Journal of Convergence for Information Technology
Vol. 9. No. 6, pp. 13-18, 2019
e-ISSN 2586-4440
DOI : https://doi.org/10.22156/CS4SMB.2019.9.6.013

사물인터넷과 모바일 IP의 융합을 위한 효율적 인증 메커니즘

이윤정[1], 조정원[2], 김철수[1], 이봉규[1*]
[1]제주대학교 전산통계학과 교수, [2]제주대학교 컴퓨터교육과 교수

Efficient Authentication for Convergence of IoT and Mobile IP

YunJung Lee[1], Jungwon Cho[2], Chul-Soo Kim[1], Bong-Kyu Lee[1*]
[1]Professor, Department of Computer Science and Statistics, Jeju National University
[2]Professor, Department of Computer Education, Jeju National University

요 약 본 논문은 제한된 컴퓨팅 파워와 자원을 갖는 IoT 와 Mobile IPv6 (MIPv6) 환경에서, 모바일 기기와 홈에이전트/대응노드 간의 바인딩 업데이트 메시지에 효율적이고 안전한 쌍방향 인증 프로토콜 제안한다. 이 프로토콜은 MIPv6의 메시지 교환에 기반으로 하여 최소한의 수정으로 통신주체 양쪽에 대하여 최적화된 인증과 공개키 교환을 동시에 만족한다. 최소한의 메시지교환으로 쌍방향 인증이 가능하며, 인증을 위한 교환 메시지 수를 최소화하였고, ECC 공개키 기반 키쌍을 사용으로 각각 노드에서의 연산양이 적으며 교환되는 메시지 크기가 작아서 네트워크 부담도 기존의 연구들에 비해 상대적으로 적다. 향후에는 본 논문에서 제안하는 프로토콜을 구체적으로 구현하여 성능분석 연구를 진행할 예정이다.

주제어 : MIPv6, Binding, 인증, IPSec, IKE, 사물인터넷, 보안

Abstract This paper proposes efficient and secure two-way authentication protocol for binding update messages between mobile devices and home agents / correspondent nodes in IoT and Mobile IPv6 (MIPv6) environments with limited computing power and resources. Based on the MIPv6 message exchange, the proposed protocol satisfies both the authentication and the public key exchange optimized for both sides of the communication with minimum modification. In the future, we will carry out a performance analysis study by implementing the proposed protocol in detail.

Key Words : MIPv6, Binding, Authentication, IPSec, IKE, IoT, Security

1. 서론

미래 인터넷은 현재보다 더 확대된 유비쿼터스 모바일 인터넷 환경을 제공할 것이다. 이동성의 지원은 새로운 영역에 대한 미래 인터넷의 적용 가능성을 증가시키고 있다. 스마트폰이나 태블릿 등의 모바일 플랫폼은 유비쿼터스 위치, 상황 인식, 소셜 네트워킹 및 환경과의 상호 작용을 기반으로 엄청난 범위의 응용 프로그램을 가능하게 하고 있다.

미래 인터넷의 잠재력은 스마트폰에만 국한되지 않는다. 사물인터넷(IoT)는 진화된 인공지능과 현실 세계에 대한 통합을 한 차원 더 높이는 미래 인터넷의 새로운 영역이다. IoT의 주요 목표는 실제 개체와 이벤트에서 데이터를 수집하는 것이다.

이동성이 보장되어야하는 사물에 IoT 장치를 부착하여 실제 환경에서 사용하는 시나리오의 예(ex, 사람 몸에 부착된 IoT 바이오센서 등)는 무수히 많다. 따라서 이동성과 동적 시스템을 다루는 것이 IoT 솔루션의 핵심 요구 사항이며 따라서 적절한 지원이 제공되어야 한다. 이러한 IoT 기기는

* This work was supported by the research grant of Jeju National University in 2017.
*Corresponding Author : Bong-Kyu Lee(bklee@jejunu.ac.kr)
Received May 17, 2019
Revised May 31, 2019
Accepted June 20, 2019
Published June 28, 2019

전력소비, 계산, 통신, 메모리 등에서 제한된 자원과 환경에 놓여있을 경우가 많다. 본 논문에서는 이러한 IoT 기기의 이동성을 지원하기 위한 프로토콜인 Mobile IPv6 (MIPv6)[1]에 안전성과 보안을 제공하는 방법을 제시하고자 한다.

