Chapter 8 – MILITARY RELEVANCE: SECURITY, INTERCEPTABILITY, ECM ISSUES

8.1 GENERAL SECURITY ISSUES

Many security issues arise in wireless networks because of the fact that wireless is a shared medium and everything that is transmitted or received over a wireless network can be intercepted. Because of the large range of the transmissions (a few kilometers), the 802.16 signal is particularly vulnerable since it is made available (for interception and detection) to anyone located within this large perimeter.

To secure a mobile wireless network, one must consider the following attributes: availability, confidentiality, integrity, authentication, and non-repudiation.

- **Availability** ensures the survivability of network services despite denial of service attacks. A denial of service attack could be launched at any layer of a wireless network. On the physical and media access control (MAC) layers, an adversary could employ jamming to interfere with communication on physical channels. On the network layer, an adversary could disrupt the routing protocol and disconnect the network. On the higher layers, an adversary could bring down high-level services. One such target is the key management service, an essential service for any security framework.
- **Confidentiality** (secrecy) ensures that certain information is never disclosed to unauthorized entities. Network transmission of sensitive information, such as strategic or tactical military information, requires confidentiality. Leakage of such information to enemies could have devastating consequences. Routing information must also remain confidential in certain cases, because the information might be valuable for enemies to identify and to locate their targets in a battlefield.
- **Integrity** guarantees that a message being transferred is never corrupted. A message could be corrupted because of benign failures, such as radio propagation impairment, or because of malicious attacks on the network.
- **Authentication** enables a node to validate the identity of the peer node it is communicating with. Without authentication, an adversary could masquerade a node, thus gaining unauthorized access to resource and sensitive information and interfering with the operation of other nodes.
- Finally, **non-repudiation** ensures that the origin of a message cannot deny having sent the message. Non-repudiation is useful for detection and isolation of compromised nodes. When a node A receives an erroneous message from a node B, non-repudiation allows A to accuse B using this message and to convince other nodes that B is compromised.

Two types of attacks are considered in communications:

- **Passive Attacks** – These types of attacks typically involve eavesdropping of data. The major advantage for the attacker in passive attacks is that in a wireless environment the attack is usually impossible to detect. This also makes defending against such attacks difficult.
- **Active Attacks** – These involve actions performed by adversaries, for instance the replication, modification and deletion of exchanged data.

8.2 SECURITY CONSIDERATIONS FOR 802.11

The US standard IEEE 802.11 with its several extensions or versions (indicated by small letters) gives specifications for WLAN systems. A WLAN system is a radio system with a typical range from several

ten up to several hundred meters. The main purposes are to connect client-PCs and servers with each other and with peripheral equipment like printers. The necessary bandwidth is generally higher than that of a WPAN system because of the requirements to exchange larger files and to run lavish applications across the network. The nominal data rates reach from 1 Mbps for the older system versions up to 54 Mbps for the newer ones. The maximum allowed transmitter power depends on the region (e.g. Europe or US), the application and the frequency range. EIRP values (Equivalent Isotropically Radiated Power) for indoor applications are typically limited to 100 or 200 mW and for outdoor applications to 1 W.

The 802.11 wireless networks operate in one of two modes, ad-hoc or infrastructure mode. In the ad-hoc mode the network is self organizing its structure and each client is able to communicate directly with the other clients within the network. The ad-hoc mode is designed such that only the clients within transmission range (within the same cell) of each other can communicate. If a client in an ad-hoc network wishes to communicate outside of the cell, a member of the cell must operate as a gateway and perform routing. In infrastructure mode, each client sends all of its communications to a central station or Access Point (AP). The AP is responsible for the synchronization, for energy economy measures and for the multiple access steering in the LAN. The AP acts as an Ethernet bridge and forwards the communications onto the appropriate network, either the wired network, or the wireless network. Roaming between APs is supported.

Above the MAC layer a 802.11 system looks like every other 802.x LAN and provides comparable services, e.g. in connection with the often used wired Ethernet LAN (IEEE 802.3). The mechanisms for the channel access in the MAC layer are the same for all 802.11 versions. The access method is the CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance). With this method the channel activity is observed and a new transmission is only started, if an appropriate channel is found. In addition, the mobility management is done in the MAC layer. Only slow motion is allowed for the mobile terminals. The transport of information is done in the packet switched mode.

