Kablosuz Ağlarda Güvenli Yönlendirme Protokolleri

Muhammet ÜNAL[1], M. Ali AKCAYOL[2*]

Gazi Üniversitesi, Mühendislik Mimarlık Fakültesi, Bilgisayar Mühendisliği Bölümü, Maltepe, 06570, Ankara
muhunal@gazi.edu.tr, akcayol@gazi.edu.tr

Özet— Mobil tasarsız ağlar kendi kendilerini otomatik olarak düzenler ve kablosuz iletişim yaparlar. Bir düğüm erişim mesafesi dışında olan düğümlerle diğer düğümler aracılığıyla paketlerin bir düğümden diğer düğüme iletilmesini sağlayarak haberleşebilmektedir. Kablosuz ağlarda iletişim herkese açık ortamda yapıldığı için veri güvenliğinin sağlanması kablolu ağlara göre daha zordur. Güvenliğin sağlanabilmesi için veri paketlerinin güvenli yollar seçilerek yönlendirilmesi gerekmektedir. Bu çalışmada kablosuz teknolojiler ve bu teknolojiler için önerilmiş güvenli yönlendirme protokolleri ele alınarak incelenmiştir. Bu protokollerin çözüm yöntemleri, avantajları ve dezavantajları araştırılmış ve birbirleriyle karşılaştırılmıştır. Son olarak güvenli yönlendirme için çalışma yapılabilecek araştırma konuları önerilmiştir.

Anahtar kelimeler— Güvenli yönlendirme, kablosuz ağlar

Secure Routing Protocols in Wireless Networks

Abstract— Mobile Ad-hoc Networks are self-organized automatically and communicate with each other. A node can communicate with any other node that is outside its wireless transmission range by forwarding packets hop by hop. Security is difficult in wireless networks compared to wired networks, because of the wireless medium. To assure security in wireless networks, data packets must be routed through secure paths. In this paper, wireless technologies and secure routing protocols proposed for these technologies are reviewed. Solution methods of the protocols, advantages and disadvantages are investigated, and compared with each other. Finally, future research directions for secure routing are given.

Keywords— Secure routing, wireless network

1. GİRİŞ

Haberleşme eski çağlardan itibaren insan hayatında çok önemli yer tutmaktadır. Bir zamanlar ulak ve duman gibi yöntemler ile uzun zaman alan ve kısa mesafelerde yapılan haberleşme, elektriğin bulunuşu ile yeni bir boyut kazanmıştır. 1820 yılında telgrafın icadı [1] ile bakır teller üzerinden başlayan kablolu iletişim insanların mobil haberleşme ihtiyaçları sonucunda telsiz ile kablosuz boyuta taşınmıştır. Bilgisayarların kullanılmaya başlaması ile bilgisayarlar arası haberleşme ihtiyacı ortaya çıkmıştır. Ethernet gibi kablolu teknolojiler kullanılarak gerçekleştirilen bilgisayarlar arası haberleşme, bu teknolojilerin kurulumunun zor ve maliyetli olması nedeniyle günümüzde yerini kablosuz teknolojilere bırakmaktadır [2].

Kablosuz teknolojiler iletim ortamı olarak açık havayı kullanmaktadırlar. Böylece herhangi bir fiziki bağlantıya ihtiyaç duymamaktadırlar. Bu nedenle kablosuz teknolojilerin getirdiği mekândan bağımsızlık büyük bir rahatlık sağlamaktadır.

2. KABLOSUZ TEKNOLOJİLER

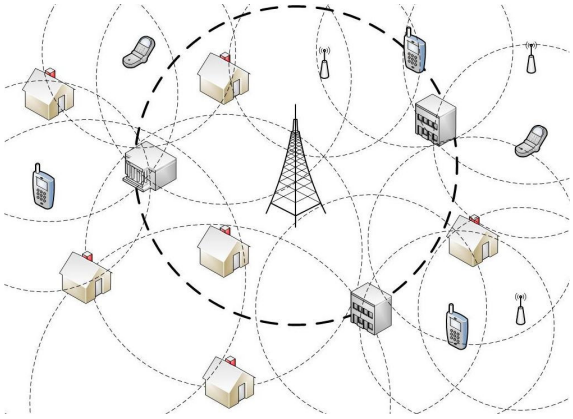
Kablosuz haberleşme 1895 yılında Guglielmo Marconi'nin Wight adasından 29 Km uzaklıktaki bir römorköre yaptığı yayın ile başlamıştır [1]. İlk kablosuz haberleşme teknikleri analogdur. Bugün kablosuz haberleşme sistemlerinin birçoğu dijital bitler kullanarak iletişim yaparlar. Bu haberleşme sürekli bit iletimi veya "paket radyo" adı verilen paketler halindeki bit grupları ile oluşmaktadır [3]. Kablosuz ağlarda paket tabanlı ilk network ALOHANET adında 1971 yılında Hawaii Üniversitesinde geliştirilmiştir [3]. 4 adaya dağılmış 7 kampüsteki bilgisayar merkezleri Oahu'da bulunan merkez bilgisayarı ile haberleşmiştir. Sistem, hub olarak merkez bilgisayarını kullanan yıldız topolojisinde bir ağ mimarisine sahiptir. Haberleşmek isteyen iki bilgisayar merkezi hub üzerinden haberleşmek zorundaydı. ALOHANET kanal erişimi ve yönlendirme

protokollerinin ilk şekillerini içermektedir [3]. ALOHANET'i oluşturan temel fikirler bugün hala kullanımdadır.

