# NEDEN 3G KABLOSUZ HABERLEŞMEYE GEÇİLMELİ

**Fatma AKGÜN[1], Ercan BULUŞ[2]**
[1]Trakya Üniversitesi Müh.-Mim. Fakültesi Bilgisayar Mühendisliği Bölümü, EDİRNE
[2]Namık Kemal Üniversitesi Çorlu Müh. Fakültesi Bilgisayar Mühendisliği Bölümü, TEKİRDAĞ
[1]fatmaakgun@trakya.edu.tr, [2]ercanbulus@corlu.edu.tr

## ABSTRACT

*Nowadays, in communication systems, the usage of wireless network has increased by the popularity of studies on wireless networks. Because of this increase, some security problems have arised. In this study, communication systems from the first system, which is called Analog system to wireless network systems, have been classified. In the following section, the structure of widely used second generation wireless communication system called GSM and the encryption and authentication algorithms used in this system have been explained. In our study, the third generation communication system which is recently used has been detailed and advantages of security of the third generation communication system against the GSM have been explained. In conclusion, it has been seen that third generation communication system are faster and more secure than previous systems.*

**Key words:** *Wireless Communication, GSM, UMTS, authentication, encryption,, security.*

## 1. GİRİŞ

Teknoloji son yüzyıl içerisinde büyük atılım yapmıştır. İnsanoğlunun gereklerine uygun yardımcı alet ve araçların üretilmesi için gerekli bilgi ve yetenek, teknolojiyi ifade ettiğinden teknolojinin, bilimin uygulamacı yönü olduğu kabul görmektedir. Etrafımızdaki her şey artık insan yaşam standardını kolaylaştırmak için tasarlanmıştır. Bu gelişmelerin en önemlilerinden biri de haberleşmede yapılan büyük değişimlerdir. İlk analog sistemden bu yana, bilimde yapılan yenilikler ile kablosuz haberleşme teknolojisi sayısal bir iletişim sağlayarak haberleşmede güvenlik ve daha hızlı veri iletişimi ile dünyada büyük etki yaratmıştır. Kablosuz ağ iletişimi ile kullanıcıların zamandan ve mekândan bağımsız olarak, hareket özgürlüklerine sahip olabildikleri bir iletişim şekli sağlanmıştır.

## 2. HABERLEŞME SİSTEMLERİ

Haberleşme sistemi 1. nesil analog haberleşme, 2. nesil kablosuz haberleşme, 2.5. nesil kablosuz haberleşme, 3. nesil kablosuz haberleşme ve 4. nesil kablosuz haberleşme olmak üzere çeşitlere ayrılmaktadır.

### 2.1. Haberleşme Tipleri

#### 2.1.1 Birinci Nesil Haberleşme (1G)

Birinci nesil haberleşmede temel ses iletim hizmetinin sağlanmasına yönelik bir sistem geliştirmek amaçlanmıştır. Analog haberleşme sistemine dayalıdır. 1970-1990 yılları arasında büyük etki yaratmıştır. Amerika'da AMPS (Advanced Mobile Phone System), İngiltere'de TACS (Total Access Communication System) ve Avrupa'da NMT (Nordic Mobile Telephone) sistemleri kullanılmıştır.

#### 2.1.2 İkinci Nesil Kablosuz Haberleşme(2G)

Ses iletiminin analog sistemden sayısal sisteme geçmesi ile daha güvenilir ve hızlı veri aktarımı sağlanmıştır. Aktarımda çeşitli kriptografik uygulamalar kullanılmıştır. Avrupa'da GSM (Global System for Mobile Communication)[1], Japonya'da PDC (Personal Digital Cellular), Kuzey Amerika'da CDMA (Code Divison Multiple Access) kullanılmıştır.

