IPSec Benzetim Yazılımı: Tasarım ve Gerçekleme

Umut Tekin [1] İbrahim Soğukpınar [2]

[1,2] Bilgisayar Mühendisliği Bölümü, Gebze Yüksek Teknoloji Enstitüsü, Kocaeli
[1] e-posta: umuttekin@uekae.tubitak.gov.tr [2] e-posta: ispinar@bilmuh.gyte.edu.tr

Özetçe

IPSec, IP haberleşme protokolü üzerine tanımlanmış standart güvenlik mimarisidir. Artan güvenlik ihtiyaçları ve IP'nin kullanımının yaygınlaşması ile birlikte IPSec'in de kullanımı artacaktır. IPSec güvenlik mimarisinin kullanımının artmasıyla beraber mevcut ağ protokolleri ve algoritmaları ile IPSec'in ortak kullanımına ilişkin hem güvenlik hem de ağ performansı alanlarında yeni araştırma konularının ortaya çıkacağı açıktır. Aynı zamanda günümüzde bilgisayar ağları üzerine yapılan çalışmalar için benzetim ortamları yadsınamaz bir gereksinim haline gelmiştir. Bu çalışma kapsamında IPSec üzerine yapılacak bilimsel ve endüstriyel çalışmalara altyapı olabilecek bir IPSec modelleme yazılımı gerçeklenmiş ve bu makalede yazılımın tasarımı, yetenekleri ve avantajları anlatılmıştır.

1. Giriş

Günümüz bilgisayar ağlarında temel olarak kullanılan iletişim protokolü IP'dir ve IPSec [1] ; ağ katmanında IP protokolü için tasarlanmış yaygın kullanımlı standartları oturmuş bir güvenlik mimarisidir. IPv4 için zorunlu olmayan IPSec, IPv6 protokolüyle birlikte tüm ağ cihazlarda şart koşulmuştur. Gelişen IP teknolojisi ile birlikte her geçen gün güvenlik ihtiyaçları artmakta ve IPSec protokolün kullanımı yaygınlaşmaktadır. IPSec protokolünün kullanımın artmasıyla beraber bugün için düşünülmeyen birçok alanda yeni araştırma konularının ortaya çıkacağı açıktır.

Özellikle bilgisayar ağları gibi dağıtık sistemlerde yapılan çalışmaların gerçek hayatta denenmeden önce benzetim ortamlarında denenmesi artık vazgeçilmez bir gereksinim haline gelmiştir. Günümüzde, gerçek dünyada denenmesi kimi zaman imkânsız veya yüksek maliyetli çalışmalar, ilk önce benzetim ortamlarında yapılmaktadır. Ancak yapılan araştırmalar sonucunda güncel ve yaygın kullanımlı bir IPSec benzetim altyapısının olmadığı görülmüştür. Çok yaygın kullanıma sahip olan OMNET++ [2] ve NS-2 [3] benzetim ortamında herhangi bir IPSec benzetim modülü bulunmazken, ulaşılabilen en kapsamlı çalışmanın NIST IPSec and IKE Simulation Tool(NIIST) [4] olduğu görülmüştür ki bu çalışmanın 2003 yılında durdurulmuş olduğu ve halen geliştirme aşamasında bekletildiği gözükmektedir.

Bilgisayar ağları üzerine benzetim ortamında yapılan çalışmalarda en büyük gereksinimlerden biri de, benzetim ortamının hali hazırda desteklediği mevcut modelleme zenginliğidir. Yapılan bir çalışmanın en nihayetinde mevcut protokoller ve algoritmalar ile birlikte çalışabilirliğinin ölçülmesi gerekmektedir. Örneğin; ağ üzerinde gezginlik ile ilgili yapılan bir çalışmanın yönlendirme protokollerini nasıl etkileyeceği çok önemlidir. Bu sebeple modellemenin yapılacağı benzetim ortamı, zengin kütüphanelere sahip olmalıdır. Akademik çevrelerde sıklıkla kullanılan ve zengin modelleme kütüphanelerine sahip NS-2 ve OMNET++ benzetim araçları çalışma kapsamında incelenmiş ve bir sonraki bölümlerde anlatılacak bazı avantajları nedeniyle uygulamalar için OMNET++ benzetim ortamı seçilmiştir.

Bu çalışma kapsamında esnek ve geliştirilebilir bir IPSec benzetim modellemesi ve gerçeklemesi yapılmıştır; böylece IPSec üzerine yapılacak bilimsel ve endüstriyel çalışmalara altyapı olabilecek bir benzetim altyapısının oluşturulması amaçlanmıştır. Bu kapsamda öncelikle IPSec protokolünden ve modellemenin gerçeklendiği OMNET++ benzetim ortamından bahsedilmiştir. Ardından IPSec protokolünün yazılımsal özellikleri ve benzetim modellemeleri anlatılarak avantajları ortaya konulmuştur. Sonuç bölümünde ise yapılan örnek modelleme ve ölçümler ortaya konularak ileriki çalışmalar anlatılmıştır.

