Gazi Üniv. Müh. Mim. Fak. Der.
Cilt 28, No 3, 587-594, 2013

Journal of the Faculty of Engineering and Architecture of Gazi University
Vol 28, No 3, 587-594, 2013

KABLOSUZ ÇOKLU ORTAM ALGILAYICI AĞLARINDA DAMGALAMA İLE GÜVENLİ VERİ KÜMELEME***

Ersin ELBAŞI*, Suat ÖZDEMİR**
*Türkiye Bilimsel ve Teknolojik Araştırma Kurumu, ANKARA
**Gazi Üniversitesi, Mühendislik Fakültesi, Bilgisayar Mühendisliği Bölümü, ANKARA
ersin.elbasi@tubitak.gov.tr, suatozdemir@gazi.edu.tr

(Geliş/Received: 16.01.2012; Kabul/Accepted: 12.04.2013)

ÖZET

Kablosuz Çoklu ortam Algılayıcı Ağları (KÇAA) birden çok algılayıcı ünitesine sahip algılayıcı düğümlerinin oluşturduğu ısı, nem v.b. basit veriler dışında video ve fotoğraf gibi verilerin de toplanabildiği bilgi toplama ağlardır. KÇAA'lar genellikle askeri yada sivil izleme/takip uygulamalarında kullanıldıkları için bu ağlarda güvenliğin sağlanması bir zorunluluktur. Geleneksel kablosuz algılayıcı ağlarında olduğu gibi, KÇAA'ları oluşturan algılayıcı düğümleri de enerji ve bantgenişliği açısından oldukça kısıtlıdır. Bu nedenle KÇAA'larda veri toplama işlemi hem güvenli hem de enerji etkin bir şekilde yapılmak zorundadır. Bu çalışmada KÇAA'larda veri toplama işlemini güvenli ve enerji etkin hale getirecek sayısal damgalama tabanlı veri kümeleme protokolü geliştirilmiştir. Geliştirilen protokolde algılayıcılar gizlemek istedikleri verileri fotoğraf verisi içine saldırılara karşı dayanıklı bir algoritma ile gömmekte ve bu damgalanmış veriler ise veri kümeleyiciler tarafından kümelenmektedir. Performans analizi ve benzetim çalışmaları, önerilen sistemin güvenli veri kümeleme sağlarken veri iletim miktarında da azalmaya neden olduğunu göstermektedir.

Anahtar kelimeler: Heterojen kablosuz algılayıcı ağlar, gizli veri kümeleme, güvenlik, damgalama

SECURE DATA AGGREGATION IN WIRELESS MULTIMEDIA SENSOR NETWORKS VIA WATERMARKING

ABSTRACT

Wireless Multimedia Sensor Networks (WMSNs) consist of a large number of sensor nodes that have multiple sensing units. Unlike traditional wireless sensor networks, WMSNs are used to collect multimedia data such as video or image. As WMSNs are employed by military or civil surveillance/tracking applications security of these Networks must be ensured. As in traditional wireless sensor networks, sensor nodes in WMSNs are resource limited. Hence, data collection in WMSNs must be performed in an energy efficient way. In this study, a watermarking based protocol that ensures secure and energy efficient data collection in WMSNs is proposed. In the proposed protocol, sensor nodes embed the secret data into image data using an attack resilient watermarking algorithm and data aggregators aggregate the image data. Performance analysis and simulations show that the proposed protocol ensures secure data aggregation and reduces the amount of data transmission.

Keywords: Heterogeneous wireless sensor networks, concealed data aggregation, security, watermarking

1. GİRİŞ (INTRODUCTION)

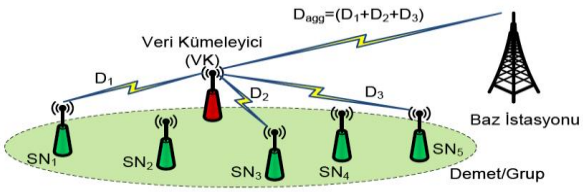
Kablosuz algılayıcı ağ (KAA)'lar kullanılacakları alana hızla atılabilen, esnek, kendi kendine organize olarak ağ altyapısını kurabilen çok sayıda algılayıcı düğümünden oluşan, oldukça yeni bir teknolojidir [1]. Her bir algılayıcı düğüm bir ya da daha fazla algılayıcı, küçük miktardaki işlemleri gerçekleştirebilen işlem birimi, yakın mesafedeki düğümler ile haberleşmeyi sağlayan alıcı-verici ile çok kısıtlı bir güç biriminden oluşur. Düşük kurulum ve işletim maliyetleri sebebiyle, KAA'lar birçok alandaki (sağlık, askeri, çevresel vb.) bilgi toplama, izleme ve takip gibi uygulamalarda kullanılmaktadır. Donanım alanındaki hızlı gelişmeler tek bir algılayıcı düğümünün görsel ve işitsel birden çok bilgi toplama

modülüne sahip olmasına olanak tanımıştır. Örneğin, Cyclops resim alma ve işleme modülü Crossbow MICA2 düğümlerine kolaylıkla eklenebilmektedir [2]. Bu hızlı gelişmeler KAA literatüründe Kablosuz Çoklu ortam Algılayıcı Ağ (KÇAA) kavramının ortaya çıkmasına neden olmuştur. KÇAA'lar KAA'lara göre daha gelişmiş algılayıcı düğümlerinden oluşan, her düğümün birden çok çeşit veri toplayabildiği ve bu verilerin işlenmesi ile daha karmaşık karar verme işlemlerinin yapılabildiği bir KAA türüdür [3].

