제33회 한국정보처리학회 춘계학술발표대회 논문집 제17권 제1호 (2010. 4)

VANET에서 CPU 성능을 보장하는 핸드오버 인증프로토콜

조신영*, 김승환*, 임헌정*, 정태명**
*성균관대학교 전자전기컴퓨터공학과
**성균관대학교 정보통신공학부
{sycho, shkim ,hjlim99}@imtl.skku.ac.kr, tmchung@ece.skku.ac.kr

Shin-Young Cho*, Seung-Hwan Kim*, Hun-Jung Lim*,
Tai-Myoung Chung**
*Dept. of Electrical and Computer Engineering, Sungkyunkwan Univ.
**School of Information Communication Engineering, Sungkyunkwan Univ

요 약

VANET에서 빠른 핸드오버를 위한 Fast MIPv6를 사용하는데 있어 Mobile Node이 다음 Access Router로 이동함에 따라 새로운 주소를 생성하고 이전주소를 새로운 주소로 교환하는 과정인 Fast Binding Update가 안전하게 수행하기 위해 핸드오버 인증 프로토콜이 사용된다. 본 논문에서는 핸드오버 인증 프로토콜 중 Kempf가 제안한 SEND기반의 핸드오버 인증 프로토콜이 Sybil 공격 및 DoS 공격에 보안상 취약하므로 생기는 CPU 성능 저하 문제를 인증과정을 수행하기 전에 Access Router의 주소 리스트를 사용하여 완화시키는 방법을 제안한다. 그로 인해 CPU 성능의 효율성을 보장하도록 한다.

1. 서론

VANET(Vehicular Ad Hoc Networks)은 차량 간의 통신을 통해 차량의 운전자에게 현 교통 상황이나, 고속도로 사고 등의 유용한 정보가 제공되어 보다 안전한 차량 운행을 할 수 있게 하고, 이외에도 이메일, 메신저, 웹 검색 등 기존 인터넷 서비스가 운전자에게 제공해주는 통신 기술이다. VANET은 차량 간 혹은 도로에 설치되어있는 RSU(Road Side Unit)와 차량 간에 무선 통신을 통해 위의 서비스를 운전자에게 제공해준다.

차량이 이동 중에도 VANET을 통해 멀티미디어 등의 서비스를 받기 위해서는 MIPv6(Mobile IPv6)기술이 필요하다. 기존의 MIPv6에서는 MN(Mobile Node)이 현재의 네트워크에서 다른 네트워크로 이동하는 핸드오버 기간 동안에 CN(Corresponding Node)에서 MN으로 패킷을 전송하게 되면 전송되는 패킷이 손실되는 문제점을 가지고 있다. 이를 방지하기 위해서 Fast MIPv6를 사용한다.

FMIPv6는 MN이 새로운 네트워크로 이동하기 전에 NAR(Next Access Router)에 대한 정보 및 새로운 동적 IPv6 주소인 NCoA(New Care-of Address)구성 등을 미리 수행함으로 핸드오버 지연과 패킷 손실을 줄이고 빠른 핸드오버를 지원하기 위한 메커니즘이다.

FMIPv6의 동작과정에서 NCoA를 설정할 때 MN이 AR에게 FBU(Fast Binding Update) 패킷을 보내어 새로운 주소를 이전주소와 바꾸는 과정을 수행한다. 이때 이 과정은 안전하게 수행되어야 한다. 그렇지 않으면 공격자가 새로운 주소 설정 과정을 악의적으로 사용하여 AR에게 DoS공격을 하거나 패킷 경로 재설정하는 등의 문제가 생길 수 있다.