Kablolu ağların bant genişliğinin yeterli olması nedeniyle kablosuz ağların belirli bir standarda kavuşması zaman almıştır [2]. 1991 yılında Uluslararası Elektrik Elektronik Mühendisleri Enstitüsü (Institute of Electrical and Electronics Engineers-IEEE) öncülüğünde IEEE 802.11 grubu kurulmuştur. Bu grup 1999 yılında IEEE 802.11 standardını geliştirmiştir [4]. Bu standart açık alanda 100 metre gibi kısa mesafeler için 11 Mbps bağlantı hızı ile haberleşmeyi sağlayabilmektedir. Haberleşme mesafesi açısından bu standart kablosuz yerel alan ağları (Wireless Local Area Networks-WLAN) oluşturmaktadır [5]. Bu standartta merkezde bir erişim noktası (Access Point-AP) ve ona bağlı istasyonlar (Stations-STA) bulunmaktadır. STA'lar genelde AP kullanarak haberleşse bile kendi aralarında tasarsız bir ağ da kurabilirler. Bugün gelişen ihtiyaçlar ışığında, WLAN standardı olan IEEE 802.11 standardının IEEE 802.11a, 802.11b, 802.11g, 802.11n ve 802.11i gibi yeni versiyonları geliştirilmiş ve bu standart daha yaygın kullanılır hale getirilmiştir [6-9].

Daha geniş alanlarda kablosuz veri iletişimi için çalışmalar, 1996 yılında bazı telefon şirketlerinin DSL ve kablolu televizyon veri sistemlerinin yetersiz mesafeleri dolayısıyla alternatif genişbant kablosuz haberleşme sistemleri geliştirme çalışmalarıyla başlamıştır [5]. 1997 yılında genişbant İnternet erişimi için Cleary çok kanallı çok noktalı dağıtım sistemlerini (Multichannel Multipoint Distribution System-MMDS) geliştirmiş, 30 Mbps uygulamalı ve 27 Mbps kullanılabilir paylaşımlı hızlarla haberleşebilen 50 Km yarıçaplı sistem önermiştir [6]. 2000 yılında Agne Nordbotten yerel çok noktalı dağıtım sistemlerini (Local Multipoint Distribution System-LMDS) geliştirmiş, 38 Mbps uygulamalı, 25.6 Mbps kullanılabilir paylaşımlı hız ve 5 Km yarıçapa sahip sistemleri önermiştir ve bu sistemlerin kablolu sistemlerle karşılaştırmalarını yapmıştır [7]. Küçük köy ve kasabalar için bu sistemin daha uygun olabileceğini göstermiştir . IEEE bünyesinde kurulan Çalışma Grubu 16, 2002 yılında IEEE 802.16 standardını oluşturmuştur [8]. 802.16 standardı tek noktadan çok noktaya (Point to Multipoint-PMP) topolojisinde sadece sabit ve birbirini gören antenler arasında 10-66 GHz bant aralığında haberleşmeyi düzenlemektedir. Kullanılan bant genişliği ve modülasyon tipine göre 36-135 Mbps uygulamalı bant genişliğine sahiptir [9, 10].

2003 yılında birbirini görmeyen antenler için 2-11 GHz bant aralığını kullanan IEEE 802.16a standardı yayınlanmıştır [9]. Bu standart aynı zamanda mesh teknolojisini de desteklemektedir. Çeşitli hata düzeltmeleri ve düzenlemeler ile bu iki standart birleştirilerek 2004 yılında IEEE 802.16-2004 adı altında yayınlanmıştır[9]. 2005 yılında mobil kullanıcılar için IEEE 802.16e, 2006 yılında IEEE 802.16f, ve 2007 yılında IEEE 802.16g, IEEE 802.16k standartları düzenlenmiş ve bu standart diğer standartlarla beraber IEEE 802.16-2007 adı ile yayınlanmıştır [11]. Böylece IEEE 802.16-2007 standardı 2-11 GHz ile birbirini görmeyen antenlerin haberleşmesini, 10-66 GHz ile birbirini gören antenlerin haberleşmesini, 2-6 GHz ile mobil kullanıcıların haberleşmesini sağlayan toplu bir standart halini almıştır. IEEE 802.16 standardında mobil kullanıcıların maksimum veri iletişim ve hareket hızları sırasıyla 30 Mbps ve 30 Km/s'dir [11-14]. Hızlı tren gibi daha yüksek hareketlilik gerektiren hızlar için IEEE 802.20 mobil genişbant kablosuz erişim (Mobile Broadband Wireless Access-MBWA) standardına yönelik çalışmalar devam etmektedir. Şu anda taslak halinde olan çalışmalarda 250 Km/s hareket hızlarında ve 1-10 Mbps paylaşımsız hızları desteklemesi planlanmaktadır [15, 16]. Şekil 1.'de belirli bir altyapıya sahip fakat ana yapıya ulaşamayan düğümler için tasarsız aracı düğümlerin bulunduğu hibrit bir kablosuz ağ yapısı örnek olarak verilmiştir.



