Kablosuz Geçici Ağlarda Yönlendirme Saldırılarının Analizi ve Önlenmesi

İbrahim Zağlı[1] Güray Yılmaz[2] Coşkun Sönmez[3]

[1,2]Bilgisayar Mühendisliği Bölümü, Hava Harp Okulu, İstanbul
[3]Bilgisayar Mühendisliği Bölümü, Yıldız Teknik Üniversitesi, İstanbul

[1]e-posta: zagli@hho.edu.tr [2] e-posta: gyilmaz@hho.edu.tr
[3] e-posta: acsonmez@yildiz.edu.tr

Özetçe

Hareketli Geçici Ağlar, düğümler arası bağlantıların çok zorlu bir iletişim ortamı oluşturacak kadar değişken ve çoğunlukla tutarsız olduğu, kendiliğinden ortaya çıkan (erişim noktası v.b. olmadan) kablosuz ağlardır. Bu nedenle, her düğüm komşularının ötesindeki düğümlerle haberleşebilmek için diğer düğümlere muhtaçtır ve diğerlerinin iletişimini desteklemek için bir yönlendirici gibi hareket etmek zorundadır. Ağ içerisindeki bir düğüm belirgin bir biçimde arızalı olması veya ağ kaynaklarını sadece kendisinin kullanmak istemesi ya da daha da kötüsü belirli bir düğüm veya düğüm grubunun iletişimini engellemeye çalışması sonucu protokol kurallarının gerektirdiğinden farklı hareket edebilir. Hareketli Geçici Ağlar üzerinde yönlendirme işlemini gerçekleştirmeye çalışan protokoller için kritik problem sahalarından birisi yönlendirme ihlallerinin ayırt edilmesi ve olumsuz etkilerinin azaltılmasıdır. Bunun yapılabilmesi ve ağ üzerinde adil ve etkin kaynak kullanımının sağlanabilmesi için ihlal modelleri hakkında yeterli bilgiye sahip olunması gerekir. Bu çalışma kapsamında, literatürde üzerinde çalışılan ihlal yöntemleri sebep oldukları sonuçlar açısından analiz edilerek temel savunma yöntemleri tasarlanmıştır.

1. Giriş

Yakın gelecek için en umut vadeden sayısal iletişim ortamı olması nedeniyle, özellikle son 10 yılda Hareketli Geçici Ağlar (HGA) üzerinde bir çok araştırmacı tarafından çok yönlü araştırmalar yapılmaktadır [1,2,3]. Hareketli Geçici Ağlar, düğümler arası bağlantıların çok zorlu bir iletişim ortamı oluşturacak kadar değişken ve çoğunlukla tutarsız olduğu, kendiliğinden ortaya çıkan (erişim noktası v.b. olmadan) kablosuz ağlardır [1].

Herhangi bir merkezi yönetim mekanizmasının yokluğunda, HGA bünyesinde, her düğüm komşularının ötesindeki düğümlerle haberleşebilmek için diğer düğümlere muhtaçtır ve diğerlerinin iletişimini desteklemek için bir yönlendirici gibi hareket etmek zorundadır. Bu sebeplerden dolayı, HGA araştırmalarında yoğun olarak çalışılan temel konulardan biri de yönlendirme protokolleri olmuştur [4,5,6].

Veri paketlerini herhangi bir düğümden (kaynak) bir diğer düğüme (hedef) aktarmak için ihtiyaç duyulacak ara düğümlerin tespit edilmesi olarak tanımlanabilecek olan temel HGA yönlendirme probleminin üstesinden gelmek üzere araştırmacılar tarafından çok çeşitli ve bazıları yoğun şekilde kabul görmüş (AODV, TORA, vb.) önerilerde bulunulmuştur [8]. Veri paketlerinin takip edecekleri yolun tespit edilmesi işlemine yol tespiti adı verilir. Yol keşfi ve yol seçimi olarak iki bölüme de ayrılabilecek olan yol tespiti işlemi gerek herhangi bir ihtiyaç ortaya çıkmadan önce (proaktif, pro-active), gerekse ihtiyaç ortaya çıktığı anda (on-demand) gerçekleştirilebilir [16]. Her iki durumda da etkili ve sağlıklı bir iletişim ortamının oluşabilmesi için HGA'yı oluşturan düğümlerin yüksek seviyede eş güdüm içerisinde olmaları çok önemlidir.

Son dönemde gelişen çoklu ortam uygulamalarının yaygınlaşması ile HGA üzerinde bu uygulamaların ihtiyaç duydukları kalite kısıtlarının karşılanabilmesi için yönlendirme protokolleri seviyesinde özel önlemler alınmasının gerekliliği ortaya çıkmıştır [1,6]. Bunu en temel nedeni, hareketliliğin sonucu zaten oldukça yetersiz, değişken olan ağ kaynaklarının içerisinden belirli kısıtlara uygun olanların seçilmeye çalışılmasının zorluğudur. Bütün bunlara ilave olarak yönlendirmenin gerçekleştirilmesi için gereken eşgüdüm unsuru bu şartlar altında çok daha kritik bir hal almaktadır. Bu alanda bir çok bilimsel çalışma yapılmış olsa da henüz uluslararası standart olarak kabul görmüş mevcut bir çalışma bulunmamaktadır [5].

Ağ içerisindeki bir düğümün belirgin bir biçimde arızalı olması veya ağ kaynaklarını sadece kendinin kullanmak istemesi ya da daha da kötüsü belirli bir düğüm veya düğüm grubunun iletişimini engellemeye çalışması sonucu protokol kurallarının gerektirdiğinden farklı hareket ettiği duruma *yönlendirme ihlali* adı verilir.

Kalite kısıtlı olsun ya da olmasın HGA üzerinde yönlendirme işlemini gerçekleştirmeye çalışan protokoller için kritik problem sahalarından biri yönlendirme ihlallerinin ayırt edilmesi ve olumsuz etkilerinin azaltılması konusudur. Bunun yapılabilmesi ve ağ üzerinde adil ve etkin kaynak kullanımının sağlanabilmesi için ihlal modelleri hakkında yeterli bilgiye sahip olunması gerekir. Yönlendirme ihlallerinin bazı ortak noktaları olmasına rağmen, uygulamada olan yönlendirme protokolü kuralları değişiklik gösterebileceğinden alınacak önlemlerin de protokol bazında değerlendirilmesi gerekmektedir.

Son dönemde, *telaş saldırıları* [18], *solucan deliği saldırıları* [19] ve *sybil saldırıları* [17] gibi belirli ihlal modellerine odaklı çeşitli önerilerde bulunulmuştur. Bunlara ilave olarak ağ üzerinde güven düzeyi bilgisine dayalı bir yapı oluşturmaya yönelik çözüm yöntemleri de önerilmiştir [4,5,6].

Önerilen yöntemlerin büyük çoğunluğu kurallara uyan düğümlerin menzilleri içerisindeki süregelen iletişimi dinlemelerine yönelik önlemler içermektedirler [7,14,15,16]. İletişimin dinlenmesi aynı zamanda değerlendirilmesi anlamına gelmektedir. Ayrıca, bu değerlendirme sonucunda etraftaki düğümler için karar verilen bir güven seviyesi bilgisi diğer düğümler ile paylaşılarak, bütün düğümlerin hareket

tarzı hakkında fikir edinilmekte ve bu bilgiye dayanarak düğümlerin iletişim ağından faydalanma seviyelerine karar verilmektedir [9]. Bu yaklaşım, en temel anlamda, kurallara uyan düğümler için sürekli fazladan işlem maliyetine sebep olmaktadır.