Özellikle askeri izleme uygulamalarında KÇAA'lar erişilmesi zor, uzak ve tehlikeli bölgelere genelde bir hava aracı yardımı ile atıldıklarından, çoklu ortam algılayıcı düğümlerinin bataryalarının değiştirilmesi çok zor hatta çoğu zaman olanaksızdır. Bu nedenle KÇAA'lar başlıca görevleri olan veri toplama, iletme ve işlenme görevlerini enerji etkin bir şekilde yaparak ağın kullanım ömrünü uzatmak zorundadırlar. Genelde çok sayıda algılayıcı düğümünden oluşan KÇAA'larda, algılayıcılar kendilerini gruplara ayırarak enerji tüketimlerini azaltırlar [1,3]. Bu gruplama işleminin amacı her grupta bir algılayıcıyı grup lideri olarak seçerek veri toplama ve aktarım görevlerini seçilen grup lideri üzerinden yapmaktır (Şekil 1). Güç kaynakları sınırlı olan algılayıcılardan oluşan KÇAA'larda toplanılan veriyi enerji etkin bir şekilde özetleyebilmek için veri kümeleme çok önemli bir gerekliliktir [2]. Her bir algılayıcının verisini ayrı ayrı baz istasyonuna göndermektense, bir grup içerisindeki algılayıcı verilerinin grup lideri tarafından toplanarak özetlenmesi/kümelenmesi yani artık verinin ayıklanarak verinin kümelenmesi algılayıcıların enerji tüketimlerini düşürür ve KÇAA'nın kullanım ömrünü artırır [2,4].

Veri kümeleme gerekliliğinin yanı sıra, özellikle hassas askeri KÇAA uygulamalarında, algılayıcılardan baz istasyonuna gizli veri aktarımını sağlayan güvenlik protokolleri mutlaka kullanılmalıdır. Ancak, algılayıcıların düşük işlemci ve radyo kapasiteleri geleneksel güvenlik protokollerinin KÇAA'larda uygulanmasına olanak tanımaz [4,24]. Dahası, algılayıcıların fiziksel güvenlikleri sağlanamadığından, algılayıcılar her an kötü niyetli kişilerce ele geçirilip, yeniden programlanabilir [1]. Bu tip algılayıcılar "ele geçirilmiş algılayıcılar" olarak tanımlanır ve genelde ağdaki diğer algılayıcılar ele geçirilmiş algılayıcıları fark edemez [1]. Bu sebeplerden dolayı, KÇAA'larda kullanılacak olan güvenlik protokolleri bu ağların kendilerine has özellikleri ve "ele geçirilmiş algılayıcılar" göz önüne alınarak tasarlanmış olmalıdır [4].

KÇAA'larda hem veri kümeleme hem de veri gizliliği vazgeçilmez unsurlar olmasına rağmen, bu iki unsurun bir arada uygulanabilmesi çok zordur [2,4]. Veri kümeleyicilerin aldıkları her veriye açık olarak ulaşma ihtiyacına karşın veri gizliliğini sağlayan protokoller verinin gönderildiği alıcı (baz istasyonu) dışında başka hiçbir algılayıcının verinin şifresini çözmesini istememektedirler [2,4]. Çok farklı amaçlara sahip olmaları nedeni ile, veri şifrelemeye dayalı klasik güvenlik algoritmaları ve veri kümeleme algoritmalarının bir arada kullanılması mümkün değildir [2]. Bu nedenle hem veri gizliliğini hem de verinin kümeleyiciler tarafından işlenebilmesini sağlayacak yeni yöntemlere ihtiyaç vardır. Bu çalışmada KÇAA'larda veri kümelemeyi etkilemeden veri gizliliğini sağlayacak sayısal damgalama tekniklerine dayalı bir güvenli veri kümeleme protokolü geliştirilmiştir. Önerilen Damgalama Tabanlı Güvenli Veri Kümeleme (DTGVK) protokolünde algılayıcılar tarafından toplanan ve gizli kalması gereken veriler yine algılayıcılar tarafından elde edilmiş olan imge dosyalarının içine sayısal damgalama ile gömülmektedir.



Şekil 1. Veri kümeleme **(Figure 1.** Data aggregation**)**

Veri kümeleyiciler algılayıcı düğümlerinden içine gizli veri gömülmüş olan bu imge verisini toplamakta ve bu veriler Huffman kodlama metodu ile kümelenerek baz istasyonuna iletilmektedir. İmgelerin içerisine veri gömme işlemi algılayıcı düğümü ve baz istasyonu arasında paylaşılan gizli anahtara bağlı yapıldığından, gizli anahtar elde edilmeden veri kümeleyicilerin yada kötücül düğümlerin resim içerisindeki veriyi elde etmeleri mümkün değildir. Dahası kullanılan sayısal damgalama yöntemi damgayı silmeye, hasar vermeye yönelik ya da algoritmayı çalışamaz hale getirmek için yapılan saldırılara karşı dayanıklıdır. Bu sayede önerilen protokol veri gizliliğini sağlarken aynı zamanda veri kümelemeye izin verdiğinden, ağda gönderilen veri miktarını azaltarak KÇAA kullanım ömrünü artırmaktadır. Önerilen protokolün güvenlik analizi yapılmış ve ağ veri iletim trafiğine olan pozitif etkisi yapılan deneysel çalışmalar ile gösterilmiştir.

Ağ içerisinde aktarılan veri miktarını düşürüp enerji tasarrufu sağlamasının yanı sıra, KAA'larda veri kümeleme protokolleri doğruluk hassasiyeti yüksek olmayan algılayıcı verilerini birleştirerek doğruluk derecesi yüksek veriye ulaşılmasını da sağlar [4]. Enerji etkinliğinin artırılması ve ağ kullanım ömrünün artırılması için KAA'larda veri kümeleme kaçınılmaz bir gerekliliktir. Aynı şekilde, veri gizliliğinin sağlanması KAA'ların birçok uygulama alanı için vazgeçilmezdir [1]. Güvenlik problemlerini en aza indirebilmek için gönderilen verinin gönderici tarafından şifrelenmesi ve sadece baz istasyonu

tarafından şifrenin çözülmesi istenir. Buna karşın veri kümeleme işlemi verinin gönderildiği yol üzerindeki algılayıcıların veriyi görerek kümeleme yapmalarını gerektirir. Birbirine zıt bu iki amaç, veri gizliliği ve veri kümeleme protokollerinin bir arada tasarlanmasını ve geliştirilmesini gerektirmektedir [2]. Bu gereklilik birçok araştırmacıyı güvenli veri kümeleme metotları üzerinde çalışmaya zorlamıştır [2,4,5,6,7,8]. Veri kümeleme için verilerin her düğümde çözülüp tekrar şifrelenmesi gerektiğinden, bu çalışmalarda veri gizliliği ve veri kümeleme ancak sıçrama bazında (hop-by-hop) gerçekleştirebilir. Hem uçtan uca veri gizliliğini hem de veri kümelemeyi sağlayabilmek için homomorfik şifrelemeye dayalı veri kümeleme yöntemleri önerilmiştir [9-14]. Homomorfik şifrelemeye dayalı çalışmalar güvenli veri kümeleme açısından oldukça başarılı sonuçlar verseler dahi, yüksek hesaplama maliyeti nedeniyle her zaman kullanılmaları mümkün değildir. [15]'de önerilen çalışmada ise orijinal veri yerine regresyon analizi ve polinom ifadeler kullanarak güvenli veri kümeleme işlemi gerçekleştirilmiş bu sayede hem enerji verimliliği hem de güvenlik sağlanabilmiştir.

