Grup Anahtarı Oluşturma Protokolleri ve Uygulamaları

Orhan Ermiş[1], Şerif Bahtiyar[2], Emin Anarım[3], M. Ufuk Çağlayan[1]

[1] Boğaziçi Üniversitesi, Bilgisayar Mühendisliği Bölümü, İstanbul
[2] Progress ArGe Merkezi, Provus Bilgi Teknolojileri, İstanbul
[3] Boğaziçi Üniversitesi, Elektrik-Elektronik Mühendisliği Bölümü, İstanbul

orhan.ermis@boun.edu.tr
serifbahtiyar@provus.com.tr
anarim@boun.edu.tr,
caglayan@boun.edu.tr

Özet: İnternetin yaygınlaşması ile birlikte güvenli grup iletişiminin önemi de artmıştır. Grup anahtarı kurma protokolleri güvenli bir şekilde grup anahtarı oluşturulmasını sağlayan kriptografik protokollerdir. Bu protokoller değişik amaçlara ve değişik ağ tiplerine göre dizayn edilmişlerdir. Biz bu çalışmamızda öncelikli olarak grup anahtarı oluşturma protokollerini ve özelliklerini tanımlayacağız. Daha sonra ise uygulama alanları hakkında bilgi vereceğiz.

Anahtar Sözcükler: Grup Anahtarı Oluşturma Protokolleri, ağ güvenliği, gizlilik, hata toleransı, dinamik gruplar, araç ağları, sensor ağları.

Group Key Exchange Protocols

Abstract: The pervasive usage of the Internet has made secure group communications a significant issue. Group-key exchange protocols are cryptographic protocols that provide secure group communications. These protocols have been designed for different networks with different purposes. In this study, we will introduce the group key exchange protocols and their properties. Later, their application area will be presented.

Keywords: Group-key exchange protocols, network security, privacy, fault tolerant, forward secrecy, dynamic groups, vehicular networks, sensor networks.

1. Giriş

İnternetin yaygınlaşması ile birlikte bir çok konuda olduğu gibi grup iletişiminde de güvenliğin önemi artmıştır. Grup iletişimini güvenli bir şekilde sağlayabilmek için çeşitli şifreleme algoritmaları kullanılır. Bu yapıdaki en büyük problem ise kullanılan şifreleme algoritması için anahtarın katılımcılar arasında dağıtılması ya da oluşturulmasıdır. Bu problemin çözümü ise grup anahtarı kurma/oluşturma protokolleridir.

Grup anahtarı oluşturma protokolleri iki ana başlık altında incelenir: Grup Anahtarı Anlaşma (GAA) Protokolleri ve Grup Anahtarı Dağıtma (GAD) Protokolleri.

Grup anahtarı anlaşma protokolleri, daha çok dağıtık sistemlerde kullanılan ve katılımcıların eşit hesaplama gücüne sahip olduğu sistemlerde tercih edilen protokollerdir. Genel olarak, ağın içerisinde bulunan ve kurulacak olan grup oturumuna dahil olacak bütün katılımcıların dahil olması ile anahtarın oluşturulması sağlanır.

Grup anahtarı dağıtma protokolleri ise hiyerarşik yapıya sahip sistemler için tercih edilen bir yöntemdir. Güvenilir bir otorite tarafından anahtarın katılımcılara dağıtılması sağlanır.

Grup anahtarı oluşturma protokolleri [1]'de anlatılan Diffie-Hellman protokolü ile beraber başlamıştır. Bu çalışmada iki katılımcının herhangi bir merkezi otorite olmaksızın nasıl kendi anahtarlarını diğer katılımcıya açıklamadan ortak anahtarda karar kılınabileceği anlatılmıştır ve anahtar oluşturma protokollerinin temeli sayılır. Daha sonra ise [2]'de çoklu katılımcılı ağlara uyarlanmıştır. Bu protokollerin sensor ağlarından konferans ağlarına kadar geniş bir uygulama alanı vardır. Kullanıldığı ağın ve katılımcıların özelliklerine göre değişik çalışma prensiplerine göre tasarlanırlar.

