SIECI BEZPRZEWODOWE IEEE 802.11

Mariusz Piwiński
Instytut Fizyki
Wydział Fizyki, Astronomii i Informatyki Stosowanej
Uniwersytet Mikołaja Kopernika w Toruniu
ul. Grudziądzka 5, 87-100 Toruń
Mariusz.Piwinski@fizyka.umk.pl

Abstract. Wireless networks are one of the most evolving ITC technologies. However, there are many limitation and vulnerabilities connecting with this way of communication. In this paper the IEEE 802.11 standards will be presented and discussed together with software for planning and analyzing wireless computer networks.

1. Wstęp

Dynamiczny rozwój usług teleinformatycznych spowodował, iż stały się one nieodzowną częścią naszego życia. Powszechny dostęp do Internetu sprawił, iż podłączane są do niego coraz to nowe urządzenia. Oprócz typowych „hostów" takich jak komputery, tablety czy smartfony, coraz częściej w interfejs sieciowy wyposażane są urządzenia, które jeszcze do niedawana zupełnie nie były kojarzone z sieciami komputerowymi. Sytuacja ta sprawia, że problemy związane z bezpieczeństwem sieciowym dotyczą coraz szerszej sfery naszego życia [25,27]. Obserwowane obecnie zjawisko polegające na podłączaniu do sieci coraz to nowych urządzeń gromadzących, przetwarzających i wymieniających między sobą informacje zostało po raz pierwszy opisane przez Kevina Ashtona w 1999 roku jako Internet Rzeczy (*ang. Internet of Things*) [1]. Firma Cisco rozszerzyła tą definicję na Internet Wszechrzeczy (*ang. Internet of Everything – IoE*) obejmujący oddziałujące ze sobą poprzez sieć cztery elementy: ludzi, dane, procesy oraz rzeczy. Oznacza to, iż oprócz typowej komunikacji między ludźmi (P2P) pojawiła się dodatkowo komunikacja maszyn z ludźmi (M2P) oraz komunikacja pomiędzy maszynami (M2M). Wzajemne interakcje między tymi elementami prowadzą do automatycznego tworzenia, wymiany i analizy dużej ilości danych, które stają się podstawą do tworzenia zupełnie nowych funkcji urządzeń

oraz systemów. Przykładem implementacji tego typu rozwiązań jest system bankowy z obsługą kont, krat płatniczych oraz automatycznymi zleceniami płatności spływającymi z innych systemów informatycznych.

Zgodnie z obecnymi szacunkami do sieci podłączonych jest około 20 mld urządzeń. W roku 2020 liczba ta ma wynosić około 50 mld. Oznacza to podłączenie do Internetu około 2,7% wszystkich urządzeń działających na świecie [8]. Zastosowanie w nich interfejsu bezprzewodowego wydaje się rozwiązywać wszystkie problemy związane z budową infrastruktury kablowej, Jednakże podczas stosowania technologii bezprzewodowych należy mieć pełną świadomość sposobu ich działania, który w efekcie jest znacznie bardziej zawodny niż transmisja realizowana w oparciu o przewody miedziane lub światłowodowe.

2. Standard IEEE 802.11

Charakteryzując transmisję realizowaną w ramach standardu IEEE 802.11 należy podkreślić, iż zgodnie ze swoimi założeniami miała ona wykorzystywać nielicencjonowane pasmo. Oznacza to, iż urządzenia pracujące w tym standardzie można wykorzystywać bez potrzeby ponoszenia opłat związanych z użytkowaniem pasma radiowego. Oczywiście wybrane pasmo powinno być uznane za nielicencjonowane w możliwie największej liczbie państw. Ostatecznie standard IEEE 802.11 w większości implementacji wykorzystuje dwa pasma radiowe w zakresie 2,4 GHz oraz 5 GHz. Od czasu gdy w 1997 roku opublikowano jego pierwszą wersję ulega on cały czas modyfikacjom, które mają na celu zwiększenie dostępnej maksymalnej transmisji, zwiększenie bezpieczeństwa oraz optymalizację zarządzania. Kolejne rozszerzenia standardu IEEE 802.11 dotyczące sposobu transmisji danych zostały opisane jako a, b, g, n, ac oraz ad. Szczegóły dotyczące standardów przedstawia Tabela 1.

