DÖRDÜNCÜ NESİL KABLOSUZ AĞLAR ARASINDA KARŞILIKLI KİMLİK DOĞRULAMA UYUMLULUĞU İÇİN YENİ BİR ÇÖZÜM

Şerif Bahtiyar[1,2] Fatih Alagöz[2] M. Ufuk Çağlayan[2]

[1]Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü
TÜBİTAK-UEKAE, 41470, Gebze, Kocaeli
[2]Boğaziçi Üniversitesi, Bilgisayar Mühendisliği Bölümü 80815 Bebek-İstanbul

[1]e-posta: bahtiyars@uekae.tubitak.gov.tr [2] e-posta: {alagoz,caglayan}@boun.edu.tr

Anahtar sözcükler: Dördüncü Nesil Kablosuz Ağlar, Gezgin Düğüm, Kimlik Doğrulama, Uyumluluk

ABSTRACT

The fourth generation wireless networks (4G) are expected to provide ubiquitous wireless communications at high data rates and large variety of services, as their main properties will be the secure interoperability and seamless roaming among various wireless network technologies. One of the major problems of these networks is the authentication interoperability, when a mobile node roams between two authentication domains. In this paper, we propose a novel solution that contains new concepts related with the authentication interoperability of 4G. Furthermore, we explain the authentication interoperability solution of 4G according to movement of a mobile node by various scenarios. Finally, we analyze the proposed solution to highlight the way for future researches related with authentication interoperability of these networks.

1. GİRİŞ

Zaman ve teknoloji ilerledikçe, insanlar bilgiye her an, güvenli bir şekilde ve kabloların sınırlaması olmadan daha çok erişmeye ihtiyaç duyacaklardır. Ayrıca insanların, bulundukları ve daha sonra gidecekleri yerlerden bağımsız olarak, aynı zamanda ve sürekli yüksek kalitede servislere gereksinimleri olacaktır. Bu nedenle, yüksek veri miktarını kaldırabilecek ve farklı ağ ortamlar arası gezginliğe olanak sağlayacak bir altyapıya ihtiyaç duyulmaktadır [1-2]. O yüzden, tüketicilere yönelik ağ sistemlerine ve cihazlarına büyük talep vardır ve bu talep hızla artmaktadır.

Dördüncü nesil (4G) ağlar, üçüncü nesil (3G) ağlar gibi tamamen tanımlı olmamasına rağmen, 4G ağların uçtan uca taşıma teknolojisi IP protokolü olacaktır [3]. 4G gezgin ağlarla ilgili çalışmalar bütün haberleşme katmanlarında devam etmektedir. Çalışma alanımızla ilgili olan özellikler kısaca aşağıdaki gibi nitelendirilebilir:

- Hücresel, kablosuz, Kablosuz Yerel Alan Ağ (KYAA), dar-alan bağlantıları ve kablolu bağlantılar gibi değişik erişim teknolojileri arasında yatay haberleşme
- Diğer servisler için ortak bir platform
- IP tabanlı, ortak, esnek, görülmez, merkezi bir ağ bağlantısı
- Merkez ağı, değişik erişim teknolojili ağlara birleştiren ileri düzeyde fiziksel erişim teknolojisi
- Değişik erişim teknolojileri arasında, global dolaşım ve iç içe çalışma; hem yatay (sistem içinde) hem de dikey (sistemler arasında) bağlam değiştirebilme
- Tamamıyla paket-anahtarlamalı ağlar
- Bütün ağ bileşenleri sayısal
- Düşük maliyetli
- Gezginliği, güvenliği ve servis kalitesini (QoS) de içeren görülmez servis anlaşma işlemi [2], [4- 6].

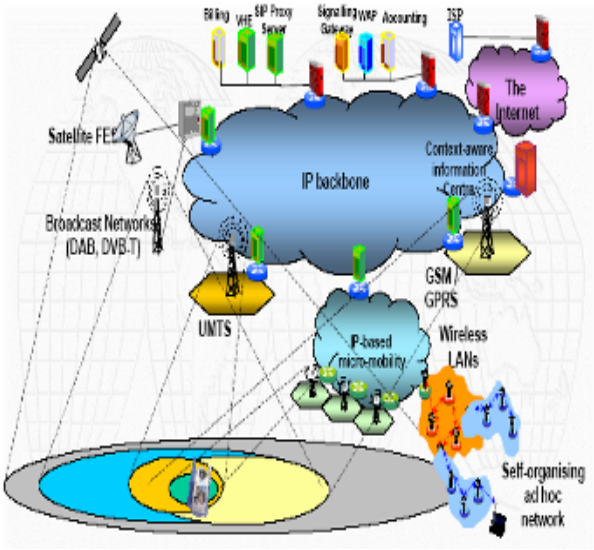
4G kablosuz ağlarda, temel araştırma faaliyetlerinden biri güvenliktir.