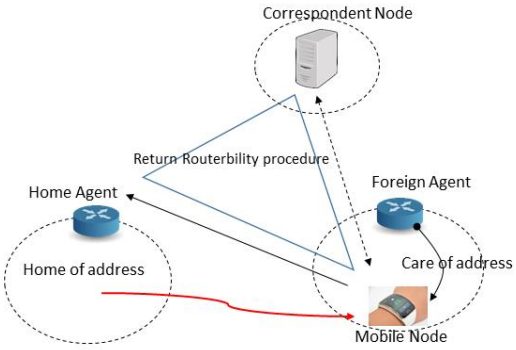

Fig. 1. Mobile Node Mobility on MIPv6 : Mobile Node get care of address from Foreign Agent as moving to Foreign Agent area, and it happen Binding update exchange between Mobile Node and Correspond Node

MIPv6는 차세대 프로토콜인 IPv6기반 위에서 이동성을 위한 표준을 부가하는 체계로 이루어지고 있다[2, 3]. Fig. 1은 MIPv6에서 모바일 노드(Mobile Mode, MN) 인 경우의 시나리오를 보여주고 있다. MIPv6의 기본 구성 요소는 MN, 대응노드(Correspondent Node, CN), 홈 네트워크 (Home Network), 홈 에이전트(Home Agent, HA), Home of Address (HoA), Care of Address (CoA)이다. 본 논문의 관심영역은 MN의 CoA와 HoA를 HA에 알려주기 위한 Binding Update 에 효율적인 경량 인증 방법을 제공함에 있다. Binding Update 과정 중, 공격자는 CoA 변조, 재전송공격, 중간자공격, DoS 공격 등을 가할 수 있다[4]. 이를 효과적으로 방어하기 위한 방법으로 IPSec을 들 수 있는데, 저전력, 적은 메모리 등 제한된 가용성을 갖는 IoT 기기가 모바일 노드나 대응노드(CN) 인 경우, 많은 시스템 자원과 네트워크 자원을 사용하는 IPSec[5, 6]을 이용한 인증과 보안은 실질적으로 적용이 힘들다.

본 논문은 이러한 환경의 Mobile IPv6 (MIPv6)에서 바인딩 업데이트 메시지의 양방향 인증 기능을 위한 보안 프로토콜을 기술한다. 여기서, MN과 CN은 자신의 공개키와 HoA를 개인키를 통해 해시함으로써, MN의 HoA 소유권을 인증할 수 있고, 중간자공격도 예방할 수 있다. 또한, Time Stamp를 통해 재전송공격도 예방할 수 있다. 본 논문은 MIPv6의 메시지 교환에 기반하여 최소한의 수정으로 통신 주체 양쪽에 대하여 최적화된 인증과 공개키 교환을 동시에 만족시키는 프로토콜을 제안한다.

본 논문의 구성은 다음과 같다. 제 2장에서는 이동성 관리 기술과 이동성 업데이트를 위해 고려해야하는 보안요구사항에 대해 설명하고 관련연구에 대해 살펴본다. 제 3장에서는 본 논문에서 제안하는 프로토콜에 대해 설명한다. 제 4장에서는 제안된 프로토콜에 대한 안전성 분석과 기존연구들과의 비교분석을 통해 안전성과 효율성을 증명한다. 마지막으로 제 5장에서 결론을 맺는다.

2. 보안이슈와 관련연구

2.1 바인딩 업데이트 보안문제

MIPv6에서의 바인딩 업데이트에는 모바일 노드 MN이 이동한 네트워크에서 받은 CoA를 홈 에이전트 HA에게 등록하는 경우와 경로 최적화를 위해 자신의 CoA를 대응노드 CN에게 알리는 두 가지 경우가 있다[7].

Binding Update 에서 발생할 수 있는 보안 문제는 다음과 같다.

