Mobil İletişim Teknolojilerinin Yapısı ve Kullanılan Şifreleme Algoritmaları

Fatma AKGÜN

2. Baskı

PEGEM AKADEMİ

Doç. Dr. Fatma AKGÜN

MOBİL İLETİŞİM TEKNOLOJİLERİNİN YAPISI VE KULLANILAN ŞİFRELEME ALGORİTMALARI

ISBN 978-625-7052-94-8

Pegem Akademi Yayıncılık, 1998 yılından bugüne uluslararası düzeyde düzenli faaliyet yürüten **uluslararası akademik bir yayınevi**dir. Yayımladığı kitaplar; Yükseköğretim Kurulunca tanınan yükseköğretim kurumlarının kataloglarında yer almaktadır. Dünyadaki en büyük çevrimiçi kamu erişim kataloğu olan **WorldCat** ve ayrıca Türkiye'de kurulan **Turcademy.com** tarafından yayınları taranmaktadır, indekslenmektedir. Aynı alanda farklı yazarlara ait 2000'in üzerinde yayını bulunmaktadır. Pegem Akademi Yayınları ile ilgili detaylı bilgilere http://pegem.net adresinden ulaşılabilmektedir.

1. Baskı: Haziran 2020, Ankara
2. Baskı: Ekim 2024, Ankara

Yayın-Proje: Zeynep Güler
Dizgi-Grafik Tasarım: Beyza Nur Erdoğan
Kapak Tasarımı: Pegem Akademi

Baskı: Sonçağ Yayıncılık Matbaacılık Reklam San Tic. Ltd. Şti.
İstanbul Cad. İstanbul Çarşısı 48/48 İskitler/Ankara

Yayıncı Sertifika No: 51818
Matbaa Sertifika No: 47865

İletişim

Pegem Akademi: Shira Ticaret Merkezi
Macun Mahallesi 204 Cad. No: 141/33, Yenimahalle/Ankara
Yayınevi: 0312 430 67 50
Dağıtım: 0312 434 54 24
Hazırlık Kursları: 0312 419 05 60
İnternet: www.pegem.net
E-ileti: pegem@pegem.net
WhatsApp Hattı: 0538 594 92 40

ÖN SÖZ

Bilim ve teknolojide yapılan gelişmeler ile kullanıcıların zaman ve mekân bağımsız olarak hareket özgürlüklerine sahip olabildiği mobil iletişim sistemleri ortaya çıkarılmıştır. Kablolu iletişim sisteminin yarattığı sıkıntı ve kısıtlamalar, insanlar arasında kablosuz iletişim sağlayan mobil haberleşme sistemine geçişi hızlandırmıştır. Mobil iletişim teknolojisinde, kullanıcıların güvenli haberleşmesini sağlamak üzere sistem üzerinde kimlik doğrulama algoritmaları ve bunun yanı sıra veri şifreleme algoritmaları kullanılmıştır. Bu sayede iletişim yapısının güvenliği ve güvenilirliği sağlanmıştır.

Bu kitap geçmişten günümüze mobil haberleşme teknolojilerini, bu teknolojilerin çalışma mantığını, teknoloji içerisinde kullanılan donanım yapısı ve mobil iletişim teknolojilerinde kullanılan kimlik doğrulama ve veri şifreleme algoritmalarını içermektedir. Kitabın ilk bölümünde genel olarak mobil teknolojilerin tarihçesinden bahsedilmiştir. Kitabın ikinci bölümünde mobil haberleşme sistemi içerisinde kullanılan donanım birimlerinden, mobil haberleşme mantığından, mobil haberleşme içerisinde kullanılan kanal erişim yöntemlerinden ve 2G mobil haberleşme teknolojisinden başlanarak 5G mobil haberleşme teknolojiyi de ele alan haberleşme teknolojileri ve çalışma mantığı anlatılmıştır. Üçüncü bölümde genel olarak şifreleme kavramı, akış şifreler, blok şifreler ve HASH algoritmaları yer almıştır. Son bölüm olan dördüncü bölümde ise mobil haberleşme teknolojileri içerisinde kullanılan kimlik doğrulama algoritmaları ve veri şifreleme teknikleri üzerinde durulmuştur. Gerçekleştirilen bu kitap, mobil haberleşme teknolojinin nasıl gerçeleştiği, zaman ve mekân bağımsız hareket özgürlüğü sunan bu teknolojinin içerisinde ne tür şifreleme algortimalarının yer aldığı ve güvenli veri iletişimin nasıl sağlandığını merak eden lise, üniversite, lisansüstü öğrencileri, öğretmen, öğretim elemanı, kamu ve özel sektör çalışanları ve tüm bireylere yönelik hazırlanmıştır. Kitabın özellikle mobil haberleşme teknolojilerinin gelişimi, mobil haberleşme çeşitleri ve kimlik doğrulama/veri şifreleme algoritmaları konusunda önemli bir kaynak olabileceği düşünülmektedir.