8.3 THE STANDARDS/SYSTEMS

At present, the mostly used system version is the 802.11b, which works in the license-exempt IMS frequency band around 2.4 GHz. It uses PSK modulation types and a DSSS technique with a channel bandwidth of 22 MHz. The nominal data rates are 5.5 and 11 Mbps. The purpose of the DSSS technique with its short code length of 8 chips is to improve the separation against other users in the IMS frequency band and to separate transmitted information bits from each other. The type for the spreading/coding method used here is CCK (Complementary Code Keying). The separation of different channels used in parallel is done with FDMA. The available frequency band reaches from about 2.40 GHz to 2.48 GHz and is divided into fourteen overlapping channels which give the available frequency set pattern. Within this frequency range only three non-overlapping channels each with a width of 22 MHz can be used in parallel. In Europe the parallel use of more than three of such channels is in fact allowed but in these cases there are frequency overlaps.

In the US influenced countries the probably most interesting realization in the future will be the version 802.11a which uses the frequency band around 5 GHz. The development takes care of the regulation concerning the US license-exempt band in this frequency region. This band is exclusively reserved for WLAN applications, other systems like e.g. microwave ovens are not allowed. The nominal data rates reach from 6 up to 54 Mbps. The bandwidth of each channel is 20 MHz and up to 12 non-overlapping channels will be available. The modulation types are PSK with 2 and 4 states and QAM with 16 and 64 states. The modulation type actually used depends on the requested data rate. As the competitive systems in Europe (HIPERLAN II) and Japan (HISWANa: High Speed Wireless Access Network, Version a), IEEE 802.11a uses the OFDM method too. This frequency multiplexing method allows high data rates with comparatively good robustness against frequency diversity disturbances. The use of the

today's 802.11a version is not allowed in Europe because it is not fitted to the features DFS (Dynamic Frequency Selection) and TPC (Transmit Power Control). These features are prescribed in Europe and should prevent conflicts with the HIPERLAN II system.

The version 802.11g is comparatively new. The aim is to enable higher data rates in the 2.4 GHz band, at present 22 Mbps. 802.11g shall be backward compatible with 802.11b. For high data rates, OFDM and for the lower data rates CCK shall be used. At present it seems, that the work within this group does not show quick progress. The reason could be, that the development tendency is more directed towards the version 802.11a with its higher available frequency bandwidth and data rates.

The 802.11h standard is the version 802.11a, supplemented by DFS and TPC which are necessary for the use in the European 5 GHz band. DFS seeks the frequency channels with the best availability and TPC minimizes the transmitted power. These features should prevent serious conflicts with HIPERLAN II.

802.11i includes extensions of the MAC protocol with improved mechanisms for security and authentication. The approval is planned for the year 2003.

8.4 INTERCEPTABILITY

The standardized 802.11 parameters of RF frequencies, bandwidths, waveforms, protocol formats and the security mechanisms are well known. In addition, the WLAN principle is not well suited to sophisticated protection measures against interception. Because of the requirement of setting up radio connections in a flexible manner with comparatively cheap equipment, the hurdles for getting network access have to be moderate. On the civil market several tools for monitoring 802.11 radio traffic are offered, partly free of charge. One example is the *Netstumbler* which could be used together with the *Orinoco* WLAN board of Agere Systems. But a monitoring is only possible within comparatively small distances from the network, caused by the mostly low emitted power and the high radio frequencies with their limited transmission range.

There would be perhaps some interception difficulties if some of the elementary parameters of the 802.11 signals/systems were changed. This could have been done with the aim to adapt to specific (e.g. military) requirements. An example could be the choice of a lower radio frequency for extending the transmission range. Other elementary parameters concern the methods of modulation, spreading and multiplexing. To intercept such special systems with unknown parameters, the requirements for an interception receiver concerning bandwidth, dynamic range and speed could be demanding.

The available 802.11 products (802.11b systems) have several protocol security mechanisms, but these mechanisms do not constitute high hurdles for a well equipped interceptor. While overcoming these hurdles, the access to the foreign network opens up several possibilities. The aim of the activities subsequently possible (e.g. intrusion and insertion of falsified information) could go beyond the classical interception tasks (examination of technical characteristics, identification, traffic analysis, message content). Nevertheless most of the weaknesses of the protocol security mechanisms are discussed in this section and not in the next section concerning ECM issues because they concern primarily the interception.

At the lowest level the acceptance of a requesting terminal is regulated by means of an ID number, the ESSID (Electronic System ID). An administrator has entered the ESSIDs into all involved APs and mobile terminals in advance. The ESSID indicates the access entitlement of a terminal but does not allow its unambiguous identification. There are two weaknesses concerning the ESSID: Firstly, it is no problem to find a general access number with the aim to monitor the radio traffic. Secondly, most terminals schedule the option *any* in their configuration file. With this setting the terminal will be allowed to get access to any network.