첫 번째, CoA 나 HoA 변조로 인한 중간자 공격. (1) CoA를 변조: 어떤 MN가 HA로 Binding Update 메시지를 전송할 때, 공격자는 해당 Binding Update 메시지를 가로채서 CoA를 변조하여 해당 MN 의 현 위치에 대한 잘못된 정보를 줄 수 있다. 만약 HA가 이 정보를 수신한다면, 해당 MN은 패킷을 받지 못하고 대신, 다른 노드가 원치 않는 패킷을 수신하게 된다. (2) HoA 변조: CN 으로 Binding Update 메시지를 전송할 때, 악의를 가진 MN이 자신의 HoA를 희생자(victim)의 HoA로 설정을 변조하여 거짓 정보를 전송할 경우, CN이 이 정보를 받아들인다면, CN이 희생자로 전송하고자 하는 패킷이 공격자 MN을 거치게 되므로 공격자 MN은 가용성(availability)와 기밀성(confidentiality)를 모두 위협한다.

두 번째, DoS 공격. 공격자 MN이 자신의 CoA를 거짓으로 전송하는 경우, CN은 모바일 노드로 보내는 패킷을 모두 변조된 CoA로 전송하여 DoS 공격을 할 수 있다. CN으로 의미 없는 Binding Update 메시지를 한꺼번에 다량 전송할 경우에는 CN에서 그 메시지가 유효하지 않음을 눈

치 채기 전에 자원을 고갈시켜 CN을 대상으로 DoS 공격을 할 수 있다.

세 번째, 재전송 공격: 공격자는 오래된 바인딩 업데이트 메시지를 재전송(replay) 공격으로 패킷들을 MN의 이전 위치로 전송하여 MN 이 패킷을 수신하지 못하게 할 수 있다.

이런 공격들을 막기 위해서 MN이 Binding Update 메시지를 전달할 때 HA로는 IPSec ESP 를 이용하여 패킷을 보호하고, CN으로 Binding Update 메시지를 전송할 때에는 보안 메커니즘으로 Return Routerbility (RR)을 이용하고 있다[8].

그러나 저전력, 적은 메모리 등 제한된 가용성을 갖는 IoT 기기가 MN나 CN 인 경우 많은 시스템 자원과 네트워크 자원을 사용하는 IPSec을 이용한 인증과 보안은 실질적으로 적용이 힘들다는 문제점이 있다. IPSec 의 키 교환 메커니즘인 IKE[6] 프로토콜은 많은 메시지 교환을 요구하고, 현재 진행 중인 키 교환 상대의 상태정보 저장을 필요로 한다. 상태정보 저장은 서비스 거부 공격에 악용될 수 있으며, IKE 의 다량의 지수 계산은 DDoS 공격에 대하여 취약성을 갖는다. Binding Update 보안의 이상적인 목표는 해당 HoA와 CoA의 정당한 소유자인 모바일 노드만이 <HoA, CoA>를 포함하는 Binding Update 메시지를 보낼 수 있도록 보장하는 것이다[7].

2.2 관련연구

SPAM [9]은 PMIPv6의 인증과 Hand over 절차의 인증 향상을 위한 방법을 제안하였다. PMIPv6는 네트워크기반의 이동성 관리 기술로, 모바일 노드 MN이 이동성 관리에 관여하지 않으므로 MN에 부과되는 신호 오버헤드가 감소한다. 그러나 복잡한 인증절차, 패킷손실, 보안상의 위협 등의 문제를 가지고 있다. 또한 대칭키의 사용과 해시만으로 인증지연을 제거하였으나, 여전히 IPsec 의 사용으로 오버헤드가 발생한다.

J. Lee [10]은 DMM에서 동적 터널링을 통하여, MN과 분산된 앵커 간의 안전한 인증 방법을 제안하였다. MN 의 인증을 위해 상호인증 방식의 서버 클라이언트 모델을 사용함에 따른 비용이 발생한다.

G. O'shea & M. Roe [11]은 MN과 HA 사이, MN과 CN 사이의 바인딩 업데이트에 단방향 인증을 제공하는 기법을 제안하고 있다. 그러나 해시와 공개키를 포함하는 단 하나의 인증 메시지로 인증과 무결성, 재전송공격 방지 문제를 해결하고자 하고 있지만, 상대로부터의 확인 메시지를 고려한다면 실제로는 두 개의 메시지 인증절차로 봐야하며, 상대 노드의 경우 인증이 불가능하다. 또한 DoS 공격은 고려하고 있지 않다.

