SEA Şifreleme Algoritması Kullanarak Güvenli Kablosuz Algılayıcı Ağ Haberleşmesinin Gerçekleştirilmesi

Cüneyt BAYILMIŞ, Murat ÇAKIROĞLU

***Özet*— Kablosuz Algılayıcı Ağ (KAA)'ların sınırlı kaynaklara sahip olması ve herkese açık olan kablosuz iletişim ortamı üzerinden haberleşmesi etkin güvenlik çözümlerinin geliştirilmesini zorlaştırmaktadır. Güvenilir iletişimin en önemli gereksinimi olan şifreleme/şifre çözme prosedürlerinin genellikle çok karmaşık ve işlem yükünün oldukça fazla olması popüler şifreleme algoritmalarının KAA'larda kullanılabilirliğini güçleştirmektedir. Bu sebeple KAA'larda kullanılan şifreleme algoritmalarından mümkün olan en az işlem yükü ile en uygun güvenlik seviyesini sağlaması beklenmektedir. Bu çalışmada, blok tabanlı yeni bir şifreleme algoritması olan Ölçeklenebilir Şifreleme Algoritması (Scalable Encryption Algorithm, SEA) kullanılarak KAA'larda güvenli iletişimin gerçekleştirilmesi amaçlanmaktadır. MICAz düğümleri üzerinde gerçeklemesi yapılan SEA algoritmasının başarımı bellek gereksinimi, çalışma zamanı, güvenlik ve esneklik kriterleri açısından ele alınmakta ve elde edilen sonuçlar Skipjack algoritması ile karşılaştırılmaktadır.**

***Anahtar Kelimeler*—Kablosuz Algılayıcı Ağlar, Güvenlik, SEA**

I. GİRİŞ

Kablosuz Algılayıcı Ağ (KAA)'lar, bakım gerektirmeden uzun yıllar çalışabilmeleri ve çok çeşitli alanlarda kullanılabilmeleri sebebiyle hem endüstriyel uygulamalarda hem de akademik çalışmalarda çok popüler bir alan haline gelmiştir. KAA'ları meydana getiren düğümler, genellikle iki adet standart pil ile beslenen, veri saklama/işlem kapasitesi sınırlı olan ve kısa mesafeli kablosuz ortam üzerinden haberleşen tümdevrelerdir [1]. Kaynakları sınırlı olan bu düğümlerin, çoğu uygulama için dış ortamda bulunması ve kablosuz olarak haberleşmesi KAA'ların çeşitli saldırılara maruz kalma riskini arttırmaktadır. Bu sebeple güvenliğin en önemli tasarım ölçütü olduğu askeri ve tıbbi uygulamalar başta olmak üzere birçok uygulama alanında kablosuz algılayıcı ağların veri gizliliği, bütünlüğü, tazeliği ve kimlik doğrulaması gibi hayati güvenlik gereksinimlerini karşılaması gerekmektedir [2-5].

KAA'ların kısıtlı donanımsal kaynaklara sahip olması, bilgisayar ağlarında kullanılan geleneksel güvenlik çözümlerinin KAA'larda doğrudan kullanılmasını güçleştirmektedir. ECC, RSA, AES, T-DES, RC5 gibi popüler şifreleme algoritmalarının gerektirdiği işlem yükünün oldukça fazla olması, bu algoritmaların saklama ve işlem yapma kabiliyeti sınırlı olan kablosuz algılayıcı düğümleri üzerinde gerçeklenmesini zorlaştırmaktadır. Ayrıca kullanılan şifreleme algoritmasının düğümlerin işlem yükünün ve iletilen paket boyutlarının artmasına yol açması beraberinde enerji tüketimlerinin de önemli ölçüde artmasına ve düğümlerin yaşam sürelerinin azalmasına neden olmaktadır. Bu sebeple KAA'larda kullanılan şifreleme algoritmalarından mümkün olan en az işlem yüküyle istenilen güvenlik gereksinimlerini karşılaması beklenmektedir. Sınırlı komut setine ve işlem yapma kabiliyetine sahip işlemciler için geliştirilmiş, basit şifreleme rutinleri içeren fakat doğrusal/farksal kriptanaliz tekniklerine karşı dayanıklı olan SEA (Scalable Encryption Algorithm-Ölçeklenebilir Şifreleme Algoritması) şifreleme algoritması [6-7], bu özellikleri sebebiyle KAA'ların güvenlik gereksinimlerini karşılayabilecek niteliktedir.

