

## **Host Identity Protokol (HIP) \***

**Zeynep Gürkaş-Aydın<sup>1</sup>, Hakima Chaouchi<sup>2</sup>, Halim Zaim<sup>1</sup>**

<sup>1</sup> İstanbul Üniversitesi, Bilgisayar Mühendisliği Bölümü

<sup>2</sup> Telecom&Management SudParis Department LOR

zeynepg@istanbul.edu.tr, hakima.chaouchi@it-sudparis.eu, ahzaim@istanbul.edu.tr

**Özet:** İnternet'in başarısı, yıllar boyunca iki adet isim alanı kullanımı (DNS ve IP adresleri) ile kullanıcıların ihtiyaçlarını gidermek için yeterli olmuştur. İnternet kullanıcılarının sayısı arttıkça, ihtiyaçlar da aynı oranda artmaktadır. Daha fazla gezginlik veya güvenlik gibi ihtiyaçlar ortaya çıkmıştır. Ne Mobile IP (gezginlik için) ne de IPsec (güvenlik için) tüm problemlere çözüm olmuştur, sadece bir yönden çözümler getirmiştir. Ayrıca, tüm çözümler TCP/IP protokolüne dayanmaktadır ve hiçbiri tamamıyla yeni bir çözüm sunmamaktadır.

Günümüz internet mimarisinde, IP adreslerinin hem konum tanımlama hem de oturum tanımlama şeklinde iki rolü bulunmaktadır. IP adreslerinin bu ikili rolü gezginlik yönetimi ve desteklenen host sayısı gibi konularda birçok problem yaratmaktadır. Bu problemleri çözmek için, IETF ve IRTF tarafından "Host Identity Protokol (HIP)" adında yeni bir protokol önerilmiştir. HIP'in temel fikri IP adreslerinin konum tanımlama ve kimlik (oturum) tanımlama prosedürlerinin ayrılmasıdır. HIP, kendi isim alanını ve doğasında bulunan güvenlik prosedürleri ile beraber ortaya çıkmıştır. Bu isim alanı, "Host Identity (HI)" adı verilen kriptografik bir anahtar olarak tanımlanabilir.

Bu makale Host Identity Protokol için bir giriş bilgisi sunmaktadır. Ayrıca, HIP'in temel prosedürlerinden, bağlantı başlatma aşamasında kullanılan Base Exchange (BE) ve yeni bir ağ bileşeni olan Rendezvous Server (RVS) tanıtılmaktadır. Son bölümde ise, güvenlik açısından HIP'e alternatif olarak sunulan Lightweight HIP tanıtılmakta ve HIP ile aralarındaki farklar belirtilmektedir.

**Abstract:** For years, Internet's success was enough for users' needs by using two basic namespaces: DNS and IP addresses. As the number of Internet users' increases, the needs also increased. The necessity of further mobility or security has revealed. None of the proposals such as Mobile IP (for mobility) or IPsec (for security) addressed the all problems, tried to solve just from one side. Also, all of them were based on TCP/IP protocol suite; there were not any completely new solution.

In today's internet architecture, IP addresses have dual role as location identification and session identification. This dual role of IP addresses has several problems such as number of hosts supported or mobility management. In order to solve these problems, IETF and IRTF proposed a new protocol called "Host Identity Protocol (HIP)". The main idea of HIP is to separate the identification and location procedures. HIP proposes a new namespace and security for host in its nature. This namespace is composed from Host Identities (HI) which is a cryptographic entity.

This paper is an introduction for Host Identity Protocol. It also includes the basic procedures of HIP such as Base Exchange for connection initiation and the new component Rendezvous Server. At the last section, an alternative proposal to HIP about its security procedures, Lightweight HIP (LHIP) is introduced and a comparison between HIP and LHIP is introduced.

**Anahtar Kelimeler:** Host Identity Protocol, HIP, Rendezvous Server, RVS, HIT.

\* Bu çalışma, İstanbul Üniversitesi Fen Bilimleri Enstitüsüne bağlı olarak yürütülen doktora tezinin bir bölümüdür ve TÜBİTAK Yurtdışı Araştırma Burs Programı tarafından desteklenmiştir.

