Gazi Üniv. Müh. Mim. Fak. Der.
Cilt 23, No 2, 365-373, 2008

J. Fac. Eng. Arch. Gazi Univ.
Vol 23, No 2, 365-373, 2008

KABLOSUZ ALGILAYICI AĞLARINDA HOMOMORFİK ŞİFRELEME İLE GÜVENLİ VERİ KÜMELEME

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

(Geliş/Received: 19.07.2007; Kabul/Accepted: 12.12.2007)

ÖZET

Artık veri aktarımını önlemek ve istenilen bilgiyi özetleyebilmek için Kablosuz Algılayıcı Ağlarında (KAA) veri kümeleme vazgeçilmez bir ihtiyaçtır. Genelde saldırılara açık ortamlarda kullanılmaları sebebiyle KAA'lar için bir başka önemli gereklilikte ağ üzerinde taşınan verinin gizliliğinin sağlanmasıdır. Ancak geleneksel veri kümeleme protokollerinde veri kümeleme işlemi sırasında veri gizliliğini sağlamak mümkün değildir. Bu çalışmada literatürdeki veri kümeleme teknikleri incelenip bunların veri gizliliğini sağlayan güvenlik algoritmaları ile olan ilişkileri incelenmiştir. Buna ek olarak homomorfik şifrelemeye dayanan yeni ve orijinal bir *güvenli veri kümeleme* protokolü sunulmuştur. Geliştirilen protokolde homomorfik şifreleme tekniği kullanılarak şifrelenmiş veriler üzerinden veri kümeleme yapmak mümkündür ve bunun sonucu olarakta kümeleme işlemi sırasında veri gizliliği sağlanabilmektedir.

Anahtar Kelimeler: Algılayıcı ağları, veri kümeleme, veri gizliliği

SECURE DATA AGGREGATION IN WIRELESS SENSOR NETWORKS VIA HOMOMORPHIC ENCRYPTION

ABSTRACT

Data aggregation is essential for wireless sensor networks to reduce data redundancy and to summarize relevant and necessary information without requiring all pieces of the data. Data confidentiality is another critical requirement for wireless sensor networks as these networks are usually deployed in hostile environments. In traditional data aggregation techniques, however, it is not possible to provide data confidentiality during data aggregation. In this study, we give an overview of the existing data aggregation techniques and examine how they interact with data confidentiality algorithms. In addition, we present a novel *secure data aggregation* protocol which is based on privacy homomorphic encryption. Due to privacy homomorphism, the proposed protocol allows data aggregation over encrypted data and therefore provides data confidentiality during data aggregation.

Keywords: Sensor networks, data aggregation, data confidentiality.

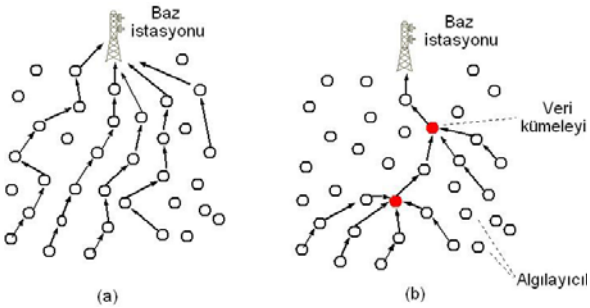
1. GİRİŞ (INTRODUCTION)

Düşük maliyetli algılayıcı mimarilerindeki gelişmeler Kablosuz Algılayıcı Ağlarını (KAA) yeni ve popüler araştırma alanı yapmıştır [1]. Bu ağlar çok sayıda sınırlı kapasiteli, kısa mesafeli vericiye sahip, düşük güçlü ve düşük maliyetli algılayıcının kolayca erişilemeyen ve çoğu zaman güvenilir olmayan bir ortama rasgele bırakılmasıyla oluşur. KAA'larda planlanmış bir ağ omurgası yoktur ve algılayıcılar tarafından ortak gayret sarf ederek toplanan veriler merkezi bir baz istasyona diğer algılayıcılar üzerinden gönderilir. Çok sayıda algılayıcıdan oluşan KAA'larda, algılayıcılar kendilerini gruplara ayırarak enerji tüketimlerini azaltırlar [1,2]. Bu gruplama işleminde her grupta bir algılayıcı veri kümeleme ve aktarımı görevlerini yapmak üzere grup lideri olarak seçilir. Güç kaynakları sınırlı olan algılayıcılardan oluşan KAA'larda artık veri aktarımını önlemek ve istenilen veriyi enerji etkin bir şekilde özetleyebilmek için veri kümeleme çok önemli bir gerekliliktir [2]. Her bir algılayıcının verisini baz istasyona

göndermektense, bir grup içerisindeki algılayıcı verilerinin grup lideri tarafından toplanarak özetlenmesi yani artık verinin ayıklanarak verinin kümelenmesi algılayıcıların enerji tüketimlerini düşürür ve böylece KAA'nın kullanım ömrünü artırır [2,3].

KAA'ların uygulama alanları askeri projelerden sağlık uygulamalarına veya iklim izleme uygulamalarına kadar uzanır [1]. Düşman hatlarının gözetlenmesi ya da sınır bölgelerinin gözetlenmesi gibi hassas KAA uygulamalarında, algılayıcılardan baz istasyonuna gizli veri aktarımını sağlayan güvenlik protokolleri mutlaka kullanılmalıdır. Ancak, algılayıcıların düşük işlemci ve radyo kapasiteleri geleneksel güvenlik protokollerinin KAA'larda uygulanmasına olanak tanımaz [4]. Dahası, algılayıcıların fiziksel güvenlikleri sağlanamadığından, algılayıcılar her an kötü niyetli kişilerce ele geçirilip, yeniden programlanabilir. Bu tip algılayıcılar "ele geçirilmiş algılayıcılar" (compromised nodes) olarak tanımlanır ve ağdaki diğer algılayıcılar genelde ele geçirilmiş algılayıcıları fark edemez [1]. Bu sebeplerden dolayı, KAA'larda kullanılacak olan güvenlik protokolleri bu ağların kendilerine has özellikleri ve "ele geçirilmiş algılayıcılar" göz önüne alınarak tasarlanmış olmalıdır.

