情報保護學會論文誌
第17卷 第1號, 2007. 2

IPv6 환경에서 해쉬 함수 기반 강건한 주소 생성 및 검증 기법*

경 계 현,† 고 광 선, 엄 영 익‡
성균관대학교

A Strong Address Generation and Verification Scheme using Hash Functions in the IPv6 Environments

Gyehyeon Gyeong,† Kwangsun Ko, Young Ik Eom‡
Sungkyunkwan University

요 약

IPv6 프로토콜은 네트워크에 참여하는 노드가 별도의 관리자 작업 없이 자동으로 주소를 생성하는 방법을 제공하며, 생성된 주소는 사용되기 전에 유일성 검증을 위하여 Duplication Address Detection(DAD) 메커니즘을 수행한다. 하지만 검증 과정에서 악의적인 노드의 공격에 의해 이미 사용하고 있는 주소로 판단되어 주소 생성이 실패할 가능성이 존재한다. 따라서 본 논문에서는 해쉬 함수를 기반으로 주소를 생성하고 검증함으로써, 빠르고 강건한 주소 생성과 및 검증 메커니즘을 보인다. 이 기법은 공항, 터미널, 회의실과 같이 많은 노드들의 무선 네트워크 참여가 빈번한 공공장소에서 SEND 메커니즘보다 더욱 효과적으로 주소 생성 및 검증을 할 수 있다.

ABSTRACT

The IPv6 protocol provides the method to automatically generate an address of a node without additional operations of administrators, Before the generated address is used, the duplicate address detection (DAD) mechanism is required in order to verify the address. However, during the process of verification of the address, it is possible for a malicious node to send a message with the address which is identical with the generated address, so the address can be considered as previously used one; although the node properly generates an address, the address cannot be used. In this paper, we present a strong scheme to perform the DAD mechanism based on hash functions in IPv6 networks. Using this scheme, many nodes, which frequently join or separate from wireless networks in public domains like airports, terminals, and conference rooms, can effectively generate and verify an address more than the secure neighbor discovery (SEND) mechanism.

Keywords : *Address Configuration, IPv6, Hash Function, DAD, Security*

접수일: 2007년 1월 16일; 채택일: 2007년 2월 7일
* 본 연구는 정보통신부 및 정보통신연구진흥원의 대학 IT연구센터 지원사업의 연구결과로 수행되었음.
(IITA-2006-C1090-0603-0027)
† 주저자, gyehyeon@ece.skku.ac.kr
‡ 교신저자, yieom@ece.skku.ac.kr

Ⅰ. 서 론

IPv6 프로토콜에서는 동일한 링크 상에 존재하는 인접 노드들 간의 관계 설정에 관련된 메시지와 일련의 절차를 정의하는 Neighbor Discovery(ND) 프로토콜을 새롭게 제시하였다.[1] 이러한 ND 프로토콜의 기능 중 일부인 DAD 메커니즘은 IPv6 네트워크에 연결된 노드가 통신을 위해 사용하는 주소를 생성한 후, 해당 주소의 유일성을 검증하기 위해 사용 되지만 악의적인 목적을 가진 노드에 의해 서비스거부공격을 받음으로써, 실패할 가능성이 있다.[2] 이러한 취약성을 해결하기 위하여 주소의 소유권 증명이 가능하도록 하는 SEcure ND(SEND) 메커니즘이 제안 되었지만, 주소 생성 및 검증에 많은 시간을 필요로 하고 있다.[3] 본 논문에서는 주소 자동설정 과정에서 생성한 주소의 유일성 검증을 위한 DAD 메커니즘을 수행할 때 해쉬 함수를 이용함으로써, SEND와 동일한 보안 수준을 제공하면서도 적은 시간이 소요되는 강건한 주소 생성 및 검증 기법을 보인다. 이러한 해쉬 함수를 이용한 주소 생성 및 검증 기법은 익명성이 요구되고 유동인구가 많은 공항과 터미널과 같이 무선 네트워크 참여가 빈번한 공공장소에서 신속하게 주소 생성 및 검증이 가능하도록 지원할 수 있다.

