Tasarsız Ağlarda Yönlendirme Güvenliği Üzerine Kapsamlı Bir Araştırma

Yılmaz VURAL[1], Murat AYDOS[2]*, Mehmet TEKEREK[3]

[1,2]Hacettepe University, Computer Engineering Department, Ankara, Turkey
[3]Kahramanmaraş Sütçüimam University, Computer Education and Instructional Technology Department, Turkey
yvural@hotmail.com, maydos@hacettepe.edu.tr, tekerek@ksu.edu.tr

(Geliş/Received: 25.01.2015; Kabul/Accepted: 05.04.2016)
DOI: 10.17671/btd.64124

Özet— Tasarsız ağlar, paylaşılan kablosuz bir kanal üzerinde acil veya özel ağ çözümleri için alt yapısı olmadan hareketli düğümlerin bir araya gelmesiyle oluşan geçici ağlardır. Merkezi bir denetim mekanizmasının olmaması, kablosuz ortamların doğası, düğümlerin hareketliliği, ağa katılan her bir düğümün yönlendirici olarak görev yapması gibi nedenlerden dolayı tasarsız ağlar geleneksel ağlara göre daha savunmasızdır. Ancak tasarsız ağların bu topolojisi kişisel alan ağlarından kurtarma operasyonlarına kadar birçok uygulama içinde ideal bir ortam sunmaktadır. Çalışma kapsamında; tasarsız ağlarda tanımlanmış, güvenlik tehditleri veyönlendirme protokolleri incelenerek tespitler ve değerlendirmeler yapılmıştır. Çalışma ile tasarsız ağlarda mevcut yönlendirme protokollerinin güçlü ve zayıf yönleri tehditler farkındalığıyla incelenerek yapılan tespit ve değerlendirmelerin gelecekte ortaya konulacak yaklaşımlara katkı sağlaması hedeflenmiştir. Sonuç olarak yeni yapılacak olan çalışmalarda,güvenliğin temel unsurları olan gizlilik, bütünlük ve erişilebilirlik odaklı saldırılara karşı dirençli, enerji verimliliği yüksek, güvenlik-performans-enerji üçlüsünün ağırlıklarını ilgili probleme göre otonom olarak ayarlayabilecek yeni protokoller üzerinde durulması gerekmektedir.

Anahtar Kelimeler— Tasarsız ağlar, güvenik tehditleri, güvenli yönlendirme protokolleri

A Detailed Study on Routing Security for Ad Hoc Networks

Abstract— Ad-hoc networks are temporary networks, which use wireless media that consists of interconnected nodes without a common network infrastructure using wireless media for immediate and dedicated network solutions. Ad-hoc networks are much vulnerable against the threats compared to the traditional networks due to its nature of lacking of a central control mechanism and the individual attitude of each node. In this study, the security threats and the routing protocols defined for ad hoc networks are investigated and the findings are evaluated. The aim of the study is to reach a generalized conclusion on the existing routing protocols in ad-hoc networks by evaluating the advantages and disadvantages of these protocols. In this paper, it is shown that the routing and security protocols to be used in ad-hoc networks should be designed by providing a resistance, robustness and high energy efficiency in order to overcome security treats aiming for confidentiality, integrity and accessibility. The balance between resistance to threats, high energy efficiency and robustness should be carefully considered and implemented in an autonomous way by weighting each of them for a specific task.

Keywords— Ad-hoc Networks, security threats, secure routing protocols

1. GİRİŞ (INTRODUCTION)

Günümüzde istenilen her yerden her an işlerini yönetebilme ve yapabilme fırsatını veren mobil cihazların kullanımı oldukça yaygınlaşmış, mobil cihazlar üzerinden verilen hizmetlerin çeşitliliği artmıştır. Mobil cihazlardaki uygulamaların yaygın kullanılmasına bağlı olarak mobil cihazlar arasında altyapı gerektirmeyen doğrudan bilgi paylaşımını öngören düşük maliyetli ağ yaklaşımları ön plana çıkmaya başlamıştır. Ağlar altyapı gereksinimlerine göre; daha önceden kurulu bir altyapıya ihtiyaç duyan

geleneksel ağlar ve altyapı kurulumu gerektirmeyen tasarsız ağlar (Ad-Hoc) olmak üzere ikiye ayrılmaktadır [1].

Tasarsız ağ çatısı altında bilgi ve yetenek paylaşımı yapılarak bir sorunun çözülmesi amacıyla mobil ve diğer cihazlar bir araya gelmektedir.Bu ağlar acil veya özel durumlar için sabit bir ağ alt yapısı olmadan minimum yapılandırmayla kısa bir süre içerisinde çalışır hale gelmesi gerekmektedir. Sabit bir altyapıya ihtiyaç duyulmaması, düğümlerin hareketli olması gibi özelliklerinden dolayı kişisel alan ağlarından arama kurtarma faaliyetlerine kadar birçok alanda tasarsız ağlaraihtiyaç duyulmaktadır. Özgün yapıdaki bu ağlar savunma, eğitim, sağlık, ulaştırma vb. gibi birçok sektörde kendisine yaygın bir kullanım alanı bulmaktave nispeten yeni bir alan olarak dikkat çekmektedir.

Altyapısı olan planlı ağlarda ağ düğümleri erişim noktaları veya sabit baz istasyonları tarafından kapsanan alanlar içerisinde ağa bağlanarak birbirleriyle iletişim kurarlar. Paylaşılan bir kablosuz kanal üzerinde sabit altyapı olmadan kurulan tasarsız ağlarda düğümler kendi yapılandırmalarını merkezi bir yapıya ihtiyaç duymadan yapabilmektedir.Ağa katılan hareketli düğümler genellikle saldırıya açık güvensiz ortamlar üzerinden haberleşirler. Bir düğüm erişim mesafesindeki komşu düğümlerle doğrudan haberleşirken, komşu olmayan diğer düğümlerle ara düğümler üzerinden haberleşmektedir [2,3].

Güvenilir olmayan ortamlarda tasarsız ağlara dahil olan düğümler içerisinde kötü niyetli düğümlerin bulunmasıtasarsız ağlardaki güvenlik zafiyetlerinin başında gelmektedir. Ağa dâhil olan kötü niyetli düğümün yönlendirici olarak çalışmasıtasarsız ağlarda güvenliğin en zayıf halkasını oluşturmaktadır. Ağdaki paketlerinkötü niyetli düğümlerce bilinçli olarakyanlış yönlendirilmesiyle yapılan saldırıdan ağdaki bir düğümden ağın tamamına kadar geniş ölçekte tüm düğümler olumsuz olarak etkilenmekte ve yönlendirme güvenliği ön plana çıkmaktadır.

Yönlendirme güvenliği açısından geleneksel ve tasarsız ağlara farklı şekilde yaklaşmak gerekmektedir. Geleneksel ağlarda çalışan yönlendirme protokolleri,merkezi bir denetim ve koruma altında olduğundan ekstra güvenlik tedbirlerine ihtiyaç duymamaktadır.Ancak buna karşın değişken ve hareketli topolojiye sahip olan güvensiz ortamlar üzerinden haberleşen dinamik yapıdaki tasarsız ağlarda yönlendirme protokollerinin güvenlik bakış açısıyla iyileştirilmesi ve saldırılara karşı dirençli hale getirilmesi gerekmektedir.

Temel bilgi güvenliği ilkesi olan en zayıf halkanız kadar güvendesiniz yaklaşımı dikkate alındığında tasarsız ağların en zayıf halkasını yönlendirme işlemleri oluşturmaktadır. Saldırılara karşı dirençli yönlendirme protokollerinin kullanılması tasarsız ağlarda yüksek seviyede güvenliğin sağlanması açısından oldukça önemlidir. Kaynakların kısıtlı olduğu, düğümlerin, topolojinin ve bağlantı durumunun değişken olduğu tasarsız ağlarda geleneksel yönlendirme protokolleri yerine bu ağlara özgü geliştirilen yönlendirme protokolleri kullanılmaktadır [4]. Tasarsız ağlar için geliştirilen yönlendirme protokolleri kötü niyetli düğümlerin davranışlarını engelleyebilmekte ve yüksek seviyede güvenliğin sağlanmasına katkıda bulunmaktadır.