KAA'larda hem veri kümeleme hem de veri gizliliği vazgeçilmez unsurlar olmasına rağmen, bu iki unsurun bir arada uygulanabilmesi çok zordur. Bunun başlıca sebebi, veri kümeleyicilerin aldıkları her veriye açık olarak ulaşma ihtiyacına karşın güvenlik protokollerinin verinin gönderildiği alıcı (baz istasyonu) dışında başka hiçbir algılayıcının verinin şifresini çözmesini istememesidir [4]. Bir başka deyişle 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. Ancak buna karşın veri kümeleme protokollerinde, enerji tüketimini düşürmek için grup liderleri (veri kümeleyiciler) mutlaka şifrelenmiş verileri çözmeli ve artık veriyi ayıklayarak istenilen bilgiyi özetlemelidir. Kısacası, hem veri gizliliğini hem de veri kümelemeyi bir arada yapabilmek için, KAA veri kümeleme protokolleri veri gizliliğini de hesaba katarak geliştirilmelidir [4].



Şekil 1. (a) Veri kümeleme işlemi yapılmayan KAA (b) Veri kümeleme işlemi KAA. ((a) Sensor network without data aggregation (b) Sensor network with data aggregation.)

Bu çalışmada literatürdeki "veri kümeleme" ve "güvenli veri kümeleme" üzerine yapılan çalışmalar incelenip, homomorfik şifrelemeye dayanan yeni ve orijinal bir "güvenli veri kümeleme" protokolü sunulmuştur. İlk olarak KAA'lar için yeterli güvenliğe sahip, toplama homomorfisi özelliği taşıyan, enerji etkin bir şifreleme algoritması geliştirilmiştir. Daha sonra geliştirilen şifreleme algoritmasının homomorfik özelliği kullanılarak veri kümeleyicilerin şifrelenmiş veriler üzerinden kümeleme yapabilmelerini sağlayan güvenli veri kümeleme protokolü geliştirilmiştir. Geliştirilen protokol KAA'larda veri gizliliğinin ve kümelemenin bir arada gerçekleştirilmesine olanak tanır. Yapılan benzetim çalışmaları geliştirilen protokolün sağladığı güvenliğin yanı sıra ağdaki toplam enerji tüketimini düşürdüğünü de göstermiştir.

Makalenin geri kalan kısmı şu şekilde organize edilmiştir. 2. ve 3. Bölümlerde sırasıyla KAA'larda veri kümeleme ve güvenli veri kümeleme protokolleri incelenmiştir. 4. Bölüm geliştirilen güvenli veri kümeleme protokolünü sunarken 5. Bölümde deneysel çalışma sonuçları verilmiştir. Sonuç ve çıkarımlar is 6. Bölümde yer almaktadır.

2. VERİ KÜMELEME (DATA AGGREGATION)

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 [5]. Veri kümeleme her algılayıcıda gerçekleştirilebilecek bir işlem olmasına rağmen, genelde algılayıcılar gruplara ayrılır ve her gruptaki bir algılayıcı veri kümeleyici (grup lideri) olarak görevlendirilir. Veri kümeleyiciler algılayıcılardan verileri toplar, artık veriyi ayıklar, veriyi özetler ve özetlenmiş anlamlı bilgiyi baz istasyonuna gönderir. Aksi takdirde her bir algılayıcının verisi tek tek baz istasyona gönderilmek zorundadır ve bu da gereksiz enerji tüketimine sebep olur. Şekil 1'de veri kümelemenin veri aktarımına olan etkisi gösterilmiştir. Algılayıcı ağları için çok önemli olan veri kümeleme konusunda literatürde birçok çalışma yapılmıştır [6,7,8,9].

Bu konudaki en önemli çalışmalardan birisi olan "Directed Diffusion" [6] adlı protokol enerji tasarrufunu sezgisel bir yönlendirme algoritması ve buna bağlı veri kümeleme ile sağlar. Algılayıcılardan istenen ölçüm görevleri "özellik-değer" çiftleriyle isimlendirilir. Bu "özellik-değer" çiftleri baz istasyonu tarafından ağ içerisinde yayımlanır ve bu şekilde verinin izleyeceği yol belirlenir. Veriler belirlenen yol üzerinde ilerlerken veri kümeleme gerçekleştirilir.

PEGASIS (Power-Efficient GAthering in Sensor Information Systems) [7] adlı çalışmada, algılayıcılar çemberler oluştururlar. Bir çemberde her algılayıcı veriyi ancak belirli bir yönde bir komşusundan alıp diğer komşusuna gönderebilir. Veriler çember ileriside yol alırken algılayıcılar tarafından kümelenir. Çemberde yer alan tüm algılayıcıların verisi kümelendikten sonra bir algılayıcı tarafından baz istasyonuna gönderilir. Enerji tüketimini dengelemek için baz istasyonuna veri gönderme işlemi algılayıcılar arasında sırayla yapılır.

Tiny AGgregation (TAG) veri tabanı sorgulama dillerine benzeyen bir veri toplama ve kümeleme protokolüdür [8]. TAG "dağıtım" ve "toplama" şeklinde iki aşamadan oluşur ve maksimum, minimum, toplama, ortalama, gibi verileri algılayıcılardan toplayabilir. Dağıtım aşamasında istenen bilgi bir ağaç oluşturularak ağa yollanır ve toplama aşamasında aynı ağaç üzerinde yapraklardan köke doğru veri kümelenerek baz istasyona ulaşır.

Ağdaki algılayıcıların yönlendirme açısından verimli olarak gruplanmasına dayanan LEACH [9] protokolü veri kümelemeyi yönlendirme ile birleştirmek amacıyla önerilmiştir. LEACH protokolünde grup liderleri dinamik olarak kalan enerji seviyesi gibi bir metriğe bağlı olarak seçilir. Her grup lideri grup içerisindeki algılayıcıların verisini kümeleyerek baz istasyona gönderir.

SPIN [10] algılayıcılar arasında anlaşmaya dayalı bir protokol grubudur. SPIN'de algılayıcılar veri transferinden önce komşularıyla anlaşarak gereksiz veri aktarımını önlemeye çalışırlar. Anlaşma sırasında her veri tipi algılayıcılar tarafından isimlendirilir ve aynı veri tipine sahip komşu algılayıcılardan sadece gerekli olanlar veri aktarımı yaparlar.

