Sahte Baz İstasyonu Saldırı Tespit Algoritması
Fake BTS Attack Detection Algorithm

Ömer Faruk ÇELİK, Refik SAMET

Bilgisayar Mühendisliği Bölümü Ankara Üniversitesi
samet@eng.ankara.edu.tr, ofcelik@ankara.edu.tr

Özet

Dünya çapında yaygın olarak kullanılan iletişim sistemi GSM bazı güvenlik problemlerine sahiptir. Bu güvenlik problemlerinden bir tanesi mobil terminal ile baz istasyonu arasında karşılıklı doğrulamanın olmamasıdır. Bu durum GSM'in (baz istasyonlarının ve mobil terminallerin) sahte baz istasyonu ataklarına maruz kalmasına neden olmaktadır. Ayrıca, mobil terminal kimliğinin çalınması, tele kulak, mobil terminal ve baz istasyonu sahteciliği ve diğer ortadaki adam (man-in-the-middle) saldırıları sahte baz istasyonu kullanılarak gerçekleştirilebilmektedir. Bundan dolayı, sahte baz istasyonu saldırılarının tespit edilmesi oldukça önemlidir. Bu makalede sahte baz istasyonu saldırıları analiz edilmiştir ve bu saldırıların tespit edilmesine yönelik bir algoritma geliştirilmiştir. Ayrıca yapılan simülasyon ile sahte baz istasyon saldırılarının, geliştirilen algoritma yardımıyla tespit edilebilirliği gösterilmiştir.

Abstract

GSM is widely used communication system around the world and it has some security problems; one of them is lack of mutual authentication between mobile station and base station. GSM (mobile stations and base stations) is subject to fake base station attacks by exploitation of GSM's mutual authentication weakness. In addition, MS identity theft, eavesdropping, impersonation of network/MS attacks and other kinds of man-in-the-middle attacks can be made by fake base station. Thus, detection of fake base station attacks is crucial. This paper presents analysis of fake base station attacks and proposes algorithm for detection those attack. Besides, by the help of proposed algorithm, simulation shows feasibility of fake base station attack detection.

1. Giriş

Mobil İletişim için Küresel Sistem (Global System for Mobile Communication - GSM), %90 market payı ile dünyada en yaygın kullanılan mobil iletişim sistemi olup, 219 ülke ve bölgede kullanılmaktadır [1]. Uluslararası Telekomünikasyon Birliğinin (International Telecommunication Union - ITU) yaptığı araştırmaya göre 2008 yılı sonunda dünya geneli İnternet kullanan insan sayısı 1,5 milyar iken, 4,1 milyar GSM aboneliği bulunmaktaydı. 2013 yılı sonlarında ise GSM aboneliği sayısı neredeyse 7 milyara ulaşmıştır [2]. 25 yıllık bir teknoloji için bu büyük bir başarıdır. Bununla birlikte, GSM'in yaygın olarak kullanılan bir iletişim protokolü olduğu açıktır ve bu sebeple GSM güvenliği oldukça önemlidir.

GSM teknolojisinin güvenliği, var olduğu andan itibaren araştırmacıların ilgi odağında olmuştur. Ancak, GSM'in güvenlik problemleri hala devam etmektedir. Bu problemlerden bir tanesi, uçtan uca kriptolama kullanılmaması; ikincisi büyük gökkuşağı tabloları (rainbow tables) ile saldırılabilen GSM hava arayüzündeki (um interface) kripto zafiyeti [3]; üçüncüsü ise, Mobil Terminal (MT) ve Baz İstasyonu (BTS) arasında karşılıklı doğrulamanın olmamasıdır. Karşılıklı doğrulama eksikliğini kullanarak tele kulak, MT kimliği çalınması ve seçici yakalama (selective interceptor) saldırıları gibi çeşitli sahte BTS saldırıları yapılabilmektedir. Sahte BTS atakları MT kimliği çalma gibi nispeten tehlikesiz olabileceği gibi insansız hava araçlarının sahte BTS saldırısı kullanarak MT'nin yerini kestirip hava saldırısı yapması gibi ölümcül de olabilmektedir [4]. Bu çalışmada, GSM'in karşılıklı doğrulama zafiyeti ve bu zafiyeti istismar eden sahte BTS saldırıları ele alınacaktır.