## 1. Giriş

Host Identity Protokolü (HIP), IETF [1] ve IRTF [2] tarafından günümüz internet dünyasında karşılaşılan zorlukları çözebilmek için geliştirilen yeni bir protokoldür. Mobile IP'ye alternatif olarak, HIP doğasında güvenlik, gezginlik gibi konular için mimarisinde çözümler barındırır. TCP/IP mimarisinde ağ ve iletim katmanları arasında yer almaktadır. HIP'in varlığı ile taşıma katmanı protokolleri IP adresleri yerine kriptografik host tanımlayıcıları kullanabilmektedir. Özellikle son yıllarda artan İnternet kullanımı ve ortaya çıkan yeni ihtiyaçlar, temel TCP/IP teknolojisinin yeterli olmakta zorlandığı bir noktaya varmıştır. Kullanıcıların farklı ağlar arasında hareket edebileceği ve aynı anda farklı ağlarla bağlantı kurabileceği gerçeği zamanla ortaya çıkmıştır. Ayrıca, internetin kullanım alanı büyüdükçe birçok güvenlik problemi ortaya çıkmıştır. Güvenlik eksikliği de aynı zamanda mevcut IP gezginlik sstemlerinin gelişimini engellemiştir. HIP, bu problemlere çözüm üretmek amacıyla TCP/IP mimarisine tam olarak entegre olabilecek bir protokol olarak geliştirilmiştir [3].

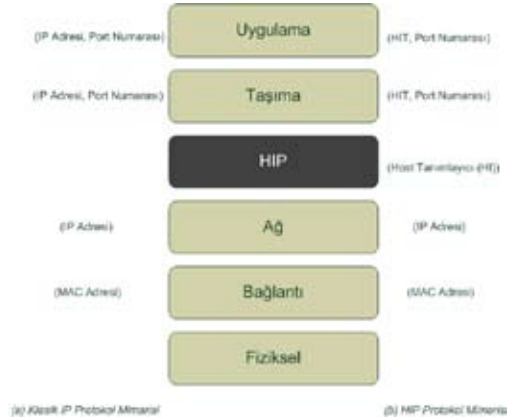
## 2. Host Identity Protokol (HIP)

Günümüz İnternet mimarisinde, IP adreslerinin iki ana görevi bulunmaktadır. Bunlardan biri konumlayıcı (locator) olması diğeri de kimlik tanımlayıcı (identifier) olmasıdır. IP adresinin konumlayıcı rolü özellikle ağ katmanında yönlendirme işlemleri için kullanılmaktadır. Bir host bir ağdan diğerine hareket ettiğinde IP adresi de değişmektedir ve hostun konumu artık bu yeni adres ile belirlenmektedir. Taşıma ve diğer üst katmanlar açısından düşünüldüğünde ise IP adresinin host'u bağlantı ve haberleşme boyunca tanımlama rolü de bulunmaktadır. Bu açıdan bakıldığında ise,

IP adresinin haberleşme boyunca değişikliğe uğraması istenmeyen bir durumdur.

IP adreslerinin ikili rolünün getirdiği problemlere çözüm olarak HIP'in önerdiği çözüm Host Identity (HI) kavramıdır. HI kısaca bir açık/gizli anahtar çiftinin açık anahtar kısmıdır. Bu anahtar genel olarak HI'nın bir 128 bit versiyonu olan Host Identity Tag (HIT) olarak gösterilebilmektedir ve tüm İnternet üzerinde benzersiz olması gerekmektedir. HI'nın diğer bir gösterim yolu de lokal amaçlarla kullanılabilen 32 bitlik Local Scope Identity (LSI)'dir.

Şekil 1'de HIP'in TCP/IP mimarisinin hangi noktasında yer aldığı ve kullanılan değerler bakımından klasik mimariye göre farklılıkları gösterilmektedir [3].