İmgelerin damgalanması konusunda ise son yıllarda oldukça başarılı çalışmalar yapılmış, özellikle logo ya da gürültü şeklindeki damgalar imgelere gömülmüştür. Uzamsal alanlarda yapılan çalışmalar Cox [16] ile başlamış, ancak bazı saldırılar karşısında dayanaksız olan bu algoritmalar önce Piva'nin [17] Ayrık Kosinüs Dönüşümü (AKD) alanında yapmış olduğu çalışmalarla, daha sonra Dugad'in [18] ve Zhu'nun [19] Ayrık Dalgacık Dönüşümü (ADD) alanında yapmış olduğu çalışmalarla hem daha güvenilir hem de saldırılara karşı daha dirençli olmuş ve çalışmalardan iyi sonuçlar alınmıştır. Eskicioğlu ve Elbaşı [20,21] yapmış olduğu çalışmalarda, çeşitli alanlara dönüştürülen imgede düşük ve yüksek bantlarda yapılan gömme işlemi; bazı saldırılarda yüksek frekanslarda, bazı saldırılarda ise düşük frekanslarda daha güvenilir sonuçlar vermiştir.

Makalenin geri kalan kısmı şu şekilde organize edilmiştir. 2. Bölümde sistem modeli ve kullanılan damgalama metodu ile ilgili ön bilgiler verilmiştir. 3. Bölümde önerilen veri kümeleme protokolü detaylı olarak anlatılmıştır. 4. Bölümde güvenlik ve performans analizi sonuçları verilmiştir. Sonuç ve çıkarımlar ise 5. Bölümde yer almaktadır.

2. SİSTEM MODELİ (SYSTEM MODEL)

Bu bölümde çalışmada yapılan kabuller ve kullanılan teknikler ile ilgili ön bilgi verilmiştir.

2.1 Ağ ve tehdit modeli (Network and threat model)

Bu çalışmada gruplara ayrılmış yoğun bir şekilde hedef alana rastgele atılmış algılayıcı düğümlerinden ve kaynak açısından zengin bir baz istasyonundan oluşan statik bir KÇAA öngörülmüştür. Ağı oluşturan düğümler birden çok algılayıcı modülüne sahip olup ve her grup içinde bir düğüm veri kümeleyici olarak görevlendirilmiştir. Düğümler arasındaki enerji tüketimini dengelemek için zaman içerisinde dinamik olarak seçilen veri kümeleyiciler çevrelerindeki diğer algılayıcılardan topladıkları verileri sıkıştırıp ya da özetleyip çok zıplamalı linkler üzerinden uzaktaki bir baz istasyonuna göndermekle yükümlüdürler. Algılayıcı düğümlerinin sınırlı kaynaklara sahip oldukları kabul edilmiştir.

Kablosuz iletişimin özellikleri nedeniyle algılayıcı düğümleri tarafından gönderilen paketler, kötücül kişiler tarafından toplanabilir ve tekrar gönderilebilir. Bu gibi tekrarlama saldırılarının önlenmesi amacıyla, ağ içindeki tüm mesajlaşmalarda zaman damgaları ve rastgele bit dizileri kullanılmaktadır. Aynı şekilde, ağ içindeki bütün mesajlar şifrelenerek ve imzalanarak gönderilir. Şifrelenmiş veriler sadece baz istasyonu tarafından çözülür. Algılayıcı düğümleri izlenecek olan hedef alana gözetimsiz olarak atıldıklarından, algılayıcı düğümlerinin fiziksel güvenliğinin sağlanması mümkün değildir. Bu nedenle algılayıcı düğümleri düşman güçler/kötü niyetli kişiler tarafından ele geçirilebilir ve ağa karşı kullanılabilir [1]. Bu çalışmada önerilen veri kümeleme protokolü algılayıcı düğümlerinin ele geçirilmesini engellemekten ziyade, ele geçirilmiş düğümlerin veri kümeleme sonucunu etkilemesini önlemeyi hedeflemektedir. Ağın işleyişini engellemeyi amaçlayan yönlendirme protokollerine karşı olan saldırılar bu çalışmanın konusunun dışında kalmaktadır. Bu çalışmanın damgalama kısmında kullanılan yöntem JPEG sıkıştırma, histogram denkleştirme, süzgeçleme, tekrar boyutlandırma, Gauss gürültüsü, Gama düzeltimi, döndürme ve karşıtlık ayarı gibi çok bilinen saldırılara karşı oldukça başarılıdır.

2.2 Veri kümeleme (Data aggregation)

Çoklu ortam verilerinin kümelenmesinde en büyük/en küçük/ortalama gibi basit kümeleme fonksiyonları kullanılamamaktadır. Bu çalışmada gizli veriler imgelerin içine gömüldükleri için, imgelerin kümelenmesi amacı ile herhangi bir sıkıştırma algoritması kullanılabilir. Bu çalışmada Huffman kodlama metodu kümeleme için kullanılmıştır. Önerilen protokol imgeleri JPEG formatında elde ettiğinden, bu formatı sıkıştırmak için önce imgeler bloklara ayrılmakta ve bloklar üzerinde ayrık kosinüs dönüşümü uygulanmaktadır. Farklı algılayıcı düğümlerinden elde edilen bu veriler üzerinde Huffman kodlama uygulanarak veri kümeleme gerçekleştirilmektedir.

