Gazi Üniv. Müh. Mim. Fak. Der.
Cilt 31, No 1, 161-169, 2016
DOI: 10.17341/gummfd.79097

Journal of the Faculty of Engineering and Architecture of Gazi University
Vol 31, No 1, 161-169, 2016

SAHTE GSM BAZ İSTASYONU SALDIRI TESPİT ALGORİTMASI

Refik SAMET, Ömer Faruk ÇELİK
Ankara Üniversitesi, Mühendislik Fakültesi, Bilgisayar Mühendisliği Bölümü, Ankara
samet@eng.ankara.edu.tr, cengofc@gmail.com

(Geliş/Received: 27.01.2015; Kabul/Accepted: 14.12.2015)

ÖZET

GSM'in yaygın kullanımına rağmen GSM'e ait güvenlik sorunları devam etmekte ve bu açıklar bilgi güvenliğini önemli ölçüde tehdit etmektedir. Söz konusu güvenlik açıkları arasında mobil terminal ve GSM baz istasyonu arasında karşılıklı doğrulamanın olmaması öne çıkmaktadır. Bu durum, ortadaki adam saldırılarına kapı aralamakta ve GSM baz istasyonları ve mobil terminallerin saldırıya uğramasına neden olmaktadır. Ayrıca söz konusu saldırı ile mobil terminalin kimliğinin çalınması, tele kulak, mobil terminal ve GSM baz istasyonu sahteciliği ve benzeri ortadaki adam saldırıları gerçekleştirilmektedir. Bu sebeple sahte GSM baz istasyonu saldırılarının tespit edilmesi ve kullanıcıların ve operatörlerin bu saldırılardan haberdar edilmesi oldukça önemlidir. Yapılan çalışmada bahse konu saldırılar analiz edilmiş olup, bu saldırıların tespit edilmesine yönelik bir algoritma geliştirilmiştir. Ayrıca, gerçek veriler kullanılarak simülasyon yapılıp, sahte GSM baz istasyonu saldırılarının geliştirilen algoritma ile tespit edilebilirliği gösterilmiştir.

Anahtar Kelimeler: GSM güvenliği, sahte GSM baz istasyonu saldırıları, saldırı tespiti, ortadaki adam saldırıları

FAKE GSM BASE STATION ATTACK DETECTION ALGORITHM

ABSTRACT

Despite the common usage, GSM has some security problems that seriously threaten information security. Lack of mutual authentication between base station and mobile terminal becomes prominent among security leaks of GSM and causes man-in-the middle attacks. In addition, by using fake base station attacks, attackers can get mobile terminal identity and eavesdropping, impersonation of mobile terminal and base station and other types of man-in-the-middle attacks can be taken place. Therefore, detection of fake base station attacks and warning mobile terminal users and GSM operators would be pretty important. In this work, fake base station attacks are analyzed. Then, fake base station attack detection algorithm is developed. Besides, by the help of proposed algorithm, feasibility of fake base station attack detection has been shown by simulation which is based on real GSM network values.

Keywords: GSM security, fake base station attacks, attack detection, man-in-the-middle attacks

1. GİRİŞ (INTRODUCTION)

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]. Avrupa tarafından geliştirilmiş olan GSM, Dünya tarafından kabul görmüş olup, 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. Görüldüğü gibi, GSM yaygın olarak kullanılan bir iletişim protokolüdür ve bu sebeple GSM güvenliği oldukça önemlidir. GSM teknolojisinin güvenliği, GSM'in kullanılmaya başlandığı andan itibaren araştırmacıların ilgi odağında olmuştur. Ancak, GSM'in güvenlik problemleri hala devam etmektedir [3-5]. Bu problemlerden en önemlileri uçtan uca

kriptolama kullanılmaması, büyük gökkuşağı tabloları (rainbow tables) ile saldırılabilen GSM hava arayüzündeki kripto zafiyeti [6], 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 saldırıları MT kimliği çalma gibi nispeten tehlikesiz olabileceği gibi insansız hava araçlarının sahte BTS saldırısı kullanarak MT'nin coğrafi konumunu belirleyip hava saldırısı yapması gibi ölümcül alanlarda da kullanılabilmektedir [7]. Bu çalışmada, GSM'in karşılıklı doğrulama zafiyeti ve bu zafiyeti istismar eden sahte GSM baz istasyonu saldırıları ele alınacaktır. Konu ile ilgili literatürde sahte BTS saldırılarının nasıl gerçekleştirileceğine dair çeşitli çalışmalar olmasına rağmen, sahte BTS saldırılarının tespit edilip kullanıcının uyarılmasına yönelik pek bir akademik çalışmaya rastlanılmamıştır. 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. Bölüm 1'de çalışmanın tanıtımı yapılmış ve öneminden bahsedilmiş, GSM tarihçesi ve GSM mimarisinden bahsedilmiştir. Bölüm 2'de sahte BTS saldırıları ile ilgili çalışmalar incelenmiştir. Bölüm 3'de ilgili GSM protokollerinin analizi yapılmış ve sahte BTS saldırı tespit algoritması önerilmiştir. Bölüm 4'de, sahte BTS algoritmasının simülasyonu yapılmıştır. Bölüm 5'de ise sonuç ve yapılması planlanan işlere yer verilmiştir.

2. İLGİLİ ÇALIŞMALAR (RELATED WORKS)

Yapılan literatür araştırmaları sonucunda sahte GSM baz istasyonu ile ilgili bulunan az sayıda çalışmaların detayları aşağıda özetlenmiştir.