Konu ile ilgili literatürde sahte BTS saldırılarının nasıl geliştirileceğine dair çeşitli çalışmalar olmasına rağmen, sahte BTS saldırılarının tespit edilip kullanıcının uyarılmasına yönelik pek bir çalışma bulunmamaktadır. Bu nedenle, sahte BTS saldırılarına karşı önlemlerin geliştirilmesi ve MT kullanıcısının sahte BTS ataklarına karşı uyarılması önem arz etmektedir. Bu çalışmayla, sahte BTS saldırı teknikleri analiz edilmekte ve bu saldırıların tespit edilmesine yönelik bir algoritma önerilmektedir.

Çalışmanın diğer bölümlerinin içerikleri söyle özetlenebilir. İkinci bölümde, sahte BTS saldırıları ile ilgili çalışmalar incelenmiştir. Üçüncü bölümde, ilgili GSM protokollerinin analizi yapılmış ve sahte BTS saldırı tespit algoritması önerilmiştir. Dördüncü bölümde, sahte BTS algoritmasının simülasyonu yapılmıştır. Beşinci bölümde ise sonuç ve yapılması planlanan işlere yer verilmiştir.

2. İlgili Çalışmalar

Yapılan literatür araştırmaları sonucunda sahte BTS saldırılarının tespit edilmesine yönelik çalışmalara rastlanmamasına rağmen, sahte BTS saldırıları ile ilgili incelenen çalışmalar aşağıda özetlenmiştir.

[5] numaralı çalışmada, konferans salonları veya uçaklar gibi MT'lerin aktif olmaması gereken alanlarda, MT'lerin tespit edilip yasaklanması için bir sistem geliştirilmiştir. Çalışmaya

göre, MT'ler birkaç durumda kendini şebekeye tanıtmaktadırlar, yani kendilerine özgü olan IMSI (International Mobile Subscriber Identity) numaralarını şebekeye bildirmektedirler. Bu çalışmada yazarlar bu durumların 3'ünden bahsetmişlerdir: 1) Gelen/giden aramalarla; 2) Zamanlayıcıların (T3211, T3213 ve T3212) süresinin dolmasıyla; 3) Yeni bir bölgeye (Location Area) girilmesiyle. Birinci durum için, MT'nin kendini şebekeye tanıtması RF alıcılar ile tespit edilebilmekte ancak uygulanabilir olmamaktadır. İkinci durumda MT'nin kendini şebekeye tanıtmasının yakalanması zordur çünkü söz konusu zamanlayıcıların süresi her GSM operatöründe değişiklik göstermekte ve bu süreler genellikle saat mertebesinde olmaktadır. Çalışmanın hedefi üçüncü durumla ilgili olup, bu durumun 2 adımı vardır. İlk adım, [6] yardımıyla hedef alandaki bütün aktif BTS'leri devre dışı bırakmaktır. İkinci adım ise, farklı bir LAI (Location Area Identifier) değerine sahip sahte BTS kullanmaktır. Çalışmaya göre, MT ile gerçek BTS'lerin bağlantısı kesildiğinde, MT otomatik olarak yeni BTS'ler arayacaktır. MT'nin bulabileceği tek BTS ise sahte BTS olacaktır. Sonrasında, MT sahte BTS'e bağlanacak ve BTS'in LAI değerinden farklı bir bölgeye ait olduğunu değerlendirecektir. Farklı bölgedeki BTS'e bağlanılması lokasyon güncelleme sürecini başlatacak ve MT'nin kendini sahte BTS'e tanıtmasına sebep olacaktır. Bu bilgiler ışığında, sahte BTS saldırılarının anlaşılması için beklenmedik LAI değişiklikleri takip edilmelidir.

[7] numaralı çalışmada, GSM protokolünü hedef alan gerçek zamanlı dedektör sistemi geliştirilmiştir. Geliştirilen dedektör sistemi 3 parçadan oluşmaktadır. 1. parça, [5]'de geliştirilen "GSM MT dedektörü", ikincisi lokal veri tabanı, üçüncüsü ise saeçici yakalama (selective interceptor) cihazıdır. Çalışmayla, belirli bir bölge içinde kalan MT'ler "GSM MT Dedektörü" ile tespit edilmekte ve tespit edilen MT kimlikleri lokal veri tabanında toplanmaktadır. Sonrasında ise, MT'ler lokal veri tabanından kontrol edilerek seçici olarak engellenip bırakılabilmektedir. Bu çalışmada, [5]'e ek olarak MT'nin kendini ağa tanıtması için 2 yöntem daha kullanılmıştır. Bunlar ise, MTlerin açılışta ve çağrı düşüp tekrar bağlanmak istediğinde yaptığı lokasyon güncelleme istekleridir.

