Radio Jamming Attacks Against Two Popular Mobile Networks

Mika Ståhlberg
Helsinki University of Technology
Mika.Stahlberg@iki.fi

Abstract

The dependence on Mobile Networks is growing. The success of the Internet was followed by Denial of Service attacks. What if the same happens to Mobile Networks? This paper gives an introduction to the concept of Radio Jamming and explores jamming resistance of two popular mobile networks: GSM and WLAN. Radio interfaces of the two systems are analysed and effective jamming-to-noise ratios are calculated. Based on the results, suggestions on how to increase the jamming resistance of the networks are given.

Keywords: GSM, WLAN, Jamming, Electronic attack, Denial of Service, DOS, Spread Spectrum

1 Introduction

When authorized users are not provided a requested service within a defined maximum waiting time, we say that a Denial of Service (DOS) violation has occurred [6]. Probably the first DOS attack used in electronic communications was the jamming of military radio frequencies. In military terms jamming is the "soft kill" part of an Electronic Attack (EA), which focuses on the offensive use of electromagnetic spectrum or directed energy to directly attack enemy combat capability [19]. Mobile networks have made it possible to perform DOS attacks against civilian networks by using communications jamming techniques. This paper explores the threats caused by jamming to mobile networks and the vulnerability of GSM and WLAN systems to jamming attacks. Some other DOS attack methods against the two networks are also briefly described.

A large portion of present mobile systems operate in the UHF band i.e. frequencies from 300 MHz to 3 GHz. In the UHF band, obstacles such as buildings cause a lot of attenuation, and therefore radio waves propagate almost completely along the line-of-sight. Base stations are usually located in relatively open space and use wide beam antennas in order to cover a large area and are therefore vulnerable to jamming. Even the narrow-beam implementations of UHF have relatively large antenna beam widths. Therefore, especially for satellite communications, UHF does not offer protection from jamming and can be easily disturbed using unsophisticated techniques [19].

Jamming is performed by transmitting a signal to the receiving antenna at the same frequency band or sub-band as the communications transmitter transmits. It is important to

notice that transmission can never be jammed - jamming hinders the reception at the other end. The problem here for the jammer is that only transmitters can be found using direction finding and the location of the target must usually be known by the jammer as jamming power is never infinite. Transmitters can be attacked by means of physical destruction or by High Power Microwave (HPM) weapons, that can cause transmitter circuits to malfunction. HPM is not discussed in this paper. Jamming is successful when the jamming signal denies the usability of the communications transmission. In digital communications, the usability is denied when the error rate of the transmission cannot be compensated by error correction. Usually a successful jamming attack requires that the jammer power is roughly equal to signal power at the receiver.

The effects of jamming depend on the jamming-to-signal ratio (J/S), modulation scheme, channel coding and interleaving of the target system. If the jammer does not have the output power to jam a wide band continuously, it can increase its instantaneous jamming level by pulsed jamming. In pulsed jamming, the jammer sweeps a large band jamming each narrow sub-band for a short period of time. [14]

Jamming-to-Signal ratio (ignoring propagation effects) can be calculated according to Equation 1. [19]

$$\frac{J}{S} = \frac{P_j G_{jr} G_{rj} R_{tr}^2 L_r B_r}{P_t G_{tr} G_{rt} R_{jr}^2 L_j B_j} \tag{1}$$

where

P_j = jammer power
P_t = communication transmitter power
G_{jr} = antenna gain, jammer $\Longrightarrow$ communication(com) receiver
G_{rj} = antenna gain, com receiver $\Longrightarrow$ jammer
G_{rt} = antenna gain, com receiver $\Longrightarrow$ com transmitter
G_{tr} = antenna gain, com transmitter $\Longrightarrow$ com receiver
B_r = communications receiver bandwidth
B_j = jamming transmitter bandwidth
R_{tr} = range between communications transmitter and receiver
R_{jr} = range between jammer and communications receiver
L_j = jammer signal loss (including polarization mismatch)
L_r = communication signal loss

An examination of Equation 1 indicates that the jammer ERP (Effective Radiated Power), which is the product of antenna gain and output power, should be high if maximal jamming efficiency is required. On the other hand, in order to prevent jamming, the antenna gain toward the communication partner should be as high as possible while the gain towards the jammer should be as small as possible. As the equation shows, the antenna pattern, the relation between the azimuth and the gain, is a very important aspect in jamming.

Distance has a strong influence on the signal loss. If the distance between jammer and receiver is doubled, the jammer has to quadruple its output in order for the jamming to have the same effect. It must also be noted here that jammer path loss is often different from the communications path loss. In a military environment, jammers are often located in aircraft, helicopters, or Unmanned Aerial Vehicles (UAV) as the line-of-sight propagation

gives them an advantage over communication transmitters located on the ground.

Most digital communications systems require a synchronisation signal to be transmitted between the communicating devices. Jamming can be concentrated on the synchronization signal, cutting effectively the entire transmission. Synchronized systems are very vulnerable to jamming. Once the synchronization is lost, the jammer can end its transmission and restart jamming after resynchronisation is achieved. However, it is usually very difficult for the jamming system to know when the synchronisation is lost. [15]

Classic jamming transmission is simply band-limited noise (barrage jamming, denial jamming). The objective is to inject an interference signal into the communications frequency so that the actual signal is completely submerged by the interference. Depending on the transmission, some other waveform might be more effective. Waveforms useful for jamming include noise-modulated FM, noise bursts, CW tones (spot jamming), and swept signals (swept-spot jamming). Usually it is useful to use a jamming waveform similar to the waveform being jammed. Deceptive jamming that uses previously recorded play-back signals can also be used. [19]

2 Spread-spectrum radio techniques

Spread spectrum is a radio technology that makes eavesdropping, direction finding and jamming difficult. In spread-spectrum communications the signal is spread in accordance to a pseudorandom code over a frequency band excess of the minimum bandwidth necessary to send it. Despreading is accomplished through correllation with the code. Several spread-spectrum techniques exist. The two most common ones are direct sequence (DS) and frequency hopping (FH). Two or more techniques can be combined into a hybrid form of spread spectrum.

Spread-spectrum modulation was originally developed for military applications. In military radio environment the ability to resist jamming is very important. Lately, many civilian applications have utilised the unique characteristics of spread spectrum as it provides multipath reduction and makes multiple-access communications possible. In multiple-access, a number of users share a common channel without an external synchronising mechanism.

In DS transmission, the signal is spread over the entire band by a random binary string (the spreading code). A number of users can use the same band, causing only relatively small interference to each other. Protection against jamming waveforms is provided by purposely making the communications signal occupy a far wider bandwidth than the minimal necessary bandwidth. This causes the communications signal to resemble noise so as to blend it into the background.

