Gazi Üniv. Müh. Mim. Fak. Der.
Cilt 25, No 1, 131-139, 2010

J. Fac. Eng. Arch. Gazi Univ.
Vol 25, No 1, 131-139, 2010

HETEROJEN KABLOSUZ ALGILAYICI AĞ TEMELLİ SINIR İZLEME SİSTEMLERİNDE GİZLİ VERİ KÜMELEME

Suat ÖZDEMİR
Bilgisayar Mühendisliği Bölümü, Mühendislik Fakültesi, Gazi Üniversitesi, Maltepe, Ankara, 06570
suatozdemir@gazi.edu.tr

(Geliş/Received: 17.02.2009 ; Kabul/Accepted: 06.05.2009)

ÖZET

Heterojen Kablosuz Algılayıcı Ağ (HKAA) temelli sınır izleme sistemleri sismik, video, ısı, ses gibi çeşitli algılayıcı türlerinin bir arada çalışarak sınır güvenliğini sağladıkları sistemlerdir. Bu sistemlerde elde edilen değişik türdeki veriler merkezi bir baz istasyonunda ya da veri toplayıcılarda analiz edilerek sınır güvenliği için tehlike oluşturan durumlar ortaya çıkarılır. Ancak toplanan verinin çok çeşitli olması, güvenlik derecesi yüksek kablosuz algılayıcı ağlar için gerekli olan veri kümeleme işleminin gizli bir şekilde yapılmasını zorlaştırır. Bu çalışmada HKAA temelli sınır izleme sistemlerinde şifrelenmiş değişik veri türlerinin gizli olarak kümelenmesine olanak sağlayan yeni bir veri kümeleme protokolü sunulmuştur. Önerilen protokolün özgün yönü toplanan verilerin kümelenmesi esnasında değişik veri tiplerinin tek bir paket olarak kümelenebilmesi ve baz istasyonunun kümelenmiş veriyi çözdüğünde verileri türlerine göre ayrı ayrı elde edebilmesidir.

Anahtar Kelimeler: Heterojen kablosuz algılayıcı ağlar, gizli veri kümeleme, güvenlik.

CONCEALED DATA AGGREGATION IN HETEROGENEOUS WIRELESS SENSOR NETWORK BASED BORDER SURVEILLANCE SYSTEMS

ABSTRACT

Heterogeneous wireless sensor network (HWSN) based border surveillance systems are composed of several types of sensors such as video, temperature, seismic, and sound sensors. The data collected in these networks are analyzed by data aggregators or a central base station to determine illegal activities inside the border region. Due to high security requirements, concealed data aggregation is vital for mission critical HWSNs. However, since multiple sensor types that generate different data types, performing concealed data aggregation in these networks is not a trivial task. In this paper, a concealed data aggregation protocol that allows aggregation of multiple data types in border surveillance systems. The novel idea behind the paper is that the proposed concealed data aggregation protocol is able to aggregate different sensor data types into a single data packet. Moreover, the base station is able to obtain each different data type separately when it decrypts the aggregated data.

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

1. GİRİŞ (INTRODUCTION)

Kablosuz algılayıcı ağlar (KAA), 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 kullanılmaktadırlar. Algılayıcı ağlarının en çok kullanıldıkları alanlardan birisi de sınır koruma ve izleme sistemleridir. Geleneksel sınır izleme sistemleri gözlem kuleleri, video kayıt sistemi, gezici sınır koruyucuları, kontrol merkezleri ve çeşitli algılayıcılardan oluşan kurulumu ve işletimi zahmetli ve masraflı sistemlerdir. Dağlık ve sarp sınır bölgelerine sahip ülkelerin bu tip sınır koruma sistemlerini kurmaları çok daha zor ve

masraflıdır. Örneğin, Amerika Birleşik Devletleri'nin karasal sınırlarının büyük kısmı dikenli tel ve duvar benzeri yapılarla korunurken sadece %2'lik kısmı yer algılayıcıları ve kamera sistemleri ile izlenmektedir [2]. Bu durumun başlıca sebebi sınır izleme ve koruma sistemlerinin yüksek kurulum ve işletim maliyetleridir. Öte yandan, KAA temelli sınır izleme sistemleri hem kurulum ve işletim maliyeti açısından hem de etkinlikleri bakımından geleneksel sınır izleme sistemlerine karşı oldukça üstündürler.

Sınır izleme ve koruma sistemlerinde kullanılan Heterojen Kablosuz Algılayıcı Ağlar (HKAA) genelde sismik, video, ısı, ses gibi çeşitli algılayıcıların bir arada çalıştığı çoklu uygulamalı sistemlerdir. Şekil 1'de HKAA temelli bir sınır izleme sistemi örneği verilmiştir. HKAA temelli sınır izleme sistemlerinde algılayıcıların verisi toplandıktan sonra veri kümeleyiciler ya da baz istasyonu tarafından illegal aktiviteler tespit edilerek gerekli birimler (asker, sınır koruma memurları, vb.) harekete geçirilir. Sınır güvenliğinin önemi nedeniyle bu ağlarda taşınan verinin gizli kalması ve taşıma esnasında asla değiştirilmemesi gerekmektedir.

Sınır izleme sistemlerinde kullanılan HKAA'larda veri gizliliğinin şart olması ve çeşitli veri tiplerinin baz istasyonuna gönderiliyor olması nedeniyle, bu sistemlerde KAA'lar için mutlak bir gereklilik olan veri kümeleme işlemini gerçekleştirmek oldukça zorlaşmaktadır. Bunun başlıca iki sebebi vardır: (1) 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 [3]. Bir diğer ifade ile, veri gizliliğini sağlayan güvenlik protokolleri uçtan uca gizliliği (end-to-end confidentiality) tercih ederler ve bunu başarmak için de algılayıcı tarafından şifrelenen verinin sadece baz istasyonu tarafından çözülmesini isterler. Öte yandan, veri kümeleme protokolleri veri kümeleyicilerde şifrelenmiş verilerin çözülmesini ve kümeleme işlemi ile istenilen bilginin mümkün olduğunca özetlenmesini hedeflemektedirler. Burada temel amaç ağda gönderilen veri miktarının azaltılması yoluyla ağ enerji tüketiminin düşürülmesi ve ağ ömrünün uzatılmasıdır. (2) HKAA'larda çeşitli türdeki verilerin bir arada kümelenmesi sorundur. Klasik KAA'larda genelde tek bir veri tipi vardır ve algılayıcılardan toplanan tek tip veri kendi arasında kümelenerek baz istasyonuna gönderilir. Ancak çeşitli algılayıcı tiplerinden oluşan heterojen bir KAA'da bu yaklaşımla veri kümelemeden yeterli verim alınması mümkün değildir. Örneğin, HKAA'da eğer n tane değişik algılayıcı türü varsa n değişik veri tipi olacaktır. Her bir veri tipinin kendi arasında kümelenmesi durumunda, veri kümeleyiciden baz istasyonuna n tane kümelenmiş veri paketi gönderilmesi anlamına gelecektir.