FMIPv6 핸드오버 인증키 교환 프로토콜들이 이러한 문제를 해결하기 위해서 많이 연구되고 있다. FMIPv6 핸드오버 인증 기술은 AAA 인증 서버의 유무에 따라 AAA 기반과 Non-AAA 기반으로 분류될 수 있다. AAA 서버를 기반으로 하는 인증은 높은 보안성을 제공해 주지만, 핸드오버를 수행할 때마다 AAA 인증서버와 통신을 해야 한다. MN의 잦은 인증 요청으로 MN과 AAA 인증 서버 간의 인증 트래픽이 폭주하여 패킷의 지연 및 손실이 발생 할 수 있다.

Non-AAA 기반 인증 방식은 AAA서버가 없으므로 AAA서버를 AR이 대신하여 MN과 인증과정을 수행한다. MN과 AR간의 인증이 이루어지 지므로 패킷의 지연 및 손실이 적은 장점이 있지만 MN과 AR이 신뢰가 없을 때 높은 보안성을 제공하기 위해 공개키 암호 방식과 같이 인증해줄 수 있는 알고리즘을 사용해야 한다. 공개키 암호 방식은 많은 연산이 필요하므로 자원이 한정적인 이동 단말에 적합하지는 않다.

본 논문에서는 Non-AAA를 기반으로 인증하는 Kempf의 핸드오버 인증 프로토콜이 Non-AAA를 기반으로 하는 방식에서 가장 큰 보안 문제가 되는 PBS(Perfect Ba-

ckward Secrecy)를 제공하지만 Sybil 및 DoS 공격에 취약한 것을 보완하기 위한 새로운 메커니즘을 제시했다.

본 논문은 다음과 같이 구성된다. 2장에서 관련연구로써 Kempf의 핸드오버 인증 프로토콜의 절차와 특징, 인증 할 때 사용되는 SEND의 정의와 SEND에 사용되는 CGA의 주소 형식,에 대하여 살펴보고, Kempf의 핸드오버 인증 프로토콜의 보안적 안정성을 위협하는 Sybil 공격에 대해서도 살펴본다. 3장에서는 Sybil공격 및 DoS 공격으로 인해 CPU의 성능 저하를 해결하기 위한 메커니즘을 제안한다. 4장에서는 결론과 향후 연구 방향에 대해 기술하였다.

2. 관련연구

2.1 Kempf의 핸드오버 인증 프로토콜

Kempf의 핸드오버 인증 프로토콜은 공개키 연산을 사용하는 CGA(Cryptographically Generated Address)기반의 SEND(SEcure Neighbor Discovery) 방식을 사용하여 공개키 알고리즘인 RSA의 암·복호화 및 서명·검증 해시 함수를 통해 인증을 제공해준다.

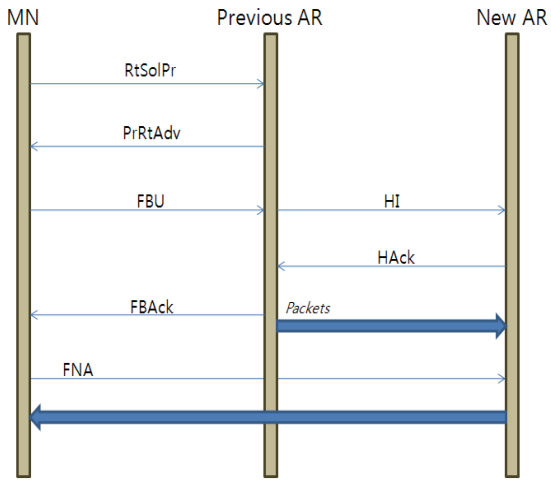
SEND의 주요기능은 이웃 탐색(Neighbor Discovery) 메시지의 송신자 주소가 실제 메시지 송신자의 주소와 일치하는 지를 증명해주고, 디지털 서명을 통한 송신자 인증과 메시지의 무결성을 제공하는 것이다. 이를 통해 공격자가 특정 노드를 사칭하여 이웃탐색 메시지 보내지 못하도록 한다. 또한 재전송 공격(Relay Attack)을 방지하기 위해, Redirect와 같은 단방향 메시지에는 타임스탬프(Time Stamp) 값을 이용하고, Solicitation/Advertisement와 같은 양방향 메시지에는 임의의 수 Nonce를 이용한다.