2.3. Sayısal damgalama (Digital watermarking)

Damgalama metodu logo ya da gürültü gibi bit sıralarının çoklu ortam elemanlarına görünür ya da görünmez şekilde gömülmesi işlemidir. Başarılı bir damgalama algoritmasından beklenen özellikler şöyle sıralanabilir. (*i*) Damga güvenli olmalı, saldırılarla kolaylıkla silinmemeli ya da elde edilmemelidir. (*ii*) Damga çıkarma algoritması güvenilir olmalı ve bütün saldırılara karşı dirençli olmalıdır. (*iii*) Veri kapasitesi yüksek olmalıdır.

Damgalama metodlarını çeşitli şekilde sınıflandırabiliriz [20,21]. TV ekranında sağ üst köşede görmüş olduğumuz kanala ait logo gözle görülen logodur. Bunun yanında gözle göremediğimiz ancak detektör kullanarak göreceğimiz logolar vardır. Eğer damga çıkarmada orijinal resmi kullanıyorsak, buna kör olmayan damgalama diyoruz. Kör damgalamada, orjinal imge ve damgaya ihtiyaç duyulmadan, sadece gizli anahtar kulanılarak damga elde edilir. Yarı-kör damgalamada ise yine orijinal imgeye ihtiyaç duyulmadan, sadece gizli anahtar ile damga kullanılarak gizli veri cıkarılır. [18,19,21].

İki türlü damga vardır. Birincisi gözle görülebilir logo şeklindeki damgalar, ikincisi ise rastgele sayı sıralarıdır (PRN). Video damgalamada özellikle zamana dayalı veri olduğu için çerçeve ortalama, çerçeve düşürme ve çerçeve değiştirme gibi saldırılar yapılmaktadır ve bu saldırılara karşı dayanıklı bir algoritma üretmek daha zordur [16,20].

3. DTGVK PROTOKOLÜ (DTGVK PROTOCOL)

Bu bölümde DTGVK protokolü detaylı olarak açıklanmıştır. DTGVK protokolü algılayıcılar tarafından verinin toplanması, gizli verinin imgeler içine gömülmesi ve verinin kümelenmesi olarak 3 aşamadan oluşmaktadır. Şekil 2 de DTGVK protokolü özetlenmektedir.

Şekil 2. DTGVK protokolü (**Figure 2.** DTGVK protocol)

3.1 Veri toplanması (Data Collection)

DTGVK protokolünde algılayıcı düğümlerinin ısı nem gibi rakamsal ölçüm değerleri ve imgeler (fotoğraflar) olarak iki tür veri topladıkları kabul edilmiştir. Bu verilerden rakamsal verinin gizli olması gerekmektedir. İmgeler ise açık bir şekilde ağ içinde gönderilebilir. Bu bağlamda her algılayıcı düğümü yaptığı ölçümlere ait rakamsal verileri elde ettiği bir imge veri içine Bölüm 4.2 de açıklanan sayısal damgalama metodu ile gömmektedir. Görsel içine gömülmüş olan gizli veri algılayıcı tarafından ve bağlı bulunduğu veri kümeleyiciye göndermektedir.

3.2 Sayısal Damgalama ile Verilerin Gömülmesi ve Çıkartılması
(Data Embedding and Extraction via Digital Watermarking)

Gizli ısı, nem v.b. rakamsal gizli verilerin algılayıcılar tarafından toplanan RGB formatındaki görüntülere gömmek için görüntü öncelikle RGB renk formatından YUV renk formatına dönüştürülür. Birincil renklerin (kırmızı, yeşil ve mavi) harmanlanması ile elde edilen renk RGB olarak adlandırılır. Y ışıklılık, U ve V ise renklilik bileşimi taşıyan renk formatı ise YUV olarak adlandırılır. RGB formatındaki görüntü aşağıda verilen yöntem ile YUV formatına dönüştürülür.

$$R,G,B,Y \in [0,1]$$
$$U \in [-0.436,0.436]$$
$$V \in [-0.615,0.615]$$
$$Y=0.299R+0.5876G+0.11B$$
$$U=-0.147R-0.289G+0.436B$$
$$V=0.615R-0.515G-0.100B$$

YUV formatına çevrilen görüntülerde Y görüntüsü tek tabaka Ayrık Dalgacık Dönüşümü (ADD) alanına çevrilir. Gizli rakamsal verileri temsil eden ikili damga dört eşit parçaya bölünerek sırasıyla LL, LH, HL ve HH bantlarına gömülür. Elde edilen katsayılar ters çevrilerek gizli rakamsal verilerin gömüldüğü görüntü elde edilir. Algılayıcı düğümleri gizli rakamsal veriyi (D) Şekil 3 de verilen damgalama algoritmasını kullanarak görselin içine gömer.

Damgalama Algoritması

Girdi: Gizli rakamsal veri (D), imge (I)
Çıktı: Gizli rakamsal veri D'yi içeren imge I_D
1: Orijinal RGB renkli I imgesini YUV'ye çevir.
2: Y imgesini iki tabaka Ayrık Dalgacık Dönüşümü (ADD) ile yeni bir alana çevir.
3: İkili damgayı eşit büyüklükteki gömme yapılacak bant sayısı kadar parçalara ayır.
4: Elde edilen her bir banttaki (LL,LH,HL ve HH) katsayılarına V_{ij} damganın bir parçasını aşağıda verildiği gibi göm.

$$V_{D,ij} = V_{i,j}^{k} + \alpha_k \times D_{i,j} \quad where \quad i = 1..n; \quad j = 1,...,m; \quad k = 1,2,3,4$$

5: ADD katsayılarını ters çevrirerek damgalanmış imge I_D'yi elde et.

Şekil 3. Damgalama algoritması (**Figure 3.** Watermarking algorithm)

Gizlenen verinin çıkartılmasında öncelikle RGB renk formatından YUV renk formatına dönüştürülür. Y imgesi tek tabaka ADD alanına çevrilir ve her bir banttan gizli veri çıkartılır. Elde edilen değerlerden önceden belirlenen eşik değerden (T) büyük olan piksel değerleri 1, diğerleri 0 a eşitlenerek gizli veri elde edilir. Damga çıkarma algoritması Şekil 4 de verilmiştir.