3. GÜVENLİ VERİ KÜMELEME (SECURE DATA AGGREGATION)

Veri gizliliği KAA'ların birçok uygulama alanı için vazgeçilmez bir gerekliliktir. 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 [4]. Bu gereklilik birçok araştırmacıyı güvenli veri kümeleme metotları üzerinde çalışmaya zorlamıştır [4,11,12,14].

Hu ve Evans geciktirilmiş kümelemeye dayanan bir güvenli veri kümeleme protokolü sunmuştur [11]. Protokol μTESLA güvenli yayımlama tekniğini [23] kullanarak veri kümeleyicilerin aldıkları verileri değiştirip değiştirmediklerini kontrol eder. Ancak bu yaklaşım veri gizliliği sağlamadığı gibi algılayıcıların ya da kümeleyicilerin doğru verileri gönderdiklerini garanti etmez.

Rasgele ve etkileşimli örnekleme teknikleri kullanarak kümelenen verilerin doğruluğunu ispatlayan bir protokol [12]'de sunulmuştur. Protokol "kümele" - "söz ver" - "ispat et" şeklinde üç aşamadan oluşur. Kümele aşamasında toplanan veriler kümelenir ve söz ver aşamasında her kümeleyici algılayıcı verilerinden bir Merkle özet ağacı [13] oluşturur ve bunu baz istasyonuna gönderir. İspat etme aşamasında baz istasyonu algılayıcılarla irtibata geçerek kümelenen verinin doğruluğunu Merkle özet ağacını kullanarak kontrol eder.

Güvenli ve enerji etkin bir veri kümeleme protokolü olan ESPDA (Energy-Efficient Secure Pattern based Data Aggregation) [4]'de sunulmuştur. Geleneksel veri kümeleme tekniklerinin aksine ESPDA algılayıcılardan grup liderlerine artık veri transferini engeller. ESPDA protokolünde, eğer algılayıcılar aynı veriyi algılarlarsa, öncelikle bu algılayıcılardan biri hariç diğerleri uyku moduna geçirilir ve aktif algılayıcılar verilerini temsil eden örüntü kodlarını üretirler. Grup liderleri veri kümeleme işlemini örüntü kodları üzerinden gerçekleştirir ve sadece farklı veriler şifrelenmiş olarak algılayıcılardan grup liderlerine gönderilir. Örüntü kodları kullanımı sayesinde grup liderleri veri kümeleme işlemini şifrelenmiş verileri kullanarak yapabilir. Bunun sonucunda algılayıcılar baz istasyon ile uçtan uca güvenli iletişim kurabilirler.

ESPDA protokolünün bir uzantısı olarak, işlenmemiş verilerin algılayıcılardan grup liderlerine transferini azaltan güvenli diferansiyel veri kümeleme (SDDA) protokolü [14]'de sunulmuştur. Algılayıcılardan grup liderlerine artık veri transferini azaltmak için SDDA işlenmemiş veri yerine veriler arasındaki farkı (diferansiyel veri) transfer eder ve veri kümelemeyi verileri temsil eden örüntü kodlarını kullanarak yapar. SDDA in veri transferi sırasında, işlenmemiş veri bir referans veri ile karşılaştırılır ve sadece fark verisi transfer edilir.

[15]'de yazarlar homomorfik şifrelemeye dayalı bir veri kümeleme protokolü sunmuşlardır. Önerilen metot [16]'da geliştirilen ve çok fazla işlem gücü gerektiren homomorfik şifreleme algoritmasını kullanır. Fakat günümüzün sınırlı kaynaklara sahip algılayıcı düğümleri bu tip şifreleme algoritmalarını uygulayabilecek kapasiteye sahip değildirler [1]. [24]'de düşük kapasiteli algılayıcılara daha uygun bir güvenli veri kümeleme algoritması geliştirilmiştir. Bu makalede geliştirilen veri kümeleme protokolü ile [24]'de önerilen protokol şifreleme metodu olarak birbirlerine benzese de, gizli anahtar dağılımı ve kullanımında birbirlerinden çok farklıdırlar. Temel olarak [24]'de geliştirilen teknik *merkezi* bir yaklaşım sergiler ve ağdaki tüm algılayıcı düğümlerinin merkez

istasyonla bir gizli anahtar paylaşması gerektirir. Algılayıcı ağlarında merkezi yaklaşımlar tercih edilmezler [1]. Buna karşın, bu makalede önerilen teknik *dağıtık* yaklaşım göz önüne alınarak geliştirilmiştir ve her bir algılayıcı düğümü kendisiyle merkez istasyon arasındaki kendine en yakın iki veri kümeleyici ile anahtar paylaşımında bulunur. [24]'de önerilen teknikte şifrelenmiş ve kümelenmiş verinin çözülebilmesi için veri gönderen bütün düğümlerin ID numaraları merkez istasyona gönderilmek zorundadır ve bu da veri aktarım miktarını önemli ölçüde artırır. Bu makalede geliştirilen teknikte ise düğüm ID'leri sadece veri kümeleyicilere kadar gönderilir. Bunun yanı sıra, [24]'de önerilen teknikte her bir düğüm baz istasyonu ile paylaştığı anahtarı her şifreleme işlemi öncesinde senkronize etmelidir. Düğümlerin ve baz istasyonunun birbirlerinden çok uzak olmaları sebebiyle senkronizasyon işlemini çok miktarda veri aktarımına sebep olur. Dahası, baz istasyonu bütün düğümlerle anahtar paylaştığından, her düğümle senkronizasyon yapmak durumundadır ve gerçek zamanlı uygulamalarda bu önemli bir zaman kaybına yol açar. Bu makalede geliştirilen teknikte ise, dağıtık bir yaklaşım ile her bir algılayıcı düğümü sadece veri kümeleyicisi ile paylaştığı rasgele sayı üreticisini senkronize eder.

