Düzce Üniversitesi Bilim ve Teknoloji Dergisi

Araştırma Makalesi

Kısa Mesafe Kablosuz İletişim ve Açık Anahtarlı Kriptografi ile Doğrulanmış Konum Bildirimi

Ahmet CEZAYİRLİ [*]

[*]*Bilgi-İletişim Teknolojileri Bölümü, Netaş Telekomünikasyon A.Ş., İstanbul, TÜRKİYE*
** Sorumlu yazarın e-posta adresi : cezayirli@netas.com.tr*

ÖZET

Bu makalede, yaşadıkları şehrin ve özellikle yaşadıkları ülkenin dışında başka bir yere giden kişilerin, gerçekten bu yerde olduklarının doğrulanarak istenen kişilere bildirim yapılabilmesi için bir cihaz ve bu cihaza dayalı yöntemler önerilmektedir. Önerilen cihaz, kayıtlı sabit noktalara yerleştirilir ve kişisel mobil aygıtlar ile yalnızca kısa mesafe kablosuz ağda haberleşir. İnsanların, mobil aygıtlarını çoğu zaman, seyahate çıktıklarındaysa hemen her zaman, yanlarında bulundurdukları varsayımıyla, bir mobil aygıtın konumu bilinen sabit bir cihazın yakınında olduğunun doğrulanması, o aygıta sahip kişinin de o kayıtlı konumda olduğu anlamına gelmektedir. Kısa mesafe kablosuz ağ iletişiminde kullanılan verilerin açık anahtarlı kriptografi (AAK) ile şifrelenmesiyle, o yerel ağda bulunulduğu ispatlanabilir hale getirilmekte ve böylece ilgili kişinin belli bir zaman için belli bir konumda olup olmadığının doğrulanması mümkün kılınmaktadır.

Anahtar Kelimeler: *Konum doğrulama, Konum bildirimi, Konum ispatı, Konum paylaşımı*

Notification of Verified Locations using Short-Range Wireless Communication and Public-Key Cryptography

ABSTRACT

In this paper, we propose a device and methods, based on this device, in order to create notifications about verified locations of people to other people in their contact lists, when they arrive in another city, and in particular, in another country other than homeland. The proposed device is stationary at a known and recorded location, and it communicates with personal mobile devices only in short-range wireless network. With the assumption that a personal mobile device is with its owner most of the time, and almost always during a trip, verification that the mobile device is in the vicinity of a stationary device means that its owner is also in that certain location. Using public-key cryptography in encryption of data in the short-range wireless communication, it becomes provable to be in that local network, and hence it is possible to verify, whether a particular person was at a particular location in a particular time.

Keywords: *Location verification, Location notification, Location proof, Location sharing*

Geliş: 28/05/2018, Düzeltme: 29/11/2018, Kabul: 31/12/2018

I. GİRİŞ

Akıllı telefonların oldukça yaygınlaşması, mobil internet kullanımının, sosyal medyanın ve aynı zamanda kişisel mobilitenin de artmasıyla, insanlar normal yaşam alanları dışında başka ülke veya şehirlere gittiklerinde kendi iletişim listelerinde bulunan kişilere yer bildirimi yapma ihtiyacı hissetmektedirler. Facebook, Foursquare, Skype gibi bazı çok yaygın kullanılan uygulamalar, istenildiğinde kullanıcıya dair konum bildirimi yapabilmektedir. Ancak, bu uygulamalardaki konum bilgisi ya kullanıcının kendi beyanına, ya mobil cihazın algıladığı GPS sinyalinin içeriğine, ya da bağlantı yapılan IP adresinin kayıtlı olduğu ülke/şehire göre yapılmaktadır. Cihaz ayarlarının değiştirilmesi ve serbestçe yüklenip kullanılabilen çeşitli uygulamalar sayesinde bu konum belirtme yöntemlerinin üçü de kolayca yanıltılabilmektedir. Şöyle ki, kişi kendi konumunu elle seçiyorsa kasten farklı bir konum seçmiş olabilir. Konum bilgisi cihazın GPS birimi üzerinden alınıyorsa, bu cihazın kullanıcısı cihazın GPS modülünü devre dışı bırakıp farklı bir konumdaymış gibi gerçekçi konum sinyalleri üreten FakeLocation gibi uygulamalar sayesinde kolayca kendisini dünyanın istediği herhangi bir yerindeymiş gibi gösterebilir. Yine, cihazda internet erişimi için VPN kullanarak, tüm internet trafiğini başka bir ülkedeki vekil sunucu (*proxy server*) üzerinden gerçekleştirmek ve IP adresine dayalı konum bilgilendirmesi yapan uygulamaları bu şekilde yanıltmak oldukça kolaydır.

Başka bir yöntem ise, kullanıcıların gittikleri konumlarda çektikleri ve içinde kendilerinin de bulunduğu fotoğraf ve videoları paylaşmaları olarak düşünülebilir. Ancak bu yöntemin konum bildirimi için kullanılmasının da bir takım zorlukları ve doğruluk şüpheleri bulunmaktadır. Fotoğraflar, kolay kullanılabilen bazı uygulamalarca arka planı değiştirilerek uzman olmayan bir çok kişi için inandırıcı olabilecek kalitede farklılaştırılabilmekte, yanlış bir izlenim yaratılabilmektedir. Ayrıca, konum bilgisinin fotoğrafta gözüken arka plandan anlaşılabilmesi için, bu arka planın çok bilinen yerlerden olması gerekmektedir. Örneğin arka planda Eiffel Kulesi'nin gözüktüğü gerçek bir fotoğraf, o kişinin Fransa'da ve Paris'te bulunduğunun kanıtı olsa da, eğer söz konusu kişi Fransa'nın fazla bilinmeyen başka bir yerine gitmiş ise, oradaki arka plan ile çekeceği fotoğraf gerçek olmasına rağmen onu görenlerce kişinin hangi şehirde olduğu anlaşılamayacak, hatta hangi ülkede olduğu bile büyük olasılıkla belirsiz kalacaktır. Aynı durum video çekimleri için de geçerlidir. Üstelik video çekimlerinin, fotoğraflara bakan kişilerin sayısına oranla daha az kişi tarafından izlenmesi de olasıdır.

