

# Risk Analysis – IEEE 802.11p

Report by H. Viittala

Ajoneuvon / työkoneen langattomat lähiverkot (ALMA)

| Version | Date       | Author | Status   | Notes            |
|---------|------------|--------|----------|------------------|
| 0.1     | 30.7.2009  | HV     | Draft    | Document created |
| 0.2     | 31.7.2009  | HV     | Draft    | Sent to Juha I.  |
| 1.0     | 21.8.2009  | HV     | Final    | Sent to Juha I.  |
| 2.0     | 21.12.2009 | Jl     | Accepted |                  |

## TERMS AND ABBREVIATIONS:

|                  |  |
|------------------|--|
| $\Delta f$       | Subcarrier frequency spacing   |
| $B_{\text{SIG}}$ | Signal bandwidth   |
| $C/N$            | Carrier-to-noise power ratio   |
| $N_{\text{SD}}$  | Number of data subcarriers   |
| $N_{\text{SP}}$  | Number of pilot subcarriers  |
| $N_{\text{ST}}$  | Total number of subcarriers  |
| $T_{\text{FFT}}$ | Inverse fast Fourier transform (IFFT)/ Fast Fourier transform (FFT) period |
| $T_{\text{GI}}$  | Guard interval duration  |
| $T_{\text{SYM}}$ | Symbol interval  |
| AC               | Access Category  |
| AES              | Advanced Encryption Standard   |
| AP               | Access Point   |
| BSSID            | Basic Service Set Identification   |
| BPSK             | Binary Phase Shift Keying  |
| BSS              | Basic Service Set  |
| CCH              | Control Channel  |
| CEPT             | European Conference of Postal and Telecommunication                        |
| CRC              | Cyclic Redundancy Check  |
| CSMA/CA          | Carrier Sense Multiple Access with Collision Avoidance                     |
| CTS              | Clear-To-Send  |
| DCF              | Distributed Coordination Function  |
| DSRC             | Dedicated Short Range Communications                                       |
| EAP              | Extensible Authentication Protocol   |
| EDCA             | Enhanced Distributed Channel Access  |
| EIRP             | Effective Isotropic Radiated Power   |
| FCC              | Federal Communication Commission   |
| FEC              | Forward Error Correction   |
| FFT              | Fast Fourier Transform   |
| GI               | Guard Interval   |
| HC               | Hybrid Coordinator   |
| HCCA             | HCF Controlled Channel Access  |
| HCF              | Hybrid Coordination Function   |
| I2V              | Infrastructure-To-Vehicle  |
| IFFT             | Inverse Fast Fourier Transform   |
| ITS              | Intelligent Transport System   |
| LOS              | Line-Of-Sight  |
| MAC              | Medium Access  |
| NAV              | Network Allocation Vector  |
| NLOS             | Non-LOS  |
| OBU              | Onboard Unit   |
| OFDM             | Orthogonal Frequency Division Multiplexing                                 |
| PCF              | Point Coordination Function  |
| PER              | Packet Error Rate  |
| PHY              | Physical   |
| QAM              | Quadrature Amplitude Modulation  |
| QoS              | Quality-of-Service   |
| QPSK             | Quaternary Phase Shift Keying  |
| QSTA             | Quality-of-Service Station   |
| RMS              | Root Mean Square   |
| RSU              | Roadside Unit  |

|       |                                   |
|-------|-----------------------------------|
| RTS   | Request-To-Send                   |
| SSID  | Service Set Identify              |
| STA   | Station                           |
| TBTT  | Target Beacon Transmission Time   |
| TKIP  | Temporal Key Integration Protocol |
| TPC   | Transmission Power Control        |
| V2V   | Vehicle-To-Vehicle                |
| WBSS  | Wave BSS                          |
| WEP   | Wired Equivalent Privacy          |
| Wi-Fi | Wireless Fidelity                 |
| WLAN  | Wireless Local Area Network       |
| WMM   | Wi-Fi Multimedia                  |
| WPA   | Wi-Fi Protected Access            |

## TABLE OF CONTENTS

|  |    |
|--|----|
| 1. INTRODUCTION .....                            | 6  |
| 2. SPECTRUM ALLOCATION .....                     | 6  |
| 3. IEEE 802.11.....                              | 7  |
| 3.1. IEEE 802.11 OFDM PHY .....                  | 7  |
| 3.2. IEEE 802.11 MAC.....                        | 9  |
| 3.3. CONCLUSION .....                            | 11 |
| 4. IEEE 802.11P – AMENDMENT TO IEEE 802.11 ..... | 13 |
| 4.1. PHY LAYER AMENDMENTS .....                  | 13 |
| 4.2. MAC LAYER AMENDMENTS.....                   | 15 |
| 4.3. CONCLUSION .....                            | 15 |
| 5. SECURITY.....                                 | 18 |
| 6. CONCLUSION.....                               | 20 |
| 7. REFERENCES .....                              | 21 |

## LIST OF FIGURES

|   |    |
|---|----|
| FIGURE 1. SPECTRUM ALLOCATION IN THE USA AND EUROPE. ....   | 7  |
| FIGURE 2. TRANSMIT SPECTRUM MASK OF 802.11 IN THE 5 GHZ BAND. ....                                      | 9  |
| FIGURE 3. MAC ARCHITECTURE OF 802.11. ....  | 10 |
| FIGURE 4. PER PERFORMANCE OF 802.11 OFDM PHY. ....  | 11 |
| FIGURE 5. MEAN DELAYS FOR DIFFERENT ACS UNDER EDCA. ....  | 12 |
| FIGURE 6. WI-FI UNIT SHIPMENTS. ....  | 12 |
| FIGURE 7. TRANSMISSION MASKS OF CLASS A TO D OPERATIONS IN THE 5.9 DSRC SPECTRUM. ....                  | 14 |
| FIGURE 8. BER FOR AN URBAN ROAD AND A MOTORWAY WITH BPSK (LEFT) AND QPSK (RIGHT) IN A LOS CHANNEL. .... | 16 |
| FIGURE 9. PER FOR AN URBAN ROAD AND A MOTORWAY WITH BPSK (LEFT) AND QPSK (RIGHT) IN A LOS CHANNEL. .... | 16 |
| FIGURE 10. PACKET LOSS AS A FUNCTION OF VEHICLE DENSITY. ....   | 17 |
| FIGURE 11. AVERAGE DELAY AS A FUNCTION OF VEHICLE DENSITY. ....   | 17 |
| FIGURE 12. GENERAL SECURITY ATTACKS AGAINST WLANS. ....   | 18 |
| FIGURE 13. WEP PRIVACY USING RC4 ALGORITHM. ....  | 19 |

## LIST OF TABLES

|  |    |
|--|----|
| TABLE 1. CHANNEL USE IN THE DSRC SPECTRUM IN THE USA. ....                     | 6  |
| TABLE 2. 802.11 OFDM PHY PARAMETERS. ....                                      | 8  |
| TABLE 3. 802.11 OFDM PHY TIMING RELATED PARAMETERS. ....                       | 8  |
| TABLE 4. MAXIMUM ALLOWABLE OUTPUT POWER BY REGULATORY DOMAIN. ....             | 9  |
| TABLE 5. RECEIVER PERFORMANCE REQUIREMENTS FOR TYPE 1 AND TYPE 2 DEVICES. .... | 14 |
| TABLE 6. DEVICE CLASSES AND TRANSMIT POWER LEVELS. ....                        | 14 |
| TABLE 7. SWOT ANALYSIS OF 802.11P. ....  | 20 |

## 1. Introduction

The IEEE 802.11p is the draft amendment to the IEEE 802.11 standard [1] intended for vehicle-to-vehicle (V2V) ad hoc communication in high-speed vehicular environment [2]. The IEEE 802.11p amendment will be based on the ASTM E 2213-03 document [3].