Bu çalışma kapsamında, ikinci bölümde daha önceki çalışmalarda belirlenmiş olan saldırı türleri analiz edilmiş, üçüncü bölümde ihlal modellerinin temel özellikleri, zayıflıkları ve doğurdukları sonuçlar incelenmiştir. Takiben dördüncü bölümde, bu çalışmaların ışığında belirlenen anahtar özelliklere karşı beş temel savunma modeli tasarımları açıklanmıştır.

2. Saldırı Türlerinin Analizi

Yönlendirme protokollerinin büyük çoğunluğunda yürütülen işlemleri 3 ana aşamaya ayırmak mümkündür [1];

- Yol keşfi ve seçimi
- Veri paketi iletimi
- Yol bakımı

Yol keşfi ve seçimi aşamasında, kaynak düğümden hedef düğüme ulaşmak için, veri paketlerinin sırasıyla iletileceği ara düğümler tespit edilmeye çalışılır. Bu aşama ağ içerisindeki yüksek katılımlı işbirliğinin başlaması gereken aşamadır. Genellikle "RREQ" adı verilen nispeten çok küçük boyutlu bir yol istek paketinin ağ içerisinde yayınlanması yoluyla başlar. Bazı protokollerde "RREQ" paketi hedef düğüme ulaştığında bazılarında ise "RREQ" yayınına cevap olarak yayınlanan "RREP" isimli cevap paketlerinin kaynağa ulaşmasıyla sona erer. Toplanan bilgi kullanılarak hedef ya da kaynak düğüm tarafından veri paketlerinin izleyeceği yola karar verilir [10,12,13]. Özellikle değişikliğe aşırı hassas olan kalite kısıtlı iletişimde kullanılan yönlendirme protokollerinde yol seçimi işlemi daha sonraki aşama içerisine aktarılabilmektedir [1].

Veri paketlerinin iletimi aşaması, yol keşfinin başarılı şekilde tamamlanmasını müteakip başlar. İletişimin esasen gerçekleştiği aşama bu aşamadır. Önceki aşamada kesin olarak belirlenmiş olan ya da iletim sırasında belirlenmesi için gerekli bilgilerin toplanmış olduğu yol kullanılarak veri paketleri hedef düğüme ulaştırılır.

Üçüncü aşama, HGA mevcut olduğu sürece tekrarlanan bir aşamadır. Bu aşamada, ağ içerisinde iletişim devam ederken değişen durumlara hızlı şekilde reaksiyon göstererek yönlendirme işleminin arzu edilen şekilde devam etmesine olanak sağlamaya çalışılır. Değişen bağlantı durumlarının ve komşuluk bilgilerinin etraftaki diğer düğümlere özel bir bilgi paketi yardımıyla rapor edilmesi ve alınan bilgi paketlerinin gerektirdiği hareket tarzının yerine getirilmesi şeklinde çalışır [1].

Yönlendirme protokolü ihlalleri bahsi geçen aşamalardan herhangi birisinde olabileceği gibi birden fazla aşamaya yayılmış birleşik bir saldırı şeklinde de gerçekleşebilir.

Belirli bir düğüm ya da düğüm grubu tarafından yönlendirme protokolü kurallarının ihlal edilmeye çalışılmasının sebepleri;

- Ağın belirli bir bölgesindeki iletişimi engellemek,
- Belirli bir düğümün iletişimini engellemek,
- Ağ kaynaklarının kendisine tahsisini sağlamak
- Arıza durumları

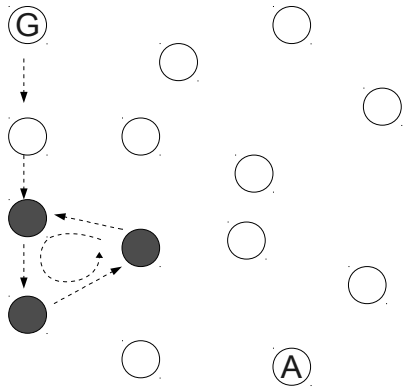
olarak sıralanabilir [13]. Bu amaçlara ulaşmak için saldırgan düğüm (veya düğüm grubu) tarafından gerçekleştirilebilecek farklı ihlal modelleri konu alınarak bir çok çalışma yapılmış ve yapılmaktadır [17,18,19]. Bu bağlamda en çok kullanılan ihlal modelleri ortak ve ayrılan noktalarının bulunması amacıyla analiz edilmişlerdir.

2.1. Yönlendirme çemberi

Yönlendirme çemberi (loop), sahte yönlendirme paketleri göndererek veri paketlerinin belirli sayıda düğüm arasında döngüye girmesini sağlamak yoluyla enerji ve bant genişliğini tüketmeyi amaçlayan ihlal türüdür. Saldırgan düğüm yol keşfi aşamasında normal şekilde davranabileceği gibi kendi üzerinden geçen yolun seçilmesini sağlamaya yönelik çok cazip cevaplar da verebilir.

Sonraki aşamada, Şekil 1'de gösterildiği gibi, saldırgan düğüme iletilmek üzere ulaşan veri paketleri eğer saldırgan düğüm yalnız ise yol keşfi aşamasına katılmayan bir düğüme gönderilebilir ya da varsa diğer saldırgan düğümler yardımıyla belirli bir grup düğüm arasında dolaşması sağlanabilir. Her iki durumda da dışarıdan gözlendiğinde söz konusu saldırgan düğümün gelen veri paketlerini ilettiği görülecektir. İhlalin anlaşılması için gözleyen düğüm tarafından her paketin hangi düğüme iletilmesi gerektiğinin bilinmesine ihtiyaç vardır. Böyle bir bilginin bütün düğümler tarafından kaydedilmesine çalışmak iletişimle doğrudan ilgili olmayan düğümlerin çok fazla gereksiz işlem gücü ve bellek harcaması anlamına geleceği değerlendirilmelidir.

Literatürde kabul görmüş halleriyle birçok HGA yönlendirme protokolü bu saldırıya açıktır [25]. Yol keşfine katılmayan düğümlere veri paketi iletilmesi durumunda paketi alan düğüm saldırgan değil ise durumun rapor edilerek saldırgan düğümün iletişimin dışında tutulmasını sağlamak mümkündür ve tek saldırgan olduğu durumda basit ve etkili bir yöntem olacaktır. Birbirlerine komşu olan bir grup saldırgan düğüm kullanıldığında savunulması oldukça zor, çok etkili bir saldırı olarak kalacaktır.



Şekil 1: Yönlendirme çemberi saldırısı.

2.2. Yönlendirme kara deliği

Yönlendirme kara deliği (blackhole), saldırgan düğüme ulaşan bütün paketlerin göz ardı edildiği ihlal biçimidir. Amacı; HGA üzerinde iletişimin engellenmesi olabileceği gibi, kaynakların başkaları tarafından kullanılmasını engellemek de olabilir. Bazen bir düğüm istem dışı hatalı çalıştığında ortaya çıkabilir. Örneğin, ayarları yanlış yapılmış bir güvenlik duvarı uygulaması, gelen bütün paketlerin göz ardı edilmesine sebep olabilir. Her iki durumda da hızla tespit edilip bertaraf

edilmediği takdirde süregelen iletişimler açısından ciddi sonuçlar doğuracaktır [11,20].

