Jamming 공격, 주행 중에 메시지를 전달하는 과정에서 공격 차량에 의한 메시지 삭제·변조를 통해 차량 통신을 방해하는 In-transit Traffic Tampering 공격 등이 존재한다. 아울러 어플리케이션에 악성코드가 삽입 되어 사용자가 어플리케이션을 다운 받은 후 차량과 디바이스의 통신을 하면 개인정보 및 차량 정보가 유출되는 공격과 Jamming Attack과 비슷한 공격으로 스마트폰에 다량의 데이터를 전송하여 서비스를 이용하지 못하게 하는 서비스 거부 공격이 있다. 허가받지 않은 사용자가 인증서버로부터 인증을 받아 통신을 요청한 사용자 대신에 차량 내 M2M 기기와 통신하여 개인정보 획득 및 차량 오작동을 시키는 사용자 인증 위장 공격 등이 존재한다[1].

III. 스마트폰을 이용한 상호 인증 기법

지능형 자동차 내 M2M 기기와 사용자의 디바이스 통신 환경은 무선 환경이며, 신뢰받지 않은 제 3자에 의한 위장공격을 차단한다고 가정한다.

3.1 시나리오

사용자의 스마트폰 및 차량 내 M2M 기기를 VID(Vehicle IDentification)와 신뢰 할 수 있는 제 3기관 TS(Trust Server)로 표기한다. 사용자가 스마트폰을 이용하여 VID와의 통신을 원할 때, 사용자의 스마트폰은 TS로 사용자의 인증에 필요한 인증서를 전송한다. 스마트폰은 사용자의 인증서가 임시로 저장되지 않아야 한다. TS는 사용자 및 VID의 정보를 보유하고, 등록과 VID의 키 관리를 담당한다. 기존 인증방식은 스마트폰 사용자가 인증서버에 인증을 요청할시 스마트폰 사용자만 인증서버로부터 인증을 받아 VID의 정당성을 확인하였다. 기기간 상호 인증방법은 스마트폰에서 VID와의 통신을 위해 접속요청시 스마트폰 사용자가 정당한 사용자인지 TS로부터 인증을 받는다. VID는 TS로부터 정보를 받아 접속을 요청한 사용자가 TS로부터 인증을 받은 사용자인지 확인 할 수 있다.

3.2 상호 인증

사용자가 스마트폰을 이용하여 자신의 차량 내의 VID에게 연결을 요청할 때 사용자는 TS로부터 본인 인증을 받아 VID와 안전하게 통신이 되어야 한다. 인증이 진행시 단순 ID와 패스워드 입력을 통한 인증보다는 좀더 복잡한 인증 과정을 통하는 것이 상호인증에 안전하다.

- Setp1. 사용자는 자신의 ID와 패스워드를 스마트폰에 입력하면 스마트폰은 사용자의 ID, MAC 주소, 패스워드를 이용하여 만든 비밀 키를 TS에게 보낸다.
- Step2. TS는 사용자의 패스워드를 기반으로 한 사용자의 마스터 키(MK:Master Key)를 찾아서 사용자 정보를 포함하고 있는 TK(Ticket Key)1와 세션키를 만든다. TS는 자신의 MK를 이용하여 TK1를 암호화 하고 TK1와 세션키를 사용자에게 보낸다.

- Step3. 사용자는 암호화된 TK1와 세션키를 가지고 VID와 접속할 준비를 한다.
- Step4. 사용자는 TS에게 TK1와 세션키로 암호화한 TimeStamp를 보낸다. TS는 MK를 사용하여 TK1를 복호화하고 세션 키를 이용하여 TimeStamp를 복호화 한다. 사용자가 TS의 세션 키를 사용할 수 있기 때문에 TS는 정당한 사용자 인지를 확인 할 수 있다.
- Step5. TS는 사용자와 VID를 위한 TK2를 각각 하나씩 만든다. 각 TK2에는 사용자 이름, VID 이름, TimeStamp를 가지고 있으며 새로운 키인 SK(Shadow Key)를 포함한다.
- Step6. TS는 서버의 TK2를 VID의 MK로 암호화 한다. TS는 MK로 암호화 된 TK2를 사용자와 공유한 세션 키로 다시 암호화 하고 사용자에게 이것을 전송한다.
- Step7. 사용자는 세션 키를 이용하여 MK로 암호화 된 TK2를 복호화 한다. 복호화로 인해 사용자는 VID의 TK2와 SK를 알 수 있다. 사용자는 SK를 사용하여 TimeStamp를 암호화 하고 VID에게 암호화 된 TimeStamp와 TK2를 보낸다. 두 가지를 받은 VID는 MK를 사용하여 TK2를 복호화 하고 SK를 이용하여 TimeStamp를 복호화 한다.