4G kablosuz sistemler standartlaşmadığından, 4G kablosuz sistemlerin bir parçası olması beklenen değişik kablosuz teknolojileri destekleyen global güvenlik uyumunu sağlayacak bir çözüm bulunmamaktadır. *Bria* ve arkadaşları bilgi ve haberleşme alanındaki anahtar gelişmeleri ki bunlardan biri güvenliktir tanımlamışlardır [7]. *Barton* ve arkadaşları Gezgin Internet Protokolü ile IP Güvenlik protokolünün değişik şekilde birleştirilmiş alternatiflerini içeren kablosuz bağlantılarda güvenliği sağlamak amaçlı bir çalışma ortaya koymuşlardır [8]. Başka bir çalışmada, hay beye ağlarda cihazları gizlemeye olanak verecek bir güvenlik protokolü (SERAN - Security Equipment protocol in Routing in Ad hoc Networks) sunulmuştur [9]. Bu makalede, 4G ağlarda karşılıklı kimlik doğrulama uyumluluğunu sağlayacak bir çözüm sunulmuştur.

Çalışmamızın geri kalanı şu bölümlerden oluşmaktadır. Bölüm 2'de 4G ağların genel mimarisi özetlenmiştir. Bölüm 3'te, önerilen çözümün en önemli kısımlarından biri olan Kimlik Doğrulama Dönüştürücü Geçidi (KDDG) tanımlanmıştır. Bölüm 4'te değişik kimlik doğrulama senaryoları, önerilen çözüm doğrultusunda sunulmuştur. Bölüm 5'te, senaryoların değerlendirilmesi verilmiştir. Son Bölüm sonuç kısmına ayrılmıştır.

2. 4G AĞLARIN GENEL MİMARİSİ

Gezgin yeni veri servislerindeki güncel gelişmeler, değişik kablosuz ve kablolu ağların bir arada var olmalarını gerektirmektedir. Ancak, bunlardan hiç biri genel bir çözüm olarak değişik sebeplerden dolayı düşünülememektedir. Bu sebepler, genel olarak, çözümlerin belirli bir grup servis ve uygulamaya yönelik olması, belirli bir coğrafik kapsama alanında uygulanabilmesi, belirli bir bant genişliği ve gecikme ile çalışmalarından kaynaklanmaktadır. Üstelik, bu veri ağları arasında her hangi bir entegrasyon bulunmamaktadır; her biri kendi fiziksel erişim teknolojisine, kullanıcı kimlik doğrulama mekanizmasına ve gezginlik yönetim prosedürlerine sahiptir [10]. Bu durum, dünyanın her tarafındaki araştırmacıları 4G ağlarının araştırılmasına yöneltmiştir. 4G ağların yüksek hız, yüksek kapasite, bit başına düşük maliyet, IP tabanlı servisler gibi özellikleri içermesi tasarlanmaktadır. 4G sistemlerinin hepsi açık sistem yaklaşımına dayalı birleşik, global bir ağlarıdır. 4G ağlarının amacı, mevcut merkezi hücresel ağları, IP tabanlı dünya çapında tek bir merkezi hücresel ağ standardında birleştirmektir. Bu yeni ağın, kontrol, video, IP üzerinde ses gibi bir çok servisi desteklemesi planlanmaktadır. Ancak, 3G tamamen hayata geçmediğinden, araştırmacılar 2010 yılında hayata geçmesi planlanan bu yeni "kablosuz dünyaya" kendi fikir ve çalışmaları ile katkıda bulunmaya çalışmaktadırlar [4], [11-12].



Şekil 1. 4G ağlarının genel mimarisi [17]

4G kablosuz ağların, hava ara yüzünde 20 Mbit/s ile 100 Mbit/s arasında veri iletim oranını desteklemesi beklenmektedir. 4G ağlarına yönelik, izlediğin kadar öde, evden alışveriş, elektronik ticaret ve çevrim içi veri dağıtımı gibi yeni yayınlar ve veri uygulamaları düşünülmektedir veya geliştirilmeye başlanmıştır. Bir de, Internet'in hızlı büyümesi ve bütün dünyada kabul görmesi, güvenli ve yüksek bant genişliğine olan ihtiyaç gün geçtikçe artmaktadır [13-16].