[3] numaralı çalışmada, konferans salonları veya uçaklar gibi MT'lerin aktif olmaması gereken alanlarda, MT'lerin tespit edilip yasaklanması için bir sistem geliştirilmiştir. Çalışma kapsamında GSM protokolünün ilgili kısımları analiz edilmiş olup, çalışmaya göre, MT'ler birkaç durumda kendini şebekeye tanıtmaktadırlar, yani kendilerine özgü olan IMSI 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 iki adımı vardır. İlk adım, sinyal bozucu (jammer) yardımıyla hedef alandaki bütün aktif BTS'leri devre dışı bırakmaktır [8]. İkinci adım ise, farklı bir LAI 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 tetikleyecek ve MT'nin IMSI numarasını sahte BTS'e iletmesine sebep olacaktır. Çalışmada kısmi başarı elde edilmiş olup bu alanda ilerlemeler olabileceği gösterilmiştir. Bu bilgiler ışığında, sahte BTS saldırılarının anlaşılması için beklenmedik LAI değişikliklerinin takip edilmesi gerektiği anlaşılmaktadır. [9] numaralı çalışmada, GSM protokolünü hedef alan gerçek zamanlı detektör sistemi geliştirilmiştir. [3]'de olduğu gibi bu çalışmada da ilgili GSM protokolü analiz edilmiştir. Geliştirilen detektör sistemi üç parçadan oluşmaktadır. Birinci parça, önceki çalışmada geliştirilen "GSM MT detektörü" [3], ikincisi lokal veri tabanı, üçüncüsü ise seçici yakalama cihazıdır. Çalışmayla, belirli bir bölge içinde kalan MT'ler "GSM MT Detektörü" ile tespit edilmekte ve tespit edilen MT kimlikleri lokal veri tabanında toplanmaktadır. Sonrasında ise, MT'ler lokal veri tabanından kontrol edilerek seçici olarak engellenip bırakıla bilinmektedir. Bu çalışma ile ilk çalışma daha etkin kullanılmış olup [3], söz konusu çalışma ürünleştirilmeye çalışılmıştır. Yapılan çalışmalarda hedef MT'lerin sadece bir kısmı saldırının etkisine girmiş olup, saldırının etki etme süresinin gerçek ortamda kullanılamayacak kadar uzun olduğu değerlendirilmektedir. [10] ve [11] numaralı çalışmalarda, yazılımsal radyo teknolojisi (software radio technologies - SDR) kullanılarak sahte BTS geliştirilmiştir. Bu çalışmada önceki iki çalışmanın aksine sahte BTS geliştirilirken, gerçek BTS'ler sinyal bozucu ile engellenmemiştir [3], [9]. Ayrıca, sahte BTS geliştirilirken farklı bir yaklaşım ve yazılımsal radyo teknolojisi kullanılması hem masrafları düşürmüş hem de performansı önemli oranda artırmıştır. Yapılan çalışmalarda GSM protokolü detaylı olarak incelenmiş, protokolün açıkları geliştirilen yazılım ve donanımlarla manipüle edilerek son kullanıcıya hitap edebilecek performansta bir ürün ortaya konulmuştur. Yine [10] ve [11]'de bir tane mühendislik modu aktif olan MT kullanılmıştır. Söz konusu MT ile çevredeki aktif BTS'lere ait verilere erişilmektedir. 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 olası bir devir durumunda, MT'yi

