Yardımlaşan Nesne Ağlarında Güvenlik Sorunları ve Çözümler

Mithat Dağlar **Erdal Çayırcı**

Deniz Bilimleri ve Mühendisliği Enstitüsü
Deniz Harp Okulu, İstanbul
mdaglar@dho.edu.tr cayirci@cs.itu.edu.tr

Anahtar sözcükler: Yadımlaşan Nesne, duyarga ve tetikleyici ağları, tasarsız ağlar, duyarga ağları güvenliği

Abstract

Cooperating object networks mostly use sensor and actuator nodes. Due to the hardware limitations of these nodes, wireless communication medium, real-time requirements, heterogeneous infrastructure, high density, scalability requirements, mobility, heavy environmental conditions, and cost considerations, these networks are subject to many security problems. In this paper, issues that are related to the security in cooperating object networks, holes stem from these issues, possible attacks and solution proposals are investigated.

Özet

Yardımlaşan nesne ağları büyük ölçüde duyarga ve tetikleyici düğümler kullanmaktadır. Bu düğümlerin donanımsal kısıtları, kablosuz iletişim ortamı, gerçek zamanda işlem ihtiyacı, heterojen yapı, düğüm sayısının fazlalığı, ölçeklenebilirlik ihtiyacı, gezginlik, uygulama ortam şartlarının ağırlığı ve maliyet gibi hususlardan kaynaklanan nedenlerle yardımlaşan nesne ağları pek çok güvenlik açığı ile karşı karşıya bulunmaktadır. Bu bildiride yardımlaşan nesne ağlarının güvenliğine etki eden özellikleri, bu özelliklerden kaynaklanan güvenlik açıkları, muhtemel saldırı türleri ve çözüm önerileri incelenmektedir.

1. Giriş

Duyarga (sensor) ve tetikleyici (actuator) ağlarının imkan ve kabiliyetlerinden daha iyi istifade edebilme arayışlarının bir neticesi olarak ortaya çıkan "Yardımlaşan Nesne Ağları", dünyanın çeşitli yerlerindeki üniversite ve firmaların da katılımıyla önem kazanmaya başlayan bir konsept haline gelmiştir. Henüz teorik temellerin oluşturulması aşamasında bulunan ve literatürü olgunlaşmamış bu konseptin yakın bir gelecekte duyarga ve tetikleyici ağları alanında etkin bir konuma sahip olacağı ve araştırma/geliştirme faaliyetlerinin önemli bir kısmının bu konu üzerinde odaklanacağı değerlendirilmektedir.

En geniş anlamıyla yardımlaşan nesneler (YN) "belli bir amacı gerçekleştirmek üzere, ortamla ve birbirleriyle etkileşebilen ve iş birliği içerisinde üzerlerine düşen görevleri otonom olarak gerçekleştirebilen duyargalar, tetikleyiciler ve yardımlaşan nesneler" şeklinde tanımlanabilir [1]. Bu tanımdan da anlaşılacağı üzere, bir YN sadece bir duyarga ya da tetikleyici olabileceği gibi, YN'lerin bir araya gelmesiyle oluşan karmaşık bir nesne de olabilir. Dolayısıyla, bu nesnelerden oluşan bir ağ, klasik duyarga-tetikleyici ağlarına göre çok daha heterojen bir yapıya sahip olacaktır.

YN ağları ile gerçekleştirilmesi hedeflenen

- Ana kara güvenliği (Homeland security),
- Askeri sistemler,
- Yıkım onarımı,
- Arama kurtarma

gibi pek çok uygulama genellikle zaman-kritik ve hayati önem arz eden bir özelliğe sahiptir. Bu nedenle, klasik kablosuz (wireless), altyapısız (ad hoc) duyarga ağlarında karşılaşılan tüm güçlükler bu ağlar için daha da belirgin ve hassas hale gelmektedir. Güvenlik bu güçlüklerin en önemlilerinden biridir. Düğümlerin (node) donanımsal kısıtları, kablosuz iletişim ortamı, gerçek zamanda işlem ihtiyacı, heterojen yapı, düğüm sayısının fazlalığı, ölçeklenebilirlik ihtiyacı, gezginlik, uygulama ortam şartlarının ağırlığı ve maliyet gibi hususlardan kaynaklanan nedenlerle YN ağları pek çok güvenlik açığıyla karşı karşıyadır. Güvenliğin temel hedefi olan gizlilik, bütünlük ve kullanılabilirliğin sağlanması, zaman-kritik ve hayati önemdeki amaçların

gerçekleştirilebilmesi için çözülmesi gereken en önemli problemlerden birini oluşturmaktadır.

Bu bildiride YN ağları güvenlik boyutunda incelenecektir. İkinci Bölümde bir YN ağı uygulama senaryosu verilecek ve bu ağların güvenliğe etki edebilecek özellikleri sunulacaktır. Üçüncü Bölümde bu özelliklerin ortaya çıkardığı güvenlik açıkları incelenecektir. Bu açıklara çözüm olarak sunulan öneriler Dördüncü Bölümde anlatılacaktır. Beşinci Bölüm sonuç için ayrılmıştır.

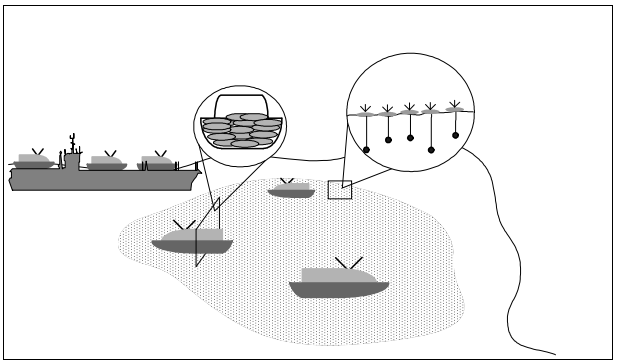
2. YN ağlarının özellikleri

Kişisel ya da diz üstü bilgisayarlar gibi donanımsal ve yazılımsal olarak güçlü düğümlerden meydana gelen ve kablolu bir mimari ile oluşturulan klasik bilgisayar ağları ile karşılaştırıldığında YN ağları kendilerine özgü pek çok özellik göstermektedirler. Bu benzersiz özelliklerin birçoğu güvenlik probleminin çözümünü büyük ölçüde güçleştirmektedir. Ancak, saldırganların da genellikle aynı kısıtlamalar ile bağlı olmaları, bu özelliklerin bazı durumlar için ihtiyaçlar doğrultusunda kullanılabilmesini de mümkün kılmaktadır [2]. Bu bölümde YN ağlarının kendine özgü özellikleri ve güvenlik ihtiyaçları sualtı gözetleme ve savunma sistemi (SGSS) örneği üzerinde incelenecektir.