사용자와 VID 모두 SK를 가지고 있으며, 사용자가 TimeStamp를 암호화 하기 위해 SK를 사용했기 때문에 사용자가 정당한 사용자인지 확인이 가능하다. 사용자 역시 VID가 TimeStamp를 얻기 위해 SK를 사용해야만 했기 때문에 MIC가 정당한 기기인지 알 수 있다.

3.3 검증 결과

기존 인증방법으로는 ID, Password를 통해 간단한 사용자 인증만으로 사용자를 확인하여 M2M 기기와의 접속을 승인했다. 그러나 이러한 방법은 공격자가 사용자의 인증정보를 얻음으로써 접속을 요청한 사용자 대신에 M2M 기기와의 통신을 수행하여 사용자 정보를 수집, 도용, 변조, 삭제를 할 수 있는 위협요소가 발생한다. 사용자가 제 3기관과의 암호화 및 키 교환을 통해 정당한 사용자 인지를 확인하고 M2M 기기 역시 제 3기관으로부터 사용자의 정보를 받아 정당한 사용자인지 MK1을 통해 1차 확인한 후, M2M 기기가 사용자와 키를 교환함으로서 사용자가 정당한 사용자인지 MK2를 통해 2차 확인을 한다. 이러한 암호화 및 키 교환으로 인해 사용자 역시 M2M 기기가 자신의 기기 맞는지에 대한 여부를 확인 할 수 있다.

IV. 차량 간 상호 인증

M2M에서 기기간의 인증을 위해 클러스터 인증 절차를 제안하였다. 클러스터내에서 CH(Cluster Head)를 통해 차량 내 M2M 기기 및 신뢰 할 수 있는 제 3기관의 상호 인증이 이루어져 기기간의 안전한 통신을 할 수 있다.

4.1 클러스터링 기법

클러스터링을 통한 인증 기법은 잦은 네트워크의 변화에 효율적으로 그룹화 하여 관리하는 기법이다. 클러스터내의 기기나 장치들을 관리하는 CH를 두어 각 장치를 관리한다. 클러스터내로 새롭게 진입 하는 장비나 기기는 CH간에 상호 인증을 통해 상호 신뢰성을 보장해주는 기법이다[8].

4.2 시나리오

사용자의 차량 내 M2M 기기를 VID로 표기하고, 신뢰 할 수 있는 제 3기관을 TS로 표기한다. 사용자를 기준으로 사용자 차량중 신뢰할 수 있는 차량 2, 4를 CH(Cluser Head)로 선정한다. 사용자 주변 클러스터

내에는 사용자로부터 인증 받은 기기들이 존재하며, 사용자가 클러스터내의 기기들 중 가장 신뢰할 수 있는 기기를 CH로 선정한다고 가정한다. 그림 1의 Cluster A는 차량 1, 2, 3은 Cluster B는 차량 4, 5, 6으로 상호 인증 된 상태라 가정한다. TS는 인증기관으로서 모든 기기에 대한 등록, 인증에 대한 모든 관리를 담당하며, 위장공격 및 무선 통신에 대한 가로채기 공격으로부터 안전하다고 가정한다. 사용자 차량은 TS로부터 인증 받은 정당한 사용자이며, TS로부터 인증을 받은 CH와 인증 된 주변 클러스터내의 기기는 하나의 네트워크가 된다.

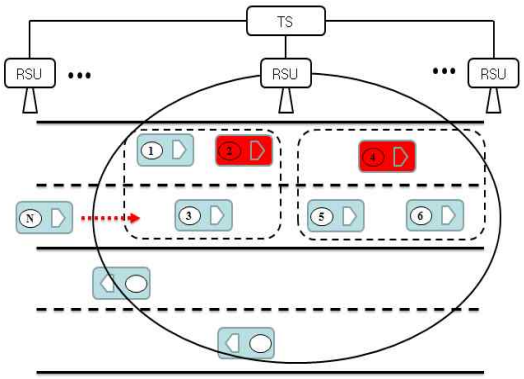

그림 2. 새로운 차량 진입
Fig. 2 New Vehicle Entry

4.3 상호 인증

그림 1에서 하나의 클러스터에 진입하려는 차량 N은 상호 간 안전한 통신을 위하여 등록하여야 한다. 모든 기기는 통신을 위하여 인증서를 발급 받아 TS에 등록을 해야 한다.