Kitap, Trakya Üniversitesi Fen Bilimleri Enstitüsü Bilgisayar Mühendisliği Anabilim Dalı'nda Doç.Dr. Ercan Buluş danışmanlığında hazırlamış olduğum doktora tezinin geliştirilmiş ve yeniden düzenlenmiş biçimidir. Tezimin hazırlanması sürecinde desteğini esirgemeyen, tez çalışmasının her aşamasında beni düşünceleri ile yönlendiren, bilgilerinden faydalandığım değerli hocam ve danışmanım Sayın Doç. Dr. Ercan BULUŞ' a teşekkürlerimi sunarım. Ayrıca kitabın yeniden düzenlenme aşamasında desteğini esirgemeyen eşime, çocuklarıma ve kitabın okuyucu ile buluşmasını sağlayan Pegem Akademi Yayıncılık'a sonsuz teşekkürlerimi sunmak isterim.

Haziran 2020

Dr. Öğr. Üyesi Fatma AKGÜN

Doç. Dr. Fatma AKGÜN

Fatma AKGÜN 1980 yılında İstanbul'da doğdu. İlk ve orta öğrenimini İstanbul' da tamamladı. 1998 yılında kaydolduğu T.Ü. Müh.-Mim. Fakültesi Bilgisayar Mühendisliği Bölümü'nden 2002 yılında başarıyla mezun oldu. 2002 yılında T.Ü. Mühendislik Mimarlık Fakültesi Bilgisayar Mühendisliği Bölümü'nde Araştırma Görevlisi kadrosuna atandı ve aynı yıl Trakya Üniversitesi Fen Bilimleri Enstitüsü'ne bağlı olarak Yüksek Lisans eğitimine başladı. Yüksek lisansını 2004 yılında başarıyla bitirdi. 2005 yılında Trakya Üniversitesi Fen Bilimleri Enstitüsü Bilgisayar Mühendisliği Ana Bilim Dalı'nda doktora çalışmalarına başladı. 2008 yılında T.Ü. Eğitim Fakültesi Bilgisayar ve Öğretim Teknolojileri Eğitimi Bölümü Öğretim Görevlisi kadrosuna başvurdu ve çalışmaya başladı. 2011 yılında doktorasını tamamlayıp, 2012 yılında T.Ü. Eğitim Fakültesi Bilgisayar ve Öğretim Teknolojileri Eğitimi Bölümü'nde Dr. Öğretim Üyesi kadronuna atandı. Evli ve iki çocuğu olan Fatma AKGÜN halen T.Ü. Eğitim Fakültesi Bilgisayar ve Öğretim Teknolojileri Eğitimi Bölümü'nde akademik çalışmalarına ve görevine devam etmektedir.

SUNU

Güvenli haberleşme yapabilmek için alt tarafta çalışan güçlü haberleşme algoritmalarına ihtiyaç vardır. Bu algoritmalar insanlık tarih boyunca insanların birbirileriyle başkalarının haberi olmadan haberleşmeye çalışmaları sonucunda çıkmış ve gelişmiştir. Günümüzde bu algoritmalar kriptoloji bilimi altında incelenmektedir.

Kriptoloji kelimesi antik yunandaki kullanılan kryptos (gizli) graphy (yazı, yazma) kelimelerinin birleşiminden türemiştir. Türkçe'de kriptoloji daha çok şifreleme bilimi olarak isimlendirilmektedir. En eski şifreleme biçimlerinden biri, ilk olarak Eski Mısır'da M.Ö. 1900'de yaşayan Khnumhotep II'nin mezarında bulunan sembol değişimidir. Buradaki sembollerin anlaşılması için bir şifre veya anahtar gerektirdiği görülür. Antik Yunanlılar şifreli bir mesajı göndermek için köleleri kullanmışlardır. Mesajı göndermek için kölelerin saçlarını tıraş etmişler, daha sonra da gönderecekleri mesajı kölelerin kafasına yazarak saçlarının uzamasını beklemişlerdir. Birkaç ay sonra da köle hedefine doğru yola çıkmış ve gittiği yerde tekrar saçları tıraş edilerek mesajın okunması sağlanmıştır.

