VANET에서의 보안 위협 및 대처 방안

나진한* 박영호** 문상재***

(JinHan Na*, YoungHo Park**, SangJae Moon***)

요 약 VANET 환경에서는 차량간 잘못된 정보의 전송이 교통 혼잡 뿐 아니라 치명적인 사고를 일으킬 수 있으므로 VANET 환경에서의 응용들이 안전하고 신뢰성 있게 제공하기 위해서는 보안성 확보가 필수적으로 요구된다. 본 논문에서는 VANET에서 안전성을 제공하기 위하여 VANET에서의 보안 위협 및 공격 유형을 분석하고 대처방안을 제시하며 제공되는 대표적인 인증 프로토콜 방식을 분석한다.

핵심주제어 : VANET, 보안 서비스, 보안 위협, 인증, 보안 공격

Key Words : VANET, security service, security threat, authentication, security attack

Ⅰ. 서 론

최근 국내외적으로 ITS(intelligent transportation system)를 위한 연구가 활발히 이루어지고 있으며 ITS의 핵심기술로 부상하고 있는 VANET (Vehicular Ad hoc Network)은 지능형 차량에 무선통신 기술을 지원하기 위하여 IEEE802.11 [1] 기반의 기술을 사용하고 있다. [2,3]

VANET(Vehicular Ad hoc Network) 환경에서는 차량간 잘못된 정보의 전송이 교통 혼잡 뿐 아니라 치명적인 사고를 일으킬 수 있으며 과금에 관련된 사기의 위험이 발생할 수 있고 통신 정보를 추적하여 운전자의 프라이버시를 침해할 수 있다. 따라서 VANET 환경에서 응용들이 안전하고 신뢰성 있게 제공되기 위해서는 VANET 환경에서 발생할 수 있는 보안 위협 및 공격 유형을 정확하게 분석하여 이를 대처할 수 있는 방안들을 연구하는 것이 필요하다. VANET은 정보가 쉽게 노출될 수 있는 이동 차량 통신 환경이라 보안이 더욱 중요하며 정보보호 기술의 개발이 이러한 문제를 해결하는 최선의 방법이라 할 수 있다. [3-5]

VANET 환경에서의 응용들이 안전하고 신뢰성 있게 제공되기 위해서는 가입자의 인증 및 데이터의 보호와 같은 보안성 확보가 필수적으로 해결되어야 한다. VANET는 전파를 통한 무선 환경으로 제한된 대역폭을 사용해야 하며 이동 단말기의 계산 능력의 한계, 이동성과 다양한 부가 서비스 기능의 제공 등 많은 제약 요인과 특수성이 고려되어야 한다.

또한 이동 차량과 노변장치 간의 통신뿐만 아니라 가입자와 부가 서비스 제공자간의 통신도 고려해야 하므로 기존의 보안 프로토콜 및 알고리즘을 그대로 사용할 수 없다. 따라서 무선 환경 및 차량단말기 처리능력, 그리고 사용자와 부가 서비스 제공자간의 통신을 고려한 VANET보안 프로토콜 및 알고리즘

* 경북대학교 전자전기컴퓨터학부 석사과정
** 경북대학교 산업전자전기공학부 교수
*** 경북대학교 전자전기컴퓨터학부 교수

본 연구는 교통체계 효율화 사업 "u-Transportation 기반 기술 개발" 연구단 과제의 2세부 과제 "u-TSN 통신프로토콜 및 모듈 개발"의 지원으로 수행되었음

개발이 이루어져야 한다.[3-5]

본 논문에서는 VANET에서 안전성을 제공하기 위하여 VANET에서의 보안 위협 및 공격 유형을 분석하고 대처방안을 제시한다. 또한, VANET 상에서 제공되는 대표적인 V2V 및 V2C 인증 프로토콜을 분석한다. 보안 공격은 크게 안전에 관련된 공격, 과금에 기초한 공격 그리고 프라이버시 공격으로 분류할 수 있으며 구체적인 방법으로는 위조 정보 공격, 네트워크 동작의 중단, ID 노출 공격, ID나 속도 혹은 위치 정보를 속이는 방법 등이 있다. 이러한 공격들에 대처하기 위해서는 ELP(Electronic License Plate), EDR(Event Data Recording), 안전 위치장치 등과 같은 보안 툴박스들이 활용될 수 있으며 인증, 기밀성 등의 정보보호 기술이 사용되어야 한다.

