Skipjack Şifreleme Algoritması Kullanarak Gecikme Duyarlı ve Enerji Etkin Kablosuz Algılayıcı Ağ Güvenlik Hizmeti

Providing Security Service with Skipjack Encryption Method for Delay Sensitive and Energy Aware Wireless Sensor Networks

Necla Bandırmalı[1], İsmail Ertürk[1], Celal Çeken[1], Cüneyt Bayılmış[2]

[1]Elektronik ve Bilgisayar Eğitimi Bölümü
Kocaeli Üniversitesi
bandirmali@kocaeli.edu.tr, erturk@kocaeli.edu.tr, cceken@kocaeli.edu.tr

[2]Elektronik ve Bilgisayar Eğitimi Bölümü
Sakarya Üniversitesi
cbayilmis@sakarya.edu.tr

Özet

Kablosuz Algılayıcı Ağlar (KAA'lar) sınırlı kaynaklara sahip küçük algılayıcı düğümlerden oluşmaktadır. Buna bağlı olarak, geleneksel ağlarda kullanılan birçok protokol KAA'lara doğrudan uygulanamamaktadır. Bunların başında güvenlik protokolleri yer almaktadır. Güvenlik protokollerinin temelini ise iletilecek verinin şifrelenmesini sağlayan algoritmalar oluşturur. Ayrıca, sınırlı kaynaklara sahip KAA'larda güvenlik hizmeti sunulurken, algılayıcı düğümler, iletişim ortamının en etkin şekilde paylaşımını sağlayan bir ortam erişim protokolüne de ihtiyaç duymaktadır. Bu bildiride sunulan çalışmada, Skipjack şifreleme algoritması ve Enerji-etkin ve Gecikme-duyarlı Merkezileştirilmiş Ortam Erişim Kontrol (EGMOEK) protokolü kullanılarak güvenli, gecikme duyarlı ve enerji etkin bir KAA oluşturulması amaçlanmaktadır.

Abstract

Wireless Sensor Networks (WSNs) contain nodes with very limited energy, memory and computational sources; however, they can provide many cost-effective solutions for many types of applications. Consequently, classical methods such as security protocols are usually inappropriate for WSNs to be directly applied. Security protocols are primarily based on encryption algorithms and used to provide a reliable communication. They are always employed together with a medium access control (MAC) protocol effectively sharing the wireless system sources among the wireless sensor nodes. The paper presents a Skipjack encryption-based security approach and an energy & delay-aware MAC integration work to allow reliable communications in WSN applications.

1. Giriş

Kablosuz Algılayıcı Ağlar (KAA'lar), tabii olayların, otomasyon ortamlarında üretim seviyesindeki cihazların, yerküre hareketlerinin izlenmesinden sağlık ve askeri uygulamalara kadar çok değişik alanlarda kullanılmaktadır. KAA'lar, özellikle askeri uygulamalar başta olmak üzere birçok uygulama alanında, veri gizliliği, bütünlüğü, tazeliği ve kimlik doğrulaması gibi güvenlik gereksinimlerini sağlamak zorundadır. KAA'lar geleneksel ağlardan farklı olarak sınırlı kaynaklara (enerji vb.) sahip olduklarından klasik güvenlik tekniklerinin doğrudan uygulanması açısından önemli dezavantajlarla karşı karşıyadır.

Bu çalışmada, literatürde sunulan Skipjack şifreleme algoritmasının, Enerji-etkin ve Gecikme-duyarlı Merkezileştirilmiş Ortam Erişim Kontrol (EGMOEK) protokolü kullanılarak, KAA uygulamaları için modellenmesi ve benzetimi sunulmaktadır.

Bildirinin 2. bölümünde KAA'lar ve KAA güvenliği hakkında kısa bilgiler verilmektedir. 3. ve 4. bölümlerde Skipjack şifreleme algoritması ve KAA EGMOEK protokolü incelenmektedir. 5. bölümde ise Skipjack şifreleme algoritmasının EGMOEK protokolüyle kullanımı sunulmaktadır. Bu bölüm, kablosuz algılayıcı düğüm ve merkezi düğüm olmak üzere iki süreç modelini açıklamaktadır. Bölüm 6'da OPNET geliştirme ve benzetim yazılımı kullanılarak gerçekleştirilen örnek bir KAA modeli (EGMOEK + Skipjack) sunulmaktadır ve modele ait kablosuz düğüm uçtan uca gecikme ve enerji kullanımı sonuçları verilmektedir. Son bölümde ise sonuçlar ve değerlendirmeler yer almaktadır.