One bit of data is mapped onto a pattern of several "chips" in the frequency plane. The number of chips that represent one bit of data is called the spreading ratio. The choice of the spreading ratio is very important. If it is greater, the interference effects are reduced; if smaller, it will make better use of the spectrum [16]. The gain in signal-to-noise ratio obtained by the use of spread-spectrum is called processing gain. Processing gain for Direct-sequence spread spectrum (DSSS) can be calculated using Equation 2 [19].

$$G_p = \frac{r_c + r_s}{r_s} \approx \frac{r_c}{r_s} \tag{2}$$

where r_c is the chip rate and r_s the message symbol rate.

For example, if the processing gain is 30 dB, the jammer would have to increase its jamming power by 30 dB in order to offset the added protection of the spreading. Similarly, an eavesdropper or a direction finder would have a 30 dB disadvantage compared to a friendly receiver in being able to detect the signal. A higher processing gain makes jamming more difficult. If the required jamming-to-signal ratio for effective jamming is known, the gain can also be calculated as presented in Equation 3 [4].

$$G_p = (\frac{E_s}{N_0})_{output} + \frac{J}{S} + L_{system} \tag{3}$$

where $(E_s/N_0)_{output}$ is the theoretical output signal-to-noise ratio per symbol. (J/S) is the jamming margin (the jamming signal power relative to the desired signal power), and L_{system} is the sum of the system implementation losses.

An exception must be noted here - the "near-far" problem in jamming. If the jamming transmitter is very close to the receiver but the communications signal comes from far away, the jammer might get a "power advantage" and the reception of the weaker signal is not possible, even if it would be theoretically possible because of the processing gain . [2]

In FH, the signal hops from subchannel to subchannel transmitting short bursts of data at each channel for a set period of time (dwell time). The hopping sequence must be synchronised. There are two kinds of hopping radios available - slow and fast hoppers. Slow hoppers change their frequency at a pace of 50 to 500 hops per second. FH systems can be jammed with narrow-band or wide-band jamming signals or the jammer can sweep the entire band [15].

If the jammer spreads its energy over the entire frequency range of the communication signal, FH systems have the processing gain presented in Equation 4 [19].

$$G_p = \frac{\beta_n}{\beta_m} \tag{4}$$

Where β_n is the frequency band over which the hopping occurs and β_m is the message bandwidth.

If the jammer power is not sufficient to jam the entire band of the FH transmission, the jammer should hop along (follow-on jamming). This is quite difficult as, in modern systems, the jammer does not know the frequency of next hop. Slow hoppers with 100 hops per second dwell on each frequency for approximately 10 ms. To jam a very error resistant signal, roughly 20% of the bits should be in error. Therefore, the jammer must begin jamming in at most 8 ms, not counting the signal travel time [19]. It must be noted that it will take some time for the jammer to tune into the new frequency, start jamming, and increase the jamming power to the necessary level. Radio signals propagate so fast that the geometry and distances between the communications transmitter, receiver, and the jammer have virtually no effect on the required response time for the follow-on jammer. [15]

Today, protection against sophisticated fast-follower military jammers would require a hop rate of 10,000 hops per second [19]. These jammers are able to follow even a pseudo-random frequency hopping sequence because after the transmitter hops away from the previous frequency, the jammer scans the entire band in search for the new frequency and starts to jam again [15].

Increased hopping rate does not change the bit-error-rate of the communications signal. This is due to the fact that, although on slow hopping systems the jammed sequences are longer, in fast hopping systems they appear more often. A fast hopping system gives an advantage only against follow-on jammers. [15]

3 DOS attacks against GSM

3.1 Description of the GSM system and radio interface

In the GSM network, the Base Station Subsystem (BSS) takes care of the radio resources. In addition to Base Tranceiver Station (BTS), the actual RF tranceiver, BSS consists of three parts. These are the Base Station Controller (BSC), which is in charge of mobility management and signalling on the Air-interface between Mobile Station (MS), the BTS, and the A-interface between BSS and Mobile Services Switching Center (MSC).

The GSM Air-interface uses two different multiplexing schemes: TDMA (Time Division Multiple Access) and FDMA (Frequency Division Multiple Access). The spectrum is divided into 200 kHz channels (FDMA) and each channel is divided into 8 timeslots (TDMA). Each 8 timeslot TDMA frame has a duration of 4,6 ms (577 μs/timeslot) [20]. The GSM transmission frequencies are presented in Table 1.

	Downlink	Uplink
GSM900	935-960 MHz	890-915 MHz
DCS1800	1710-1785 MHz	1805-1880 MHz

Table 1: GSM frequency bands

The timeslots are called physical channels. A physical channel is full duplex and several logical channels can share it. The GSM system has several different logical channel types. In addition to traffic channels (TCH), the GSM system has control channels.

When a MS enters the network, it first looks for beacon frequencies of the nearby Base Tranceivers by scanning all possible channels. All base stations transmit their beacon frequencies at a fixed frequency and power level. The MS finds the beacon frequency by searching the frequency with the highest signal level for a timeslot with a sequence of "00000..." - a sinewave - which is transmitted on the Frequency Correction Channel (FCCH). FCCH is one logical channel in the physical channel called the Broadcast Control Channel (BCCH) and it is used for bit sychronization. BCCH is always on the 0-timeslot of the beacon frequency. [17]

After MS achieves bit synchronization, it finds the Synchronization Channel (SCH) from the BCCH physical channel. From the SCH, the MS derives frame synchronization. Then

the MS can find the logical channel BCCH also located in the physical channel BCCH. The logical channel BCCH transmits important BTS information such as the frequency hopping sequences, other frequencies, and neighbouring cells. [18]

In addition to the three downlink control channels FCCH, SCH and BCCH, there are also three call control logical channels located in the physical channel BCCH. The Paging Channel (PCH) is used when the network wants to contact the MS. The MS monitors all PCH channels on the BCCH-frequency. When the MS is turned on, the network knows the location area (LA) where the MS is located. A location area may consist of several cells. Thus the MS is paged in all cells in the LA. The MS recognises a page directed to it by the identity number in the paging information (either IMSI - International Mobile Subscriber Indentity or TMSI - Temporary Mobile Subscriber Identity). When the MS wants to request service from the network or it is replying to a page, it sends a service request on the Random Access Channel (RACH). The network replies to a request from the MS on the Access Grant Channel(AGCH). The combination of PCH and AGCH is often called PAGCH (Paging and Access Grant Channel), but this name is not denifined in the GSM Specifications. Table 2 presents logical control channels located on the physical BCCH channel. [20]

Downlink	1. Frequency Correction Channel (FCCH)
	2. Synchronisation Channel (SCH)
	3. Broadcast Control Channel (BCCH)
	4. Paging Channel (PCH)
	5. Access Grant Channel (AGCH)
Uplink	6. Random access channel (RACH)

Table 2: GSM control channels

The MS measures the Signal-to-Noise ratio of cells from BCCH and the location updates are decided according to these measurement results. The MS keeps a list of the best BCCH-frequencies according to the selection criteria used by the operator. In a multi-frequency cell, only one frequency is required to have the BCCH on its 0-timeslot.