Bu çalışmada, KAA'ların düşük maliyetli olarak güvenli haberleşme ihtiyaçlarını karşılayabilmek amacıyla SEA şifreleme algoritmasının kablosuz algılayıcı düğümleri üzerinde gerçeklemesi yapılmış ve gerçeklemeden elde edilen performans değerleri sunulmuştur.

Bu makalenin literatüre temel katkıları şunlardır;

- KAA'larda SEA şifreleme algoritması kullanılarak güvenli iletişimin düşük maliyetle gerçekleştirilmesi,
- SEA şifreleme algoritmasının gerçeklemesinin idealleştirilmiş benzetim ortamları yerine MICAz kablosuz algılayıcı ağ platformu üzerinde yapılması.

Makalenin geri kalan kısımları şu şekilde düzenlenmiştir: Bölüm 2'de KAA güvenliği hakkında bilgi verilmektedir. 3. Bölümde SEA şifreleme algoritmasının özellikleri açıklanmakta, Bölüm 4'de SEA algoritmasının gerçeklemesinde kullanılan deney düzeneği ve araçlar tanıtılmaktadır. Bölüm 5'de ise gerçeklemeden elde edilen sonuçlar sunulmakta ve son bölümde makale sonuçlandırılmaktadır.

Cuneyt Bayılmış ve Murat ÇAKIROĞLU, Sakarya Üniversitesi, Teknik Eğitim Fakültesi, Bilgisayar Sistemleri Öğretmenliği, Esentepe Kampusü, Sakarya, Tel:2642956456, Fax:2642956421
e-mail: {cbayilmis, muratc}@sakarya.edu.tr

II. KABLOSUZ ALGILAYICI AĞLARDA GÜVENLİK

Askeri ve tıbbi uygulamalar, doğal felaketlerin tespiti, bina güvenlik sistemleri v.b. birçok alanda kullanılmakta olan KAA'ların çeşitli türdeki saldırılara karşı güvenilir bir şekilde çalışabilmesi son derece hayati önem arz etmektedir. Ancak, düşük maliyetin sağlanabilmesi için donanımsal kaynakları sınırlı olan düğümlerin tercih edilmesi, geleneksel güvenlik tekniklerinin KAA'larda kullanılmasını zorlaştırmaktadır. Bununla birlikte, algılayıcı düğümlerinin çoğu uygulama için dış ortamda bulunması ve paylaşımlı olan kablosuz ortam üzerinden haberleşmesi saldırganların işini kolaylaştırmakta ve KAA'ların güvenlik açısından diğer ağlara nazaran daha fazla risk taşımasına sebep olmaktadır. KAA'larda güvenlik 3 temel perspektifte incelenebilir [2]:

- KAA'ların güvenliğini kısıtlayan unsurlar,
- KAA güvenlik gereksinimleri,
- KAA güvenliğini tehdit eden saldırılar ve savunma yöntemleri.

A. KAA Güvenliğini Kısıtlayan Unsurlar

KAA'lar, geleneksel ağlara oranla daha fazla sınırlamaya sahip özel bir ağ hüviyetindedir. Sınırlı donanımsal kaynaklar, güvenli olmayan iletişim kanalı, düğümlerin uzun süreler boyunca gözetimsiz çalışması gibi sebepler, geleneksel güvenlik tekniklerinin doğrudan KAA'larda kullanılmasını zorlaştırmaktadır. Güvenli bir ağ tasarımı gerçekleştirebilmek için bu sınırlamaları dikkate almak gerekmektedir.

