Kablosuz Algılayıcı Ağlarında Güvenlik: Sorunlar ve Çözümler

Majid Meghdadi [1], Suat Özdemir[2*], İnan Güler[3]

[1] Bilgisayar Mühendisliği Bölümü Mühendislik Fakültesi, Zanjan Üniversitesi, Zanjan, İran
[2] Bilgisayar Mühendisliği Bölümü, Mühendislik Mimarlık Fakültesi, Gazi Üniversitesi, Ankara, Türkiye
[3] Elektronik-Bilgisayar Bölümü, Teknik Eğitim Fakültesi, Gazi Üniversitesi, Ankara, Türkiye
meghdadi@mail.znu.ac.ir, suatozdemir@gazi.edu.tr, iguler@gazi.edu.tr

Özet— Günümüzde düşük maliyetli algılayıcı mimarilerindeki ve kablosuz iletişimdeki gelişmelerle beraber Kablosuz Algılayıcı Ağları (KAA) izleme ve takip etme gibi birçok uygulamada kullanılmaya başlanmıştır. Genelde gözetimsiz ortamlarda kullanılmaları ve kaynakları kısıtlı algılayıcılardan oluşmaları sebebiyle, KAA'lar içerden ve dışarıdan gelebilecek birçok güvenlik atağına karşı savunmasızdırlar. Özellikle askeri ve sağlık uygulamaları gibi güvenlik yönünden hassas veri iletiminin yapıldığı KAA'larda veri gizliliğini ve bütünlüğünü sağlayacak güvenlik mekanizmalarına fazlasıyla ihtiyaç vardır. Daha da önemlisi, KAA'ların kendilerine has özellikleri sebebiyle bu güvenlik mekanizmaları sistem tasarımı aşamasında geliştirilmelidir. Bu çalışmada, KAA'ların güvenlik sorunlarına ait önemli çalışmalar araştırılmış, karşılaşılan engeller ve gereklilikler sunulmuştur.

Anahtar Kelimeler— Kablosuz algılayıcı ağları (KAA), KAA'larda güvenlik, DoS atakları.

Security in Wireless Sensor Networks: Problems and Solutions

Abstract— The recent advances in low-power integrated circuits and wireless communications have enabled Wireless Sensor Networks (WSNs) to be used in many activities such as surveillance and tracking. Due to their unattended nature and resource-constrained sensor nodes, however, WSNs are extremely vulnerable to any kind of internal or external security attacks. Especially for military applications where usually security sensitive data are carried over, there is a tremendous need for security mechanisms that ensure data confidentiality and integrity. In addition, because of the unique properties of WSNs, these security mechanisms must be developed during system design process. In this paper, we survey the "state-of-the-art" in WSN security and present the obstacles and requirements.

Keywords — Wireless sensor networks (WSN), WSN security, DoS attacks.

1. GİRİŞ

Düşük maliyetli algılayıcı mimarilerindeki ve kablosuz iletişimdeki gelişmeler Kablosuz Algılayıcı Ağlarını (KAA) yeni ve popüler araştırma alanı yapmıştır [1]. Bu ağlar çok sayıda sınırlı kapasiteli, kısa mesafeli vericiye sahip, düşük güçlü ve düşük maliyetli algılayıcının kolayca erişilemeyen ve çoğu zaman güvenilir olmayan bir ortama rastgele bırakılmasıyla oluşur. Her bir algılayıcı düğümü çevresindeki sıcaklık, nem, basınç gibi nicelikleri ölçebilme, basit hesaplama işlemleri yapabilme ve diğer algılayıcı düğümleri veya merkezi baz istasyonuyla haberleşme yapabilme özelliklerine sahiptir. KAA'larda planlanmış bir ağ omurgası yoktur ve algılayıcılar tarafından ortak gayret sarf ederek toplanan veriler merkezi bir baz istasyonuna diğer algılayıcılar üzerinden gönderilir.

KAA'ların uygulama alanları askeri projelerden sağlık uygulamalarına veya iklim izleme uygulamalarına kadar uzanır [1]. Düşman hatlarının gözetlenmesi ya da sınır bölgelerinin gözetlenmesi gibi hassas KAA uygulamalarında, algılayıcılardan baz istasyonuna gizli veri aktarımını sağlayan güvenlik protokolleri mutlaka kullanılmalıdır. Ancak, algılayıcıların düşük işlemci ve radyo kapasiteleri geleneksel güvenlik protokollerinin KAA'larda uygulanmasına olanak tanımaz [2]. Dahası, algılayıcıların fiziksel güvenlikleri sağlanamadığından, algılayıcılar her an kötü niyetli kişilerce ele geçirilip, yeniden programlanabilir. Bu tip algılayıcılar "ele

geçirilmiş algılayıcılar" (compromised nodes) olarak tanımlanır ve ağdaki diğer algılayıcılar genelde ele geçirilmiş algılayıcıları fark edemez [1]. Bunlara ek olarak, algılayıcı düğümlerinin yapısı, ele geçirilmiş algılayıcılar, ağ boyutu gibi faktörlerden dolayı, KAA'lar geleneksel ad-hoc ağlardan farklılık gösterir ve bu yüzden geleneksel ad-hoc ağlar için geliştirilmiş olan güvenlik çözümleri KAA'larda kullanılamaz. Tablo 1 de KAA'lar ve geleneksel ad-hoc ağlar arasındaki farklar özetlenmiştir. Bu sebeplerden dolayı, KAA'larda kullanılacak olan güvenlik protokolleri bu ağların kendilerine has özellikleri ve "ele geçirilmiş algılayıcılar" göz önüne alınarak tasarlanmış olmalıdır. Bu makalede KAA'lara özel güvenlik problemleri ve bunlara karşı geliştirilen bazı savunma mekanizmaları özetlenmiştir.