II. 보안 위협 및 공격 유형

2-1. 보안 위협

VANET 보안시스템을 구축하려면 VANET 환경에서 발생하는 보안 위협과 공격 유형을 분석하는 것이 필요하다. 본 장에서는 이러한 VANET 환경에서의 일반적인 보안 위협과 공격 유형을 분석 기술한다. VANET 환경에서 발생하는 보안 위협은 크게 안전한 메시지에 관련된 공격, 과금에 기초한 공격 및 프라이버시 공격으로 세가지로 분류할 수 있다.

안전한 메시지에 관련된 공격은 VANET 구축 후 차량 간 안전한 메시지 교환에 관련된 위협으로 중요한 문제이다. 이러한 공격 결과는 교통혼잡 뿐 아니라 치명적 사고로 생명에 영향을 줄 수도 있다.

과금에 기초한 공격은 VANET에서 toll 징수, 위치기반 서비스 과금, 보험 등의 금전적 처리가 필요하며 이는 금전적 사기의 위험이 있을 수 있다.

프라이버시 공격은 VANET의 중요한 문제 중 하나로 개인의 프라이버시에 관련된 문제이다. VANET에서는 서로간의 통신을 통하여 운전자를 추적할 수 있으며 이는 운전자의 프라이버시를 침해할 수 있다.

VANET 환경에서 구체적인 공격 유형은 위조 정보 공격, 네트워크 동작 중단, ID나 속도 혹은 위치 정보를 속이는 방법, ID 노출 공격 등이 있을 수 있으며 그 의미는 다음과 같다.[3,5]

(1) 위조 정보 공격

이 공격은 공격자가 다른 운전자의 결정에 영향을 주기위하여 차량 네트워크에 그릇된 정보를 유포하는 경우이다. 예를 들어 그림 1(a)와 같이 여러 운전자가 결탁하여 그들의 목적지에 빨리 도착하도록 도울 수 있다. 앞선 운전자가 길이 혼잡하다는 정보를 뒤의 차들에게 보내면 뒤 따르던 차들은 그들의 경로를 변경할 것이고 결탁된 뒤의 운전자는 목적지에 빨리 도착할 수 있을 것이다. 반대로 잘못된 정보로 특정한 길을 혼잡하게 만들 수도 있다. 이 공격은 안전한 메시지에 관련된 공격 위협의 한 유형이다.

(2) 네트워크 동작 중단

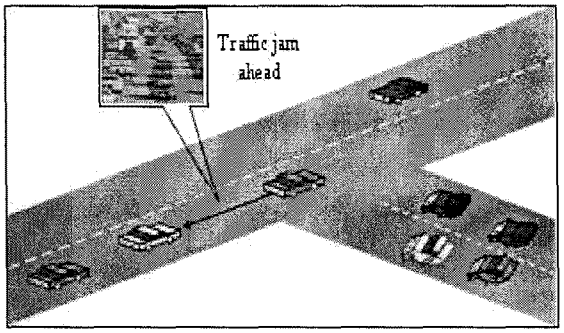
이 공격은 안전에 관련된 기능을 수행하는 네트워크를 막는 것이다. 잘못된 결과를 가질 메시지를 보내거나 무선채널 방해신호(DoS 공격)를 보냄으로 차량이 안전 메시지를 교환하지 못하게 한다. 예를 들어 그림 1(b)와 같이 악의의 공격자가 야간 운전 시 두 차량에 서로 다른 메시지를 보낸다. 한 차량은 앞에 혼잡이 있다는 경고 메시지를 받으면 속도를 줄이고 뒤따르는 다른 차량은 도로사정이 좋다는 메시지를 받아 속도를 높이면 극단적인 경우 두 차가 충돌할 수 있다. 다른 예는 무선채널상의 재밍과 같이 DoS 공격을 하여 안전에 관련되거나 과금에 관련된 정보를 주고받지 못하게 할 수 있다.