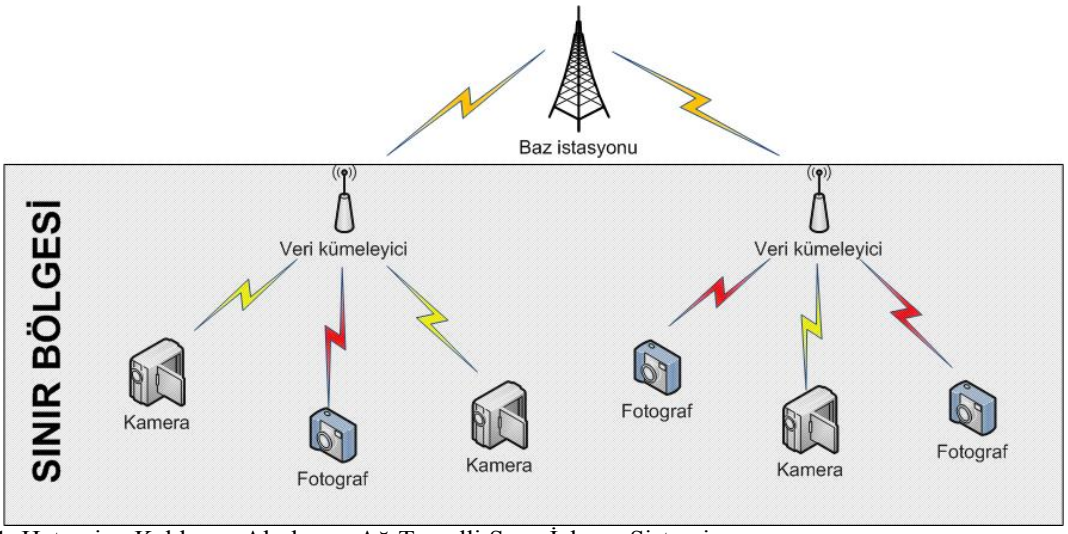
Bu makalede* HKAA temelli sınır izleme sistemleri için geliştirilmiş olan homomorfik şifrelemeye dayalı bir gizli veri kümeleme protokolü sunulmuştur. Önerilen protokol homomorfik şifreleme sayesinde verilerin kümeleyiciler tarafından şifresi çözülmeden kümelenmesini sağlar. Böylece HKAA içinde bir yandan uçtan-uca veri gizliliği sağlanmış olurken aynı zamanda da veri kümeleme işlemi gerçekleştirilir. Ayrıca, önerilen veri kümeleme protokolünde kullanılan homomorfik şifreleme algoritması sayesinde farklı veri tipleri tek bir pakette kümelenebilmekte ve baz istasyonu kümelenmiş paketi çözerken her bir veri tipini ayrı ayrı elde edebilmektedir. Bu sayede klasik veri kümeleme protokollerinde her bir algılayıcı türünün verisi ayrı bir paket olarak kümelenebilirken, önerilen sistemde bütün algılayıcı türlerinin verisi sadece bir paket olarak kümelenebilmektedir. Buna bağlı olarak, ağ içinde gönderilen veri miktarında azalma olmaktadır. Şekil 2'de bu durumu açıklayan bir örnek verilmiştir. Yukarıdaki satırlarda verilen özellikler bu çalışmanın bilime katkısı olarak nitelendirilebilir, bilgilerimiz dahilinde HKAA'larda çeşitli veri tiplerini kullanarak gizli veri kümeleme işlemini gerçekleştirebilen başka bir çalışma yoktur.

Makalenin geri kalan kısmı şu şekilde organize edilmiştir. 2. Bölümde gizli veri kümeleme alandaki önemli çalışmaları özetleyen kısa bir literatür özeti verilmiştir. 3. Bölümde sistem modeli ve homomorfik şifreleme ile ilgili ön bilgiler verilmiştir. 4. Bölümde önerilen veri kümeleme protokolü detaylı olarak anlatılmıştır. 5. Bölümde güvenlik ve performans analizi sonuçları verilmiştir. Sonuç ve çıkarımlar ise 6. Bölümde yer almaktadır.

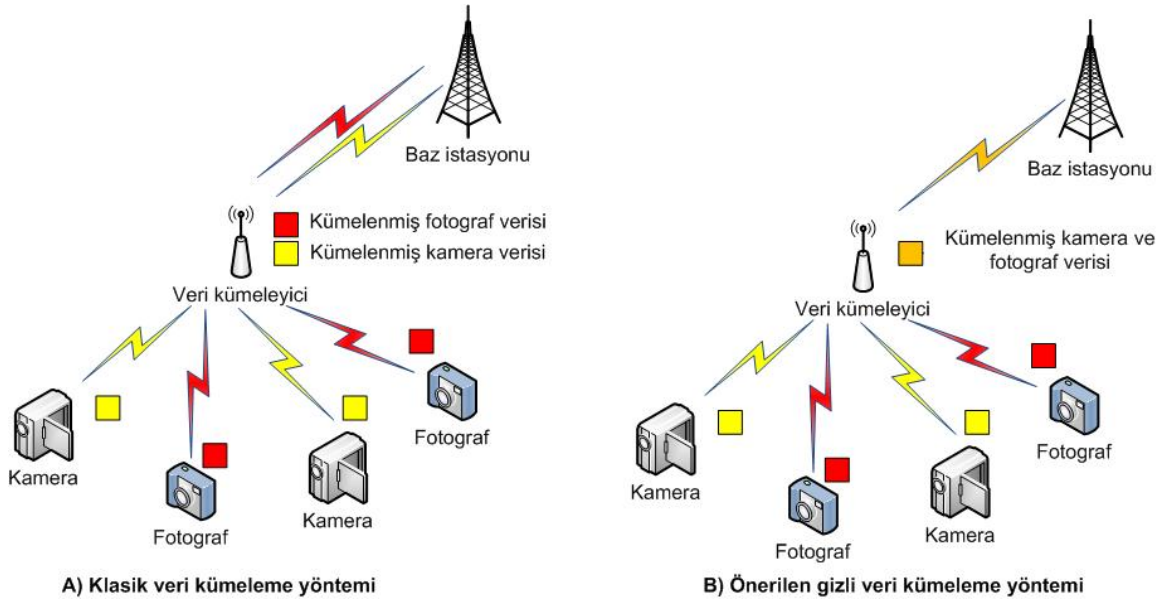
2. İLGİLİ ÇALIŞMALAR (RELATED WORK)

Ağ içerisinde aktarılan veri miktarını düşürüp enerji tasarrufu sağlamasının yanı sıra, KAA'larda veri kümeleme protokolleri doğruluk hassasiyeti yüksek olmayan bireysel algılayıcı verilerinin ortalamalarını alıp toplanan verideki hata payını azaltarak, 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 [3]. Bu gereklilik birçok araştırmacıyı güvenli veri kümeleme

* Bu çalışma Gazi Üniversitesi 06/2007-44 nolu Bilimsel Araştırma Projesi tarafından desteklenmektedir.



