İSTANBUL TEKNİK ÜNİVERSİTESİ

FEN BİLİMLERİ ENSTİTÜSÜ
BİLGİSAYAR MÜHENDİSLİĞİ ANABİLİM DALI

BBL 601 AĞ GÜVENLİĞİ

TASARSIZ AĞLARDA GÜVENLİK

Hazırlayan: Tuba Gümüş, 504041534

Tarih : 15.04.2005

Dizin

Dizin 2
1. GİRİŞ 3
1.1 Tasarsız Ağ Uygulamaları 3
1.2 Tasarsız Ağların Özellikleri ve Karşılaşılan Zorluklar 3
1.2.1 Sınırlı kaynaklar 3
1.2.2 Dinamik topoloji değişikliği 4
1.2.3 Kendiliğinden yapılanma 4
1.2.4 Geçici ağ hizmeti 4
1.2.5 Benzer bileşenler 4
1.2.6 Kısa menzil 4
2. GÜVENLİK SORUNLARININ NEDENLERİ 5
3. GÜVENLİK HEDEFLERİ 5
3.1 Ulaşılabilme 5
3.2 Asıllama 5
3.3 Bütünlük 5
3.4 Güvenirlik 5
3.5 İnkar edememe 6
4. AĞ KATMANLARINDA GÜVENLİK ÖNLEMLERİ 6
4.1 Fiziksel Katmanda Güvenlik 6
4.2 Veri Bağı Katmanında Güvenlik 6
4.3 Ağ Katmanında Güvenlik 7
4.3.1 Yol atama teknikleri 7
4.3.2 Yol atama protokollerine saldırılar 9
4.3.2.1 Değişiklik yaparak saldıranlar (modification) 9
4.3.2.2 Taklit ederek saldıranlar (impersonation) 10
4.3.2.3 Asılsız veri ile saldıranlar (fabrication) 10
4.3.3 Önerilen yol atama protokolleri 10
4.3.3.1 SRP (The Secure Routing Protocol) 11
4.3.3.2 ARIADNE 11
4.3.3.3 ARAN 12
4.3.4 Yol atamada güvenlik gereksinimleri 13
4.4 Ulaşım Katmanında Güvenlik 14
4.4.1 Simetrik gizli anahtarların düzenlenmesi 14
4.4.2 Açık anahtar tabanlı düzen 14
4.4.2.1 PGP'ye dayalı, kendi kendine düzenlenen açık anahtar yönetimi 15
4.1.2.2 Polinom şeklindeki gizli bilgi paylaşımına dayalı asıllama 15
4.5 Uygulama Katmanında Güvenlik/IDS 15
5. SONUÇ 16
Kaynaklar 16

1. GİRİŞ

Tasarsız ağlar, sabit bir altyapının ve merkezi sunucuların olmadığı kendiliğinden yapılanan ağlardır. Tasarsız ağlarda düğümler dinamik olarak, süratle ve rastgele yerleşirler. Genelde anlık bir ihtiyacı ya da belirli bir amacı yerine getirmek üzere geçici olarak oluşturulurlar. Her düğüm gerektiğinde yönlendirici olarak çalışır[36][20].

NIST (National Instute of Technology) tasarsız ağları 2 kategoride sunmaktadır[27]:

1. Gezgin tasarsız ağlar (Mobile ad hoc Networks, MANETs)
2. Duyarga ağları (Wireless Ad Hoc Sensor Networks)

Gezgin tasarsız ağlar sivil uygulamalar için daha çok tercih edilir. Daha ucuz, hafif ve kolay kullanılır olması beklenir. Diz üstü bilgisayarlar, PDA'lar gezgin tasarsız ağ uygulamalarında yaygın olarak kullanılmaktadır. Duyarga ağları ise daha çok askeri amaçlıdır. MANET'e oranla çok daha fazla düğüm içerir ve aygıtları daha kısıtlıdır. Duyarga ağları başarısız olmaya daha eğilimlidir[28].

1.1 Tasarsız Ağ Uygulamaları

Tasarsız ağlar farklı amaçlar için kullanılabilirler[2],[4],[8],[21],[27]:

- **Askeri operasyonlarda:** Uçaklar, tanklar ve hareket halindeki kadro iletişim sağlayabilir.
- **Afet bölgesi kurtarma çalışmalarında:** Mevcut iletişim yapısının çalışmadığı sel, deprem gibi kriz yönetiminde, ilk yardım durumlarında
- **Ticari amaçlı:** Sergilerde ya da satış sunumlarında iletişimi sağlamak için
- **Toplantı veya konferanslarda**: Katılanların etkileşimini sağlamak için (aynı fiziksel ortamın kullanıldığı varsayımı ile, DSSS ya da FHSS)
- **Yasal zorunluluk nedeniyle:** Sabit bir altyapının kurulmasının yasal olarak mümkün olmadığı yerlerde

1.2 Tasarsız Ağların Özellikleri ve Karşılaşılan Zorluklar

Tasarsız ağların özellikleri kısıtlarıyla birlikte aşağıda açıklanmıştır.

1.2.1 Sınırlı kaynaklar

Tasarsız ağ bileşenlerinin sınırlı kaynakları yapılacak güvenlik çalışmalarını da sınırlamaktadır. [28]de bu kısıtlar küçük bir merkezi işlem birimi (CPU), az bellek, kısıtlı bantgenişliği ve sınırlı batarya olarak özetlenmiştir.

- **Küçük merkezi işlem birimi ve az bellek:** İşlemcinin hesaplama gücü kısıtlı olduğundan karışık hesaplamalar yavaş yapılır.

- **Kısıtlı bant genişliği:** Tüm iletişim telsiz ortam üzerinden gerçekleşir. Bandgenişliği kısıtlı olduğundan sabit kanal ayırma yöntemleri yerine bandgenişliğini daha etkin kullanan, hız ve erişim gecikmesi bakımından hizmet kalitesi sağlayan dinamik kanal ayırma yöntemleri uygulanmalıdır[21].

- **Sınırlı batarya:** Batarya ömrünün sınırlı olması diğer telsiz sistemlerde olduğu gibi tasarsız ağlarda da dikkat edilmesi gereken bir unsurdur. Yol atamadaki güç tüketimi en aza indirilmeye çalışılmalıdır. Düğümler bu gücü ekonomik olarak tüketmek için alıcılarını periyodik olarak açarlar. Bu yüzden düğümlerin uyanık olduğu zamanı beklemek gerekebilir.

1.2.2 Dinamik topoloji değişikliği

Tasarsız ağlarda kayda değer sıklıkta topoloji değişiklikleri beklenir. Düğümler ağa istediği zaman katılır ve istediği zaman ağı terk eder. Bunun sonucu olarak sık sık yayınlanan güncelleme bilgileri ağ kaynaklarını meşgul eder. Bu değişiklikler ile ilgili bilginin geç gelmesi ise ağda yol atamada istikrarsızlığa sebep olur[25]. Verimlilik (efficiency) ve yanıtlama (responsiveness) arasındaki dengeyi sağlamak oldukça zordur. [17]de düğüm gezginliğinin daha güvenli bir ağ yapılanmasını sağlayabileceği tartışılsa da genel görüş bunun aksidir.

