Yeni Bir Kablosuz Algılayıcı Ağ Veri Bağı Katmanı Güvenlik Protokolü

Necla BANDIRMALI, İsmail ERTÜRK

ÖZET

Kablosuz Algılayıcı Ağlar (KAA'lar), enerji kaynakları ve hesaplama yetenekleri oldukça sınırlı küçük algılayıcı düğümlerden oluşmaktadır. Maliyet–etkin uygulamalar için tercih sebebi olan bu özelliklerin beraberinde getirdiği olumsuzluklara bağlı olarak geleneksel ağlar için tasarlanan güvenlik protokolleri KAA'larda doğrudan kullanılamamaktadır. KAA iletişim güvenliği konusunda yapılan çalışmalar, genellikle enerji, bellek ve işlemci gibi sınırlı düğüm kaynaklarının etkin kullanımı üzerine odaklanmaktadır. Bununla birlikte, özellikle sağlık alanındaki KAA uygulamalarında yüksek güvenlik sağlayan protokollere olan ihtiyaç günümüzde artan bir önem kazanmaktadır. Bu makalede, SEA blok şifreleme algoritması ile birlikte veri gizliliği ve güvenilirliğini arttırmak için kullanılan CTR ve CBC–MAC asıllama/bütünlük denetim yaklaşımlarının bütünleşik yapıda kullanımıyla geliştirilen ve kısaca YP (Yeni Bir KAA Veri Bağı Katmanı Güvenlik Protokolü) olarak adlandırılan yeni bir protokol sunulmaktadır. YP'nin sunmuş olduğu güvenlik düzeyi, kullanılan yaklaşımlarla dinamik olarak yükseltilebilmektedir. Elde edilen sonuçlar göstermektedir ki, 96-bit veri blok/anahtar boyutuna sahip güvenlik düzeyinde, TinySEC'e kıyasla, YP'nin KAA düğüm enerji tüketim değerine olumsuz etkisi bulunmazken, 192-bit veri blok/anahtar boyutuna sahip oldukça yüksek güvenlik düzeyinde, ihmal edilebilir bir artış görülmektedir.

Anahtar Kelimeler: KAA, Veri Bağı Katmanı Güvenlik Protokolü, Yüksek Güvenlik.

A New Data Link Layer Security Protocol for Wireless Sensor Networks

ABSTRACT

A Wireless Sensor Network (WSN) consists of several tiny sensor nodes with very limited sources. This important node characteristic usually results in difficulties in employing most of the common wireless network protocols in WSNs unfavorably. The effective usage of limited sensor node energy & other sources is of importance in WSN security researches. Moreover, research on especially increasing network security of the WSNs employed in health applications recently receives a remarkable attention. In this paper, a new highly secure WSN data link layer security protocol named hereafter as YP is proposed and its fundamental performance evaluation is presented. It combines the CTR and CBC–MAC approaches with the SEA block encryption algorithm for increased data confidentiality and authentication & integrity functions, respectively. The security level of the YP can be dynamically boosted up employing these methods together. In addition, using the proposed YP with the 96-bit data block/key size has a trivial effect on the WSN node energy consumption that is ignorably increased compared to that of the traditional TinySEC protocol while employing the YP with the 192-bit data block/key size providing an extremely high level of security.

Keywords: WSN, Data Link Layer Security Protocol, High Security.

1. GİRİŞ

Kablosuz Algılayıcı Ağlar (KAA'lar), oldukça değişik uygulama alanlarında kullanılmaktadır. KAA'lar, özellikle askeri uygulamalar başta olmak üzere birçok alanda veri gizliliği, bütünlüğü, tazeliği ve kimlik doğrulaması gibi temel güvenlik gereksinimlerini sağlamak zorundadır. Geleneksel ağlar için tasarlanan ve günümüzde birçok uygulamada yaygın olarak kullanılan güvenlik yöntemleri; kablosuz algılayıcı düğümlerin, kısıtlı enerji kaynaklarına, yetersiz bellek kapasitelerine ve sınırlı işlem kabiliyetlerine sahip olmaları, kolay erişilebilir ve fiziksel saldırılara açık alanlara yerleştirilmeleri ve insanlarla/ölçüm yapılacak fiziksel ortamla doğrudan etkileşimde bulunmalarından dolayı, KAA'larda doğrudan uygulanamamaktadır. Günümüzde, KAA uygulamalarının ve içerdikleri düğümlerin bu özellikleri göz önüne alınarak çeşitli güvenlik protokolleri geliştirilmektedir (1, 2, 3).

Güvenlik konusunda yapılan araştırmalar ve uygulamalar, KAA alanındaki diğer tüm çalışmalarda olduğu gibi, genellikle enerji ve diğer kaynakların etkin kullanımı üzerine odaklanmaktadır.

Literatürde veri güvenilirliği için geliştirilmiş sınırlı sayıda güvenlik protokolü bulunmaktadır. Bu protokollerin başında SPINS (Security Protocols for Sensor Networks) yer almaktadır. Diğer önemli protokoller ise TinySEC ve LLSP (Link Layer Security Protocol)'dir. SPINS ve LLSP protokollerinin cihazlar üzerinde uygulaması gerçekleştirilmemiştir. Fakat TinySEC, hâli-

Makale 30.10.2009 tarihinde gelmiş,28.12.2009 tarihinde yayınlanmak üzere kabul edilmiştir.

N. BANDIRMALI, İ. ERTÜRK, Kocaeli Üniversitesi Teknik Eğitim Fakültesi, Elektronik ve Bilgisayar Bölümü 41380 Kocaeli

e-posta : bandirmali@kocaeli.edu.tr,ertürk@kocaeli.edu.tr

Digital Object Identifier 10.2339/2009.12.4, 235-242.

hazırda Mica2 cihazlarında kullanılan bir güvenlik protokolüdür. Bu sebeple TinySEC protokolü bu alanda referans çalışma olarak değerlendirilmektedir. TinySEC ve LLSP, düğüm enerjisinin etkin kullanımı esas alınarak geliştirilmiş protokollerdir ve bunlarda kullanılan şifreleme yaklaşımları başta sağlık ve askeri KAA uygulamaları olmak üzere üst düzey güvenlik gerektiren alanların gereksinimlerini karşılayacak şekilde tasarlanmamıştır. Protokollerin bu alandaki eksikliği göz önüne alınarak, enerji tüketimini ve kaynak kullanımını çok fazla arttırmadan önemli KAA uygulamalarında yüksek güvenlik sağlayan protokollere olan ihtiyaç günümüzde artan bir önem kazanmaktadır (1).