B. KAA Güvenlik Gereksinimleri

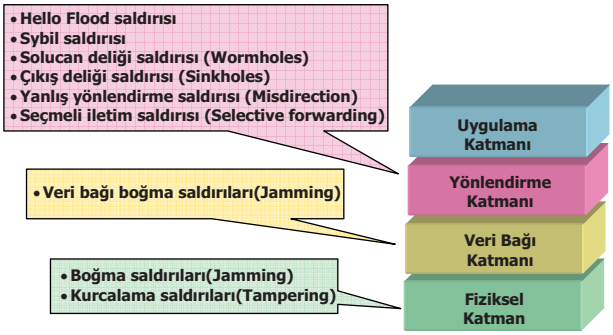
KAA'lar, geleneksel bilgisayar ağlarının ihtiyaç duyduğu güvenlik gereksinimlerine ek olarak sadece kendine has olan güvenlik gereksinimlerine de sahiptir. Bu özel gereksinimlerin birçoğu KAA'ların dış ortamda olmalarından kaynaklanmaktadır.

KAA güvenli iletişim gereksinimleri özetle şunlardır:

- Veri gizliliği (Data Confidentiality)
- Veri bütünlüğü(Data Integrity)
- Veri tazeliği (Data Freshness)
- Kimlik doğrulama (Authentication)
- Kendi kendini örgütleme (Self Organization)
- Zaman eşlemesi (Time Synchronization) ,
- Güvenli konum belirleme (Secure Localization)

C. Saldırlar ve Savunma Önlemleri

KAA'lar yapısı gereği birçok türdeki saldırılara karşı açıktır. Özellikle farklı katmanlardaki fonksiyonların işleyişini bozmayı hedefleyen Hizmet Engelleme (Denial of Service-DoS) Saldırıları KAA güvenliği için önemli bir tehdit unsurudur. Şekil 1'de KAA katmanlarını etkileyen DoS Saldırıları görülmektedir. DoS saldırıları dışında trafik analiz, düğüm kopyalama (node replication), gizliliğin ortadan kaldırılması (attacks against privacy) gibi birçok saldırı türü KAA için önemli tehditlerdendir [4-5].



Şekil 1. KAA katmanlarını etkileyen DoS saldırı türleri

Yukarıda bahsedilen saldırıların birçoğunun vermiş olduğu zararlar veri gizliliği, bütünlüğü ve tazeliğinin sağlanmasının yanında iletişimin kimlik denetimi ile gerçekleştirilmesi sayesinde en aza indirilebilir. Bu sebeple güvenli iletişimde, düğümlerin bir şifreleme yöntemiyle paketleri şifrelemesi, bütünlüğünü kontrol etmesi ve kimlik denetimini gerçekleştirmesi gerekmektedir. Literatürde sunulan güvenlik çözümlerinden SPIN [8] ve INSENS [9] protokolleri RC5, TinySec güvenlik paketi [10] Skipjack ve 802.15.4 standardı AES şifreleme algoritmalarını kullanmaktadır. Bu çalışmada yeni bir şifreleme algoritması olan SEA'nın algılayıcı düğümleri üzerinde gerçeklemesi üzerinde durulmaktadır. Bu sebeple bir sonraki bölümde SEA algoritması ayrıntılı olarak incelenmektedir.

III. ÖLÇEKLENEBİLİR ŞİFRELEME ALGORİTMASI (SCALABLE ENCRYPTION ALGORITHM, SEA)

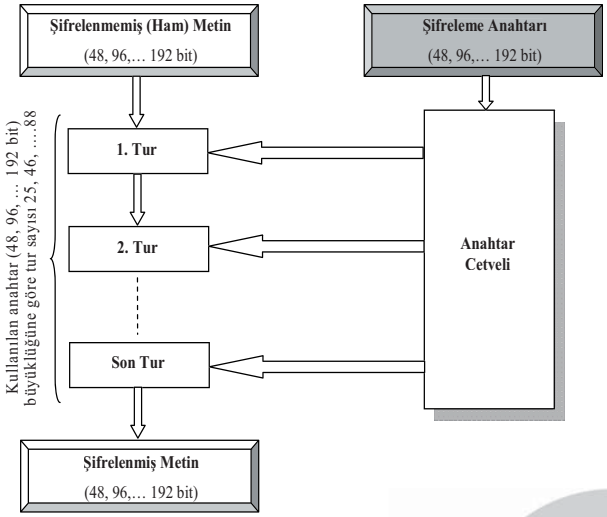
SEA, bellek büyüklüğü ve işlem gücü gibi sınırlı kaynaklara sahip gömülü sistemlere yönelik geliştirilmiş, bir şifreleme algoritmasıdır [6-7]. Simetrik blok şifreleme yaklaşımına dayanan SEA'nın tasarım kriterleri küçük bellek alanı, küçük kod büyüklüğü ve sınırlı komut setidir. Bu sebeple sadece, ÖZEL VEYA, bit/kelime rotasyonları, mod 2^b toplama ve s-box gibi bit operasyonlarını kullanır.