1.2.3 Kendiliğinden yapılanma

Bu özellik tasarsız ağlara özeldir ve diğer ağlardan ayırt edicidir. Ağın denetimi, yönetimi ve yol atama için merkezi bir otorite yoktur. Gezgin düğümlerin her biri gerektiğinde yol atama fonksiyonunu yerine getirirler. Gizli bilginin paylaşılması, anahtarların dağıtılması 3. şahıslara gerek duyulmadan da yapılabilir[20].

1.2.4 Geçici ağ hizmeti

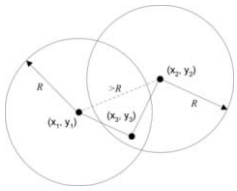
Tasarsız ağlar belirli bir amacı yerine getirmek için geçici olarak kurulur. Bu amaç yerine getirildikten sonra kesilir. Sonuçta sadece belli bir zaman aralığında var olan geçici ağlar söz konusudur.

1.2.5 Benzer bileşenler

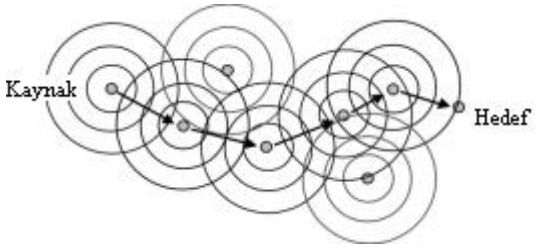
Tasarsız ağlarda işlem yükü ağa katılanlara eşit şekilde yüklenmiştir.

1.2.6 Kısa menzil

Tasarsız ağlarda iletimde genellikle kızılötesi ya da radyo frekansı kullanılmaktadır. Dolayısıyla iletim menzili kısadır. IrDA (Infrared Data Association), veri protokolünde 2 aygıt arasındaki iletim mesafesi 2 m olarak belirtilirken[29], düşük güçlü bileşenler ile bu aralık 20-30cm'e düşebilir.



Menzil uzaklığını arttırmak için paketler iletim aralığındaki komşu düğümlere gönderilir. Bu düğümler de hedefe ulaşana kadar paketleri ilerletirler. Tasarsız gezgin ağlar çok sekmeli ağlardır(multi-hop networks).



Tasarsız ağlarda güvenlik konulu bu çalışmada ilerleyen bölümler sırasıyla güvenlik sorunlarının nedenleri, güvenlik hedefleri, ağ katmanlarında güvenlik önlemleri ve sonuç başlıklarına ayrılmıştır.

2. GÜVENLİK SORUNLARININ NEDENLERİ

Tasarsız ağların altyapısının, merkezi bir denetiminin olmaması gibi karakteristik özellikleri güvenlik politikalarının gerçekleştirilmesinde kısıt olarak karşımıza çıkar[4]. Rastgele ve ani yerleşen kullanıcılar, dolayısıyla dinamik olarak değişen ağ topolojisi güvenlik çözümlerinin de dinamik olmasını gerektirir. Saldırıya açık telsiz ortamda çoklu iletişim ve son derece kısıtlı özkaynaklar ile daha da zorlaşan güvenlik konusu çözülmesi gereken ve hala üzerinde çalışılmakta olan bir sorundur.

3. GÜVENLİK HEDEFLERİ

Güvenlik, özellikle güvenliğe duyarlı uygulamalarda tasarsız ağlar için önemli bir konudur. Bu konuda ulaşılması beklenen nitelikler aşağıdaki gibidir[1]:

1. Ulaşılabilme
2. Güvenirlik
3. Bütünlük
4. Asıllama
5. İnkar edememe

3.1 Ulaşılabilme

Ağ hizmetlerinin hizmet aksatma (DoS) saldırılarına rağmen rağmen varlığını koruması hedeflenir. DoS saldırıları tasarsız ağların her katmanında gerçekleştirilebilir. Kötü niyetli kullanıcı fiziksel ve MAC katmanlarında ağa mesaj yığarak kanallarda çatışma yaratabilir, ağ katmanında yol atama protokolünün çalışmasını aksatarak ağ bağlantısını koparabilir ve daha üst katmanlarda üst düzey hizmetleri çökertebilir.

3.2 Asıllama

Haberleşilen düğümün iddia ettiği düğüm olup olmadığı sınanmalıdır. Bir düğüm başka bir düğümün yerine geçerek yetkisi olmadığı halde kaynağa erişmemeli ve diğer düğümlerin işleyişine müdahale etmemelidir.

3.3 Bütünlük

Bu nitelik iletilen mesajın bütünlüğünün bozulmayacağı garanti edilir. Mesaj kötü niyetli olmayan bozucu bazı etkenlere maruz kalabilir ya da ağda kötü niyetli saldırılara uğrayabilir. Verinin bütünlüğü korunmalıdır.

3.4 Güvenirlik

Güvenirlik niteliği bilginin yetkisi olmayan kullanıcılara açılmaması hedeflenir. Askeri ya da stratejik bilgiler gibi hassas bilgilerin ağda iletimi güvenirliği gerektirir. Bu gibi bilgilerin rakibe sızması hüsranla sonuçlanabilir. Yol atama bilgisinin güvenirliği de bazı durumlarda daha değerli olabilir. Savaş alanında düşman bu bilgiye göre nişan alabilir.

3.5 İnkar edememe

Mesajı gönderen düğüm daha sonra göndermediğini iddia edememelidir. A düğümü B düğümünden hatalı bir mesaj aldığında bu mesajı kullanarak B'yi suçlayabilmeli ve diğer düğümleri bu konuda ikna edebilmelidir.

Güvenlik konuları [28]'de ayrıntılı olarak anlatılmıştır.

4. AĞ KATMANLARINDA GÜVENLİK ÖNLEMLERİ

Tasarsız ağlarda güvenlik önlemleri ağ katmanlarına göre aşağıda verilmiştir[24]:

Katman	Güvenlik Konuları
Uygulama	Zararlı kodları, sızmaları belirleme
Ulaşım	Asıllama ve veri şifreleme ile uçtan uca iletişim güvenliğinin sağlanması
Ağ	Yol atama protokollerine saldırıları önleme
Veri bağı	MAC protokolünün korunması ve bağ katmanı güvenlik desteği
Fiziksel	İşaretleri hizmetlere saldırıdan(DoS) korumak

Tasarsız ağlarda katmanların haberleşme protokolleri düğümlerin verilen şartlara uyacağı varsayımı ile tasarlanmıştır. Bu protokoller güvenilmeyen ortamlarda gerçeklenmek istendiğinde bazı düğümler protokol şartnamesine aykırı davranabilir. Bu düğümlerin amacı telsiz ortama daha sık erişip diğer düğümlerden daha fazla bilgiye sahip olmak ya da diğer düğümlerin ihtiyacı olan paketleri iletmeyi reddederek güç tasarrufu yapmak olabilir(selfishness)[13],[32].

Kötü niyetli düğümlerin davranışlarının önüne geçebilmek için katmanlı bir güvenlik mekanizması uygulanmalıdır.

4.1 Fiziksel Katmanda Güvenlik

Bu katmanda yerleştirilen *frekans sekmeli* güvenlik mekanizması (FHSM) gibi fiziksel koruma mekanizmaları veri çerçevesininin kaynaktan hedefe ilerlerken dinlenilmesini (eavesdropping), yolunun kesilip durdurulmasını, değiştirilmesini ya da düşürülmesini engelleyebilir.

4.2 Veri Bağı Katmanında Güvenlik

Veri bağı katmanında ağ üzerindeki bilgisayarların çatışma olmadan medyaya erişimi yönetilir. MAC (Medium Access Control) protokolü ortamın adil olarak paylaşılmasını sağlar(üstel geri çekilme).