[8] ve [9]'da, yazılımsal radyo teknolojisi (software radio technologies - SDR) kullanılarak sahte BTS geliştirilmiştir. Bu çalışmada, [5] ve [7]'nin aksine sahte BTS geliştirilirken, gerçek BTS'ler sinyal bozucu (jammer) ile engellenmemiştir. Ayrıca, sahte BTS geliştirilirken farklı bir yaklaşım ve yazılımsal radyo teknolojisi kullanılması hem masrafları düşürmüş hem de performansı önemli oranda artırmıştır. Geliştirilen sistemde bir tane mühendislik modu olan MT kullanılmıştır. Söz konusu MT ile çevredeki aktif BTSler tespit edilebilmektedir. Tespit edilen BTS'ler hücre seçilme kriteri olan C2 parametresine göre (cell reselection criterion) güçlüden zayıfa sıralanmaktadır. Sahte BTS bahse konu MT'den BTS'lere ait bilgileri alıp, ortamdaki en zayıf BTS gibi davranmakta ve hedef MT'lerin kendisine bağlanmasını sağlamaktadır. Gerçek BTS'in taklit edilmesinin sebebi, normal BTS'lerin komşu BTS'lere ait bilgileri BCH (Broadcast Channel) kanalından yayınlamalarıdır. Böylece MT'ler tereddüt etmeden sahte BTS'e bağlanmaktadır. Sahte BTS, taklit ettiği BTS'in MCC (Mobile Country Code) ve MNC (Mobile Network Code) gibi GSM operatörlerine ait olan bilgilerini de taklit etmelidir. Bu nedenle, her GSM operatörü için ayrı sahte BTS kullanılmalıdır. Bununla birlikte, MT'nin kendini sahte BTS'e tanıtması için MT'lerde lokasyon güncelleme prosedürü tetiklenmelidir. Söz konusu tetiklenme için sahte BTS'in LAI değeri gerçek BTS'lerden farklı olmalıdır. Çalışmadaki en kritik bölüm, sahte BTS'in yayın yapan en güçlü BTS olmasa bile kendini MT'lere seçtirebilmesidir. MT'ler, her 5 saniyede BTS'lerin BCCH (Broadcast Control Channel) kanalını okuyup, C2 parametresine göre BTS'leri güçlüden zayıfa dizmektedir. MT için BTS seçimi BTS'lerin C2 parametrelerine göre yapılmaktadır. C2 parametresi MT'nin BTS'e yakınlığı ve bazı ofset değerleri ile hesaplanmaktadır. Ofset değerlerine pozitif/negatif değerler verilerek MT'nin spesifik bir BTS'i seçimi teşvik edilebilmekte veya engellenebilmektedir. Çalışmada, geliştirilen sahte BTS, C2 parametresini değiştirerek MT'lerin kısa sürede kendisine bağlanmalarını sağlayabilmiştir. Ayrıca, farklı LAI kullanarak MT'lerde lokasyon güncelleme prosedürünü tetikleyebilmiştir. Sonuç olarak, sahte BTS saldırılarının tespit edilebilmesi için sıra dışı C2 değerleri önemli bir gösterge olacaktır. Ayrıca, zayıf olan BTS'in beklenmedik şekilde seçilmesine de dikkat edilmelidir.

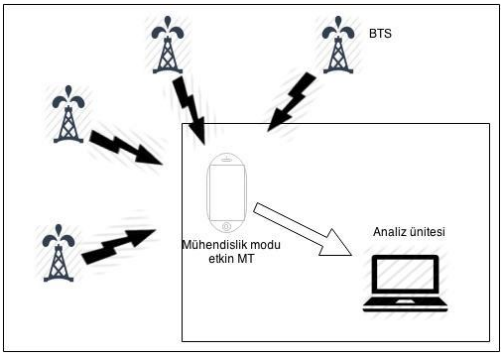
Sahte BTS saldırısı, BTS ve MT arasında gerçekleşen bir tür man-in-the-middle saldırısıdır. Yukarıdaki çalışmalara göre, sahte BTS saldırıları için MT'nin BTS'e bağlanması gerekmektedir. Bu bağlantının sağlanması için C2 parametresinin manipüle edilmesi önem arz etmektedir. Ayrıca farklı bir LAI kullanarak MT'nin kimliğinin alınması da gerekmektedir. Sahte BTS saldırı tespit algoritması yukarıdaki yaklaşımlar göz önünde bulundurularak geliştirilmiştir.