Bu makalede sunulan çalışmada (YP), özellikle sınırlı kaynakları bulunan düğümlerde kullanılan SEA (Scalable Encryption Algorithm, Ölçeklenebilir Şifreleme Algoritması) blok şifreleme algoritması ile CTR (Counter, Sayaç) blok şifreleme yaklaşımı ve CBC–MAC (Cipher Block Chaining Message Authentication Code, Şifre Blok Zincirlemesi Mesaj Asıllama Kodu) asıllama/bütünlük yaklaşımı bütünleşik olarak kullanılarak, yeni bir KAA veri bağı katmanı güvenlik protokolü tasarımı gerçekleştirilmiştir (1). YP içerisinde CTR yaklaşımı ile arttırılmış veri gizliliği temin edilirken, CBC–MAC yaklaşımı ile asıllama ve veri bütünlüğü için önemli bir katkı sağlanmaktadır.

Makalenin 2. bölümünde, KAA güvenlik protokolleri hakkında kısa bilgiler verilmektedir. 3. bölümde geliştirilen yeni KAA veri bağı katmanı güvenlik protokolü ve tasarım süreci açıklanmaktadır. Bu bölümde ayrıca, geliştirilen protokolün geleneksel TinySEC ve LLSP ile karşılaştırmalı değerlendirmesi sunulmaktadır. Son bölümde ise, çalışma özetlenerek kısa bir değerlendirme yapılmaktadır.

2. MEVCUT KAA GÜVENLİK PROTOKOLLERİ

Güvenli olmayan iletişim kanallarını, etkin bir şekilde kullanılabilir hale getirmek amacıyla önerilmiş birçok genel güvenlik protokolü bulunmaktadır.

Kablolu ağlar için RC4 şifreleme algoritmasını kullanan WEP (Wired Equivalent Privacy) ve daha sonra yine aynı şifreleme algoritmasını kullanan TKIP (Temporal Key Integrity Protocol) ile kablosuz ağlar için AES şifreleme algoritmasını kullanan AES–CCMP (Advanced Encryption Standard–Counter Mode with Cipher Block Chaining Mode Protocol) protokolü geliştirilmiştir. Ayrıca, Internet güvenliğini sağlamak için IPSec (Internet Protocol Security), SSL/TLS (Secure Sockets Layer/Transport Layer Security) ve SSH (Secure Shell) gibi protokoller literatürde sunulmuştur. Ancak, bu protokollerin KAA'larda kullanımı, kablosuz algılayıcı düğümlere göreceli olarak aşırı işlem yükü getirmektedir. Zira bu düğümler, hesaplama kabiliyetleri oldukça sınırlı küçük donanımlardır (1, 4).

Özellikle KAA'larda veri bağı katmanı güvenliği için geliştirilmiş birkaç önemli ve tercih edilen güvenlik protokolü bulunmaktadır. Bunlardan SPINS (5) protokolü, SNEP ve µTESLA olmak üzere iki güvenlik bloğundan oluşmaktadır. SNEP (Secure Network Encryption Protocol), RC5 blok şifreleme algoritmasıyla birlikte CTR ve CBC–MAC yaklaşımlarının birlikte kullanıldığı bir protokoldür. µTESLA ise, sınırlı kaynaklara sahip ortamlar için asıllanmış yayın (broadcast) sağlayan bir protokoldür. KAA'lar için geliştirilmiş olan bu güvenlik protokolünün enerji maliyet hesabı incelendiğinde, hesap karmaşıklığından çok, ek veri iletiminin sisteme aşırı yük getirdiği saptanmıştır. Ayrıca bu protokolün hiçbir gerçeklemesi yapılmamıştır.

KAA'lar için geliştirilen ve birçok uygulamada kullanılmakta olan bir diğer güvenlik protokolü ise TinySEC'tir (6). TinySEC, güvenlik için sadece asıllama ve asıllama & şifreleme olmak üzere iki farklı kullanım seçeneği sunmaktadır. Sadece asıllama seçeneğinde, Mesaj Asıllama Kodu (MAK) ile tüm paket doğrulanmakta, veri şifrelenmemektedir. Asıllama & şifreleme seçeneğinde ise, veri hem şifrelenmekte hem de paket (başlık+veri) bir MAK ile doğrulanmaktadır. TinySEC'te, mesaj gizliliğini sağlamak için SKIPJACK simetrik blok şifreleme algoritması, blok şifreleme yöntemlerinden birisi olan CBC yaklaşımı ile birlikte kullanılmaktadır. Şifrelemenin güvenliğini arttırmak için ayrıca 8 baytlık bir başlangıç vektörü (IV) bulunmaktadır. Mesaj bütünlüğü ve doğruluğunu sağlamak için CBC–MAC yaklaşımı ile 4 baytlık bir MAK hesaplanmakta ve pakete eklenmektedir.

KAA'lar için geliştirilen bir başka güvenlik protokolü de, enerji etkin veri bağı katmanı güvenlik protokolü LLSP'dir (7). LLSP'de mesaj gizliliği, simetrik blok şifreleme algoritmalarından AES ve CBC yaklaşımının bir arada kullanılması ile sağlanmaktadır. AES, güvenliği yüksek ve mevcut kablosuz ağlarda kullanılan bir şifreleme algoritmasıdır. TinySEC'e benzer şekilde, bu protokolde de şifrelemenin güvenliğini arttırmak için bir başlangıç vektörü (IV) kullanılmakta ve mesaj bütünlüğü/doğruluğu için CBC–MAC yaklaşımı ile 4 baytlık bir MAK elde edilmektedir.