During a call, MS transmits and receives on its own Traffic Channel a burst only in one of the eight timeslots. During the other timeslots, the MS monitors the BCCH levels and information on the neighbouring cells. The GSM system uses slow Frequency Hopping (FH), which means that the frequency changes after each burst (once every 4.6 ms). The use of FH is optional for GSM networks but all GSM phones must support it. All physical channels, except the 0-timeslot of BCCH-channel can hop. A 6-bit Hopping Sequence is transmitted on BCCH and both MS and BTS have a frequency list indicating to which frequencies and in which order to hop. The hopping algorithm is presented in [20]. The uplink hopping follows the downlink hopping with a fixed delay. [18]

Power control is optional for the the BTS, and BCCH must use a constant power level because of the measurements carried out by the MS. Power control is triggered by field strength and reception quality measurements at the BTS or MS. If the measurement average from a 480 ms period is not within the limits, the output power in the other end of the connection is altered accordingly [18]. The GSM maximum transmitting powers are presented in Table 3.

	max	min
GSM900		
MS	39 dBm⋆	5 dBm
BTS	58 dBm	9 dBm
DCS1800		
MS	30 dBm	0 dBm
BTS	46 dBm	17 dBm

⋆) Only for car antennas. The maximum transmitting power of GSM900 hand phones in the market is 37 dBm. According to the specifications, power is adjusted in 2 dB steps.

Table 3: GSM system transmitting powers [21]

The GSM signal uses Gaussian Minimum Shift Keying (GMSK) with a modulation index of 0.5 and a modulation speed of 271 kbps. The normalised bandwidth (WT_b) of the Gaussian filter used before the modulation stage is 0.3. GMSK belongs to the Frequency Shift Keying (FSK) family and is robust against fading and interference. Ninety-nine percent of the power of the GMSK signal is confined to a bandwidth of 250 kHz. This means, that for all practical purposes, GSM sidelobes are virtually zero outside the 250 kHz and the effect of co-channel interference is practically negligible. [11]

The required bit error rate (BER) before any error correction for a static channel is less than 10^{-4} [21]. This requires the a S/N-ratio of 9-12 dB. With advanced Viterbi decoders, the minimum S/N can be as low as 4-8 dB [14]. Viterbi demodulation is a maximum likehood technique which finds the most probable emitted sequence according to assumptions on the possible signals and on the noise [22]. The interference is specified as uncorrellated and random GSM signal.

3.2 Jamming of the GSM System

Frequency Hopping in GSM is intended for the reduction of fast fading caused by movement of subscribers. The hopping sequence may use up to 64 different frequencies, which is a small number compared to military FH systems designed for avoiding eavesdropping and jamming [14]. The jammer can also listen to BCCH and derive the hopping sequence in advance. Also, the speed of GSM hopping is just over 200 hops/s, which can be followed by a follow-on jammer. GSM FH provides no real protection against jamming attacks.

FH does make it difficult for direction finders to locate a MS, as MS sends on each channel for only one timeslot, that is 577 μs at a time. Only DF equipment that can determine the direction in less than that time or can follow the frequency hopping can pinpoint the direction.

GSM system has a very efficient interleaving and forward error correction (FEC) scheme. This leads to the assumption that jammers can gain no advantage from pulsed jamming [14]. In [14] it was shown that as the specified system S/N ratio is 9 dB, a jammer requires a 5 dB S/J in order to succesfully jam a GSM channel. The optimal GSM S/N is 12 dB, after which the system starts to be disrupted.

GSM system is designed to withstand sudden cuts in Traffic Channel (TCH) connections.

These cuts are normally caused by brutal propagation losses due to obstacles such as bridges or tunnels. A connection can also be cut if the user detaches MS battery in the middle of the connection. Another cell could often be used to continue communication when the original BTS has lost connection. The GSM architecture provides two prodedures for this: handover when the connection is still available and call re-establishment when the original connection is totally lost. Handover decisions are made based on transmission quality and reception level measurements carried out by the MS and the BTS. In jamming situations call re-establishment is probably the procedure the network will take in order to re-connect the jammed TCH. At the moment when connection is lost, a timer starts ticking in the MSC. If re-establishment is not achieved when the timer has reached the maximum time set by the operator, the connection loss is total [17].

It is clear that uplink jamming is in most cases easier than downlink, as the base station antenna is usually located in a mast or a high building. This makes it economical for the jammer to overpower the small maximum output of MS. In case the jammer wants to jam only the traffic sent by a single MS, it should be able to distinct the bursts sent by the target and jam only them. If the cell uses frequency hopping, the jammer must be able to follow the MS transmit frequency. This is very difficult compared to the effect and makes it more feasible for the jammer to jam all available traffic channels. Uplink TCH jamming is further hindered by handovers and call re-establishment. Basically, the handover possibility demands that, in addition to the TCH, at least the RACH control channels of all BTSs in the area need to be jammed in order to cut transmission. If the goal of jamming is to cut existing connections, the jamming has to last at least until the call re-establishment timer at the MSC expires and the connection is released. This means that an existing call can be cut by a few seconds of effective jamming.

In a more cost efficient scenario, the jammer should target the RACH control channel. This would prevent all MSs from requesting any service from that cell. Note that network originated calls also require the MS to request service on RACH. This jamming technique will not cut active calls and is therefore ineffective in some situations. An example of the required power for RACH jamming is shown in Figure 1.

The GSM RACH random access scheme is very simple: when a request is not answered, the mobile station will repeat it after a random interval. The maximum number of repetitions and the time between them is broadcast regularly on BCCH. After a MS has tried to request service on RACH and has been rejected, it may try to request service from another cell [17]. Therefore, the RACH channels of all BTSs in the area should be jammed.

From an examination of the GSM channel architecture it is obvious that downlink Control Channels (FCCH, SCH and BCCH) should be targeted if the existence of a cell needs to be hidden by jamming [14]. These channels are easy to recognise and use a constant power output. By jamming the synchronisation information it is possible to prevent the MS from detecting a valid GSM network at all.