Şekil 1. HIP Protokol Mimarisi

### 2.1. İnternet İsim Alanları

İsim alanları bir host'un veya bir servisin internet ortamında benzersiz bir şekilde tanımlanmasına imkan sunarlar. Günümüz internetinde hostlar için iki adet isim alanı kullanılmaktadır: IP adresleri ve DNS alan adları. DNS alan adları kullanımı ve okunması kolay host isimleri sunmaktadır. Ancak bir host'un var olan IP adresini DNS üzerinde güncellemesi gezginlik anında

çok yavaş bir işlem olacaktır. Ayrıca bir çok host'un DNS üzerinde değişiklik yapma hakkı olmayabilir. Ayrıca DNS güvenli olmayan ve kolayca bilgileri ele geçirebilir bir servistir.

Varolan bu iki isim alanının üç ana dezavantajı bulunmaktadır.

1. Taşıma katmanındaki bağlantıları kesmeden host adresini değiştirmek mümkün değildir.
2. Host'un doğrulanması söz konusu değildir. IP adresleri dinlenerek (spoofing) ele geçirebilmektedir.
3. Gizlilik sağlayan (privacy preserving) iletişim sağlanamamaktadır.

## 2.2. Host Tanımlama Metotları

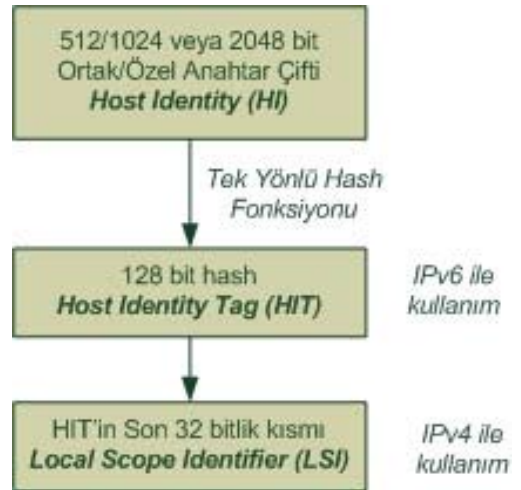
HIP, host tanımlayıcılardan (HI) oluşan yeni bir isim alanı (namespace) kavramı getirmektedir. HI'ler üst katmanlarda tanımlayıcı rolünü üstlenmektedir.

Açık anahtarın uzunluğu 512, 1024 veya 2048 bit olabilir ve genellikle RSA algoritması tarafından üretilmektedir. Yeni anahtarların üretimi zaman alıcı bir işlem olduğundan dolayı sadece eski anahtarlar gizliliği ihlal edildiğinden üretilirler. Host tanımlayıcı olarak data paketlerinde ve üst katmanlarda kullanılan açık anahtar büyük ve değişken boyutludur ve uzunluğu da kullanılan kriptografik algoritmanın tipine bağlı olarak değişebilmektedir. Bu durumun üst katmanlarda yol açabileceği problemlere engel olmak adına HIP'te iki adet sabit uzunluklu tanımlayıcı tipi tanımlanmıştır:

**a) Host Identity Tag (HIT) :** HI'nın 128 bitlik gösterimidir. HI üzerinde bir kriptografik hash fonksiyonu ile elde edilir. Hash fonksiyonunun kullanmanın iki adet avantajı bulunmaktadır. Bunlardan ilki sabit uzunluklu olması ve üst katmanlarda kullanımının daha kolay olmasıdır. İkincisi ise protokolde tutarlı bir formatta temsil ediliyor olmasıdır. HIT'ler HIP paketlerinin gönderici ve alıcılarını temsil ederler.

**b) Local Scope Identifier (LSI) :** LSI ise HI'nın genellikle 32 bitlik bir gösterimidir. Var olan API'ler ve protokoller tarafından kullanılabilir. HIT'den daha kısa olması bir avantajdır ancak sadece lokal kullanıma uygundur. Genellikle halen sadece IPv4 destekleyen uygulamalar tarafından kullanılabilir.