LLSP'nin TinySEC protokolünden en önemli olumlu farkı; aynı paketlerin tekrar gönderilip gönderilmediğinin denetimini yapmak için kullanılan sayaç değerinin paket başlığına eklenmesi yerine, gönderici ve alıcı arasında bir kaymalı kaydedici (shift register) kullanılmasıdır. Böylece paket ek yükü (overhead) azalmaktadır (8). TinySEC ve LLSP protokolleri KAA'lar için geliştirilmiş protokoller olmasına rağmen, bu protokollerde kullanılan blok şifreleme algoritmaları geleneksel ağlarda da kullanılan algoritmalardır. Bu üç protokol tasarlanırken temel ölçüt olarak "enerji etkin" çözümler olması hedeflendiğinden "yüksek güvenlik" ve "veri güvenilirliği" ikinci planda tutulmuştur. Bu makalede sunulan yeni güvenlik protokolünde, geleneksel eşleniklerinden üstün olarak, aşağıdaki iki kıstas üzerinde durulmaktadır;

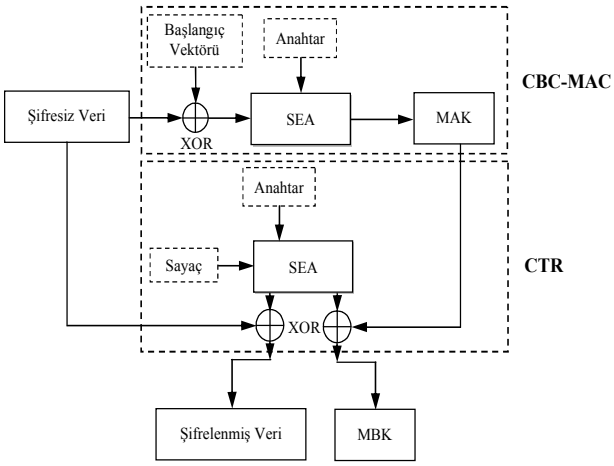
- Özellikle sınırlı kaynakları bulunan düğümler için tasarlanan bir blok şifreleme algoritması kullanmak ve,

- Güvenlik seviyesinin, bu alandaki en önemli çözümlerinden biri olan, IEEE 802.11i kablosuz standardı AES–CCMP (9) 'de kullanılan yaklaşımlarla arttırılırken enerji tüketiminin belirli bir seviyede tutulmasını sağlamaktır.

3. YENİ BİR KAA VERİ BAĞI KATMANI GÜVENLİK PROTOKOLÜ–YP

Yeni bir KAA güvenlik protokolü geliştirirken, güvenlik düzeyi, başarım (gecikme, bellek kullanımı ve enerji tüketimi) ve kullanılırlık gibi üç temel ölçüt göz önüne alınmaktadır. Farklı KAA uygulamalarının gereksinimleri esas alındığında, bunların öncelikleri değişebilmektedir. Örneğin, çevresel izlemede veri (mesaj) gizliliği çok büyük önem taşımazken, sağlık ve askeri uygulamalarda güvenilirlik ilkelerini oluşturan veri gizliliği/bütünlüğü, asıllama ve kaynak/hedef doğrulaması oldukça önemlidir. Bundan dolayı, örneğin sağlık uygulamaları için planlanan bir çalışmada, enerji etkin bir güvenlik protokolü yerine, veri güvenilirliği arttırılmış bir güvenlik protokolü tasarımı amaçlanmalıdır. Geleneksel olarak, yüksek güvenlik sağlayan yöntemler aşırı hesaplama gerektirmektedir ve bunların küçük algılayıcı düğümlerde kullanımı, enerji tüketiminin oldukça artmasına yol açmaktadır.

Bu makalede sunulan KAA veri bağı katmanı güvenlik protokolü (**YP**), özellikle sınırlı kaynakları bulunan düğümlerde kullanılan SEA blok şifreleme algoritması ile veri gizliliği ve güvenilirliğini arttırmak için kullanılan CTR ve CBC–MAC asıllama/bütünlük denetim yöntemlerinin birlikte (bütünleşik) kullanılmasıyla geliştirilmiş bulunmaktadır (Şekil 1). Gerçeklenen bu yeni protokolde CTR yaklaşımı ve SEA şifreleme algoritması kullanılarak veri gizliliği ve güvenilirliği arttırılırken, CBC–MAC asıllama yaklaşımı ile veri bütünlüğü ve doğruluğu sağlanmaktadır (1).

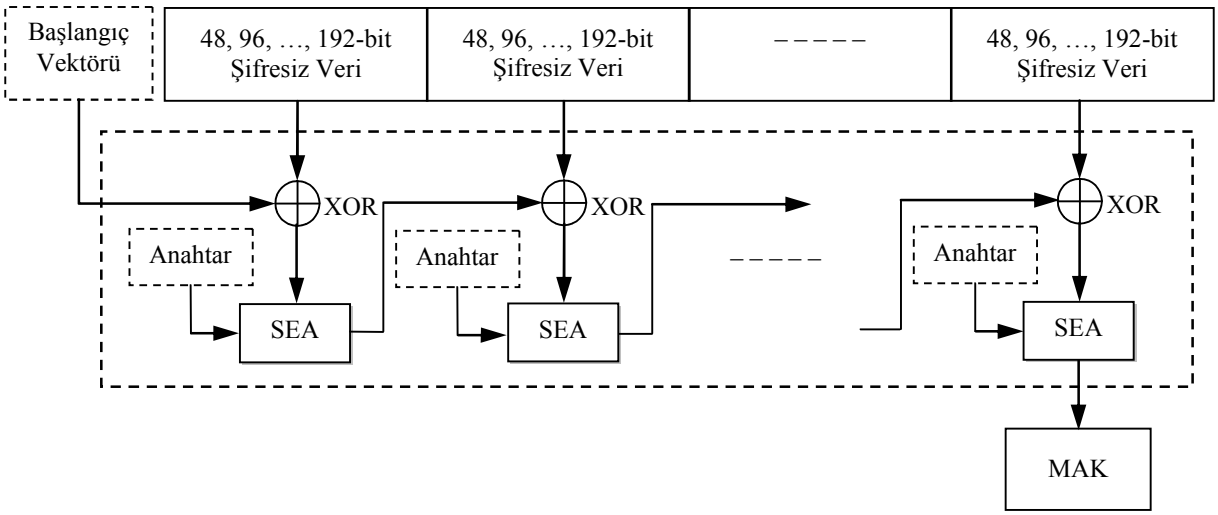


Şekil 1. Önerilen YP'nin blok şeması.