Vehicular safety communication requires real-time communication with high reliability imposing a set of new requirements on wireless communication systems. To meet real-time requirement, channel access should be timely and predictable. [2] High-speed vehicles on a complex road environment present challenges at the physical (PHY) layer level.

## 2. Spectrum allocation

The dedicated short range communications (DSRC) spectrum of 75 MHz at 5.9 GHz has been allocated to be used exclusively for V2V and infrastructure-to-vehicle (I2V) communications by the Federal Communication Commission in the USA. The DRSC band is free but licensed spectrum. The DSRC spectrum is divided in seven 10 MHz wide channels. The channel number 178 is control channel (CCH) and it is reserved for safety communications only. Channels 172 and 184 are designed for public safety applications. The channel use is summarized in Table 1. [4],[5]

Table 1. Channel use in the DSRC spectrum in the USA

| Channel No. | Freq. Range [MHz] | Max. EIRP <sup>1</sup> [dBm] | Channel Use     |
|-------------|-------------------|------------------------------|-----------------|
| 170         | 5850-5855         | -                            | Reserved        |
| 172         | 5855-5865         | 33                           | Service Channel |
| 174         | 5865-5875         | 33                           | Service Channel |
| 175         | 5865-5885         | 23                           | Service Channel |
| 176         | 5875-5885         | 33                           | Service Channel |
| 178         | 5885-5895         | 33/44.8                      | Control Channel |
| 180         | 5895-5905         | 23                           | Service Channel |
| 181         | 5895-5915         | 23                           | Service Channel |
| 182         | 5905-5915         | 23                           | Service Channel |
| 184         | 5915-5925         | 33/40                        | Service Channel |

<sup>1</sup>EIRP = Effective Isotropic Radiated Power

The frequency spectrum within the band of 5.875 – 5.925 GHz has been designated for intelligent transport systems (ITS) by European Conference of Postal and Telecommunication (CEPT) in Europe. The maximum EIRP for an ITS station is limited to 23 dBm/MHz. The frequency sub-band 5.875 – 5.905 GHz has been allocated for a non-exclusive basis for ITS road safety applications. [6] The DSRC channel use in the USA and Europe are presented in Figure 1.

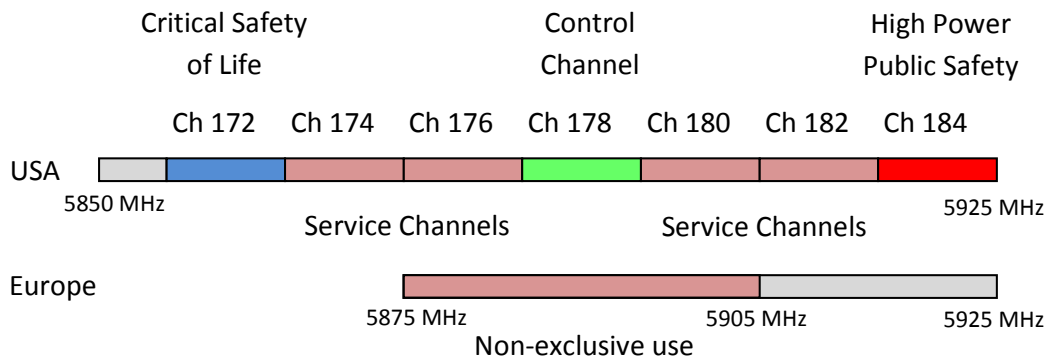


Figure 1. Spectrum allocation in the USA and Europe.

### 3. IEEE 802.11

The IEEE 802.11x standard family, known also as WLAN (wireless local area network) or Wireless Fidelity (Wi-Fi), consists of over-the-air modulation techniques using the same basic protocol. In 2007, the new edition of the IEEE 802.11 standard was published including amendments 1 – 8 (802.11a/b/d/g/h/i/j/e). [1] The 802.11p amendment will be based on the OFDM PHY (orthogonal frequency division multiplexing physical layer) of the 802.11 standard, formerly known as the 802.11a standard. The OFDM PHY was chosen for 802.11p since it is already operating in the 5 GHz band, and hence, it is not difficult to configure radios to operate in the 5.9 GHz band. Therefore, only the OFDM PHY will be discussed here.

#### 3.1. IEEE 802.11 OFDM PHY

The OFDM PHY of the IEEE 802.11 standard provides communications with data rates of 6, 9, 12, 18, 24, 36, 48 and 54 Mbps having the 20 MHz channel spacing in the 5 GHz ISM band. The support of data rates of 6, 12 and 24 Mbps are mandatory. When OFDM system applies a “half-clocked” operation, i.e., using 10 MHz channel spacing, the data rates above are halved and mandatory supported data rates are 3, 6 and 12 Mbps. There is also a “quarter-clocked” operation using 5 MHz channel spacing presented in the standard. An OFDM symbol is formed by 52 subcarriers including data and pilot subcarriers in each operation mode. When same number of subcarriers is utilized with different bandwidth, OFDM timing parameters are changed correspondingly. All operation modes apply binary phase shift keying (BPSK), quaternary phase shift keying (QPSK), 16-or 64-quadrature amplitude modulation (16-QAM or 64-QAM) modulation with forward error correction (FEC) coding, i.e., convolutional coding having a coding rate of 1/2, 2/3 or 3/4. The data rate and timing related parameters are summarized in Table 2 and Table 3, respectively. [1]

In Table 2, it is also presented minimum receiver sensitivity, adjacent and alternate channel rejection levels for OFDM PHY. Adjacent or alternate channel rejection is measured by setting a signal power 3 dB above the rate dependent sensitivity and raising a power of an interfering signal in an adjacent or nonadjacent channel until the packet error rate (PER) of 10 % is caused. Power difference between an interfering signal and a desired signal is corresponding rejection. [1]

Table 2. 802.11 OFDM PHY parameters

| Mode | Data Rate [Mbps] (20 MHz Channel Spacing) | Data Rate [Mbps] (10 MHz Channel Spacing) | Modulation | Convolutional Coding Rate | Minimum Receiver Sensitivity [dBm] | Adjacent Channel Rejection [dB] | Alternate Channel Rejection [dB] |
|------|---|---|------------|---------------------------|------------------------------------|---------------------------------|----------------------------------|
| 1    | 6   | 3   | BPSK       | 1/2                       | -82                                | 16                              | 32                               |
| 2    | 9   | 4.5                                       | BPSK       | 3/4                       | -81                                | 15                              | 31                               |
| 3    | 12  | 6   | QPSK       | 1/2                       | -79                                | 13                              | 29                               |
| 4    | 18  | 9   | QPSK       | 3/4                       | -77                                | 11                              | 27                               |
| 5    | 24  | 12  | 16-QAM     | 1/2                       | -74                                | 8                               | 24                               |
| 6    | 36  | 18  | 16-QAM     | 3/4                       | -70                                | 4                               | 20                               |
| 7    | 48  | 24  | 64-QAM     | 2/3                       | -66                                | 0                               | 16                               |
| 8    | 54  | 27  | 64-QAM     | 3/4                       | -65                                | -1                              | 15                               |

= Mandatory

Table 3. 802.11 OFDM PHY timing related parameters

| Parameter  | Value (20 MHz Channel Spacing)   | Value (10 MHz Channel Spacing)   |
|--|----------------------------------|----------------------------------|
| Number of data subcarriers ( $N_{SD}$ )  | 48                               | 48                               |
| Number of pilot subcarriers ( $N_{SP}$ )   | 4                                | 4                                |
| Number of subcarriers, total ( $N_{ST}$ )  | 52                               | 52                               |
| Subcarrier frequency spacing ( $\Delta f$ )  | 0.3125 MHz (20 MHz/64)           | 0.15625 MHz (10 MHz/64)          |
| Inverse fast Fourier transform (IFFT)/ Fast Fourier transform (FFT) period ( $T_{FFT}$ ) | 3.2 $\mu s$ ( $1/\Delta f$ )     | 6.4 $\mu s$ ( $1/\Delta f$ )     |
| Guard interval (GI) duration ( $T_{GI}$ )  | 0.8 $\mu s$ ( $T_{FFT}/4$ )      | 1.6 $\mu s$ ( $T_{FFT}/4$ )      |
| Symbol interval ( $T_{SYM}$ )  | 4 $\mu s$ ( $T_{GI} + T_{FFT}$ ) | 8 $\mu s$ ( $T_{GI} + T_{FFT}$ ) |
| Signal bandwidth ( $B_{SIG}$ )   | 16.6 MHz                         | 8.3 MHz                          |