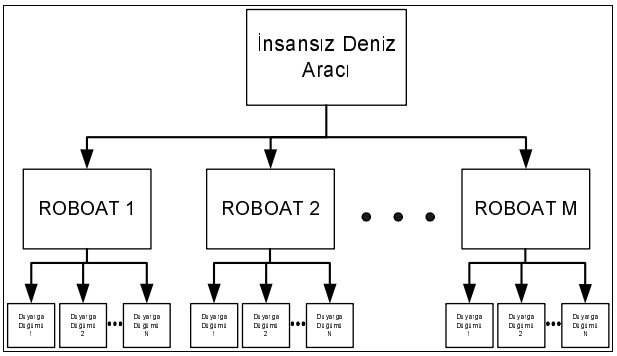
2.1 Sualtı Gözetleme ve Savunma Sistemi

Körfez, liman ve boğaz yaklaşma suları ve girişleri kriz ve harp dönemlerinde düşman sızmalarına karşı oldukça hassas bölgelerdir. Özellikle denizaltılar ve insansız denizaltı vasıtaları bu gibi taktik ve stratejik öneme sahip yerler için büyük bir tehdit oluşturmaktadır. Bu tehditlere karşı koyabilmek maksadıyla firkateyn, denizaltı ve helikopter gibi önemli miktarda denizaltı savunma harbi (DSH) unsurlarının bu bölgeler için ayrılmasını gerektirmektedir. Kriz ve harp döneminin açık denizlerdeki ihtiyaçları açısından oldukça değerli bu unsurların DSH maksadıyla bu bölgelerin savunmasında kullanılması maliyet-etkin olmamakta ve diğer bölgelerde zafiyet alanları meydana getirmektedir.

Bu bölgelerin gözetimi ve savunulması maksadıyla YN ağlarının kullanılması bu dezavantajları ortadan kaldırabileceği gibi daha iyi bir kaplama maliyet-etkin bir şekilde sağlanabilecektir. Bu maksatla geliştirilen bir SGSS şu şekilde çalışmaktadır: Üzerinde küçük ve hafif su üstü vasıtaları (ROBOAT) ve torpidolar bulunan bir su üstü vasıtası ROBOAT'ları harekat bölgesine taşımaktadır. Birer YN olan ROBOAT'lar bir tahrik sistemi ve bir radyo alıcı-vericisine sahip olup, görevleri üzerlerindeki denizaltı duyargalarını (DD) harekat sahasına dağıtmaktır.



Şekil 1: SGS Sistemi



Şekil 2: SGSS İlişki Şeması

Her DD düğümü ses, sıcaklık ve manyetik duyargaları, bir adet radyo alıcı/vericisi, deniz içerisinde aşağı yukarı hareket edebilmeyi sağlayan bir mekanizma ve düğümün satıhta kalmasını sağlayan ve radyo alıcı/vericisini üzerinde bulunduran bir şamandıradan oluşmaktadır. ROBOAT'lar tarafından su sathına bırakılan her DD, harekat sahasının maksimum kaplamasını sağlamak üzere kendi derinliğini otomatik olarak ayarlamaktadır. DD'ler de birer YN'dir ve ROBOAT'lar ile birlikte geniş bir YN ağı oluşturmaktadırlar.

Duyargalardan herhangi birinin muhtemel bir denizaltı teması alması durumunda, bahse konu bölgenin daha hassas algılanması maksadıyla ROBOAT'lar tarafından o bölgeye ilave duyargalar atılmaktadır. Temasın kesin denizaltı olarak sınıflandırılması durumunda, ROBOAT'lar tarafından durum bir işaret ile kendilerini bölgeye getiren su üstü aracına bildirilmekte ve torpido angajmanı için bölge boşaltılmaktadır. Torpido angajman sonucunun kıymetlendirilmesi de yine ROBOAT'lar tarafından bölgeye atılan uygun

duyargalara sahip YN'ler tarafından gerçekleştirilmektedir.

Görev sonunda su üstü aracı tarafından yapılan bir yayımla tüm düğümler duyargalarını satha çekmekte ve düğümler ROBOAT'lar tarafından toplanmaktadır.

2.2 YN ağlarının güvenliğe etki eden özellikleri

Tablo 1. DD ve ROBOAT iletişim donanımı.

CPU	16 bit M16C
Bellek	256 KB flaş
	20 KB RAM
Haberleşme	916 MHz radyo
Band Genişliği	10 Kb/s

Donanımsal kısıtlılık: YN ağları büyük ölçüde duyarga ve tetikleyicilerden meydana gelecektir. Klasik ağları oluşturan güçlü kişisel ve diz üstü bilgisayarlarla karşılaştırıldığında bu düğümler son derece az işlem gücü, ana bellek ve sabit disk kapasitesine sahiptir. Tablo 1'de SGSS projesinde kullanılan duyarga düğümlerine ait teknik özellikler verilmiştir. Klasik ağ düğümleri için geliştirilmiş uygulamaların pek çoğuna ait parametrelerin dahi bu bellek ve sabit disklere sığmayacağı, işlem zamanının ise gerçek zaman (real-time) gereksinimlerine cevap veremeyeceği açıktır. Yine klasik ağ düğümlerine nazaran duyarga ve tetikleyiciler için güç en kıymetli bileşen olup, oluşturulan YN ağının uzun süre (uygulamaya bağlı olarak haftalarca, aylarca ve hatta yıllarca) hizmet verebilmesi için son derece tasarruflu kullanılması gerekmektedir. Bu düğümler üzerinde bulunan alıcı ve vericiler de yine son derce düşük band genişliğine sahiptir. Duyarga algılamalarının baz istasyonuna iletiminin haricinde haberleşme paketlerine eklenecek her bit bu band genişliği için bir yük oluşturacak ve dahası güç kullanımını artıracaktır. Moore kanununun duyarga ve tetikleyiciler için bu imkanları artırmaktan ziyade maliyeti azaltmak yönünde etki göstereceği düşünüldüğünde [2][3] yakın ve orta vadede YN ağları için geliştirilecek tüm uygulama ve protokollerin bu kısıtlı imkanları en iyi şekilde kullanacak biçimde optimize edilmesi gerekecektir.