2. IPSec ve Ağ Benzetim Yazılımları

IPSec, IP ağlarının güvenliği için IETF [5] tarafından tanımlanmış Internet Protokolü güvenlik standardıdır. Kendi içerisinde güvenli yerel alan ağlarının, güvensiz ağlar (örneğin Internet) üzerinden güvenli olarak haberleşmesini sağlar.

IPSec' in avantajları şu şekilde sıralanabilir:

- Tüm üst katmanlar(üçüncü katman ve yukarısı) için güvenlik sağlar.
- Uygulamalarda değişiklik gerektirmez.
- Ağdaki tüm IP trafiği korunur. (ICMP vb.)
- Üçüncü katmanda çalıştığı için yönlendiricilerle birlikte kullanıma uygundur.
- Ayrı bir cihaz olarak gerçeklenmeye uygundur.(düşük maliyet, esneklik, kolay yönetilebilirlik)

IPSec protokolünün güvenlik mimarisinde tanımlanan güvenlik hizmetlerini söyle sıralayabiliriz:

- **Veri gizliliği**: Gizlililik, verinin sadece izin verilen kişilerin, izin verilen yollarla erişimini garanti etmektir ve şifreleme ile sağlanır.
- **Veri kaynağının asıllanması:** Veri göndericisinin kimliğinin doğrulanmasıdır. İmzalama yöntemleri ile sağlanır.
- **Veri bütünlüğü:** Verinin iletim esnasında değişmediğinin garanti edilmesidir. Şifreleme, mesajların anlaşılamamasını sağlamaktadır, ancak iletilen mesajın değiştirilmesine karşın bir etkinliği yoktur.
- **Yinelenmiş paketlerin reddedilmesi:** Aynı iletim verisinin, ağdaki herhangi bir kişi tarafından tekrar gönderildiğinin fark edilip verinin atılması işlemidir.
- **Kısmi Trafik akış gizliliği:** Tünel kipinde iç IP adreslerinin ve akan trafik miktarının gizlenmesidir.
- **Filtreleme ve ayrıştırma:** Güvenlik derecesine göre öğelerin ayrıştırılması, trafik filtreleme yapılmasıdır.

IPSec güvenli ve güvensiz ara yüzler arasında bir sınır oluşturur. Bu sınır üzerinden geçen tüm trafik akışı, IPSec yapılandırmasından sorumlu kullanıcı tarafından belirlenen erişim kontrollerinden geçer.

Bu kontroller sonucu paket üzerinde üç temel işlev yapılabilir:

- Paket açık bir şekilde sınırdan geçirilebilir.
- Paket sınırdan geçirilmez ve atılabilir.
- Pakete AH [6] ya da ESP [7] ile güvenlik servisleri uygulanabilir.(IPSec uygulanır)

Bu kapsamda genel olarak güvenli arayüz kırmızı arayüz, güvensiz arayüz siyah arayüz olarak da adlandırılmaktadır. Güvenli arayüz dış fiziksel bir arayüz olabileceği gibi, dâhili bir arayüz de olabilir. IPSec gerçeklemeleri sınırın her bir tarafı için birden fazla fiziksel veya mantıksal ara yüze sahip olabilirler. IPSec aynı zamanda çoklu güvenlik servisleri sağlayabilmektedir. Bunu sağlamaktaki amaç, herkesin her zaman her güvenlik servisine ihtiyaç duymamasıdır. Sözgelimi bir uygulama için, bütünlük ve asıllama servislerine ihtiyaç duyulurken, gizlilik servisi gereksiz olabilir.

IPSec, çoklu algoritmaların kullanılabilmesine destek vermektedir. Çünkü bugün güvenli olduğu düşünülen bir algoritma, gelecekte kırılarak güvensiz hale gelebilir. Böylece bazı algoritmalar zamanla güvensiz hale gelse de IPSec çatısı güvenilirliğini sürdürür. Ağ ortamında yüksek başarım ihtiyacı nedeniyle genellikle simetrik algoritmalar kullanılır.