The GSM system has a feature that further eases jamming operations: the system gives feedback to the jammer about jamming efficiency by increasing all power agile channel power levels when the jamming is successful [14]. This makes it easy for an intelligent jammer to optimise its use of power. Usually, the efficiency of a jamming attack is very difficult to determine, which leaves the jammer in doubt.

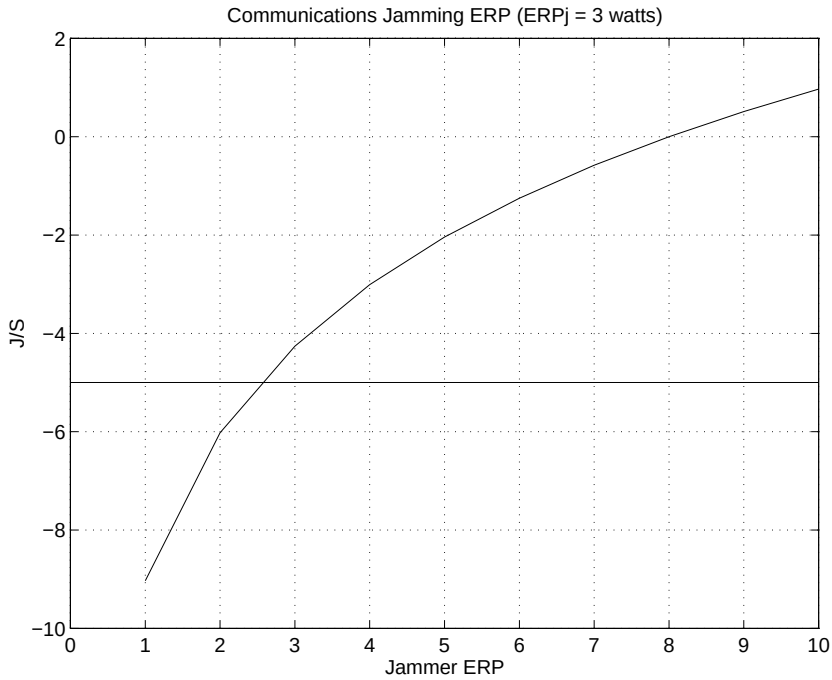

Figure 1: Example of RACH jamming effectiveness calculated using Equation 1. Antenna gain towards both the MS and jammer is supposed to be 12 dBi. Jammer antenna gain is also 12 dBi. MS has a maximum output power of 2 W. Distance from Jammer to BTS is twice the distance between MS and BTS. As the needed J/S for GSM jamming is -5 dB the needed ERP (horizontal axis) can be seen from the graph (2.5 W).

3.3 Jamming efficiency and avoidance

As most GSM traffic today is still circuit switched voice communications, a very efficient jamming attack does not have to sustain jamming efficiency. If a phone call is cut every 5 seconds, the service can certainly be considered denied. SMS messages only need a few seconds for transmission, and not even that because the sending MS does not necessarily have to wait for an acknowledgement from the server. Complete Denial of Service would therefore require that MS cannot request any service from the Network.

The GSM radio interface is resistant to interference compared to most public mobile telephone systems. The greatest problem for withstanding jamming for GSM is its channel architecture. The control channels are easy to isolate and jam. Jamming the reception of a single MS is quite difficult as its location is difficult to determine using Direction Finding (DF). Therefore jamming attacks should concentrate on the uplink and especially uplink RACH control channel. As most BTSs are located in high places, uplink jamming seems to be the jamming method of choice against GSM.

Existing connections can be cut by jamming the Traffic Channel used by the connection and the Random Access Channels of all other cells located in the area. This will prevent the system from re-establishing the connection through some other base station. This jamming has to be sustained until the network ends its attempt to re-establish the lost connection. This usually means that the channels have to be jammed for at least a few seconds.

Effects of jamming can be reduced by using directional antennas in BTSs. The cell sizes should be as small as possible in order to make full use of the limited maximum output power of the MS equipment and to increase the number of possible call re-establishment cells. GSM phones could also use directional antennas, but that would reduce their mobility. Frequency Hopping in GSM is too slow to reduce the effects of jamming. It does, however, make jamming target identification more difficult because it hinders DF.

3.4 Other denial of service methods

A man-in-the-middle attack can be made against GSM encryption. Because in some countries encryption is forbidden, the GSM standard has encryption as an option only. This flaw is not dangerous by itself, but because a MS does not authenticate the BTS, it can be used for eavesdropping. An attacker can purchase base station equipment and set up a BTS of his own with encryption turned off. MS will connect to attackers BTS, if it has the characteristics of the operator and a better signal than the best of "real" base stations. The phony or spoofed station sits between MS and BTS forwarding (and intercepting) all traffic between them without either one knowing that it is there. [7]

The Man-in-the-middle attack could also work as a Denial-of-Service attack. The attacker could send a "busy" signal to the MS each time it wanted to place a call and "forget" to forward any calls to the MS. Also, it is possible for the BTS to respond to a service request on the RACH with a message forbidding the mobile station to access the channel within a specified time. Unlike in a collision situation, the MS is required to stay in the serving cell upon receiving such a message, unless it relocates to another cell because of measurement results [17].

There are also other methods for GSM DOS. Certain GSM equipment have flaws that make it possible for attackers to launch a DOS attack against them. An example of such an attack is the SMS DOS attack threat found in Nokia phones in August 2000 [9].

4 DOS attacks against IEEE802.11b WLAN

4.1 Description of WLAN system and radio interface

The IEEE 802.11 standard defines three physical layers to be used in Wireless Local Area Network (WLAN) transmissions: two spread-spectrum radio techniques and an infrared (IR) specification. IR WLAN is not within the scope of this paper. The radio-based standards operate within the industrial, scientific and medical (ISM) band at 2.4-2.4853 GHz. These frequencies are recognized by international regulatory agencies, such as FCC (USA), ETSI (Europe), and MKK (Japan) for unlicenced radio operations. This means that as long as regulatory requirements of transmitting power and bandwidth are met, anyone can operate a transmitter at the ISM band even without a licence. IEEE 802.11 radiated power (ERP) in the EU is 1-100 mW. In the USA, WLAN and other ISM equipment can have an ERP up to 1 W.

