TAŞINABİLİR ETMENLERLE ÇOK KATILIMCILI SÖZLEŞMELERİN SAYISAL İMZALANMASI

Alper UĞUR Murat AYDOS

Pamukkale Üniversitesi Bilgisayar Mühendisliği Bölümü
Morfoloji Binası Kınıklı Kampüsü, 20017 DENİZLİ
{augur, maydos}@pamukkale.edu.tr

Anahtar sözcükler: sayısal imza, taşınabilir etmenler, sözleşme imza protokolleri
Keywords: digital signature, mobile agents, contract-signing protocols

ÖZET

Bu bildiride, çok katılımcılı sözleşmelerin sayısal ortamda adil ve imtiyazsız olarak imzalanmasının taşınabilir etmenler teknolojisi kullanılarak gerçeklenmesi ile ilgili yapılan çalışma ortaya konulmuştur.

Yapılan uygulamada etmen platformu protokolde tüm veri değişimini gözlemleyen ve yanlış bir durumda devreye girecek olan güvenilir üçüncü taraf görevini üstlenmiş olup hareketli etmenler katılımcıları temsil etmektedirler.

Bu çalışma ile çok katılımcılı sözleşmelerin sayısal ortamda imzalanması üzerine analiz yapılmış, uygulamanın daha verimli ve kriptografik olarak güvenli hale getirilmesi amaçlanmıştır.

1.GİRİŞ

Bir sözleşmeyi, belirli bir metin üzerinde reddedilemez olarak yapılan anlaşma olarak tanımlayabiliriz. Sözleşmelerin reddedilemez olması özellikleri hem taraflar için hem de evrensel olarak geçerliliği ve kabul edilebilirliği bakımından önemlidir. Her türlü ticari işlem çağımızın sunduğu imkânlarla elektronik ortama taşınmış ve bu işlemler için gereken sözleşmelerin de taşınmasını gerekli kılmıştır.

Elektronik ortamdaki sözleşmeler de tıpkı geleneksel, kağıt üzerindeki sözleşmeler gibi eş zamanlılık gerektirir. Bu tip bir sözleşmede, sözleşme tüm katılımcılar tarafından aynı yerde ve aynı anda imzalanır ve bu uygulama, karşılıklı dürüstlük ve adillik özelliklerinin yerine getirilmesini sağlar.

Bundan yola çıkarak sayısal ortamdaki sözleşme imzalanmasına adil değişim probleminin genişletilmiş hali olarak yaklaşabiliriz. Değişimden kasıt sözleşme üzerindeki sayısal imzaların karşılıklı olarak değiş tokuşudur. Sonuç olarak ya tüm katılımcılar, her katılımcı tarafından imzalanmış sözleşmeye sahip olacak ya da hiçbir katılımcı diğerlerinden farklı olarak bir belge elde edemeyecektir.

Herhangi bir katılımcının protokolün herhangi bir noktasında diğerlerine üstünlüğü engellenirse bu tip bir protokolü "imtiyazsız" olarak adlandırabiliriz.[1]

Elektronik ortamda genelde iki taraf arasında yapılan sözleşmelerde sayısal imzalarla resmileştirilen taahhütlerin değişimi için karmaşık bir yapıya ihtiyaç duyulmamaktadır. Fakat katılımcı sayısı n olarak alındığında n>3 katılımcılı bir sözleşme için benzer bir basitlik söz konusu değildir. Bu gibi durumda hiçbir katılımcı ilk imzalayan taraf olmak istememektedir. Bu problemin çözümü için çalışmalar yapılmakta ve birkaç öneri ön plana çıkmaktadır. Bu çalışmalarda temel fikir her bir katılımcının birbirlerine üstünlük sağlamayacak şekilde gizin farklı bir parçasını bilmeleridir. Bunun yanında belirtilen fikrin eksikliklerini gidermek için güvenilir bir üçüncü tarafın protokole dahil edilmesi gündeme gelmiştir. Güvenilir üçüncü tarafın protokoldeki rolü tüm veri alışverişini gözlemleyerek ters giden herhangi bir durumda ya da protokol iptali istendiğinde devreye girerek kurulmuş olan protokolün adilliğini ve imtiyazsızlığını sağlamaktır. Böyle kurulmuş bir protokol üzerinde anlaşılacak sözleşme için tüm katılımcılar için daha güvenilir bir ortam hazırlamış olmaktadır.