Scytale ismindeki silindir bir araç (şekil 1), Antik Yunanlılar ve özellikle Sparta'lılar tarafından sembollerin yerleri değiştirilerek şifreli mesajları iletmekte kullanılmıştır. Bu yöntem sıra değiştirmeli şifreleme yönteminin ilk örneği kabul edilmektedir. Bir baston ya da çubuğun etrafına sarılan şerit şeklinde kesilen deri parçasına iletilecek mesaj yazılır. Şerit bastondan geri çıkarıldığında mesajın çözülmesi artık çok zordur. Mesajı okuyabilmek için aynı çapta ve boyutta çubuk bulmanız gerekmektedir.

Şekil 1. Scytale şifre çubuğu

Antik Yunan şehri Megalopolis'li tarihçi Polybius dama tahtası denen iki boyutlu bir şifreleme sistemi geliştirdi. Bu sistemin özelliği, alfabedeki harflerin, iki boyutlu bir tabloya yerleştirilmesi ve ardından bu tablodaki satır ve sütun numaralarına göre okunmasıdır. Örneğin "ercan" kelimesinin şifrelenmiş karşılığı; 15 42 13 11 33 olarak bulunurdu.

	1	2	3	4	5
1	a	b	c	d	e
2	f	g	h	i/j	k
3	l	m	n	o	p
4	q	r	s	t	u
5	v	w	x	y	z

Şekil 2. Dama (Polybius) tahtası

Osmanlı da en çok kullanılan yöntem yazının mürekkep yerine limon suyu kullanılarak yazılmasıydı. Böylece yazılan kâğıt kötü niyetli birinin eline geçtiğinde boş bir sayfa ile karşı kaşıya gelirdi. Çözümü kâğıdın yanmaya yakın derecede ısıtılmasıydı, böylece yazılmış yazı ortaya çıkmaktaydı.

Günümüze gelindiğinde yöntemler gitgide karmaşıklaşmış dolayısıyla çözüm daha da zorlaşmıştır. Devam eden sayfalarda kıymetli öğrencim Fatma AKGÜN tarafından günümüz bilgi çağında kullanılan mobil haberleşme teknikleri ve bu teknolojiler üzerinde kullanılan modern şifreleme yöntemlerinden bahsedilecektir. Bu serüvenin nereye vardığı gayet güzel bir tarzda başarılı bir şekilde anlatılmıştır.

Mayıs 2020

Doç. Dr. Ercan BULUŞ

Canlarım Ada ve Ahmet Ata'ya…

İÇİNDEKİLER

Ön Söz iii
Sunu v

1. BÖLÜM
GİRİŞ

Giriş 1

2. BÖLÜM
MOBİL HABERLEŞME TEKNİKLERİ

Mobil Haberleşme Yapı Elemanları 5
MS-Mobil İstasyon (Mobile Station) 5
SIM-Abone Kimlik Modulü (Subscriber Identity Module) 5
BTS-Baz İstasyon Alıcı-Vericisi (Base Transmission System) 6
BSC-Baz İstasyonu Kontrolcüsü (Base Station Controller) 8
TRAU-Geçiş ve Adaptasyon Birimi (Transcoder and Adaptation Unit) 8
SS7–Sinyalleşme Sistemi (Signalling System) 8
MSC-Mobil Anahtarlama Merkezi (Mobile Switching Center) 9
HLR-Abone Bölge Kaydı (Home Location Register) 9
VLR-Misafir Bölge Kaydı (Visitor Location Register) 9
AuC-Kimlik Doğrulama Merkezi (Authentication Center) 9
EIR-Cihaz Kimlik Kayıtçısı (Equipment Identity Register) 10
GMSC-Mobil Anahtarlama Merkezi Geçici (Gateway Mobile Switching Center) 10
NSS-Ağ Anahtarlama Merkezi (Network Switching Center) 10
Çoklu Erişim Yöntemleri 10
FDMA Teknolojisi 10
TDMA Teknolojisi 11
CDMA Teknolojisi 12
OFDM Teknolojisi 13
OFDMA Teknolojisi 14
Cep Telefonu Haberleşme Mantığı 15
2G Teknolojisi 16
GSM Haberleşme Sistemi 16
CDMA Haberleşme Sistemi 21
PDC Haberleşme Sistemi 22
2,5G Teknolojisi 23
HSCSD Haberleşme Sistemi 24
GPRS Haberleşme Sistemi 24

