YÜKSEK RİSKLİ KABLOSUZ ALGILAYICI AĞLARDA GÜVENLİK VE ŞİFRELEME UYGULAMASI

Necla BANDIRMALI İsmail ERTÜRK Celal ÇEKEN Cüneyt BAYILMIŞ

Kocaeli Üniversitesi
Teknik Eğitim Fakültesi
Elektronik ve Bilgisayar Eğitimi Bölümü
41380 Kocaeli
e-posta: {bandirmali, erturk, cceken, bayilmis}@kou.edu.tr

ABSTRACT

Providing a secure and reliable communication in wireless sensor networks especially for military and health applications is of much importance. Offering cost-effective solutions to this requirement has lead to many research works on new security protocols as well as cryptology. This paper explains both the fundamental DES algorithm as it is the reference work for current cryptography techniques and the Skipjack algorithm employed in most of the wireless sensor networks. It also shows the basic simulation models for both algorithms realized using OPNET Modeler, followed by preliminary comparative simulation results.

Keywords: Wireless Sensor Networks, Security, Cryptography Techniques

1. GİRİŞ

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 olduğundan klasik güvenlik tekniklerinin doğrudan uygulanması açısından önemli dezavantajlarla karşı karşıyadır. KAA'ların sınırlı enerji ve hesaplama yetenekleri göz önüne alınarak geliştirilen çeşitli güvenlik protokolleri ve şifreleme algoritmaları bu çalışmada değerlendirilmektedir.

Bu bildirinin 2. bölümünde KAA'lar hakkında kısa bilgi verilmektedir. 3. bölümde KAA'larda güvenlik ve güvenlik protokolleri açıklanmaktadır. 4. bölümde ise KAA uygulamaları için önerilen şifreleme yöntemlerinden DES ve Skipjack algoritmaları açıklanmaktadır. Son bölümde ise bu algoritmaları içeren KAA örneklerinin OPNET geliştirme ve benzetim yazılımı yardımıyla gerçekleştirilmesi sunularak, KAA düğümlerinin uçtan uca gecikme sonuçlarına etkileri karşılaştırmalı olarak incelenmektedir.

2. KABLOSUZ ALGILAYICI AĞLAR

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 uygun olmaları nedenleriyle gün geçtikçe popülerliği artmaktadır. KAA'ların kullanım alanlarına örnek olarak, askeri uygulamalar, çevresel uygulamalar, endüstriyel uygulamalar, tıbbi uygulamalar, bina otomasyonu ve ticari uygulamalar verilebilir. KAA'ların sundukları avantaj ve dezavantajlar aşağıda kısaca özetlenmektedir.

Avantajları:

- Hareketlilik: Kablosuz haberleşen düğümler kapsama alanı içerisinde herhangi bir kısıtlama olmaksızın hareket edebilmektedirler. Bu özellik, KAA'ya dinamik bir ağ topolojisi sağlar.
- Taşınabilirlik: Herhangi bir kablolama ve enerji altyapısı gerektirmediğinden mevcut ağ, kurulu olduğu alandan başka bir yere kolaylıkla taşınabilir.
- Yeniden kullanılabilirlik: Fiziksel ortamdan çeşitli verileri algılamayı amaçlayan KAA düğümleri, defalarca ve farklı uygulamalarda yeniden kullanılabilir.
- Kolay kullanım: Algılayıcı düğümler, herhangi bir ayar gerektirmeden kendi aralarında dinamik bir biçimde organize olarak, değişen koşullara kolayca ayak uydurabilirler.
- Ölçeklenebilirlik: Mevcut bir KAA'ya yeni algılayıcı düğümlerin ya da başka bir KAA'nın dahil edilmesi kolaylıkla ve dinamik bir şekilde gerçekleştirilebilmektedir.
- Düşük maliyet: Kablosuz iletişim ve mikro-elektromekanik sistem teknolojisindeki

gelişmelere paralel olarak KAA düğümlerinin maliyetleri sürekli düşmektedir.