3. Sahte Baz İstasyonu Saldırı Tespit Algoritması

3.1. Sistem Mimarisi

Önceki bölümlerde bahsedildiği gibi literatür araştırmalarında sahte BTS saldırıları ile ilgili çalışmalar olmasına rağmen, bu saldırıların tespit edilmesine yönelik çalışmaya rastlanılmamıştır. Bu makale, sahte BTS saldırılarının tespiti alanına katkıda bulunacaktır.

Önerilen sistem mimarisi Şekil 1'de verilmektedir.

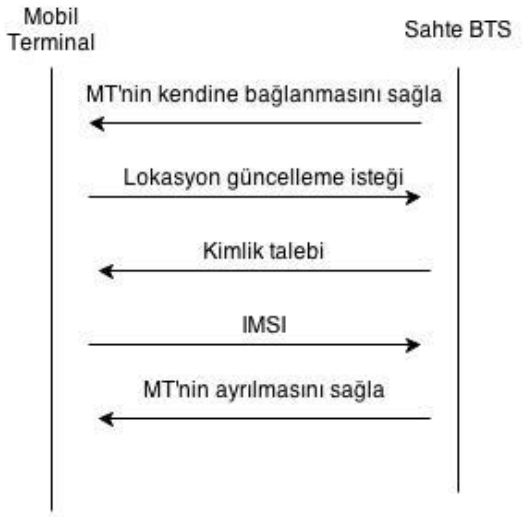


Şekil 1: Sistem Mimarisi.

Şekil 1'deki MT, kendi bölgesindeki aktif BTS'leri tespit edip, Cell ID ve LAI gibi bilgileri almak için her BTS'in BCCH

kanalını okumaktadır. MT, BTS'lerden topladığı bilgileri "Analiz Ünitesine" yollamaktadır. MT, BTS'lerden okuduğu bilgiyle otomatik olarak hesapladığı C1 ve C2 parametrelerini de analiz ünitesine göndermektedir. Analiz ünitesi olarak, geliştirilen algoritmayı çalıştırabilecek herhangi bir PC veya akıllı telefon kullanılabilmektedir. Analiz ünitesi MT'nin gönderdiği verileri sahte BTS saldırı tespit algoritmasına göre değerlendirip, şüpheli durumlar için kullanıcıyı uyarmaktadır.

Basit bir sahte BTS saldırısı Şekil 2'deki gibi olmaktadır.



Şekil 2: Örnek Sahte BTS Saldırısı

İkinci bölümde ve [10]'da açıklandığı üzere, MT'lerde lokasyon güncellemenin tetiklenebilmesi için sahte BTS'in gerçek BTS'lerden farklı bir LAI değeri olmalıdır. MT'nin lokasyonunun takip edildiği durumlarda ise sahte BTS MT'yi tekrar tekrar yakalamak zorundadır. Yani MT'deki LAI değerinin beklenmedik şekilde değişmesi de tespit algoritması için parametre olacaktır.

3.2. Protokol Analizi

Sahte BTS saldırıları için, MT'nin yakalanması ve bırakılması çetin bir iştir. [5] ve [7]'de bu iş için sinyal bozucu sistemler kullanılmıştır [6]. Fakat bu sistemlerde her BTS için ayrı bir sinyal bozucu ünite gerekmekte ve sinyal bozucunun zamanlamasını ayarlarken zorluklarla karşılaşılmaktadır. Ancak, C2 parametresinin manipüle edilerek kullanılması, hem masrafı düşürmekte hem de performansı önemli ölçüde artırmaktadır [8]. [9] ve [11]'e göre C1 (path loss criterion parameter) parametresi hücre seçiminde kullanılmakta ve aşağıdaki gibi hesaplanmaktadır .

$$C1 = (A - Max(B, 0)) \quad (1)$$
$$A = RLA\_C - RXLEV\_ACCESS\_MIN \quad (2)$$
$$B = MS\_TXPWR\_MAX\_CCH - P \quad (3)$$

Sınıf 3 DCS 1800'ler için,

$$B = MS\_TXPWR\_MAX\_CCH + POWER\_OFFSET - P \quad (4)$$

Yukarıdaki formüllerde;

RLA_C ulaşılan ortalama değerler;
RXLEV_ACCESS_MIN MT'nin sisteme erişmesi için gerekli minimum sinyal seviyesi;
MS_TXPWR_MAX_CCH MT'nin sisteme erişmesi için gerekli olan en fazla TX güç seviyesi,
POWER_OFFSET MS_TXPWR ile karşılıklı olarak kullanılan güç ofset değeri ve
P ise MT'nin maximum RF güç çıkışıdır.