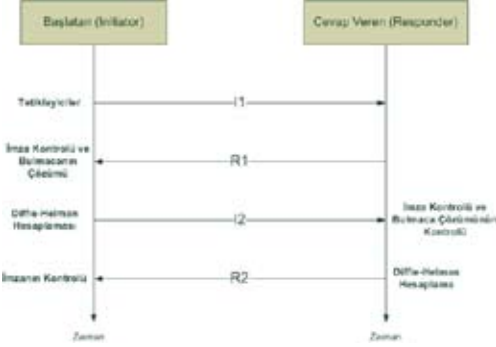
Şekil 2'de HI, HIT ve LSI parametrelerinin elde edilmesi blok şema şeklinde gösterilmektedir. HIT, IPv6 adresleri ile aynı uzunlukta olduğu için üst katman uygulamalarında rahatlıkla IP adreslerinin yerine kullanılabilir. HIT'lerin sabit uzunluklu olması, açık/gizli anahtar çiftlerinin üretilmesi için kullanılan kriptografik algoritmayı protokolden bağımsız duruma getirmektedir. LSI ise, HIT'in son 32 biti ile oluşturulabilen bir tanımlayıcıdır. Daha kısa uzunluklu oldukları için, farklı iki ortak anahtardan aynı iki tanımlayıcının oluşma olasılığı HIT'e göre daha fazladır. Bu yüzden LSI'ların kullanımı lokaldir ve benzersiz olarak tanımlanamazlar.



Şekil 2. HI, HIT ve LSI'nin elde edilmesi

HIP Base Exchange (BE), iki host arasında bir HIP bağlantısı kurulmadan önce gerçekleştirilen bir kriptografik anahtar değişim prosedürüdür, bir başka deyişle dört yönlü bir el sıkışmadır. Bu el sıkışmayı başlatan host Başlatan (Ini-

tiator), diğer host ise Cevap Veren (Responder) olarak tanımlanmaktadır. BE, dört mesajdan (I1,R1,I2,R2) meydana gelmektedir ve klasik bir Diffie-Hellman anahtar değişimi gerçekleştirir. Şekil 3'de dört yönlü BE prosedürü gösterilmektedir.



Şekil 3. HIP Base Exchange

**I1 Paketi :** BE, I1 paketinin bağlantıyı başlatan host tarafından gönderilmesiyle başlar. I1 mesajı bir HIP bağlantısı başlatmak için bir tetikleyici olarak da tanımlanabilir. I1 paketi BE prosedüründe şifrelenmeyen veya imzalanmayan tek pakettir. Kendisinin ve eğer biliniyorsa karşı taraftaki host'un HIT'ini içerir.

**R1 Paketi :** I1 paketini alan host, paketteki HIT değerinin kendi HIT değeri ile uyup uymadığını kontrol eder ve HIP bağlantısının kurulmasını kabul edip etmeyeceğine karar verir. Eğer kabul edecekse R1 paketini yollar ve bu paket, BE'nin devam etmesi için iletişimi başlatan host'un çözmesi gereken bir bulmaca içerir. Bulmacanın amacı, cevap verecek olan hostun DoS ataklarından korunmasını sağlamaktır. Ayrıca bu paket Diffie-Hellman anahtar değişiminin ilk kısmını da içerir. Bu paketin bulmaca kısmı hariç diğer kısımları imzalanmıştır.

**I2 Paketi :** BE'yi başlatan host tarafından alınan R1 paketinden sonra, bir önceki adımdaki bulmacanın çözümünü ve Diffie-Hellman anahtar değişiminin bir sonraki kısmını I2 paketi ile karşı hosta yollar. I2 paketinin tamamı imzalı

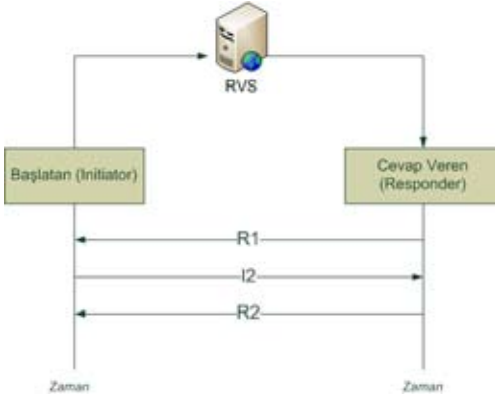
halde gönderilmektedir. Cevap veren host, I2 paketinden başlatan hostun Diffie-Hellman ortak anahtarını elde eder ve Diffie-Hellman oturum anahtarını hesaplar ve böylece bir HIP bağlantısının kurulacağını onaylar.