Grup anahtarı anlaşma protokollerinin belli başlı güvenlik özellikleri kimlik doğrulama (authentication), hata toleransı (fault-tolerance) ve ileri gizlilik (forward secrecy) şeklinde sıralanır.

Grup anahtarı anlaşma protokolleri için bir diğer önemli özellik ise grup yapısının dinamik ya da statik olarak tasarlanmasıdır. Dinamik gruplar protokole daha esnek yapı katarken. Statik gruplar ise genellikle katılımcıların değişmediği ağlarda kullanılırlar.

Biz bu çalışmada, grup anahtarı oluşturma protokollerinden, önemli özellikleri ve uygulama alanları hakkında bilgi vereceğiz.

Bildirinin sonraki bölümünde konferans anahtarı oluşturma protokollerinin daha iyi anlaşılması için gerekli tanımlamaları yapacağız. Üçüncü bölümde, protokollerin önemli özellikleri hakkında bilgi verilecektir. Sonraki bölümde ise uygulama alanları ve farklılıkları ile ilgili bilgi verilecektir. Altıncı bölüm ise makalenin sonlandırıldığı bölüm olacaktır.

2. Genel Tanımlamalar

Bu bölümde grup anahtarı anlaşma protokolleri ile ilgili genel tanımları yapacağız. Konferans ağındaki katılımcıların bulunduğu küme: $\mathcal{U}=\{U_1, U_2, \ldots U_n\}$, ile gösterilir ve kümenin eleman sayısı: $|\mathcal{U}| \geq 2$ olmalıdır. Katılımcı listesinin elemanı olan her bir katılımcının bu listeyi bildiği kabul edilir.

Konferans anahtarı oluşturma protokolleri genel olarak açık anahtar şifreleme yöntemini kullanırlar. Açık

anahtar şifreleme yöntemine göre her bir katılımcının açık-özel anahtar çifti bulunur. Örnek olarak: $p = 2q + 1$; p ve q büyük asal sayılar olsun. Her bir U_i katılımcısı için Uzun süreli özel anahtar: $x_i \in Z_q^*$ p. Uzun süreli ortak anahtar: $y_i = g^{x_i} \, mod \, p$ şeklinde ifade edilir.

Protokolün kurallarına harfiyen uyan katılımcılara *iyi niyetli katılımcı* denir. İyi niyetli katılımcıların, konferans anahtarını doğru şekilde hesaplamasını önlemeye çalışan katılımcılara ise *kötü niyetli katılımcı* denir.

3.Konferans Anahtarı Oluşturma Protokolleri ve Özellikleri

Önceden bahsettiğimiz gibi konferans anahtarı anlaşma protokolleri, öncelikli olarak Diffie ve Hellman tarafından iki katılımcı için geliştirilmiştir [1]. Daha sonra ise Ingemarsson, ikiden fazla katılımcı için konferans anahtarı dağıtım protokolü geliştirmiştir [2]. Daha sonra ise aşağıdaki özelliklere göre gelişimini sürdürmüştür:

Kimlik Doğrulama: Bu özellik, katılımcıların oluşturulacak olan gruba dahil olup olmadıklarını kontrol etmek için kullanılır. Kimlik doğrulama ile ilgili de bir çok çalışma olsa da genel olarak, gruba dahil olan katılımcıların, grubun içerisindeki diğer katılımcıları ve onlara ait açık anahtarları bildiği kabul edilir. [4]'te bahsedilen çalışma, grup anahtarı oluşturma protokollerinde kimlik doğrulama özelliğine ilk örneklerdendir.

Hata Toleransı: Eğer grubun içerisindeki bir katılımcı, grup anahtarı oluşturma esnasında, diğer katılımcıların doğru anahtarı hesaplamasını engellemeye çalışırsa bu katılımcının tespit edilip, katılımcı kümesinden çıkartılmasını sağlayan özelliktir. İlk olarak Tzeng tarafından [7]'de anlatılmıştır. Daha sonra da bu özellikten faydalanan bir çok protokol olmuştur. Örnek olarak [8, 9, 10, 12]'deki çalışmalar gösterilebilir.