Yol keşfi aşamasında yayınlanan paketler de dâhil olmak üzere gelen bütün paketleri göz ardı etmesi halinde yol keşfine katılmadığı için, saldırgan düğüme veri paketi iletilmeyecektir. Bu durum ilk bakışta güvenli gibi görünse de özellikle düğüm yoğunluğunun az olduğu ağ ortamlarında ağın belirli bölgelerine erişimi güçleştirebilecek ve bölümlenmeye sebep olabilecektir. Bu tür ihlallerin asıl tehlikeli oldukları durum, bilinçli olarak sadece veri paketlerinin göz ardı edildiği, diğer protokol paketlerine tamamen normal davranıldığı durumdur. Yol keşfi ve yol bakımı amacıyla yayınlanan paketlere normal cevaplar veren bir saldırgan düğüm, kendisine yönlendirilmek üzere gönderilen veri paketlerini göz ardı ederek iletişimi engelleyecektir. Genellikle geriye raporlama yapmayacağı ya da olumlu raporlar göndereceği için tespit edilmesi güçtür [28].

Yol keşfine katıldığı durumlarda, yol seçimi aşamasını ara düğümlere dağıtan yönlendirme protokolleri [1] üzerinde bile etkili olabileceğinden bu durumu tespit eden bir mekanizmanın kurulmasına ihtiyaç olabileceği değerlendirilmektedir.

2.3. Yönlendirme gider deliği

Yönlendirme gider deliği (sinkhole), saldırgan düğümün bütün yönlendirmeyi üzerine alacak şekilde kontrol paketleri yayınlayarak kendisine ulaşan veri paketlerinin silindiği ya da içeriğinin değiştirildiği saldırı biçimidir [25]. Kara delik saldırılarından farklı olarak paketleri üzerine çekmek için yol keşfi aşamasına müdahale etmektedir. Literatürde ki birçok çalışmada kara delik saldırılarıyla girişimli şekilde ele alınmışlardır. Ayrıca ileride bahsedilecek olan gri delik saldırılarına da çok benzemektedirler.

Veri paketlerinin göz ardı edilmesi, protokolün ağ üzerinde çalışmasını engelleyecektir. Çünkü yol üzerinde saldırgan düğümden sonra yer alan düğümlerin olup biten ile ilgili herhangi bir bilgileri olmayacaktır. Daha da kötüsü, özellikle UDP iletişiminde, kaynak düğüm ile saldırgan düğüm arasında yer alan düğümlere de herhangi bir problem rapor edilmediği için, iletişimin sorunsuz devam ettiği varsayılacaktır. TCP iletişim kendi standardında bulunan ACK uygulaması sayesinde en azından iletişimin normal olmadığı bilgisini edinecektir. Yönlendirme protokolü seviyesinde, kaynak ve hedef düğüm arasında ve/veya ara düğümler arasında iletişim süresince gerçekleşen periyodik bir raporlama sisteminin bu tür bir saldırıyı tespit (ve önleme) açısından etkili olabileceği değerlendirilmektedir.

2.4. Zıt bölgeye yönlendirme

Saldırgan düğüme ulaşan veri paketlerinin hedef düğümün olmadığı bölgeye doğru yönlendirilmesi yoluyla iletişimi engellemeyi amaçlayan ihlal biçimidir. Düğümlerin fiziksel yerleşimleriyle ilgili genel olarak bilgi sahibi olunmasını gerektirir [21]. Ayrıca uyarlamalı yönlendirme kullanan protokollerde yol keşfi aşamasına katılmamış, yani yol isteğine cevap vermemiş düğümlere ulaşan veri paketleri genellikle göz ardı edilmektedir [1]. Ağa yeni katılmış düğümlerin doğrudan iletişime katkı sağlamasının istendiği durumlarda, ilk defa karşılaşılan iletişimler yeni bir yol keşfinin başlamasına sebep olabilir. Böyle bir durumda, bahsi geçen ihlal şekli hem gereksiz kontrol paketi yayınlanmasına hem de iletişimin gereksiz olarak ağı meşgul etmesine sebep olur. Bunun yanında, ara düğümlere ulaşan ilgisiz veri paketleri ağ üzerinde yanlış bir şeylerin olduğunun işaretçisi olarak kullanılıp tedbir alınması için harekete geçilmesini sağlayabilirler.

2.5. Gri delik

Gri delik (grayhole) saldırısı, saldırgan düğümün sadece belirli paketleri göz ardı ettiği diğerlerine ise normal usullerde davrandığı ihlal biçimidir [22]. Örneğin, sadece yönlendirme paketlerini geçirip diğerlerini silmek, ya da belirli hedeflere giden veri paketlerini silmek diğerlerini normal olarak işlemek gibi. Bu saldırı türünün, tespit edilmesi ve kaçınılması en zor saldırı türü olduğu değerlendirilmektedir. Genellikle tespit edilmesi için teknik bilgi kadar -herhangi bir düğümün hedef olması için sebeplerin analiz edilmesi gibi- düşünsel bilginin de kullanılması gerekebilir. Bu durum çoğunlukla ve doğal olarak saldırı tespitinde insan etkileşimine olan ihtiyacı gündeme getirmektedir. Çalışmamız, IP iletişimi ağ katmanı içerisinde kaldığı için, kullanıcı etkileşimini içeren çözümler kapsam dışında kalmaktadır. Bu yüzden muhtemel saldırı sebeplerini göz ardı ederek, gerçekleşen iletişimin analizi yolu ile saldırının tespit edilmeye çalışılması gerektiği varsayılmıştır.

Saldırgan düğümün davranış şekli, daha çok, ağ üzerinde tutarsız, tamamen rastlantısal iletişim problemleri varmış gibi algılanacak şekilde sonuçlar doğuracaktır.

Birçok yönlendirme protokolü ağ üzerinde herhangi bir problem oluştuğunda mevcut imkanları maksimum seviyede kullanarak problemli bölgenin etrafından dolaşmaya çalışacak şekilde tasarlanmıştır [1,6,12,25]. Ancak bu sürecin çalışabilmesi için genellikle problemin oluştuğu düğümün cevap vermeyi kesmesi ya da problemi bir adım gerisindeki düğüme rapor edebilmesi gerekmektedir.

Bahse konu saldırı biçimlerinde ise iki durum da söz konusu değildir. Bir adım gerideki düğüm açısından iletişim gayet normal olarak devam etmektedir. Saldırgan düğümün bir adım ilerisindeki düğüm açısından ise herhangi bir iletişim olmadığı için her şey normaldir. Bu durumda sadece saldırgan düğüm problemin farkındadır ve onunda bu durumu rapor etmek gibi bir niyeti olmayacağı açıktır. İlk akla gelen iki seçenekten birisi, sonraki düğüm seçiminde rastlantısallığı devreye alarak belirli oranda paketin saldırgan düğüme doğru gitmemesini garanti altına almak olabilir ki, bu durum şans faktörünü ön plana çıkaracağından yeterli olmayacaktır. Diğer seçenek ise, iletişimin "sonraki düğüm" olarak seçilmeyen düğümler tarafından sessizce kontrol edilmesi olabilir. Buna benzer çözümler Kara Delik saldırılarına karşı teklif edilmiştir [2,24].