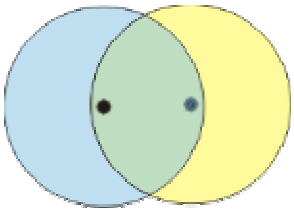
Bu katmanda yapılacak saldırılarda kötü niyetli düğüm, NAV(Network Allocation Vector)'ın boyunu değiştirebilir ve komşu düğümlerin boş(idle) kalacağı zaman dilimi için büyük sayılar atayabilir, çerçeveler arası boşlukları(SIFS,DIFS) azaltabilir, küçük geri çekilme değerleri seçebilir[13].

Başarılı bir güvenlik planı olası tüm aldatma şekillerini dikkate almalıdır. En zor sezme görevlerinden biri geri çekilme sayısının değiştirilip değiştirilmediğinin anlaşılmasıdır[30]. Seçilen geri çekilme sayısı rastgele olduğundan herhangi bir düğümün seçtiği küçük geri çekilme değerinin şans eseri mi yoksa kasıtlı mı olduğunun anlaşılması zordur. [13]te 802.11 MAC protokolünde geri çekilme mekanizmasıyla ilgili bir koruma ve sezme yöntemi tartışılmıştır. Yine [5]'te önerilen bağ katmanında asıllanmış yol atama tekniği ile ARP'de yalancı kayıtlar azaltılmıştır.

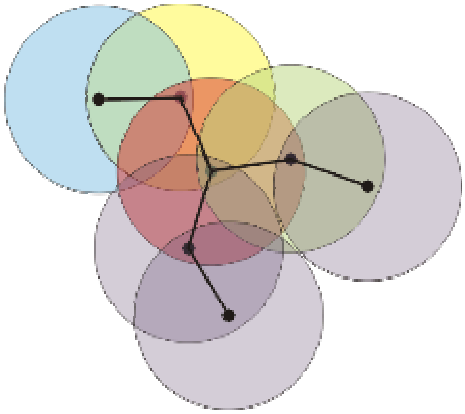
4.3 Ağ Katmanında Güvenlik

Tasarsız gezgin ağlarda çok sekmeli bağlantı 2 aşamada sağlanır:

1. Bağ katmanı protokolleri üzerinden tek sekmeli bağlantının sağlanması



2. Kurulan bağlantının ağ katmanında **yol atama** ve veri iletimi protokolleri ile çok sayıda sekmeye genişletilmesi



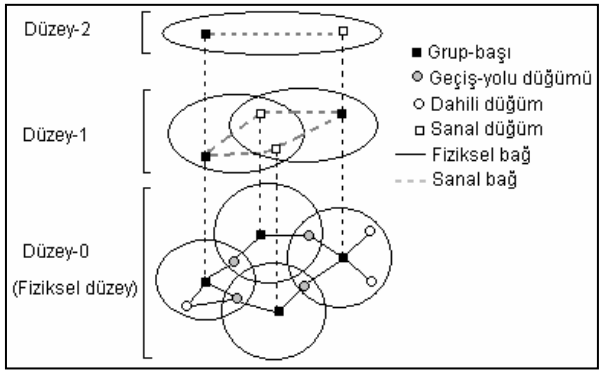
Dolayısıyla tasarsız ağlarda güvenlik konusu büyük ölçüde ağ katmanındaki yol atama protokolleri ile ilişkilidir.

4.3.1 Yol atama teknikleri

Tasarsız ağlarda yol atama teknikleri **yapılarına göre** yatay ve hiyerarşik olarak 2'ye ayrılabilir[21]:

1. Yatay yol atama(flat routed): Her düğüm ağdaki diğer bütün düğümlere giden yol bilgilerinin bulunduğu bir yol atama tablosu tutar. Düğüm sayısı arttığında tablolar büyür ve yol atamanın getirdiği işlem süresi yükü artar. Bu yüzden bu teknik ile elde edilen sonuçlar büyük ağlarda kabul edilebilir düzeyde değildir.

2. Hiyerarşik yol atama: Birbirine yakın uç düğümler öbek(cluster) oluştur. Bir düğüm öbek başı seçilir. Öbek başı o öbek için yol atama görevini yerine getirir. Öbek başları bir üst düzeyde yine öbek oluşturarak hiyerarşik yapının üst düzeyini oluştururlar. Her düzeydeki öbeğin üyeleri sadece kendi öbeklerindeki düğümlerin bilgilerini tutarlar. Diğer öbeklerdeki düğümlere ulaşım öbek başları üzeriden sağlanır.



Hiyerarşik yol atama yöntemi ile atama tablolarının büyüklüğü dolayısıyla yol atamadaki işlem yükü azaltılmıştır. Ancak bu teknikle en iyi yol her zaman bulunamaz.

Tasarsız ağlarda yol atama protokolleri 3 sınıfta incelenebilir:

1- Tabloya dayalı yol atama (Proactive): Erişilebilen bütün ağ varışlarına sürekli olarak yol sağlayan bir tekniktir. Genellikle en kısa yol bulunur. Yol atama işleminde gecikme azdır. DSDV(Dynamic Destination-Sequenced Distance Vector)[31] tabloya dayalı bir yol atama algoritmasıdır.

2- İstekle tetiklenen yol atama (Reactive): Yollar sadece iletişim istendiğinde sağlanır ve topoloji değişikliklerine karşı korunur. Varışa giden herhangi bir yol bulunur. İşlem yükü ve kaynak kullanımı bakımından tercih edilir. Ancak yol aramadaki gecikme görece fazladır. AODV(Ad Hoc On Demand Vector) ve DSR(Dynamic Source Rouiting) istekle tetiklenen yol atama algoritmalarıdır.

AODV[12] ve DSR[15] ilk bakışta benzer görünse de kayda değer farkları bulunmaktadır. Bu iki protokolün yol atama mekanizmaları oldukça farklıdır; DSR bir kaynak yol atayıcı ile saklanmış kayıtları kullanırken AODV yol atama tablosuna dayanan bir yaklaşım seçer. DSR her varış noktası için birden çok yol sağlayabildiği gibi her varışa giden yolu sekme sekme bilir. Diğer yandan, AODV'deki düğümler sadece bir önceki ve bir sonraki sekmenin hangisi olduğunu bilir ve her varış için tek bir yol sağlarlar. Yani DSR kullanan düğümler AODV kullanan düğümlere göre daha çok ağ bilgisine ulaşabilir. Bu da herhangi bir bağlantı koptuğunda DSR'ı tüm ağı istila etmekten kurtarır.

AODV'de sıra numaraları ve TTL kullanılarak eski yol atama kayıtları yenileri ile değiştirilir. DSR zamanı dolan yolların ağdan silinmesini sağlayan bir mekanizmaya sahip değildir. Zincirin bir halkası koptuğunda kaynak düğüme bir hata mesajı gönderilir. Bu mesaj ile

kaynak düğüm yol atamada o halkayı içinde bulunduran tüm yol kayıtlarını siler. Ancak ağdaki diğer düğümler ancak kopuk halkayı kullanmaya çalıştıklarında hatanın farkına varabilirler. Bu yüzden DSR'ın eski yol atama bilgisi ile ağı kirletmesi olasıdır. AODV'nin yaklaşımının kusursuz olmadığı da görülmelidir. Çünkü geçerli yollar da zaman aşımına uğradığı için silinebilir.