**R2 Paketi :** BE'yi sonlandıran pakettir. Tüm HIP paketine ait bir imza içerir. Bu pakete bağlantıyı başlatan hostu tekrar (replay) saldırılarından korumak için ihtiyaç duyulmaktadır [4,5].

#### 2.4. Rendezvous Server (RVS)

Bir HIP hostunun erişilebilir olması için IP adresinin bir noktada saklanması gerekmektedir. Günümüzde genel olarak bu saklama işlemi için DNS sunucuları kullanılmaktadır. DNS sistemiyle ilgili problemler ise daha önceki bölümlerde belirtildiği gibi, gezginlik durumunda konum bilgisinin güncellenmesinde gecikmeler meydana gelmesi ve sistemin yavaş olmasıdır. Bu problemi çözmek amacıyla, HIP protokolü ile beraber yeni bir ağ elemanı tasarlanmıştır. Randevu Sunucusu (Rendezvous Server [RVS]) adı verilen bu eleman HIP haberleşmesi ile ilgili her türlü detayı saklamaktadır. Sadece RVS'nin konum bilgisi DNS sunucularında saklanmaktadır. Birbirleri ile HIP protokolü ile haberleşmek isteyen hostlar bağlı oldukları RVS'lere HIT'leri ve o anki IP adresleri ile kayıt olmak zorundadır. Şekil 4, RVS'nin varlığında BE prosedürünün nasıl gerçekleştiğini göstermektedir [6].

RVS tüm hostların ağ içinde erişebileceği ortak bir nokta durumundadır. Bir host (I) iletişim kurmak istediği diğer bir host (R) ile BE başlatmak istediğinde I1 paketini direkt olarak karşı hosta değil RVS'ye yollamaktadır. Host I, RVS'nin IP adresini DNS aracılığıyla öğrenir ve RVS'ye BE'yi başlatmak için I1 paketini yollar. Bu durumda RVS, gelen paketin HIT'inin kendi kayıtlarında kontrol eder ve eğer varsa bu paketi ilgili IP adresine yollar. Bu adımdan sonra BE'nin diğer mesajları RVS'ye gerek duymaksızın direkt olarak host I ve host R arasında gönderilir.



Sekil 4 : RVS'nin varlığında HIP Base Exchange

## 2.5. HIP'te Gezinlik ve Çoklu Konumluluk (Mobility and Multi-Homing)

Bir host o an bağlı olduğu ağ içinde veya başka bir ağa hareket ettiğinde IP adresi değişmektedir ve bu adresi bağlı olduğu diğer hostlara HIP UPDATE paketleri içinde LOCATOR parametresi ile haber vermektedir. Bu UPDATE paketi HIP protokol kurallarına göre gönderilir. ESP protokolünün varlığında ise karşılıklı hostlardan biri karşılıklı güvenlik bağlantısını yeniden kurmak ve hatta yeni bir Diffie-Hellman anahtarı üretmek isteyebilir. Tüm bu işlemler UPDATE paketinin içinde bulunan ek parametrelerle yollanan bilgiler dahilinde tetiklenir.

Çoklu Konumluluk (multi homing) özelliğine sahip bir HIP hostu, farklı erişim ağlarına erişebilen farklı arayüzler için birden çok IP adresine sahiptir. Ağdaki konumunu belirten birden çok adresi olduğu için de, haberleşmek istediği tüm diğer hostlara bu adresleri haber vermelidir. Bunu gerçekleştirmek için, UPDATE mesajları içinde LOCATOR bilgilerini bildirir ve hatta tercih ettiği adresi konusunda da bilgilendirebilir. Birden çok adres içeren bir UPDATE mesajını alan bir host, olası yanlış güncellemeleri önlemek için bu adreslerinin her birinin erişilebilirliğini kontrol etmek durumundadır [7].