Ⅱ. 배경 지식 및 관련 연구

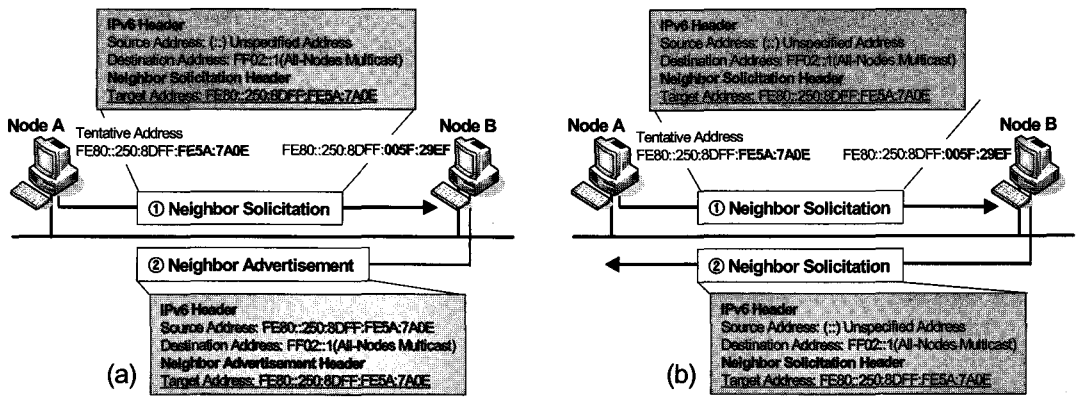
본 절에서는 ND 메커니즘의 주소 생성 및 검증을 위해 사용되는 SEND 메커니즘과 DAD 메커니즘에서의 공격 발생 가능성에 대해 자세히 설명한다.

2.1 SEND 메커니즘

비상태형 주소 자동설정 방식은 노드가 자신이 사용할 IPv6 주소를 생성한 후, DAD 메커니즘을 이용하여 생성된 IPv6 주소의 유일성을 확인하는 DAD 메커니즘을 거치게 된다.[4] 주소 생성과정의 보안을 위하여 ND 프로토콜에 다양한 보안 옵션을 통하여 보안성을 제공하는 SEND 메커니즘을 이용할 수 있다. SEND 메커니즘은 X.509 기반에서 공개키를 이용하여 주소를 생성하는 Cryptographically Generated Addresses (CGA) 방식을 사용하며, 이러한 CGA 주소를 사용한 메시지를 수신한 노드는 해당 주소의 공개키에 해당하는 인증서를 통하여 해당 메시지를 전송한 노드의 주소에 대한 소유권을 검증할 수 있다.[5] 하지만 한번의 CGA 주소 생성에 P3-696MHz 시스템에서 평균 1.7964초라는 상당히 고비용이 요구되며 이는 휴대형 단말기를 이용한 무선 네트워크 환경에서 해결해야할 매우 중요한 문제이다.[6] 또한 소유권 검증 과정에도 많은 시간이 소요된다.

2.2 DAD 메커니즘에서의 서비스거부공격

DAD 서비스거부공격은 새로운 노드가 네트워크에 진입하기 위해 주소를 생성하는 단계에서 수행되는 공격으로, DAD 메커니즘에서 사용하는 ND 프로토콜 자체적으로 IPv6 주소에 대한 소유권을 증명할 방법을 제공하지 않는 특성을 악용한다.[7] 이러한 공격은 DAD 수행과정에서 두 가지 형태로 나타날 수 있다. 첫째로 [그림 1]에서 노드 A는 주소를 생성하여 DAD를 수행



[그림 1] DAD의 두 가지 서비스거부공격

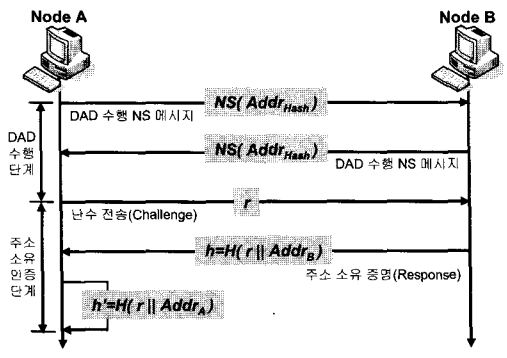
〔표 1〕 제안 기법의 세 가지 전제조건

	전제조건	표 준	제안 기법
1	IPv6 Link-local 주소 생성 방법	MAC 주소 이용	난수 사용
2	Target Address 항목	생성된 IPv6 주소	생성된 IPv6 주소의 해쉬값
3	IPv6 목적지 주소	Solicited-Node 멀티캐스트 주소	All-Node 멀티캐스트 주소