Oldukça esnek bir yapıya sahip olan SEA, $\mathbf{SEA_{n,b}}$ şeklinde ifade edilmektedir ve farklı metin, anahtar/kelime uzunlukları üzerinde çalışabilmektedir. Ayrıca, değişken tur sayılarıyla Feistel yapısına dayanan SEA, aşağıdaki parametreler ile tanımlanmaktadır:

- n: ham metin ve anahtar büyüklüğü
- b:kelime büyüklüğü
- $n_b = \frac{n}{2b}$: Feistel dallanması başına kelime sayısı
- n_r: Şifreleme tur sayısı

SEA algoritmasının gerçeklemesinde n ve b parametreleri hedef işlemcinin özelliğine uygun olarak seçilebilir. Ancak anahtar ve ham metin büyüklüğü 48, 96, …, 192 bit gibi 6'nın katları olması gerekmektedir. Bir diğer önemli nokta ise uygun bir güvenlik düzeyinin sağlanabilmesi için kelime uzunluğunun b≥8 ve tur sayısının en az $n_r = \frac{3n}{4} + 2.(n_b + [b/2])$ olması gerekmektedir. Şekil-2'de

SEA algoritmasının yapısı görülmektedir.



Şekil 2. Ölçeklenebilir şifreleme algoritması (SEA)

IV. SEA ALGORİTMASININ GERÇEKLEMESİ

SEA algoritmasının gerçeklemesi, Crossbow firmasının popüler bir ticari ürünü olan MICAz kablosuz algılayıcı düğümleri üzerinde TinyOS [11] işletim sistemi kullanılarak gerçekleştirilmiştir. MICAz, 128 KB kod, 4KB veri hafıza içeren ve 16 MHz hızında çalışan ATMEGA128L mikrodenetleyiciye sahiptir. Kablosuz iletişimi Chipcon CC2420 alıcı/verici tüm devresini kullanarak 250 Kbit/s hızında gerçekleştirebilmektedir.

SEA algoritmasının en önemli özelliklerinden biri farklı işlemci büyüklüklerinde ve farklı anahtar/ham metin büyüklüklerinde çalıştırılabilmesidir. Bu çalışmada anahtar /ham metin büyüklüğü 96 bit ve kelime uzunluğu 8 bit olarak seçilmiştir. ($SEA_{96,8}$).

İlk olarak C dilinde yazmış olduğumuz ve daha sonra nesC diline uyarladığımız SEA algoritmasının gerçeklenmesinde ve başarımının ölçülmesinde kullanılan araçlar şunlardır:

- Algılayıcı düğümlerinin TinyOS işletim sistemi üzerinde gerçeklenen SEA algoritmasını kullanarak güvenli iletişim gerçekleştirebildiğini analiz etmek için kablosuz algılayıcı ağ düzeneği (Şekil-3).
- SEA algoritmasının algılayıcı düğümlerin belleğinde kapladığı alan, düğümlerin şifreleme/şifre çözme işlemlerinde harcadığı süre ve SEA'nın sağlayabildiği bant genişliği ölçütlerinin elde edilmesi için AVR Studio 4 [13] ve AVR GCC [14] yazılımları kullanılmıştır.