2. Kablosuz Algılayıcı Ağlar ve Güvenlik Hizmeti

KAA'lar, sınırlı kapasiteye sahip, kısa mesafede kablosuz ortam üzerinden haberleşebilen düşük güçlü, düşük maliyetli ve çok fonksiyonlu algılayıcı düğümlerinden meydana gelmektedir [1]. KAA'ların kurulum kolaylığı, düşük bakım gereksinimleri ve çok değişik uygulama alanlarına sahip olmaları nedenleriyle gün geçtikçe popülerliği artmaktadır.

KAA'ların kullanım alanlarına örnek olarak, askeri uygulamalar, çevresel uygulamalar, endüstriyel uygulamalar ve ticari uygulamalar verilebilir. KAA'ların uygulamalar açısından oldukça önemli olumlu yanlarının yanı sıra olumsuz özellikleri de bulunmaktadır;

- *Avantajları:* Hareketlilik, taşınabilirlik, yeniden kullanılabilirlik, kolay kullanım, ölçeklenebilirlik ve düşük maliyet.
- *Dezavantajları:* Kısıtlı kaynaklar, yönetim ve izlenebilirlik zorluğu, yüksek hata olasılığı, düşük servis ve kalitesi desteği.

Geleneksel ağlarda kullanılan birçok protokol/yöntem algılayıcı düğümlerin sınırlı kaynaklarından dolayı KAA'larda doğrudan uygulanamamaktadır. Bunların başında da güvenlik protokolleri yer almaktadır. IPSec, SSL/TLS ve SSH gibi güvenlik protokolleri internet güvenliğini sağlamak için yeterli iken KAA'lara aşırı işlem yükü getirdiğinden kullanılması uygun değildir.

KAA'larda güvenlik, üç temel kategoride değerlendirilir;

- Algılayıcı ağ güvenliğindeki engeller,
- Güvenli KAA gereksinimleri,
- Saldırılar ve savunma önlemleri [2].

Bir güvenlik yaklaşımı geliştirirken, kablosuz algılayıcı düğüm kaynaklarının (veri belleği, mikroişlemci, güç kaynağı vb.) kapasitelerini göz önüne almak gerekmektedir. KAA veri güvenilirliği için güvenli olmayan haberleşme de bir başka tehdit unsurudur. Algılayıcı düğümler, uzun zaman gözetimsiz bırakıldığından fiziksel saldırılara da maruz kalabilmektedir. Ayrıca uzaktan yönetildikleri için enerji durumları bilinemeyebilir ve ağ içerisinde diğer düğümlerle bağlantısının devam edip etmediğinin kontrolü mümkün olmayabilir [3].

Geleneksel bilgisayar ağlarıyla bazı ortak özelliklere sahip olsalar da KAA'ların kendilerine özgü veri gizliliği, veri bütünlüğü, veri tazeliği, kullanılabilirlik, kendini örgütleme (self–organization), senkronizasyon, güvenli yer belirleme ve kimlik doğrulama gibi çeşitli gereksinimleri bulunmaktadır [3, 4].

KAA'ların güvenliğini tehdit eden hizmet engelleme (denial of service, DoS), Sybil, trafik analiz, düğüm kopyalama (node replication), gizliliğin ortadan kaldırılması (attacks against privacy) ve fiziksel olmak üzere birçok saldırı tipi ve bunlara karşı geliştirilen çeşitli savunma yöntemleri bulunmaktadır [3, 4, 5, 6, 7, 8].

Veri gizliliğini sağlamak için literatürde birçok şifreleme algoritması sunulmaktadır. Bu algoritmalardan KAA'larda kullanımı uygun olan ve yüksek güvenilirlik sağlayan Skipjack algoritması bir sonraki bölümde ayrıntılı olarak incelenmektedir.