Alanyazında tasarsız ağlarda güvenliğin sağlanabilmesi amacıyla güvenli yönlendirme protokolleri konusunda çeşitli çalışmalar bulunmaktadır[4,5]. Bu çalışmalar incelendiğinde tasarsız ağlarda yüksek düzeyde güvenliğin sağlanamadığı tespit edilmiştir. Bilinen ve her geçen gün çeşitlenerek artan saldırılara karşı dirençli olan güvenli yönlendirme protokollerine duyulan ihtiyaç devam etmektedir. Yönlendirme protokollerinin saldırılardan asgari düzeyde etkilenmesi ve saldırılara karşı dirençli olabilmesi için güvenlik bakış açısıyla yeniden ele alınması gerekmektedir.

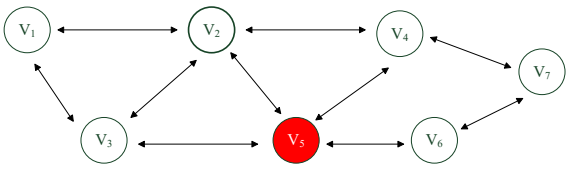
Çalışma kapsamında tasarsız ağların yapısı ve bu ağlara uyarlanmış yönlendirme protokolleri özetlenerek güvenlik tehditleri incelenmiş, alan yazında tasarsız ağlarda yönlendirme güvenliğinin sağlanabilmesi için sunulan güvenli yönlendirme protokolleri sunulmuştur.Çalışma ile, tasarsız ağlarda mevcut yönlendirme protokollerinin güçlü ve zayıf yönlerinin tehditler farkındalığıyla incelenerek yapılan tespit ve değerlendirmelerin gelecekte ortaya konulacak yaklaşımlara katkı sağlaması hedeflenmiştir.

Sonuç olarak; bilgi toplumunun ayrılmaz bir parçası olacak olan tasarsız ağlarda, güvenliğin temel unsurları olan gizlilik, bütünlük ve erişilebilirlik odaklı saldırılara karşı dirençli, enerji verimliliği yüksek, güvenlik-performans-enerji üçlüsünün ağırlıklarını ilgili probleme göre otonom olarak ayarlayabilecek yeni yaklaşımlara ihtiyaç vardır.

2. TASARSIZ AĞLAR ve YÖNLENDİRME PROTOKOLLERİ (AD-HOC NETWORKS and ROUTING PROTOCOLS)

2.1. Tasarsız Ağlar (Ad-Hoc Networks)

Hareketli düğümlerin doğrudan birbirleriyle bağlantı kurarak haberleşmelerini sağlayan tasarsız ağlar 1970'li yılların başlarında ortaya çıkmıştır [6]. Belli bir amacı gerçekleştirmek üzere, düğümlerin işbirliği çerçevesinde üzerlerine düşen görevleri otonom olarak gerçekleştirmesi ve yardımlaşması esasına dayanan tasarsız ağlar, mobil veya sabit düğümler tarafından dinamik olarak herhangi bir altyapı gereksinimi olmadan otonom bir yapıda kurulmaktadır. Şekil-1'de 7 düğümden oluşan örnek bir tasarsız ağın temsili gösterimi verilmiştir.



Şekil 1. Tasarsız ağların temsili gösterimi

Şekil-1 incelendiğinde V_5 düğümünün saldırı yapmak üzere ağa katılan kötü niyetli bir düğüm olduğu görülmektedir. Tasarsız ağlarda, düğümler iletişim kuran istemci rolü dışında, altyapı olmamasına bağlı olarak diğer komşu düğümlere ağ paketlerini ileten bir yönlendirici olarak da görev yapmaktadır. Tasarsız ağları geleneksel ağlardan ayıran en önemli özelliklerin başında komşu düğümlerin doğrudan birbirleriyle haberleşmesi gelmektedir.

Komşu düğümler tek bir atlama (single-hop) ile uzaktaki düğümler ise çoklu atlamalarla (multi-hop) birbirleriyle haberleşmektedir. Ağ'da komşu olmayan düğümler doğrudan haberleşemediğinden, düğümlerin haberleşmesi kaynak ile hedef düğüm arasındaki ara düğümler üzerinden çoklu atlama ile sağlanmaktadır. Birçok farklı uygulamayı destekleyecek esneklikte olan tasarsız ağlar oldukça geniş alanda kullanılmaktadır [7].

Kişisel haberleşmeler, ortak yaşam alanlarında bulunan kitleye mobil cihazlar üzerinden duyuru reklamların yapılması, acil durumların takip edilebilmesi (polisiye vakalar, yangın söndürme, doğal afetler, arama kurtarma, kriz yönetimi vb.), askeri operasyonlar (taktik saha operasyonları, tatbikatlar, görev güçleri vb.), ev ağları, eğitim uygulamaları, sağlık uygulamaları; tasarsız ağların kullanıldığı alanlardan bazılarıdır. Duyarga teknolojisindeki gelişmeler tasarsız ağların her geçen gün yeni uygulama alanları bulmasını sağlamaktadır.

Tasarsız ağlar geleneksel ağlar ile karşılaştırıldığında, altyapıların kurulumu, bakımı ve idamesi noktasında maliyetleri oldukça düşük olmasına rağmen, özgün yapısından kaynaklanan önemli zorlukları beraberinde getirmektedir [8,9].Tasarsız ağların zorlukları aşağıda maddeler halinde verilmiştir.

- *Güvenlik:* Ağa katılan güvensiz düğümlerin olması, kötü niyetli düğümlerin aynı anda hem kullanıcı hemde yönlendirici olması, kablosuz ortamların kullanılması, temel ağ güvenlik bileşenlerinin olmaması,
- *Sınırlı kaynaklar:*İletişim için kullanılan kablosuz kanalın sınırlı bant genişliğine sahip olması, mobil düğümlerin pil ömrünün az ve yetersiz olması,
- *Değişken topoloji:* Ağdaki ani değişikliklere göre yolların yeniden oluşturulması, paket kayıplarına veya saldırılara bağlı olarak yolların bozulması vb. gibi sebeplerden dolayı tasarsız ağlarda değişken bir ağ topolojisine sahip olunması,
- *Heterojen düğümler:* Ağa dâhil olan düğümlerin, dizüstü bilgisayarlar, kişisel sayısal asistanlar, akıllı telefonlar ve akıllı sensörler gibi heterojen yapıdaki cihazlardan oluşması,
- *Dağıtık Yapı:*Ağa katılan düğümlerin belirli bir coğrafi alana yayılan bağımsız düğümlerden oluşmasından dolayı ağda dağıtık bir yapı olması,
- *Birlikte çalışabilirlik:* Ağ'ın bakım ve idame görevleri, eşleme ve işbirliğine dayalı olarak düğümler arasında paylaşım esasına göre yapıldığından dağıtık çevredeki düğümlerin işbirliğinin sağlanması

gibi zorluklar çözümlenmesi ve göz önünde bulundurulması gereken zorluklardır.

Bu çalışma kapsamında tasarsız ağların önemli zorluklarından birisi olan güvenlik konusuna ayrıca değinilmiştir. Dinamik ağ topolojisi, kaynak kısıtları, kablosuz paylaşım ortamları, fiziksel açıdan savunmasız düğümler, uçtan uca ağ mimarisi, düğümlerin yönlendirici rolleri, merkezi bir denetim mekanizmasının olmaması gibi ağın yapısal özellikleri önemli güvenlik tehditleri olarak karşımıza çıkmaktadır [9].