IP bağlantısız olmasına rağmen IPSec bağlantı tabanlıdır. Çünkü güvenliğin sağlanabilmesi için en azından bir anahtarın paylaşılmasına ve belirli bir süre kullanılmasına ihtiyaç vardır. IPSec bağlamında bağlantı, Güvenlik Birliği Bağlantısı(GBB) olarak adlandırılır. GBB iki uç arasında tek yönlü bir bağlantıdır ve her GBB bir güvenlik tanımlayıcısına sahiptir. Eğer her iki yönde güvenlik isteniyorsa, iki güvenlik birliğine ihtiyaç duyulur. Güvenlik tanımlayıcıları güvenli bağlantılar üzerinde akan paketler içinde taşınırlar ve güvenli paketin işlenmesi için gerekli anahtar gibi güvenlik parametrelerinin bulunmasında kullanılırlar.

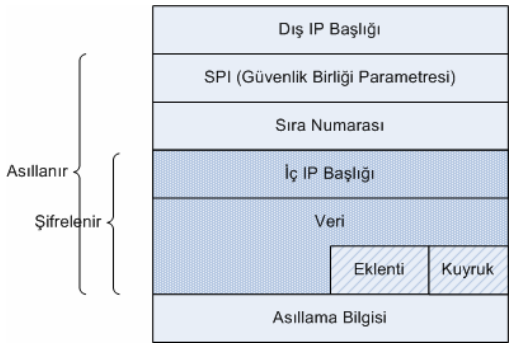
IPSec temelde iki ana parçadan oluşur. İlk parça; pakete eklenecek güvenlik tanımlayıcısı, bütünlük kontrol değeri ve diğer bilgileri taşıyan iki başlık yapısını tarif eder. İkinci parça ise anahtarların kurulması ile ilgilenen IKE [8]' dir. IKE protokolü haberleşen uçlar arasında anahtarların dinamik olarak belirlenmesi ile ilgilenen bir protokoldür.

IPSec iletim kipi ve tünel kipi olmak üzere iki kipte kullanılabilir. İletim kipinde IPSec başlığı IP başlığından hemen sonra gelir ve IP başlığındaki protokol alanı, IPSec başlığının takip ettiğini gösterir. Tünel kipinde gerçek tüm IP paketi (IP başlığı, IPSec başlığı vs...) tamamen yeni bir IP başlığı tarafından kapsüllenir. Tünel kipi, tünelin son uca varmadan önce başka bir düğümde bitmesi ile ayrı bir IPSec güvenlik geçidinde gerçeklemeye uygundur. Böylece yerel ağdaki diğer bilgisayarlar IPSec' ten habersiz olarak güvenli haberleşebilirler. Tünel kipi ile birlikte, yerel ağdaki iç ağ adreslerinin saklanması sağlanır ve böylece güvensiz bölgede hangi iki bilgisayarın birbiriyle ne kadar iletişim kurduğu anlaşılamaz. Kısmi trafik akış gizliliği servisi sağlanmış olmakla birlikte yine de hangi ağ grupları arasında haberleşme yapıldığı, paketlerin çıkış noktasına bakılarak anlaşılabilir. Tünel kipinde çalışma modeli Şekil 1 de gösterilmiştir. Buna göre güvenilen A ve B ağları arasında IPSec protokolü kullanılarak Internet üzerinde sanal ve güvenli bir yol oluşturulur. Bu çalışma kapsamında da IPSec in tünel kipinde çalışma modu modellenmiştir.

Şekil 1: IPSec Tünel Kipi

IPSec protokolünün iki adet farklı güvenlik servis kipi bulunmaktadır. AH servisi sadece veri bütünlüğü sağlarken, ESP servisi hem gizlilik hem de bütünlüğü sağlamaktadır. Bu çalışma kapsamında yaygın kullanımı ve veri gizliliğini de sağlaması sebebiyle ESP güvenlik servisi modellenmiştir.

ESP başlığı iki 32-bitlik sözcük içerir. Bunlar SPI ve sıra numarasıdır. SPI bağlantı tanımlayıcıdır. Bu tanımlayıcıyla kullanılan şifreleme, asıllama algoritmalarına ve kullandıkları anahtarlara ulaşılır. Sıra numarası ise şifrelenmiş paketlerin kötü niyetli kişilerce tekrar tekrar gönderilmesini engellemek için paketlere yerleştirilen ve her pakette arttırılan bir sayıdır. Genellikle bu alanı ilklendirme vektörü(IV) izler. IV, ESP başlığının bir parçası değildir ve şifreleme algoritmasının CBC kipte çalıştırıldığı durumlarda kullanılır. IV' nin kullanılıp kullanılmayacağı ve kullanılacaksa boyutunun ne olacağı, şifreleme algoritmasına ve bu algoritmanın kipine bağlıdır. Çalışma kapsamında, AES-CBC ve SHA-1 algoritmaları gerçeklenip kullanılmıştır.