Çizelge 1. Geleneksel Ad-Hoc Ağlar (AHA) ve Kablosuz Algılayıcı Ağlar (KAA) arasındaki farklar

	AHA	**KAA**
Açık anahtar altyapısı	Kullanılır	Kullanılmaz
Gizli anahtar altyapısı	Kullanılır	Kullanılır
Hareketlilik (Mobility)	Çoğunlukla	Bazen
İşbirlik (Collaboration)	Az	Çok
Haberleşme topolojisi	One-to-one	Many-to-one One-to-many
Kaynak	Normal	Çok sınırlı

2. KAA'LARIN KARAKTERİSTİKLERİ

Daha öncede bahsedilen kaynak açısından kısıtlı algılayıcılar ve KAA'ların boyutları, güvenlik çözümleri üreten araştırmacıların önüne yeni zorluklar çıkarmaktadır. Bu bölümde geleneksel güvenlik protokollerini KAA'larda kullanmayı engelleyen ve sadece KAA'lara ait karakteristikler özetlenmiştir. Bu bölümde açıklanan karakteristiklerin protokol tasarımı ve geliştirilmesi sırasında dikkate alınması protokolün kullanılabilirliğini artırmaktadır [3].

2.1. Büyük ölçek

KAA'ların genel uygulamaları (örneğin askeri gözetleme uygulamaları) coğrafi açıdan geniş bir alanın kapsanmasını gerektirir. Ayrıca düğümlerin yüksek ölüm oranları, kısıtlı radyo kapasiteleri, güvenilirliği düşük ucuz algılayıcılar sebebiyle KAA'lar genelde çok büyük ölçekte olabilir ve bir KAA'daki düğüm sayısı on binleri aşabilir [2].

2.2. Kısıtlı kaynak

KAA'ların düşük kurulum ve işletim maliyetli olma zorunluluğu algılayıcı düğümlerinin donanım açısından sade olmasını gerektirir [1]. Bu nedenle KAA'larda işlem ve iletişim kaynakları kısıtlıdır. Örneğin genel bir algılayıcı türü olan (TelosB) 16 bitlik, 8 MHz işlemci, 48KB ana hafıza, 1024 KB anlık belleğe sahiptir [4]. Ayrıca algılayıcı bataryalarının değiştirilmesi çok zor hatta çoğu zaman imkansız olduğundan ve KAA'ların yaşam süresi bu bataryaların kullanım sürelerine bağlıdır. İşlemci kapasitesinin düşüklüğü, hafıza ve radyo iletiminin kısıtlı olması, ağ ömrünün batarya ömrü ile sınırlı olması KAA'lar için tasarlanan her protokolü etkilemektedir.

2.3. Artıklılık

KAA'ları oluşturan algılayıcı düğümlerinin yaşam sürelerinin önceden kestirilememesi ve algılayıcıların kısa radyo iletişim aralıkları, KAA'larda düğüm artıklığını zorunlu kılmaktadır. Bu nedenle KAA'lar kurulurken algılayıcı düğümleri yüksek dereceli bir artıklılıkla kullanılırlar. Bu yüksek dereceli düğüm artıklılığı sayesinde tek bir düğümün vaktinden önce kullanılmaz duruma gelmesi, sistemin kapasitesini çok fazla etkileyemez. Ancak düğüm artıklılığı nedeniyle her olay birden fazla algılayıcı düğümü tarafından algılanır ve dolayısı ile ağda taşınması gereken veri miktarı artar. Başka bir deyişle artıklık baz istasyonuna gönderilen verilerin miktarını artırmakta ve ağın yaşam süresini azaltmaktadır. Veri artıklılığından kurtulmak için veri kümeleme protokolleri kullanılmaktadır [1].

2.4. Güvenlik

Askeri sistemler ve tıbbi takip sistemleri gibi KAA uygulamaları güvenlik açısından çok hassastırlar. Algılayıcı düğümlerinin kısıtlı kaynaklarından dolayı geleneksel güvenlik mekanizmaları KAA'larda kullanılamaz. Buna ek olarak KAA'larda geleneksel ağlarda görülmeyen algılayıcıların fiziksel güvenliklerinin olmaması sorunu vardır. Algılayıcıların fiziksel güvenlikleri sağlanamadığından, ağdaki algılayıcı düğümleri her an kötü niyetli kişilerce ele geçirilip, kötü amaçlar için kullanılabilirler. Bu nedenlerden dolayı KAA'ların güvenlik mekanizmaları algılayıcı düğümlerinin kaynak kısıtları ve kötücül algıyıcılar göz önüne tutularak tasarlanmalıdır.