Şekil 1. Tasarsız aracı düğümlerin bulunduğu, anaçatıya sahip, hibrit bir kablosuz ağ yapısı örneği.

3. KABLOSUZ AĞLARDA GÜVENLİK ÇALIŞMALARI

Kablosuz ağların iletişim hızlarını ve erişim menzillerini arttırmak için yapılan çalışmaların yanı sıra bu ağların güvenliği konusunda da çalışmalar yapılmaktadır [20-31]. Kablosuz ağlarda veriler kablolu ağlarda olduğu gibi paketler halinde iletilmektedirler [17]. Gönderilen paketlerin içindeki bilgilerin, ağa karşı bozucu saldırılar yapılsa bile, hızlı bir şekilde ve değişmeden hedef adresine iletimi çok önemlidir. Veri paketlerinin ağ üzerinde takip edecekleri güvenli yolun hesaplanmasından yönlendirme protokolleri sorumludurlar. Kablolu ağlarda, paketlerin yönlendirilmesi amacıyla iç alan (intra-domain) ve dış alan (inter-domain) olmak üzere iki alan mevcuttur. İç alanda çoğunlukla mesafe vektörü (distance vector) yönlendirme protokolü veya bağ durumu (link state) yönlendirme protokolleri kullanılmaktadır. Dış alanda ise sınır kapısı (border gateway) yönlendirme protokolü kullanılmaktadır [17]. Bu protokoller daha çok hatların kopması veya düğümlerin bozulması gibi basit hata durumlarına yönelik tasarlanmışlardır [18]. Çünkü kablolu ağlarda saldırı gerçekleştirebilmek için o ağa

fiziksel olarak bağlı olmak gerekir. Bu nedenle kablolu ağlarda güvenlik ikinci planda kalmıştır. Fakat kablosuz ağlarda ağa bağlanmak için fiziksel bir bağlantı gerekmemektedir. Kablosuz bir ağa, gerekli donanımı bulunan herhangi bir kişi rahatlıkla erişebilmektedir. Ayrıca kablolu ağlarda yönlendirme görevi yönlendiricilerde olduğu halde kablosuz ağlarda bu görev çoğunlukla hem kablosuz yönlendiricilerin hem de o ağı kullanan mobil kullanıcıların sorumluluğundadır [19].
Kablosuz ağlarda bu nedenlerle güvenlik daha ön plandadır. Böylece kablosuz ağlarda yönlendirme protokolleri üzerinde güvenliğin arttırılmasına yönelik birçok çalışma yapılmıştır [20-31]. Bu bölümün geri kalan kısmında yapılan bu çalışmalar detaylı olarak incelenmiştir.

3.1. SEAD

Hu vd. [20] tarafından önerilen "Güvenli verimli ad hoc mesafe vektörü" (Secure Efficient Ad-hoc Distance Vector-SEAD) proaktif bir yönlendirme protokolüdür. "Hedef sıralı mesafe vektörü" (Destination Sequenced Distance Vector-DSDV) baz alınarak tasarlanmıştır [21]. DSDV ile ortak olan hedef, metrik, bir sonraki atlama (next hop) ve sıra numarası gibi alanların yanı sıra SEAD yönlendirme tablosu her giriş için bir hash değeri sağlamaktadır. İlgili makalede metrik ve sıra numaralarına saldırı düzenlenmesini engellemek için yönlendirme güncellemeleri konusu üzerinde durulmuştur. Önerilen güvenlik protokolünde tek yönlü hash zincir fonksiyonu olarak adlandırılan H fonksiyonu, anahtar özelliktir. Her düğüm $h_1, h_2, h_3, ..., h_n$ değerleri listesini hesaplamaktadır. h_0'ın rassal başlangıç değerine göre $0 < i \leq n$ alınarak $h_i = H(h_{i-1})$ hesaplanmaktadır. Makale h_n'in gönderilmek istenen tüm alıcılara dağıtım mekanizmasının var olduğunu kabul etmektedir. Bir düğüm H fonksiyonunu ve h_n değerini biliyorsa herhangi bir h_i değerini hesaplayıp h_n ile karşılaştırıp giriş doğrulama işlemini gerçekleştirebilmektedir. Yönlendirme güncellemesinin doğrulanması için her yönlendirme tablosu girişine bir hash değeri düğümler tarafından eklenmektedir. j metriği ve i sıra numarası ile h_{n-mi+j} değeri yönlendirme güncellemesi için doğrulamada kullanılmaktadır. Burada maksimum ağ çapı $m-1$ olarak alınmıştır. Saldırgan kendisine bildirilen hash değerinden daha küçük indeks değerlerine sahip bir hash değeri hesaplayamayacağı için, aynı hedefe daha büyük sıra numarası veya daha iyi bir metrik değeri ile yönlendirme bildiremeyecektir.
SEAD diğer düğümlerdeki sıra numarasını ve yönlendirme metriğini değiştirerek, yanlış yönlendirme durumları ortaya çıkarmaya çalışan saldırganlara karşı güçlü bir protokoldür. Fakat SEAD saldırganın bir sonraki atlama düğümü yanıltmasını veya yönlendirme güncellemesindeki hedef alanını değiştirmesini engelleyememektedir. Ayrıca saldırganın bir önceki güncellemeden öğrendiği sıra numarası ve metriği kullanarak başka bir hedefe yeni bir yönlendirme güncellemesi göndermesini engelleyememektedir [20].