3- Hibrid yol atama(Hybrid): Önceden belirlenen kriterlere veya değişen ağ topolojisine göre tabloya dayalı ya da istekle tetiklenen yol atama tekniklerinden biri seçilerek kullanılır. Ağın farklı fiziksel alanlarında ve zamanın farklı dilimlerinde her iki yöntemden de faydalanılır. Yol atama işleminde gecikme ile kaynak kullanımı arasında bir denge kurulur.

Tasarsız ağlarda ölçeklenebilirlik sorunu dinamik öbek oluşturma yöntemleri ile giderilebilir. Yine öbekler ile tabloya dayalı ve istekle tetiklenen yol atama arasında geçiş sağlanabilir. Öbeğin büyüklüğünün ne kadar olacağı sorusu öbekte bulunan düğümlerin gezginlik karakteristikleri göz önüne alınarak dinamik bir yapı ile çözülebilir.

4.3.2 Yol atama protokollerine saldırılar

Tasarsız ağlarda yol atama protokollerine saldırılar 3 sınıfta incelenebilir[4]:

1. Değişiklik yaparak saldıranlar (modification)
2. Taklit ederek saldıranlar (impersonation)
3. Asılsız veri üreterek(uydurarak) saldıranlar (fabrication)

Aşağıdaki saldırı çeşitleri, tasarsız ağlarda istekle tetiklenen protokollerin temsilcisi olan AODV ve DSR göz önüne alınarak anlatılmıştır

4.3.2.1 Değişiklik yaparak saldıranlar (modification)

Kötü niyetli düğümler denetim mesajlarını değiştirerek veya yönlendirme bilgisindeki değerleri çarpıtarak DoS saldırılarına ve ağ trafiğinin yeniden yönlendirilmesine neden olabilir. Aşağıda değiştirme yoluyla AODV ve DSR'ye yapılan birkaç saldırı kısaca anlatılmıştır.

Değiştirilmiş yol sıra numaraları ile yeniden yönlendirme: AODV ve DSDV (Destination-Sequenced Distance-Vector Routing) gibi protokoller belirli varış noktalarına giden yollara monoton artan sıra numaraları atarlar. Daha yüksek sıra numaralı yol tercih edilir. Bu yüzden AODV'de herhangi bir düğüm, gerçek değerinden daha büyük bir varış sıra numarasına sahip yolun varlığını ilan ederek trafiği kendine çekebilir.

Değiştirilmiş sekme sayısı ile yeniden yönlendirme: AODV'de yol bulma mesajındaki sekme sayısı alanı değiştirilerek yeniden yönlendirme saldırısı düzenlenebilir. Yol atama kararı başka diğer metriklerle yapılamadığı zaman AODV sekme sayısı alanını kullanarak en kısa yolu tayin eder. Kötü niyetli düğümler yol isteğindeki (route request,RREQ) sekme sayısı alanını sıfırlayarak yeni oluşturulacak yolda yer alma şanslarını arttırırlar. Benzer şekilde, sekme sayısı alanını sonsuza götürerek oluşturulacak yolda bulunmamayı da sağlayabilirler. Bu saldırı bir sonraki bölümde anlatılacak olan yalancı kayıtla (spoofing) birleştiğinde en çok tehdit eden saldırı haline gelebilir.

Değiştirilmiş kaynak yolu ile hizmeti yadsıma saldırısı: DSR kaynak yol mekanizmasını kullandığı için yolları veri paketlerinde açıkça belirtir. Bu yollarda herhangi bir bütünlük denetimi söz konusu değildir. Basit bir hizmeti yadsıma saldırısı (DoS) paket başlıklarındaki kaynak yollar değiştirilerek gerçekleştirilebilir. Paket varış noktasına ulaştırılamaz.

Tünel saldırısı: Tasarsız ağlar herhangi iki düğümün komşu olarak konumlanabileceğini varsayar. Tünel saldırısı iki ya da daha cok düğümün varolan veri yolları üzerinde mesaj değiş tokuş etmek üzere birlikte çalışması durumunda oluşabilir. İşbirliği içerisindeki bu kötü niyetli düğümler komşu gibi davranabilir ve iyi niyetli ara düğümlerin yol uzunluğu ölçüsünü düzgün arttırmasını engelleyerek var olan yolların uzunluğunu yanlış gösterebilir.

Kötü niyetli düğümler mevcut çok sekmeli yollar üzerinde tünel kurmak yerine aralarındaki uzun menzilli yönlü telsiz ya da telli bağlantıları da kullanabilir. Böyle bir bağlantı haksız da olsa saldırgan düğümlere başlangıç ve varış arasında en kısa gecikmeli yol üzerinde bulunma üstünlüğünü sağlar. Bu saldırı şekli literatürde solucan deliği saldırısı (wormhole attack) olarak anılır[26]. Ancak kötü niyetli düğümler gerçekten en kısa gecikmeli yol üzerinde ise bu yolun seçilmesi yol atama protokolüne bir saldırı olarak düşünülmeyebilir. Solucan deliği saldırılarına karşı bir savunma mekanizması [26]da anlatılmıştır.

4.3.2.2 Taklit ederek saldıranlar (impersonation)

Bir düğüm kendisinden çıkan paketlerde IP ya da MAC adresinde değişiklik yapıp kimliğini bilerek yanlış gösterirse ve zaten diğer saldırılarla (değişiklik yaparak saldırı) birleşim içindeyse yalancı kayıt saldırıları (spoofing) meydana gelir. Bu saldırı türünde kötü niyetli düğüm saptanması zordur.

4.3.2.3 Asılsız veri ile saldıranlar (fabrication)

Asılsız veri saldırıları sahte yol atama mesajlarını içerir. Özellikle komşu düğüm ile bağlantı kurulamadığını iddia eden yalancı hata mesajının verildiği saldırıların geçersiz olduğunu teyit etmek zor olabilir.

AODV ve DSR'de yol hatalarını çarpıtmak: AODV ve DSR'de aktif yol üzerindeki varış düğümünün ya da ara düğümlerin hareket etmesi halinde yolda bağlantıda olan düğüm akıştaki diğer aktif düğümlere yol hata mesajı yayımlar. Böylece ilgili yol tüm düğümlerde geçersiz kabul edilir. Sürekli gönderilen ve yol üzerindeki bağlantıyı kopmuş gibi gösteren yol hata mesajları kaynak ve hedef düğümleri arasındaki haberleşmenin önüne geçen bir saldırıdır(DoS).

DSR'de yol kayıtlarını zehirlemek: DSR'de bir düğüm kaynak ve hedef arasındaki yolda olmadığı halde kulak misafiri olduğu bir paket başlığındaki yol atama bilgisini kendi yol kayıtlarına ekleyebilir. Saldırgan bu durumdan faydalanır ve paket başlıklarında geçersiz yol içeren paketleri aktararak yol kayıtlarını zehirleyebilir.

4.3.3 Önerilen yol atama protokolleri

Güvenli yol atamada önerilen protokollerin çoğu istekle tetiklenen yol atama protokollerinden AODV ve DSR üzerine geliştirilmiş ve iyileştirmeye gidilmeye çalışılmıştır. Mevcut yol atama protokolleri, yol atama fonksiyonunun işleyişine kasten engel olmak isteyen kötü niyetli düğümlerin gerçekleştirdiği aktif saldırıları dikkate alırken pasif saldırıları ve

bencillik(selfishness) sorunu ile ilgilenmemektedir. Bunun yanı sıra, bir takım güvenlik yapısının mevcut olduğu kontrollü bir ortam, mevcut güvenli yol atama protokollerinin çözümünün önkoşuludur.