2.5. Veri Merkezli İşleme

Veri merkezli işleme KAA'ların en önemli özelliklerindendir. Algılayıcı düğümlerin ID'leri uygulamalar için çoğu zaman önemli değildir. Bu nedenle KAA uygulamalarında adlandırma düzeni çoğunlukla veriye yöneliktir (data oriented). Örneğin bir çevre gözetim sisteminde sıcaklık ölçümü yapmak için "X,Y ve Z düğümlerinden sıcaklık ölçüm değerlerini topla"

şeklinde değil, "(X_1,Y_1,X_2,Y_2) koordinatları ile sınırlandırmış bölgeden sıcaklık ölçüm değerlerini topla" şeklinde olur. O bölgedeki algılayıcı düğümlerinin ID lerinin uygulama için bir önemi yoktur.

2.6. Tahmin Edilememezlik

Algılayıcıların donanımlarının fiyatının çok düşük olması, hava durumu ve zor çevre koşulları gibi nedenlerle algılayıcı düğümlerinde ölçüm hataları çok yaygındır. Çok sayıda dağıtılmış düğüm tarafından paylaşılan kablosuz iletişim ortamı istenmeyen tıkanıklık ve engellemelere neden olmaktadır. Yüksek bit hata oranı, düşük bant genişliği ve çok sayıda algılayıcı düğümünün aynı iletim ortamını kullanması nedeniyle, KAA'larda iletişim yüksek tahmin edilememezlik gösterir. Bu tahmin edilememezlik, genelde sistem parametrelerinin çevrim-dışı (off-line) tasarımını engellemektedir. Bu nedenle KAA tasarımında çevrim-içi (on-line) gözetim ve geri-beslemeli kontrol, yüksek servis kalitesini (quality-of-service) sağlamak için gereklidir.

2.7. Gerçek Zamanlı Kısıtları

KAA'lar gerçek dünya işlemlerinde kullanıldıklarından çoğu zaman gerçek zaman kısıtlamalarına uymaları gerekmektedir. Gözetim sistemlerinde, örneğin iletişimdeki gecikme doğrudan doğruya uygulamanın hedef bulma niteliğini olumsuz yönde etkilemektedir. Kablosuz iletişimin tabiatından ve trafik yoğunluğunun önceden tahmin edilememesinden dolayı, KAA'ların katı-gerçek-zamanlı (hard-real-time) kısıtlamaları garanti etmesi beklenemez ancak olasılık temelli araştırmalar zaman kısıtlamalarının belli seviyelerde garanti edilmesini sağlayabilmektedir.

3. KAA'LARDA GÜVENLİK GEREKSİNİMLERİ

Bir önceki bölümde bahsedildiği gibi güvenlik KAA'ların en önemli sorunlarından biri sayılmaktadır. Bu bölümde KAA'larda ne tür güvenlik gereksinimlerine ihtiyaç olduğunu açıklanmaktadır. Bu gereksinimlerden çoğu geleneksel kablolu ve kablosuz ağlar içinde vardır ancak bu makalede güvenlik gereksinimleri KAA'lar açısından incelenmektedir.

3.1. Veri Gizliliği

Veri gizliliği KAA'larda, toplanan veriye yetkisiz kişilerin erişiminin engellenmesini garantiye almaktadır ve hassas KAA uygulamalarında en önemli gereksinimden biridir. Bir algılayıcı düğüm çevreden okuduğu verileri komşularına sızdırmamasının sağlaması gerekir [2,5]. Özellikle askeri uygulamalarda düğümlerde depolanan veriler çok hassas olabilir. Ayrıca birçok uygulamalarda düğümler çok hassas verileri, (örneğin, anahtar dağılımı) kablosuz iletim ortamı üzerinden diğer algılayıcı düğümlerine aktarmak zorundadırlar. Bunlara ilaveten yönlendirme verileri de kötücül düğümlere karşı, gizli tutulmalıdır. Çünkü kötücül düğümler bu verilerden yararlanarak ağın performansını düşürebilirler. Bu nedenlerle KAA'larda veri aktarımı için güvenli bir iletişim kanalı oluşturulması çok önemlidir. Hassas verileri gizli tutmak için standart yaklaşım, verinin bir gizli anahtar ile şifrelenmesidir. Düşük enerji tüketimlerinden dolayı KAAlarda gizli anahtar alyapısına dayalı şifreleme algoritmaları kullanılmaktadır.

3.2. Veri Bütünlüğü

Veri gizliliği kötücül düğümlerin veriyi ele geçirememesini garanti edebilir ama verinin yetkisiz kişilerce değiştirilmesini engelleyemez. Veri bütünlüğü iletişimde mesajın değiştirilmemesini garanti etmektedir. Bir kötücül düğüm mesajları bozarak ağın düzgün çalışmamasına neden olabilir. Dahası, doğrudan doğruya bir kötücül düğüm olmadan da mesajlar aktarım esnasında da bozulabilir. Bu nedenle veri bütünlüğü için mesaj kimlik kanıtlama doğrulama kodları (message authentication codes) ya da dairesel kodları (cyclic codes) kullanmak zorunludur.