Kablosuz iletişim: YN ağları hemen hemen tamamıyla kablosuz iletişim yapacaklardır. Bu ortam gürültü kirliliğine açık olup, bit hata oranı (BER) oldukça yüksektir. Ortama eklenecek yapay bir gürültü (örneğin radyo karıştırması) bu oranı daha da artırabilecek ve hatta ağ haberleşmesini tamamen durdurabilecektir. Güç harcaması kısıtlamaları nedeniyle düğümler üzerinde bulunan vericilerin menzilleri, kablolu ya da yüksek çıkış gücü ile kablosuz iletişim yapan klasik ağ düğümlerine nazaran çok daha sınırlıdır. Bu husus duyarga algılamalarının doğrudan baz istasyonuna iletimi yerine, çok sayıda düğüm üzerinden düğümden-düğüme geçirilerek iletilmesini zorunlu hale getirmektedir.

Heterojen Yapı: Bölüm 1 de verilen tanımdan da anlaşılacağı üzere bir YN basit bir duyarga olabileceği gibi YN'lerin bir araya gelmesiyle oluşan üst seviye bir nesne de olabilir. Bu özelliklere sahip düğümlerden oluşan bir ağ, donanım ve yazılım açısından oldukça heterojen bir yapıya sahip olacaktır. Ağ çapında kullanılacak uygulama ve protokollerin bu heterojenliği göz önüne alarak geliştirilmesi zorunludur. Ağı birbirine bağlayan zincirde imkan ve kabiliyet açısından "en zayıf halkayı" duyargalar oluşturmaktadır. Bu nedenle, geliştirilen uygulama ve protokoller bir yandan yukarıda izah edilen donanımsal kısıtlar altında işlev yapabilirken, diğer taraftan daha fazla imkan ve kabiliyete sahip düğümlerin bu imkan ve kabiliyetlerinin atıl kalmamasını sağlamalıdır. Bu husus, büyük ölçüde homojen bir yapıya sahip klasik ağlar ya da kablosuz, altyapısız duyarga ağları için geliştirilen protokol ve uygulamalardan farklı olarak daha karmaşık yazılımları ortaya çıkarmaktadır. Daha karmaşık yazılımlar gözden kaçabilecek hata miktarını artırmakta ve dolayısıyla daha fazla güvenlik açığına neden olabilmektedirler.

Ölçeklenebilirlik ihtiyacı (Scalibility): YN ağlarını diğer altyapısız duyarga ve tetikleyici ağlarından ayıran en önemli özelliklerden biri, bu ağların ölçeklenebilir olmaya duyduğu ihtiyaçtır. Bu ağlar genellikle geniş bir uygulama sahasını kapsamak üzere pek çok düğümü bünyesinde barındıracaktır. SGSS'i örnek olarak ele alırsak, bu uygulama, harekat sahasının genişliğine bağlı olarak yüzlerce hatta binlerce duyarga düğümünü ve en azından birkaç ROBOAT'u içerecektir. Pek çok nedene bağlı olarak (örneğin bataryanın tükenmesi gibi) zaman zaman duyargalardan bazıları ağ bağlantısından düşecektir. Düşen bu düğümlerin yerini almak ya da belli bir coğrafi bölgenin daha hassas olarak incelenmesini sağlamak üzere ROBOAT'lar tarafından yeni duyargalar atılacaktır. Dolayısıyla, klasik ağlar ve kablosuz, altyapısız duyarga ve tetikleyici ağlarına göre, YN ağ topolojisi çok daha dinamik bir yapıya sahip olacaktır.

Gezginlik (Mobility): Pek çok YN uygulama senaryosu ağdaki düğümlerin belli bir seviyeye kadar hareketli olmasını gerektirmektedir. Hareketliliğin seviyesi uygulama ihtiyaçlarına bağlı olarak değişmektedir. Örneğin SGSS senaryosunda ROBOAT'lar satıh üzerinde tamamen hareketli iken duyarga düğümleri sadece su içerisinde aşağı ve yukarı hareket kabiliyetlerine sahiptir. Bunun yanı sıra uygulama ortamına bağlı olarak düğümler ortam şartlarına tabi olarak istem dışı da hareket edebilmektedirler (örneğin

SGSS senaryosunda duyargaların akıntı nedeniyle hareketli olması gibi).

Ortam: YN ağları genellikle, deniz, açık hava, kimyasal maddeler tarafından kirletilmiş, yıkıma maruz kalmış ve benzeri gibi fiziksel olarak elverişsiz ortamlarda hizmet vermektedirler. Klasik ağları oluşturan düğümler (örneğin kişisel veya diz üstü bilgisayarlar) korumalı bir mevkie yerleştirilerek fiziksel güvenlikleri kolaylıkla sağlanabilirken, YN ağlarında özellikle duyarga ve tetikleyicilerin bu olumsuz ortamlarda fiziksel güvenliklerinin sağlanabilmesi çoğunlukla bu kadar kolay olmayacaktır. Bu nedenle çevresel faktörlerin ya da saldırganların bu düğümlere fiziki zarar vermeleri daha kolay olacaktır.