본 논문은 IPSec을 사용하지 않고 제한된 IoT와 MIPv6 환경에서 사용할 수 있는, Binding Update 쌍방향 인증을 위한 보안 프로토콜을 제안한다. 여기서, MN과 CN은 자신의 공개키와 HoA 를 개인키를 통해 해시함으로써, MN의 HoA 소유권을 인증할 수 있고, 중간자공격도 예방할 수 있다. 또한, 타임스탬프를 통해 재전송공격도 예방할 수 있다.

3. 제안하는 MIPv6 쌍방향 인증 프로토콜 : Two-way Auth

본 논문은 제한된 자원을 갖는 IoT 환경을 고려하여, ECC (Elliptic curve cryptography) 공개키 방식을 사용하기로 한다. RSA 방식의 키길이는 1024 비트 정도인 반면, ECC의 키길이는 160 비트 정도로 짧고, 계산량도 RSA 보다 현저하게 적으면서도 비슷한 수준의 안전도를 제공하므로 IoT 기기에 필수적이라고 하겠다. 제안하는 프로토콜은 다음과 같은 과정으로 진행된다. 모바일 노드가 처음 초기화되면 ECC 공개키 암호방식으로 (공개키, 개인키) 쌍이 생성되어 즉시 안전한 로컬 스토리지에 저장된다.

제안하는 인증 프로토콜(Two-way Auth)이 포함된 MIPv6 의 전체적인 진행과정은 Fig. 2와 같다.

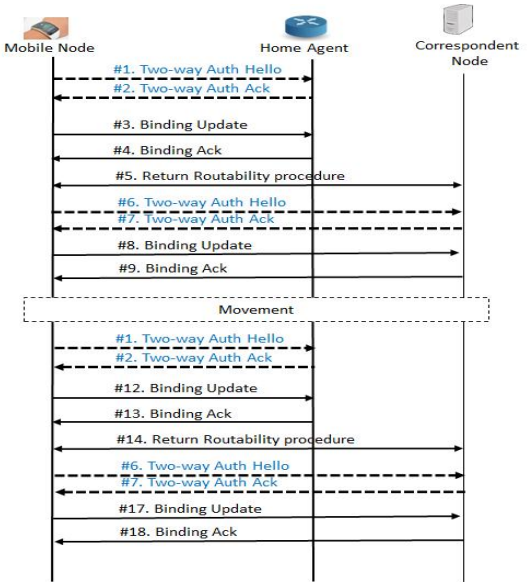

Fig. 2. Message Sequence on MIPv6 including Two-way Auth.

1. Mobile Node (MN)이 Home Agent (HA)로 바인딩 업데이트를 보내기에 앞서, MN는 HA에게 인증을 위한 Two-way Auth. Hello를 전송한다.
2 HA는 MN에게 Two-way Auth Ack 을 전송한다.
3. MN 이 HA 에게 Two-way Auth 방식으로 인증된 바인딩 업데이트 메시지를 보낸다.
4. HA 가 MN 에게 Two-way Auth 방식으로 인증된 바인딩 확인 메시지를 보낸다.
5. Correspondent Node (CN) 으로부터 MN으로의 패킷전송 요청이 들어오면, MN, HA, CN은 Route Optimization을 위하여 RR(Return Routability) 프로시저를 수행한다.
6. MN과 CN 사이의 바인딩 업데이트 과정의 인증을 위해 MN은 CN으로 Two-way Auth Hello를 전송한다.
7 CN은 MN으로 Two-way Auth Ack를 전송한다.
8. MN 이 CN 에게 Two-way Auth 방식으로 인증된 바인딩 업데이트 메시지를 보낸다.
9. CN 이 MN에게 Two-way Auth 방식으로 인증된 바인딩 확인 메시지를 보낸다.