#### 2.1.3 2.5G Kablosuz Haberleşme

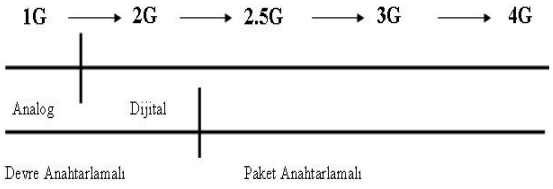
Veri iletim hızının artışı ve daha geniş bir kapsama alanına hizmet vermesi sağlanmıştır. Bu sayede 3G sistemlere öncelik olacak bir uygulama olmuştur. HSCSD (High Speed Circuit Switched Data), GPRS (General Packet Radio Service)[1] ve EDGE (Enhanced Data Rates for GSM Evolution) bu teknolojiyi kullanan sistemlerdir.

#### 2.1.4 Üçüncü Nesil Kablosuz Haberleşme (3G)

Yüksek hızlı kablosuz iletişim sistemi sağlamak ve mevcut olan tüm hücresel sistemleri tek bir yapı altında toplamak amaçlanmıştır.

#### 2.1.5 Dördüncü Nesil Kablosuz Haberleşeme (4G)

Yüksek mobilite, yüksek veri iletim hızı ve IP tabanlı karma ağ yapısı oluşturma amaçlanmaktadır. Gelecekte tamamen geçilmesi istenen sistemdir.

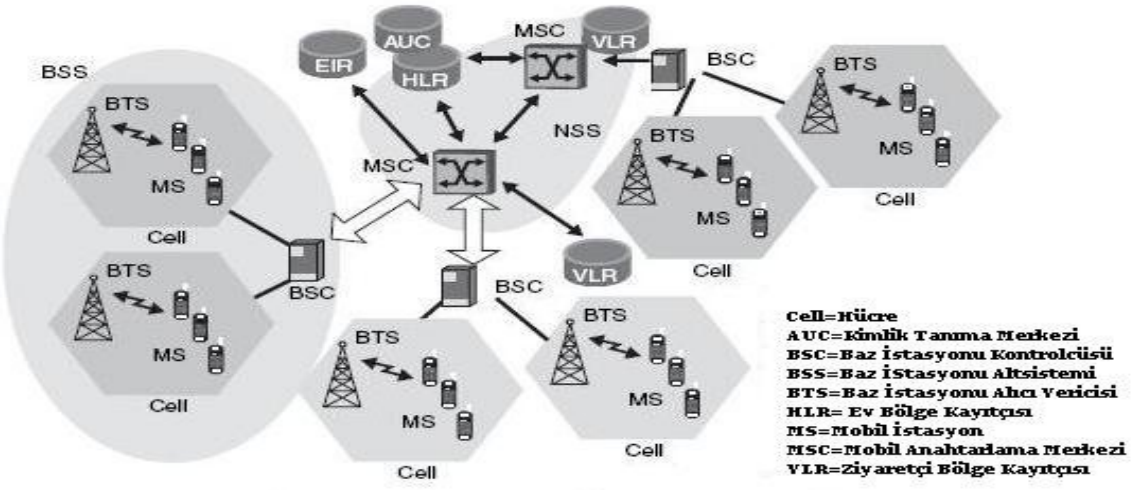



Şekil 1. Kablosuz Haberleşme Sistemleri Geçişi

## 3. İKİNCİ NESİL HABERLEŞME SİSTEMİ (GSM)

GSM bugün dünyada yoğun kullanılan mobil telefon sistemidir. Avrupa'da 1982 yılında 900 Mhz frekans hızında, "European Conference of Postal and Telecomunications-CEPT" tarafından geçiş sıkıntısı olmadan, sadece telefon içerisindeki kartı değiştirerek her yerden haberleşme sağlayabilen, çok güçlü hücresel bir teknoloji hayata geçirilmiştir. Bu konferansın ardından GSM haberleşme standartlarını belirlemek üzere 1989 yılında "European Telecommunications Standarts Institute-ETSI" kuruldu ve bu GSM haberleşme standardı olarak kabul edildi.

GSM haberleşme sistemi üç kısımdan oluşur. Mobil istasyon yani mobil cihaz ve içerisinde bulunan SIM (Subscriber Identity Module- Abone Kimlik Modülü) kart ilk kısım, baz istasyonu alt sistemi ikinci kısım ve mobil servis anahtarlama merkezi üçüncü kısım olmak üzere bir bütün halde işlem yapılmaktadır[2][3][4].