In the 802.11, transmission power control (TPC) service is used to satisfy regulatory requirements including a specification for maximum transmit power and a mitigation requirement for each allowed channel. A station (STA) may select any transmit power in a channel within the following constraints:

- Before transmitting in a channel, a STA determines a regulatory maximum transmit power and a local maximum transmit power for a channel in a current regulatory domain
- An access point (AP) shall use a transmit power less than or equal to a regulatory maximum transmit power level for a channel. However, the AP shall also ensure a regulatory mitigation requirement is met.
- A STA that is not an AP shall use a transmit power less than or equal to a local maximum transmit power level for a channel.

A transmit power may dynamically adapted by a STA by using any criteria, e.g., path loss and link margin estimates. The maximum transmit power levels in the USA and Europe are tabulated in Table 4 and the transmit spectrum mask is illustrated in Figure 2, respectively. [1]

Table 4. Maximum allowable output power by regulatory domain

| Frequency Band [GHz] | United States Maximum Output Power With up to 6 dBi Antenna Gain [mW] | Europe (EIRP) [mW] |
|----------------------|---|--------------------|
| 5.15 – 5.25          | 40 (2.5 mW/MHz)   | 200                |
| 5.25 – 5.35          | 200 (12.5 mW/MHz)   | 200                |
| 5.470 – 5.725        | -   | 1000               |
| 5.725 – 5.825        | 800 (50 mW/MHz)   | -                  |

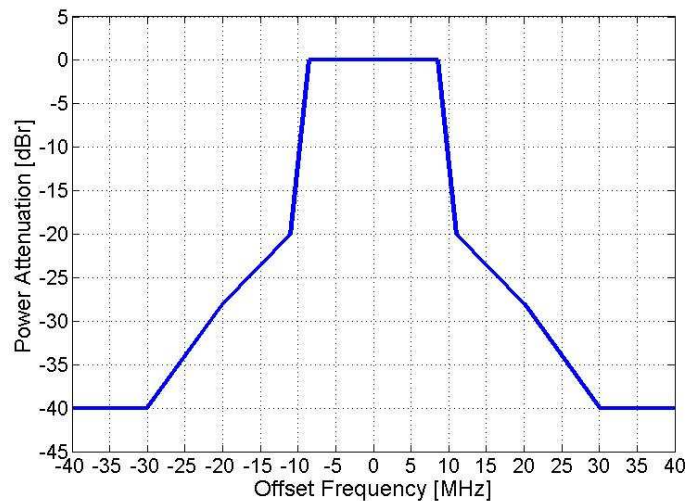


Figure 2. Transmit spectrum mask of 802.11 in the 5 GHz band.

In OFDM PHY, three temperature ranges are specified. Type 1, defined as 0°C to 40°C, is designated for office environments. Type 2, defined as -20°C to 50°C, and Type 3, defined as -30°C to 70°C are designated for industrial environments. [1]

### 3.2. IEEE 802.11 MAC

The architecture of the 802.11 medium access (MAC) sublayer can be described, as depicted in Figure 3, providing point coordination function (PCF) and hybrid coordination function (HCF) through distributed coordination function (DCF). The DCF is the fundamental channel access method, also known as carrier sense multiple access with collision avoidance (CSMA/CA), and it should be implemented in all STAs. HCF is not present in non quality-of-service (QoS) STAs, whereas HCF and DCF are present in QoS implementation. PCF is optional for non-QoS and QoS STAs. [1]

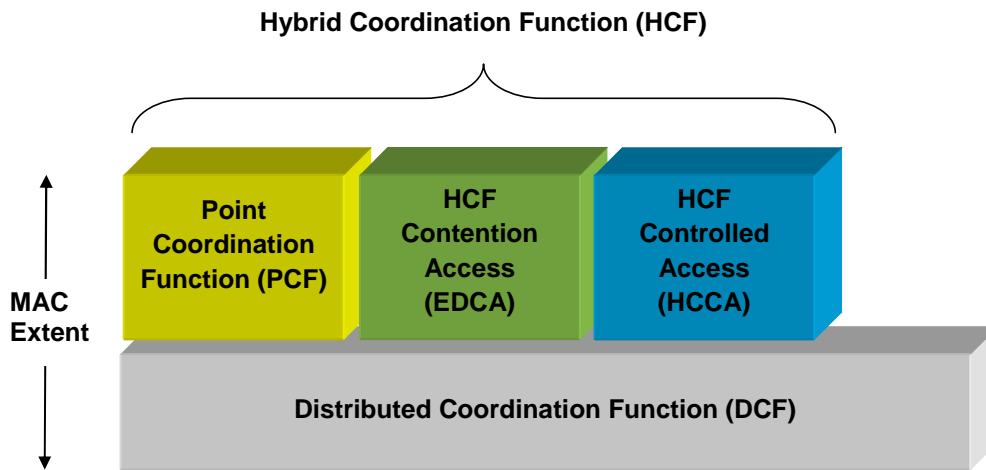


Figure 3. MAC architecture of 802.11.

DCF is the mandatory feature basing on the CSMA/CA protocol. It utilizes request-to-send/clear-to-send (RTS/CTS) and network allocation vector (NAV) information. A random back off timer is applied in DCF. A STA waits random period if the channel is in the use. After this time period, the station attempts to access the medium again. DCF provides only best effort applications, all stations compete for the channel with the same priority. It does not make difference between real-time multimedia traffic and data applications. In other words, DCF does not have any provision to support QoS. [1]

The optional PCF supports time-bounded delivery of data frames [1]. In this mode, an AP grants access to an individual station to the medium by polling the station during the contention free period. If the AP does not poll stations, the stations cannot transmit frames. Although PCF was designed to support time-bounded multimedia applications, it has three major problems that lead poor QoS [7]:

- It was designed to support only a single-class round robin scheduling algorithm. This cannot handle different QoS requirements.
- The AP schedules the beacon transmission at the target beacon transmission time (TBTT), but the AP has to contend to access the medium. This can delay the beacon transmission. In addition, STAs are allowed to transmit even if the frame transmission cannot end before the next TBTT.
- The transmission time of the polled STA is difficult to control for PCF. The polled station is allowed to send frame with various length. This may introduce various transmission rates. Therefore, the AP cannot guarantee delay and jitter performances for other STAs.

HCF is only usable for QoS network configurations and it should be implemented in all QoS STAs (QSTA). It combines functions from DCF and PCF with some enhancements to support QoS. HCF has two methods to access medium:

- *Enhanced distributed channel access (EDCA)*, i.e., contention-based channel access function designed for supporting prioritized traffic.

- *HCF controlled channel access (HCCA)*, i.e., contention free polling mechanism supporting parameterized traffic. HCCA is controlled by the hybrid coordinator (HC), which is co-located with the AP.

HCCA is very advanced coordination function but very complex. Therefore, Wi-Fi Multimedia (WMM) certified products provide only EDCA method thus far [8].

IEEE 802.11 MAC sublayer applies 32-bit cyclic redundancy check (CRC) code. It is calculated over all the files of the MAC header and the frame body field for better error control.