MN의 이동으로 인해 Binding Update가 다시 실행되면 위의 과정을 반복하게 된다.

Two-way Auth 프로토콜은 <MN, HA> 사이, 혹은 <MN, CN> 사이의 바인딩 업데이트를 위한 인증에 적용된다. Route Optimization 과정의 인증과 보안은 RR 프로시저가 담당한다고 가정한다.

다음의 표기법을 사용하여 Two-way Auth 프로토콜을 기술한다 :

- A'm : MN의 CoA
- Am : MN의 HoA
- Ac : HA/CN의 주소
- (PKm, SKm) : MN의 ECC (공개키, 개인키)쌍
- H(m) : m의 해시;
- Tm : MN의 타임스탬프
- {m}SKm : m을 키 SKm로 서명한 값

Two-way Auth 프로토콜의 상세 알고리즘은 다음과 같다.

(1) Two-way Auth Hello 전송 :
MN이 HA/CN 에게 (A'm, Ac, Am, PKm, Tm, {H(A'm, Ac, Am, PKm, Tm)}SKm) 가 포함된 Two-way Auth Hello 메시지를 보낸다.

(2) HA/CN에서 MN 인증 :
① HA/CN 은 타임스탬프 Tm을 확인하여 재전송 공격을 막는다.
② {H(A'm, Ac, Am, PKm, Tm)}SKm을 MN의 공개키 PKm 으로 검증한 뒤, 자체적으로 (A'm, Ac, Am, PKm, Tm)를 해시한 값과 보내온 H(A'm, Ac, Am, PKm, Tm) 값을 비교하여 MN에 대한 인증과 메시지 무결성을 확인한다. 일치하지 않으면 메시지 전체를 무시한다.

(3) Two-way Auth ACK 전송 :
HA/CN는 (2) 과정에서 인증과정에 문제가 없으면, (PKc, Tm {H(PKc, Tm)}SKc) 이 포함된 Two-way Auth ACK 메시지를 보낸다.

(4) MN에서 HA/CN 인증 :
① MN은 타임스탬프 Tm을 확인하여 재전송공격을 막는다.
② {H(PKc, Tm)}SKc을 HA/CN의 공개키 PKc 로 검증한 뒤, 자체적으로 해시값 H'(PKc, Tm) 생성하고 보내온 H(PKc, Tm) 값을 비교하여 HA/CN에 대한 인증과 메시지 무결성을 확인한다. 일치하지 않으면 메시지 전체를 무시하고 더 이상의 바인딩 업데이트를 진행하지 않는다.

이후의 MIPv6 바인딩 업데이트와 바인딩 응답 메시지들에 대한 인증은 다음과 같다.

(1) MN은 HA/CN에게 M의 바인딩 업데이트 전체와 타임스탬프 Tm을 MN 본인의 개인키 SKm 서명하여 HA/CN에게 보낸다.
(2) HA/CN는 받은 값을 MN의 공개키 PKm 으로 검증한다.
(3) HA/CN는 (2)가 검증되면 HA/CN의 바인딩 응답 전체를 HA/CN 본인의 개인키 SKc 서명하여 M에게 보낸다.
(4) MN은 받은 값을 HA/CN의 공개키 PKc 로 검증한다.

4. 안전성 분석과 성능분석

4.1 안전성 분석

(1) CoA 위조공격

공격자는 Binding Update 에서 MN의 CoA 위조하여 하여 궁극적으로 MN으로 향하는 패킷에 대한 가로채기 공격을 가할 수 있다. 이에 HA는 Two-way Auth 프로토콜 과정에 얻은 MN의 공개키 PKm, 로 BU 메시지를 검증하고 일치하지 않으면 BU메시지를 무시하고 바인딩 캐시에 저장하지 않음으로서 CoA 공격을 막아낼 수 있다.

(2) 재전송 공격

공격자는 예전의 Binding Update 메시지를 재전송하여 현재의 MN이 아닌 다른 MN에게로 패킷이 향하게 하는 재전송 공격을 가할 수 있다. Two-way Auth 프로토콜은 Binding Update 에 타임스탬프 Tm을 포함시키고 수신측이 이 타임스탬프의 유효성을 검증하여 일치하지 않으면 패킷을 폐기한다.