3.1. YP Veri Asıllaması, Bütünlüğü ve Güvenilirlik

Asıllama olmaksızın sadece şifrelemenin kullanılması güvenilir değildir. Asıllama yapılmadan şifrelenmiş veriler, şifresiz veride tahmin edilebilir değişikliklere sebep olabilmektedir. Asıllama mekanizması bulunmayan alıcılar, üçüncü şahısların saldırıları ile veride oluşan değişiklikleri saptayamayabilir. Ayrıca asıllanmamış veriler "kes ve yapıştır" saldırılarına da açıktır. Bu olumsuzlukları da göz önünde bulundurarak güvenlik protokolleri geliştirilirken, veri asıllamasını ve bütünlüğünü sağlamak amacıyla MAK kullanılmaktadır. MAK, iletilen veriyi şifrelemeyip, verinin hedefe doğru bir şekilde ulaştığını tespit/teyit etmek amacıyla geliştirilmiş bir yöntemdir.

Önerilen YP'de, MAK hesabı CBC–MAC yaklaşımı kullanılarak yapılmaktadır. CBC–MAC oldukça etkili, hızlı ve güvenlidir. Geleneksel güvenlik protokol-



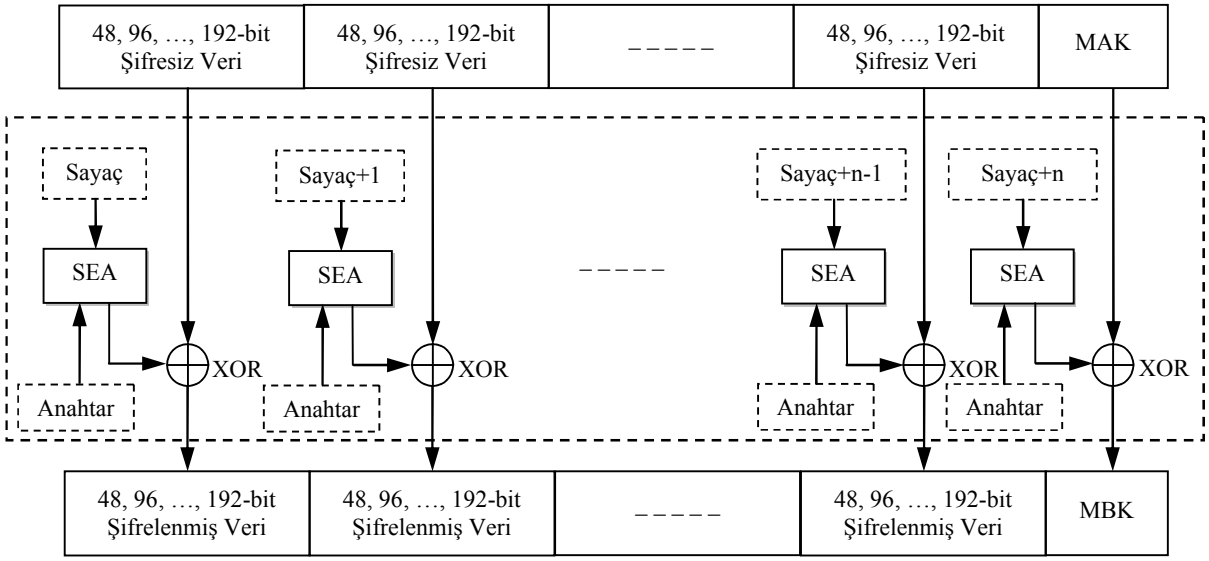
Şekil 2. YP'de CBC–MAC yaklaşımıyla MAK hesabı.

leri 8 ya da 16 baytlık MAK kullanmakla birlikte, KAA'larda veri asıllaması için çoğunlukla 4 baytlık MAK değeri yeterli olabilmektedir. Bu durumda dahi saldırıda bulunan bir düğüm, belirli bir veri için oluşturulan MAK değerini ancak 2^{31} denemeden sonra elde edebilir (10). Şekil 2'de görüldüğü gibi YP'de şifrelenmiş veri blokları birbirine zincirlenmiş bir yapıdadır. Burada SEA algoritmasının girdisini, XOR'lanmış mevcut şifresiz veri bloğu ve önceki şifreli veri bloğu oluşturmaktadır. Şifrelenmiş en son veri bloğunun ilk 4 baytı MAK değeri olarak seçilmekte ve pakete eklenmektedir. Saldırıda bulunan bir düğüm şifrelenmiş veride herhangi bir değişiklik (veri ekleme, bozma vb.) yaptığında, bu durum, paketteki mevcut MAK değeri ve alıcı (hedef) düğümün hesapladığı MAK değeri ile karşılaştırılarak kolaylıkla tespit edilebilmektedir (1).

3.2. YP Veri Gizliliği ve Güvenilirlik

Literatürde, özellikle sınırlı kaynaklar için geliştirilmiş çok az sayıda şifreleme algoritması (örneğin TEA ve Yuval's proposal (11, 12)) bulunmaktadır. Hâlihazırda basit doğrusal ve farksal şifre analiz yöntemleriyle dahi incelendiğinde, bu algoritmaların kanıtlanabilir derecede güvenlik sağlayamadığı bilinmektedir. Kablolu ya da kablosuz ağlarda kullanılabilen simetrik blok şifreleme algoritmalarından AES ve benzerleri ise KAA uygulamaları açısından genellikle yüksek maliyet, düşük güvenlik düzeyi ve yetersiz başarım gibi önemli olumsuz özelliklere sahiptir. Bu nedenlerle, önerilen yeni KAA veri bağı katmanı güvenlik protokolünde, kanıtlanabilir derecede güvenliği yüksek, başta doğrusal ve farksal şifre analiz yöntemlerine karşı olmak üzere dayanıklı ve özellikle sınırlı kaynaklar için geliştirilmiş olan SEA simetrik blok şifreleme algoritması kullanılmaktadır. Uygulama çalışmaları sonucunda, SEA şifreleme algoritmasının geleneksel AES şifreleme algoritmasına kıyasla, kaynakları (bellek, enerji ve mikroişlemci) olukça verimli kullanarak daha yüksek başarım sağladığı ortaya konulmuştur. Bu nedenle SEA, düşük şifreleme maliyetiyle, sınırlı kaynaklara sahip sistemlerde etkin kullanım için oldukça uygundur. Ek olarak, SEA veri blok büyüklüğü, AES (128-bit) şifreleme algoritmasının aksine sabit değildir. İstenen güvenlik düzeyine uygun ve dinamik bir şekilde değişik veri blok büyüklüklerinde (48, 96, …, 192-bit) şifreleme yapılabilmektedir (1, 13, 14, 15).