Maliyet: Daha önce de belirtildiği üzere Moore kanununun duyarga ve tetikleyiciler için maliyeti azaltma yönünde etki edeceği değerlendirilmektedir [2][3]. YN ağları genellikle alternatifleri yüksek maliyete sahip oldukları ya da insan sağlığı ve güvenliğini daha az tehlikeye sokmaları nedeniyle tercih edilmektedir. Örneğin sualtı gözetlemesinin gemiler yerine YN ağları ile yapılması daha az maliyet getirmekte ve kıymetli unsurların daha aktif görevlerde kullanılmasını sağlamaktadır. Bu maksatla çok sayıda sualtı duyargası ve belli sayıda ROBOAT harekat ortamına bırakılmaktadır. Bu düğümlerin toplam maliyetinin alternatif gözetlemenin maliyetini geçmesi durumunda YN ağı tercih sebebi olmaktan çıkacaktır. Bu nedenle YN ağları için geliştirilecek uygulama ve protokollerin maliyeti artırmaması gerekmektedir.

Gerçek zamanda işlem ihtiyacı: YN ağları genellikle zaman-kritik ve hayati öneme sahip uygulamalarda kullanılacaktır. Bu uygulamalar gerçek zamanda işlem ihtiyacı göstermektedirler. Bu nedenle, özellikle duyarga düğümlerinin esas görevi olan ortamın algılanması ve bunun en seri biçimde baz istasyonuna gönderilmesi öncelikli bir husustur. Bu işlemi yavaşlatacak her türlü güvenlik protokolü ve uygulaması gerçek zamanda işlem yapmaya engel teşkil edecektir.

3. YN ağlarında güvenlik açıkları

YN ağlarına özgü yukarıda açıklanan özellikler, klasik bilgisayar ağları ve diğer duyarga ağlarına göre çözümü daha güç güvenlik açıkları ortaya çıkarmaktadır. Uygulamaların çoğunlukla zaman-kritik ve hayati öneme sahip olması nedeniyle, güvenliğin temel hedefi olan gizlilik, bütünlük ve kullanılabilirliğin sağlanması bu ağlar için daha da fazla bir önem arz etmektedir. Bu bölümde YN ağları için bu üç hedefe yönelik tehditler ve bazı saldırı yöntemleri incelenecektir. İnceleme süresince aşağıdaki varsayımlar kabullenilecektir [3][4][5]:

- Kablosuz iletişim güvensizdir. Saldırgan düğümler arası iletişimi duyabilir ve kendisi de aynı kanalda yayım yapabilir.
- YN ağlarının fiziksel güvenliğinin zayıf olması nedeniyle, saldırgan ağa kendi düğümlerini dahil edebilir.
- Saldırgan YN ağında bulunan bazı düğümleri ele geçirip yeniden programlayarak kendi amaçları doğrultusunda kullanabilir.
- Ele geçirilen bir düğümdeki tüm donanım, bilgi ve yazılım saldırgan tarafından anlaşılabilirdir.
- Baz istasyonları güvenlidir.

3.1 Gizliliğe yönelik tehditler

YN ağı uygulamalarının hemen tamamı ağ içerisinde iletilen ve saklanan bilgilerin gizliliğini zorunlu kılmaktadır. Özellikle askeri uygulamalarda elde edilen bilgilerin düşmanın eline geçmemesi kritik bir öneme sahiptir. Ancak kablosuz iletişim ortamı ve iş birlikçi düğümler gizlilik için ciddi tehditler oluşturmaktadır. Özellikle baz istasyonu ve kümeleme noktalarına (aggregation points) yakın bölgelerdeki trafik saldırgan için önemli bilgiler içermektedir.

YN ağındaki bilgiye ulaşmak maksadıyla saldırgan tarafından aşağıdaki yöntemler kullanılabilir:

Pasif dinleme: Uygun bir mevkie ağın çalışma frekansına ayarlanmış bir alıcı yerleştirerek trafiği pasif olarak dinleyebilir.

İşbirlikçi düğüm kullanma: Fiziksel ya da mantıksal bir saldırı gerçekleştirerek ağdaki bazı düğümleri ele geçirmek ya da ağa kendi düğümlerini eklemek suretiyle oluşturacağı iş birlikçi düğümleri kendisine bilgi sızdırmak maksadıyla programlayabilir [5].

3.2 Bütünlüğe yönelik tehditler

Bütünlük, verinin gerçekten gönderici olduğunu iddia eden düğüm tarafından gönderilmiş olması (kaynak bütünlüğü) ve bozulmadan/değiştirilmeden (veri bütünlüğü) alıcıya ulaşması anlamına gelmektedir. Saldırgan, bir YN ağında veri bütünlüğünü iki yöntemle tehdit edebilir:

Dinleme ve aktif transmisyon: Uygun bir mevkie yerleştireceği ağ frekansına ayarlanmış bir alıcı ve verici ile ağ trafiğini dinler ve duyduğu verinin içeriğini değiştirerek alıcı düğümlere gönderir. Ya da ağ içerisinde bir düğüm gibi davranarak ağa sahte bilgi enjekte eder.

İşbirlikçi düğüm kullanma: Daha önce bahsedilen yöntemlerle elde edeceği iş birlikçi düğümleri kullanır. Bu düğümlere gelen verilerin

içeriğini değiştirerek alıcı düğüme gönderir veya ağa sahte bilgi enjekte eder.

Saldırgan tarafından içeriği değiştirilmiş ya da ağa enjekte edilmiş veri ya hiç kullanılamaz durumdadır ya da daha kötüsü, kullanılabilecek durumdadır ve yanlış bir veridir. YN ağlarının büyük bir çoğunluğunun zaman-kritik ve hayati öneme sahip uygulamalar için kullanıldığı göz önüne alındığında, bu tehdidin vahim sonuçlar doğurması kaçınılmazdır. Örneğin sualtı savunma senaryosunda, ele geçirilmiş bazı düğümlerin sahte denizaltı temas bilgisini ROBOAT'lara iletmesi sahte temasa torpido angajmanı gerçekleştirilmesine neden olacaktır. Tam tersi olarak, denizaltı teması tespit etmiş düğümlere ait verileri, denizaltı yokmuş gibi değiştirmek suretiyle iletmesi denizaltının imha edilememesi ile neticelenecektir. Her iki durumda da YN ağı kendinden beklenen fonksiyonu yerine getiremediği gibi saldırgan lehine kullanılmış olacaktır.

