

Seminar Paper

Security in Mobile Telephony: The Security Levels in the Different Handy Generations

Christoph Hanser, Simon Moritz, Farjola Zaloshnja, Qin Zhang

{ christoph.hanser.0371, simon.moritz.1675, qin.zhang.2742 }

@student.uu.se, fzaloo2@um.edu.mt



UPPSALA
UNIVERSITET

Abstract

In mobile telephony, there are several vulnerabilities like interception, fabrication, and denial of services. Security aspects have been improved in every new generation of mobile system. This seminar paper explains security in each generation and discusses how security is ensured in mobile telephony.

This paper was written for the Security Computer Systems course held by Björn Victor at the University of Uppsala, Sweden.

Table of Contents

1 Introduction	1
2 First Generation Technology	2
3 Second Generation Technology	3
4 Third Generation Technology.....	3
3G Security Architecture	4
Principles for 3G Security.....	4
Important changes from 2G to 3G.....	5
Possible 3G attacks and security architecture responses	5
Conclusion about 3G Security Features	7
5 Fourth Generation Technology.....	8
6 Conclusion	10
A References.....	11

List of Abbreviation

1G, 2G, 2.5G, 3G, 4G	Generations of Wireless Telephone Technology
AMPS	Advanced Mobile Phone Service
CDMA	Code Division Multiple Access
ESN	Electronic Serial Number
FDMA	Frequency Division Multiple Access
GPRS	General Packet Radio Service
GSM	Global System for Mobile Communication
GSN	GPRS Support Node
HLR	Home Location Register
IMSI	International Mobile Subscriber Identity
IP	Internet Protocol
MIN	Mobile Identification Number
MSC	Mobile Switching Center
NMT	Nordic Mobile Telephone
OFDM	Orthogonal frequency-division multiplexing
RNC	Radio Network Controller
VLR	Visitor Location Register
SGSN	Serving GSN
TACS	Total Access Communication System
TMSI	Temporary Mobile Subscriber Identities
WAP	Wireless Application Protocol
WDM	Wideband Code Division Multiple Access

1 Introduction

The newest large wave in telecommunication, mobile telephony, has spread over the whole world. Still, more and more people are connecting to the mobile network. At the same time, network providers are offering new services like MMS, telephone manufacturer are implementing new features like cameras, Internet games, or office products, and some companies are developing business strategies like billing (i.e. enabling people to pay with their mobile phones).

The more possibilities, more concrete: features and applications, exist in cell phones, the more they prone to be attacked. In addition, the more services are used and trusted, the more technical vulnerabilities might come to the surface and might motivate attackers to abuse these mobile services. New programs which blend the computer and telephony world are a good example for that as they introduce problems like viruses and worms into the telephony world. Another recent example is the trend to trade via mobile phones, called m-commerce which makes it also interesting for hackers to harm users (Grami & Schell 2004, p.1).

Several security threads have been detect in mobile telephony. Fabrication of other users' identity, called "cloning" in mobile telephony, enables thieves, for example, to bill their own calls to someone's account. Interception of talks which is called eavesdropping or scanning enabled hackers to listen other peoples' calls (Wikipedia 2005a and Precisesecurity.com 2005). Gong (2005, p.13) lists furthermore threads of integrity and denial of services.

To tackle these threads, Jøsang and Sanderud (2003, p.1f) state several security aspects in mobile telephony. Firstly, confidentiality of traffic, location, and users' address should be established to prevent interception and privacy thread. Secondly, authentication of users and data must be offer to tackle fabrication. Furthermore, they add non-repudiation, i.e. authentication with the help of third parties, as a needed security aspect.

These security aspects should be ensured by the security standards developed by the cell phone industry. For every mobile telephone generation a standard has been published including more and more security. In the 1980s, the first generation of mobile phone technology (1G) provided analog voice-only communication. The next generation (2G) offered digital voice applications using GSM (in 2.5G GPRS) and low-speed data service to download Internet packages, i.e. WAP. The third generation (3G) resumed at the beginning of this century and focuses on packet data instead of voice. The actually specified fourth generation (4G) intends to enable broadcast IP-based multimedia services, and should be published around 2010 (Grami & Schell 2004, p.1 and Wikipedia 2005a).