3.2. ARIADNE

Hu vd. [22] "etkin talebe dayalı güvenli bir yönlendirme protokolü" (An efficient on-demand secure routing protocol-ARIADNE) önermişlerdir. Bu protokol simetrik kriptografiye dayanmaktadır. Düğümlerdeki yönlendirmelerin saldırıya uğramasının engellenmesi amaçlanmaktadır. ARIADNE ortam erişim kontrol (Media access control-MAC) adresi seviyesinde, iki düğüm arasında, paylaşılmış bir anahtar vasıtasıyla, yönlendirilmiş mesajların doğrulamasını sağlamaktadır. Fakat yönlendirilmiş mesajların güvenli olarak doğrulanması için "zaman etkin kaynak kayıp toleranslı doğrulama" (timed efficient stream loss-tolerant authentication-TESLA) yayın doğrulama protokolünü kullanmaktadır [23]. ARIADNE "dinamik kaynak yönlendirme" (dynamic source routing-DSR) temelli bir yapıdadır [19]. DSR gibi iki temel fonksiyon içermektedir ve yönlendirmenin keşfi ve bakımından sorumludur.
ARIADNE paylaşılmış anahtarların ve tek yönlü hash fonksiyonunun verimli bir bileşimini kullanmaktadır. Mesajın doğrulanması amacıyla alıcı ve verici için gizli bir anahtar paylaşılmaktadır. Şifreleme doğrulamayı sağlamaktayken hash mekanizmasıysa düğümler arası atlamanın doğruluğunu sağlamaktadır. Ölü bir bağın olması durumunda yönlendirme hata mesajı gönderilene iletilmektedir ve ara düğümler seçilen yoldaki ölü bağları kullanan yönlendirmeleri kaldırmaktadırlar. ARIADNE yönlendirme bilgisinin değiştirilmesine ve tekrar üretilmesi saldırılarına karşı önemli bir koruma sağlamaktadır. TESLA'nın gelişmiş bir versiyonu olan "geçici bağ" (Temporal Leashes-TIK) ile beraber kullanıldığında wormhole [24] saldırılarına karşı bağışıklık sağlamaktadır. Fakat bencil düğüm saldırılarına karşı açık bir yapısı bulunmaktadır. Gerçek hayatta kullanılması, anahtar değişimlerinin yapılması karmaşık olduğu için uyarlanması zordur [22].

3.3. SAR

Seung vd. [25] "güvenlik bilinçli yönlendirme" (security aware routing-SAR) protokolü önermişlerdir. Bu protokol "talebe dayalı mesafe vektör yönlendirme" (Ad-hoc on-demand distance vector routing-AODV) [26] tabanlı ve talebe dayalı bir yönlendirme protokolüdür. SAR bir düğümün güvenlik seviyesini ve yönlendirmenin güvenlik özelliklerini bir araya getirip kullanarak, istenen yönlendirme için kullanılmak üzere bütünleşmiş güvenlik metriği oluşturmaktadır. Yönlendirme metriği olarak güvenlik kalitesi (QoP-Quality of Protection) oluşturulmuş böylece yol keşfiyle güvenli yollar elde edilmiştir. QoP vektörü güvenlik seviyesi ile uygun kriptografik tekniklerin bir kombinasyonudur. SAR, hiyerarşi tabanlı bir notasyon oluşturarak, Tasarsız kablosuz ağların değişik güvenlik seviyelerine bölünmesini sağlamaktadır. Böylece kaynak ile hedef

noktası arasındaki haberleşmede görev alacak düğümler için gerekli olan minimum güvenlik seviyesini sağlamaktadır. Kablosuz olarak birbirine bağlı bir ağ olsa bile gerekli güven seviyesini sağlayacak yol olmayabilmektedir. SAR, AODV den daha az yol üretmesine rağmen oluşturulan bu yollar belirli bir güvenlik seviyesini sağlamaktadır [25].

3.4. SRP

Papadimitratos vd. [27] "güvenli yönlendirme protokolü" (Secure Routing Protocol-SRP) önermişlerdir. SRP yol keşfini engelleyecek saldırılara karşı koruma sağlamaktadır. Böylece sistemin topolojik bilgisinin doğru elde edilmesi garanti edilmektedir. SRP'de başlangıç ve hedef düğümleri arasındaki ara düğümler haberleşirken, verilerin kriptografik onaylanmasına ihtiyaç duymadan yapılabilmesi için düğümler arası güvenlik ilişkisi kurmak temel fikirdir. Bu güven ilişkisinin kaynak ve hedef arasında paylaşılacak ortak $K_{Gİ}$ anahtarı ile elde edilebileceği kabul edilmektedir. Bu güvenlik ilişkisinin yönlendirme başlangıç fazından daha önce var olması gerekmektedir [27].