Aşağıda üzerinde en çok durulan güvenli yol atama protokollerinden bazıları anlatılmıştır.

4.3.3.1 SRP (The Secure Routing Protocol)

SRP[11], mevcut istekle tetiklenen yol atama protokollerine uyumlu bir uzantı olarak tasarlanmıştır. SRP, yol bulma yönteminin aksamasına yol açan saldırı türleri ile savaşır ve doğru topoloji bilgisini elde etmeyi garanti eder: SRP, yol bulmayı başlatan düğümün sahte cevapları fark etmesine ve atmasına izin verir. SRP, başlangıç(B) ve varış(V) noktaları arasında bir güven birliğinin(GB) var olmasına güvenir. GB haberleşen düğümlerin açık anahtarına dayanan hibrid anahtar dağıtımı kullanılarak kurulabilir.B ve V birbirlerinin açık anahtarlarını kullanarak gizli bir simetrik anahtar($K_{B,V}$) değiş tokuş edebilir ve güvenli bir kanal oluşturabilirler. B ve V daha sonra karşılıklı birbirlerini ve yol mesajlarını asıllayabilir.

SRP'de yol keşif tekniğini belirten tekil belirteçler ve anahtarlı hash algoritması ile hesaplanan mesaj asıllama kodunu(MAC) içeren 6 kelimelik bir başlık istenir. Yol isteğinde(RREQ-route request) bulunan başlangıç düğümü tüm IP başlığını, RREQ paketini ve paylaşılan gizli $K_{B,V}$ anahtarının mesaj asıllama kodunu üretmek zorundadır. Ara düğümler RREQ'i varışa doğru iletirken diğer düğümlerden gelen sorgulama sıklığına göre düğümlere ters orantılı bir öncelik değeri atar. Israrla sürekli RREQ göndererek ağı kirleten kötü niyetli düğümler düşük öncelik öncelikli olduklarından en son hizmet görürler ya da görmezlikten gelinirler.

RREQ'i alan hedef düğüm(varış düğümü) istenen alanların anahtarlı hash halini hesaplayıp bunu SRP başlığındaki MAC ile karşılaştırmak suretiyle RREQ'in asıllığını ve bütünlüğünü kontrol eder. RREQ geçerli ise başlangıç düğümünün RREQ'i gönderdiği yolla yol cevabını(RREP) gönderir. Kaynak(başlangıç) düğüm, hedef düğümü tarafından oluşturulan MAC ile bütünlüğü sınar, beklemekte olan belirteçlerle eşleşmeyen tekrar saldırılarını atar.

SRP' yol kayıtlarının zehirlenmesi saldırılarına hala açıktır. Bunun önüne geçebilmek için SRP'nin ara düğüm cevap jetonu (Intermediate Node Reply Token –INRT) yöntemi kullanan 2 ayrı alternatifi de sunulmuştur. SRP'de yol koruma mesajlarının onaylanması mekanizması da yeterince kurulamamıştır.

4.3.3.2 ARIADNE

[33]'de DSR tabanlı, uzlaşmaya dayanan ve yüksek verimli bir simetrik şifrelemeye bel bağlayan bir istekle tetiklenen yol atama protokolü sunulmuştur. ARIADNE varış düğümünün başlangıç düğümünü asıllamasını, başlangıç düğümünün gelen RREP mesajında sunulan ve hedefe giden yol üzerindeki tüm ara düğümleri asıllamasını, ara düğümlerin de RREQ ve RREP mesajlarındaki düğüm listesinden bir önceki düğümü silemeyeceklerini garanti eder.

ARIADNE'de asıllama ve bütünlüğü sağlamak üzere temel RREQ mekanizması ek alanlarla genişletilmiştir. Başlagıç düğümü yol isteğinde bulunurken

<ROUTE REQUEST, başlangıç, varış, id, zaman aralığı, hash zinciri, düğüm listesi, MAC listesi >

mesajındaki ikinci ve üçüncü alanı alanı sırasıyla kendi adresine ve varış adresine, dördüncü alanı daha önceki haberleşmelerde kullanılmayan bir belirtece, beşinci alanı TESLA'daki beklenen varış değerinin en kötü ihtimaline,altıncı alanı $MAC_{KB,V}$ (başlangıç, varış, id, zaman aralığı)' na, son iki alandaki düğüm ve MAC listelerini ise boş listelere atar.

Ara düğümler, mesela A düğümü, gelen RREQ mesajında <başlangıç,id> kısmını kontrol ederek daha gelen bir istek olup olmadığını denetler. Daha önce aynı istek gelmediyse zaman aralığının geçerliliğini denetler. Geçerli zaman aralığındaki bir mesaj ise kendi adresini düğüm listesine ekler, hash zinciri alanını H[A, hash zinciri] olarak değiştirir, MAC listesi alanına tüm RREQ'ın MAC'ini atar. MAC oluştururken istekte belirtilen zaman aralığı indis olmak üzere K_{Ai} TESLA anahtarını kullanır. Sonunda değiştirdiği RREQ'ı yayınlar.

Varış düğümü belirtilen anahtarların zaman aralığında geçerliliğini ve hash zincirini denetledikten sonra yol cevabını gönderir:

<ROUTE REPLAY, varış, başlangıç, zaman aralığı, düğüm listesi, MAC listesi, hedef MAC, anahtar listesi>

ARIADNE simertrik anahtar yöntemini kullandığında verimli çalışır ancak haberleşen düğümler arasında paylaşılan bir gizlilik vardır ve elde edilmesi her zaman mümkün olamaz[4].

4.3.3.3 ARAN

ARAN[4], ağdaki kötü niyetli düğümler ya da 3. şahıslar tarafından yürütülen saldırılara karşı istekle tetiklenen bir yol bulma algoritması olarak önerilmiştir. ARAN ile asıllama, mesaj bütünlüğü ve inkar edememe gibi asgari güvenlik politikaları sağlanır. ARAN bir ön ruhsatlandırma süreci ile başlar. Daha sonra zorunlu bir uçtan uca asıllama aşaması ile devam eder. Zorunlu olmaya, en kısa güvenli yol sağlama aşaması da vardır.

ARAN güvenilir bir sertifika sunucusunun(C) varlığını gerektirir: gezgin düğümler ağa girmeden önce C tarafından imzalanmış bir sertifika isterler. Bu sertifika, düğümün IP adresini, açık anahtarını, sertifikanın oluşturulduğu zamanı ve sertifikanın kullanım süresinin sonunu gösteren bir zaman damgasını içerir. Tüm düğümlerin C'nin açık anahtarını bildiği ve yeni sertifikalara sahip olabildiği varsayılır.

ARAN protokolünün birinci aşamasında kaynak düğümün planladığı hedefe ulaştığını tasdik etmesi amaçlanır. Bu aşamada kaynak dönüş yolunu seçmesi için hedefe güvenir. Kaynak düğümü, A, hedef düğüme, B, ulaşmada yol bulma sürecini başlatmak için yol bulma paketi olarak adlandırılan RDP(route discovery packet)'yi yayımlar.