Bütün değerler dBm formatındadır ve yukarıdaki tanıma göre, C1 değeri MS ve BTS arasındaki mesafe ile ters orantılıdır. C2 parametresi ise hücre seçimi için kullanılır ve aşağıdaki gibi tanımlanır [11].

PENALTY_TIME <> 11111 için,

$$C2 = C1 + CELL\_RESELECT\_OFFSET - TEMPORARY\_OFFSET * H(PENALTY\_TIME - T) \quad (5)$$

PENALTY TIME = 11111 için,

$$C2 = C1 - CELL\_RESELECT\_OFFSET \quad (6)$$

Komşu hücreler için,

$$H(x) = 0 \; for \; x < 0 \quad (7)$$
$$H(x) = 1 \; for \; x \geq 0 \quad (8)$$

Hizmet veren hücre için,

$$H(x) = 0 \quad (9)$$

T, hesaplanan en güçlü BTS'ler listesinde her BTS için tutulan zamanlayıcıdır.

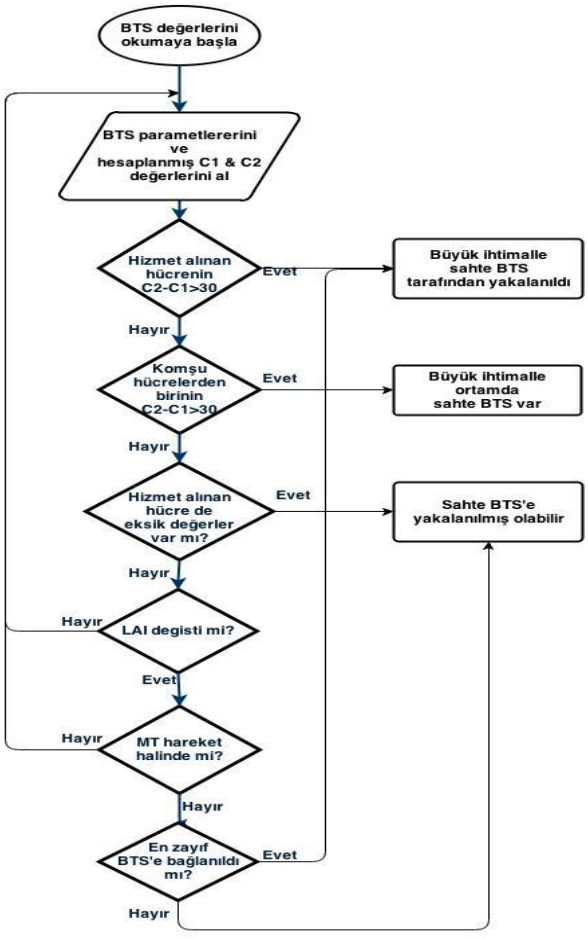
CELL_RESELECT_OFFSET, TEMPORARY_OFFSET, PENALTY_TIME, CELL_BAR_QUALIFY değerleri opsiyonel olarak BTS'in BCCH kanalından yayınlanmaktadır. Eğer yayınlanmıyorsa olağan değerleri sıfıra eşittir ve bu şekilde C2=C1 olur. Türkiye'nin Ankara ilinde yapılan testlere göre her BTS için C1 ve C2 değerleri olağan koşullarda olduğu gibi birbirine eşit çıkmışlardır. Yukarıdaki hesaplamalara ve [12]'ye göre BTS'ler arasında öncelik tanıma yukarda bahsedilen opsiyonel parametreler ile yapılmaktadır. Opsiyonel parametreler C2 değerini değiştirmek için kullanılabilir ve BTS'in hesaplanmış C2 değeri ne kadar yüksek olursa MT'nin BTS'i seçme ihtimali o kadar artar. C2 değerinin olağan dışı bir şekilde C1 değerinden farklı olması Şekil 3'de gösterilen sahte BTS tespit algoritması için önemli bir girdi olacaktır.

3.3. Algoritma tasarımı

Şekil 3'de sahte BTS tespit algoritmasının akış şeması verilmektedir. Algoritma ağ değerlerini ve MT lokasyonunu değerlendirmektedir. Algoritmada 3 durum bulunmaktadır.

Birinci durum, C2 parametresinin manipülasyonu ile ilgilidir. Önceki bölümlerde açıklandığı gibi C2, ofset parametreleri değiştirilerek hücre seçimini etkilemek için kullanılabilmektedir. MT'nin BTS'e uzaklığını gösteren C1 parametresi yüksek olmasa bile, yani sahte BTS hedef MT'ye en yakın BTS olmasa bile sahte BTS, C2 değerini manipüle ederek MT'lerin kendine bağlanmasını sağlayabilmektedir.