Şekil 1. Heterojen Kablosuz Algılayıcı Ağ Temelli Sınır İzleme Sistemi (Heterogeneous Wireless Sensor Network Based Border Surveillance System)



Şekil 2. HKAA temelli sınır izleme sistemleri için önerilen gizli veri kümeleme yöntemi ile klasik veri kümeleme yöntemi arasındaki fark (The difference between traditional data aggregation method and the proposed approach)

metotları üzerinde çalışmaya zorlamıştır [3,5,6,7]. Bu çalışmalarda veri kümeleme için verilerin her düğümde çözülüp tekrar şifrelenmesi gerektiğinden, veri gizliliği ve veri kümeleme ancak sıçrama bazında (hop-by-hop) gerçekleştirebilir. Yakın zamanda, hem uçtan uca veri gizliliğini hem de veri kümelemeyi sağlayabilmek için homomorfik şifrelemeye dayalı veri kümeleme yöntemleri önerilmiştir [8,10,11,12].

Homomorfik şifrelemeye dayalı Gizli Veri Kümeleme (Concealed Data Aggregation) adlı protokol [8] numaralı çalışmada sunulmuştur. Bu protokolde algılayıcı düğümleri baz istasyonu ile ortak bir anahtar paylaşır. Çalışmada veri kümeleyiciler şifrelenmiş algılayıcı verilerini çözmezler ve veri kümelemeyi şifrelenmiş veriler üzerinden yaparlar. Böylece ağdaki herhangi bir düğüm veri kümeleyici olabilir. Önerilen metot [9] numaralı kaynakta Domingo-Ferrer tarafından geliştirilen homomorfik şifreleme algoritmasını kullanır. Yazarlar Domingo-Ferrer'in şifreleme algoritmasının gerçekleştirimi oldukça pahalı açık anahtar altyapısına dayanmasına rağmen, günümüzün sınırlı kaynaklara sahip algılayıcı düğümleri üzerinde uygulanabilir olduğunu göstermişlerdir.

Hem uçtan uca veri gizliliğini hem de veri kümelemeyi sağlayabilen bir diğer çalışmada [10], yazarlar açık anahtar altyapısına dayalı homomorfik şifreleme algoritmalarının algılayıcı düğümleri için pahalı işlemler olduğunu öne sürmüş ve heterojen bir ağ yapısı kullanmışlardır. Bu heterojen ağda normal düğümlerin yanında, kaynak açısından zengin veri kümeleyici düğümler kullanılmıştır. Ağda veri toplama görevi normal algılayıcılar tarafından yapılırken, homomorfik şifreleme ve veri kümeleme kaynak açısından zengin olan özel düğümler tarafından gerçekleştirilmektedir.

Düşük kapasiteli algılayıcılara daha uygun simetrik anahtar yapısına dayalı bir gizli veri kümeleme algoritması [11] numaralı çalışmada geliştirilmiştir. Ancak geliştirilen yöntem merkezi bir yaklaşım sergiler ve ağdaki tüm algılayıcı düğümlerinin bir gizli anahtar paylaşmasını gerektirir. Geliştirilen algoritmada şifrelenmiş ve kümelenmiş verinin çözülebilmesi için veri gönderen bütün düğümlerin ID numaraları merkez istasyona gönderilmek zorundadır ve bu da veri aktarım miktarını fazlaca artırır. Bunun yanı sıra, her bir düğüm baz istasyonu ile paylaştığı anahtarı her şifreleme işlemi öncesinde senkronize etmelidir. Düğümlerin ve baz istasyonunun birbirlerinden çok uzak olmaları sebebiyle senkronizasyon işlemi çok miktarda tekrarlı veri aktarımına sebep olur. [11]'de geliştirilen veri kümeleme algoritmasının eksik yönlerini [12]'de tamamlanarak daha gelişmiş ve KAA'ların kısıtlı kaynak yapısına daha uygun bir veri kümeleme protokolü sunulmuştur.

3. SİSTEM MODELİ VE HOMOMORFİK ŞİFRELEME (SYSTEM MODEL AND HOMOMORPHIC ENCRYPTION)

Bu bölümde çalışmada yapılan kabuller ile ağ ve tehdit modeli verilmiştir. Ayrıca, HKAA temelli sınır izleme sistemleri için bu çalışmada önerilen veri kümeleme protokolünün dayandığı homomorfik şifreleme ile ilgili genel bir bilgi de sunulmuştur.

3.1. Ağ ve Tehdit Modeli (Network and Threat Model)

Bu çalışmada gruplara ayrılmış çok sayıda algılayıcı düğümlerinden ve kaynak açısından zengin bir baz istasyonundan oluşan ve izlenecek olan sınır bölgesine rastgele bir şekilde bırakılmış/atılmış olan statik bir kablosuz algılayıcı ağı öngörülmüştür. Ağı oluşturan düğümler çeşitli algılayıcı tiplerine sahiptir ve bazı düğümler 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. Örneğin, Mica2 [15] tipi algılayıcı düğümlerinde 4 MHz'lik 8-bit Atmel mikroişlemci, 128 KB komut hafızası ve 4 KB RAM bulunmaktadır.

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 sınır bölgesine gözetimsiz olarak atıldığından, algılayıcı düğümlerinin fiziksel güvenliğinin sağlanması mümkün değildir. Bu nedenle algılayıcı düğümleri düşman güçler/kötü niyetli kişiler tarafından ele geçirilebilir ve ağa karşı kullanılabilir [1]. Kablosuz algılayıcı ağlarda bu tip ele geçirilmiş algılayıcı düğümlerinin fark edilmesi genelde mümkün değildir. Ele geçirilmiş algılayıcı düğümleri ağın işleyişini engellemek, toplanan veriyi bozmak ya da toplanan veriyi öğrenmek için birçok saldırı gerçekleştirebilirler [1,13]. Ayrıca ele geçirilmiş algılayıcı düğümü bir veri kümeleyici ise, kümelenen veriyi değiştirebilir ve baz istasyonunu yanıltabilir. 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 dışında kalmaktadır.