(3) 중간자 공격

공격자는 MN과 HA 사이 혹은 MN과 CN 사이에서 전송되는 패킷을 가로채어 Binding Update 를 변조하는 중간자 공격을 가할 수 있다. Two-way Auth 프로토콜에서, HA나 CN은 MN의 공개키 PKm과 Tm를 가지게 되고 이를 통해 메시지 무결성을 확인하게 되며 유효하지 않으면 메시지를 폐기하므로써 이를 방어할 수 있다.

(4) DoS 공격

공격자는 한꺼번에 많은 양의 변조한 Binding Update 를 HA나 CN으로 보내어 해당 시스템을 접속 불가능 상태로 만드는 DoS 공격을 가할 수 있다. 본 프로토콜은 이에 대한 방어책은 고려하고 있지 못하다. 이를 방어하기 위해서는 IPSec의 전체적인 사용이 필요하지만, 제한적인 컴퓨팅파워를 갖는 IoT 기기 상황에서는 당장은 IPSec의 사용을 고려하기 힘들다.

4.2 성능분석

Two-way Auth 프로토콜은 공개키 방식으로 ECC 방식의 사용을 전제로 하고 있다. RSA 방식은 1024 비트 이상의 키길이를 갖는데 반해, ECC 방식은 160 비트 정도의 키길이를 갖는다. 이는 공개키를 포함하는 Two-way Auth 메시지의 길이를 전체적으로 크게 줄일 수 있으므로, 네트워크의 부담을 줄일 수 있다. 또한 한번 Two-way Auth 이 실행되고 나면, 주고받은 공개키를 계속 사용할 수 있으므로 MN이 다른 네트워크로 이동하여도 추가적인 Two-way Auth 메시지 교환은 할 필요가 없기 때문에 네트워크나 MN의 요구를 처리해야하는 HA에게 더 이상의 부담을 주지 않는다.

계산양의 측면에서 살펴보면, ECC 알고리즘을 처리하기 위한 계산량도 RSA 보다 획기적으로 줄일 수 있기 때문에 제한적인 자원과 컴퓨팅 파워를 갖는 IoT가 MN인 경우라면 Two-way Auth 프로토콜 처리에 드는 계산량은 큰 문제가 되지 않는다.

인증처리를 위한 프로토콜 메시지 수의 측면에서 보면, IPSec은 키협상과 프로토콜 파라미터들을 체결하기 위한 프로토콜로 IKEv2를 사용한다면, 이 과정에서 적어도 8번 이상의 메시지 교환이 일어나야한다. 이에 비해 Two-way Auth은 2번에 메시지교환으로 양쪽의 인증을 다 해결할 수 있다. 또한 제한적인 컴퓨팅파워를 갖는 IoT 기기는 IPSec의 사용이 불가능하다.

다음 Table 1은 본 논문의 Two-way Auth과 [9-11]을 비교한 것이다.

Table 1. Comparison of protocols

	SPAM [9]	J. Lee [10]	O'shea [11]	Two-way Auth
Authentication method	IKE /IPsec	Server-Client	One Way Auth.	Two Way Auth.
Exchange Messages	8	4	2	2
Usage of Computing Resource	very high	high	low	low
Network Overload	very high	high	low	low
Secuity Stability	very high	medium	low	high
Interoperability with IoT	low	low	medium	high

5. 결론

본 논문은 MIPv6 바인딩 업데이트 메시지들에 대한 안전성과 효율성을 제공하는 인증 프로토콜을 제안하였다. 제안하는 Two-way Auth 프로토콜은 제한된 컴퓨팅 파워를 갖는 IoT 환경에서 최소한의 메시지를 교환하므로 네트워크의 부담을 줄이고 각각의 노드에서의 계산량을 경감시킬 수 있다. 또한 모바일 기기와 대응노드는 자신의 공개키와 HoA를 개인키로 서명하므로 서 모바일 노드의 HoA 소유권을 인증할 수 있고, 중간자 공격을 막을 수 있고, Time Stamp를 통해 재전송 공격을 예방할 수 있다.