2.2. Tasarsız Ağlarda Yönlendirme (Routing in Ad-Hoc Networks)

Tasarsız ağlarda yüksek hareketlilik, düşük enerji tüketimi gibi ağa özgü gereksinimleri dikkate alan yönlendirme protokolleri kullanılmaktadır. Kurulu bir ağ altyapısı ve bileşenlerinin (yönlendirici, anahtar, vb.) olmamasına bağlı olarak tasarsız ağlarda yönlendirme işlemi kaynakları ağa dâhil olan düğümler tarafından yapılmaktadır. Düğümler yönlendirme görevlerini, tasarsız ağların kısıtlarına uygun olarak tasarlanmış yönlendirme protokolleri aracılığıyla yapmaktadır. Yönlendirme protokolleri, kaynak düğümden hedef düğüme gönderilecek paketler için en uygun yolun bulunması ve yönlendirme mesajlarının düğümler arasında paylaşımının yapılmasını sağlarlar[10].

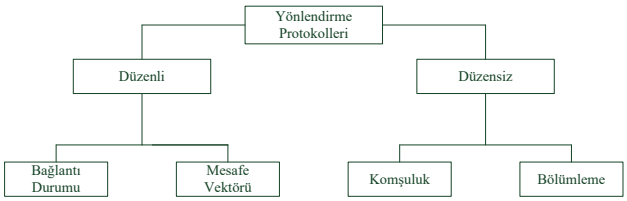
Düğümler birer yönlendirici olarak davranıp yönlendirme protokolleri ile işbirliği içinde çalışmak zorundadır. Yönlendirme bilgisinin değişimi, kaynak ile hedef arasındaki en uygun yolun bulunması, yolların bakımı, trafiğin en aza indirgenmesi, dinamik yapıdaki ağ topolojisinin güncel olarak tutulabilmesi yönlendirme protokollerinin görevlerinden önemli olanlarıdır. Mobile Ad-hoc Networks (MANET) çalışma grubu tasarsız ağlardaki yönlendirme protokolleri ile ilgili standardizasyon çalışmalarını yönetmektedir [11].

Tasarsız yönlendirme protokollerinin gereksinimleri aşağıda maddeler halinde verilmiştir

- En az gecikmeyle en kısa yolun bulunması,
- Bozulan yolların çıkartılarak yolun yeniden hızlı bir şekilde hesaplanabilmesi,
- Dağıtık olarak çalışabilmesi,
- Kaynakları etkin kullanması
- Ağın büyüklüğüne göre ölçeklenmesi
- Hizmet kalitesi desteği verebilmesi,
- Zamana duyarlı trafik desteğinin verilebilmesi,
- Saldırılara karşı dirençli olması.

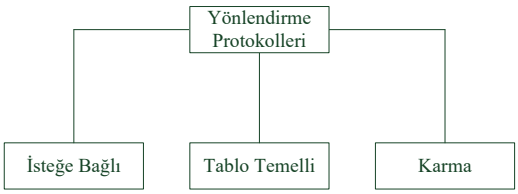
Tasarsız ağlarda görev yapan yönlendirme protokollerini ağ içerisinde yaptıkları görev dağılımına göre düzenli ve düzensiz olarak iki sınıfa ayırmak mümkündür.Düzensiz

olarak çalışan protokoller komşuluk ve bölümleme yöntemiyle yönlendirme yaparken düzenli görev dağılımıyla çalışan protokoller ise bağlantı durumu veya mesafe vektörüne göre yönlendirme yapmaktadır [12]. Tasarsız ağlarda düğümlerin görevlerine göre kullanılan yönlendirme protokollerinin sınıflandırılması Şekil-2'de gösterilmiştir.



Şekil 2. Düğüm görevlerine göre sınıflandırma

Yönlendirme protokollerini, yönlendirme bilgilerinin bulunması ve güncellenmesi mekanizmalarına göre reactive (isteğebağlı),proactive (tablo temelli) ve hybrid (karma) olmak üzere üç gruba ayrılmakta ve Şekil-3'de verilmektedir [13].



Şekil 3. Yönlendirme yöntemlerine göre sınıflandırma

İsteğe bağlı yönlendirme protokolü, bir düğüm tarafından ihtiyaca bağlı (on-demand) olarak yol bulma sürecinin başlatılması esasına göre çalışır. Bu yaklaşımda yolların keşfedilmesi ve yolların bakımı olmak üzere iki ana operasyon yapılmaktadır. İsteğe bağlı yaklaşımda kaynak düğüm tasarsız ağ içerisinde gideceği hedef düğüm için yayın (broadcast) isteği başlatır. Yayın sürecinde, kaynakla hedef arasındaki keşfedilen ara düğümler hafızaya alınarak yol bulunur. Hedef düğüm isteği aldığında, kaynak düğüm ile iletişimi sağlamak için belirlenen bu yolu tersine doğru kullanır. Ad-Hoc On-demand DistanceVector (AODV), Dynamic Source Routing (DSR), TemporallyOrdered Routing Algorithm (TORA), FlowState in theDynamic Source Routing Protokol(FSDSR), Power-Aware DSR-based Protocol isteğe bağlı yaklaşımla çalışan protokollere örnek olarak verilebilir [14,35,36].

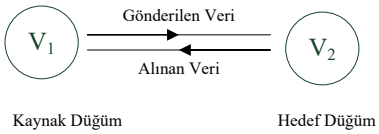
Tablo temelli yönlendirme protokolü, düğümlerde yerel yönlendirme tablolarının tutulması ve bu tabloların yönetilerek, her bir ağ düğümündeki ağ topolojisi bilgilerinin periyodik olarak güncel tutulması esasına dayanmaktadır. Tablo temelli yönlendirme yaklaşımında, düğümlerdeki topoloji bilgisi ile ilgili değişimler düzenli olarak güncelleştirilen ve düğümün kendisi tarafından bakımı yapılan yönlendirme tablosunda tutulmaktadır. Her düğüm kendisine doğrudan bağlı olan komşu düğümlerin listesini belirleyip yerel yönlendirme tablosunu oluşturduktan sonra topoloji kontrol mesajlarını yayın yöntemi ile diğer düğümlerle periyodik zaman aralıklarında duyurur.

Ağ topolojisinin dinamik olmasına bağlı olarak meydana gelecek çok sayıdaki tablo güncellemesi düğümlerdeki kısıtlı kaynakların tüketilmesini olumsuz etkileyecektir. Ancak yol bulmadaki gecikmenin düşük olması sebebiyle gerçek zamanlı trafikler için iyi sonuçlar verecektir. Destination Sequence Distance Vector (DSDV), Wireless Routing Protcol (WRP), ZHLS (Zone-basedHierarchical Link State Routing Protocol), Optimized Link State Routing (OLSR) tablo temelli protokollere örnek olarak verilebilir [15].

Hibrid yaklaşımda, her iki yaklaşım yönteminin birlikte kullanılmasıyla kontrol yükü ve gecikme arasında bir denge sağlanarak etkin bir yönlendirme yaklaşımı ortaya koyulmaya çalışılmıştır. Karma yaklaşımda ağ bölgelere ayrılır ve her bölge içinde farklı düğümler bulunur. Bölge içinde kalan düğümler kendi aralarında tablo temelli yönlendirme kullanılırken, bölge dışında kalan düğümler arasında isteğe bağlı yönlendirme yaklaşımı kullanılmaktadır. Zone Routing Protocol (ZRP), Core Extraction Distributed Ad Hoc Routing Protocol (CEDAR) karma yaklaşımla geliştirilmiş olan protokollerdir [16,37,38].

3. TASARSIZ AĞLARDA GÜVENLİK(SECURITY IN AD-HOC NETWORKS)

Bilgi güvenliğinin sağlanmasında uyulması ve uygulanması gereken birçok güvenlik unsuru vardır. Tasarsız ağlarda gizlilik, bütünlük, erişilebilirlik, kimlik doğrulama, mahremiyet ve inkâr edememe sağlanması gereken önemli güvenlik unsurlarıdır. Tasarsız ağlarda iki düğüm arasındaki normal haberleşmeyi gösteren temsili çizim Şekil-4'de verilmiştir. Normal haberleşmede kaynak düğümden çıkan bilgi bütünlüğü bozulmadan hedef düğüme iletilir.