Dezavantajları:
- Kısıtlı kaynaklar: KAA düğümlerinin hesaplama kabiliyetleri (hızları), bellek kapasiteleri ve güçleri sınırlıdır.
- Yönetim ve izlenebilirlik zorluğu: KAA düğümleri, algılama ve basit hesaplama gibi temel gereksinimler öngörülerek tasarlandıklarından, uzaktan yönetim ve trafik mühendisliği için gerekli algoritmalar, KAA'lar için yüksek oranda kaynak kullanımına sebep olmaktadır.
- Yüksek hata olasılığı: Algılama ortamının coğrafik ve fiziksel özelliklerinden kaynaklanan olumsuz etkiler ile kablosuz iletişim karakteristiklerine bağlı olarak, bit hata oranı kablolu sistemlere kıyasla çok yüksek olmaktadır.
- Servis kalitesi: Yüksek bit hata oranı ve dinamik topolojiden dolayı sınırlı bir servis kalitesi desteği sunmaktadır.

3. KAA'LARDA GÜVENLİK VE GÜVENLİK PROTOKOLLERİ

Geleneksel ağlarda kullanılan güvenlik teknikleri, aşağıda belirtilen nedenlerden dolayı KAA'larda doğrudan uygulanamamaktadır. Bunlar KAA düğümlerinin;
- Kısıtlı enerji kaynaklarına, yetersiz veri saklama kapasitesine ve sınırlı işlem kabiliyetlerine sahip olmaları,
- Kolay erişilebilir alanlara yerleştirildiklerinden fiziksel saldırılara açık olmaları, ve
- İnsanlarla ve ölçüm yapılacak fiziksel ortam ile doğrudan etkileşimde bulunmalarıdır [2].

KAA'larda güvenlik, üç temel kategoride değerlendirilir;
- Algılayıcı ağ güvenliğindeki engeller,
- Güvenli KAA gereksinimleri,
- Saldırılar ve savunma önlemleri.

3.1. KAA Güvenliğindeki Engeller

KAA'ların, geleneksel ağlarla karşılaştırıldığında birçok kısıtlaması bulunmaktadır. Bunlar için güvenlik mekanizmaları geliştirirken, kısıtlamaların neler olduğunu değerlendirerek güncel güvenlik tekniklerinden faydalanmak gerekmektedir.

Bir güvenlik yaklaşımı geliştirirken, kablosuz algılayıcı düğüm kaynaklarının (veri belleği, mikroişlemci, güç kaynağı) kapasitelerini göz önüne almak gerekmektedir. Ayrıca bu kaynaklar, küçük/sınırlı bir algılayıcı düğümde yer almaktadır.

Güvenli olmayan haberleşme, KAA veri güvenirliği için başka bir tehdit unsurudur. KAA güvenliği, haberleşmede kullanılan tanımlanmış protokoller yardımıyla temin edilmektedir.

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. Tüm bu dezavantajlarına rağmen, merkezi bir yönetim noktasının bulunmaması ise KAA yaşam süresini arttırmaktadır [3].

3.2. Güvenli KAA Gereksinimleri

Geleneksel bilgisayar ağlarıyla bazı ortak özelliklere sahip olsalar da KAA'lara özgü çeşitli gereksinimler bulunmaktadır. Bunlar;
- Veri gizliliği,
- Veri bütünlüğü,
- Veri tazeliği,
- Kullanılabilirlik,
- Kendini örgütleme (self–organization),
- Senkronizasyon,
- Güvenli yer belirleme, ve
- Kimlik doğrulama şeklinde sıralanabilir [3, 4].

3.3. Saldırılar ve Savunma Önlemleri

KAA düğümleri, birçok uygulamada uzaktan izlenilen bir ortama rasgele yerleştirilmektedir. Bu nedenle ortamda korunmasız olarak bulunan düğümler, çeşitli saldırılarla kolaylıkla ele geçirilebilir ve fiziksel hasara maruz bırakılabilir. Ayrıca yeniden programlanarak saldırı üreten zararlı düğümler haline çevrilebilme riskini barındırırlar. Bu dezavantajlar sebebiyle, algılayıcı ağlar diğer ağlara nazaran oldukça az güvenilirdir.