In our seminar paper we intend that the reader gets a brief overview about security in mobile telephony and knows the important facts of the secure standards. We will concentrate on the security levels in 1G, 2G and especially 3G, and, thus, do not target specific applications like m-commerce or other security issues which have non-technical origins like theft of cell phones (here, damage can be limited with PIN codes).

To reach this goal, we will discuss FDMA, CDMA, WCDMA, and OFDM in the subsequent chapters, and finish our paper with an comparison of the security standards and a conclusion.

2 First Generation Technology

There are three mainly used mobile phone systems based on analog technology of 1G: AMPS (Advanced Mobile Phone Service), TACS (Total Access Communication System) and NMT (Nordic Mobile Telephone). All of them used cellular networks to send analog voice signals with the help of FDMA (Frequency Division Multiple Access). (Gong, 2005, p. 78-79)

The AMPS has been the American analog cellular standard since the 1970s. In sense of security, one of the shortcomings of AMPS is the lack of inherent security features (authentication and data encryption) in the standard. And as a primitive analog wireless communications protocols, it provides no security services. Therefore, the calls can be easily intercepted and the Mobile Identification Number (MIN) and Electronic Serial Number (ESN) can then be extracted from the intercepted call. Then analog wireless phones can be easily cloned using MINs and ESNs got from the interception. (DISA 2002)

The TACS is the European version of AMPS, and have almost the same security property (which is insecure actually) as AMPS. (Wikipedia 2005a)

The NMT, which started in 1970, has mainly been used in the Nordic countries, Eastern Europe and Russia. The original NMT specification has a disadvantage that voice traffic was not encrypted. So anyone willing to intercept would just have to buy a scanner and tune it to the correct frequency. As a result, some scanners have had the NMT bands "deleted" so they could not be accessed. However, this is not particularly effective as it isn't that hard to obtain a scanner that doesn't have these restrictions; and it is also possible to re-program a scanner so that the "deleted" bands can be accessed again. But later versions of the NMT specifications defined optional analog scrambling. If both the base station and the mobile phone supported scrambling, they could agree upon using it when initiating a phone call. Also, if two users had mobile phones supporting scrambling, they could turn it on during conversation even if the base stations didn't support it. In this case voice would be scrambled all the way between the two mobile stations. While the scrambling method was not at all as strong as encryption in newer digital phones, such as GSM, it did prevent casual listening with scanners. (Wikipedia 2005b)

3 Second Generation Technology

While cell phones of 1G mainly used the FDMA standard, the next generation of mobile phones implemented (among others) the Code Division Multiple Access (CDMA) standard. CDMA intends to meet the handover-problem explained in the last chapter. It allows a “soft handover”, i.e. the user does not have a quality loss if he moves from one cell station to another. CDMA achieves this by using special orthogonality codes which help to separate different users and enable access to a shared memory without interference (Schiller 2003, p. 82ff).

According to Gong (2005, p.12), the security of CDMA is mainly implemented in Global System for Mobile Communication (GSM). GSM allows:

- Authentication of subscribers using shared-secret cryptography
- Encryption of radio interface, i.e. communication between subscriber and base station. Here, GSM encrypts calls with so-called A5/1 and A5/2 stream ciphers.
- Confidentiality of the subscriber's identity using a hardware security module on each cell phone's called SIM (Subscriber Identity Module) which stores a cryptovariable. (Gong 2005 and Wikipedia 2005c)

However, Wikipedia (2005c) complains that serious weaknesses have been found in both algorithms as it is possible to break A5/2 in real-time in a ciphertext-only attack. These security weaknesses have to be solved by the next generation of cell phones.

4 Third Generation Technology

The move from 2G to 3G cellular systems is expected to substantially raise bandwidth demands, primarily on the support network. Third Generation cellular systems were developed with the aim of offering high-speed data connectivity to mobile customers as well as satisfying call traffic exigencies. 3G systems are defined by the International Telecommunications Union (ITU) as being capable of supporting high-speed data rates in the range of 144 Kbps to more than 2 Mbps, depending on the medium conditions, congestion, motion and mobile speed and are also subject to fading channels and other constraints that affect 2G system models. Wideband Code Division Multiple Access (WCDMA) is the dominating 3G technology, WCDMA uses a new spectrum with a 5 MHz carrier, providing 50 times higher data rate than in present GSM networks and 10 times higher data rate than in GPRS networks, also known as 2.5G networks for having come in between the two generations. WCDMA handles up to 2 Mbps for local area access or 384 Kbps for wide area access and it enables better use of available spectrum and more cost-efficient network solutions.