Diğer taraftan, mobil cihazların GSM baz istasyonlar ile kurdukları bağlantılar da belli bir bölge içinde bulunulduğunun kanıtıdır ve konum doğrulama için kullanılabilir. Nitekim operatörler bunu ücretlendirme seçenekleri için zaten kullanmaktadır, ve ayrıca bazı adli olayların çözümünde de baz istasyon ile mobil cihaz arasında kurulan bağlantının zamanı ve süresi gibi bilgiler aydınlatıcı olmaktadır. Ancak, baz istasyonların kişisel olarak başlatılabilecek bir konum doğrulama işleminde kullanılabilmesi için yazılımlarında değişiklik yapılması ve asıl kullanım amaçları dışında bir kullanım sağlamalarına sıcak bakılması gerekmektedir. Ayrıca, baz istasyonların kapsama alanı oldukça geniş olduğu için (tipik olarak bir kaç km), konumdaki hata payı da çok yüksek olacaktır. Bu çalışmada önerilen yöntemde, yukarıdaki kısıtlar ortadan kaldırılmaktadır. Güvenlik ve doğruluk derecesi çok yüksektir.

Konum doğrulamasına ilişkin literatürdeki çalışmaların önemli bir kısmı böyle bir sosyal ihtiyaçtan ziyade, genellikle cihaz/veri güvenliği ve veri trafiğindeki performans artırımı açısından ele alınmıştır. Kişisel konumun belirlenmesi ve doğrulanması amacıyla kapalı alanlardaki yerel ağları kullanan ilk çalışmalar ise 2000'li yılların başlarında yapılmaya başlanmıştır. Waters ve Felten, 2002'de yayınladıkları bir teknik raporda [1], bir Erişim Noktası'na (EN) konum yöneticisi rolü atayarak, ona

bağlı mobil cihazın iletişim sinyallerinin gidiş-dönüş zamanını ölçen ve bununla orantılı olarak mobil cihazın konumunu belirleyerek bir doğrulayıcı birime konum kanıtı sunabilen bir protokol önermişlerdir. Bu raporu esas alan bir başka çalışmada ise, Sastry, Shankar ve Wagner, çoklu verici kullanmışlar ve her bir vericinin sinyal gidiş-dönüş zamanlarını önceden belirlenmiş bir kesinlikte ölçme koşulu getirmişlerdir [2]. Capkun ve arkadaşları, uzaklık kısıtları ve sinyal zaman bilgilerinin kullanıldığı sensör ağlarında konum bilgisinin güvenli şekilde elde edilmesine yönelik yapılabilecek saldırıları analiz etmişler ve güvenli konum doğrulaması için yaklaşım sunmuşlardır [3]. Microsoft araştırma ekibinden Saroiu ve Wolman, 2009'da yaptıkları bir çalışmada [4], EN üzerinden konum kanıtına yönelik bir protokol önermişler, ancak konum kanıtı yaratılmasının ve doğrulanmasının detaylarını belirtmemişlerdir. Aynı yazarlar, 2010'da yayınladıkları başka bir çalışmada [5] ise, EN üzerinden yapılan konum kanıtı oluşturma işleminin güvenliğini sağlamak için, kullanıcı ve EN arasındaki haberleşmenin çok kısıtlı bir zaman diliminde yapılmasını, bu kısıtlı zaman içinde tamamlanamazsa işlemin reddedilmesini içeren bir çözüm önermişlerdir. Başka bir yaklaşım, Luo ve Hengartner tarafından önerilen VeriPlace isimli bir mimaridir [6], ancak burada konum doğrulaması için üç adet farklı güvenilir üçüncü parti gerekmekte ve pahalı bir çözüm olarak gözükmektedir. 2013 yılında yayınladıkları bir çalışmalarında Wang, Zhu ve Pande aynı konumda bulunan iki veya daha fazla cihazın kullanıldığı STAMP adında bir konum kanıtlama yöntemi önermişlerdir [7]. Bu yöntemde, cihazlardan biri 'kanıtlayıcı' rolünde, diğer(ler)i ise 'tanık' rolünde bulunmakta ve birbirleriyle Bluetooth ya da Wi-Fi üzerinden haberleşmektedir; ancak konum kanıtı sağlamak için gereken süre kullanılan anahtarın büyüklüğü ve kanıtlayıcı ile tanık arasındaki uzaklıkla doğrusal olarak artmaktadır. STAMP'ın bu dezavantajını ve çarpışma saldırılarına karşı gerçek-zamanda etkisizliğini gidermek için, Liu ve arkadaşları 2016 yılında iki yeni yöntem sunmuşlardır [8]. STAMP yöntemindeki modele benzeyen ve kanıtlayıcı ile tanık arasında Bluetooth haberleşmesini esas alan bir başka çözüm de, 2013'te Zhu ve Cao tarafından APPLAUS adı verilerek sunulmuştur [9]. Kötü niyetli partilerin yanlış konum bildirimi için yapabileceği ataklara dayanıklı çözümler geliştirme konusunda, Miettinen ve arkadaşları, mobil cihazın sensörleri ile elde edilebilecek ortam gürültüsü, ışık düzeyi gibi verilerle ikinci kimlik doğrulaması önermişlerdir [10]. Mobil ajanların taşıtlar olduğu durumlar için, Zhang ve arkadaşları Vproof adını verdikleri bir konum doğrulama sistemi önermişlerdir [11]. 2016 yılında yayınlanan bir çalışmada [12], Wi-Fi EN ve Bulanık Kasa yöntemi ile güvenli ve hızlandırılmış bir konum doğrulama sistemi Javali ve arkadaşları tarafından sunulmuştur. Bahsedilen tüm bu yöntemler, esas olarak konum tabanlı servislerin düzgün çalışabilmesi için tasarlanmıştır. Ni ve arkadaşları ise, 2016'da yayınladıkları bir çalışmalarında [13], doğrulanmış konum bildirimi problemini mobil sosyal ağ servisleri açısından ele almış ve belli bir kişinin yakınında bulunan başka kişilerin mobil cihazlarının tanıklığına dayalı bir sistem önermişlerdir.