EDGE Haberleşme Sistemi 26
3G Teknolojisi 27
UMTS Haberleşme Sistemi 28
CDMA2000 Haberleşme Sistemi 29
4G Teknolojisi 31
LTE Haberleşme Sistemi 33
WI-MAX Haberleşme Sistemi 36
5G Teknolojisi 37

3. BÖLÜM
ŞİFRELEME KAVRAMI

Akış Şifreler 43
Tek Kullanımlık Şerit Sistemi 44
Blok Şifreler 46
HASH Algoritmaları 49
Anahtarsız Hash Fonksiyonları 50
Anahtarlı Hash Fonksiyonları 50

4. BÖLÜM
MOBİL HABERLEŞMEDE GÜVENLİK

GSM Haberleşme Sistemi 53
Kimlik Tanıma Algoritması 53
Şifreleme Anahtarı Üretme Algoritması 54
Ses ve Veri Şifreleme Algoritması 55
CDMA Haberleşme Sistemi 59
Kimlik Tanıma ve Şifreleme Anahtarı Üretme Algoritması 61
Sinyal Şifreleme Algoritması 62
Veri Şifreleme Algoritması 64
GPRS Haberleşme Sistemi 67
Kimlik Tanıma ve Şifreleme Anahtarı Üretme Algoritması 68
Ses ve Veri Şifreleme Algoritması 70
UMTS Haberleşme Sistemi 71
Kimlik Tanıma ve Şifreleme Anahtarı Üretme Algoritması 71
Ses ve Veri Şifreleme Algoritması 75
S Kutuları 81
CDMA2000 Haberleşme Sistemi 85
Kimlik Tanıma ve Şifreleme Anahtarı Üretme Algoritması 85
WIMAX Haberleşme Sistemi 92

Wi-Max Ağlarında Güvenlik Gereksinimleri 92
Doğrulama İşlemindeki Adımlar 93
Anahtar Oluşumu 94
Veri Şifreleme 94

Kaynakça 97

1. BÖLÜM

GİRİŞ

Teknoloji, insanoğlunun gereklerine uygun yardımcı alet ve araçların üretilmesi için gerekli bilgi ve yetenek olarak kabul edilirken, ayrıca bilimin uygulamacı yönü olarak da ifade edilebilir. Yapılan yoğun çalışmalar sonucu son yıllarda teknoloji alanında önemli gelişmeler kaydedilmiştir. Bu gelişmelerin başında kablosuz haberleşme sistemleri gelmektedir. Kablosuz ağ iletişimi ile kullanıcıların zamandan ve mekândan bağımsız olarak, hareket özgürlüklerine sahip olabildikleri, radyo frekansları üzerinden iletişim sağlayan bir haberleşme sistemi sağlanmıştır. Hücresel tabanlı mobil radyo servisinin temeli ilk olarak İngiltere'de Bell Labs tarafından 1970 yıllarının başında ortaya atılmıştır. Bu servis ile temel ses iletim hizmetinin sağlanmasına yönelik çalışan bir sistem geliştirmek amaçlanmıştır ve sistem 1970 – 1990 yılları arasında dünyada büyük etki yaratmıştır. Analog işaretleme tabanlı ve Devre-Anahtarlamalı bir iletişim ortamı sağlayan bu sistem üzerinde Frekans Bölmeli Çoklu Erişim (FDMA) / Frekans Bölmeli İki Yönlü İletişim (FDD) teknolojileri kullanılmıştır. Bu teknoloji ilk olarak Analog Mobil Telefon Servisi (Advanced Mobile Phone Service- AMPS) adı altında 1979 yılında Chicago'da (Illinois, ABD) gerçekleştirilmiştir. 1983 yılında kullanıma açılan sistem Asya, Latin Amerika, Okyanus ülkeleri gibi yerleşim yerlerinde hizmet vermiştir. AMPS'in bir türevi olan Toplu Erişim İletişim Sistemi (TACS) ise İngiltere'de 1985'te servise sokulmuştur. 1986 yılında ise Kuzey Avrupa'da İskandinavya'yı kapsaması amaçlanan İskandinav Mobil Telefon sistemi (NMT) geliştirilmiştir. NMT ilk olarak İskandinavya'da, daha sonra ise orta ve güney Avrupa'da ki bazı ülkelerde kullanılmıştır. NMT'nin NMT-450 ve NMT-900 olmak üzere iki versiyonu ortaya çıkarılmıştır. NMT-450, 450MHz frekansını kullanan daha eski bir sistem olarak hizmet verirken, NMT-900 ise 900MHz bandında daha sonraları kullanılmaya başlanmıştır.