3.3 Kullanılabilirliğe yönelik tehditler

YN ağları için kullanılabilirlik en genel anlamda, belirlenmiş amaca uygun olarak, duyarga algılamalarının değerlendirilmesi ve tetikleyiciler vasıtasıyla uygun reaksiyonun gösterilmesidir. Ağa yapılacak bir servis dışı bırakma (DoS) saldırısı, kullanılabilirliği ortadan kaldıracak ve düğümlerin işlevini görememesine neden olacaktır.

Saldırgan YN ağına DoS saldırılarını genel olarak aşağıdaki yöntemlerle gerçekleştirebilir [5]:

Fiziksel katmanda yapılan saldırı: Fiziksel olarak ya da elektronik yöntemlerle ağdaki düğümlere zarar vererek kullanılmaz duruma getirebilir. Diğer bir yöntem de ağ frekansına ayarlanmış güçlü bir verici ile muhabere karıştırması yaparak ağın tümünün ya da bir bölümünün iletişiminin engellenmesidir.

Güç tüketiminin artırılması: Bir verici vasıtasıyla, belirlenmiş düğümlere sahte paketler göndererek işlem yapmasını sağlayabilir ve böylece güç tüketimine neden olur. Bu düğümlerin alınan paketleri yönlendirmeleri durumunda başka düğümlerin de saldırıdan etkilenmesine ve dolayısıyla ağ genelinde bir güç kaybına neden olabilirler.

İşbirlikçi düğümlerin kullanılması: Daha önce belirtilen yöntemlerle elde edeceği düğümleri kullanarak gereksiz paketler enjekte eder, yönlendirme döngüleri oluşturur ve böylece ağ trafiğini artırır. Artan trafik diğer düğümlerin iletişimini engellediği gibi, paketlere yapılacak gereksiz işlemler (mesela yönlendirme) neticesinde güç tüketimini artırır.

3.4 YN ağlarına yapılabilecek saldırı yöntemleri

Kablosuz duyarga ağlarına yapılabilecek başlıca saldırı yöntemleri [3] ve [6]'da detaylı olarak incelenmiştir. Duyarga düğümlerinin güvenlik açısından, "en zayıf halkayı" oluşturmaları nedeniyle, bu yöntemlerin YN ağları için de en önemli saldırılar olacağı değerlendirilmektedir.

*Taklit edilen (*spoof*), değiştirilen ve yeniden gönderilen yönlendirme bilgisi:* Doğrudan ağ yönlendirmesine yapılan bir saldırı türüdür. Saldırgan yönlendirme bilgisini taklit ederek, değiştirerek veya daha önce gönderilmiş paketleri yeniden göndererek yönlendirme döngüleri oluşturmaya, ağ trafiğinin belli bölgelere ulaşmasını engellemeye, bu trafiği iş birlikçi düğümler üzerine çekmeye, trafik yollarını uzatmaya ya da kısaltmaya, ağı parçalara ayırmaya, sahte hata mesajları üretmeye ve noktadan-noktaya gecikmeyi artırmaya çalışır.

Seçici İletim (Selective forwarding): Bu saldırı türünde saldırgan, iş birlikçi düğümleri kullanarak ya da muhabere karıştırması yaparak paketlerin alıcıya ulaşmasını engeller. Saldırının en basit yolu iş birlikçi düğümlerin kara delik gibi davranmaları ve kendilerine ulaşan tüm paketleri ağdan düşürmeleridir. Ancak bu çaptaki bir engellemede ağa bir saldırı yapıldığının anlaşılması kolay olacaktır. Tespiti zorlaştırmak ya da ortadan kaldırmak için iş birlikçi düğümler hedef düğümlere ait paketleri ağdan düşürürken diğer düğümlere ait paketleri geçirirler.

Sink deliği saldırısı (sinkhole attack): Saldırgan ağ trafiğini belli bir merkeze odaklamak için iş birlikçi düğümleri en iyi yönlendirme seçeneği olarak takdim eder. Böylece diğer düğümlerin kendilerine gelen trafiği bu iş birlikçi düğümlere yönlendirmelerini sağlar. İşbirlikçi düğümler hakkında yapılan bu takdim sahte olabileceği gibi, ağ dışından destekleme ile (örneğin güçlü bir verici kullanarak paketleri direkt olarak baz istasyonuna göndermek gibi) doğru da olabilir. Bu saldırının saldırgan açısından en önemli avantajı seçici iletim saldırısını kolay hale getirmesidir. İşbirlikçi düğümler saldırganın belirlediği düğümlere ait paketleri ağdan düşürürken diğerlerini ileteceklerdir.

Sybil saldırısı: Bu saldırıda iş birlikçi düğümler kendilerini ağa farklı farklı kimliklerle tanıtırlar. Böylece özellikle aksaklığa dayanıklılık (fault-tolerant) amacıyla geliştirilmiş yöntemlerin işlevsiz kalmasına neden olurlar. Örneğin paketlerin kaybolması ihtimalini azaltmak maksadıyla çoklu yol (multi-path) yöntemini kullanan bir protokol bu işlemi yaparken aslında tüm paketleri böyle bir iş birlikçi düğüme gönderiyor

olabilir. Sybil saldırısının bir diğer uygulama hedefi de coğrafik yönlendirme kullanan ağlardır. Bu tür ağlarda iş birlikçi düğümler kendilerini birden fazla noktada bulunuyormuş gibi tanıtabilirler.

Solucan delikleri (wormholes): Bu saldırı türünde saldırgan, ağın bir bölgesinde alınan mesajları, gecikmesi az olan bir link üzerinden ağın başka bir bölgesine tüneller. Saldırı birbirine olan hop sayılarını düşük gösteren iki iş birlikçi düğüm kullanılarak gerçekleştirilir. Genellikle sink deliği saldırısı veya seçici yönlendirme saldırıları ile birlikte kullanılır.

Hello baskını saldırısı (hello flood attack): Saldırgan güçlü çıkış gücüne sahip bir verici vasıtasıyla ağa "hello" mesajı gönderir. Bu mesajı alan düğümler vericinin kendilerine komşu bir düğüm olduğunu düşünür ve yönlendirme tablolarını buna göre oluştururlar. Ancak bu düğümlerin çıkış gücü yeterli olmadığından sahte düğüme göndermek isteyecekleri mesajlar kaybolacaktır. Saldırganın baz istasyonuna kaliteli bir yolunun bulunduğunu ilan etmesi ile tüm düğümler mesajlarını bu düğüme iletmeye çalışacak ve böylece ağ trafiği kesilecektir.