## 3. HIP ve Güvenlik

HIP, hostları tanımlamak ve bilgiyi şifrelemek ve bütünlüğünü korumak amacıyla kullanılan anahtarları üretmek için ortak anahtar kriptografisi kullanılmaktadır. Ancak, ortak anahtar kriptografisi yüksek güvenilirlikle beraber özellikle az kaynaklara sahip cihazlar için göz ardı edilemez bir hesaplama yükü ile beraber gelmektedir ve bu durum HIP'in küçük cihazlarda kullanılmasını zorlaştırmaktadır. Lightweight HIP (LHIP), HIP'in küçük cihazlarda da rahatça kullanılabilmesi için önerilmiştir. LHIP, bilginin şifrenmesi ve host doğrulama kısımlarını, HIP kontrol paketleri için bütünlük sağlanmasını daha az hesaplama maliyeti ile gerçekleştirmek adına göz ardı etmektedir. Böylece, az kaynaklı cihazların da HIP'in gezinlik ve çoklu konumluluk (multi-homing) özelliklerini kullanmasını sağlamayı amaçlamaktadır [4,8].

### 3.1. Lightweight HIP (LHIP)

HIP'in güvenli iletişim için paketlerin bütünlük koruması için kullandığı yöntemler ortak anahtar kriptografiye dayanmaktadır. Hostlar, Hash Mesaj Doğrulama Kodalarını (Hash Message Authentication Codes (HMACs)) ve anahtarlar için de doğrulanmış Diffie-Hellman (DH) anahtar değişimini kullanır. Ayrıca bazı paketlerin de şifrenmesi için RSA veya DSA algoritması kullanılmaktadır. HIP'in ortak anahtar kriptografiye olan bağımlılığını azaltmak için, LHIP HIP kontrol mesajlarını doğrulamak için yeni bir metot önermektedir. Bu metotlar genellikle kriptografik hash fonksiyonlarına ve tek yönlü hash zincirlerine dayanmaktadır. Bu doğrulama yönteminin temelini interaktif hash zincirleri (IHC) ve tek kullanımlık imzalar oluşturmaktadır.

LHIP'in doğrulama fonksiyonları temel HIP'e görünmezdir ve katman olarak HIP'in altında yer alır. HIP verilerinin korunma işlemi LHIP'e bırakılmıştır. Bu yüzden LHIP, HIP'in kontrol paketlerini koruma özelliğini iptal eder. HIP, korunmayan kontrol paketlerini LHIP'e

yollar ve LHIP de gerekirse kendi doğrulama mekanizmalarını devreye sokar. Ayrıca, korunamayan (payload) ve korunması gerekmeyen paketler de mevcuttur. Şekil 5'te LHIP'in TCP/IP Veri (Korunmasız) katmanları arasındaki mevcut yapısı gösterilmektedir.



Şekil 5. LHIP Protokol Mimarisi

LHIP ve HIP, aynı isim alanını paylaşırlar fakat LHIP bazı özel durumlar hariç HI'leri doğrulamaz. Bu durum, LHIP'e, HIP isim alanını aşırı ortak anahtar kriptografi hesaplamaları yapmadan kullanması için izin verir. Bir LHIP bağlantı kurulumu ise HIP bağlantı kurulumuna benzerdir. Haberleşmek isteyen iki host öncelikle yine dört yönlü el sıkışma şeklinde olan Base Exchange (BEX) işlemini gerçekleştirirler. Ancak isminden de anlaşıldığı gibi LHIP'de, BE'deki tüm adımlar hesaplama yükünü azaltmak amacıyla modifiye edilmiştir. LHIP'in bir bağlantıyı istediği zaman normal bir HIP bağlantısına çevirme şansı mevcuttur. Kısacası LHIP, HIP'in yerini almaya bir protokol değil, HIP'i genişleten bir protokoldür [8].