Bu makalede sunulan çalışmada, diğer güvenlik protokollerinden farklı olarak, veri gizliliği ve güvenilirliğini arttırmak için, blok şifreleme yaklaşımlarından birisi olan CTR kullanılmaktadır. CTR yaklaşımıyla birlikte, geleneksel TinySEC protokolünde paket başlığına eklenen ve ek yük getiren bir sayaç değerine gerek kalmamaktadır. Şekil 3'de görüldüğü gibi SEA ile şifrelenen rastgele oluşturulmuş bir sayaç değeri ve şifresiz veri bloğu XOR'lanmakta ve şifrelenmiş veri bloğu elde edilmektedir. Böylece MAK değerinin de şifrelenerek alıcıya (hedefe) iletilmesi sağlanmaktadır. Diğer bir ifadeyle hem veri hem de MAK değeri şifrelenmektedir. Sonuç olarak veri gizliliği artarken, aynı zamanda eklenen sayaç ile veri tazeliği de temin edilmektedir (1, 10).



Şekil 3. YP'de CTR yaklaşımıyla veri şifreleme.

3.3. YP Tasarım Aşamaları

Şekil 4'de görüldüğü gibi şifrelenecek veri (mesaj), seçilen güvenlik düzeyine uygun ve dinamik olarak belirlenebilen boyuttaki veri bloklarına (48, 96, …, 192-bit) bölündükten sonra üzerinde işlem yapılmaktadır. MAK değeri, veri ve anahtar üzerinden CBC–MAC asıllama yaklaşımı kullanılarak aşağıdaki işlemler sonunda hesaplanmaktadır (1):

- İlk veri bloğu ve başlangıç vektörü (IV) XOR işlemine tabi tutularak elde edilen değer SEA ile şifrelenmektedir.
- İkinci veri bloğu ve şifrelenmiş ilk blok XOR'lanarak elde edilen değer SEA ile şifrelenmektedir.
- Bu süreç, bütün veri blokları şifreleninceye kadar tekrar edilmektedir.

- En son şifrelenmiş veri blok değerinin ilk en önemli (MSB) 32 biti MAK değeri olarak kullanılmaktadır.

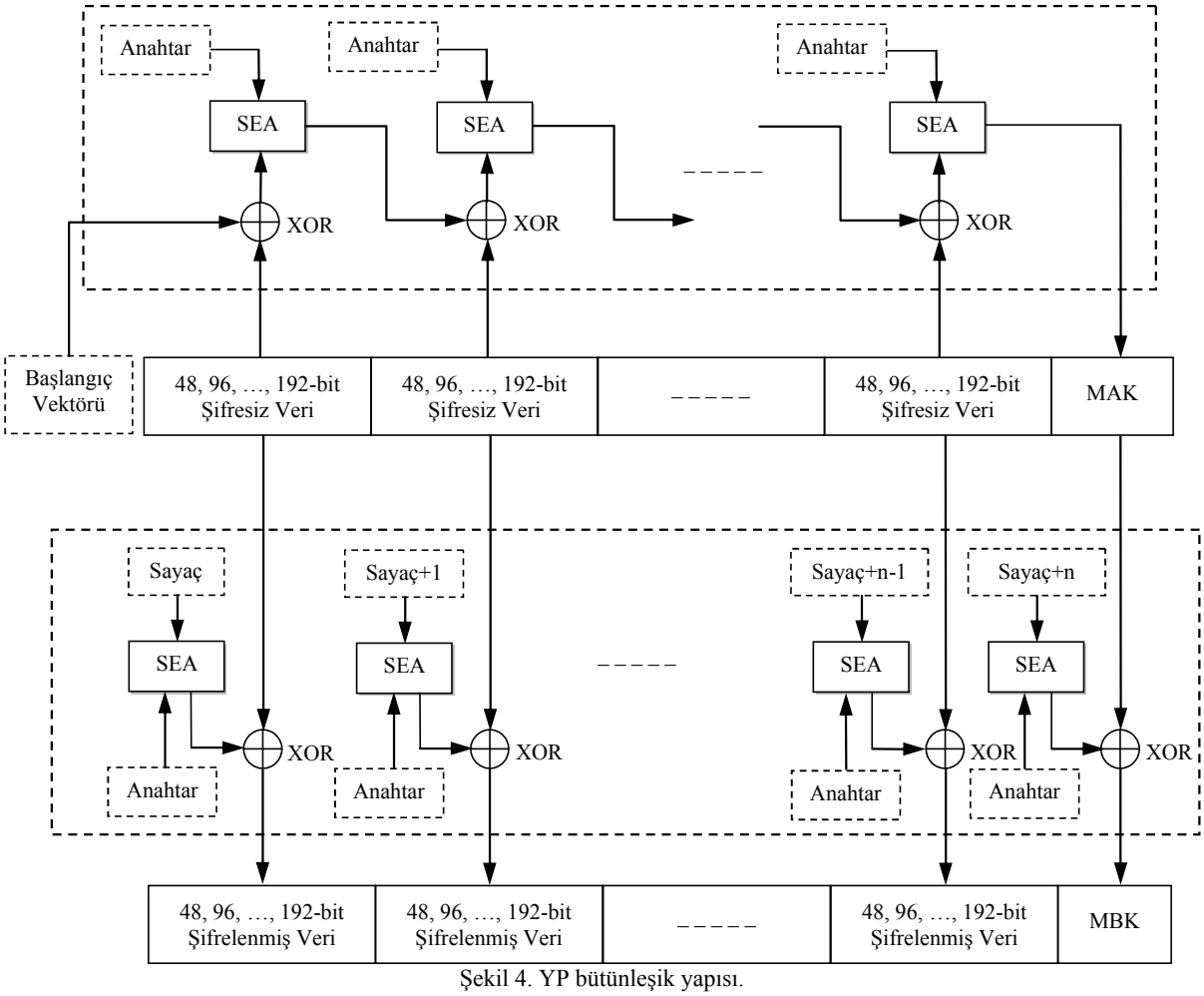
SEA ile şifrelenmiş veri blokları elde edilirken, CTR yaklaşımının bütünleşik kullanımı aşağıdaki işlemler ile gerçekleştirilmektedir:

- SEA ile şifrelenen bir sayaç değeri ve ilk şifresiz veri bloğu XOR'lanarak ilk şifrelenmiş veri bloğu elde edilmektedir.
- Sayaç değeri bir arttırılarak tekrar şifrelenir. Şifrelenmiş yeni sayaç değeri ve ikinci şifresiz veri bloğu XOR'lanarak ikinci şifrelenmiş veri bloğu elde edilmektedir.
- Bu süreç, tüm veri blokları bitinceye kadar tekrar edilmektedir.
- Son olarak, CBC–MAC yaklaşımı kullanılarak elde edilen MAK değeri ve şifrelenmiş en son sayaç değerinin (Sayaç+n) XOR'lanmasıyla Mesaj Bütünlük Kodu (MBK) elde edilmektedir.

Böylece alıcısına (hedefe) iletilmeden önce hem veri hem de pakete eklenen MAK değeri şifrelenmiş olmaktadır. Bu iki yöntemin SEA ile bütünleşik kullanımı, yeni geliştirilen YP'nin, TinySEC ve LLSP protokollerinden kanıtlanabilir ve oldukça üst derecede güvenli olduğunu analitik bir yaklaşımla doğrulamaktadır. Ayrıca bu yöntemlerle birlikte veri gizliliği, asıllaması ve bütünlüğüne ek olarak, şifreleme için kullanılan sayaç değeri tekrar gönderme saldırılarını da önlemektedir.

3.4. Önerilen YP'nin Geçerliliği ve Değerlendirmesi

KAA güvenlik protokollerinin değerlendirmesinde oldukça önemli olan bellek kullanım ve enerji tüketim ölçütleri, önerilen YP ile LLSP ve TinySEC nicel karşılaştırmasında da esas alınmaktadır. Güvenlik düzeyinin niteliği açısından ise özellikle içermekte olduğu SEA ile CTR ve CBC–MAC yaklaşımlarının bütünleşik kullanımı, önceki bölümlerde detaylandırıldığı gibi, YP'yi karşılaştırmada kullanılan bu iki geleneksel güvenlik protokolüne kıyasla hâlihazırda oldukça üstün kılmaktadır. Bu tür protokollerde, güvenlik ve veri güvenilirlik düzeylerini belirleyen somut ve sayısal (ölçülebilir) bir kıstas bulunmamasına bağlı olarak, bu bölümde önerilen çalışmanın nitelik kıyaslamasının üzerinde detaylıca durulmamaktadır (1).



Şekil 4. YP bütünleşik yapısı.

Örnek KAA uygulamalarında da kullanılabilecek YP, TinySEC ve LLSP'nin bellek kullanım ve enerji tüketim değerlerini elde edebilmek için AVRStudio ve WinAVR yazılımları kullanılmış bulunmaktadır. AVRStudio, ATMEL firması tarafından üretilen ve ATMEL AVR mikrodenetleyiciler için Assembly ve C dillerinde programların yazılarak derlenebildiği bir geliştirme ve benzetim aracıdır. KAA uygulamalarında yaygın olarak tercih edilen Micaz kablosuz algılayıcı düğümleri, 128 Kbayt kod belleği, 4 Kbayt veri belleği ve 16 MHz hızında çalışan ATMEGA 128L mikrodenetleyicisi içermektedir. Micaz özellikleri esas alınarak, sunulan bu çalışmada gerçeğe yakın sonuçlar elde edebilmek amacıyla YP, TinySEC ve LLSP'nin, AVRStudio ve WinAVR yazılımlarıyla derlenerek benzetimleri gerçekleştirilmiş bulunmaktadır. Sonuçların anlamlı ve karşılaştırmalı değerlendirilebilmesi için üç protokolde de işlem gören veri boyutu sabit ve eşit (768 bit) kabul edilmektedir.

SEA işlem sürelerinin başarım karşılaştırmasının anlamlı ve kolay olması için $SEA_{(192,192)}$, $(SEA_{(96,96)}+(CTR+CBC–MAC))^{YP}$ ve $(SEA_{(192,192)}+(CTR+CBC–MAC))^{YP}$ uygulamalarına ait şifreleme ve şifre çözme toplam süreleri $SEA_{(96,96)}$'ya göre normalize edilerek sunulmaktadır. Normalize işlemi yapılırken, $SEA_{(96,96)}$ uygulamasına ait şifreleme ve şifre çözme toplam süresi "1 saniye" kabul edilerek, $SEA_{(192,192)}$, $(SEA_{(96,96)}+(CTR+CBC–MAC))^{YP}$ ve $(SEA_{(192,192)}+(CTR+CBC–MAC))^{YP}$ şifreleme ve şifre çözme toplam süreleri nispî olarak yeniden hesaplanmaktadır. Örneğin; şifreleme ve şifre çözme toplam süreleri $SEA_{(96,96)}$ için 5,5 ms ve $(SEA_{(96,96)}+(CTR+CBC–MAC))^{YP}$ için 10,3 ms kabul edilsin. Bu durumda, $SEA_{(96,96)}$'ya ait şifreleme ve şifre çözme toplam süresine göre normalize $(SEA_{(96,96)}+(CTR+CBC–MAC))^{YP}$ şifreleme ve şifre çözme toplam değeri 1,87 (1,87=10,3/5,5) olarak hesaplanır. Diğer bir ifadeyle, $(SEA_{(96,96)}+(CTR+CBC–MAC))^{YP}$ uygulaması için $SEA_{(96,96)}$'ya kıyasla yaklaşık olarak 1,87 kat daha fazla gecikme görülmektedir.