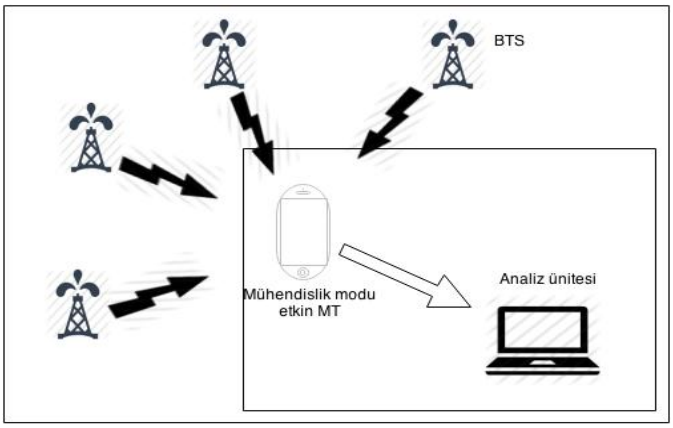
yönlendirmek amaçlı, BCH'dan (Broadcast Channel) yayınlamalarıdır. Böylece MT'ler tereddüt etmeden sahte BTS'e bağlanmaktadır. Sahte BTS, taklit ettiği BTS'in MCC (Mobile Country Code) ve MNC (Mobile Network Code) gibi GSM operatörlerine ait olan bilgilerini de taklit etmelidir. Bununla birlikte, MT'nin 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'ını (Broadcast Control Channel) 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 kullanılarak MT'lerde lokasyon güncelleme prosedürü tetiklenebilmiştir. Sonuç olarak, sahte BTS saldırılarının tespit edilebilmesi için sıra dışı *C2* değerleri önemli bir gösterge olacağı, ayrıca zayıf olan BTS'in beklenmedik şekilde seçilmesine de dikkat edilmesi gerektiği anlaşılmıştır. [12] ve [13] numaralı çalışmalarda kriz ve acil durum yönetim faaliyetleri kapsamında felaket bölgesinde insanların varlığını, sayısını ve yerlerini tespit etmek için "IMSI Catcher" cihazının kullanılması önerilmiştir. GSM standartlarına göre MT'ler kendilerini BTS'lere tanıtmak zorunda olup BTS'lerin ise kendilerini MT'lere tanıtması gerekmemektedir. Bu çalışmada kullanılan "IMSI Catcher" cihazı bu güvenlik açığından yararlanarak MT'lerin kendine bağlanmasını zorlamaktadır. Yani, geliştirme aşamasında olan [12] ve [13] numaralı çalışmalarda "IMSI Catcher" cihazı ile kriz ve acil durum yönetimi faaliyetlerinde yardım ve kurtarma çalışmalarının etkinliğinin artırılması hedeflenmektedir. [14] numaralı çalışmada sahte baz istasyonu saldırıları analiz edilmiştir ve bu saldırıların tespit edilmesine yönelik bir algoritma geliştirilmiştir. Hâlihazırda İnternet üzerinden sahte BTS saldırısı yapan cihaz "IMSI Catcher" adı altında satılmaktadır. Septier firmasının web sayfasında el tipi ve standart cihazlar satışa sunulmaktadır. Söz konusu cihazların spesifikasyonları incelendiğinde, cihazların 3G ağında çalışamadığı için cihazın bulunduğu ortamdaki 3G BTS'leri sinyal bozucu ile bastırıp MT'leri 2G kullanmaya zorladığı, sonrasında da mevcut saldırı cihazı kullanılarak ortamdaki MT'lere ait IMSI numaralarının toplanabildiği öğrenilmiştir. 3G ağında 2G'de bulunan karşılıklı doğrulama eksikliği kapatıldığından bu cihazların 3G'de çalışmaması beklenen bir durum olup ortamdaki 3G BTS'lerin sinyal bozucu kullanılarak bastırılmış olması sahte BTS saldırısı hususunda algoritma için belirleyici unsurlardan birisi olacaktır [15]. İnternet ortamında başlangıç aşamasında sahte BTS saldırılarının tespit edilmesine yönelik bazı çalışmalara rastlanmıştır. Bunlar arasında en gelişmiş olanlar SnoopSnitch [16] ve AIMSICD [17] isimli ANDROID uygulamalarıdır. SnoopSnitch güvensiz ağ ve sahte GSM baz istasyonu, kullanıcı izleme/dinleme, SS7 saldırıları gibi mobil tehditler hakkında BT'leri uyarmak için mobil radyo verilerini analiz etmektedir. AIMSICD ise BTS bilgi tutarlılığını, LAC/hücre kimliği tutarlılığını ve komşu hücre bilgisini kontrol ederek, sinyal kuvvetini izleyerek, vb. yöntemlerle sahte "IMSI Catcher" cihazlarını tespit etmeyi hedeflemektedir. Geliştirme aşaması devam eden bu uygulamalar sınırlı kullanım altyapısına sahiptir, İnternet ortamında erişilen bilgilerin dışında bu uygulamalarda kullanılan yöntemlere ait akademik çalışmalara rastlanmamıştır. Sahte BTS saldırı tespit algoritması yukarıdaki belirtilen yaklaşımlar göz önünde bulundurularak geliştirilmiştir.

3. SAHTE GSM BAZ İSTASYONU SALDIRI TESPİT ALGORİTMASI (FAKE BASE STATION ATTACK DETECTION ALGORITHM)

Bu çalışma ile GSM protokolü incelenmiş, sahte BTS saldırıları analiz edilmiş, [20] numaralı çalışmada önerilen algoritma iyileştirilmiş ve uygulaması yapılmış olup, çalışmanın sahte BTS saldırılarının tespiti alanına katkı sağlayacağı düşünülmektedir.

3.1 Sistem Mimarisi (System Architecture)

Sahte BTS saldırılarının tespitine yönelik önerilen sistem mimarisi Şekil 1'de sunulmaktadır. Şekildeki mühendislik modu etkin olan MT, kendi bölgesindeki aktif BTS'leri tespit edip, Cell ID, MCC, MNC, LAI gibi BTS'ler ile alakalı bilgileri almak için erişim alanındaki BTS'lerin BCCH'ını okumaktadır. Söz konusu MT, BTS'lerden topladığı bilgileri "Analiz ünitesine" yollamaktadır. Ek olarak, MT BTS'lerden okuduğu bilgileri kullanarak otomatik olarak hesapladığı *C1* (path loss criterion) ve *C2* (cell reselection criterion) parametrelerini de analiz ünitesine göndermektedir. Geliştirilen algoritmayı çalıştırabilecek herhangi bir PC veya akıllı telefon analiz ünitesi olarak kullanılabilmektedir. Analiz ünitesi, MT'nin gönderdiği verileri sahte BTS saldırı tespit algoritmasına göre değerlendirip, şüpheli durumları kullanıcıya raporlamaktadır. Mühendislik modu etkin MT ile analiz ünitesinin bağlantı şekilleri ve bulunduğu fiziksel konumlar ihtiyaçlara göre değiştirilerek daha esnek mimariler oluşturmak mümkün olabilecektir. Bu kapsamda mevcut mimariye alternatif olarak merkezi bir analiz ünitesi kurulup, GSM bilgilerini toplayan MT'ler, İnternet üzerinden bilgileri merkezi analiz ünitesine gönderip, sonuçlarını alabileceği mimarilerin kullanımı da imkân dâhilindedir. Ayrıca GSM bilgilerini toplayan