3.5. ARAN

Sanzgiri vd. [28] "Tasarsız ağlar için güvenli bir yönlendirme protokolü" (a secure routing protocol for ad hoc networks-ARAN) önermişlerdir. ARAN talebe dayalı bir yönlendirme protokoldür. Bu protokol yönetilebilir açık ortamlarda güvenli haberleşmeyi sağlamak üzere tasarlanmıştır. Protokol açık anahtar altyapısını kullanmaktadır. Yönetilebilir açık ortamlardaki düğümler haberleşmenin başlangıcından önce birbirleriyle başlangıç parametrelerini paylaşırlar. Oturum anahtarları karşılıklı değiştirilir veya sertifika sunucusu gibi üçüncü şahıs üzerinden dağıtılır. ARAN'da her düğümün bir sertifikası vardır. Düğümler güvenilir sertifika sunucusuna kimliklerini güvenli bir şekilde doğrulattıktan sonra sunucudan bir sertifika alırlar. Düğümler bu sertifikaları kullanarak birbirlerinin doğrulamasını yaparlar ve yönlendirme mesajlarının iletimini gerçekleştirirler. Sertifika, düğümün IP adresini açık anahtarı ve sertifikanın başlangıç ve bitiş tarihini içermektedir. Bu alanlar sertifika sunucusu tarafından işaretlenir ve sabitlenir.

Doğrulama sırasında, hedef noktasına güvenli bir yol aranmaktadır. Ağdaki ara düğümlerin her biri iki adres tutmaktadır. Bu adresler bir önceki düğüm ile hedef düğüm adresleridir. Yönlendirme mesajındaki tüm bilgiler başlangıç düğümünün özel anahtarı tarafından işaretlenmiştir ve sabittir. Zaman damgası (t) ve özel bir sayı (N_I) dan oluşan bir bileşim, verinin yeni olup olmadığını ve zaman bilgisini kontrol etmektedir. Başlangıç düğümü her yönlendirme yolu için keşif isteğinde bulunduğunda N_I özel sayısı artmaktadır. İmza, yolu değiştirecek ve döngü oluşturabilecek spoofing saldırılarını engeller.

Güvenli yol oluşturma işlemi aşağıda kısaca açıklanmıştır. Kaynak düğümü ile hedef düğümü arasında iletişim için bir yol keşif paketi (YKP) yayınlanır [28]. İlk defa YKP'yi alan her düğüm diğer ara düğümlerin imzalarını çıkarır, daha sonra kendi anahtarı ile YKP'yi imzalar ve tüm komşu düğümlerine yayınlar. Bu olay hedef düğüme YKP paketi ulaşana kadar devam etmektedir. Hedef düğüm YKP paketini aldıktan sonra cevap paketini kaynak düğüme aynı yol üzerinden geri gönderir. Kaynak düğüm cevap paketini aldığında hedef düğümün imzasını ve N_I özel sayısını kontrol eder. Bu değerler doğru ise güvenli yol kurulumu tamamlanmış olur.

Düğümlerde yer alan yönlendirme tablolarında bulunan yönlendirme girdileri zaman aşımına uğrar ve belli bir süre kullanılmadıkları zaman otomatik olarak kaldırılırlar. Ayrıca hareketlilikten kaynaklanan yol kopmalarında düğümler hata mesajı göndererek göndericiyi uyarırlar.
ARAN önceden belirlenmiş kriptografik sertifikalar kullanarak, doğrulama ve inkâr etme gibi atakları engeller. Yapılan benzetimler yol keşfinde ve bu yolların yönetiminde başarılı olduğunu fakat paketlerin çok büyümeleri nedeniyle toplam yönlendirme yükünün ağır olduğunu göstermiştir. Ağır simetrik kriptografik hesaplamalar gerektirdiğinden enerji yönünden de başarılı değildir. Ayrıca wormhole saldırılarını engellemez. Eğer düğümler arasında zaman senkronizasyonu yoksa tekrar saldırılarına karşı da açıktır.

3.6. *SAODV*

"Güvenli AODV" (Secure AODV-SAODV), Zapata [29] tarafından önerilmiş AODV paketlerinin güvenli olarak iletilmesini sağlayan bir genişletme protokolüdür. AODV mesajlarının güvenliğini sağlamak amacıyla iki mekanizma kullanılmaktadır. Mesajın açık bölgeleri için sayısal imza ve atlama bilgisi için hash zincirleri kullanılmaktadır [29].
Protokol asimetrik kriptografi kullandığı için anahtar yönetim mekanizmasına ihtiyaç duymaktadır. Böylece bir düğüm ağda görev alan diğer düğümlerle güvenli bir haberleşme başlatabilir. Bir düğüm başka bir düğümle haberleşmek istediğinde Max_Atlama_Sayısı alanını IP başlığında bulunan yaşam süresi (Time To Live-TTL) bölümünden alır. Gönderilecek Top_Hash değerinin hesaplanması için Max_Atlama_Sayısı, rastgele çekirdek değeri kadar hash fonksiyonuna sokulur. Yol istek veya yol tekrarı alan bir düğüm Max_Atlama_Sayısı'ndan atlama sayısı çıkarılarak elde edilen değeri Top_Hash değeri ile karşılaştırılır.