3. Skipjack Şifreleme Algoritması

Sunulan çalışmanın temelini oluşturan Skipjack şifreleme algoritması ve güvenilirlik düzeyi hakkında bilgiler bu bölümde verilmektedir.

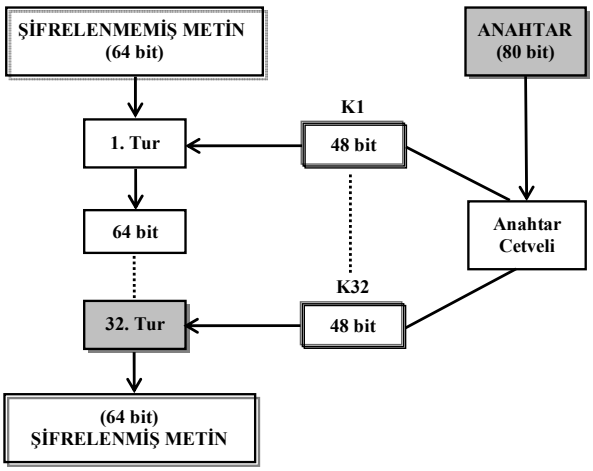
1987 yılında geliştirilen Skipjack şifreleme algoritması, 1993'te kullanılmaya başlanmış bir simetrik anahtar blok şifreleme yöntemidir. Şekil 1'de görülen algoritmanın akış şemasından da anlaşılacağı üzere, 64 bitlik şifrelenmemiş veri blokları 80 bitlik anahtar kullanarak 32 döngü sonunda şifrelenerek, şifrelenmiş veri blokları elde edilmektedir. Döngü sayısı arttıkça algoritmanın güvenliği de üssel olarak artmaktadır. Skipjack, gizli olarak tutulması gereken (hassas) her türlü veriyi şifrelemek için kullanılan, yüksek güvenilirlikli bir algoritmadır.

Kural A ve Kural B olarak adlandırılan iki yöntemin arka arkaya yinelenerek (8 defa Kural A, 8 defa Kural B ve arkasından tekrar 8 defa Kural A, 8 defa Kural B) çalışmasıyla 32 döngü sonunda şifrelenmiş metin elde edilir [9].

Şifreleme algoritmalarının başarımı şu ana kriterlere göre belirlenir:

- Kırılma süresinin uzunluğu,
- Şifreleme/çözme işlemlerinde harcanan zaman (zaman karmaşıklığı),
- Şifreleme/çözme işlemlerinde ihtiyaç duyulan bellek miktarı (bellek karmaşıklığı),
- Bu algoritmaya dayalı şifreleme uygulamalarının esnekliği,
- Bu uygulamaların dağıtımındaki kolaylık ya da algoritmaların standart hale getirilebilmesi ve
- Algoritmanın kurulacak sisteme uygunluğu [10].

Bu kriterler ve kablosuz algılayıcı düğüm özellikleri göz önüne alınarak Skipjack algoritması incelendiğinde, algoritmanın hem güvenilir hem de KAA'larda kullanım için uygun olduğu değerlendirilmektedir [11, 12].



Şekil 1: Skipjack şifreleme algoritması.

4. Gecikme Duyarlı ve Enerji Etkin Merkezileştirilmiş OEK (EGMOEK) Protokolü

Bu bölümde, KAA'lar için geliştirilen ve literatürde sunulan EGMOEK protokolü kısaca açıklanmaktadır. EGMOEK protokolü, öncelikli olarak uygulandığı KAA'nın yaşam süresini uzatmayı hedeflemektedir. Enerji tüketimini düşürmekle birlikte özellikle zaman kritik uygulama trafikleri için daha iyi bir paket iletim gecikmesi sağlamaktadır.

Bildiride sunulan çalışma da, EGMOEK protokolünü Skipjack şifreleme algoritmasıyla kullanarak güvenli, enerji etkin ve gecikme duyarlı bir KAA uygulaması amaçlanmaktadır.