İleri Gizlilik: Grup anahtarı oluşturma protokolleri genelde açık anahtar şifreleme temelli olduğundan daha önceki bölümde bahsetmiştik. Açık anahtar şifreleme her ne kadar çok güvenli bir şifreleme yöntemi olsa da açık anahtarların uzun süreli kullanımları güvenlik açığı doğurur. Çünkü, belli sayıda kullanımdan sonra anahtarlar, şifreleme algoritmalarının sağladığı rastgele görünümü kaybedebilirler. Bu durumda da eğer bir katılımcının özel anahtarı açığa çıkarsa, o anahtara bağlı olarak oluşturulmuş bütün grup anahtarları açığa çıkabilir.

Bu özellik ilk olarak [9]'da [3]'te bahsedilen yapının grup anahtarı anlaşma protokollerine uyarlanması ile kullanılmaya başlamıştır. Daha sonra da [13] ve [15]'te kullanılmıştır.

Dinamik grup işlemleri: Grup anahtarı protokolleri ilk olarak statik katılımcı gruplarına göre tasarlanmışlardır. Bu yapılar, bir grup anahtarında olması gereken her oturumda yeni anahtar oluşturmasını en iyi şekilde sağlayan yapılardır.

Statik gruplar için protokol tasarlanması her ne kadar avantajlı gözükse de teknolojinin gelişimi ile birlikte dezavantajlı bir hal almıştır. Çünkü ağ oturumunu oluşturan katılımcıların hareketli katılımcılar olma ihtimali ya da ağın kendisinin dinamik bir yapıya sahip olma ihtimali de vardır. Bu varsayıma göre statik grup mantığını kullanıldığında, gruptaki her bir değişim için protokolün yeniden çalıştırılması gerekir. Bu durumda sistemin genel performansı düşecektir. İşte bu yüzden dinamik gruplar tercih edilir. Böylece bütün grup için protokolü çalıştırmadan, sadece bir kaç katılımcının protokolü baştan çalıştırmasıyla yeni anahtar elde edilir.

Protokollerin bu bölümde belirtilen özelliklere göre kıyaslamaları Tablo 1'de verilmiştir.

Protokoller	***Kimlik Doğrulama***	***Hata Toleransı***	***İleri Gizlilik***	***Dinamik Grup İşlemleri***
Burmester ve Desmedt [4]	Var	Yok	Yok	0
Li ve Piepryzk [6]	Var	Var	Yok	0
Tzeng [7]	Var	Var	Yok	0
Tseng [9]	Var	Var	Var	0
Katz ve Yung [5]	Var	Yok	Var	0
Tseng [11]	Var	Var	Var	2
Cheng, ve diğerleri [14]	Var	Var	Var	2
Shi ve diğerleri [8]	Var	Kısmi	Yok	0
Yi [17]	Var	Var	Var	4

Tablo 1: Grup Anahtarı Oluşturma Protokollerinin Özelliklerine Göre Kıyaslamaları

4. Grup Anahtarı Oluşturma Protokollerinin Kullanım Alanları

Grup anahtarı oluşturma protokolleri tele-konferans, video konferans ya da bir grup içerisinde veri paylaşımı yapılması en bilinen uygulama alanlarıdır. Bu bölümde bilinen alanlar haricinde sensor ağları ve araç ağları gibi daha az bilinen sistemlerdeki kullanımlarına değineceğiz.

4.1 Sensor Ağlarında Grup Anahtarı Oluşturma Protokolü Kullanımı

Sensor ağlarındaki grup anahtarının kullanımı diğer yapılara göre farklılık azletmektedir. Çünkü sensorlar düşük kapasiteli enerji kaynaklarına sahiptirler. Bu yüzden açık anahtar şifreleme gibi yüksek hesaplama gücü gerektiren işlemler tercih edilmez.
Sensor ağları için tercih edilen grup anahtarı oluşturma protokolü [17] ve [18]'de verilmiştir. Bu yapılara göre büyük bir anahtar havuzundan (ör: 2^{64}) daha küçük bir anahtar havuzu seçilir (ör: 2^{20}). Bu havuz ağdaki bütün

sensorlara aktif hale getirilmeden önce küçük gruplar halinde dağıtılır. Daha sonra sensorlar aktif hale gelince komşuluklarında bulunan diğer sensorlar ile kendi anahtar havuzlarında bulunan ortak anahtarı bulmaya çalışırlar. Böylelikle, açık anahtar şifrelemenin getireceği hesaplama yükü yerini iki sensor arasındaki ortak anahtarı arama yüküne bırakmış olur.