SAODV diğer düğümlerdeki sıra numarasını ve yönlendirme metriğini değiştirerek yapılan saldırılara karşı dirençli olmakla beraber saldırganın yönlendirme güncellemesindeki hedef alanını değiştirmesini engelleyememektedir. Ayrıca saldırganın bir önceki güncellemeden öğrendiği sıra numarası ve metriği kullanarak başka bir hedefe yeni bir yönlendirme güncellemesi göndermesini engelleyememektedir [29].

3.7. SLSP

"Güvenli bağ durum protokolü" (Secure link state protocol-SLSP) kablosuz ağlar için proaktif düzenli bir bağ durum yönlendirmesi sunmaktadır [30]. Her düğüm kendisine R adet atlamadan oluşan bir alt ağ oluşturur. Oluşan bu alt ağ o düğümün haberleşme alanı olarak adlandırılır. Düğümlerin genel anahtar sertifikaları haberleşme alanlarında imzalanmış genel anahtar paketleri ile iletilir. Bağ durumu bilgisi peryodik olarak komşu bulma protokolü (NLP-Neighbour Location Protokol) ile yayınlanır [30].

Bir düğüm, bir bağ düğüm güncelleme paketi aldığında, paketi daha önce aldığı ve yedeklediği genel anahtarı ile doğrular, daha sonra atlama_sırası'nı ise tek yönlü hash tabloları ile doğrular.

SLSP zararlı düğümlere karşı çok etkili olmakla beraber, toplu yapılan saldırılara karşı etkili olamamaktadır [30].

3.8. FLSL

Nie vd. [31] "Bulanık mantık tabanlı güvenlik seviyeli yönlendirme protokolü" (fuzzy logic based security-level routing protocol-FLSL) önermişlerdir. Bu protokolde eldeki imkânlarla en yüksek seviyede güvenli iletişim sağlanabilmesi için bulanık mantık kullanılmaktadır. Protokolde anahtar uzunluğu (l) anahtar değiştirme frekansı (f) ve düğüm sayısı (n) alınmış ve çıktı olarak güvenlik seviyesi (s) belirlenmiştir. Bu değişkenler arasında $s \propto l \bullet f \bullet n^{-1}$ bağıntısı olduğu önerilmiştir. Bu denklemde güvenlik seviyesi (s) ile anahtar uzunluğu (l), anahtar değiştirme frekansı (f) ve düğüm sayısının tersi arasında bir doğru orantının olduğu önerilmiştir. Bu değerler bulanıklaştırılarak istenen güvenlik seviyesine ulaşılmaya çalışılmıştır [31].

Bu yöntem, diğer yöntemlerin parametrelerinin optimizasyonu konusunda yardımcı olma amaçlı olarak herhangi bir yönlendirme protokolüne ek olarak kullanılmaktadır. Böylece kullanılan sistemin imkanları dahilinde olabilecek en üst seviyede çalışması hedeflenmiştir.

FLSL beraber kullanıldığı protokolün avantaj ve dezavantajlarını göstermekle beraber, kullanılan protokolün, istenilen güvenlik seviyesi için optimum çalışmasını sağlar.

3.9. YÖNLENDİRME PROTOKOLLERİNİN AVANTAJLARI VE DEZAVANTAJLARI

Literatürde bulunan önemli kablosuz güvenli haberleşme protokolleri, bu protokollerin avantajları ve dezavantajları Çizelge 1.'de verilmiştir.

Çizelge 1. Literatürde bulunan önemli kablosuz güvenli haberleşme protokolleri, bu protokollerin avantajları ve dezavantajları.