(3) ID나 속도 혹은 위치 정보를 속이는 방법

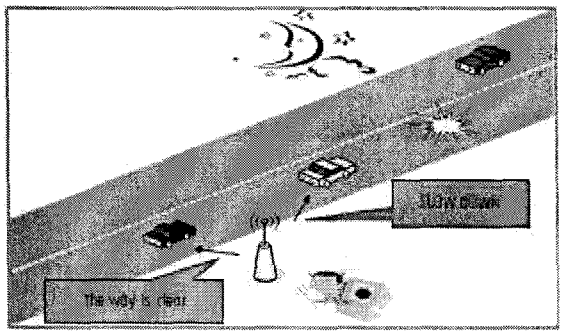
이 공격은 신뢰에 기반 한 것으로 운전자는 어떤 시간에 차의 위치에 관련된 정보를 속이고 싶어질 수도 있다. 예를 들어 그림 1(c)와 같이 한 차량이 사고가 났을 때 차가 사고가 난 그 위치에 있지 않았다고 주장하고자 위치와 속도 정보를 변조할 수 있다. 또한, 다른 사람의 ID를 사칭하여 과금에 관련된 공격을 할 수도 있다.

(4) ID 노출 공격

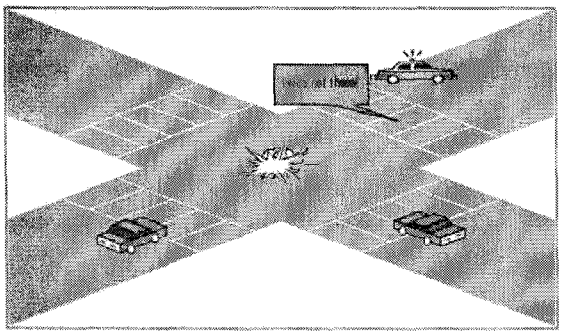
이 공격은 Big Brother 시나리오로 볼 수 있다. 그림 1(d)와 같이 글로벌 감시자는 목적된 차량의 경로와 어떤 목적의 데이터를 사용하는지 감시할 수 있다. 이를 위하여 글로벌 감시자는 목적지 부근의 차량이나 노변 구조물을 이용할 수 있다. 예를 들어, 목적지 주변에 바이러스를 퍼뜨리고 요구된 데이터를 수집할 수 있다



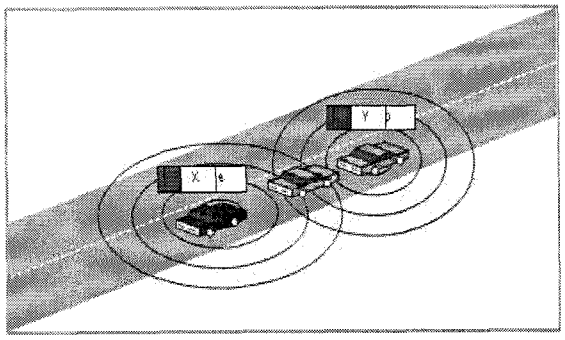
(a) 위조 정보 공격



(b) 네트워크 동작 중단



(c) ID나 속도 혹은 위치 정보를 속이는 방법



(d) ID 노출 공격

그림 1. VANET에서 발생할 수 있는 공격 유형.

2-2. 공격 유형

VANET 환경에서의 보안 취약점은 재밍(jamming), 위조(forgery), 전송 데이터 변조(tampering), 가장(impersonation), 프라이버시 침해 그리고 보드 상 변조가 가능하며 그 의미는 다음과 같다.

(1) 재밍(Jamming)

공격자는 암호학적인 메카니즘을 사용하지 않고 간섭신호를 발생하여 차량 네트워크의 수신 범위에서 통신을 방해할 수 있다.

(2) 위조(Forgery)

데이터의 정확성과 적시성은 중요하며 잘못된 정보는 차량 네트워크에 치명적인 결과를 가져올 수 있다.