Şekil 4. İki düğüm arasındaki normal haberleşme

Saldırılara açık ve geleneksel ağlara göre daha savunmasız olan bu ağlarda, kötü niyetli bir düğüm önlem alınmadığı takdirde ağdaki yetkisi olmayan trafiği izleyebilir, değiştirebilir, silebilir, kısıtlı ağ kaynaklarını bilinçli olarak tüketebilir, kötü niyetli diğer düğümlerle işbirliği yaparak ağı kullanılmaz hale getirecek saldırılar yapabilir.

Tasarsız ağlarda, düğümlerin yönlendirici olarak çalışmaları, saldırıya açık kablosuz ortamlardan haberleşmelerin yapılması, düğümlerin fiziksel olarak zayıf korunması, saldırgan düğümün ağa katılmasında merkezi bir kontrol mekanizmasının olmaması güvenlik

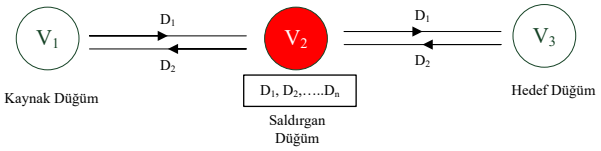
açısından dikkat edilmesi gereken hususların başında gelmektedir. Ağ katmanında yapılan saldırılar yönlendirme protokollerinin zafiyetlerini kullanan kötü niyetli düğümlerin komşularına yanlış yol bilgisi vermesi veya komşularından gelen paketleri yanlış düğümlere yönlendirmesi esasına dayanmaktadır [17].

Saldırılar, düğümlerin yetkilerine göre iç veya dış, ağdaki trafiğin etkilenmesine göre aktif veya pasif saldırılar olarak sınıflandırılmaktadır. Dış saldırılarda, kimlik doğrulaması yapmamış ve ağın dışında olan saldırgan düğüm büyük hacimli sahte yönlendirme bilgilerini ağa enjekte ederek tıkanıklığa sebep olacak saldırılara odaklanmıştır. İç saldırılarda, kimlik doğrulaması yapmış olan ve ağın bir parçası olan saldırgan ağ kaynaklarını ve yetkilerini kötüye kullanarak ağ genelini tehdit eden daha ciddi saldırılara odaklanmıştır. Ağ içerisinden yapılan saldırıların tespit edilmesi dışarıdan yapılan saldırılara oranla daha zordur.

Pasif saldırılar, ağın normal çalışmasını etkilemeyen gizlilik ihlaline sebep olan dinleme ve izleme amaçlı saldırılar olup tespit edilmesi oldukça zordur. Aktif saldırılar, ağın normal çalışmasını bozan gizlilik, bütünlük ve erişilebilirlik ihlallerine sebep olan içten veya dıştan yapılan saldırılardır [18]. Tasarsız ağlarda saldırganlar tarafından kullanılan güvenlik tehditleri takip eden alt bölümlerde açıklanmıştır.

3.1. Dinleme (Eavesdropping)

Kablosuz ortamlarda ağ üzerinden iletilen yönlendirme paketlerinin dinlenerek analiz edilmesine yönelik saldırıların yapılmasında kullanılan pasif saldırı yöntemidir. Bu yönteme ait temsili çizim Şekil-5'de verilmiştir. Saldırgan üzerinden geçen veri trafiğini dinleyerek kayıt eder ve tüm haberleşmeyi yetkisi olmadan dinler.



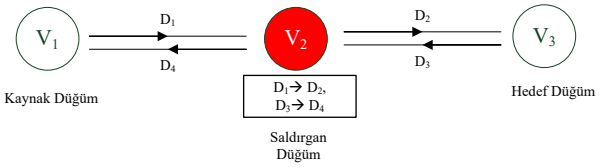
Şekil 5. Dinleme saldırısı

Bu yöntemde, saldırgan ağın çalışmasına müdahale etmez, ağ trafiğini üzerinden geçirerek dinler ve yetkisi olmayan bilgileri elde ederek analizler yapar. Tasarsız ağlarda bu yöntem ile yapılan saldırıları güvenlik çözümlerinin fark etmesi genellikle zordur. Bu yöntemle ağdaki düğümlerin yerlerinin tespit edilmesi, ağ topolojisinin çıkartılması, kritik düğümlerin tespit edilmesi gibi ağ için çok önemli olan bilgilere saldırgan düğümün dinlediği bilgiler analiz edilerek erişilebilecektir.

Saldırgan, dinleme ve izleme yöntemiyle elde ettiği bu bilgileri aktif saldırı yöntemlerini kullanarak çok daha etkin saldırılar düzenleyebilecektir. Fiziksel erişimin önemli bir kısıt olduğu dinleme ve izleme saldırılarına karşı kablosuz ortamlar daha savunmasız olduğundan tasarsız ağlarda gizlilik ihlalleri ciddi saldırıların ilk aşamasını oluşturmaktadır. Bu saldırı ağ üzerindeki bilgilerin gizlilik ve mahremiyetini hedef alan tespit edilmesi oldukça zor olan saldırılardır [19].

3.2. Değiştirme (Modification)

Değiştirme yöntemiyle, saldırgan yönlendirme mesajlarının içeriğini değiştirerek ağdaki paketlerin bütünlüğüne yönelik saldırılar gerçekleştirir. Tasarsız ağlarda düğümlerin hareketliliği ve merkezi bir denetim mekanizması olmamasına bağlı olarak kötü amaçlı düğümler sahte mesajlarla diğer düğümleri kandırarak ağdaki etkinliklerde kendilerini ön plana çıkartıp mesaj değiştirme saldırıları yaparlar. Değiştirme saldırılarına ait temsili gösterim Şekil-6'da verilmiştir. Saldırgan düğüm üzerinden geçen trafiği amaçları doğrultusunda değiştirerek verinin bütünlüğünü bozarak veri değiştirme saldırışını yapar.



Şekil 6. Değiştirme saldırısı

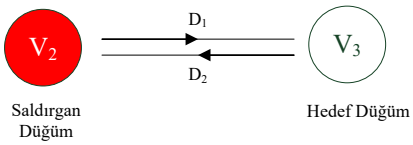
Değiştirme yöntemiyle yapılabilecek saldırıların başında paketlerin yanlış yönlendirilmesi (misrouting) gelmektedir. Saldırgan düğüm, paketleri yanlış hedefe yönlendirerek paketlerin ağda gereksiz yere dolaşmasına ve yaşam süresi dolunca paketlerin ağdan düşmesine sebep olacaktır. Paketlerin ağda dolaşması ağ genelinde tıkanıklığa yol açarken, paketleri orijinal hedefine ulaştıramayan kaynak düğüm sürekli olarak yeniden paket üreteceği için kısıtlı olan enerjisini ve bant genişliğini gereksiz yere tüketecektir [20].

Kara Delik (Black Hole) değiştirme saldırı yöntemini kullanan diğer bir aktif saldırı tipidir. Saldırgan düğüm, şifresiz olarak iletişim yapan iki düğümün arasına kendisini konumlandırdığında, paketler üzerinde her türlü değişikliği yapabilir. Kara delik saldırısında kötü niyetli düğüm ağdaki yönlendirme isteklerine yanlış cevaplar vererek en kısa yol olarak kendisini komşularına tanıtır ve gelen tüm paketleri üzerine alır. Kötü niyetli düğüm üzerine aldığı tüm paketleri silerek hizmet engelleme saldırısı yapabilir veya saldırının anlaşılmaması amacıyla paketleri dinleyerek gerçek yoluna yeniden yönlendirebilir [21].

Solucan Deliği (Worm Hole) değiştirme saldırı yöntemini kullanan diğer bir aktif saldırı tipidir. Bu saldırıda iki kötü niyetli düğümün işbirliğine ihtiyaç duyulmaktadır. İşbirliği yapan kötü niyetli düğümler birbirleri arasında yüksek iletişim kalitesine sahip bir kanal oluştururlar. Daha sonra yönlendirme için bu kanalın duyurusunu yaparak çevredeki düğümlerden paket toplarlar. Bu kanal üzerinden geçen paketler gerçek hedefine iletilmezler veya değiştirilerek iletilirler [22].