Protokol	**Güvenlik Mekanizması**	**Avantajları**	**Dezavantajları**
SEAD [20]	Tek yönlü hash zincirleri	Saldırganın yönlendirme güncelleme paketlerine daha iyi metrik veya sıra numarası yerleştirerek saldırı düzenlemesini engellemektedir.	• DSDV ile beraber kullanılmaktadır. • Yönlendirme güncelleme paketlerini korumak için tasarlanmıştır. • Saldırganın diğer alanları değiştirmesini engelleyememektedir. • Saldırganın öğrendiği sıra numarası ve metriği kullanarak yeni yol güncellemeleri göndermesini engelleyememektedir.
ARIADNE [22]	Tek yönlü hash zincirleri	Saldırganın aralarında belirli bir anahtar anlaşması olmayan düğümlerin haberleşme yollarının değişmesini engellemektedir.	• DSR ile kullanılmaktadır. • Yönlendirme bilgisinin değiştirilmesi saldırılarını engellemektedir. • Bencil düğüm saldırılarına açıktır.
SAR [25]	Korunma kalitesi metriği	Yol güncelleme paketlerinde tekrar saldırılarını engellemek için sıra numaraları ve zaman damgaları kullanmaktadır.	• AODV ile beraber kullanılmaktadır. • Üretilen yol ara-düğüm sayısı anlamında en kısa yol olmayabilir, fakat daha güvenlidir. • Değiştirme ve üretim saldırılarına karşı koruma sağlamaktadır.
SRP [27]	Güvenli sertifika sunucusu	Yönlendirme keşfini engelleyen saldırılara karşı koruma sağlamaktadır. Böylece sistemin topolojik bilgisinin doğru elde edilmesi sağlanmaktadır.	• DSR ve ZRP ile beraber kullanılmaktadır. • Yönlendirme yönetim mesajları için doğrulama mekanizması bulunmamaktadır. • Wormhole saldırılarına açıktır.
ARAN [28]	Güvenli sertifika sunucusu	Doğrulama ve inkar edememe servisleri sağlamaktadır.	• AODV ve DSR ile beraber kullanılmaktadır. • Ağır asimetrik şifreleme hesapları gerektirmektedir. • Dakik zaman senkronizasyonu yoksa wormhole saldırılarına açıktır.
TESLA [23]	Tek yönlü hash fonksiyonu	Güvenli iletişim sağlamak için birbirine bağlı ve geciktirilmiş zaman senkronizasyonu kullanmaktadır.	• DoS saldırılarına açıktır. • Zararlı düğümler buffer overflow durumu oluşturabilmektedir.
SLSP [30]	• Tek yönlü hash fonksiyonu • Asimetrik Kriptografi	Çoklu düğüm saldırılarına karşı zayıftır.	• LSP ile beraber kullanılmaktadır. • Ağ küçük bölgelere bölünmüştür.
FLSL [31]	Bulanıklaştırılmış güvenlik parametreleri	Network büyüklüğüne ve diğer parametrelere göre sistem güvenliğini en üst seviyede tutulması amaçlanmaktadır.	Sybil ve wormhole saldırılarına açıktır.

4. SONUÇLAR VE ÖNERİLER

Bu çalışmada güvenli yönlendirme protokolleri araştırılmış ve SEAD, ARIADNE, SAR, SRP, ARAN, SAODV, SLSP ve FLSL protokollerinin avantaj ve dezavantajları sunulmuştur.

Tasarsız ağlar dinamik ve değişen bir topolojiye sahiptirler. Belirli bir altyapının bulunmaması nedeniyle düzenlenme ve denetlenme yetilerinden yoksundur. Ayrıca kanallar ve düğümler saldırıya açıktırlar.

Bu çalışmada, kablosuz ağlarda yapılan saldırılara karşı korunmak için önerilen yönlendirme protokolleri incelenmiştir. Önerilen protokollerde saldırılara karşı tek yönlü zincir hash fonksiyonlarının ve kriptografinin ön plana çıktığı gözlemlenmiştir. Her protokol belirli bir saldırıyı engellemek için çalışmış diğer saldırılarla ilgilenmemiştir. Her tür saldırıya karşı dirençli bir protokol ihtiyacı hala sürmektedir.

Önerilen çözümler çeşitli saldırılara karşı belirli bir seviyeye kadar güvenlik sağlasa da, çok sayıda kablosuz cihazın birbirleriyle hızlı, etkin ve güvenli haberleşmesini sağlayacak protokollere ihtiyaç duyulmaktadır.

KAYNAKLAR

[1] N. P. Reid, R. Seide, **Wi-Fi (802.11) Network Handbook**: Osborne/McGraw-Hill, 2002.

[2] A. Perrig, J. D. Tygar, **Secure Broadcast Communication in Wired and Wireless Networks**: Springer, 2003.

[3] N. Abramson, "Development of the Alohanet," Ieee Transactions on Information Theory, vol. 31, no. 2, pp. 119-123, 1985.

[4] B. P. Crow, I. Widjaja, J. G. Kimvd., "IEEE 802.11 wireless local area networks," Ieee Communications Magazine, vol. 35, no. 9, pp. 116-126, Sep, 1997.

[5] M. S. Kuran, T. Tugcu, "A survey on emerging broadband wireless access technologies," Computer Networks, vol. 51, no. 11, pp. 3013-3046, Aug 8, 2007.

[6] K. Cleary, "Internet via MMDS", **International Broadcasting Convention**, pp. 79-82, 1997.

[7] A. Nordbotten, "LMDS systems and their application," Communications Magazine, IEEE, vol. 38, no. 6, pp. 150-154, 2000.

[8] B. Fong, N. Ansari, A. C. M. Fongvd., "On the scalability of fixed broadband wireless access network deployment," Communications Magazine, IEEE, vol. 42, no. 9, pp. S12-S18, 2004.

[9] "IEEE Standard for Local and Metropolitan Area Networks Part 16: Air Interface for Fixed Broadband Wireless Access Systems," IEEE Std 802.16-2004 (Revision of IEEE Std 802.16-2001), pp. 1-857, 2004.