### 3.2. HIP ve LHIP'in Güvenlik Amaçları

#### 3.2.1. HIP'in Amaçları

##### 1. Veri Güvenliği (Payload Security) :

HIP tarafından iletilen bir verinin içeriğine erişim sadece o HIP bağlantısını paylaşan hostlara özel olmalıdır. İki host güvenli olmayan iletişim kanalları üzerinden güvenli bir şekilde veri gönderilebilirler.

##### 2. Protokol Güvenliği (Protocol Security) :

Güvenli bir protokol, iletişim boyunca meydana kasıtlı veya kasıtsız meydana gelebile-

cek hataları önleyebilmeli ve keşfedebilmelidir. Protokol güvenliği sadece haberleşen hostlarla sınırlı değildir, aynı zamanda haberleşme kanalı ve iletişime doğrudan veya dolaylı yoldan katılan tüm ara düğümler ve ağ elemanları ile de ilgilidir.

**3. İsim alanı Güvenliği (Namespace Security) :** HIP ile hostlar arasında güvenilir haberleşmenin sağlanması ve hostların üvünlü bir şekilde tanımlanması amaçlanmaktadır. İsim alanı da hatalı kullanımdan korunmalıdır. Ayrıca, HIP kimlik hırsızlığı ve kimlik taklitçiliğinden (impersonation) korunmalıdır.

Daha önceki bölümlerde de bahsettiğimiz gibi, farklı güvenlik tekniklerinin kombinasyonu ve kriptografik protokoller ile bu amaçlara ulaşma sağlanmaktadır. Bu amaçlara ulaşmak için HIP ağırlıklı olarak ortak anahtar kriptografiye dayanan yöntemler kullanılmaktadır. Protokol güvenliği RSA ve HMAC imzalar ile sağlanmaktadır. HMAC algoritmasının kullandığı gizli anahtar ise Diffie-Hellman anahtar değişimi tarafından sağlanmaktadır. Bu anahtar değişimleri de RSA imzaları tarafından korunmaktadır. HIP'te veri güvenliği ise ESP enkapsülleme ve simetrik şifreleme anahtarları (D-H) ile sağlanmaktadır. Kısacası veri güvenliği, ESP protokolüne, Diffie-Hellman anahtar değişimine ve RSA imzalarına dayanmaktadır. İsim alanı güvenliği ise RSA imzalarına dayanmaktadır. Tüm bunlardan anlaşılacağı gibi HIP'te, üst seviye amaçların sağlanması bahsedilen tüm güvenlik mekanizmalarının birbirlerini tamamlamasıyla mümkündür. Aralarından birinin çıkarılması diğer tüm güvenlik amaçlarını etkileyecektir.

#### 3.2.2. LHIP'in Amaçları

**1. Yüksek Performans :** Zayıf cihazlar için daha yüksek performans için ortak anahtar kriptografinin kullanımı azaltılmaktadır. Özellikle BE ve gezginlik durumunda kullanıcıların yeni konum bilgilerinin güncellenmesi kısmında uzun gecikmeler olabilmektedir.

**2. Protokol Güvenliği :** LHIP'de sağlanan

protokol güvenliği sağlanmalıdır. Protokole yapılabilecek saldırılar günümüzde TCP/IP'ye yapılan saldırı sayısından daha kötü olmamalıdır.

**3. İsim alanı Güvenliği :** Belirli bir kapsamda sağlanmalıdır. Doğrulama olmasa dahi , bir LHIP bağlantısı boyunca kimlik taklitçiliği yapılmasına izin verilmemesi gerekir.LHIP isim alanı çakışmalarına çözüm bulabilmelidir.

**4. Uyumluluk :** HIP ile belirli bir kapsamda uyumlu olmalıdır. İsim çözümleme gibi servisler LHIP ve HIP tarafından ortak kullanılabilir. LHIP, HIP ile benzerlikler göstermeli ve gezginlik ve çoklu konumluluk anlamında hizmet sağlayabilmelidir. HIP'in uyumlu olduğu uygulamalarla uyum sağlayabilmelidir. LHIP bağlantıları istenildiği zaman HIP bağlantısına yükseltilebilmelidir.