YP için uyarlanan veri güvenilirliği arttırılmış SEA şifreleme algoritması karşılaştırmalı başarım sonuçları Tablo 1'de sunulmaktadır. $(SEA_{(96,96)}+(CTR+CBC–MAC))^{YP}$ uygulamasının şifreleme ve şifre çözme toplam süresi $SEA_{(96,96)}$'ya kıyasla 1,92 kat daha fazlayken bu değer $SEA_{(192,192)}$ uygulaması için 2,50 ve $(SEA_{(192,192)}+(CTR+CBC–MAC))^{YP}$ uygulaması için ise 4,68 katına çıkmaktadır. Önerilen protokolde güvenlik düzeyini arttırıcı ilave işlevler şifreleme ve şifre çözme sürelerini de göreceli olarak arttırmaktadır.

Tablo 1. YP için uyarlanan veri güvenilirliği arttırılmış SEA işlem süreleri.

	Normalize[nz] Şifreleme ve Şifre Çözme Toplam Süresi
$SEA_{(96^{vb},96^{ab})}$	1^{nz}
$SEA_{(192,192)}$	2,50
$SEA_{(96,96)}+(CTR+CBC–MAC)^{YP}$	1,92
$SEA_{(192,192)}+(CTR+CBC–MAC)^{YP}$	4,68

[nz]: Tablodaki diğer değerler, standart $SEA_{(96,96)}$ toplam şifreleme ve şifre çözme süresi "1 saniye" esas alınarak normalize edilmiş sonuçlardır.
[vb]: Veri blok boyutu (bit).
[ab]: Anahtar boyutu (bit).

Tablo 2'de YP ve LLSP'nin, TinySEC ile normalize edilen bellek kullanım değerleri karşılaştırmalı olarak görülmektedir. 96-bit veri blok/anahtar boyutlu YP'nin bellek kullanım değeri, standart TinySEC protokolüne kıyasla 1,57 kat daha fazlayken, bu değer 192-bit veri blok/anahtar boyutlu (oldukça yüksek güvenlik düzeyinde) YP protokolü için 1,78'e çıkmaktadır. Benzer bir şekilde standart LLSP için değerlendirme gerçekleştirildiğinde ise bellek kullanım miktarının 2,26 kat arttığı sonucuna ulaşılmaktadır. Geliştirilen ve içerdiği yeni yaklaşımlara bağlı olarak güvenlik düzeyi oldukça üst düzeyde bulunan YP protokolü ile TinySEC protokolü karşılaştırıldığında bellek kullanımda ortaya çıkan bu artışın, genel olarak KAA düğümlerine nispî olarak aşırı bir yük getirmediği değerlendirilmektedir.

Tablo 2'de ayrıca YP ve LLSP'nin, TinySEC ile normalize edilen enerji tüketim değerleri karşılaştırmalı olarak sunulmaktadır (1). 96-bit veri blok/anahtar boyutlu YP'nin enerji tüketim değerinin, TinySEC protokolüne kıyasla az da olsa düştüğü görülmektedir. Bu değer 192-bit veri blok/anahtar boyutlu YP protokolü için 2,14 kat yükselmektedir. Benzer bir yaklaşımla LLSP için yapılan değerlendirmede ise enerji tüketim değerinin 12,01 kat arttığı sonucuna ulaşılmaktadır. YP'nin iletişim güvenlik düzeyini ve veri güvenilirliğini dinamik olarak oldukça üst düzeye çıkarmakla birlikte, TinySEC ile kıyaslandığında enerji tüketiminin çok fazla artmadığı görülmektedir. Ayrıca diğer geleneksel yöntem olan LLSP'nin basit ölçekte bir güvenlik iyileştirmesi getirmesine rağmen, TinySEC'e kıyasla enerji tüketiminin çok yüksek düzeyde ortaya çıkması da dolaylı olarak YP'nin üstünlüğünü kanıtlamaktadır. Düğümlerde protokollerin çalışması ile tüketilen enerji değerleri ve toplam çalışma süreleri (şifreleme ve şifre çözme) doğru orantılı olarak değişmektedir. Dolayısıyla, bu bölümde ayrıca çalışma süresi karşılaştırması yapmaya gerek görülmemiştir.

Tablo 2. YP ile geleneksel protokollerin enerji tüketim ve bellek kullanım karşılaştırması.

	Normalize[nz] Bellek Kullanım Değeri	**Normalize[nz] Enerji Tüketim Değeri**
$TinySEC_{(64,80)}$	1^{nz}	1^{nz}
$LLSP_{(128,128)}$	2,26	12,01
$YP_{(96,96)}$	1,57	0,88
$YP_{(192,192)}$	1,78	2,14

[nz]: Tablodaki diğer değerler, geleneksel $TinySEC_{(64,80)}$ bellek kullanım değeri "1 bayt" ve enerji tüketim değeri "1 joule" esas alınarak normalize edilmiş sonuçlardır.

Elde edilen sonuçlardan genel olarak anlaşılmaktadır ki güvenlik düzeyini arttırıcı tüm ek işlevler, beklenildiği gibi uygulamaların toplam çalışma sürelerini (şifreleme/şifre çözme) olumsuz etkilemektedir (1). Bu durum, paralelinde özellikle enerji tüketim göstergesinde önemli bir artışa yol açmaktadır. Tüm bileşenleriyle genel bir KAA uygulaması için düşünüldüğünde, bu artışın özellikle kablosuz iletişim (RF) için gerekli enerji miktarından oldukça küçük kalması gerçeği, önerilen YP'nin kullanılabilirliğini desteklemektedir.

4. SONUÇ

KAA düğümleri sınırlı kaynaklara (hesaplama/bellek kapasitesi) ve enerjiye sahip olduklarından, geleneksel ağlarda kullanılan güvenlik protokollerinin doğrudan KAA'lara uygulanması aşırı işlem yükü getirmektedir. Bu konuda literatürde sunulan çalışmalar, genellikle enerjiyi en verimli şekilde kullanmayı hedefleyen KAA güvenlik protokollerinden oluşmaktadır. Ancak askeri ve sağlık uygulamaları gibi bazı hassas ortamlarda, kısıtlı enerji kaynaklarının etkin kullanımından çok, iletilen veri güvenilirliğinin (doğruluğunun) garanti edilmesi daha önemli olmaktadır.