3.3. Uydurma (Fabrication)

Uydurma yöntemiyle yapılan saldırılarda, saldırgan diğer düğümlerin kaynaklarını tüketmek veya ağın işleyişini bozmak amaçlı ağda karmaşaya neden olacak yanlış yönlendirme mesajlarını (güncellemeleri, hata mesajları, vb.) kendisi oluşturarak ağa duyurur. Uydurma saldırısına ait temsili gösterim Şekil-7'de verilmiştir. Bu yöntemi kullanan kötü niyetli bir düğüm diğer düğümlerin kaynaklarını tüketmek için ağda mevcut olmayan bir düğüme yönlendirme yapabilir veya yapacağı gereksiz duyurularla diğer düğümlerin enerjilerini tüketerek hizmet aksattırma saldırılarını gerçekleştirebilir.



Şekil 7. Uydurma saldırısı

Uydurma yöntemiyle yapılan hizmet aksattırma saldırıları sonucunda, yönlendirme fonksiyonu tamamen bozulur ve ağın çalışması tamamen durur. Yönlendirme mesajı çoklama (route salvaging), uykudan uyandırma (sleep deprivation) ve yeniden oynatma (replay) bu yöntem ile yapılabilecek saldırı tiplerine örnek olarak verilebilir.

Tasarsız ağlar kaynak düğümden gönderilen paketlerin hedef düğüme başarılı şekilde ulaşmasını garanti edemezler. Yönlendirme mesajlarının çoklanması saldırıları, kötü niyetli açgözlü (greedy) ara düğümler tarafından yapılır. Saldırılar veya ağda meydana gelen arızalardan dolayı hedefine ulaşmayan paketler kaynak düğüm tarafından yeniden oluşturularak hedefine yollanır. Bu saldırı yönteminde kaynak ile hedef arasında yer alan kötü niyetli ara düğümler herhangi bir hata mesajı almamalarına rağmen paketleri yeniden oluştururlar ve ağ üzerinde birçok kopya paketler oluştururlar. Gereksiz paketlerle uğraşan ara düğümler ve hedef düğümler kısıtlı olan enerjilerini boşa harcarken, ağda bulunan birçok gereksiz kopya paket bant genişliğini boş yere tüketerek sıkışıklığa yol açarlar [23].

Ağdaki düğümler enerjilerini verimli kullanabilmek amacıyla ağda etkin olmadıkları zaman diliminde uyku durumuna geçerek enerjilerini verimli kullanırlar. Uykudan uyandırma yöntemiyle yapılan saldırılarda kötü niyetli düğüm, ağda yer alan düğümlerin enerjisini bitirmeye yönelik gereksiz paketlerin gönderilmesi, ihtiyaç duyulmayan yolların sorgulanması gibi yöntemlerle mobil düğümleri devamlı ağda aktif ederek kısıtlı olan enerjilerini tüketmeye çalışır [24].

Yeniden oynatma saldırısında ise, kötü niyetli düğüm daha önceden kayıt ettiği trafiği ağa enjekte ederek tekrar saldırısını gerçekleştirir. Ağ yönlendirmesine doğrudan yapılan bir saldırı türüdür. Saldırgan daha önce gönderilmiş paketleri dinleme yöntemleriyle kayıt edip farklı bir zamanda hedef düğüme yeniden göndererek yönlendirme döngüleri oluşturmaya, trafiği kendi belirlediği düğümler üzerine çekmeye, yollarını uzatmaya ya da kısaltmaya, ağı parçalara ayırmaya, sahte hata mesajları üretmeye ve noktadan-noktaya gecikmeyi artırmaya çalışır. Görünüşte normal ağ davranışları sergilenerek yapılan bu saldırıların tespit edilmesi oldukça zordur.

3.4. Kesme (Interrupt)

Kesme yöntemiyle yapılan saldırılar, kaynak düğüm ile hedef düğüm arasındaki paketlerin iletimine engel olmak amacıyla yapılır. Kötü niyetli ara düğümler yönlendirme mesajlarının hedef düğümlere ulaştırılmasını engellemek amacıyla yönlendirme mesajlarına müdahale ederler. Ayrıca doğrudan hedef düğüme saldırı düzenlenerek hedef düğümün erişilemez hale getirilmesiyle de saldırı gerçekleştirebilir.

Ağın normal işleyişini engelleyen kesme saldırılarının yapılabilmesi için uydurma, değiştirme ve dinleme yöntemiyle yapılan saldırılardan yararlanılır. Örneğin, saldırgan, hedef düğümün erişilebilirliğini kesmek istediğinde, hedef düğüme giden tüm yolları yok edecek şekilde yönlendirme mesajlarının içeriğini değiştirebilir.

Paket düşürme ve yayın saldırıları kesme yöntemiyle yapılan saldırılara diğer örnekler olarak verilebilir.Paket düşürme saldırıları ile yönlendirme mesajları hedef alınır. Saldırgan düğüm doğrudan kendisine gelen paketi henüz keşif sürecinde ağdan düşürerek keşif paketlerinin hedef düğüme ulaşmasını engeller. Yayın saldırılarında ise saldırgan düğüm çok büyük gereksiz mesajlar oluşturur ve bu mesajları yayın ile hedef düğüme göndererek hedef düğümü erişilemez hale getirerek kesme saldırısını gerçekleştirir [25]. Kötü niyetli ara düğüm, yönlendirme sürecine katılan ara düğümlerin merkezi bir denetim mekanizması olmamasına bağlı olarak işbirliği eksikliklerini kullanarak da kesme saldırıları gerçekleştirebilir.

4. TASARSIZ AĞLARDA GÜVENLİ YÖNLENDİRME (SECURED ROUTING IN AD-HOC NETWORKS)

Daha önce değinilen yönlendirme algoritmalarının güvenlik tehditlerine bağlı olarak tasarsız ağlarda saldırılara maruz kalınmaması için yönlendirme protokollerinin güvenlik gereksinimleri dikkate alınmalıdır. Tasarsız ağlarda güvenli yönlendirme yapılabilmesi için yönlendirme protokolünün,

- İki düğüm arasında bir yol varsa, doğru yolun bulunarak istenen düğüm ile bağlantı kurulduğunun garanti edilmesi,
- Kötü niyetli düğümlerin ağın dışında tutulması,
- Yönlendirmelerin yüksek hesaplama gücü gerektirmemesi,
- Düğüm adreslerinin ifşa edilmemesi,
- Problem oluştuğunda en az insan müdahalesi gerektirmesi,
- Düğümlerdeki olası yönlendirme hatalarına rağmen ağın düzgün çalışmaya devam etmesi [26]gibi önemli gereksinimleri sağlaması gerekmektedir.

Normal ağlarda, yönlendirme bilgilerinin gizli bilgiler olmaması sebebiyle, bütünlük ve erişilebilirlik unsurlarının sağlanması, fazla enerji tüketimi ve hesaplama gücü gerektiren gizliliğin sağlanması unsuruna göre daha ön plana çıkmaktadır. Ancak askeri amaçlı tasarsız ağlarda özellikle taktik sahada görev yapan düğümlerin yerinin tespit edilmemesi amacıyla yönlendirme bilgilerinin gizliliğinin sağlanması gerekmektedir. Bütünlük ve gizliliğin sağlanmasında sayısal imza ve özetleme, gizliliğin sağlanmasında ise şifreleme algoritmaları kullanılmaktadır. Takip eden alt başlıklarda güvenlik mekanizmalarının uyarlandığı yönlendirme protokolleri sunulmaktadır.