[10] M. Cao, W. C. Ma, Q. Zhangvd., "Analysis of IEEE 802.16 mesh mode scheduler performance," Ieee Transactions on Wireless Communications, vol. 6, no. 4, pp. 1455-1464, Apr, 2007.

[11] "IEEE Standards for Local and metropolitan area networks - Part 16: Air Interface for Fixed and Mobile Broadband Wireless Access Systems - Amendment 3: Management Plane Procedure and Services," IEEE Std 802.16g 2007 (Amendment to IEEE Std 802.16-2004), pp. 1-202, 2007.

[12] "IEEE Standard for Local and metropolitan area networks Part 16: Air Interface for Fixed and Mobile Broadband Wireless Access Systems Amendment 2: Physical and Medium Access Control Layers for Combined Fixed and Mobile Operation in Licensed Bands and Corrigendum 1," IEEE Std 802.16e-2005 and IEEE Std 802.16-2004/Cor 1-2005 (Amendment and Corrigendum to IEEE Std 802.16-2004), pp. 1-822, 2006.

[13] "IEEE Standard for Local and metropolitan area networks Part 16: Air Interface for Fixed Broadband Wireless Access Systems-Amendment 1: Management Information Base," IEEE Std 802.16f-2005 (Amendment to IEEE Std 802.16-2004), pp. 1-245, 2005.

[14] "IEEE Standard for Local and Metropolitan Area Networks Media Access Control (MAC) Bridges Amendment 5: Bridging of IEEE 802.16," 802.16k-2007 (Amendment to IEEE Std 802.1D-2004), pp. 1-14, 2007.

[15] W. Bolton, X. Yang, M. Guizani, "IEEE 802.20: mobile broadband wireless access," Wireless Communications, IEEE [see also IEEE Personal Communications], vol. 14, no. 1, pp. 84-95, 2007.

[16] "IEEE Draft Standard for Local and Metropolitan Area Networks - Standard Air Interface for Mobile Broadband Wireless Access Systems Supporting Vehicular Mobility - Physical and Media Access Control Layer Specification," IEEE Unapproved Draft Std 802.20/D4.1m, 2008.

[17] E. Cole, R. Krutz, J. W. Conley, **Network Security Bible**: Wiley Pub., 2005.

[18] H. Li, Z. Chen, X. Qinvd., "Secure routing in wired networks and wireless ad hoc networks," Technical Report, 2002.

[19] D. B. Johnson, D. A. Maltz, "Dynamic Source Routing in Ad Hoc Wireless Networks," Mobile Computing, 1996.

[20] Y.-C. Hu, D. B. Johnson, A. Perrig, "SEAD: secure efficient distance vector routing for mobile wireless ad hoc networks," Ad Hoc Networks, vol. 1, no. 1, pp. 175-192, 2003.

[21] E. P. Charles, B. Pravin, "Highly dynamic Destination-Sequenced Distance-Vector routing (DSDV) for mobile computers," SIGCOMM Comput. Commun. Rev., vol. 24, no. 4, pp. 234-244, 1994.

[22] Y. C. Hu, A. Perrig, D. B. Johnson, "Ariadne: A secure on-demand routing protocol for ad hoc networks," Wireless Networks, vol. 11, no. 1-2, pp. 21-38, Jan-Mar, 2005.

[23] A. Perrig, R. Canetti, D. Tygarvd., "The TESLA Broadcast Authentication Protocol," vol. 5, no. 2, pp. 2-13, 2002.

[24] Y. C. Hu, A. Perrig, D. B. Johnson, "Wormhole detection in wireless ad hoc networks," Department of Computer Science, Rice University, Tech. Rep. TR01-384, June, 2002.

[25] Y. Seung, N. Prasad, K. Robin, "Security-aware ad hoc routing for wireless networks", **Proceedings of the 2nd ACM international symposium on Mobile ad hoc networking and computing**, Long Beach, CA, USA, 2001,

[26] C. E. Perkins, E. M. Royer, "Ad-hoc on-demand distance vector routing", **Mobile Computing Systems and Applications, 1999. Proceedings. WMCSA '99. Second IEEE Workshop on**, pp. 90-100, 1999.

[27] P. Papadimitratos, Z. J. Haas, "Secure routing for mobile ad hoc networks", **SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2002)**, pp. 01.27-31, 2002.

[28] K. Sanzgiri, B. Dahill, B. N. Levinevd., "A secure routing protocol for ad hoc networks", **Network Protocols, 2002. Proceedings. 10th IEEE International Conference on**, pp. 78-87, 2002.

[29] M. G. Zapata, N. Asokan, "Securing ad hoc routing protocols", **3rd ACM workshop on Wireless security**, pp. 1-10, 2002.

[30] P. Papadimitratos, Z. J. Haas, "Secure Link State Routing for Mobile Ad Hoc Networks", **2003 International Symposium on Applications and the Internet**, pp., 2003.

[31] J. Nie, J. Wen, J. Luovd., "An adaptive fuzzy logic based secure routing protocol in mobile ad hoc networks," Fuzzy Sets and Systems, vol. 157, no. 12, pp. 1704-1712, 2006.