2. ÇOK KATILIMCILI SÖZLEŞME PROTOKOLLERİ

Çok katılımcılı sözleşme protokolleri için şimdiye kadar sunulan yapılardan en önemlileri Baum-Waidner ve Garay-MacKenzie protokolleridir. [1,2] Bu protokollerde önerilen şema adillik ve imtiyazsızlık özellikleri uyarınca katılımcıların birbirlerine belirli eşik seviyesine ulaşıncaya kadar güvenilir üçüncü taraf huzurunda sözleşmeyi imzalayacaklarına dair söz vermeleri ve eğer gerekli söz seviyesine ulaşılmışsa protokolün imzalanmasıdır. Bu asıl protokol şeması ile birlikte

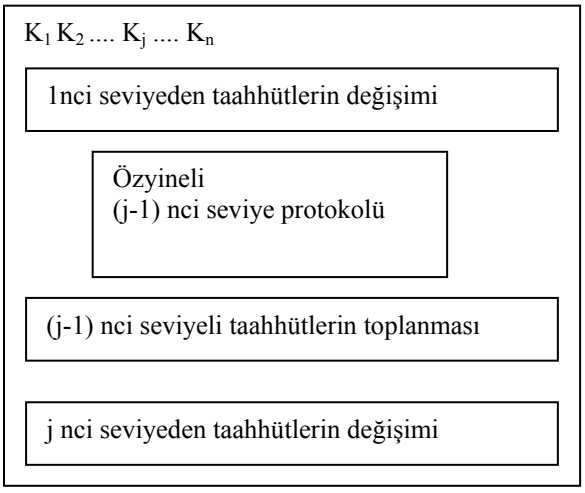
[1] Bu bildiride, literatürde *abuse-free* (suistimalsiz) olarak geçen protokol için ifade edilen durumun karşılığı olarak anlam bakımından *imtiyazsız* kavramının kullanılması uygun bulunmuştur

sözleşme protokolü için kurtarma ve iptal/sonlandırma olarak adlandırılan iki ek protokol de genel şemaya dâhil edilebilir. Katılımcılar tarafından genelde ana protokol kullanılmakta olup diğer ek protokoller katılımcılar bir yanlışlık olduğunu düşündükleri takdirde devreye sokulur. Bir katılımcı bu iki ek protokol ile güvenilir üçüncü tarafa başvurduğunda tekrar ana protokole dönemeyecektir. Bu gibi bir kontrol mekanizması katılımcıların kurulan protokole karşı güvenini artırıcı bir rol üstlenmektedir. [3]
Özyineli olarak kurulan ana protokol n adet katılımcı için n seviyeye bölünür. Her bir seviye farklı yeterlilikteki taahhütleri içerir.

n: katılımcı sayısı
Kj: katılımcı **j**
***j, x*:** farklı yeterlilikteki seviyeler

Durum:
Seviye – *j*
(**Kj** den **K1** e ***j*** seviyeli sözleşme imza taahhütlerinin değişimi)

- **Kj, Kj+1 Kn** aralığındaki tüm katılımcılardan 1nci seviyeden taahhüdü almasıyla başlar.
- **Kj, Kj-1 K1** aralığındaki tüm katılımcılara kendi ***1***nci seviyeden taahhüdünü gönderir.
- ***j-1*** nci seviyenin tamamlanmasını bekler.
- ***j-1*** nci seviye sonunda **K1 Kj-1** aralığındaki tüm katılımcılar ***j-1***nci seviyeli taahhütleri değişmiş olurlar.
- **Kj, K1 Kj-1** aralığındaki tüm katılımcılardan ***j-1***nci seviyeli taahhütleri alır.
- **Kj** den **K1** e ***j*** seviyeli taahhüt değişimi olur. (Bununla birlikte diğer tüm üst seviyeli taahhüt değişimleri de özyineli olarak kapanır.)