3.2. Homomorfik Şifreleme (Homomorphic Encryption)

Homomorfik şifreleme açık metin üzerinde yapılan matematiksel bir işlemin şifrelenmiş bir metin üzerinde yapılabilmesini sağlayan bir şifreleme türüdür [8,9]. Örnek olarak E'nin şifrelemeyi D'nin şifre çözme işlemini, K'nin de şifrelemede kullanılan gizli anahtarı temsil ettiğini kabul edelim. Ek olarak + ve * işaretleri de Q seti üzerinde toplama ve çarpma işlemlerini temsil etsin. Eğer

$$a+b = D_K(E_K(a)+E_K(b)) \forall a,b \in Q$$

eşitliği sağlanıyorsa şifreleme fonksiyonu E'nin homomorfik toplama özelliği taşıdığı kabul edilir ve eğer

$$a*b = D_K(E_K(a)*E_K(b)) \forall a,b \in Q$$

eşitliği sağlanıyorsa şifreleme fonksiyonu E'nin homomorfik çarpma özelliği taşıdığı kabul edilir. Homomorfik toplama ve homomorfik çarpma özelliği taşıyan şifreleme fonksiyonları şifrelenmiş veri üzerinde çarpma ve toplama yapmaya izin verdiğinden, veri kümeleyiciler toplama ve çarpmaya dayalı kümeleme işlemlerini verinin aslını görmeden şifrelenmiş veri üzerinde uygulayabilirler. Bu hem veri kümeleyicilerde şifreleme anahtarı bulunması zorunluluğunu ortadan kaldırır, hem de ele geçirilmiş veri kümeleyicilerin veriyi görmesini engeller. Homomorfik gizlilik simetrik ya da açık anahtar alt yapısı kullanılarak gerçekleştirilebilir [8,11]. Açık anahtar altyapısına dayalı homomorfik şifreleme algoritmaları anahtar dağılımı açısından avantajlı olmalarına karşın yüksek işlemci gücü ve enerji ihtiyaçları vardır. Öte yandan simetrik anahtar alt yapısını kullanan homomorfik şifreleme algoritmaları düşük enerji ve işlem gücü ihtiyaçlarına karşın algılayıcı düğümleri arasında şifreleme anahtarlarının

dağıtımını gerektirir. Eliptik eğri kriptolojisine dayalı homomorfik şifreleme algoritmaları ise hem anahtar dağılımı gerektirmez hem de enerji ve işlemci gücü ihtiyaçları açık anahtar altyapısına dayalı homomorfik şifreleme algoritmalarından daha düşüktür. Bu nedenle, bu çalışmada Boneh ve arkadaşları tarafından geliştirilen eliptik eğri kriptolojisine dayalı homomorfik şifreleme algoritması kullanılmıştır [14]. Dahası, Boneh'in şifreleme algoritması [14] farklı anahtarlarla şifrelenmiş verilerin kümelenebilmesine olanak sağladığı için HKAA temelli sınır izleme sistemlerinde farklı tipteki algılayıcı düğümlerine farklı anahtarlar atanarak kullanılabilir. Ayrıca bu algoritma hem homomorfik toplama hem de homomorfik çarpma özelliği gösterir, ancak homomorfik çarpma özelliği yüksek işlem gücü gerektirdiğinden bu çalışmada önerilen protokol sadece toplama homomorfisinden faydalanır. Aşağıda Boneh'in homomorfik şifreleme algoritmasının temel prensipleri verilmiştir.

Anahtar üretimi:
Bir açık anahtar (*PK*) ve bir gizli anahtar (*SK*) üretebilmek için aşağıdaki işlemler sırayla yapılır.

1- Verilen bir güvenlik parametresi $\tau \in \mathbb{Z}$ için (q_1, q_2,*E*,*n*) dörtlüsü üretilir. *E*'nin dönüşsel bir grup oluşturan eliptik eğri noktaların oluşturduğu bir set olduğunu kabul edelim. Ayrıca *E*'nin derecesi (order) *n* ve $n=q_1*q_2$ olsun.
2- *E* seti içinden derecesi *n* olan *g* ve *u* diye iki rastgele sayı seçilir. Ayrıca derecesi q_1 olan $h=u^{q2}$sayısı belirlenir.
3- Açık anahtar $PK=(n,E,g,h)$ ve gizli anahtar $SK=(q_1)$ olarak belirlenir.

Şifreleme:
$T>q_2$ şartını sağlayan bir *T* tamsayısı belirlenir. *T*'nin bit olarak uzunluğu yaklaşık olarak q_2'nin bit uzunluğuna eşit olmalıdır. Şifrelenecek olan mesajlar kümesi *M*'nin {*0,1,2,…,T*} tamsayı seti içinde olması gerekir. Bir mesaj *m*'yi açık anahtar PK ile şifrelemek için bir rastgele sayı $r \leftarrow \{0,1,2,\ldots,n-1\}$ seçilir ve şifrelenmiş mesaj $C= g^m + h^r$ olarak hesaplanır. Burada + işlemi eliptik eğri noktalarının toplanmasını, a^b ise *a* ve *b* eliptik eğri noktalarının içsel (scalar) çarpımını ifade eder.

Şifre Çözme:
Şifrelenmiş bir *C* mesajını gizli anahtar $SK=q_1$ ile çözebilmek için C^{q1} hesaplanır. Burada dikkat edilmesi gereken nokta $C^{q1}= (g^m + h^r)^{q1} = (g^{q1})^m$ olduğudur. $\hat{g} = g^{q1}$ olduğunu kabul edersek, şifrelenmiş veriden *m* mesajının elde edilebilmesi için C^{q1}'in $\hat{g}$ tabanında logaritmasının alınması mümkün olacaktır. Mesaj *m* 0 ve *T* arasında bir tamsayı değer olduğu için bu logaritma $O(\sqrt{T})$ zamanı içerisinde Pollard'ın lambda metodu [24] kullanılarak çözülebilir.

Kümeleme:
$C_1= g^{m1} + h^{r1}$ ve $C_2= g^{m2} + h^{r2}$ gibi iki şifrelenmiş mesaj Boneh'in algoritmasına göre $C_0= C_1+C_2= g^{(m1+m2)} + h^{(r1+r2)}$ şeklinde kümelenebilir.

Boneh'in algoritmasının homomorfi özelliğinin ispatı gibi detaylara [14] numaralı çalışmada erişilebilir. Bir sonraki bölümde Boneh'in homomorfik şifreleme algoritmasından faydalanarak ve farklı algılayıcı türleri için farklı anahtarlar kullanarak, HKAA'larda gizli veri kümelemenin nasıl gerçekleştirildiği anlatılmaktadır.