TDMA çerçeve yapısıyla geliştirilen EGMOEK protokolü, Merkezi Düğüm (MD) ve Algılayıcı Düğüm (AD)'ler olmak üzere birbirini tamamlayan iki ana süreç modelinden oluşmaktadır. Bütün AD'ler iletim, boş ve uyku olmak üzere üç işlem moduna sahiptir. Uyku modu, sadece gecikme duyarlılığı olmayan AD'ler tarafından daha az enerji tüketimi sağlamak için kullanılır. Zaman hassasiyeti olmayan AD'lerin tümü periyodik olarak uyku moduna girer. Bir AD, daha çok bantgenişliğine ihtiyaç duyduğunda, MD'ye ekstra zaman dilimi isteğini gönderir. Şayet, Slot Tablosu (ST)'nda, boş zaman dilimi varsa, MD, istekte bulunan AD'ye bu boş zaman dilimini tahsis eder. Sonuç olarak, özellikle gecikme duyarlı veri trafikleri için daha iyi gecikme sonuçları elde edilebilir. EGMOEK protokolünün temel özellikleri aşağıda yer almaktadır:

- Merkezileşmiş mimarisi ve TDMA zamanlama tekniğinden dolayı, enerjinin gereksiz harcanmasına yol açan (örneğin, çarpışma, kulak misafiri olma, kontrol paketi ek yükü gibi) birçok özelliği denetlemeye gerek duymaz.
- Zaman hassasiyeti olmayan AD'ler, enerji tüketimlerini de azaltmak (KAA yaşam süresini arttırmak) için periyodik olarak uyku durumuna girerler.
- Senkronizasyon işlemi basittir.
- AD'ler kendini örgütlemeyi, bağlantı ve ekstra zaman dilimi isteğini kullanarak kolaylıkla başarabilmektedir.
- MD'de kullanılan zamanlama algoritması bantgenişliğinin ve enerji kaynaklarının etkin kullanılmasına olanak tanır. Böylece, gecikme duyarlı veri trafikleri için tahsis edilen ekstra zaman dilimleri gecikme başarımının da iyileşmesini sağlar [13].

5. Skipjack Şifreleme Algoritmasıyla EGMOEK Protokolünün Modellenmesi

Bu bölümde, Skipjack şifreleme algoritmasının EGMOEK protokolü kullanılarak modellenmesi sunulmaktadır. Bu model, kablosuz algılayıcı düğüm ve merkezi düğüm olmak üzere iki süreçten oluşmaktadır.

5.1. Kablosuz Algılayıcı Düğüm Modeli

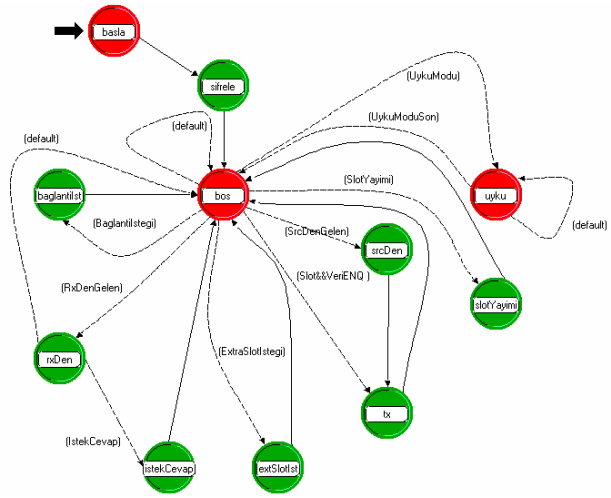
Şekil 2'de görülen kablosuz algılayıcı düğüm EGMOEK modeli, aşağıdaki temel fonksiyonları içermektedir:

- Bağlantı kurma,
- Gecikme duyarlı trafikler için ekstra zaman dilimi isteği,
- Önceden tahsis edilen zaman dilimlerini kullanma,
- Önceden tahsis edilen zaman dilimlerinden tahsis bilgisini kaldırma,
- Kendi zaman dilimlerinde verilerini gönderme ve
- Zaman hassasiyeti olmayan algılayıcı düğümler için enerji tüketimini azaltan uyku (radyo alıcı/vericilerini kapatma) işlemi.