### 3.3. Conclusion

The 802.11 OFDM PHY is operating in the license-free 5 GHz ISM band. This may raise a concern about coexistence with other systems in that band, e.g., IEEE 802.16 (WiMAX). WiMAX is a promising alternative to deploy fixed networks in rural areas and frequency band at 5 GHz is one example which may be shared between WiMAX and 802.11. In addition, the FCC defined UWB band is crossing over with the 5 GHz ISM band. In [9], coexistence between 802.11 and WiMAX is studied from the perspective of the PHY layer concluding that both systems can work in the same band. The effect of UWB transmission on 802.11 OFDM PHY is studied in [10] by using experimental measurements. According to the results, UWB does not cause any harmful performance degradation for a LOS 802.11 link when realistic activity factor for UWB is applied. In a non-LOS (NLOS) link, UWB has strong influence on performance of 802.11.

The 802.11 OFDM PHY provides the robust PHY having BPSK and QPSK modulations with good channel coding combined with OFDM scheme. OFDM is robust against intersymbol interference (ISI) and multipath fading channel. In Figure 4, packet error rate (PER) performances of different modes of 802.11 OFDM PHY are illustrated in the Rayleigh channel having RMS (root mean square) delay spread of 50 ns.  $C/N$  refers to the carrier-to-noise power ratio. In the simulations, the payload size was set to 512 bytes for all modes.

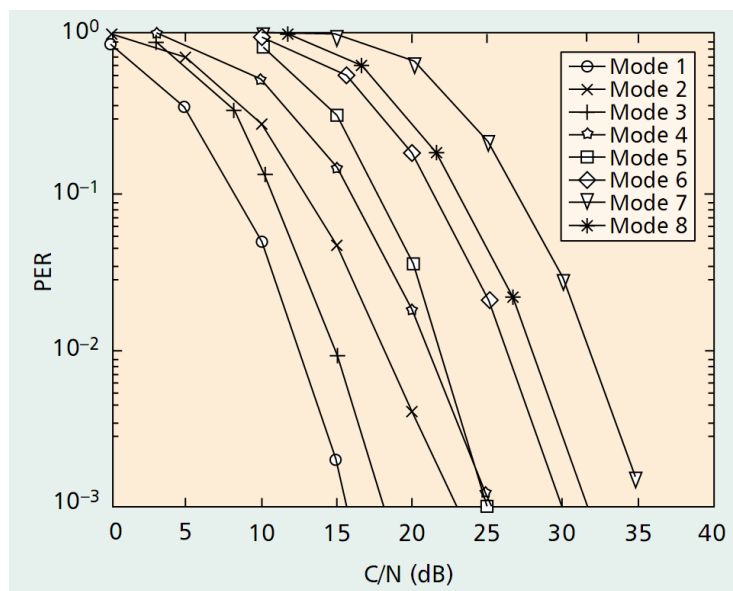


Figure 4. PER performance of 802.11 OFDM PHY.

The performance of QoS supported 802.11 MAC is studied in [12]. In Figure 5, it is presented mean delays for different access categories (AC) under EDCA mode. As it can be seen, the highest-priority voice flows have lower mean delay than the video and background flows. The mean

delay of voice is around 5 ms even when the number of QSTA is as high as 14. The suitability of 802.11 QoS MAC for real-time communications in the automation industry is evaluated in [13], [14]. The drawback of using 802.11 QoS MAC for real-time communications in industry is that the standard is designed to achieve high throughput, and therefore, it is optimized to transmit large data files. When small payloads are used, the overhead introduced by the MAC and PHY layers is comparatively very high. The second drawback is the complexity of the MAC layer. The applicability of 802.11 QoS MAC for real-time communications depends on the QoS requirements of the applications.

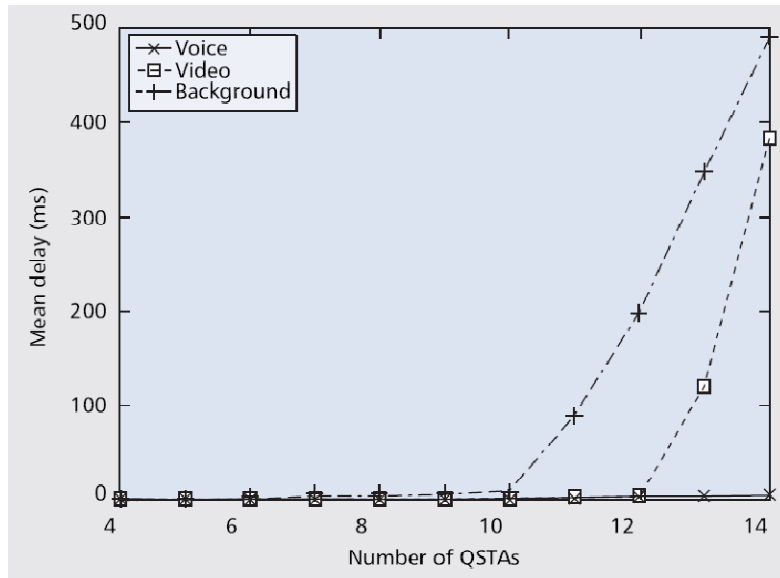


Figure 5. Mean delays for different ACs under EDCA.

Widely adaptation in home and office environments with plenty of products available is the strength of the 802.11. Since having a strong alliance behind, i.e., Wi-Fi Alliance [15], standards are expected to undergo continuous improvements. Wi-Fi chipset sales reached 387 million units in 2008, and it is expected to double by year 2012 as illustrated in Figure 6 [16].

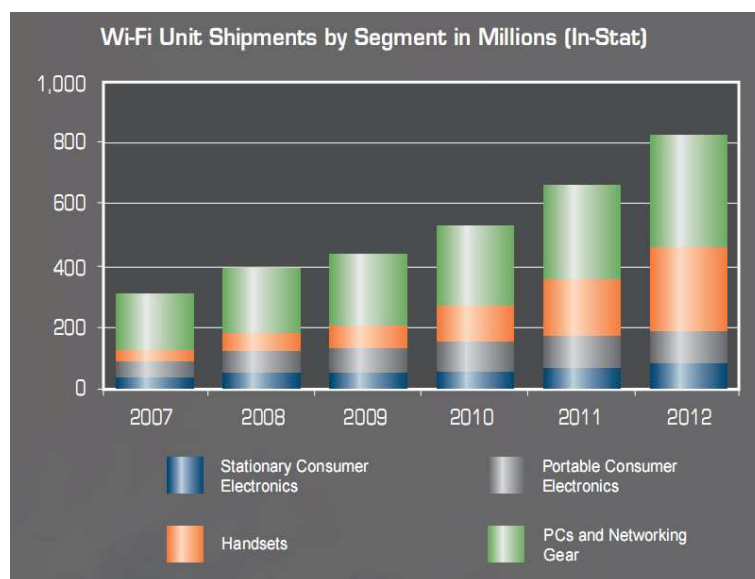


Figure 6. Wi-Fi unit shipments.

## 4. IEEE 802.11p – Amendment to IEEE 802.11

The IEEE 802.11p is an extension to the IEEE 802.11 standard defining enhancements for high-speed vehicle environment [3]. IEEE 802.11p PHY layer is based on the OFDM PHY layer of the 802.11. The amendment is meant to [17]:

- Describe the functions and services required for operation in a rapidly varying environment and exchange messages without having to join a Basic Service Set (BSS), i.e., one AP together with all associated STAs .
- Define the WAVE signaling technique and interference functions.