In a WLAN system using frequency the hopping technique, the frequency band is divided

into 75 different 1 MHz subchannels with dwell times of no longer than 0.4 seconds. The sender and the receiver agree on a hopping pattern, and data is sent over a sequence of subchannels. Each conversation with the network occurs over a different hopping pattern, and the patterns are designed to minimize the chance of two senders using the same subchannel simultaneously. FHSS uses two- or four-level FSK modulation scheme with respective modulation indices of 0.32 and 0.16. FH limits the transmission speed of WLAN systems to 2 Mbps because the bandwidth of each subchannel is only 1 MHz. If the whole band of 75 channels is used effectively, as required by the regulations, the system must hop often. The 1 MHz bandwidth limits the transmission speed and the hopping further reduces it because of hopping overhead. Since every hop causes some lapses in communications due to tuning and power adjustment, the hopping rate causes an overhead. 11 Mbps (IEEE 802.11b) WLAN systems do not use FH even on speeds of 1-2 Mbps. [1]

In the direct sequence mode, the band is divided into 13 different 22 MHz subbands. Only three of these subbands are completely non-overlapping and only these three can be used on 11 Mbps systems (IEEE 802.11b). IEEE 802.11 uses an 11-chip Barker sequence to encode all data sent over the air. Each 11-chip sequence represents a single data bit. A sequence is converted into a symbol (waveform) that can be sent over the air. Symbols are sent at the rate of 1 MSps (million symbols per second) and the modulation depends on the data rate. In IEEE 802.11 5.5 and 11 Mbps data rates, Barker sequences are not used but instead a method called Complementary Code Keying (CCK) is specified. A description of CCK can be found in [5]. CCK consists of 64 8-bit code words. As a set, these codes have unique mathematical properties, that allow them to be distinguished even in substantial noise. The data rates and modulation techniques are presented in Table 4.

Data Rate	Code Lenght	Modulation	Symbol Rate	Bits/Symbol
1 Mbps	11 (Barker)	DBPSK	1 MSps	1
2 Mbps	11 (Barker)	DQPSK	1 MSps	2
5.5 Mbps	8 (CCK)	DQPSK	1.375 MSps	4
11 Mbps	8 (CCK)	DQPSK	1.375 MSps	8

Table 4: IEEE 802.11 DSSS Data rates. [5]

802.11 WLANs use dynamic rate shifting allowing data rates to be automatically adjusted to compensate for the changing nature of the radio channel. This means that in a jamming situation the jammer is able to cut transmission if and only if he can jam a 1Mbps WLAN radio channel.

By regulations, a Direct Sequence Spread Spectrum (DSSS) system in the ISM band must have a minimum of 10 dB processing gain. With 1 Mbps 11 bit Barker code the processing gain is 10.4 dB (using Equation 2) and, with 11 Mbps CKK, 11 dB [5]. Note that any high-rate modulation is more susceptible to jamming, multipath interference and filter distortion than lower rate modulation because of the higher required SNR (E_s/N_0). Processing gain is the reason why DS is so jamming resistant.

4.2 WLAN Medium Access Control

Most wireline LANs use Carrier Sense Multiple Access with Collision Detection (CSMA/CD) as the Medium Access Control (MAC) protocol. WLAN systems use Distributed Foundation Wireless Medium Access Control (DFWMAC) schemes because of the "near/far"-problem: in radio systems, transmission drowns out the ability of the station to "hear" a collision. Distributed Co-ordination Function Carrier Sense Multiple Access with Collision Avoidance (DCF CSMA/CA) avoids this problem by requiring the receiver to send an ACK-message if the sent packet was received intact. If the sender does not receive an ACK or the ACK is not intact, the data is retransmitted after a random period of time.

CSMA/CA is a mandatory MAC-scheme in all WLAN products. It does not, however, solve all the problems of access control in a radio environment. The hidden node problem shown in Figure 2 causes CSMA/CA to be ineffective. Node C cannot hear node A, so if node A is transmitting to B, node C will not know this and it may send to B as well. Only B can solve this problem. [16]

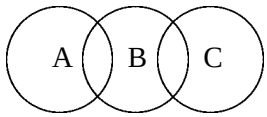

Figure 2: The hidden node problem

The IEEE 802.11 optional solution to the hidden node problem is DCF with RTS/CTS. The procedure is the following 4-way handshake [10]:

1. The sender listens to the channel before it sends. If the medium is free for the duration of a Inter-Frame Space (IFS), the station can start sending a Ready to Send message (RTS). RTS contains the destination and the duration of the transmission. IFS depends on the service type. If the medium is busy, the sender has to wait for a free IFS and, additionally, for a random back-off time.
2. The destination sends a Clear to Send (CTS) message. This message tells the sender that it can send without the fear of collision at the destination (hidden node problem).
3. The sender sends its data packet by packet.
4. The destination acknowledges the reception by sending an ACK-message after each received packet. If a packet is not acknowledged, it is retransmitted.

One other standardised solution to the hidden node problem exist: Point Co-ordination Function (PCF). DFWMAC-PCF is an access method that splits access time into a DCF-period and a PCF period where the access point polls stations according to a list.

4.3 Jamming of WLAN

Frequency hopping is designed to avoid narrow-band jamming by hopping from one frequency to another in a rapid pace. Interference on a single frequency will only affect the packets sent on that frequency. On the other hand, all bits within a packet are transmitted on the same frequency. Because of this, bit errors within a packet are not uncorrelated events. The low modulation indices of 2FSK (0.32) and 4FSK (0.16) result in extremely high symbol cross-correlation coefficients, 0.85 and 0.95 respectively. High Cross-correlation will correspond to the spreading of one bit effect on the modulator over many bit intervals. It can be assumed that a single bit error will cause the packet checksum (CRC) to indicate a bad packet, resulting in packet error and retransmission. [13]

Microwave ovens can be considered as narrow-band swept jammers. They operate on the ISM band and are therefore a source of some interference for WLAN. In [13] it was shown that the signal strenght of a FHSS radio must exceed jammer power from a microwave oven by 16 dB in the 1 Mbps mode and 22 dB in the 2 Mbps mode for reliable transmission. These results can be generalised for all narrow-band noise jammers.

Unlike FH, DS is not frequency agile and thus even narrow band jamming falls most likely in the band. DSSS systems are resistant to jamming because of the processing gain caused by the spreading process. Also, the despreading process converts the remaining interference into wideband white noise and the DBPSK/DQPSK modulation methods are more power efficient than the FSK-methods employed by FHSS. As a result, IEEE 802.11 DSSS systems reject about 90% of the energy of a jammer. Moreover, due to the short inter-chip intervals, direct sequencing provides good resistance over narrow-band follow jammers [19], although it might be theoretically possible to follow the spikes in the spectrum.

