KABLOSUZ ALGILAYICI AĞLARINDA VERİ KÜMELEME UYGULAMALARI

Arda ÖZTÜRK

YÜKSEK LİSANS TEZİ
BİLGİSAYAR MÜHENDİSLİĞİ

GAZİ ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

ŞUBAT 2012
ANKARA

KABLOSUZ ALGILAYICI AĞLARINDA VERİ KÜMELEME UYGULAMALARI

Arda ÖZTÜRK

YÜKSEK LİSANS TEZİ
BİLGİSAYAR MÜHENDİSLİĞİ

GAZİ ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

ŞUBAT 2012
ANKARA

Arda ÖZTÜRK tarafından hazırlanan "KABLOSUZ ALGILAYICI AĞLARINDA VERİ KÜMELEME UYGULAMALARI" adlı bu tezin Yüksek Lisans tezi olarak uygun olduğunu onaylarım.

Yrd. Doç. Dr. Suat ÖZDEMİR …….…….
Tez Danışmanı, Bilgisayar Mühendisliği Anabilim Dalı

Bu çalışma, jürimiz tarafından oy birliği ile Bilgisayar Mühendisliği Anabilim Dalında Yüksek Lisans tezi olarak kabul edilmiştir.

Prof. Dr. Ali AKCAYOL …….…….
Bilgisayar Mühendisliği Anabilim Dalı, G.Ü.

Yrd. Doç. Dr. Suat ÖZDEMİR …….…….
Bilgisayar Mühendisliği Anabilim Dalı, G.Ü.

Yrd. Doç. Dr. Özcan ÖZTÜRK …….…….
Bilgisayar Bilimleri Anabilim Dalı, Bilkent Ü.

Tarih:
03/02/2012

Bu tez ile G.Ü. Fen Bilimleri Enstitüsü Yönetim Kurulu Yüksek Lisans derecesini onamıştır.

Prof. Dr. Bilal TOKLU …….…….
Fen Bilimleri Enstitüsü Müdürü

TEZ BİLDİRİMİ

Rapor içindeki bütün bilgilerin etik davranış ve akademik kurallar çerçevesinde elde edilerek sunulduğunu, ayrıca tez yazım kurallarına uygun olarak hazırlanan bu çalışmada bana ait olmayan her türlü ifade ve bilginin kaynağına eksiksiz atıf yapıldığını bildiririm.

Arda ÖZTÜRK

KABLOSUZ ALGILAYICI AĞLARINDA VERİ KÜMELEME UYGULAMALARI

(Yüksek Lisans Tezi)

Arda ÖZTÜRK

GAZİ ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ
Şubat 2012

ÖZET

Kablosuz Algılayıcı Ağ (KAA) uygulamaları sahip oldukları avantajlardan dolayı günümüzde birçok alanda kullanılmaktadır. Uygulama gereksinimleri doğrultusunda KAA' ları oluşturan algılayıcı cihazlar genellikle çok küçük boyutlarda ve tek kullanımlık olarak tasarlanmaktadır. Bu nedenden dolayı bu cihazlar genellikle kısıtlı işlem gücü, enerji kaynaklarına ve iletişim kapasitesine sahiptirler. Bu kısıtlar veri iletişimi sırasında tekrarlı olarak gönderilen paketlerin engellenmesi gerekliliğini ortaya çıkartmaktadır. Enerji verimliliğini sağlamak için geliştirilen HEED, LEACH gibi veri demetleme yaklaşımları, ağın kendi içerisinde gruplara ayrılmasını sağlayarak ağ içerisinde veri akışının kontrol altına alınmasını sağlarlar. Demetleme yöntemleri genel olarak enerji verimliliğine katkı sağlamakla birlikte KAA' ların kendine özgü karakteristik özellikleri dikkate alındığında enerji verimliliğinin daha da iyileştirilebileceği görülmüştür. Bu çalışma dahilinde benimsenen Veri kümeleme yaklaşımları sayesinde tekrarlı veri iletiminin önüne geçilmekte ve sıradan demetleme yaklaşımlarına göre %70' e varan enerji tasarrufu sağlanabilmektedir. KAA' larda güvenlik, enerji verimliliği kadar önemli bir konudur. İletişimin güvenliğini sağlayabilmek için gönderilen verilerin şifrelenmesi gerekmektedir. Veri kümeleme yaklaşımları sağladıkları büyük faydalara rağmen standart şifreleme algoritmalarını desteklememektedir. Bunun için veri kümeleme fonksiyonlarını uygularken aynı zamanda şifrelemeye açık bir algoritmaya

ihtiyaç duyulmaktadır. Bu çalışmadan benimsenen Eliptik Eğri Şifreleme (ECC) yaklaşımı homomorfizm özelliği sayesinde şifrelenmiş veri üzerinde aritmetik işlemler yapılmasına izin vermektedir. ECC bu özelliği sayesinde KAA' larda güvenli veri kümelemeyi olanaklı kılan etkin bir çözüm yöntemi olarak ön plana çıkmaktadır. Bu çalışmada önerilen Eliptik Eğri ile Güvenli Veri Kümeleme (EEiGVK) Prosedürü ile KAA' ların iki önemli sorunu olan enerji tüketimi ve güvenlik ihtiyacına birlikte çözüm olabilecek yeni bir yaklaşım geliştirilmiştir.

Bilim Kodu : **902.1.014**
Anahtar Kelimeler : **Kablosuz Algılayıcı Ağlar, Demetleme, Veri Kümeleme, Eliptik Eğri Şifreleme, Güvenli Veri Kümeleme**
Sayfa Adedi : **95**
Tez Yöneticisi : **Suat ÖZDEMİR**

DATA AGGREGATION APPLICATIONS IN WIRELESS SENSOR NETWORKS
(M. Sc. Thesis)

Arda ÖZTÜRK

GAZİ ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ
February 2012

ABSTRACT

Wireless Sensor Networks (WSN) applications are being used in various fields due to numerous advantages that they provide. According to requirements of the applications, the sensor nodes that form WSNs are usually designed in small volumes and for one-time use only. Clustering applications such as HEED or LEACH, which are developed to provide energy efficiency, divide network into inner clusters and make it possible to manage packet transmission through the network. Although clustering applications help to maintain energy efficiency, when considering the typical properties of WSNs, it was understood that we can still improve energy efficiency. With the Data Aggregation approach which is adopted in this thesis, we can eliminate redundant data transmission. Thanks to that, it is possible to obtain energy efficiency up to 70% against standard clustering applications. Security is an another important issue in WSNs. To provide secure communication, data are needed to be encrypted. But in contrast to great advantages that they provide data aggregation approaches do not support standard encryption applications. For this reason, there is a need for an encryption algorithm which can work with data aggregation applications. The Elliptic Curve Cryptograph (ECC) approach, which is adopted in this thesis, allows performing arithmetical operations over encrypted data due to its homomorphism property. Thanks to privacy homomorphism property ECC is an efficient solution for WSNs that allows secure data aggregation. With the

proposed "Eliptik Eğri İle Güvenli Veri Kümeleme (EEiGVK)" Procedure, it is aimed to develop a new approach that can be an integrated solution to two major problems of WSNs, the energy consumption and the security issues.

Science Code : **902.1.014**
Key Words : **Wireless Sensor Networks, Clustering, Data Aggregation, Elliptic Curve Cryptography, Secure Data Aggregation**
Number of Pages : **95**
Thesis Supervisor : **Suat ÖZDEMİR**

TEŞEKKÜR

Çalışmalarım boyunca değerli yardım ve katkılarıyla beni yönlendiren, kıymetli tecrübelerinden faydalandığım hocam Yrd. Doç. Dr. Suat ÖZDEMİR' e, tüm hazırlık ve çalışma süresince hiçbir konuda sıkıntı çekmememem için yardımlarını esirgemeyen değerli hocam Prof. Dr. Şeref SAĞIROĞLU' na, çalışma konum ile ilgili bilgi birikimimin oluşmasında değerli katkıları bulunan Prof. Dr. M. Ali AKCAYOL hocama, aklıma takılan her türlü soru ve sorunda yardımlarını esirgemeyen değerli hocam Yrd. Doç. Dr. Hasan Ş. BİLGE' ye, tüm çalışmalarım boyunca yardım ve destekleri ile beni hiçbir zaman yalnız bırakmayan değerli arkadaşım ve meslektaşım Bilgisayar Mühendisi Tuğba SARP' a ve manevi desteklerinden ötürü değerli aileme teşekkürü bir borç bilirim.

İÇİNDEKİLER

ÇİZELGELERİN LİSTESİ

Çizelge **Sayfa**

ŞEKİLLERİN LİSTESİ

Şekil **Sayfa**

Şekil **Sayfa**

1. GİRİŞ

Kablosuz Algılayıcı Ağları (KAA) genellikle geniş bir alana yayılmış çok sayıda küçük algılayıcı cihazın en az bir görevi yerine getirmek üzere bir araya getirilmesiyle oluşan ağlardır. KAA' ların yerine getirmesi hedeflenen görevler cihazların bulundukları ortamı gözlemleyebilmesi, yorumlayabilmesi gibi bazı karakteristik fonksiyonları gerektirmektedir. Sahip oldukları avantajlardan dolayı günümüzde birçok alanda çeşitli ihtiyaçları karşılamak için KAA' lardan faydalanılmaktadır.

KAA uygulamaları incelendiğinde genellikle ağı oluşturan algılayıcı cihazların zorlu fiziksel şartlara sahip bölgelere yerleştirildiği görülmektedir. Ortam koşullarından dolayı cihazların zarar görmesi ve çalışamaz hala gelmeleri KAA' larda olası bir durumdur. Ağın tasarımı yapılırken bu gibi özellikleri de dikkate alınmaya çalışılmaktadır. KAA' ların bir diğer genel özelliği de kontrol edilmesi zor, uzak alanlara kuruluyor olmalarıdır. Bu özellikleri birkaç ciddi sorunu da beraberinde getirmektedir. Öncelikle ağın bulunduğu coğrafi konumun çalışma alanından uzakta olması ağın kontrol edilmesini zorlaştırmakta hatta imkansız kılmaktadır. Bu durum da ağı dışarıdan gelebilecek saldırılara karşı tehlikelere açık hala getirmektedir. Kötü niyetli kişiler tarafından ağ içerisinde ki veri akışı dinlenebilir; algılayıcı cihaz veya cihazlar deforme edilebilir ya da kasıtlı olarak yanlış sonuç elde edebilecek şekilde değiştirilebilir. Ağ içerisindeki haberleşme planlanırken bu gibi güvenlik açıkları da giderilmeye çalışılmaktadır. Bu noktada ise KAA' ların zayıf olduğu diğer bir konu ön plana çıkmaktadır. Algılayıcı cihazlar genellikle tek kullanımlık olarak tasarlanmaktadır. Bir algılayıcı cihaz görev yapacağı ortama yerleştirildikten sonra bataryası bitene kadar çalışabilmektedir. Genellikle çok sayıda ve çok geniş alanlara yerleştirildikleri için batarya ömürleri bittikten sonra algılayıcı cihazların toplanarak bataryaların yenilenmesi çok maliyetli bir süreç olacağından cihazlar tek seferlik olarak tasarlanmaya çalışılmaktadır. Bu da işlem kapasitelerinin ve enerji kaynaklarının çok kısıtlı olması anlamına gelmektedir. Bu yüzden KAA' larda güvenlik uygulamaları geliştirilmeye çalışılırken kısıtlı enerji kaynakları dikkate alınmalıdır.

Çalışmanın ilk kısmında KAA alanında yapılan araştırmalar ve bu çalışmayı yapmaya iten sorunlar genel olarak anlatılmaya çalışılmıştır. Yazının ikinci bölümünde ise çalışmanın konusu ile ilgili olarak literatürde ne gibi başka çalışmalar yapıldığından bahsedilmiştir. Takip eden bölümde KAA ile ilgili literatüre yer alan tanımlara yer verilmiştir. Daha sonra KAA konseptinin çıkış noktasından ve gelişimi açıklanmıştır. KAA' ların tarihsel süreçteki yeri açıklandıktan sonra günümüzde çeşitli alanlarda kullanılmakta olan KAA uygulamalarından örnekler sunularak bu ağların görev, sorumluluk ve gereksinimleri gösterilmeye çalışılmıştır. Yazının sonraki bölümünde KAA' lara daha teknik bir perspektiften yaklaşarak genel karakteristik özellikleri sıralanmıştır. KAA uygulamalarının genel özellikleri tanıtıldıktan sonra ağı oluşturan algılayıcı cihazlar ile ilgili daha detaylı teknik bilgiler verilmiş bu sayede ağ üzerinde planlanabilecek optimizasyonlarda nelere dikkat edilmesi gerektiği ifade edilmeye çalışılmıştır. Algılayıcı cihazların gereksinimleri de açıklandıktan sonra bunları dikkate alarak KAA' larda uygulanılmakta olan enerji verimliliği ve güvenlik yaklaşımlarından bahsedilmiştir. Yazının son kısmında ise KAA' lara özel gereksinimleri dikkate alarak bunları sağlayabilecek güvenlik ve enerji verimliliği yapısından kısaca bahsedilmektedir.

2. MOTİVASYON

Kablosuz Algılayıcı Ağları (KAA) genellikle geniş bir alana yayılmış çok sayıda küçük algılayıcı cihazın en az bir görevi yerine getirmek üzere bir araya getirilmesiyle oluşan ağlardır [1, 2, 4, 44]. KAA' ların yerine getirmesi hedeflenen görevler cihazların bulundukları ortamı gözlemleyebilmesi, yorumlayabilmesi gibi bazı karakteristik fonksiyonları gerektirmektedir. Sahip oldukları avantajlardan dolayı günümüzde birçok alanda çeşitli ihtiyaçları karşılamak için KAA' lardan faydalanılmaktadır.

KAA uygulamaları incelendiğinde genellikle ağı oluşturan algılayıcı cihazların zorlu fiziksel şartlara sahip bölgelere yerleştirildiği görülmektedir [43, 44]. Ortam koşullarından dolayı cihazların zarar görmesi ve çalışamaz hala gelmeleri KAA' larda rastlanabilen bir durumdur. Ağın tasarımı yapılırken bu gibi özellikleri de dikkate alınmaya çalışılmaktadır. KAA' ların bir diğer genel özelliği de kontrol edilmesi zor, uzak alanlara kuruluyor olmalarıdır. Bu özellikleri birkaç ciddi sorunu da beraberinde getirmektedir. Öncelikle ağın bulunduğu coğrafi konumun çalışma alanından uzakta olması ağın kontrol edilmesini zorlaştırmakta hatta imkansız kılmaktadır. Bu durum da ağı dışarıdan gelebilecek saldırılara karşı tehlikelere açık hala getirmektedir [28, 29, 30 32]. Kötü niyetli kişiler tarafından ağ içerisinde ki veri akışı dinlenebilir; algılayıcı cihaz veya cihazlar deforme edilebilir ya da kasıtlı olarak yanlış sonuç elde edebilecek şekilde değiştirilebilir. Ağ içerisindeki haberleşme planlanırken bu gibi güvenlik açıkları da giderilmeye çalışılmaktadır. Algılayıcı cihazlar genellikle tek kullanımlık olarak tasarlanmaktadır. Bir algılayıcı cihaz görev yapacağı ortama yerleştirildikten sonra bataryası bitene kadar çalışabilmektedir. Genellikle çok sayıda ve çok geniş alanlara yerleştirildikleri için batarya ömürleri bittikten sonra algılayıcı cihazların toplanarak bataryaların yenilenmesi çok maliyetli bir süreç olacağından cihazlar tek seferlik olarak tasarlanmaya çalışılmaktadır. Bu da işlem kapasitelerinin ve enerji kaynaklarının çok kısıtlı olması anlamına gelmektedir [25, 43, 44]. Enerji tüketimi direkt olarak ağın ömrünü de belirlediği için KAA' lar ile geliştirme yaparken dikkat edilmesi gereken bir diğer önemli konudur.

KAA' ların genel özellikleri değerlendirildiğinde iki önemli unsur ön plana çıkmaktadır;

- Güvenlik
- Enerji Tüketimi

Yukarıda listelenen iki kritik özellik KAA' lar ile ilgili yapılan neredeyse bütün çalışmaları etkileyen kilit nokta olarak dikkat çekmektedir. Literatürde gerek güvenlik gerekse enerji tüketimini iyileştirmek için yapılan çalışmalar incelendiğinde bu iki önemli özelliğin bir birleriyle çakışmakta olduğu görülmüştür [43-47, 49, 50]. Edinilen izlenimlere göre bir KAA' ağın güvenliği arttırılmak istendiğinde ağın enerji tüketimi artmakta ve dolayısıyla ömrü kısalmaktadır. Benzer şekilde ağdaki enerji tüketimi azaltılmak için geliştirilen yaklaşımlar güvenliği sağlamak adına kullanılan şifreleme uygulamalarını kullanılabilmesini engellemektedir [28, 30, 36]. Bu da ağda güvenlik zaaflarına neden olabilmektedir. Güvenlik ve enerji tüketimi arasındaki bu sorun KAA' lar için incelenmesi gereken önemli bir konu olarak ön plana çıkmaktadır. Bu çalışma KAA alanındaki bu ihtiyaç fark edilerek yapılmıştır. Yapılan çalışmalar dahilinde KAA' larda enerji tüketimini azaltmaya çalışırken güvenlik yaklaşımlarının kullanılmasını da destekleyecek bir çözüm yolu geliştirilmeye çalışılmıştır. Sonuç olarak Eliptik Eğri Şifreleme (ECC) yaklaşımı benimsenerek uygulanacak olan KAA' larda güvenli veri kümeleme yöntemi ile tespit edilen sorun için etkili bir çözüm sunulmaya çalışılmıştır. ECC algoritması kullanılarak tasarlanan çözüm ile hem ağ içerisindeki enerji tüketimi dengeleyebilen hem de kabul edilebilir ölçülerde güvenlik sağlayabilen bütünleşik bir çözüm sunulmaya çalışılmıştır.

3. İLGİLİ ÇALIŞALAR

Literatürde KAA ile ilgili çalışmalar incelendiğinde edinilen izlenim gerek güvenlik gerekse enerji tüketimi konularının bu alanda geliştirilmesi gereken açık noktalar olarak görüldüğü yönündedir. Bu doğrultuda her iki alanda da çok sayıda araştırma yapılmış ve çeşitli çözüm önerileri geliştirilmeye çalışılmıştır. Fakat çok az sayıda çalışma bu iki sorunu birden ele alarak bütünleşik bir çözüm üzerinde düşünme yoluna gitmiştir.

KAA alanında yapılan ilk çalışmalar ağ içerisinde yer alan tüm cihazların güvenli bir şekilde haberleştiğini varsayarak topolojik yaklaşımlar ya da yönlendirme yaklaşımları gibi diğer konulara odaklanmaktaydı. Fakat gerçek hayattaki uygulamalarda bu ne yazık ki bu şekilde olmamaktadır. Ağlar genellikle denetimden uzak bölgelere kuruldukları için önlem alınmadığı sürece ciddi güvenlik açıkları taşımaktaydılar. KAA' larda ki bu açık fark edildikten sonra güvenlik üzerine yapılan araştırmalar yoğunluk kazanmıştır [29].

KAA güvenli veri iletişimi sağlamak için en genel güvenlik yaklaşımı olan şifreleme yöntemlerine başvurulmaktadır [27, 28, 29, 38]. İletilen verilerin şifrelenerek kötü niyetli kullanıcılara karşı gizlenmesi sağlandıktan sonra yetkilendirme gibi güvenlik arttırıcı yaklaşımlara da başvurulabilir. Şifreleme yapılmadığı takdirde gönderilen tüm paketler herkes tarafından okunabileceği için ağ içi iletişim kolaylıkla çözülerek ağ saldırılara karşı açık hale getirilmiş olacaktır [28]. Çalışmanın önceki bölümlerinde sıklıkla altı çizildiği üzere enerji tüketimi KAA için hayati önem taşıyan bir konudur ve KAA' lar üzerinde şifreleme yaklaşımları geliştirilirken de özellikle dikkat edilen bir unsur olarak ön plana çıkmaktadır [27, 28, 29, 44].

Ağ üzerinde şifreleme yöntemi ile güvenliği sağlamanın en kolay yolu yalnızca ağ tarafından bilinen bir anahtarı kullanarak iletilen verilerin şifrelenmesidir. Literatürde Açık Anahtar Şifreleme olarak bilinen bu yaklaşım diğer karmaşık şifreleme yaklaşımlarına göre daha az maliyetlidir. TinySec KAA' lar için geliştirilen ilk şifreleme uygulamalarından biridir [27, 32]. Bağlantı katmanı seviyesinde çalışan

bir uygulama olan TinySec ağa enerji tüketimi, gecikme ve paket başlığı boyutunda ortalama %10 artışa neden olmaktadır. Benzer şifreleme yaklaşımlarına göre getirdiği ek maliyetler küçük sayılabilecek olan TinySec ilk zamanlarda KAA için ideal bir çözüm olarak görülse de zamanla birçok güvenlik açığı ortaya çıkartılmıştır ve yeterince güvenlik sağlayamadığı kanaati uyandırmıştır [32]. Daha sonra yapılan çalışmalarda günümüzde birçok farklı uygulamada ve gelişmiş ağ yapılarında güvenliği sağlamak için yaygın olarak kullanılan RSA şifreleme algoritmaları KAA' lar için uygulanmaya çalışılmıştır. Standart RSA uygulamalarında şifreleme yapmak için 1024bit ya da 2048bit uzunluğunda anahtarlar kullanılmaktadır. Kısıtlı enerji kapasitesine sahip ve genellikle çok küçük veri paketleri ile çalışan algılayıcı cihazlar için bu anahtar boyutları ciddi enerji tüketimi anlamına gelmektedir [39]. Bu durum RSA uygulamalarının enerji kaynaklarının kısıtlı olduğu enerji tüketiminin hayati önem taşıdığı KAA' lar için uygulanabilirliğini çok düşürmektedir [32].

Açık anahtar şifreleme yaklaşımları genellikle TinSec gibi çok fazla güvenlik sağlayamamaktadır. Açık anahtar ile yapılan şifreleme karmaşıklaştırılmak istendiğinde ise anahtar uzunlukları ve buna bağlı olarak işlem maliyetleri artmaktadır. Bunun için cihazlar arasında gerçekleşen anahtar değişimi süreci üzerinde çeşitli geliştirmeler yaparak bu anahtarların oluşturulması ve kullanılması KAA' lar için daha uygun hale getirilmeye çalışılmıştır. Anahtar değişimi esnasında algılayıcı düğümler bir birlerine karşılıklı olarak kim olduklarını ve de gerçekten o ağa ait olduklarını ispatlayacak, bir nevi imza niteliği taşıyan anahtarlarını gönderirler. İki tarafta karşıdakinin iletişime geçmek açısından güvenli bir düğüm olduğuna inandığında cihazlar iletişime başlarlar. Literatürde sıkça adı geçen ve KAA' larda en yaygın olarak kullanılan anahtar değişimi yaklaşımı Diffie-Hellman (D-H) Anahtar değişimi metodudur [29, 37]. D-H metodunun yaygın olarak tercih edilmesinin nedeni işlem kümesini kısıtlayarak işlem maliyetini azaltmasıdır. Standart matematiksel yöntemler benimsendiğinde üretilecek olan özel anahtarlar karmaşıklaştırılmak istendiğinde hem anahtarı oluşturmak için harcanılan enerji artmakta hem de anahtar boyutu büyüdüğü için imzalanan veri paketinin büyüklüğü artacağından veri iletimi için harcanan enerji artmaktadır. D-H anahtar değişimi yönteminde işlemler kısıtlı bir mod kümesi üzerinden yapılmakta bu da uygulanan

yöntemin karmaşıklığı ne olursa olsun anahtar boyunun büyümemesini sağlamaktadır [37]. KAA' larda enerji tüketimi kritik bir konu olduğu için D-H yaklaşımı uygun bir çözüm yöntemi olarak görülmektedir.

Yapılan geniş kapsamlı incelemelerde KAA' larda geliştirilen güvenlik yaklaşımlarının nerdeyse tamamının enerji kısıtlarına takıldığı görülmüştür. Enerji tüketiminin KAA için çok önemli olmasının genellikle araştırmacıları daha güvenli şifreleme yaklaşımları geliştirmekten alı koyduğu ya da belirli ölçülerde engellediği görülmüştür. Bu nedenle ağ üzerinde enerji tüketimi dengelenebilirse güvenlik gibi diğer önemli alanlarda da daha rahat geliştirmeler yapılabileceği düşünülerek bu alanda yapılan çalışmalara da ağırlık verildiği görülmüştür.

Literatürde yer alan çalışmalar incelendiğinde KAA' larda enerji tüketimini dengelemeye yönelik ilk çalışmalar arasında demetleme yaklaşımları görülmektedir. Demetleme yaklaşımlarında genel amaç ağ içerisindeki veri iletimini düzenlemektir. Veri iletimi esnasında hata yapmaya yatkın olan algılayıcı cihazlar kendi aralarında kontrolsüz bir şekilde veri alış verişi yapmaya çalıştıklarında çok ciddi bir enerji israfı meydana gelmektedir. Demetleme yaklaşımları algılayıcı cihazları gruplara ayırarak daha kontrollü bir şekilde iletişim kurmalarını sağlamaya çalışmaktadır. Demetleme yaklaşımları uygulanırken demetler üzerinde yönetimin sağlanması için her demetten bir demet lideri seçilir ve genellikle iletişim de bu demet lideri üzerinden yapılır. Demetleme algoritmaları demetlerin oluşturulması ve demet lideri seçme açısından farklılık gösterirler. HEED, MRECA, LEACH ve EEDC, KAA' larda yaygın olarak kullanılan demetleme yaklaşımlarındandır [32, 33, 34, 35]. Bu yöntem enerji tüketimini dengelediği için bir derece tasarruf sağlayabildiyse de hala ağ üzerinde birçok paketin tekrarlı olarak iletilmesine izin vermektedir. Demetleme yaklaşımlarının bu açığı kısa sürede fark edilerek üzerinde araştırma ve geliştirmeler yapılmaya başlanmıştır.

Demetleme yaklaşımlarını daha anlamlı ve işlevsel hale getirebilmek için yapılan en etkili çalışma veri kümeleme yaklaşımlarıdır. Veri kümele yaklaşımlarında algılayıcı düğümler kendilerine gelen verileri çeşitli aritmetik ya da mantıksal işlemlere tabi

tutarak işleme giren verilerin tamamını özetler nitelikte tek bir veri elde ederler ve sadece bu özet veriyi iletirler [28, 30, 32, 40, 41, 42, 45]. Bir önceki paragrafta belirtildiği üzere demetleme yaklaşımları veri iletişiminin belirli doğrultularda ilerlemesini sağlamaktan öteye gidememektedir. Her ne kadar bu sayede aynı verinin bir çok komşu cihaza gereksiz yere gönderilmesi engellenmiş olsa da hala tüm algılayıcı cihazlardan gelen veriler tekrar tekrar iletilerek baz istasyonuna kadar iletilmeye çalışılmaktadır [44, 45]. Örneğin bir veri demetinde demet liderine bağlı on adet düğüm varsa demet lideri bunların hepsinden gelen toplam on adet veriyi iletmekle yükümlüdür. Veri kümele yaklaşımları bu noktada anlam kazanmaktadır [43, 45]. Örnekte bahsedilen demet yapısında demet lideri olan algılayıcı cihaz kendisine gönderilen on adet veri paketini çeşitli gruplama fonksiyonlarına tabi tutarak tek bir özet veri oluşturabilirse iletmesi gereken paket sayısı ondan bire düşecektir [43]. Yapılan çalışmalar incelendiğinde veri kümeleme etkili bir şekilde planlandığında %70' e varan enerji tasarrufu sağlanabilmektedir [1, 28]. Enerji tüketiminden elde edilen bu ciddi kazanç ile daha güvenilir şifreleme yaklaşımları geliştirilebilmesi mümkün olabilecektir. Bu noktada bir konunun altının çizilmesinde fayda olduğu düşünülmektedir; veri kümeleme yaklaşımlarının verimli bir şekilde kullanabilmesi için demetleme yaklaşımlarının benimsenmesine de gerek yoktur. Her bir algılayıcı düğüm kendisine gönderilen verileri kümeleyerek iletime bu şekilde devam edebilir.