4.1. Secure Efficient Ad Hoc Distance Vector (SEAD)

Secure Efficient Ad Hoc Distance Vector (SEAD), Tablo temelli yönlendirme yaklaşımıyla çalışan Destination-Sequenced Distance Vector (DSDV) protokolü esas alınarak tasarlanmıştır. Hedef, metrik, bir sonraki durak ve sıra numarası gibi ortak alanlar içermekle birlikte SEAD yönlendirme tablolarında her bir girdi için özetleme değeri tutmaktadır. Önerilen güvenlik protokolünde özetleme zincir fonksiyonu olarak adlandırılan H fonksiyonu anahtar kavram olarak kullanılmaktadır. Her düğüm $h_0, h_1, h_2, \ldots h_n$ değerlerinin bir listesini $h_i=H(h_i\text{-}1)$ $0<i\leq n$ olacak şekilde hesaplamaktadır. Burada h_n değerinin tüm düğümlere güvenli olarak dağıtımını yapan bir mekanizmanın var olduğu ve h_0 rastgele bir değer aldığı varsayımı yapılmıştır. Bir düğüm H fonksiyonunu ve h_n değerini biliyorsa herhangi bir h_i değerini hesaplayıp h_n ile karşılaştırarak giriş doğrulama işlemini gerçekleştirebilmektedir. Yönlendirme güncellemesinin doğrulanması için her yönlendirme tablosu girişine bir özetleme değeri ara düğümler tarafından eklenmektedir.

Saldırgan kendisine bildirilen özet değerinden daha küçük indeks değerlerine sahip bir özet 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 karsı güçlü bir protokoldür. SEAD saldırganın bir sonraki atlama düğümü yanıltmasını veya yönlendirme güncellemesindeki hedef alanını değiştirmesini, bir önceki güncellemeden öğrendiği sıra numarası ve metriği kullanarak başka bir hedefe yeni bir yönlendirme güncellemesi göndermesini engelleyememektedir [27].

4.2. A Secure On-Demand Routing Protocol for Ad Hoc Networks (ARIADNE)

ARIADNE simetrik şifrelemeyle düğümlerdeki yönlendirmelerin değiştirilmesine yönelik saldırıların engellenmesini amaçlayan yol keşfi ve yol bakımı gibi temel işlevleri sağlayan DSR tabanlı reaktif yönlendirme protokolüdür. ARIADNE, iki düğüm arasında, paylaşılmış bir anahtar ve mesaj doğrulama kodu (MAC) vasıtasıyla, yönlendirilmiş mesajların kimlik doğrulamasını sağlamaktadır. Hedef düğümün kaynak düğümün kimliğini doğrulamasını, başlangıç düğümünün gelen RREP mesajında sunulan ve hedefe giden yol üzerindeki tüm ara düğümlerin kimliklerinin doğrulanmasını, ara düğümlerin RREQ ve RREP mesajlarındaki düğüm listesinden bir önceki düğümü silemeyeceklerini garanti etmektedir. ARIADNE'de kimlik doğrulama ve veri bütünlüğünün sağlanabilmesi amacıyla temel RREQ paketi ek alanlarla genişletilmiştir. Başlangıç düğümü yol isteğinde bulunurken aşağıdaki paketi ağa duyurur.

<RREQ, başlangıç, varış, ID, zaman aralığı, özet zinciri, düğüm listesi, MAC listesi>

Ara düğümler, gelen RREQ mesajında *<başlangıç, id>* kısmını kontrol ederek daha önce gelen bir istek olup olmadığını denetler. Daha önce aynı istek gelmediyse zaman aralığının geçerliliğini denetleyerek kendi adresini düğüm listesine ekler, özet zinciri alanını *H [A, özet zinciri]* olarak değiştirir, MAC listesi alanına tüm RREQ'ya ait MAC'ini atayarak değiştirdiği RREQ ağda yayınlar. Varış düğümü belirtilen anahtarların zaman aralığında geçerliliğini ve özet zincirini denetledikten sonra yol cevabını ağa duyurur. ARIADNE, yönlendirme bilgisinin değiştirilmesi ve tekrar üretilmesi saldırılarına karsı önemli bir koruma sağlamaktadır [28].

4.3. Security Aware Routing (SAR)

Seung ve arkadaşları AODV temelli Security Aware Routing-SAR protokolünü önermişlerdir [29]. SAR geleneksel yol keşfi yapan AODV, DSR gibi yönlendirme protokollerinin tasarsız ağlara güvenlik bakış açısıyla uyarlanmış halidir. SAR, güven hiyerarşisine dayalı tasarsız kablosuz ağların değişik güvenlik seviyelerine bölünmesini sağlamaktadır. Kaynak ile hedef düğüm arasındaki haberleşmede görev alacak ara düğümler için gerekli olan minimum güvenlik seviyesi bu hiyerarşi ile sağlanmaktadır.

SAR, yönlendirme metriklerinin içerisine ilgili düğümün güvenlik seviyesini ekler. Düğümler bir güven hiyerarşisi içerisinde düzenlenmiş ve her bir düğüme güvenlik/önem/yetenek seviyelerini gösteren numaralar atanmıştır. RREQ ve RREP paketleri şifreli olup her seviyeye güvenlik gereksinimlerine göre anahtar uzunlukları belirlenmiş şifreleme anahtarları atanmıştır. Bu şekilde, paketler sadece güvenli düğümler yoluyla yönlendirilir; düğümler gerekli güvenlik seviyesinde değilse kontrol paketlerini bile okuyamadığı için, paketleri düşürmek zorunda kalır.

4.4. Secure Routing Protocol (SRP)

Papadimitratos ve Haas, yönlendirme başlangıç aşamasından önce düğümler arasında güven ilişkisi gerektiren, yol keşfini engelleyecek saldırılara karşı koruma sağlayan DSR temelli Secure Routing Protocol-SRP önermiştir [30]. Yönlendirme için yol keşfi başlatıldığında SRP düğümün RREQ paketi içerisine sıra numarası, nonce ve mesaj doğrulama kodu (MAC) alanlarını ekler. MAC paylaşılan gizli anahtar, nonceve sıra numarasının özetlenmiş değerini içermektedir. Hedef

düğüm tarafından RREP mesajında MAC içerisine bulunan yol dâhiledilir ve ağa duyurusu yapılır.

Yol keşfinde kötü niyetli orta düğümler kendi adreslerini RREQ ve RREP mesajları içerisine eklememesi durumunun var olması önemli bir güvenlik açığı olarak değerlendirilmiştir.

4.5. Authenticated Routing for Ad Hoc Networks-(ARAN)

Sanzgiri ve arkadaşları, asimetrik şifreleme (açık anahtar altyapısı) kullanarak güvenliği sağlamak üzere isteğe bağlı yaklaşımla çalışan ARAN önermişlerdir [31]. ARAN güvenilir bir sertifika sunucusu (CS) gerektirmektedir. Düğümler ağa girmeden önce CS tarafından imzalanmış bir sertifika talebinde bulunurlar. Sertifika, düğümün IP adresini, açık anahtarını, sertifikanın oluşturulduğu zamanı ve sertifikanın kullanım süresinin sonunu gösteren bir zaman damgasını içermektedir. Tüm düğümlerin yeni bir sertifikaya sahip oldukları ve CS'nin açık anahtarını tüm düğümlerin bildiği varsayılmaktadır. Düğümler, güvenilir sertifika sunucusuna kimliklerini doğrulattıktan sonra sunucudan sertifika alırlar ve bu sertifikayla tüm mesajlarını sayısal olarak imzalayarak yönlendirme mesajlarının iletimini gerçekleştirirler.

Ağdaki ara düğümlerin her biri iki adres tutmaktadır. Bu adresler kendisine paketi ileten düğüm ile hedef düğüme ait adreslerdir. Yönlendirme mesajındaki tüm bilgiler başlangıç düğümünün özel anahtarı tarafından imzalanmıştır. Kaynak düğüm ile hedef düğümü arasında iletişim için RREQ paketi duyurulur. RREQ ilk defa alan her düğüm diğer ara düğümlerin imzalarını çıkarır, daha sonra kendi özel anahtarı ile RREQ imzalayarak komsu düğümlerine duyurur. Hedef düğüm RREQ paketini aldıktan sonra RREP paketini kaynak düğüme imzalayarak aynı yol üzerinden geri gönderir. Kaynak düğüm RREP paketini aldığında hedef düğümün imzasını kontrol ederek güvenli yol kurulumunu tamamlar. ARAN protokolünün kullandığı asimetrik şifrelemeden dolayı kaynak tüketiminin (bellek, işlemci, bant genişliği vb.) yüksek olması bu yaklaşımın olumsuz yönlerinden birisidir.