Şekil 2: ESP Paket Yapısı

Şifreleme algoritmasının blok kipte çalışması durumunda, verinin, şifreleme algoritmasının blok boyunun tam katı olması için paketin sonuna doldurma yapmak gerekebilir. Bu durumda sona doldurma(eklenti) eklenir ve doldurma boyu ESP kuyruk alanına yazılır. Doldurma miktarı ve şekli kullanılan şifreleme algoritmasına bağlıdır. Bir sonraki başlık alanı, ESP başlığından sonraki protokol alanı değerini içerir. ESP HMAC bütünlük ve asıllama kontrolünü destekler. Asıllama kontrol değeri paketin en sonuna koyulur ve böylece donanım tabanlı gerçeklemelerde paket ağdan bit bit geldikçe HMAC değeri hesaplanarak paketin sonundaki değer ile

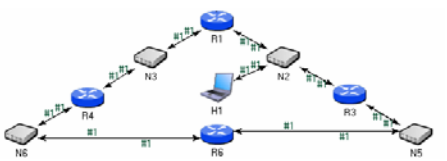
karşılaştırılır. ESP servisinin paket yapısı Şekil 2 de ayrıntılı olarak gösterilmiştir.

IPSec, yukarıdaki paragraflarda da anlatıldığı gibi oldukça geniş ve gerçeklenmesi güç bir mimaridir. Endüstriyel ve akademik çevrelerde, IPSec üzerine yapılan çalışmalarının genellikle çalışan ağ platformları üzerinde yapılarak denendiği gözlemlenmiştir. Bu kapsamda ya Linux OS gibi açık kaynak koda sahip sistemlerin mevcut IPSec yığınları değiştirilmiş ya da çalışma için protokolün sadece kısıtlı bir bölümü gerçeklenmiştir [10]. Ancak çalışmaların gerçek ağ ortamında denenmesi hem maliyetli hem riskli hem de elde edilen sonuçlarının kısıtlı olması anlamına gelmektedir. Hâlbuki benzetim ortamında yapılan çalışmalar az maliyetli ve risksiz olmaktadır. Bunun yanı sıra örneğin bir benzetim ortamında yapılan bir günlük çalışmayla gerçek dünyadaki yıllara karşılık düşürülebilmektedir ki bu da çok zengin sonuçların elde edilebilmesi anlamına gelmektedir. Fakat ağ benzetim araçları üzerine yapılan inceleme göstermiştir ki; NS-2, OMNET++ ve OPNET gibi popüler ağ benzetim araçlarında IPSec modülleri bulunmamaktadır. Bu gereksinimden yola çıkılarak tasarlanan ve gerçeklen IPSec ağ modelleme yazılımı, bir sonraki bölümde anlatılacak olan OMNET++ ağ benzetim aracına eklenebilecek şekilde gerçeklenmiştir.

2.1. OMNET++

Ağ benzetim araçları; ağ protokollerinin ve algoritmalarının gerçeklenmesi ve denenmesi için tasarlanmış yazılımlardır. Bu çalışmalara ilişkin çeşitli parametreler gerçek ağ ortamındaymış gibi bu araçlar kullanılarak analiz edilebilmekte ve çeşitli sonuçlar elde edilebilmektedir. Information Sciences Institute tarafından geliştirilmiş olan NS-2 en popüler açık kodlu ağ benzetim aracıdır. NS-2 programı genellikle yönlendirme konusundaki çalışmalarda kullanılmaktadır. Diğer bir önemli benzetim aracı ise ticari bir program olan OPNET [9]'dir. OPNET ise daha çok askeri ve gezgin ağ uygulamalarının geliştirilmesinde kullanılmaktadır.

OMNET++, nesneye dayalı olarak C++ dili ile geliştirilmiş açık kaynak kodlu ve ayrık zamanlı benzetim aracıdır. OMNET++ özellikle telekomünikasyon uygulamalarının ve bilgisayar ağlarının benzetimi amacıyla tasarlanmıştır. Nesne tabanlı yapısı sayesinde oldukça modüler olan OMNET++, kolay geliştirmeye olanak tanımaktadır. Gelişkin ve güçlü görsel ara yüzleri aracın kullanımı ve aynı zamanda benzetim sonuçlarının tahlil edilmesini kolaylaştırmaktadır. Çalışma kapsamında NS-2 ve OMNET++ benzetim araçları detaylı olarak incelenmiştir. Her ne kadar NS-2 en yaygın kullanılan ve en zengin kütüphanelere sahip benzetim aracı olsa da OMNET++ aracının tamamen C++ ile yazılmış, güçlü dokümantasyonlara sahip ve daha kolay anlaşılabilir olması sebebiyle bu çalışma için NS-2 den daha uygun olduğuna karar verilmiştir. IPSec modellemesi ve yazılım geliştirmesi OMNET++ benzetim ortamına uyumlu olarak yapılmıştır.