향후에는 본 논문에서 제안하는 프로토콜을 구체적으로 구현하여 성능분석 연구를 진행할 예정이다.

REFERENCE

[1] C. Perkins, D. Johnson & J. Arkko. (2011). *Mobility support in IPv6.* IETF RFC 6275.

[2] M. B. Yassein, S. Aljawarneh & W. Al-Sarayrah. (2017). Mobility Management of Internet of Things: Protocols, Challenges and Open Issues. *IEEE ICEMIS 2017.*
DOI : 10.1109/ICEMIS.2017.8273021

[3] J. Montavont, D. Roth & T. Noël. (2014). Mobile IPv6 in Internet of Things: Analysis, experimentations and optimizations. *Ad Hoc Networks, 14,* 15-25.
DOI :10.1016/j.adhoc.2013.11.001

[4] S. Choi & S. Koh. (2016). Use of Proxy Mobile IPv6 for Mobility Management in CoAP-based Internet-of-Things Networks. *IEEE Communications Letters, 20(11),* 2284-2287.
DOI : 10.1109/LCOMM.2016.2601318

[5] IPSec : *Security Architecture for the Internet Protocol,* IETF RFC 4301.

[6] Internet Key Exchange (IKEv2) Protocol, IETF RFC 4306.

[7] G. S. Lee. (2002). http://www.tta.or.kr/data/reportDown.jsp?news_num=549

[8] G. Lee, S. Lee, J. Park & Y. Kim. *Mobile IPv6 Security Issues and Solutions.* http://kidbs.itfind.or.kr/WZIN/jugidong/1050/105001.htm

[9] M. Chuang, J. Lee. & M. Chen. (2013). SPAM: A secure password authentication mechanism for seamless handover in proxy mobile IPv6 networks. *IEEE Systems Journal, 7(1),* 102-113.

[10] J. Lee. (2016). Secure authentication with dynamic tunneling in distributed IP mobility management. *IEEE Wireless Communications, 23(5),* 38-43.

[11] G. O'shea & M. Roe. (2001). Child-proof Authentication for MIPv6 (CAM). *ACM Computer Couunications Review, 31(2),* 4-8.

이 윤 정(YunJung Lee) [정회원]

- 2002년 8월 : 고려대학교 컴퓨터학과 (이학박사)
- 2004년 9월 ~ 현재 : 제주대학교 전산통계학과 교수
- 관심분야 : 정보보안, 유무선 보안
- E-Mail : rheeyj@jejunu.ac.kr

조 정 원(Jungwon Cho) [종신회원]

- 2004년 2월 : 한양대학교 전자통신전파공학과 (공학박사)
- 2004년 9월 ~ 현재 : 제주대학교 컴퓨터교육과 교수
- 2012년 12월 ~ 현재 : 한국정보과학회 전산교육시스템연구회 위원장
- 2018년 7월 ~ 현재 : 제주대학교 지능소프트웨어교육센터 센터장
- 관심분야 : 컴퓨팅 교육, 지능정보윤리, 지능형시스템, 멀티미디어
- E-Mail : jwcho@jejunu.ac.kr

김 철 수(Chul-Soo Kim) [정회원]

- 1980년 2월 : 제주대학교 수학교육과 (이학사)
- 1982년 2월 : 연세대학교 수학과(이학석사)
- 1988년 8월 : 연세대학교 수학과(이학박사)
- 1989년 4월 ~ 현재 : 제주대학교 전산통계학과 교수
- 관심분야 : 빅데이터, 데이터마이닝
- E-Mail :kimcs@jejunu.ac.kr

이 봉 규(Bong-Kyu Lee) [정회원]

- 1995년 2월 : 서울대학교 컴퓨터공학과 (공학박사)
- 1996년 3월 ~ 현재 : 제주대학교 자연과학대학 전산통계학과(교수)
- 관심분야 : 패턴인식, 인공지능
- E-Mail : bklee@jejunu.ac.kr