MANET에서 SEND를 사용한 효과적인 중복 주소 검사

김승환*, 최영현*, 임헌정*, 정태명**
*성균관대학교 전자전기컴퓨터공학과
**성균관대학교 정보통신공학부
e-mail:shkim@imtl.skku.ac.kr, yhchoi@imtl.skku.ac.kr,
hjlim99@imtl.skku.ac.kr, tmchung@ece.skku.ac.kr

Effective Duplicated Address Detection Using SEND in MANET

Seung-Hwan Kim*, Young-Hyun Choi*, Hun-Jung Lim*,
Tai-Myoung Chung**
*Dept of Electrical and Computer Engineering, Sungkyunkwan University
**School of Information and Communication Engineering, Sungkyunkwan

요 약

IPv6기반 MANET(Mobile Ad hoc Network)에서 이웃 노드를 찾기 위한 목적으로 ND(Neighbor Discovery) 프로토콜을 사용한다. ND 프로토콜의 경우 메시지 위조, 변조와 같은 취약점이 존재하기 때문에 보안성을 강화한 SEND(SEcure Neighbor Discovery) 프로토콜이 디자인되었다. 본 논문은 MANET에서 두 개의 네트워크가 병합 될 때 발생 할 수 있는 DAD(Duplicated Address Detection) Storm과 경로 상에 악의적 노드가 있는 경우에 발생하는 문제점을 해결하기 위해 SEND를 사용하였으며, 개인키를 가지고 있는 사용자만 서명할 수 있는 제한 사항을 해결하기 위해 위임 서명을 사용하였다.

1. 서론

IPv6는 인접 노드를 발견하기 위한 목적으로 ND(Neighbor Discovery) 프로토콜을 사용한다. MANET(Mobile Ad hoc Network)에서 IPv6를 사용할 경우 인접 노드를 찾기 위해 ND를 사용한다. 하지만 ND 프로토콜은 메시지 위조, 변조와 같은 보안 취약점이 존재한다. 따라서 이를 보안하기 위해서 SEND(SEcure Neighbor Discovery)란 프로토콜이 등장하였다[1]. 본 논문에서는 SEND를 이용하여 DAD(Duplicated Address Detection) Storm이 발생할 경우 이를 완화하기 위한 방법을 제안한다.

본 논문의 구성은 다음과 같다. 2장에서는 관련연구로써 SEND에 대해서 살펴보고, 3장에서는 본 논문에서 제안하는 메커니즘에 대해서 알아본다. 4장은 제안한 메커니즘에 대해 안전성을 분석하고, 마지막으로 5장에서는 결론을 맺는다.

2. 관련연구

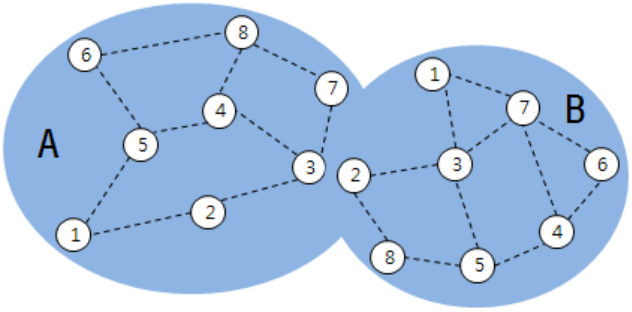
2.1 SEND(SEcure Neighbor Discovery)

SEND 프로토콜은 ND 프로토콜에 존재하는 보안 취약점을 해결하기위해 디자인되었다. CGA(Cryptography Generation Address)를 사용하여 주소를 생성하며 주소 생성 시 사용된 것을 바탕으로 주소를 검사한다[2]. DAD 메시지를 송신한 노드가 응답 메시지를 받으면 CGA 옵션에 정의되어있는 공개키로 정당한 사용자에 의해 서명이 된 메시지인지 확인한다. 이러한 과정을 통해 SEND는 기존 ND에서 발생할 수 있는 Duplicate Address Detection DoS Attack에 대응한다. 그리고 중복된 IP가 정당하게 만들어 졌는지 CGA 옵션에 정의된 매개변수를 이용하여 확인하는 과정을 거친다.

2.2 부분 위임 서명

위임 서명 방식은 서명자에 의해 선택된 위임 서명자가 서명자를 대신하여 서명할 수 있는 방식을 말한다. 그리고 부분 위임 서명 방식은 위임 서명 방식의 한 종류로 서명자가 위임 서명자를 통제하기 위한 방법을 말한다[3].

2.3 DAD Storm



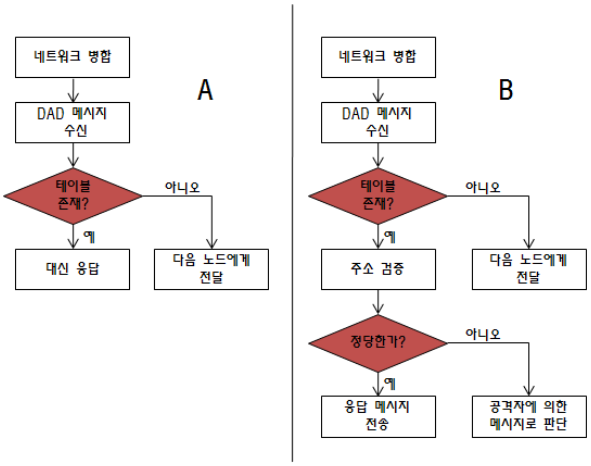
(그림 1) 다른 두 개의 네트워크가 합쳐질 경우

DAD storm 이란 (그림 1)과 같이 다른 두 개 이상의 네트워크가 병합되는 경우에 발생한다. 네트워크가 병합하면 모든 노드들은 자신이 사용하고 있는 IP의 중복 여부를

확인하기 위해 DAD를 수행한다. 따라서 병합된 네트워크에는 많은 트래픽이 발생하게 된다.