Sunulan çalışmada EGMOEK protokolüne, ortamdan algıladığı veriyi Skipjack algoritmasıyla şifreleyerek MD'ye gönderilmesini sağlayan yeni bir fonksiyon daha eklenmiştir. Böylece EGMOEK modelinin, dış ortamdan gelecek olan veri gizliliği saldırılarına/ataklara karşı güvenli olması amaçlanmaktadır. Bu ek işlem, sistemdeki hesaplama karmaşıklığını arttırmakla birlikte sistemin güvenliğini de arttırmaktadır.

Kablosuz algılayıcı düğüm süreç modelindeki her bir durum makinesi aşağıdaki şekilde çalışmaktadır:

- "*basla*" durum makinesi, benzetimdeki diğer süreçler başlatılana kadar bir gecikme gerçekleştirir ve kontrol değişkenleri yüklenir.
- "*boş*" durum makinesi, bir kesme isteği gelinceye kadar beklenir.
- "*baglantıIst*" durum makinesi, bağlantı kurma bilgisini içeren bağlantı istek paketini oluşturur ve merkezi düğüme bu paketi gönderir.
- "*istekCevap*" durum makinesi, merkezi düğüm tarafından tahsis edilen zaman dilimlerinin (slot) sayısını belirler.
- "*srcDen*" durum makinesi, üst katmandan gelen algılanmış veriyi alır, paketlere böler ve paketleri kuyruğa ekler.
- "*sifrele*" durum makinesi, "*srcDen*" durum makinesinde bölünmüş olan paketler içerisindeki veriyi Skipjack algoritmasına göre şifreler.
- "*tx*" durum makinesi, üst katmandan alınan veri paketleri algılayıcı düğüm için tahsis edilen zaman dilimlerinde hedefine gönderilir.
- "*uyku*" durum makinesi, zaman hassasiyeti olmayan trafikler, sahip oldukları enerjiyi korumak için özel bir zaman aralığında alıcı/vericilerini kapatırlar.
- "*extSlotIst*" durum makinesi, gecikmeye duyarlı trafiklerde ekstra bantgenişliği ihtiyacını bildirmek için ekstra zaman dilimi istek paketi oluşturur.
- "*slotYayimi*" durum makinesinde, ekstra zaman dilimi dağılım paketi oluşturulur ve merkezi düğüme gönderilir.
- "*rxDen*" durum makinesi, algılayıcı düğüme gelen tüm paketleri işler [13].



Şekil 2: Kablosuz algılayıcı düğüm süreç modeli.

5.2. Merkezi Düğüm Modeli

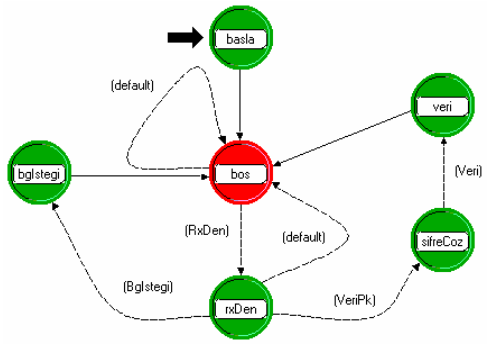
Merkezi düğüm, aynı küme (cluster) içerisinde bulunan algılayıcı düğümlerin çevreden algıladığı tüm verileri toplamakta ve algılayıcı düğümlerin kablosuz ortama erişimini düzenlemektedir. Şekil 3'te görülen EGMOEK protokolünde

amaçlanan merkezi düğüm fonksiyonları üç temel süreç içermektedir:

- Herhangi bir algılayıcı düğüm için zaman dilimi tahsisi,
- Merkezi düğüme gelen veri paketlerini üst katmana gönderme ve
- Zaman dilimi tablosunu (ST) kullanarak gecikmeye duyarlı veri trafikleri için ekstra zaman dilimleri tahsis etme/dağıtmadır.