Şekil.1. n katılımcılı sözleşme imza protokolü (Seviye- j)

Tüm n seviyeden taahhütler tamamlandığında her katılımcı tüm diğer katılımcılardan **n** seviyede taahhüt almış olur ve sözleşme değişimi başlamaya hazırdır. Bu değişimde her katılımcı diğerlerine **n+1** seviyeli taahhüdüyle birlikte anlaşılan metin üzerinde imzasını gönderir. Değişimin tamamlanması için **Kj** katılımcısı **Kn** ile **Kj+1** arasındaki katılımcılardan **n+1** seviye taahhüdü ve sözleşmeyi bekler. Bunları elde ettiğinde **Kj** kendi imzasını ve **n+1** seviyeli taahhüdü tüm katılımcılara gönderir ve **Kj-1** ile **K1** arasındaki katılımcıların imzalarını ve **n+1** seviyeli taahhüdünü bekler. Bunlar da elde edilince **Kj** sözleşmeyi elde etmiş olur ve protokol **Kj** için sonlanır.
Eğer beklenen iletiler alınmamışsa **Kj** ya **T** (güvenilir üçüncü taraf) ile bağlantı kurabilir ya da protokolden ayrılabilir.
Protokolden çıkış diğer katılımcıların mağdur olmamasını sağlayacak bir biçimde olacaktır. Eğer **Kj** hiçbir taahhüt göndermemişse protokolden kısıtlamasız, doğrudan ayrılabilir. Eğer taahhüt göndermişse **T** ile bağlantı kuracaktır. Bununla birlikte **Kj** eğer hiçbir taahhüt almamışsa çıkış için **T** ile bağlantı kurar. Eğer diğer katılımcılardan bir taahhüt almışsa kurtarma için **T** ile bağlantı kurar.
Kurtarma protokolünde **T** ana protokol sürecinde katılımcılar arasındaki taahhüt geçmişinden elde ettiği bilgileri kullanır. Eğer yeterli seviyede taahhüt elde edilmişse katılımcıların imzalarını kullanarak protokolün tamamlanmasını sağlar.
Güvenilir üçüncü tarafın gözleminde protokol tamamlandığında **T** ya tüm katılımcıların sayısal olarak imzaladığı sözleşmenin değiş tokuşunu sağlar ya da üzerinde anlaşılan sözleşmede imzaları toplayarak kendi sayısal imzasıyla sözleşmeyi imzalar ve dağıtımını yapar.
Protokolde tüm taahhütler ve anlaşılan sözleşme katılımcılar arasında güvenli kanallar varsayılarak gönderilmektedir. İletinin belirli bir sürenin üstünde gecikmesi katılımcıların kurtarma protokolünü başlatması için yeterli olacaktır.

3. ELLİPTİK EĞRİ SAYISAL İMZALAMA ALGORİTMASI

Sayısal imzalama algoritması olarak Elliptik eğri sayısal imzalama algoritması (EESİA) kullanılarak hem taşınabilir etmen tanımlamaları hem de sözleşmenin imzalanmasının ve doğrulanmasının daha hızlı olması sağlanmıştır. Aşağıda özetlenen bu algoritma ile ilgili detaylara [4] den ulaşılabilir.
E: $GF(2^k)$ de tanımlı elliptik eğri
n: derece
P: seçilmiş nokta
ECDSA Anahtar Üretimi:
Taşınabilir etmen A aşağıdaki basamakları uygular:
1.Rasgele bir tamsayı seçer ($d \in [2,n-2]$)
2.Q=dxP yi hesaplar.
3. açık ve gizli anahtarlar sırasıyla (E,P,n,Q) ve d dir.

ECDSA İmza Üretimi:
Taşınabilir etmenin m metnini imzalaması aşağıdaki gibidir.
1.Rasgele bir tamsayı seçer ($k \in [2, n-2]$)
2.kx$P=(x_1,y_1)$ ve $r = x_1 \bmod n$ değerlerini hesaplar.
($x_1 \in GF(2^k)$ve r!=0)
3.$k^{-1} \bmod n$ değerini hesaplar.
4.$s = k^{-1} (H(m)+ d.r) \bmod n$ değerini hesaplar. (H güvenli hash algoritması SHA-256 , s!=0)
5. m metnine ait imza (r,s) ikilisidir.

ECDSA İmza Doğrulanması:
Taşınabilir etmen B nin veya etmen platformu T nin m metni üzerindeki (r,s) imzasını doğrulaması aşağıdaki gibidir.
1.$c=s^{-1} \bmod n$ ve H(m) değerlerini hesaplar.
2.u_1=H(m). C mod n ve $u_2 = r.c \bmod n$ değerlerini hesaplar.
3.u_1x P + u_2 x Q =(x_0,y_0) ve $v = x_0 \bmod n$ değerlerini hesaplar.
4.Eğer v=r ise imza doğrulanmış olur.