4. HOMOMORFİK ŞİFRELEME İLE GÜVENLİ VERİ KÜMELEME (SECURE DATA AGGREGATION VIA HOMOMORPHIC ENCRYPTION)

Güvenli veri kümelemeyi sağlamak için simetrik anahtar şifrelemesi kullanıldığında, kümeleyicilerin önce şifrelenmiş veriyi çözmeleri daha sonra da kümelemeyi yapıp sonucu tekrar şifrelemeleri gerekmektedir. Ancak bu veri gizliliğin kaybolması anlamına gelmektedir. Buradan yola çıkarak hem uçtan uca veri gizliliğini sağlama hem de güvenli veri kümelemeyi başarmak için, bu çalışmada homomorfik şifreleme tekniklerinden faydalanılmıştır [15].

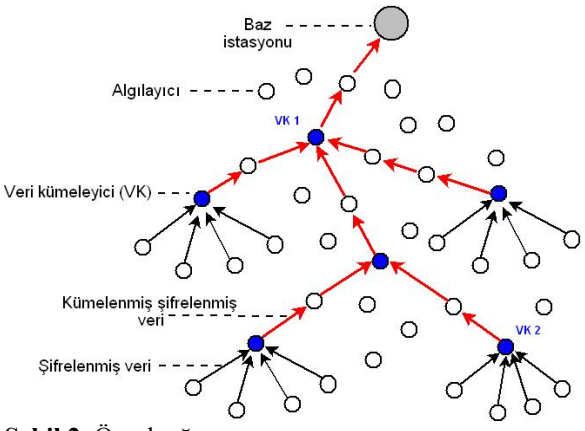
Homomorfik şifreleme açık metin üzerinde yapılan matematiksel bir işlemin şifrelenmiş bir metin üzerinde yapılabilmesini sağlayan bir şifreleme türüdür [16]. Örnek olarak *E*'nin şifrelemeyi *D*'nin şifre çözme işlemini, *K*'nin de şifrelemede kullanılan gizli anahtarı temsil ettiğini kabul edelim. Ek olarak + ve * işaretleri de Q seti üzerinde toplama ve çarpma işlemlerini temsil etsin. Eğer

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

ise şifreleme fonksiyonu *E*'nin homomorfik toplama özelliği taşıdığı kabul edilir ve eğer

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

ise 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



Şekil 2. Örnek ağ yapısı.(Example of network structure.)

uygulayabilirler. Homomorfik gizlilik simetrik ya da açık anahtar alt yapısı kullanılarak gerçekleştirilebilir [16,17]. Ancak açık anahtar şifrelemesinin gerektirdiği yüksek işlemci gücünü ve enerji ihtiyacını düşük kapasiteli ve sınırlı kaynaklara sahip algılayıcılarla karşılamak mümkün değildir [1,4]. Bu sebeple bu çalışmada enerji etkin, simetrik anahtar alt yapısını kullanan bir homomorfik şifreleme algoritması geliştirilmiştir. Geliştirilen bu şifreleme algoritması KAA'larda sıklıkla ihtiyaç duyulan toplama homomorfisi özelliğine sahiptir [15]. Geliştirilen şifreleme algoritması ve güvenli veri kümelemede nasıl kullanıldığı bu bölümün geri kalan kısmında anlatılmıştır.

4.1 Ağ ve sistem modeli (Network and system model)

Bu çalışmada gruplara ayrılmış çok sayıda algılayıcıdan ve kaynak açısından zengin bir baz istasyonundan oluşan statik bir algılayıcı ağı öngörülmüştür. Ağda Mica2 [17] tipi algılayıcılar kullanılmıştır. Mica2 tipi algılayıcılar 4Mhz 8bit Atmel mikro işlemciye, 128KB komut hafızasına ve 4KB RAM'e sahiptirler. Ağdaki algılayıcılardan bazıları veri kümeleyici (VK) olarak görevlendirilmişlerdir. VK'lar çevrelerindeki algılayıcılardan ve diğer VK'lardan aldıkları verileri kümelemekle görevlidirler. Enerji tüketimini dengelemek için her algılayıcı belli bir süre VK'lık görevini yürütür [9]. Örnek bir ağ yapısı Şekil 2'de gösterilmiştir.

4.2 Homomorfik şifreleme algoritması (Homomorphic encryption algorithm)

Bu alt bölümde KAA'ların veri gizliliği ve kümeleme ihtiyaçlarını bir arada karşılayabilecek olan homomorfik şifreleme algoritması verilmiştir. Öncelikle *D*'nin bir veri setini, *K*'nin bir gizli anahtar setini ve *R*'nin de bir rasgele sayı setini temsil ettiğini kabul edelim, bu durumda geliştirilen toplama homomorfisi özelliğine sahip şifreleme fonksiyonu *E* aşağıdaki gibi ifade edilir.

$$E:(D,K,R)\to D$$
$$E(d,k,r)=(d+k+r)\bmod n$$
$$\forall d\in D,\forall k\in K,\forall r\in R$$

Önerme 1: E fonksiyonu toplama homomorfisi özelliğine sahiptir.

İspat: d_1 ve d_2 D setine ait iki ayrı veriyi, k_1 ve k_2 K setine ait iki ayrı gizli anahtarı ve r_1 ve r_2 de R setine ait iki ayrı rasgele sayıyı temsil etsin. Bu durumda

$$E(d_1,k_1,r_1)=(d_1+k_1+r_1)\bmod n$$
$$E(d_2,k_2,r_2)=(d_2+k_2+r_2)\bmod n$$
$$E(d_1,k_1,r_1)+E(d_2,k_2,r_2)=$$
$$(d_1+k_1+r_1+d_2+k_2+r_2)\bmod n$$
$$E(d_1,k_1,r_1)+E(d_2,k_2,r_2)=$$
$$E(d_1+d_2,k_1+k_2,r_1+r_2)$$

ifadeleri $\forall d\in D,\forall k\in K,\forall r\in R$ için doğru olduğundan E fonksiyonu toplama homomorfisi özelliği taşır. □

Önerilen şifreleme algoritmasında dikkat edilmesi gereken nokta, veri gizliliğinin tam olarak sağlanabilmesi için her şifreleme operasyonunda rasgele sayı *r*'nin değiştirilmesi gerekir. Bu çalışmada "sahte rasgele sayı üreticileri" (SRSU) (Pseudo Random Number Generator) kullanılarak *r*'nin her şifreleme işleminde değiştirilmesi sağlanmıştır. Rasgele sayının sürekli olarak değiştirilmesi şifrelenmiş verilerin "seçilmiş açık metin" ve "seçilmiş şifrelenmiş metin" gibi ataklara karşı korunmasını sağlar [20].