2.6. En iyi yolu seçmeme

En iyi yolu seçmeme (detour), saldırgan düğümün, kendisine gelen veri paketlerini göndereceği ara düğümü seçerken rapor edilmiş en uygun yolu seçmek yerine daha kötü olduğu rapor edilmiş yolu seçerek, kurallara kısmen uyarken diğer yandan iletişimi kötü yönde etkilemeyi amaçlayan saldırı biçimidir. Genellikle belirli bir bölgedeki ağ kaynaklarının diğer iletişimler tarafından kullanılmasını engellemek ya da hedef aldığı bir düğüme doğru olan iletişimi engellemek amacıyla gerçekleştirilir. Bu saldırı türünün tespit edilebilmesi için saldırgan düğümün yaptığı tercihlerin komşu düğümler tarafından değerlendirilmesinin etkin bir yöntem olabileceği değerlendirilmektedir [26].

Saldırgan düğüm kendisine gelen her veri paketini sonraki düğüme ileteceği için, dışarıdan bakıldığında son derece normal hareket ettiği gözlemlenir. Ancak en kötü yolu seçmesinden dolayı, en iyi ihtimalle gereksiz yeni bir yol keşfinin başlamasına sebep olur ya da en kötü durumda veri paketinin hedefe ulaşamayıp kendisinden sonraki bir noktada kaybedilmesine sebep olur. Bu özelliği nedeniyle de tespit edilmesi oldukça zorlaşmaktadır. Tedbir olarak, yol keşfi aşamasında aynı seviyede bulunan düğümlerin yol isteklerine verilen duyabildikleri cevapları analiz ederek, daha sonra bu düğümler tarafından yapılan duyabildikleri tercihleri verdikleri cevaplara göre değerlendirip derecelendirerek, gerçek problem noktasını tespit edilmesi sağlanabilir. Bu tespit doğru olarak yapılabilirse uygun bir raporlama yöntemiyle çevre düğümler tarafından saldırgan düğüm iletişimden soyutlanabilir.

2.7. Bölümleme

Bölümleme (partitioning), sahte yönlendirme paketleri yayınlamak yoluyla mevcut ağ yapısını parçalara ayırarak belli bir bölgenin diğer düğümlerle iletişimi engellemeye çalışan ihlal biçimidir [13]. Bu saldırı türü genellikle kaynak veya hedef düğüm tarafından yol tayini yapılan yönlendirme protokollerinde etkili olmaktadır. Uyarlamalı yönlendirme protokollerinde etkili olabilmesi için öncelikle yanlış yol isteği cevapları yayınlamak yoluyla yönlendirmeyi kendi üstüne çekmek daha sonra gelen veri paketlerini geri yansıtarak bölümlemeyi gerçekleştirmeye ihtiyaç duyar. Bu durumda dahi uzun süreli etkili olabilmesinin mümkün olmadığı değerlendirilmektedir. Özellikle geri besleme yöntemleri kullanılarak yapılan tercihlerin doğruluğunun sınandığı durumlarda kısa sürede tespit edilebilecek bir saldırı türü olduğu değerlendirilmektedir.

Saldırgan düğüm, yönlendirme protokolü kuralları içinde hareket edeceği varsayımıyla düşünüldüğünde, etkili olmak için özellikle belirli bir gölgeden gelen bütün isteklere çok cazip cevaplar verecektir [23]. Belirli bölgelerden gelen veri paketlerini diğer bölgeye geçirmeyecek şekilde hareket edecektir. Uyarlamalı yönlendirme protokollerinde iletişim üzerinde uzun süre etkili olamayacaktır, çünkü, bu tür protokoller [1] belirli bir düğümde oluşabilecek ani problemlere karşı en hızlı şekilde cevap verecek biçimde tasarlanmıştır. Bu sebepten dolayı söz konusu düğüm hızla iletişim güzergâhının dışına itilerek etkisiz konumda kalacaktır. Eğer protokol kurallarına uymayarak doğrudan paketlerin silinmesi şeklinde hareket edilecek olursa bu durumda da "Sinkhole" sadırı tipine karşı alınması gereken önlemlerin etkili olacağı değerlendirilmektedir.

2.8. Sanal düğüm ekleyerek üzerinden geçen yolu uzun gösterme

Saldırgan düğümün, yol keşfi sırasında sahte düğümler ekleyerek kendi üzerinden geçen yolların gerçekte olduğundan daha uzun görünmelerini sağlamaya çalıştığı saldırı biçimidir. Uyarlamalı yönlendirme protokollerinde yol keşfi sırasında cevap paketlerinin değiştirilmesi yoluyla saldırgan düğümün kendisi üzerinde veri paketi iletilmesini engellemeye çalışması şeklinde uygulanır [25]. Veri iletiminin tamamı üzerinde büyük bir etkisi olmasa da, ağ kaynaklarının kullanılmasını kısıtladığı için istenmeyen bir durumdur. En ideal durum ağ üzerindeki düğümler tarafından sağlanan imkânların ağ üzerinde gerçekleşen bütün iletişim tarafından etkin şekilde kullanılması olduğu için herhangi bir düğümün buna benzer bir davranış içine girmesi istenmeyen bir durumdur. Yol keşfi aşamasında; İstek ve/veya cevap paketlerinde bulunan sıra numaralarının değiştirilmesi ya da kalite kısıtlı yönlendirme söz konusu kısıt değerinin bilinçi olarak kötü hesaplanması yoluyla aldatıcı bilgi sağlanması, veri iletim aşamasında ise; tamamen normal hareket ederek gizli kalmaya çalışması şeklinde gerçekleşir.

Öncelikle, yönlendirme protokolü istek ve cevap paketlerindeki sıra numaraları gerektiği şekilde gerçekleşmediğinde bu paketleri göz ardı etmek üzere tasarlanmalıdır. Bu sayede sıra numaralarının gerektiğinden farklı atanması o düğümü iletişim güzergahı dışında bırakmaktan başka etki yaratmayacaktır. Saldırgan düğümün devre dışı bırakılması zaten istenen durum olduğundan dolayı bu yöntemle amaca ualaşılacağı değerlendirilmektedir. Yine de bu gibi durumlara karşılık ağ üzerinde "ne kadar verirsen o kadar alırsın" prensibine dayanan bir öncelik mekanizmasının kurulmasının bu gibi saldırılara karşı caydırıcı etkisi olabileceği değerlendirilmektedir.