Etmen platformu aynı algoritmayı kullanarak taşınabilir etmenler arasındaki taahhütleri imzalayarak bunların geçerliliğini sağlamaktadır.

4.UYGULAMA, TAŞINABİLİR ETMENLER ve GÜVENLİK

Çok katılımcılı sözleşmelerin adil ve imtiyazsız olarak karşılıklı imzalanmasının eşzamanlılığı gerektirdiği açıktır. Bu ise tüm katılımcıların aynı zamanda aynı yerde olma zorunluluğunu gerektirmektedir. Elektronik ortamda bu zorunluluk katılımcıların akıllı etmenler ile temsil edilmesiyle bir yük olmaktan çıkar.
Halihazırda etmen teknolojisinin ağ yönetiminden elektronik ticarete birçok dağıtık sistemde kullanımı söz konusudur. Tipik özellikleri ve sağladığı avantajlar etmenlerin özellikle taşınabilir etmenlerin bahsedilen protokol için kullanılmalarını elverişli kılmıştır.
Çoklu-etmen sistemleri bibirleriyle belirli bir takım görevleri yerine getirmek için çalışan ve iletişim kuran etmenlerce oluşturulan sistemlerdir. Etmenleri çevresi ve diğer etmenler ile iletişim kurabilen ve deneyim kazanıp bunları kullanabilen, çözüm üretebilme, planlama, karar verebilme ve öğrenme yeteneklerine sahip yazılım programları olarak tanımlayabiliriz. [5]
Tekrar kullanılabilirlilik özellikleri üretilen etmenin görev bağımsız çalışabilmesini sağlayacaktır. Ölçeklilik ve hızlılık özellikleri taşınabilir etmenlerin dağıtık sistemlerde hareketlerini kolaylaştırır. Tüm bu avantajlarının yanı sıra taşınabilir etmenlerin sürekli ağ bağlantısı olmayan dağıtık sistemlerde kullanılabilirlikleri tasarlanan uygulama için işlevsellik açısından istenen bir özelliktir.

Etmen platformunun güvenilir üçüncü tarafın rolünü üstlendiği çok katılımcılı sözleşme imza protokolü uygulamasında tüm katılımcılar taahhüt ve imzalama yeteneğine sahip taşınabilir etmenleriyle yer almaktadırlar.
Etmen platformuna dahil olan temsilci taşınabilir etmenler etmen platformunun onayıyla ilk seviyeden protokolün kurulmasına başlamaktadırlar. Etmenler karar verebilme yeteneğine sahip olduklarından protokol kurulumu uyarınca gelmesi gereken herhangi bir iletinin zamanında iletilmemesi durumunda platforma kurtarma ya da ayrılma için başvurabileceklerdir. Bu şekilde kurulacak protokolün işleyişi elektronik ortamda taşınabilir etmenler ile otonom hale gelecektir.
Taşınabilir etmen teknolojisinin kullanıldığı bu, çok katılımcılı sözleşme imzalama protokolünde dikkat edilmesi gereken adillik ve imtiyazsızlık özelliklerinin yanı sıra güvenlik unsuru da önem taşımaktadır. Çünkü sistem güvenliğindeki eksiklikler protokolde diğer özelliklerin sağlanması için kurulan düzeneklerin atlatılmasına yetecektir.
Taşınabilir etmenler söz konusu olduğunda dikkat edilecek dört esas güvenlik durumu göz önünde bulundurmak gerekmektedir.

- Etmenin platforma karşı güvenliği
- Platformun etmene karşı güvenliği
- Etmenlerin diğer etmenlere karşı güvenliği
- Etmenler ve platformdan oluşan sistemin dış varlıklara karşı güvenliği [6]

