Kablosuz Algılayıcı Ağlarında Grup Anahtarı Yönetim Protokollerinin Başarım Değerlendirmesi

M. Denizhan Erdem[1], Orhan Ermiş[1], Can Tunca[1], Sinan Işık[1,2], M. Ufuk Çağlayan[1], Cem Ersoy[1]

[1]Boğaziçi Üniversitesi, Bilgisayar Mühendisliği Bölümü, NETLAB, İstanbul
[2]Boğaziçi Üniversitesi, Matematik Bölümü, İstanbul
mehmet.erdem@boun.edu.tr,
orhan.ermis@boun.edu.tr,
can.tunca@boun.edu.tr,
isiks@boun.edu.tr,
caglayan@boun.edu.tr,
ersoy@boun.edu.tr

Özet: Kablosuz algılayıcı ağları, kısıtlı enerji, hesaplama ve iletişim kabiliyetine sahip cihazlardan oluştuğu için, geleneksel ağlarda kullanılan güvenlik tekniklerinin doğrudan uygulanamayacağı yaygın bir şekilde kabul görmektedir. Teknolojideki son gelişmeler ile birlikte algılayıcı cihazların yetenekleri önemli ölçüde gelişmiştir. Bu çalışmada amacımız, daha güvenilir olsa bile grup anahtarı yönetiminin karmaşıklığının yüksek olması sebebiyle kısıtlı yetenekleri olan algılayıcı cihazlarda uygulanabilir olmadığı hipotezini tekrar değerlendirmektir. Bu sebeple iki temel yöntem olan grup anahtarı ön dağıtımı ve grup anahtarı oluşturma yöntemlerini gerçek algılayıcı cihazlar üzerinde çalıştırarak, enerji harcaması, işlem zamanı ve güvenilirlik ölçütleri açısından değerlendirdik.

Anahtar Sözcükler: Grup anahtarı yönetim protokolleri, ağ güvenliği, gizlilik, kablosuz algılayıcı ağları, grup anahtarı ön-dağıtım protokolleri.

Performance Evaluation of Group Key Management Protocols in Wireless Sensor Networks

Abstract: Since wireless sensor networks are composed of sensor devices with limited energy, computation, and communication capabilities, it has been widely accepted that traditional security techniques used in traditional networks cannot be applied directly. With the recent advances in technology, the capabilities of sensor devices improved significantly. Our aim in this study is to reevaluate the hypothesis that although it is more secure, group-key management is not viable for sensor devices due to high complexity. Hence, we evaluated the performance of two fundamental methods, namely group-key pre-distribution and group-key agreement in terms of energy expenditure, processing time and reliability via execution on real sensor devices.

Keywords: Group-key agreement protocols, network security, privacy, wireless sensor networks, group-key pre-distribution schemes.

1. Giriş

Kablosuz Algılayıcı Ağları (KAA) belirli bir bölgede veri toplamak amacıyla kullanılan çok sayıda algılayıcıdan oluşan ağlardır. Sağlık sistemlerinden, askeri sistemlere kadar geniş kullanım alanları vardır. Her iletişim sisteminde olduğu gibi KAA'larda da grup içerisinde bulunan katılımcıların güvenli bir şekilde haberleşmesi gereken durumlar olabilir. Özellikle aktarılan verinin hassas olduğu askeri ünite takibi gibi uygulamalarda, gerek bilgi gizliliği, gerekse kimlik doğrulaması önem taşımaktadır. Bu durumlarda güvenlik şifreleme algoritmaları ile sağlanır. Şifreleme algoritmalarının katılımcılar arasında güvenli bir şekilde çalışması katılımcıların ortak anahtara sahip olması ile mümkündür. Ortak anahtar belirlenmesini sağlayan sistemlere grup anahtarı yönetim protokolleri denir. Grup anahtarının efektif bir şekilde katılımcılara dağıtılması kriptografide hala üzerinde çalışılan bir problemdir. KAA'lar gibi enerji, iletişim ve hesaplama kısıtları olan ağlarda ise bu problem daha karmaşık hale gelir. Bu çalışmada amacımız, grup anahtarı yönetiminin karmaşıklığının yüksek olması sebebiyle kısıtlı yetenekleri olan algılayıcı cihazlarda uygulanabilir olmadığı hipotezini tekrar değerlendirmektir.