Önerme 2: E şifreleme fonksiyonu veri gizliliğini sağlar.

İspat: Şifrelenecek veri *d*'nin her biri *k* boyutunda parçalara bölünerek şifrelenecek olduğunu kabul edelim ve her bir parçayı *m* ile gösterelim. E şifreleme fonksiyonun veri gizliliğini sağladığını göstermek için E ile şifrelenmiş bir mesaj *m* için, *m* mesajını "şifrelenmiş veriyi görerek doğru olarak tahmin etme olasılığı" ile "şifrelenmiş veriyi görmeden doğru olarak tahmin etme olasılığının" birbirine eşit olduğu göstermek yeterlidir. (Gösterim kolaylığı açısından rasgele sayı *r* ispata dahil edilmemiştir.)

$$\forall m,\forall c,\Pr[m=M\mid E(m,k)=c]=\Pr[m=M]$$

$$\Pr[m=M\mid E(m,k)=c]=\frac{\Pr[m=M\wedge E(m,k)=c]}{\Pr[E(m,k)=c]}$$
$$\Pr[m=M\wedge E(m,k)=c]=$$
$$\Pr[m=M]\Pr[E(m,k)=c\mid m=M]$$

Eğer $m=M$ olduğunu biliyorsak, $E(m,k)=c$ olması için K'yi doğru olarak bilmemiz gerekir. k'nin herhangi bir değeri alma olasılığı 2^{-k} olduğundan $\Pr[E(m,k)=c\mid m=M]=2^{-k}$ yazılabilir. Buradan $\Pr[m=M\wedge E(m,k)=c]=\Pr[m=M]2^{-k}$ yazılabilir. $\Pr[E(m,k)=c]$ ise aşağıdaki gibi ifade edilebilir.

$$\Pr[E(m,k)=c]=\sum_{m'\in\{0,1\}^k}\Pr[m'=M]\Pr[E(m,k)=c\mid m'=M]$$
$$\Pr[E(m,k)=c]=\sum_{m'\in\{0,1\}^k}\Pr[m'=M]2^{-k}$$
$$\Pr[E(m,k)=c]=2^{-k}\sum_{m'\in\{0,1\}^k}\Pr[m'=M]=2^{-k}$$

Buradan $\Pr[m=M\mid E(m,k)=c]$ aşağıdaki gibi yazılabilir

$$\Pr[m=M\mid E(m,k)=c]=\frac{\Pr[m=M\wedge E(m,k)=c]}{\Pr[E(m,k)=c]}$$
$$\Pr[m=M\mid E(m,k)=c]=\frac{2^{-k}\Pr[m=M]}{2^{-k}}$$
$$\Pr[m=M\mid E(m,k)=c]=\Pr[m=M]$$

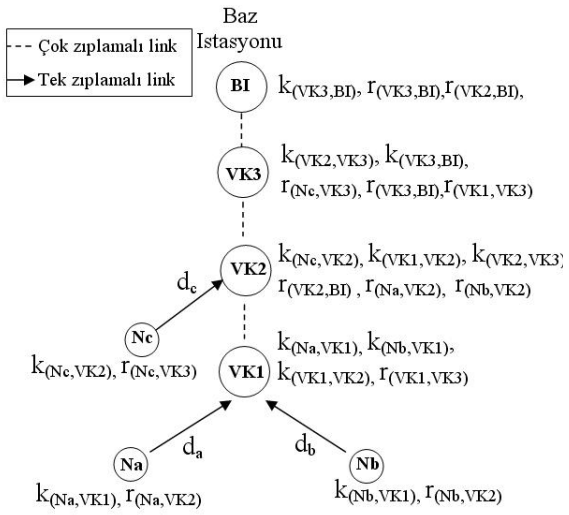
Bu da E fonksiyonun ürettiği şifrelenmiş verinin orijinal veriden bağımsız olduğunu yani veri gizliliği sağladığını ispat eder. □

4.3 Gizli anahtar paylaşımı (Secret key sharing)

Geliştirilen homomorfik şifreleme algoritmasının ağ içerisinde kullanılabilmesi için *k* ve *r*'leri gerekli algılayıcılara ve kümeleyicilere uygun olarak dağıtacak bir anahtarlama protokolüne ihtiyaç vardır. Her algılayıcı ve VK verisini gönderdiği baz istasyona giden yol üzerindeki bir sonraki VK ile [22]'de geliştirilen anahtar dağıtımı protokolünü kullanarak bir gizli anahtar üzerinde anlaşır. Buna ek olarak her bir algılayıcı ve VK baz istasyona giden yol üzerindeki ikinci VK ile ortak tohumla başlatılmış bir SRSU paylaşır. Bir SRSU'yu paylaşan bir algılayıcı çifti, her şifreleme operasyonunda paylaştıkları SRSU'yu senkronize olarak çalıştırırlar. Böylece her şifreleme operasyonunda kullanılan rasgele sayı değiştirilmiş olur. Anahtar dağıtımını daha iyi açıklayabilmek için Şekil 3'te örnek bir ağ verilmiştir. Şekilde görüldüğü gibi algılayıcı *Na* veri kümeleyici *VK1* ile $k_{(Na,VK1)}$ gizli anahtarını paylaşırken, veri kümeleyici *VK2* ile ortak SRSU'dan elde edilmiş $r_{(Na,VK2)}$ rasgele sayısını paylaşır. Aynı şekilde *Nb, Nc, VK1, VK2* ve *VK3*'ün sahip oldukları gizli anahtarlar ve rasgele sayılar Şekil 3'te verilmiştir.

4.4 Güvenli veri kümeleme (Secure data aggregation)

Ağ kurulumundan sonra algılayıcılar ve VK'lar arasında gizli anahtar dağılımı gerçekleştirilir ve baz istasyonu ağdan toplamak istediği bilgiyi (sıcaklık, nem, ışık vb.) μTESLA [23] tekniğini kullanarak güvenli bir şekilde yayınlar. İstenilen bilgi doğrultusunda algılayıcılar ölçümlerini yapar ve bu ölçümlere ait veriyi bölüm 4.2'de verilen homomorfik şifreleme algoritmasıyla şifreleyerek VK'lara gönderirler. Her VK şifrelenmiş verilerin şifrelerini çözmeden kümeler ve kümelenmiş veriyi tekrar şifreler. Bu şekilde katmanlı olarak kümelenen verinin şifresi ancak baz istasyon tarafından çözülebilir.