3.3. Kaynak Doğrulama

KAA'lar ortak kablosuz ortamı kullandığından, kötücül düğümlerden gelen mesajları veya yanıltma paketlerini bulmak için, kaynak doğrulama mekanizmalarına ihtiyaç vardır. Kaynak doğrulama metotları bir düğümün iletişim halinde olduğu düğümün kimliğini doğrulayabilmesini sağlamaktadır. Bir kötücül düğüm, kaynak doğrulama olmadan bir başka düğümün rolünü yaparak hassas bilgileri elde edebilir ve başka düğümlerin işleyişlerine engel olabilir. Eğer sadece iki düğüm iletişimdeyse kaynak doğrulama gizli anahtar kriptografisi (symmetric key cryptography) ile yapılabilir. Alıcı ve verici bir ortak gizli anahtar (secret key) paylaşımı ile tüm gönderilen mesajların doğrulama kodunu hesaplayabilir. Ancak, yayımlama (broadcast) türü iletişimde kaynak doğrulama için daha kompleks çözümlere ihtiyaç vardır. Perrig et. al. µTESLA [5] adlı güvenli yayımlama protokolünde gizli anahtarların açıklanmasını geciktirerek gizli anahtar kriptografisi ile yayımlama türü iletişimde kaynak doğrulamayı başarmıştır. µTESLA her bir düğüme özel olarak gönderilmiş "özetlenmiş anahtar zincirlerine" (hashed key chains) bağlıdır. Ancak her bir düğüme anahtar zincirlerinin güvenli olarak gönderilmesi bir sorundur. µTESLA nın bu eksikliği [6,7] nolu çalışmalarda giderilmiştir.

3.4. Kullanılırlık

Kullanılırlık KAA'ların servis devamlılığını servis reddi (denial-of-service -DoS) atakları sırasında da devam ettirebilmesidir. DoS atakları KAA'ın her protokol katmanında gerçekleştirilebilirler ve seçilen kurban düğümleri etkisiz hale getirebilirler. DoS ataklarına ek olarak aşırı iletişim ya da aşırı hesaplama yükü düğümün bataryasını beklenenden daha çabuk bitirebilir. KAA'nın kullanılırlığın sağlanamaması çok ciddi sonuçlara yol açabilir. Örneğin askeri bir izleme uygulamasında, eğer

bir kaç tane düğüm doğru çalışmazsa, düşman birlikleri KAA'nın çalışmayan bu bölümünden içeri sızabilirler. Kullanılırlık KAA'larda genelde algılayıcı düğüm artıklığı ile sağlanmaktadır.

3.5. Lokalizasyon

KAA'larda düğümlerinin yerlerinin doğru olarak tespit edilebilmesi çok kritik özelliktir. Çünkü KAA'ların yararlı olması düğümlerin yerlerinin doğru olarak tespit edilebilmesine bağlıdır. Örneğin bir yangın uyarı sisteminde yangın çıkan yerin koordinatlarının doğru belirlenmesi için algılayıcıların koordinatları önceden doğru olarak bilinmelidir. Ayrıca yer bilgileri birçok sistemin fonksiyonelliğinde (system functionalities) kullanılır. Örneğin yer bilgisi sorgulama [8], coğrafi yönlendirme algoritmaları [9,10,11] ve ağ kapsam kontrolü [12] vb. Bu nedenle doğru algılayıcı düğümlerinin yer bilgilerinin doğru olarak tespiti bu protokollerin performansında önemli bir rol oynar.

4. KAA'LARDA GÜVENLİK ATAKLARI

Kablosuz algılayıcı ağlarda ağ güvenliğine karşı saldırıları iki grupta sınıflandırabiliriz:

- İç ataklar
- Dış ataklar

İç ataklarda saldırgan kişi bir ya da daha fazla algılayıcı düğümünü fiziksel olarak ele geçirir (node compromise). Dolayısı ile saldırgan bu algılayıcı düğümlerine ait tüm gizli anahtar bilgisine sahiptir ve ağın içinden saldırılar düzenleyebilir. Buna karşın dış ataklarda saldırgan ağdaki düğümlere ait gizli anahtar bilgisine sahip değildir ve sadece dışarıdan kendine ait algılayıcı düğümlerini kullanarak KAA'nın çalışmasını engellemeye çalışabilir. Atak tiplerinde olduğu gibi, KAA'larda saldırganları da işlem güçlerine göre iki gruba ayırmak mümkündür:

- Laptop sınıfı saldırganlar
- Algılayıcı düğüm sınıfı saldırganlar

Laptop sınıfı saldırganlar güçlü cihazlara, örneğin büyük batarya, güçlü işlemci, güçlü radyo veya daha hassas antene vb. sahiptirler. Ayrıca laptop sınıfı saldırgan yüksek bant genişliğine ve az gecikmeli iletişim yetisine sahiptirler [13]. Bir laptop sınıfı saldırgan kaynaklarını kullanarak birden çok düğüm gibi davranabilir, iletim ortamını domine edebilir ve ağın her noktasına erişebilir. Buna karşın algılayıcı düğüm sınıfı saldırganlar sadece yakın çevresindeki düğümlere engel olabilir ve düşük işlem ve gücü ve bant genişliğine sahiptir. Bu sebeple laptop sınıfı saldırganlar her zaman algılayıcı düğüm sınıfı saldırganlara göre daha tehlikelidir. Çizelge 2 atak ve saldırgan türlerini ve bunların zarar derecelerini özetlemektedir.