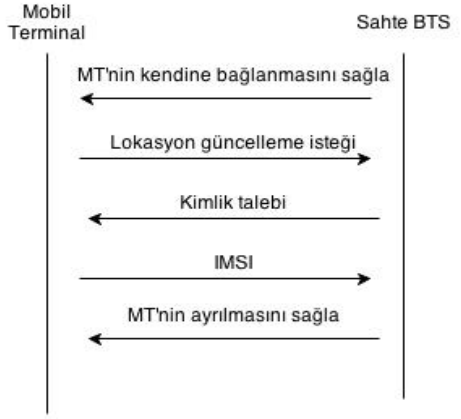


Şekil 1. Sistem Mimarisi (System Architecture)

MT ile analiz ünitesini uygun bir donanım kullanarak tek bir platformda toplayıp, sonuçları hızlı bir şekilde analiz eden mobil bir sistem kurulumu da söz konusu saldırıların tespitini oldukça kolaylaştıracaktır.

3.2 Protokol Analizi (Protocol Analysis)

Sahte BTS saldırıları ortadaki adam saldırılarının tipik örneklerindendir. Söz konusu saldırı türünün çeşitli varyasyonları olmasına rağmen hepsinin ortak noktası MT'lerle BTS arasına girilmesi ve MT'lerin IMSI/IMEI numaralarının ele geçirilerek hedeflerin tanınmasıdır. Temel bir sahte BTS saldırısı Şekil 2'deki gibi gerçekleşmektedir. MT'lerin sahte BTS ile kimliğinin ele geçirilmesi lokasyon güncelleme sürecinin tetiklenmesi ile yapılabilmektedir [10], [11]. İkinci bölümde ve ilgili GSM spesifikasyonlarında açıklandığı üzere, lokasyon güncellemesinin tetiklenebilmesi için birçok yöntem bulunmaktadır [18]. Telefonda saklanan son kayıtlı lokasyon verisine, GSM operatörü tarafından belirlenen zamanlayıcının süresine ve MT kullanıcısının çağrı başlangıç ve bitişine müdahale edilemediğinden, sahte BTS'ler kendilerini başka bir lokasyon bölgesinden göstererek lokasyon güncelleme sürecini tetikleyip kullanıcının kimlik bilgilerine ulaşabilmektedirler [10], [11].



Şekil 2. Örnek Sahte BTS Saldırısı (Sample Fake BTS Attack)

Şekil 2'de de görüldüğü gibi, Sahte BTS saldırısı yapmak için öncelikle MT ile GSM ağı arasına sahte BTS kullanarak girilmesi gerekmektedir. Önceki çalışmalarda sinyal bozucu sistemler kullanılmış ve MT için bağlanmaya aday GSM baz istasyonlarını bastırarak, MT'nin sahte BTS'i seçmesi beklenmiştir [3], [9]. Fakat bu sistemlerde her BTS için ayrı bir sinyal bozucu ünite gerekmekte ve sinyal bozucunun zamanlamasını ayarlarken zorluklarla karşılaşılmaktadır. Literatürdeki son makalelerde ise *C1* ve *C2* parametresinin manipüle edilerek kullanılması yöntemi seçilmiş ve bu yöntem hem masrafı düşürmüş hem de performansı önemli ölçüde artırmıştır [10]. [11] ve [19]'e göre *C1* parametresi hücre seçiminde kullanılmakta ve aşağıdaki gibi hesaplanmaktadır.

$$C1 = (A - Max(B, 0)) \quad (1)$$

$$A = RLA_C - RXLEV_ACCESS_MIN \quad (2)$$

$$B = MS_TXPWR_MAX_CCH - P \quad (3)$$

GSM 'in 1800 MHz'de çalışan ilk türevi 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, *P* ise MT'nin maksimum RF güç çıkışıdır. Bütün değerler dBm formatındadır ve yukarıdaki tanıma göre, *C1* değeri MS ve BTS arasındaki mesafe ile ters orantılıdır. *C2* parametresi ise *C1* parametresi ile beraber hücre seçimi için kullanılmakta ve aşağıdaki gibi tanımlanmaktadır.

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 zamanlayıcı olup, *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 yaklaşık olarak *C2=C1* olur. Türkiye'nin Ankara ilinde yapılan testlerde, test edilen BTS'ler için GSM protokolüne de uygun şekilde Eş. (10)'da belirtilen ilişki gözlemlenmiştir.

$$|C2 - C1| \leq 4 \quad (10)$$

Eşitlikte gözüken hata payı anlık olmakta ve hemen eşitlenmekle birlikte, hava arayüzü aracılığıyla yayınlanan değerlerin iletim ortamı kaynaklı bozulması olarak değerlendirilmektedir.

Yukarıdaki hesaplamalara ve GSM protokolünün ilgili kısımlarına göre BTS'ler arasında öncelik tanımak için söz konusu opsiyonel parametreler kullanılmaktadır [20]. 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 (Algorithm Design)

Şekil 3'de sahte BTS tespit algoritmasının akış şeması verilmektedir. Algoritma sıra dışı durumlarla karşılaştığında üç tür rapor üretmektedir. Birinci rapor "Kırmızı Alarm" uyarısı, ikinci rapor "Sarı Alarm" uyarısı ve üçüncü rapor ise "Yeşil Alarm" uyarısıdır. MT'in sahte BTS'e yakalanma durumu "Kırmızı Alarm", "Sarı Alarm" ve "Yeşil Alarm" ile en tehlikeliden tehlikesize doğru sıralanmıştır. Algoritmada karar verilmesini sağlayan 9 ana adım bulunmaktadır. Şekil 3'de gösterilen sahte BTS saldırı tespit algoritmasında da işaretlenen bu adımlar aşağıda detaylandırılmıştır.