4G teknolojisinin geliştirilmesinde karşılaşılan en önemli problemlerden biri, farklı teknolojili çok sayıda gezgin ve kablosuz ağın arasında erişimin nasıl sağlanacağıdır. 4G kablosuz ağlar, global yönlendirmeyi sağlamak amacıyla daha fazla özelleşmiş yerel-alan radyo erişim ağlarını IP merkezli bir ağda birleştirebilirler. Daha fazla özelleşmiş yerel-alan radyo erişim ağları hay beye yönlendirme gibi genel özellikleri içerecek, QoS ve kendi kendine organizasyon gibi yeni özelliklerden oluşacaklardır [4], [11], [15].

4G yerel alan ağları trenler, kamyonlar, binalar veya hay beye kaynaklı oluşmuş, rasgele organize olan ve biri birinin radyo etki alanı içerisinde kalan cihazların kurulumundan oluşacaktır. Bu tür ağlarda yönlendirme işlemi yeni mimarilerin yapısına bağlı olacaktır [18]. Şekil 1'de, 4G ağlarına yönelik önerilmiş olası bir mimarisi gösterilmiştir [17].

4G ağlarına yönelik olası mimariler [1], [11], [18-19] kaynaklarında verilmiştir.

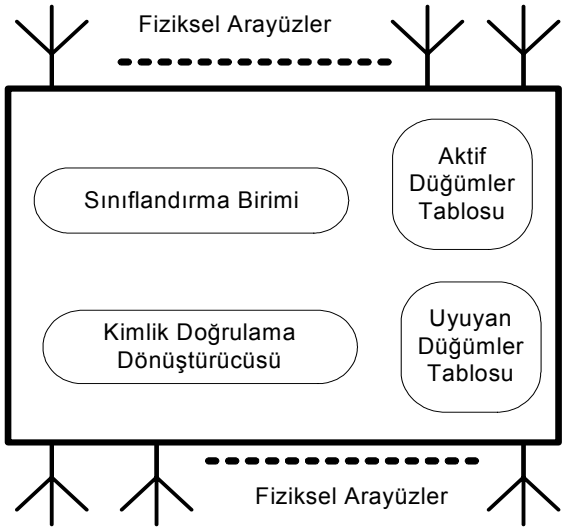
3. KDDG

Kimlik Doğrulama Dönüştürücü Geçidi (KDDG), 4G kablosuz ağlar arasında karşılıklı kimlik doğrulama uyumluluğuna yönelik önerilen çözümü sağlamada kullanılan anahtar bileşen olarak tanımlıyoruz.

Şekil 2'de temel mimarisi ile gösterilen KDDG aşağıdaki özelliklerden oluşmaktadır:

- KDDG, bir Gezgin Düğüm (GD) için GD'nin bulunduğu ağa göre iki farklı durum alabilir. Eğer GD, KDDG ile aynı ağda ise, KDDG ilgili GD için Aktif Düğümler Tablosunda (ADT) bir kayıt bulunduracaktır. Diğer taraftan, eğer GD, KDDG'nin bulunduğu ağının bir komşu ağında ise, KDDG bu düğüm için Uyuyan Düğümler Tablosunda (UDT) bir kayıt bulunduracak ve bu düğüm için uyku durumunda bulunacaktır. KDDG'nin bir düğüm için uyku durumunda olması, bu düğümün komşu bir ağda olduğunu ve her an için KDDG'nin bulunduğu ağa geçebileceği anlamına gelmektedir. GD'nin yukarıda anlatılan ağların dışında başka bir ağda bulunması durumunda, KDDG'de GD ile ilgili herhangi bir kayıt bulunmayacaktır.

- 4G ağları için erişim teknolojileri çalışmaları halen devam etmektedir. Dolayısıyla KDDG'nin her çeşit erişim teknolojileri ile çalışmasına olanak sağlayacak 4G ağlarında kullanılan her çeşit fiziksel erişim teknolojisinin ara-yüzüne sahip olacağı varsayılmıştır.
- KDDG birden fazla kimlik doğrulama mekanizmasını desteklemektedir. Aynı teknolojiyi kullanan veya farklı teknolojileri kullanan ağların hepsinin kendine özgü kimlik doğrulama mekanizmaları vardır. İki farklı ağ arasında karşılıklı kimlik doğrulamayı sağlamak amacıyla KDDG bu ağların kimlik doğrulama yöntemlerini bilmek zorundadır.
- KDDG bir Kimlik Doğrulama Dönüştürücüsüne (KDD) sahiptir. KDD, 4G ağlar için KDDG'de tanımlanmış kimlik doğrulama yöntemlerini birbirine dönüştürmektedir.