KAA'larda grup anahtarının kullanımı diğer yapılara göre farklılık göstermektedir. Çünkü algılayıcıların hesaplama ve iletişim kabiliyetleri düşüktür. Bu yüzden geleneksel grup anahtarı oluşturma protokolündeki gibi yüksek ek yük gerektiren işlemler algılayıcılarda tercih edilmez. KAA'lar için tercih edilen grup anahtarı oluşturma protokolleri [8, 9, 11, 12]'te verilmiştir. Bu yapılara göre büyük bir anahtar havuzundan (ör: 2^{64}) her algılayıcı için daha küçük anahtar kümeleri seçilir (ör: 2^{20}) ve bu kümeler ağdaki algılayıcılara konumlandırma öncesinde dağıtılır. Sonra, algılayıcılar aktif hale gelince, komşuluklarındaki diğer algılayıcılar ile kendi anahtar kümelerinde bulunan ortak anahtarı bulmaya çalışırlar. Böylelikle, grup anahtarı yönetim protokolündeki yüksek hesap gücü gerektiren işlemler yerini iki algılayıcı arasındaki ortak anahtarı arama yüküne bırakmış olur.

Grup anahtarı ön dağıtım protokolleri, yukarıda verdiğimiz örnek de göz önünde bulundurulduğunda, daha iyi başarıma sahip olsalar da geleneksel yöntemlere göre anahtar dağıtımının güvenliği açısından dezavantajlıdır. Çünkü algılayıcılar üzerindeki anahtar havuzları sıklıkla değiştirilemezler. Bu da herhangi bir algılayıcının ele geçirilmesini ya da iki algılayıcı arasındaki iletişimin gözlemlenebilmesini kolay kılar. Grup anahtarı ön dağıtım protokolleri KAA'larda ilk olarak 2002 yılında Eschenauer ve Gligor tarafından [6] önerilmiştir. Günümüzde algılayıcı teknolojileri geçtiğimiz 12 yıla göre daha fazla gelişmiştir. Bu sebepten dolayı geleneksel grup anahtarı oluşturma protokollerinin KAA'larda uygulanabilirliğinin yeniden değerlendirilmesi gerekmektedir. Bizim bu çalışmadaki en önemli motivasyonumuz, geleneksel yöntemler kullanılarak anahtarların algılayıcılar arasında dağıtılmasıdır.

Bu çalışmada, Burmester ve Desmedt tarafından önerilmiş geleneksel grup anahtarı yönetim protokolü [3] ile [6]'de tanımlanmış grup anahtarı ön dağıtım protokolünün KAA'lardaki uygulanabilirliği gösterilmiş ve önemli sonuçlar elde edilmiştir.

Bildirinin bir sonraki bölümünde, grup anahtarı yönetim protokolleri ile ilgili genel tanımlamalar verilmektedir. Daha sonra ise grup anahtarı yönetim protokollerinin tarihsel gelişimleri ve özelliklerinden bahsedilmiştir. Dördüncü bölümde [3] ve [6]'deki protokollerin KAA'lardaki uygulamaları ve başarım değerlendirmesi sonuçları paylaşılmıştır. Beşinci ve son bölüm ise planlanan gelecek çalışmaları özetlemektedir.

3. Grup Anahtarı Yönetim Protokolleri

Grup anahtarı yönetim protokolleri grup içerisindeki katılımcılara güvenli bir şekilde ortak anahtar dağıtılmasını sağlayan protokollerdir. Bu protokollerin ilki, Diffie ve Helmann [1] tarafından sadece iki katılımcı içeren gruplar için önerilmiştir. Daha sonra bu çalışma, ilk defa iki katılımcıdan fazla katılımcı içeren gruplara uygulanmıştır [2].