(3) 전송 데이터 변조(Tampering)

한 노드가 relay로 사용될 수 있으며 이때 수신 데이터를 보내지 않거나 변경할 수 있으며 이는 위조와 마찬가지로 치명적인 위협이 될 수 있다.

(4) 가장(Impersonation)

차량 사용자를 가장하여 메시지를 위조, 변경 및 재사용 할 수 있다.

(5) 프라이버시 침해

차량 네트워크상에서 특정한 차량의 정보를 엿들을 수 있으며 이는 그 차량의 프라이버시를 침해할 수 있다.

(6) 보드 상 변조

보드 상의 하드웨어 장치를 변경시킴으로 다른 차량으로 가장 혹은 잘못된 데이터를 보낼 수 있다.

III. 보안 대처 방안

본 장에서는 VANET 환경에서의 보안 취약점 및 발생하는 공격들을 대처할 수 있는 방안에 관하여 기술한다. VANET는 전파를 통한 무선 환경으로 제한된 대역폭을 사용해야 하며 이동 단말기의 계산 능력의 한계, 이동성과 다양한 부가 서비스 기능의 제공 등 많은 제약 요인과 특수성이 고려되어야 한다.

또한 이동 차량과 노변장치 간의 통신뿐만 아니라 가입자와 부가 서비스 제공자간의 통신도 고려해야 하므로 기존의 보안 프로토콜 및 알고리즘을 그대로 사용할 수 없다. 따라서 무선 환경 및 차량단말기 처리능력, 그리고 사용자와 부가 서비스 제공자간의 통신을 고려해야 한다. VANET 환경에서의 발생하는 보안공격들을 대처할 수 있는 방안 중 하나로 보안 툴박스를 사용할 수 있으며 보안 툴박스 [5]의 종류 및 의미는 다음과 같다.

(1) ELP(Electronic License Plates)

ELP는 차량을 확인하는데 사용되며 정부기관에서 공포해야 할 사항이다.

(2) 차량 PKI(Public Key Infrastructure)

PKI는 네트워크를 위한 전형적인 보안구조이나 차량 네트워크에 사용하기에는 키 분배나 연산량 등의 문제점이 존재한다.

(3) EDR(Event Data Recording)

EDR은 비행기의 블랙 박스와 유사하게 사고와 같이 비정상적인 상황에서 발생하는 중요한 파라미터를 기록하는 장치이다.

(4) Tamper-proof 하드웨어

차량은 ELP나 차량 PKI 암/복호키와 같은 보안정보를 저장할 위조방지 하드웨어 필요하다.

(5) 데이터 상관관계

DoS 공격과 같이 가짜 정보 공격은 쉽게 노출되지 않으며 이를 막기 위하여 데이터 상관관계 기술을 이용한다. 이는 수신 정보의 신뢰성, 일관성, 적합성 등으로 정보를 결정한다.

(6) 안전 위치장치

한 차가 사고가 난 책임을 회피하려고 위치를 속이려할 때 이 기술이 필요하다. GPS가 일반적으로 자동위치 시스템이나 보안이 부족하다.

VANET에 보안서비스를 제공하기 위해서는 가입자의 인증 및 데이터의 보호와 같은 보안성 확보가 필수적으로 해결되어야 한다.

VANET는 전파를 통한 무선 환경으로 제한된 대역폭을 사용해야 하며 이동 단말기의 계산 능력의 한계, 이동성과 다양한 부가 서비스 기능의 제공 등 많은 제약 요인과 특수성이 고려되어야 한다. 또한 이동 차량과 노변장치 간의 통신뿐만 아니라 가입자와 부가 서비스 제공자간의 통신도 고려해야하므로 기존의 보안 프로토콜 및 알고리즘을 그대로 사용할 수 없다. 따라서 무선 환경 및 차량단말기 처리능력, 그리고 사용자와 부가 서비스 제공자간의 통신을 고려한 VANET보안 프로토콜 및 알고리즘 개발이 이루어져야 한다.

VANET 환경에서 차량의 인증을 수행하기 위해서는 인증기관이 차량들에게 개인/공개키를 제공해야만 한다. 향후 VANET는 전 세계적으로 확대될 것이므로 인증기관 설정 문제는 조심스럽게 접근해야하며 최근 이슈가 되고 있는 개인 프라이버시 문제도 고려되어야 한다.