Şekil 3: OMNET++ Ağ Modelleme Örneği

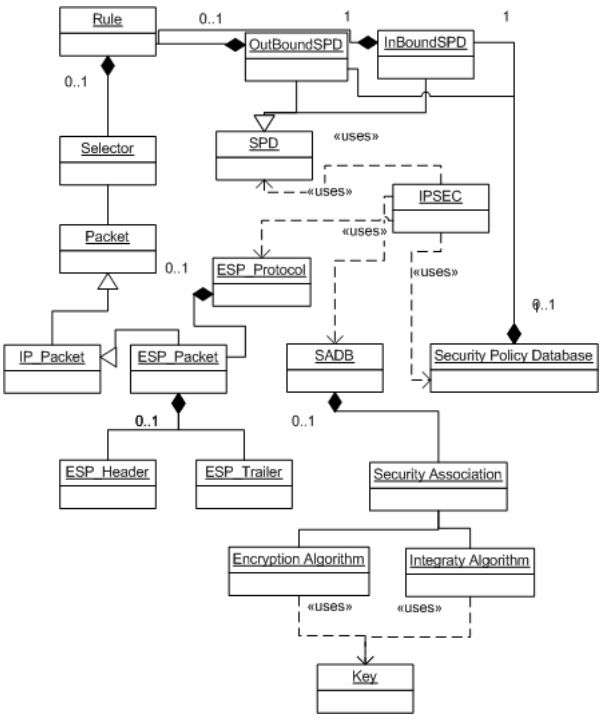
IP, IPv6, MPLS, Mobil IP ,OSPFv2 , RIPv2, Ethernet, Arp vb.. gibi birçok protokol için hazır kütüphaneleri bulunan OMNET++ benzetim ortamında; bilgisayar ağlarına ilişkin performans, gecikme, hata adeti gibi değişkenler rahatlıkla ölçülüp trafik mühendisliği yapılabilmektedir. Yeni geliştirilen ağ protokollerin ve algoritmaların gerçeklenip mevcut ağ modellerinin üzerinde denenmesi ve karşılaştırılması mümkün olmaktadır. Şekil 3 de OMNET++ aracıyla yapılmış örnek bir ağ modellemesi gösterilmektedir.

Çalışma kapsamında yapılan IPSec modellemesi OMNET++ benzetim çatısı üzerine inşaa edilmesine rağmen yazılımın arayüzleri olabildiğince modüler tasarlandığından, gereksinim duyulduğu takdirde mevcut modelleme yazılımı NS-2 gibi farklı benzetim araçlarında da kolaylıkla çalışabilir hale getirilebilir.

Geliştirilen IPSec benzetim modelinin, model ağ üzerindeki denemelerinde ise OMNET++ benzetim aracının hazır modelleme kütüphanelerinden biri olan INET modüllerinden faydalanılmıştır. INET kütüphanesi genel olarak; yönlendirici, anahtar, terminal ve server gibi temel ağ cihazlarının ve TCP, UDP, IP gibi temel ağ protokollerinin modellemelerini içermektedir.

3. IPSec Modellemesi ve Benzetim Yazılımı

Çalışma kapsamında IPSec protokolünün yazılımı tasarlanmış ve gerçeklenmiştir. Tasarım yapılırken yazılım, nesneye dayalı yönteme göre analiz edilerek modellenmiştir. Tasarımda nesneye dayalı yöntem en verimli şekilde kullanılmaya çalışılmıştır. Yazılımın modüler ve yeniden kullanılabilir olması temel hedef olarak seçilmiştir ve tasarım esnasında çeşitli tasarım kalıplarından faydalanılmıştır.



Şekil 4: IPSec UML - Sınıf Diyagramları

Genel olarak Şekil 4'de ki UML diyagramında gösterildiği gibi IPSec yazılımının uygulama modeli tasarlanmıştır. Her ağ güvenlik cihazının(VPN), bir güvenlik yönetimi yapılandırması vardır ve bu yapılandırmada güvenlik ile ilgili ayarlar yapılır. Bu yapılandırma dosyası modeldeki her IPSec modülü için dışarıdan okunmaktadır ve sınıflar bu konfigürasyonlara göre yapılandırılmaktadır. Güvenlik yönetimi yapılandırması, güvenlik politika veri tabanını(SPD) yönetir. Güvenlik politikası veri tabanını kuralları(Rule) içerir. Her kural bir ya da daha çok sayıda seçici(Selector) içerir. Seçiciler IP paketindeki hedef veya varış adresleri ile, yine hedef veya varış kapıları olabilir. IP Paketinin(IP_Packet) bir kurala uyması için, kuralın içerdiği tüm seçicilere uyması gerekir. Her kuralın bir de kararı (IPSec) vardır. Karar seçilen pakete ne yapılacağını belirler. Karar; açık geçir, durdur ya da IPSec uygula olabilmektedir.