Operator can gradually evolve from GSM to WCDMA, protecting investments by re-using the GSM core network and 2G/2.5G services.

3G Security Architecture

In 3G networks, mobile stations are connected to hosting networks by means of a radio link to a particular base station. Multiple base stations of the network are connected to a Radio Network Controller (RNC) and multiple RNCs are controlled by a GPRS Support Node (GSN) in the packet-switched case or a Mobile Switching Center (MSC) in the circuit-switched case. The Visitor Location Register (VLR) and the serving GSN keep track of all mobile stations that are currently connected to the network. Every subscriber can be identified by their International Mobile Subscriber Identity (IMSI). In order to protect against profiling attacks, this permanent identifier is sent over the air interface as infrequently as possible. Instead, locally valid Temporary Mobile Subscriber Identities (TMSI) are used to identify a subscriber whenever possible.

Every 3G subscriber has a dedicated home network with which a long term secret key is shared. The so-called Home Location Register (HLR) keeps track of the current location of all subscribers of the home network. Mutual authentication between a mobile station and a visited network is carried out with the support of the current Serving GSN (SGSN) or the mobile switching center or VLR respectively. 3G systems support encryption of the radio interface as well as integrity protection of the signaling messages.

Principles for 3G Security

System security is based on GSM security. Security features from GSM that have “proven to be needed and robust” (Gong 2005), although in September 2003 a Haifa Technion team claimed to have found an effective way to crack the encoding system for cellular telephone conversations conducted over GSM (Global System for Mobile) networks.

Being aware of the GSM security holes, important new security features and services offered had to be designed and implemented; 3G had to correct the problems with GSM by addressing its real security weaknesses. One of the main objectives of 3G security is to ensure that the implementation of security features and mechanisms can be extended and enhanced as required by new threats and services. Until a certain point GSM did provide strong subscriber authentication and over-the-air transmission encryption but different parts of an operator network became vulnerable to attacks. In April 1998, Smartcard Developer Association along with two U.C Berkeley researchers suspected that they have cracked the COMP128 algorithm, which is stored on the SIM. The reason behind this was the secrecy of designing algorithms and use of weakened algorithms like A5/2 and COMP 128. According to Srinivas (2001), one of the other claims was made by the ISAAC security research group. They asserted that a fake base station, which would allow a man-in-the-middle attack. One of the other possible scenarios is of insider attack. In the GSM system, communication is encrypted

only between the Mobile station and the Base Transceiver station but within the provider network, all signals are transmitted in plain text, which could give a chance for a hacker to step inside.

Important changes from 2G to 3G

The following problems existed in 2G and have been solved by specific changes in 3G:

- Changes were made to defeat the false base station attack. The security mechanisms include a sequence number that ensures that the mobile can identify the network.
- Key lengths were increased, unlike in the case of vulnerable wireless WEP, to allow for the possibility of stronger algorithms for encryption and integrity. Mechanisms were included to support security within and between networks.
- Security is based within switches rather than base stations as in the case of GSM. Therefore, links are protected between base stations and switches.
- When roaming between networks, such as between a GSM and 3G, only the level of protection supported by the smart card will apply. Therefore a GSM smart card will not be protected against the false base station attack when in a 3G network.

Possible 3G attacks and security architecture responses

Many of the security enhancements required to 2G systems are intended to counteract attacks which were not perceived to be feasible in 2G systems. This includes attacks that are, or are perceived to be, possible now or very soon because intruders have access to more computational capabilities, new equipment has become available, and the physical security of certain network elements is questioned.

In order to perform the attacks the attacker has to possess one or more of the following capabilities:

1) Eavesdropping.

This is the capability that the attacker listens in on signaling and data connections associated with other users. An example of a possible attack is one that requires a modified base station and that cannot authenticate messages received over the radio interface.

The target user is enticed to camp on the false base station. When the target user or the intruder initiates a call the network does not enable encryption by spoofing the cipher mode command. The attacker however sets up his own connection with the genuine network using his own subscription. The attacker may then subsequently eavesdrop on the transmitted user data. In 3G system mandatory cipher mode command with message authentication and replay inhibition allows the mobile to verify that encryption has not been suppressed by an attacker.