Enerji tüketimini ciddi oranda azaltabilen veri kümeleme yaklaşımları beraberinde çeşitli dezavantajları da getirmektedir [43, 44, 45]. Gecikme süreleri bu dezavantajlardan birisidir. Algılayıcı cihazlar veri kümele yaklaşımları kullanarak kendilerine gönderilen veri paketlerini bir kümeleme fonksiyonuna tabi tutarak tek bir özet veri ürettiklerini söylemiştik. Bu süreçten anlaşılabileceği gibi cihaz bir seferde ne kadar çok paketi birden kümeleme fonksiyonuna sokarsa çıkan paket tek bir tane olacağı için veri iletiminde o kadar kazanç sağlamış olur. Bu durumda eğer iletilen verinin gerçek zamanlı olması uygulama açısından kritik değil ise veri iletimi esnasında bekleme süreleri eklenerek kümeleme yaklaşımlarının daha etkin kullanılması sağlanabilir. Ağdaki veri akışını mümkün olduğunca gerçek zamanlı tutmaya çalışsak bile gelen paketlerin kümeleme fonksiyonlarına girmesi ufak da

olsa gecikmelere neden olacaktır. Bunun dışında veri kümeleme yaklaşımlarının ortaya çıkardığı en büyük sorun standart şifreleme uygulamaları ile birlikte etkin bir şekilde kullanılmaya elverişli olmamalarıdır [42, 43, 44, 45, 46]. Şifreleme algoritmaları verileri çeşitli aritmetik işlemlere tabi tutarak içeriklerinin değişmesine neden olurlar. Şifrelenmiş veriler veri kümeleme fonksiyonlarına sokulduklarında elde edilen sonuç orijinal verilerin aynı fonksiyona sokulmasından elde edilecek sonucun şifrelenmiş hali olmamaktadır. Bu nedenle algılayıcı cihazlar her aldıkları veri paketini öncelikle deşifre etmek zorunda kalırlar [28, 44, 46]. Cihaz ancak aldığı tüm veri paketlerini deşifre ettikten sonra hepsini birden bir kümeleme fonksiyonuna sokabilir ve özet bir sonuç üretebilir. Bu da cihazın aldığı paket sayısı kadar deşifreleme işlemi yapması anlamına gelmektedir. Kablosuz algılayıcı cihazların zaten çok kısıtlı enerji kaynaklarına sahip oldukları ve şifreleme/deşifreleme işlemlerinin yoğun matematiksel işlemler gerektiren maliyetli işlemler oldukları göz önüne alınırsa bu şekilde bir akış KAA' lar için kesinlikle uygun gözükmemektedir. Literatürde yer alan çalışmalar incelendiğinde KAA' larda veri kümeleme yaklaşımlarının beraberinde getirdiği güvenlik açıklarının incelenmesi gereken bir araştırma konusu olarak görüldüğü anlaşılmaktadır. Bu sorunun tespiti üzerine yapılan ilk çalışmalarda şifrelemenin veri kümeleme için uygun olmadığı varsayılarak şifrelemeye ihtiyaç duymadan ağ içerisindeki iletişim daha güvenli bir hale getirilmeye çalışılmıştır. Bu yaklaşım benimsenerek ortaya atılan düşüncelerden bir tanesi filtreleme yöntemidir. Filtreleme yöntemi kapsam olarak genele hitabeden bir çözüm şekli değildir. Bu yöntem sadece az sayıda ortam parametresi üzerinde çalışan ve bu ortam parametreleri genellikle dar spektrumlara sahip olan uygulamalarda kullanılabilmektedir. Filtreleme yaklaşımında algılayıcı cihazların elde ettiği değerler filtrelenerek anlamsız bulunan değerler veri iletimine hiç sokulmamaktadır. Bu sayede cihazlardan bir veya birkaç tanesi teknik nedenlerden dolayı sağlıksız çalışmaya başlarsa ya da kötü niyetli kullanıcılar tarafından ağa yanıltıcı veriler aktarılıyor ise bunlar görmezden gelinmeye çalışılmaktadır. Örneğin deniz suyu sıcaklığını ölçen bir uygulamada cihazların ölçtüğü değerler -4 derece ve 50 derece aralığında filtrelendiğinde bir bölgedeki algılayıcı cihazların hepsi 30 derece ölçüm yaparken arızalanan bir tanesi sıcaklık değeri olarak 999 derece gönderiyor ise bu değer filtre aralığının dışında kalacağından iletişime katılmaması

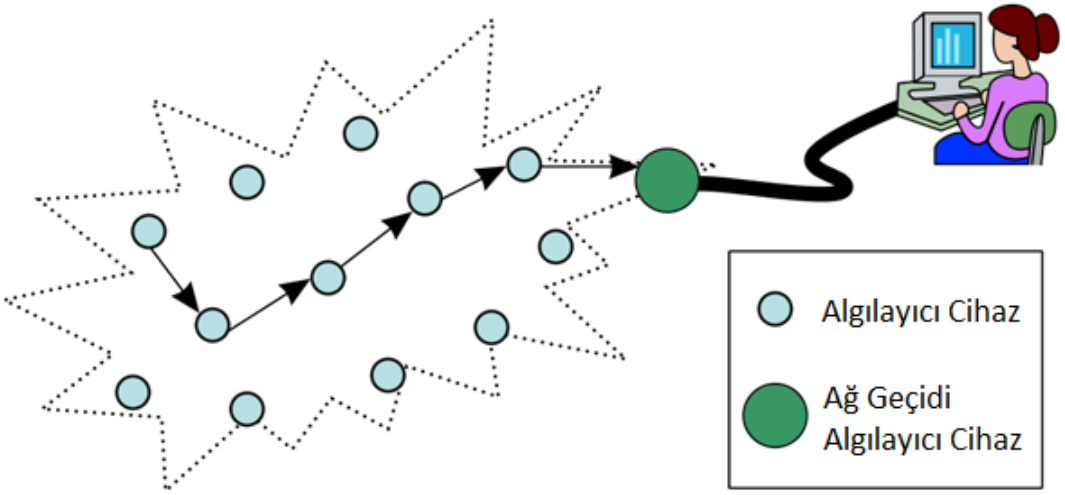
sağlanmaktadır. Dolayısıyla örnekte geçen bölgeye ait anlamlı bir ortalama sıcaklık değeri elde edilebilmektedir. Veri kümeleme işlemini şifreleme yapılmaksızın daha güvenli bir hale getirmek için uygulanan bir diğer yöntemde ise algılayıcı cihazların bir birlerini sürekli kontrol ederek güvenli bir ortam oluşturulmaya çalışılmıştır. Wagner tarafından geliştirilen yöntemde kümeleme özelliğine sahip algılayıcı cihazlar Merkel Ağaç yapısı kullanarak komşularındaki veriyi doğrulayabilmektedir. Bu sayede baz istasyonuna iletilen bir veri paketinin kaynağına kadar izi sürülerek onaylanabilmektedir [28]. KAA' larda şifreleme yaklaşımları kullanılmaksızın veri kümeleme yapılabilmesi için güvenli bir iletim ortamı oluşturmaya yönelik bir diğer çalışma da 2009 yılında Suat Özdemir tarafından yapılmıştır [48]. Yapılan bu çalışmada algılayıcı cihazlar bir birlerini güvenilirlik ilkesi üzerinden değerlendirmektedir. Ağ içerisinde yer alan bütün algılayıcı cihazlar diğer komşularının hareketlerini değerlendirerek onların güvenilirliğini belirlemeye çalışır. Örneğin bir algılayıcı cihazın yakınında yer alan komşusu istenilen bir ortam parametresi ile ilgili cihazın kendisine göre çok farklı değerler tespit ediyorsa bu o komşunun güvenilirliği azaltıcı bir unsuz olarak değerlendirilebilmektedir. Benzer şekilde bir algılayıcı cihaz veri gönderi isteklerine çoğunlukla cevap vermeyen ve bu isteklerin tekrarlanmasına neden olan bir komşusunu veri iletişimi açısından güvensiz olarak nitelendirebilmektedir. Bütün bu otonom kontroller sağlanılarak ağ içerisinde iletilen verinin mümkün olan en güvenilir kaynaklardan ve yine mümkün olan en güvenilir şekillerde iletilebilir hale gelmesi hedeflenmektedir [48].

Şifreleme yaklaşımları benimsenmeksizin veri kümeleme işlemini güvenli hale getirmek adına yapılan çalışmalar genellikle sadece yanlış olma ihtimalleri yüksek olan verilerin iletimden elenmesine yöneliktir. Olası sorunlara karşı bir çözüm üretmekten daha çok hatalı durumlardan ağ nasıl daha az etkilenir sorusuna cevap verebilmektedirler. Bunun dışında ağın geneli için güvenliği sağlamaktan çok uzaktırlar. Sadece bu gibi yöntemler benimsendiğinde ağ halen aktif pasif birçok saldırıya karşı açık halde olacaktır. KAA' larda ciddi avantajlar sağlayan veri kümeleme yaklaşımlarının yarattığı bu güvenlik zaafları düşünüldüğünde veri kümelemeye izin verebilecek bir şifreleme algoritmasının geliştirilmesinin gerekliliği çok daha iyi anlaşılabilmektedir.

Literatürde Eliptik Eğri Kriptolojisi olarak geçen ECC yaklaşımı homomorfizm özelliği sayesinde şifrelenmiş veriler üzerinde aritmetik işlemler yapılabilmesine olanak sunmaktadır. Verileri üçüncü dereceden bir eliptik eğri üzerinde yer alan noktalara taşıyarak şifreleme işlemini gerçekleştiren ECC algoritmasının KAA' lar için sağlayacağı faydalar bununla da sınırlı kalmamaktadır. Sonlu kümeler üzerinde çalışmaya da elverişli olan ECC algoritmalarında verileri şifrelemek için kullanılan anahtarlar eş değer şifreleme uygulamalarına göre çok daha küçük boyutlardadır. Örneğin RSA uygulamasında 2048 bitlik anahtar tercih edilirken yalnızca 210 bitlik bir anahtar kullanılarak aynı derecede güvenli şifreleme yapılabilmektedir [52]. Ek paket maliyetlerinin küçük olması ve veri kümeleme fonksiyonlarını desteklemesi açısından ECC algoritması KAA' lar için son derece uygun ve etkili bir çözüm yöntemi olarak ön plana çıkmaktadır. ECC veri kümeleme yaklaşımları ile birlikte kullanılarak KAA' lar için etkili ve güvenilir veri gruplama çözümünü sunabilmektedir.

4. KABLOSUZ ALGILAYICI AĞLAR

Kablosuz algılayıcı ağlar (KAA), sensör cihazları adı verilen bir grup küçük otonom sistemin en azından bir görevi yerine getirmek üzere bir araya getirilmesiyle oluşturulan ağlardır. Uygulamanın amacına yönelik olarak değişiklik gösterebilecek olan görev çeşitlerinin tamamı bu ağ tipinin karakteristik bir özelliği olarak cihazların bulunduğu ortama ait parametre veya parametrelerin gözlemlenebilmesini gerektirmektedir [1, 4]. KAA özellikle son yıllarda akademik açıdan önemli bir inceleme konusu olarak ön plana çıkmaktadır. Akademik çalışmaların yanı sıra savunma sanayi başta olmak üzere birçok farklı sektör için gelecek vadeden bir yatırım alanı olmaya başlamıştır. Gelişmekte olan teknolojiyle birlikte bu alanda gerek bilimsel gerekse ticari uygulamalar geliştirilmekte olup günümüzde birçok farklı ihtiyacı gidermek için kullanılmaktadırlar ve çok daha fazla sayıda uygulama için araştırma-geliştirme çalışmaları sürdürülmektedir.

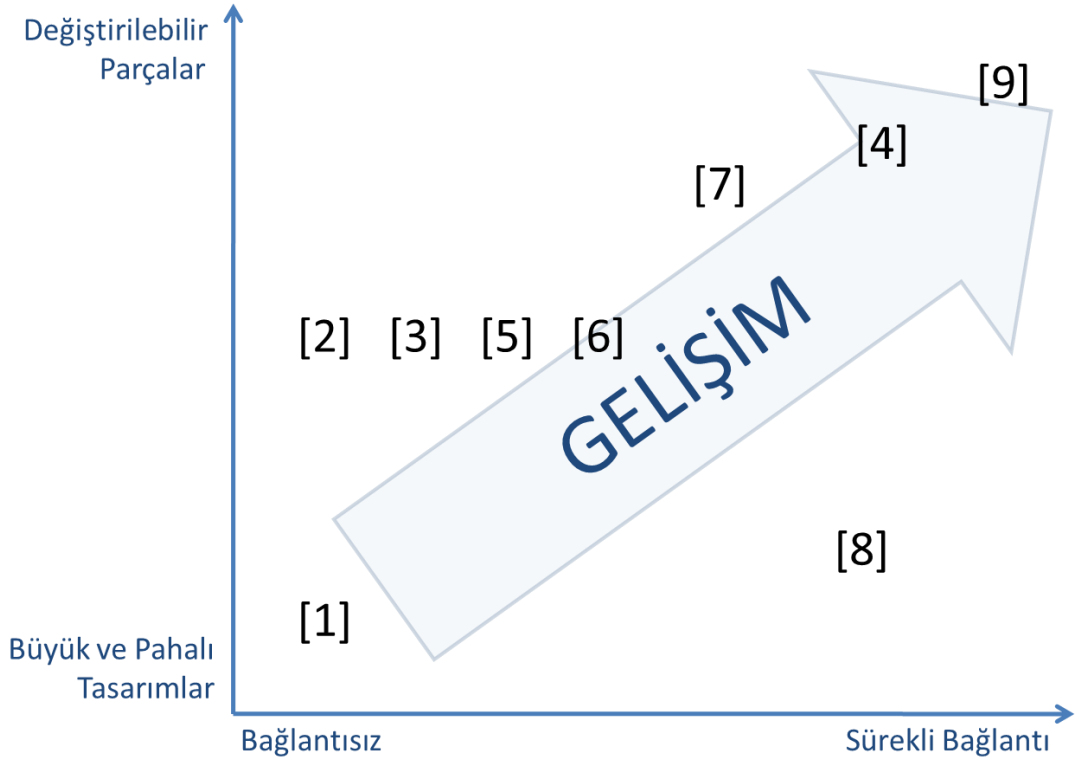


Şekil 4.1. Genel KAA topolojisi

4.1. KAA Gelişim Süreci

Bilgisayarların icat edilmesiyle teknolojik açıdan birçok heyecan verici yeni keşiflerin önünü açan süreç başlamıştır. 1940’ lı yıllarda geliştirilen ilk bilgisayar anca çok geniş bir odaya sığabilecek büyüklükteydi ve günümüzde ortalama bir

bilgisayarın tükettiğinden yüzlerce kat daha fazla enerji tüketmekteydi [5]. Entegre devre teknolojisinin gelişmesi ile birlikte devasa boyutlardaki bilgisayarlar avuç içine sığabilecek kadar küçük ebatlarda üretilebilmeye başlandı. İlerleyen teknoloji ile birlikte bilgisayar üzerine çalışan firmalar artık tek bir görevi uzun süre yerine getirmek üzere tasarlanan büyük, hantal makineler yerine çok amaçlı ve modüler cihazlar geliştirmeye ve bu alanda yatırımlar yapmaktadırlar. Bilgisayar teknolojilerinde meydana gelen gelişmelere paralel olarak iletişim sektöründe de önemli ilerlemeler kaydedilmiştir. Bilgisayarlar arası ilk bağlantı makinelerin kablolar ile birbirlerine bağlanması şeklinde yapılırken, günümüzde kızılötesi ışıklar ve radyo dalgaları gibi birçok farklı bağlantı ortamı kullanılarak kablosuz iletişim sağlanabilmektedir. Bunların yanı sıra uydu teknolojileri ile iletişimin kapsamı neredeyse sınırsız hale getirilebilmektedir. Gerek bilgisayar gerekse iletişim teknolojilerinde paralel olarak meydana gelen bu gelişmelerle birlikte üretilen yeni cihazların mümkün olduğunca küçük ve bir birleriyle her türlü ortamda kolaylıkla iletişime geçebilir şekilde tasarlanması şeklinde bir eğilimi ortaya çıkarmıştır. İşte Kablosuz Algılayıcı Ağlar Konsepti bu tarz bir eğilimin sonucunda ortaya çıkmıştır ve gündeme geldiği günden itibaren ilgi uyandıran, gelecek vadeden bir araştırma/geliştirme konusu olarak dikkat çekmektedir [11].



Şekil 4.2. KAA gelişim süreci;
Cihazların sınıflandırılması [1]:
1- IBM S/360 (1960)
2- Apple II/IBM PC/C 64 (1980)
3-486er PC'ler/Amiga ve modem/Akustik coupler/BTX (1980' lerin ortaları)
4- Cep telefonları (1980'lerin sonu)
5- Pentium sınıfı PC'ler, İnternet (1990'lar)
6- Boring PC ve always-on dönemi (1990'ların ortası)
7- GPRS özelliği olan PDA'lar (1990'ların sonu)
8- "Connected Car Concept"
9- Sensor Networks

4.2. Uygulama Alanları

Temelde ortam gözlemleme, çevre kontrol, ortam değişkenlerini takip etme gibi bir görevi yerine getirmek üzere geliştirilmekte olan KAA' ları uygulama alanları açısından geniş bir yelpazeye sahiptir. Daha spesifik olarak bahsedecek olursak günümüzde doğal ortam gözlemleme, nesne takibi, nükleer reaktör kontrolü, endüstriyel süreç takibi, yangın alarmı, trafik kontrolü ve hatta hasta takibi gibi bir çok uygulamada KAA' lar kullanılmaktadır. Tüm uygulamalarda genel yaklaşım

belirli bir alanda istenilen verilerin elde edilmesi ve takibi için kablosuz algılayıcı cihazlar yerleştirilerek bir ağ yapısı oluşturulması şeklindedir.

4.2.1. Alan gözlemleme

Alan gözlemleme KAA' ların en yaygın olarak kullanıldığı konulardandır. Bu tarz uygulamalarda genellikle çok sayıda kablosuz algılayıcı cihaz geniş bir alana yerleştirilerek o alan içerisinde her hangi bir olayın tespiti ya da takibini yapmaları beklenmektedir[9]. KAA kullanarak alan gözlemleme tasarım amaçları ve getirdikleri faydalar değerlendirirliğinde genellikle askeri uygulamalar geliştirmek açısından idealdir. Sınır takip sistemleri, savaş alanı gözlemleme sistemleri bu çeşit uygulamalara en güzel örneklerdendir [10]. KAA kuruldukları alanda kurulum amaçlarına hizmet eden bir bilgili tespit ettiği anda bu bilginin baz istasyonuna iletilmesi gerekmektedir. Bu noktada ağın amacına uygun olarak uygulamada farklılıklar görülebilir. Örneğin iletilmesi gereken veri çok kritik ise uygun yönlendir algoritması ile direkt olarak baz istasyonuna iletilmeye çalışılabilir. Hatta gözlemlenen alan uzakta ise ağın içerisine uydu iletişimi olan bazı özel cihazlar yerleştirerek elde edilen verinin önce bu cihazlara yönlendirilmesi daha sonra buradan uydu haberleşmeciliği ile baz istasyonuna iletilmesi sağlanabilmektedir. Bu tarz uygulamalar coğrafi açıdan geniş bir alana yayılabileceği için KAA tasarlanılırken verinin kritikliğinin yanı sıra ağın ömrü gibi bazı diğer etkenlerin de dikkate alınması gerekebilir. Eğer iletilecek olan veri gerçek zamanlı olmak zorunda değil ise ufak bir gecikme zamanı göze alınarak ağ içerisinde veri iletimi esnasında veri kümeleme gibi yöntemlere başvurulabilir [9].

4.2.2. Doğal ortam gözlemleme

Askeri uygulamalar dışında KAA kullanarak alan gözlemlemenin tercih edildiği bir diğer alan ise bilimsel çalışmalardır. Ekolojik ortamların gözlemlenmesi ise KAA kullanılarak uygulama geliştirilen bilimsel araştırma alanlarının başında gelmektedir [17, 19]. Özellikle bir habitatta yaşayan canlı popülasyonu ya da popülasyonlarını gözlemlemek; beslenme, üreme, göç etme, sosyal ilişkiler kurma gibi yaşamsal

aktivitelerini incelemek için KAA ile geliştirilen uygulamalar tercih edilmektedir [18]. Bu alanda geliştirilmiş olan bazı uygulamalar şunlardır [12, 13, 14, 15, 16, 19];

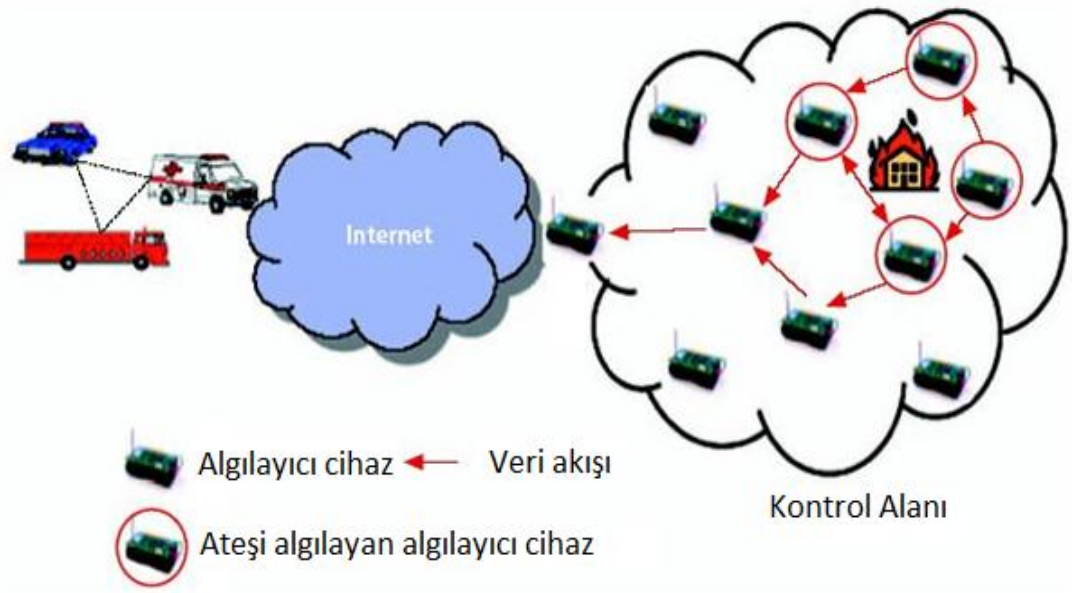
- ZebraNet
- Argo - Deniz suyu gözlemleme projesi
- PODs Project - Hawaii' deki nadir bitkilerin ekolojik olarak incelenmesi
- PODs Project - Hawaii' deki volkanik faaliyetlerin incelenmesi
- California; Redwoods Ormanları
- Great Duck Island Project
- Tungurahua – Aktif Volkan gözlemleme projesi

Şekil 4.3. KAA uygulama örnekleri

4.2.3. Erken uyarı sistemleri

KAA uygulamalarının geliştirdiği bir diğer önemli alan ise erken uyarı sistemleridir. Bu tür uygulamalarda coğrafi bir bölge ya da bir yerleşke algılayıcı cihazlar kullanılarak oluşturulan bir ağ yardımıyla sürekli gözlemlenerek tehlikeli bir durum ya da bir felakete dair belirtiler tespit edildiğinde ilgilileri uyararak can ve mal kayıplarına yol açılmasının önüne geçilmeye çalışılmaktadır. Bu tarz uygulamalara örnek olarak özellikle kapalı alanlarda yaygın olarak kullanılan yangın uyarı sistemleri örnek verilebilir. Bu sistemlerde kullanılan duman ve ısı sensörleri bulundukları ortamda tehlikeli orandaki duman miktarı veya sıcaklık normalin üstüne çıkarsa genel bir alarm verip tehlike daha da büyümeden insanların durumdan

haberdar olmasını sağlar. Benzer uygulamada örneğin bir nehrin yatağındaki suyun derinliği ve debisi gibi değerler sürekli ölçülerek her hangi bir olası sel felaketi önceden tespit edilerek yerel halk uyarılabilir.



Şekil 4.4. Erken uyarı sistemleri

4.2.4. Tarım ve hayvancılık uygulamaları

Tarım ve hayvancılık gibi sektörlerde de KAA uygulamalarının avantajlarından faydalanılmaktadır. İngiltere' de yapılan bir çalışmada bir çiftliğin arazisi harita üzerinde belirli genişliklerde sanal bölümlere ayrılmıştır. Çiftlikte yer alan ineklerin boyunlarına yerleştirilen tasmalar ile ineğin çiftlikteki konumu takip edilmektedir. İnek sanal çitlere yaklaştıkça boynuna yerleştirilen tasmadan hayvan için rahatsız edici olan bazı sesler çıkartılmakta bu sayede ineklerin sanal çitlere yaklaşması engellenmektedir [20]. Bu uygulama sayesinde çok sayıda çiftlik çalışanı tarafından yapılacak iş ve çitlerin maliyeti gibi birçok faktörden tasarruf sağlanabilmiştir.

KAA uygulamalarının avantajlarından faydalanılan bir diğer alan ise tarım sektörüdür. Bitkilerin gelişimini etkileyecek faktörler gözlemlenerek gerekli müdahalenin zaman kaybetmeden yapılması sağlayarak daha sağlıklı ürünler elde

edilebilir. Bitkinin üzerinde yetiştiği toprağın su durumu, içerdiği vitamin ve mineraller; havanın nem oranı, sıcaklık gibi değerler sürekli olarak gözlemlenerek her hangi bir değer azaldığında beklenilen düzeye çıkartılması otomatize edilebilmektedir. Bu da ürün kalitesini arttıracağı gibi süreci de hızlı ve daha az maliyetli hali getirmektedir. Tarımsal KAA uygulamalarına örnek olarak Oregon (USA)' da üzüm bağlarında kullanılan sistem gösterilebilir. Şarap üretimi için yetiştirilen üzümler bağlara kurulan KAA ile sürekli olarak gözlemlenmektedir. Uygulamanın asıl amacı üzümler olgunlaşır olgunlaşmaz hasadının yapılmasını sağlayarak daha kaliteli şarap üretebilmektir. Uygulama bunun dışında sulama, gübreleme gibi sistemlerin kontrolü; don olaylarına karşı koruma sağlamak, topraktaki mantar seviyesini kontrol etmek gibi birçok destekleyici faaliyeti de yerine getirmektedir [21].

KAA' ların tarım ve hayvancılık gibi uygulamalarda asıl tercih edilme nedeni ve kullanım şekli süreçlerin takibini, kontrolünü kolaylaştırmaktır. Bu sayede süreçler optimize edilirken elde edilen ürün kalitesi de arttırılabilmektedir.

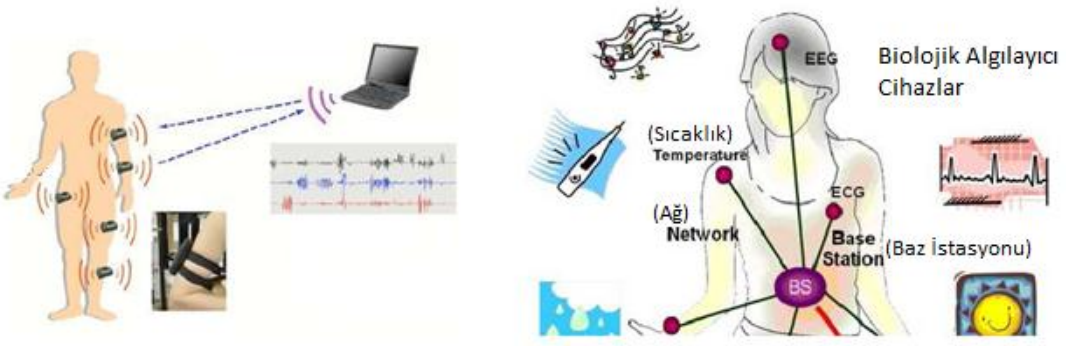
4.2.5. Ev uygulamaları

KAA uygulamalarının ticari değerleri ve potansiyelleri fark edildikten sonra bu alanda çeşitli firmalar tarafından birçok araştırma/geliştirme çalışması yapılmaya başlanmıştır. Ticari amaçlı çalışmaların başında da akıllı ev sistemleri gelmektedir. Akıllı ev sistemleri ev içerisine yerleştirilen çok sayıda ve farklı özelliklere sahip algılayıcı cihaz ile o evde yaşayan insanların ve o insanlara ait aktivitelerin farkında olan sistemlerdir [22]. KAA kullanılarak geliştirilen akıllı ev sistemleri geliştirilen otomasyonlar ile desteklenerek kullanıcıların ihtiyaçlarını hissederek bu ihtiyaçlara göre kendiliğinden aksiyon alan ev gereçleri geliştirilmektedir. Örneğin eve birisi geldiğinde sistem bunu fark ederek girişte yer alan ışıkları açacak veya eğer istenilirse televizyon karşısında yer alan koltuğa birisi oturduğunda açılacak şekilde ayarlanabilecek [22, 23].

KAA kullanılarak ev içi kullanım amaçlı geliştirilen bir diğer uygulama ise güvenlik ve uyarı sistemleridir. Bu sistemlerde eve hırsız girmesi gibi durumlarda olay anında alarm devreye girerek ve izinsiz giren kişiye karşı evde yaşayanlar uyarılabilir ve hatta gerekli entegrasyonlar yapılarak polisin anında olaydan haberdar olması sağlanabilir.

4.2.6. Sağlık uygulamaları

Sağlık uygulamaları KAA' ların kullanıldığı bir diğer uygulama alanıdır. Bu tip uygulamalarda kablosuz algılayıcı cihazlar sağlık durumu takip edilecek olan hastanın vücuduna saat, bileklik, kolye, kemer gibi çeşitli aksesuarlar kullanarak ya da deri altına gömülerek yerleştirilmektedir. Bu sayede takip edilen hastanın sağlık durumu ile ilgili vücut sıcaklığı, kan basıncı hatta kandaki şeker oranı gibi değerler anlık takip edilebilmektedir. Bu şekilde bir çözüm özellikle kronik hastalıkları olan insanların ve yaşlılar tedavi süreçlerine büyük katkıda bulunabilmektedir[24].



Şekil 4.5. KAA' ların kullanıldığı sağlık uygulamaları

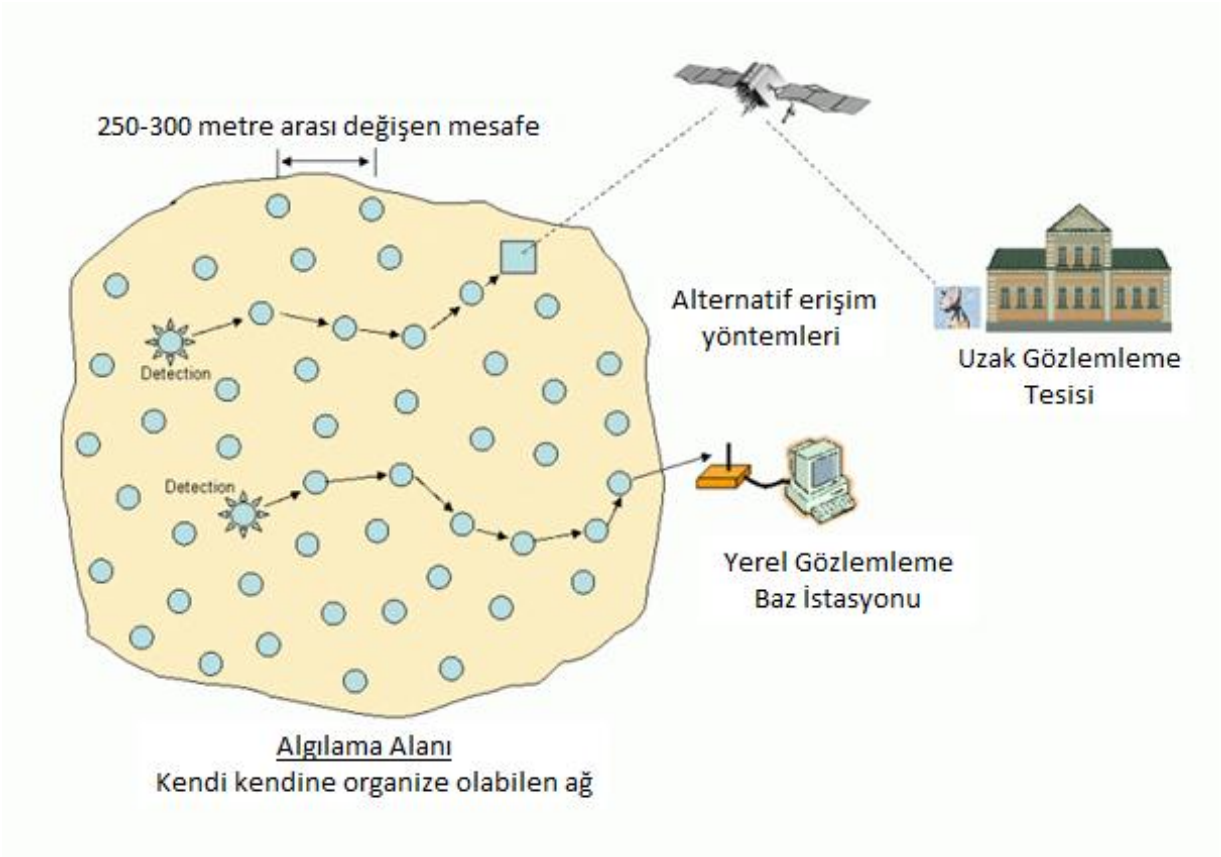
4.2.7. Endüstriyel uygulamalar

KAA' ların uygulamalarının yaygın olarak kullanılmaya başladığı bir diğer sektör ise endüstridir. Endüstiryel kuruluşlarda üretim süreci boyunca ürünler algılayıcı ağlar yardımıyla izlenerek durumları takip edilebilmektedir. Bu sayede süreçler otomasyon çözümleriyle desteklenerek hem hızlandırılabilmekte hem de üretim kalitesi arttırılabilmektedir. KAA uygulamalarının endüstri alanında sağladığı bir diğer

avantaj ise kaynakların daha verimli kullanılmasında yardımcı olabilmesidir. Kaynakların tamamı üretim süreci boyunca algılayıcı cihazlar kullanılarak sürekli gözetim altında tutulabilir. Bu sayede ihtiyaç duyulduğunda sadece duyulan ihtiyaç kadar kaynağın kullanılabilmesi sağlanabilmektedir.

4.3. KAA' ların Karakteristik Özellikleri

Kablosuz Algılayıcı Ağlar geliştirilme amaçlarına uygun olarak bir veya birden fazla algılayıcı cihazın bir araya getirilmesiyle oluşturulmaktadır. KAA karakteristik özellikleri dikkate alındığında, çok geniş bir alana yayılması planlanan, çok sayıda (yüzlerce hatta binlerce) algılayıcı cihazın bir araya gelmesiyle oluşturulan; cihazların bulundukları ortamları dinleme, çevresel faaliyetleri yorumlama, kablosuz iletişim kurabilme gibi yeteneklere sahip olduğu ve çok sıçramalı veri taşınmasına elverişli ağ yapıları olarak değerlendirilebilmektedir [2, 44, 49]. Fakat belirtildiği üzere KAA kullanılarak geliştirilen uygulamalar çeşitlilik gösterdiği için ağ tasarımları da belirgin ölçüde farklılıklar göstermektedir. Örneğin askeri amaçla tasarlanmış bir KAA' da kullanılan topolojik yaklaşım kullanılarak belirli bir alanda yaşan bir canlıya ait popülasyon gözlemlenebilir [49]. Fakat bir insanın kalp atış hızı, kan basıncı, vücut sıcaklığı gibi değerlerini gözlemlemek amacı ile geliştirilen bir sağlık uygulaması hem ağın bulunacağı fiziksel ortam açısından oldukça kısıtlıdır hem de çok daha az sayıda algılayıcı cihaz kullanılarak oluşturulabilmektedir. Bu nedenle KAA' lar uygulama alanlarına göre çok farklı karakteristiklere sahip olabilirler. Bütün KAA uygulamaları değerlendirildiğinde hepsinin ortak özelliği olarak; kablosuz iletişim kurabilme özelliğine sahip, bulundukları ortamı algılayabilme yeteneği olan cihazlardan oluşan özel amaçlı ağ yapıları oldukları söylenebilmektedir.