The communications occur between stations on the roadside (roadside unit, RSU) and mobile radio units (onboard units, OBU), between mobile units, and between portable units and mobile units. A channel is generally line-of-sight (LOS) with distances less than 1000 m between RSUs and mostly high speed, but occasionally stopped and slow moving, vehicles or between high-speed vehicles. [3]

### 4.1. PHY layer amendments

The 802.11p PHY exploits the OFDM PHY of 802.11 with 10 MHz channel spacing. The key reason to the selection of 10 MHz channel spacing instead of 20 MHz is an increased RMS delay spread in the vehicular environments. Due to the 10 MHz channel spacing, two-folded timing parameters provide longer guard interval to offset increased RMS delay, and therefore, preventing intersymbol interference in the vehicular environments. The data rate dependent and timing related parameters are presented in Table 2 and Table 3, respectively. The support of transmitting and receiving at data rates of 3, 6 and 12 Mbps is mandatory. [3], [17]

Since 802.11p introduces an environment where vehicles are closely distributed on a road, it creates increased concern for cross channel interference. Therefore, adjacent and alternate channel rejection levels are more stringent than 802.11. Two categories of channel rejection capabilities are defined designated as type 1 and type 2. Receiver requirements of type 1 are mandatory, whereas type 2 requirements are optionally. Requirements are summarized in Table 5. [3], [17]

In 802.11p, devices are categorized into four classes from A to D. Each class has its own output power and transmit spectrum mask. Maximum output power and transmit spectrum mask for each class are presented in Table 6 and Figure 7, respectively. [3]

Four temperature ranges are specified in 802.11p. Type 1, defined as 0°C to 40°C, is designated for office environments. Type 2, defined as -20°C to 50°C, and Type 3, defined as -30°C to 70°C are designated for industrial environments. Type 4, defined as -40°C to 85°C, is designated for automotive environments. [3]

Table 5. Receiver performance requirements for type 1 and type 2 devices

| Data Rate [Mbps] (10 MHz Channel Spacing) | Type 1                             |                                 |                                  | Type 2                             |                                 |                                  |
|---|------------------------------------|---------------------------------|----------------------------------|------------------------------------|---------------------------------|----------------------------------|
|   | Minimum Receiver Sensitivity [dBm] | Adjacent Channel Rejection [dB] | Alternate Channel Rejection [dB] | Minimum Receiver Sensitivity [dBm] | Adjacent Channel Rejection [dB] | Alternate Channel Rejection [dB] |
| 3   | -85                                | 18                              | 34                               | -85                                | 37                              | 44                               |
| 4.5                                       | -84                                | 17                              | 33                               | -84                                | 36                              | 43                               |
| 6   | -82                                | 16                              | 32                               | -82                                | 35                              | 42                               |
| 9   | -80                                | 15                              | 31                               | -80                                | 34                              | 41                               |
| 12  | -77                                | 13                              | 29                               | -77                                | 32                              | 39                               |
| 18  | -70                                | 11                              | 27                               | -70                                | 30                              | 37                               |
| 24  | -69                                | 8                               | 24                               | -69                                | 27                              | 34                               |
| 27  | -67                                | 4                               | 20                               | -67                                | 23                              | 30                               |

= Mandatory

Table 6. Device classes and transmit power levels

| Device Class | Maximum Device Output Power [dBm] |
|--------------|-----------------------------------|
| A            | 0                                 |
| B            | 10                                |
| C            | 20                                |
| D            | 28.8 or more                      |

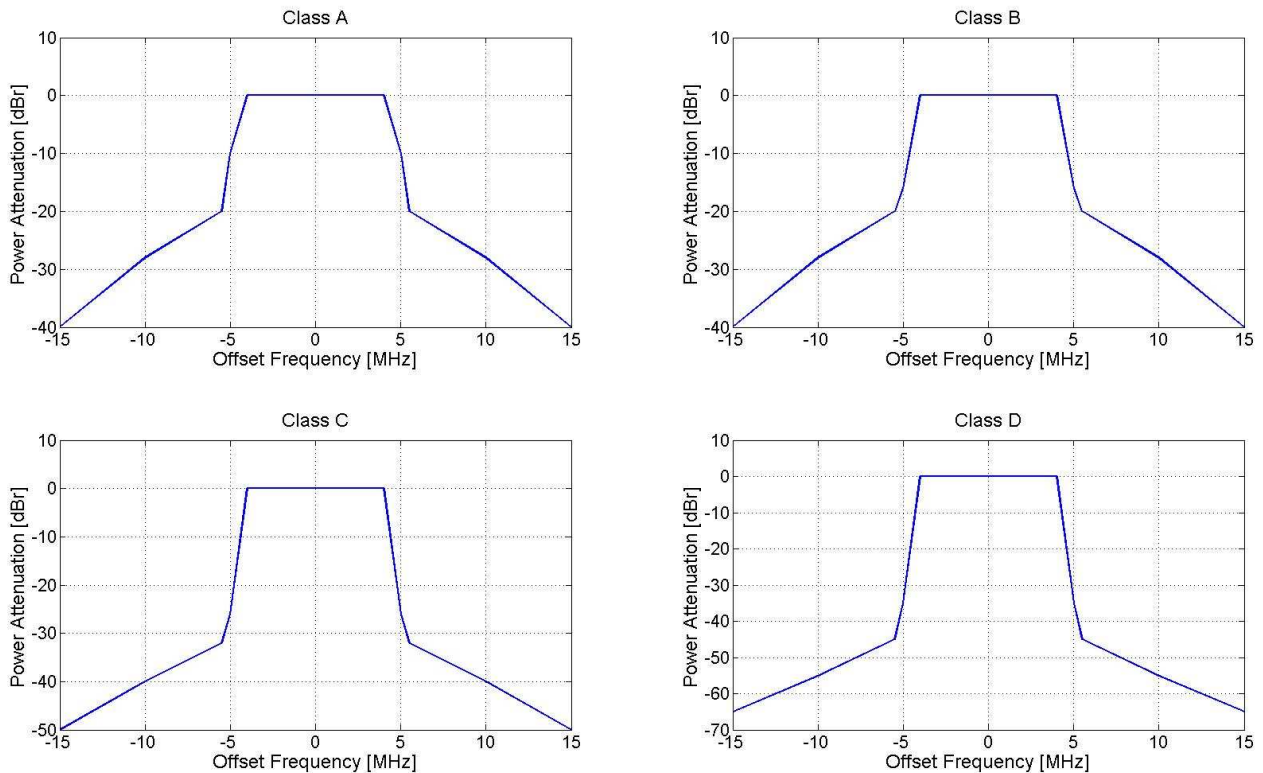


Figure 7. Transmission masks of class A to D operations in the 5.9 DSRC spectrum.

## **4.2. MAC layer amendments**

The main problem of adaptation of 802.11 MAC to 802.11p is being too time-consuming connection establishment due to channel scanning and executing multiple handshakes. The key amendment introduced by 802.11p is the “WAVE mode” of a STA. In this mode, a STA is allowed to transmit and receive data frames with the “wildcard” BSSID (basic service set identification) and without the need to belong to a BSS of any kind a priori. BSSID is the name of a BSS known to radios at the MAC level. [17]

The overlong overhead of the traditional BSS setup is solved by introducing the new BSS type, i.e., WAVE BSS (WBSS). In WBSS, a STA can decide to join and completing joining process of a WBSS by only receiving WAVE advertisement with no further interactions. In other words, WAVE STA advertise a WAVE BSS by using the demand beacon that is well known beacon frame and needs not to be periodically repeated. [17]

Another amendment is to expand wildcard BSSID usage. When all 48 bits of BSSID is set to ‘1’, the BSSID is indicated as wildcard. In expanded wildcard BSSID usage, a station already belonging to a WBSS, i.e., configured with a particular BSSID can still transit frames with wildcard BSSID in order to reach all neighboring STAs in cases of safety concerns. [17]

## **4.3. Conclusion**

The 802.11p is operating in the licensed DSRC band, and thus, there should not be such interference as in the ISM bands. It is also providing support for higher mobility of STAs that may be necessary when communication between working machines is considered. It depends on an application and its requirements defining is basic 802.11 enough or is 802.11p needed. The 802.11p PHY is mainly already included in 802.11, i.e., 10 MHz channel spacing with doubled timing parameters. But if a STA should rapidly open communication link with an AP as the original purpose of 802.11p, then 802.11 MAC is not enough.

