차량 통신에서 MAC Security 기반의 사용자 프라이버시 보호기법

임헌정, 이준원, 김태경*, 정태명**
성균관 대학교 전자전기컴퓨터 공학과
서울신학대학교 교양학부*
성균관 대학교 정보통신공학부**
e-mail : {hjlim99, jwlee}@imtl.skku.ac.kr, tkkim@stu.ac.kr**, tmchung@ece.skku.ac.kr**

Privacy Protection Mechanism using MAC Security in VANET

Hun-Jung Lim, Jun-Won Lee, Tae-Kyung Kim*, Tai-Myoung Chung**
Dept. of Computer Engineering, Sungkyunkwan University
Dept. of Liberal Art, Seoul Theological University*
School of Information Communication Engineering, Sungkyunkwan University**

요 약

통신기술이 발달하면서 차량 통신에 대한 연구가 활발히 진행되고 있다. 주 연구 분야로 라우팅 및 위치정보 기반의 주소 설정과 통신, 보안 문제 해결 등이 있다. 차량은 지극히 개인적인 공간이므로 운전자의 위치 및 식별정보에 대한 보호가 필요하다. 이러한 연구는 운전자 프라이버시 보호 측면에서 보안기능과는 별도로 연구가 진행되고 있다. 기존의 프라이버시 보호 기술들은 각 계층별 프라이버시 보호는 만족하고 있지만, 계층별 정보들의 연결을 통해 프라이버시를 공격하는 연관 공격(Relation Attack)에 대하여서는 취약함을 보이고 있다. 따라서 본 논문에서는 MAC Security 기술을 이용하여 운전자의 프라이버시를 보호하는 기법을 제안하려 한다. 제안하는 기법은 네트워크 접속 계층 주소를 제외한 나머지 정보를 암호화 하기 때문에 물리 주소로 인한 프라이버시가 침해가 발생 하더라도 다른 계층의 정보를 알 수 없으므로 네트워크 계층의 위치 정보 및 응용계층의 사용자의 식별 정보 등을 보호 함으로 상관 공격에 안전하다. 물리 주소 역시 해당 도메인에서 유일한 식별 정보 이므로 멀티 도메인 통신이 이루어 지는 인터넷 상에서는 운전자의 프라이버시를 보호 할 수 있다.

1. 서론

통신 기술의 발단은 사용자로 하여금 장소 및 시간의 제약 없이 네트워크 연결성을 제공할 수 있게 되었다. 최근에는 네트워크 기술을 사용자 단말기와의 접목에서 벗어나 차량과도 연동하여 이동하는 차량(V2V) 및 통신망(V2I)과 데이터를 주고받게 하여 사용자의 편의성과 운전에 도움을 주고 있다. 이러한 통신기술을 차량통신(Vehicular Ad-hoc NETwork: VANET) 이라고 한다. 중심 연구 분야로는 차량 간 통신 시 라우팅 기법, 위치정보 기반의 주소 설정 및 데이터 전송, 통신망과의 연동 시 이동성 지원 기술, 통신 시 보안기능/프라이버시 예방 등이 있다. 특히 프라이버시 예방은 차량통신의 특성상 위치 및 개인식별 정보의 활용 빈도가 높고, 정보의 노출은 운전자의 이동 패턴과 위치 추적이 가능하다는 점에서 보안기능과는 별도로 연구가 필요 하다. [1]에 따르면 프라이버시 보호란 개인의 속성(식별, 위치 등)정보를 타인에게 노출할지를 스스로 결정할 수 있는 권리라고 표현하고 있다. 이러한 프라이버시 보호가 없다면 사용자 및 운전자가 언제, 어디서, 무엇을 하는지에 대한 정보 등이 노출될 수 있다. 일반적으로 프라이버시는 아래와 같이 세 분류로 나눌 수 있다[2].

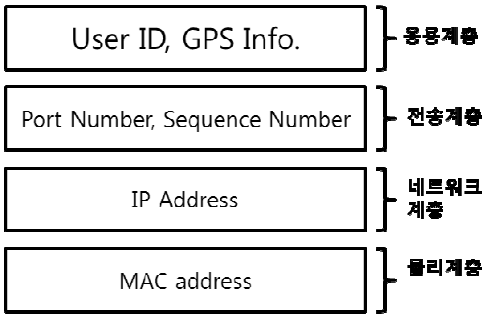
- 데이터 프라이버시(Data Privacy) : 통신상에 전송하는 데이터 보호
- 식별정보 보호(Identity Privacy) : 통신 주체에 대한 식별 정보 보호
- 위치정보 보호(Location Privacy) : 통신 주체의 위치정보 보호

하지만 일반적으로 데이터 프라이버시는 암호화 등의 방법을 통하여 쉽게 보호 할 수 있으므로 차량 통신에서는 식별정보 보호와 위치 정보 보호에 초점을 두고 있다. 본 논문에서도 위 두 방식에 초점을 맞추었다.