4. HETEROJEN KABLOSUZ ALGILAYICI AĞLARDA GİZLİ VERİ KÜMELEME (CONCEALED DATA AGGREGATION IN HETEROGENEOUS WIRELESS SENSOR NETWORKS)

Tek bir çeşit algılayıcıdan oluşan KAA'larda sadece bir açık/gizli anahtar çiftine ihtiyaç vardır, bu sebeple bir önceki bölümde anlatılan Boneh'in homomorfik şifreleme algoritması kullanılarak gizli veri kümeleme yapılabilir. Ancak birçok algılayıcı tipinden oluşan HKAA'larda değişik veri tiplerinin bir arada şifreli olarak kümelenebilmesi için birden fazla açık/gizli anahtar çiftine ihtiyaç duyulmaktadır. Bu çalışmada önerilen gizli veri kümeleme protokolünde, eğer her bir algılayıcı tipi için farklı bir açık/gizli anahtar çifti kullanılırsa, tüm algılayıcı türlerine ait veriler bir arada kümeleyebilmekte ve baz istasyonu şifrelenmiş ve kümelenmiş veriyi aldığında her bir algılayıcı türüne ait veriyi ayrı ayrı elde edebilmektedir. Ancak önerilen gizli veri kümeleme işleminde birden fazla açık/gizli anahtar çifti kullanabilmek için Boneh'in homomorfik şifreleme algoritmasında aşağıdaki değişiklilerin yapılması zorunludur.

Anahtar üretimi:
k adet değişik algılayıcı türüne sahip bir HKAA için, *k* tane açık anahtar (*PK*) ve bir tane gizli anahtar (*SK*) üretebilmek için aşağıdaki işlemler sırayla yapılır:

1. Verilen bir güvenlik parametresi $\tau \in \mathbb{Z}$ için (q_1,q_2,q_3,..q_{k+1},*E*,*n*) grubu üretilir. *E*'nin dönüşsel bir grup oluşturan eliptik eğri noktaların oluşturduğu bir set olduğunu kabul edelim. Ayrıca *E*'nin derecesi (order) *n* ve $n=q_1* q_2 * \ldots *q_{k+1}$ olsun.
2. *E* seti içinden derecesi *n* olan *k+1* tane rastgele sayı seçilir (u_1,u_2,u_3,…u_{k+1}). Ayrıca derecesi q_{k+1} olan bir *h* sayısı aşağıdaki gibi belirlenir.

$$h = u^{\beta}_{k+1} \text{ ve } \beta = \prod_{i=1}^{k} q_i$$

3. Şimdi *k* değişik algılayıcı türü için üretilecek açık anahtarları oluşturacak olan *k* tane *P* değeri aşağıdaki gibi üretilebilir

$P_z = g^{\alpha}$ ve $\alpha = \prod_{t=1,t\neq z}^{k+1} q_t$ z=1,2,…,k

Buna göre z'inci algılayıcı türüne ait açık anahtar $PK^z = (n, E, P_z, g, h)$ şeklinde hesaplanır. Bütün PK^z'lere ait gizli anahtar ise $SK=(q_1, q_1, q_1,\ldots, q_{k+1})$ şeklinde ifade edilir.

Şifreleme:

$T_z > q_z$ şartını sağlayan bir T_z tamsayısı belirlenir. T_z'nin bit olarak uzunluğu yaklaşık olarak q_z'nin bit uzunluğuna eşit olmalıdır. Herhangi bir z türü algılayıcının verisi M $\{0,1,\ldots,T_z\}$ kümesinde bir tamsayı olarak ifade edilmelidir. m mesajını PK^z açık anahtarı ile şifrelemek için rastgele $r \leftarrow \{0,1,\ldots.n-1\}$ sayısı seçilir ve şifrelenmiş mesaj $C = P_z^{m_z} + h^r$ olarak hesaplanır. Burada + işlemi eliptik eğri noktalarının toplanmasını a^b ise a ve b eliptik eğri noktalarının içsel (scalar) çarpımını ifade eder.

Kümeleme:

$\sum m_t$ ifadesinin i türü algılayıcıların verilerinin toplamını ifade ettiğini kabul edelim. O halde k tane şifrelenmiş veri $C_z = P_z^{m_z} + h^{r_z}$ $(z=1.....k)$ bir C' şifrelenmiş verisi olarak aşağıdaki gibi şifrelenebilir.

$$C' = \sum_{t=1}^{k} (P_t^{\sum m_t} + h^{r_t})$$

Şifre Çözme:

Şifre çözme sırasında baz istasyonu şifrelenmiş veri C' den her bir algılayıcı türüne ait verileri ayrı ayrı çıkarabilmektedir. Bunun için aşağıdaki ifadenin doğru olduğunu düşünelim.

$$\widehat{g_z} = g_z^{\alpha} \quad \alpha = \prod_{t=1,t\neq z}^{k+1} q_t \quad z=1,2,\ldots,k$$

Buna göre baz istasyonu herbir algılayıcı türü z'nin verisi $\sum_{t=z} m_t$ 'yi $(C')^{\alpha}$'nın ayrık logaritmasını $\widehat{g_z}$ tabanında alarak elde edebilir. Buna bağlı olarak her bir algılayıcı türü z'nin verisi aşağıdaki gibi bulunur.

$$\sum_{t=z} m_t = log_{\widehat{g_i}} (C')^{\alpha} \quad ve \quad \widehat{g_i} = g_z^{\alpha}$$

$$\alpha = \prod_{t=1,t\neq z}^{k+1} q_t \quad z=1,2,\ldots,k$$

Yukarıda verilen veri kümeleme işlemini daha iyi açıklayabilmek için aşağıda bir sınır izleme ve koruma sistemi örneğinde yapılan gizli veri kümeleme işlemi anlatılmaktadır.

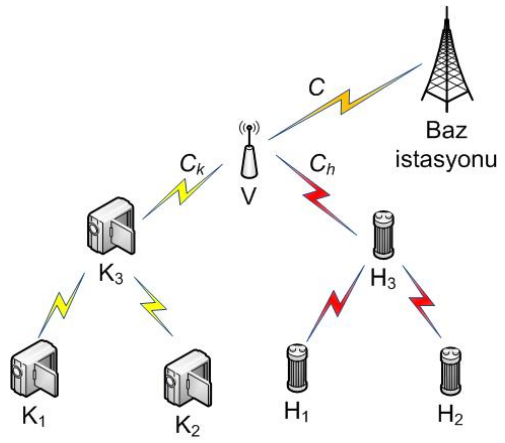
Örnek: Örneğin anlaşılabilirliğinin artırılması amacıyla sınır izleme sisteminin sadece 2 tür algılayıcıdan (kamera ve hareket) oluştuğunu kabul edelim. Kamera algılayıcıları $PK^k=(n,E,P_k,g,h)$ açık anahtarına ve hareket algılayıcıları $PK^h=(n,E,P_h,g,h)$ açık anahtarına sahip olsunlar. Yine basitliği sağlamak amacıyla, ağın sadece üç tane kamera algılayıcısı (K_1, K_2 ve K_3), üç tane hareket algılayıcısından (H_1, H_2 ve H_3) ve bir tane de veri kümeleyici düğümden (V) oluştuğunu kabul edelim. Şekil 3'te örnekte kullanılan ağ yapısı verilmiştir. P_k P_h ve h'nin dereceleri hesaplama kolaylığı için aşağıdaki gibi küçük asal sayılar olarak seçilmiştir.