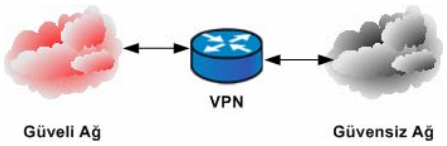
Yazılım tarafından üzerinde işlem yapılan Internet paketi(IP_Packet), IP başlığı içermektedir. Paket, ESP paketi ise aynı zamanda ESP baslığı(ESP_Header) ve ESP kuyruk(ESP_Trailer) alanlarını içermektedir. Paketlerin hepsi OMNET++ benzetim ortamının temel paket sınıfı olan cMessage sınıfından türetilmiştir, bu sadeye bu paketlerde benzetim ortamına özgü fiziksel hat hata yüzdeleri ve zaman mührü gibi değişkenleri de taşımaktadır.

Güvenli ara yüz paketleri(ESP) paketleri, Güvenlik Birliklerine (Security Association - SA) göre açılır ya da oluşturulurlar. SA'lar güvenlik birliği veri tabanında (SADB) tutulur. Güvenlik birlikleri şifreleme algoritmaları, bütünlük algoritmaları ve bu iki işlemi birden yapabilen birleşik algoritmaları kullanırlar. Algoritmalar şifreleme ve asıllama işlemleri için anahtar (Key) kullanırlar. ESP paketini açmak ve oluşturmak için gerekli tüm bilgileri güvenlik birliği (SADB) tutmaktadır.

OMNET++'ın mevcut ağ modüllerinden alınan IP paketleri IPSec giriş modülüne verilir. IPSec giriş(IPSec-Outbound) modülü IP paketini kapsüller(Encapsule) ve ESP paketini oluşturur. IPSec çıkış(IPSec-Inbound) modülü ise, ESP paketini açar(Decapsule) ve iç IP paketini çıkarır. En nihayetinde oluşturulan IP paketleri tekrar OMNET++ ortamına enjekte edilmektedir. Aynı zamanda OMNET++ ortamında ESP paketlerinin ayırt edilebilmesi için ESPPacket tipinde benzetim ortamının diğer modellemelerine uygun bir paket sınıfı tipi tanımlanmıştır. Bu sayede ağda seyahat eden IP paketlerinden hangilerinin ESP paketi olduğu anlaşılabilmekte ve ESP paketi ile ilgili sıra numarası(SPI) gibi değişkenler de gerçek zamanlı olarak izlenebilmektedir.

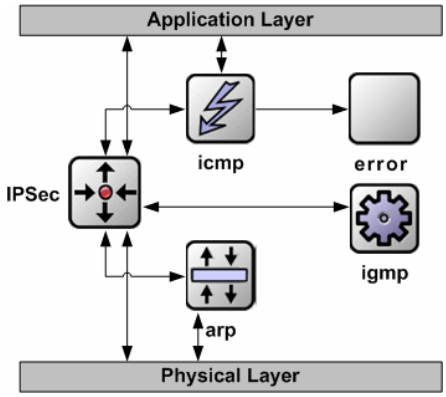
3.1. IPSec Benzetim Modeli

IPSec günümüz IP ağlarında en çok tünel kipinde, güvenli yerel alan ağlarını, güvensiz ağlar üzerinden sanal ve güvenli tüneller ile bağlamak için kullanılmaktadır. Benzetim modeli de bu ihtiyaçtan yola çıkılarak tünel kipinde IPSec - ESP yapan bir ağ güvenlik geçidi(VPN) şeklinde yapılandırılmıştır. Ancak IPSec in diğer kullanım tiplerine ilişkin modelleri de, ihtiyaç duyulduğu takdirde çok az bir değişiklik yapılarak kolaylıkla tanımlanabilir. Modelin en üst katmanı Şekil 5'de gösterildiği gibi güvenli ve güvensiz ağlara, ara yüzleri bulunan bir güvenlik ağ geçidi(VPN) gibi modellenmiştir.



Şekil 5: VPN Modellemesi

Benzetim modelinin Şekil 6'da gösterilen ağ katmanında ise IPSec yığını; arp, icmp, igmp protokol yığınları ve hata(error) modülleri ile detaylandırılmıştır. Her katmandaki modüller birbirleri ve bir üst katmandaki modüller ile OMNET++ ortamına özgü çeşitli mesaj kapılarıyla(Gates) bağlanmışlardır. Modüller arasındaki bağlantılar şekillerdeki oklar aracılığıyla gösterilmektedir. Bu bağlantılar, modüller arasında paketlerin seyahat edebilmesini sağlamakta ve her modül kendisine gelen paketler için kendine özgü çeşitli işlemler yapmaktadır.