The BER and PER performances of the 802.11p (802.11a with 10 MHz channel spacing) are studied in [18]. The data rates of 6 Mbps and 12 Mbps were analyzed in urban and motorway environments. The results for BER and PER are presented in Figure 8 and Figure 9, respectively. In PER simulations, packet length was set to 20 bytes.

The performance of the 802.11p MAC layer is considered in [19]. A WAVE environment of 2-200 vehicles with varying inter-vehicle distances and varying speeds were simulated and analyzed. Nodes were configured to broadcast 500 bytes messages with 6 Mbps transmission rate. PER and average delay as a function of vehicle density with speed of 48 km/h are illustrated in Figure 10 and Figure 11, respectively. Based on the simulation results, the authors concluded that vehicle speed does not have a significant impact on any of performance metrics.

There are very few, or any, chipsets available supporting 802.11p PHY and MAC. Regardless of small number of 802.11p chip manufactures, there exist few complete systems, e.g., ‘Otto on Board’ by MARK IV Industries [20] and ‘Multiband Configurable Networking Unit (MCNU)’ by TechnoCom [21]. Both systems are operating 5.9 GHz DSRC band and supporting the 802.11p standard.

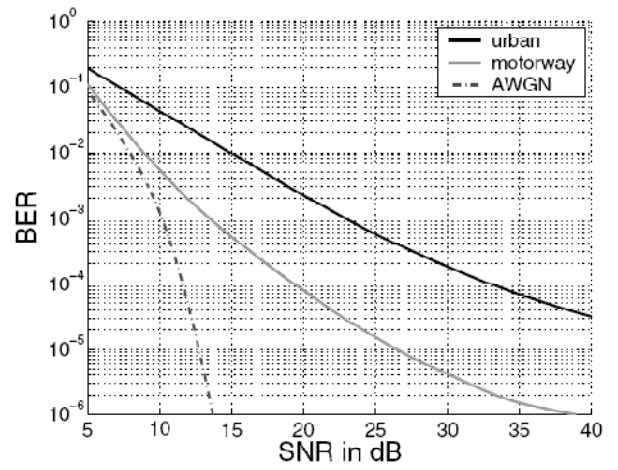
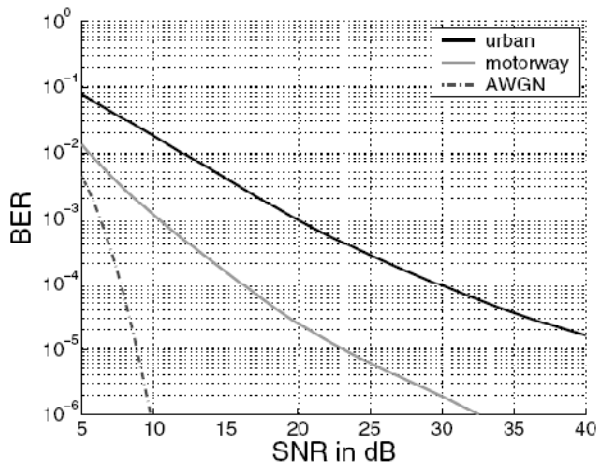


Figure 8. BER for an urban road and a motorway with BPSK (left) and QPSK (right) in a LOS channel.

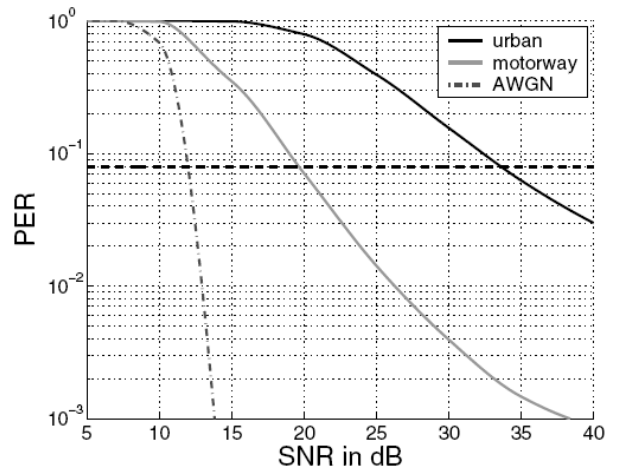
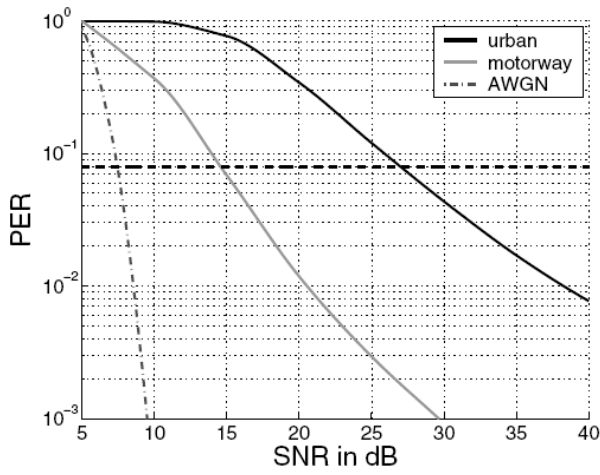


Figure 9. PER for an urban road and a motorway with BPSK (left) and QPSK (right) in a LOS channel.

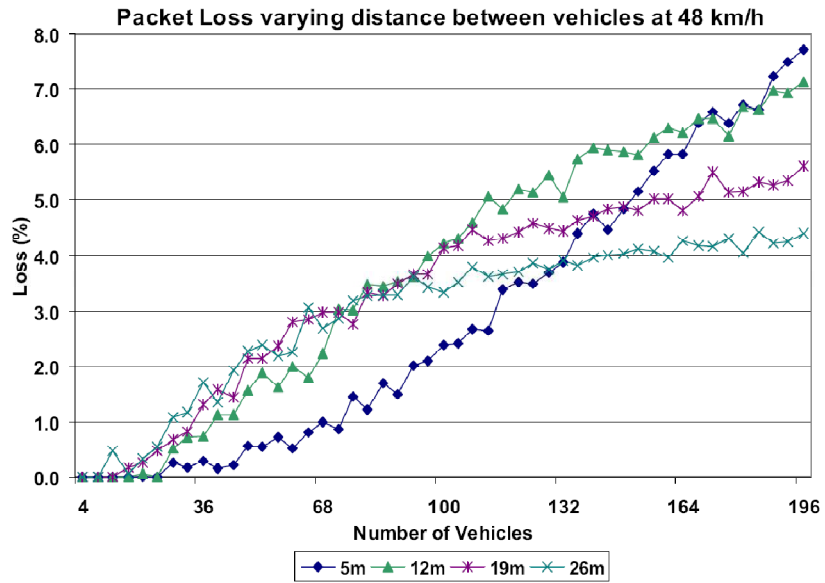


Figure 10. Packet loss as a function of vehicle density.