3. 본론

DAD Storm이 발생할 때 공격자가 모든 패킷에 대해 주소가 있는 것처럼 응답할 경우 많은 노드가 주소를 할당받지 못하는 문제가 생기게 된다. 본 논문에서 제안하는 메커니즘은 이러한 문제를 해결한다.



(그림 2) SEND의 사용여부에 따른 비교

A의 경우는 SEND를 사용하지 않고 테이블을 참조하여 이전 노드가 대신 응답해주는 것이다. 그리고 B의 경우는 제안하는 방식으로 테이블을 참조하며 SEND를 사용하여 대신 응답하는 경우이다. 만일 A의 경우 (그림 1)의 A네트워크 3번 노드가 악의적인 노드라면 (그림 1)의 A, B네트워크에서 DAD를 목적으로 전송된 NA(Neighbor Advertisement)메시지에 대해 위조된 NS(Neighbor Solicitation) 메시지로 응답함으로써 해당 노드가 IP를 할당 받지 못하게 할 수 있다. 따라서 (그림 1)의 A, B네트워크에 존재하는 모든 노드들은 계속 IP를 재생성하는 문제점이 발생한다. 하지만 제안하는 방식 즉, B의 경우 주소가 정당하게 생성되었는지, NA메시지가 정당한 노드로부터 전송되어 왔는지에 대해 검사한다. 예를 들어, (그림 1)의 B네트워크 6번 노드가 DAD 메시지를 전송하였고, 이를 받은 악의적인 노드는 주소가 있다고 거짓정보를 보내더라도 6번 노드는 서명 정보를 이용하여 즉시 확인이 가능하다.

이와 같이 서명을 통해 정당한 노드로부터 응답이 온 것임을 확인 할 수 있다. 따라서 IP가 중복임을 확인했을 때 응답을 하기 위해서는 서명정보가 필요하다. 하지만 대신 응답을 하는 노드는 먼저 주소를 사용하고 있는 노드의 개인키를 알지 못하기 때문에 서명을 할 수 없는 문제가 발생한다. 본 논문에서는 이 점을 해결하기 위해 위임 서명을 사용하였다. 서명자로부터 위임키를 전달받은 위임 서명자는 NS 메시지를 전송 할 때 위임키로 서명하여 전송한다. 따라서 NS 메시지를 수신한 노드는 메시지에 포함된 공개키와 주소 생성 시 사용되었던 정보를 이용하여 정당한 사용자에 의해 현 주소가 사용되고 있고, 정당한 방법으로 만들어 진 주소임을 확인할 수 있다.

4. 제안하는 방법에 대한 분석

<표 2>는 본 논문에서 제안하는 방법과 일반적인 경우와 비교를 한 표이다.

<표 2> 제안한 메커니즘과의 비교

	DAD	패킷량	DB
일반 ND사용	낮음	상	IP, MAC
대리 응답 사용	낮음	중	IP, MAC
SEND, 대리 응답 사용	높음	중	IP, MAC, 공개키, modifier, 위임키

- DAD : 중복 주소 검사 시 악의적 노드가 개입하여 IP를 할당 하지 못하게 하는 공격에 대한 방어 정도
- 패킷량 : DAD수행 시 네트워크에 발생 또는 전달되는 패킷의 수
- DB : 각 노드들이 유지 및 관리해야하는 데이터베이스의 크기

DAD의 경우 서명을 통해 NA, NS메시지가 정당한 사용자로부터 전송된 메시지임을 확인 할 수 있다. 따라서 공격자는 무작위로 IP 주소가 사용 중이라고 할 수가 없으므로 Duplicate Address Detection DoS Attack에 더 안전하다.

두 개의 네트워크가 병합될 경우 DAD Storm이 발생하더라도 각 노드들이 알고 있는 정보에 대해서 미리 응답함으로써 다음 노드로 전달하는 패킷을 줄일 수 있다.

5. 결론 및 향후 연구

MANET에서 ND를 사용할 때 중간 노드 중 공격자가 존재하는 경우가 발생할 수 있다. 이를 보안하기 위해서 본 논문에서는 SEND와 대리 응답을 사용하여 해결 하였다. 4장에서 볼 수 있듯이 제안하는 메커니즘은 공격자로부터 더 안전한 것을 확인 할 수 있다. 비록 각 노드가 유지 및 관리해야하는 데이터베이스의 크기는 다른 방법보다 크다는 단점이 있다. 하지만 이러한 단점을 지니면서 공격자로부터 안전하다는 장점이 더 크다고 볼 수 있다.

향후 연구로는 본 논문에서 제안하는 메커니즘에 대해 수치적인 성능평가를 통해 제안하는 방식의 우수성을 검증하겠다.

참고문헌

[1] J.Arkko, Ed. Ericsson et al., "SEcure Neighbor Discovery", RFC3971, March 2005.

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

[3] Mambo M, Usuda K, Okmamoto E, "Proxy signatures: delegation of the power to sign message", IEICE Transaction Functional E79-A(9), 1996