Şekil 3. Gizli anahtar ve rasgele sayı dağılımı örneği. Her algılayıcının sahip olduğu gizli anahtar ve rasgele sayılar algılayıcının yanında gösterilmiştir.(Secret key and random number distribution example. Each sensor's secret key and random numbers are given next to that sensor.)

Daha kolay anlaşılabilmesi için, protokolün isleyişi detaylı olarak aşağıdaki örnek kullanılarak anlatılmıştır.

Örnek: Şekil 3'te algılayıcılar *Na* ve *Nb* ölçüm değerleri olan d_a ve d_b'yi *VK1*'e şifreleyerek aşağıdaki gibi gönderirler.

$$Na \rightarrow VK1 : (d_a + k_{Na,VK1} + r_{Na,VK2}) \bmod n$$
$$Nb \rightarrow VK1 : (d_b + k_{Nb,VK1} + r_{Nb,VK2}) \bmod n$$

VK1 bu şifrelenmiş verilerden kendine ait olan gizli anahtarları ($k_{Na,VK1}$ ve $k_{Nb,VK1}$) çıkartır ve kümeleme işlemini yapar

$$(d_a + r_{Na,VK2}) \bmod n + (d_b + r_{Nb,VK2}) \bmod n =$$
$$(d_a + d_b + r_{Na,VK2} + r_{Nb,VK2}) \bmod n$$

VK1 bu yeni kümelenmiş veriyi *VK2* ile paylaştığı gizli anahtarı ve *VK3* ile paylaştığı rasgele sayıyı kullanarak yeniden şifreler ve daha sonrada kümelenmiş şifrelenmiş veriyi *VK2*'ye gönderir.

$$VK1 \rightarrow VK2 : (d_a + d_b + k_{VK1,VK2}$$
$$+ r_{VK1,VK3} + r_{Na,VK2} + r_{Nb,VK2}) \bmod n$$

Ayrıca, *VK2* algılayıcı *Nc* den de d_c verisini aşağıdaki şekilde alır.

$$Nc \rightarrow VK2 : (d_c + k_{Nc,VK2} + r_{Nc,VK3}) \bmod n$$

VK2 bu verileri aldığında önce kendine ait olan gizli anahtar ve rasgele sayıları ($k_{VK1,VK2}$, $k_{Nc,VK2}$, $r_{Na,VK2}$ ve $r_{Nb,VK2}$) çıkartır ve kümeleme işlemini gerçekleştirir.

$$(d_a + d_b + r_{VK1,VK3}) \bmod n + (d_c + r_{Nc,VK3}) \bmod n$$
$$= (d_a + d_b + d_c + r_{Nc,VK3} + r_{VK1,VK3}) \bmod n$$

VK2 bu kümelenmiş veriyi *VK3* ile paylaştığı gizli anahtarı ve baz istasyonu *BI* ile paylaştığı rasgele sayıyı kullanarak yeniden şifreler ve daha sonrada kümelenmiş şifrelenmiş veriyi *VK3*'e gönderir.

$$VK2 \rightarrow VK3 : (d_a + d_b + d_c + k_{VK2,VK3} +$$
$$r_{VK2,BI} + r_{Nc,VK3} + r_{VK1,VK3}) \bmod n$$

VK3'e başka veri gelmediği için kümeleme işlemine gerek yoktur, bu sebepten *VK3* aldığı veriden kendine ait olan gizli anahtar ve rasgele sayıları ($k_{VK2,VK3}$, $r_{Nc,VK3}$ ve $r_{VK1,VK3}$) çıkartır ve *BI* ile paylaştığı gizli anahtarı ve rasgele sayıyı kullanarak yeniden şifreler ve daha sonrada bu veriyi *BI*'ye gönderir.

$$VK3 \rightarrow BI : (d_a + d_b + d_c +$$
$$k_{VK3,BI} + r_{VK3,BI} + r_{VK2,BI}) \bmod n$$

BI bu şifrelenmiş veriden kendine ait değerleri ($k_{VK3,BI}$, $r_{VK3,BI}$ ve $r_{VK2,BI}$) çıkardığında ağda toplanan kümelenmiş veriyi elde etmiş olur.

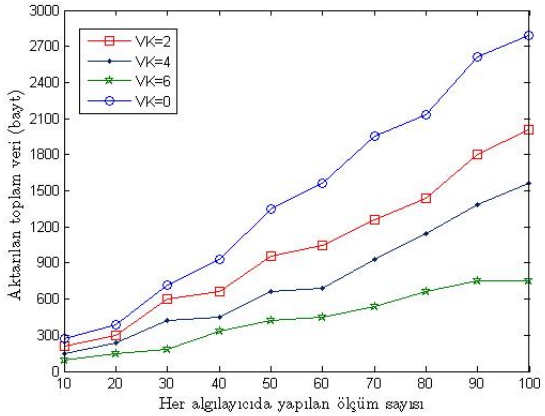
$$(d_a + d_b + d_c) \bmod n =$$
$$(d_a + d_b + d_c + k_{VK3,BI} + r_{VK3,BI} + r_{VK2,BI}) \bmod n$$
$$- (k_{VK3,BI} + r_{VK3,BI} + r_{VK2,BI}) \bmod n$$

Örnekte de görüldüğü üzere şifreleme algoritmasının toplama homomorfisi özelliği sayesinde her *VK* verinin içeriğini bilmeden kümeleme yapabilmekte ve baz istasyonu da şifrelemiş veriyi çözerek kümelenmiş veriye ulaşabilmektedir.