$[RDP; IP_B; sertifika_A; N_A; t\ ]K_A$

RDP paketi, bir paket tipi belirtecini(RDP), hedefin IP adresini(IP_B), A'nın sertifikasını($sertifika_A$), rastgele bir sayı(N_A) ve içinde bulunulan zamanı(t) içermektedir. Tüm bu parametreler A'nın gizli anahtarı ile şifrelenmiştir. A yol bulma işlemini her tekrarlayışında N_A sayısını bir arttırır.

Her düğüm mesajı aldığı düğümü kaydeder ve mesaj içeriğini imzalayarak tüm komşularına iletir. Bu imza yolda değişiklik yaparak ya da döngü oluşturarak düzenlenen aldatma saldırılarının önlenmesini sağlar.

A'nın komşusu X olsun. X aşağıdaki mesajı yayımlayacaktır.

[[RDP; IP_B; $sertifika_A$; N_A; t] K_A]K_X; $sertifika_X$

Ara düğümler (NA ; IPA) çiftini daha önce gördülerse mesajı iletmezler. X'in sertifikasında A'nın IP adresi yer alır. Monoton artan rastgele sayılar da son gelen sayıların saklanmasını kolaylaştırır. X'in komşusu Y, mesajı aldığında sertifikayı kullanarak imzayı onaylar. Daha sonra önce RDP'den X'nin sertifikasını siler, sonra aşağıdaki mesajı yayımlar.

[[RDP; IP_B; $sertifika_A$; N_A; t] K_A]K_Y; $sertifika_Y$

Sonunda, mesaj hedef B tarafından alınır. B bir kaynak ve sayı çifti için ilk aldığı RDP'ye cevap verir. İlk gelen RDP paketinin en kısa yoldan geldiği garantisi yoktur. B, aynı yoldan cevap paketini(REP) A'ya gönderir. B tarafından gönderilen REP'i alan ilk düğüm Z olsun. B, Z'ye aşağıdaki mesajı gönderir:

[REP; IP_A; $sertifika_B$; N_A; t] K_B

REP RDP'nin geldiği yoldan kaynağa iletilir. Tüm REP mesajları iletenin imzasını taşır. Her düğüm bir önceki düğümün imzasını kontrol eder. Böylece kötü niyetli düğümlerin A'yı taklit etmesi ve tekrar saldırıları önlenir. Hedef dışındaki düğümler hedefe giden yolu bilseler bile hedef yerine cevap veremezler.

ARAN protokolünün ikinci safhasında kaynak tarafından başlatılan yol bulma sürecinin cevabında en kısa yolun alındığı garanti edilir. Birinci safhadaki gibi kaynak bir en kısa yol doğrulaması (SPC, shortest path confirmation) mesajı yayınlar. SPC'nin SDP'den farkı hedefin(B) sertifikasını ve B'nin açık anahtarıyla şifrelenmiş tüm mesajı içeren iki ek alandır. İç içe imzalanmış ve şifrelenmiş SPC mesajı biçimi ara düğümlerin yol uzunluğunu değiştirerek mesaj bütünlüğünü bozmasını engeller.

Bunun yanı sıra, ARAN protokolünün yolu koruma safhası yol hata paketlerinin de imzalanması ile güvenli hale getirilmiştir. Hata mesajını gönderen düğümün imzası ile inkar edememe ilkesi de sağlanır.

ARAN protokolünün kullandığı asimetrik şifreleme yöntemi merkezi işlem birimi(CPU) ve enerji kullanımı göz önüne alındığında ekonomik değildir.

DSDV[31] tabanlı tabloya dayalı güvenli bir yol atama protokolü olan SEAD[34] da açık anahtarla imzalanan hash zincirlerini kullanır.

4.3.4 Yol atamada güvenlik gereksinimleri

Güvenli yol atama protokolleri kötü niyetli düğümlerin varlığında kaynaktan hedefe yol bulma fonksiyonunu başarmak için [4]'te 3 ayrı tasarsız ağ ortamı için sıralanan güvenlik gereksinimlerini yerine getirmelidir:

1. Yol işaretleri aldatılmamalıdır.
2. Asılsız yol atama mesajlarının ağa girmesi engellenmelidir.
3. Yol atama mesajları iletimde protokol fonksiyonunun işleyişi dışında değiştirilmemelidir.
4. Zararlı eylemler dahilinde yol atama döngülerinin oluşturulması engellenmelidir.
5. Yeniden yönlendirmeye izin verilmemeli, en kısa yollar korunmalıdır.

Bu *açık* ortamda tüm düğümler yetkili olarak kabul edilmiştir. Otoyolda araba kullanan ya da kentte yürüyen bu ortamda düşünülebilir.

Yetkili olmayan düğümlerin yol bulma ve hesaplamadan men edilmesi ile *kontrollü açık* ortam gereksinimi de karşılanmış olur. Ancak bu gereksinim yetkili düğümlerin de kötü niyetli davranabileceği gerçeğini dışarıda bırakmaz. Kontrollü açık ortamlarda açık anahtarların, oturum anahtarlarının ya da sertifikaların önceden belirlenmesi olanağı olduğu kabul edilir. Bu ortamdaki gezgin düğümlerin ortak bağlamda ve yakın coğrafyada olması beklenir. Toplantı katılımcıları, kampüsteki öğrenciler bu ortamda düşünülebilir.

Kontrollü düşman ortamında ise yukarıdaki gereksinimlerin yanı sıra ağ topolojisinin ne düşmana ne de yetkili kabul edilen düğümlere açık bırakılmaması istenir. Bu ortam savaş meydanındaki askeri düğümler ya da felaket bölgesindeki kurtarma ekibi için oluşturulabilir. Böyle bir ortamda düğümler müşterek bir kaynak tarafından yerleştirilebilir. Böylece güvenlik parametreleri önceden belirlenebilir. Bu ortamdaki ayırt edici güvenlik tehlikesi donatımın fiziksel olarak ele geçirilmesi ve yönetiminin ele alınması ile dost düğüm taklidi yapılmasıdır. Bu yüzden yol atama protokolü mesajlarında düğüm konumunun duyurulması istenmez.

4.4 Ulaşım Katmanında Güvenlik

Tasarsız ağlarda düğümlerin asıllanması ve yol atama bilgilerinin bütünlüğünün korunarak onaylanması güvenliğin temel yapıtaşlarıdır. Her iki yapıtaşı da uygun anahtarların kullanılmasında bir *anahtar yönetim mekanizması*nın varlığını gerektirir. Önerilen güvenli yol atama protokolleri için anahtar yönetimi yaklaşımı iki kategoride toplanabilir.

4.4.1 Simetrik gizli anahtarların düzenlenmesi

Gizli anahtarlar haberleşen düğümler arasında oturum anahtarı oluşturmada kullanılabilir. Anahtar sunucu içeren adanmış bir yapı kurulabilirse oturum anahtarlarının Kerberos gibi bir anahtar dağıtım protokolü ile otomatik dağıtımı söz konusu olabilir.

4.4.2 Açık anahtar tabanlı düzen

Her düğüm RSA gibi asimetrik algoritma tabanlı bir gizli-açık anahtar çiftine sahiptir. Bu anahtar çifti ile asıllama ve bütünlüğü koruma fonksiyonlarını yerine getirir.

SRP(Secure Routing Protocol), paylaşılan gizli anahtar tabanlı bir güvenlik birliği düzeni üzerine çalışır. Önerilen diğer yol atama protokollerinin çoğu, örneğin ARIADNE, asıllamayı sağlamak için güvenilen üçüncü bir otoritenin(TTP, trusted third party) açık anahtar sertifikalarını yayınladığı açık anahtar düzeneğine güvenmektedir.