LHIP, hesaplama maliyetini azaltmaya çalışırken, HIP'in birinci ve ikinci amaçlarını sürdürse de üçüncü amacı göz ardı etmektedir. Yüksek performansa sağlayabilmek için veri güvenliği göz ardı edilmektedir. LHIP, hesaplama maliyetini azaltmak için ortak anahtar kriptografi işlemlerinin miktarını azaltmayı önermektedir. LHIP, Diffie-Hellman anahtar değişimini ve buna bağlı olarak da paketleri doğrulamak veya şifrelemek için bir anahtar veya HMAC kullanamaz. Bu yüzden, simetrik anahtarlarla dayanmayan iletim protokolleri kullanmak durumundadır. HIP verisi için hiçbir bütünlük mekanizması kullanılmamaktadır. Tüm güvenlik, doğrulama ve bütünlük yöntemleri kontrol mesajları için geçerlidir. Ortak anahtar imzalarını kullanarak hostların tanınması işlemi gerçekleştirilemez ancak LHIP bağlantısı kurlumu sırasında karşılıklı hostlardan istenen bilgiler doğrultusunda doğrulama gerçekleşebilir. LHIP, BEX boyunca ortadaki adam saldırılarına karşı bir koruma sağlayamaz ancak BEX'den sonra bu tip saldırılara karşı özellikle konum güncellemeleri sırasında koruma sağlayabilmektedir. Bu da özellikle sık sık yer değiştiren mobil cihazlar için oldukça önemli bir özelliktir [3,8].

#### **4. Sonuç**

Bu makalede Host Identity Protokol (HIP) hakkında genel bilgiler verilmiş ve HIP'in güvenlik mekanizmalarından bahsedilmiştir. HIP halen gelişmekte olan ve üzerinden çalışılmakta olan bir protokoldür. HIP'in taşıma ve ağ katmanları arasında yeni bir katman olarak tasarlanması sebebiyle, tam olarak kullanıma geçebilmesi için mevcut sistem üzerinden bir takım değişikliklerin yapılması gerekmektedir. Bu durum kısa vadede uygulama düzeyinde bir takım problemlere sebep olabilecektir. HIP'in getirdiği yeni isim alanı HI ve bu kayıtları tutacak olan RVS sunucusunun verimliliği HIP'in genel çalışma performansında oldukça etkili olacaktır. Gezinlik anlamında ise, makro gezginlik konusunda Mobile IP'nin görevini yerine getirebilmektedir ve Mobile IP'ye alternatif olarak tasarlanmıştır ancak mikro gezginlik anlamında helen eksiklikleri bulunmaktadır ve bu konuda çeşitli çalışmalar devam etmektedir. LHIP ise, HIP'in hesaplama yükü getiren kriptografik işlemleri üzerinde köklü düzenlemeler yapan ve bu şekilde zayıf mobil cihazlar üzerinde de çalışmasını hedefleyen bir protokoldür ve henüz tasarım aşamasındadır.

#### **Kaynaklar**

- [1]IETF, Internet Engineering Task Force, <http://www.ietf.org/>
- [2]IRTF, Internet Research Rask Force, <http://www.irtf.org/>
- [3] "Host Identity Protocol (HIP)-Towards the Secure Mobile Internet", Andrei Gurtrov, Wiley Publications.2008
- [4] RFC 5201, "Host Identity Protocol", R. Moskowitz ,P. Nikander, T. Henderson, April 2008
- [5] RFC 4423, "Host Identity Potocol (HIP) Architecture", R. Moskowitz, P. Nikander, May 2006

[6] RFC 5204, "Host Identity Protocol (HIP) Rendezvous Extension", J. Laganier, L. Eggert, April 2008

[8] Internet Draft, "LHIP Lightweight Authentication Extension for HIP", T. Heer, February 2007

[7] RFC 5206, "End-Host Mobility and Multihoming with the Host Identity Protocol", P. Nikander, , T. Henderson, C. Vogt, J. Arkko, April 2008