본 논문의 구성을 다음과 같다. 1 장의 서론에 이어 2 장의 관련연구를 통하여 기존의 프라이버시 보호 기법과 각 공격 기법에 대하여 알아보았다. 3 장에서는 제안방식으로 MAC Security(MACsec)를 통하여 프라이버시를 보호 기법에 대하여 기술하였다. 4 장에서 기존의 연구대비 제안 방식의 장점에 대하여 분석하면서 결론을 맺었다.

2. 관련 연구

기존 차량통신에서의 프라이버시 공격 중 식별정보에 대한 공격은 각 계층별로 존재하는 유일정보에 대한 추적을 통하여 이루어 졌다. 즉, 네트워크 접속 계층의 MAC 주소, 네트워크 계층의 IP 주소, 전송계층의 TCP 포트 및 시퀀스 번호, 응용계층의 사용자 ID 등이 있다. 사용자는 단대단 통신 및 사용자에게 특화된 서비스를 위하여 상위 계층의 주소 정보 및 ID 정보를 서비스 공급 업체에 전송 한다. 공격자는 지속적인 트래픽 감시를 통하여 해당 사용자의 위치 및 행동패턴에 대한 정보를 얻을 수 있게 된다. 위치 정보에 대한 공격은 네트워크 접속 계층에서는 전파의 강약정보를 이용한 삼각측량법과 네트워크계층의 도메인별 네트워크 프리픽스 할당을 역 추적 하는 기법 등이 있다. 이러한 각 계층별 프라이버시 침해 요소들을 정리하면 (그림 1)과 같다. .

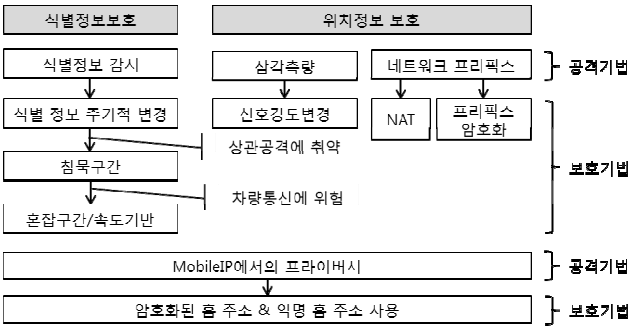


(그림 1) 계층별 프라이버시 침해 요소

식별정보에 대한 대표적인 보호 기법으로는 익명정보를 (pseudonyms)의 주기적 변경하여 공격자의 추적을 방지 할 수 있다[3]. 하지만 이 방식은 공격자가 과거 식별정보와 새 식별정보를 감시 하는 상관 공격(Correlation Attack) 에는 취약하다. [4]에서는 상관공격에 대한 방지 방법으로 침묵구간(Silent Period)을 정의하고 사용자가 식별정보를 변경 시 일정한 시간여유를 두게 하였다. 하지만 차량 통신에서 전송되는 메시지들은 운전자의 생명에 영향을 미치므로 침묵구간은 사고의 위험성을 가지고 있다. [5]에서는 혼합구간(Mix-Zone)을 정의하여 이 구간에서 모든 차량이 동시에 식별정보를 변경함으로써 공격자의 추적을 어렵게 하는 방식을 제안하였다. [6]에서는 별도의 혼합구간 없이 차량의 속도(30Km/h)가 느려지면 사고의 위험성이 적으므로 이 시기에 침묵구간 및 혼합구간의 방식을 적용 하는 방식을 제안 하였다.

위치정보에 대한 보호기법은 네트워크 접속 계층과 네트워크 계층으로 나눌 수 있다. 삼각측량을 이용한 공격에 대하여서는 통신 신호 강도 변경을 통해 방지가 가능하다. 하지만 네트워크 계층에서의 보호는 좀 더 복잡한 메커니즘이 필요 하다. 네트워크 계층의 IP 주소는 인터넷상에서 단말기에 대한 식별정보로써 유일성과 불변성을 가지고 있어야 한다. 하지만, 네트워크 접속 계층에서 사용하는 지속적인 값 변경의 방식을 IP 주소에 적용할 경우 불변성을 만족할 수 없어 통신 단절의 문제점을 가지고 온다.