Aşağıda tasarsız ağlarda açık anahtar altyapısının karışıklığını ele alan iki yaklaşım anlatılmıştır. İlki PGP'ye benzer kendi kendine düzenlenen açık anahtar yönetimidir. İkincisi

ise polinom şeklindeki gizli bilgi paylaşımına dayanan bir açık anahtar sertifika mekanizmasıdır.

4.4.2.1 PGP'ye dayalı, kendi kendine düzenlenen açık anahtar yönetimi

[20]de açık anahtar tabanlı düzen ele alınarak kendiliğinden düzenlenen açık anahtar yönetim sistemi önerilmiştir. Bu yöntem kendiliğinden yapılanan tasarsız ağ kavramının doğası ile örtüşmektedir. Sabit bir sunucuya ya da güvenilir bir otoriteye ihtiyaç duyulmadan düğümlerin kendi açık anahtarlarını üretmeleri, saklamaları, dağıtmaları ve imha etmeleri esas alınmıştır. Bu yöntemde herhangi bir şekilde bir düğüm kümesinin belirli görevleri olması beklenmez. Her düğüm eşit şartlardadır. Bu yaklaşım merkezi bir denetim olmadan düğümlerin ağa girip çıkabildiği açık ortamlar için geliştirilmiştir.

PGP'de de olduğu gibi sertifika mekanizması kullanıcıların kişisel bilgilerine dayanır. Ancak PGP'de sunuculardaki sertifika klasörlerinde tutulup dağıtılan sertifikalar bu modelde kullanıcıların kendisi tarafından gerçeklenir. Kullanıcılar sertifikalarını yerel kullanıcı depolarında saklarlar. İki kullanıcının birbirlerinin açık anahtarlarını onaylaması gerektiğinde sertifika depolarını birleştirip bu birleşim içinde uygun sertifikaları bulmaya çalışırlar.

Bu yaklaşımın başarısı büyük ölçüde yerel sertifika deposu yapısından ve sertifika grafiklerinin karakteristiğinden kaynaklanmaktadır.

4.1.2.2 Polinom şeklindeki gizli bilgi paylaşımına dayalı asıllama

Ağın erişimini iyi niyetli düğümlerle sınırlamak için bütün düğümlerin işbirliği içinde olduğu güvenli tasarsız ağlarda kritik bir işlemdir. Bunu sağlamak için [22]de önerilen yaklaşımda düğümlerin ağa erişimi için geçerli bileti olması beklenmektedir. Gizli sayısal imza anahtarı, açık anahtar sertifikalarını üretmeleri için polinom şeklindeki gizli bilgi paylaşımına dayalı bir grup imzası mekanizması ile çok sayıda düğüme dağıtılır. Böylece yayınlama, yenileme ve imha etme sertifika hizmetleri de bu düğümlere dağıtılmış olur. Hiçbir düğüm tamamen güvenilir değildir ve erişimi tekeline alamaz. Birden fazla düğüm(komşu düğümler) birlikte başka bir düğümün davranışını gözetler, biletini onaylar ya da imha eder (localized trust model). Düğümlerin taşıdığı sertifikalar ortak sertifika anahtarı SK ile imzalanmıştır. SK'nın bir şekilde her düğüme iletilmesi gerekir. Bu işlemi başlatmak için en az ilk k düğüme bu anahtarın verilmesi gerekir. Bu düğümler işbirliği içinde anahtarı diğer düğümlere yayarlar. Düğümler yer değiştirdiğinde yeni komşuları ile güven ilişkisine girme isteğinde bulunur. Kötü niyetli düğümler için tüm ağda *suçlama* duyurusu yapıldığından kötü niyetli düğümler sürekli yer değiştirerek faaliyetlerine devam edemezler.

4.5 Uygulama Katmanında Güvenlik/IDS

Tasarsız ağların güvenliği sızmaların şifreleme ve asıllama gibi önlemlerle tam olarak korunamaz. Örneğin karşılıklı ödün vererek anlaşmaya varan kötü niyetli düğümler söz konusu olduğunda önerilen çözümler yeterli değildir. Sistem ikinci bir savunma mekanizmasına ihtiyaç duymaktadır. Sızma sezme sistemi (IDS, intrusion detection system) ağdaki şüpheli davranışları algılayıp alarm veren bir yapıdadır. Sızma sezme sistemleri ağı sürekli gözlemleyerek sıra dışı etkinlikleri fark etmeye çalışır. Ağ kaynaklarını hedef alan düşmanca faaliyetleri belirleyip cevap veren bu sistem temelde biriktirilmiş denetim bilgilerine dayanır. Bu bilgiler daha sonra kullanılmak üzere belirsiz bir şekilde depolanabildiği gibi bekleyen proses için geçici olarak da saklanabilir. Bilgilerin nereden ve nasıl toplanacağı, sızmalara nasıl cevap verileceği konfigürasyon ayarları ile denetlenir.

Yönlendirici gibi merkezi denetim noktaları olmayan tasarsız ağlarda sızma belirleme sistemlerinin kullanacağı bilgi o an düğüme giren ve çıkan trafik ile sınırlıdır. Diğer bir anahtar gereksinim de bu sistemlerin kullandığı algoritmaların dağıtılmış olmasıdır. Bir düğümün ağın sadece bir kısmını görebildiği gerçeği de hesaba katılmalıdır. Özellikle ağın düşman ortamında bulunması durumunda düğümlerin bir ya da birkaçının ele geçirilmesi mümkündür. Eğer sızma belirleme sistemlerinin kullandığı algoritmalar işbirliği içinde çalışıyorsa hangi düğümlere güvenileceği şüphelidir. Bu yüzden tasarsız ağlarda sadece dışarıdan gelen saldırılara değil ağın içinden gelen saldırılara karşı da tedbirli olunması gerekir[2].

5. SONUÇ

Tasarsız ağlar herhangi bir altyapıya ihtiyaç duymadan sağladığı olanaklar ile farklı uygulama alanlarında giderek daha yaygın olarak kullanılmaktadır. Gezgin düğümler arasında korunan güvenli bir haberleşmenin sağlanması konusu son zamanlarda birçok araştırmacının ilgi odağı haline gelmiştir. Saldırıya açık telsiz ortamda çoklu iletişim, merkezi bir denetim mekanizmasının olmayışı, rastgele ve ani yerleşen kullanıcılar, dolayısıyla dinamik olarak değişen ağ topolojisi tasarsız ağlarda saldırılara karşı güvenlik önlemlerinin her katmanda düşünülmesini gerektirir. Güvenli yol atama, anahtar yönetimi ve sızma belirleme bu güvenlik önlemlerinin başlıcalarıdır. Ancak bu yazıda önerilen çözümler tüm saldırılara karşı koyamadığı gibi bazı gerçekçi olmayan varsayımlar da yaparlar. Örneğin, anahtar yönetimi için bir yapının var olduğu varsayımı tasarsız ağların altyapısız doğasına aykırıdır. Kısıtlı özkaynaklar ile daha da zorlaşan güvenlik konusu çözülmesi gereken ve hala üzerinde çalışılan bir sorundur. Tasarsız ağlar için geliştirilen teknoloji ilerledikçe daha gerçekçi ve kapsamlı çözümlerin getirilmesi beklenmektedir.