Bu çalışmada, konum doğrulama ve bildirim problemi tamamen sosyal gereksinimler açısından incelenmiş ve buna uygun yöntemler önerilmiştir. Önerdiğimiz konum doğrulama cihazının işlevsel bakımdan benzerleri, yukarıdaki bazı çalışmalarda 'kanıtlayıcı' ismiyle rol almaktadır. Ancak, bahsedilen çalışmalarda bu cihaz genellikle Wi-Fi EN olarak verilmiştir. Halbuki EN'leri konum doğrulama işlevi için kullanmak, GSM baz istasyonların bu amaçla kullanılmasında olduğu duruma benzer şekilde, EN'ler için özel yazılım gerektirecek ve onlara ek bir yük getirecektir. EN kullanılması, bu cihazlar için bakım sorunu, enerji sorunu gibi pratik uygulama problemlerini de yanında taşımaktadır. Bizim önerdiğimiz konum doğrulama cihazı ise, açık alan uygulamalarına ve pil ile uzun süre çalışmaya elverişli, oldukça düşük maliyetli cihazlardır. Üstelik bu çalışmada önerilen yöntemlerden üçünde, bu cihazın internet bağlantısı olmasına da gerek yoktur. Literatürde karşılaşılan yöntemlerin önemli bir kısmında [7–9, 13], tanık rolü ile görev alan başka kullanıcı mobil cihazlarına da ihtiyaç duyulmaktadır. Bu makalede önerilen yöntemlerde ise, konum doğrulama cihazı dışında herhangi bir tanık cihaza ihtiyaç bulunmamaktadır. AAK'nın kullanımı açısından bakıldığında, yukarıda değinilen çalışmaların çoğunda [3–7, 9, 12, 13]

AAK'nın kullanıldığı görülmektedir. [2] ve [11]'de ise, sistem karmaşıklığını artırmamak ve hızı etkilememek için AAK'dan özellikle kaçınıldığı belirtilmektedir.

Makalenin geri kalan kısmı şöyle düzenlenmiştir: İkinci bölümde, açık anahtarlı kriptografiye aşina olmayan okuyucular için AAK kısaca anlatılmıştır. Üçüncü bölümde, bu çalışmanın esasını oluşturan sistem ve yöntemler detaylı olarak sunulmuştur. Dördüncü bölümde bu yöntemler bir tablo halinde özetlenmiş ve her biri uygulama pratikleri açısından yorumlanmıştır. Beşinci bölümde ise tüm çalışmanın genel değerlendirmesi yer almaktadır.

II. AÇIK ANAHTARLI KRİPTOGRAFİ

Asimetik kriptografi olarak da bilinen açık anahtarlı kriptografi, biri özel (gizli) ve biri de açık olmak üzere bir çift anahtar kullanır. Asimetrik olmasının nedeni, şifreleme için kullanılan anahtar ile çözümleme için kullanılan anahtarın aynı olmamasıdır. Bu iki anahtarın birbiri ile matematiksel bir bağlantısı bulunmaktadır ve bu bağlantı da açıktır, yani bilinmektedir. Ancak bu matematiksel bağın ve açık anahtarın biliniyor olmasına rağmen, özel anahtarın tahmin edilebilmesi için gereken hesaplamanın karmaşıklığı yine de çok yüksektir ve yeterince büyük anahtarlar kullanıldığında algoritmanın kırılması çok çok zordur. A partisine ait açık anahtarı u_A ile, şifrelenecek veriyi X ile, şifreleme fonksiyonunu da f ile gösterirsek, $Y = f_{u_A}(X)$ şifrelenmiş veriyi verir. Bunu çözebilmek için A'nın özel anahtarı r_A gereklidir. Deşifre fonksiyonunu g ile gösterdiğimizde, $X = g_{r_A}(Y)$ işlemi ile orijinal veriye ulaşılabilir. Özel anahtar r_A, yalnızca A tarafından bilindiği için, Y'den X'i hesaplama işi yalnızca A tarafından başarılabilir [14].