위치정보를 가지고 있는 네트워크 프리픽스 정보를 변경 시에는 효율적인 라우팅이 어렵다. 문제 해결을 위해서 [7]에서는 프리픽스 정보를 암호화 하여 적법한 라우터만 프리픽스 정보를 복호화 하는 방법을 제안 하였다. Network Address Translation(NAT)를 이용하여 단말기의 위치정보를 보호할 수도 있다[8]. 하지만 NAT 의 경우 프라이버시 문제 해결이라는 장점은 있지만 IP 주소의 유일성과 불변성을 보장할 수 없어 많은 제약이 사항이 발생한다. 차량의 이동성을 지원하기 위해 개발된 MobileIP 의 경우에는 2007 년부터 문제점에 대한 논의가 시작되었다[9]. [10]에서는 MobileIP 에서의 프라이버시 문제 해결을 위하여 암호화된 홈 주소(eHoA)와 익명 홈 주소(pHoA)를 사용하여 통신선로상의 공격자 및 악의적인 상대노드(Correspond Node)로부터의 프라이버시 보호방법을 제안 하였다. (그림 2)는 기존의 프라이버시 공격 및 보호 기법을 도식화 한 것이다.



(그림 2) 프라이버시 공격 및 보호 기법

기존의 프라이버시 보호 기법들의 효율성을 평가 하기 위하여 두 개의 공격모델을 기반으로 분석 하였다.

- 상관 공격(Correlation Attack) : 과거와 현재의 식별정보의 상관 정보를 이용하는 공격기법이다. 동일한 단말기에서 전송되는 두 개의 다른 값의 유추를 이용하여 공격한다.
- 연관 공격(Relation Attack) : 동일한 단말기의 서로 다른 계층의 정보의 연관관계를 이용하는 공격기법이다. 한 계층의 정보가 보호되더라도 다른 계층 정보의 감시를 통하여 보호된 계층의 정보 유출이 가능하다.

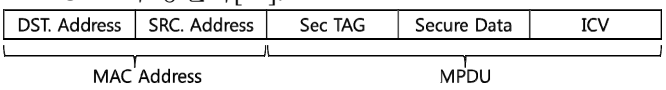
<표 1> 프라이버시 보호 방법 비교

Solution	ID.Pri	Loc.Pri	CorAtck	RelAtck
Pseudonyms id [3]	○	×	×	×
Silent period[4]	○	×	○	×
SLOW[6]	○	×	○	×
NAT[8]	○	○	○	×
Prefix Encryption [7]	×	○	−	×
eHoA&pHoA[10]	○	○	−	×
Mix-zone[5], [6]	○	×	○	×

분석결과 모든 프라이버시 보호 기법들은 연관공격에 지극히 취약한 것으로 나타났다. 이는 네트워크 모델 설계 시 요구되었던 투명성(Transparency)에 기인한 것으로 보인다. 따라서 본 논문에서는 MACsec 를 이용한 연관공격 방지 기법을 제안 하려 한다.

3. 제안 방식

MACsec 는 IEEE802.1AE 에서 정의한 네트워크 접속 계층 보안프로토콜로 단대단(Point-to-point) 인증, 무결성 검증, 데이터 암호화를 수행하여, 방화벽, IDS/IPS 에서 차단할 수 없는 데이터 스니핑, DoS 공격 등의 위험으로부터 네트워크 접속 계층의 안전을 보장한다. MACsec 프레임은 (그림 3)과 같이 MAC Address 와 MPDU 로 구성된다[11].



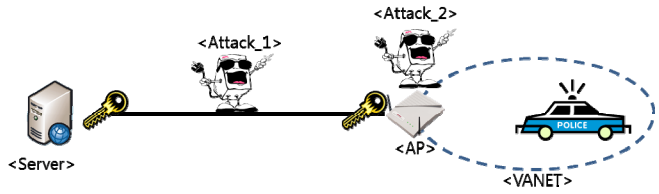
(그림 3) MACsec Frame Format

MAC Service Data Unit (MSDU)는 일반적으로 GCM-AES-128 에 의해 되면서 SecureDATA 와 Integrity Check Value(ICV)를 생성한다. SecTAG 는 데이터의 캡슐화, 암호화 및 인증에 대한 주요 정보를 포함하고 있다. 사용자는 MACsec 프레임을 통해 <표 1>의 정보를 수신하여 암호화된 데이터를 검증한다[12].

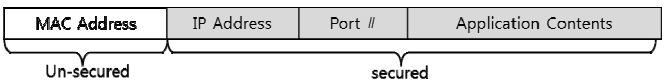
<표 2> SecTAG 구성정보

Classification	Specific Information	Size
MACsec type	0x88E5	2Byte
TCI + AN	TAG control infor. Association # within the channel	1 Byte
SL	Short length	1 Byte
PN	Packet #	4 Byte
SCI	MAC Src Address + Port ID Association #	8 Byte

사용자 간의 MACsec 통신은 CA (secure Connectivity Association) → SA (Secure Association) → SC (Secure Channels)의 순서로 진행되며, SA 과정 중 상호간의 SAK(SA Key)를 교환하는 과정을 통해 SC(Secure Channel)이 형성된다. 각각의 사용자는 고유의 SC 를 형성하게 되므로 SC 에 참여하지 않은 사용자는 암호화된 MACsec 프레임을 만들거나 해독할 수 없다. MACsec 의 보호 범위를 표현하면 (그림 4,5)와 같다.