IV. 인증 기술

VANET 환경에서 도로상의 사고, 위험물, 노면결빙, 응급차량 등의 정보를 신속하게 다른 차량에게 전달해야 하며 이 경우 잘못된 정보의 전달로 치명적인 사고를 유발할 수 있으므로 차량 간 전송 데이터의 인증이 필요하다. 또한, 차량 사용자 인증 및 과금을 위해서는 차량과 센터간의 인증이 필요하다. 최근 발표된 대표적인 V2V 인증 프로토콜로

는 [3]이 있으며 V2C 인증 프로토콜로는 [6]이 있으며 그 내용은 다음과 같다.

4-1. V2V 인증 프로토콜

VANET 환경에서는 차량이 고속으로 이동하므로 차량 간 데이터 전송이 일 방향으로 이루어지는 것이 바람직하며 위험 정보를 후방의 차량들에게 전송 시 목적지가 정해지지 않은 브로드캐스트로 전송하는 것이 필요하다. 본 V2V 인증 프로토콜에서는 신뢰된 인증서버(CA)를 사용하며 CA의 공개키는 모든 노드에 알려진다. 각 노드는 VANET에 들어가기 전 인증서버로부터 인증서를 요구해야 하고 인증서버는 노드의 실체를 인증한 후 인증서를 배부한다. 한 노드 S는 다음과 같이 인증서버로부터 인증서를 수신한다.

$$CA \rightarrow S : Cert_s = [S, K_{S+}, t, e]K_{CA-}$$

여기서 S는 시작노드의 주소, K_{S+}는 S의 공개키, t는 인증이 이루어진 timestamp이고 e는 인증서가 만료되는 시간이다. 이러한 인증서를 사용하면 통신 노드들이 송신 노드의 공개키를 알기 위하여 인증서버에 접속해야하는 시간을 줄일 수 있으며 VANET과 같이 고속으로 인증이 이루어져야 하는 경우에는 유용하게 활용될 수 있다.

$$\begin{aligned}
&S \rightarrow broadcast \\
&[(S,*,N,t,cert_S,M)_{K_S}] \\
&A \rightarrow broadcast \\
&[(\ (S,*,N,t,cert_S,M)_{K_{S-}}(A),cert_A)_{K_{A-}}] \\
&B \rightarrow broadcast \\
&[(\ (S,*,N,t,cert_S,M)_{K_{S-}}(A,B),cert_B)_{K_{B-}}] \\
&C \rightarrow broadcast \\
&[(\ (S,*,N,t,cert_S,M)_{K_S}(A,B,C),cert_C)_{K_{C-}}]
\end{aligned}$$

그림 2. 차량 간 일 방향 브로드캐스트 인증 프로토콜.

그림 2는 VANET에서의 차량 간 인증 프로토콜을 나타낸 것이다. 차량 간 인증을 하기 위하여 시작노드 S는 난수 N, timestamp t, 시작노드의 인증서 $cert_S$ 그리고 메시지 M을 포함하는 서명된 패킷을 방송한다. *는 방송용임을 나타내며 목적지가 있을 경우 *값 대신 목적지 주소를 사용하면 되고 N과 t는 네트워크에서 패킷이 새로운 것임을 나타낸다. 노드 B는 A의 인증서 값 $cert_A$를 확인하여 서명 값을 검사한다. B는 시작노드 S의 인증서 $cert_S$를 확인하고 수신된 경로요구 패킷의 서명 값을 확인하기 위하여 인증서 내의 키를 사용한다. 만약, 서명 값이 맞으면 이전 A의 서명 값을 제거하고 노드 리스트에 자신의 주소 B를 첨부하고 B의 서명 값을 첨가해서 패킷을 방송한다. 노드 리스트는 패킷의 경로를 알 수 있으며 필요시 중간노드의 경로 수를 제한하여 패킷의 존속경로를 정할 수 있다.