SEND가 기반으로 하는 기술은 디지털 서명(Digital Signature)과 CGA이다. SEND에서는 IKE(Internet Key Exchange)에 의한 키 분배를 사용하지 않고, 각 노드들이 직접 공개키를 교환한다. CGA는 각 노드들이 직접 키를 교환할 수 있도록 한다. CGA는 공개키 서명방식과 IPv6 주소를 결합하는 방식으로 IPv6에 인터페이스 ID에 해당하는 주소가 된다. IPv6 주소에서 처음 64bit는 서브넷 프리픽스 값을 설정하고, 주소에 나머지 64bit에는 인터페이스 ID 대신에 공개키와 보조 파라미터를 일방향 해시 함수로 연산하여 나온 160 bit 길이의 해시 값에 처음 64bit 사용하여 주소를 생성하여 설정한다.

검증은 수신 받은 상대방이 CGA주소를 생성할 때에 사용 했던 공개키와 보조 파라미터를 가지고 해시값을 재계산하여 인터페이스 ID 부분과 비교하는 과정을 통해 이루어진다. CGA 주소 검증을 한 후에 이웃 탐색 프로토콜 옵션인 CGA 옵션에 포함된 공개키를 이용하여 RSA Signature 옵션에 포함된 디지털 서명을 검증한다. 공격자가 자신이 생성한 개인키와 공개키로 서명한 경우에도 CGA주소에 인터페이스 ID와 해시 값을 비교하면 검증이 가능하다. 이 과정을 통해 송신노드에 대한 인증이 이뤄지고, 메시지의 무결성이 증명 된다.

이러한 SEND 방식을 인증에 사용한 Kempf의 핸드오버 인증 프로토콜은

Non-AAA기반의 Kempf의 핸드오버 인증 프로토콜은 PBS(Perfect Backward Secrecy)를 제공하지 않는 Wang의 인증 프로토콜[6]의 방법보다 안전한 인증키 교환 방법을 제공한다. Kempf의 핸드오버 인증 프로토콜은 다음 (그림 1)와 같은 절차를 가진다.



(그림 1) Kempf의 핸드오버 인증 프로토콜

핸드오버를 하기 전에 MN(Mobile Node)은 Privious AR에게 자체 내에서 공개키/개인키 한 쌍을 생성한다. 그런 후에 MN이 생성한 공개키를 RtSolPr(Router Solicitation for Proxy)에 포함시켜 Previous AR에게 보낸다. Previous AR에서는 SEND를 사용하여 RtSolPr를 검증하고, RtSolPr이 검증되면 새로운 핸드오버 인증키를 생성하여 MN이 보낸 공개키로 암호화하여 PrRtAdv(Proxy Router Advertisement)에 포함시키고, MN에게 전송한다.

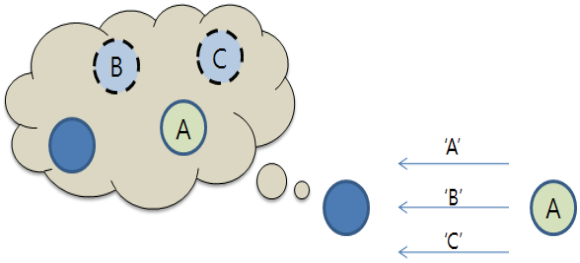
SEND로 암호화 된 PrRtAdv를 수신 받으면, MN은 먼저 SEND를 이용하여 PrRtAdv를 검증한다. MN은 자신의 공개키와 부합하는지 확인하고, 틀릴 경우 PrRtAdv를 버리고, 맞을 경우 그 공개키와 쌍으로 만들었던 자신의 개인키로 복호화를 하여 핸드오버 인증키를 획득한다. 나중을 위해 핸드오버 인증키를 따로 보관해 둔다.