2.9. Diğer düğümleri karalama

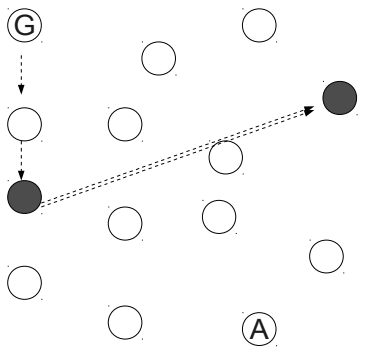
Gözlemci düğüme ya da komşu düğümlere belirli bir düğüm hakkında yanlış bilgiler vererek, o düğümün haksız yere saldırgan olarak tanımlanmasına sebep olmaya çalışan saldırı biçimidir. Bu saldırı türü ağ üzerinde bilinen bir saldırı tespit sistemi var olduğunda kullanılabilen bir türdür. Eğer kullanılan saldırı tespit sistemi ağ üzerindeki diğer düğümlerin komşu düğümler hakkında edindiği tecrübelere dayanıyor ise, bu durumda bu saldırı türü tehlikeli olabilmektedir [23]. Bahsi geçen türde saldırı tespit sistemleri kullanan HGA'larda, kötü niyetli düğümlerin, tespit sistemini yanlış yönlendirebilecekleri gerçeği göz önünde bulundurulmadır. Bu tür hareketler aslında bir yönlendirme protokolü ihlali değildir. Saldırı tespit sistemlerinin kendisinin ihlal edilmesidir. Ancak eğer söz konusu olan yönlendirme protokollerinin ihlallere karşı korunması ise, geliştirilen yönteme karşı uygulanabilecek saldırıların da göz önünde bulundurulması gerekir. Bu ihlal türü bu amaçla inceleme kapsamına alınmıştır. Az düğüm tarafından sağlanan raporların güvenirliliğinin düşük kabul edilmesinin gerekliliğini göz önüne çıkarmaktadır.

2.10. Solucan deliği

Solucan deliği (wormhole), birbirinden uzakta konuşlanmış iki saldırgan düğümün aralarında oluşturdukları özel bir iletişim yolu ile (VPN benzeri) birine gelen veri paketlerinin doğrudan diğerine aktarılması yoluyla yönlendirmenin bozulmaya çalışıldığı saldırı biçimidir (Şekil 2) [19]. Ağ üzerindeki diğer düğümler tarafından iki normal düğüm arasındaki normal bir iletişim olarak algılanacağı için tespit edilmesi oldukça zor bir saldırı türüdür. Ancak iki ayrı konumdaki iki ayrı düğüm tarafından kendine özgü kuralları olan bir iletişim gerektirdiğinden gerçekleştirilmesi de aynı oranda güç olan bir saldırı biçimi olduğu değerlendirilmektedir. Ayrıca, ilk saldırgan düğümün komşuları açısından incelendiğinde kara delik saldırılarına çok benzer şekilde iletilen paketlerin aktarılmadığına yönelik belirtiler vereceği için, aynı grup içinde ele alınmalarının uygun olacağı değerlendirilmektedir. Yönlendirme istek ve/veya cevap paketlerinin de solucan deliği üzerinden aktarılması durumunda uyarlamalı yönlendirme kullanan protokoller çok uzak noktalarda düşük sıra numaralı istek paketlerinin yayınlanmasına sebep olabilir.

Bu durum çok sayıda gereksiz istek ve cevap paketinin ağ içerisinde tekrarlanarak yayınlanması anlamına gelecektir.

Solucan deliği üzerinden aktarılan veri paketleri ilk düğüm üzerinde kaybolmuş gibi algılanacaktır. Yol keşfi aşamasında istek ve cevap paketleri aktarılmaz ise, veri paketleri B noktasına komşu düğümler tarafından yabancı trafik olarak algılanıp göz ardı edilerek silinecektir. Bu durum aslında "kara delik" saldırılarına benzemektedir [11]. "Kara Delik" saldırılarına yönelik alınan önlemlerin büyük ölçüde bu tür saldırılara karşı da etkili olacağı, ayrıca, çevre düğümler tarafından gözleme dayalı saldırı tespit sistemleri "solucan deliği" iletişimini tespit edebilecek şekilde tasarlanabileceği değerlendirilmektedir.



Şekil 2: Solucan deliği saldırısı.

2.11. Telaş saldırıları

Sadece ilk gelen yönlendirme isteğine cevap verilen ve diğerlerinin dikkate alınmadığı protokollerde, herhangi bir ara işlem yapmadan gelen istek paketlerini hızla yayınlayarak diğer düğümlerin başkasından gelen istekleri göz ardı etmelerini sağlamaya çalışan saldırı biçimidir 2.11. (hızlı "RREQ" yayını). Başarılı olduğu taktirde bütün trafiği kendi üzerine toplamış olacağından, diğer saldırı türlerine geçiş aşamasında kullanılabilir [25]. Ayrıca, bütün isteklere karşılanma durumunu incelemeden olumlu cevap verdiği için, ilave işlem yapmasa da iletişimi olumsuz yönde etkileyeceği çok açıktır. Bu sebeple istek ve cevap mekanizmasının ve yol seçimi işleminin bu tür saldırıları bertaraf edecek şekilde ele alınması zorunluluk haline gelmektedir. Basit olarak ilk gelen cevaba işlem yapılsa bile gelen diğer cevapların kaydedilerek alternatif durumlarda kullanılmasını sağlamak şeklinde tedbir alınabilir. Doğrudan hedefmiş ya da hedefe komşuymuş gibi hızlı cevaplar.

Doğrudan komşu olan düğümlere başlatılan iletişimlerde yol keşfinin kullanılmaması bu gibi saldırıların komşu düğümler tarafından etkili olmasının önüne geçilmesi açısından önemli olduğu değerlendirilmektedir. Ancak, ilk kuşak komşulardan uzakta olan saldırganlar için ilave tedbirlerin alınmasının gerekliliği aşikârdır. Bu yüzden, verilen cevapların tutarlılığının diğer komşu düğümler tarafından da değerlendirildiği, çoğul katılımlı bir yol keşfi tasarım çalışmasının gerekli olabileceği değerlendirilmektedir. Ayrıca, sahte cazip cevap paketleri kaynak düğüm tarafından iletişimin hemen başlatılmasına ve saldırgan düğüm tarafından paketlerin göz ardı edilerek iletişimin engellenmesine sebep verebilir. Bu açıdan yaklaşıldığında kara delik saldırıları ile büyük benzerlik göstermektedir.

2.12. Denizanası saldırıları

Kara delik saldırılarında olduğu gibi, saldırgan düğümün gelen veri paketlerini değişken şekilde gereğinden fazla bekleterek göndermesi yoluyla uçtan uca veri iletim süresini uzatmayı amaçlayan saldırı biçimidir. Özellikle TUQR [1] benzeri kalite kısıtlı yönlendirme (KKY) kullanan protokoller üzerinde ciddi etkileri olabilecek türden saldırılardır. Yol keşfi ve yol bakımı aşamalarında tamamen kuralla uygun davranırken, veri paketlerinin iletimi aşamasında kendisine ulaşan veri paketlerini -örneğin kuyruklama algoritmasını değiştirmek yoluyla- gerekenden uzun süre bekletip daha sonra yönlendirerek paket iletimini geciktirmeyi amaçlarlar. Başarılı olduklarında, özellikle çoklu ortam uygulamalarının aksamasına sebebiyet verirler. Ağ üzerinde oluşacak sorunları taklit eder şekilde davrandıkları için tespit edilmeleri oldukça zor ancak aynı zamanda ağ sorunlarına verilene tepkilere maruz kalacakları için bertaraf edilmeleri de aynı oranda kolay olabilecek saldırılar oldukları değerlendirilmektedir [26].

Bu tür saldırıları tespit etmek ve karşı koymak için yapılabilecek en pratik çözüm, yine, çok noktalı harici kontrole dayanan derecelendirme sistemi ile bu tür düğümlerin kuyruk algoritmalarını algılamaya çalışarak karar verecek bir sistem geliştirmek olarak değerlendirilmektedir.