Sunulan çalışmada, orijinal EGMOEK modelinden farklı olarak, MD (Merkezi Düğüm) tarafından alınan şifreli verilerin şifre çözme işlemlerini gerçekleştirmek amacıyla bir fonksiyon daha bulunmaktadır. Bu süreçteki her bir durum makinesi aşağıdaki şekilde çalışmaktadır:

- "*basla*" durum makinesinde, süreç başlar ve kontrol değişkenlerine ilk değer ataması yapılır.
- "*bos*" durum makinesi, bir kesme gelene kadar burada bekler.
- "*rxDen*" durum makinesi, gelen veri paketinin formatına uygun olan bir sonraki durum makinesine paketi gönderir.
- "*sifreCoz*" durum makinesinde, veri paketinin içindeki şifreli verinin Skipjack algoritmasıyla şifresi çözülür.
- "*bgIstegi*" durum makinesi, bağlantı isteklerini işler ve ekstra slot isteklerini kabul eder ya da tahsisi kaldırır. Ayrıca, slot tablosunu yöneten "adaletli dağılım algoritması"nı da çalıştırır.
- "*veri*" durum makinesinde, "algılanmış bilgi", özel bir görevi yerine getirmek için üst katmana gönderilir [13].



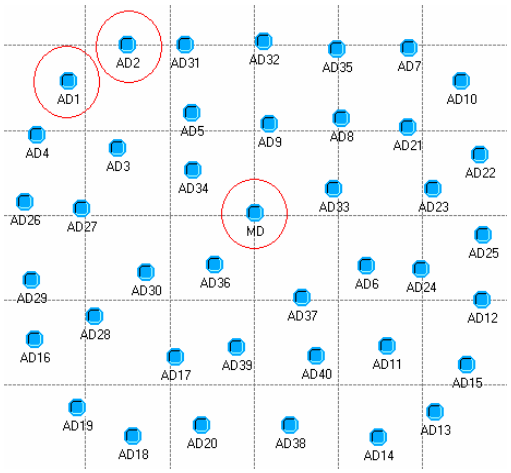
Şekil 3: Merkezi düğüm süreç modeli.

6. Ağ Modeli ve Benzetimi

Bu bölümde, Skipjack algoritmasını içeren bir KAA uygulama modelinin ve benzetiminin OPNET geliştirme ve benzetim yazılımı yardımıyla gerçekleştirilmesi sunularak, Skipjack şifreleme algoritmasının EGMOEK protokolündeki uçtan uca gecikme ve enerji tüketimi sonuçlarına etkisi incelenmektedir.

Şekil 4'te sunulan ağ modelinde, 40 adet KAA düğümü ve bir adet diğer algılayıcı düğümlere göre kaynakları daha iyi olan MD bulunmaktadır. Uygulamada, algılayıcı düğümler, ortamdan algıladıkları bilgileri (algı), Skipjack algoritmasıyla şifreleyerek MD'ye göndermektedir.

Ortama rastgele dağıtılan 40 adet algılayıcı düğümden bazıları gecikme duyarlı diğerleri de zaman hassasiyeti olmayan düğümlerdir. Zaman hassasiyeti olmayan algılayıcı düğümler, 50 saniye aktif durumda, 50 saniye uyku durumunda bulunurlar. Tablo 1'de, gerçekleştirilen uygulama modellerinde kullanılan benzetim parametreleri verilmektedir.



Şekil 4: Güvenli KAA uygulama benzetim modeli.

Tablo 1: Benzetim parametreleri.

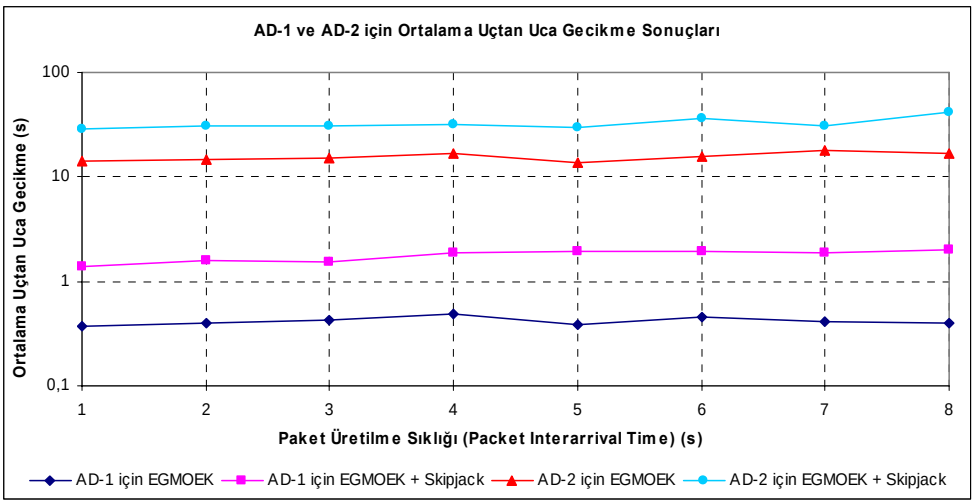
AD Trafik Kaynakları	1000* Bayt
Alış/Veriş Bit Hızı	1 Mbit/s
Verici Gücü (MD ve AD'ler)	10 mW
KAA Düğüm Sayısı	40
Alan Büyüklüğü	100 m x 100 m
*Üstel dağılım fonksiyonu kullanılarak üretilmiştir.	