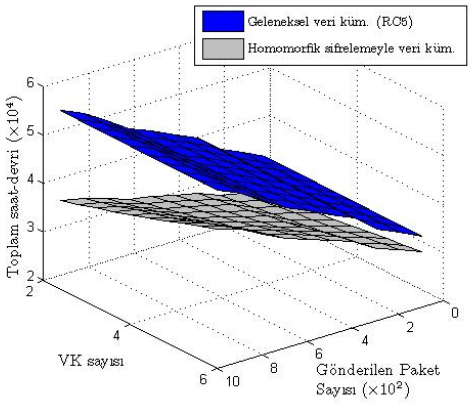
5. DENEYSEL SONUÇLAR (EXPERIMENTAL RESULTS)

Deneysel çalışmalarda algılayıcı ağları için geliştirilmiş olan QualNet ağ benzeticisi [25] kullanılmıştır. Her bir benzetim senaryosu 20 defa çalıştırılmış ve sonuçların ortalaması alınmıştır. Benzetim senaryolarında 100 algılayıcı ve ağ içerisinde dağıtılmış değişik sayıda (2-6) VK kullanılmıştır. Algılayıcıların gönderdiği paket büyüklüğü 64-bit olarak sabitlenmiş ve geleneksel veri kümeleme protokolünde RC5 simetrik şifreleme algoritması kullanıldığı varsayılmıştır.

İlk olarak veri kümelemenin veri aktarımına olan etkisi incelenmiş ve sonuçlar Şekil 4'de verilmiştir. Şekilde görüldüğü üzere ağdaki veri kümeleyici sayısı arttıkça, ağdaki toplam veri aktarımı düşmektedir. Bunu başlıca sebebi veri kümeleyicilerin komşu algılayıcılardan aldıkları verilerden artık veriyi ayıklamaları ve özet bilgiyi baz istasyonuna göndermeleridir. Veri aktarımı algılayıcılar için



Şekil 4. Veri kümelemenin ağdaki toplam veri aktarımına olan etkisi. Veri kümeleyici sayısı arttıkça ağdaki toplam veri aktarımı düşer ve bu da ağın kullanım ömrünün artmasına sebep olur.(The effect of data aggregation on data transmission. As the number of data aggregators increases the total amount of data transmission is decreased which results in prolonging the lifetime of the network.)



Şekil 5. Geleneksel veri kümeleme protokolü ile bu çalışmada geliştirilen güvenli veri kümeleme protokolünün enerji tüketimlerinin karşılaştırılması. Enerji tüketimi protokolde kullanılan toplam saat devri olarak gösterilmiştir. (Energy consumption comparison of traditional data aggregation protocol and our secure data aggregation protocol. Energy consumption is total clock cycle measurement of the protocol.)

önemli bir enerji kaybına sebep olduğundan [1,4], ağdaki veri aktarımı miktarının düşmesi ağın kullanım ömrünü uzatır.

Ayrıca, geliştirilen protokolün enerji tüketim performansı geleneksel veri kümeleme protokolü ile karşılaştırılmıştır. Geleneksel veri kümeleme protokolünde *VK*'ların aldıkları verinin önce şifresini çözüp, kümeleme işlemini yapıp daha sonrada tekrar şifreleme yaptıkları kabul edilmiştir. Tablo 1'de Mica2 tipi algılayıcıların 32 bitlik verilerdeki çeşitli operasyonlar için saat-devri (clock-cycle) ölçümleri verilmiştir [15]. Bu ölçümler kullanılarak gerçekleştirilen benzetim çalışmasının sonuçları her kümeleyicide şifre çözümünü ve tekrar şifrelemeyi gerektiren geleneksel veri kümeleme için ve güvenli veri kümeleme protokolü için Şekil 5'de karşılaştırılmıştır. Şekilde görüldüğü üzere geliştirilen güvenli veri kümeleme protokolünün enerji tüketimi geleneksel protokolden daha azdır. Bunun sebebi hem kullanılan şifreleme algoritmasının enerji etkin olması hem de *VK*'ların aldıkları her veri için şifre çözme/ şifreleme işlemi yapmalarına gerek olmamasıdır.

Tablo 1. Mica2 tipi algılayıcıların saat-devri ölçümleri ([15] den alınmıştır).(Clock-cycle measurements of Mica2 motes. Adopted from [15].)

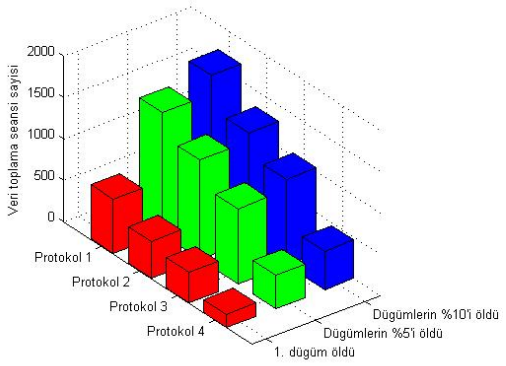
Şifreleme	236
Şifre Çözme	236
Toplama	4
Karşılaştırma	4
Çarpma	40
Bölme	700
Kare Alma	1500

Bir diğer deneysel çalışmada geliştirilen protokolün KAA ömrünü nasıl etkilediği incelenmiştir. Benzetim senaryosunda veri kümelemenin etkisini ortaya çıkarmak amacıyla 6 tane VK kullanılmıştır ve her bir algılayıcı düğümünün başlangıçta 2J enerjiye sahip olduğu kabul edilmiştir. Çalışmada enerji modeli olarak [26] geliştirilen model ve gerçekleme senaryosu kullanılmıştır. Bu senaryoda baz istasyonu ağdan periyodik olarak veri ister ve her bir isteğin cevaplanması bir "veri toplama seansı" olarak kabul edilir [26].

Ağ ömrü aşağıdaki iki şekilde tanımlanmış ve iki tanım içinde ölçümler yapılmıştır: *(i)* KAA ömrü: Ağın kurulmasından ilk algılayıcı düğümünün ölmesine kadar gerçekleştirilebilen veri toplama seansı sayısı *(ii)* KAA ömrü: Ağın kurulmasından sonra algılayıcı düğümlerinin belirli bir yüzdesinin ölümüne kadar gerçekleştirilebilen veri toplama seansı sayısı.