Şekil 3'de SEA algoritmasının gerçekleştirildiği bir dizüstü bilgisayar, bir merkezi düğüm ve bir kablosuz algılayıcı düğümden oluşan KAA deney düzeneği görülmektedir. Algılayıcı düğüm merkezi düğüm ile 200 paket/s hızında şifrelenmiş veri iletişimi gerçekleştirmektedir. Merkezi düğüm ise almış olduğu şifreli veriyi çözerek USB bağlantısı üzerinden bilgisayara aktarmaktadır. Bilgisayarda merkezi düğümden gelen bilgiyi göstermektedir. Bu düzenek ile düğümlerin SEA algoritmasını kullanarak şifreleme, şifre çözme ve kimlik doğrulama işlemlerini gerçek uygulamalarda başarılı bir şekilde gerçekleştirebildiği kontrol edilmektedir.

Şekil 3. Kablosuz algılayıcı ağ deney düzeneği

V. GERÇEKLEME SONUCU VE DEĞERLENDİRME

Şifreleme algoritmalarının başarımının ölçülmesinde, çalışma zamanı (şifreleme/şifre çözme işlemlerinde harcanan süre), bellek gereksinimi, bant genişliği, güvenlik (kırılma süresinin uzunluğu), esneklik, standartlaştırılabilme, hedeflenen sisteme uygunluk kriterleri göz önüne alınmaktadır [12]. Bu çalışmada SEA şifreleme algoritmasının başarım değerlendirmesi aşağıdaki kriterlere göre yapılmaktadır.

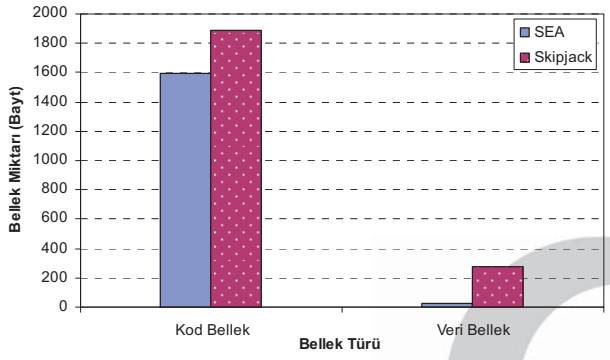
- Bellek gereksinimi,
- Çalışma zamanı ve bant genişliği
- Güvenlik ve esneklik

Şifreleme algoritmalarının hedeflenen cihaz ve ortamlara olan yüksek bağımlılığından dolayı değerlendirilmesi ve birbirleriyle karşılaştırılması oldukça zordur. Buna rağmen fikir vermesi açısından SEA şifreleme algoritması, TinySec güvenlik paketi içerisinde kullanılan Skipjack şifreleme algoritması ile karşılaştırılmaktadır. Her iki algoritmanın C dilinde yazmış olduğumuz versiyonları AVR Studio 4 ve AVR GCC araçları yardımıyla derlenerek benzetilmiş ve ihtiyaç duydukları bellek miktarları, şifreleme/şifre çözme süreleri ve bant genişlikleri elde edilmiştir.

A. Bellek Gereksinimi

Şekil 4'de SEA ve Skipjack algoritmalarının şifreleme ve şifre çözme işlemleri için ihtiyaç duyduğu bellek miktarları

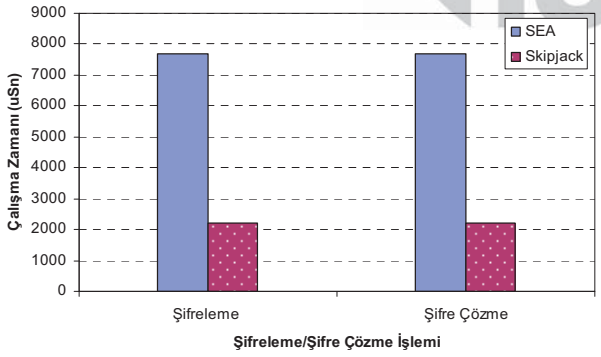
görülmektedir. SEA, kod belleğinde 1598 bayt yer kaplarken veri belleğinde sadece 25 bayt'lık bir alan tutmaktadır. Skipjack algoritması kod bellekte 1884 bayt, veri bellekte ise 274 baylık alan kaplamaktadır. Her iki algoritmanın ihtiyaç duyduğu kod bellek miktarları birbirine yakınken SEA, Skipjack algoritmasına oranla yaklaşık olarak 11 kat daha az veri bellek alanı kullanmaktadır. SEA'nın oldukça düşük veri belleğine ihtiyaç duyması, temelinin basit bit operasyonlarına dayanmasından kaynaklanmaktadır.