Şekil 2. KDDG'nin temel mimarisi

- KDDG bir Kimlik Doğrulama Sınıflandırma Birimine (KDSB) sahiptir. KDSB, GD'nin bulunduğu ağa göre komşu ağlarının kimlik doğrulama güvenlik seviyelerini GD'nin o an bulunduğu ağın kimlik doğrulama güvenlik seviyesine göre göreceli olarak belirler. Diğer bir değişle, KDSB hangi kimlik doğrulama güvenlik mekanizmasının belirli bir güvenlik mekanizmasına dönüştürülebileceğine karar verir. Örneğin, eğer $ağ_i$'nin kimlik doğrulama metodu $KDME_i$'nin kimlik doğrulama güvenlik seviyesi, $ağ_j$'nin kimlik doğrulama metodu $KDME_j$'nin kimlik doğrulama güvenlik seviyesinden yüksek ise $KDME_j$, $KDME_i$'ye dönüştürülebilir. Çünkü $ağ_i$'nin kimlik doğrulama yöntemi $ağ_j$'nin kimlik doğrulama yönteminden daha kuvvetlidir. Diğer taraftan, $KDME_i$'nin kimlik doğrulama güvenlik seviyesi düşük olduğundan $KDME_i$, $KDME_j$'ye dönüştürülemez.

4. KİMLİK DOĞRULAMA SENARYOLARI

Bu çalışmamızda, GD'nin değişik erişim teknolojili ağlar içinde ve arasında dolaştığı kabul edilmiştir. Bu doğrultuda, olası beş farklı senaryo incelenmiştir. Bu senaryolar;

1. Kendi ağında kimlik doğrulama,
2. Yabancı ağda kimlik doğrulama,
3. Farklı erişim teknolojileri arasında dikey bağlam değiştirmede kimlik doğrulama,
4. Aynı teknoloji ve aynı kuruluşun içinde tek kimlik doğrulama etki alanında yatay bağlam değiştirmede kimlik doğrulama,
5. Aynı teknoloji içinde ancak farklı kimlik doğrulama etki alanlarında farklı kuruluşlar arasında yatay bağlam değiştirmede kimlik doğrulama.

A.Kendi Ağında Kimlik Doğrulama

Bu seçenek GD'nin kendi ağında olduğu tipik durumu ifade etmektedir. Belirli bir GD ile ilgili kimlik doğrulama niceliklerinin bulunduğu ağ, ilgili GD'nin kendi ağıdır. Aslında, değişik teknolojilerin kendine özgü kimlik doğrulama mekanizmaları vardır ve bu teknolojiler genellikle sadece kendi kimlik doğrulama yöntemlerini kullanırlar. Hatta bu durum, aynı teknolojili fakat farklı kimlik doğrulama mekanizmasına sahip farklı kuruluşlar için de geçerlidir. Bu senaryo, belirli bir GD'nin kendi ağında kimlik doğrulamasını gerçekleştirirken bu ağda bulunan KDDG'nin ilgili GD'yi kayıt edip komşu KDDG'leri bu GD ile ilgili haberdar etmesinden oluşur.

Kendi ağında kimlik doğrulama işleminin adımları aşağıdaki gibidir:

1. GD kendi ağıda kullandığı, kendi nüfuz alanına özgü kimlik doğrulama yöntemine göre kimlik doğrulama işlemini gerçekleştirir.
2. GD'nin kendi ağı, KDDG'yi yeni kimlik doğrulama işlemi ile ilgili haberdar eder veya kullanılan kimlik doğrulama yöntemine göre KDDG kimlik doğrulama işlemini duyar.
3. KDDG komşu ağlarını ve bunların kullandığı kimlik doğrulama yöntemlerini bilir. Ayrıca, KDDG bulunduğu ağa göre (GD'nin kendi ağına göre) komşu ağlarının kimlik doğrulama güvenlik seviyelerini bulur.
4. KDDG, GD'nin kendi ağının kullandığı kimlik doğrulama yöntemini, kimlik doğrulama güvenlik seviyesi GD'nin kendi ağının kimlik doğrulama güvenlik seviyesinden yüksek olan komşu ağların kimlik doğrulama yöntemine dönüştürür.
5. KDDG ilgili GD'yi, KDDG'nin bulunduğu ağın aktif üyesi olarak kaydeder. Diğer bir değişle, KDDG kendi ADT'sinde kimlik doğrulama işlemini gerçekleştiren GD ile ilgili bir kayıt bulundurur.