Jak widać z przedstawionego zestawienia w ramach jednego standardu możliwa jest realizacja transmisji danych z kilkoma określonymi prędkościami. W odróżnieniu od typowych technologii stosowanych w sieciach przewodowych takich jak np. Ethernet w przypadku transmisji bezprzewodowych pasmo transmisji uzależnione jest od mocy odbieranego sygnału. Analizując jakość sygnału urządzenia uzgadniają ze sobą odpowiedni sposób kodowania danych, który ostatecznie determinuje maksymalną prędkość transmisji. Zatem użytkownik odbierający bardzo słaby sygnał od punktu dostępowego będzie mógł komunikować się z nim z bardzo małą prędkością. Wybór innego, bardziej zaawansowanego kodowania mógłby skutkować dużą ilością błędów w transmitowanych danych. Komunikujące się ze sobą urządzenia cały czas monitorują poziom sygnałów, co pozwala na ciągłą optymalizację sposobu przesyłania danych.

Tabela 1. Standardy IEEE 802.11 [4].

Nazwa	Wspierane szybkości [Mb/s]	Pasmo [GHz]	Szerokość kanału [MHz]	Liczba strumieni MIMO	Typ modulacji
802.11	1, 2	2,4	22	1	FHSS, DSSS, IR
802.11a	6, 9, 12, 18, 24, 36, 48, 54	5	20	1	OFDM
802.11b	1, 2, 5.5, 11	2,4	22	1	HR-DSSS,CCK
802.11g	1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54	2,4	20	1	HR-DSSS, CCK, OFDM
802.11n	100, 150, 300, 450, 600	2,4 lub 5	20, 40	4	OFDM
802.11ac	433, 867, 1300, 1733, ..., 6928	5	20, 40, 80, 160	8	OFDM
802.11ad	do 6912	60	2,16	1	OFDM

Początkowy brak systemu zewnętrznej certyfikacji urządzeń oraz liczność standardów powodowały, iż urządzenia różnych producentów teoretycznie spełniające wszystkie wymogi dotyczące transmisji danych w praktyce miały problem z wzajemną komunikacją. W związku z powyższym zostały powołane organizacje certyfikacyjne mające na celu weryfikację zgodności produkowanych urządzeń z opublikowanymi standardami. W przypadku urządzeń bezprzewodowych działających w standardzie IEEE 802.11 organizacją zajmującą się ich certyfikacją jest Wi-Fi Alliance [23]. Pomyślne przeprowadzenie serii testów dla konkretnego urządzenia skutkuje nadaniem mu etykiety potwierdzającej zgodność z testowanymi standardami.

Potocznie bezprzewodowe sieci komputerowe określane są mianem sieci Wi-Fi (*ang. Wireless Fidelity*). Należy jednak podkreślić, iż nazwa ta obejmuje zestaw wszystkich standardów oraz protokołów służących do budowy bezprzewodowych sieci komputerowych, a sieci lokalne (LAN) są tylko małą ich częścią. Stąd w celu bardziej precyzyjnego określenia technologii bezprzewodowych stosowanych w sieciach lokalnych często stosuje się skrót WLAN (*ang. Wireless Local Area Network*).