Şekil 4.6. Örnek bir KAA topolojisi

Kablosuz algılayıcı ağları genellikle ad-hoc ağ yapısı kullanmaktadır. Bu yapıda her bir kablosuz algılayıcı cihaz çoklu-sıçrama (multi-hop) destekleyecek şekilde yönlendirme yapabilme kabiliyetine sahiptir [44]. Yani elde edilen bir verinin baz istasyonuna iletilmesi esnasında veri birden fazla ara düğüm üzerinden yönlendirilerek iletilebilmektedir [2]. Fakat sadece noktadan noktaya veri iletişimin yapıldığı kablosuz algılayıcı ağları da vardır.

KAA' ların konumlandığı ortamların coğrafi özellikleri, ağların dağıtık yapısı, cihazların donanımsal açıdan zayıf ve nazaran dayanıksız oluşu bu ağları fiziksel saldırılara karşı savunmasız kılmaktadır. Ayrıca bu tip ağlar genellikle geniş alanlara kurulduğu ve uzaktan erişim yolu ile bağlantı sağlandığı için cihazların güvenliğinin garanti edilebilmesi de çok zordur. Bu da saldırganlar tarafından cihazların çalışamaz hale getirilebilmesine ya da kötü amaçlı veriler üretilecek şekilde değiştirilebilmesine olanak tanıyabilmektedir. Kablosuz algılayıcı cihazlar donanımsal olarak kısıtlı

özelliklere sahip olduğundan güvenliği sağlayabilmek için karmaşık yetkilendirme ya da şifreleme algoritmaları geliştirmek çok zor veya olanaksızıdır. KAA' ların iletişim karakteristikleri de güvenli iletişimin sağlanmasını engellemektedir. Kablosuz algılayıcı ağlar aralarında veri transferi yaparken genellikle basit kablosuz iletişim teknikleri benimserler ve kullanılan sinyallerin gücü enerji kıtsından dolayı mümkün olduğunca düşük tutulmaya çalışılmaktadır. Bu nedenden dolayı iletilen paketler ortam gürültüsünden ya da zayıflama gibi diğer faktörlerden dolayı kısmen veya tamamen bozulabilir. Sonuç olarak veri iletişimi esnasında kayıp veya eksik veri paketleri oluşabilmektedir. Yüksek hata oranı uygulama geliştirilirken hataların düzeltilmeye çalışılması için yapılan işlemleri de anlamsız kılmaktadır. Bu yüzden uygulamalarda genellikle hataların tespit edilip düzeltilmeye çalışılması yerine aynı verinin yeniden gönderilmeye çalışılması şeklinde bir yaklaşım benimsenmektedir. Fakat hata kontrolünün çok az yapılması veya hiç yapılıyor olması şifreleme algoritmalarında kullanılan anahtarlar gibi bazı kritik verilerin uygulamalarda kullanılabilmesini zorlaştırmaktadır. Ağın iletişim kapasitesi açısından yeterliliğini sağlayabilmek yine de sağlıklı iletişim yapılabileceğini garanti edememektedir. KAA' larda veriler algılayıcı cihazlar arasında genellikle broadcast yöntemiyle iletilmektedir. Bu yüzden bir kaynaktan bir anda gönderilen bir veri paketleri ağ içerisinde çeşitli noktalarda çakışmaya yol açabilmektedir [40, 44, 45, 46, 47, 49]. Özellikle çok sayıda algılayıcı cihazdan oluşan kablosuz ağlarda bu durum değerlendirilmesi gereken ciddi bir sorun olarak ön plana çıkmaktadır.

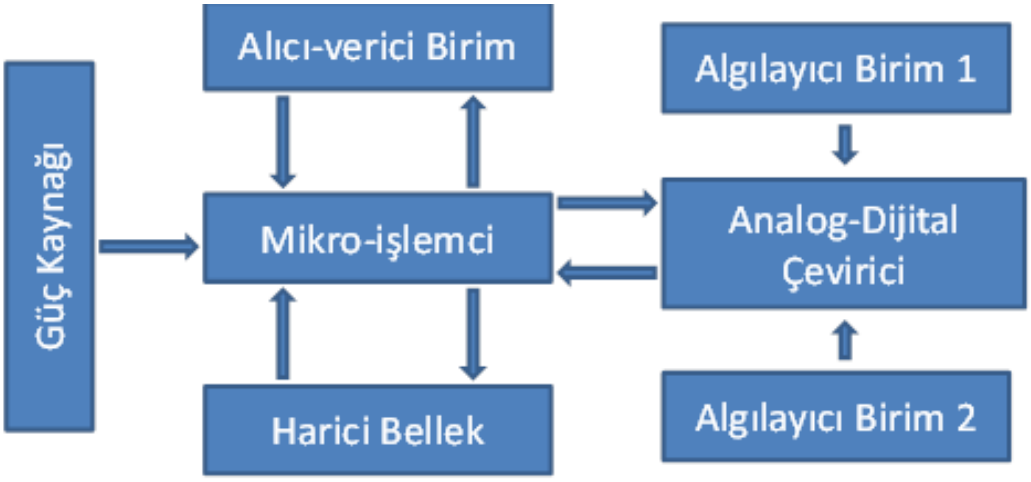
KAA' ların karakteristik özelliklerini kısaca aşağıdaki gibi sıralayabiliriz [7];

- Kablosuz iletişim
- Ölçeklenebilirlik
- Küçük boyutlarda algılayıcı cihazlar
- Kısıtlı enerji kaynağı ve işlem kapasitesi
- Zorlu çevresel faktörler
- Algılayıcı cihazların hataya yatkın olması
- Dinamik ağ topolojileri
- İletişimin hataya yatkın olması

- Algılayıcı cihazların homojen ya da heterojen özellikler taşıması
- Geniş bir alana kurulum
- Beklenmedik/kötü niyetli aktivitelere maruz kalabilme

5. KABLOSUZ ALGILAYICI CİHAZLAR

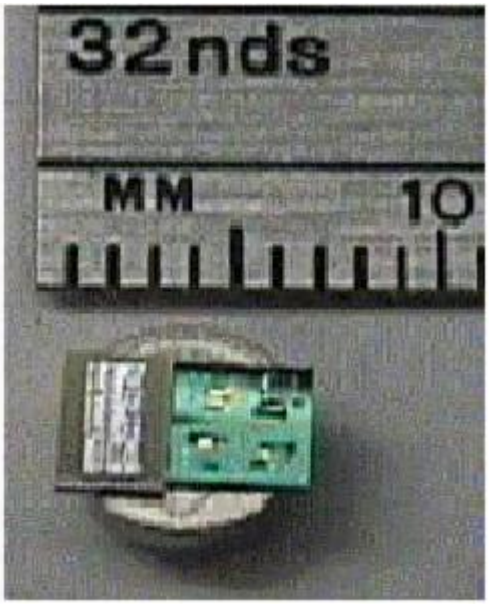
Bir kablosuz algılayıcı cihazda kullanım amacına yönelik olarak bir veya birden fazla algılayıcı bulunmaktadır. Bunun yanı sıra iletişim için genellikle bir radyo vericisi ya da benzer bir kablosuz iletişim cihazı, küçük bir mikro işlemci, hafıza birimi ve enerji için batarya veya pil gibi küçük enerji kaynakları bulunaktadır [6,8].



Şekil 5.1. Standart kablosuz algılayıcı cihaz mimarisi

Kablosuz algılayıcı cihazların işlevleri uygulama alanlarına göre farklılıklar gösterebildiği gibi büyüklükleri de farklılıklar göstermektedir. Bir kablosuz algılayıcı cihazının büyülüğü ayakkabı kutusu ebatlarından bir toz tanesine kadar değişebilmektedir. Yapılan çalışmalar genellikle algılayıcı cihazların boyutlarını mümkün olduğunca küçültmek üzerinedir ve ilk defa 1998 yılında Berkley Üniversitesinde başlatılan Smart Dust projesi ile cihazların milimetrik ölçülerde üretilmesi fikri ortaya atılmıştır [3, 25]. Cihazların maliyetleri de büyüklükleri gibi değişiklik göstermektedir. Bir kablosuz algılayıcı yüzlerce dolara mal olabileceği gibi sadece birkaç dolar maliyetle üretilebilenleri de vardır. Genellikle cihazların büyüklüğü maliyeti ve kapasitesi ile doğru orantılı olarak artmaktadır. Fakat çalışmanın devamında daha detaylı olarak açıklanacak nedenlerden dolayı işlem kapasitesi daha düşük olsa bile genellikle daha küçük ve daha az maliyetli cihazlar tercih edilmektedir. Bu alanda yapılan çalışmalar çoğunlukla yeterli işlem ve iletişim

kapasitesini sağlayacak şekilde daha az maliyetle daha küçük kablosuz algılayıcı cihazlar üretebilmek yönündedir.



Şekil 5.2. Prototip bir Smart Dust algılayıcı cihazı

5.1. Kablosuz Algılayıcı Cihazlarda Enerji Tüketimi

KAA kullanılarak uygulamalarının çalışma süreleri ağı oluşturan kablosuz algılayıcı cihazların bataryalarının ömrüne bağlıdır. Genellikle algılayıcı cihazlar tek kullanımlık olarak tasarlandığı için maliyetleri mümkün olduğunca düşük tutulmaya çalışılmaktadır. Benzer şekilde cihazın boyutları da olabildiğince küçük tutulmaya çalışılmaktadır. Bunlar gibi ekonomik ve tasarımsal nedenlerden ötürü kablosuz cihazlar kısıtlı enerji kaynaklarına sahiptirler [44].

Bir algılayıcı cihaz genel olarak ortamı dinlemek, ortamdan elde ettiği veri üzeriyi işlemek, çevresindeki diğer algılayıcı cihazlar ile iletişime geçmek, ürettiği veri paketlerinin iletimini sağlamak gibi belirli fonksiyonları yerine getirmek için enerjisini harcar. Bunun dışında cihazlarda enerji tasarrufu sağlayabilmek için geliştirilen uyku modunda da küçük de olsa bir miktar enerji tüketilmektedir. Aşağıda algılayıcı cihazlarda çeşitli durumlarda harcanılan enerji miktarları gösterilmektedir [1];

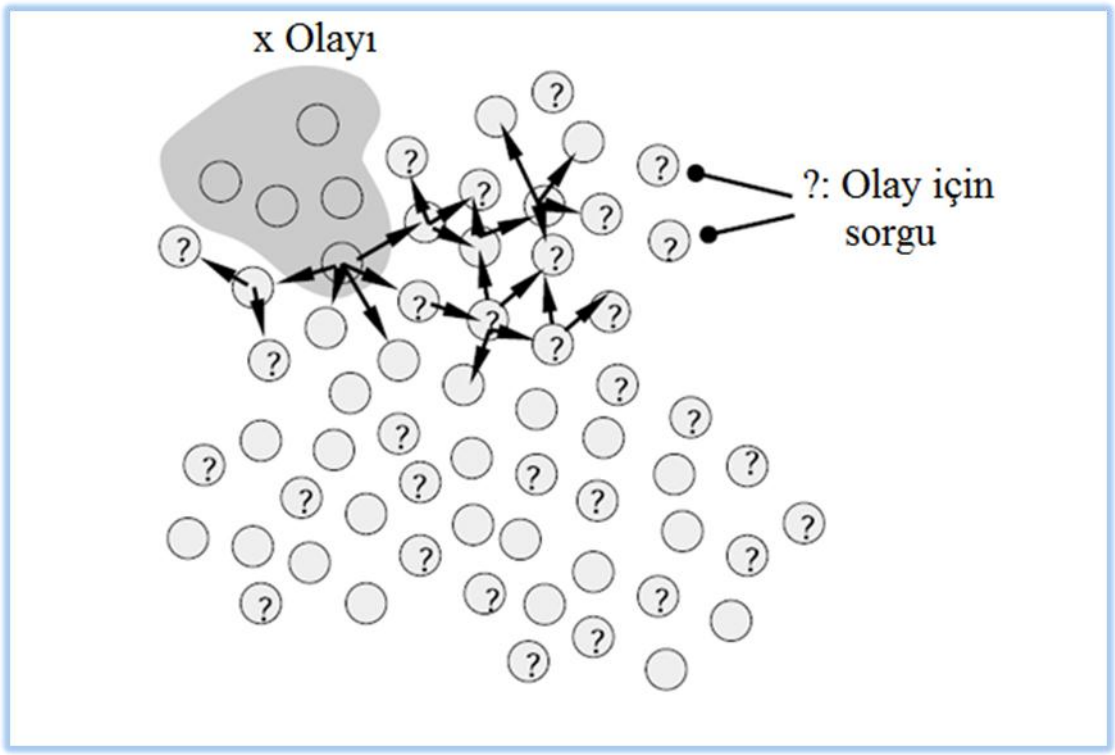
Çizelge 5.1. Standart bir ESB(Electronic Sensor Board)' ye ait enerji tüketim değerleri (Ölçümler 4,5 Volt ile yapılmıştır)

P_{CL}	12,0mA	Çalışma esnasında enerji tüketimi
P_{TX}	12,0mA	Veri göndermek için fazladan tüketilen enerji
P_{RX}	4,5mA	Veri almak için gönderilen enerji
P_{SL}	0,008mA	Uvku modunda tüketilen enerji

Çizelgede görüldüğü gibi bir algılayıcı cihaz açık konumdayken (işlemcisi ve sensörleri aktif haldeyken) uyku moduna göre tam 1500 kat daha fazla enerji tüketmektedir. Benzer şekilde veri aktarımının veri almaya göre tam 3 kat daha maliyetli olduğu açıkça görülebilmektedir. Enerji tüketim değerleri donanımdan donanıma değişiklik gösterse de fonksiyonel bazda enerji tüketim oranları aşağı yukarı aynı olacaktır. Bu değerlere bakıldığında öncelikle uyku modunun algılayıcı cihazlar açısından ne kadar hayati önem taşıdığı görülmektedir. Uyku modu özelliğinin günümüzde mevcut donanımsal kısıtlara rağmen algılayıcı ağ konseptini anlamlı kılan en temek faktör olduğu söylenebilmektedir [1].

Çizelge 5.1.' de gösterilen sayısal değerler kısıtlı olan enerji kaynaklarının hangi amaçlar için daha yoğun bir şekilde tüketildiğini de açıkça ortaya koymaktadır. Bu değerler baz alınarak algılayıcı cihazların toplam enerji tüketimi optimize edilmek istendiğince öncelikle veri iletişiminin gözden geçirilmesi düşünülebilmektedir. Bunun nedeni veri iletiminin tekrarlama içeren bir işlem olmasıdır. Algılayıcı cihaz ortamdan elde ettiği veriyi iletimi hazırlamak için üzerinde sadece bir kere işlem yapması yeterli olabilmektedir. Fakat cihazların iletim birimleri de çok kuvvetli olmadığı için ya da gürültü gibi çevresel faktörlerden kolaylıkla etkilenebildiklerinden veri iletimi hata yapmaya çok açıktır. Bu da veri paketlerinin iletilememe, yanlış veya eksik iletilme gibi nedenlerden ötürü tekrar tekrar iletilmesini gerektirebilir [43]. Yani bir algılayıcı cihaz ürettiği her bir veri için birçok kez veri göndermeye çalışabilir. Bunun yanı sıra KAA' lar çok sayıda algılayıcı cihazın bir araya gelmesiyle oluştukları için bu cihazların kendi aralarında

koordine olabilmesini ve veri iletiminde ortaklaşa çalışabilmesini gerektirmektedir. Bu durumda her cihaz genellikle sadece kendi ürettiği verinin değil komşularından kendine gelen tüm veri paketlerinin de iletiminden sorumludur. Bu da algılayıcı cihazın bulunduğu ortamda meydana gelen bir olay için tek bir veri paketi oluşturmasına rağmen çok sayıda veri paketini göndermek zorunda olması anlamına gelmektedir.



Şekil 5.3. KAA içerisinde veri transferi

Kablosuz algılayıcı cihazların enerji tüketimini etkileyen faktörler dikkate alınarak KAA uygulamalarında ağın ömrünü uzatabilmek için daha etkili çözümler tasarlanması mümkündür. Genel olarak bir KAA yapmak üzere tasarlandığı görevleri yerine getirirken harcanılan enerjinin çok büyük bir kısmının ağ içerisinde elde edilen verilen baz istasyonuna kadar taşınması esnasında tüketildiği görülmektedir [43, 44]. Bu nedenle ağın ömrünü uzatmak isteniyorsa veri paketlerinin taşınmasında optimizasyonlar yapılması ciddi kazanç sağlayacaktır. Sayısal değerler ile örneklemeye çalışırsak bir kablosuz algılayıcı cihazın veriyi işleme şeklinde optimizasyonlar yapılarak enerji tüketimi 12mA' den 10mA' e düşürdüğümüzü

varsayarsak bu algılayıcı cihaz başına toplam 2mA’ lik bir kazanç sağladığımız anlamına gelmektedir fakat eğer veri iletimi esnasında gereksiz paketlerin gönderilmesi engellenirse veri paketi başına 12mA kazanç sağlanılabilir. KAA’ larda veri iletiminin genellikle tekrarlı bir süreç şeklinde ilerlediğini düşünürsek bu tip bir optimizasyon ile enerji tüketimine ciddi katkılar sağlanabileceğini söyleyebiliriz.

6. KAA' LARDA ENERJİ VERİMLİLİĞİ

KAA' larda ağın ömrünü belirleyen en önemli faktörlerden birisi de ağdaki veri iletişimidir. Çünkü kablosuz algılayıcı cihazları harcadıkları enerjinin büyük bir kısmını veri alışverişi sırasında harcamaktadırlar. Örneğin Berkley firması tarafından üretilen ve yaygın olarak kullanılan algılayıcı cihazlarda 1 bitlik verinin iletilmesi için harcanan enerji tam 800 adet komutu işlemekte harcanan enerjiye eşittir [59]. Kablosuz algılayıcı cihazları arasında haberleşmenin başlaması için kullanılan protokoller, paket başlıkları, veri güvenliği ya da bütünlüğünü sağlamak için kullanılan işaret paketleri gibi iletişim ile ilgili unsurlar enerji tüketimini direkt olarak etkilemektedir [1].

Daha kompleks güvenlik yaklaşımları iletilen verilen için daha büyük paket başlıkları demektir ki bu da kablosuz algılayıcı cihazın birim veri için daha çok enerji tüketmesi anlamına gelmektedir [27]. Bu noktada verinin güvenliği/güvenilirliği ile enerji tüketimi arasındaki dengeyi çok iyi kurmak gerekmektedir. Benimsenecek olan yaklaşım ağın ve iletişimin güvenliğini kabul edilebilir oranlar dahilinde sağlarken aynı zamanda paket başlıklarının çok büyümemesini sağlamalıdır.

Çizelge 6.1. Güvenlik uygulamalarının getirdiği paket başlığı boyutu

	Uygulama verisi	Paket Başlığı	Toplam Boyut	İletim Zamanı	Veri İletimindeki Artış
Ham veri	24	39	63	26.2	-
TinySec +Yetkilendirme	24	40	64	26.7	%1.6
TinySec +Yetkilendirme +Şifreleme	24	44	68	28.3	%7.9

Veri iletişimine harcanan enerjiyi optimize ederken paket başlıklarının küçük tutulmasının yanında güvenlik uygulamalarına yardımcı olarak kullanılabilecek başka yöntemler de vardır. Bu yöntemlerden özellikle kablosuz algılayıcı ağlarında sıklıkla kullanılan iki tanesi şunlardır;

- Kümeleme
- Veri Gruplama

Bu yöntemler kullanılarak ağ içerisinde gerçekleşen paket veri iletimi düzenlenerek enerji tüketimi optimize edilmeye çalışılmaktadır [28]. Bu yaklaşımlarda genel olarak iletilen veri ile değil o verinin nasıl iletildiği ile ilgilenirler. Örneğin kümeleme yaklaşımlarında algılayıcı düğümlerin her biri elde ettikleri veriyi baz istasyonuna göndermek yerine kendi aralarında kümeler oluştururlar ve iletecekleri veriyi küme lideri olarak seçilen algılayıcı düğüme iletirler. Bu sayede belirli bir sorgu için tüm veriler belli başlı ana yollar üzerinden iletilmektedir. Gruplama yaklaşımlarında ise tüm düğümler elde ettikleri sonuçları göndermek yerine belirli sayıda kablosuz algılayıcı cihaz elde ettikleri sonuçları bir gruplama fonksiyonuna tabi tutarak tek bir sonuç üretir ve gruplama fonksiyonuna giren tüm verileri özetleyen tek bir veri iletilir. Her iki yaklaşım ile ilgili detaylı açıklama çalışmanın devamında verilecektir.

Kablosuz algılayıcı ağ tasarlanırken veri gruplama yaklaşımları benimsenirse ağın güvenlik yapısında da köklü değişikliklere gidilmesi gerekmektedir. Çünkü bozuk bir düğümün tüm ağa erişimi var ve kolaylıkla sonucu bozabilir [29]. Güvenlik yaklaşımları kurgulanırken bu faktör hesaba katılmalıdır. Veri kümeleme yaklaşımının benimsenmediği bir topolojide veri paketi direkt olarak baz istasyonundan gönderilen bir anahtar kodu ile şifrelenerek tekrar baz istasyonuna gönderilebilir. Veri üzerinde gruplama yapılmayacağı için veri paketleri tek sıçrama ya da çok sıçrama yöntemlerinin herhangi biri ile gönderilebilir. Ve son olarak baz istasyonuna ulaştığında şifrelendiği özel anahtar kullanılarak tekrar deşifre edilebilir. Fakat veri gruplama yaklaşımları benimsenmek istenirse şifreli veri standart gruplama fonksiyonlarına tabi tutulamayacağı için önce deşifre edilmesi

gerekmektedir. Birçok algılayıcı cihazdan gönderilen verilerin hepsi deşifre edildikten sonra gruplama fonksiyonuna tabi tutulurlar ve elde edilen sonuç tekrar şifrelenerek ağa iletilir ki bu durum şifreleme/deşifreleme işlemlerinin defalarca tekrarlanmasını gerektirmektedir. İşte bu yüzden Açık anahtar şifreleme metodu ile ağın güvenliği sağlanabilse de direkt olarak veri gruplama yöntemleri ile birlikte kullanılması oldukça maliyetlidir. Bu çalışmada teorik olarak homomorfik matematiksel işlemler kullanılarak şifreleme/deşifreleme maliyetlerini arttırmadan veri gruplamanın avantajlarından nasıl faydalanılacağı anlatılacaktır [30].

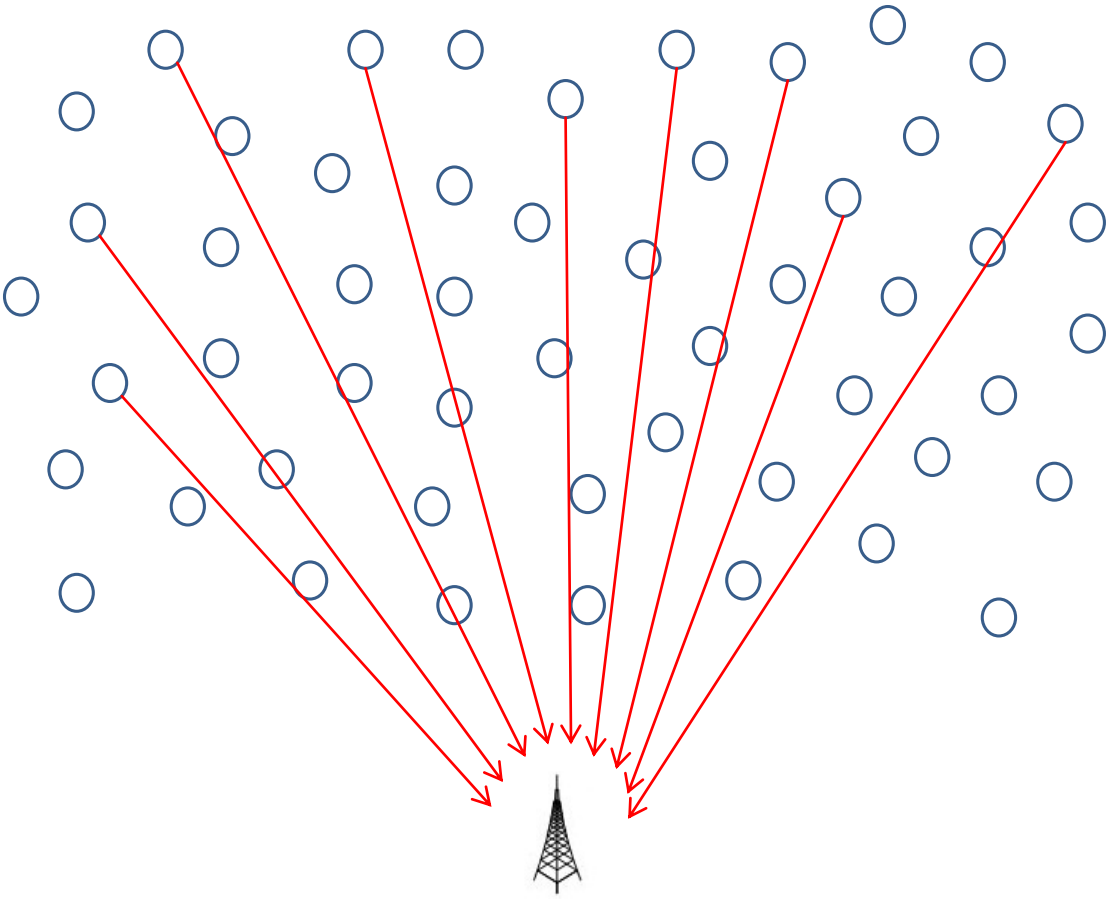
Kablosuz algılayıcı ağlarında her cihaz bulunduğu alanı kendi algılama kabiliyetlerince özetlemektedir. Edinilen veri benimsenen her hangi bir yönlendirme metodolojisi ile baz istasyonuna iletilir. KAA ile uzakta yer alan geniş bir bölge kolaylıkla gözlemlenebilir çünkü bu düşük maliyetli algılayıcı cihazlar genellikle kullanıcı müdahalesi olmaksızın kendi kendilerini organize edebilme yetisine sahiptirler. Fakat bu özellikleri algılayıcı cihazların genellikle kullanıcıların gözetiminden uzakta olması anlamına gelmektedir. Bu durum da ağı dışarıdan gelebilecek her türlü tehlikeye ya da kötü niyetli müdehaleye karşı savunmasız kılabilmektedir. Bu durum doğal yaşam gözetleme gibi çeşitli uygulamalarda risk düşük olduğu için kabul edilebilir olabilir fakat özellikle savunma sanayi gibi alanlarda hayati önem taşımaktadır. Bu yüzden hem her bir cihazın hem de ağın tamamının minimum güvenlik gereksinimlerine karşılık verebilecek düzeyde korunmasının sağlanması gerekmektedir.

Bir algılayıcı düğümün yaşam süresi çok uzun değildir. Örneğin MICAz algılayıcı cihazı iki adet AA pil ile çalışmaktadır. Cihazlar minimum enerjiyle maksimum süre çalışabilmek için çeşitli çalışma modlarına sahiptirler. Ağ tipleri ve çalışma şekiller çok farklılık gösterse de ortalama bir kablosuz algılayıcı cihazının çalışma ömrü 9 ay civarındadır [28]. Şifreleme gibi güvenlik yaklaşımları geliştirilirken KAA' ların bu özelliklerinin de dikkate alınması gerekmektedir. Çünkü istenildiği kadar karmaşık güvenlik algoritmaları kullanılmış olsun, eğer bu durum tüm algılayıcı cihazların enerjilerini birkaç günde tüketmelerine neden olacaksa sağlanılan güvenliğin uygulamada hiçbir getirisi olmamıştır demektir. Bu nedenle güvenlik yaklaşımları

tasarlanırken ya da tasarlanmadan önce enerjinin optimum kullanımı dikkate alınmalıdır. Çalışmanın bu bölümünde açıklanacak olan kümeleme ve veri gruplama yaklaşımları bu ihtiyacı KAA' uygulamalarının kısıtlarını sağlayacak şekilde karşılayabilme potansiyelleri olan ve bu alanda yaygın olarak başvurulan iki temel yaklaşımdır.

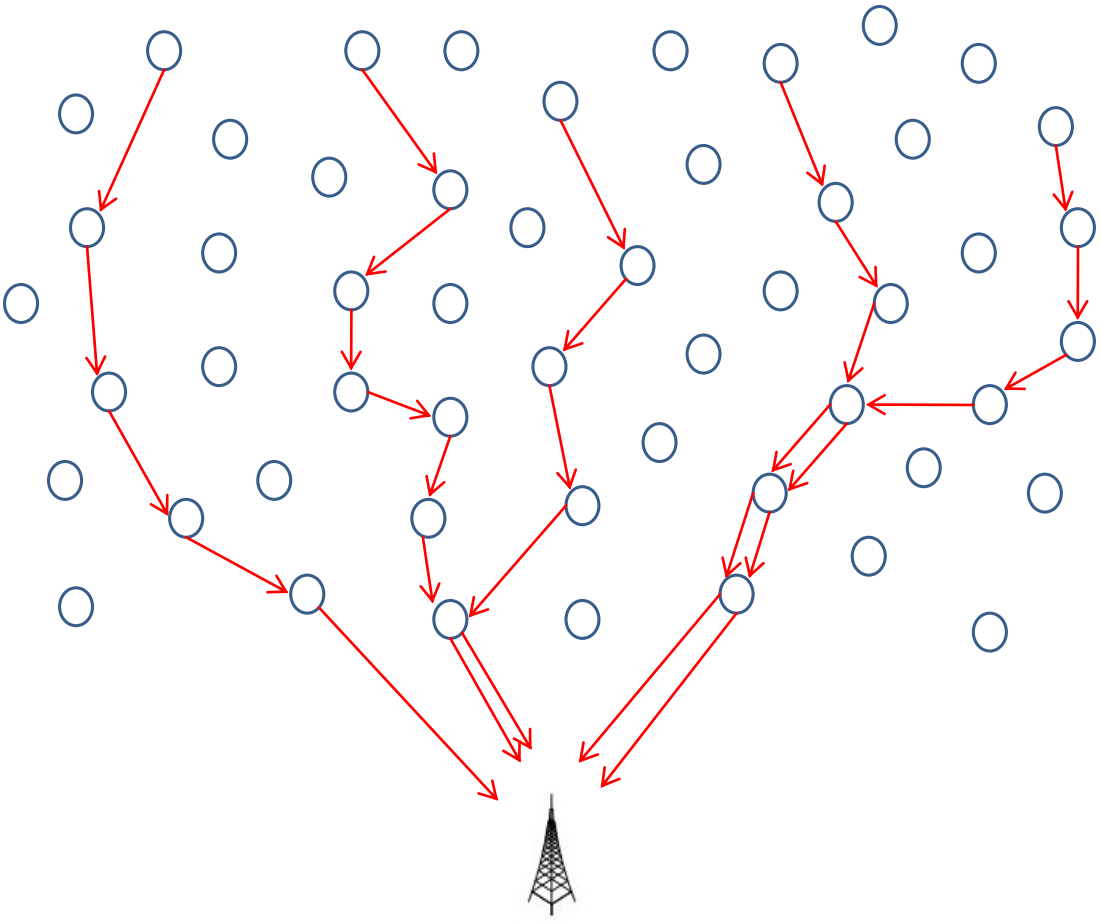
6.1. Demetleme

Ağın ömrünü uzatmaya yönelik yaklaşımlardan olan Demetleme yaklaşımları önceden de belirtilmiş olduğu üzere genel olarak ağ içerisinde iletilen paketlerin içeriği ile değil ne şekilde iletilecekleri ile ilgilenirler. Her hangi topolojik yaklaşım benimsenmemiş standart bir kablosuz algılayıcı ağda algılayıcı cihazlar elde ettikleri veriyi münferit olarak oluşturacakları rotalar üzerinden baz istasyonuna iletmeye çalışırlar [28]. İletim şekli konusunda çeşitli alternatif yaklaşımlar benimsenebilmektedir. Örneğin her bir algılayıcı cihaz elde ettiği veriyi tek sıçrama yaptırarak baz istasyonuna iletmeye çalışabilir. Fakat bu durum KAA konsepti için çok uygun değildir. Genellikle kablosuz algılayıcı cihazların geniş bir alana yayılması ile oluşturulan KAA' larda her hangi bir algılayıcı cihazın baz istasyonuna olan uzaklığı çok fazla olabilmektedir. Donanımsal olarak kısıtlı özelliklere sahip algılayıcı cihazların direkt olarak uzak mesafelere veri iletebilmeleri de çok olanaklı gözükmemektedir. Tek sıçramaya alternatif olarak uygulanabilecek bir diğer yaklaşım her algılayıcı cihaz elde ettiği veriyi seçtiği bir komşusuna göndererek baz istasyonuna iletmeye çalışmasıdır. Bu da belirli bir bölge üzerinden elde edilen verilerin iletilebilmesi için çok sayıda rota oluşması ve birçok algılayıcı cihazın gereksiz yere veri iletimine katılmasına neden olmaktadır.