Şekil 4. SEA ve Skipjack algoritmalarının bellek gereksinimleri

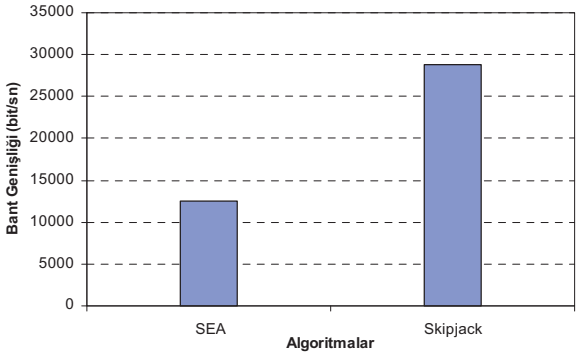
B. Çalışma Zamanı ve Bant genişliği

Şekil 5'de SEA ve Skipjack algoritmalarının çalışma zamanları görülmektedir. SEA algoritmasının şifreleme/şifre çözme süresi (7708 us), Skipjack algoritmasının şifreleme/şifre çözme süresinden (2220 us) yaklaşık olarak 3,5 kat daha fazladır. Bu SEA ve Skipjack şifreleme algoritmalarının kullanmış oldukları anahtar/ham metin büyüklüğü, algoritmalarına ait kural tabloları ve tur sayılarının farklılıklarından kaynaklanmaktadır. Örneğin SEA bu çalışma için 96 bit anahtar ve ham metin kullanırken, Skipjack 80 bit anahtar ve 64 bit ham metin kullanmaktadır. Bir başka fark olarak da SEA'nın bu çalışma için 93 tur Skipjack'in ise 32 tur ile şifreleme rutinlerini gerçekleştirmesidir.



Şekil 5. SEA ve Skipjack algoritmalarının şifreleme/şifre çözme işlemleri için harcadıkları zaman

Şekil 6'da SEA ve Skipjack algoritmalarının sağlayabildikleri bant genişlikleri görülmektedir. Her iki algoritma şifreleme ve şifre çözme işlemlerinde aynı bant genişliklerini sağlamaktadır. Şekilden görüldüğü gibi SEA algoritması, Skipjack algoritmasından yaklaşık 2,3 kat daha az bant genişliği sağlamaktadır (SEA: 12454 bit/s, Skipjack:28828 bit/s).



Şekil 6. SEA ve Skipjack algoritmalarının kullandıkları bant genişlikleri (şifreleme ve şifre çözme işlemleri için aynı bant genişliğini kullanmaktadırlar)

C. Güvenlik ve Esneklik

Skipjack, çalışma zamanı ve bant genişliği açısından SEA'ya oranla daha verimli olmasına rağmen sağlayabildiği güvenlik seviyesi açısından daha gerilerdedir. Skipjack algoritmasının 31 turlu indirgenmiş versiyonu ve 32 turlu tam versiyonlarının kırılabileceği literatürde gösterilmektedir [15,16]. Bunun yanında SEA algoritması için herhangi bir kriptanaliz çalışması henüz bulunmamaktadır. Ayrıca SEA'nın parametreye bağlı olarak yapılandırılabilmesi istenilen güvenlik seviyesinin ayarlanabilmesine imkân tanımaktadır.

VI. SONUÇ

Bu çalışmada MICAz düğümlerden oluşan temel bir kablosuz algılayıcı ağ üzerinde SEA şifreleme algoritması kullanarak güvenli iletişim gerçekleştirilmiş ve SEA şifreleme algoritmasının KAA'lar için uygunluğu bellek kullanımı, çalışma zamanı, bant genişliği, güvenlik ve esneklik kriterleri açısından değerlendirilmiştir. SEA'nın başarımının kıyaslanmasında KAA uygulamalarında popüler olarak tercih edilen Skipjack algoritması kullanılmıştır. Her iki algoritmanın başarım değerlendirmesi aynı koşullarda gerçekleştirilmiştir.