4-2. V2C 인증 프로토콜

VANET 환경에서는 사용자 인증과 과금 문제를 해결하기 위하여 V2C 인증이 필요하며 대표적인 프로토콜은 [6]에서 제안한 KCM-VAN (kiosk centric payment protocol for VANETs) 모델을 사용하며 entity 간의 메시지 교환과정에서 별도의 암호화 과정이 진행하기 위하여 [7]에서 제안한 암호화 방식을 사용한다.

본 V2C 인증 프로토콜은 시스템 초기화와 사용자 등록 과정과 결제 프로토콜로 진행된다. 시스템 초기화 및 사용자 등록 과정에서는 User P_i는 비밀키 X_i를 생성하기 위해 K_{si}를 선택하고 $x_i = g^{K_{si}}$를 계산하여 시스템 인증기관에게 X_i,와 ID_{P_i}를 전송하면 시스템 인증기관은 $K_{P_i} = (X_i - ID_{P_i})^{h(IDP_i)^{-1}} \bmod N$을 통해 P_i의 공개키를 계산하고 레지스터에 저장/클라이언트의 금융기관에 알리면 클라이언트의 임시ID(NID)를 발급하게 된다. 결제 프로토콜은 그림 3과 같이 진행된다.

클라이언트(C)는 서비스 제공자인 merchant (M)에게 자신의 임시ID(NID_C)와 TID, MID, MP를 요구하면 M은 C에게 암호화[7]를 사용하여 TID, MID, MP를 C에게 전송한다.

C는 암호화[7]를 사용하여 클라이언트의 금융기관(I)만 복호화 할 수 있도록Price, TST_C, TC, ID_M 그리고 h(OI)를 포함한 VSRequest만들고 OI, Price TST_C NID_C, ID_I를 다시 M만 복호화 할 수 있도록 암호

화하여 전송한다.

M은 전송받은 데이터의 TST_C를 통해 Timeless를 검증하여 성공하면 TST_M으로, OI를 h(OI)로 대체, TID를 추가하여 Payment Gateway(PG)만 복호화 할 수 있도록 암호화한 VCRequest를 생성하고 ID_M과 함께 PG에게 전송한다.

이를 받은 PG는 복호화 하여 해당 금액만큼 C의 거래은행에서 금액을 출금하여 M의 거래은행(A)에 금액을 입금시킨다. 은행상의 거래가 마치게 되면 거래은행은 PG에게 I가 C에게 Stt,h(OI)를 암호화 하여 전송하는 데이터를 포함한 VSResponse, Stt, h(Stt, h(OI))을 전송 이를 다시 M만 복호화 할 수 있도록 암호화한 VCReponse를 M에게 전송한다.

M은 자신의 OI 정보와 전송받은 VCReponse의 OI 정보를 비교하여 일치하지 않으면 PG에게 거래실패를 알리고 복구 과정을 진행하거나 재전송을 요구하게 되고 일치하면 전송 받은 VSResponse를 C만 복호화 할 수 있도록 PResponse로 암호화하여 C에게 전송, 거래를 마치게 된다.

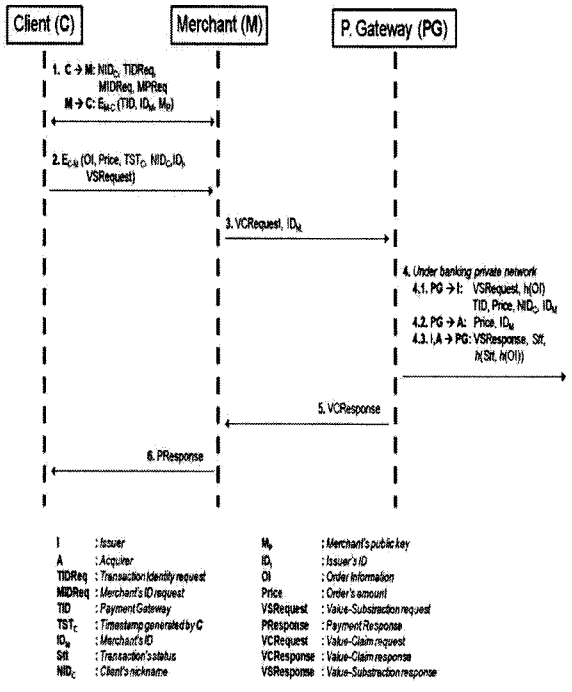


그림 3. KCM-VAN 결제 프로토콜.