4.6. Security Protocols for Sensor Network (SPINS)

SPINS tasarsız ağlar için geliştirilmiş ve sınırlı kaynağa sahip ortamlar için optimize edilmiş bir yönlendirme protokolüdür [32]. Sensor Network Encyrption Protokol (SNEP) ve Micro Timed Efficient Stream Loss-Tolerant Authentication (µTESLA) olmak üzere güvenliği sağlayan iki bileşenden oluşmaktadır. SNEP noktadan noktaya haberleşmeyi güvenli kılan verinin doğrulanması ve güncel olmasından sorumlu bir alt protokoldür. µTESLA Yayın (broadcast) mesajının doğruluğunu sağlamakla görevlidir.

Mevcut protokollerin çoğunluğunun kullandığı asimetrik şifrelemede imzaları oluşturmak ve doğruluğunu sağlamanın maliyeti yüksek olduğundan, SPINS µTESLA alt protokolü aracılığıyla kimlik doğrulama için simetrik şifreleme algoritmaları kullanmaktadır. µTESLA Hizmet aksattırma saldırılarına (DoS) saldırılarına karşı sağlamlık sağlayan verimli ve güvenli bir yayın protokolüdür.

4.7. Cooperation of Nodes Fairness in Dynamic Ad-hoc Networks (CONFIDANT)

İsteğe bağlı yaklaşımla çalışan ve DSR protokolünü esas alan CONFIDANT protokolü, ağ monitörü, itibar, güven ve yol yöneticisi gibi bileşenlerden oluşmaktadır [33]. Her bir düğüm, komşularının davranışlarını izleyerek ve onun itibarıyla ilgili bilgiyi yaptığı davranışlara göre belirli periyotlarla puanlayarak güncel olarak tablolarda tutar. Eğer kötü niyetli bir düğüm tespit edilirse, diğer düğümlere o düğümle ilgili alarm mesajı gönderilir. Düğümlerle ilgili oluşturulan alarm sayısına göre düğümlerin güvenilirliği güven yöneticisi tarafından diğer düğümlere duyurulur.

Güven yöneticisinde alarm bilgileri, güven seviyeleri ve dost düğümler, itibar yöneticisinde reyting ve kara liste olmak üzere düğümler sınıflandırılmakta ve bu bilgiler tablolarda tutulmaktadır. Tablolar belirli zaman dilimlerinde dost düğümler arasında değiştirilerek güncel olarak dost düğümlerde tutulur. Yol yöneticisi dost düğümlerin bulunduğu tabloya göre güvenli yolu ağa duyurur. CONFIDANT yaklaşımının, farklı bileşenlerin birlikte çalışması, kaynakların fazla tüketilmesi ve tabloların yönetimi gibi dezavantajları vardır.

4.8. Secure Link State Protocol (SLSP)

SLSP, düğümlerin durum bilgilerinin dağıtımı, güvenli yol keşfi ve yol bilgilerinin dağıtımından sorumlu olan Papadimitratos ve Haas tarafından önerilen proaktif yaklaşımlı, açık anahtar altyapısını kullanan güvenli bir yönlendirme protokolüdür [34].

Her düğüm kendisine belirli sayıda atlamadan oluşan ve iletişim alanı olarak adlandırılan bir alt ağ oluşturur. SLSP her bir alan için o alandaki düğümlere genel anahtar dağıtımını yapar. Düğümler özel anahtarı ile yönlendirme bilgilerini imzalarlar ve periyodik olarak genel anahtarlarını içeren sertifikaları broadcast ile ağa duyururlar. Paketleri alan düğümler paketi gönderen düğümün genel anahtarı ile aldıkları paketi doğrularlar.

SLSP komşuların tespit edilmesinde güvenli bir protokol tanımlar. Her bir düğüm fiziksel adresi (MAC) ile IP adresini özel anahtarlarıyla imzalayarak komşularına komsu bulma protokolü NLP (Neighbour Location Protokol) ile duyururlar. SLSP birden fazla saldırganın işbirliği içerisinde yapacakları saldırılara karşı koruma sağlayamaması ve açık anahtar alt yapısının yüksek hesaplama gücü gerektirmesi gibi önemli dezavantajları vardır.

4. SONUÇLAR (CONCLUSION)

Bu çalışmada tasarsız ağlar ve yönlendirme protokollerine genel bir bakış sağlanarak, güvenlik tehditleri ve güvenli yönlendirme protokolleri üzerinde gelecekte bu alanda yapılacak yeni çalışmalara yön vermek amacıyla öneriler ve değerlendirmeler yapılmıştır.Kurulum açısından düşük maliyete sahip olan tasarsız ağlar, özellikle algılayıcı

(sensor) ağlarla birlikte her geçen gün kendisine yeni uygulama alanları bulan güncel bir alandır. Dinamik ve değişken bir ağ topolojisine sahip olmaları, sabit ve kurulu bir altyapının olmaması, merkezi bir denetim mekanizmasının olmaması, düğümlerin yazılım ve donanım kabiliyetleri açısından heterojen yapıda olması, heterojen düğümlerin birlikte çalışabilirliği, güvenlik gibi konular tasarsız ağların özgün yapısıyla beraberinde getirdiği zorluklardır.

Geliştirilecek uygulamalarda, saldırıya açık kablosuz ortamlarda merkezi bir denetim mekanizması olmadan ağa dâhil olan düğümlerin yönlendirici olarak görev yapmalarına bağlı olarak oluşan yönlendirme ile ilgili güvenlik zayıflık ve zafiyetlerine karşı önlemlerin yüksek seviyede alınması gereği açıktır. Ancak bu güvenlik önlemleri alınırken ağın dinamik yapısı ve kısıtlı kaynakları gibi tasarsız ağların yapısına özgün kısıtlar mutlaka düşünülmelidir.

Bu çalışmada incelenen güvenli yönlendirme protokollerinin saldırıların tamamına karşı koruma sağlamadığı ayrıca önerilen protokoller içerisinde, güvenlikle ilgili bazı varsayımların tasarsız ağlarda gerçekleştirilmesinin zor olduğu tespit edilmiştir. Örneğin, açık anahtar altyapısı düğümlerde yüksek hesaplama gücü gerektiren anahtar dağıtımı ve merkezi sertifika sunucusu gibi altyapılı ağlara uygun olarak tasarlanan çözümlerin tasarsız ağlarda düşük maliyetlerle gerçekleştirilmesi zor olan varsayımlardır.

Tasarsız ağlarda kısıtlı kaynaklar ile daha da zorlaşan güvenlik konusu çözülmesi gereken ve hala üzerinde çalışılan önemli bir konudur. Önerilen güvenli protokollerde bütünlük saldırılarına karşı özetleme fonksiyonlarının, gizlilik ve erişilebilirlik saldırılarına karşı simetrik veya asimetrik şifreleme algoritmalarının, kimlik hırsızlığı ile ilgili saldırılarda sayısal imzanın ön plana çıktığı gözlemlenmiştir. Bu çalışmada incelenen güvenlik bakış açısıyla gözden geçirilen güvenli protokollerin belirli saldırıları engellemek için tasarlandığı ancak gizlilik, bütünlük ve erişilebilirlik saldırılarının tamamına karşı dirençli olan ayrıca kısıtlı ağ kaynaklarını daha etkin kullanan güvenli protokol yaklaşımlarına olan ihtiyaçların ise halen devam ettiği tespit edilmiştir.