[11] ve bu çalışma kapsamında yapılan testlere göre C1 ve C2 parametreleri sıra dışı bir durum olmadığı takdirde birbirine eşitlerdir. Bundan dolayı C2-C1>30 olması, sıra dışı bir duruma işaret etmektedir. Birinci durumun da 2 kısmı vardır. Birinci kısımda, hizmet veren hücrenin C2 ve C1 değerleri arasındaki farkın 30'dan fazla olması durumunda, Önerilen algoritma "MT'nin büyük ihtimalle sahte BTS'e yakalandığı" sonucuna varacaktır. İkinci kısımda ise, yani komşu hücrelerden bir tanesinin C2 ve C1 değerleri arasındaki farkın 30'dan büyük olması durumunda, Algoritma "büyük ihtimalle MT'nin yakınlarında sahte BTS çalışmaktadır" sonucuna varacaktır. 30 değeri hatalı pozitif (false-positive) sonuçları elemek için ve BTS-MT arasındaki hava arayüzünde yaşanması muhtemel sinyal bozulmalarını elemine edebilmek için seçilmiştir. Ayrıca, sahte BTS'in MT'leri daha hızlı yakalayabilmesi için C2 ve C1 arasındaki fark 30 değerinden daha büyük olmalıdır.



Şekil 3: Sahte BTS Saldırı Tespit Algoritması

Algoritmadaki ikinci durum, sahte BTS'in eksik konfigürasyonu ile ilgilidir. BTS'ler kendi yakınlarında bulunan komşu hücrelerine ait bilgileri BCH kanalından yayınlamalıdırlar [12]. Sahte BTS'in sahada kullanıldığı ve hareket halinde olunan durumlarda komşu hücreler sürekli değişmekte ve değişen komşu hücreleri güncellemek zaman almaktadır. Bu nedenle, eksik yapılandırılmış BTS'in sahte BTS olması muhtemeldir. Eksik yapılandırılmış BTS için başka bir örnek ise sahte BTS için hiç var olmayan bir Cell ID seçilmesidir [5]. Eğer bağlanılan BTS daha önceki BTS'lerin komşu hücreler listesinde yoksa bağlanılan hücre sahte BTS olabilir. Bunlara ek olarak, hizmet veren hücre o alanda yayın yapan tek hücre ise, diğer BTS'ler sinyal bozucu ile bastırılmış olabilir [7] ve yalnızca bağlanılan sahte BTS'e izin verilmiş olunabilir.

Üçüncü durum farklı LAI kullanılmasını analiz etmektedir. MT'nin kimliğinin alınabilmesi için sahte BTS, MT'de lokasyon güncelleme prosedürünü tetiklemelidir. Yukarıda anlatıldığı gibi, MT'de lokasyon güncelleme prosedürünü tetiklemek için sahte BTS, hizmet veren hücreden farklı bir LAI kullanmalıdır. Bu nedenle, MT hareket etmezken gerçekleşen LAI değişiklikleri şüpheyle karşılanmalıdır. Ayrıca, sahte BTS ortamdaki en zayıf BTS'i seçip onun yerine geçmektedir [8], [9]. [9]'da tasarlandığı gibi eğer MT hareket etmiyorsa ve önceki durumda en zayıf olan BTS'e bağlandıysa ve üstüne LAI değişikliği olduysa, MT büyük ihtimalle sahte BTS'e bağlanmış diyebiliriz. Bağlanılan BTS en zayıf olmasa bile eğer MT hareket etmiyorsa ve LAI değişikliği olduysa da sahte BTS'e yakalanılmış olabilir.

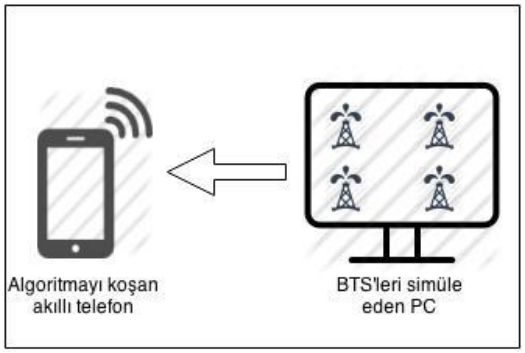
Sonuç olarak, bahse konu senaryolar çeşitli alarmlar üretmektedir. Algoritmanın bir döngüsünde sadece bir alarm üretilebileceği gibi birden çok alarm da üretilebilmektedir. Algoritma devamlı çalışmalı ve karar yukarıda bahsedilen durumların hepsi göz önünde bulundurulduktan sonra verilmelidir. Sahte BTS tespit algoritmasının yardımıyla, ortamda sahte BTS saldırısının tespitine yönelik alarmlar üretilmekte ve üretilen alarmlar saldırıya maruz kalınmış olunmasına dair önemli ipuçları vermektedir.