1. Mühendislik modu etkin olan MT GSM ağ değerlerini okumaya başlar.

2. Cell ID, MCC, MNC, LAC, hizmet veren ve komşu hücreler gibi GSM ağ değerleri ve GSM ağ değerlerinden hesaplanmış *C1* ve *C2* parametreleri analiz ünitesine gönderilir.

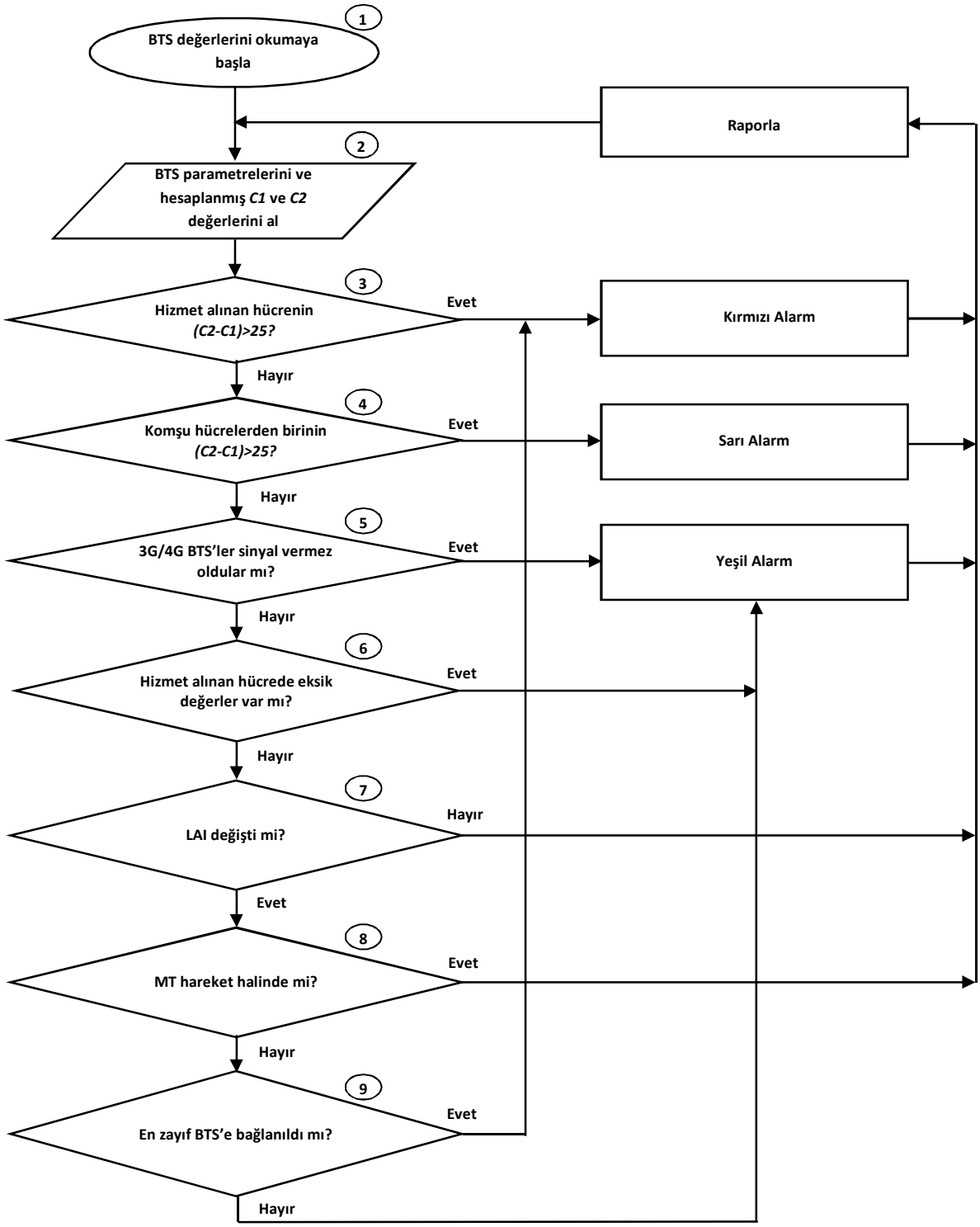
3. Önceki bölümlerde açıklandığı gibi *C2*, ofset parametreleri değiştirilerek hücre seçimini etkilemek için kullanılabilmektedir. MT'nin BTS'e uzaklığını gösteren *C1* parametresi yüksek olmasa bile, yani sahte BTS hedef MT'ye en yakın BTS olmasa bile sahte BTS, *C2* değerini manipüle ederek MT'lerin kendine bağlanmasını sağlayabilmektedir. Önceki bölümlerde de bahsedildiği gibi sıra dışı bir durum olmadığında *C1* ve *C2* parametreleri yaklaşık olarak birbirine eşit çıkmaktadır. Bundan dolayı hizmet alınan hücrenin *C2* ve *C1* değerleri arasındaki farkın 25'ten büyük olması MT'nin sahte BTS'e yakalandığını göstermekte ve "Kırmızı Alarm" raporu üretilmektedir. 25 değeri hava ara yüzünde yaşanması muhtemel bozulmaları ve hatalı-pozitif (false-positive) sonuçları elemek için deneysel olarak seçilmiştir.