4.2 Araç Ağlarında Grup Anahtarı Oluşturma Protokolü Kullanımı

Araç ağlarındaki yapı da genel olarak diğer ağlardan farklılıklar içermektedir. En önemli özellik araç ağlarındaki katılımcıların mobil yapıya sahip olmasıdır. Bu yüzden Klasik anahtar oluşturma protokolleri ile tam performansı elde etmemiz çok güçtür.

Araç ağları ile ilgili protokollerin daha detaylı kıyaslaması [16]'da verilmiştir. Bir örnek ile açıklayacak olursak [19]'daki sistemi göz önüne alabiliriz. Burada yol kenarı üniteleri kullanılarak diğer araçlar ile ilgili gerekli bilgiler elde edilir ve bu bilgileri kullanarak Diffie Hellman tabanlı bir protokol ile iki araç arası ortak anahtar oluşturulur.

5. Sonuç ve Öneriler

Grup anahtarı oluşturma protokolleri bir çok ağ için kullanılan ve anahtarın güvenli şekilde oluşturulmasını sağlayan protokollerdir.

Bu çalışmada grup anahtarı dağıtma protokolleri ile ilgili genel tanımlar verilmiştir. Daha sonra ise protokoller özelliklerine göre sınıflandırılmıştır. Ayrıca, sensor ağları ve araç ağları gibi özel durumlardaki kullanımları ile ilgili de bilgi verilmiştir. Protokol özelliklerini kullanılarak simülasyonu ve diğer ağların özelliklerine göre yapılandırılmaları da sonraki adımlarda yapılacak iş olarak tanımlanabilir.

7. 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]Diffie, W., van Oorschot, P. C. and Wiener, M. J., "Authentication and Authenticated Key Exchanges", **Design, Codes and Cryptography**, 2: 107-125 (1992).

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

[5] Katz, J., Yung, M. Scalable protocols for authenticated group key exchange. **Journal of Cryptology**, 20, pp. 85–113. (2007).

[6]Li, C.-H. and Piepryzk, J., "Conference Key Agreement from

Secret Sharing", **ACISP**, Australia, (1999).

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

[8]Shi, T., Guo, Y. ve Ma, J., "A Fault-Tolerant and Secure Multi-Conference-key Agreement Protocol", **International Conference on Communications Circuits and Systems**, China, (2004).

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

[10]Tseng, Y.-M., "A Robust Multi-Party Key Agreement Protocol Resistant to Malicious Participants", **The Computer Journal**, 48:480-487 (2005).

[11] Tseng, Y.-M., "A communication efficient and fault-tolerant conference-key agreement protocol with forward secrecy", **The Journal of Systems and Software**, 80:1091-1101 (2007)

[12] 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).

[13] X. Yi, (2004). "Authenticated key agreement in dynamic peer groups". **Theoretical Computer Science**, 326, pp. 363–382.

[14] Cheng, Z.-Y., Liu, Y., Chang, C.-C., Guo, C., A fault-tolerant group key agreement protocol exploiting dynamic setting. **International Journal of Communication Systems**, 26, (2013).

[15] Ermiş, O., Bahtiyar, Ş., Anarım, E. ve Çağlayan. M.U., "An Improved Fault-Tolerant Conference-Key Agreement Protocol with Forward Secrecy", **SIN 2013**, Aksaray, Türkiye (2013).

[16] Ermiş, O., Bahtiyar, Ş., Anarım, E. ve Çağlayan. M.U., "Open Problems for Group Key Agreement Protocols on Vehicular Ad-hoc Networks", **ICCVE 2013**, Las Vegas, USA (2013).

[17] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A survey on sensor networks", **IEEE Communications Magazine**, vol.40, no.8, pp. 102-114, (2002).

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

[19] B. Zan,, M. Gruteser, and F. Hu, "Key Agreement Algorithms for Vehicular Communication Networks Based on Reciprocity and Diversity Theorems", **IEEE T. Veh. Tech.** 62(8),pp. 4020-4027 (2013).