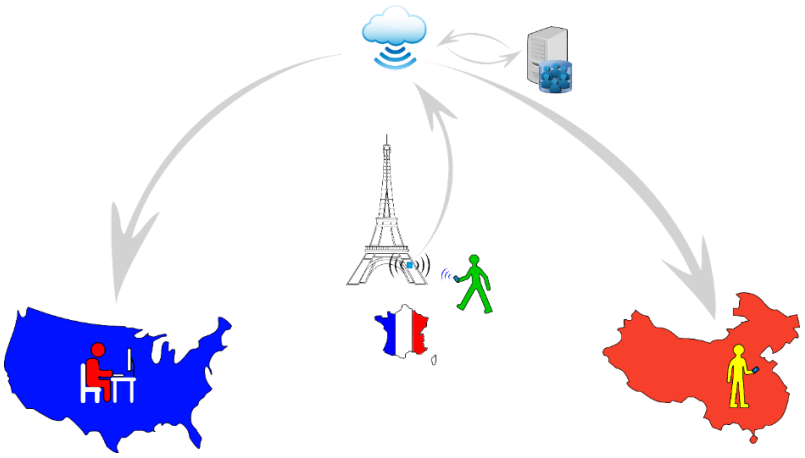
Açık anahtarlı kriptografinin en önemli ve sık başvurulan uygulaması RSA algoritmasıdır. Bu algoritmada, şifrelenecek veri bloklar halinde tamsayılara çevrilir, şifreleme ve deşifre için modüler üs alma fonksiyonu kullanılır ve her iki işlem için de kullanılan fonksiyon aynıdır ($f \equiv g$). Örneğin şifrelenecek verinin bir bloğunu X ile gösterirsek, $Y = X^e \bmod n$ bize RSA ile şifrelenmiş veri bloğunu verir. Bu blok, $X = Y^d \bmod n$ operasyonu ile deşifre edilir. Burada kullanılan e ve d, sırasıyla açık ve özel anahtarların birer parçasıdır. Bu algoritmada açık anahtar $u \stackrel{\text{def}}{=} [e, n]$ ve özel anahtar $r \stackrel{\text{def}}{=} [d, n]$ olarak tanımlanır. Açık anahtarı oluşturan e ve n biliniyor olmasına rağmen, bunları kullanarak d'yi hesaplamak günümüzdeki bilgisayarların işlem hızı ile pratikte imkansızdır. RSA'nın gücü, çok büyük sayıların (1024-bit, 2048-bit, 4096-bit) çarpanlarına ayrılmasının çok zor olmasından kaynaklanmaktadır.

RSA uygulamasında, önce çok büyük iki asal sayı (p ve q) seçilir. Bunların çarpımı ile n bulunur ($n = p \times q$). Daha sonra n için Euler totient fonksiyonu $\phi(n)$ hesaplanır. p ve q asal sayılar olduğu için, $\phi(n) = (p-1)(q-1)$'dir. $(1, \phi(n))$ açık aralığından bir tamsayı olmak üzere $\phi(n)$ ile ortak böleni olmayan bir e sayısı seçilir. Seçilen bu sayıdan, $d \stackrel{\text{def}}{=} e^{-1} \bmod \phi(n)$ olmak üzere d sayısı bulunur. Böylece, açık anahtar $u = [e, n]$, ve özel anahtar $r = [d, n]$ olarak belirlenmiş olur. Şifrelemeye tabi tutulacak veriler bloklar halinde n'den küçük bir tamsayıya dönüştürülür ve örneğin yukarıda belirtildiği gibi bu sayı X ise $Y = X^e \bmod n$ ile şifrelenir. Aynı veri, $X = Y^d \bmod n$ işlemi ile tekrar elde edilebilir. RSA algoritması asimetrik bir algoritmadır fakat açık ve özel anahtarlar birbirine göre simetrik olarak kullanılabilir. Bir başka deyişle, veri u ile şifrelenip r ile çözülebildiği gibi, aynı veri aynı operasyonlarla r ile şifrelenip u ile çözülebilir. u ve r'nin nicel değerlerinin hangisinin açık anahtar hangisinin özel anahtar olacağı konusunda bir önemi yoktur. Bu özellik sayesinde, RSA

algoritmasının iki farklı ve önemli işlev için kullanılması mümkün olmaktadır. Birincisinde, yalnızca tek bir partinin (örneğin A) deşifre edebileceği bir çıktı üretilmek isteniyorsa veri u_A ile şifrelenir. r_A özel anahtarına sahip parti yalnızca A olduğu için, deşifre işlemi yalnızca A tarafından başarılabilir. İkincisinde ise, veri r_A ile şifrelenip ilgili diğer partilere gönderilir. A'nın açık anahtarı u_A bu partilerce bilindiği için, kendilerine ulaşan verinin u_A ile deşifre edildiğinde anlamlı bir sonuç çıkması halinde, bunun A tarafından şifrelenmiş olduğu kanıtlanmış olur. Bu türden kullanım özellikle elektronik imza uygulamalarının esasını oluşturmaktadır [14]. Bu çalışmada önerilen yöntemlerin tümünde, açık anahtarlı kriptografinin bu ikinci tür kullanımına, yani elektronik imzada olduğu gibi göndericinin doğrulanabilmesi özelliğine yer verilmiştir.

III. YÖNTEM

Bu bölümde, doğrulanmış konum bildirimi için beş farklı yöntem detaylı olarak anlatılacaktır. Her yöntem için kullanılan fiziksel araçlar temelde aynı olmasına rağmen, uygulama katmanında farklılıklar mevcuttur. Yöntemlerin tümünde, bir konum doğrulama cihazı, konum doğrulama sunucusu ve kullanıcının mobil cihazı bulunmaktadır. Konum doğrulama cihazı, belli bir konumda sabit olarak bulunan bir elektronik cihaz olup, Bluetooth ya da Wi-Fi gibi bir kısa mesafe kablosuz yerel ağ aracılığıyla, kendisine ulaşan mobil cihazların konum doğrulama işlemini yapmak üzere özel olarak tasarlanmıştır. Konum doğrulama sunucusu, bulut üzerinde bulunan gerçek veya sanal bir sunucudur. Üzerindeki uygulama sayesinde kullanıcı cihazları ve konum doğrulama cihazı ile internet üzerinden haberleşebilir. Kullanıcının mobil cihazında ise, ki bu tipik olarak bir akıllı telefon ya da tablet olacaktır, konum doğrulama işlemini başlatan ve aşağıda tarif edilen yöntemlerle bu işlemin belli aşamalarını gerçekleştiren bir uygulama bulunmaktadır. Tüm durumlarda, her bir konum doğrulama cihazının kimlik bilgisi, açık anahtarı ve cihazın yerleştirilmiş olduğu sabit konum bilgisi, konum doğrulama sunucusu üzerindeki ya da onun erişimine her an açık bir noktadaki veritabanında kayıtlı bulunmaktadır. Dolayısıyla, aşağıda anlatılan yöntemlerde konum doğrulama sunucusunun, konum doğrulama cihazının kimlik bilgisini elde etmesi, aynı zamanda o cihazın bulunduğu konumu da bilmesini sağlar. Kullanıcının mobil cihazı ile konum doğrulama cihazı arasındaki iletişim yalnızca kısa mesafe kablosuz yerel ağ üzerinden yapılabileceği için, konum doğrulama cihazının bilinen konumu, aynı zamanda – gerekli doğrulamaların yapılması halinde – onunla kısa mesafeli yerel ağ üzerinden iletişim kuran mobil cihazın da yaklaşık konumuna eşit olacağı anlamını taşımaktadır. İstenen doğruluk değerine göre kablosuz yerel ağ tasarımı yapılabilir ve konum doğrulama cihazının kablosuz iletişim gücü istenilen şekilde kısıtlanarak konumdaki doğruluk derecesi artırılabilir. Örneğin gerekli minimum yakınlığın 10 metreden küçük olması ya da 250 metreden küçük olması gibi ayarlamalar kolaylıkla yapılabilir.