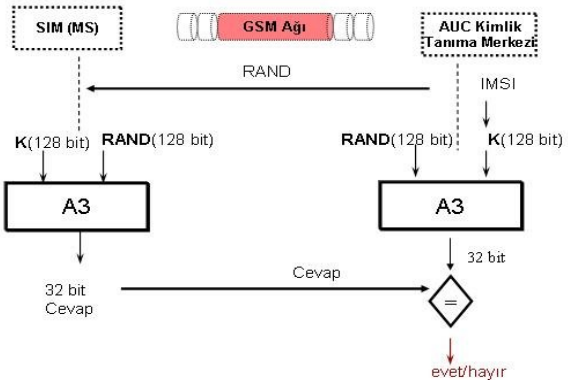



Şekil 2. GSM haberleşme yapısı[5]

GSM haberleşme sisteminde, iletişim sayısal olarak yapılabildiğinden, haberleşmede çeşitli kriptografik algoritmalar da uygulanabilmiştir. Kimlik tanımlama için A3 algoritması, şifreleme anahtarı üretimi için A8 algoritması ya da bazı ülkelerde A3/A8 yerine COMP128[6] algoritması ve ses/verinin şifrelenmesi için A5 algoritması kullanılmıştır.

### 3.1. Kimlik Tanıma Algoritması (A3)

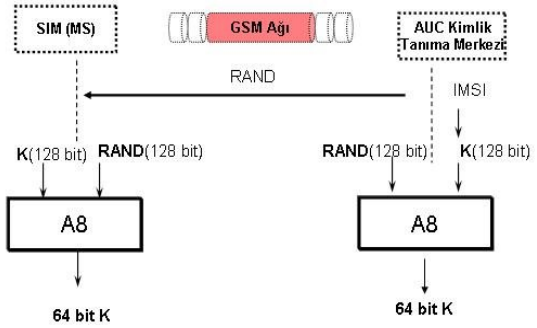
Öncelikle kullanıcının sistem tarafından kimlik tanımlama işleminden geçmesi gerekmektedir. Tek taraflı bir kimlik tanıma işlemi gerçekleşir. Sistem kullanıcıyı kimlik tanımadan geçirirken, kullanıcı sistemi kimlik tanıma işleminden geçirmez. SIM kartı içerisinde yer alan A3 algoritması, yine burada bulunan 128 bitlik gizli K anahtarını ve sistemden gelen RAND sayısı alarak, tek yönlü hash algoritmasına uyarlar ve sonuçta 32 bitlik SRES cevabını üretir. Kimlik tanımla merkezinde de bu işlemlerin aynısı gerçekleşir. Mobil anahtarlama merkezi, mobil istasyondan gelen cevap ile kimlik tanımla merkezinden gelen cevabı karşılaştırır. Eğer her iki değerde eşit ise kullanıcı yasal kullanıcıdır denir ve sisteme kabul edilir[7][8][9].




Şekil 3. A3 Kimlik Tanıma Algoritması [8]

### 3.2. Şifreleme Anahtarı Üretme Algoritması (A8)

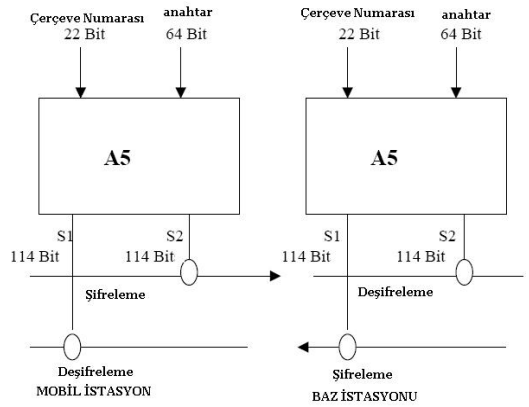
Bu algoritma, ses ve verinin şifrelenmesinde kullanılacak anahtarı üretme işlemini gerçekleştirir. Sim kart içerisinde yer alan bu algoritma, Mobil anahtarlama merkezinden gelen 128 bitlik RAND değeri ve kendinde bulunan 128 bitlik gizli K değerini alarak, tek yönlü hashing algoritmasına sokar ve 64 bitlik şifreleme anahtarını üretir[7][8][9].