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 bir çok saldırı tipi bulunmaktadır [3, 4, 5, 6, 7, 8].

3.4. KAA Güvenlik Protokolleri

Algılayıcı ağ güvenlik protokolleri iki ana grupta incelenebilir:
- **Haberleşme protokolleri**: Mesaj gizliliğini, bütünlüğünü ve kimlik denetimi sağlamak için kullanılan şifreleme algoritmalarıyla ilgilidir. Algılayıcı ağlar için geliştirilen üç temel güvenli haberleşme protokolü mevcuttur. Bunlar; SPINS, TinySEC ve LLSP'dir .Bu

algoritmalar simetrik şifreleme yöntemiyle, mesaj gizliliği, bütünlüğü ve kimlik denetimi sağlamak için geliştirilmişlerdir.

- **Anahtar yönetim mimarileri**: Haberleşme protokolleri tarafından kullanılan "anahtar"ların oluşturulmasını ve dağılımını yöneten mimarilerdir. LEAP, LKHW (Logical Key Hierarchy), Random Key Predistribution ve TinyPK bunlara örnek olarak verilebilir [9].

4. ŞİFRELEME YÖNTEMLERİ

Bu bölümde KAA uygulamaları için önerilen şifreleme yöntemlerinden klasik DES ve yaygın olarak tercih edilen Skipjack algoritmaları açıklanmaktadır.

Şifreleme algoritmaları, kullandıkları anahtar biçimine göre simetrik ve asimetrik olmak üzere iki gruba ayrılmaktadır.

Simetrik anahtar şifreleme algoritmalarında, verinin şifrelenmesinde kullanılan anahtar (private key) ile şifrelenmiş verinin şifresinin çözülmesinde kullanılan anahtar aynıdır [10]. Bunlara örnek olarak DES (Veri Şifreleme Standardı, Data Encryption Standard), 3DES, AES (İleri Şifreleme Standardı, Advanced Encryption Standard), Skipjack, RC4 ve SEA verilebilir. Simetrik anahtar şifreleme algoritmaları blok ve akış şifreleme olmak üzere ikiye ayrılmaktadır. Blok şifreleme, şifresiz (orijinal) metni veya şifreli metni bloklara bölerek şifreleme/şifre çözme işlemini yaparken, dizi şifreleme ise bir bit veya bayt üzerinde şifreleme/şifre çözme işlemlerini yapmaktadır.

Asimetrik anahtar şifreleme algoritmalarında, verinin şifrelenmesi için açık anahtar (public key), şifre çözme için ise matematiksel/mantıksal olarak açık anahtara bağlı özel bir anahtar (private key) kullanılmaktadır. Bu algoritmalara örnek olarak ise RSA (Ron **R**ivest, Adi **S**hamir, and Leonard **A**dleman) ve ECC (Elliptical Curve Cryptography) verilebilir [11].

Simetrik anahtar şifreleme algoritmaları oldukça hızlıdır, donanımla gerçekleştirilmeleri kolaydır. Bunlar "gizlilik" güvenlik hizmetini yerine getirirler, fakat; ölçeklenebilir değildirler. Güvenli anahtar dağıtımı ve bütünlük, kimlik denetimi gibi güvenlik hizmetlerini gerçekleştirmek oldukça zordur. Asimetrik anahtar şifreleme algoritmalarında ise anahtar yönetimi ölçeklenebilir, kırılması zor ve bütünlük, kimlik denetimi gibi güvenlik hizmetleri kolaylıkla sağlanabilir olmakla birlikte simetrik anahtar şifreleme algoritmalarıyla karşılaştırıldıklarında yaklaşık 1500 kat kadar yavaştır. Ayrıca anahtar uzunlukları bazı uygulamalar için kullanışlı değildir.