4. Bu adım, küçük bir farkla üçüncü adımla aynı mantığa dayanmaktadır. Üçüncü adımda hizmet veren hücreye bakılırken bu adımda komşu hücrelere bakılmaktadır. Komşu hücrelerden birinin *C2* ve *C1* değerleri arasındaki farkın 25'ten büyük olması ortamda sahte BTS olduğunu göstermekte ve "Sarı Alarm" raporu üretilmektedir.

5. İkinci bölümde de anlatıldığı gibi 3G ile birlikte karşılıklı doğrulama özelliği getirilmiş ve mevcut sahte BTS benzeri cihazlar çalışmaz olmuşlardır. Bu nedenle saldırganlar 3G BTS'leri sinyal bozucu ile bastırıp, MT'yi GSM kullanmaya zorlamaktadırlar. Bu nedenle ortamdaki 3G BTS'lerin kaybolup 2G BTS'lerin bulunmaya devam etmesi MT'nin sahte BTS'e yakalanma riskinin bulunduğunu göstermekte ve "Yeşil Alarm" raporu üretilmektedir.

6. Önceki bölümlerde aktarıldığı gibi BTS'ler kendisini tanıtan bazı değerleri BCH'dan yayınlayacak şekilde yapılandırılmaktadır. Bu değerler arasında Cell ID, MCC, MNC, LAI ve komşu hücrelere ait bilgiler bulunmaktadır. Söz konusu bilgilerden bazılarının eksik olması MT'nin sahte BTS'e yakalanma riskinin bulunduğunu göstermekte ve "Yeşil Alarm" raporu üretilmektedir.

7. LAI değişikliği MT'nin kimliğinin tespit edilmesi için gereklidir. MT'nin LAI bilgisi değişmediyse geliştirilen algoritma mevcut hataların en kritiğini kullanıcıya bildirip, sonuca vardığı tüm uyarıları



Şekil 3. Sahte BTS Saldırı Tespit Algoritması (Fake BTS Attack Detection Algorithm)

detaylı olarak raporlamalıdır. Sonrasında ise algoritma birinci adımdan tekrar başlamalıdır. Eğer LAI bilgisi değiştiyse, inceleme devam etmelidir.

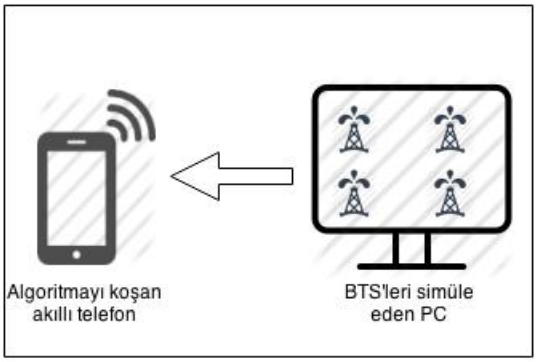
8. MT'nin hareket halinde olması ile bir lokasyon bölgesinden çıkılıp diğerine girilme ihtimali olduğundan kesin bir sonuca varılması mümkün değildir bu nedenle bir önceki adımdaki gibi algoritma mevcut hataların en kritiğini kullanıcıya bildirip, sonuca vardığı tüm uyarıları detaylı olarak raporlamalıdır. Sonrasında ise algoritma birinci adımdan tekrar başlamalıdır. Eğer MT sabitken LAI değişiyorsa şüpheli durum devam etmekte ve incelemeye devam edilmelidir.

9. MT'nin LAI bilgisinin değişimi ancak yeni bir BTS'e bağlanılması ile oluşabilmektedir. Son bağlanılan BTS'in komşu BTS'ler listesinde en zayıf

BTS olması MT'nin sahte BTS'e yakalandığını göstermekte ve "Kırmızı Alarm" raporu üretilmektedir. Son bağlanılan BTS'in komşu BTS'ler listesinde en zayıf BTS olmaması MT'nin sahte BTS'e yakalanma riskinin bulunduğunu göstermekte ve "Yeşil Alarm" raporu üretilmektedir.

4. GELİŞTİRİLEN ALGORİTMANIN SİMÜLASYONU (SIMULATION OF DEVELOPED ALGORITHM)

Bu bölümde geliştirilen algoritmanın gerçek verileri kullanan simülasyonu yapılmıştır. Üçüncü bölümde verilen sistem mimarisinin iki ana öğesi bulunmaktadır. Bunlar GSM sinyallerini analiz eden mühendislik modu etkin test telefonu ve analiz ünitesidir. Bu kapsamda BTS'leri simüle etmek için kullanılan PC Windows 7 işletim sistemine ve Intel Core2 Duo işlemciye sahiptir. Simülasyon yazılımı ise Java ile geliştirilmiştir. Şekil 3'de gösterilen algoritma ANDROID 4.4.2 sürümüne sahip Google Nexus 4 model akıllı telefonda koşmaktadır. PC ile akıllı telefon arasındaki veri aktarımı geliştirilen protokol üzerinden yapılmakta ve aralarındaki bağlantı ise Wi-Fi Hotspot teknolojisi kullanılarak sağlanmaktadır. Bağlantı şekli, kullanılması planlanan mimariye göre değiştirilebilmektedir. Simülasyon için seçilen mimari Şekil 4'de sunulmaktadır.