3.3 Veri kümeleme (Data Aggregation)

Önerilen protokolde gizli veri görseller içine gömüldüğünden klasik anlamdaki veri kümeleme metotlarının (ortalama vb.) kullanılması mümkün

değildir. Görsel veriler için yapılabilecek veri kümeleme işlemi sıkıştırma ile yapılabilmektedir. Bu nedenle bu çalışmada veri kümeleme işlemi literatürde detaylı olarak çalışılmış ve doğruluğu kanıtlanmış olan Ayrık Kosinüs Dönüşümü (AKD) ve Huffman kodlama [22] yöntemleri kullanarak yapılmıştır. Veri kümeleyici algılayıcı düğümleri tarafından toplanan her bir veriyi önce 4 parçaya böler ve her bir parça için AKD işlemi uygular. AKD işleminden elde edilen seyrek matrislerin en büyük K katsayısı K-en-büyük-kodlama algoritması kullanılarak bulunur ve matrisin geri kalan kısmı atılır. Her blok için elde edilen K katsayısı haricinde kalan diğer katsayılar atılır. Her bloğu temsil eden K katsayıları için Huffman kodlama metodu uygulanır ve veri kümeleyiciden baz istasyonuna gönderilen veri miktarı azaltılmış olur. AKD ve Huffman kodlama tekniklerinin detayları için [22] numaralı referansa başvurulabilir.

Damga Çıkarma Algoritması

Girdi: Gizli rakamsal veri D'yi içeren imge I_D
Çıktı: Gizli rakamsal veri D
1: RGB renkli I_D imgesini YUV'ye çevir.
2: Y imgesinde iki tabaka ADD uygula.
3: Damgayı her bir banttan aşağıdaki şekilde çıkart.

$$V^*_{D,ij} = (V^k_{D,ij} - V^k_{i,j})/\alpha_k \quad where \quad i = 1...n; \quad j = 1,...,m; \quad k = 1,2,3,4$$

4: Eğer $D^*_{i,j} > T$ ise $D^*_{i,j} = 1$ değilse $D^*_{i,j} = 0$

Şekil 4. Damga çıkarma algoritması
(**Figure 4.** Watermark extraction algorithm)

4. PERFORMANS ANALİZİ (PERFORMANCE ANALYSIS)

4.1 Güvenlik analizi (Security analysis)

Güvenlik analizi olarak gömülen verilere karşı yapılan saldırılara karşı sistemin dayanıklılığı ölçülmüştür. Analizde Şekil 5'te verilen ve Gazi Üniversitesi Mühendislik Fakültesinden elde edilen imgelere Şekil 6'da verilen gizli veriler ADD tekniğiyle daha önce açıklandığı gibi gömülmüştür.

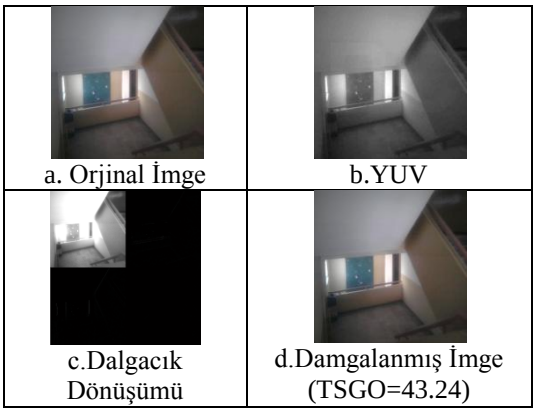
Şekil 5. Dört farklı noktadan alınmış resim verileri
(**Figure 5.** Image data taken from four different point)

Şekil 6. Gömülecek veriler (**Figure 6.** Embedding data)

Şekil 7'de sırasıyla algılayıcılar tarafından elde edilen orijinal görüntü, RGB formatında bulunan bu görüntünün YUV formatına dönüşmüş hali, Y imgesinin Ayrık Dalgacık Dönüşümlü hali ve rakamsal gizli verinin saklandığı imge verilmiştir. Elde edilen Tepe Sinyal Gürültü Oranı (TSGO) değeri damgalanmış görüntünün orijinal görüntü ile çok yakın görüntü kalitesinde olduğunu göstermektedir. TSGO gizli verinin damga olarak gömüldüğü imgenin görüntü kalitesini ölçmek için kullanılan bir yöntemdir.

$$TSGO = 20xlog_{10}(\frac{255}{OKHK})$$

OKHK orijinal imge ile verinin saklandığı imge arasındaki ortalama karesel hatanın karekköküdür.



Şekil 7. Orjinal, Gri Tonlu, ADD ve Damgalanmış Görüntüler
(**Figure 7.** Original, Gray Scale, DWT and watermarked images)

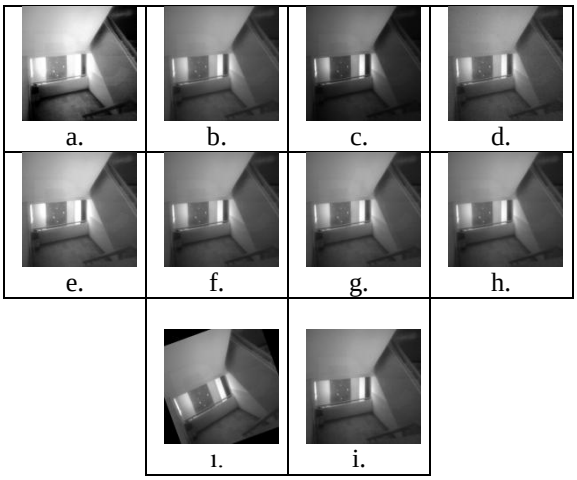
Şekil 8'de ise damgalanmış görüntüye yapılan bazı saldırılar sonucunda görüntü ve görüntü kalitesini gösteren TSGO değerleri verilmiştir. JPEG sıkıştırma, JPEG2000 sıkıştırma, histogram denkleştirme, alçak geçiren süzgeçleme, yüksek geçiren süzgeçleme, tekrar boyutlandırma, Gauss gürültüsü, Gama düzeltimi, döndürme ve karşıtlık ayarı gibi çok bilinen saldırılara karşı görüntü kalitesinde çok az bir değişim olmaktadır.