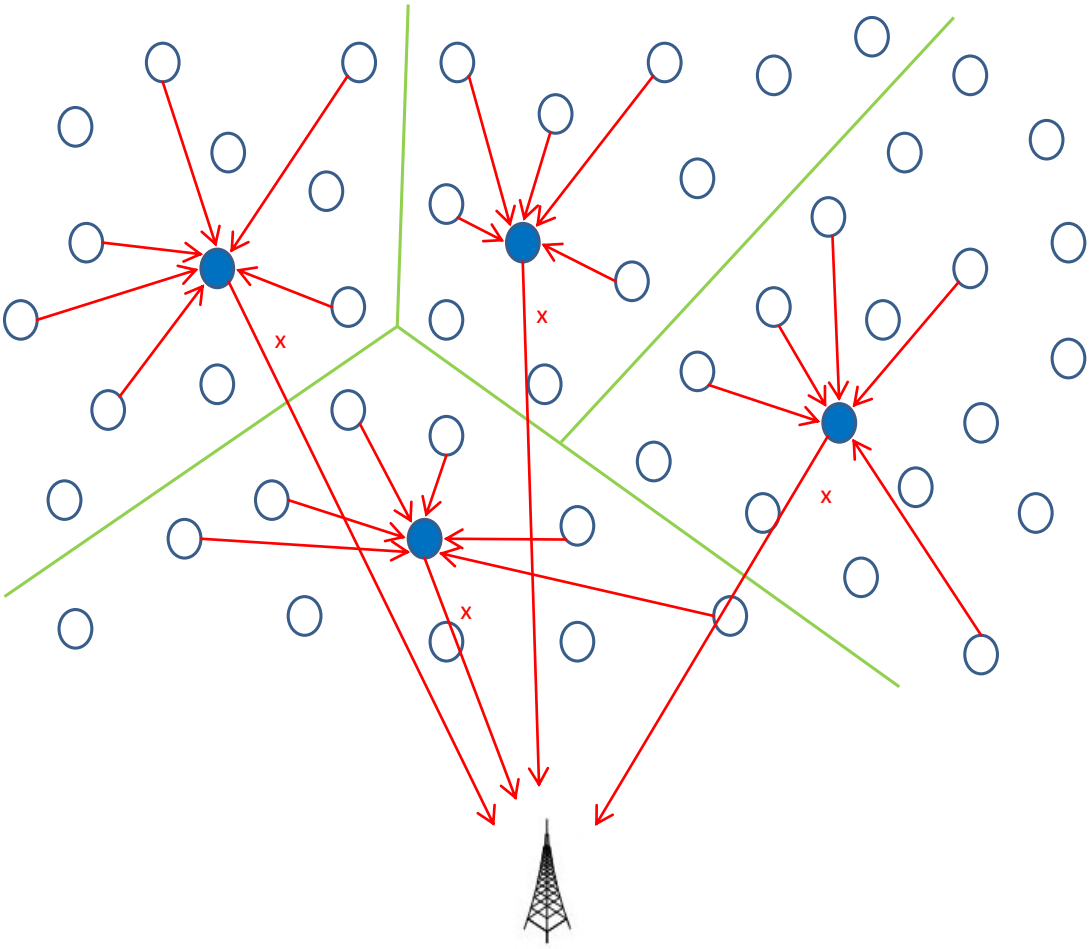
Şekil 6.1. KAA’ larda tek sıçramaları veri iletişimi

Demetleme yaklaşımlarında ise algılayıcı cihazlar ağa özel, statik ya da dinamik olarak tanımlanmış çeşitli niteliklere göre kendi aralarında gruplar oluştururlar. Her grup kendi içerisinde bir algılayıcı düğümü grup lideri olarak seçer. Bir grup içerisinde yer alan tüm algılayıcı ağlar bir veriyi baz istasyonuna iletmek istedikleri zaman grup lideri olan algılayıcı cihaza gönderirler. Veri iletişiminin geri kalan kısmı grup liderleri üzerinden devam ettirilmektedir.

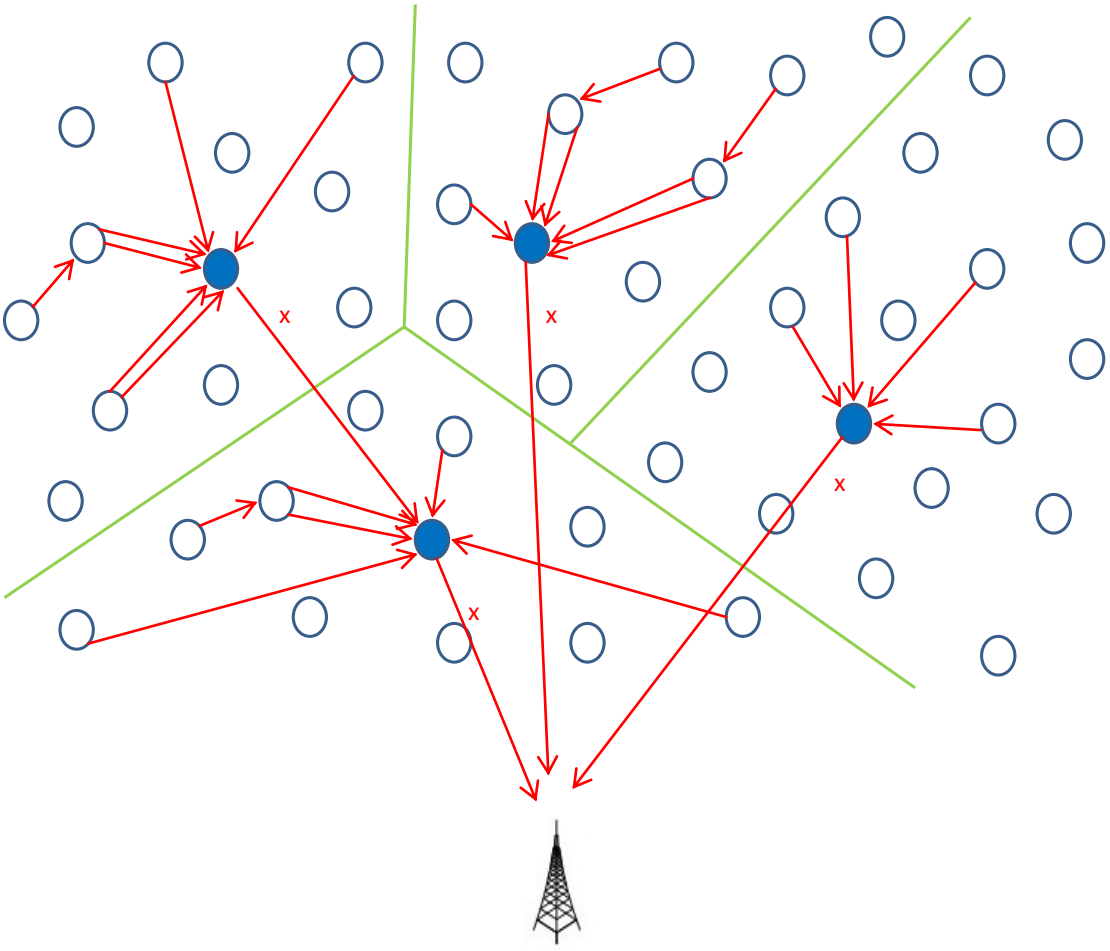


Şekil 6.2. KAA' larda çok sıçramaları veri iletişimi

Bu yöntem şu açıdan çok önemlidir; her bir algılayıcı cihaz veri iletişimine geçebilmek için öncelikle etrafındaki diğer tüm algılayıcı cihazları tespit etmek, hangisi ile iletişime geçeceğine karar vermek ve iletişime geçmeden önce gerekli protokolleri yerine getirmek gibi çeşitli adımları gerçekleştirmek durumundadır. Bu işlemlerin tamamı algılayıcı düğümler arasında daha veri iletişimine başlamadan önce bile karşılıklı çok sayıda paketin gidip gelmesine neden olmaktadır. Bu süreç basit bir veri iletişimi için bile çok sayıda algılayıcı cihazın kontrolsüz bir şekilde enerjilerini harcamalarına neden olmaktadır. Veri iletişimi belirli bir demet lideri üzerinden yapıldığında algılayıcı cihazlar arasında iletişimini başlatmak için yaşanan bu süreçten nerdeyse tamamen ortadan kalkmaktadır. Her düğüm demet liderini bildiği için etrafındaki bütün düğümleri ayağa kaldırmaz. Bu da ağın geneline bakıldığında kayda değer bir enerji tasarrufu sağlamaktadır.



Şekil 6.3. KAA' larda demetleme yaklaşımı ile tek sıçramalı veri iletimi



Şekil 6.4. KAA' larda demetleme yaklaşımı ile çok sıçramalı veri iletimi

Bu yaklaşımda dikkat edilmesi gereken bir nokta demet liderlerinin nasıl seçileceği konusudur. Bir gruba ait trafiğin tamamı sürekli olarak ya da belirli bir süre için seçilmiş olan demet liderleri üzerinden yapılacağından bu cihazların enerjilerinin çok daha çabuk tükenmelerine yol açacaktır. Demet liderlerinin seçilmesinde benimsenen yöntemlere göre farklı demetleme yaklaşımları geliştirilmektedir.

6.1.1. HEED (Hybrid Energy Efficient Distributed)

Birden fazla ağ parametresini değerlendirerek çalışan HEED yaklaşımı diğer demetleme yaklaşımlarına göre biraz daha karmaşık bir yapıya sahiptir. Demetler oluşturulup demet liderleri seçilirken algılayıcı cihazların kalan enerji miktarlarının birincil parametre olarak değerlendirildiği HEED yaklaşımında ikincil parametreler

olarak düğümlerin komşularına olan uzaklıkları gibi etkenler de göz önüne alınmaktadır. Demetleme işlemi kısa periyotlarla iteratif olarak yinelenir. Bu şekilde gerekli görülürse demet liderleri sıklıkla değiştirilerek enerji tüketiminin orantılı bir şekilde ağın geneline yayılması sağlanabilmektedir [33].

6.1.2. MRECA(Mobility resistant efficient clustering)

MRECA, HEED' e göre daha statik bir yaklaşımdır. HEED yaklaşımında demetler iteratif olarak sürekli yenilenirken MRECA yaklaşımında demetleme işlemi deterministik olarak bir kere yapılmaktadır. Demetlerin aktif kalma süresi ve demet liderinin seçimi de yine deterministik yöntemlerle gerçekleştirilmektedir. Her algılayıcı cihaz belirlenen süre boyunca ağ üzerinde yalnız bir demete ait olacak şekilde gruplanır ve algoritma cihaz bu demet üzerinden tek bir mesaj iletecek şekilde işler [34].

6.1.3. LEACH (Low Energy Adaptive Clustering Hierarchy)

LEACH yaklaşımı genellikle bir uç kullanıcının uzak bir ortam ile ilgili gözlemleme yapma ihtiyacı duyduğu durumlarda kullanılan dinamik bir demetleme yaklaşımıdır. Bu yaklaşımda uzak ortam ile ilgili verilerin en kısa şekilde sonucu kullanıcıya ulaştıracak bir baz istasyonuna iletilmesi beklenmektedir. Bu noktada ağın ömrünü uzatabilmek ve ağ içerisinde veri iletişimini azaltabilmek için algılayıcı cihazlar arasında demetleme yapılabilir. LEACH yaklaşımı bu amaç doğrultusunda geliştirilmiştir [35].

6.1.4. EEDC (Dynamic clustering and energy efficient routing)

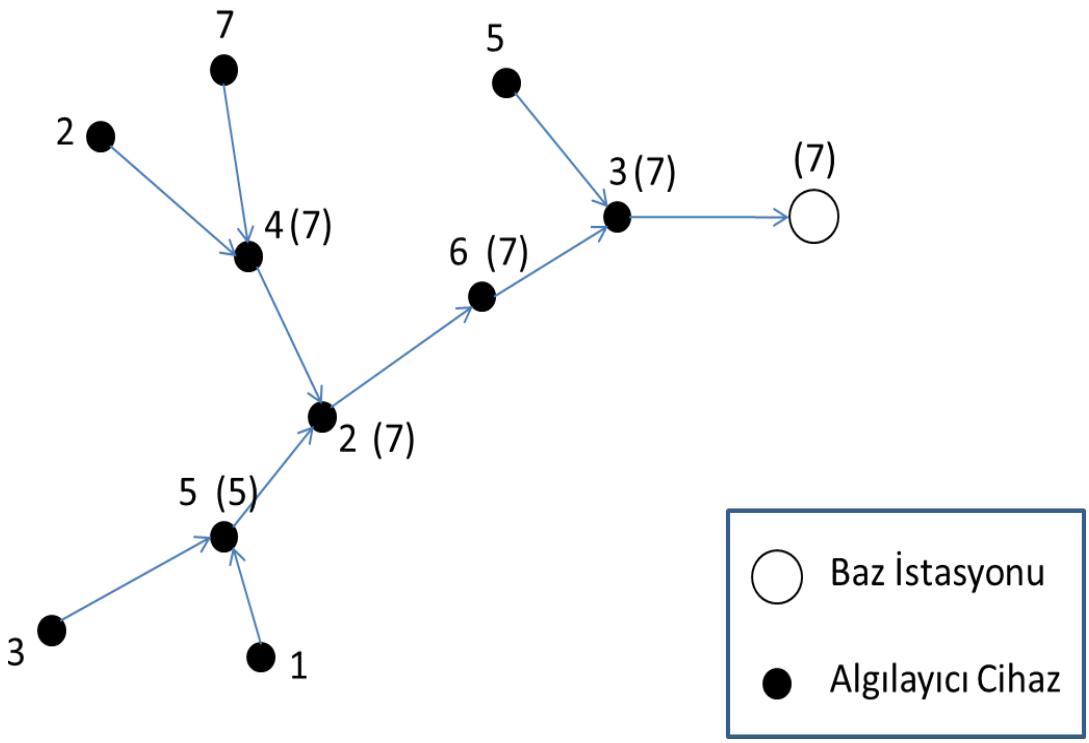
EEDC yaklaşımı iki katmanlı hiyerarşik bir ağ yapısı içermektedir. Bu yapıda iletişimin tamamı demet liderleri üzerinden sürdürülmektedir. Algılayıcı cihazların her biri direkt olarak demet lideri ile haberleşirler bu sayede demet içi yönlendirme maliyetlerini ortadan kaldırmak amaçlanmaktadır. Demet içerisinde yer alan

algılayıcı cihazlar sinyal gücü gibi niceliklerine göre karşılaştırılarak içlerinden birisi demet lideri olarak seçilir.

Demetleme kapsamında yukarıda bahsedilen yöntemlerin dışında da ağın enerji tüketimini optimize etmeye yarayan bazı diğer yaklaşımlar da vardır. En kısa yol ve minimum spinning tree algoritmaları bu yöntemlerin başında gelmektedir. Bu yöntemler belirlenerek tüm ağ içerisinde en az maliyetle tüm algılayıcı cihazlara ulaşabilecek bazı rotalar belirlenerek veri iletimi kontrol altına alınabilir. Uygulamaların sonraki safhalarında bu rotalar üzerlerinde yer alan algılayıcı cihazların enerji durumlarına göre kendilerini dinamik olarak yenileyebilirler.

6.2. Veri Kümeleme

Tipik bir KAA' da çok sayıda cihaz uygulamaya göre değişiklik gösteren çeşitli verileri konumlandırıldıkları ortamdan toplarlar. Algılayıcı cihazlar daha sonra bu verileri işlenmeleri, yorumlanmaları, değerlendirilebilmeleri ve son olarak da uygulamalar tarafından kullanılabilmeleri için merkezi bir baz istasyonuna iletirler. Algılayıcı cihazların kendi aralarında haberleşmesi işlemi maliyetli bir işlemdir. Özellikle komşu olarak konumlanmış algılayıcı cihazlar arasındaki veri transferi sırasında ciddi miktarda enerji boşa harcanmaktadır çünkü komşu cihazlardan elde edilen veri çoğunlukla tekrarlıdır. Ayrıca KAA' lar genellikle çok sayıda algılayıcı cihazdan oluştuğu için tüm ağdan elde edilen veri tek bir baz istasyonu tarafından işlenebilmek için çok fazla sayıda olabilmektedir [58, 59]. Cihazların teknik kısıtlarından dolayı enerji tüketiminin büyük önem taşıdığı bu çeşit ağlarda özellikle veri transferi ciddi bir enerji tüketim maliyeti teşkil etmektedir. Veri transferi esnasında harcanılan enerjiyi azaltmak için uygulanılan genel yaklaşım çeşitli kaynaklardan gelen verilerin bir arada aktarılması şeklindedir. Dağıtık yapıdaki verilerin bu şekilde bir araya getirilerek işlenmesi işlemi genel olarak *veri kümeleme* olarak adlandırılmaktadır.



Şekil 6.5. Ağdan maksimum değerin elde edildiği bir veri kümeleme örneği

Veri kümeleme, fazlalık olan veri iletişiminin kaldırılması ve baz istasyonu tarafından işlenmek üzere bütünleşik veri üretilmesi için farklı kaynaklardan gelen verilerin birleştirilmesi işlemi olarak tanımlanmaktadır [58]. KAA' larda veri kümeleme işlemi genellikle farklı algılayıcı cihazlardan elde edilen verilerin iletim esnasında ara adımlarda birleştirilmesi ve elde edilen bütünleşik verinin baz istasyonuna doğru yönlendirilmeye devam edilmesini içermektedir [43, 44, 58]. Şekil 6.5.' te yer alan örnekte maksimum değer alma işlemi yapan bir veri kümeleme fonksiyonu kullanılarak uygulanmış bir veri kümeleme örneği yer almaktadır. Burada her bir algılayıcı cihaz kendilerine gelen veri paketlerini teker teker göndermek yerine bu veri değerlerini kendi aralarında karşılaştırarak en yüksek değeri tespit eder ve sadece onu gönderir. Bu şekilde veri transferi esnasında harcanan enerji açısından ciddi bir kazanç elde edilebilmektedir. Örnekte yer alan sayılardan parantez içerisinde olmayanları algılayıcı cihazlar tarafından bulundukları ortamdan elde edilen sayılardır. Parantez içerisinde yer alan sayı değerleri ise o algılayıcı komşularından aldığı verileri veri kümeleme işlemine tabii tuttuktan sonra

bir sonraki algılayıcı cihaza elde etmek üzere elde ettiği değeri ifade etmektedir. Veriler bu şekilde gruplanarak sadece tek bir özet ve ya kritik veri iletilerek aktarım devam ettirildiğinde her sıçramada bir çok tekrarlı paketin gereksiz yere iletilmesinin getireceği fazladan enerji tüketimi maliyetinden kurtulunacaktır. Örnek şekildeki yaklaşım tüm ağ içerisinden elde edilen değerler arasında üst veya alt sınırların kritik olduğu bir uygulama için çok uygun bir tercih olacaktır (Örneğin sıcaklık kontrolü, yangın alarmı, …vb.). Veri kümeleme yaklaşımında maksimum değer alma yaklaşımının yanı sıra elde edilen verileri özetlemek için ağın amacına uygun olarak; toplamını alma, aritmetik ortalamasını alma, minimum değer bulma gibi çok sayıda çeşitli veri kümeleme yaklaşımlarından faydalanılabilmektedir.

Veri kümeleme yaklaşımı, algılayıcı düğümler tarafından toplanılan kritik verilerin baz istasyonu tarafından erişilebilir olmasını enerji verimliliği açısından uygun ve minimum gecikme süreleri ile sağlamayı hedefler. İyi planlanarak uygulandığında kayda değer enerji tasarrufu sağlayabilecek olan bu yöntemin servis kalitesi açısından beraberinde getirdiği çeşitli handikaplar da vardır. Farklı kaynaklardan gelen veriler ağ içerisinde yer alan kümeleme özelliğine sahip algılayıcı cihazlar tarafından veri kümeleme işlemine tabi tutularak iletilirler. Yapılan kümeleme işlemi de belli bir zaman alacağı için iletim esnasında gecikmeler olacaktır. İletilecek olan bir veri baz istasyonuna taşınana kadar ne kadar çok kümeleme işlemine tabii tutulursa gecikme payı o kadar artacaktır. Ayrıca birden fazla kaynaktan elde edilen aynı tipteki veriler birleştirilerek işleme sokulan tüm verileri özetler nitelikte tek bir veri paketi oluşturulmaktadır. Bu da verinin hassasiyetinin kaybolmasına yol açacaktır. Örneğin;

$$Ag_{(n)} = \frac{V_1 + V_2 + \cdots + V_n}{n} = V_A \qquad (6.1)$$

Yukarıdaki denklemde yer alan Ag bir veri kümeleme fonksiyonu V' ler ise farklı algılayıcı cihazlar tarafından toplanılan aynı tipteki veriler olsun. Ag fonksiyonu basitçe tüm girdi değerlerini toplayarak ortalamasını alıp işleme sokulan tüm verileri özeteler nitelikte tek bir veri oluşturacaktır. $V_1 = 7.002$, $V_2 = 7.003$, $V_3 = 7.997$

ve $V_4 = 7.998$ şeklinde dört farklı kaynaktan delen veriyi *Ag* fonksiyonuna tabi tutacak olursak;

$$Ag_{(4)} = \frac{V_1 + V_2 + V_3 + V_4}{4} = (7.002 + 7.003 + 7.997 + 7.998)/4 \quad (6.2)$$
$$= (7.002 + 7.003 + 7.997 + 7.998)/4 = (30)/4 = 7.5 = V_A$$

Olarak hesaplanılır. Elde edilen tek bir değer farklı algılayıcı cihazlardan gelen dört farklı değer yerine bir sonraki algılayıcı cihaza iletilecektir. Örnekte de görüldüğü üzere elde edilen değer işleme sokulan tüm değerlere aşağı yukarı yakın olsa da girdilerin hepsi virgülden sonra üç karaktere kadar bir hassasiyete sahipken sonuçta elde edilen değer virgülden sonra tek karakterdir. Bunun yanı sıra kümeleme işlemine dahil olacak yanlış bir değer tüm sonucu etkileyecektir. Yine aynı örnek üzerinden gidilecek olursa $V_1 = 7.002$ olarak ölçümlenmesi gereken veri bir nedenden dolayı bozularak $V_1 = 15.002$ şeklinde iletsin ve bu şekliyle *Ag* fonksiyonuna dahil edilsin. Bu durumda işlemler aşağıdaki gibi değişecektir;

$$Ag_{(4)} = \frac{V_1 + V_2 + V_3 + V_4}{4} = (15.002 + 7.003 + 7.997 + 7.998)/4 \quad (6.3)$$
$$= (38)/4 = 9.5 = V_A$$

Olarak hesaplanacaktır. Bu durumda sonuçta elde edilen değer olması gerekenden $9.5 - 7.002 = 2.0$ birim daha fazla hesaplanmış olacaktır ki bu da yaklaşık olarak %26' lık bir hata anlamına gelmektedir. Ayrıca bu şekilde tek bir algılayıcı cihazda meydana gelen hata toplamda dört farklı kaynaktan toplanan verinin bozulmasına neden olacaktır. Böyle bir durum ağın hata toleransını da düşürecektir. Bu gibi nedenlerden ötürü KAA' larda veri kümeleme kalıtımsal olarak gelen zorlayıcı bir görevdir çünkü tasarımcılar etkili bir yapı oluşturabilmek için enerji kazancı ile gecikme süreleri, veri hassasiyeti, hata toleransı, güvenlik gibi çeşitli kriterler arasında uygun bir denge kurmayı başarmalıdırlar [44]. Bu dengenin sağlanması için de veri kümeleme yöntemleri veri paketlerinin ağ içerisinde yönlendirilme şekli ile bire bir ilişkilendirilmiştir. Bu yüzden algılayıcı ağın mimari yapısı veri kümeleme yöntemlerinin performansları açısından hayati önem taşımaktadır. Hem veri

kümeleme hem de yönlendirme işlemlerinin eş zamanlı olarak yapılabilmelerini sağlayan bazı protokoller mevcuttur. Bu protokolleri iki grup altında toplayabiliriz;

- Ağaç yapısı bazlı veri kümeleme protokolleri
- Demet bazlı veri kümeleme protokolleri

Veri kümeleme alanında yapılan ilk çalışmalar daha çok yapıldıkları zamanda kullanılan yönlendirme protokolleri üzerinde durarak bu protokollerin veri kümeleme yapılabilir hale getirilmesi konusunda yoğunlaşmışlardır. Bunun sonucunda en kısa yol ağaç yapısı üzerine kurulmuş çok sayıda veri kümeleme yaklaşımı geliştirilmiştir. Daha güncel çalışmalar ağaç yapısı bazlı mimarilerde hiyerarşik yapıdan kaynaklanan gecikme sürelerini azaltmaya odaklanmaktadırlar. Bunun için algılayıcı cihazları kendi aralarında gruplayarak veri kümeleme işlemi daha etkili hale getirilmeye çalışılmaktadır.

7. KAA' LARDA GÜVENLİK YAKLAŞIMLARI

KAA' lar sahip oldukları yönetimsel zorluklar ve işlemsel kısıtlardan dolayı her zaman güvenliklerinin geliştirilmesi açısından araştırma/geliştirme yapmaya açık bir alan olarak gözükmektedir. Bu konuda yapılan mevcut konularda araştırmacılar iki temel yaklaşım etrafında yoğunlaşmaktadırlar. Bir kısım araştırmalar tasarım aşamasının KAA' larda güvenliğin sağlanması açısından çok önemli olduğunu düşünmektedir. Bu düşünceyi benimseyen çalışmalarda ağın güvenliğinin daha ağ tasarlanırken düşünülmeye başlanması gerektiğinin altı çizilmektedir. Konu ile ilgili bir diğer fikir ise ağ üzerinde yapılan düzenlemeler ve optimizasyonlar ile ağın sağlanmasının daha doğru olduğunu öne sürmektedirler. Bu görüşü benimseyen çalışmalarda ise tasarım ve geliştirme aşamasında yapılması gereken değişikliklerin çok daha maliyetli olacağını savunmaktadırlar [32].

7.1. Şifreleme

KAA' lar genellikle gözetimden uzak ve kontrolsüz alanlarda kurulmakta ve kullanılmaktadır. KAA' ların bu özelliği onları veri aktarımının dinlenmesinden ağın işlevini bozucu nitelikte kötü amaçlı verinin ağa gönderilmesine kadar birçok aktif ve pasif saldırıyla karşı karşıya gelmesine neden olmaktadır [28]. Ağın güvenliğini sağlamak için verileri direkt olarak iletmek yerine onları yetkisiz kullanıcılar tarafından ele geçirildiklerinde kendi başlarına bir anlam ifade etmeyecek başka bir şekle dönüştürerek iletim sağlanmalıdır. Bunun için KAA' larda da şifreleme algoritmalarından faydalanılmaktadır. Şifreleme algoritmaları sayesinde cihazlar tarafından ortamdan elde edilen veriler bir veya birden fazla anahtar yardımı ile şifrelendikten sonra iletilirler. Şifreli veriler kötü niyetli kullanıcılar tarafından ele geçirilse dahi ilgili anahtar değeri veya değerlerine sahip olunmadığı sürece ham verinin elde edilmesi imkansız ya da çok zor olacaktır.

Şifreleme yaklaşımlarını kullanılan anahtar sayıları ve algoritmalar dikkate alındığında, Simetrik Şifreleme ve Asimetrik Şifreleme olarak iki ana grubu ayırabiliriz.

7.1.1. Simetrik Şifreleme

Simetrik şifreleme yaklaşımlarında şifreli olarak iletişime geçecek tüm paydaşlar tarafından bilinen tek bir şifre kullanılmaktadır. Hem şifreleme hem de deşifreleme işlemi aynı anahtar değeri (K) kullanılarak yapılmaktadır. Tek bir anahtar değeri olduğundan ve tüm işlemler aynı anahtar değeri üzerinde yapıldığından bu tarz yaklaşımlarda anahtar değerinin güvenliğinin sağlanması çok önemlidir.

Şekil 7.1. Simetrik şifreleme

KAA' ları dışarıdan gelecek saldırılara karşı korumanın en basit bir yolu sadece ağ tarafından bilinecek bir anahtar değerinin şifreleme için kullanılmasıdır [32]. Bu sayede ağ içerisindeki veri trafiği seçilen anahtar değeri kullanılarak şifrelenmiş olduğundan dışarıdan bu trafiği dinleyebilen bir kullanıcı direkt olarak iletilmekte olan verilerin içeriği hakkında bilgi sahibi olamayacaktır. Böylece ağ içerisindeki iletişim bir anlamda dışarıya karşı korunaklı hale getirilmiş olacaktır. Simetrik şifreleme algoritmaları bu tarz çözümler için son derece uygundur. Simetrik şifreleme yaklaşımlarında şifreleme işlemi genellikle iletilecek olan verinin küçük parçalara ayırılarak seçilen anahtar değeri ile blok blok işleme sokulması şeklinde yapılmaktadır. Bu nedenle asimetrik şifreleme yaklaşımlarına göre genellikle daha az maliyetlidirler. Asimetrik şifreleme yaklaşımları şifreleme yaklaşımlarına göre daha fazla güvenlik sağlayabilmelerine rağmen maliyetleri çok daha yüksektir ve genellikle daha fazla işlem gücü gerektirmektedirler. KAA' ların enerji ve işlem gücü kısıtları dikkate alındığında simetrik yaklaşımların daha kolay uygulanabildikleri görülmüştür.

Bu alanda yapılan ilk çalışmalardan birisi olan TinySec, TinyOS üzerinde bağlantı katmanında güvenlik yaklaşımı geliştirmeye çalışmıştır. Geliştirilen bu yaklaşım çok küçük paket başlıklarına ihtiyaç duyan yazılımsal bir simetrik şifreleme yaklaşımıdır.

Özellikle ilk çıktığı zamanlarda çok kabul gören bir çözüm olmakla birlikte geçen yıllar ile birlikte çeşitli açıkları olduğu ortaya çıkmış ve daha fazla güvenlik sağlayacak alternatiflerin arayışlarına gidilmiştir [27,32].