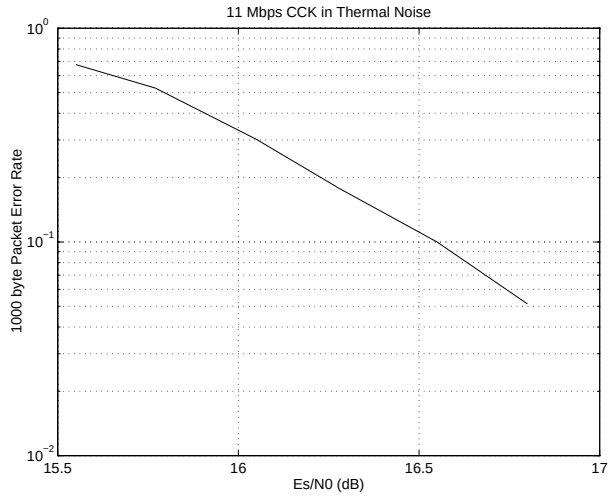

Figure 3: 11 Mbps CCK 1000 byte Packet Error Rate (PER) [5]

The reference PER is specified as 8% and can be related to BER of 10^{-5}. Figures 3 and 4 show that for 11 Mbps CCK, the (E_s/N_0) at 8% PER is 16.6 dB and, for 1 Mbps Barker code, it is 9.6 dB. System implementation losses for IEEE 802.11 cards can be expected to be 2 dB [4]. The following calculations can be made using Equation 3:

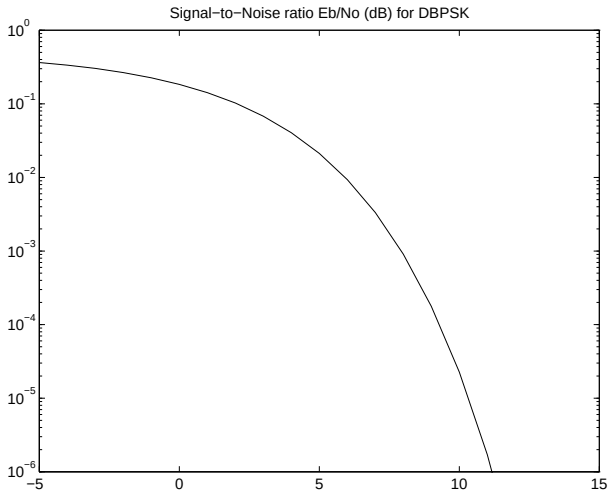

Figure 4: DBPSK bit error propabilities. $P_e = \frac{1}{2}exp(-\frac{E_b}{N_0})$ [2]

11Mbps CCK: (J/S) = G_p - (E_s/N_0) - L_{system} = 11 dB - 16.6 dB - 2 dB = -7.6 dB

1Mbps Barker 11 chip: (J/S) = 10.4 dB - 9.6 dB - 2 dB = -1.2 dB

As can be seen from the calculations above, 1 Mbps IEEE 802.11 is 6 dB less vulnerable to jamming than 11 Mbps connections. The calculation shows that, in theory, it takes a 0.8 dB stronger jamming signal to cut transmission on a WLAN connection, but if system losses are taken into account, the ratio drops to -1.2 dB. [13] shows that, not counting the system losses, 10% packet error rate to IEEE 802.11 1 Mbps data rate is caused by a relative jammer power (E_b/J_0) of -1 dB and for long packets by (E_b/J_0) of 0.5 dB. The jamming frequency must fall in band with the Spread Spectrum transmission. In real life situations, this band might be hard to find, although in WLAN there are only a few channels to choose from. The effectiveness and possibility of jamming is greatly impaired by the use of spread-spectrum techniques.

4.4 Test results

In order to verify the correct parameters for WLAN jamming, a test was performed. The test environment was an Ad Hoc WLAN composed of two laptop computers equipped with Lucent Technologies WaveLAN Turbo 11 Mbps IEEE 802.11b-compliant PCI-cards (output power 8 dBm). The jammer was a Marconi 2041 Noise Signal Generator with a maximum output of 13 dBm and an 11 dBi antenna. Signal levels were recorded with a spectral analyser and pulse widths with an oscilloscope.

In the test, the WLAN connection was subjected to different jamming signals from pulse narrowband AM to Wideband FM. Network speed was measured by sending a large file to the recipient and measuring the time. Files were transferred using Microsoft Network over IPX/SPX. The connection was encrypted with WEP 128-bit RC4.

The test WLAN used the ETSI ISM channel number 3 with center frequency 2422 MHz. The bandwidth of 22 MHz was in reality a 10 dB band of 18 MHz. The effective file

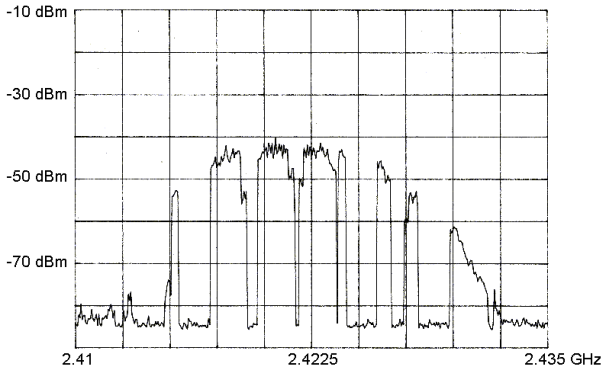

Figure 5: Spectrum of a IEEE 802.11b transmitter measured during the tests.

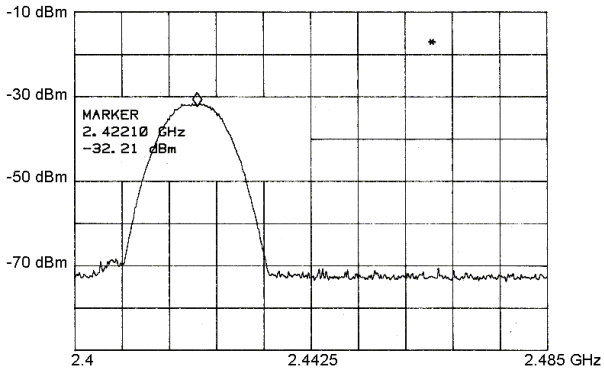

Figure 6: Location of the channel used (number 3) within the 2.4-2.485 GHz ISM band. Notice also the "maximum hold"-shape of the spectrum.

transfer rate of a 11 Mbps connection was shown to be 2.5-3 Mbps in no jamming, no traffic situation. The received signal of -49 dBm could be totally jammed with a narrow-band jamming signal of -47 dBm. This confirms the theoretical J/S calculated in 4.3. Figures 5, 6 and 7 present spectrogram pictures of the test.

4.5 Jamming efficiency and avoidance

The WLAN MAC-layer and the TCP/IP protocols require several packets to be sent in both direction before any useful data can be sent. Therefore, it is not necessary to keep a connection jammed in order to deny its use. The time between the jamming periods is dependent on the service being jammed.