Alındı taklidi (acknowledgement spoofing): Bu saldırı türünde saldırgan link katmanında kullanılan alındı paketlerinden yararlanır. İşbirlikçi düğüm, komşularının trafiğini takip ederek, bunların gönderdiği paketler için alındı mesajı yayımlar. Amaç komşularının zayıf bir linkin normal çalıştığını ya da çalışmayan bir düğümün normal faaliyet gösterdiğini düşünmelerini sağlamaktır. Böylece ağ seçici yönlendirme saldırısına da açık hale gelmektedir.

4. YN ağları için güvenlik çözümleri

Henüz teorik temellerinin geliştirilmesi aşamasında olan YN ağlarında gizlilik, bütünlük ve kullanılabilirliği sağlayabilecek, bu ağların Bölüm 2 de açıklanan özelliklerine uygun güvenlik çözümlerinin belirlenmesi ve geliştirilmesi gerekmektedir. Bu maksatla duyarga ağları için önerilen güvenlik çözümlerinden istifade edilebileceği değerlendirilmektedir. Bu bölümde önerilerden beşi incelenecektir: TinySec [2], SPINS [4], enerji verimli güvenlik protokolü [7], seviyelendirilmiş güvenlik mekanizmaları [8] ve Karantina Bölgesi Yöntemi [9].

4.1 TinySec

Berkeley Üniversitesi tarafından geliştirilen TinySec, TinyOS sürümü içerisine dahil edilmiş bir bağlantı katmanı (link layer) güvenlik mimarisidir. Tasarımda kullanım kolaylığı ve duyarga ağına en az ek yük getirmesi esas olarak alınmıştır. Klasik bilgisayar ağılarında mesaj doğrulaması, bütünlüğü ve gizliliği genellikle sondan-sona (end-to-end) güvenlik mekanizmalarıyla gerçekleştirilmektedir. Aradaki geçitler mesajın içeriği ile ilgilenmemekte, sadece mesajın başlığına bakarak yönlendirme yapmaktadırlar. Duyarga ağlarında ise en az güç tüketimi ve band genişliğinin optimum kullanımı için, kümeleme ve aynı mesajların elenmesi gibi "ağ içi işleme (in-network processing)" yapılmaktadır. Bunun başarılabilmesi için arada yönlendirme işlemi yapan düğümlerin mesaj içeriğine ulaşmaları, değişiklik yapmaları ve belki de düşürmeleri gerekmektedir. Bu nedenle, TinySec geliştirilirken, klasik ağlardaki sondan-sona güvenlik mekanizmalarının duyarga ağları için iyi bir çözüm olamayacağı, bu işlemin bağlantı katmanında yapılması gerektiği kabul edilmiştir. Ayrıca sorunu bu katmanda çözmenin, yetkisiz mesajların baz istasyonuna ulaşmadan, henüz ağa ilk girişinde yakalanmasına ve dolayısıyla DoS saldırılarına karşı duyarga ağının daha güvenli olmasına katkıda bulunacağı düşünülmüştür.

TinySec iki farklı güvenlik seçeneğini desteklemektedir:

- Kimlik kanıtlamalı (authentication) şifreleme,
- Sadece kimlik kanıtlama.

Kimlik kanıtlamalı şifrelemede veri yükü şifrelenir ve pakete bir kimlik kanıtlama kodu (MAC) eklenir. Sadece kimlik kanıtlamada ise veri yükü şifrelenmez, sadece paket doğrulaması yine bir MAC ile gerçekleştirilir. Bundan da anlaşılacağı üzere TinySec'de kimlik kanıtlama her paket için bir zorunluluk, verinin şifrelenmesi ise uygulamaya göre karar verilebilecek bir seçenektir. Mesajların şifrelenmesinde Skipjack blok şifrelemesi, 8 baytlık bir başlangıç vektörü (IV) ve şifre bloğu zincirlemesi (CBC) ile kullanılmaktadır. Anahtarlama yöntemi için herhangi bir sınır getirilmemiş olup, uygulamada arzu edilen güvenlik seviyesine göre tüm ağ için tek bir anahtar çifti (biri verinin şifrelenmesi, diğeri ise MAC'ların hesaplanması için) seçilebilir.

TinySec kimlik kanıtlamalı şifrelemenin kullanıldığı en sıkı güvenlik seviyesinde enerji, gecikme ve band genişliğine %10 ek yük getirmektedir. Sadece kanıtlamanın kullanıldığı durumlarda ise bu oran %3'e düşmektedir.

4.2 SPINS (Security Protocols for Sensor Networks)

Berkeley Üniversitesi tarafından geliştirilen SPINS, kimlik kanıtlamalı yayımda kullanılan μTESLA (Micro Version of Timed, Efficient, Streaming, Loss-tolerant Authentication Protocol) protokolü, gizliliği, iki düğüm arası kimlik kanıtlamayı ve verinin tazeliğini (data freshness) sağlayan SNEP (Secure Network Encryption

Protocol) protokolü yapı taşlarından ve bunlar üzerine oturtulmuş bir yönlendirme protokolünden meydana gelmektedir.

SNEP aşağıdaki imkanları sunmaktadır:

- *Semantik güvenlik:* Ağı dinleyen bir saldırganın, aynı düz metnin birden fazla şifreli kopyasını aldığında dahi bunlardan düz metin hakkında herhangi bir bilgi edinememesi anlamın gelen semantik güvenlik, alıcı ve gönderen arasında paylaşılan ve her mesaj alış-verişinde artırılan bir sayaç sayesinde gerçekleştirilmektedir.
- *Kimlik kanıtlaması:* Alıcı düğüm gönderinin kimliğini kullanılan MAC ile kanıtlamaktadır.
- *Tekrar koruması:* MAC içerisindeki sayaç eski mesajların tekrar gönderilmesine karşı koruma sağlamaktadır.
- *Zayıf tazelik:* Semantik güvenlik maksadıyla alıcı ve gönderen arasında kullanılan sayaç, alınan mesajın bir önceki mesajdan sonra gönderildiğini garantilemektedir.
- *Düşük haberleşme ek yükü:* Sayacın alıcı ve gönderen üzerinde tutulması, mesaj içerisine konulmaması haberleşme ek yükünü azaltmaktadır.

