

## Secure Neighbor Discovery Protokolü

Gökhan Akın<sup>1</sup>, Mehmet Burak Uysal<sup>2</sup>, Tugay Sarı<sup>3</sup>

<sup>1</sup> İstanbul Teknik Üniversitesi, Bilgi İşlem Daire Başkanlığı, İstanbul

<sup>2</sup> İstanbul Teknik Üniversitesi, Bilgi İşlem Daire Başkanlığı, İstanbul

<sup>3</sup> İstanbul Teknik Üniversitesi, Bilgi İşlem Daire Başkanlığı, İstanbul  
akingok@itu.edu.tr, uysalmeh@itu.edu.tr, saritu@itu.edu.tr

**Özet:** IPv6 networklerinde NDP(Neighbor Discovery Protocol); ortamda bulunan diğer uçların keşfi, Link Local adreslerin temini, duplike adres kontrolü, son uçların varsayılan ağ geçidine ulaşması gibi kritik görevler üstlenmektedir. Fakat bir ağın güvenliği açısından bu derece kritik rol oynayan NDP DoS, replay, redirect, MITM(Man in the middle) vb. ataklara karşı savunmasız durumdadır. NDP nin güvenilirliği sağlanmadıkça bir ağın güvenliği tehlikeye girmektedir. SeND(Secure Neighbor Discovery) Protokolü NDP nin bu zayıflığını ortadan kaldırmak için dizayn edilmiş bir protokoldür. SeND vasıtasıyla mesajların bütünlüğü güvence altına alınır, IPv6 protokolü üzerinden yapılacak diğer ataklara karşı da daha güvenli bir ağ ortamı oluşturulmaktadır. Bu makalede SeND Protokolü ile bu güvenlik sorunlarının nasıl giderildiği ele alınacaktır.

**Anahtar Sözcükler:** IPv6, NDP, SeND, IPv6 Atakları, CGA, X.509

### Secure Neighbor Discovery Protocol

**Abstract:** IPv6 nodes use the Neighbor Discovery Protocol (NDP) to discover other nodes on the link, to determine their link-layer addresses to find routers, and to maintain reachability information about the paths to active neighbors. It is used for several critical functionalities, such as discovering nodes on the same link, determining link-layer addresses, detecting duplicate addresses, finding routers, and maintaining reachability information about path to an active neighbor. If not secured, NDP is vulnerable to various attacks such as spoofing denial-of-services (DoS), replay, redirect and rogue router attacks. Secure Neighbor Discovery (SEND) was designed to ensure message integrity, prevent IPv6 address theft and replay attacks and provides a mechanism to verify routers' authority. SEND uses cryptographically generated addresses (CGAs), a digital signature, an X.509 certification and a bunch of new implementations on to NDP to protect NDP.

**Keywords:** IPv6, NDP, SeND, IPv6 Attacks, CGA, X.509

### 1. Giriş

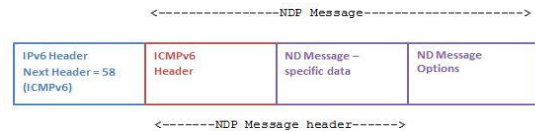
IPv4'te kullanılan ARP protokolünün yerini IPv6'da üstlenen NDP protokolünün; IPv6 ile haberleşen istemciler/yönlendiriciler arasında link-layer adreslerin tespit edilmesi ve aktif istemci/yönlendiricilerin buldukları link bilgisinin devamlılığının sağlanması gibi temel görevleri vardır. Buna ek olarak IPv6 adres çakışmasının tespitinde de NDP kullanılır. Ancak NDP birtakım MITM ataklarına (Spoofing, DoS, Replay, Redirect, Rouge Router vs.) karşı zayıftır.

Secure Neighbor Discover (SEND), NDP'deki bu zayıflıklara karşı, kriptografik üretilmiş adresler (CGAs), dijital imza, X.509 sertifikasyonu gibi birtakım güvenlik mekanizmaları getirerek IPv6 haberleşmesinde veri bütünlüğünü ve güvenliğini sağlar.

### 2. Neighbor Discovery Protokolü - NDP

NDP IPv6 ağlarında istemciler/yönlendiriciler arasında haberleşmeyi sağlayan temel yapıdır. TCP/IP İnternet

katmanında ICMPv6 mesajları kullanarak çalışır. NDP için 5 farklı ICMPv6 mesaj tipi tanımlanmıştır[2].



Şekil 1. NDP Paket Yapısı

1. Router Solicitation(RS): Yerel ağdaki istemcilerin, yönlendiricilerin tespiti ve DNS gibi bilgilerin öğrenilmesi için kullanılır. (ICMPv6 tip 133).