6.1. Benzetim Sonuçları ve Değerlendirme

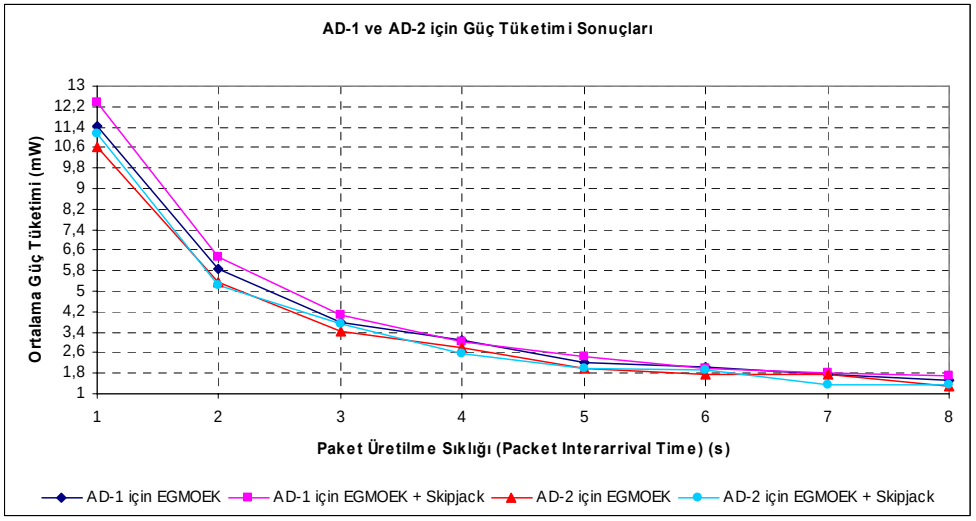
Bu bölümde, değişen ağ yükleri altında KAA uygulama modeli benzetim sonuçları sunulmaktadır. Örnek senaryoda, güvenlik hizmeti olmadan EGMOEK protokolü ile Skipjack şifreleme algoritmasının kullanılmasıyla geliştirilen EGMOEK protokolünün karşılaştırılmalı sonuçları incelenmektedir. Bütün AD uygulama mesajlarının değişen paket üretilme sıklığında (packet interarrival time), AD–1 & MD arasındaki gecikme duyarlı ve AD–2 & MD arasındaki zaman hassasiyeti olmayan veri trafikleri için ortalama uçtan uca gecikme ve güç tüketim sonuçları karşılaştırmalı olarak verilmektedir.

AD–1 ve AD–2 için paket üretilme sıklığının bir fonksiyonu olarak ortalama uçtan uca gecikme sonuçları Şekil 5'te görülmektedir. Güvenlik hizmeti olmayan uygulamadaki gecikme sonuçları, şifreleme algoritmasının eklenmesiyle elde edilen gecikme sonuçlarına göre AD–1 için yaklaşık dört kat, AD–2 için ise yaklaşık olarak iki kat daha fazladır.

Şekil 6'da AD–1 ve AD–2 için paket üretilme sıklığının bir fonksiyonu olarak güç tüketim sonuçları görülmektedir. Uyku durumuna girmediklerinden, gecikme duyarlı AD–1 trafiklerinin zaman hassasiyeti olmayan AD–2 trafiklerine göre her iki durumda da biraz daha fazla enerji tükettikleri görülmektedir. Diğer bir ifadeyle, şifreleme algoritmasının eklenmesiyle güç tüketim sonuçları hem AD–1 hem de AD–2 için güvenlik hizmeti olmayan sonuçlara göre daha yüksek çıkmıştır.