Şekil 4. Simülasyon Mimarisi (Simulation Architecture)

GSM verilerine yazılımsal yöntemlerle ulaşmak için hazır satılan ürünler bulunmaktadır. Ayrıca hâlihazırda günlük hayatta kullandığımız telefonlardan bazıları ile de söz konusu bilgilerin bir kısmına erişile bilinmektedir. Bu kapsamda Samsung, Apple, Nokia ve HTC marka telefonlardan bazı modeller incelenmiştir. İncelenen modellerden bir kısmı, GSM verilerinin sadece bir kısmını API ile kullanıcıya sunabilmektedirler. Örneğin ANDROID işletim sistemi kullanan akıllı telefonlar ve Telephony Manager API'si kullanılarak bağlı bulunan hücrenin Cell ID bilgisi, hücrenin sinyal seviyesi gibi bilgilere yazılımsal olarak erişilmekte ancak telefon tarafından hesaplanan *C1* ve *C2* değerleri gibi bilgilere ulaşılamamaktadır. İncelenen telefonlarda değişik isimlerde, değişik yöntemlerle ulaşılabilen mühendislik ekranları bulunmakta ve bu ekranlar aracılığıyla da bir kısım bilgilere görsel olarak ulaşılmaktadır. Ulaşılan bilgiler markadan markaya ve telefondan telefona değişebilmekte olup, incelenen telefonlar arasında Nokia N95 üzerinde çalışan FieldTest yazılımı ile en fazla veriye ulaşılabildiği gözlemlenmiştir. Söz konusu yazılım Ankara ilinin çeşitli bölgelerinde Vodafone ve Turkcell operatörlerine ait BTS verilerine erişmek için çalıştırılmış ve Ankara'nın Macunköy semtinden elde edilen örnek BTS verileri Tablo 1'de sunulmuştur. Tablo 1'de ilgili hücreye ait Operatör bilgileri, *C1* ve *C2* parametreleri ve komşu hücrelerinden 3 tanesine ait bilgiler bulunmaktadır. Geliştirilen algoritma FieldTest uygulamasından elde edilen verilerle çalıştırılmış olup, algoritmanın test edilebilmesi için saldırı içerikli BTS verileri de üretilip sistemde kullanılmıştır. Algoritmayı çalıştıran ANDROID uygulaması periyodik olarak dakikada bir 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 uyarı olarak gösterip diğerlerini de bilgi olarak detay kısmında raporlamaktadır. Her döngüde önce simüle edilen BTS verileri okunmakta, sonrasında akıllı telefonun GPS modülü kullanılarak lokasyon değişikliği ve ortalama hız hesaplanmaktadır. Ayrıca okunan bu değerlerden bazıları bir sonraki döngü için saklanmakta ve güncel döngü verileri ile beraber değerlendirilip sonuç üretilmektedir. MT'nin hareket halinde olup olmadığının tespiti algoritmanın 8. basamağında kullanılmaktadır. Bu bilgiye MT'nin GPS modülü kullanılarak ulaşılmaktadır. İki döngü arasındaki ortalama hız hesaplanıp 10 km/s hızın altındaysa MT hareket etmiyor kabul edilmektedir. Eğer akıllı telefon kapalı alanda bulunup GPS uydularına erişilememesi gibi bir sebeple konum

Tablo 1. Örnek BTS verileri (Sample BTS data)

Cell ID	MCC	MNC	LAI	C1	C2	NCEll_1	NCEll_2	NCEll_3	Operatör
22239	286	02	50637	38	38	22238	22236	22007	Vodafone
22238	286	02	50637	35	35	22239	22236	22214	Vodafone
22236	286	02	50637	34	34	22239	22238	22214	Vodafone
37430	286	01	31706	47	47	46156	23574	8550	Turkcell
46156	286	01	31706	41	40	37430	23574	8550	Turkcell
23574	286	01	31706	38	38	37430	46156	8550	Turkcell

bilgisine erişemeyip ortalama hız hesaplanamıyorsa, MT hareket halinde kabul edilmektedir. Algoritmadaki beşinci adımı için bir önceki döngüde en az 2 tane 3G BTS'den sinyal alınmamışsa ilgili koşul değerlendirme dışı kalacaktır aksi halde kırsal alanlarda kapsama alanında olan BTS sayısı oldukça kısıtlı olduğundan yanlış-alarm (false-positive) oranının artması kaçınılmazdır. Algoritmanın 6. koşulu için ise sadece MCC, MNC ve komşu hücre listesi değerlerine bakılmış olup, MCC ve MNC bilgilerinin hizmet alınan operatörle uyumlu, komşu hücre listesi bilgilerinde ise en az iki tane komşu hücre bilgisinin yer alması beklenmiştir.

5. SONUÇLAR (CONCLUSIONS)

GSM'in yaygın kullanımına rağmen GSM'de bir takım güvenlik açıkları bulunmaktadır. Çalışmada GSM mimarisi analiz edilmiş olup karşılıklı doğrulama açığının neden olduğu güvenlik açıkları detaylandırılmıştır. Ayrıca söz konusu açıkları kullanan saldırılar incelenmiş ve saldırıların tespit edilmesi için algoritma geliştirilip simülasyon üzerinde test edilerek saldırıların tespit edilebilirliği gösterilmiştir. Bununla birlikte, Tablo 1'de verilen GSM değerleri ve FieldTest uygulaması ile elde edilen diğer verilerle yapılan testlerde herhangi bir Sahte BTS saldırısının yer almadığı tespit edilmiştir. Çalışmanın geleceği adına söz konusu cihazın simülasyon yerine sahte BTS cihazı ile test edilmesi ve GSM için yapılan güvenlik ve risk analizlerinin 3G ve 4G gibi mobil iletişim ağları için de yapılması çalışmanın bir sonraki adımı olarak planlanmıştır.