Şekil 6: Ağ katmanı Modellemesi

Modelin fiziksel katmanında OMNET++ ortamında hazır biçimde bulunan ethernet, kablosuz veya optik bağlantılar, isteğe bağlı olarak seçilebilmektedir. Bu fiziksel bağlantıların hata olasılıkları ve gecikmeleri gibi değişkenleri istenilen değerlerde ayarlanabilmektedir. Uygulama katmanında ise UDP, TCP, Telnet, Http gibi standart protokoller yine kendilerine özgü ayarlanabilir parametreler ile kullanılabilmektedir.

Benzetim modelinde IPSec protokolünü yürüten model ağ güvenlik cihazları için; IPSec yapılan paket sayısı, politikaya uymayan paket sayısı, MTU(maximum paket uzunluğu), gecikme, kuyrukların doluluk miktarı, fiziksel hatların hata olasılıkları gibi bir çok ağ parametresi ayarlanabilmekte ve benzetim esnasında gerçek zamanlı olarak izlenebilmektedir. Aynı zamanda ağda seyahat eden IP ve ESP paketlerinin içeriğine ilişkin her türlü parametre de izlenebilmektedir.

4. Benzetim Örneği ve Ölçümler

Modelin yeteneklerini göstermek adına, güvenli ağlarda bulunan iki terminal düğümün, IPSec protokolünü yürüten ve 100Mb'lık Ethernet ara yüzleri bulunan ağ güvenlik geçitleri üzerinden haberleşmesi, Şekil 7'de gösterildiği gibi örnek

olarak modellenmiştir. Bu modelde VPN_1'in arkasında bulunan terminal-1 den, VPN_2'nin arkasında bulunan terminal-2 ye periyodik olarak değişik boylarda IP paketleri yollanmıştır ve hat kapasitesinin doluluğu ve paketlerin gecikmeleri üzerine çeşitli sonuçlar elde edilmiştir.

Trafik kapasitesi üzerine yapılan testlerde terminal-1 den 64 byte olarak %17 hat kapasitesinde terminal-2 ye yollanan paketlerin, IPSec ESP protokolü tünel kipin uygulandıktan sonra 138 byte a dönüştüğü görülmektedir. Bunun sebebi uygulanan ESP'nin sonucunda paketlere yeni başlıkların koyulması ve şifreleme için gerekli eklemeler yapılmasıdır. Dolayısıyla VPN_1 ile VPN_2 cihazının arasındaki hat kapasitesinin artan paket boyları sebebiyle %17 den %32 ye çıktığı gözlemlenmiştir. Bu artan trafik VPN_2'nin işleyemeyeceği kadar arttırıldığında, paket kayıplarının yaşanacağı açıkça gözükmektedir. Günümüz ağlarında yoğunlukla kullanılan TCP protokolünde ACK mesajlarının 64 byte olduğu düşünülürse, bu modelin TCP ile IPSec'in ortak çalıştığı ağlarda performans kestirimleri açısından çok faydalı sonuçlar üreteceği açıktır.

Şekil 7: Örnek IPSec Ağ Modellemesi

Aynı örnek ağ üzerinde gecikme testleri de yapılabilmektedir. Model ağ güvenlik cihazların IPSec-ESP paketi oluşturma ve IPSec-ESP paketi çözme işlemlerine ilişkin gecikmeleri model üzerinde ayarlanabilmektedir. Normalde IPSec yapmayan bir ağ güvenlik modelinin gecikmesi sözgelimi 10 mikro saniye olarak ayarlanabilirken, IPSec paketi oluşturan veya yapan bu cihaz için gecikmeye artı 10 mikro saniye olarak belirlenmiştir. Bu durumda normal koşullarda hedefine 20 mikro saniyede giden paketlere IPSec yapıldığı durumlarda gecikmenin 40 mikro saniyeye ulaştığı gözlemlenebilmektedir. Aynı zamanda yüksek gecikmeden dolayı cihazların kuyruklarının daha çok dolduğu da edinilen başka bir bilgi olmuştur. Model üzerinde IPSec den kaynaklanan gecikmeleri uygulanan güvenlik servisine yani şifreleme ve asıllama algoritmalarına göre belirlenebilmesi mümkün olmaktadır ve bu sayede kriptografik algoritmaların ağ performansına etkileri de ölçülebilecektir. IPSec'in günümüz ağlarında VoIP gibi gerçek zaman gereksinimi bulunan protokoller ile birlikte kullanılacağını düşünürsek [11], ağ üzerinde oluşan gecikmeden dolayı ne gibi sorunlar ortaya çıkartacağı, düzenlenecek benzetim modelleri üzerinden rahatlıkla görülebilecektir. Aynı zamanda kimi ağlarda iç içe veya birbirini kapsayan gereksiz ESP tünelleri oluşabilmektedir bu durum, paketlerin defalarca aynı güvenlik seviyelerinde ESP ye maruz kalması anlamına gelmektedir. Bu da paket gecikmelerini oldukça arttırmaktadır. Böyle durumlar da benzetim modellerinde fark edilerek düzeltilebilir.