Grup anahtarı yönetim protokolleri çeşitli amaçlar ve çeşitli özelliklere göre değişik şekilde sınıflandırılabilir: hata toleransı [5, 10] ve ileri gizlilik [7] bu protokollerin farklı kullanımlarına en iyi örneklerdendir. Bizim bu çalışmada uygulanabilirliğini test ettiğimiz Burmester ve Desmedt'in [3]'te önerdiği protokol ise diğerlerine kıyasla daha farklı bir yapıya sahiptir. Genelde grup anahtarı yönetim protokollerinde her bir katılımcı diğer katılımcıların uzun süreli açık anahtarlarını kullanarak şifreli bir şekilde kendi anahtarını grup içerisinde dağıtır. [3]'teki protokol ise bu işlemi tek seferde diğer protokoller gibi bir şifreleme işlemi yapmadan gerçekleştirir. En son adımda, grup anahtarı hesaplanırken diğer protokollere göre daha farklı bir cebirsel işlem kullanır ve sonuçta grup anahtarı oluşturulur. Bu yüzden iletişim ve hesaplama yükü bakımından en iyi performansı gösteren protokol [3]'te tanımlanan protokoldür. Bizim yapmış olduğumuz testlerde bu protokolü kullanmaktaki amacımız, KAA'lar için enerji ve hesaplama ek yükü açısından daha uygun olduğunu düşünmemizdir.

4. Grup Anahtarı Yönetim Protokollerinin Kablosuz Algılayıcı Ağlarında Başarım Değerlendirmesi

Bu bölümde, grup anahtarı yönetim protokollerinin KAA uygulamalarının başarımını değerlendireceğiz. Bu çalışmada algılayıcı cihazı olarak Arduino Fio mikro denetleyici kartları kullanılmıştır. Bu kartın üstünde kablosuz iletişim sağlamak amacıyla IEEE 802.15.4 tabanlı Xbee modülü bulunmaktadır. Testler, 3 ila 5 adet algılayıcıdan oluşan gruplarla yapılmıştır. Ayrıca Xbee modüllerinden biri de merkezi bir bilgisayara bağlanmış ve bu sayede algılayıcılar arasındaki

Tablo 1. Grup anahtar ön-dağıtım protokolünün başarım değerlendirmesi

Algılayıcı Sayısı	Toplam Çalışma Süresi	Çalışma Sayısı	Hata Sayısı	Doğruluk Yüzdesi
3	18 sa, 26 dk	29834	7	99.98%
4	16 sa, 40 dk	20857	43	99.79%
5	16 sa, 25 dk	20734	14	99.94%

iletişimin gözlemlenmesi ve ölçüm yapılması sağlanmıştır.

Arduino Fio algılayıcılarında çalışan herhangi bir işlemin ne kadar enerji harcadığını tespit etmek için her bir test belli aralıklar ile algılayıcıların pili bitene kadar çalıştırarak yapılmıştır ve pil bitene kadar kaç tekrar yapılabildiği, geçen toplam süre ve protokolün hangi doğruluk yüzdesiyle çalıştığı ölçülmüştür. Testlerde 1000 mAh kapasiteli piller kullanılmıştır.

4.1 Grup Anahtarı Ön-Dağıtım Protokolünün Uygulanması

Anahtar ön-dağıtım protokolü olarak Eschenauer ve Gligor'un protokolünü [8] uyarladık. Bu protokolde öncelikle sistemde kullanılabilecek tüm anahtarları içeren büyük bir anahtar havuzu oluşturulur. Anahtar ön-dağıtımı aşamasında her algılayıcıya bu havuzun bir alt kümesi yüklenir. Ortak anahtar keşif aşamasında her algılayıcı kendi anahtar havuzundaki anahtarların tanıtıcılarını diğer algılayıcılara iletir. Eğer herhangi iki algılayıcı arasında ortak bir anahtar varsa bu anahtar ortak anahtar olarak seçilir.