Benzetim çalışmasında bu iki ağ ömrü tanımı dahilinde ilk düğüm ölene kadar, düğümlerin %5'i ölene kadar ve düğümlerin %10'u ölene kadar yapılan veri toplama seansı sayıları gözlemlenmiştir ve sonuçlar Şekil 6'da verilmiştir. Şekil 6'da gözlemlenen protokoller ise şöyledir: *(i)* Protokol 1. Şifreleme olmadan yapılan veri kümeleme protokolü, *(ii)* Protokol 2. Bu çalışmada önerilen protokol, *(iii)* Protokol 3. Geleneksel veri kümeleme protokolü (her VK'da şifreleme/çözülme yapılan yapılması), *(iv)* Protokol 4. Hiç veri kümeleme yapılmayan protokol.

Şekilde görüldüğü gibi şifreleme olmadan sadece kümeleme yapılan 1. protokol en uzun ağ ömrünü verir. Ancak bu durumda veri gizliliğini sağlamak mümkün değildir. Hiç kümeleme yapılmayan 4. protokol ise en kısa ağ ömrüne sahiptir. Bunu sebebi algılayıcı düğümlerinin gönderdiği tüm verilerin baz istasyona gönderiliyor olmasıdır. Güvenliği ve veri



Şekil 6. Değişik veri kümeleme protokollerinin ağ ömrüne olan etkileri. (Effects of various data aggregation protocols on network lifetime)

kümelemeyi bir arada gerçekleştiren çözümlerden bu çalışmada önerilen protokol (2. protokol), her VK'da şifreleme/çözülme yapılan 3. protokolden ortalama %13 daha uzun ağ ömrüne sahiptir. Bu da geliştirilen şifreleme algoritmasının daha az enerji harcaması ve her VK'da şifreleme/çözülme yapılmamasından kaynaklanmaktadır.

6. SONUÇ (CONCLUSION)

Kablosuz algılayıcı ağlarının birçok uygulama alanında veri kümeleme ve veri gizliliği vazgeçilmez birer gerekliliktir. Ancak veri kümeleme işleminde kümeleyiciler şifrelenmemiş veriye ihtiyaç duyduklarından, veri kümeleme ve veri gizliliğinin bir arada sağlanması mümkün değildir. Bu çalışmada veri kümeleyicilerin şifrelenmiş veri üzerinden kümeleme işlemini gerçekleştirebildikleri homomorfik şifrelemeye dayalı yeni ve orijinal bir "güvenli veri kümeleme" protokolü sunulmuştur. Veri gizliliğini ve veri kümelemeyi bir arada sağlayabilmesinin yanı sıra, geliştirilen protokolün enerji tüketiminin geleneksel veri kümeleme protokollerine göre daha düşük olduğu deneysel çalışmalarla gösterilmiştir.

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. 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.
3. Fan, K.W., Liu, S., Sinha, P., Structure-free Data Aggregation in Sensor Networks, **IEEE Transactions on Mobile Computing**, 6(8), 929-942, 2007.
4. 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.
5. Lee, S., Chung, T., Data Aggregation for Wireless Sensor Networks Using Self organizing Map, **Artificial Intelligence and Simulation**, V. 3397, 508-517, 2005.
6. Intanagonwiwat, C., Govindan, R., Estrin, D., Heidemann, J., Silva, F., Directed Diffusion for Wireless Sensor Networking, **IEEE/ACM Transactions on Networking,** vol.11, no. 1, 2-16, 2003.
7. Lindsey, S., Raghavendra, C.S., PEGASIS: Power Efficient Gathering in Sensor Information Systems, **IEEE Aerospace Conference**, 1125-1130, 2002.
8. Madden, S.R., Franklin, M.J., Hellerstein, J.M., Hong, W., TAG: tiny aggregation service for ad-hoc sensor networks, **The 5th symposium on Operating systems design and implementation**, 131-146, 2002.
9. Heinzelman, W., Chandrakasan, A., Balakrishnan, H., Energy-Efficient Communication Protocol for Wireless Micro Sensor Networks, **The 33rd Hawaii International Conference on System Sciences**, 1-10, 2000.
10. Heinzelman, W., Kulik, J., Balakrishnan, H., Adaptive Protocols for Information Dissemination in Wireless Sensor Networks, **The 5th ACM/IEEE Mobicom Conference**, 1999.
11. Hu, L., Evans, D., Secure aggregation for wireless networks, **Workshop on Security and Assurance in Ad hoc Networks**, 384-392, 2003.
12. Przydatek, B., Song, D. Perrig, A., SIA : Secure information aggregation in sensor networks, **SenSys'03**, 255 – 265, 2003.
13. Merkle, R.C., Protocols for public key cryptosystems, **IEEE Symposium on Research in Security and Privacy**, 122-134,1980.
14. 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.
15. 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.
16. Domingo-Ferrer, J., A provably secure additive and multiplicative privacy homomorphism, **Information Security Conference**, LNCS 2433, 471-483, 2002.
17. Okamoto, T., Uchiyama, S., A new Public-Key Cryptosystem as Secure as Factoring, **Advances in Cryptology - EUROCRYPT'98**, 208-318, 1998.
18. Mica2 Motes, Crossbow Technologies Inc., http://www.xbow.com.

19. Seetharam, D., Rhee, S., An efficient pseudo random number generator for low-power sensor networks, **29th Annual IEEE International Conference on Local Computer Networks**, 560-562, 2004.
20. Law, Y. W., Doumen, J., Hartel, P., Survey and benchmark of block ciphers for wireless sensor networks, **ACM Transactions on Sensor Networks**, 65-93, 2006.
21. Bellare, M., Desai, A., Jokipii, E., Rogaway, P., A concrete security treatment of symmetric encryption. **IEEE Symposium on Foundations of Computer Science**, 394–403, 1997.
22. Liu, D., Ning, P., Establishing pairwise keys in distributed sensor networks, **10th ACM Conference on Computer and Communications Security (CCS)**, 52-61, 2003.
23. Perrig, A., Szewczyk, R., Tygar, D., Wen, V., Culler, D., SPINS: Security protocols for sensor networks, **Wireless Networks Journal (WINE)**, 521-534, 2002.
24. 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.
25. QualNet Network Simulator by Scalable Network Technologies., www.scalable-networks.com/
26. Heinzelman, W. R., Chandrakasan, A. and Balakrishnan, H. "An Application-Specific Protocol Architecture for Wireless Microsensor Networks," **IEEE Transactions on Wireless Communications**, vol. 1, no. 4, pp. 660–670, October 2002.