TinySec' in tam tersine Zigbee ya da 802.15.4 olarak bilinen standartlar ile donanım bazlı simetrik şifreleme yaklaşımı ortaya atılmıştır. Fakat bu yaklaşım ile tasarlanılan yapının tamamen güvenli olduğuna karar verilip uygulamaya geçirilene kadar incelenmesi gereken birçok husus bulunmaktadır [27,31].

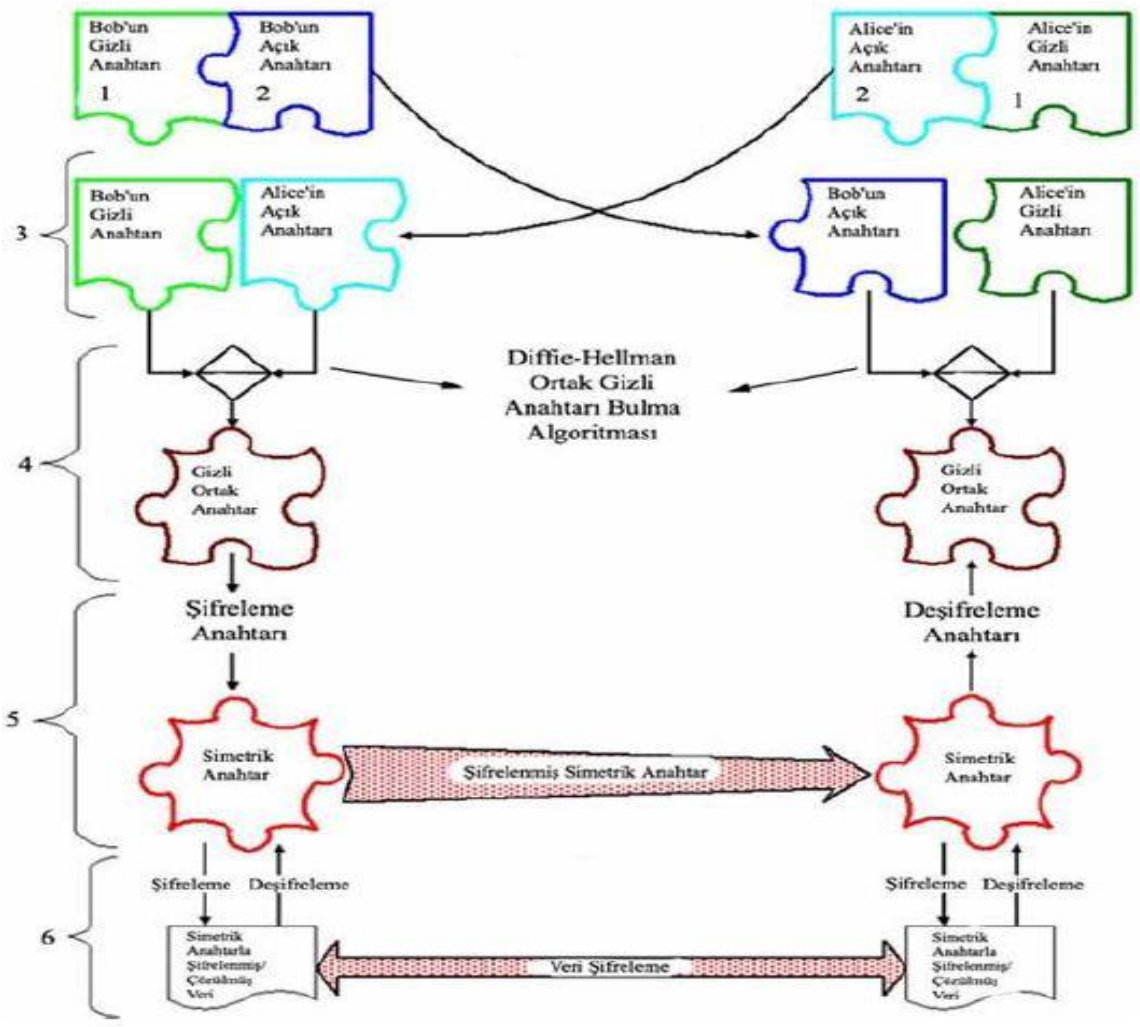
KAA'larda açık anahtar yapısının kullanılabilmesi yönünde de çeşitli çalışmalar yapılmaktadır. Ayrıca algılayıcı cihazlarda şifrelerin saklanması ya da ağ içi şifre dağıtımı gibi alanlarda da yoğun çalışmalar yapılmaktadır.

7.1.2. Asimetrik şifreleme

Asimetrik şifreleme yaklaşımlarında kullanıcıların her birinin biri açık diğeri gizli olmak üzere toplam iki adet anahtarı vardır. Kullanıcılar şifrelemeye başlamadan önce açık anahtarlarını karşılıklı olarak değiştirirler. Sonraki aşamada her kullanıcı kendi gizli anahtarı ve diğer taraftan gelen açık anahtarı bir işleme tabi tutar ve gizli ortak anahtar değerini elde eder. İletilmek istenilen veri bu gizli ortak anahtar değeri kullanılarak şifrelenir ve iletildiği tarafta ise yine iki farklı anahtar değerinin birleştirilmesi ile oluşturulan gizli ortak anahtar değeri kullanılarak deşifre edilir. Bu yöntemde iki farklı anahtar değeri kullanıldığından ve veri iletişiminin her hangi bir noktasında iletilen anahtar değeri kötü niyetli kullanıcılar tarafından ele geçirilse dahi tek başına şifreli verinin deşifre edilmesi için yeterli olmayacağından iletişimin güvenliği konmuş olacaktır.

Açık anahtar şifreleme yaklaşımlarında iki tarafın kendi açık anahtarlarını karşılıklı olarak paylaşarak bir gizli ortak anahtar elde edilmesi şifrelemenin yapılması ve iletişimin güvenliğinin sağlanması açısından hayati önem taşıyan bir süreçtir. Diffie-Hellman anahtar değiştirme yöntemi bu amaçla ilk geliştirilen yaklaşımlardan bir tanesidir. Bu yöntemde açık anahtarların karşılıklı olarak değiştirilebilmesi ve her

alıcının elde ettiği açık anahtar ile kendi gizli anahtarını kullanarak bir gizli ortak anahtar elde etmesi için üstel sayılardan faydalanılmaktadır. Sistemin güvenliği yapılan logaritmik hesaplamaların zorluğuna dayanmaktadır.



Şekil 7.2. Diffie-Hellman anahtar değişimi

Simetrik şifreleme yaklaşımlarının hepsinde Diffie-Hellman anahtar değişim yöntemindeki benzer bir anahtar değişim algoritması kullanılmakla beraber kullanılan anahtarların boyutu ve taşınma şekillerine göre sağladıkları güvenlik artmaktadır.

RSA şifreleme

R. Rivest, A. Shamir, L. Adleman tarafından 1977 yılında meydana getirilen RSA Algoritması, hem güvenlik hem de sayısal imza için kullanılmaktadır. RSA'nın güvenliği çarpanlara ayırma probleminin zorluğuna dayanır. Güvenilirlik derecesi, şifrelemede kullanılan asal sayıların büyüklüğü ile orantılıdır. RSA algoritması, hem asimetrik şifreleme, hem de sayısal imza sağlamaktadır.

RSA anahtar değişimi algoritması şu şekildedir:

1. Rastgele ve yaklaşık aynı uzunlukta p ve q asal sayıları seçilir.
2. Bu sayıların birbirleriyle çarpışmasından n = p * q sayısı elde edilir.
3. Aynı zamanda Euler fonksiyonu olarak adlandırılan bir Q = (p-1) (q-1) sayısı hesaplanır.
4. 1 ve Q arasında yer alan, Q ile 1 dışında ortak böleni olmayan bir e sayısı belirlenir. e sayısı, açık anahtar katsayısı olarak adlandırılır.
5. 1 ve Q arasında yer alan, d * e = 1 (mod Q) eşitliğini sağlayan bir d sayısı hesaplanır.
6. Hesaplanan bu değerlerden (n,e) açık anahtar, (n,d) gizli anahtar olmaktadır.

RSA şifreleme algoritması şu şekildedir:

1. Gönderici, alıcının açık anahtarı (n,e)'yi edinir.
2. Göndereceği mesaj m'yi, $c = m^e \pmod{n}$ formülüne göre şifreler ve şifrelenmiş bilgi c'yi alıcıya gönderir.

RSA şifre çözme algoritması şu şekildedir:

1. Alıcı kendi gizli anahtarı (n,d)'yi kullanarak $m = c^d \pmod{n}$'e göre şifresi çözülmüş m'yi elde eder.

Çizelge 7.1. RSA şifreleme örneği

Adım	A (gönderici)	B (alıcı)
ANAHTAR DEĞİŞİMİ		
1		p = 62, q = 53
2		n = p * q = 61 * 53 = 3233
3		Q = (p-1) (q-1) = 60 * 52 = 3120
4		1 < e < Q, e = 17
5		d * e = 1 (mod Q), d*17 = 1(mod 3120), d = 2753
6		Açık anahtar: (n, e) = (3233, 17) Gizli anahtar: (n, d) = (3233, 2753)
ŞİFRELEME		
1	B'nin açık anahtarı (n, e) = (3233, 17)'yi alır.	
2	m = 123 mesajını bu anahtarla şifreler. $c = m^e \pmod{n} = 123^{17} \pmod{3233} = 855$; c=855 B'ye gönderilir.	
ŞİFRE ÇÖZME		
1		c = 855; kendi gizli anahtarını kullanarak $m = c^d \pmod{n} = 855^{2753} \pmod{3233} = 123$; m verisi elde edilir.

RSA şifrelemesinin kablosuz ağlar için uygun olmamasının en temel nedeni; şifreleme için çok uzun anahtar değerlerine ihtiyaç duymasıdır. Uzun anahtar değerleri algılayıcı cihazların kısıtlı işlemcileri için şifrelemeyi neredeyse imkansız kılmakla birlikte şifreleme bir şekilde yapılsa dahi veri iletişimi çok maliyetli olacağı için bu yöntemin KAA' larda kullanılması çok mümkün gözükmemektedir. Bu nedenle KAA'larda RSA kadar güvenlik sağlarken bir yandan da gerek işlem gücü

gerekse veri iletişimi açısından uygulanabilir şifreleme yaklaşımları arayışına gidilmiştir.

Eliptik eğri şifreleme

Eliptik Eğri Şifreleme (ECC) literatürde, eliptik eğrilerin sonlu kümeler üzerindeki matematiksel yapılarına dayanan bir açık anahtar şifreleme yaklaşımı olarak tanımlanmaktadır [53, 54]. ECC temel olarak sayısal verileri üçüncü dereceden bir denklem ile ifade edilen bir eliptik eğri üzerinde yer alan noktalara taşınarak şifreleme işlemi gerçekleşmektedir [51, 52]. ECC' nin güçlü yanlarından birisi sonlu kümeler üzerinde çalışmak için uygun oluşudur. ECC üzerinde matematiksel işlemler yapılırken genellikle büyük asal sayılar taban kabul edilerek modlu işlemler yapılmaktadır. Bu şekilde sonlu bir küme üzerinde çalışarak hem işleme sokulan değerler kısıtlı olacağından işlemsel maliyetten hem de oluşacak paket boyu sabit olacağından iletim maliyetinden tasarruf edilmektedir. Ayrıca seçilen modül işlemi için seçilen sayıların büyük asal sayılar olması şifreleme algoritmasının kırılmasını da zorlaştırmaktadır [43, 44, 46, 51-54].

Çizelge 7.2. RSA ve ECC anahtar boyutu karşılaştırmaları [52].

RSA Anahtar Boyutu	ECC Anahtar Boyutu	RSA/ECC Anahtar Boyutu oranları
512	106	5:1
768	132	6:1
1024	160	7:1
2048	210	10:1

Kullanılan anahtar boyutları göz önüne alındığında ECC şifreleme için harcanan bit başına en yüksek güvenliği sağlayan algoritma olarak görülmektedir. Benzer derecede güvenlik sağlayan RSA gibi şifreleme algoritmalarında şifreleme logaritmik hesaplara dayandığı için şifreleme işlemi karmaşıklaştıkça anahtar boyutu üstel olarak artmaktadır. ECC algoritması bunun aksine sınırlı bir kümesini modül

özelliğini kullanarak döngüsel bir şekilde kullanmaktadır. Bu sayede şifreleme işlemi ne kadar karmaşıklaşırsa karmaşıklaşsın anahtar boyutu belirli sınırlar içerisinde olmaktadır. Çalışmanın ilerleyen kısımlarında ECC' nin nasıl uygulandığı ve ECC kullanarak nasıl enerji verimliliği sağlanabildiğine dahil daha detaylı açıklamalar yer almaktadır.

7.2. Güvenli Demetler

KAA' larda algılayıcı cihazlar verilen belirli bir görevi yerine getirebilmek üzere kendi aralarında demetler oluşturmak zorunda kalabilirler. Bu durumda ağ içerisinde genel bir güvenlik yaklaşımı benimsenmiş olsa da aynı demet içerisinde yer alan algılayıcı cihazların kendi aralarında da güvenli bir şekilde iletişim kurabilmesi gerekmektedir.

Ne yazık ki bu alanda yeterince çalışma yapılmamaktadır. Konu ile ilgili geliştirilen az sayıda çözüm yöntemi ise güvenlikten çok kaynakların daha etkin kullanımı ile ilgilidir. Bu yöntemlerde de genellikle daha üstün nitelikli algılayıcı cihazların kendi gruplarının güvenliğini sağlamak ile sorumlu olduğunu kabul etmektedir [32].

7.3. Güvenli Veri Kümeleme

KAA' larda yönlendirme ve yetkilendirme ile ilgili paket başlıkları gibi fazladan veri iletimi maliyetinden kurtulabilmek için veri kümeleme yaklaşımları benimsenebilmektedir. Bu tip yaklaşımlarda algılayıcı cihazlardan toplanan veriler baz istasyonuna iletilmeden önce çeşitli aralıklarla gruplanarak iletilirler. Fakat bir birleştirici düğümün saldırganlar tarafından ele geçirilmesi bu düğüme gelen verilerin değerlendirmeye alınmamasına ya da bozularak gönderilmesine yol açabilir [43, 44]. Kümelenmiş veri üzerinde yapılabilecek bu tür oynamalar yalnız o cihaz tarafından üretilen verinin değil ağın tamamı ya da büyük bir kısmından elde edilmiş olan verinin bozulmasına neden olabilir.

Bu alanda yapılan çalışmaların genel amacı kümeleme yapılırken bir şekilde güvenliği sağlayabilecek fonksiyonların da desteklenmesi yönündedir.

Wagner tarafından geliştirilen bir yöntemde kümeleme özelliğine sahip algılayıcı cihazlar Merkel Ağaç yapısı kullanarak komşularındaki veriyi doğrulayabilmektedir. Bu sayede baz istasyonuna iletilen verinin de saflığı kanıtlanabilmektedir. Bu alanda geliştirilen başka bir yaklaşımda ağdaki algılayıcı cihazların çokluğunu bir avantaj olarak kullanır ve kümeleme özelliğine sahip algılayıcı cihazların komşularını veri iletimini doğrulamak için kullanmaktadır. Üçüncü bir yöntemde ise alınan veriler kümeleme yapılmadan önce çeşitli filtreleme işlemlerine tabi tutulurlar. Bu sayede yanlış sonuç üretilmesi engellenmeye çalışılmaktadır [28].

Cihazların özellikle enerji kısıtları dikkate alındığında sağlıklı güvenlik uygulamaları geliştirebilmek oldukça zordur. Bu yüzden şifreleme yöntemleri gibi maliyetli güvenlik yaklaşımları benimsenmek isteniyorsa enerji kullanımı açısından da ciddi optimizasyonlar yapılması gerekmektedir. Kablosuz algılayıcı cihazların harcadığı enerjinin ortalama %70' inin iletişimin için kullanıldığı düşünülürse daha etkili iletişim teknikleri ile daha karmaşık güvenlik uygulamaları geliştirilebilir [49]. Veri kümeleme yöntemleri özellikle ağın enerji tüketiminin optimize edilmesi açısından büyük avantajlar sağlamaktadır. Bunun yanı sıra kümeleme yaklaşımları şifreleme yöntemleri ile kombine olarak kullanılarak aynı zamanda güvenliğin de arttırılması sağlanabilmektedir.

KAA' larda güvenlik ve veri kümelemenin birlikte kullanıldığı çok fazla araştırma ya da uygulama bulunmamaktadır. Konu ile ilgili olarak yayınlanmış tek çalışma Sang et al (2006) yapılmıştır [36]. Bu çalışmada güvenli veri kümeleme şemaları geliştirilmeye çalışılmıştır. Fakat bu çalışmada yer alan tanımlamalar da güvenlik uygulamaları ya da bu uygulamaların performansları hakkında detaylı analizler yapılmamıştır.

Güvenli veri kümeleme yaklaşımları incelendiğinde genel olarak iki farklı yaklaşım uygulanabilmektedir;

7.3.1. Her iletimde şifreleme

Çalışmanın önceki bölümlerinde anlatılan açık ve kapalı anahtarlı şifreleme yöntemleri bu şifreleme metoduyla kullanılabilmektedir. Bu yaklaşımda algılayıcı düğümler elde ettikleri ölçüm değerlerini şifreleyerek iletirler. Veri kümeleyici düğümler bu veri paketlerini aldıkları anda öncelikle deşifre edip orijinal mesajlar elde ederler. Daha sonra alınan tüm mesajlar veri kümeleme fonksiyonuna sokulur. Elde edilen özet bilgi tekrar şifrelenerek iletilmeye devam edilir. Bu yöntemde algılayıcı cihazlar arasında şifreleme yapıldığı için atomik düzeyde güvenlik sağlanmıştır. Bu açıdan her ne kadar güvenli gözükürse gözüksün KAA çok sayıda algılayıcı cihazdan oluşacağı için yoğun bir veri iletimi söz konusu olacaktır ve şifreleme uygulamaları zaten maliyetli uygulamalar olduğu için veri paketlerinin her iletilişte deşifre edilip tekrar şifrelenmesi ağa ciddi bir enerji maliyeti getirecektir. Bu yüzden ölçeklenebilir bir çözüm olarak görülmemektedir [28, 44, 46, 47].

7.3.2. Uçtan-uca şifreleme

Bir diğer kümeleme yaklaşımında ise şifreleme işlemi sadece algılayıcı cihazlar üzerinde yapılmaktadır. Elde edilen ölçüm değeri şifrelenerek ağa iletilir ve şifreli veri paketleri baz istasyonuna iletilene kadar deşifre edilemez. Bu yaklaşım şifreleme maliyeti açısından ağa çok ciddi bir kazanç sağlamaktadır fakat başka bir sorunu gündeme getirmektedir. Güvenli şifreleme fonksiyonları doğrusal fonksiyonlar olmadıkları için şifrelenmiş veri paketlerine standart yöntemler ile kendi aralarında toplama gibi veri kümeleme işlemlerinin uygulanabilmesi olanaklı gözükmemektedir. Bu noktada şifrelenmiş veriler üzerinde kümeleme fonksiyonları uygulayarak elde edilen kümelenmiş veriden gönderilen orijinal mesaj veya mesajlar toplamını elde etmek üzere çeşitli matematiksel fonksiyonlar geliştirilmeye çalışılmaktadır [28]. Algılayıcı cihazlar elde ettikleri veriyi şifreledikten sonra verinin baz istasyonuna iletene kadar bir daha deşifre edilmeden üzerinde veri kümeleme yaklaşımlarının uygulanabilmesini sağlayacak esnek şifreleme yaklaşımları geliştirilmeye çalışılmaktadır [43, 44, 46].

8. "ELİPTİK EĞRİ İLE GÜVENLİ VERİ KÜMELEME" PROTOKOLÜ

Kablosuz algılayıcı cihazların fiziksel özellikleri, kullanım alanları ve karakteristikleri incelendiğinde kablosuz algılayıcı ağları için sorun oluşturan durumları temel olarak iki madde altında toplanabilmektedir;

- Yetersiz donanım (kısıtlı enerji kaynağı ve işlem gücü)
- Kontrolsüz ortam (kısıtlı güvenlik).

Son yıllara kadar farklı farklı çalışmalar konu olan bu hususlar aslında bir birleriyle yakından ilişkilidir ve bu şekilde değerlendirilmesi gerekmektedir. Standart ağ yapılarında daha karmaşık şifreleme yaklaşımları tercih edilerek güvenlik seviyesi arttırılabilir. Fakat daha karmaşık şifreleme yaklaşımları işlemcinin daha çok kullanılması ve enerji tüketiminin artması anlamına geleceğinden donanımsal kısıtları olan kablosuz algılayıcı cihazlarda bu tip yöntemlerin benimsenmesi kolay olmamaktadır. Kablosuz algılayıcı ağlarda karmaşık şifreleme algoritmaları kullanabilmek için hem uygulanacak algoritmanın matematiksel olarak sadeleştirilebilmesi yani işlem ihtiyacının minimuma indirgenmesi hem de ağın genelinde enerji kullanımının bunu destekleyecek şekilde azaltılabilmesi gerekmektedir.

Eliptik Eğri ile Güvenli Veri Kümeleme (EEiGVK) protokolü bu ihtiyaçların hepsine cevap verebilecek şekilde geliştirmeye çalışılmıştır. Protokol kullandığı karmaşık şifreleme algoritması ile güvenliği arttırırken yapılan matematiksel işlemleri sadeleştirerek işlem gücü ve enerjiden kazanç sağlamaktadır. Aynı zamanda şifrelenen verilerin gruplanabilmesine olanak tanıyarak hem tekrarlı veri iletimin önüne geçmektedir hem de her iletim adımında yapılan şifreleme-deşifre etme işlemlerinin getirdiği işlem maliyetinden kurtulunması sağlamıştır.

8.1. ECC Kullanarak Verilerin Şifrelenmesi

KAA' larda güvenlik sağlanmaya çalışılırken seçilecek şifreleme algoritması çok iyi belirlenmelidir. Eğer çok basit bit güvenlik metodu uygulanırsa ağdan elde edilen verinin güvenilirliği azalabilecektir. Toplanılan verinin geçerliliği garanti edilemedikten sonra ağın daha uzun süre çalışır halde kalması anlamlılığını yitirecektir. Aksine çok kompleks güvenlik yaklaşımları kullanarak ağdan elde edilen verinin doğruluğunu garanti etmeye çalıştığımızda da kaynakları gereğinden fazla kullanarak ağın ömrünün kısalmasına neden olabilmektedir [41, 42, 44, 50]. Taşınan bilgiler ne kadar güvenli olsa da ağın ömrünün gereğinden fazla kısalması yine o ağın kullanımını anlamsızlaştıracaktır. KAA ile geliştirilen uygulamalın güvenliği ve etkinliği bu iki faktör arasındaki dengenin başarılı bir şekilde kurulabilmesinden geçmektedir.

Önceki bölümlerde belirtildiği gibi Eliptik Eğri Şifreleme temel olarak sayısal verilerin üçüncü dereceden bir denklem ile ifade edilen bir eliptik eğri üzerinde yer alan noktalara taşınarak şifreleme işlemi gerçekleşmesidir [51, 52]. Eliptik Eğriler genel olarak aşağıdaki matematiksel fonksiyon ile ifade edilmektedir;

$$y^2 = x^3 + a.x + b \tag{8.1}$$

Şifreleme işlemi de yine bu üçüncü dereceden matematiksel fonksiyonlar kullanılarak yapılmaktadır. ECC ile şifreleme yapılırken seçilen eliptik eğri üzerinde yer alan sonlu sayıda nokta kullanılarak şifreleme işlemi yapılabilir. Bu da işlem adımlarının sadeleştirerek enerjiden tasarruf edilebilmesine olanak tanımaktadır. Şifreleme için kullanılacak eliptik eğri denklemi oluşturulurken öncelikle denklem (1)' de yer alan sabit katsayılar olan *a* ve *b* belirlenmelidir. Eliptik eğri kullanarak şifreleme yapılırken eğer eğri üzerinde yer alan sonlu sayıda elemandan oluşan bir küme ile çalışılmak isteniyorsa a ve b katsayıları aşağıdaki eşitliğe uymak zorundadır;

$$4a^3 + 27b^2 \neq 0 \tag{8.2}$$

a ve *b* katsayıları kurala uygun olarak seçildikten sonra $E_p(a,b)$ noktalar kümesi belirlenir. $E_p(a,b)$' yi kısaca, belirlenen *a* ve *b* doğal sayılarına göre $y^2 = x^3 + a.x + b$ denklemini sağlayan noktalar kümesi, olarak tanımlayabiliriz. $E_p(a,b)$ kümesi içerisinden seçilen bir $\propto = (x_1, y_1)$ referans noktası, ***başlangıç noktası*** olarak adlandırılır ve eğri üzerindeki şifreleme işlemi bu referans noktası üzerinden yapılmaktadır.

Eliptik eğri üzerinde şifreleme yaparken işlem maliyetini azaltmak için işleme tabi tutulan sayı değerleri mod alma yöntemi ile kısıtlanabilmektedir. Böylece sonsuz tane sayı değeri yerine belirli aralıkta yer alan değerler ile işlem yapılabilmektedir. Mod almak için kullanılacak *n* sayısı yeterince büyük bir asal sayı olmalıdır. Bu işlem için asal sayı kullanılmasının nedeni çarpanlara ayrılamadığından denklemin çözülmesini daha zor hale getirmesidir. Bu durumda uygulanan şifreleme algoritmasının güvenliğini arttırmaktadır. Seçilecek olan asal sayı kullanılmak istenilen sayı kümesini kısıtlamaya yetecek kadar küçük fakat aynı zamanda güvenliği arttırması açısından yeterince büyük olmalıdır. Uyulama esnasında yapılan denemeler sonucunda ihtiyaca uygun olarak çeşitli değerler seçilebilmektedir.

Eliptik eğri üzerinde şifreleme işlemi, şifrelenmek istenilen her hangi bir A değerinin belirlenen bir $y^2 = x^3 + a.x + b$ doğrusu üzerine taşınması ile yapılabilmektedir. A değerini eğri üzerine taşıyabilmek için eğri üzerinde seçilen $\propto = (x_1, y_1)$ başlangıç noktası kullanılmaktadır.

$$P_A = A. \propto = A.(x_1, y_1) = (x_2, y_2) \tag{8.3}$$

Eşitlik 8.3, bir A değerinin nasıl eliptik eğri üzerine taşındığını göstermektedir.

8.1.1 Uygulama örneği

$$y^2 = x^3 + a.x + b \tag{8.4}$$

Eliptik eğri denkleminde a = 0, b = -4 ve p = 17 olsun.

$$4a^3 + 27b^2 = 4.0^3 + 27.(-4)^2 = 0 + 432 \neq 0 \quad (mod\ 17) \tag{8.5}$$

Eşitlik 8.5' e göre seçilen a ve b değerleri şifreleme işlemi için uygundur. Ayrıca mod alma işlemi için kullanılacak p değeri örneği basitleştirmek adına küçük bir asal sayı seçilmiştir. Bu durumda şifreleme işlemi için kullanılacak olan denklem aşağıdaki gibidir;

$$y^2 = x^3 - 4 \quad (mod\ 17) \tag{8.6}$$

Şifreleme işleminde kullanılacak olan noktalar kümesi $E_p(0,4)$ ise şu elemanlardan oluşmaktadır; "(2,2) , (2,15) , (4,3) , (4,14) , (5,6) , (5,11) , (6,5) , (6,12) , (7,4) , (7,13) , (8,7) , (8,10) , (11,1) , (11,16) , (13,0)". E_p kümesinin elemanlarından (2,2)' yi başlangıç noktası ($\propto$) olarak seçerek şifreleme işlemi bu nokta üzerinden yapılabilir. Örneğin "A = 8" değeri için;

$$P_A = A.\propto = 8.(2,2) = (5,6) \quad (mod\ 17) \tag{8.7}$$

değeri elde edilmektedir. Bu sayede tekil bir sayı değeri olan A verisi $y^2 = x^3 - 4$ eliptik eğrisi üzerinde yer alan ve iki farklı koordinat ile ifade edilebilen (5,6) noktasına taşınmıştır. Eliptik eğri gruplarının toplanabilirlik özelliği vardır, yani eğri üzerinde yer alan iki nokta geometrik olarak toplanılarak yine eğri üzerinde yer alan üçüncü bir nokta elde edilebilmektedir. Bu sayede eliptik eğri üzerine taşınan şifreli veriler arasında toplama, çıkarma gibi aritmetik işlemler yapılabilmektedir. Şifrelenmiş veri üzerinde aritmetik işlemler yapılabilmesi kümeleme fonksiyonlarının da kullanılabilmesine olanak sağlamaktadır.

8.2. Şifreli Verilerin Kümelenmesi

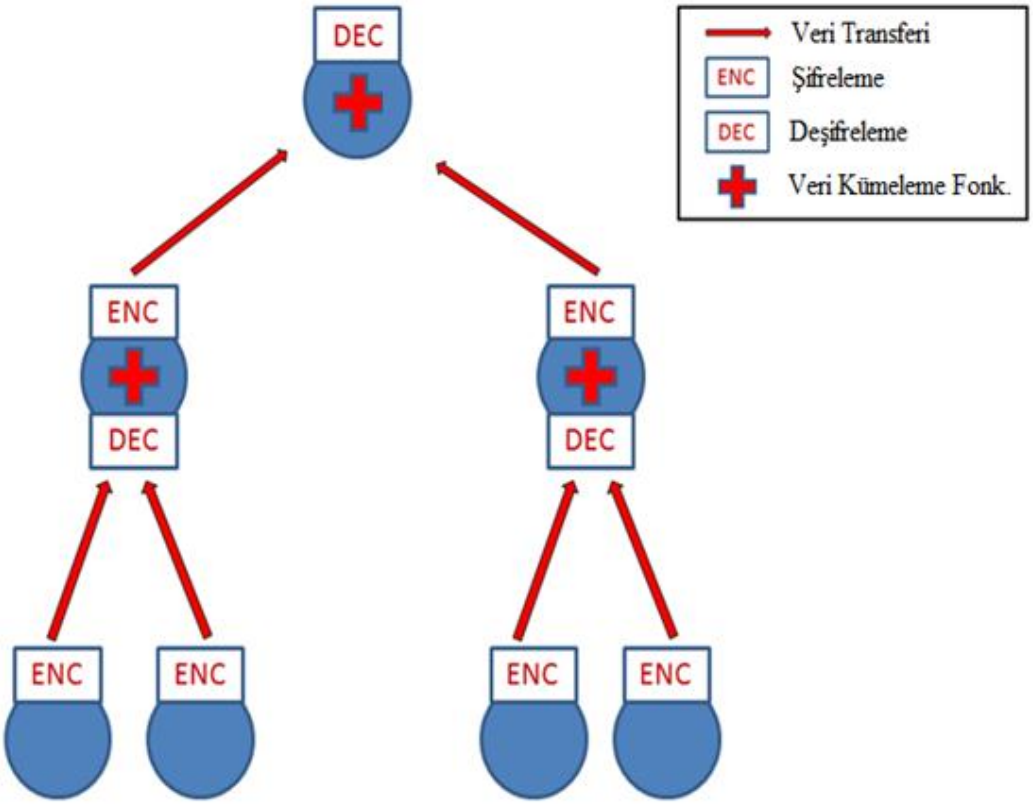
Şifreleme algoritmaları temel olarak bir değeri alıp başka bir değer kümesi üzerinde yer alan farklı bir değere taşırlar. Yapılan işlem işleme tabi tutulan değeri değiştirdiği için şifrelenen veri üzerinde toplama, ortalama alma gibi basit veri kümeleme yaklaşımları kullanılamamaktadır. Örneğin;

$$F_x = y = x + 3 \tag{8.8}$$

basit bir şifreleme fonksiyonu olsun. Bu basit örnek için bile şifrelenen verilerin toplamı asıl elde edilen değerlerin toplamının şifrelenmiş haline eşit olmayacaktır. Bu durumun çözümlenişi ise şöyledir;

$$F_{x1} + F_{x2} \neq F_{x1+x2}\ ; \tag{8.9}$$
$$(x1 + 3) + (x2 + 3) \neq (x1 + x2) + 3\ ;$$
$$x1 + x2 + 6 \neq x1 + x2 + 3$$

Bu nedenle algılayıcı cihazlar üzerinde elde edilen değerleri şifreleyip ilettiğimizde bu verilerin alıcı düğüm tarafından her hangi bir kümeleme fonksiyonuna tabi tutularak bir sonraki düğüme iletilebilmesi için deşifre edilmesi gerekmektedir. Yani standart şifreleme yöntemleri şifrelenmiş veriler üzerlerinde veri kümeleme işlemleri gibi aritmetik ya da mantıksal işlemler yapılması için elverişli değildir. Bu tarz şifreleme yöntemleri genellikle elde edilen verinin şifrelendikten sonra iletilmesini ve alıcı düğüm tarafından yeniden deşifre edilmesini gerektirmektedir (bkz. Şekil 8.1.). Ancak bu sayede alınan veri diğer düğümlerden alınan veriler ile birlikte veri kümeleme fonksiyonlarına sokularak özet bir veri oluşturulabilmektedir. KAA' ların karakteristik özellikleri değerlendirildiğinde bu yöntem uygulanabilir görülmemektedir. Şifreleme ve deşifreleme zaten algılayıcı cihazlar için fazladan kaynak tüketimi anlamına gelmekteyken bir de bu maliyetli işlemlerin her aktarım için tekrarlandığı düşünülünce bu yaklaşımın neden akla yatkın olmadığı kolaylıkla anlaşılabilmektedir. Bu noktada diğer önemli KAA kriteri olan enerjinin etkin kullanımı ön plana çıkmaktadır [41, 42, 43, 44, 45].