Çizelge 2. Atak ve saldırgan türlerinin karşılaştırılması

Atak / Saldırgan	**Dış Ataklar**	**İç Ataklar**
Laptop sınıfı	Orta Tehlikeli	Çok Tehlikeli
Algılayıcı düğüm sınıfı	Az Tehlikeli	Orta Tehlikeli

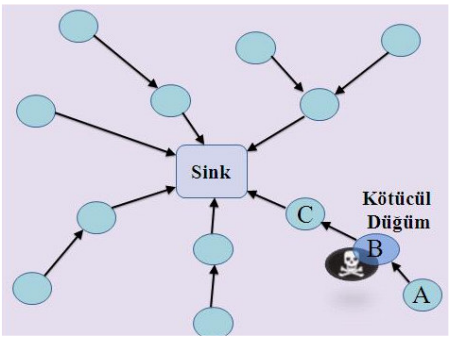
KAA'larda laptop ve algılayıcı düğümü sınıfı saldırganlar birçok iç ve dış atak çeşidi gerçekleştirebilirler. Ancak bu ataklardan en önemlisi ve tehlikelisi servis reddi (Denial of Service - DoS) ataklarıdır. Bu ataklar KAA'nın tamamını ya da bir bölümünü etkisiz hale getirmeyi amaçlamaktadırlar. Bir sonraki bölümde önemli DoS atak tipleri ve bunlara karşı geliştirilen teknikler özetlenmiştir.

5. DoS ATAKLARI VE ÇÖZÜMLER

DoS atağı bir KAA'nın kendisinden beklenen görevi yapmasının engellenmesi veya performansının büyük ölçüde düşürülmesi olarak tanımlanabilir. KAA'larda düğümler ele geçirilebilir olduğu için ağ içinden DoS atağı geliştirmek çok kolaydır. Genelde DoS atağında bir algılayıcı düğümü ağdaki kaynakları tüketmek için gereksiz paketler gönderir ve diğer algılayıcı düğümlerinin kaynaklardan veya ağ servislerinden yararlanmasını engeller. Bunun dışında çeşitli ağ katmanlarında DoS atağı gerçekleştirilebilir. Fiziksel katmanda DoS ataklar gürültü ve sıkıştırma yaratarak iletişimi engeller. DoS atakları bağlantı katmanında ise çarpışma, yorma ve eşit davranmama, şeklinde olur. Ağ ve yönlendirme katmanında paket düşürme ve hatalı yönlendirme, kara delik oluşturma şeklinde DoS atakları vardır. Taşıma katmanında ise kötücül sel ve senkronizasyonu bozma şeklinde DoS atakları bulunmaktadır. Bu ataklara karşı kaynak kullanımını ücretlendirme, güçlü kimlik doğrulama ve trafik tanımlama gibi metotlar kullanılır [14,15,16]. Bu bölümün geri kalan kısmında KAA'lardaki önemli DoS atakları açıklanmıştır.

5.1. Tekrarlama Atağı

Tekrarlama ataklarında saldıran düğüm iki düğümün arasında gönderilen mesajları tekrarlayarak ağdaki düğümlerin erken güç tükenmesine ve ağdaki trafiğin yoğunlaşmasına neden olmaktadır. Şekil 1.de görüldüğü gibi B kötücül düğümü, A düğümünden gelen mesajları C düğümüne aktardıktan sonra aynı mesajı defalarca tekrarlamaktadır. Bu şekilde C'nin kaynaklarını boşa harcayarak asıl görevini yerine getirmesini engellemektedir.

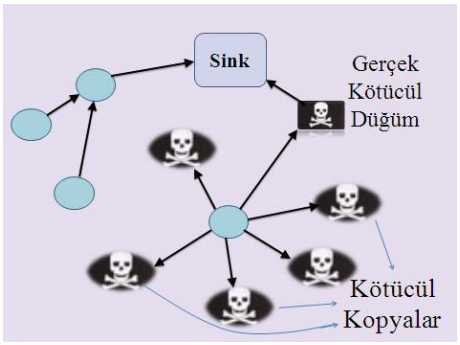


Şekil 1. Tekrarlama atağı - Düğüm B, A düğümünden gelen mesajları birçok kez tekrarlayıp C'ye göndermektedir.