KISALTMALAR (ABBREVIATIONS)

API Application Programming Interface (Uygulama Programlama Arayüzü)
BCCH Broadcast Control Channel (Yayın Kontrol Kanalı)
BCH Broadcast Channel (Yayın Kanalı)
BTS Base Transceiver Station (Baz İstasyonu)
Cell ID Cell Identity (Hücre Kimlik Numarası)
C1 Path Loss Criterion Parameter (Hücre Seçim Parametresi)
C2 Cell Reselection Criterion Parameter (Hücre Yeniden Seçim Parametresi)
DCS Digital Cellular System (Dijital Hücresel Sistem)
GPS Global Positioning System (Küresel Konumlama Sistemi)
GSM Global System for Mobile Communication (Mobil İletişim için Küresel Sistem)
IMEI International Mobile Station Equipment Identity (Uluslararası Mobil Cihaz Kimliği)
IMSI International Mobile Subscriber Identity (Uluslararası Mobil Abone Kimliği)
ITU International Telecommunication Union (Uluslararası Telekomünikasyon Birliği)
LAI Location Area Identifier (Lokasyon Alanı Değeri)
LAC Location Area Code (Lokasyon Alanı Kodu)
MCC Mobile Country Code (Mobil Ülke Kodu)
MNC Mobile Network Code (Mobil Operatör Kodu)
MT Mobile Terminal/Station (Mobil Terminal)
RF Radio Frequency (Radyo Frekansı)
PC Personal Computer (Kişisel Bilgisayar)
SDR Software Radio Technologies (Yazılımsal Radyo Teknolojisi)
2G/3G/4G Second/Third/Fourth Generation (İkinci/Üçüncü/Dördüncü Jenerasyon)

KAYNAKLAR (REFERENCES)

1. İnternet: GSM, http://en.wikipedia.org/wiki/GSM, 2015.
2. Broek, F.V.D., "Eavesdropping on GSM: State-of-affairs", **5th Benelux Workshop on Information and System Security (WISSec)**, Radboud University, Nijmegen, 1-16, Kasım 2010.
3. 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.**, Cilt 5, 275–276, 2001.
4. Ntantigian, C. ve Xenakis, C., "Questioning the Feasibility of UMTS-GSM Interworking Attacks", **Wireless Pers Commun,** Cilt 65, 157–163, 2011.
5. Ahmadian, Z., Salimi, S. ve Salahi, A., "Security Enhancements Against UMTS-GSM Interworking Attacks", **Computer Networks**, Cilt 54, 2256-2270, 2010.
6. Kalenderi, M., Pnevmatikatos, D., Papaefstathiou, I. ve Manifavas, C., "Breaking the GSM A5/1 Cryptography Algorithm with Rainbow Tables and High-end FPGAS", **22nd Field Programmable Logic and Applications (FPL) Conference**, University of Oslo, Oslo, 747-753, 29-31 Ağustos 2012.
7. İnternet: The NSA'S Secret Role in the U.S. Assassination Program, https://theintercept.com/2014/02/10/the-nsas-secret-role/, 2015.
8. Pousada-Carballo, J.M., González-Castaño, F. J., Vicente, F. I. ve Fernández-Iglesias M.J., "Jamming System for Mobile Communications", **Electron. Lett.** Cilt 34, 2166–2167, 1998.
9. González-Castaño, J.F., Vales-Alonso, J.J., Pousada-Carballo, M., Isasi de Vicente, F. ve Fernández-Iglesias, M.J., "Real-Time Interception Systems for the GSM Protocol", **IEEE Transactions on Vehicular Technology**, Cilt 51, No 5, 904-914, 2002.
10. 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), Chengdu City, China, 1-4, 23-25 Eylül 2010.

11. Song, Y., Zhou, K ve Chen, X., "Fake BTS Attacks of GSM System on Software Radio Platform", **Journal of Networks**, Cilt 7, No 2, 275-281, 2012.

12. Řezník, T., Horáková, B., ve Janiurek, D., "Emergency Support System: Actionable Real-time Intelligence with Fusion Capabilities and Cartographic Displays", **AiMT: Advances in Military Technology**, Cilt 6, No 2, 83-97, 2011

13. Řezník, T., Horáková, B., ve Szturc, R., "Advanced Methods of Cell Phone Localization for Crisis and Emergency Management Applications", **International Journal of Digital Earth**, Cilt 8, No 4, 259–272, 2015.

14. Çelik, Ö. F., Samet, R., "Sahte Baz İstasyonu Saldırı Tespit Algoritması", **ISCTurkey 2014**, 7. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı bildiri kitabı, İstanbul, Türkiye, 37-42, 17-18 Ekim 2014.

15. İnternet: Septier Communication, http://www.septier.com, 2015.

16. İnternet: SnoopSnitch, https://opensource.srlabs.de/projects/snoopsnitch, 2015.

17. İnternet: Android IMSI-Catcher Detector, https://secupwn.github.io/Android-IMSI-Catcher-Detector/, 2015.

18. ETSI, "European Digital Cellular Telecommunications System Phase", **Location Registration Procedures**, GSM 03.12-DCS Version 3.0.1 Release 1992.

19. 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), 1999.

20. 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, 1998.