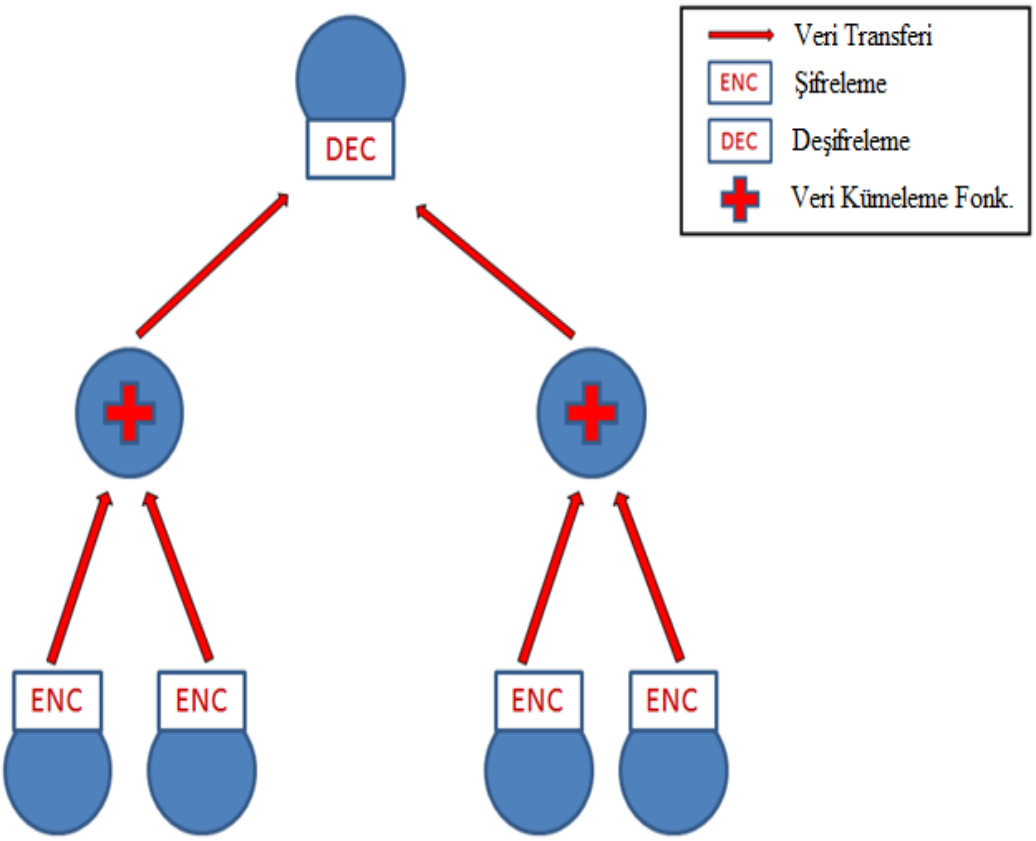


Şekil 8.1. Standart şifreleme algoritmaları kullanarak veri kümeleme

Daha önceki bölümlerde de değinildiği üzere veri kümeleme yaklaşımları kablosuz algılayıcı ağlarında enerji verimliliği açısından büyük önem taşımaktadır. Bu nedenle şifreleme algoritmaları kullanılarak güvenlik sağlanmaya çalışılırken bir yandan da veri kümeleme yaklaşımları benimsenilerek ağın enerji tüketiminin azaltılması gerekmektedir.

Yapılan araştırmalar sonucunda Eliptik Eğri Şifreleme (ECC) algoritması, kablosuz algılayıcı ağlarda güvenlik ve veri gruplama ihtiyaçlarını aynı anda karşılayabilecek ve diğer alternatif şifreleme çözümlerine göre son derece düşük çalışma maliyetlerine sahip bir yöntem olarak tespit edilmiştir. EEiGVK protokolünün temelini oluşturan ECC algoritmasının sonlu kümeler üzerinde çalışmaya olanak tanımaktadır. Bu sayede uygulanılan matematiksel işlemlerin karmaşıklığı artsa da anahtar boyutu sabit tutulabilmektedir. Sabit anahtar boyutu, ECC' nin ölçeklenebilir

bir çözüm olarak ön plana çıkmasını sağlamakla birlikte enerji tüketiminin dengelenmesi açısından da büyük avantajlar sağlamaktadır.



Şekil 8.2. ECC ile bütünleşik veri kümeleme yaklaşımı (EEiGVK Protokolü)

EEiGVK prosedürü oluşturulurken şifreleme algoritması olarak ECC' nin seçilmesinin en büyük nedeni ise homomorfizim özelliğidir. Eliptik eğriler homomorfizm özelliği sayesinde şifrelenmiş veriler üzerinde aritmetik işlemler yapılabilmesine ve dolayısıyla kümeleme fonksiyonlarının uygulanabilmesine olanak tanımaktadır. Şifrelenmiş verilerin kümeleme fonksiyonları sayesinde kümelenebilmesi ağ üzerindeki veri trafiğini büyük oranda azaltacağı gibi uçtan uca şifrelemenin de uygulanabilir olmasını sağlamaktadır. Bu durumda her veri iletiminde tekrarlı olarak yapılan şifreleme-deşifreleme işleminden de kurtulunması sağlanacaktır. İşlem maliyetlerindeki bu azalmada yine ağın ömrüne kayda değer bir katkı sağlayacaktır.

Kısıtlı enerji kaynakları ile üst düzey güvenlik sağlayabilme potansiyeli olan EEiGVK protokolü aynı zamanda kümeleme yaklaşımları benimseyerek kablosuz algılayıcı ağlarının iki önemli sorunu olan güvenlik ve enerji tüketimi konularına bütünleşik bir çözüm önerisi olarak sunulmaktadır.

8.3. Sözde Kod

Sürecin tamamı aşağıda yer alan akışta özetlenmektedir;

Başlangıç Aşaması

1. Eliptik Eğri denklemi ($y^2 = x^3 + a.x + b$) için kat sayılar (a, b) ve mod almak için kullanılacak asal sayı (p) seçilir.
2. Belirlenen kat sayılar kontrol edilerek şifreleme için uygunluğuna bakılır;
   - $4a^3 + 27b^2 \neq 0 \pmod p$ Eşitlik sağlanıyor mu?
3. Eliptik Eğri denklemini sağlayan noktalar kümesi belirlenir;
   - E_p (a, b) = V (x,y) E $y^2 = x^3 + a.x + b \pmod p$
4. Eliptik eğri denklemi, mod taban değeri olan p ve E_p tüm düğümler tarafından bilinir.

Verinin İletilmesi Aşaması

1. Ağdan her hangi bir veri çekmek isteyen algılayıcı düğüm E_p elemanları içerisinden seçtiği başlangıç noktasını ($\propto$) hedef algılayıcı düğümlere gönderir.
2. Sorguyla birlikte $\propto$ değerini de alan düğümler elde ettikleri verileri (D) $\propto$ ile çarparak eliptik eğri üzerinde bir noktaya taşırlar (E_D).
   - Çarpma işlemi noktaların geometrik olarak toplanması şeklinde yapılır;
     - n. $\propto = \propto + \propto + \ldots + \propto$ (n adet)
3. Şifrelenmiş haldeki veri (E_D) sorguyu başlatan algılayıcı cihaza iletilmek üzere geri gönderilir.

4. Veri iletimine katılan ara düğümler aldıkları verileri deşifre etmeden kümeleme fonksiyonlarına sokarlar;
   - Her ara düğüm aldığı n tane şifreli veriyi gruplayarak özet niteliği taşıyan tek bir veri üretir ve bir sonraki düğüme bunu gönderir.
   - Ara düğümler şifreli veri paketleri üzerinde deşifre etme işlemi yapmadan çalıştığından taşıdıkları verinin içeriğini bilmezler.
5. Sorguyu başlatan düğüm ağdan kendine gelen tüm şifreli veri paketlerini son bir kez kümeleme fonksiyonuna tabi tutar ve elde edilen verilerin tamamını özetler nitelikte tek bir değer elde eder.
6. Elde edilen değer başlangıç noktası ($\propto$) referans alınarak tekrar çözümlenir ve asıl iletilmek istenilen değer elde edilmiş olur.

8.4. EEiGVK Uygulama Örneği

$$y^2 = x^3 + a.x + b \quad (mod\ p) \tag{8.10}$$

Yukarıdaki eliptik eğri denklemi şablonunda;

- a = 3
- b = -7
- p = 211

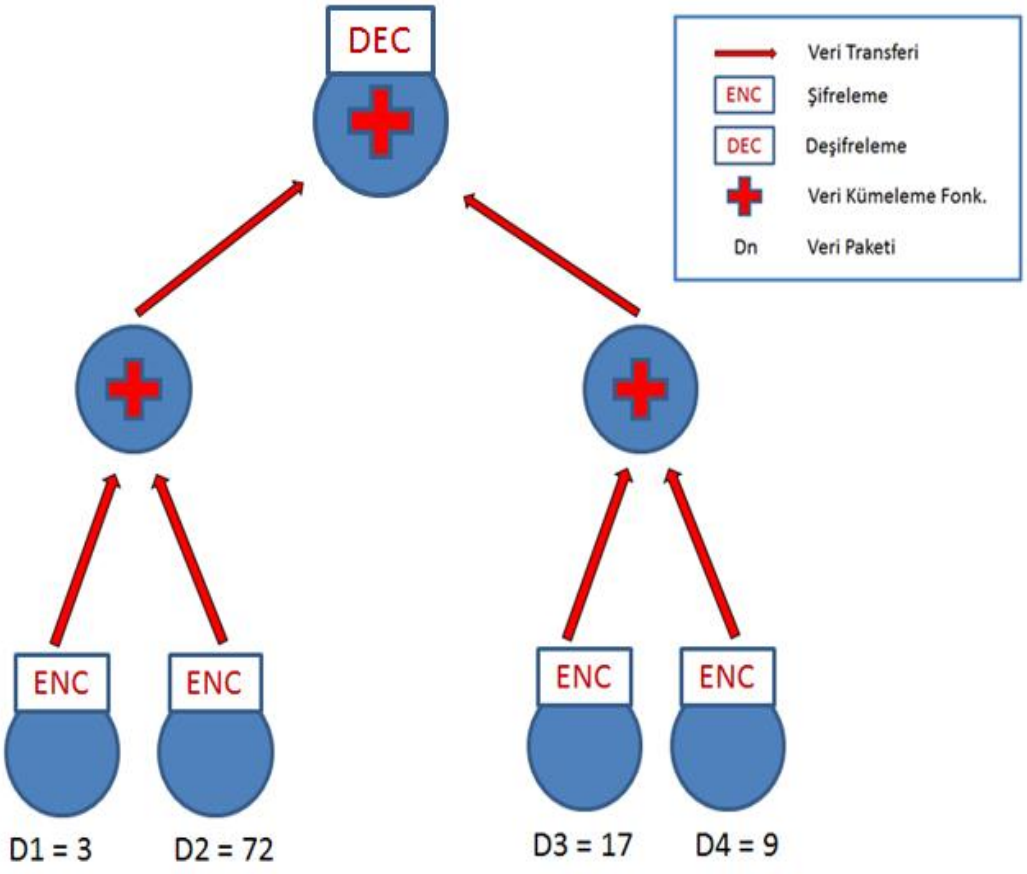
olsun. Bu durumda kullanılacak olan eliptik eğri denklemi;

$$y^2 = x^3 + 3x - 7 \quad (mod\ 211) \tag{8.11}$$

şeklinde olacaktır. Daha sonra a ve b katsayıları ilgili formülde yerine konularak denklemin şifreleme için uygunluğu kontrol edilir;

$$4a^3 + 27b^2 = 4.3^3 + 27.(-7)^2 = 108 + 1323 = 1431 = 165 \neq 0 \quad (mod\ 211) \tag{8.12}$$

Eşitlik 8.14 seçilen eliptik eğrinin ($y^2 = x^3 + 3x - 7$) şifrelemede kullanılmak için uygun olduğunu göstermektedir. Bu eliptik eğri denklemi kullanılarak uygulanacak olan örnek senaryoda; dört farklı algılayıcı cihaz tarafından elde edilen verilerin şifrelendikten sonra ikişerli olarak kümeleme fonksiyonlarına tabi tutulup iki sıçramada sorgulayıcı görevdeki algılayıcı cihaza nasıl iletildiği gösterilecektir. Kümeleme fonksiyonu olarak toplamlarını alma yönteminin benimseneceği senaryoda EEiGVK protokolünün uçtan uca nasıl uygulandığının gösterilmesi hedeflenmiştir.



Şekil 8.3. EEiGVK protokolü örneği

Şifreleme işlemine başlamadan önce belirlenen eliptik eğri üzerinde yer alan noktalar kümesi $E_p(a, b) = E_p(3, -7)$ tespit edilir. Daha önceden belirtildiği üzere $E_p(3, -7)$ kümesi a = 3 ve b = -7 olacak şekilde elde edilen eliptik eğri denklemini sağlayan noktalar kümesidir. Denklemi sağlayan noktalar hesaplanırken yapılan aritmetik

işlemlerin seçilen mod değerine göre (bu örnek için 211) yapılması gerektiği unutulmamalıdır.

$E_p(3,-7)$ kümesi belirlendikten sonra kümenin elamanı olan noktalardan bir tanesi başlangıç noktası olarak seçilir. Bu örnek için başlangıç noktası $\propto$ = (6, 4) olarak seçilmiştir. Şifreleme için kullanılacak olan eliptik eğri denkleminin ve denklemi sağlayan noktalardan oluşan E_p kümesinin tüm algılayıcı cihazlar tarafından bilindiği varsayılmaktadır. Buna rağmen B-başlangıç noktası sorguyu başlatan algılayıcı cihaz tarafından belirlenir ve değerleri elde edilmek istenilen diğer algılayıcı cihazlara gönderilir. Başlangıç noktası değerleri ilgili algılayıcı cihazlara iletildikten sonra bu cihazlar ortamdan elde ettikleri verileri teker teker seçilen başlangıç noktası ile çarpılarak eliptik eğri üzerine taşıyarak şifrelenmiş veriyi elde ederler.

E_{D1} = D1.$\propto$ = 3.(6,4) = (109,81) (*mod 211*) (8.13)

E_{D2} = D2.$\propto$ = 72.(6, 4) = (202, 9) (*mod 211*) (8.14)

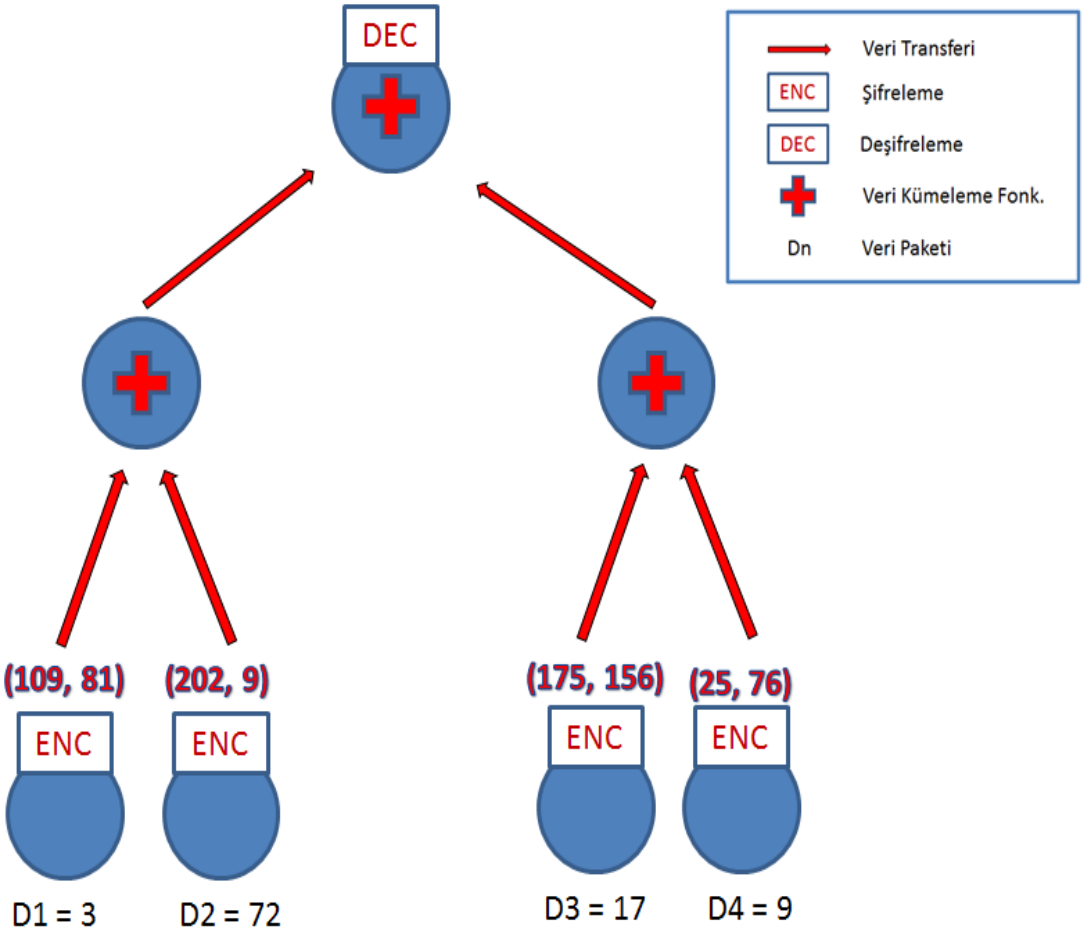
E_{D3} = D3.$\propto$ = 17.(6, 4) = (175, 156) (*mod 211*) (8.15)

E_{D4} = D4.$\propto$ = 9.(6, 4) = (25, 76) (*mod 211*) (8.16)

Yapılan matematiksel işlemlerin tamamı noktaların geometrik olarak toplanması ve çıkarılması prensibine dayandığından kullanılan eliptik eğri denklemi ve katsayıları bilinmeden anlaşılmaları çözülmesi neredeyse imkansızdır. Denklemin tamamı bilinse bile başlangıç noktası bilinmiyorsa şifrelenen orijinal asıl sayısal değerler elde edilemez.

Her algılayıcı cihaz kendisine gelen başlangıç noktasını kullanarak ortamdan elde ettiği verileri şifreledikten sonra bir sonraki algılayıcı cihaza iletir. Ara katmanda yer alan algılayıcı cihazlar kendilerine gelen şifrelenmiş verileri deşifre etmeden kümeleme fonksiyonuna tabi tutarak bir sonraki cihaza iletir. Belirtildiği üzere uygulanmakta olan örnek için değerlerin toplamını alma işlemi yapan kümeleme fonksiyonu kullanılacaktır. Yine bu örnek için birinci ara düğüm E_{D1} ve E_{D2} şifreli verilerinin, ikinci ara düğüm ise E_{D3} ve E_{D4} şifreli verilerinin geometrik olarak

toplamlarını alarak elde ettikleri değerleri sorguyu başlatan algılayıcı cihaza aktaracaktır. Ara katmanda yer alan algılayıcı cihazların her hangi bir şifreleme ya da deşifre etme işlemi yapmaya ihtiyaçları yoktur.



Şekil 8.4. Algılayıcı cihazlarda elde edilen verilerin şifrelenmesi

$$E_X = E_{D1} + E_{D2} = (109, 81) + (202, 9) = (51,194) \quad (mod\ 211) \quad (8.17)$$

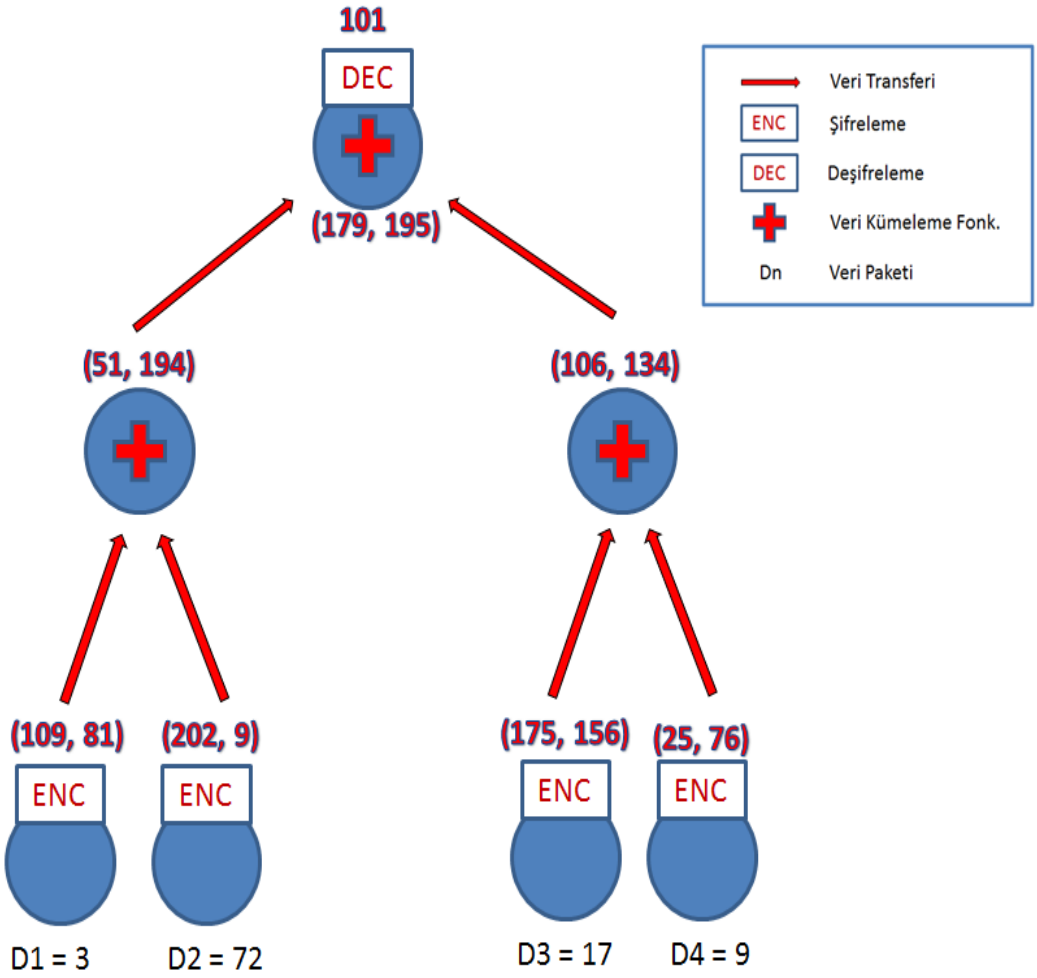
$$E_Y = E_{D3} + E_{D4} = (175, 156) + (25, 76) = (106, 134) \quad (mod\ 211) \quad (8.18)$$

Sorguyu başlatan algılayıcı cihaz kendisine gelen çok sayıda (bu örnek için iki adet) şifrelenmiş veriyi yine kümeleme fonksiyonuna tabi tutar ve bunların hepsini kullanarak tek bir değer elde eder. Uygulanmakta olan örnek için bu değer;

$$E_F = E_X + E_Y = (51, 194) + (106, 134) = (179, 195) \quad (mod\ 211) \quad (8.19)$$

olarak hesaplanılır. Elde edilen bu nihai değer yine başlangıç noktası referans alınarak deşifre edilir.

$$E_F = (179, 195) = Dn.\propto = Dn.(6, 4);\quad Dn = 101 \ (mod\ 211) \qquad (8.20)$$



Şekil 8.5. EEiGVK protokolü kullanarak şifrelenerek iletilen veri akışı

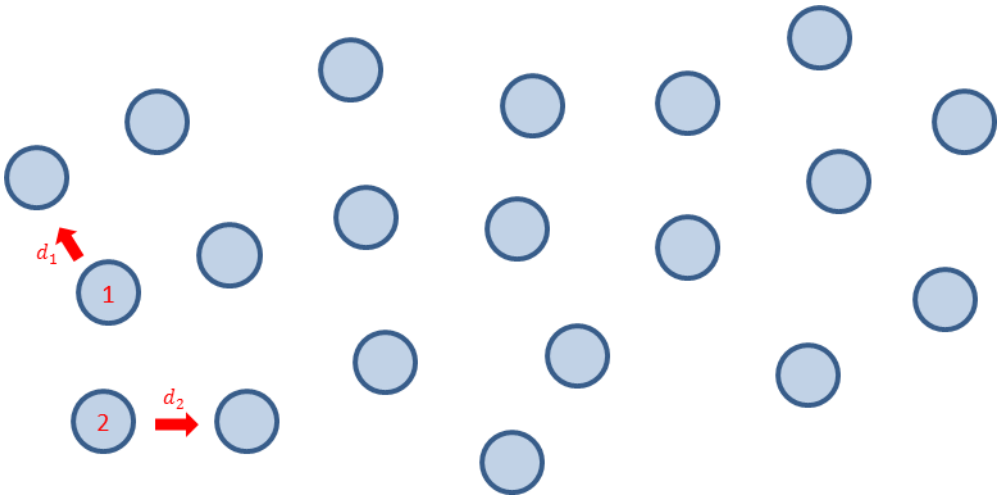
Algılayıcı cihazla tarafından şifrelenen orijinal verilerin toplamı alındığında elde edilen toplamın doğru olduğu görülmektedir.

$$D1 + D2 + D3 + D4 = 3 + 72 + 17 + 9 = 101 = Dn \qquad (mod\ 211) \qquad (8.21)$$

Verilen örnekte de açıkça görüldüğü üzere EEiGVK protokolü bir yandan eliptik eğriler gibi karmaşık matematiksel formüllere dayanan güçlü bir şifreleme algoritması ile güvenliği sağlarken öte yandan da şifrelenmiş verinin deşifre edilmeye ihtiyaç duymaksızın kümelenmesine olanak tanıyarak kablosuz algılayıcı ağları için bütünleşik bir çözüm alternatifi sunmaktadır.

9. KARŞILAŞTIRMALI SONUÇLAR

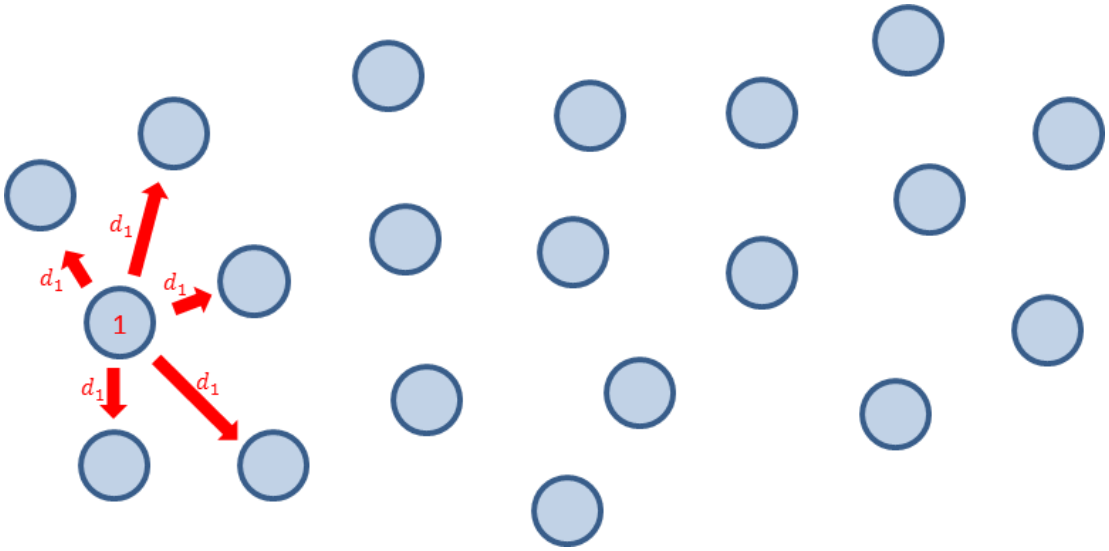
Kablosuz algılayıcı ağlarında veri transferinin ciddi bir enerji maliyetine sahip olduğu daha önceki bölümlerde belirtilmiştir. Buna göre ortalama bir algılayıcı cihazın veri işlemi esnasında harcadığı enerji veri iletimi esnasında harcadığı enerjiye eşittir (bkz. Şekil 5.3). Bunun yanı sıra algılayıcı cihazlar düşük donanımsal özelliklere sahip oldukları için veri iletimi esnasında hata almaya açıktırlar. Bu yüzden tek bir veri paketini iletebilmek için aynı paketin birden fazla gönderilmesi gerekebilir. Hata alınmadığı durumlarda bile eğer ağ topolojisi iyi bir şekilde kurgulanmamışsa aynı veri paketi komşu düğümler arasında defalarca gidip gelebilir. Bütün bunlar veri iletimi için ortaya çıkan maliyetin katlanarak artmasına neden olmaktadır. EEiGVK prosedürü tarafından uygulanan veri kümeleme yaklaşımı tekrarlı veri iletimini mümkün mertebe ortadan kaldırarak ağın geneli için ciddi bir enerji tasarrufu sağlamakta dolayısıyla ağın ömrünü kayda değer oranda arttırmaktadır.