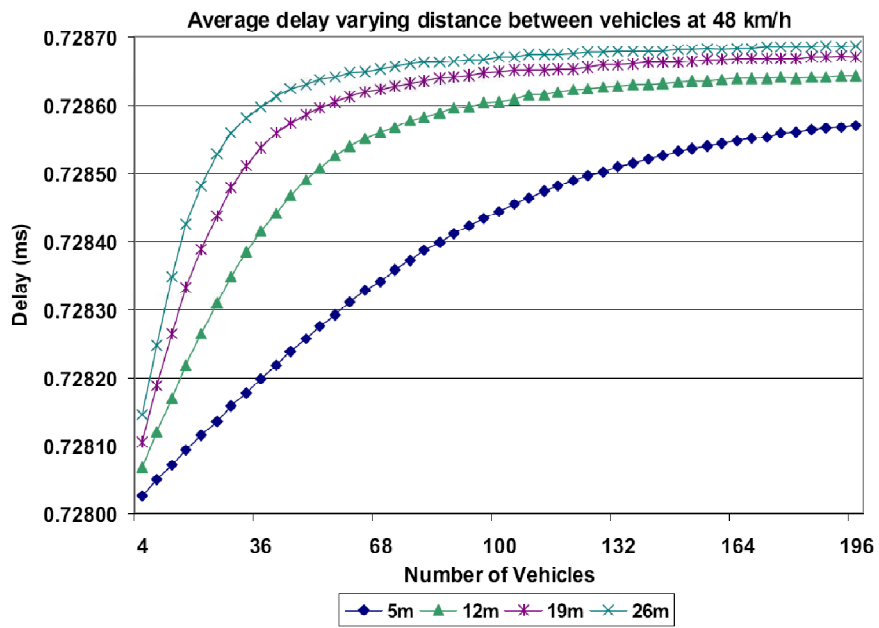


Figure 11. Average delay as a function of vehicle density.

## 5. Security

In this chapter, security issues related to the 802.11 are discussed in brief. Wireless networks are inherently unsafe from unauthorized users since packets are transmitted over the air, and thus being as fair game.

### Common wireless attacks

Networks security attacks can be classified either to be passive or active. In passive attack, a hostile device sniffs data transmission for monitoring message content or pattern of communication. The message content is modified or network is actively disturbed by sending frames in active attack. The taxonomy of general attacks against WLAN is depicted in Figure 12. [22]

Wireless attacks is either physical or software attack. Hostile device that send a strong signal at an operating frequency range is said to be physical attacker. A wireless signal cannot be transmitted until physical attack is stopped. In software attack, one type of attack is to make the media congested by sending flooding frames. [23]

Aircrack-ng is the most commonly used tool to crack wireless networks. It is a set of tools used for auditing a wireless network. [24]

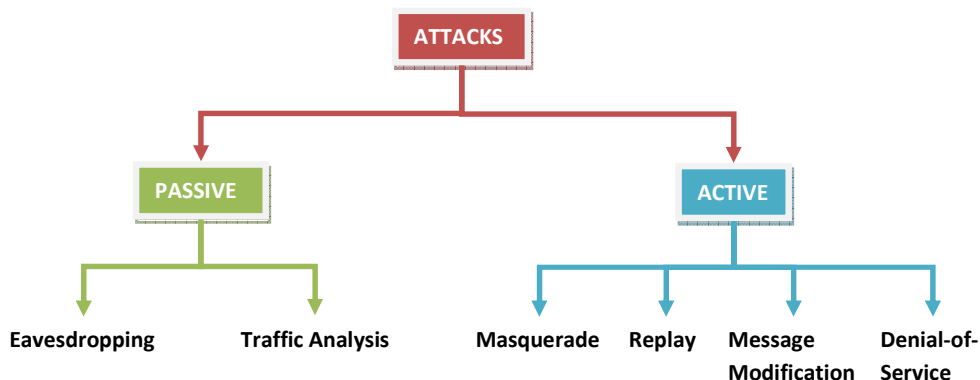


Figure 12. General security attacks against WLANs.

### Basic security features of 802.11

Service set identity (SSID) can be called as the name of the wireless network. By hiding SSID, illegal users are preventing to connect to APs. Though SSID is hidden, it can be tracked down by using association request frames. It is an invalid method to prevent misuse. [23]

In 802.11, two types of authentication service are defined. Open system authentication is the simplest one that authenticates anyone who request authentication, i.e., an AP accepts a STA without verifying the identity of the STA. In the shared-key authentication scheme, there are member who know a shared key and members who not. The weakness is that the shared key process can be sniffed. [22]

When there are a limited number of STAs, unwanted STAs can be easily filtered out by set up MAC filtering in an AP, i.e., binding MAC addresses of intruders. Allowed MAC addresses can be

easily sniffed by capturing data frames, and MAC address of illegal device can be modified to a valid address. [23]

Wired equivalent privacy (WEP) technology was developed to secure 802.11 networks. It has three security goals [22]:

- *Access Control*: Ensure that communications partners are who they pretend to be.
- *Data Integrity*: Ensure that packets are not modified during transfer.
- *Confidentiality*: Manage to avoid eavesdropping through encryption.

WEP is the simplest encryption method. It relies on a secret key shared between communicating parties to encrypt packets. The principle of WEP is presented in Figure 13 [22]. There are the 40-bit WEP (64-bit key) and stronger 104-bit WEP (128-bit key) defined in the 802.11 standard [1]. Nevertheless, the 64-bit and 128 bit keys are cracked with as few as 20000 and 40000 data frames, respectively [23].

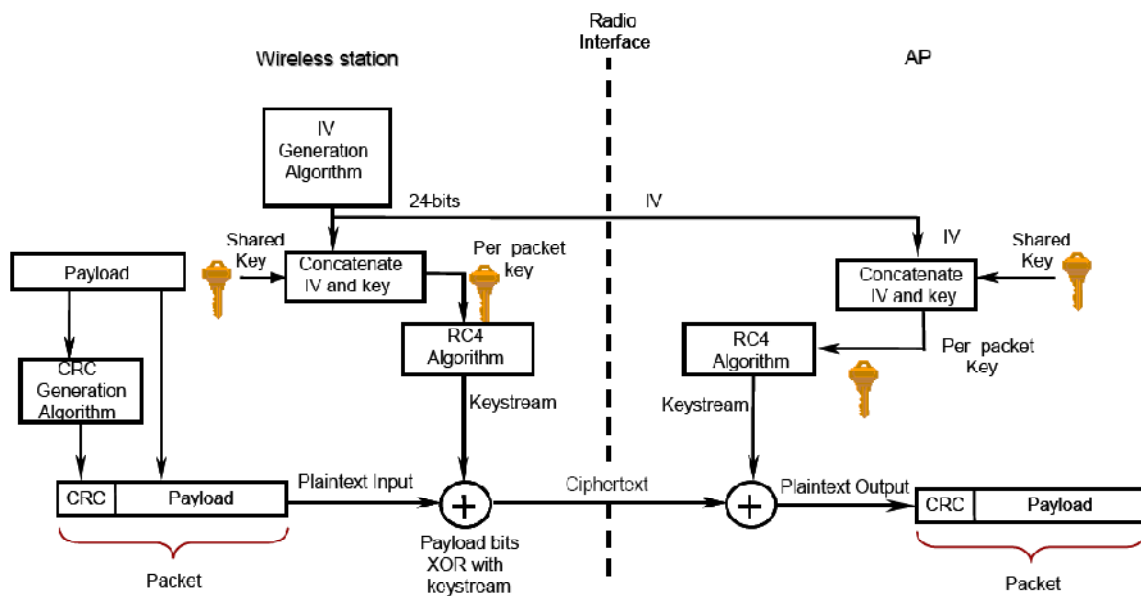


Figure 13. WEP privacy using RC4 algorithm.

### Enhanced security features

Wi-Fi protected access (WPA) addresses the flaws in WEP. It offers stronger encryption algorithm than in WEP scheme and user authentication. WPA uses temporal key integration protocol (TKIP) and employs 802.1X extensible authentication protocol (EAP). In addition, Michael message integrity check is applied to protect against packet forgeries. [25] It has been reported that TKIP can be cracked in 15 minutes [26].

An even stronger encryption mechanism through advanced encryption standard (AES) was introduced in WPA2 based on the 802.11 standard (formerly known as 802.11i). WPA2 is backwards compatible with WPA. WPA2 was developed to meet government and enterprise security requirements. [27] In 2006, support of WPA2 security was set to mandatory for Wi-Fi certified products [15].