Testlerde kullanılan büyük anahtar havuzu bin adet anahtar içermektedir. Her bir algılayıcıya yüz adet anahtar yüklenmiştir. Protokolün çalışmasını doğrulamak amacıyla, protokolün her bir tekrarı sonunda her algılayıcı hangi algılayıcılarla bağlantı kurduğunu bilgisayara aktarır ve protokolün başarılı olup olmadığına karar verilir. Grup içindeki tüm algılayıcıların diğer algılayıcılarla doğrudan haberleşebildiği varsayılmıştır. Bu sebeple kurulamamış tek bir bağlantı bile genel başarısızlık olarak kabul edilmiştir.

3 ila 5 algılayıcı için başarım değerlendirmesi sonuçları Tablo 1'de verilmiştir. Algılayıcılar her anahtarı iletmeden önce 5 ms beklemektedir.

3.2 Grup Anahtarı Oluşturma Protokolünün Uygulaması

Grup anahtarı oluşturma protokolü algoritması olarak Burmester ve Desmedt'in önerdiği protokol [3] temel alınmıştır.

Algılayıcılara öncelikle 4 tane değer yüklenmiştir (ilk üç özellik [4] temel alınaraktan):

- **q:** Algoritmanın çalışması için gereken büyük asal sayı
- **p: 2q+1**, aynı zamanda asal olması gerekmektedir
- $\boldsymbol{\alpha}$, öyle ki $G_q = \{i^2 | i \in Z_q^*\}$ alt grubu için üreteç,
- **Kimlik numarası (id):** Algoritmanın çalışması için iletilen değerlerin kime ait olduğunun bilinmesi gerekmektedir

Tablo 2. Grup anahtar oluşturma protokolünün başarım değerlendirmesi

Algılayıcı Sayısı	Toplam Çalışma Süresi	Çalışma Sayısı	Hata Sayısı	Doğruluk Yüzdesi
3	17 sa, 54 dk	126524	498	99,61%
4	16 sa, 39 dk	93730	1864	98,01%
5	16 sa, 13 dk	78096	1723	91,80%

Bu değerleri kullanarak algoritma üç adımda çalışır:

1. Her algılayıcı rastgele $\mathbf{r_i}$ sayısını (mod **q**'da) seçer. Sonra $\boldsymbol{Z_i = \alpha^{r_i}\ (mod\ p)}$ değerini oluşturur ve diğer algılayıcılara iletir.
2. Her algılayıcı, diğer algılayıcıdan gelen $\boldsymbol{Z}$ değerlerini aldıktan sonra şu değeri hesapları ve yayımlar:

$$X_i = \left({Z_{i+1}}/{Z_{i-1}}\right)^{r_i}\ (mod\ p)$$

3. Her algılayıcı bu değerleri elde ettikten sonra ortak anahtar $\boldsymbol{K}$'yı şu denklemi çözerek oluşturur:

$$K_i \equiv (z_{i-1})^{nr_i} * {X_i}^{n-1} * {X_{i+1}}^{n-2} \dots X_{i-2}$$

Bu adımların sonunda her algılayıcıda aynı $\boldsymbol{K}$ anahtarı oluşmuştur ve bu anahtar grup anahtarı olarak kullanılır.

Test amacıyla 32-bit anahtar, $\boldsymbol{P}$ değeri ve 3 ila 5 arası algılayıcı kullanılmıştır. Paket çakışmalarını en aza indirgemek amacıyla her yayımdan önce $\boldsymbol{id}$*50 ms beklenmektedir.