Şekil 9'da ise damgalanmış görüntüden çıkartılan gizli veriler Benzerlik Oranları (BO) ile verilmiştir. Hiçbir saldırıya uğramayan görüntüden elde edilen orijinal gizli verinin benzerlik oranı 1 dir. JPEG sıkıştırma, JPEG2000 sıkıştırma, Histogram denkleştirme, alçak geçiren süzgeçleme, yüksek geçiren süzgeçleme, tekrar boyutlandırma, Gauss gürültüsü, Gama düzeltimi, döndürme ve karşıtlık ayarı gibi saldırılardan sonra çıkartılan gizli verilerin benzerlik oranı ise 0,54 ile 0,73 arasında olup rahatlıkla ayırt edilebilir özelliktedir. Benzerlik Oranı elde edilen gizli verinin orijinal veri ile olan benzerliğini ölçer.

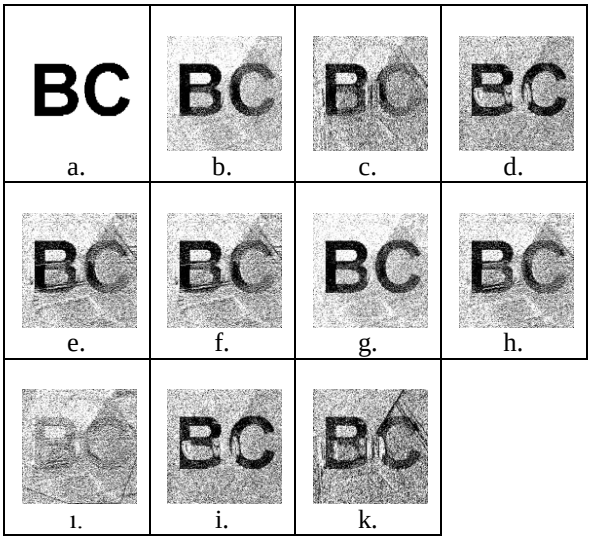
$$BO = \frac{B}{B+F}$$

Bu karşılaştırılan ikili verilerde benzer olan toplam

piksel sayısını, F ise farklı olan toplam piksel sayısını vermektedir.

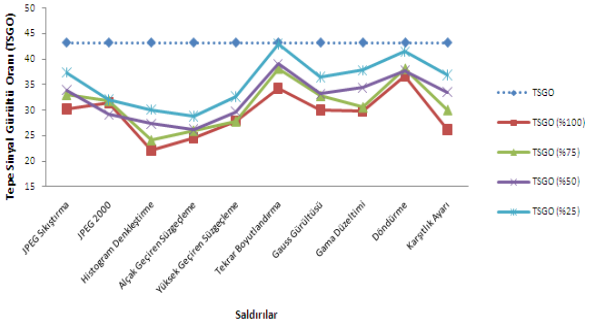


Şekil 8. Saldırılardan sonra veri ve TSGO değerleri a. JPEG Sıkıştırma (TSGO = 30.23), b. JPEG 2000 Sıkıştırma (TSGO = 31.48),c. Histogram Denkleştirme (TSGO = 22.14) , d. Alçak Geçiren Süzgeçleme (TSGO = 24.59), e. Yüksek Geçiren Süzgeçleme (TSGO = 27.91), f. Tekrar Boyutlandırma (TSGO = 34.27), g. Gauss Gürültüsü (TSGO = 30.05), h. Gama Düzeltimi (TSGO = 29.78), ı. Döndürme (TSGO = 36.71), i. Karşıtlık Ayarı (TSGO = 26.17)
(**Figure 8.** Image data and PSNR values after attacks)

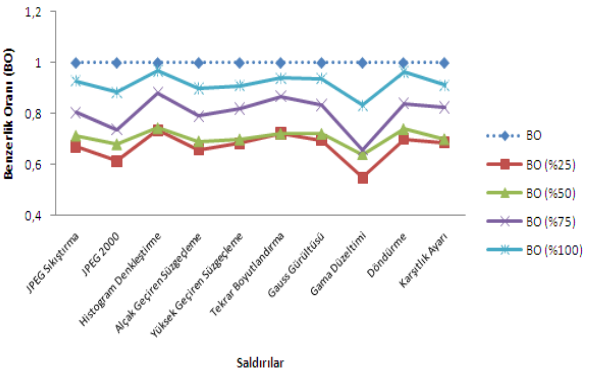


Şekil 9. Saldırılardan sonra çıkartılan damga (logo) ve benzerlik oranları (BO) a. Orijinal (BO=1.0000), b. JPEG Sıkıştırma (BO=0.6712) , c. JPEG 2000 Sıkıştırma (BO=0.6147), d. Histogram Denkleştirme (BO=0.7352), e. Düşük Geçirme Süzgeçleme (BO=0.6594), f. Yüksek Geçirme Süzgeçleme (BO=0.6841), g. Tekrar Boyutlandırma (BO=0.7231), h. Gauss Gürültüsü (BO=0.6956), ı. Gama Düzeltimi (BO=0.5497), i. Döndürme (BO=0.7002), k. Karşıtlık Ayarı (BO=0.6874) (**Figure 9.** Extracted watermark(logo) and similarity ratios after attacks)

Başarılı bir damgalama algoritmasında gömülen bit sayısı da oldukça önemlidir. Bit sayısı arttıkça damgalanan imgenin TSGO değeri düşük olacak ve verimiz saldırılara karşı daha dayanıksız olacaktır. Şekil 10'da de verilen grafikte gizli sayısal verinin tamamı gömüldüğünde ve sırasıyla %75, %50, %25 küçültüldüğünde saldırılar sonrası elde edilen TSGO değerleri verilmiştir. Sayısal gizli veri %25 ine kadar küçültülerek imge içerisine gömülmesi sonucunda elde edilen TSGO değerleri damgalanmamış orijinal imgenin TSGO değerine daha yakın olup, görüntü kalitesi daha yüksektir. Şekil 11'de ise aynı yöntemle yapılan damgalama sonucunda bazı saldırılar sonrası elde edilen Benzerlik Oranı (BO) değerleri verilmiştir.