하는 노드이고, 주소가 다른 노드 B는 공격자라고 가정할 경우, 첫 번째로 〔그림 1〕(a)에서 노드 A가 DAD를 수행하기 위해 Neighbor Solicitation(NS) 메시지를 전송하면 노드 B는 노드 A가 전송한 NS 메시지의 'Target Address' 필드를복제하여 가상의 Neighbor Advertisement(NA) 메시지를 전송할 수 있으며, NA 메시지를 수신한 노드 A는 DAD 메커니즘을 실패하게 된다. 두 번째로 〔그림 1〕(b)에서 노드 A가 DAD 메커니즘을 수행하기 위해 NS 메시지를 전송하면 공격자도 동일한 NS 메시지를 전송함으로써 서로 다른 노드가 동일 주소로 DAD 메커니즘을 수행하고 있는 것으로 가장한다. 결국 DAD 메커니즘을 수행하는 노드가 자신의 NS 메시지와 동일한 NS 메시지를 받으면 절대로 해당 주소를 사용하지 못하도록 명시되어 있기 때문에 노드의 DAD 수행과정은 실패하게 된다.[3]

Ⅲ. 해쉬 함수 기반 주소 검증 기법 설계

DAD 메커니즘을 수행하는 노드가 앞에서 기술한 것과 같은 서비스거부공격에 노출되는 이유는 전송하는 NS 메시지의 'Target Address' 필드에 자신이 생성한 IPv6 주소를 평문으로 포함시키기 때문이다. 본 절에서는 이러한 사실에 착안하여 'Target Address' 필드에 설정되는 IPv6 주소를 해쉬 값으로 변환하여 적용함으로써 생성된 주소를 숨기는 방법과 주소를 검증하는 기법에 대해 상세히 기술한다.



〔그림 2〕 Challenge-Response 프로토콜

3.1 ND 메시지 변경

제안 기법이 동작하기 위해서 DAD 메커니즘을 수행하는 노드는 〔표 1〕에서 보이는 세 가지 조건에 만족하도록 NS 메시지 형식을 수정한다. 먼저 MAC 주소를 이용하여 IPv6 네트워크의 임시 링크로컬 주소를 생성하지 않고 난수를 사용한다. 두 번째는 공격자가 DAD 메커니즘을 수행하는 노드가 전송하는 NS 메시지를 보더라도 원래 주소를 알 수 없도록 하기 위해서 'Target Address' 필드에 IPv6 주소의 크기와 동일한 128비트 크기를 가지는 주소의 해쉬 값으로 대체한다. 마지막 세 번째는 Solicited-Node 멀티캐스트 주소의 하위 24 비트는 생성한 IPv6주소를 기반으로 NS 메시지는 All-Node 멀티캐스트 주소를 사용한다.

3.2 검증 기법 설계

〔표 1〕의 첫 번째 조건에 따라 네트워크에 진입하려는 노드는 난수 알고리즘 $R()$을 통하여 난수를 생성하여 주소를 구성한다. 이렇게 생성된 주소는 IPv6 임시 링크로컬 주소이며, 암호학적으로 안전한 해쉬 알고리즘인 $H()$를 이용하여 IPv6 주소를 생성한 후 NS 메시지의 'Target Address' 필드를 설정한다. 생성된 NS 메시지를 이용한 DAD 메커니즘이 정상적으로 종료하면 해당 주소를 노드에 할당한다. 이러한 과정으로 주소 설정을 마친 노드들은 DAD 메커니즘을 수행하는 또 다른 노드로부터 NS 메시지를 수신할 수 있다. 이 경우 NS 메시지의 'Target Address' 필드에 있는 해쉬 값과 자신이 DAD 메커니즘 수행 시에 생성한 해쉬 값을 비교하여 그 결과 두 값이 일치하면 NA 메시지를 전송해 해당 주소가 이미 사용 중임을 통지한다.