6. KDDG, kimlik doğrulama güvenlik seviyeleri GD'nin kendi ağının kimlik doğrulama güvenlik seviyesinden yüksek veya eşit olan komşu ağlarının KDDG'lerini kimlik doğrulamasını gerçekleştiren GD ile ilgili olarak Düğüm Bilgilendirme Mesajları (DBM) ile haberdar eder.
7. Komşu ağlarının KDDG'leri, ilgili GD'yi uyuyan bir üye olarak kendi UDT'lerine kaydederler. Bir KDDG'de uyuyan üye olarak kayıtlı bulunan bir GD, bu üyenin uyuyan üye olarak kayıtlı olan KDDG'nin ağında şimdilik bulunmadığını anlamına gelir. Ancak, UDT'de kayıtlı bulunan bir GD'nin komşu bir ağda olduğu, kimlik doğrulama güvenlik seviyesi bu ağ ile uyuştuğu ve her an yatay veya dikey bağlam değiştirme ile bu kimlik doğrulama nüfuz alanına geçebileceği anlamını taşır.

KDDG, ADT'sinde kayıtlı bulunan GD'lerin durumları ile ilgili olarak komşu ağların KDDG'lerini periyodik olarak DBM'ler ile haberdar etmesi gerekir. Bir KDDG, UDT'sinde kayıtlı bulunan GD'ler ile ilgili belirli bir zaman dilimi içerisinde (Δt) bir DBM almaz ise (UDT'de kayıtlı bir GD ile ilgili son alınan DBM'dan sonra Δt zaman sonra yeni bir DBM almaz ise) ilgili GD'yi UDT'den siler. Zaman dilimi (Δt), ilgili ağın güvenlik subay veya memuru tarafından belirlenecektir.

B.Yabancı Ağda Kimlik Doğrulama

Bu senaryo, GD'ye yabancı ağda (yabancı kimlik doğrulama etki alanında) güç verildiğinde gerçekleştirilen kimlik doğrulama durumunu açıklamaktadır. Bir GD için, yabancı ağ (yabancı kimlik doğrulama etki alanı), ilgili GD'nin kimlik doğrulama bilgilerinin bulunmadığı ağı (kimlik doğrulama etki alanını) ifade etmektedir. Diğer bir değişle GD, kimlik doğrulama işlemini KDDG'ler üzerinden gerçekleştirmek zorunda olduğu durumdur.

Yabancı ağda kimlik doğrulama işleminin adımları aşağıdaki gibidir:

1. Yabancı ağda bulunan bir GD'ye güç verildiğinde (örneğin, bir kablosuz haberleşme ara yüzü bulunan bir diz üstü bilgisayarı açıldığında), ilgili GD, kimlik doğrulama işlemini gerçekleştirmek için bulunduğu ağdan kimlik doğrulama talebinde bulunacaktır. Başka bir değişle, ilgili GD'nin kullandığı kimlik doğrulama yöntemine göre, GD kimlik doğrulama işlemini gerçekleştirmeye çalışacaktır. Ancak, yabancı ağ, GD'den farklı bir kimlik doğrulama yöntemi kullandığından GD'yi anlayamayacaktır. Diğer taraftan, yabancı ağda bulunan KDDG, GD'nin bu isteğini algılayacaktır.
2. KDDG, GD'den GD'nin kimlik bilgilerini isteyecektir. Bir GD'nin kimlik bilgileri, bu GD'nin kimlik doğrulama işlemi için gerekli olan temel bilgilerden oluşmaktadır. Örneğin, GD'nin yerel ağına ulaşmak için gerekli bilgiler ve (kullanılırsa) GD'nin sertifikası bunlardan bazılarıdır.
3. Yabancı ağda bulunan KDDG, GD'nin yerel ağındaki KDDG'sine bağlanır.
4. Yabancı ağdaki KDDG, GD'nin yerel ağındaki KDDG ile güvenli haberleşme kurduktan sonra, GD'yi doğrulamak için gerekli bilgileri GD'nin yerel ağındaki KDDG'ye gönderir.
5. Yerel ağdaki KDDG'ye gönderilen bu bilgilerden sonra, yabancı ağdaki KDDG, yerel ağdaki KDDG'den cevap bekleyecektir.
6. Yerel ağdaki KDDG, yabancı ağdaki KDDG'den gelen bilgiler doğrultusunda GD'nin kimlik doğrulama işlemlerini gerçekleştirmeye çalışır.
7. GD ile ilgili bilgiler, yerel ağda doğrulanamaz ise yerel ağdaki KDDG, yabancı ağdaki KDDG'yi haberdar eder. Eğer yerel ağda, GD'nin kimlik doğrulama işlemi başarı ile gerçekleştirilirse, yerel ağdaki KDDG, yabancı ağın kimlik doğrulama etki alanını kontrol eder. Eğer yabancı ağın kimlik doğrulama güvenlik seviyesi yerel ağın kimlik doğrulama güvenlik seviyesinden düşük ise, yerel ağdaki KDDG, yabancı ağdaki KDDG'ye, kimlik doğrulama işleminin sebebiyle birlikte başarısız sonuçlandığını bildirir. Diğer durumda, yerel ağdaki KDDG, gerekli kimlik doğrulama güvenlik dönüşümlerini yapar ve gerekli bilgileri, yabancı ağdaki KDDG'ye iletir.
8. Yabancı ağda bulunan KDDG, belirli bir zaman sonra yerel ağdaki KDDG'den GD ile ilgili bir yanıt alamaz ise dördüncü adıma döner. Birkaç denemeden sonra yabancı ağdaki KDDG yine cevap alamaz ise GD'ye kimlik doğrulama işlemi başarısız mesajını sebebi ile birlikte iletir. Diğer durumda, yerel ağdaki KDDG'nin göndermiş olduğu yanıta göre, yabancı ağdaki KDDG, GD'ye kimlik doğrulama işlemi başarılı veya başarısız mesajını döndürür.
9. Bundan sonraki beş adım, kendi ağında kimlik doğrulama işleminin 3. ve 7. adımlar (3. ve 7. adımlar dahil) arasındaki adımlar ile aynıdır.