İlk durum platformun güvenilir üçüncü taraf olarak yer aldığı bu sözleşme protokolü uygulamasında göz ardı edilebilir.
Platformun etmene karşı güvenliği etmenin bir takım veri, kaynak ya da imtiyazı yetkisiz ya da yetkisini kötüye kullanarak elde etmesi engellenerek sağlanmalıdır. Bu ise etmen platform arasındaki kaynak ve veri alışverişinin erişim seviyesinde sınırlandırılmasıyla mümkündür. Zaten uygulamada platform protokol sürecinde gözlemci olarak yer almakta ancak herhangi bir kurtarma ya da ayrılma isteği olduğunda devreye girmektedir. Bu esnada da sadece belirlenmiş iletilerin alışverişi yapılacağından güvenlik açık vermeyecektir. Yapılan haberleşmelerin kriptografik olarak şifrelenmesi ve katılımcı, etmen gibi aktif varlıkların kriptografik olarak kimliklerini doğrulanması ve tanımlanması güvenliği sağlayan mekanizmalardandır.
Yukarıda sayılan durumlardan en önemlisi etmenlerin diğer etmenlere karşı güvenliğidir. Bir etmen diğer etmenin veri alışverişini engellemek ya da işlevini değiştirmek isteyebilir. Eğer etmen platformunda herhangi bir kontrol mekanizması olmazsa diğer etmenlerin yönetilebilir fonksiyonlarına erişerek etmenin kodunu veya elde ettiği verileri değiştirmesi mümkün olabilir. Bir etmen kendi güvenliğini eğer güveniyorsa üzerinde çalıştığı platform ile birlikte çalışarak sağlayabilir.

Etmen platformunun güvenlik gereksinimleri doğrultusunda tasarlanması ve etmenler arası yapılan haberleşmenin kontrollü gerçekleştirilmesi zayıf kodlanmış olabilecek etmenlerin güvenlik açıklarını da önleyecektir.

Etmen platformu ve etmenlerin dış varlıklara karşı güvenlikleri bu çalışmanın kapsamında ele alınmamıştır. Yapının içinde bulunduğu sistemin bütünlüğü ve güvenliği gerek yazılımsal gerekse donanımsal olarak sağlanabilir. Ayrıca taşınabilir etmenlerin değişime uğramaksızın platformlar arasında güvenli hareket etmeleri imzalama ve kapsülleme yöntemleri kullanılarak sağlanabildiği bilinmektedir.

Platform tarafından imzalanan ve platformun kimliğini de içeren taşınabilir etmenler katılımcıya gönderilir ve katılımcılar eve dönen taşınabilir etmenin kimliğini doğrulayarak protokol sonucunda üzerinde anlaşılan sözleşmeyi elde ederler.

Taşınabilir etmen bir kopyasını üçüncü güvenilir taraf rolünü üstlenen etmen platformunda bırakarak yuvasına dönebilir. Bu şekilde platformlar arasında taşınabilir etmenin dış varlıklar tarafından hareketinin engellenmesi şeklindeki bir aktif atak sonucu herhangi bir veri kaybı söz konusu olmayacaktır. Taşınabilir etmen katılımcılara sorunsuz ulaştığında kopya etmen platformu tarafından yok edilir.

4. SONUÇ

Yapılan çalışma ile çok katılımcılı sözleşmelerin sayısal olarak imzalanması taşınabilir etmen teknolojisiyle birleştirilmiş ve otonom hale getirilmiştir. Sistemin güvenliği kimlik doğrulama, şifreleme ve imzalama gibi kriptografik yöntemlerle sağlanmış, yapılan güvenlik analizleri ile sistemin kararlılığı arttırılmıştır. Eğer uygulamanın dış varlıklara karşı güvenliği sistemden bağımsız hale getirilir ve taşınabilir etmenlerin platformlar arası yolculuklarındaki güvenlik seviyesi arttırıldığı takdirde uygulama ticari olarak kullanılabilecektir.

KAYNAKLAR

[1] Juan A. Garay and Philip D. MacKenzie. *Abuse-free multi-party contract signing*. In International Symposium on Distributed Computing, volume 1693 of Lecture Notes in Computer Science, Bratislava, Slavak Republic, 1999. Springer-Verlag.

[2] Birgit Baum-Waidner. *Optimistic Asynchronous Multi-party Contract Signing with Reduced Number of Rounds*. Lecture Notes in Computer Science - 2076

[3] R. Chadha, S. Kremer, and A. Scedrov. *Formal analysis of multi-party contract signing*. In Workshop on Issues in the Theory of Security --- WITS'04, Barcelona, Spain, 2004

[4] D. Johnson and A. Menezes, "*The Elliptic Curve Digital Signature Algorithm (ECDSA*)," Univ. of Waterloo, 1999

[5]Weiss G. (editor), Multiagent Systems: A Modern to Distributed Artificial Intelligence, The MIT Press, 1999

[6] W. Jansen and T. Karygiannis. *Mobile agents and security*. Special Publication 800-19, NIST, 1999