제안 기법에서 사용하는 해쉬 함수는 보안상 안전하기 때문에 서로 다른 주소에 의해 해쉬 값이 충돌할 가

능성은 매우 낮다. 하지만 해쉬 값이 충돌을 일으켰을 때 해쉬 값이 충돌한 원인이 주소가 동일하기 때문인지 아니면 주소는 다르지만 해쉬 값만 동일한지에 대한 판단이 필요하다. 먼저 NS 메시지에 대한 NA 메시지가 돌아왔을 경우에 송신지 주소 필드에 주소가 저장되어 있기 때문에 해쉬 값이 동일해도 송신지 주소와 자신의 주소 간 일치유무를 확인할 수 있다. 그러나 두 개 이상의 노드가 동시에 DAD 메커니즘을 실행하여 동일한 해쉬 값을 가진 NS 메시지가 전송되었을 경우는 송신지 주소를 알 수 없으므로 해쉬 값이 충돌한 원인의 구분을 위해서 [그림 2]에서 보이는 바와 같이 추가적인 Challenge-Response 인증 과정을 수행한다. 즉 노드 A가 생성한 주소의 해쉬 값 $Addr_{Hash}$을 이용하여 DAD 메커니즘 수행을 위한 NS 메시지를 구성하여 전송하고, 노드 A의 DAD 메커니즘이 종료되기 전에 노드 A가 전송한 NS 메시지와 내용이 동일한 NS 메시지를 노드 B가 전송하면, 해쉬 값이 충돌하게 되고 노드 A는 노드 B의 실제 주소 소유 여부를 확인하기 위해 Challenge-Response 프로토콜을 추가로 수행한다. 이때 노드 A는 주소 인증에 사용할 난수 r을 포함한 Challenge 메시지를 노드 B로 보내게 된다. 노드 B는 노드 A로부터 받은 난수 r과 자신의 주소 $Addr_B$를 이용하여 h를 구하여 노드 A에게 Response 메시지를 전송한다.

노드 A는 자신이 생성한 난수 r과 자신의 주소 $Addr_A$를 이용하여 h'를 구하고 노드 B로부터 받은 h와 비교하여 다르다면 해쉬 값은 충돌했지만 실제 주소는 다르기 때문에 DAD 메커니즘을 정상적으로 종료하여 생성한 주소를 노드에 설정한다. 반면에 h와 h'가 동일하다면 동일한 주소를 갖고 있다는 것을 판단할 수 있으며 주소 설정은 실패하게 된다.

3.3 보안 분석

DAD 메커니즘을 대상으로 발생할 수 있는 두 가지 서비스거부공격을 해결하는 절차는 다음과 같다. [그림 1](a)에서 보이는 NA 메시지를 전송하는 방식의 서비스거부공격은 표준 NA 메시지와 달리 공격자가 노드 A의 NS 메시지에 포함된 주소의 해쉬 값으로부터 원래 주소를 알아낼 수 없어 대응하는 NA 메시지를 생성할 수 없기 때문에 공격을 방지할 수 있다. 그러나 [그림 1](b)에서 보이는 공격자가 DAD 메커니즘 수행을 가장하여 동일한 내용의 NS 메시지를 전송하는 방식의 두 번째 서비스거부공격은 동일한 내용의 NS 메시지를 재전송하기 때문에 추가적으로 Challenge-Response 방법을 이용한다. 노드 A는 Challenge 메시지를 전송하고, 노드 B는 Challenge 메시지를 받지만 노드 A의 해쉬 이전의 원래 주소인 $Addr_A$를 알 수 없기 때문에 Response 메시지를 생성할 수 없으며, 본인의 주소로 Response 메시지를 생성한다 해도 해쉬 결과가 다르기 때문에 노드 A는 실제 주소는 충돌하지 않는 것으로 판별하고 정상적으로 DAD 메커니즘을 종료할 수 있다.

지금까지 설명한 두 가지 방법에 대해 공격자가 패킷에 포함된 해쉬 값에 대한 전수 공격을[8] 시도할 경우, NS 메시지 전송 후 대기시간인 1000ms[2] 내에 전수

[표 2] SEND와 제안 기법간 비교

평가 항목			SEND	제안 기법
보안성	NA 메시지 위조		대응	대응
	NS 메시지 위조		대응	대응
성 능	검증 알고리즘		RSA	해쉬 함수
	공개키 / 개인키		필요	불필요
	X.509 의 필요성		필요	불필요
	처리 속도	주소생성	$2C_{Hash}$	C_{Hash}
		소유권검증*	$2C_{Hash}+C_{cert}$	C_{Hash}
		소유권검증**	$2C_{Hash}+C_{cert}+C_{RSA}$	$C_{Hash}+C_{C\text{-}R}$

* SEND는 CGA인증만 할 경우이며, 제안 기법은 해쉬 충돌이 일어나지 않은 경우

** SEND는 CGA인증과 RSA 서명을 할 경우이며, 제안 기법은 해쉬 충돌로 Challenge-Response 사용

- C_{Hash} : 해쉬 함수 처리 비용
- C_{cert} : 인증서 관련 처리 비용
- C_{RSA} : RSA 전자서명 처리 비용
- $C_{C\text{-}R}$: Challenge-Response 처리 비용

공격이 무선기기를 이용하여 성공하기에는 현실적으로 불가능하다.

Ⅳ. 기존 기법과 비교

본 절에서는 기존에 제안되었던 SEND와 본 논문에서 제안하는 해쉬 함수 기반 주소 생성 및 검증 기법 간 비교를 실시한다. 평가 항목은 크게 보안성 항목과 성능 항목으로 분류할 수 있다.