KDDG'ler, KDDG ile GD arası mesajlar ve kimlik doğrulama işlemi için gerekli adımlar, kullanılan 4G mimarisine ve bağlam değiştirme algoritmalarına göre ayarlanacaktır.

C.Dikey Bağlam Değiştirmede Kimlik Doğrulama

Bu senaryo, GD farklı erişim teknolojileri kullanan ağlar arasında dolaşırken gerçekleştirdiği kimlik doğrulama işlemlerini açıklamaktadır. Bu tür bağlam değiştirmeler dikey bağlam değiştirme olarak bilinmektedir (örnek, GD'nin UMTS ile W-LAN arasında dolaşması).

Dikey bağlam değiştirmede kimlik doğrulama işleminin adımları aşağıdaki gibidir:

1. GD dikey bağlam değiştirme ile erişim noktasını değiştirdiğinde, GD'nin geçtiği yeni ağdaki KDDG bu durumu algılar.
2. GD'nin geçtiği yeni ağdaki KDDG, kendi ADT'sini ve UDT'sini, GD'ye göre değiştirir. Diğer bir değişle, yeni ağdaki KDDG, GD ile ilgili uyku durumundan aktif durumuna geçer.
3. KDDG gerekli kimlik doğrulama sınıflandırmalarını ve dönüşümleri gerçekleştirerek bilgilendirilmesi gereken komşu ağlarının KDDG'leri bilgilendirilir.
4. Bundan sonraki beş adım, kendi ağında kimlik doğrulama işleminin 3. ve 7. adımlar (3. ve 7. adımlar dahil) arasındaki adımlar ile aynıdır.

D. Tek Kimlik Doğrulama Etki Alanında Yatay Bağlam Değiştirmede Kimlik Doğrulama

Bu senaryoda, günümüzde olduğu gibi, her erişim teknolojisi kendine özgü kimlik doğrulama mekanizmasını kullanmaktadır. Bundan dolayı, 4G ağlarda, tek kimlik doğrulama etki alanında yatay bağlam değiştirmedeki kimlik doğrulama işlemi için yeni bir özellik tanımlamaya gerek yoktur.

Bir önceki paragrafta ifade edilenlere karşılık, tek kimlik doğrulama etki alanında bağlam değiştirmede kimlik doğrulama işleminin güvenliğini arttırmaya yönelik çalışmalar sürdürülmelidir.

E. Farklı Kimlik Doğrulama Etki Alanlarında Yatay Bağlam Değiştirmede Kimlik Doğrulama

Bu senaryoda, GD'nin aynı tür erişim teknolojisi kullanan ve farklı kimlik doğrulama etki alanına sahip ağlar arasındaki dolaşımı açıklanmıştır. Örneğin, Turkcell'e kayıtlı bulunan bir cep telefonunun (SIM kartının) Telsim veya Aria gibi farklı cep telefonu ağlarını, farklı kimlik doğrulama etki alanlarda yatay bağlam değiştirme ile kimlik doğrulama işlemi yaptıktan sonra kullandığı durumdur.