Şekil 4. A8 Şifreleme Anahtarı Üretme Algoritması [8]

### 3.3. Ses ve Veri Şifreleme Algoritması (A5)

Hava kanalı üzerinden ses şifrelemede kullanılan güçlü bir şifreleme algoritmasıdır. Şifrelemede akış (stream) şifreleme algoritmalarını kullanır. Üç farklı uzunlukta yazaç kullanılır. Şifreleme işlemine, 64 bitlik oturum anahtarı (K) ve 22 bitlik çerçeve numarası ($F_n$) ile başlatılır. A5 algoritmasının, A5/0, A5/1, A5/2 ve A5/3 olmak üzere çeşitli türleri bulunmaktadır[10][11].

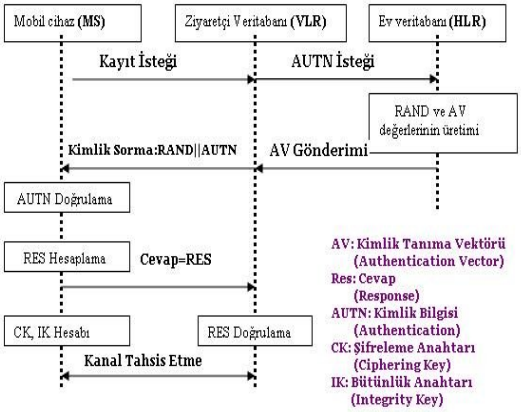



Şekil 5. A5 Şifreleme Algoritması[12]

## 4. ÜÇÜNCÜ NESİL HABERLEŞME SİSTEMİ (UMTS)

UMTS (Univesal Mobil Telephone System), GSM'in gelişmiş bir halidir. 3.nesil (3G) bir haberleşme sistemidir. Geniş bandlı çoklu ortam (ses, resim ve video aktarımı) servislerinin kullanılmasına olanak sağlayarak yüksek bit hızlarını desteklemektedir. UMTS içindeki güvenlik 128 bit şifreleme anahtar uzunluğu ile daha güçlü şifreleme algoritması ve karşılıklı kimlik doğrulaması gibi artı işlemleri kapsar. UMTS, AKA (Authentication and Key Agreement) protokol kullanarak, ağ erişim güvenliği sağlar. AKA protokolü GSM içinde gelişen ve sabit güvenlik metodları ile geliştirilmiştir. AKA karşılıklı kimlik tanıma yani her iki kısmında bir diğerinin kimliğini tanıma gibi GSM'e oranla ek güvenlik sağlar[13].

Kimlik tanıma işleminde 3 adet varlığa ihtiyaç vardır. Bunlar, kullanıcı yani mobil cihaz veya USIM (User Subscriber Identity Module), servis ağı VLR (Visitor Location Register) ve ev ortamı AUC/HLR (Authenticatiın Center/Home Location Register). Servis ağı kullanıcı ile bağlantı kuran gerçek bir ağdır. Ev ortamı, kullanıcının orijinal abone olduğu ağdır ve kimlik tanıma işleminde başlıca rol oynar.




Şekil 6. 3G içindeki AKA Protokolü[14]

AV (Authentication Vector), ev ağından ziyaretçi ağına gönderilen ve kimlik tanıma bilgilerini içeren bir bilgi kümesidir. RAND (Random Number-Rastgele Sayı), CK, IK, XRES, AUTN gibi önemli bilgilere sahiptir. Her birinin üretiminde farklı bir f fonksiyonları ve USIM/AUC içinde yer alan 128 bitlik gizli K anahtarı kullanılır.

$$RAND=\mathbf{f_0}(\text{internal state}) \quad (14)$$

Elde edilen bu RAND değeri, diğer bilgilerin elde edilmesi için tüm fonksiyonlara giriş olarak kullanılır.