Şekil 1. *Eiffel kulesini ziyaret eden bir kişinin Amerika ve Çin'deki kontaklarına bildirim yapılmasının gösterimi*

Şekil 1, önerilen yöntemlerden birinin kullanıldığı sembolik bir gösterimdir. Yeşil renk ile gösterilen bir kişi, Eiffel Kulesi ziyaretinin ABD ve Çin'de bulunan arkadaşlarına doğrulanmış olarak bildirilmesini istemektedir. Bunu yapabilmek için, Eiffel Kulesi üzerinde bulunan konum doğrulama cihazına, kendi mobil cihazının Bluetooth veya Wi-Fi haberleşmesi ile bağlanarak doğrulama işlemini kendi inisiyatifi ile başlatır. Bulut üzerinde ayrıca bir konum doğrulama sunucusu da bulunmaktadır. Şekil 1'deki gösterime göre, bulut üzerindeki sunucuya erişim konum doğrulama cihazı tarafından yapılır. Bu sayede, Eiffel Kulesi'ni ziyaret eden kullanıcının mobil cihazında internet erişiminin açık olmasına gerek kalmamaktadır; ancak aşağıda anlatılacağı gibi, internet erişiminin kullanıcı tarafından sağlanması durumunda, bu sefer de konum doğrulama cihazında internet erişimi bulunmasına gerek duyulmaması gibi bir avantaj doğmaktadır. Bu çalışmada önerilen tüm yöntemlerde, Şekil 1'de gösterilen yapıtaşları aynı kalmakta, yalnızca haberleşmenin bir bölümünün yöntemi, tarafları ve aktarılan veriler değişmektedir.

Yöntem adımlarını anlatırken Tablo 1'deki tanımlamaları kullanacağız:

Tablo 1. *Yöntem adımlarını anlatırken kullanılan tanımlamalar*

k_{ID}	: *kullanıcının eşsiz ID'si (unique ID)*
d_{ID}	: *konum doğrulama cihazının eşsiz ID'si*
r_k	: *kullanıcının özel anahtarı (private key)*
u_k	: *kullanıcının açık anahtarı (public key)*
r_d	: *konum doğrulama cihazının özel anahtarı*
u_d	: *konum doğrulama cihazının açık anahtarı*
$f_r(.)$	: r *anahtarının uygulandığı şifreleme fonksiyonu*
$g_u(.)$	: u *anahtarının uygulandığı çözme (deşifre) fonksiyonu*
x	: *konum doğrulama cihazının kayıtlı konumu*

Ayrıca, $\bar{k}_{ID} = g_{u_k}\left(f_{r_k}(k_{ID})\right)$ ve $\bar{d}_{ID} = g_{u_d}\left(f_{r_d}(d_{ID})\right)$ olarak birer $\bar{k}_{ID}$ ve $\bar{d}_{ID}$ tanımlayalım. Bu tanımlamalara göre, doğru anahtarlar ile şifreleme ve çözme yapılması halinde $\bar{k}_{ID} = k_{ID}$ ve $\bar{d}_{ID} = d_{ID}$ olduğu açıktır, ancak bu makalenin geri kalan kısımlarındaki notasyonu hafifletmek ve anlatımı kolaylaştırmak için bu tanımlamalara ihtiyaç duyulmuştur. Yine bu sebeple, gerçek bir uygulamada

mesaj paketlerinde bulunması gereken başlık kısımları (*header*) ve açık anahtarlı kriptografi için gerekebilecek doldurma (*padding*) baytları gibi kısımlara yer verilmemiştir.

A. YÖNTEM I

Önerilen ilk yöntemde kullanıcı, mobil cihazında koşan uygulama aracılığıyla, kullanıcı ID'sini (k_{ID}) hem açık olarak, hem de kendi özel anahtarı r_k ile şifreleyerek bir paket hazırlar ve bunu kapsama alanında bulunduğu kısa mesafe kablosuz ağ içindeki konum doğrulama cihazına gönderir. Gönderilen paketi şöyle gösterelim:

k_{ID}	$f_{r_k}(k_{ID})$

Konum doğrulama cihazı, gelen bu verileri, kendi ID'sinini (d_{ID}) ve o andaki zaman bilgisini (t), özel anahtarı r_d ile şifreler. Ayrıca, d_{ID}'nin açık olarak da bulunduğu şu paketi oluşturur ve konum doğrulama sunucusuna gönderir:

d_{ID}	$f_{r_d}(d_{ID})$	$f_{r_d}(t)$	$f_{r_d}(k_{ID})$	$f_{r_d}\left(f_{r_k}(k_{ID})\right)$