Analog mobil uygulamalar, kullanım amacı, kapasite, kalite ve kapsama alanı açısından ülkelere göre farklılıklar göstermiştir. Bu şebekeler genellikle global yapıdan uzak, bölgesel ve ulusal uygulamalarla sınırlı kalmıştır. Yapılan aramalarda bölgeler arası otomatik geçiş yapılamıyor ve bu sebeple aranan kişinin hangi bölgede olduğunun bilinmesi gerekiyordu. Her ne kadar analog hücresel mobil

sistemlerle, mobil haberleşme global bir yapıya kavuşturulmak istenmişse de bu tam olarak sağlanamamıştır. Analog şebekelerin yapılarından kaynaklanan kısıtlamaların olması ve bunların gelişmelere kolayca adapte olamamaları nedeniyle bu durum farklı ülkeler tarafından ortaklaşa kullanılabilecek ve yeni teknolojik gelişmelere açık olan sayısal hücresel mobil şebekelerin geliştirilmesine yol açmıştır (Özkan, 2007).

Geliştirilen çalışmaların kalitesiyle, birinci nesil analog haberleşmedeki sıkıntıları aşmak üzere hem sayısal ses hizmeti, hem de daha iyi veri iletim hizmeti sağlamak amaçlanmıştır. Gerçekleştirilen yenilikler 1990 – 2000 yılları arasında dünyada büyük etki yaratmıştır. Ortaya çıkarılan teknolojik gelişimler sayesinde düşük band genişliği ile sayısal veri işaretleme tabanlı ve Devre-Anahtarlamalı bir iletişim ortamı amaçlanmak istenmiştir. Hedeflenen sistemin TDMA / TDD, CDMA teknolojisini kullanması sağlanmıştır.

Gerçekleştirilen gelişimler ile ortaya çıkarılan teknolojinin kullanıldığı sistemler arasında, Avrupa'da mobil iletişim için kullanılan GSM, Japonya'da kullanılan ve TDMA tabanlı Kişisel Sayısal İletişim olarak da adlandırılan PDC ve Kuzey Amerika'da kullanılan CDMA teknolojileri örnek verilebilir. Bu teknolojilerden GSM sistemleri temel olarak 9,6 kbps band genişliği ve 900MHz bandını kullanmasına karşın DCS 1800 (Digital Cellular System, GSM-1800 olarak ta adlandırılır) ve DCS-1900 (veya GSM-1900) gibi farklı band genişliği kullanan türevleri de vardır (Şahin, 2006). CDMA sistemi ise hava arayüz tasarımı için farklı bir yaklaşım kullanır. TDMA'daki gibi frekans taşıyıcısının kısa zaman aralıklarına bölünmesi yerine, aynı frekans üzerindeki iletimleri ayırmak için iletişimde kullanıcılar arasında farklı kodlar kullanılmıştır. CDMA sistemi 800, 1700 ve 1900 MHz frekans aralıklarını kullanır ve 14,4 Kbps band genişliği kapasitesine sahiptir. PDC sistemi ise 9,6 Kbps band genişliği hızına sahiptir ve sistem 800 MHz, 1500 MHz ve 1900 MHz olmak üzere analog ve sayısal modların her ikisinide kullanmak üzere üç frekans bandında çalışabilir halde kullanılmıştır (Nakajima, Kohno ve Kubota, 2001).

Ortaya çıkarılan tüm bu 2G teknolojileri sayesinde, ses iletiminin analog sistemden sayısal sisteme geçilmesi ile daha önceki sistemlere oranla daha güvenilir ve sorunsuz veri aktarımı sağlanmıştır. Güvenliği sağlamak üzere aktarımda çeşitli kriptografik algoritmalar kullanılmıştır. İletişimde güvenli haberleşme amacıyla mobil kullanıcının sisteme dahil olabilmesi için öncelikle kimlik tanıma işleminden geçirilmesi hedeflenmiştir. Kontrolden sonra eğer kullanıcı doğru kişi ise sisteme dahil olması sağlanmış ve haberleşme işlemi de şifreli bir biçimde gerçekleştirilmiştir. Gerçekleştirilen bu tür yeniliklerin yanısıra, 2. Nesil sistemlerde, kimlik doğrulamanın tek taraflı yapılması, karşılıklı kimlik doğrulamanın olmayışı, yani