Bir KDDG birden fazla kimlik doğrulama etki alanları arasında hizmet verir. KDDG için erişim teknolojisinin bir önemi yoktur. Çünkü KDDG'de, orada kullanılan tüm 4G ağlarının ara yüzü bulunmaktadır. Bundan dolayı, bu durumdaki kimlik doğrulama işlemi dikey bağlam değiştirmedeki kimlik doğrulama ile aynı özellikleri taşımaktadır. Tek fark, erişim teknolojisindeki bağlam değiştirmedir.

5. SİSTEMİN DEĞERLENDİRİLMESİ

4G kablosuz ağlarda karşılıklı kimlik doğrulama uyumluluğuna yönelik önerilen çözümün değerlendirilmesi avantajları ve dezavantajları değerlendirilerek yapılmıştır.

A.Önerilen Çözümün Avantajları

Karşılıklı kimlik doğrulamaya yönelik önerilen çözümün temel avantajları aşağıdaki gibidir:

- 4G ağlar arasında global kimlik doğrulamaya olanak sağlamaktadır.
- KDDG birden fazla fiziksel erişim teknolojisini desteklemektedir. Dolayısıyla, ileride geliştirilecek yeni erişim teknolojilerinin birer erişim ara yüzünü KDDG eklemek, yeni tür ağa kimlik doğrulama için erişilmiş olunacaktır ve kolayca sisteme entegre edilebilecektir.
- Göreceli kimlik doğrulama sınıflandırılması ve kimlik doğrulama mekanizmaları arası dönüşüm gibi kimlik doğrulama güvenliğini arttıran ve 4G ağlarında global kimlik doğrulamaya olanak sağlayan yeni kavramlar sunulmuştur.
- KDDG komşu ağlardaki KDDG'leri, kendi ağıdaki aktif GD'ler hakkında ve onların kimlik doğrulama yöntemleri konusunda bilgilendirir. Bundan dolayı, GD ağ değiştirdiğinde, kimlik doğrulama işlemi için gerekli mesajların sayısı azalır. Bu durum, ağlar arasında bağlam değiştiren bir GD'nin kimlik doğrulama işlemini hızlandırır. Bundan başka, hızlı kimlik doğrulama, 4G kablosuz ağlarında başka bir araştırma konusu olan QoS'nın iyileştirilmesini sağlayabilir.
- 4G ağlarında tek kimlik doğrulama yönteminin kullanılmasına gerek yoktur. Her kuruluş kendi özel kimlik doğrulama yöntemini kullanabilir ki bu durum 4G ağlarında heterojen kimlik doğrulamaya olanak sağlar. Ayrıca bu çözüm, 4G ağlarında kimlik doğrulama işleminde tekelin oluşmasını engelleyecektir. Bundan dolayı, kimlik doğrulama işleminin maliyeti düşecektir. Bunun sonucu olarak, 4G ağlarının bir diğer amacı olan düşük maliyet hedefine katkı sağlanmış olunacaktır.

B.Önerilen Çözümün Dezavantajları

Karşılıklı kimlik doğrulamaya yönelik önerilen çözümün temel dezavantajları aşağıdaki gibidir:

- KDDG hem aktif GD'leri hem de uyuyan GD'leri yönetmesi gerekir. Bu durum, daha fazla depolama alanı ve işlemci gücü gerektirir. Örneğin, bir ağın N tane komşu ağı varsa ve her ağda ortalama M tane GD bulunuyorsa, bu durumda bir KDDG, $N*M$ uyuyan GD'nin yönetimi ve M tane aktif düğümün yönetimini gerçekleştirmek durumundadır. Kısacası, bir KDDG ortalama $M*(N+1)$ düğümden sorumlu olacaktır.
- Her KDDG, kendi ADT'sinde kayıtlı bulunan GD'ler hakkında periyodik olarak komşu ağlarının KDDG'lerini bilgilendirir. Komşu ağlardaki KDDG'leri bilgilendirmek için kullanılacak mesajlar, ağlar üzerinde fazladan yük oluşturacaktır. 4G ağlarının bir amacı da yüksek kapasiteye olanak sağlamaktır. Dolaysıyla, kimlik doğrulamadan kaynaklanan fazladan mesajların istenmeyen etkileri, 4G sistemindeki yüksek kapasitelerden dolayı en aza indirilecektir.