Konum doğrulama sunucusunda çalışan uygulama, kendisine gelen bu pakette açık olarak bulunan d_{ID}'yi okuyarak, o kimlik numarasına ilişkin konum doğrulama cihazının açık anahtarını (u_d) veritabanından okur. Daha sonra, paketteki $f_{r_d}(d_{ID})$, $f_{r_d}(t)$, $f_{r_d}(k_{ID})$ ve $f_{r_d}\left(f_{r_k}(k_{ID})\right)$ kısımlarını u_d ile deşifre eder. Deşifre ettiği kısımdan elde edilen $\bar{d}_{ID}$ ile açık kısımdan doğrudan okuduğu d_{ID} değerlerini birbirine eşit ise bu paketin gerçekten kayıtlı bir konum doğrulama cihazından geldiği anlaşılmış olur. Akabinde, $g_{u_d}\left(f_{r_d}(k_{ID})\right)$ işlemi ile k_{ID}'yi elde ederek ona ait açık anahtarı (u_k) veri tabanından okur. Paketin $f_{r_d}\left(f_{r_k}(k_{ID})\right)$ kısmından $f_{r_k}(k_{ID})$'yi elde ederek, bu değeri u_k ile çözüp $\bar{k}_{ID}$'yi bulur. Eğer $\bar{k}_{ID} = k_{ID}$ ise, o kullanıcının kimliği doğrulanmış olur ve o kimliğe ilişkin kişilerin bulunduğu rehber veritabanından okunarak, k_{ID} kimlikli kullanıcının doğrulanmış konum bilgisi (x), paket içinden elde edilen zaman bilgisi (t) ile birlikte sunucu tarafından o kişinin kayıtlı rehberindeki tüm diğer kişilere uygun şekilde iletilir. Bu iletim, örneğin basit bir SMS mesajı ile olabileceği gibi, özel bir uygulamada gözüken konum güncellemesi veya daha sofistike bir bildirim şeklinde de olabilir.

B. YÖNTEM II

Bu yöntemde kullanıcı, kapsama alanında bulunduğu konum doğrulama cihazına kendi ID'sini açık olarak göndererek doğrulama işlemini başlatır:

k_{ID}

Konum doğrulama cihazı, k_{ID}'yi ve o anki zaman değerini (t) r_d ile şifreleyip, d_{ID}'nin açık hali ile birlikte aşağıdaki paketi oluşturur ve bunu kullanıcının mobil cihazına yanıt olarak gönderir:

d_{ID}	$f_{r_d}(d_{ID})$	$f_{r_d}(t)$	$f_{r_d}(k_{ID})$

Konum doğrulama cihazı, bu paketin aynı zamanda konum doğrulama sunucusuna da gönderir. Sunucu, paketin içinde okuduğu d_{ID} ile veritabanından ona ilişkin u_d değerini okuyarak paketin şifreli kısımlarını deşifre eder. Eğer $\bar{d}_{ID} = d_{ID}$ ise, deşifre sonucu elde ettiği k_{ID}'ye ilişkin mobil hat numarasını veritabanından okur. Bu numaraya SMS mesajı ile bir doğrulama kodu gönderir. Kullanıcı cihazındaki mobil uygulama, sunucudan gelen bu SMS mesajındaki doğrulama kodunu sunucuya geri gönderir. Böylece sunucu SMS ile doğrulama sağlamış olur ve o kullanıcıya ait kişi rehberini veritabanından alarak rehberdeki kişilerin cihazlarına doğrulanmış konum (x) ve zaman (t) bildirimi gönderir.

C. YÖNTEM III

Kullanıcı, kapsama alanında bulunduğu konum doğrulama cihazına kendi ID'sini açık olarak göndererek doğrulama işlemini başlatır:

k_{ID}

Kullanıcı, aynı paketi konum doğrulama sunucusuna da gönderir. Konum doğrulama cihazı, k_{ID}'yi ve o anki zaman değerini (t) r_d ile şifreleyip, d_{ID}'nin açık hali ile birlikte aşağıdaki paketi oluşturur ve kısa mesafe kablosuz ağ üzerinden mobil cihaza yanıt olarak gönderir:

d_{ID}	$f_{r_d}(d_{ID})$	$f_{r_d}(t)$	$f_{r_d}(k_{ID})$

Konum doğrulama sunucusu, kendisine ulaşan k_{ID}'ye ait mobil hat numarasına SMS mesajı ile bir doğrulama kodu gönderir. Mobil cihazda çalışan uygulama, SMS mesajı ile gelen doğrulama kodu ile birlikte, konum doğrulama cihazından gelen yukarıdaki paketi sunucuya gönderir:

SMS_kod	d_{ID}	$f_{r_d}(d_{ID})$	$f_{r_d}(t)$	$f_{r_d}(k_{ID})$

Konum doğrulama sunucusu, SMS kodunun doğru olması halinde, paket içindeki d_{ID} ile veritabanından ona ilişkin u_d değerini okur ve paketin geri kalan kısmını bununla çözer. Eğer $\bar{d}_{ID} = d_{ID}$ ise, kullanıcıya ait kişi rehberini veritabanından alarak o kişilere kullanıcının doğrulanmış konum (x) ve zaman (t) bildirimini yapar.