$$XRES=\mathbf{f_2}(K,RAND) \quad (14)$$

$$CK=\mathbf{f_3}(K,RAND) \quad (14)$$

$$IK=\mathbf{f_4}(K,RAND) \quad (14)$$

$$AUTN=SQN\mathbf{[XOR]}AK||AMF||MAC \quad (14)$$

$$MAC=\mathbf{f_1}(K, SQN||RAND||AMF) \quad (14)$$

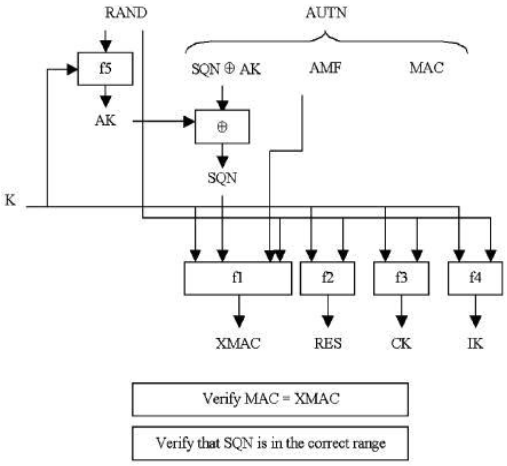
$$AK=\mathbf{f_5}(K,RAND) \quad (14)$$

Oturumun sonlanması için gerekli olan 128 bitlik CK ve IK şifreleme ve bütünlük anahtarlarıdır. AUTN içindeki SQN numarası sürekli güncellenerek against replay attack'larından korunmayı sağlar. AMF bilgi alanıdır. AK (Anonymity Key) SQN'in serilerini gözlemleyerek,

kimlik tanıma izini saklamak için SQN ile XOR'lanır. USIM, RAND, AUTN ve $f_1,f_2,f_3,f_4,f_5$ ile ilk SQN değerini hesaplar.

$$SQN=(SQN\textbf{[XOR]}AK)\textbf{[XOR]}f_5(K,RAND) \quad (14)$$

Ev ağı içinde üretilen AUTN değerindeki MAC (Message Authentication Code) değeri ile USIM içinde hesaplanan XMAC (Verify MAC) değeri, USIM içerisinde karşılaştırılır. Eğer MAC doğru ise bunu kontrol ederek bu şekilde kullanıcının kimliği tanımlanmış olur. USIM, RES'i hesaplar ve VLR'ye gönderir. USIM içinde hesaplanan RES değeri, ziyaretçi veritabanında saklı bulunan XRES değeri ile karşılaştırılır. Eğer her iki cevap değeri birbirine eşit ise bu defada baz istasyonu üzerinde kimlik tanıma işlemi gerçekleşmiş olur. Devamında USIM $f_3$ ve $f_4$ fonksiyonlarını kullanarak IK ve CK'yı hesaplar. Bu sırada güvenli kanal kurulur.




Şekil 7. Kullanıcı Tarafından Ağ'ın Doğrulanması[14]

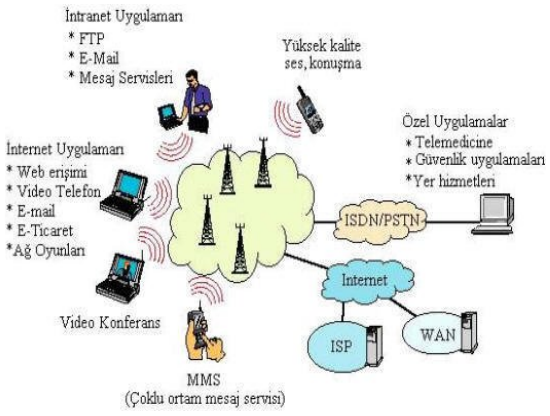
UMTS içinde kimlik tanıma algoritması, tek yönlü olmak üzere 5 adet f1, f2, f3, f4 ve f5 fonksiyonları kullanılır. AKA kimlik tanıma algoritması genelde MILENAGE olarak isimlendirilir. Algoritma tasarımında AES şifreleme standardı kullanılır. Kimlik tanıma ve anahtar anlaşması için 128 bit anahtar uzunluklu, 128 bit blok kullanan bir Blok şifreleme MILENAGE kullanılmaktadır[15][16][17].