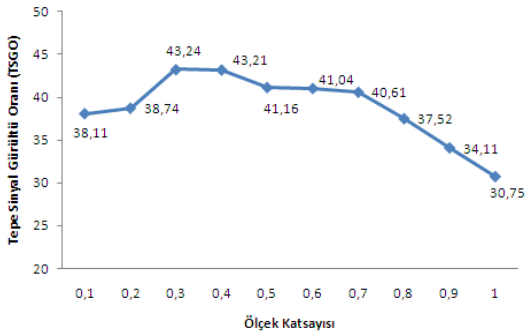


Şekil 10. Farklı boyutlardaki sayısal gizli verilerin gömülmesi sonucu elde edilen görüntü kalite ölçüleri (**Figure 10.** Image quality metrics of embedded different size of digital secret data)



Şekil 11. Farklı boyutlardaki sayısal gizli verilerin gömülmesi sonrası çıkartılan BO değerleri (**Figure 11.** SR values of embedded different size of digital secret data)

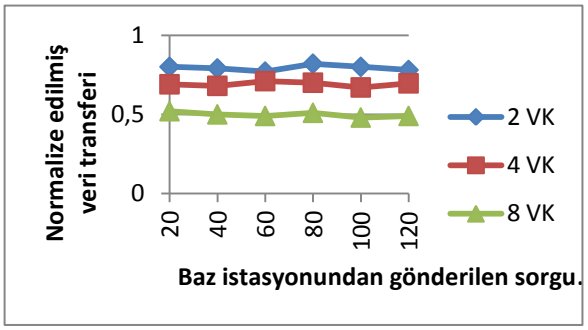
Damgalamada kullanılan ölçek katsayıları çoğu zaman deneme yanılma yöntemi ile elde edilmektedir. Bu çalışma kapsamında kullanılan imge ve sayısal gizli veri için TSGO değerinin en yüksek olduğu ölçek katsayısı 0,3 olarak kullanılmıştır. Şekil 12'de 0 ile 1 arasındaki ölçek katsayıları ile yapılan damgalama sonucunda elde edilen yeni imgenin TSGO değerleri verilmiştir.



Şekil 12. Farklı ölçek katsayıları ile yapılan damgalama sonrası elde edilen TSGO değerleri
(**Figure 12.** PSNR values after watermarking in different scale coefficients)

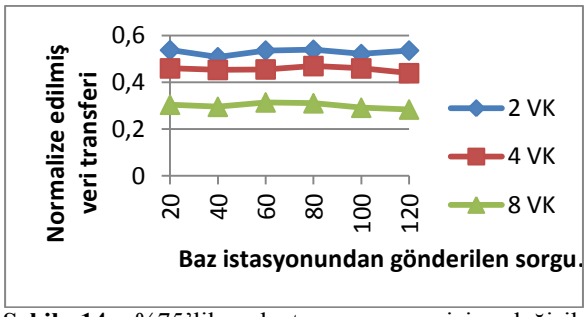
4.3 Performans değerlendirmesi (Performance evaluation)

DTGVK protokolünün veri kümeleme verimliliği algılayıcı ağları için geliştirilmiş olan TOSSIM ağ benzeticisi [23] kullanılarak ölçülmüştür. Benzetim senaryosunda 128 algılayıcı düğümü kullanılmış, bu algılayıcı düğümleri 2-4-8 gruba ayrılarak sırasıyla 2-4-8 veri kümeleyicide veri kümeleme işlemi Bölüm 3.3'te açıklandığı gibi gerçekleştirilmiştir. Benzetim senaryolarında %50 ve %75'lik sıkıştırma oranları kullanılmış ve baz istasyonundan yapılan değişik sayıdaki sorgu için ağda yapılan veri transferi miktarı ölçülmüştür. Her benzetim senaryosu 20 defa çalıştırılmış ve sonuçların ortalaması alınmıştır. Şekil 13. ve 14. DTGVK protokolü kullanıldığında ağda iletilen toplam veri miktarını DTGVK protokolü kullanılmadan gönderilen veri miktarına göre normalize edilmiş olarak göstermektedir. Alınan sonuçlar DTGVK protokolünün ağda iletilen veri miktarını düşürdüğünü göstermektedir. Ayrıca veri sıkıştırma oranın ve kümeleyici sayısının artırılmasının da veri kümeleme etkinliğini artırdığı gözlenmektedir.

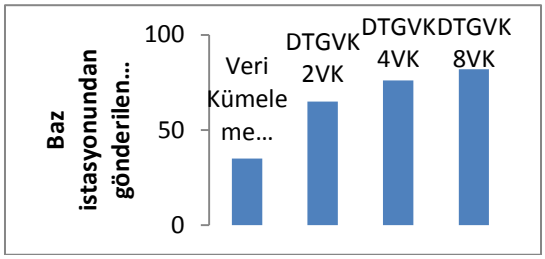


Şekil 13. %50'lik sıkıştırma oranı için değişik sayıdaki Veri Kümeleyici (VK) için elde edilen normalize edilmiş veri transferi değerleri.
(**Figure 13.** Normalized data transfer values for different number of data aggregation for %50 compression ratio)

Buna ek olarak DTGVK protokolünün enerji verimliliği açısından da değerlendirmesi algılayıcıların yaşam süresi ölçülerek yapılmıştır. Veri kümeleme olmadığı durum ve DTGVK kullanıldığı durumlar karşılaştırılmış ve sonuçlar Şekil 15'te verilmiştir. Şekil 15 ilk enerjisi biten (çalışamaz hale gelen) algılayıcı düğümünce cevaplanabilen sorgu sayısını göstermektedir. Şekilden de anlaşılacağı üzere DTGVK protokolü enerji tüketimini azalttığı için algılayıcı düğümleri daha çok sayıda sorgu cevaplayabilmekte ve daha uzun ömürlü olmaktadırlar.



Şekil 14. %75'lik sıkıştırma oranı için değişik sayıdaki Veri Kümeleyici (VK) için elde edilen normalize edilmiş veri transferi değerleri.
(**Figure 14.** Normalized data transfer values for different number of data aggregation for %75 compression ratio)



Şekil 15. Ağ içerisinde enerjisi tükenen ilk düğümün başarı ile cevaplayabildiği sorgu sayısı.
(**Figure 15.** The number of responsed queries by the first dead node in the network)

5. SONUÇLAR (CONCLUSIONS)

Bu çalışmada Kablosuz Çoklu ortam Algılayıcı Ağları (KÇAA)'larda veri toplama işlemini güvenli ve enerji etkin hale getirecek sayısal damgalama tabanlı veri kümeleme protokolü geliştirilmiştir. Geliştirilen protokolde algılayıcılar gizlemek istedikleri verileri fotoğraf verisi içine saldırılara karşı dayanıklı bir algoritma ile gömmekte ve bu damgalanmış veriler ise veri kümeleyiciler tarafından kümelenmektedir. Yapılan güvenlik analizi önerilen protokolün güvenli veri kümeleme hedefini gerçekleştirirken aynı zamanda ağ içerisinde gerçekleşen veri iletim trafiğini de azalttığını göstermiştir.