〔표 2〕에서 보안성 항목은 DAD 메커니즘을 수행하는 환경에서 일어날 수 있는 DAD 서비스거부공격에 대해 대응 가능 여부를 기술하고 있으며, SEND와 제안 기법 모두 두 가지 공격에 대응 가능함을 알 수 있다. 성능 항목에서 검증 사용 알고리즘으로 SEND 메커니즘은 X.509 기반에서 인증서와 RSA를 사용하고 제안 기법은 해쉬 함수를 사용함을 보인다. SEND 메커니즘에서 사용하는 RSA는 그 처리속도가 대칭키 알고리즘보다 약 1.000~10,000배 정도 느리며 이는 시스템 성능의 저하를 발생시키게 된다.[9] 또한 처리 속도에서 사용 알고리즘의 차이로 SEND가 제안 기법에 비해 두 배 이상의 처리 비용을 요구하는 것을 알 수 있다.

SEND의 경우 또한 주소 검증 단계에서 X.509 기반의 인증서를 통하여 주소의 소유자를 확인하기 때문에 이 과정에서 많은 처리 시간을 필요로 한다.[10] 특히 유동인구가 많은 공공장소와 같은 노드의 무선네트워크 참여가 빈번한 환경에서 SEND 메커니즘 기반 주소 생성 및 검증 과정은 네트워크 성능저하의 주요한 원인이 될 것으로 예상된다. 반면에 제안 기법의 경우 RSA에 비해 상대적으로 매우 빠른 해쉬 함수를 이용하여 처리 시간이 적고, 사전에 키 설정이 필요 없으며, X.509를 이용할 수 없는 환경에서도 사용할 수 있는 장점이 있다.

Ⅴ. 결 론

본 논문에서 제안한 방법은 해쉬 함수를 이용해 자동으로 생성된 주소를 검증하는 기법을 제시하였다. 이 방법은 주소 자체를 숨김으로써 악의적인 노드의 공격 시도를 불가능하게 한다. 또한 SEND에서 사용되는 CGA와 RSA 전자서명에 비해 상대적으로 비용이 적기 때문에 보다 빠른 시간 내에 주소설정을 수행할 수 있으며, 특히 노드의 네트워크 진입이 빈번한 무선 네트워크 환경에서 매우 유용하게 사용될 수 있다. 그러나 주소의 소유권 증명 문제를 해결하는 방법이 아니기 때문에 DAD 메커니즘 외에 발생할 수 있는 NS/NA 메시지 위장공격을 방지할 수는 없다. 따라서 ND 프로토콜의 다른 위협 요소들에는 여전히 노출되어 있다는 한계가 있다.

참고문헌

〔1〕 T. Narten, E. Nordmarkand, and W. Simpson, RFC 2461, Neighbor Discovery for IP Version 6, Dec. 1998.

〔2〕 J. Arkko, T. Aura, J. Kempf, V. m. Mäntylä, P. Nikander, and M. Roe, "Securing IPv6 neighbor and router discovery," Proc. of the 3rd ACM workshop on Wireless Security'02, pp. 77-86, Sep. 2002.

〔3〕 J. Arkko, J. Kempf, B. Zill, and P. Nikander, RFC 3971, SEcure Neighbor Discovery (SEND), Mar. 2005.

〔4〕 S. Thomson and T. Narten, RFC 2462, IPv6 Stateless Address Autoconfiguration, Dec. 1998.

〔5〕 T. Aura, RFC 3972, Cryptographically Generated Addresses (CGA), Mar. 2005.

〔6〕 박기태, 김중민, 복혁구, "IPv6의 보안기능을 강화하는 Secure ND Protocol의 구현", *정보과학회논문지*, Vol. 2, No 1, Dec. 2005.

〔7〕 P. Nikander, J. Kempf, and E. Nordmark, RFC 3756, IPv6 ND Trust Models and Threats, May. 2004.

〔8〕 G. Kedem and Y. Ishihara, "Brute Force Attack on UNIX Passwords with SIMD Computer," Proc. of the 8th USENIX Security Symposium, pp. 93-98, Aug. 1999.

〔9〕 C. P. Pfleeger and S. L. Pfleeger, *Security in Computing*, Prentice Hall PTR, Dec. 2002.

〔10〕 C. Adams and S. Lloyd, "Profiles and Protocols for the Internet Public-Key Infrastructure," Proc. of the 6th IEEE Computer Society Workshop on FTDCS'97, pp. 220-224, Oct. 1997.