2) Impersonation of a user.

This refers to the capability whereby the attacker sends signaling and/or user data to the network, in an attempt to make the network believe they originate from the target user.

3) User impersonation with compromised authentication vector.

An attack that requires a modified mobile station and the possession by the intruder of a compromised authentication vector which is intended to be used by the network to authenticate a legitimate user. The intruder uses that data to impersonate the target user towards the network and the other party.

In 3G the presence of a sequence number in the challenge means that authentication vectors cannot be re-used to authenticate. However, the network is still vulnerable to attacks using compromised authentication vectors.

4) Impersonation of the network.

This is the capability whereby the attacker sends signaling and/or user data to the target user, in an attempt to make the target user believe they originate from a genuine network.

When the target user or the genuine network sets up a connection, the false base station modifies the ciphering capabilities of the mobile station to make it appear to the network that a genuine incompatibility exists between the network and the mobile station.

The network may then decide to establish an un-enciphered connection. After the decision not to cipher has been taken, the intruder may eavesdrop on the user data.

In 3G message authentication and replay inhibition of the mobiles ciphering capabilities allows the network to verify that encryption has not been suppressed by an attacker.

5) Man-in-the-middle attack.

This is the capability whereby the attacker puts itself in between the target user and a genuine network and has the ability to eavesdrop, modify, delete, and spoof signaling and user data messages exchanged between the two parties. In order to perform a man-in-the-middle attack against a user of a 3G-only mobile station, an attacker would have to impersonate a valid network to the user. However, in the 3G-only equipment case, the combination of two specific security mechanisms protects the mobile station from this attack: the authentication token and the integrity protection of the security mode command message.

The authentication token ensures the timeliness and origin of the authentication challenge and as such protects against replay of authentication data. The integrity protection prevents an attacker from simply relaying correct authentication information while fooling the respective parties into not using encryption for subsequent communication.

6) Denial of Service.

a. De-registration spoofing

An attack that requires a modified mobile station and exploits the weakness that the network cannot authenticate the messages it receives over the radio interface. The intruder spoofs a de-registration request to the network. The network de-registers the user from the visited location area and instructs the HLR to do the same. The user is subsequently unreachable for mobile terminated services.

b. Location update spoofing

The user spoofs a location update request in a different location area from the one in which the user is roaming. The network registers in the new location area and the target user will be paged in that new area. The user is again, subsequently unreachable for mobile terminated services.

In both de-registration and location spoofing in 3G system integrity protection of critical signaling messages protects against these attacks. More specifically, data authentication and replay inhibition of the location update request allows the serving network to verify that the de-registration and the location update request are legitimate.

c. Camping on a false Base Station

An attack that requires a modified base station and exploits the weakness that a user can be enticed to camp/roam on a false base station. Once the target user camps on the radio channels of a false base station, the target user is out of reach of the paging signals of the serving network in which he is registered. The security architecture does not counteract this attack.

However, the denial of service in this case only persists for as long as the attacker is active unlike the above attacks which persist beyond the moment where intervention by the attacker stops. These attacks are comparable to radio jamming which is very difficult to counteract effectively in any radio system.

Conclusion about 3G Security Features

- Mutual Authentication - The mobile user and the serving network authenticate each other. The user and the mobile station share a secret key, PIN.
- Authentication and Key Agreement - 128 bit secret key K is shared between the home

network and the mobile user Serving Network

- Multiple Cipher and Integrity Algorithms - The user and the network negotiate and agree on cipher and integrity algorithms. At least one encryption algorithm exported on world-wide basis (KASUMI)
- Data Integrity - Signaling messages between the mobile station and RNC protected by integrity code. The integrity algorithm (KASUMI) uses 128 bit key and generates 64 bit message authentication code.
- Encryption - Signaling and user data protected from eavesdropping. Secret key, block cipher algorithm (KASUMI) uses 128 bit cipher key.
- Network-to-Network Security - Secure communication between serving networks. IP layer security provides encryption, origin authentication and integrity using standard IPsec techniques.