Klasik yaklaşımlarda kimlik kanıtlaması asimetrik yöntemlerle yapılmaktadır. Ancak duyargaların donanımsal kısıtlamaları, oldukça pahalı olan asimetrik yöntemler için son derece yetersizdir. µTESLA kimlik kanıtlamasına asimetriklik mantığını simetrik yöntemlerle kazandırmaktadır. Gönderen, yayımlanacak mesaj paketleri için sadece kendisi tarafından bilinen bir anahtar ve tek yönlü bir fonksiyon kullanarak bir MAC oluşturur. Mesaja ait anahtarı mesajın yayımından belli bir süre sonra yayımlar. Böylece paketin içeriğinin değiştirilebilmesi ihtimali ortadan kaldırılmış olur. Alıcı tarafında, bu anahtar kullanılarak bir arabellekte tutulan paketin doğruluğu kontrol edilir.

Şifreleme işleminde RC5 kullanılmaktadır. Tüm bu kimlik kanıtlama işlemi için µTESLA alıcı ve gönderen arasında gevşek de olsa bir eş zamanlamaya ihtiyaç duymaktadır.

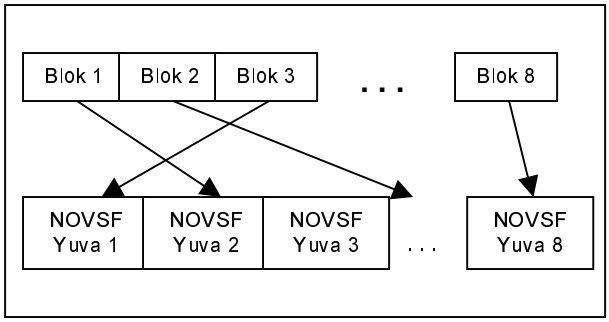
4.3 Enerji verimli güvenlik protokolü

Klasik bilgisayar ağlarında kullanılan simetrik şifreleme tekniklerinin uzun anahtar gereksinimleri ve ana bellek ihtiyaçları gibi nedenlerle duyarga ağlarında direkt olarak kullanılmaları mümkün değildir. Enerji verimli güvenlik protokolü bu sorunları bloklama yapmayan OVSF (non-blocking Orthogonal Variable Spreading Factor) kullanan kod atlaması ile ortadan kaldırmaktadır.

Her duyarga atılmadan önce kendisine gizli bir anahtar verilir. Bu anahtar baz istasyonu tarafından da bilinmektedir. Baz istasyonu periyodik olarak yeni oturum anahtarları yayımlar. Bu anahtarı alan bir düğüm kendi gizli anahtarını kullanarak o düğüme özgü gizli oturum anahtarını hesaplar. Yeni gizli anahtar kimlik kanıtlamasında ve veri tazeliğinin sağlanmasında kullanılır.

Çok uzun anahtarlar ve işlemsel olarak pahalı algoritmaların eksikliğini gidermek ve güvenliği artırmak için bu protokol, ilave enerji gereksinimine ihtiyaç göstermeyen NOVSF kod atlaması kullanmaktadır. Her NOVSF kodu 64 zaman yuvasına (time slot) sahiptir. Protokol, bir çoklayıcı yardımıyla, her oturumda veri bloklarını değişik bir permütasyonla bu zaman yuvalarına atamaktadır (Şekil 3). Bunu sağlamak üzere baz istasyonu küme başlarına (cluster head) periyodik olarak yeni permütasyonlar göndermektedir.

Kullanılan algoritmada, duyarga düğümleri öncelikle oturum anahtarını kullanarak göndereceği veriyi şifrelemekte ve daha sonra NOVSF kod atlama tekniğini uygulayarak veriyi göndermektedir. Böylece saldırılar için çift katlı bir güvenlik oluşturulmaktadır.



Şekil 3: NOVSF veri bloğu-zaman yuvası ataması [7]

4.4 Seviyelendirilmiş güvenlik mekanizmaları

Bu güvenlik yönteminde, duyarga ağı için alınacak güvenlik tedbirlerinde harcanacak enerjiyi en aza indirmek ana hedef olarak kabul edilmiştir. Bu maksatla güvenlik mekanizmaları değişik seviyede güvenlik hassasiyetine sahip

- gezgin kod
- duyarga mevkii
- uygulama-özel veri

için üç değişik seviyeye ayrılmıştır. Her üç seviyede de iletilen veriler şifrelenirken, şifrelemede kullanılan tekniğin gücü korunacak verinin hassasiyeti ile doğru

orantılı olarak artmaktadır. Şifrelemede RC6 algoritması kullanılmakta ve algoritmanın tur sayısına kumanda edilerek verinin bu üç güvenlik seviyesinden birine göre şifrelenmesi sağlanmaktadır.

- *Güvenlik seviyesi 1:* Duyarga ağına iş birlikçi kod enjekte edilmesi büyük bir güvenlik açığı oluşturacaktır. Bu nedenle gezgin kodun diğer verilere göre ağda daha az dolaşıyor olmasından da istifadeyle bu kodlara en üst seviye şifreleme işlemi uygulanır.
- *Güvenlik seviyesi 2:* Duyarga ağları için geliştirilen uygulamaların pek çoğunun, duyargaların mevkilerini her mesaj içerisine dahil edeceği öngörülmüştür. Bu nedenle seviye 2'de güçlü bir şifreleme ek yükü oldukça artıracaktır. Diğer taraftan, zayıf bir şifreleme duyarga mevkilerinin saldırgan tarafından daha kolay tespit edilmesini sağlayacaktır. Bu nedenle, ağın bir bölgesine yapılan saldırının diğer bölgeleri etkilememesi için bu güvenlik seviyesinde, ağ hücrelere bölünerek mevki tabanlı anahtarlar kullanılır.
- *Güvenlik seviyesi 3:* Ağ içerisinde en sık dolaşan veri uygulama-özel veriler olduğu için, bu seviyede güvenlikten bir miktar ödün verilerek en zayıf şifreleme yapılır. Şifreleme için kullanılacak anahtar ana anahtardan türetilir.