Şekil 9.1. Algılayıcı cihazlar arasında veri iletişimi

k adet algılayıcı cihazdan oluşan bir kablosuz algılayıcı ağı ele alalım. Veri iletişimine geçildiğinde her bir cihaz bir seferde tek bir veri paketi (d_i) ilettiği takdirde ağda iletilen veri paketi adedi aşağıdaki gibi hesaplanabilir;

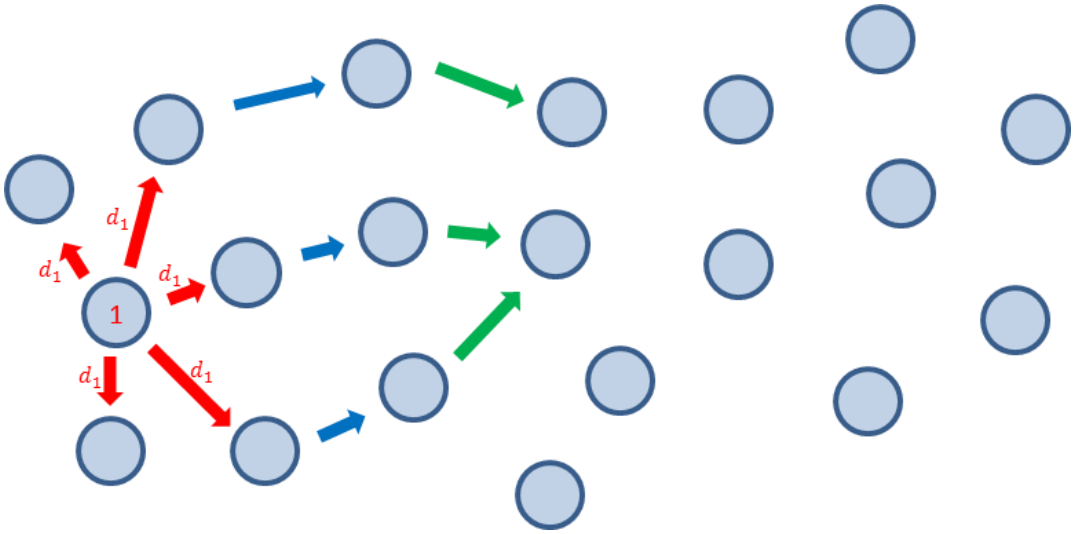
$$\sum_{i=1}^{k} d_i \tag{9.1}$$



Şekil 9.2. Veri paketinin tüm komşulara iletilerek gönderilmesi

Algılayıcı ağda, veri iletişimini şekillendiren her hangi bir yönlendirme protokolü kullanılmıyor ise ağın içerisinde yer alan her algılayıcı cihaz elde ettiği verileri komşularının tümüne ya da en yakın olanlarına göndererek verinin yayılmasını sağlayabilir. Algılayıcı cihazların elde ettikleri verileri ortalama *n* adet komşularına gönderdiklerini varsayarsak her bir iterasyonda gönderilen veri paketi adedi aşağıdaki gibi olacaktır;

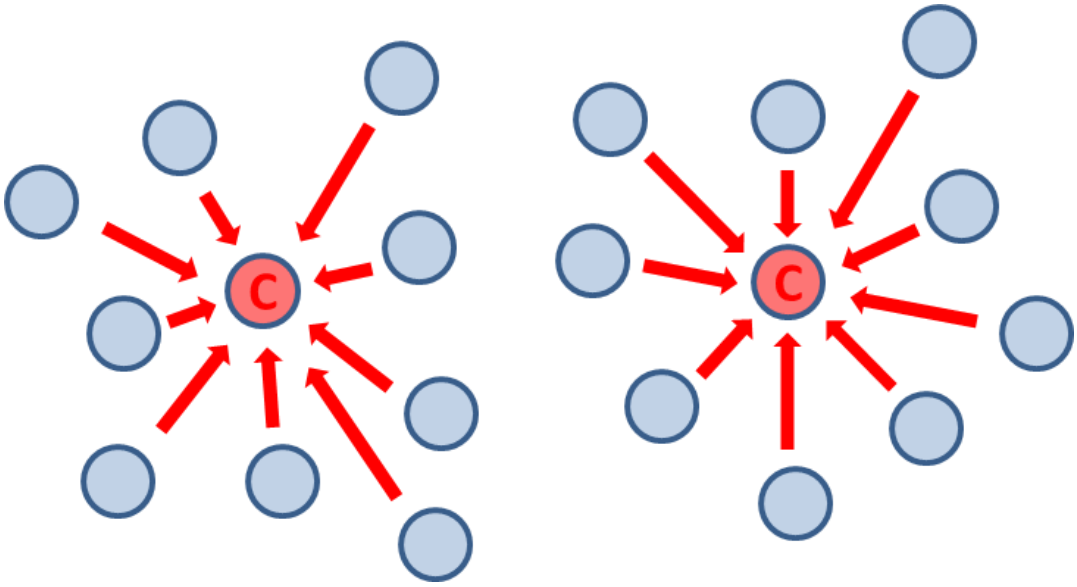
$$\sum_{i=1}^{k} n \cdot d_i \tag{9.2}$$



Şekil 9.3. Veri paketlerinin hedefe birden fazla sıçrama ile iletilmesi

Yine çalışmanın ilk bölümlerinde anlatıldığı üzere kablosuz algılayıcı ağlar genellikle geniş coğrafi konumlara yayılacak şekilde ve çok sayıda algılayıcı cihaz bir araya getirilerek oluşturulmaktadırlar. Hem cihazlar arasında mesafe olduğundan hem de veri iletimine katılacak çok sayıda algılayıcı cihaz olduğundan bir algılayıcı cihaz tarafından elde edilen veri genellikle tek seferde hedefe iletilemez. Bu nedenle veri paketleri kaynaktan çıkıp hedefe ulaşana kadar genellikle birden fazla defa iletilmektedirler. Sıçrama (h) olarak adlandırılan bu iterasyonların sayısı ağın büyüklüğüne ve benimsenen topolojiye göre değişebilmektedir. Sıçrama sayısı da denkleme eklendikten sonra ağ üzerindeki toplam veri paketi transferini hesapladığımız formülümüz aşağıdaki gibi değişecektir;

$$h \cdot \left(\sum_{i=1}^{k} n \cdot d_i\right) \tag{9.3}$$



Şekil 9.4. Veri transferinin kümeleme yöntemi ile yönlendirilmesi

Algılayıcı cihazları kendi içinde gruplayarak ağ içerisindeki veri iletişimi yönlendirmek mümkündür. Her gruptan bir algılayıcı ağ grup lideri seçilerek o grup içerisinde yer alan tüm algılayıcı cihazların elde ettikleri verileri grup liderine iletmeleri sağlanabilir. Bütün algılayıcı cihazlar oluşturdukları veriyi göndermek istediklerinde gönderecekleri cihaz belli olacağından veri paketlerinin komşular arasında tekrarlı olarak iletilmesinin önüne geçilebilmektedir. Bu durumda matematiksel modelimizdeki *n* kat sayısı ortadan kalkmaktadır;

$$h \cdot \left(\sum_{i=1}^{k} d_i\right) \tag{9.4}$$

Algılayıcı cihazların gruplanması yöntemi veri akışını yönlendirdiği ve komşu algılayıcı cihazlar arasındaki tekrarlı veri transferini engellediği için transfer maliyetini azaltmaktadır. Fakat her bir algılayıcı cihaz tarafından oluşturulan veri paketleri grup lideri üzerinden de olsa teker teker hedefe gönderilmek zorundadır. Özellikle bir birlerine yakın konumlarda yer alan algılayıcı cihazlar tarafından yapılan ölçümlerde aynı veya yakın değerler elde edileceği düşünülürse hala çok sayıda veri paketi boş yere uçtan uca taşınmaktadır. Bu noktada EEiGVK prosedürünün sunduğu çözüm veri paketlerinin grup liderleri tarafından kümelenmesini sağlamaktadır. Bu sayede grup liderleri kendilerine iletilen çok

sayıda veri paketini bir kümeleme fonksiyonuna tabi tutarak hepsini özetler nitelikte tek bir değer elde ederler ve bu değeri hedefe iletmeye çalışırlar. Dolayısıyla veri iletiminde kayda değer oranda azalma sağlanmış olur. *k* adet elemandan *c* tanesinin grup lideri olarak seçildiğini varsayalım. Her grupta eşit sayıda algılayıcı cihaz olduğunu varsayarsak ilk sıçramada iletilen veri paketi sayısı aşağıdaki gibi olacaktır;

$$c \cdot \left(\sum_{i=1}^{(k-c)/c} d_i \right) = \left(\sum_{i=1}^{k-c} d_i \right) \tag{9.5}$$

Veri paketleri grup liderleri tarafından kümeleme fonksiyonuna tabi tutularak elde edilen değerler hedefe doğru gönderileceğinden ilk sıçrama dışındaki bütün sıçramalarda sadece grup lideri sayısı kadar veri iletilecektir. Bu durumda algılayıcı cihazlar tarafından elde edilen verilerin *h* adet sıçramada hedefe iletildiğini kabul edersek matematiksel modelimiz aşağıdaki gibi olacaktır;

$$\left(\sum_{i=1}^{k-c} d_i \right) + (h-1).c \tag{9.6}$$

9.1 EEiGVK Prosedürü ile Veri Kümeleme

Örneğin altmış dört (64) algılayıcı cihazdan oluşan bir ağı ele alalım. Her hangi bir yönlendirme algoritmasının benimsenmemesi halinde algılayıcı cihazlar tarafından elde edilen veriler komşular arasında tekrarlı olarak iletilecektir. Bu duruma örnek olarak her algılayıcı cihazın elde ettiği veriyi dört (4) komşusuna gönderdiğini ve veri paketlerinin ortalama üç sıçramada hedefe ulaştırılabildiklerini varsayalım. Ele alınan örneklerde transfer maliyetleri paket bazında irdelendiğinden veri paketi (d_i) boyutlarını sabit olarak kabul edilecektir. Bu durumda toplam paket transferi maliyeti;

$$h \cdot \left(\sum_{i=1}^{k} n \cdot d_i \right) = \tag{9.7}$$

$$3 \cdot \left(\sum_{i=1}^{64} 4 \cdot d_i \right) =$$

$$3 \cdot 64 \ (\ 4 \ ) = 768$$

Yani bu şekilde basit bir ağdan her hangi bir veri toplanmak istendiğinde algılayıcı düğümler arasında toplamda 768 adet veri transferi gerçekleşeceği öngörülmektedir. Fakat günümüzde bu denli basit konfigürasyonlara sahip ağlara genellikle rastlanmamaktadır. Artık her hangi bir kablosuz algılayıcı ağ kurgulanırken en azından ağ içerisindeki veri transferini yönlendirmeye yönelik çalışmalar yapılmakta, buna uygun topolojiler ve prosedürler benimsenmektedir. Çalışma içerisinde ele alınan bir enerji verimliliği yöntemi olarak algılayıcı cihazların kümelenmesi bu amaç doğrultusunda sıkça tercih edilen bir yaklaşımdır. Algılayıcı cihazların kendi aralarında guruplara ayrıldığı ve her algılayıcı cihazın ortamdan elde ettiği verileri sadece kendi ait olduğu gurubun liderine gönderdiği ve her veri paketinin ortalama üç sıçramada hedefe ulaştığı uygulama örneğini ele alacak olursak ağ içerisindeki toplam veri transferi adedi aşağıdaki gibi hesaplanabilir;

$$h \cdot \left(\sum_{i=1}^{k} d_i\right) = 3 \cdot \left(\sum_{i=1}^{64} d_i\right) = 3.\ (\ 64\ ) = 192 \qquad (9.8)$$

Örnekte açıkça görülebildiği gibi algılayıcı cihazların paketleri bütün komşularına teker teker göndermek yerine belirli bir hedefe göndermeleri yapılan veri transferi sayısını kayda değer ölçüde azalmıştır. EEiGVK prosedürü grup lideri olan algılayıcı cihazların kendilerine gelen bütün veri paketlerini kümeleme fonksiyonuna tabi tutmasına olanak tanımaktadır. Bu sayede grup liderleri bütün paketleri teker teker göndermek yerine tek bir veri paketi göndererek takip eden sıçramalarda taşınacak olan veri paketi sayısının ciddi oranda azalmasını sağlayabilmektedirler. Yukarıdaki örneklere konu olan ağın EEiGVK prosedürü uygulanarak kendi içinde dört farklı gruba bölündüğü ve veri paketlerinin ortalama üç sıçramada hedefe ulaştığı bir örnek uygulama örneğini ele alacak olursak ağ içerisindeki toplam veri transferi adedi aşağıdaki gibi hesaplanabilir;

$$\left(\sum_{i=1}^{k-c} d_i\right) + (h-1).c = (\ 64 - 4\ ) + (\ 3 - 1\ ) .\ 4 = 60 + 8 = 68 \qquad (9.9)$$

Yukarıdaki örneklerde yer alan kablosuz algılayıcı ağ kurgularını iletilen paket sayılarına göre değerlendirecek olursak EEiGVK prosedürü kullanıldığında her hangi

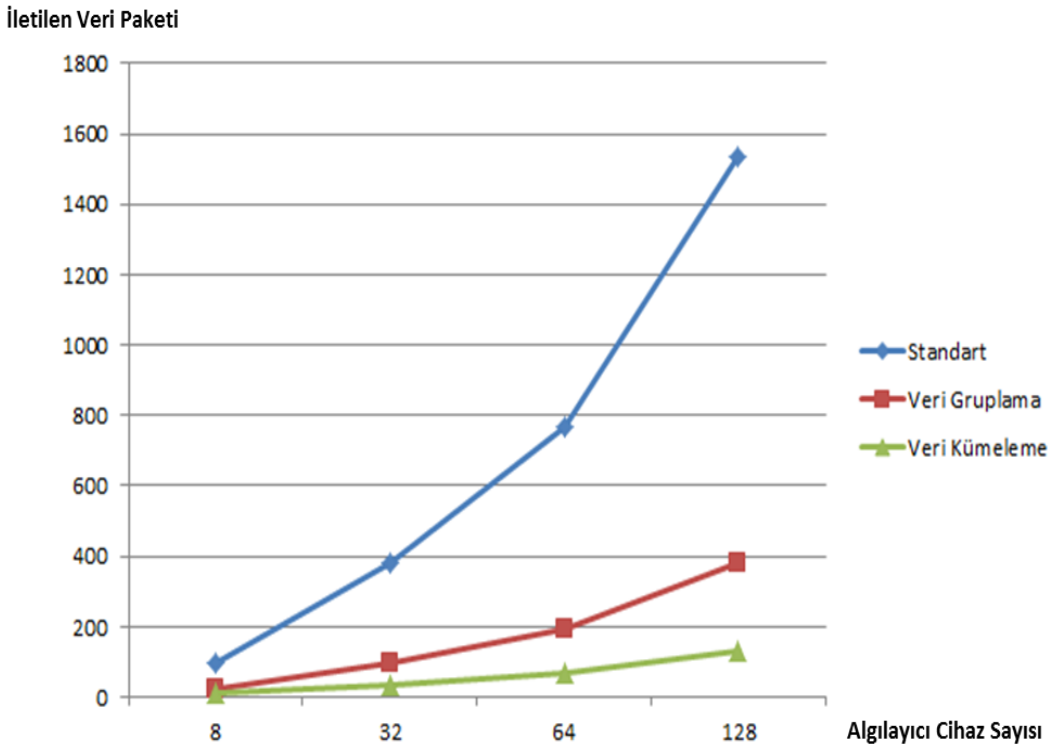
bir prosedür kullanılmayan ağ yapısına göre %92' ye varan bir enerji tasarrufu sağlanabilmektedir. Daha önce belirtildiği üzere günümüzde bu denli basit ağ topolojilerine rastlamak çok mümkün olmamakla birlikte yine de aradaki fark dikkat çekicidir. Aynı şekilde EEiGVK prosedürünün kullanıldığı ağ kurgusunu sadece kümeleme yaklaşımı benimsenin ağ kurgusu ile karşılaştırdığımızda veri transferi için harcanılan enerjinin yaklaşık olarak %65 oranında azaldığı görülmektedir. Veri transferinin algılayıcı cihazlar için ciddi bir enerji tüketimi gerektirdiği çalışmanın ilk bölümlerinde detaylı olarak anlatılmıştır. Veri transferindeki bu ciddi azalma hem her bir algılayıcı cihazın enerjisini şifreleme yaparak güvenliği arttırmak gibi farklı işler için kullanabilmelerine olanak tanıyacak hem de genel olarak ağın ömrünün uzamasını sağlayacaktır.

9.1.1. Sonuçların karşılaştırılması

Bir önceki bölümde oluşturulan matematiksel modeller baz alınarak kablosuz algılayıcı ağlarında hiçbir veri yönlendirme protokolünün kullanılmaması, verilerin gruplanarak iletilmesi ve veri kümeleme yaklaşımının benimsenmesi durumları karşılaştırmalı olarak incelenmiştir. Tüm durumlar için sıçrama sayısının ortalama olarak üç (3), gruplama ve kümeleme yapılan durumlarda ise küme sayısının sabit olarak dört (4) kabul edildiği durumlarda ağ içerisinde iletilen paket sayılarının gösterildiği çizelge ve diyagram aşağıdaki gibidir.

Çizelge 9.1. Ağ yapılarına göre veri iletişimi sayıları

(Cihaz Sayısı)	Standart Ağ	Veri Gruplama	Veri Kümeleme
8	96	24	12
32	384	96	36
64	768	192	68
128	1536	384	132



Şekil 9.5. Ağ yapılarına göre veri iletişimi sayıları

9.2. EEiGVK Prosedürü ile Şifreleme

EEiGVK prosedürü kümeleme yaklaşımı kullanarak veri transferi için harcanan enerjiyi minimuma indirirken bir yandan da şifrelenmiş verilerin deşifre edilmeye ihtiyaç duyulmaksızın kümeleme fonksiyonlarına girebilmelerine olanak tanımaktadır. Çeşitli üstel fonksiyonlar kullanarak şifreleme yapılan standart yaklaşımlarda şifrelenmiş veriler üzerinden aritmetik işlemler yapılamadığından verinin her transfer sonrasında deşifre edilmesi gerekmekte, aksi takdirde kümeleme Yaklaşımları kullanılamamaktadır. Her gelen verinin deşifre edildiği durumlarda ise deşifre etme işlemi için çok fazla enerji harcanması gerekecektir. Bu şekilde benimsenmesi planlanan kümeleme yaklaşımının maliyeti artacak ve bu yaklaşımın kullanımı anlamını yitirecektir. EEiGVK prosedüründe veriler, Eliptik Eğri Şifreleme yaklaşımı kullanılarak şifrelenmektedir. Bu sayede şifrelenmiş veriler kullanılarak aritmetik işlemler yapılabilmekte, dolayısıyla deşifre etme ihtiyacı duyulmaksızın uçtan uca şifreleme yapılabilmektedir. Bu durumda kümeleme

yaklaşımları etkin bir şekilde bir yandan da verinin kaynaktan hedefe gidene kadar şifreli bir şekilde taşınması sağlanarak ağın güvenliği arttırılmış olmaktadır.

Eliptik eğri şifreleme yaklaşımı kümeleme fonksiyonlarının uygulanmasına olanak tanıyarak veri transferi açısından ağın geneline büyük bir katkı sağlarken aynı zamanda şifreleme yaparken daha az kaynak tüketerek işlem bazında da enerji tasarrufu sağlamaktadır. Çalışmanın bu kısmında ECC ile en yakın rakiplerinden birisi olan RSA şifreleme yaklaşımına ait uygulama sonuçları karşılaştırmalı olarak irdelenecektir. Karşılaştırmaların tamamı işlemci zamanı ve frekans cinsinden yapılacaktır.

9.2.1. Başlangıç aşaması

Gerek ECC gerekse RSA şifreleme algoritmaları incelendiğinde her iki algoritmanın da uygulama süreçleri açısından ortak aşamalara sahip oldukları görülmüştür. Algoritmalar baz alınarak geliştirilen şifreleme uygulamaları şifrelemeye başlamadan önce bir başlangıç aşamasından geçmektedir. Başlangıç aşamasında şifreleme esnasında kullanılacak matematiksel denklemler, asal sayılar, matrisler, nokta kümeleri gibi alt bileşenleri oluşturulmakta ve kullanıma hazır hale gelmektedir. Başlangıç adımı her cihaz için tek seferlik bir aşama olmakla birlikte tek bir veri paketinin şifrelenmesine oranla daha maliyetli bir aşamadır.

ECC, RSA3 ve RSA5 uygulamalarının başlangıç aşamasına ait işlem maliyetlerini gösteren tablolar aşağıdaki gibidir;

Çizelge 9.2. ECC uygulamasının başlangıç aşamasına ait işlem maliyetleri

BAŞLANGIÇ AŞAMASI (ECC)	i1	i2	i3	ORTALAMA
Frekans	1555	1623	1648	1609

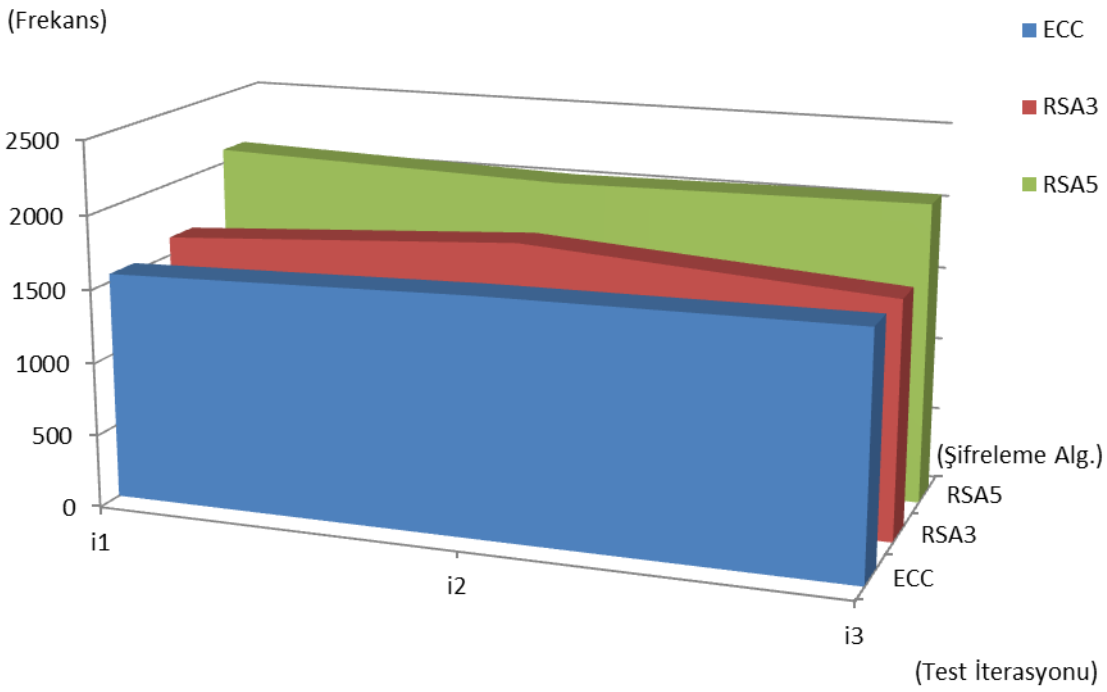
Çizelge 9.3. RSA3 uygulamasının başlangıç aşamasına ait işlem maliyetleri

BAŞLANGIÇ AŞAMASI (RSA3)	i1	i2	i3	ORTALAMA
Frekans	1626	1782	1618	1676

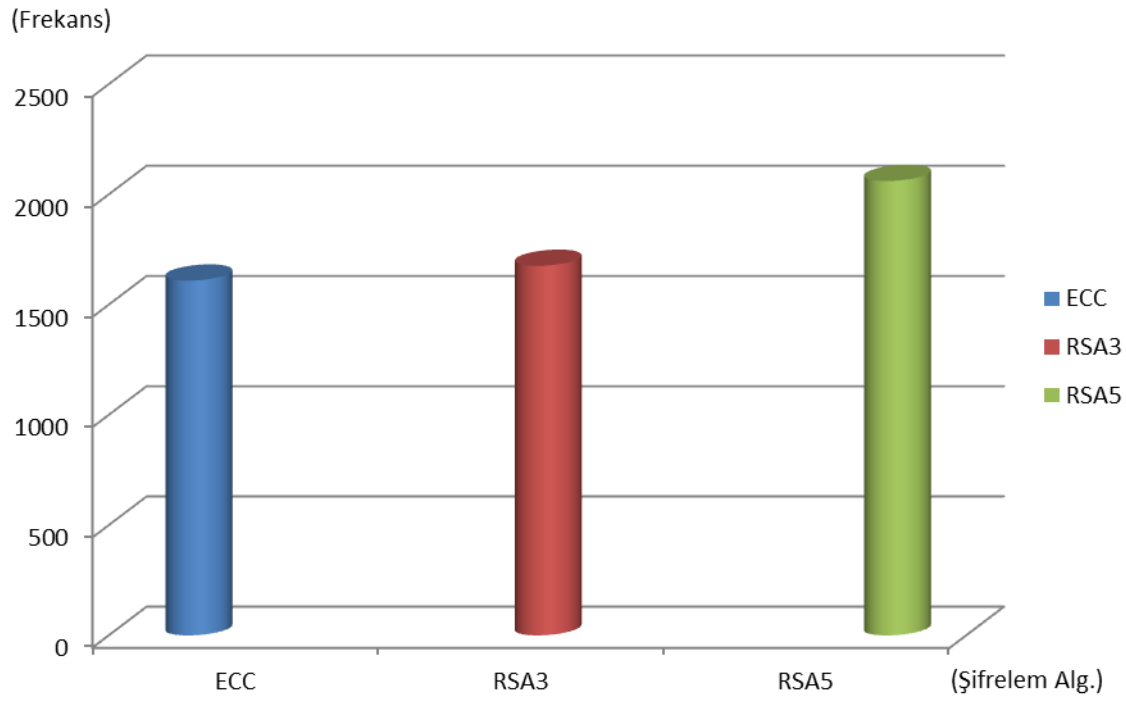
Çizelge 9.4. RSA5 uygulamasının başlangıç aşamasına ait işlem maliyetleri

BAŞLANGIÇ AŞAMASI (RSA5)	i1	i2	i3	ORTALAMA
Frekans	2097	2025	2059	2061

Yapılan incelemelerde işlem maliyetleri açısından genel bir fikir elde edilebilmesi için tüm testler üçer tekrar şeklinde yapılmıştır (i1, i2, i3). Test sonuçlarına bakıldığında işlem zamanı olarak üç şifreleme uygulamasının da çalışma zamanı olarak benzerlik gösterdiği görülmektedir. Fakat daha detaylı bir kriter olarak frekans dikkate alındığında işlem maliyetleri arasındaki farklar daha belirgin olarak görülebilmektedir. Buna göre başlangıç aşamasındaki yapılan işlemlerin kaç işlemci atışında yapıldıklarını incelersek ECC şifreleme uygulaması en az maliyetle şifreleme yapmaya hazır hale gelmektedir. Buna rağmen RSA3 algoritması baz alınarak geliştirilen uygulama ile aralarında çok fazla bir fark olmamakla birlikte RSA5 temelli uygulamanın şifreleme yapmaya hazır hale gelmek için diğer iki uygulamadan daha çok işlem yapması gerekmektedir. Farklar sayısal olarak değerlendirildiğinde ECC algoritması başlangıç aşamasında işlem maliyeti açısından RSA3' e göre %4, RSA5 uygulamasına göre ise %22 avantaj sağlamaktadır.



Şekil 9.6. Şifreme algoritmalarının karşılaştırmalı iteratif başlangıç maliyetleri



Şekil 9.7. Şifreme algoritmalarının karşılaştırmalı ortalama başlangıç maliyetleri

9.2.2. Şifreleme aşaması

Uygulamalar çalıştırıp şifreleme yapmaya hazır hale geldikten sonra hepsi aynı veri paketini şifrelemek için kullanılmıştır. Uygulama bazında işlem maliyetlerini gösteren tablolar aşağıdaki gibidir;

Çizelge 9.5. ECC uygulamasının şifreleme aşamasına ait işlem maliyetleri

ŞİFRELEME (ECC)	i1	i2	i3	ORTALAMA
Frekans	75	82	80	79

Çizelge 9.6. RSA3 uygulamasının şifreleme aşamasına ait işlem maliyetleri

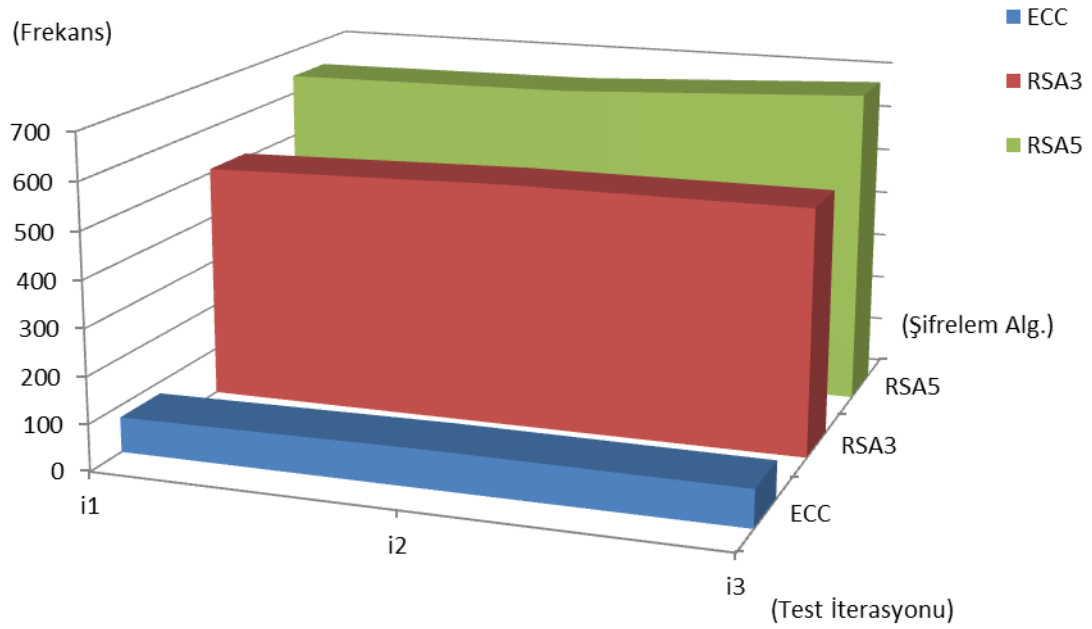
ŞİFRELEME (RSA3)	i1	i2	i3	ORTALAMA
Frekans	509	525	556	530

Çizelge 9.7. RSA5 uygulamasının şifreleme aşamasına ait işlem maliyetleri

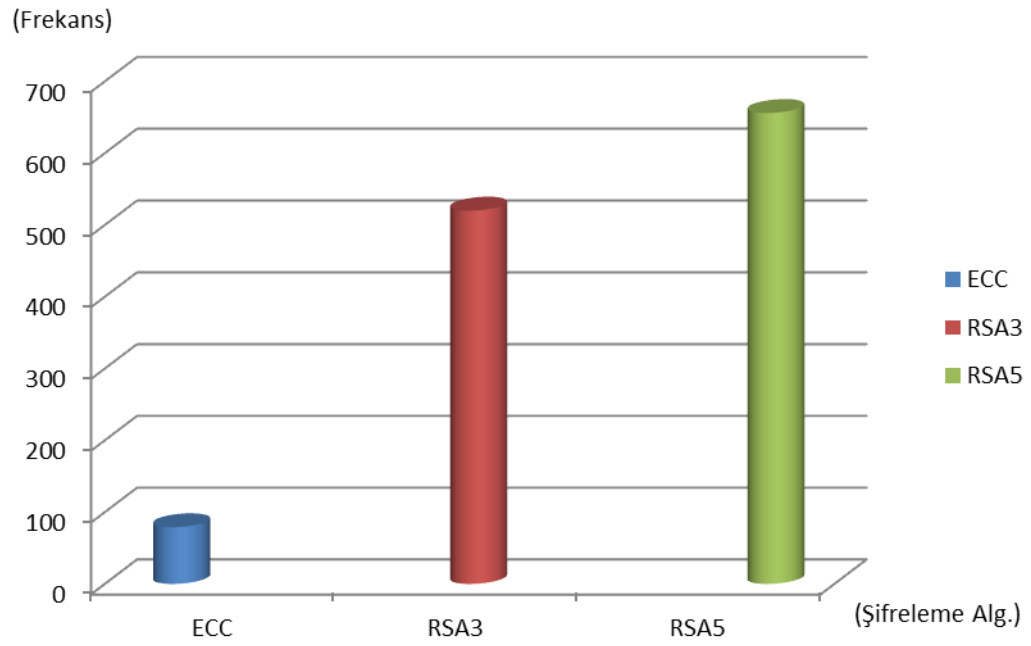
ŞİFRELEME (RSA5)	i1	i2	i3	ORTALAMA
Frekans	641	647	678	656

Şifreleme yapılırken kullanılan kaynaklar ve ortay acıkan işlem maliyetleri incelendiğinde yine işlemci zamanı açısından tüm uygulamaların çok küçük zaman aralıklarında işlemi sonlandırabildiği gözlemlenmiştir. Bir kez daha frekans bazında işlem maliyetleri incelendiğinde ECC temelli uygulamanın diğerlerine oranla kayda değer oranla daha az maliyetle şifreleme işlemini gerçekleştirebildiği görülmüştür. Sayısal değerler üzerinden gidilecek olursa ECC algoritması kullanarak şifreleme yapan uygulama RSA3 kullanan uygulamaya göre %85, RSA5 kullanan uygulamaya göre ise tam %88 oranında tasarruf sağlamaktadır. ECC uygulamasının bu başarısı karmaşık aritmetik işlemleri geometrik yaklaşımlar kullanarak yapabilmesinden kaynaklanmaktadır. Diğer şifreleme uygulamaları reel ve doğal sayılar ile çalışırken ECC şifreleme algoritmasında eliptik eğri üzerinde yer alan noktalar geometrik olarak işleme tabi tutulmaktadırlar. Bu durum şifreleme için gerekli aritmetik

işlemlerin sadeleştirilebilmesine olanak tanımakta ve işlem maliyetlerini kayda değer ölçüde azaltmaktadır.