MN는 핸드오버를 하기 위해 NCoA를 설정하려고 할 때, Previous AR에게 FBU(Fast Binding Update) 패킷을 보내어 이전 주소를 새로운 주소로 바꾸는 과정을 수행한다. 이때 이전에 따로 보관해둔 핸드오버 인증키로 인증을 위한 MAC을 생성하여 FBU 패킷 안에 포함 시켜 전송한다. Previous AR이 인증자가 포함된 FBU를 받으면, MN의 주소를 사용하여 MN과 공유하는 핸드오버 인증키를 찾는다. 그런 후에 새로운 인접 기지국인 New AR에게 HI(Handover Initiation) 패킷을 새로 사용할 IP주소를 포함시켜 보낸다. New AR이 HI 메시지를 받아 새로 사용할 IP 주소의 중복검사를 하여 검사에 대한 정보를 HAck(Handover Acknoledge)에 포함시켜 Previous AR에게 보내준다.

중복여부를 Previous AR이 MN에게 FBAck 메시지에 포함시켜 MN에게 전송하고, 주소가 중복일 경우에는 새로운 주소를 생성하여 위의 과정을 다시 수행하고, 중복이 아닐 경우 중복검사를 받은 주소를 사용한다.

2.2 Sybil 공격

Sybil 공격은 한 노드가 자신의 식별자를 가지고 여러 개의 식별자를 만들어 네트워크에서 사용하므로 상대방 노드로 실제 하나의 노드만 존재함에도 여러 개의 노드가 존재하는 것으로 오인하게 만드는 공격이다. 다음 (그림 2)은 Sybil 공격의 개념도이다.



(그림 2) Sybil 공격

악의적인 노드 A가 자신의 식별자로 A, B, C 세 개를 제시하여 주변의 정상적인 노드들이 실제로는 A만이 존재하는데 노드 B와 노드 C도 존재하는 것으로 오인하도록 한다.

이와 같은 경우 정상적인 노드는 노드 A, B, C가 존재한다고 오인하고 있기 때문에 A, B, C 중 우회경로를 선택하여 메시지를 보내지만 결국에는 그 메시지가 공격자에게 전달되게 된다.

3. 본론

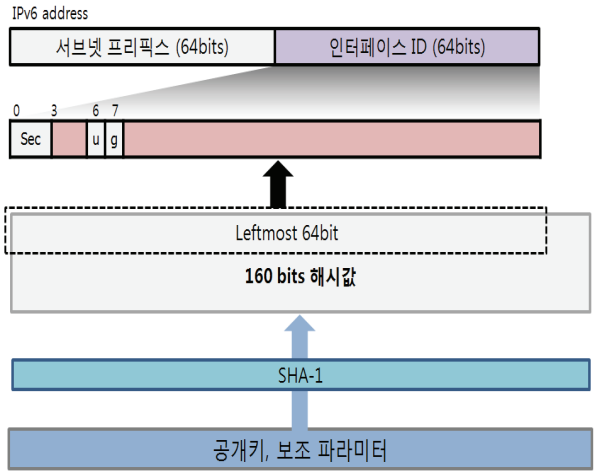
본 논문에서는 Kempf의 인증 프로토콜의 보안 위협 요소를 보완하므로 이전보다 안정적이고, 성능 면에서 효율적이도록 하였다.

3.1 Kempf의 인증 프로토콜의 문제점

Kempf의 핸드오버 인증 프로토콜은 Non-AAA를 기반으로 하는 방식에서 가장 큰 보안 문제가 되는 PBS(Perfect Backward Secrecy)를 제공한다는 면에서는 큰 장점이 있지만 SEND를 이용하여 CGA 기반으로 자체 생성된 인증서를 사용하고, 각 노드가 직접 공개키를 교환하기 때문에 Sybil 공격에 취약하다.[4]

SEND에서 CGA의 주소 형식은 오른쪽(그림 3)과 같다. IPv6 주소의 마지막 64bit에 인터페이스 ID 대신에 공개키와 보조 파라미터를 일방향 해시 함수로 연산한 값을 넣어 자체적으로 인증서를 생성한다.