2. Router Advertisement(RA): RS mesajlarına cevap olarak kullanılan mesaj tipidir (solicited RA), İstemciler/yönlendiriciler periyodik olarak RA mesajı gönderirler (unsolicited RA) (ICMPv6 tip 134).
3. Neighbor Solicitation(NS): Komşu ağın ulaşılabilir olduğunun kontrolü ve istemcilerin/yönlendiricilerin link layer adreslerinin öğrenilmesi için kullanılır (ICMPv6 tip 135).
4. Neighbor Advertisement(NA): NS sorgu mesajlarına cevap olarak (solicited NA) ve komşu istemcileri/yönlendiricileri NS sorguları olmadan bilgilendirmek (unsolicited NA) için kullanılır (ICMPv6 tip 136).
5. Redirect Message(RM): Belli bir hedef için daha iyi bir yol varsa istemcileri, yönlendiricileri bilgilendirmek için kullanılır (ICMPv6 tip 137).

## 2.1 NDP Zayıflıkları

**Spoofing:** Kötü niyetli birisinin ağdaki bir istemcinin IP adresini ele geçirecek şekilde haberleşmeye dahil olmasıdır[4].

**Denial of Service:** DoS atakları sistem kaynaklarının kullanımını aşırı derecede yükselterek istemciler arasındaki ağ trafiğini engellemeye yöneliktir.

**Replay / Redirect:** Replay atağı yapan istemci, mevcut trafiğe girerek paketleri kendi üstünden replay eder, Redirect atağında ise atak yapan istemci ICMP "Time exceeded" ve "destination unreachable" mesajlarıyla yanlış bilgilendirme yapabilir. IPv6 trafiğinde, ICMPv6 RM mesajıyla yönlendiriciler kendi aralarında "first-hop" bilgilendirmesi yaparlar.

**Rogue Router:** Bilinmeyen/istenmeyen bir yönlendiricinin atak yapan kişi tarafından ağa dahil edilmesidir.

## 3. Secure Neighbor Discovery-SEND

SEND'in güvenlik konusunda NDP'ye getirdiği önlemler aşağıdaki gibidir [1]

- Kontrollü istemci/yönlendirici tespiti,
- Kullanılan adresin kullanıcının kendisine ait olduğunun doğrulanması,
- Mesaj koruması,

Ayrıca SEND varolan NDP paket yapısına ek olarak

yeni "option" ve iki yeni ICMPv6 mesaj tipi getirmiştir. Bunlar;

- Kriptografik Üretilmiş Adresler (CGAs),
- RSA İmza opsiyonu,
- **Nonce and Timestamp** opsiyonu
- **Certificate Path Solicitation(CPS)** ve **Certificate Path Advertisement(CPA)** mesajları

### 2.1.1. RSA İmza Opsiyonu

Komşu yönlendiricilerin birbirlerini tespit aşamasında iletilen mesajları korumak için RSA imzası kullanılır. SEND haberleşen iki uç arasında öncelikli olarak uygulanan RSA imzası haberleşen iki uç arasında public ve private key'ler paylaşılırak sağlanır[1].

### 2.1.2. Kriptografik Üretilmiş Adresler (CGAs) Opsiyonu

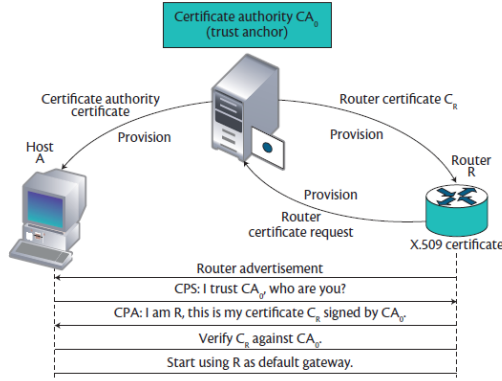
SEND ND mesajının geldiği adresin bizim haberleştiğimiz kişi olduğunu doğrulamak için CGA opsiyonunu kullanır. CGA mekanizmasıyla PKI,CA gibi üçüncü parti uygulamasına gerek kalmadan "IPv6 address authentication" sağlanmış olur.

CGA'nın dinamik olarak ürettiği IPv6 adreslerinin sol 64 bitlik yarısında, yönlendirici tarafından anons edilen alt ağ öneki, sağ 64 bitlik yarısında da CGA adres üretme mekanizmasına tabi tutulmuş kriptografik bir değer olan Interface Identifier (ID) bulunur. CGA üretimindeki parametreleri aşağıdaki gibidir[2];

- **Modifier:** 128 bitlik rastgele bir değerdir.
- **Subnet Prefix:** Yönlendirici tarafından anons edilen 64 bitlik alt ağ önekidir.
- **Collision Count:** IP çakışmasını önlemek için kullanılan 8 bitlik bir değerdir.
- **Public Key:** RSA tarafından sağlanan değişken uzunluklu anahtardır.