Bu atak için en basit çözüm her mesaja bir sayaç alanı ekleyerek mesajın tekrarlanmasına engel olmak olabilir, ancak KAA'larda hafızanın kısıtlı olması böyle bir çözümü uygulanabilir kılmaz. Tekrarlama atakları veri bağlantısı katmanında gerçekleştirilir ve geleneksel ağlarda Bloom süzgeci kullanılarak önlenebilir [17]. Bloom süzgeci çözümünde her düğüm için bir tane tablo tutulur. Yüksek düğüm sayısı ve bellek kısıtları nedeniyle bu çözüm KAA'lar için uygun değildir. KAAlar tekrarlama atakları için yapılan çalışmalarda ise Karlof et. al. mesaj doğrulama ve veri bütünlüğüne ve gizliliğine dayalı bir çözüm getirmiştir [18]. Bir diğer çalışmada tekrarlama atağına karşı μTESLA doğrulama yönteminden faydalanılmıştır [7].

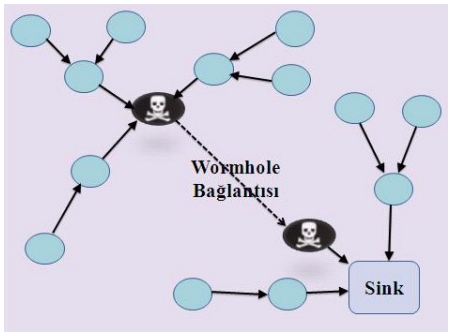
5.2. Sybil Atak

Sybil atakta bir kötücül algılayıcı düğümü kendisini ağdaki diğer düğümlere birden fazla kimlikle tanıtır. Bu durumda, kurban olarak seçilen olan düğüm bu kötücül düğümden gelen mesajları farklı düğümlerden geliyormuş gibi algılar. Kötücül düğüm bu şekilde kurban olarak seçtiği düğümlerin mesaj alıp vermesini engelleyebilir. Dahası, Sybil atak yolu ile bir kötücül düğüm sürekli yanlış bilgi göndererek ağda toplanan bilgiyi fazlasıyla değiştirebilir (Şekil 2). Böylece baz istasyonunda yanlış bilgi toplanmasına neden olarak karar verme mekanizmasını yanıltabilir.



Şekil 2. Sybil atak - Bir kötücül düğüm kendisini kopyalamaktadır.

Genelde Sybil atağa karşı "radyo kaynak testi" ve "rastgele anahtar dağıtımı" metodlarından yararlanılmaktadır. Bunlardan başka Newsome et al. [19] sybil atak için birkaç tane çözüm vermişlerdir. Bu çözümlerde yer ve kod doğrulama ve rastgele anahtar dağıtımından yararlanılmıştır. Ayrıca, Kulkarni et al. [20] iletişim esnasında doğrulama ve gizlilikten yararlanarak sybil atağa karşı bir çözüm geliştirilmiştir.



Şekil 3. Solucan deliği (Wormhole) atağı - iki kötücül düğüm baz istayonuna doğru yüksek kaliteli bir veri iletim hattının reklamını yaparlar ve veri toplarlar.

5.3. Solucan deliği (wormhole) Atağı

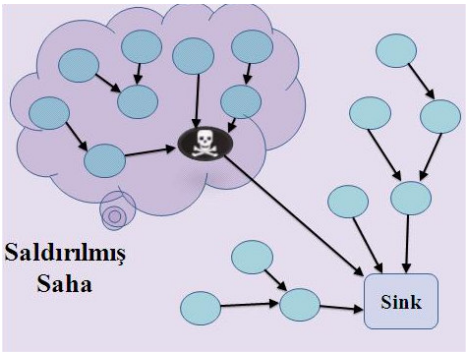
Bu tür atakta iki kötücül düğüm birbirleri arasında yüksek iletişim kalitesine sahip bir kanal oluştururlar. Daha sonra yönlendirme için bu kanalın reklamını yaparak çevredeki algılayıcılardan baz istasyonuna gönderilmek üzere veri toplarlar (Şekil 3). Ancak baz istasyonu yakınındaki kötücül düğüm toplanan veriyi baz istasyonuna iletmeyebilir ya da verileri değiştirerek baz istasyonuna gönderebilir. Hu et. al. [21] iletişimdeki düğümlerin senkronizasyonu yardımıyla bu atağa karşı bir savunma tekniği vermiştir. Hu ve Evans [22] yönlü antenler kullanarak solucan deliği atağını önlemişlerdir.

5.4. Kara delik (blackhole) Atağı

Eğer kötücül bir düğüm kendini iletişim halindeki iki düğümün arasına yerleştirirse, iletilen paketlere her şeyi yapabilir. Kara delik atağında kötücül düğüm kendini baz istasyonuna en yakın düğüm olarak lanse eder ve çevredeki algılayıcılardan baz istasyonuna gönderilmek üzere veri toplarlar [13]. Gerçekte bu atakta kötücül düğüm baz istasyonundan uzak olabilir. Saldırının amacı toplanan verilerin baz istasyonuna ulaştırılmamasıdır. (Şekil 4).

Kara delik ataklarını engellemek için bazı araştırmacılar ad-hoc ağlarında kullanan metotları KAA'larda kullanmışlar. Karakehayov [23] kara delik ataklarına karşı "REWARD" adlı bir algoritma geliştirmişlerdir. Bu algoritmada yönlendirme tekniğinden yararlanarak iki çeşit mesaj ile atağın kaynağı tespit edilir. Ngai et al. [24] ise bu atak için yeni bir metot vermiştir. Bu metotda önce

bir bölgeden gelen verilerin birbiri ile uyumlu olup olmadığına bakılır ve ağda atak olup olmadığı tespit edilir. En son olarak da ağın veri akımının analizi yardımıyla kötücül düğümü bulunur.