The fact that WLAN uses a very high frequency with a low output power makes it very difficult, if not impossible, for the attacker to jam a network within a building from outside. On the other hand, access networks located outdoors seem very vulnerable to jamming. It is possible to jam an indoor WLAN by planting a small dispensable jamming device inside the premises. That jammer could be set to start jamming at a specific time or it could be activated remotely. Locating a well-hidden dispensable jammer could be difficult without

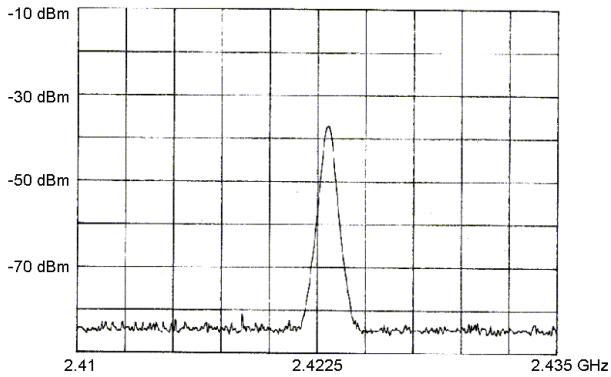

Figure 7: Narrow-band jamming signal used in the jamming tests (2422 MHz).

a field strength meter or direction finding equipment. Moreover, deliberate jamming might not be the first cause for the network problems the local system administrator will think of.

The DSSS scheme used by IEEE 802.11 provides a roughly 10 dB processing gain, i.e. protection against jamming. This is not very much compared to advanced military systems, but does make jamming much harder. The protection provided by Direct Sequence can be summarised as follows:

1. DSSS signal is hard to detect and the direction of the transmitter is difficult to find.
2. In theory, the transmission band is hard to determine. WLAN specifications define only 13 channels, so educated guesses are easy to make.
3. The jamming requires a higher J/S ratio than against traditional signals (Processing Gain).
4. Despreading reduces jamming into white noise.

Because of the low output power of IEEE 802.11 equipment and the relatively wide beam widths of WLAN Nomad Access APs, jamming of an outdoor WLAN is possible and very effective. If someone would want to jam an access network, he would be able to do that with relatively simple equipment sold in open markets. The jamming could probably even be carried out within the regulations of the ISM band.

4.6 Other denial of service methods

In addition to jamming and TCP/IP DOS attacks, WLAN systems are also vulnerable to some other denial of service attacks. These attacks are briefly described here.

The MAC scheme used by WLAN poses a serious threat especially to poorly authenticated Access WLAN systems located outdoors. Any device that can submit a WLAN packet in a CDMA/CA system can jam the system by sending these packets constantly. Other stations will think the network is occupied and they will wait for the specified period. In the RTS/CTS scheme, the same effect can be achieved by sending valid RTS packets.

This way the jammer would not need a high power output, but the results would be the same as in regular jamming. 802.11 provides for MAC layer encryption and access control mechanisms, which are known as Wired Equivalent Privacy (WEP). Using WEP, data is encrypted with a 40-bit RC4 algorithm and access points will authenticate stations by sending them encrypted challenge packets [1]. The station must use its key to encrypt and send the correct response in order to gain network access. However, WEP does not prevent DOS attacks that constantly request service from the access point or replay attacks that make the transmission channel seem occupied to other stations.

WLAN architecture also gives an opportunity for anyone trying to attack a network: "AP spoofing". Every WLAN access point in an infrastructure network (as oppose to Ad Hoc) has a network name. The network names of APs (Access Point) belonging to a system are the same. A subscriber makes the choise between different APs with the same network name according to the S/N of their signal. The AP with the highest S/N is chosen.

If an attacker would set up an AP of his own closer to the subscriber or would have a better S/N by some other method, that subsciber would connect the the attacking AP. This AP could then deny all service from the subscriber.

It should be noted here that both these attacks could be performed within the regulations of the ISM band. As ISM is free, this would make it impossible for network operators to prevent the attacks by legal action.

5 Conclusions

Wireless networks are not vulnerable to cable-cutting DOS attacks as wireline networks. In wired networks, it is pretty common for a excavator to cut dug-in cabling. Still, other types of DOS, such as TCP/IP DOS, are possible and radio jamming poses a new, dangerous threat for public mobile networks.

From the attacks described and the results stated in this report, it becomes obvious that jamming or denial of service in general was not very high in priority when the two systems were designed. Both GSM and IEEE 802.11 are relatively resistant to interference but their architecture (especially GSM) and spectrum spreading techniques are not designed to dodge deliberate jamming.

Protection against jamming attacks is very difficult. On regulated bands it is easy for authorities to locate jammers, so the attacker can only jam for limited periods.

The jamming resistance of a mobile network can be increased by several means.

1. Currently the infrastructure of the network often contains radio relay links. If these links are replaced by fiber-optic cables, the threat of jamming is limited to the interfaces between base stations and subscribers.

2. The use of highly directive antennas with low sidelobes will hinder jamming by both directing emitted power towards receiver and attenuating received power from all other directions but the transmitter.

3. Cell sizes of cellular networks should be minimized as the maximum power output of mobile equipment is very limited. Small cell sizes will also increase the possibilities of avoiding jamming by handover to another cell.

4. Use of antijam modulation schemes will restrict the injection of disrupting signals. [19]

5. Use of Frequency Hopping forces the jammer to spread its transmission power to a wide band [15] and reduces Direction Finding possibilities. Direct sequence techniques will reduce jamming efficiency through processing gain. DF possibilities are also reduced by processing gain (low S/N) and also because numerous transmitters may transmit on the same band simultaneously.

6. Slowing down the data rate will increase resistance to jamming. As the transmission rate decreases, the signal-to-noise ratio needed for a successful transmission will decrease and the signal power per symbol will increase.

7. Compression of data will allow the use of error correction and redundancy addition on the signal [15].

8. The benefits of pulsed jamming can be negated by effective pseudo-random bit interleaving and forward error correction [14].

9. Channel architecture should be designed keeping the jamming threat in mind. Hopping sequences and spreading codes should not be broadcasted unencrypted. Synchronisation should be as hard to jam as possible and the network traffic should not be reliant on just a single non-frequency-agile control channel as in GSM.

Antenna gain is very important in avoiding jamming. For instance, a 10 dB increase in antenna gain in both ends will force the jammer to increase its effective radiated power by 20 dB (100 times larger power). Also, directing a pattern minimum towards the jammer will further decrease the effects of jamming. Because of the importance of antenna patterns for jamming avoidance, jamming is difficult to avoid if the jammer is located in the same direction as the communications transmitter.