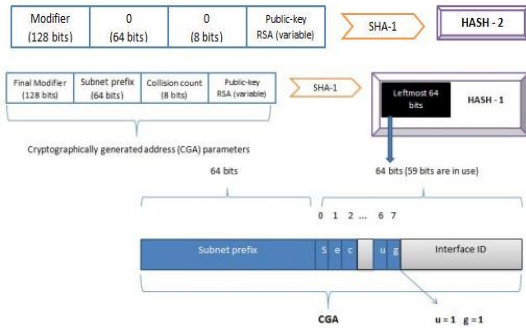
CGA üretiminde esas olan noktalardan biri "**sec**" parametresinin üretimidir. Interface Identifier'ın sol tarafında 3 bitlik bir kısım olan *sec* brute force ataklarına karşı CGA'nın dayanıklılığıyla ilgili bir parametredir. CGA ilk olarak üretimi *hash2* değerinin elde edilmesiyle başlar. Eğer *hash2* değerinin sol taraftaki  $16 * sec$  bitleri sifıra eşitse, süreç *hash1* değerini hesaplayarak devam eder, bu değer sifıra eşit değilse istemci modifier değerini 1 *hash2* değerini gerekli işlem sifıra eşit olana kadar tekrar hesaplar. 64 bitlik *hash1* değerini elde ettikten sonra Interface Identifier'ı elde etme için ilk 3 bitlik kısma *sec* bitleri getirilir, 7. ve 8. bitler ise (*u* ve *g*

bitleri) sıfıra ayarlanır. Son olarak 64 bitlik Subnet Prefix ve 64 bitlik Interface Identifier birleştirilerek CGA elde edilmiş olur[3].



Şekil 2. HASH-2 Oluşturulması

RFC'de belirtildiği üzere öntanımlı olarak SHA-1 hash algoritması kullanılmaktadır ancak başka bir algoritmada kullanılabilir. *Hash2* değeri, modifier değerindeki 9 oktet sıfır biti ve soldan sağa publik key'in konulması işleminin yukarıda bahsedilen şartı sağlayana kadar ayarlanmasıyla elde edilir. Bu hesaplama elde edilen parametreler *hash1* değerini hesaplamakta kullanılır. *Hash1* değeri final modifier, subnet prefix, collision count ve public keyin uygun biçimde ayarlanmasının ardından elde edilen sol 64 bitlik değerdir[3].



Şekil 3. CGA Oluşturulması ve Yapısı

Şekil 4. X.509 sertifika doğrulama adımları [1]

CGA üretiminde kullanılan parametreler (final modifier, subnet prefix, collision count ve public key) NDP mesaj opsiyonunda komşuluk kurulan diğer uca yollar, böylelikle komşuluk doğrulanmış olur. Sonuç olarak SEND ile haberleşmede CGA kullanılmasıdaki asıl önemli nokta kötü niyetli kullanıcının istemcilerin link layer adreslerini öğrenememesi ve kullanamamasıdır.

## Nonce ve Timesatmp Opsiyonu

Timestamp opsiyonu ND mesajlarını istenmeyen duyurulardan (unsolicited advertisements) korumak için kullanılır. 1 Ocak 1970, 00.00'dan beri saniyeleri tutan 64 bitlik bir değerdir. Nonce opsiyonu ise duyuru (advertisement) ve talep (solicitation) mesaj çeiplerinin sırasını belirlemede kullanılan rastgele bir değerdir[1].

### 2.1.3. CPS ve CPA Mesajları

CPS ve CPA mesajları SEND ile gelen iki yeni ICMPv6 mesaj tipi olup yönlendiricilerin doğrulanması ve yetkilendirilmesinde kullanılır[1]. İstemci ve yönlendirici arasında iletilen bu mesajlar, üçüncü parti bir bağlantı ile yönlendiricinin X.509 sertifika kontrolünün yapılmasına dayanır.

## 4. Sonuç

Hesaplama mekanizmasının getirdiği yük ve buna bağlı fazla bant genişliği kullanımı olmasına rağmen SEND, Kriptografik Üretilmiş Adresler (CGAs), dijital imza, X.509 sertifikasyonu gibi birtakım güvenlik mekanizmaları getirerek IPv6 haberleşmesinde veri bütünlüğünü ve güvenliğini sağlamış ve NDP'nin maruz kaldığı güvenlik sorunlarının üstesinden gelebilmiştir.

## 5. Referanslar

- [1] AlSa'deh A, Meinel C; "Secure Neighbor Discovery" IEEE Security & Privacy, Volume: 10, Issue: 4, Pages: 26-34; July-Aug 2012
- [2] Arko J, Kempf J, Zill B, Nikander P; "Secure Neighbor Discovery" RFC 3972; March 2005
- [3] Aura T; "Cryptographically Generated Addresses" RFC 3971; March 2005
- [4] Gaeil A, Kiyong K, Jongsoo J, Yonghee J; "Analysis of SEND Protocol through Implementation and Simulation"; Convergence Information Technology, 2007. International Conference; Page(s): 670 – 676; 21-23 Nov. 2007