5. Sonuç ve İleriki Çalışmalar

Çalışma kapsamında esnek ve geliştirilebilir bir IPSec modellemesi tasarlanmış ve gerçeklenmiştir. IPSec modellemesi yaygın kullanılan OMNET++ benzetim ortamındaki mevcut protokoller ile uyumu bozmayacak şekilde gerçeklenmiştir. Böylece mevcut ağ haberleşmesi algoritmaları ve protokolleri ile birlikte IPSec mimarisi üzerine çalışma yapılmasına olanak tanımaktadır. Örnek bir model üzerinde kısaca özellikleri anlatılan modellemenin bilimsel ve endüstriyel çalışmalara altyapı olabilecek bir modelleme yazılımı olduğu düşünülmektedir.

Günümüzün popüler ağ teknolojilerinden olan servis kalitesi(QoS), çoklu yayın(Multicast) ve gezgin IP(Mobil-IP); IPSec ile birlikte kullanıldığında birçok problem ortaya çıkmaktadır. Örneğin IPSec uygulandığında, IP başlığında bulunan servis kalitesi alanları şifrelenmekte dolayısıyla bu alan anlaşılamaz hale gelmektedir, IPSec noktadan noktaya tasarlandığı için çoklu yayın desteklenmemektedir ve gezgin IP ile dinamik biçimde kurulması gereken sanal tüneller için düğümlerin elle yapılandırılması gerekmektedir. Aynı zamanda IPSec yapan düğümler için otomatik ve güvenli anahtar dağıtma yöntemleri geliştirilmelidir çünkü IKE gibi mevcut protokoller günümüz için yetersiz kalmaktadır. Tüm bu problemler IPSec kapsamında üzerinde çalışılması gereken araştırma alanlarından yalnızca bazılarıdır.

Çalışma kapsamında geliştirilen IPSec model yazılımı kullanılarak, günümüz ağları için örnek verilen problemler üzerine araştırmalar çok daha kolay ve hızlı bir şekilde yapılabilecektir. Tüm bunların yanı sıra; IPSec in ağ üzerinde kullanımına ilişkin, güvenlik analizleri yapılabilir, güvenlik zafiyetleri önceden tespit edilerek önlenebilir ve ağ üzerinde IPSec den kaynaklanacak gecikmeler minimuma indirilecek şekilde tasarımlar yapılarak çeşitli performans iyileştirmeleri daha kolay biçimde yapılabilecektir.

İleriki çalışmalar kapsamında IPSec modeli IPv6'yı da içine alabilecek şekilde genişletilip geliştirilecektir. Bu sayede tasarlanan modelin gezgin tasarsız ağlarda (MANET) da IPSec kullanımına ilişkin çeşitli güvenlik ve performans iyileştirmesi çalışmalarında kullanılması planlanmaktadır.

6. Kaynakça

[1] Kent S. ve Seo, K., Security Architecture for the Internet Protocol, RFC 4301.

[2] OMNET++, " OMNET++ Simulator, http://www.hit.bme.hu/phd/vargaa/omnetpp/."

[3] NS-2, "NS-2 Simulator, http://www.isi.edu/nsnam/ns/."

[4] NIIST, "NIST IPSec and IKE Simulation Tool, http://www.antd.nist.gov/niist/. "

[5] IETF, "The Internet Engineering Task Force, http://www.ietf.org/."

[6] Kent S., IP Authentication Header(AH), RFC 4302.

[7] Kent S., IP Encapsulating Security Payload (ESP), RFC 4303.

[8] D. Harkins, D. Carrel., The internet key exchange (IKE). RFC 2409.

[9] OPNET, "http://www.opnet.com/."

[10] Castanier, F., Ferrante, A., and Piuri, A Packet Scheduling Algorithm for IPSec Multi-Accelerator Based Systems. 15th IEEE international Conference on (Asap'04)

[11] Barbieri, R., Bruschi, D., and Rosti, E. Voice over IPsec: Analysis and Solutions. (December 09 - 13, 2002). ACSAC. IEEE Computer Society.