## 6. Conclusion

The DSRC spectrum band at 5.9 GHz is reserved for ITS applications worldwide, e.g., the spectrum within 5.875 – 5.925 GHz and 5.850 – 5.925 GHz in Europe and the USA, respectively. The IEEE 802.11 task group p defines PHY and MAC enhancements to 802.11 standard required to support ITS applications. The enhancement 802.11p will be based on the ASTM E 2213-03 document. Since 802.11 OFDM PHY is already operating near to the DRSC frequency band, it was justified to choose OFDM PHY as baseline. The 802.11p PHY applies the 10 MHz channel spacing and more stringent receiver requirements than original 802.11. The MAC layer is modified by minimizing the size of the needed overheads to accelerate the establishment time for communication.

Applicability of 802.11p for communications between working machines depends strongly on nature of data and requirements for QoS. 802.11 was originally designed for multimedia purposes where packet sizes are large, PER is in order of 1% and delay may be large and vary, whereas real-time applications require quite short packets, very short and constant delay and error-free transmission. In 802.11, EDCA and HCCA modes were introduced for QoS networks. Nowadays, only EDCA mode is implemented in chipsets. EDCA is contention-based channel access method and may not fulfill stringent real-time requirements. Even though MAC improvements of 802.11p the contention-based channel access may still be insufficient in terms of real-time communications.

802.11 has very strong power behind the scenes due to Wi-Fi Alliance. Since 802.11 is widely adapted across the world and it is expected that an almost one billion chipsets are shipped in 2011 alone [28], continuous development of 802.11 will be ensured. Still, there are not many or any chipsets of 802.11p available at present.

Table 7. SWOT analysis of 802.11p

|                        | <i>Helpful</i>  | <i>Harmful</i>  |
|------------------------|---|---|
| <i>Internal Origin</i> | <p><b><u>Strengths</u></b></p> <ul style="list-style-type: none"> <li>• Licensed spectrum</li> <li>• Robust PHY</li> <li>• Strong security (WPA2)</li> </ul>  | <p><b><u>Weaknesses</u></b></p> <ul style="list-style-type: none"> <li>• Modified MAC good enough for real-time applications?</li> <li>• QoS requirements of application</li> </ul> |
| <i>External Origin</i> | <p><b><u>Opportunities</u></b></p> <ul style="list-style-type: none"> <li>• Strong Wi-Fi Alliance</li> <li>• Global spectrum for ITS</li> <li>• Widely adapted 802.11 standards</li> <li>• Continuous improvements of 802.11</li> </ul> | <p><b><u>Threats</u></b></p> <ul style="list-style-type: none"> <li>• When 802.11p chipsets available?</li> </ul>   |

## 7. REFERENCES

- [1] IEEE Standard for Local and Metropolitan Area Networks: Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. Doc: IEEE Std 802.11-2007, 1232 p., 2007.
- [2] IEEE 802.11 Task Group p – Wireless Access in Vehicular Environments, [http://www.ieee802.org/11/Reports/tgp\\_update.htm](http://www.ieee802.org/11/Reports/tgp_update.htm)
- [3] ASTM E2213 - 03 Standard Specification for Telecommunications and Information Exchange Between Roadside and Vehicle Systems — 5 GHz Band Dedicated Short Range Communications (DSRC) Medium Access Control (MAC) and Physical Layer (PHY) Specifications, <http://www.astm.org/Standards/E2213.htm>
- [4] The Federal Communication Commission (FCC), Amendment of the Commission's Rules Regarding Dedicated Short-Range Communication s Services in the 5.850 – 5.925 GHz band (5.9 GHz band). Report and Order, Doc: FCC 03-324, 78 p, 2004.
- [5] The Federal Communication Commission (FCC), Amendment of the Commission's Rules Regarding Dedicated Short-Range Communication s Services in the 5.850 – 5.925 GHz band (5.9 GHz band). Memorandum Opinion and Order, Doc: FCC 06-110, 78 p, 2006.
- [6] The Electronic Communications Committee (ECC), Decision on the Harmonized use of the 5875 – 5925 MHz Frequency Band for Intelligent Transport Systems (ITS). Doc: ECC/DEC/(08)01, 5 p., 2008.
- [7] Q. Ni, "Performance Analysis and Enhancements for IEEE 802.11e Wireless Networks," IEEE Network, pp. 21 -27, July/August 2005.
- [8] Wi-Fi Alliance, "Wi-Fi CERTIFIED™ for WMM™ – Support for Multimedia Applications with Quality of Service in Wi-Fi® Networks," White paper, 15 p., 2004.
- [9] X. Fu, W. Ma and Q. Zhang, "The IEEE 802.16 and 802.11a Coexistence in the Licence-Exempt Band," in Proc. of WCNC, pp. 1942 – 1947, 2007.
- [10] M. Hämäläinen, A. Isola, J. Saloranta and J. Linatti, "UWB Coexistence Measurements with IEEE802.11a". in Proc. of IET Seminar on Ultra Wideband Systems, Technologies and Applications, London, p. 186 – 190, April 20, 2006.
- [11] A. Doufexi et al., "A Comparison of the HIPERLAN/2 and IEEE 802.11a Wireless LAN Standards," IEEE Comm. Magazine, pp. 172 – 180, May, 2002.
- [12] Q. Ni, "Performance Analysis and Enhancements for IEEE 802.11e Wireless Networks," IEEE Network, pp. 21 – 27, July/August, 2005.
- [13] M. Maury, "Realtime Communications over IEEE 802.11e in Industrial Environment," Master's Thesis, KTH School of Electrical Engineering, Stockholm, Sweden, 88 p., 2006.
- [14] M. Jäger, "IEEE 802.11e in Industrial Environment: A Quality of Service Survey," Master's Thesis, KTH School of Electrical Engineering, Stockholm, Sweden, 86 p., 2005.
- [15] Wi-Fi Alliance. [Online]. Available at: <http://www.wi-fi.org>.
- [16] Wi-Fi Alliance, "Annual Report 2008," Report, 6 p., 2008.
- [17] D. Jiang and L. Delgrossi, "IEEE 802.11p: Towards an International Standard for Wireless Access in Vehicular Environments", in Proc. of VTC'08, pp. 2036 – 2040, 2008.
- [18] J. Maurer, T. Fügen and W. Wiesbeck, "Physical Layer Simulations of IEEE802.11a for Vehicle-to-Vehicle Communications," in Proc. of VTC-Fall, pp. 1849 – 1853, 2005.
- [19] Todd Murray, Tammy Murray, M. Cojocari and H. Fu, "Measuring the Performance of IEEE 802.11p Using ns-2 Simulator for Vehicular Networks," in Proc. of EIT, pp. 498 – 503, 2008.
- [20] MARK IV Industries, "OTTO On Board™," Technical Specification, 2 p., 2005.
- [21] Technocom, "Multiband Configurable Networking Unit," Technical Specification, 2 p., 2007.

- [22] T. Karygiannis and L. Owens, "Wireless Network Security – 802.11, Bluetooth and Handheld Devices", NIST, Special Publication 800-48, 119 p., 2002.
- [23] K. Meng, Y. Xiao and S.V. Vrbsky, "Building a Wireless Capturing Tool for WiFi," Security Comm. Networks, John Wiley & Sons, Ltd., 15 p., April, 2009.
- [24] Aircrack-ng. [Online]. Available at: <http://www.aircrack-ng.org>.
- [25] Wi-Fi Alliance, "Wi-Fi Protected Access: Strong, Standard-based, Interoperable Security for Today's Wi-Fi Networks," White paper, 10 p., 2003.
- [26] M. Beck and E. Tews, "Practical Attacks Against WEP and WPA," Report, 12 p., 2008.
- [27] Wi-Fi Alliance, "Introducing WPA2™ and WMM™," PowerPoint presentation, 2004.
- [28] ABIresearch, "One Billion Wi-Fi Chipsets to Ship in 2011 Alone." [Online]. Available at: <http://www.abiresearch.com/press>, August, 2009.