Şifreleme algoritmalarının başarımı 6 ana kritere göre belirlenir:

a) Kırılabilme süresinin uzunluğu,
b) Şifreleme ve çözme işlemlerine harcanan zaman (zaman karmaşıklığı),
c) Şifreleme ve çözme işleminde ihtiyaç duyulan bellek miktarı (bellek karmaşıklığı),
d) Bu algoritmaya dayalı şifreleme uygulamalarının esnekliği,
e) Bu uygulamaların dağıtımındaki kolaylık ya da algoritmaların standart hale getirilebilmesi, ve
f) Algoritmanın kurulacak sisteme uygunluğu.

Teorik olarak, simetrik anahtar kullanan şifreleme algoritmaları, olası bütün anahtarları sırasıyla denemek yoluyla kırılabilir. Olası anahtarların denenmesi işlemi de, anahtarın uzunluğu arttıkça güçleşecektir. Buna örnek oalrak Tablo 1'de belirli anahtar uzunluklarına göre şifreyi deneyerek bulma zamanları verilmiştir.

Tablo 1. Anahtar uzunluklarına göre şifre çözme zamanları.

Anahtar Uzunluğu	Sayı Değeri	10^6 şifre/s	10^9 şifre/s	10^{12} şifre/s
32 bit	$4x10^9$	36 dak	2.16 s	2.16 ms
40 bit	10^{12}	6 gün	9 dak	1 s
56 bit	$7.2x10^{16}$	1142 yıl	1 yıl 2 ay	10 saat
64 bit	$1.8x10^{19}$	292000 yıl	292 yıl	3.5 ay
128 bit	$1.7x10^{38}$	$5.4x10^{24}$ yıl	$5.4x10^{21}$ yıl	$5.4x10^{18}$ yıl

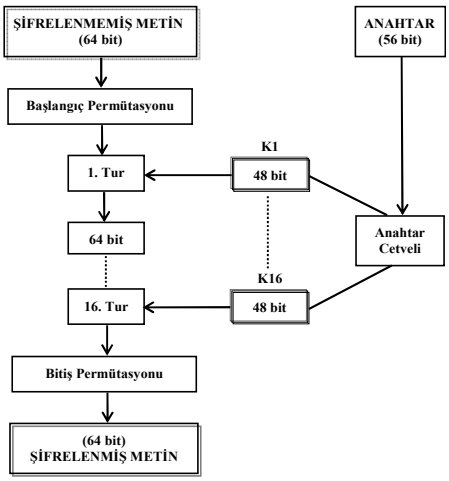
Alt bölümlerde, literatürde ilk sunulan ve bir çok çalışmada referans olarak kullanılan DES simetrik şifreleme algoritmasının ve KAA'larda güvenliği sağlamak için geliştirilen Skipjack algoritmasının, OPNET simülasyon yazılımı kullanılarak geliştirilen modelleri sunulmaktadır. Ayrıca elde edilen sonuçlar, kısaca karşılaştırmalı olarak değerlendirilmektedir.

4.1 DES Şifreleme Algoritması

DES, simetrik anahtar blok şifreleme algoritmasıdır (Şekil 1). Bu algoritma, 64 bitlik veri bloklarını, 64 bitlik bir anahtarın 8. ve katları (8, 16, 24, 32, 40, 48, 56 ve 64) bitlerini gözardı ederek, 56 bitlik anahtar yardımıyla şifrelemektedir.

DES algoritması, bu alanda ilk geliştirilen şifreleme yöntemidir. KAA'larda kullanılması uygun olarak görülmekle birlikte aşırı kod uzunluğu, enerji tüketimini ve bellek kullanımını, uygulamalar tarafından kabul edilemez miktarlarda arttırmaktadır. 16 döngü sonunda şifrelenmiş metnin elde edilmesi, algoritmayı güçlü yapmakla birlikte

anahtar uzunluğunun küçük olmasından dolayı güvenliğini azaltmaktadır.