2.13. Kaynakları tüketen saldırılar

Normalden fazla sayıda kontrol paketleri yayınlamak ya da rastgele hedef düğümlere veri paketleri göndermeye çalışarak ağ üzerindeki düğümlerin kontrol paketleri yayınlanmasına sebep olmak yoluyla ağ üzerindeki kontrol paket iletişimini arttırarak normal iletişimin engellenmesine çalışan saldırı biçimidir. Uyarlamalı protokollerin aynı hedefe ulaşmaya çalışan iletişime ilerleyen aşamalarda bütün ağı meşgul etmeden cevap geliştirebileceği düşünüldüğünde bu tür protokollere karşı fazla etkili olamayacak bir saldırı türü olduğu, ancak yönlendirme tablolarında gereksiz yere büyüme yaratacağı için yine de olumsuz etkilerinin olacağı değerlendirilmektedir [21].

Bu tür saldırıların uyarlamalı yönlendirme protokollerini etkileyebilmesi için saldırgan düğümün belirli bir düğüme sürekli olarak iletişim kurması gerekmektedir. Aksi halde, veri iletimi olmadan yol keşfi yapmaya çalışması ilk seferinde etkili olsa da daha sonraki denemelerde yönlendirme tabloları üzerinden cevap verileceği için etkili olamayacaktır. Ancak başka bir düğümle eş güdümlü olarak düzenlenen saldırılarda iletişimin içeriğinin incelenmesi mümkün olamayacağı için çözüm bulunması oldukça zordur. Bu sebeple alınabilecek en mantıklı tedbir olarak ağ kaynaklarına kota uygulanması düşünülebilir. Şöyle ki; herhangi bir düğüm ilk kuşak komşularından uzaktaki herhangi bir düğümle iletişim için belirli bir süre içinde belirli bir oranda bant genişliği veya iletişim zamanı kullanabilir. Belirlenen eşik değer aşıldığında ya iletişim durdurulur ya da tahsis edilen kaynaklar en aza indirilerek (örn: kuyruk önceliği düşürülerek) muhtemel bir saldırının etkili olma oranı düşürülebilir.

3. İhlal Modelleri

Önceki bölümde analiz edilen ihlal türleri sonuçları açısından incelenerek, saldırgan düğümlerin yönlendirme protokollerinin hangi aşamalarında ne tür ihlaller gerçekleştirerek iletişimi ne şekilde etkiledikleri tespit edilmeye çalışılmıştır. İnceleme sonuçları Tablo 1'de özetlenmiştir.

Buna göre, yönlendirme protokolü ihlallerinin doğurduğu sonuçların algılanmasına ve bu sonuçların düzeltilmesine yönelik tedbirler alınmasının zaman içerisinde geliştirilecek yeni ihlal şekillerinin tespit edilmesine ve önlenmesinde de etkili olabileceği değerlendirilmektedir.

Tablo 1: İhlal şekilleri sınıflandırması

Yönlendirme Aşaması	İhlal Şekli	Sonuçları
Yol keşfi	Hızlı, doğru olmayan cevaplar	İletişimin aksaması ve gereksiz ilave yol keşfi faaliyetleri
	İstek ve/veya cevap paketinin iletilmemesi	İletişimin engellenmesi, kaynakların etkin kullanılamaması
Veri Paketi İletimi	İlgisiz rastgele veri paketleri gönderimi	Gereksiz yere tetiklenen yol keşfine yönelik kontrol paketi yayılımı
	Veri paketlerinin yanlış yöne iletilmesi	
	Veri paketlerinin düzenli veya düzensiz şekilde silinmesi	İletişimin kesilmesi, geri raporlanamayan iletişim sorunları
Yol keşfi / Veri Paketi İletimi	Belirli bir iletişime özel olarak ilgili paketlerin düzenli veya düzensiz şekilde silinmesi	Hedefte bulunan iletişimin aksaması veya tamamen engellenmesi

Problem bu açıdan incelendiğinde, yol keşfi aşamasında saldırgan düğümlerin kullanabilecekleri iki ihlal şekli tespit edilebilmiştir. Birincisi doğru olmayan cevapları normal düğümlere göre çok hızlı oluşturmaları ve yayınlamaları, diğer ise belirli bir tip ya da bütün kontrol paketlerini hiç iletmemek biçiminde gerçekleşmektedir. Bir diğer aşama olan veri iletimi aşaması ise en etkili saldırıların gerçekleştiği aşamadır. Bu aşamada, saldırgan düğümlerin gerçekleştirdikleri ihlaller sonucunda ortaya çıkan temel durum veri paketinin olması gereken yol üzerinden seyahat etmemesidir. Bu aşamada gerçekleştirilen saldırılar genellikle ağ üzerindeki iletişim problemleriyle benzer belirtiler oluşturur. Oluşan durum iletişim problemlerinden ayırt edilebilmelidir. Bunların dışında bazı saldırı türlerinin iki aşamayı da birlikte kullanarak hareketlerindeki tutarsızlıkları gizlemeyi başarabilmektedir. Bu nedenle, ağ üzerinde yönlendirme faaliyetlerinin topyekûn ele alınarak değerlendirilmesi gerekmektedir.

4. Savunma Modelleri

Önceki bölümde analiz edilen saldırı yöntemlerinin ortak noktalarının incelenmesi sonucunda yönlendirme protokollerinde uygulanabilecek ihlallerin büyük çoğunluğunun engellenmesi için alınması gereken önlemlerin beş ana gruba ayrılabileceği değerlendirilmiştir. Buna göre;

4.1. İlgisiz veri paketi engelleme sistemi

Bölüm 2.1, 2.4, ve 2.10'da incelenen ihlal türlerinde karşılaşıldığı gibi, yol keşfi ve yol seçimi aşamalarından geçmemiş bağlantılara ait veri paketleri ile olumsuz şekilde sistemin etkilenmeye çalışan saldırılara karşı direnç gösterebilmek için bahsi geçen türde bir veri paketi alan düğüm bu durumu hemen bir kontrol paketi yardımıyla diğer düğümlere rapor etmelidir.

Bunu yapabilmek için yol keşfi aşamasında tekrarlı gelen yol istek paketlerini göz ardı etmeden önce gönderen düğüm bilgisini kaydederek, ileride kendisine ulaşan veri paketlerine ilişkin yol keşfine katılmamış olan düğümleri ayırt etmekte kullanabilir.

4.2. Sınırlandırılmış paket takip sistemi

Özellikle uyarlamalı yönlendirme protokolleri, HGA üzerinde oluşabilecek yerleşim değişimleri ve iletişim problemlerinin ortaya çıkardığı sorunlara karşı direnebilmek ve iletişimin devamlılığını sağlayabilmek için bu gibi durumları yol üzerinde geriye doğru raporlayarak düzeltici işlem uygulama prensibini göre tasarlanmışlardır. Kalite kısıtlı iletişimde, paketlerin yeniden gönderimini engellemek ve mümkün olduğunda diğer imkânları kullanarak ilgili paketi hedef düğüme ulaştırabilmek önemlidir. Herhangi bir ağ sorunu olmadığı halde veri paketlerinin kaybedilmesine yol açan yönlendirme ihlallerinin karşısında daha hassastırlar.