5 Fourth Generation Technology

Even though the 3G standard is relatively newly implemented, the world is waiting for a new mobile generation technology, a new standard which will develop the system even further and take the security to a higher level. This technology of wireless devices we might refer to as the next generation, e.g. 4G. A leading wireless company NTT DoCoMo is already testing 4G communication at 100Mbps while moving the device, and 1Gbps while it is still. NTT DoCoMo are planing to release their first commercial network in 2010. However, in Japan and some parts of China they are already trying 4G out, using OFDM (Orthogonal Frequency Division Multiplexing) as the technique. In an article from 7th of August 2004, 4Gcouk mentions that “Wi-LAN Inc., a global provider of broadband wireless communications products and technologies, today announced it has successfully demonstrated its LIBRA 5800 TM operating in a full mobility environment, including both high speed (vehicular) and seamless hand-off capability applying the Wide-band Orthogonal Frequency Division Multiplexing (W-OFDM) technology.” (4Gcouk 2004)

In addition to OFDM, 4G devices may use OFDMA (Orthogonal Frequency Division Multiple Access) to better allocate network resources to multiple users. (Wikipedia 2005e)

An OFDM baseband signal is the sum of a number of orthogonal sub-carriers with data on each sub-carrier being independently modulated commonly using some type of quadrature amplitude modulation (QAM) or phase-shift keying (PSK). OFDM is the modulation scheme used by 802.11a and 802.11g WLANs. The method transports data using many carrier waves, with each wave carrying part of the message. The OFDM method has the following advantages when compared to spread spectrum modulation (DISA 2002):

- higher data rate over a smaller bandwidth

- more non-overlapping channels
- increased resistance to reflected multipath signals
- increased resistance to interference

The benefits of using OFDM are many. Others than the above mentioned are high spectrum efficiency and that it is easy to filter out noise. If a particular range of frequencies suffers from interference, the carriers within that range can be disabled or made to run slower. Also, the upstream and downstream speeds can be varied by allocating either more or fewer carriers for each purpose. Some forms of Rate Adaptive DSL use this feature in real time, so that bandwidth is allocated to whichever stream needs it most. (Wikipedia 2005f)

The technique using OFDM gives a possibility to add new not yet standardized methods in it. One can use these orthogonal signals over the sub-carriers in several other ways. This is currently a research area with hints to possibilities such as adding security which makes it impossible for unrecognized eavesdropping. Whenever one reads a message it changes enabling the receiver B to notice whenever a eavesdropper C is reading. B can therefore drop the message and ask the sender A for a new one until they safely have set up a connection.

OFDM is almost always used in conjunction with channel coding, an error correction technique, to create coded orthogonal FDM (COFDM). It is a complex technology to implement but it is now widely used in digital telecommunications systems to make it easier to encode and decode such signals. The system has found use in broadcasting as well as certain types of computer networking technology. This is particularly due to the fact that such signals show good resistance to multipath fading.

4G generation will probably also provide non-repudiation services (cf. chapter 1), key recovery, universal access to any type of media and devices and Integrate services (including payment and charging) as it probably will use public-key algorithms for key agreement giving privacy and authentication to the system. (Gong 2003)

In this technology it will also become more interesting to use IP-based multimedia services. VoIP is probably becoming the “killer” application (4Gcouk 2004). Mobile video calls will have better features, better frame rates etc. 4G will probably become more than only a telephony standard. It might end up like a huge WLAN. The mobile telephones will not only be phones, but more like a computer which could be used for phone calls. With more advanced features the security need will grow.

The fourth generation will probably become an IP based technology with more, or at least as many, possibilities as a regular internet user has today when sitting home on his stationary computer. It will probably only be the amount of storage which will differ, even if this also might be solved in different way.

6 Conclusion

This essay's aim: “The reader gets a brief overview about security in mobile telephony and knows the important facts of the secure standards.” We hope that we could give an overview about the different security standards used by mobile phone's generations. We have to admit, that the borders between the standards are not so clear, and depending on sources the standards might be associated different to the mobile generations. However, it should be clear that there is an evolution in the standards from FDMA to CDMA to WCDMA and that security was added in every place.

While 1G was stigmatized as almost no-security standard and the following generation improved only few in security terms (but was concerned mainly on technical improvements), 3G added significant important security features which meet nearly all required security aspects: mutual authentication, authentication and key agreement, multiple cipher and integrity algorithms, data integrity, encryption and network-to-network security are provided.

In our paper we have also given an outlook what might happen in the future. The 4G technology will take the security to a higher level as it probably will use public-key algorithms for key agreement which will enable privacy and authentication.