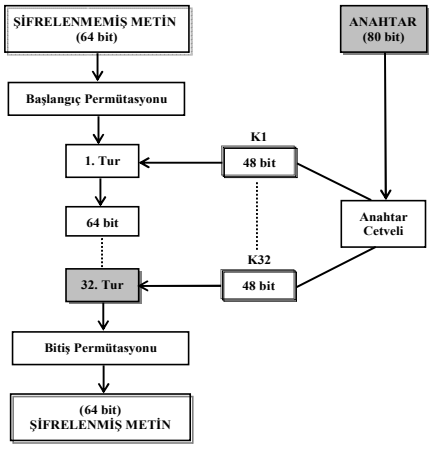
Şekil 1. DES Algoritması.

4.2. Skipjack Şifreleme Algoritması

Skipjack algoritması da DES algoritması gibi simetrik anahtar blok şifreleme yöntemini kullanmaktadır (Şekil 2). 64 bit uzunluğundaki veri, 80 bit anahtar kullanılarak ve 32 döngü sonunda şifrelemektedir.

DES ile karşılaştırıldığında Skipjack, daha basit ve az işlem gerektiren bir algoritmaya ve daha uzun anahtar büyüklüğüne sahiptir. Ayrıca şifrelenmiş metnin 32 döngü sonunda elde edilmesi oldukça önemli bir avantaj sunmaktadır.

Anahtar uzunluğunun ve döngü sayısının fazla olması Skipjack algoritmasını DES algoritmasından daha güvenli kılmaktadır. Buna ek olarak, az işlem gerektiren aritmetik/lojik yapısı sayesinde ise KAA'larda kullanım için oldukça önemli bir tercih sebebidir.

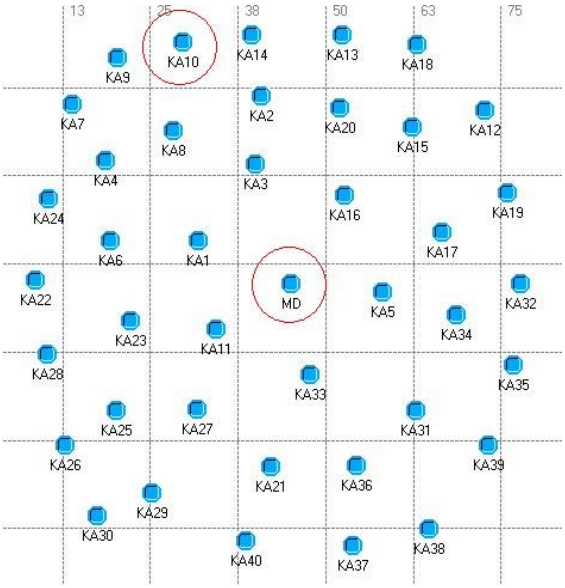


Şekil 2. Skipjack Algoritması.

5. MODELLEME VE BENZETİM

Bu bölümde DES ve Skipjack algoritmaları içeren KAA örneklerinin OPNET geliştirme ve benzetim yazılımı yardımıyla gerçekleştirilmesi sunularak, kullanılan algoritmaların, KAA düğümlerinin uçtan uca gecikme sonuçlarına etkileri karşılaştırmalı olarak incelenmektedir.

Şekil 3'de sunulan ağ modelinde, 40 adet KAA düğümü ve bir adet diğer algılayıcı düğümlere göre kaynakları daha iyi olan MD (Merkezi Düğüm) bulunmaktadır. Uygulamada, 40 adet algılayıcı düğüm, ortamdan algıladıkları bilgileri (algı), önceden belirlenen DES ya da Skipjack algoritması ile şifrelemek suretiyle MD'ye göndermektedir. Tablo 2'de, gerçekleştirilen uygulama modellerinde kullanılan benzetim parametreleri verilmektedir.