Güvenilirlik için yani lineer ve diferansiyel kriptanaliz saldırılarına direnmek için MISTY1 blok şifreleme ve **MISTY1** üzerine kurulan 128 bit anahtar kullanan 64 bit blok ve 8 döngülü Feistel şifreleme kullanan **KASUMI** algoritması kullanılmaktadır[18][19].

## 5. ÜÇÜNCÜ NESİL HABERLEŞMENİN AVANTAJLARI

GSM sisteminin geliştirilmesinin sebebi, analog sistemde bazı ciddi sıkıntıların yaşanması ile başlamıştır. Analog sistemde, sahte kullanıcılar kendileri için yasal olmayan hattı ele geçirip, görüşmeler yaparak ücretlerin yasal kullanıcıya yansımasına neden oluyorlardı. Diğer önemli bir konuda, konuşmalar şifreli yapılmadığından dolayı hattı dinleyen bir kişi tarafından kolayca anlaşılabiliyordu. Bu tür sıkıntılardan dolayı GSM sistemi geliştirilmiştir. GSM'in ortaya çıkması ve teknolojinin ilerlemesiyle, çeşitli saldırı türleri ortaya çıkmıştır. SIM karta yönelik yapılan saldırılar ile gizli anahtar değeri elde edilerek SIM kart kolayca klonlanabiliyordu yada GSM üzerinde kullanıcı ve baz istasyonu arasında karşılıklı kimlik doğrulaması yapılmadığından saldırganlar tarafından sahte baz istasyonları kurularak, haberleşme ele geçirilebiliyordu. BTS ve BSC arasında aktarım şifresiz yapıldığından ve eğer mikro dalga frekansı kullanılıyor ise bu tür frekansları tespit edebilen teknik cihazlar ile veriye ulaşım saldırgan tarafından sağlanabiliyordu. Bu tür sıkıntılardan kurtulmak ve haberleşmede yüksek bit iletim hızı sağlamak üzere UMTS sistemi geliştirilmiştir.

UMTS, hem simetrik hem de asimetrik veri transferine olanak veren, devre ve paket-anahtarlamalı ağ hizmetlerinin aynı anda verilebilmesini mümkün kılan ve IP protokolünü destekleyen bir şebekedir[20]. UMTS sayesinde; Dünyanın her yerinde kullanılabilme ve sorunsuz geçiş sağlanabilmesi, hızlı Intranet/Internet olanağı, video konferans olanağı, çoklu ortam multimedia desteği ile video ve audioların sorunsuz akışı, mobil ticaret imkânı, hem paket hem devre anahtarlamalı veri trafiğinin desteklenmesi, 2 Mbit/s veri hızıyla, genişbant teknolojilere geçiş sağlanabilmiştir[21][22].




Şekil 8. UMTS Şebekenin Hizmetleri [20]

Tüm bu gelişmelerin yanında güvenli aktarımda da büyük yenilik sağlamıştır. Kimlik doğrulamada hem istasyon hem de kullanıcının kimlik sorgulaması yapılarak güvenilirlik sağlanmıştır. Ayrıca GSM içinde kullanılan A5 şifreleme algoritmaları kırılmış iken UMTS, içinde veri şifrelemesinde KASUMI algoritması adı verilen güçlü algoritmalar ve 64 bit yerine 128 bitlik anahtar kullanılmıştır. Bununla beraber bütünlük kontrolü içinde şifrelemede bütünlük algoritması uygulanmıştır. Replay saldırılarından korunmak ve sahte erişimler ile konuşmaya dahil olmamak için yani man-in-the-middle ataklarına karşın sekronize olarak USIM ve AuC veritabanı içinde SQN sıra numarası kullanılmıştır. Bilgi sahasının gizliliği için AMF adı verilen kimlik yönetim sahası kullanılmıştır.