Şekil 5: Güvenlik hizmetsiz EGMOEK ve Skipjack şifrelemeli EGMOEK protokolleri için ortalama uçtan uca gecikme sonuçları.



Şekil 6: Güvenlik hizmetsiz EGMOEK ve Skipjack şifrelemeli EGMOEK protokolleri için güç tüketim sonuçları.

7. Sonuçlar

Sunulan çalışma, özellikle yüksek güvenilirlik düzeyi gerektiren ve gecikmeye karşı duyarlı KAA uygulamaları için örnek bir model içermektedir.

KAA uygulamalarında, güvenliği arttırmak için eklenen şifreleme mekanizmalarının düğüm enerji tüketim miktarlarını ve ortalama uçtan uca gecikme sürelerini arttırması beklenen bir sonuçtur. Burada uygulamaların ihtiyaçlarının iyi tespit edilmesi oldukça önemlidir. Zira, basit bir geniş ölçekli çevre ya da endüstriyel KAA uygulamasında güvenlik çok fazla önem taşımazken enerji tüketiminin büyük önemi bulunmaktadır. Diğer yandan, askeri ve sağlık uygulamalarında ise güvenlik büyük önem taşırken algılayıcı düğüm enerji tüketimi nispeten göz ardı edilebilir bir parametre olarak değerlendirilmektedir.

8. Kaynaklar

[1] Akyildiz I. F., Su W., Sankarasubramaniam Y., Cayirci E., "Wireless Sensor Networks: Survey", Computer Networks, Vol. 38, pp. 393–422, 2002.

[2] Perrig A., Stankovic J., Wagner D., "Security in Wireless Sensor Networks", Communication of the ACM, Vol. 47, pp. 53–57, 2004.

[3] Xiao Y., "Security in Distributed, Grid, Mobile, and Pervasive Computing", CRC Press, 2006.

[4] Perrig A., Szewczyk R., Wen V., Culler D., Tygar J.D., "SPINS: Security Protocols for Sensor Networks", Wireless Networks Journal, 2002.

[5] Wood A.D., Stankovic J.A., "Denial of Service in Sensor Networks", IEEE Computer Magazines, pp. 54–62 , 2002.

[6] Çakıroğlu M., Özcerit A. T., Çetin Ö., Ekiz H., "MAC Layer DoS Attacks in Wireless Sensor Networks: A Survey", International Conference on Wireless Networks, ICWN'06, 2006.

[7] Newsome J., Shi E., Song D., Perrig A., "The Sybil Attack in Sensor Networks: Analysis & Defenses", Proceedings of the IEEE Third International Symposium on Information Processing in Sensor Networks (IPSN), pp. 259–268, 2004.
[8] Karaboğa D., Ökdem S., "Kablosuz Algılayıcı Ağlarında Güvenli İletişim Teknikleri", Ulusal Elektronik İmza Sempozyumu, Gazi Üniversitesi, 2006.
[9] Musthyala K., Manchikanti S., "Skipjack Algorithm", Project Work.
[10] Tektaş M., Baba F., Çalışkan E.M., "Şifreleme Algoritmalarının Sınıflandırılması ve Bir Kredi Kartı Uygulaması", Third International Advanced Technologies Symposium, Ankara, 2003.
[11] Bandırmalı N., Ertürk İ., Çeken C., Bayılmış C., "Yüksek Riskli Kablosuz Algılayıcı Ağlarda Güvenlik ve Şifreleme Uygulaması", 2. Ağ ve Bilgi Güvenliği Ulusal Sempozyumu, KKTC, 2008.
[12] Karlof C., Sastry N., Wagner D., "TinySec: A Link Layer Security Architecture Wireless Sensor Networks", SENSYS'04, USA, 2004.
[13] Ceken C., "An Energy Efficient and Delay Sensitive Centralized MAC protocols for Wireless Sensor Networks", Computer Standard and Interfaces, 2008.
[14] http://www.opnet.com.