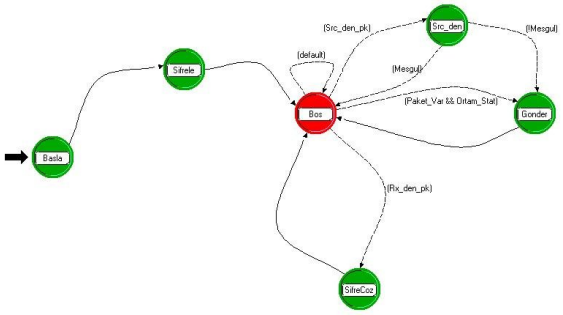


Şekil 3. KAA ağ uygulaması benzetim modeli.

Tablo 2. Benzetim Parametreleri.

Trafik Kaynakları	1000* bayt/s
Alış/Veriş Bit Hızı	1 Mbit/s
Verici Gücü	MD = 10 mW ve KA = 10 mW
KAA Düğüm Sayısı	40
Alan Büyüklüğü	100 m x 100 m
Kanal Modeli	Free Space Propagation Model (LoS)
*Üstel dağılım fonksiyonu kullanılarak üretilmiştir.	

Gerçekleştirilen KAA ağ uygulamasında kullanılan DES ve Skipjack şifreleme algoritmalarının "proses model"i Şekil 4'de sunulmaktadır. "sifrele" ve "sifrecoz" prosesleri yalnız DES ya da Skipjack algoritmalarını gerçekleştirirken, diğer prosesler, her iki uygulama için benzer şekilde çalışmaktadır.



Sekil 4. DES ve Skipjack şifreleme algoritmalarının proses modeli.

Tablo 3'de DES ve Skipjack şifreleme algoritmalarının benzetim örneklerinden elde edilen şifreleme ve şifre çözme zamanları görülmektedir. DES algoritmasının şifreleme zamanı, Skipjack algoritmasının yaklaşık olarak 577 katıdır. Şifre çözme zamanı ise yaklaşık olarak 606 katıdır. Bu sonuçlara göre bir değerlendirilme yapıldığında, yeteri kadar güvenli olmayan DES şifreleme algoritmasının, başarım açısından da Skipjack şifreleme algoritmasına göre çok yavaş olduğu görülmektedir.

Tablo 3. DES ve Skipjack şifreleme algoritmalarının şifreleme ve şifre çözme zamanları.

	Şifreleme Zamanı	**Şifre Çözme Zamanı**
DES	1420 ms	1480 ms
SKIPJACK	2,46 ms	2,44 ms

6. SONUÇ

Bu bildiride sunulan çalışmada, KAA'larda kullanılan güvenlik protokolleri ve şifreleme algoritmaları incelenmiştir. KAA'larda kullanılmak üzere geliştirilmekte olan şifreleme yöntemleri için referans kabul edilen DES şifreleme algoritmasının ve yine KAA'larda yaygın olarak kullanılan Skipjack şifreleme algoritmasının OPNET modelleme ve benzetim yazılımı kullanılarak benzetimi yapılmıştır. Her iki algoritmanın başarım karşılaştırması, şifreleme ve şifre çözme zamanları ölçütüne göre sunulmuştur. KAA'ların sınırlı kaynakları göz önüne alındığında, Skipjack şifreleme algoritmasının DES şifreleme algoritmasına göre KAA'lar için daha uygun olduğu görülmektedir.

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] http://www.auburn.edu/~caseykl/research/security/SecurityinWirelessSensorNetworks.doc.

[10] Yerlikaya T., Şifreleme Teknikleri ve Güncel Uygulama Olanakları, Yüksek Lisans Tezi, Trakya Üniversitesi, F.B.E., 2002.

[11] Cobb C., Cryptography for Dummies, Wiley Publishing, Inc., 2004.

[12] Tektaş M., Baba F., Çalışkan E.M., Şifreleme Algoritmalarının Sınıflandırılması ve Bir Kredi Kartı Uygulaması, 3rd International Advanced Technologies Symposium, Ankara, 2003.

[13] http://www.opnet.com.