İster kalite kısıtlı olsun ister olmasın iletişimin daha etkin yapılabilmesi için, HGA üzerinde tasarlanmış yönlendirme protokollerinin bir düğümden diğerine iletilen veri paketinin hedefe ulaşana dek yol üzerindeki üçüncü bir düğüme iletildiğinden emin olmasını sağlayacak bir sisteme ihtiyaç duyar.

Kablosuz iletişimin doğası gereği bir düğüm alıcı menzili içerisindeki düğümlerin iletişimlerini dinleyebilir. Bu özellik kullanılarak bir düğüm aktarmış olduğu veri paketinin yol üzerindeki düğüm tarafından aktarılıp aktarılmadığını, hangi düğüme ve ne kadar süre sonra iletildiğini tespit edebilir. Bu bilgi sayesinde aktardığı veri paketinin akıbeti ve sonraki düğüm olarak seçtiği komşusunun davranış özellikleri hakkında bilgi edinebilir. Bu bilgi Bölüm 4.5'de açıklanacak olan raporlama sistemine benzer bir sistem yardımıyla söz konusu düğümün komşularına aktarılabilir. Bu sayede istenmeyen şekilde davranış gösteren düğümler hızla ağ üzerindeki iletişim ortamından soyutlanarak olumsuz etkilerinden azaltılabilir.

Normal ağ protokollerinde, üst katmanlara ya da diğer düğümlere iletilmek üzere düğümün kendisine yönelmemiş paketlerle ilgili herhangi bir bilgi yönlendirme katmanına ulaşmayacaktır. Bu nedenle, bu sistemin uygulanabilmesi için, yönlendirme protokollerinin çalıştığı ağ katmanından daha alt katmanları da içerisine alan bir çalışma yapılmasının gerektiği değerlendirilmektedir.

4.3. Çapraz kontrol sistemi

Yukarıda bahsi geçen, sınırlandırılmış paket takip sistemine benzer özellikler taşısa da, Çapraz Kontrol Sisteminin daha geniş kapsamlı bir görev alanı bulunmaktadır. Temel hedef,

yol keşfi ve seçimi aşamasında, yol üzerinde hedefe kendisinden daha yakın olan düğümlerin verdikleri cevapları kaydederek, daha sonra iletişimin gerçekleştiği esnada bütün iletişimlere ait hareket modellerini takip edip, normal dışı ve şüpheli görünen davranışların rapor edilmesidir.

Bu yaklaşıma benzer şekilde önerilmiş sistemler bulunmaktadır. Temel dezavantajı, bütün iletişimi takip etmeye çalışacağından dolayı işlem gücü ve bellek ihtiyacının yanında güç tüketimini de diğer çözümlere nazaran arttıracak olmasıdır.

4.4. Uyarlamalı yük dengeleme protokolü

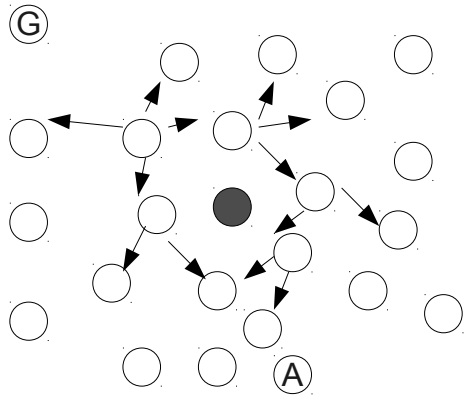
HGA kapsamındaki kaynakların tüketilmesine ya da iletişimin engellenmesine yönelik olarak, protokol kurallarına tamamen uygun davranırken yoğun bir şekilde paket ileten saldırılara karşı düğümler üzerindeki kuyruk algoritmasının uyarlamalı bir şekilde yeniden düzenlenmesi yoluyla iletişim kısıtlamasına gidilebileceği değerlendirilmektedir. Bu uygulama aynı zamanda ağ üzerindeki kaynakların adil dağılımını sağlama görevini de yerine getirebilir. Kalite kısıtlı yönlendirmenin kullanıldığı ortamlarda yük dengelemesi yaparken kalite kısıtına ilişkin düzenlemelerin göz önünde bulundurulmasına ihtiyaç vardır.

Her normal işleyen düğüm üzerinde, kendi üzerinden geçen veri paketlerinin iletişim bazında yoğunluğu hesaplanarak belirli bir eşik değer üzerine çıkan iletişimler için önceliğin düşürülmesi şeklinde tasarlanmıştır. Bu tasarım ağ üzerindeki sıkışmalara tepki veren diğer çözümlerle birleştiğinde, mevcut kaynaklarla mümkün olan en etkin iletişimin sağlandığı bir ortamın oluşturulmasına büyük katkı sağlayacaktır.

4.5. Kısıtlı yayılımlı iletişim raporlama sistemi

HGA üzerinde yönlendirme protokollerinin tasarlanmasında en kritik bilgi, iletilen veri paketinin sonraki düğüm tarafından başka bir düğüme doğru şekilde iletilip iletilmediği bilgisidir. Bu bilginin sağlanması birçok ihlal davranışını sonuçları açısında açığa çıkaracak ve doğru tasarlanmış bir tepki sistemi ile etkin şekilde bertaraf edilmesinin yolunu açacaktır.

Her ara düğüm, süre gelen iletişim içerisinde, belirli aralıklarla veya herhangi bir tetikleme mekanizmasının harekete geçirmesi sonucunda iletişimde bulunduğu komşu düğümleri hakkında o düğümü çevreleyen komşuları aracılığıyla bilgi toplaması prensibine dayanır. Bu sistemin belirli aralıklarla tekrarlanmak üzere tasarlanmasının ağ iletişimindeki problemlere karşı da ilave hassasiyet geliştirilmesi açısından uygun olacağı değerlendirilmektedir.



Şekil 3: Kısıtlı yayılım gösterimi

Tasarlanmaya çalışılan bu tip raporlama sistemlerinin temel problemi, yayınlan raporlamanın ilgisiz düğümler tarafından alınması ve ayrıca gerektiğinden fazla yayılmasından dolayı ağ üzerinde kontrol paketi yükünü arttırmasıdır. Bu problemin aşılabilmesi için, sorgulamada kullanılacak olan kontrol paketlerinin sadece hedefteki düğümü sarmalayan komşu düğümleri arasında yayılmasını sağlayacak bir sistem tasarlanmalıdır [27].

Bu sistem, kontrol paketlerine konulacak bir sayacın paketin iletildiği düğümler tarafından eksiltilmesi ile sağlanabilir. Sadece sıfırdan büyük sayaç değerine sahip olan paketlerin iletildiği bir ortamda örneğin başlangıç değeri 3 olan bir sayaç sayesinde, raporlama ve sorgu paketlerinin sadece istenilen bölgede yayılması sağlanmış olacaktır (Şekil 3). Özellikle düğüm sayısının oldukça fazla ve düğümlerin iletişim menzillerinin düşük olduğu ortamlarda, diğer iletişimlerin etkilenmesini engellemek açısından etkili olacağı değerlendirilmektedir.