Değişik ve giderek artan uygulama alanları da dikkate alındığında, KAA düğümleri tarafından iletilen verilerin doğruluğu, bütünlüğü ve gizliliği, ancak iletişim güvenliği ve veri güvenilirliği arttırılmış yeni bir güvenlik protokolü geliştirilerek sağlanabilir. Önerilen YP'de özellikle sınırlı kaynaklar için tasarlanmış bir simetrik blok şifreleme algoritması olan SEA ile protokolün veri güvenilirliğini arttırmak için CTR ve CBC–MAC yaklaşımları bütünleşik olarak kullanılmaktadır. SEA algoritması ve CTR yaklaşımı ile veri gizliliği ve tazeliği sağlanırken SEA algoritması ve CBC–MAC yaklaşımı ile veri asıllaması/bütünlüğü temin edilmektedir. Böylece KAA uygulamaları için dinamik olarak belirlenebilen oldukça yüksek güvenlikli iletişim imkânı, bellek kullanımda ve özellikle enerji tüketimde geleneksel çözümlere kıyasla önemsiz bir oranda artış gerçekleşmektedir.

KAA uygulamalarında, veri güvenilirliğini arttırmak için eklenen yaklaşımların toplam çalışma süresi, bellek kullanımı ve enerji tüketim miktarlarını arttırması beklenen bir sonuçtur. Bu bakımdan uygulamaların ihtiyaçlarının iyi tespit edilmesi oldukça önemlidir. Zira geniş ölçekli basit bir çevre ya da endüstriyel KAA uygulamasında güvenlik çok fazla önem taşımazken enerji tüketiminin büyük önemi bulunmaktadır. Diğer yandan, askeri ve sağlık uygulama alanlarında ise güvenlik büyük önem taşırken, algılayıcı düğüm enerji tüketimi, nispeten göz ardı edilebilir bir gösterge olarak değerlendirilmektedir ki bu gerçek önerilen YP'nin kullanılabilirliğini desteklemektedir.

5. KAYNAKLAR

1. Bandırmalı N., Ertürk İ., KAA'lar için Güvenilirliği Arttırılmış Güvenlik Protokolü, 3rd International Conference on Application of Information and Communication Technologies, 1–5, Azerbaycan, Bakü, 14–16 Ekim 2009.
2. Akyildiz I. F., Su W., Sankarasubramaniam Y., Cayirci E., Wireless Sensor Networks: Survey, Computer Networks, Cilt 38, No 2, 393–422, 2002.
3. Perrig A., Stankovic J., Wagner D., Security in Wireless Sensor Networks, Communication of the ACM, Cilt 47, No 6, 53–57, 2004.
4. Bandırmalı N., Çeken C., Ertürk İ., Bayılmış C., Skipjack Şifreleme Algoritması Kullanarak Gecikme Duyarlı ve Enerji Etkin Kablosuz Algılayıcı Ağ Güvenlik Hizmeti, Elektrik ve Elektronik ve Bilgisayar Mühendisliği Sempozyumu, ELECO 2008, Bursa, 152–157, 26–30 Kasım 2008.
5. Perrig A., Szewczyk R., Wen V., Culler D., Tygar J.D., SPINS: Security Protocols for Sensor Networks, Wireless Networks, Cilt 8, No 5, 521–534, 2002.
6. Karlof C., Sastry N., Wagner D., TinySEC: A Link Layer Security Architecture for Wireless Sensor Networks, 2nd ACM Confrerence on Embedded Networked Sensor Systems, SENSYS 2004, Maryland, USA, 162–175, 03–05 November 2004.
7. Ren J., Li T., Aslam D., A Power Efficient Link Layer Security Protocol (LLSP) for Wireless Sensor Networks, Military Communications Conference, MILCOM 2005, New Jersey, USA, Cilt 2, 1002–1007, 17–20 October 2005.
8. Lighfoot L.E., Ren J., Li T., An Energy Efficient Link Layer Security Protokol for Wireless Sensor Networks, IEEE Electro/Information Technology Conference, EIT 2007, IL, USA, 233–238, 17–20 May 2007.
9. Samiah A., Aziz A., Ikram N., An Efficient Software Implementation of AES-CCM for IEEE 802.11i Wireless Standard, 31st Annual International Computer Software and Applications Conference**,** COMPSAC'07, Beijing, China, 689–694, 23–27 July 2007.
10. Jonsson J., On the Security of CTR+CBC-MAC, Selected Areas in Cryptography, Cilt 2595, Editör: Nyberg K., Heys H., Springer LNCS, 76–93, 2003.
11. Wheeler D.J., Needham R., TEA, a Tiny Encryption Algorithm, 2nd Fast Software Encryption International Workshop**,** FSE'95, Cilt 1008, Springer LNCS, 363–366, 1995.
12. Yuval G., Reinventing the Travois: Encryption/MAC in 30 ROM Bytes, 4th Fast Software Encryption International Workshop**,** FSE'97**,** Cilt 1267, Springer LNCS, 205–209, 1997.

13. Standaert F.-X., Piret G., Gershenfeld N., Quisquater J.-J., SEA: A Scalable Encryption Algorithm for Small Embedded Applications, Smart Card Research and Advanced Applications**,** Cilt 3928, Editör: Domingo-Ferrer J., Posegga J., Schreckling D., Springer LNCS, 222–236, 2006.
14. Macé F., Standaert F.-X., Quisquater J.-J., FPGA Implementation(s) of a Scalable Encryption Algorithm, IEEE Transactions on Very Large Scale Integration (VLSI) Systems, Cilt 16, No 2, 212–216, 2008.
15. Bandirmali N., Erturk I., Ceken C., Securing Data Transfer in Delay-sensitive and Energy-aware WSNs Using the Scalable Encryption Algorithm, International Symposium on Wireless and Pervasive Computing, ISWPC'09, Melbourne, Australia, 1–6, 11–13 February 2009.