P_k'nin derecesi ve q_1'in değeri 11
P_h'nin derecesi ve q_2'nin değeri 13
h'nin derecesi ve q_3'ün değeri 17
n'nin derecesi $n=q_1\, q_2\, q_3$=2431

Kamera algılayıcıları K_1 ve K_2 ile hareket algılayıcıları H_1 ve H_2 sınır bölgesinde topladıkları verileri aşağıda gösterildiği gibi şifreleyerek sırasıyla K_3 ve H_3'e gönderirler. Şifreleme işlemi sırasında r değerleri rastgele üretilerek kullanılmaktadır.

K_1 mesaj $M_k^1 = 1$'i üretir ve $C_k^1 = P_k^1 + h^4$ şeklinde şifreler.
K_2 mesaj $M_k^2 = 3$'ü üretir ve $C_k^2 = P_k^3 + h^6$ şeklinde şifreler.
H_1 mesaj $M_h^1 = 4$'ü üretir ve $C_h^1 = P_h^4 + h^2$ şeklinde şifreler.
H_2 mesaj $M_h^2 = 2$'yi üretir ve $C_h^2 = P_h^2 + h^7$ şeklinde şifreler.

K_1 ve K_2 şifrelenmiş mesajlarını K_3'e, H_1 ve H_2'de şifrelenmiş mesajlarını H_3'e gönderir. K_3 C_k^1 ve C_k^2'yi $C_k = P_k^4 + h^{10}$ olarak kümeler. Aynı şekilde, H_3 de C_h^1 ve C_h^2'yi $C_h = P_h^6 + h^9$ olarak kümeler. Kümelenen C_k ve C_h ağdaki veri kümeleyici düğüm V'ye gönderilir. V ise C_k ve C_h'yi $C = P_k^4 + P_h^6 + h^{17}$ şeklinde kümeler. h'nin derecesi 17 olduğundan, $h^{17}=\infty$ yazılabilir ve ∞ eliptik eğri matematiğinde toplamada etkisiz elemandır, bu yüzden $C = P_k^4 + P_h^6 + h^2$ yazılabilir. Kümeleme işleminden sonra V düğümü C'yi baz istasyonuna gönderir.



Şekil 3. Örnek için ağ yapısı (Network structure of the example)

Baz istasyonu kamera algılayıcılarının verisini ortaya çıkarmak için öncelikle $C^{q_2 q_3} = (P_k^4 + P_h^6 + h^2)^{221}$ değerini hesaplar. a[b] işlemi eliptik eğri noktalarının scalar çarpımını ifade ettiğinden, $C^{q_2 q_3}$ değeri $P_k^{884} + P_h^{1326} + h^{442}$ olarak yazılabilir. $h^{17}=\infty$, $P_k^{11}=\infty$ ve $P_h^{13}=\infty$ olduğundan, eliptik eğri matematiği kullanarak $C^{q_2 q_3} = P_k^4$ olarak yazılabilir. Son olarak baz istasyonu $C^{q_2 q_3}$ değerinin ayrık logaritmasını $\widehat{g_k} = g_k^{q_2 q_3}$ tabanında alarak kamera algılayıcılarının kümelenmiş verisini 4 olarak elde eder. Aynı şekilde hareket algılayıcılarının verisini elde edebilmek için baz istasyonu $C^{q_2 q_3}$ değerinin ayrık logaritmasını $\widehat{g_k} = g_k^{q_2 q_3}$ tabanına göre hesaplar.

Örnekte de görüldüğü gibi, önerilen protokol kullanılarak iki farklı algılayıcı türüne ait veri tipleri bir paket olarak kümelenebilmekte ve baz istasyonu iki farklı türdeki veriyi de ayrı ayrı elde edebilmektedir.

5. PERFORMANS ANALİZİ (PERFORMANCE ANALYSIS)

Bu bölümde önerilen protokolün güvenlik analizi ve performans değerlendirmesi yapılmaktadır.

5.1. Güvenlik Analizi (Security Analysis)

Önerilen protokolde eliptik eğri kriptolojisine bağlı açık anahtar yapısı kullanılmaktadır ve gizli anahtara sadece baz istasyon sahiptir. Ağ içerisinde şifrelenerek kümelenen veriler ancak ve ancak baz istasyonu tarafından çözülebilir. Bu nedenle önerilen protokol gizli veri kümeleme protokollerinin ana amacı olan uçtan uca veri gizliliğini sağlamaktadır. Kullanılan homomorfik şifreleme algoritmasında, gizli anahtara sahip olmayan herhangi bir algılayıcı düğümünün ya da saldırganın şifrelenmiş bir mesajı çözebilmek için açık anahtar parametrelerinden biri olan *n* parametresini hesaplayabilmesi gerekir ki, *n* yeterince büyük seçildiğinde bunu yapmak çok zordur [14]. Yer problemi nedeniyle, kullanılan homomorfik şifreleme algoritmasının değişik kriptolojik ataklara karşı olan dayanımı burada verilmemiştir, ancak bu detaylara [14] numaralı çalışmadan erişilebilir. Ayrıca, bu çalışmanın amacının dışında kalsalar da, kablosuz algılayıcı ağlarındaki mesaj doğruluğunun korunması, tekrarlama saldırıları vb. güvenlik gereksinimleri mesaj doğrulama kodları, zaman damgaları ve rastgele bit dizileri kullanılarak önlenebilmektedir. Kullanılan homomorfik şifreleme algoritması diğer güvenlik mekanizmalarının uygulanmasına engel değildir.

5.3. Performans Değerlendirmesi (Performance Evaluation)

Performans değerlendirmesinde TinyECC projesinden [16] elde edilen sonuçlar referans olarak alınmış ve bu çalışmada önerilen sistemin uygulanabilirliği gösterilmiştir. TinyECC projesi değişik algılayıcı platformlarında eliptik eğri kriptografisinin uygulanabilirliğini gösteren kapsamlı bir proje olup, proje dahilinde değişik algılayıcı modelleri kullanılarak şifreleme, anahtar paylaşımı ve imza üretme gibi bir çok kriptografik işlem uygulanmıştır. Hem TinyECC hem de bu çalışmada önerilen protokol eliptik eğri kriptolojisine dayalı olduklarından, her iki çalışmada da şifreleme ve kümeleme işlemleri sadece eliptik eğriler üzerindeki noktaların çarpımından ve toplanmasından oluşmaktadır. Bu nedenle TinyECC projesi önerilen protokolün performans değerlendirmesi için referans olarak alınmıştır.