결제 프로토콜은 클라이언트의 임시ID를 사용하여 익명성을 보장하고 각 entity 간의 메시지 교환 과정에 사용된 암호화[7]를 통해 메시지를 보호하고 있다. 그리고 프로토콜에서 타임스탬프를 사용하여 메시지의 freshness를 보장함으로서 재생 공격에 안전할 수 있다. Impersonating 공격에 대해서 C는 암호화[7]를 사용하여 클라이언트의 금융기관(I)만 복호화 할 수 있는 유효한 시스템 사용자로서 인증을 통과하기 위해 그 자체의 유효한 공개 키 K_{P_I}가 필요한데 만약 공격자가 가지고 있지 않으면 도청을 해야만 한다. 그리고 $h(ID_{P_I})^{-1}$를 계산하기 위해서는 p′과 q′를 알아야 하지만 이는 factoring problem이기 때문에 공격에 성공하기 어렵기 때문에 impersonating 공격은 실패하게 된다.

V. 결 론

VANET 환경에서 응용들이 안전하고 신뢰성 있게 제공되기 위해서는 보안성 확보가 필수적으로 이루어져야 한다. 본 논문에서는 VANET에서의 보안 위협 및 공격 유형을 분석하고 대처방안을 제시하였다. 구체적인 공격 방법으로는 위조 정보 공격, 네트워크 동작의 중단, ID 노출 공격, ID나 속도 혹은 위치 정보를 속이는 방법 등이 있으며 보안 공격들에 대처하기 위해서는 ELP, 차량 PK, EDR, tamper-proof 하드웨어, 데이터 상관관계, 안전 위치장치 등과 같은 보안 툴박스들이 활용할 수 있다. 또한, 본 논문에서는 VANET 상에서 제공되는 대표적인 V2V 및 V2C 인증 프로토콜들을 분석하였으며 추후 제공될 VANET 보안시스템에 활용할 예정이다. 인증 서비스는 V2V, V2I/I2V 및 V2C로 분류하여 제공되어야 하며 사용될 보안 알고리즘은 차량단말기 처리능력을 고려하여 제공되어야 한다. 차량들에게 개인/공개키를 제공하기 위해서는 인증기관이 필요하며 최근 이슈가 되고 있는 개인 프라이버시 문제도 고려되어야 한다. 이러한 VANET 보안을 견고하게 제공하기 위해서는 기술적, 경제적 및 사회적 융합 난제들이 극복되어야 할 것으로 여겨진다.

참 고 문 헌

[1] IEEE802.11, Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, 2007.

[2] Hannes Hartenstein and Kenneth P. Laberteaux "A Tutorial Survey on Vehicular Ad Hoc Networks," IEEE Communication Magazine, pp.164-171, June 2008.

[3] 나진한, 박요한, 박영호, 문상재,"디지털 서명을 이용한 차량간 브로드캐스트 인증 프로토콜,"한국정보보호학회 영남지부 학술발표회논문집, pp.71-74, 2009년 2월

[4] Maxim Raya, Panos P., and Jean-Pierre Hubaux "Secureing Vehicular Communications," IEEE Wireless Comm. Vol.13, No. 5, pp.8-15, 2006.

[5] Maxim Raya and Jene-Pierre Hubaux "Security Aspect of Inter-Vehicle Communication," Swiss Transport Research Conference, pp.1-14, March 2005.

[6] J.T.Isaac,J.S.Camara, S.Zeadally, and J.T.Marquez, "A Secure Vehicle-to-Roadside Communication Payment Protocol in Vehicular Ad Hoc Network," Computer Communications, Vol.31, pp.2478-2484, 2008.

[7] J. Zhang, W. Zou, D. Chen, Y. Wang, "On the security of a digital signature with message recovery using self-certified public key," Informatica, Vol.29, No.3, pp.343 - 346, 2005.