6. SONUÇ

4G kablosuz mobil ağların sıradan bir insanın hayatında köklü değişiklikler yapması ve kişinin yaşam kalitesinde fark edilebilir yararlar sağlaması beklenmektedir. Bu ağların temel özelliği, daha çok zeki olmaları ve dünyayı güvenli, sınırlamalardan bağımsız bir şekilde birleştirebilmeleridir.

Bu çalışmada, 4G kablosuz ağlarda karşılıklı kimlik doğrulama uyumluluğuna yönelik bir çözüm önerilmiş ve önerilen çözümün avantaj ve dezavantajları analiz edilmiştir. Önerilen çözüm beş farklı senaryo ile sunulmuştur. Buna ek olarak, göreceli kimlik doğrulama ve kimlik doğrulama mekanizması dönüştürme gibi özgün özellikleri içeren KDDG cihazı tanıtılmıştır. Bu özellikler, 4G kablosuz ağlarda, farklı kimlik doğrulama etki alanları arasında global karşılıklı kimlik doğrulama uyumluluğunu sağlamaya olanak vermektedir. Bu doğrultuda, gelecekteki çalışmamız göreceli kimlik doğrulama sınıflandırması ve kimlik doğrulama dönüştürme algoritmalarının geliştirilmesi olacaktır.

TEŞEKKÜR

Bu çalışma Boğaziçi Üniversitesi Araştırma Fonu tarafından desteklenmiştir. Proje No. BAP 04 S 104.

KAYNAKLAR

[1] Algoja A, A business model for fourth generation wireless mobile networks, Tik-110.501 Seminar on Network Security, 2000

[2] Kellerer W., Vögel H., Steinberg K. E., A communication gateway for infrastructure-independent 4G wireless access, IEEE Communications Magazine, pp. 126-131, March 2002

[3] Koucheryavy Y. and Moltchanov D., On quality of service and performance evaluation in 4G all-IP networks, WIRELESS, MOBILE and ALWAYS BEST CONNECTED 1st International ANWIRE Workshop, Glasgow UK, April 2003

[4] Santhi K. R., Srivastava V. K., Kumaran G. S., Butare A., Goals of true broad band's wireless next wave (4G-5G), IEEE, pp. 2317-2321, 2003

[5] Jamalipour A. and Tekinay S., Fourth generation wireless networks and interconnecting standards, IEEE Personal Communications, pp. 8-9, October 2001

[6] Kanter T., An application architecture for mobile interactive spaces, 3rd IEEE WMCSA, December 2000

[7] Bria A., Overall design of 4th generation wireless infrastructures (4GW)-a project overview & some lessons learned, Proceedings Radiovetenskap och Kommunikation 2002, Stockholm, Sweden, June 2002

[8] Barton M. et al., Integration of IP mobility and security for secure wireless communications, IEEE International Conference on Communications (ICC), New York, NY, April 2002

[9] Othman J. B., Xue X., SERAN: a new protocol to hide an equipment in ah hoc networks, Proceeding of the Eighth IEEE International Symposium on Computers and Communication (ISCC'03), 2003

[10] Cappiello M., Floris A., Veltri L., Mobility amongst heterogeneous networks with AAA support, IEEE, 2002

[11] Misra A., IDMP-based fast handoffs and paging in IP-based 4G mobile networks, IEEE Communications Magazine, pp. 138-145, March 2002.

[12] Yamao Y., Otsu T., Fujiwara A., Murata H., Yoshida S., Multi-hop radio access cellular concept for fourth-generation mobile communications system, IEEE PIMRC, 2002

[13] Chatterjee S., Fernando W. A. C., Wasantha M. K., Adaptive modulation based MC-CDMA systems for 4G wireless consumer applications, IEEE, June 2003

[14] Fitzek F., Koepsel A., Wolisz A., Khrishnam M., Reisslein M., Poviding application-level QoS in 3G/4G wireless systems: a comprehensive framework based on multi-rate CDMA, IEEE Wireless Communications, Vol. 9, pp. 42-47, April 2002

[15] Varshney U. and Jain R., Issues in emerging 4G wireless networks, Computer Communications, pp. 94-96, June 2001

[16] Borras-Chia J., Video services over 4G wireless networks: not necessarily streaming, IEEE, 2002

[17] Ruiz P. M., Beyod 3G: fourth generation wireless networks,II Jornadas de Internet NG, Madrid, October 2002

[18] Safwat A., A-cell: a novel multi-hop architecture for 4G and 4G+ wireless networks, IEEE, pp. 2931-2935, 2002

[19] Morand L., Tessier S., Global mobility with mobile IP "all IP" networks, IEEE, 2002