Bu çalışmada önerilen protokolün gerçeklenmesi için Crossbow'un Imote2 türü algılayıcı düğümleri kullanılmıştır. Imote2 türü algılayıcıların genel özellikleri Tablo 1'de verilmiştir. Imote2 (416Mhz) algılayıcısı [15] için, TinyECC projesi sonuçları çalışma zamanı açısından incelendiğinde, eliptik eğri kriptolojisi ile şifreleme işlemi 24.26 ms, bir mesajın imzalanması ise 11.80 ms sürmektedir. Imote2'ye göre çok daha eski kaynak açısından sınırlı olan Mica2 (8Mhz) [15] türü algılayıcılarda bu süreler sırasıyla 3907.46 ms ve 2001.62 ms olarak ölçülmüştür. Eliptik eğri şifreleme algoritması gerçeklendiğinde tüketilen hafıza miktarları incelendiğinde, Imote2 için 17728 byte ROM ve 2064 byte RAM ihtiyacı olduğu görülmüştür.

Tablo 1. Imote2 türü algılayıcıların özellikleri [15]
(Imote2 specifications [15])

İşlemci	Intel PXA271
SDRAM Hafıza	32 MB
Flash Hafıza	32 MB
Aktif modda enerji tüketimi	31 mA
Transceiver	TICC2420
Frekans bandı (ISM)	2400-2483.5 MHz
Data rate	250 kb/s
Tx power	-24-0 dBm
I/O	USB
Güç	3xAAA, 5.0V

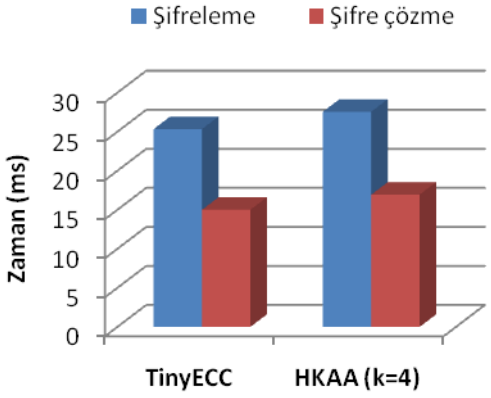
Algılayıcı düğümleri için önemli ve kısıtlı bir kaynak olan enerji tüketimi değerlerine bakıldığında ise Imote2'nin şifreleme işlemi için 5.7 mj ve imza operasyonu içinse 2.86 mj enerji harcadığı görülmektedir. Aynı işlemler için MicaZ [15] türü algılayıcıların enerji tüketimine bakıldığında ise sırasıyla 93.78 mj ve 83.84 mj değerleri görülmektedir. Ancak TinyECC projesinde eliptik eğri şifrelemesi 160 bitlik sonlu alan üzerinde gerçekleştirilmiştir. Buna karşın bu çalışmada Boneh'in eliptik eğri algoritması [14]

1024 bitlik sonlu alan kullanarak gerçeklenmiştir. Bu sebeple, TinyECC projesi enerji tüketim değerlerini karşılaştırma amacı ile kullanabilmek için, bu sonuçların 1024 bitlik sonlu alanda elde edilmiş sonuçlara çevrilmiştir. Bu bölümün geri kalan kısmında şifreleme ve kümeleme işlemleri için TinyECC projesi ve bu çalışmada elde edilen enerji tüketimi, kod boyutu ve çalışma zamanı değerleri karşılaştırılmıştır.

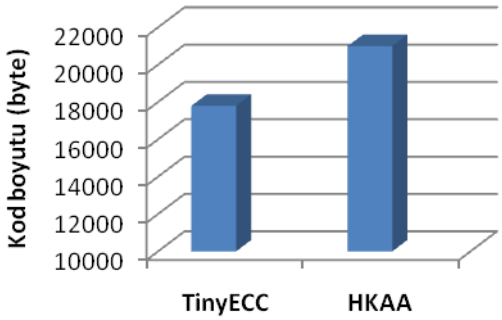
Şekil 4'te TinyECC ve bu çalışma için şifreleme ve şifre çözme zamanları verilmiştir. Şifreleme açısından iki algoritmanın da yaklaşık aynı değerleri verdikleri görülmektedir. Algoritmaları gerçekleştirmek için gerekli olan kod boyutları Şekil 5'te verilmiştir. TinyECC bu çalışmada önerilen sisteme göre daha az yer kaplamaktadır. Dahası, TinyECC'nin kod boyutu optimizasyon işlemiyle daha da düşürülebilmektedir [16]. Şekil 6'da şifreleme işlemi için kullanılan enerji miktarları verilmiştir. Önerilen protokolde veri türü sayısı arttıkça harcanan enerji artmaktadır ve 4 farklı tür algılayıcı verisi şifrelendiğinde bu çalışmada önerilen sistemin enerji tüketim performansının TinyECC'ye eşit olduğu görülmektedir. Şekil 7'de ise önerilen sistemde veri kümeleme için harcanan enerji miktarı verilmektedir. Şifreleme ile paralel olarak veri türü sayısı arttıkça harcanan enerji artmaktadır. Enerji tüketim değerleri TinyECC çalışmasında olduğu gibi, $E=U*I*t$ formülü ile yaklaşık olarak hesaplanmıştır. Güç kaynağı olarak 2 tane AA pil kullanıldığından U = 3.0 V olarak alınmıştır [16]. Ayrıca, Imote2 algılayıcı düğümleri radyo açık durumda 104Mhz hızla çalıştıklarında çekilen akım miktarı 66mA olarak alınmıştır. Yukarda verilen sonuçlar ve TinyECC projesinde elde edilen sonuçlar dikkate alındığında eliptik eğri kriptolojisine dayalı şifrelemenin ve dolayısı ile bu çalışmada önerilen gizli veri kümeleme protokolünün Imote2 türü algılayıcılar üzerinde kolaylıkla gerçeklenebilir olduğu görülmektedir.