(그림 4) 네트워크상의 MACsec 의 보안 범위



(그림 5) 통신포맷상의 MACsec 의 보안 범위

본 논문의 제안 방식에서는 차량통신의 프라이버시 보호를 위하여 MACsec 을 사용한다. (그림 4)에서 메시지를 전송하기 전 차량은 접속 포인트(AP)와 보안관계(Security Association)를 맺게 된다. 이후 전송되는 모든 데이터는 (그림 5)와 같이 물리 주소(MAC Address)부분을 제외하고 모두 암호화 되어서 전송된다. 이를 수신한 접속포인트는 사전에 교환된 정보를 기반으로 네트워크계층의 IP 주소를 복호화 후 다음 홉의 물리 주소로 바꾸어 전송하게 된다. 따라서, (그림 4)에서 공격자 Attacker_1 이 전송중인 데이터를 획득하더라도 물리 주소 이외의 상위계층 정보를 얻지를 못한다. 또한, 획득한 물리 주소 역시 차량의 주소가 아니고 이전 홉의 주소이므로 무의미 하다. Attacker_2 역시 전송 중 데이터의 물리 주소 이외의 정보를 얻지 못한다. 비록 차량의 주소를 직접적으로 획득할 수 있지만 해당 주소의 유일성은 해당 도메인에서만 유일하기 때문에 해당 정보만으로 차량을 식별하기 어렵다. 또한, 상위 계층의 정보와 연동이 불가능하므로 위치 정보 역시 안전하다.

4. 결론

본 논문에서는 기존 차량통신에서의 프라이버시 공격기법과 보호 기법을 분석하였다. 분석결과 대부분의 보호기법은 연관공격에 취약하였다. 하지만 MACsec 을 이용할 경우 물리 주소 이외의 모든 계층 정보가 암호화 되기 때문에 연관공격에 안전하다. 또한 노출되는 물리 주소 역시 지역적인 정보이므로 이를 기반으로 차량을 식별하기는 어렵다. 하지만 본 제안 방식 사용은 데이터 전송 시 보안관계 설립과정과 메시지 암/복호화의 부하가 발생하게 된다.

향후 연구에서는 차량통신에서의 MACsec 활용 시 성능평가를 실시 하려 한다.

ACKNOWLEDGMENT

본 논문은 중소기업청에서 지원하는 2010 년도 산학연공동기술개발사업(No. 00044301)의 연구수행으로 인한 결과물임을 밝힙니다

참고문헌

[1]S. T. Kent, L. I. Millett, IDs--Not that Easy: Questions about Nationwide Identity Systems, Natl Academy Pr, 2002.

[2]A. R. Beresford, F. Stajano, "Location privacy in pervasive computing" Pervasive Computing, IEEE, Vol.2, No.1, pp.46-55, 2005.

[3]M. Gruteser, D. Grunwald, "Enhancing location privacy in wireless LAN through disposable interface identifiers: A quantitative analysis," Mobile Networks and Applications, Vol.10, No.3, pp.315-325, 2005.

[4]L. Huang, K. Matsuura, H. Yamane, and K. Sezaki, "Enhancing wireless location privacy using silent period" , Vol.2, pp.1187-1192, 2005.

[5]J. Freudiger, M. Raya, M. Felegyhazi, P. Papadimitratos, and J. P. Hubaux, "Mix-zones for location privacy in vehicular networks" , 2007.

[6]L. Buttyán, T. Holczer, A. Weimerskirch, and W. Whyte, "Slow: A practical pseudonym changing scheme for location privacy in vanets" , pp.1-8, 2010.

[7]J. Trostle, H. Matsuoka, M. M. B. Tariq, J. Kempf, T. Kawahara, and R. Jain, "Cryptographically protected prefixes for location privacy in ipv6" , pp.142-166, 2005.

[8]P. Srisuresh, M. Holdrege, "RFC 2663" IP Network Address Translator (NAT) Terminology and Considerations, 1999.
[9]R. Koodli, "RFC 4882: IP address location privacy and mobile IPv6: Problem statement" , 2007.
[10]Y. Qiu, "RFC 5726 : Mobile IPv6 location privacy solutions" , 2010.
[11]"IEEE standard for local and metropolitan area networks : Media access control (MAC) security :IEEE-SA standards board" , 2006.
[12]이준원, 박선호, 금기호, 정태명, "MACsec(802.1AE) 프로토콜 기반 대형마켓 보안 네트워크 설계", 한국정보처리학회, Vol.17, No.1, pp.804-807, 2010.