5. Sonuç

HGA üzerinde yönlendirme protokollerinin temel problemlerinden birisi olan ihlallerin incelenmesi ve sınıflandırılması, genel anlamda ihlallerin anlaşılması ve etkin çözümler geliştirilebilmesi için gereklidir. Bu amaçla, bu çalışma kapsamında, bugüne dek çalışılmış ve incelenmiş olan ihlal türlerinden öne çıkanlar detaylı şekilde analiz edilmiştir.

Gerçekleştirilen analiz çalışmasının ardından, incelenen saldırı yöntemlerinin doğurduğu sonuçlar sınıflandırılmaya çalışılmış, elde edilen sınıflandırma sonrası saldırıların ortak olarak etkiledikleri protokol işlev ve aşamaları tespit edilmiş, bu aşamalarda söz konusu sonuçların oluştuğunu tespit edip düzeltici işlem yapmaya yönelik prensipler ortaya konulmuştur.

Belirlenen prensipleri yansıtacak şekilde 5 ayrı savunma modeli tasarlanmıştır. Bu modeller yardımıyla literatürde yaygın olarak çalışılan saldırı türlerinin ve ihlal şekillerinin tespit edilip önlenebileceği öngörülmektedir.

Bu çalışmada elde edilen savunma modelleri sonraki aşamalarda, belirgin protokollere savunma sistemleri tasarlayabilmek için kullanılması amaçlanmıştır.

6. Kaynakça

[1] Zagli, I. ve Song, M., ``TUQR: A Topology Unaware QoS Routing Protocol for MANETs", Proceedings of the 5th WSEAS International Conference on Telecommunications and Informatics, Istanbul, Turkey, May 27-29, 2006 (pp 207-212) .

[2] Badis, H. ve Al Agha, K. 2004 “An efficient QOLSR extension protocol for QoS in ad hoc networks”, Vehicular Technology Conference, 2004, (pp2650 – 2653).

[3] K.-C. Wang ve P. Ramanathan 2003 “End-to-end delay assurances in multi-hop wireless local area networks”, in Proc. IEEE GLOBECOM, 2962–2966.

[4] Jiang S., He D. ve Rao J., “A Prediction-Based Link Availability Estimation for Routing Metrics in MANETs” IEEE/ACM Transactions on Networking, Vol. 13, No. 6, 2005 , (pp1302 - 1312)

[5] Lian J., Li L. ve Zhu X., "A Multi-Constraint QoS Routing Protocol with Route-Request Selection Based on Mobile Predicting in MANET " International Conference on Computational Intelligence and Security Workshops , 2007, (pp342 – 345).
[6] Walrand J., "Implementation of QoS Routing for Manets ", SmartNets report, 2007.
[7] Schweitzer C. M., Carvalho T. C. ve Ruggiero W., "A Distributed Mechanism for Trust Propagation and Consolidation in Ad Hoc Networks ", ICOIN 2006, (pp156 – 165).
[8] E. M. Royer and C. K. Toh, "A review of current routing protocols for ad hoc mobile wireless networks", IEEE Personal Communications Magazine, vol. 6, no. 2, 1999, (pp. 46–55).
[9] Yang H., Shu J., Meng X. ve Lu S., "SCAN: Self-Organized Network-Layer Security in Mobile Ad Hoc Networks ", IEEE Journal on Selected Areas in Communications, vol. 24, no. 2, 2006 , (pp261 – 273).
[10] Buchegger S., Boudec J.Y.L., "Self-Policing Mobile Ad Hoc Networks by Reputation Systems ", IEEE Communications Magazine , 2005, (pp101 – 107).
[11] Luo J., Fan M., Ye D., "Black Hole Attack Prevention Based on Authentication Mechanism", IEEE ICCS, 2008, (pp173 – 177).
[12] Kamhoua C.A., Pissinou N., Miller J. ve Makki S.K., "Mitigating Routing Misbehavior in Multi-hop Networks Using Evolutionary Game Theory ", IEEE Globecom 2010 Workshop on Advances in Communications and Networks , 2010, (pp1957 – 1962).
[13] Nath R., Sehgal P. K., Sethi A. K., "Effect of Routing Misbehavior in Mobile Ad Hoc Network ", IEEE 2nd International Advance Computing Conference , 2010, (pp218 – 222).
[14] Boodnah J., Poslad S., "A Trust Framework for Peer-to-Peer Interaction in Ad Hoc Networks ", Computation World , 2009, (pp707 – 712).
[15] Liu Z., Joy A. W. ve Thompson R. A. , "A Dynamic Trust Model for Mobile Ad Hoc Networks ", Proceedings of the 10th IEEE International Workshop on Future Trends of Distributed Computing Systems (FTDCS'04), 2004.
[16] Karri G.R., Khilar P.M., "Routing Misbehavior Detection and Reaction in MANETs ", 5th International Conference on Industrial and Information Systems, ICIIS 2010 , (pp80 – 85).
[17] Newsome J., Shi E., Song D. ve Perrig A., "The Sybil Attack in Sensor Networks: Analysis & Defenses ", PSN'04, 2004 .
[18] Hu Y., Perrig A. ve Johnson D. B., "Rushing Attacks and Defense in Wireless Ad Hoc Network Routing Protocols", WiSe 2003.
[19] Hu Y., Perrig A. ve Johnson D. B., "Packet Leashes: A Defense against Wormhole Attacks in Wireless Ad Hoc Networks ", Rice University Department of Computer Science Technical Report TR01-384 , 2002.
[20] Zhang X.Y., Sekiya Y. ve Wakahara Y., "Proposal of a Method to Detect Black Hole Attack in MANET ", ISADS '09 International Symposium on Autonomous Decentralized Systems, 2009, (pp1-6).
[21] Hu Y.C., Perrig A., Johnson D.B., "Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks ", Journal Wireless Networks archive Volume 11 Issue 1-2, 2005, (pp21 – 38).
[22] Ngai E.C.H., Liu J. ve Lyu M.R., "On the Intruder Detection for Sinkhole Attack in Wireless Sensor Networks ", IEEE ICC, 2006 , (pp3383 – 3389).
[23] Sharma S. ve Singh M., "Defending Wireless Ad Hoc Network from Single and Cooperative Black Holes ", First International Conference on Emerging Trends in Engineering and Technology , 2008, (pp134 – 139).
[24] Umuhoza D., Agbinya J.I. ve Omlin C.W., "Estimation of Trust Metrics for MANET Using QoS Parameter and Source Routing Algorithms ", The 2nd International Conference on Wireless Broadband and Ultra Wideband Communications , 2007, (pp80 – 85).
[25] Nguyen H.L. ve Nguyen U.Y., "Study of Different Types of Attacks on Multicast in Mobile Ad Hoc Networks ", Proceedings of the International Conference on Networking, International Conference on Systems and International Conference on Mobile Communications and Learning Technologies (ICNICONSMCL'06) , 2006, pp(149 – 154).
[26] Aad I., Hubaux J.P., ve Knightly E.W., "Denial of Service Resilience in Ad Hoc Networks ", ACM Mobicom, 2004.
[27] Dokuker S., Erten Y.M., Acar C.E., "Performance analysis of ad-hoc networks under black hole attacks ", SoutheastCon, 2007. Proceedings. IEEE, (pp148 – 153).
[28] Tamilselvan T., Sankaranarayanan V., ""Prevention of Blackhole Attack in MANET ", The 2nd International Conference on Wireless Broadband and Ultra Wideband Communications (AusWireless 2007) , 2007, (pp21 – 26).