D. YÖNTEM IV

Kullanıcı, kapsama alanında bulunduğu konum doğrulama cihazına kendi ID'sini açık olarak göndererek doğrulama işlemini başlatır:

k_{ID}

Konum doğrulama cihazı, k_{ID}'yi ve o anki zaman değerini (t) r_d ile şifreleyip, d_{ID}'nin açık hali ile birlikte aşağıdaki paketi oluşturur ve bunu kullanıcının mobil cihazına kısa mesafeli kablosuz yerel ağ üzerinden gönderir:

d_{ID}	$f_{r_d}(d_{ID})$	$f_{r_d}(t)$	$f_{r_d}(k_{ID})$

Mobil cihazda koşan uygulama, gelen bu pakete kendi kimlik bilgisini de özel anahtarıyla şifreleyip ekleyerek aşağıdaki paketi oluşturur ve bunu konum doğrulama sunucusuna gönderir:

$f_{r_k}(k_{ID})$	d_{ID}	$f_{r_d}(d_{ID})$	$f_{r_d}(t)$	$f_{r_d}(k_{ID})$

Konum doğrulama sunucusu, bu paket içindeki d_{ID} ile veritabanından ona ilişkin u_d anahtarını alır. Önce, $g_{u_d}\left(f_{r_d}(d_{ID})\right)$ işlemi ile $\bar{d}_{ID}$'yi elde eder. Eğer $\bar{d}_{ID} = d_{ID}$ sağlanıyorsa, $g_{u_d}\left(f_{r_d}(k_{ID})\right)$ işlemi ile k_{ID}'yi elde ederek u_k anahtarını veritabanından okur. $g_{u_k}\left(f_{r_k}(k_{ID})\right)$ işlemi ile $\bar{k}_{ID}$'yi bulur. Eğer $\bar{k}_{ID} = k_{ID}$ ise, hem konum doğrulama cihazı, hem de kullanıcı kimliği doğrulanmış demektir. Daha sonra d_{ID} kimlikli konum doğrulama cihazının konum bilgisini (x) ve k_{ID} kimlikli kullanıcının kişi rehberini okuyarak rehberdeki kişilerin cihazlarına doğrulanmış konum (x) ve zaman (t) bildirimi gönderir.

E. YÖNTEM V

Kullanıcı, kapsama alanında bulunduğu konum doğrulama cihazına kendi ID'sini açık olarak göndererek doğrulama işlemini başlatır:

kID

Konum doğrulama cihazı, k_{ID}'yi ve o anki zaman değerini (t) r_d ile şifreleyip, d_{ID}'nin açık hali ile birlikte aşağıdaki paketi oluşturur ve bunu kullanıcının mobil cihazına gönderir:

d_{ID}	$f_{r_d}(d_{ID})$	$f_{r_d}(t)$	$f_{r_d}(k_{ID})$

Mobil cihazda koşan uygulama, bu paketi kişi rehberindeki kişilerin cihazlarına internet üzerinden dağıtır. Rehberde kayıtlı cihazlara bu mesaj ulaştığında, her biri, gelen paketi konum doğrulama sunucusuna gönderir. Sunucu, d_{ID} değerini okuyarak veritabanından ona ilişkin u_d anahtarını alır ve yukarıdaki yöntemlerde olduğu gibi $\bar{d}_{ID}$'yi elde eder. Eğer $\bar{d}_{ID} = d_{ID}$ eşitliği sağlanıyorsa, t ve k_{ID}'yi çözerek, d_{ID} kimlikli cihazın konum bilgisi (x) ile birlikte, bildirim yapılacak cihazlara yanıt olarak gönderir. Bu verileri alan mobil uygulama, sunucudan gelen mesajdaki k_{ID} değerini, yukarıdaki mesajı internet üzerinden kendisine doğrudan gönderen kullanıcıya ait rehberinde kayıtlı bulunan kimlik ile karşılaştırır. İkisi aynı ise, doğrulanmış konum (x) ve zaman (t) bildirimini kendi kullanıcısına yapar. Bu yöntemde, bildirim yapmak isteyen kişi ile bildirim yapılan kişinin karşılıklı olarak birbirlerinin rehberlerinde kayıtlı olması, ayrıca k_{ID}'nin de bu rehberlerde kişilerle ilişkilendirilmiş olarak bulunması gerekmektedir. Böylece, son doğrulama işi dağıtık olarak kullanıcı cihazlarında yapılabilmektedir ve konum doğrulama sunucusunda kullanıcıların kişi rehberlerinin kayıtlı olması gereksinimi ortadan kaldırılmaktadır.

IV. DEĞERLENDİRME

Doğrulanmış konum bildirimleri için bu makalede önerilen yöntemlerin birbirlerine göre farklılıkları, konum doğrulama cihazı, sunucu ve mobil uygulama tasarımı açısından belirleyici olacaktır. Tablo 2'de bu farklılıklar özetlenmiştir:

Tablo 2. *Önerilen yöntemlerin uygulanmasında ihtiyaç duyulan tipik özellikler ve gereksinimler ('M': mobil cihaz, 'S': sunucu, '+': gerekli, '-': yok)*

Özellik/Gereksinim	Yöntem I	Yöntem II	Yöntem III	Yöntem IV	Yöntem V
Mobil cihazda internet erişimi	–	–	+	+	+
Konum doğrulama cihazında internet erişimi	+	+	–	–	–
Mobil cihazda açık/gizli anahtar bulunması	+	–	–	+	–
SMS gönderimi yapması zorunlu olan taraflar	–	S & M	S	–	–
Kişi rehberinin bulundurulması gereken yer	S	S	S	S	M

Tablo 1'de, görüldüğü gibi, Yöntem I ve Yöntem II'de doğrulanmış konum bildirimleri yapabilmek için kullanıcının mobil cihazında internet erişimi olmasına gerek yoktur. Özellikle yurtdışında internet kullanımının yüksek maliyetli olması nedeniyle yurtdışı dolaşımda internet erişiminin herkes tarafından kullanılamadığı düşünüldüğünde, Yöntem I ve Yöntem II, genel işletim maliyetlerinde (OPEX) tasarruf sunmaktadır. Diğer taraftan Yöntem III, Yöntem IV ve Yöntem V'te ise, konum doğrulama cihazında internet erişimi bulunmasına gerek yoktur ve bu sayede çok basit, dayanıklı ve pil ile çalışabilen konum doğrulama cihazları yapılıp kullanılabilir; böylece yatırım maliyetleri (CAPEX) aşağı çekilebilir. Günümüzdeki mobil cihazların bellek ve işlem kapasiteleri düşünüldüğünde, AAK kullanımı önemli bir kısıt oluşturmamakla birlikte, Yöntem II, Yöntem III ve Yöntem V'te, kullanıcının mobil cihazında AAK anahtarları bulunmasına gerek yoktur ve bu mobil uygulama için fazladan basitlik sağlar. Yöntem I, Yöntem IV ve Yöntem V'te, taraflardan hiçbirinin SMS mesajı göndermelerine gerek yoktur. Yöntem V'te, ayrıca, kişi rehberinin sunucu üzerinde kayıtlı olmasına da gerek yoktur.