Şekil 9.8. Şifreme algoritmalarının karşılaştırmalı iteratif şifreleme maliyetleri



Şekil 9.9. Şifreme algoritmalarının karşılaştırmalı ortalama şifreleme maliyetleri

9.2.3. Deşifre etme aşaması

Deşifre etme aşamasında şifrelenmiş şekilde alınan veri paketi çözülerek asıl iletilmek istenilen değer elde edilmektedir. Bu aşama işlem adımları bakımından şifreleme aşamasına benzese de aslında daha karışık ve maliyetlidir. Uygulamalar tarafından aynı değerler şifrelenerek elde edilen şifreli veriler, yine her uygulama kendi oluşturduğu şifreli veriyi çözümleyecek şekilde deşifre etme işlemine tabi tutulmuştur. Uygulama bazında işlem maliyetlerini gösteren tablolar aşağıdaki gibidir;

Çizelge 9.8. ECC uygulamasının deşifre etme aşamasına ait işlem maliyetleri

DEŞİFRE (ECC)	i1	i2	i3	ORTALAMA
Frekans	143	152	156	151

Çizelge 9.9. RSA3 uygulamasının deşifre etme aşamasına ait işlem maliyetleri

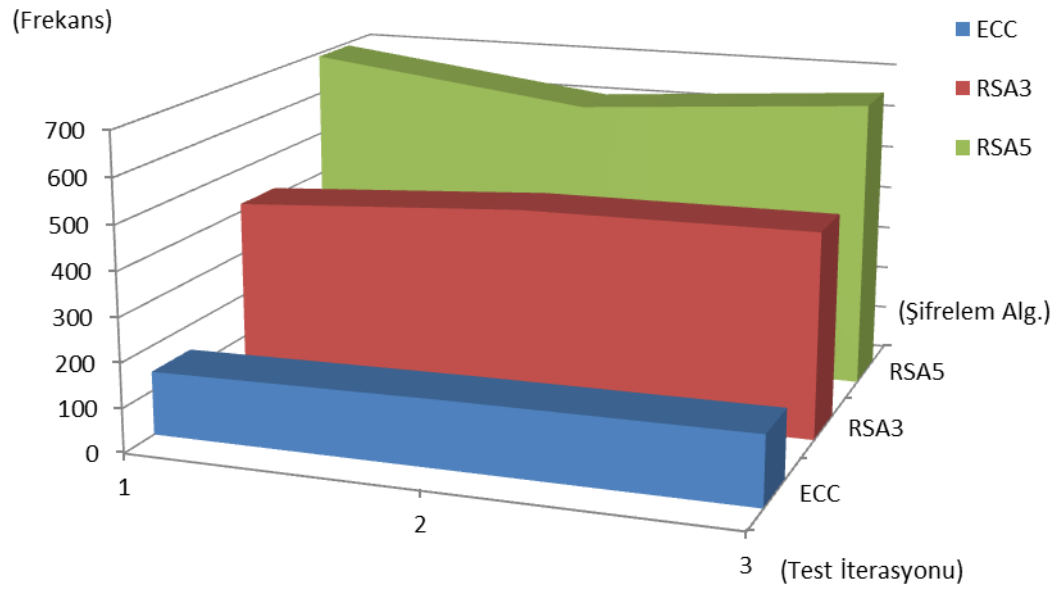
DEŞİFRE (RSA3)	i1	i2	i3	ORTALAMA
Frekans	418	458	463	447

Çizelge 9.10. RSA5 uygulamasının deşifre etme aşamasına ait işlem maliyetleri

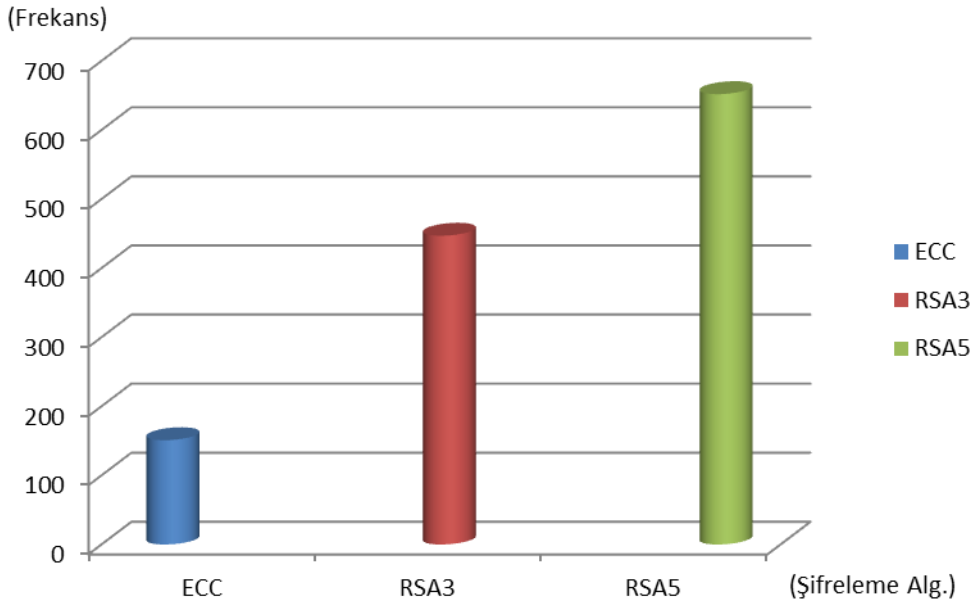
DEŞİFRE (RSA5)	i1	i2	i3	ORTALAMA
Frekans	692	609	655	652

Deşifre aşamasında ECC kullanarak şifreleme yapan uygulamanın işlem maliyeti şifreleme işlemine göre artmış olmakla birlikte yine de hem RSA3 hem de RSA5 ile şifreleme yapan uygulamalara göre işlem maliyetlerinde kayda değer oranda kazanç sağlanmaktadır. Ortalama değerler üzerinden hesaplayacak olursak ECC kullanılarak deşifre etme işlemi yapan uygulama, RSA3 ile deşifre etme işlemi yapana göre %67, RSA5 kullanana göre ise %77 oranında daha az maliyet ile işlemi yapabilmektedir. Ayrıca ECC ile şifreleme yapıldığında kümeleme yaklaşımları da benimsenebilmektedir. Bu sayede oluşturulduğu kaynakta şifrelenen veri paketinin hedefe ulaşana kadar bir daha deşifre edilmesine gerek kalmamaktadır. Böylece

tekrar tekrar yapılan şifreleme-deşifre etme işlemlerinin getireceğim maliyetten kurtulunacaktır. RSA3 ve RSA5 gibi şifreleme algoritmaları ise şifreli veri üzerinde aritmetik işlem yapılabilmesine izin vermediğinden eğer kümeleme yaklaşımları benimsenmek isteniyorsa her sıçramada veri paketlerinin tamamı önce deşifre edilmeli, daha sonra kümeleme fonksiyonu sonunda elde edilen değer tekrar şifrelenerek iletilmelidir.



Şekil 9.10. Şifreme algoritmalarının karşılaştırmalı iteratif deşifre maliyetleri



Şekil 9.11. Şifreme algoritmalarının karşılaştırmalı ortalama deşifre maliyetleri

Şifreleme-deşifre etme işlem çiftinin uygulanma sayısında ciddi oranlarda azalma sağlayacak olan EEiGVK protokolünün getireceği tek ek maliyet kümeleme fonksiyonları olacaktır. Aynı veri paketleri üzerinde toplama işlemi yapan bir kümeleme fonksiyonu çalıştırıldığında elde edilen maliyet değerleri aşağıdaki gibidir;

Çizelge 9.11. ECC ile veri kümeleme işlemine ait maliyet değerleri.

KÜMELEME (ECC)	i1	i2	i3	ORTALAMA
Frekans	4	6	5	5

Yukarıdaki tablodan da kolayca görülebileceği gibi kümeleme işlemi diğer tüm aşamalara göre çok daha az maliyetli bir işlemdir. Kazandırdığı diğer bütün enerji tasarrufları da dikkate alındığı getirdiği bu ek maliyetler kolaylıkla göz ardı edilebilmektedir. Kablosuz algılayıcı ağlara ait bütün kısıtlar ve ihtiyaçlar ele alınarak incelendiğinde EEiGVK prosedürü son derece başarılı bir çözüm olarak ön plana çıkmaktadır.

10. SONUÇ

Yapılan çalışma kapsamında kablosuz algılayıcı cihazlar ve bu cihazların bir araya getirilmesiyle oluşturulan kablosuz algılayıcı ağlara ait teknik ve karakteristik özellikler derinlemesine irdelenmeye çalışılmıştır. Cihazlara ve ağlara ait bahsi geçen özellikler incelendiğinde bu ağ tipine ait belirli geliştirme alanları tespit edilmiştir. Tespit edilen ihtiyaçlar incelendiğinde güvenlik gerekisinmleri ve donanımsal kısıtları bu ihtiyaçlar arasında en kritik olanları olarak göze çarpmaktadır. Bu tez çalışması kapsamında ortaya çıkarılan Eliptik Eğri Şifreleme ile Güvenli Veri Kümeleme Protokolü bu iki kritik soruna karşı bütünleşik bir çözüm önerisi olarak tasarlanmıştır.

EEiGVK protokolü tasarlanırken ağın güvenliğini mümkün olduğunca üst seviyeye taşırken ağın geneline ait enerji tüketimini de mümkün olduğunca minimuma indirmeye çalışmanın yöntemleri aranmıştır. Literatürde yer alan çalışmaların da ışığında ağ genelinde enerji tüketimini optimize edebilmek için veri kümeleme yönteminin uygulanılabilecek en uygun yöntemlerden biri olduğuna karar verilip bu yaklaşım benimsenmiştir. Bu sayede ağ içerisindeki veri iletişimi kayda değer oranda azaltılarak ciddi oranda enerji tasarrufu sağlanabilmiştir. Yine yapılan araştırmalarda geleneksel veri kümeleme yaklaşımları şifreleme algoritmaları ile birlikte kullanılmaya uygun olmadıkları görüşmüştür. Bunun yanı sıra kümeleme yapılmaksızın sadece şifreleme algoritmalarının algılayıcı cihazlarda kullanılmasının bile donanımsal kısıtlardan dolayı başlı başına zorlayıcı bir sorun olduğu görülmüştür. Bu iki soruna çözüm olarak da homomorfizm özelliğine sahip olan Eliptik Eğri Şifreleme algoritması benimsenmiştir. EEŞ düşük işlem maliyetleri ile kablosuz algılayıcı cihazlar üzerinde uygulanmaya çok müsait olmakla birlikte veri kümelme yaklaşımları ile birlikte de uygulanabildiğinden iki soruna birden çözüm olabilecek tümleşik bir çözüm geliştirilebilmesine olanak tanımıştır.

Geliştirilen bu yeni protokol ile algılayıcı ağın güvenliği sağlanırken aynı zamanda ağ içerisindeki enerji tüketimi ciddi oranda azaltılabilecek bu sayede ağın daha uzun süre görevini yerine getirmesi sağlanabilecektir.

KAYNAKLAR

1. Haenselmann, T., "Energy-Efficient Data Acquisition By Adaptive Sampling for Wireless Sensor Networks", ***Proceedings of the 5th International ICST Conference on Communications and Networking in China***, 1-6 (2010).

2. Romer, K., Mattern, F., "The Design Space of Wireless Sensor Networks", ***Wireless Communications, IEEE*** , 11 (6) : 54-61 (2004).

3. İnternet: Universtiy of Berkley, "Smart Dust Project", http://robotics.eecs.berkeley.edu/~pister/SmartDust/ (2010).

4. Culler, D., Estrin, D., Srivastava, M., "Overview of sensor Networks", ***IEEE Computer***, 37 (8) : 41-49 (Ağustos 2004).

5. İnternet: Penn Computing, "Approximate Desktop, Notebook, & Netbook Power Usage", http://www.upenn.edu/computing/provider/docs/hardware/powerusage.html (2010).

6. Simon, J., Martinović, G., "Distant Monitoring and Control for Mobile Robots Using Wireless Sensor Network", ***10th International Symposium of Hungarian Researchers on Computational Intelligence and Informatics***, (14 Ekim 2009).

7. Nutt, G., "A Note on Scaling Wireless Sensor Networks", ***Department of Computer Science Technical Report***, CU-CS-1001-05 (Aralık 2005).

8. Hill, J., Szewczyk R., Woo, A., Hollar, S., Culler, D., Pister, K., "System Architecture Directions for Networked Sensors", ***Department of Electrical Engineering and Computer Sciences University of California, Berkeley, ACM SIGPLAN Notices***, 35 (11) : 93-104 (2000).

9. Nakamura, E. F., Loureiro, A. F., Frery, A. C., "Information fusion for wireless sensor networks: Methods, models, and classifications", ***ACM Computing Surveys***, 39 (3) : Makale 9 (Eylül 2007).

10. Winkler, M., Tuchs, K.-D., Hughes, K., Barclay, G., "Theoretical and practical aspects of military wireless sensor Networks", ***Journal of Telecommunications and information technology***, 2 : 37-45 (2008).

11. Zennaro, M., Pehrson, B., "Wireless Sensor Networks: a great opportunity for researchers in Developing Countries", ***Royal Institute of Technology***, 1-7 (Ağustos 2008).

12. Juang, P., Oki H., Wang, Y., Martonosi, M., Peh L. S., Rubenstein D., "EnergyEfficient Computing for Wildlife Tracking: Design Tradeoffs and Early Experiences with ZebraNet", ***Princeton University***, (Ekim 2002).

13. İnternet: "ARGO - Global Ocean Sensor Network", www.argo.-ucsd.edu (2010).

14. Biagioni, E., Chen, S., A Reliability Layer for Ad-Hoc Wireless Sensor Network Routing", ***System Sciences, 2004. Proceedings of the 37th Annual Hawaii International Conference***, DOI: 10.1109/HICSS.2004.1265705 (2004).

15. İnternet: "PODs Project", http://www2.hawaii.edu/~esb/pods/index.html (2010).

16. Yang, S., "Redwoods go high tech: Researchers use wireless sensors to study California's state tree", ***UCBerkleyNews***, (28 Temmuz 2003).

17. Suri, A., Iyengar, S.S., Cho, E., "Ecoinformatics using wireless sensor networks: An overview", ***Ecological Informatics***, 1 (3) : 287-293 (Kasım 2006).

18. Polastre, J. R., "Design and Implementation of Wireless Sensor Networks for Habitat Monitoring", Yüksek Lisans Tezi, ***University of California at Berkeley***, (2003).

19. Mainwaring, A., Polastre, J., Szewczyk, R., Culler, D., Anderson J., "Wireless Sensor Networks for Habitat Monitoring", ***Intel Corporation***, IRB-TR-02-006 (Haziran 2002).

20. Butler, Z., Corke P., Peterson, R., Rus, D., "Networked Cows: Virtual Fences for Controlling Cows", ***Robotics and Automation, 2004. Proceedings. ICRA '04. 2004 IEEE International Conference***, 5 : 4429-4436 (2004).

21. Ulrich, T., "Wireless Network Monitors H2O: System saves resources, increases yield in Cabernet vineyard", ***Wines & Vines Magazine***, (Temmuz 2008).

22. Mukhopadhyay, S. C., Gaddam A., Gupta G. S., "Wireless Sensors for Home Monitoring - A Review", ***Recent Patents on Electrical Engineering***, 1 (1) : 32-39 (2008).

23. Olivier, L., "Designing a smart home environment using a wireless sensor networking of everyday objects", Yüksel Lisans Tezi, ***Umea University***, (27 Kasım 2008).

24. Malan, D., Jones, T. F., Welsh, M., Moulton, S., "CodeBlue: An Ad Hoc Sensor Network Infrastructure for Emergency Medical Care", ***Harvard Sensor Network Labs***, (14 Temmuz 2008).

25. Kahn, J. M., Katz, R. H., Pister, K. S. J., "Emerging Challenges: Mobile Networking for Smart Dust", ***Journal of Communications and Networks***, 2 (3) : 188–196 (Eylül 2000).

27. Karlof, C., Sastry, N., Wagner, D., "TinySec: A Link Layer Security Architecture for Wireless Sensor Networks", ***Proceedings of the 2nd international conference on Embedded networked sensor systems***, DOI: 10.1145/1031495.1031515 : 162-175 (2004).

28. Marıa Albath, J. G., "Energy Efficıent Clusterıng And Secure Data Aggregatıon In Wıreless Sensor Networks", Doktora Tezi, ***Missouri University of Science And Technology***, (2008).

29. Walters, J. P., Liang, Z., Shi, W., Chaudhary, V., "Wireless Sensor Network Security: A Survey", ***Security in Distributed, Grid, and Pervasive Computing***, Bölüm 17 (2006).

30. Girao, J., Schneider, M., Westhoff, D., "CDA: Concealed Data Aggregation in Wireless Sensor Networks", ***Communications, 2005. ICC 2005. 2005 IEEE International Conference on WSN***, DOI: 10.1109/ICC. 2005.1494953 , 5 : 3044-3049 (2005).

31. İnternet: David, G., "802.15.4 vs ZigBee", http://www.sensor-networks.org/index.php?page=0823123150 (2010).

32. Kaplantzis, S., Mani, N., "Classification Techniques for Network Intrusion Detection", ***Proceedings of the IASTED International Conference on Networks and Communications Systems***, (Mart 2006).

33. Younis, O., Fahmy, S., "Distributed Clustering in Ad-hoc Sensor Networks: A Hybrid, Energy-Efficient Approach", ***INFOCOM 2004. Twenty-third Annual Joint Conference of the IEEE Computer and Communications Societies***, DOI: 10.1109/INFCOM.2004.1354534, Cilt: 1 (2004).

34. Li, J. H., Yu, M., Levy, R., Teittinen, A., "A Mobility-Resistant Efficient Clustering Approach for ad hoc and sensor Networks", ***ACM SIGMOBILE Mobile Computing and Communications Review***, ISSN:1559-1662, 10 (2) : 1-12 (2006).

35. Heinzelman, W., Chandrakasan, A., Balakrishnan, H., "Energy-Efficient Communication Protocols for Wireless Microsensor Networks", ***System Sciences, 2000. Proceedings of the 33rd Annual Hawaii International Conference on WSN***, 2010.

36. Sang, Y., Shen, H., Inoguchi, Y., Tan Y., Xiong, N., "Secure Data Aggregation in Wireless Sensor Networks: A Survey", ***Parallel and Distributed Computing, Applications and Technologies, 2006. PDCAT '06. Seventh International Conference on WSN***, DOI: 10.1109/PDCAT.2006.96 : 315-320 (2006).

37. Akyildiz, I., Su, W., Sankarasubramaniam, Y., Cayirci, E., "A Survey on Sensor Networks", ***IEEE Communications Magazine***, 40 (8) : 102-116 (2002).

38. Söderlund, R., "Energy Efficient Authentication in Wireless Sensor Networks", ***Emerging Technologies and Factory Automation, 2007. ETFA. IEEE Conference on WSN***, 10.1109/EFTA.2007.4416950 : 1412-1416 (2007).

39. Amin, F., Jahangir, A. H., Rasifard, H., "Analysis of Public-Key Cryptography for Wireless Sensor Networks Security", ***World Academy of Science, Engineering and Technology***, 41: 41-91 (2008).

40. Huang, S., Shieh, S., J. D,. Tygar, "Secure encrypted-data aggregation for wireless sensor networks", ***Wireless Networks***, 16(4): 915-927 (2010)

41. Burgess, M., Disney, M., Stadler, R., "Network Patterns in Cfengine and Scalable Data Aggregation", ***21st Large Installation System Administration Conference (LISA' 07)***, (2007).

42. Alzaid, H., Foo, E., Nieto, J. G., "Secure Data Aggregation in Wireless Sensor Network: a survey", ***Australasian Information Security Conference (ACSC2008)***, (2008).

43. Özdemir, S., "Concealed Data Aggregation in Heterogeneous Sensor Networks using Privacy Homomorphism", ***Pervasive Services, IEEE International Conference***, DOI: 10.1109/PERSER.2007.4283909 : 165-168, (2007).

44. Özdemir, S., Xiao, Y., "Secure data aggregation in wireless sensor networks: A comprehensive overview", ***Elsevier, Computer Networks***, 53 : 2022-2037 (2009).

45. Huang S., Shieh S., "SEA: Secure Encrypted-Data Aggregation in Mobile Wireless Sensor Networks", ***Computational Intelligence and Security, International Conference on WSN***, DOI: 10.1109/CIS.2007.207 : 848 – 852 (2007).

46. Mlaih, E., Aly, S. A., "Secure Hop-by-Hop Aggregation of End-to-End Concealed Data in Wireless Sensor Networks", ***INFOCOM Workshops 2008, IEEE*** , DOI: 10.1109/INFOCOM.2008.4544601 : 1-6 (2008).

47. Wang, X., Li, J., "Energy Efficient Secure Data Aggregation Framework in Wireless Networks", ***Personal, Indoor and Mobile Radio Communications, 2009 IEEE 20th International Symposium***, DOI: 10.1109/PIMRC.2009.5449925 : 1-6 (2009).

48. Özdemir, S., "Functional Reputation Based Data Aggregation for Wireless Sensor Networks***", Networking and Communications, 2008. WIMOB '08. IEEE International Conference on Wireless and Mobile Computing***, DOI: 10.1109/WiMob.2008.102 : 592 – 597 (2008).

49. Özdemir, S., Cam, H., Nair, P., Muthuavinashiappan, D., "Energy-efficient secure pattern based data aggregation for wireless sensor networks", *Elsevier, Computer Communications*, DOI: 10.1016/j.comcom.2004.12.029, 29 : 1-10 (2005).

50. Castelluccia, C., Mykletun, E., Tsudik, G., "Efficient aggregation of encrypted data in wirelesssensor networks", ***Mobile and Ubiquitous Systems: Networking and Services, (MobiQuitous 2005) The Second Annual International Conference***, DOI: 10.1109/MOBIQUITOUS.2005.25 : 109-117 (2005).

51. Munivel, E., Ajit, G.M., "Efficient Public Key Infrastructure Implementation in Wireless Sensor Networks", ***Wireless Communication and Sensor Computing (ICWCSC 2010) International Conference***, DOI: 10.1109/ICWCSC .2010.5415904 : 1 – 6 (2010).

52. Wei-hong, W., Yu-bing, L., Tie-ming, C., "The study and application of elliptic curvecryptography library on wireless sensor network", ***Communication Technology (ICCT 2008) 11th IEEE International Conference***, DOI: 10.1109/ICCT.2008.4716252 : 785 – 788 (2008).

53. Hamed, A.I., El-Khamy, S.E., "New Low Complexity Key Exchange and Encryption protocols for Wireless Sensor Networks Clusters based on Elliptic Curve Cryptography", ***Radio Science Conference, 2009 (NRSC 2009)*** : 1-23 (2009).

54. Liu, A., Ning, P., "TinyECC: A Configurable Library for Elliptic Curve Cryptography in Wireless Sensor Networks", ***International Conference on Information Processing in Sensor Networks***, DOI: 10.1109/IPSN.2008.47 : 245-256 (2008).

EKLER

EK-1 Eliptik Eğri Şifreleme uygulaması

```
class Program
{

    //static String equation = "";
    static int a = 0;
    static int b = 0;
    static int p = 0;
    static int nMax = 0;
    static ArrayList ECCPoints;

    static Stopwatch stopwatch = new Stopwatch();

    static Point genetor;
    static Point pointA;
    static Point pointB;
    static Point pointSum;

    static void Main(string[] args)
    {
        testECC();
    }


    static void testECC()
    {


        a = 0;
        b = -4;
        p = 211;


        stopwatch.Start();
        generatePointSet(a, b, p);
        stopwatch.Stop();
        Console.WriteLine("\n\nKümedeki elemen sayısı : " +
        ECCPoints.Count);
        Console.WriteLine("CPU Time : " + stopwatch.ElapsedMilliseconds);
        Console.WriteLine("CPU Tick : " + stopwatch.ElapsedTicks);
        stopwatch.Reset();

        genetor = new Point(2, 2);

        stopwatch.Start();
        nMax = findInfinity(genetor);
        stopwatch.Stop();
        Console.WriteLine("\n\nMaksimum değer : " + nMax);
        Console.WriteLine("CPU Time : " + stopwatch.ElapsedMilliseconds);
        Console.WriteLine("CPU Tick : " + stopwatch.ElapsedTicks);
        stopwatch.Reset();


        //System.Threading.Thread.Sleep(100);


        Console.WriteLine("\n\nA  : " + 32);
```

EK-1 (Devam) Eliptik Eğri Şifreleme uygulaması

```
            stopwatch.Start();
            pointA = pointMultiplication(genetor, 32);
            stopwatch.Stop();
            Console.WriteLine("Şifreli değer : " + pointA.toString());
            Console.WriteLine("CPU Time : " + stopwatch.ElapsedMilliseconds);
            Console.WriteLine("CPU Tick : " + stopwatch.ElapsedTicks);
            stopwatch.Reset();


            Console.WriteLine("\n\nB  : " + 33);
            stopwatch.Start();
            pointB = pointMultiplication(genetor, 33);
            stopwatch.Stop();
            Console.WriteLine("Şifreli değer : " + pointB.toString());
            Console.WriteLine("CPU Time : " + stopwatch.ElapsedMilliseconds);
            Console.WriteLine("CPU Tick : " + stopwatch.ElapsedTicks);
            stopwatch.Reset();

            stopwatch.Start();
            pointSum = addPoints(pointA, pointB);
            stopwatch.Stop();
            Console.WriteLine("\n\nPa + Pb : " + pointSum.toString());
            Console.WriteLine("CPU Time : " + stopwatch.ElapsedMilliseconds);
            Console.WriteLine("CPU Tick : " + stopwatch.ElapsedTicks);
            stopwatch.Reset();


            Console.ReadLine();

        }

        static Point addPoints(Point P, Point Q)
        {
            int Rx;
            int Ry;

            int difX = P.getX() - Q.getX();
            difX = modulo(difX, p);
            int difY = P.getY() - Q.getY();
            difY = modulo(difY, p);

            int s = modularDivision(difY, difX, p);

            Rx = (Convert.ToInt32(Math.Pow(s, 2)) - P.getX() - Q.getX());
            Rx = modulo(Rx, p);
            Ry = (-P.getY() + s * (P.getX() - Rx));
            Ry = modulo(Ry, p);
            Point R = new Point(Rx, Ry);

            return R;
        }

        static Point doublePoint(Point P)
        {
            if (P.getY() != 0)
            {
```

EK-1 (Devam) Eliptik Eğri Şifreleme uygulaması

```
int Rx;
        int Ry;

        int s = modularDivision((3 *
        Convert.ToInt32(Math.Pow(P.getX(), 2)) + a),
                                (2 * P.getY()), p);

        Rx = Convert.ToInt32(Math.Pow(s, 2) - (2 * P.getX()));
        Rx = modulo(Rx, p);
        Ry = -P.getY() + s * (P.getX() - Rx);
        Ry = modulo(Ry, p);

        Point R = new Point(Rx, Ry);

        return R;
    }
    else
        return null;
}

static int modulo(int x, int mod)
{
    x = x % mod;
    if (x < 0)
        x = x + mod;
    return x;
}

static int findModularReverse(int num, int mod)
{
    int reverse = 1;

    while (num * reverse % mod != 1)
        reverse++;

    return reverse;
}

static int modularDivision(int x, int y, int mod)
{
    double xD = (double)x;
    double yD = (double)y;
    int result = 0;

    if ((x / y) == (xD / yD))
        result = (x / y) % mod;
    else
        result = (x * findModularReverse(y, mod)) % mod;


    return result;
}

static int findDiscreteLogarithm(Point P, Point Q)
{
    int k = 2;
```

EK-1 (Devam) Eliptik Eğri Şifreleme uygulaması

```
            Point R;

            R = doublePoint(P);

            while (!(R.getX() == Q.getX() && R.getY() == Q.getY()))
            {
                R = addPoints(R, P);
                k++;
            }

            return k;
        }

        static Point pointMultiplication(Point P, int n)
        {
            Point R = new Point();
            R = doublePoint(P);
            for (int i = 0; i < n - 2; i++)
                R = addPoints(R, P);
            return R;
        }

        static int findInfinity(Point P)
        {
            int inf = 3;
            int Rx;
            int Ry;
            int s;
            Boolean loop = true;
            Point R = doublePoint(P);

            while (loop)
            {
                int difX = P.getX() - R.getX();
                difX = modulo(difX, p);
                int difY = P.getY() - R.getY();
                difY = modulo(difY, p);

                if (difX != 0)
                {
                    s = modularDivision(difY, difX, p);

                    Rx = (Convert.ToInt32(Math.Pow(s, 2)) - P.getX() -
R.getX());
                    Rx = modulo(Rx, p);
                    Ry = (-P.getY() + s * (P.getX() - Rx));
                    Ry = modulo(Ry, p);
                    R.setX(Rx);
                    R.setY(Ry);
                    inf++;
                }
                else
                    loop = false;
            }
            return inf;
        }
```

EK-1 (Devam) Eliptik Eğri Şifreleme uygulaması

```
        static void generatePointSet(int a, int b, int p)
        {
            ECCPoints = new ArrayList();
            double param1, param2, param3, param;

            for (int x = 0; x < p; x++)
            {
                param1 = Math.Pow(x, 3);
                param2 = a * x;
                param3 = b;
                param = param1 + param2 + param3;
                param = param % p;
                findRoot(x, param, p);
            }
        }

        static void findRoot(int x, double check, int mod)
        {
            double y = 0;
            Point ECCPoint;

            while (y < mod)
            {
                if ((y*y) % mod == check)
                {
                    ECCPoint = new Point();
                    ECCPoint.setX(x);
                    ECCPoint.setY(Convert.ToInt32(y));
                    ECCPoints.Add(ECCPoint);
                    y++;
                }
                else
                    y++;
            }
        }
    }
```

ÖZGEÇMİŞ

Kişisel Bilgiler

Soyadı, adı	: ÖZTÜRK, Arda
Uyruğu	: T.C.
Doğum tarihi ve yeri	: 08.01.1987 Ankara
Medeni hali	: Bekar
Telefon	: 0 (312) 352 37 17
Faks	: -
e-mail	: ardaozturrk@hotmail.com.

Eğitim

Derece	Eğitim Birimi	Mezuniyet tarihi
Lisans	Gazi Üniversitesi/ Bilgisayar Mühendisliği	2008
Lise	Milli Piyango Anadolu Lisesi	2004

İş Deneyimi

Yıl	Yer	Görev
2008-2011	Türk Telekom A.Ş.	Mühendis
2011-	Türk Telekom A.Ş.	Mühendis

Yabancı Dil

İngilizce, İspanyolca, Almanca

Hobiler

Tenis, Müzik