Son olarak yeni yapılacak olan çalışmaların, güvenliğin temel unsurları olan gizlilik, bütünlük ve erişilebilirlik odaklı saldırılara karşı dirençli, enerji verimliliği yüksek, güvenlik-performans-enerji üçlüsünün ağırlıklarını ilgili probleme göre otonom olarak ayarlayabilecek yeni protokoller üzerinde durması gerekmektedir.

KAYNAKLAR (REFERENCES)

[1] E. C. Perkins, “Ad Hoc Networking”, Addison-Wesley Professional, Boston, 5-14, 2000.

[2] S.R. Alotaibi, “Stability of Secure Routing Protocol in Ad hoc Wireless Network” Ph.D. Thesis, De MontfortUniversity, United Kingdom, 9-11, 2010.

[3] T.A. Nguyen, “Evaluations of Secure Manet Routing Protocols In Malicious Environments”, Master of ScienceThesis, Unıversıty of Houston-Clear Lake, Texas , 7-12, 2006.

[4] R. Badonnel, R. State, O. Festor, Elsevier, Washington, “Handbook of Network andSystem Administration”, 331-360, 2008.

[5] M. Ünal, M.A. Akçayol. “Kablosuz Ağlarda Güvenli Yönlendirme Protokolleri”. Bilişim Teknolojileri Dergisi, Vol. 1, No. 3, 7-13, Eylül, 2008

[6] E.M. Royer, C. K. Toh, “A Review of Current Routing Protocolsfor Ad-Hoc Mobile Wireless Networks”, IEEE Personal Communications, 6(2), 46-54, 1999.

[7] P. Ghosekar, G. Katkar, P. Ghorpade, “Mobile Ad Hoc Networking: ImperativesandChallenges”, IJCA Special Issueon MANETs, 3(1), 153-158, 2010.

[8] C.K. Toh, “AssociativityBased Routing For Ad Hoc Mobile Networks”, Wireless Personal Communications,4(2), 1-36, 1997.

[9] E. D. Sharp,“Information Security in the Enterprise”, Information Security Management Handbook Fifth Edition, Tipton, F. H., Krause, M., Auerbach Publications, New York, 1199-1200, 2004.

[10] C.K. Toh, “Ad Hoc Mobile Wireless Networks: Protocols and Systems”, Prentice- Hall, New Jersey, 34-37, 2002.

[11] İnternet: Mobile Ad-hoc Networks (manet) “Description of WorkingGroup” http://datatracker.ietf.org/wg/manet/charter, 08.12.2015.

[12] S. K. Sarkar, Basavaraju, T. G.,Puttamadappa, C., “Ad-Hoc Mobile Wireless Networks: Principles, Protocols, and Applications,” Auerbach Publications, Boca Raton, 2008.

[13] M. Abolhasan, T. Wysocki, E. Dutkiewicz, “A review of routing protocols for mobile ad hoc networks”, Ad Hoc Networks, Vol. 2, No.1, 1-22, 2004.

[14] İnternet: Ad-hoc on-demanddistancevector (AODV) Routing, http://www.ietf.org/rfc/rfc3561.txt, 08.12.2015.

[15] İnternet: Optimized link staterouting (OLSR) protocol, http://www.ietf.org/rfc/rfc3626.txt, 08.12.2015.

[16] Z. J. Haas,“A newroutingprotocolforthereconfigurablewirelessnetworks”, Universal Personal Communications, 2(1), 562–566, 1997.

[17] P. Yang, S. Zheng, “Security Management in Hierarchical Ad Hoc Network”, InfotechandInfonetInternational Conferences, Vol. 2, No.1, 642 – 649, 2001.

[18] K. Singh, R. S. Yadav, Ranvijay, “A ReviewPaper On Ad Hoc Network Securıty”, International Journal of ComputerScienceand Security, Vol. 1, No. 1, 52-65, 2007.

[19] J. Kong,X. Hong, M. Gerla, “A New Set of Passive Routing Attacks in Mobile Ad Hoc Networks”, MILCOM 2003, Vol. 2, No. 1, 796-801,2003.

[20] I. Gupta, H.Sadawarti, S. N. Panda, “Security Attacks: Vulnerability in Ad Hoc Networks”, UNIASCIT, Vol.2, No.1, 179-182, 2012.

[21] H. Deng, W. Li, D. Agrawal, “Routing security in wireless ad hoc networks,” IEEE Communications Magazine, Vol. 40, No. 10, 70-75, 2002.

[22] Y. Hu, A. Perrig, D. Johnson, “Packetleashes, A defenseagainstwormholeattacks in wireless ad hoc networks” Twenty-Second AnnualJoint Conference, 1976-1986, 2003.

[23] S-Y. Ni, Y-C.Tseng, Y-S.Chen, J-P. Sheu,"The Broadcast Storm Problem in a Mobile Ad Hoc Network", Proc. ofthe 5th annual ACM/IEEE internationalconference on Mobile computingandnetworking, 151-162, 1999.

[24] M. Pirretti, S. Zhu, V. Narayanan, P. Mcdaniel, M. Kandemir, “TheSleepDeprivation Attack in Sensor Networks: Analysis andMethods of Defense”, International Journal of Distributed Sensor Networks, Vol. 2, No. 3, 267-287, 2006.

[25] Y. A. Huang, F. Fan, W. Lee, P. S. Yu, “Cross-Feature Analysis forDetecting Ad-Hoc Routing Anomalies,” The 23rd International Conference on Distributed Computing Systems (ICDCS), 478-489, 2003.

[26] C. S. R. Murthy, B. S. Manoj, “Ad Hoc Wireless Networks: Architectures and Protocols”, Prentice Hall, New Jersey, 490-495 2004.

[27] Y-C. Hu, D. B. Johnson, A. Perrig, "SEAD: Secureefficient distance vector routing for mobile wireless ad hoc networks", Ad Hoc Networks, Vol.1, No. 1, 175–192, 2003.

[28] 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, 21–38, 2005.

[29] S. Yi, P.Naldurg, R. Kravets, "Security-aware ad-hoc routing for wireless networks", ACM Symposium on Mobile Ad Hoc Networking and Computing, 286-292, 2001.

[30] P. Papadimitratos, Z.J. Haas, "Secureroutingfor mobile ad hoc networks" Communication Networks and Distributed SystemsModelingandSimulation Conference (CNDS), 27–31, 2002.

[31] K. Sanzgiri, B. Dahill, B. N. Levine, C. Shields, E. M. B. Royer, "A secureroutingprotocolfor ad hoc networks" International Conference on Network Protocols (ICNP), 78–89, 2002.

[32] A. Perrig, R. Szewczyk, J. J. Tygar, V. Wen, D. D. Culler, "SPINS: Security Protocolsfor Sensor Networks", Wireless Networks, Vol. 8, No. 5, 521-534, 2002.

[33] S. Buchegger, L.J-Y. Boudec, "Performance Analysis of the CONFIDANT Protocol(Cooperation Of Nodes: Fairness In Dynamic Ad-hoc NeTworks)", The Third ACM International Symposium on Mobile Ad Hoc Networking and Computing, 226-236, 2002.

[34] P. Papadimitratos, Z. J. Haas, "Secure link stateroutingfor mobile ad hoc networks", International Symposium on Applications and the Internet (SAINT '03), 379-383, 2003.

[35] Y-C. Hu, D. B. Johnson, D. A. Maltz,"FlowState in theDynamic Source Routing Protocol Internet Draft", work in progress, June, 2001.

[36] D. Djenouri, N. Badache,"On EliminatingPacketDroppers in MANET: A Modular Solution", Ad hoc Networks Journal, Vol 7, No. 6, 1243–1258, Elsevier Publisher, August 2009.

[37] Z. J. Haas, M. R. Pearlman, P.Samar,"TheZone Routing Protocol (ZRP) for Ad Hoc Networks", Internet Draft, work in progress, July, 2002.

[38] J-N. Marioand, I-T. Lu, "A peer-to-peertwo-level link stateroutingfor mobile ad-hoc wireless network". Thespecialissue on Wireless Ad Hoc Networks of IEEE JSAC, Vol. 17, No. 8, 1415-1425, Aug. 1999.