4. Geliştirilen Algoritmanın Simülasyonu

Bu bölümde geliştirilen algoritmanın simülasyonu yer alacaktır. Gerçek ve sahte BTS'leri simüle eden bir program geliştirilip algoritma bu programla test edilmiştir.

BTS'leri simüle eden program Java ile geliştirilmiş olup standart bir PC'de çalışmaktadır. Şekil 1'de bulunan hem Mobil Terminal hem de Analiz ünitesi için ANDROID işletim sistemi 4.4.4 sürümüne sahip LG Nexus 4 akıllı telefon kullanılmıştır. PC ve akıllı telefon arasındaki iletişim, akıllı telefon tarafından oluşturulan geçici Wi-Fi erişim noktası üzerinden sağlanmaktadır. Geliştirilen algoritma akıllı telefon üzerinde çalışmakta ve algoritma neticesinde oluşan alarmlar akıllı telefonda gösterilmektedir. Simülasyonun mimarisi Şekil 4'de gösterilmektedir.

Algoritmayı çalıştıran ANDROID uygulaması periyodik olarak çalışmakta ve PC tarafından simüle edilen BTS'lerin bilgilerini okumaktadır. Sonrasında, uygulama BTS'den gelen verileri algoritmaya göre değerlendirmekte ve alarmları oluşturmaktadır. Eğer birden çok alarm üretildiyse, uygulama en ciddi olanı ekranda gösterip diğerlerini de bilgi olarak göstermektedir. Algoritmanın döngüleri 30 saniyede bir çalışmaktadır. Her döngüde önce simüle edilen BTS verileri okunmakta, sonrasında akıllı telefonun dâhili GPS modülü kullanılarak lokasyon değişikliği hesaplanmaktadır. Ayrıca okunan bu değerler belirli bir süre akıllı telefonda tutulmakta ve algoritma tarafından değerlendirilip sonuç üretilmektedir.



Şekil 4: Simülasyon Mimarisi

Akıllı telefonda çalışan sahte BTS tespit algoritması Bölüm 3,3'de anlatılan durumlarla karşılaştığında 3 şekilde uyarıda bulunmaktadır. Birincisi, "yüksek ihtimalle sahte BTS'e yakalandınız" uyarısıdır. Bu uyarıda, MT'nin hizmet aldığı hücre büyük ihtimalle sahte BTS'dir. İkincisi, "yüksek ihtimalle ortamda sahte BTS çalışmaktadır" uyarısıdır. Bu uyarıda ise komşu hücrelerden birisi büyük ihtimalle sahte BTS'dir ve MT sahte BTS'e yakalanmak üzere olabilir. Üçüncüsü, "sahte BTS'e yakalanılmış olabilir" uyarısıdır. Bu uyarıda ise hizmet alınan hücrenin sahte BTS olma ihtimali vardır. Algoritmanın çalışma döngüsü olarak 30 saniye seçilmiştir, çünkü [9]'da sahte BTS'in telefonların çoğunu yakalaması yaklaşık 40 saniye sürmüştür. Tespit algoritmasını 30 saniyede bir çalıştırarak mevcut saldırıların kaçırılmaması sağlanmaya çalışılmıştır. Gerçek ortamda test edilmesi durumunda, BTS'lerin BCH kanalının okunması zaman alacağı için uygulamanın daha sık çalıştırılması gerekecektir.

Yapılan testler sonucunda simülasyonun hedef senaryolara karşı beklenilen alarmları ürettiği tespit edilmiş olup gerçek ortamda test edildiğinde benzer sonuçların çıkması beklenilmektedir. Akıllı telefonda çalışan uygulamanın sahte BTS cihazına karşı çalışabilmesi için BTS'lerin verilerini okuyan kısmın değiştirilmesi gerekmektedir. Veri okuma kısmının değiştirilmesi için ya akıllı telefonun radyo modülü kullanılmalı ya da akıllı telefona BTS değerlerini okuyabilen harici bir cihaz bağlanması gerekmektedir. Geliştirilen uygulama yalnızca bir GSM operatörü için kullanılabilmektedir. Geliştirilen uygulamanın bütün GSM operatörleri için kullanılabilmesi için her operatöre ait BTS verilerinin okunabilmesi ve algoritmanın her operatör için tekrar işletilmesi gerekmektedir.