The authentication mechanisms allow only the entitled terminals to take part in the communication. The checking is done in the Link Level Authentication process between the involved stations. The mechanisms use the MAC addresses of the mobile terminals, which are stored in the AP access list. But it is possible to change the MAC address within most of the available products. Such a manipulated terminal will be allowed to get access to foreign networks. With many of the available products an additional weakness is the awkwardness of the authentication process within larger networks. The consequence may be, that the complex authentication process is not used. In this way the access to such a foreign network would be made easier.

Although the ciphering of the information content could be done by means of the WEP (Wired Equivalent Privacy) protocol, the security of the today's simple version with a key length of 40 bit is limited. WEP uses a static key. If the key is known there is no longer any protection. This concerns not only the data ciphering but also the higher quality authentication protocol because therein WEP is used too. Otherwise, if the key is not known, one has the possibility to observe the traffic for a longer time and to extract important information. Using this information it is possible to compute the key and decipher the information content. The available tools for these tasks are e.g. *Airsnort* and *Wepcrack,* which are offered in the Internet, free of charge. By means of these tools the key could be extracted within a few hours. There are two additionally weaknesses: Firstly, WEP is only an optional system feature, it is not included in the standard. Companies who offer 802.11 conform products are not obliged to offer the WEP protocol. Secondly, products offered from different companies could have different key lengths. This often causes non-interoperability while using WEP. As a consequence, only the simple common WEP protocol is used or WEP is not used at all. In this way the interception would be made easier.

8.5 ESM AND ECM FOR THE IEEE 802.16 STANDARDS

The 802.16 standards provide certain protection measures against signal interception on the MAC layer with possible improvements for satisfying not only commercial but also military use. It also has been mentioned that the main weakness is provided by the physical layer because of its highly vulnerability to signal detection, direction finding, and jamming. This assumption may be based on commercial needs, for example:

- W-MAN radio base stations use antennas with relatively broad sector beams of up to 90° beamwidth for covering as many terminal stations as possible.
- Distances between the base and terminal stations reach from 2 km (at 42 GHz) to 15 km (at 2.4 GHz), dependent on the used frequency band.
- The possible frequency bands are allocated to the user and known to the public.

Under these circumstances it will be possible for an adversary to locate his ESM/ECM equipment within the radio path between the base and the terminal station for detecting the downlink signal and jamming the uplink signal.

However, tactical military applications will not be dependent so much on commercial aspects. That means, military may use measures able to reduce considerably the danger of signal detection by an adversary, which is the pre-condition for effective jamming, for example:

- The radio base stations may have antenna structures of smaller beamwidth, for example 15° or less. For detecting the downlink signal, the ESM equipment needs to be located then more precisely to the radio path.
- The distances between the base and terminal stations may be less than a few km. In this case an adversary will have difficulties to put his ESM equipment within the radio path near the base station. He has to try to detect the more attenuated signal from a place behind a terminal station.

- The base stations may use power control. This function is not yet included in the IEEE 802.16, but in the ETSI standards for Hiperman and Hiperaccess. However, one can assume, that the power control function will be overtaken also from the 802.16 standards. Using the power control function, together with the measures mentioned before, will make it harder for an adversary to detect the downlink signal.
- In difference to commercial providers, who have to use allocated frequency bands publicly known, military may have the choice among a number of frequency bands within the lower frequency range of 2 – 11 GHz (802.16a), or the upper range of 10 – 66 GHz (802.16-2001). Accordingly, an adversary does not know the used frequency bands a priory and has to search for the downlink signal within rather broad frequency ranges. Of course, this task would become still more difficult, if one would change the used frequency band within more or less short periods.
- If one uses the frequencies around 60 GHz for short distances one would have the advantage of, compared to other frequencies in this range, very high propagation attenuation.
- Military may prefer the standard 802.16a for the frequency range 2 – 11 GHz due to the requirement of only near line of sight conditions. This would include the advantage to transmit by OFDM, a technique which is robust against frequency selective disturbances or narrow band jamming.

As mentioned above, effective signal jamming needs to detect the signal before. Of course, a base or terminal station may be jammed by an adversary's jammer without detecting a signal. But, taking into account the above described measures, it would need much power over a broad frequency range for the jamming signal to obtain sufficient effectiveness, with a high probability of physical destruction of the adversary's jammer.

For the susceptibility and ESM and ECM for the whole spectrum of IEEE 802.11 series of standards see Chapter 8, specifically devoted to this issue.

8.6 ECM ISSUES

It seems not difficult to jam a whole WLAN network if the jammer could be placed near enough. The comparatively high radio frequencies have limited transmission range. While the nominal ranges are limited to several hundred meters, the application of directional jammer antennas, possibly combined with higher transmitter powers, could extend the range. Smart jamming in kind of intelligent jamming of single terminals is probable of minor importance because of the limited geometrical network extension. An exception would be the case, where the jammer is placed inside of a network, e.g. in a local area mission.