Konum doğrulama cihazının fiziksel özellikleri ve bildirimlerin yapılmasında hangi tarafa daha fazla kolaylık sağlanacağına karar verilmesi, yukarıdaki yöntemlerden hangisinin seçileceğini de belirleyecektir. Bunun yanı sıra, iki veya daha fazla yöntemin değişimli olarak kullanılması da mümkündür. Bunu sağlamak için, yukarıdaki mesaj paketlerinin her birine, seçilen yöntemi belirten bir alan eklenmesi ve paketi yorumlayan tarafların paketi ilgili yöntemin koşullarına göre yorumlaması yeterlidir. Kullanıcı ID'si (k_{ID}) internete çıkan hiç bir pakette açık olarak gönderilmediği için, sunulan yöntemler doğrulanmış yer bildirimi yaparken kişisel mahremiyetin korunmasını da gözetmektedir.

V. SONUÇ

Bu çalışmada, kişilerin diledikleri başka kişilere doğrulanmış ve güvenilir konum bildirimleri yapabilmeleri için bir cihaz ve yöntemler önerilmiştir. Güvenli konum bildirimi için günümüzde hazır bulunan ve makalenin Giriş bölümünde özetlenen mevcut yöntemlerle kıyaslandığında, önerilen

sistemin oldukça yalın ve düşük maliyetli olması, konum doğrulama cihazı ve uzak sunucu dışında başka bir cihaza, özellikle başka 'tanık' partilere gereksinim duyulmaması, çeşitli durumlara göre seçimler ve esneklik sağlayabilmesi bu çalışmanın temel katkılarıdır. Çalışmanın odak noktası, kişiler arası doğrulanmış konum paylaşımı olsa bile, aynı cihaz ve yöntemler belli bir zamanda belli bir yerde bulunulduğunun ispatı amacıyla da kullanılabilir. Örneğin konum doğrulama cihazlarının zaman damgası gibi bir çıktı üretip bunu yerel ağ üzerinden talep eden mobil cihazla paylaşması ve çıktının o cihazda kaydedilmesi ile, gerektiğinde adli amaçlarla (*forensic computing*) kullanılabilen bir sistem de elde edilebilir. Böyle bir sistemin detayları bu alanda sonraki çalışmalara konu olabilir.

VI. KAYNAKLAR

[1] B. R. Waters and E. W. Felten, "Secure, Private Proofs of Location," Princeton University, ABD, Rap. TR-667-03, 2002.

[2] N. Sastry, U. Shankar and D. Wagner, "Secure Verification of Location Claims," 2. ACM Workshop on Wireless Security, San Diego, ABD, 2003, pp. 1–10.

[3] S. Capkun, et al., "Secure Location Verification with Hidden and Mobile Base Stations," *IEEE Transactions on Mobile Computing*, vol. 7, no. 4, pp. 470–483, 2008.

[4] S. Saroiu and A. Wolman, "Enabling New Mobile Applications with Location Proofs," 10. Workshop on Mobile Computing Systems and Applications, Santa Cruz, ABD, 2009, pp. 3.1–3.6.

[5] S. Saroiu and A. Wolman, "I am a sensor, and I approve this message," 11. Workshop on Mobile Computing Systems & Applications, New York, ABD, 2010, pp. 37–42.

[6] W. Luo and U. Hengartner, "VeriPlace: A privacy-aware location proof architecture," 18. SIGSPATIAL International Conference on Advances in Geographic Information Systems, New York, ABD, 2010, pp. 23–32.

[7] X. Wang, J. Zhu and A. Pande, "STAMP: Ad hoc spatial-temporal provenance assurance for mobile users," 21. IEEE International Conference on Network Protocols, Göttingen, Almanya, 2013, pp. 1–10.

[8] M. Liu, et al., "Privacy-preserving distributed location proof generating system," *China Communications*, vol. 13, no. 3, pp. 203–218, 2016.

[9] Z. Zhu and G. Cao, "Toward Privacy Preserving and Collusion Resistance in a Location Proof Updating System," *IEEE Transactions on Mobile Computing*, vol. 12, no. 1, pp. 51–64, 2013.

[10] M. Miettinen, et al., "I Know Where You are: Proofs of Presence Resilient to Malicious Provers," 10. ACM Symposium on Information, Computer and Communications Security, Singapur, 2015, pp. 567–577.

[11] Y. Zhang, et al., "VProof: Lightweight Privacy-Preserving Vehicle Location Proofs," *IEEE Transactions on Vehicular Technology*, vol. 64, no. 1, pp. 378–385, 2015.

[12] C. Javali, et al., “I Am Alice, I Was in Wonderland: Secure Location Proof Generation and Verification Protocol,” IEEE 41st Conference on Local Computer Networks, Dubai, BAE, 2016, pp. 477–485.

[13] X. Ni, et al., “A mobile phone-based physical-social location proof system for mobile social network service,” *Security and Communication Networks*, vol. 9, no. 13, pp. 1890–1904, 2016.

[14] W. Stallings, *Cryptography and Network Security: Principles and Practices*, 3. ed., New Jersey, ABD: Pearson Education, 2003, ch. 9, pp. 258–278.