The idea of smart antennas is to use base station antenna patterns that are not fixed, but adapt to the current radio conditions. This can be visualized as the antenna directing a beam toward the communication partner only. By maximizing the antenna gain in the desired direction and simultaneously placing minimal radiation pattern in the directions of the interferers, the quality of the communication link can be significantly improved. In personal and mobile communications, the interferers are other users. There are papers describing the use of smart antennas for both the GSM [23] and WLAN [3].

Recently jamming has been also used in non-hostile applications. In quiet spaces, such as libraries, jamming can be used to prevent mobile phones from operating. In hospitals, GSM and other digital signals can cause medical equipment to malfunction. Jamming can prevent GSM phones from detecting base stations and therefore keep phones in receive-only mode. One example of this kind of commercial jamming equipment is the C-Guard Cellular FireWall [8]. The C-Guard and other such devices could also be used with malicious intent. For instance, a burglar could use it to suppress the alarm sent by a wireless household or car alarm system.

This paper gives some guidelines of the threat posed by jamming on two popular mobile systems. However, it is very difficult to say anything very precise about the efficiency of jamming in a general situation, as there are so many parameters. Antenna patterns, modulation, data rate, range, terrain, weather, receiver threshold, transmitter power , synchronisation scheme, error correction, processing gain, even the number of sun spots, all have effect on evaluating jamming.

It could be very difficult for a user to recognise a jamming attack on a communications system. The effects of jamming on communications equipment usually resemble a bad connection and a deliberate attack will not be the first cause of the problem the target will think of. When the attack is recognised as a deliberate jamming attack, the jammer has to be located using direction finding. It will be a lengthy process to recognise the problem and shut down the jammer.

DOS attacks emerged on the Internet as its popularity grew and business became dependent on the networks. Why would someone want to perform a DOS attack against a WLAN or a GSM network? The answer is the same why someone would perform a DOS attack on the Internet: for excitement, adventure, thrills, money, power, revenge,... . When the dependence on wireless systems increases, so does the probability of jamming crime and electromagnetic terrorism.

References

[1] 3Com IEEE802.11b Wireless LANs Technical Paper. 13p. <http://www.3com.com/mobile/wireless/pdf/whitepaper.pdf> [referred 10.10.2000]

[2] Ahlin, Lars & Zander, Jens: Principles of Wireless Communications. Studentlitteratur, Lund, 1998. 525p.

[3] Anderson, Cynthia E. & Wickert, Mark A.: The Performance of a Wireless LAN Access Node Using Antenna Beamforming for Dynamic and Static Users. Radio and Wireless Conference, August 1999, pp.27-30.

[4] Andren, Carl: Intersil Prism II radio Jamming Margin Test. Intersil Corporation. January 2000. 9p. <http://www.intersil.com/prism/papers/jamming_margin_test_r2.doc> [referred 17.10.2000]

[5] Andren, Carl & Webster, Mark: CCK Modulation Delivers 11Mbps High Rate IEEE 802.11 Extension. Harris Semiconductor, Palm Bay, Florida. 1998. 8p. <http://www.intersil.com/prism/papers/CCK_Mod_Delivers_11Mbps.htm> [referred 17.10.2000]

[6] Gligor, Virgil D.: A note on the denial-of-service problem. Proceedings of 1983 IEEE Symposium on Research in Security and Privacy. 1983. pp. 139-149.

[7] Cell Phone Flaw Opens Security Hole. Interactive Week, 18 September 2000. <http://www.zdnet.com/intweek/stories/news/0,4164,2630342,00.html> [referred 19.10.2000]

[8] C-Guard Cellular FireWall. Netline Communications Technologies Inc. Israel. <http://www.cguard.com/English/latests/> [referred 19.10.2000]

[9] Denial-of-Service Threat Found in Some Nokia Phones. Newsbytes. 31 August 2000. <http://www.info-sec.com/denial/00/denial_083100a_j.shtml> [referred 19.10.2000]

[10] Fullmer, Chane L. & Garcia-Luna-Aceves, J.J.: Complete Single-Channel Solutions to Hidden Terminal Problem in Wireless LANs. Communications, ICC '97 Montreal, Towards the Knowledge Millennium, IEEE International Conference on, Vol. 2, 1997, pp. 575-579.

[11] Haykin, Simon: Communications Systems. 4th Edition. John Wiley & Sons, New York. 2000. 816p.

[12] Henttu, Pertti: A New Interference Suppression Algoritm Against Broadband Constant Envelope Interference. 21st Century Military Communications. MILCOM 2000 Los Angeles. 5p.

[13] Intersil Corporation: Effects of Microwave Interference on IEEE 802.11 WLAN Reliability. IEEE P802.11 - 98/240, May 1998, 22p. <http://www.wlana.com/PDF/Effects%20of%20Interference%20on%IEEE802.11%20WLAN%20Reliability.PDF> [referred 25.9.2000]

[14] Kosola, Jyri: Communications COTS and EPM. MSc Thesis, The Royal Military College of Science, Department of Aerospace, Power and Sensors, Shrivenham 1998, 108p.

[15] Kosola, Jyri & Solante, Tero: Digitaalinen taistelukenttä - Informaatioajan sotakoneen tekniikka. Maanpuolustuskorkeakoulu, julkaisusarja 1 N:o 7. 2000. 402 p.

[16] Marincic, A. & Milovanovic, D.: Wireless local area networks. Telecommunications in Modern Satellite, Cable and Broadcasting Services, 4th International Conference on, Vol. 1, 1999. pp. 291-299.

[17] Mouly, Michel & Pautet, Marie-Bernadette: The GSM System for Mobile Communications, Europe Media Duplication S.S, 1992. 695 p.

[18] Penttinen, Jyrki: GSM-tekniikka. WSOY, Porvoo 1999, 349 p.

[19] Schleher, D. Curtis: Electronic Warfare in the Information Age. Artech House, Norwood MA. 1999, 605 p.

[20] Technical Specification GSM 05.02 version 5.1.0. ETSI, August 1996. 38p.

[21] Technical Specification GSM 05.05 version 5.0.0. ETSI, March 1996. 48p.

[22] Turletti, Thierry: GMSK in a nutshell. Laboratory of Computer Science, Massachusetts Institute of Technology, April 1996. <ftp://ftp.tns.lcs.mit.edu/pub/papers/gmsk.ps.gz> [referred 6.10.2000]

[23] Wells, M.C.: Adaptive antennas for frequency re-use in every cell network. Mobile Communications Towards the Year 2000. 1994. pp. 11/1-11/6.