## SONUÇLAR

Bu çalışmada kablosuz ağ haberleşmesinin günümüz için önemi, kablosuz ağ gelişimi, bu sistemler altyapısında kullanılan güvenlik mekanizmaları, bunların zayıf yönleri ve bunlara karşı alınabilecek önlemler anlatılmıştır. Özellikle dünyada yoğun bir biçimde kullanılan 2G ve henüz bazı ülkelerde kullanıma yeni başlanmış olan 3G kablosuz haberleşme sistemi üzerinde durulmuştur. 3G sisteminin 2G sistemi üzerinde kurulduğu, 2G sisteminde yaşanan güvenlik sorunlarına çözüm amaçlı ve gelecek nesil haberleşme sistemleri için de bir yapı teşkil edebileceği vurgulanmıştır. Dünyadaki birçok ülkede kullanılan kablosuz haberleşme operatörleri, 3G konusunda bir hayli geri kalmış olmalarına rağmen, dünyadaki geçişi iyi analiz etmek suretiyle ve yapılan hatalardan ders alınarak bu dezavantajı avantaja dönüştürebilirler.

## KAYNAKLAR


[1] Chengyuan PENG, GSM and GPRS Security, Seminar on Network Security, 2000.

[2] Martin SAUTER, Communication Systems for the Mobile Information Society, 2006.

[3] Yong LI , Yin CHEN, Tie-Jun MA, Security in GSM, Telecommunications Software and Security, 2003.

[4] Jorg EBERSPACHER, Hans Jorg VOGEL, GSM Switching, Services and Protocols,1999.

[5] Praphul CHANDRA, Bulletproof Wireless Security, Communications Engineering Series, Elsevier, 2005.

[6] Billy BRUMLEY, A3/A8 & COMP128, Special Course on Cryptology, Helsinki University of Technology, 2004.

[7] Jörg EBESPACHER, Hans-Jörg VOGEL and Christian BETTSTETTER, GSM Switching, Services and Protokols, Second Edition, 2001.

[8] Wireless Security, www.jenkinsweb.net /Wireless%20Security-rev6.doc

[9] İmran ERGÜLER, Alper KARAHİSAR, Emin ANARIM, GSM İletişim Sistemindeki Zayıflıklar ve Olası Saldırılar, SAVTEK, 2004.

[10] Jovan Dj. GOLIC, Cryptanalysis of Alleged A5 Stream Cipher, School of Electrical Engineering, University of Belgrade, Beograd Yugoslavia, 1997.

[11] Alex BURYIKOV, Adi SHAMIR, David WAGNER, Real Time Cryptanalysis of A5/1 on a PC, Fast Software Encryption Workshop 2000.

[12] Lauri TARKKALA, Attacks against A5, Seminar on Network Security, 2000.

[13] Mohammad Ghulam RAHMAN and Hideki Imai, Security in Wireless Communication, Faculty of Information and Communication Engineering, University of Tokyo, Institute of Industrial Science, 4-6-1, Komaba, Tokyo, 153-8505, Japan, 2002.

[14] Minho SHIN, Justin MA, Arunesh MISHRA and William A. ARBAUGH, Wireless Network Security and Interworking, IEEE, ISSN 0018-9219 Vol. 94, No:2, pp 455-466,February 2006.

[15] Kaisa NYBERG, Cryptographic Algorithms For UMTS, ECCOMAS, 2004.

[16] GERAN Network Access Security, On the Introduction and Use of UMTS AKA in GSM, Ericsson, 2004.

[17] Specification of the 3GPP Confidentiality and Integrity Algorithms, Document1: f8 and f9 Specifications, 2000.

[18] Specification of the 3GPP Confidentiality and Integrity Algorithms, Document2: KASUMI Specifications, 1999.

[19] Mitsuru MATSUI and Toshio TOKITA, MISTY, KASUMI and Camellia Cipher Algorithm Development, Information Technology R&D Center, 2001.

[20] Üçüncü Nesil Mobil Haberleşme Sistemleri, EFLMD, 2005.

[21] Markus UNTERLEITNER, GSM, GPRS, UMTS (IMT 2000 Architecture), Advanced Computer Networks.

[22] Afşin BÜYÜKBAŞ, CDMA VE UMTS: Üçüncü Nesil Mobil Haberleşeme Teknolojilerinin Karşılaştırılması, Telekomünikasyon Kurumu, Uzmanlık Tezi, 2005.