Sonuçlar Tablo 2'de gösterilmiştir. Çalışma sayısı, pil bitene kadar yapılabilen tekrar sayısını ifade etmekle birlikte, protokolün harcadığı enerji ile ters orantılı değişkenlik gösteren bir ölçüttür. Toplam çalışma zamanının çalışma sayısına oranı ise protokolün bir tekrarının çalışma süresi ve dolayısıyla hesaplama karmaşıklığı hakkında fikir vermektedir. Sonuçları grup anahtarı ön-dağıtım protokolü sonuçlarıyla (Tablo 1) kıyaslarsak, grup anahtar oluşturma protokolünün sanılanın aksine hem enerji hem de çalışma süresi ölçütleri açısından fazla ek yük getirmediğini görüyoruz. Fakat, grup anahtar oluşturma protokolünün her bir tekrarının daha kısa sürede çalışmasına rağmen doğruluk yüzdesinin daha az olduğu, bu yüzden başarılı anahtar oluşturma için birden fazla kez çalışması gerekebileceği de göz önünde bulundurulmalıdır.

4. Sonuç ve Öneriler

KAA'lar güvenliğin ve verimliliğin önemli olduğu ağlardır. Bu çalışmada, bu alanda kullanılabilecek iki temel protokolün gerçek ortamda başarım-larını değerlendirdik. Elde ettiğimiz sonuçlar, geleneksel grup anahtar oluşturma protokollerinin, güncel cihazlarda sanıldığından daha yüksek başarımla çalıştığını göstermektedir.

İleride daha fazla algılayıcıyla ve daha büyük anahtarlarla çalışmayı planlıyoruz. Daha büyük anahtarlar

daha fazla işlem gerektireceği için başarım etkilenecektir.

Bu çalışmada yapılan ölçümler hem iletişim hem de hesaplama yüklerini içermektedir. Gelecek çalışmalarda bu iki faktör ayrı ayrı ölçülecek ve daha sağlıklı bir kıyaslama yapılacaktır.

6. Kaynaklar

[1] Diffie, W. ve Hellman, M. E., "New Directions in Cryptography", **IEEE Transactions on Information Theory**, 22: 644-654, (1976).

[2] Ingemarsson, I., Tang, D. and Wong, C.K., "A Conference Key Distribution System", **IEEE Transactions on Information Theory**, 28:714-719 (1982).

[3]Burmester, M. and Desmedt, Y., "A Secure and Efficient Conference Key Distribution System (Extended Abstract)", **Eurocrypt**, Italy, (1994).

[4] Boneh, D., "Decision Diffie-Hellman Problem", **Proceedings of the Third International Symposium on Algorithmic Number Theory**, USA, (1998).

[5] Tzeng, W.-G., "A Secure Fault-Tolerant Conference-Key Agreement Protocol", **IEEE Transactions on Computers**, 51:373-379, (2002).

[6] L. Eschenauer ve V.D. Gligor, "A key management scheme for distributed sensor networks", **CCS**. Washington DC, USA (2002).

[7] Tseng, Y.-M., "An Improved Conference-Key Agreement Protocol with Forward Secrecy", **Informatica, Lith. Acad. Sci.**, 16:275-284 (2005).

[8] Dong, J., Pei, D. ve Wang, X, "A Key Predistribution based on 3-Designs.", **INSCRYPT**, LNCS 4990: 81-92 (2007).

[9] Du, W., Deng, J., Han, Y.S. ve Varshney, P.K., "A Key Predistribution Scheme for Sensor Networks Using Deployment Knowledge" **IEEE Transactions on Dependable and Secure Computing,** 3:62-77 (2006).

[10] Huang, K.-H., Chung, Y.-F., Lee, H.-H., Lai, F. and Chen, T.-S., "A Conference Key Agreement Protocol with Fault Tolerant Capability", **Computer Standards and Interfaces**, **31:**401-405 (2009).

[11] Jolly, G., Kuşçu M.C., Kokate, P. ve Younis, M. "A Low-Energy Key Management Protocol for Wireless Sensor Networks" , Proceedings of the Eight IEEE International Symposium on Computers and Communication (2003).

[12] Rasheed, A. ve Mahapatra, R.N., "The Three-Tier Security Scheme in Wireless Sensor Networks with Mobile Sinks", **IEEE Transactions on Parallel and Distributed Systems**, 23:958-965 (2013).