Şekil 4. Kara delik (balackhole) atağı - Bir kötücül düğüm kendini komşularına baz istasyonuna en yakın düğüm olarak lanse eder ve veri toplar.

5.5. Fiziksel katmandaki ataklar

Fiziksel ataklar KAA'lara özgü bir ataktır ve geleneksel ağlarda görülmez. Bu ataklar sonucunda algılayıcılar tamamen kullanılmaz hale getirilebilir, yeniden programlanarak kötücül algılayıcı düğümü olarak kullanılabilir ya da yok edilen düğümler başka kötücül düğümlerle değiştirilebilirler [25,26]. Bir algılayıcı fiziksel olarak "jamming" ve "tampering" diye adlandırılan iki şekilde etkisiz hale getirilebilir. Jamming'e karşı spread-spectrum ve mod değiştirme gibi savunma teknikleri kullanılmaktadır. Tampering'in engellenmesi ise ancak tamper-proofing adı verilen düğümleri fiziksel olarak erişilmez kılan metodla mümkündür.

5.6. Taşıma katmanındaki ataklar

Taşıma katmanı uçtan uca iletimi denetler. KAA'lar bu katmanda iletim yükünü hafifletmek için çok basit protokoller kullanır. Bu sebepten dolayı kötücül algılayıcılar için taşıma katmanında DoS atağı gerçekleştirmek çok kolaydır. Bu katmandaki en kolay atak Internet'deki TCP SYN selinde olduğu gibi sel atağıdır. Sel atağında bir kötücül düğüm çevresindeki bir kurban düğüme birçok iletişim başlatma isteği göndererek kurbanın iletişim kaynaklarını tüketmek ister. Bu atağa karşı iletişim istek sayısının kısıtlanması ya da client puzzle tekniklerinin uygulanması ile çözüm bulunabilir.

5.7. Hello seli atağı

Düğümler kendilerini komşularına tanıtmak için "Hello" paketleri gönderiler. Taşıma katmanındaki iletişim istek seli gibi, bu atakta da bir kötücül düğüm 'Hello' paketini birçok düğüme göndererek komşularının iletişim yetilerini kısıtlamak istemektedir. Bu tür atakta kötücül düğümün hem yüksek güçte sinyal gönderme kabiliyetine hem de güçlü işlemciye sahip olması gerekir. Ayrıca bu atak uzaktan laptop sınıfı bir saldırgan tarafından gerçekleşiyorsa, düğümler 'Hello' paketini aldıktan sonra uzaktaki düğümü komşu olarak kabul edip baz istasyonuna gönderilecek mesajları bu düğüm aracıyla gönderirler. Mesajları toplayan saldırgan kara delik atağıyla bu mesajları yok edebilir. Hamid et al. [27] bir olasılık temelli bir protokolde iki yönlü doğrulama ve çoklu-yol çoklu-baz istasyon kullanarak bu atağı önlemiştir.

6. SONUÇLAR

Bu makalede KAA güvenlik sorunları servis reddi (Denial of Service Atakları-DoS) atakları açısından incelenmiş ve önemli DoS atakları verilerek bunlara karşı alınabilecek önlemler belirtilmiştir. Sonuç olarak, kablosuz algılayıcı ağlarının güvenliği konusunda birçok araştırma yapılmış olsa da, halen birçok noktanın çözüm beklemekte olduğu görülmüştür. Örneğin, KAA'larda algılayıcı batarya gücü en büyük sınırlayıcı etken olduğundan, güvenlik protokolleri enerji etkinliği ve tam güvenlik sağlama arasında bir denge kurmaya zorlanmaktadırlar. Hem yüksek güvenlik hem de enerji verimliliği sağlayacak kriptografik fonksiyonların geliştirilmesi KAA'ların güvenliğinin sağlanmasında önemli bir ilerleme sağlayacaktır. Bunlara ek olarak, her ne kadar bu makalede ele alınmadıysa da, KAA'ların gizli anahtar dağıtım protokolleri ölçeklenebilirlik ve fiziksel ataklara dayanıklılık açısından geliştirilmelidir. Bu gibi güvenlik sorunları çözüldüğünde yakın zamanda KAA'ları günlük hayatımızın içinde birçok uygulamada görmek kaçınılmaz olacaktır.

KAYNAKLAR

[1] A Akyildiz, I.F. Su, W. Sankarasubramaniam, E. Cayirci, "A survey on sensor Networks", **IEEE Communications Magazine,** vol.40, no.8 , pp. 102-114, 2002.

[2] D.W. Carman, P.S. Krus, B.J. Matt, "Constraints and approaches for distributed sensor network security", **Technical Report 00-010, NAI Labs, Network Associates, Inc.,** Glenwood, MD, 2000.

[3] H. Chan ,A. Perrig. "Security and privacy in sensor networks", ***IEEE Computer Magazine***, pp 103–105, 2003.