- Step1. 차량 N이 클러스터 A에 진입을 하기 위해 차량 3에게 연결을 요청하고 자신의 인증서를 전송한다.
- Step2. 요청을 받은 차량 3는 CH인 차량 2에게 차량 3에 대한 인증을 요청하고 차량 3에 대한 인증서를 전송한다.
- Step3. 차량 2는 TS에게 차량 N에 대한 정보를 전송한다.
- Step4. TS는 자신의 서버에서 차량 N에 대한 인증서 값을 찾아 차량 2에게 전송한다.
- Step5. 차량 2는 차량 3로부터 받은 값과 TS로부터 받은 값을 비교한 후 차량 N이 정당한 사용자이면 접속 승인 메시지와 자신의 인증서 값을 차량 3에게 전송한다.
- Step6. 차량 3는 차량 2로부터 받은 정보를 확인하여 자신의 인증서 값을 차량 N에게 전송한다.
- Step7. 차량 N은 차량 3에게 받은 차량 2와 차량 3의 정보를 확인하고 이들의 정보와 자신의 인증서 값을 TS에게 전송한다.
- Step8. TS는 받은 정보를 확인하여 차량 N에게 차량 3와 차량 2가 정당한 사용자임을 알려준다.

4.4 검증 결과

공격자가 기기와의 통신과정 중에 인증정보를 얻음으로써 접속을 요청한 사용자 대신에 M2M 기기와의 통신을 수행하여 사용자 정보를 수집, 도용, 변조, 삭제의 가능성을 없앴다.

요청한 기기와 요청 받은 기기 모두 서버로부터 인증을 받도록 함으로써 정당한 사용자임을 알 수 있게 하였으며, 상호 인증을 통해 위장공격에 안전한 통신을 제공 할 수 있다.

Ⅴ. 결론

M2M 통신의 응용 분야인 지능형 자동차의 텔레매틱스를 중심으로 보안의 취약성을 알아보고, 이 중 사용자와 차량 내 기기의 인증 취약성 공격에 대비하기 위한 인증 기법을 제안하였다. 사용자의 스마트폰과 차량 내 M2M기기, 제 3기관 모두가 상호 인증을 받음

으로써 허가받지 않은 사용자로부터의 위장 공격을 예방 할 수 있다.

참고문헌

[1] Seong-Gwon Yeo, Keun-Ho Lee, “A Security Survey in Telematics”, Journal of Korea Convergence Society, Vol.1.No.4, pp.1-7, December 2011

[2] Keun-Ho Lee, “Analysis of Security Threat in Machine to Machine Communication”, Journal of The Korea Academia-Industrial Cooperation Society, Vol.11, No.1, pp. 416-419, May 2010

[3] Keun-Ho Lee, “Analysis of Security Threat in Machine to Machine Communication”, Journal of The Korea Academia-Industrial Cooperation Society, Vol.11, No.1, pp. 416-419, May 2010

[4] Yu-chang Kim, “The Trend of Technology and Prospect of M2M”, Telit Korea, pp.66, July 2009

[5] Seong-il Park "M2M Terminal in Mobile Communication Network", Journal of Information Science, Vol.28, No.9 pp.40-43, September 2010

[6] Sang-u Kang, Se-jin Park, "Security Enhan- cement method design in VANET using Authenticated Boot of TPM", Journal of Korea Computer Congress, Vol.36, No.1(D), 2009

[7] Douceur, J.: The Sybil Attack. In: First Intrnational Workshop on Peer-to-Peer Systems, March 2002, pp.251 - 260, 2002

[8] Gab-Sang Ryu, Keun-Ho Lee " Authentication based on Cluster in Machine to Machine", Journal of Korea Knowledge Information Technology Society, Vol.5, No.6, December 2010

감사의 글

“이 논문은 2011년도 정부(교육과학기술부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임(No.2011-0010457)”

저자소개

이근호(Keun-Ho Lee)

2006년 고려대학교 컴퓨터학과(이학박사)
2006년~2010년 (주)삼성전자 DMC연구소
2010년~현재 백석대학교 쿰인성개발원 팀장

2010년~현재 백석대학교 정보통신학부 전임강사
※ 관심분야 : M2M 보안, 이동통신보안, 융합 보안, 개인정보보호