공격자가 시행하는 Sybil 공격은 공격자가 CGA 기반으로 임의의 주소를 여러 개 생성하여 Previous AR로 하여금 자신의 주위에 여러 개의 MN들이 있다고 오인하도록



(그림 3) CGA의 주소 형식

한다. 공격자는 실제로 존재하지 않는 이 MN들을 이용하여 Previous AR의 CPU성능을 소모시켜 성능을 저하시키는 DoS 공격을 감행할 수 있다. 임의의 MN들에 의해 인증 요청 메시지가 다량으로 AR에게 전달이 되고, AR은 이들의 인증 요청을 처리하기 위해 RSA 서명 검증을 하고, 핸드오버 인증키를 보내주기 위해 또 다시 RSA 암호화의 과정을 수행하게 된다. 이로 인해 CPU의 성능을 소모시키게 된다.

이렇듯 Sybil 공격이 가능하고 이를 악용한 DoS공격이 가능한 것은 Kempf의 인증 프로토콜이 자체 생성된 인증서를 사용하고, 연산량이 많은 RSA연산이 기본인 SEND 프로토콜을 사용하기 때문이다.

3.2 제안 방식

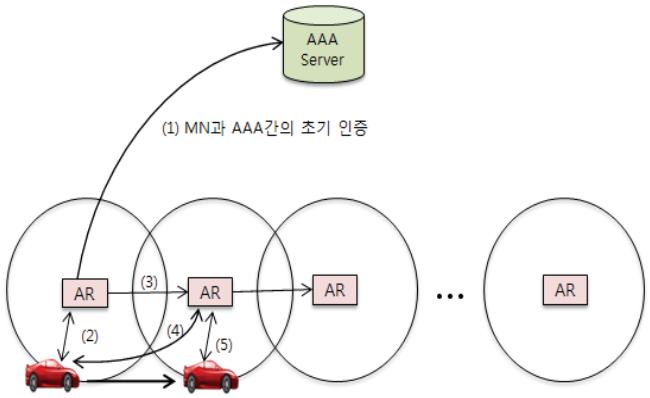
본 논문은 Sybil 공격이 발생 했을 때 대량으로 들어오는 인증 요청으로 인해 DoS와 같은 문제 발생할 경우에 대응하기 위해 현 인증 프로토콜에 새로운 메커니즘을 추가하였다. 인증 과정에서 발생하는 CGA 주소 검증과 핸드오버 인증키 전달을 위한 RSA연산의 횟수를 줄이므로 CPU의 성능저하를 보완하는 방식을 제안한다.

제안하는 메커니즘을 추가한 핸드오버 인증프로토콜의 전체적인 개요는 (그림 4)와 같다.

각 AR들에게는 pair-wise key가 미리 분배되어 있어, 서로 인접한 두 개의 AR들은 공통된 키를 보관하고 있음을 가정한다. 인증과정에서 AR간의 통신을 수행할 때에 AR이 보관하고 있는 공통의 키로 안전한 통신을 제공한다. 차량이 처음 VANET에 들어오게 되면 정상적인 MN일 경우 AAA서버와 초기 인증과정을 수행하므로 정상적인 한 노드가 여러 주소를 가질 수 없다고 가정한다.