Deneysel sonuçlar incelendiğinde SEA algoritmasının Skipjack algoritmasından daha az bellek gereksinimine ihtiyaç duyduğu görülmektedir. Ancak SEA'nın şifreleme ve şifre çözme süresi Skipjack algoritmasına oranla daha fazla ve sağlayabildiği bant genişliği daha düşüktür. Bunun temel sebebi SEA'nın daha fazla tur ile şifreleme işlemlerini gerçekleştirmesidir. Bununla beraber Skipjack'in kriptanalizinin yapılması ve SEA'ya karşı henüz bir saldırının gerçekleştirilmemesi güvenlik açısından SEA'yı daha avantajlı kılmaktadır. Ayrıca SEA'nın farklı kelime uzunluklarına sahip işlemcilere (8 bit, 32 bit vb.) uygun olarak yapılandırılabilmesi, anahtar ve ham metin büyüklüklerinin

değiştirilebilmesi farklı türdeki kablosuz algılayıcı ağ platformlarında kolaylıkla kullanılabilmesini mümkün kılmaktadır.

TEŞEKKÜR

Yazarlar Doç.Dr. İsmail ERTÜRK Bey'e MICAz kablosuz algılayıcı düğümleri sağladığı için teşekkür etmektedirler

KAYNAKLAR

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

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

[3] N. Bandırmalı, C. Bayılmış, I. Ertürk, "Kablosuz Algılayıcı Ağlarda Güvenlik", *Ulusal Teknik Eğitim, Mühendislik ve Eğitim Bilimleri Genç Araştırmacılar Sempozyumu, UMES'07*, 2007, pp. 37–40.

[4] M. Çakıroğlu, A.T. Özcerit, "Denial of Service Attack Resistant MAC Protocol Design for Wireless Sensor Networks", *J. Fac. Eng. Arch. Gazi Univ*, vol. 22, no 4, 2007, pp. 697-707.

[5] M. Çakıroğlu, A.T. Özcerit, Ö. Çetin, H. Ekiz., "MAC Layer DoS Attacks in Wireless Sensor Networks: A Survey", *Proc. of the ICWN'06*, 2006.

[6] F. -X. Standaert, G. Piret, N. Gershenfeld, J.-J. Quisquater., "SEA: A Scalable Encryption Algorithm for Small Embedded Applications", *CARDIS 2006, Lecture Notes in Computer Science*, vol. 3928, April 2006, pp. 222-236.

[7] F. Macé, F.-X. Standaert, J.-J. Quisquater, "FPGA Implementation(s) of a Scalable Encryption Algorithm", *IEEE Transactions on Very Large Scale Integration (VLSI) Systems,* vol. 16, no.2, Nov. 2007, pp. 212 – 216.

[8] A. Perrig, R. Szewczyk, J. D. Tygar, V. Wen, and D. Culler, "SPINS:Security Protocols for Sensor Networks", *Wireless Networks*, vol. 8, 2002, 521-534.

[9] J. Deng, R. Han, S. Mishra, "INSENS: Intrusion-tolerant routing in wireless Sensor NetworkS". *Technical Report CU CS-939-02, Department of Computer Science, University of Colorado*, November 2002.

[10] C. Karlof, N. Sastry and D. Wagner , "TinySec: Link Layer Security for Tiny Devices" , [Online], Available: www.cs.berkeley.edu/~nks/tinysec/

[11] TinyOS Kullanımı [Online] http://docs.tinyos.net/index.php/Using_TinyOS

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

[13] Atmel Corporation. Avr studio 4.12, build 498. Available from: http://www.atmel.com/dyn/products/tools_card.asp?tool_id=2725.

[14] AVR-GCC, Ücretsiz AVR C ve Assembler Derleyicisi, http://gcc.gnu.org/

[15] E. Biham, A. Bikyukov, A. Shamir, "'Cryptanalysis of Skipjack reduced to 31 rounds using impossible differentials", Proc. of Eurocrypt' 99, 1999, pp. 12-23

[16] R. Chung-Wei Phan, "Cryptanalysis of full Skipjack block cipher", Electronics Letters, Vol. 38, No. 2, January 2002.