TEŞEKKÜR (ACKNOWLEDGEMENT)

Bu çalışma Gazi Üniversitesi 06/2011-09 numaralı Bilimsel Araştırma Projesi tarafından desteklenmektedir.

KAYNAKLAR (REFERENCES)

1. Akyildiz, I.F., Su, W., Sankarasubramaniam, Y. ve Cayirci, E., "A survey on sensor networks", **IEEE Communications Magazine**, Cilt 40, No 8, 102-114, 2002.
2. Ozdemir, S., and Xiao, Y., "Secure Data Aggregation in Wireless Sensor Networks: A Comprehensive Overview" **Computer Networks**, Cilt 53, No 12, 2022-2037, 2009.
3. Akyildiz, I.F., Melodia, T. ve Chowdhury, K. R., "A survey on wireless multimedia sensor Networks", **Computer Networks**, Cilt 51,No 4, 921-960, 2007.
4. Cam, H., Ozdemir, S., Nair, P., Muthuavinashiappan, D. ve Sanli, H.O., "Energy-Efficient and secure pattern based data aggregation for wireless sensor Networks", **Computer Communications**, Cilt 29, No 4, 446-455, 2006.
5. Cam, H., Ozdemir, S., Nair, P. ve Muthuavinashiappan D., "ESPDA: Energy-Efficient and Secure Pattern-Based Data Aggregation for Wireless Sensor Networks", **Proceding of IEEE Sensors Conference**, Toronto, Canada, 2003.
6. Lee, S. ve Chung, T., "Data Aggregation for Wireless Sensor Networks Using Self organizing Map", **Artificial Intelligence and Simulation**, 508-517, 2005.
7. Hu, L. ve Evans, D., "Secure aggregation for wireless Networks", **Workshop on Security and Assurance in Ad hoc Networks**, 384-392, 2003.
8. Przydatek, B., Song, D. ve Perrig, A., "SIA : Secure information aggregation in sensor Networks", **ACM Conference on Sensor Systems**, 255 – 265, 2003.
9. Girao, J., Westhoff, D. ve Schneider, M., "Concealed Data Aggregation for Reverse Multicast Traffic in Sensor Networks: Encryption, Key Distribution, and Routing Adaptation", **IEEE Transactions on Mobile Computing**, 1417-1431, 2006.
10. Domingo-Ferrer, J., "A provably secure additive and multiplicative privacy homomorphism", **Information Security Conference**, Lecture Notes in Computer Science, 471-483, 2002.
11. Ozdemir, S., "Concealed Data Aggregation in Heterogeneous Sensor Networks using Privacy Homomorphism",**International Conference on Pervasive Services**, Istanbul, 2007.
12. Castelluccia, C., Mykletun, E. ve Tsudik, G., "Efficient aggregation of encrypted data in wireless sensor Networks", **Conference on Mobile and Ubiquitous Systems: Networking and Services**, 109-117, 2005.
13. Ozdemir**,** S., "Secure Data Aggregation in Wireless Sensor Networks via Homomorphic Encryption", **Journal of The Faculty of Engineering and Architecture of Gazi University**, Cilt 23,No 2,365-373, 2008.
14. Ozdemir S., ve Xiao, Y., "Integrity Protecting Hierarchical Concealed Data Aggregation for Wireless Sensor Networks", **Computer Networks**, Cilt 55, No 8, 1735-1746, 2011.
15. Ozdemir, S., Peng, M., ve Xiao, Y., "PRDA: Polynomial Regression Based Privacy Preserving Data Aggregation in Wireless Sensor Networks", **Wireless Communications and Mobile Computing, Wiley**, DOI: 10.1002/wcm.2369, 2013.
16. Cox I. J., Kilian J., Leighton T. ve Shamoon T., "Secure Spread Spectrum Watermarking for Multimedia," **IEEE Transactions on Image Processing**, Cilt 6, No 12,1673-1687,1997.
17. Piva A., Barni M., Bartolini F. ve Cappellini F., "DCT-based Watermark Recovering without Resorting to the Uncorrupted Orijinal Image, **International Conference on Image Processing,** Washington, DC, USA,, 1997.
18. Dugad R., Ratakonda K., ve Ahuja N., "A New Wavelet-Based Scheme for Watermarking Images," **International Conference on Image Processing**,419-423,Chicago, IL, 1998.
19. Zhu W., Xiong Z. ve Zhang Y.Z., "Multiresolution Watermarking for Images and Video," **IEEE Transactions on Circuits and Systems for Video Technology**, Cilt 9, No 4, 545-550,1999.
20. Elbasi E. ve Eskicioglu A. M., "A DWT-based Robust Semi-blind Image Watermarking Algorithm Using Two Bands," **IS&T/SPIE's 18th Symposium on Electronic Imaging, Security, Steganography, and Watermarking of Multimedia Contents Conference**, San Jose, CA, 2006.
21. Elbasi E.,"Robust MPEG Watermarking in DWT Four Bands", **Journal of Applied Research and Technology**, Cilt 10, No 2,87-93, 2012.
22. Huffman D.A., "A Method for the Construction of Minimum-Redundancy Codes", **Proceedings of the I.R.E.**,1098-1102, 1952.
23. Tiny OS Simulator. http://www.tinyos.net/. (Erişim Ocak 2012)
24. Çakıroğlu, M., Özcerit, T., Özdemir, Ç., "Boğma Saldırılarına Karşı Dinamik Kanal Atlamalı Yeni bir Güvenlik Yönteminin Tasarımı ve Başarım Analizi", **Gazi Üniv. Müh. Mim. Fak. Der.**, Cilt 26, No 4, 877-887, 2011