(2)단계에서 MN은 현재 위치하고 있는 AR과 RtSolPr, PrRtAdv 패킷 전송 과정을 통해 핸드오버 인증키를 획득한다. 그런 후 MN은 다음 AR로 핸드오버하기 위해 현재 위치한 AR에게 FBU 패킷을 전송한다. FBU 패킷을 받은 이전 AR은 주소의 중복여부를 검사하기 위해 다음 AR에

게 주소 값을 포함한 HI패킷을 전송한다. 이때 이전 AR이 영역 안에 있는 모든 노드들의 주소 리스트를 HI 패킷에 포함하여 전송하는 과정이 (3)단계이다. 이전주소와 새로운 주소가 정상적으로 교환이 되면 안정적이고, 안전한 핸드오버가 진행되게 된다(4).



(그림 4) 제안 메커니즘을 추가한 핸드오버 인증프로토콜의 개요

인증과정 (5)단계부터는 AR이 CGA 주소 검증과 핸드오버 인증키 전달하는 과정을 수행하기 전에 이전 AR에게 전달받은 주소목록과 자신의 주소 목록을 체크하여 일치하는 주소 값의 존재유무를 결정한다. 일치하는 주소 값이 존재하지 않으면 악의적인 MN으로 판단하고 인증 신청을 무시한다. 그렇게 함으로 악의적인 MN이 자신의 실제 주소 외에 여러 개의 다른 주소를 생성하여 AR의 CPU 성능이 저하되도록 공격하여도 AR은 실제 주소에 대한 인증신청 과정만을 수행하고, 그 외의 인증신청은 무시하여 CPU 성능 저하를 완화시킨다.

4. 결론

기존의 FMIPv6 핸드오버 인증 기술은 AAA기반 인증기술과 Non-AAA기반 인증기술로 분류된다. 이 중에 Non-AAA기반 인증기술은 AAA서버를 이용하지 않고, MN과 Previous AR이 핸드오버 인증키를 교환하는 방식이다. 이러한 인증방식에는 CGA기반의 SEND프로토콜을 사용하여 자체적으로 주소 값을 생성하여 설정하고, AR이 MN에게 핸드오버 인증키를 전달해주는 Kempf의 핸드오버 인증 프로토콜이 있다. Kempf의 핸드오버 인증 프로토콜은 PFS와 PBS를 제공한다는 장점이 있지만 Sybil 공격 및 DoS 공격에 있어 보안상 취약하다고 알려져 있다.

이러한 보안상의 취약점은 보완하기 위해 본 논문에서는 MN과 AR간에 인증과정에서 이전 AR과 다음 AR간에 미리 분배된 pair-wise 키로 안전한 통신 환경이 제공되고, 주소 중복을 확인하기 위한 HI패킷으로 전달할 때에 이전 AR의 주소 리스트를 포함시켜 전달한다. 이 주소 리스트를 사용하여 주소 검증과 핸드오버 인증키 전달을 위한 RSA연산을 수행해야하는 주소와 무시해도 되는 주소를 판단하여 Sybil 공격 및 Dos 공격에 의해 CPU 성능이 저하되는 것을 완화시켰다.

추후의 연구과제로는 실질적인 설계, 성능평가가 이루어져야 할 것이다.

참고문헌

[1] J. Arkko, Ed, J. Kempf, B. Zill and P. Nikander "SEcure Neighbor Discovery(SEND)" RFC 3971, 2005

[2] T. Aura "Cryptographically Ggenrated Addresses (CGA)" RFC 3972, 2005

[3] J. Kempf and R. Koodli "Distributing a Symmetric Fast Mobile IPv6(FMIPv6) Handover Key Using SEcure Neighbor Discovery(SEND)" RFC 5269, 2008

[4] 최재덕, 정수환 "빠른 이동성을 지원하는 VANET 환경의 핸드오버 인증 프로토콜" 전자공학회, 2008

[5] J. R. Douceur "The Sybil Attack" IPTPS 2002, LNCS 2429, pp251~260, March 2002

[6] H. Wang and AlRl Prasad "Fast Authentication for Inter-domain Handover" ICt 2004, LNCS 3124, pp. 973-982, 2004

[7] R. Koodli, ed. "Fast Handovers for Mobile IPv6", IETF, RFC4068, 2005