6. SONUÇLAR VE GELECEK ÇALIŞMALAR (CONCLUSIONS AND FUTURE WORK)

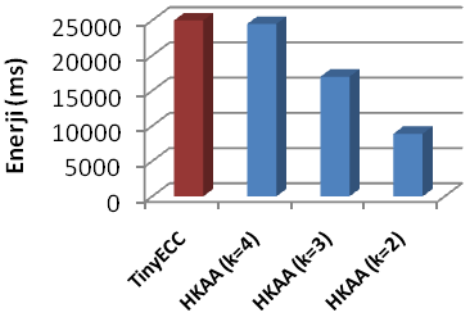
Bu çalışmada heterojen kablosuz algılayıcı ağ temelli sınır izleme sistemleri için geliştirilen yeni bir gizli veri kümeleme protokolü sunulmuştur. Önerilen protokol hem uçtan uca veri gizliliğini sağlar hem de değişik türedeki algılayıcılara ait verilerin bir arada kümelenmesine olanak sağlar. Ayrıca bu yöntemde veri kümeleme esnasında değişik veri tipleri birbirine karışmaz ve baz istasyonu kümelenmiş veriyi çözdüğünde verileri türlerine göre ayrı ayrı elde edebilmektedir. Değişik veri türlerinin gizli olarak bir



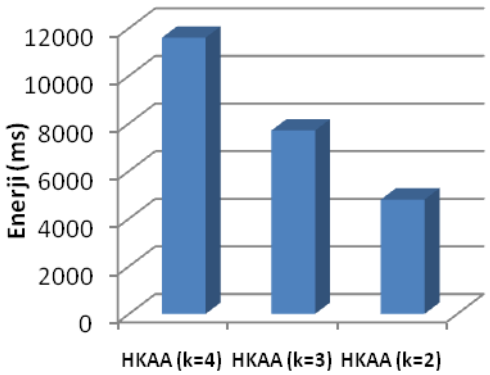
Şekil 4. Şifreleme ve şifre çözme zamanları (Encryption-decryption time)



Şekil 5. TinyECC ve önerilen protokolün şifreleme algoritmalarının kod boyutları (Code sizes of TinyECC and the proposed protocol's encryption algorithms)



Şekil 6. TinyECC ve önerilen protokolde şifreleme için enerji tüketim değerleri (Encryption energy consumption of TinyECC and the proposed protocol)



Şekil 7. HKAA'da veri kümeleme için enerji tüketim değerleri (Aggregation energy consumption of the proposed protocol)

arada kümelenebilmesi ve kümelenen verinin baz istasyonu tarafından veri türlerine göre çözülebilmesi bu çalışmanın özgün yönüdür. Yapılan güvenlik ve performas analizi sonuçları, önerilen protokolün kablosuz algılayıcı ağlarında uygulanabilir olduğunu göstermiştir.

Performans analizinde referans olarak alınan TinyECC projesinde, şifreleme işleminin mesaj büyüme oranına (message expansion rate) ait herhangi bir veri yoktur. Özellikle veri boyutunun küçük olduğu durumlarda mesaj büyüme oranı şifreleme algoritmasının verimliliğini ve uygulanabilirliğini etkiler [14]. Eliptik eğri kriptolojisine dayalı şifreleme uygulamalarında, şifrelenmiş veri eliptik eğri üzerinde bir nokta olarak ifade edilir. Her nokta P bit uzunluğunda x ve y gibi iki koordinatla belirlendiğinden, şifrelenmiş veri $2P$ bit boyutunda olur. Şifrenin kırılmasının önlenmesi için P'nin 160 ya da 320 bit uzunluğunda bir asal sayı olarak seçildiği düşünüldüğünde, her bir şifrelenmiş 320 ya da 640 bit uzunluğunda olmaktadır. Bu mesaj büyüme oranı ortalama, en büyük ya da en küçük değeri bulma gibi sayısal kümeleme işlemleri için fazla olsa da, özellikle kamera türü veriler için fazla değildir. Bu çalışmanın ilerleyen aşamalarında, önerilen protokol mesaj büyüme oranının açısından detaylı olarak incelenecektir.

KAYNAKLAR (REFERENCES)

1. Akyildiz, I.F., Su, W., Sankarasubramaniam, Y., Cayirci, E., "A survey on sensor networks", IEEE **Communications Magazine**, 40(8), 102-114, 2002.
2. Ricadela, A., Sensors everywhere, **Information Week**, Jan. 24, 2005.
3. Cam, H., Ozdemir, S., Nair, P., Muthuavinashiappan, D., Sanli, H.O., Energy-Efficient and secure pattern based data aggregation for wireless sensor networks, **Special Issue of Computer Communications on Sensor Networks**, 446-455, 2006.
4. Lee, S., Chung, T., Data Aggregation for Wireless Sensor Networks Using Self organizing Map, **Artificial Intelligence and Simulation**, V. 3397, 508-517, 2005.
5. Hu, L., Evans, D., Secure aggregation for wireless networks, **Workshop on Security and Assurance in Ad hoc Networks**, 384-392, 2003.
6. Przydatek, B., Song, D. Perrig, A., SIA : Secure information aggregation in sensor networks, **SenSys'03**, 255 – 265, 2003.
7. Cam, H., Ozdemir, S., Sanli, H.O., Nair, P., Secure differential data aggregation for wireless sensor networks, **Sensor Network Operations**, Editor: Phoha, S., La Porta, T.F., Griffin, C., Wiley-IEEE Press, 422-442, April 2006.
8. Girao, J., Westhoff, D., 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.
9. Domingo-Ferrer, J., A provably secure additive and multiplicative privacy homomorphism, **Information Security Conference**, LNCS 2433, 471-483, 2002.
10. Ozdemir, S., Concealed Data Aggregation in Heterogeneous Sensor Networks using Privacy Homomorphism, in **Proc. of ICPS 2007 : IEEE International Conference on Pervasive Services**, July 15-20, Istanbul, Turkey.
11. Castelluccia, C., Mykletun, E., Tsudik, G., Efficient aggregation of encrypted data in wireless sensor networks, **Conference on Mobile and Ubiquitous Systems: Networking and Services**, vol., no., pp. 109-117, 2005.
12. Ozdemir, S., Secure Data Aggregation in Wireless Sensor Networks via Homomorphic Encryption (manuscript in Turkish), **Journal of The Faculty of Engineering and Architecture of Gazi University**, vol.23, no.2, pp. 365-373, 2008.
13. Intanagonwiwat, C., Estrin, D., Govindan, R., Heidemann, J., Impact of network density on Data Aggregation in wireless sensor networks, **22nd International Conference on Distributed Computing Systems**, 575-578, 2002.
14. Boneh, D., God, E. and Nissim, K., Evaluating 2-DNF Formulas on Cipertexts, **Proc. Theory of Cryptography Conf. (TCC 2005),** Vol. 3374 of LNCS, Jan 2005, pp. 325-321.
15. Crossbow Inc., www.xbow.com, (Erişim: 13/02/2009)
16. Liu,A., Ning, P., TinyECC: A Configurable Library for Elliptic Curve Cryptography in Wireless Sensor Networks, in **Proceedings of the 7th International Conference on Information Processing in Sensor Networks (IPSN 2008)**, SPOTS Track, pages 245--256, April 2008.