5. Sonuç

Bu çalışmayla sahte BTS saldırıları analiz edilmiş ve bu saldırıların tespit edilmesine yönelik algoritma geliştirilmiştir. Geliştirilen algoritma simülasyon ortamında test edilip hedef durumlar için algoritmanın beklenen sonuçları ürettiği gözlemlenmiştir. Sahte BTS saldırıları geliştirilmesi konularında çalışmalar olmasına rağmen, sahte BTS saldırılarının tespitine yönelik çalışmaya literatür taramasında rastlanmaması geliştirilen algoritmanın önemini artırmaktadır. Ayrıca, sahte BTS cihazlarının gelişen teknoloji ile kolayca yapılabilmesi, hedefinin GSM gibi oldukça yaygın kullanılan bir teknoloji olması ve sahte BTS saldırıları ile tele kulak ve yer tespiti gibi saldırılar yapılabilmesi de saldırı tespit çalışmasının ne kadar gerekli olduğunu göstermektedir.

Simülasyon algoritmanın nasıl çalıştığını göstermesine rağmen sahte BTS cihazı ile test edilmesi yapılacak işler arasında en önde gelmektedir. Ek olarak, günümüzde üçüncü nesil (3G) oldukça yaygın kullanılmaya başlanmış olup dördüncü nesil (4G) ise gittikçe yaygınlaşmaktadır. Benzer saldırılar 3G ve 4G için de yapılmakta veya saldırı çalışmaları devam etmektedir. Bu saldırılara karşı benzer tespit sistemlerinin geliştirilmesi de yapılması gereken çalışmalar arasındadır.

6. Kaynaklar

[1] Direct URL http://en.wikipedia.org/wiki/GSM Last accessed 30.06.2014.
[2] F.V.D. Broek "Eavesdropping on GSM: State-of-affairs" 5th Benelux Workshop on Information and System Security (WISSec 2010), November 2010.
[3] Kalenderi, M., Pnevmatikatos, D., Papaefstathiou I. ve Manifavas C, "Breaking the GSM A5/1 cryptography algorithm with rainbow tables and high-end FPGAS" Field Programmable Logic and Applications (FPL), 22nd International Conference-IEEE, 2012.
[4] Direct URL "https://firstlook.org/theintercept/article/2014/02/10/the-nsas-secret-role/" Last accessed 30.06.2014.
[5] Vales-Alonso J., Vicente F. I., González-Castaño F. J. ve Pou-sada-Carballo J.M., "Real-time detector of GSM terminals" IEEE Commun.Lett., vol. 5, pp. 275–276, 2001.
[6] Pousada-Carballo J.M., González-Castaño F. J., Vicente F. I., ve Fernández-Iglesias M.J., "Jamming system for mobile communications,"Electron. Lett. vol. 34, pp. 2166–2167, 1998.
[7] González-Castaño Francisco J., Vales-Alonso Javier, Pousada-Carballo J.M., Fernando Isasi V. ve Fernández-Iglesias M.J., "Real-Time Interception Systems for the GSM Protocol," IEEE Transactions on Vehicular Technology, Vol. 51, No. 5, September 2002.
[8] Zhou K., Hu A. ve Song Y., "A No-Jamming Selective Interception System of the GSM Terminal" 6th International Conference on Wireless Communications Networking & Mobile Computing (WiCOM); 2010, p1-4, 4p 2010
[9] Song Y., Zhou K. ve Chen X., "Fake BTS Attacks of GSM System on Software Radio Platform" Journal of Networks, Vol. 7, No. 2, February 2012
[10] ETSI "European Digital cellular telecommunications system (Phase 1); Location Registration Procedures, (GSM 03.12-DCS version 3.0.1 Release 1992)
[11] ETSI "Digital cellular telecommunications system (Phase 2+); Radio subsystem link control, (GSM 05.08 version 8.5.0 Release 1999)," Document ETSI TS 100 911 V8.5.0 (2000-10)
[12] ETSI "Digital cellular telecommunications system (Phase 2+); Functions related to Mobile Station (MS) in idle mode and group receive mode, (GSM 03.22 version 5.3.1 Release 1996)," Document ETS 300 930 December 1998