A References

- 3GPP (2000). **3G TR 33.900** [Internet]. Available from:
<http://www.3gpp.org/ftp/tsg_sa/WG3_Security/_Specs/33900-120.pdf> [Accessed 18 Oct 2005].
- 4Gcouk (2004). W-OFDM Technology in 4G Cellular Networks. [Internet] Available from:
<<http://www.4g.co.uk/PR2004/August2004/2032.htm>> [Accessed 20 Oct 2005].
- DISA:Defence Information System Agency (2002) **Mobile and wireless devices addendum to the wireless** [Internet] Available from: <<http://iase.iii.e.disa.mil/stigs/stig/wireless-stig-v4r0.2.pdf>> [Accessed 15 Oct 2005].
- Gollmann, D. (1999). **Computer Security**. Jony Wiley & Sons, Chichester et al.
- Gong, G. (2005). **Introduction to Mobile Security**. [Internet] Available from:
<<http://www.comsec.uwaterloo.ca/~ggong/716F05/t1.pdf>> [Accessed 13 Oct 2005].
- Gong, G. (2005). **Security in 4G systems**. [Internet] Available from:
<<http://www.comsec.uwaterloo.ca/~ggong/ECE710T4/lec7-ch6a.pdf>> [Accessed 13 Oct 2003].
- Grami, A. & Schell, B.H. (2004). **Future Trends in Mobile Commerce: Service Offerings, Technological Advances and Security Challenges**. Second Annual Conference on Privacy, Security and Trust, October 13-15, 2004. Available on
<<http://www.precisecurity.com/phone-guide.htm>> [Accessed 15 Oct 2005].
- Jøsang, A. & Sanderud, G. (2003). **Security in Mobile Communications: Challenges and Opportunities**. In Proceedings of the Australasian information Security Workshop Conference on ACSW Frontiers 2003 - Volume 21 (Adelaide, Australia). C. Johnson, P. Montague, & C. Steketee, Eds. Conferences in Research and Practice in Information Technology Series, vol. 34. Australian Computer Society, Darlinghurst, Australia, 43-48.
- Meyer, U. & Wetzel, S. (2004). **A man-in-the-middle attack on UMTS**. In Proceedings of the 2004 ACM Workshop on Wireless Security (Philadelphia, PA, USA, October 01 - 01, 2004). WiSe '04. ACM Press, New York, NY, 90-97.
- Precisecurity.com (2005). **Mobile Phone Security Guidelines**. [Internet] Available from:
<<http://www.precisecurity.com/phone-guide.htm>> [Accessed 17 Oct 2005].
- Preneel, B. (2003). **Mobile network security**. [Internet] Available from
<http://www.iaik.tugraz.at/teaching/oo_angewandte%20kryptografie/slides/bart_mobile3>

b.pdf> [Accessed 18 Oct 2005].

Schiller , J. (2003). **Mobile Communications**. Second Edition. Addison-Wesley. London et al.

UMTSWorld.com (2004). **UMTS Security** [Internet]. Available from:

<<http://www.umtsworld.com/technology/security.htm>> [Accessed 18 Oct 2005].

Walker, M. (2000). **On the security of 3GPP** Networks [Internet]. Available from:

<http://www.3gpp.org/ftp/tsg_sa/WG3_Security/_Specs/33900-120.pdf> [Accessed 18 Oct 2005].

Wikipedia (2005a). **AMPS**. [Internet] Available from:

<http://en.wikipedia.org/wiki/Advanced_Mobile_Phone_System> [Accessed 20 Oct 2005].

Wikipedia (2005b). **NMT**. [Internet] Available from:

<http://en.wikipedia.org/wiki/Nordic_Mobile_Telephone> [Accessed 20 Oct 2005].

Wikipedia (2005c). **GSM**. [Internet] Available from:

<http://en.wikipedia.org/wiki/GSM#GSM_security> [Accessed 19 Oct 2005].

Wikipedia (2005e). **4G**. [Internet] Available from: <<http://en.wikipedia.org/wiki/4G>> [Accessed 19 Oct 2005].

Wikipedia (2005e). **Orthogonal frequency-division multiplexing**. [Internet] Available from:

<http://en.wikipedia.org/wiki/Discrete_multitone_modulation> [Accessed 17 Oct 2005].