[4] "Crossbow Technologies", **http://www.xbow.com**, 2007.

[5] A. Perrig, R. Szewczyk, J. D. Tygar, V. Wen, D. E. Culler," Spins: security protocols for sensor Networks", **Wireless Networking,** vol.8, no.5, pp.521–534, 2002.

[6] D.Liu, P. Ning, "Efficient distribution of key chain commitments for broadcast authentication in distributed sensor Networks", **10th Annual Network and Distributed System Security Symposium,** pp. 263–276, 2003.

[7] D. Liu, P. Ning, "Multi level µTESLA: Broadcast authentication for distributed sensor Networks", **Trans. on Embedded Computing Systems**, vol.3, no.4, pp. 800–836, 2004.

[8] H.Gupta, S.R. Das, Q. Gu, "Connected Sensor Cover: Self-Organization of Sensor Networks for Efficient Query Execution, MobiHoc", **Maryland, USA,** pp. 189-200, 2003.

[9] Y. Ko, N. H, Vaidya," Location-aided routing (LAR) in mobile ad hoc Networks", **Wireless Networks,** vol.6, pp. 321-324, 2000.

[10] B. Karp,H.T. Kung, "Greedy Perimeter Stateless Routing for Wireless Sensor Networks", **MobiCom'00, Boston, USA,** pp. 243-254, 2000.

[11] M. Mauve, J. Widmer, H. Hartenstein, "A Survey on Position-Based Routing in Mobile Ad Hoc Networks", **IEEE Network Magazine,** pp. 30-39, 2001.

[12] T. Yan,T. He, J.A. Stankovic," Differentiated Surveillance Service for Sensor Networks", **First ACM Conference on Embedded Networked Sensor Systems (SenSys '03), Los Angeles, USA,** pp.51-62, 2003.

[13] C.Karlof, D. Wagner, "Secure routing in wireless sensor networks: Attacks and countermeasures", **Elsevier's Ad Hoc Network Journal, Special Issue on Sensor Network Applications and Protocols, September**, pp. 293-315.2003

[14] A. D. Wood, J. A. Stankovic, "Denial of service in sensor Networks".**IEEE *Computer***, 35(10):54–62, 2002.

[15] A.D.Wood, J.A. Stankovic, S.H. Son, "JAM: A Jammed-Area Mapping Service for Sensor Networks", **24th IEEE Real-Time Systems Symposium,** pp. 286-297, 2003.

[16] M. Cagalj, S. Capkun, J.P. Hubaux, "Wormhole-based Anti-Jamming Techniques in Sensor Networks" **IEEE Transactions on Mobile Computing,** vol.6, no.1, pp. 100-114.

[17] A.D. Birrell. "Secure communication using remote procedure calls",**ACM Transactions on Computer Systems**, vaol.3, no.1,pp.1-14, 1985.

[18] C. Karlof,N. Sastry,D. Wagner, "TinySec: a link layer security architecture for wireless sensor networks", **Proc. of the 2nd international conference on Embedded networked sensor systems, Baltimore, MD, USA,** pp. 162 – 175,2004

[19] J.Newsome, E. Shi, D. Song, A. Perrig "The sybil attack in sensor networks: analysis & defenses", **Proc. of the third international symposium on Information processing in sensor networks, ACM,** pp. 259 – 268, 2004.

[20] S. S., Kulkarni, M. G., Gouda, A. Arora, "Secret instantiation in adhoc networks,", **Special Issue of Elsevier Journal of Computer Communications on Dependable Wireless Sensor Networks**, pp. 1–15,2005.

[21] Hu, Y.-C., Perrig, A., and Johnson, D.B., "Packet leashes: a defense against wormhole attacks in wireless networks", **Twenty-Second Annual Joint Conference of the IEEE Computer and Communications Societies.** Vol.3, pp. 1976 – 1986, 2003

[22] L.Hu, D. Evans, "Using Directional Antennas to Prevent Wormhole Attacks", **The 11th Annual Network and Distributed System Security Symposium,** 2004

[23] Z. Karakehayov, "Using REWARD to detect team black-hole attacks in wireless sensor networks", **Workshop on Real-World Wireless Sensor Networks REALWSN'05**, 2005

[24] C. .E. H. Ngai, J. Liu,M.R. Lyu1,"On the Intruder Detection for Sinkhole Attack in Wireless Sensor Networks**", IEEE confrance on communication** ,vol 8, pp. 3383 – 3389, 2006

[25] X. Wang, W. Gu, S. Chellappan, D. Xuan, T. H. Laii." Search-based physical attacks in sensor networks: Modeling and defense". **Technical report, Dept. of Computer Science and Engineering, The Ohio-State University**, 2005.

[26] X. Wang, W. Gu, K. Schosek, S. Chellappan, D. Xuan. "Sensor network configuration under physical attacks". **Technical Report Technical Report (OSU-CISRC-7/ 04-TR45)**, 2004.

[27] Hamid, M. A., Rashid, M-O., and Hong, C. S., "Routing Security in Sensor Network: Hello Flood Attack and Defense", **IEEE ICNEWS 2006, Dhaka,**2006.