Kaynaklar

[1] Lidong Zhou, Zygmunt J. Haas, Securing Ad Hoc Networks, IEEE Networks Special Issue on Network Security November/December, 1999.

[2] A. Mishra, K. Nadkarni, A. Patcha, Intrusion detection in wireless ad hoc networks, Wireless Communications, IEEE Volume 11, Issue 1, Feb 2004 Page(s):48 – 60.

[3] Yongguang Zhang, Wenke Lee, Yi-An Huang, Intrusion detection techniques for mobile wireless Networks, ACM Wireless Networks, Volume 9 Issue 5, September 2003.

[4] K. Sanzgiri, D. LaFlamme, B. Dahill, B. N. Levine, C. Shields, E. M. Belding-Royer, Authenticated routing for ad hoc Networks, IEEE Journal on Selected Areas in Communications, Vol. 23, No. 3, March 2005, Page(s): 598- 610.

[5] Jim Binkley, William Trost, Authenticated ad hoc routing at the link layer for mobile systems, ACM Wireless Networks, Volume 7 Issue 2, March 2001.

[6] Manel Guerrero Zapata, N. Asokan, Securing ad hoc routing protocols, proceedings of the ACM workshop on Wireless security, September 2002.

[7] C. Gehrmann, P. Nikander, Securing ad hoc services, a Jini view, First Annual Workshop on Mobile and Ad Hoc Networking and Computing, 2000.

[8] Yih-Chun Hu, Adrian Perrig, A Survey of Secure Wireless Ad Hoc Routing, IEEE Security and Privacy, Volume 2 Issue 3, Pages: 28 – 39, May 2004.

[9] Yi-an Huang, Wenke Lee, Intrusion detection: A cooperative intrusion detection system for ad hoc Networks, proceedings of the 1st ACM workshop on security of ad hoc and sensor networks, October 2003.

[10] Lakshmi Venkatraman, Dharma P. Agrawal, A Novel Authentication scheme for Ad hoc Networks, Wireless Communications and Networking Conference (WCNC 2000), IEEE, Vol 3 Pages 1268-1273

[11] P. Papadimitratos, Z. Haas, Secure Routing for Mobile Ad Hoc Networks, Proceedings of CNDS 2002.

[12] C. Perkins and E. Royer. Ad Hoc On-Demand Distance Vector Routing, Proceedings 2nd IEEE Workshop on Mobile Computing Systems and Applications (WMCSA'99), 1999.

[13] Alvaro A. Cárdenas, Svetlana Radosavac, John S. Baras, Ad hoc networks: Detection and prevention of MAC layer misbehavior in ad hoc networks, Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor Networks, October 2004.

[14] Asad Amir Pirzada, Chris McDonald, Establishing trust in pure ad-hoc networks, Proceedings of the 27th conference on Australasian computer science - Volume 26, January 2004.

[15] D. B. Johnson and D. Maltz. Dynamic Source Routing in Ad Hoc Wireless Networks. T. Imielinski and eds. H. Korth, editors, Mobile Computing. Kluwer Academic Publishers, 1996.

[16] Xianjun Geng, Yun Huang, Andrew B. Whinston, Defending wireless infrastructure against the challenge of DDoS attacks, Mobile Networks and Applications, Volume 7 Issue 3, June 2002.

[17] Srdjan Capkun, Jean-Pierre Hubaux, Levente Buttyán, Security & transport: Mobility helps security in ad hoc networks, Proceedings of the 4th ACM international symposium on Mobile ad hoc networking & computing, June 2003.

[18] Yih-Chun Hu, Adrian Perrig, David B. Johnson, Secure routing: Rushing attacks and defense in wireless ad hoc network routing protocols, Proceedings of the 2003 ACM workshop on Wireless security, September 2003.

[19] Hao Yang, Xiaoqiao Meng, Songwu Lu, Self-organized network-layer security in mobile ad hoc networks, Proceedings of the ACM workshop on Wireless security, September 2002.

[20] S. Capkun, L. Buttyan, J. P. Hubaux, Self-organized public-key management for mobile ad hoc networks, Mobile Computing, IEEE Transactions on Volume 2, Issue 1, Jan.-March 2003 Page(s):52 – 64

[21] M. Soytürk, A. E. Harmancı, E. Çayırcı, Gezgin Ad Hoc Ağlar ve Yol Atama, Bilişim Zirvesi '01, İstanbul, 4-7 Eylül 2000.

[22] Haiyun Luo, Jiejun Kong, P. Zerfos, Songwu Lu, Lixia Zhang, URSA: ubiquitous and robust access control for mobile ad hoc networks, IEEE/ACM Transactions on Networking, Volume 12, Issue 6, Dec. 2004 Page(s):1049 – 1063

[23] Panagiotis Papadimitratos, Zygmunt J. Haas, Secure routing: Secure data transmission in mobile ad hoc Networks, Proceedings of the 2003 ACM workshop on Wireless security, September 2003.

[24] Hao Yang; Haiyun Luo; Fan Ye; Songwu Lu; Lixia Zhang; Security in mobile ad hoc networks: challenges and solutions, IEEE Wireless Communications, Volume 11, Issue 1, Feb 2004 Page(s):38 – 47

[25] Survey and Comparison of Two Ad Hoc Routing Protocols, http://nislab.bu.edu/sc546/sc546Fall2002/adhoc/diff.htm

[26] Hu, Y.-C.; Perrig, A.; Johnson, D.B.; Packet leashes: a defense against wormhole attacks in wireless Networks, Twenty-Second Annual Joint Conference of the IEEE Computer and Communications Societies, INFOCOM 2003, Volume 3, 30 March-3 April 2003 Page(s):1976 - 1986 vol.3

[27] Mobile Ad Hoc Networks(MANETs), shttp://w3.antd.nist.gov/wahn_mahn.shtml

[28] Frank Stajano, Ross Anderson, The Resurrecting Duckling: Security Issues for Ad-hoc Wireless Networks

[29] Infrared Data Association, http://www.irda.org/

[30] M. Raya, J.-P. Hubaux, and I. Aad, Domino: A system to detect greedy behavior in IEEE 802.11 hotspots, Proceedings of the Second International Conference on Mobile Systems, Applications and Services (MobiSys2004), Boston, Massachussets, June 2004.

[31] C. R. Perkins, P. Bhagwat, Highly Dynamic Destination Sequenced Distance Vector Routing (DSDV) for Mobile Computers, ACM SIGCOMM, pages 234–244, Oct. 1994.

[32] Refik Molva and Pietro Michiardi, Security in Ad hoc Networks, Proceedings PWC 2003 (Personal Wireless Communications), September 2003.

[33] Yih-Chun Hu, Adrian Perrig, David B. Johnson, Ariadne:a secure on-demand routing protocol for ad hoc networks, Proceedings of the 8th annual international conference on Mobile computing and networking, September 2002.

[34] Y. Hu, D. Johnson, and A. Perrig, SEAD: Secure efficient distance vector routing for mobile wireless ad hoc Networks, Proceedings of WMCSA, Jun. 2002, pp. 3–13.

[35] A. Patwardhan, J. Parker, A. Joshi, A. Karygiannis and M. Iorga, Secure Routing and Intrusion Detection in Ad Hoc Networks, Third IEEE International Conference on Pervasive Computing and Communications, Kauaii Island, Hawaii, March 8-12, 2005.

[36] William Stallings, Wireless Communications and Networking, Prentice Hall,2002.