4.5 Karantina bölgesi yöntemi

Duyarga ağlarına iş birlikçi düğümler tarafından yapılacak spam saldırılarına karşı koymak için geliştirilmiş bir güvenlik mekanizmasıdır. Aşağıdaki hususlar için yöntemler içermektedir:

- *Spam saldırısının tespiti:* Baz istasyonu tarafından kendisine ulaşan mesajların içeriğe göre filtrelenmesi ve çok fazla hatalı mesaj gönderen düğümlerin tespiti ile yapılır. Diğer bir yöntem de belli bir bölgeden gönderilen mesajların frekans analizine tabi tutularak anormalliklerin belirlenmesidir.
- *Karantina bölgesinin oluşturulması:* Baz istasyonu bir spam saldırısı tespit ettiğinde bunu ağa yayımlar. Durumdan haberdar olan düğümler belirlenmiş bir süre kadar kimlik kanıtlaması yapılmamış mesajları yönlendirmezler. Herhangi bir düğüm bu süre içerisinde kimlik kanıtlaması yapılmamış bir mesaj aldığında ilk önce bir kimlik kanıtlama isteğinde bulunur. Gönderenin bunu başarı ile gerçekleştirememesi durumunda alıcı kendini karantina bölgesinde kabul eder ve komşuları ile mesajlaşmayı kimlik kanıtlama yaparak devam ettirir.
- *Kimlik kanıtlama:* Karantina bölgesindeki tüm düğümler kimlik kanıtlamalı mesajlaşma yaparken, bölgenin dışında kalan düğümler kimlik kanıtlama yapmazlar. Kimlik kanıtlama işlemi için düğümlere yüklenen gizli anahtar ve HMAC fonksiyonu kullanılarak oluşturulan kod, mesaj başlığına eklenir. Mesaj başlığına eklenen diğer bir alanda ise bir sayaç kullanılarak verinin tazeliği sağlanır.
- *Karantina bölgesinin kaldırılması:* Karantina bölgesinde bulunan bir düğüm karantina süresi içerisinde komşularından başarısız bir doğrulama faaliyeti tespit etmedi ise karantina modundan çıkar.

5. Sonuç

Gelişen yeni bir konsept olan YN ağları yakın bir gelecekte araştırma/geliştirme faaliyetlerinin odaklanacağı bir saha olacaktır. Ancak bu ağların donanımsal kısıtları, kablosuz iletişim ortamı, gerçek zamanda işlem ihtiyacı, heterojen yapı, düğüm sayısının fazlalığı, ölçeklenebilirlik ihtiyacı, gezginlik, uygulama ortam şartlarının ağırlığı ve maliyet gibi hususlardan kaynaklanan kendilerine özgü özellikleri, klasik bilgisayar ağları için geliştirilmiş güvenlik mekanizmalarının kullanılabilirliğini engellemektedir. Bu bildiride YN'lerin bu özellikleri güvenlik açısından incelenmiş, gizlilik, bütünlük ve kullanılabilirliğe yapılabilecek muhtemel saldırılar belirlenmiş ve bu saldırılara karşı geliştirilen önlemlerden beş tanesi anlatılmıştır.

YN ağları çok büyük bir oranda zaman-kritik ve hayati öneme sahip uygulamalar için kullanılacaktır. Bu durum, kablosuz, altyapısız duyarga ve tetikleyici ağlarından miras alınanlar ile yeni tanıtılan güvenlik sorunlarının çok daha ön plana çıkmasına neden olacaktır. Henüz teorik temellerinin oluşturulması aşamasında bulunan bu ağların başarısında ve kabul görmesinde en belirleyici unsurlardan biri olacak olan güvenlik konusunun da bu temeller içerisine başlangıçtan itibaren eklenmesinin uygun olacağı değerlendirilmektedir.

Kaynaklar:

[1] Cemalettin Çiftçi, Mithat Dağlar, Erdal Çayırcı, Turgay Karlıdere, Müjdat Soytürk, "Functional and Physical Decomposition of Cooperating Objects", Teknik Rapor TR-BME-05-02-15, Deniz Bilimleri ve Mühendisliği Enstitüsü, Deniz Harp Okulu, Tuzla, İstanbul, 2005

[2] Chris Karlof, Naveen Sastry, David Wagner, "TinySec: a link layer security architecture for wireless sensor networks", Proceedings of the 2nd international conference on Embedded networked sensor systems, November 2004

[3] Chris Karlof, David Wagner, "Secure routing in wireless sensor networks: Attacks and countermeasures", Proceedings of the 1st IEEE

International Workshop on Sensor Network Protocols and Applications, May 11, 2003.

[4] Adrian Perrig, Robert Szewczyk, Victor Wen, David Culler, J.D. Tygar, “SPINS: Security protocols for sensor networks”, The Seventh Annual International Conference on Mobile Computing and Networking (MobiCom 2001), 2001.

[5] Haowen Chan, Adrian Perrig, “Security and Privacy in Sensor Networks”, IEEE Computer Magazine, October 2003.

[6] Erdal Cayirci, “Wireless Sensor and Actuator Networks”, IEEE Tutorial Now.

[7] Hasan Çam, Suat Özdemir, Devasenapathy Muthuavinashiappan, Prashant Nair, “Energy Efficient Security Protocol for Wireless Sensor Networks”, IEEE VTC Fall 2003.

[8] Sasha Slijepcevic, Miodrag Potkanjak, Vlasios Tsiatsis, Scott Zimbeck, Mani B. Srivastava, “On Communication Security in Wireless Ad-Hoc Sensor Networks”, Proceesings of Eleventh IEEE International Workshops on Enabling Technologies (WETICE’02).

[9] V. Coskun, E. Cayirci, , A. Levi, S.Sancak, “Quarantine Region Scheme to Mitigate Spam Attacks in Wireless Sensor Networks,” IEEE Transactions on Mobile Computing, (to appear).