If there exist several (sub-) networks, which are wirelessly connected, it seems easier to place a jammer *between* networks than to place it *inside* a network. The victim connections between the networks will be realized with techniques in agreement with 802.11, 802.16 (WMAN) standards or other directional radio systems for larger distances.

As mentioned in the last section, it is possible to surmount the today's protocol security mechanisms by means of appropriate tools. The aim could be not only the interception but the intrusion and insertion of falsified information too. This possibility is not only given because of the weaknesses concerning authentication and data ciphering. In addition the specific realization of the CRC mechanism (Cyclic Redundancy Check) is a weakness. This mechanism is used to recognize unintentional data changes during transmission, i. e. the message integrity should be controlled. But the additional checksum bits are attached *after* the information has been ciphered. This gives the possibility to manipulate the information and afterwards adapt the checksum bits. In this way messages may be modified in transit without

detection, in violation of the security goals of the provider. The details of such measures belong more to the Information Warfare than to the Electronic Warfare section.

8.7 MILITARY RELEVANCE

The possible use of the today's 802.11 systems for own forces would be limited because of the discussed weaknesses. Nevertheless the system use is conceivable in a limited and well controlled area, e.g. in a non-distributed headquarter. The probability of fraudulent use has to be low.

A disadvantage is the lack of DFS and TPC if several different networks are used in parallel and the network distances are low. Then strong interferences are to be expected.

Another disadvantage of the 802.11b systems could be the minor data rate. Instead of the nominal 5.5 or 11 Mbps the practically reached data rates are at best between 3 and 4 Mbps, also for isolated point to point connections. The version 802.11a with its up to twelve 20 MHz channels will have more capacity.

There are perhaps two militarily interesting development tendencies: a) The recommendations and the further work of several civil groups with the aim to improve important features; and b) The possible change or adaptation of important system parameters to specific (military) requirements. In the following, some items concerning these tendencies are given.

a) Recommendations and further work of civil groups or companies:

- For WLAN participants it is recommended to consequently use the today's offered security mechanisms concerning authentication and ciphering as far as possible. It was found out that in most of the observed WLAN networks the mechanisms were not used because the participants are not really aware of the possibility or probability of fraudulent use.
- It was recommended to use the WLAN in front of a firewall, i.e. the firewall stands protectively in front of the host computer.
- Another recommendation is the application of an IDS (Intrusion Detection System).
- For information in need of protection it is recommended to use the WLAN independent VPN (Virtually Private Network) concept. A VPN is based on the so-called tunneling method, mostly realized in layer 3. The tools used in this context could be IPSEC or PPTP (Point-to-Point Tunneling Protocol). Another known security mechanism is the SSH (Secure Shell).
- Some companies use further developed methods to obtain more authentication security. These methods are combinations of the EAP (Extensible Authentication Protocol) and the suggested standard 802.1X for the controlled Ethernet access. EAP is an extension of the RADIUS (Remote Access Dial-In User Service) with PAP (Pathword Authentication Protocol) or CHAP (Challenge Handshake Authentication Protocol). With 802.1X the authorized access for larger user groups with wireless and wired terminals can be organized.
- Some companies offered further developed WEP ciphering methods: With the Agere Systems' solution *WEPplus* the generation of the initialization vectors for the ciphering is improved and the susceptibility to AirSnort should be removed. WEPplus is backward compatible with the simple WEP. RSA Data Security Inc. offered a new method called FPK (Fast Packet Keying) with which the code is changed for every new data packet.
- The weaknesses of authentication and ciphering in the today's 802.11 versions are well known and there are official endeavors to improve the mechanisms. The standardization group 802.11i is working on it. One important item is the application of the AES (Advanced Encryption Standard). Before the standardization work will be finished, the group recommends the general use of the

104 bit ciphering key length and the application of the TKIP (Temporary Key Integrity Protocol). With the TKIP the WEP key is dynamically changed. Herewith, an individual packet coding is realized and the message integrity check is improved.

b) Change or adaption of important system parameters

- Several experiments has been done using a lower radio frequency. The aim is the extension of the possible transmitting range while still exploiting the comparatively cheap COTS products. An additional advantage could be the less interference in the new frequency band. A possible disadvantage may be the reduced available bandwidth. In this case one has to reckon with reduced channel capacity.
- The variation of other important 802.11 parameters with the aim to adapt to specific use is also conceivable. Interesting features for variation could be for example the methods for modulation, spreading or multiplexing. An additional advantage of changed system parameters should be the difficulties for an adversary to use the available 802.11 monitoring or intruding systems without adaptation.