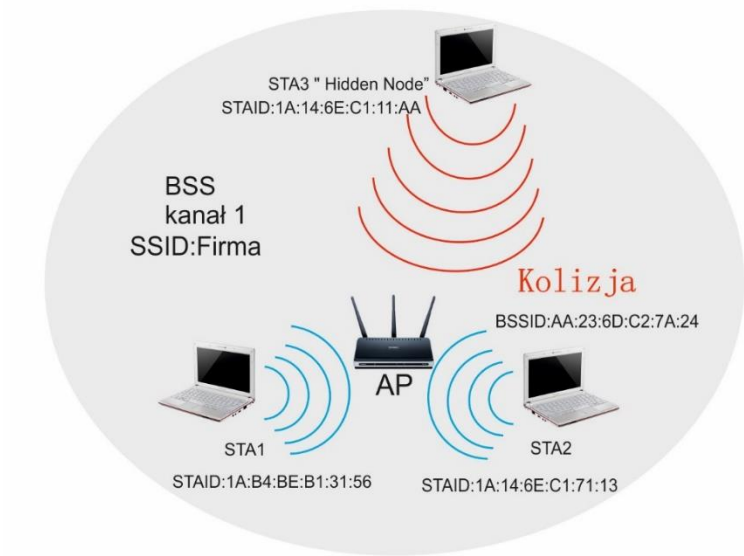
3. Architektura sieci Wi-Fi

Sieci bezprzewodowe mogą być budowane w oparciu o dwie podstawowe topologie. Pierwsza z nich opisywana jako „**ad hoc**” zakłada bezpośrednią komunikację

pomiędzy dwoma urządzeniami. Druga opisywana jako „**tryb infrastruktury**" wykorzystuje do komunikacji urządzenie pośredniczące, które nazywane jest punktem dostępowym AP (*ang. Access Point*). Obszar, na którym uruchomiona jest taka sieć nazywa się komórką sieci bezprzewodowej BSS (*ang. Basic Service Set*), a obsługiwane w niej urządzenia stacjami klienckimi STA (*ang. Station*). Sieci bezprzewodowe pracujące w standardzie IEEE 802.11 wykorzystują wiele mechanizmów znanych z sieci przewodowej IEEE 802.3, jednakże charakteryzują się znacznie większą złożonością procesu przesyłania danych. Działanie sieci typu Ethernet bazuje na możliwości jednoznacznego rozpoznania każdego podłączonego urządzenia w oparciu o jego unikalny 48–bitowy adres MAC (*ang. Media Access Control*). Takie rozwiązanie sprawia, iż sieci te nie wymagają zastosowania dodatkowego urządzenia nadzorującego ruchem. Ponadto urządzenia podłączone do wspólnego medium odbierają wszystkie sygnały wysyłane przez dowolne urządzenie znajdujące się w tym samym segmencie sieciowym. Założenia te stanowią podwaliny wykorzystywanego systemu zarządzania dostępem do medium **CSMA/CD** (*ang. Carrier Sense Multiple Access / with Collision Detection*) [3]. Oznacza on, iż urządzenie chcąc wysłać dane monitoruje stan kanału komunikacyjnego czekając na chwilę, w której kanał nie będzie wykorzystywany przez inną transmisję. Technologia ta jest charakterystyczna dla komunikacji jednokierunkowej (*ang. half duplex*), która wynikała z wykorzystywanego w tych sieciach kabla koncentrycznego (standard 10 BASE5, 10 BASE2). Technologia taka nie jest niezawodna, co może prowadzić do pojawiania się tzw. kolizji. Występują one wtedy, gdy w tym samym momencie dwa urządzenia widząc wolny kanał komunikacyjny rozpoczynają transmisję danych, co ostatecznie powoduje nałożenie się obu sygnałów. Urządzenie, które wykryje kolizję w sieci wysyła sygnał zakłócający informując o tym fakcie pozostałych użytkowników. Stacje nadawcze po odebraniu tego sygnału przerywają transmisję, co chwilowo rozwiązuje problem. Następnie niezależnie losują one czas, po którym ponowią próbę wysyłania danych, wcześniej sprawdzając stan kanału komunikacyjnego. Zakładając, iż urządzenia wylosują różne czasy, doprowadzi to do ostatecznego rozwiązania problemu. Jak należy przypuszczać rozwiązanie to będzie sprawdzało się dla niewielkiej liczby urządzeń umieszczonych w jednym segmencie sieci nazywanym domeną kolizyjną. Jednocześnie wykorzystanie koncentratora wieloportowego w naturalny sposób rozszerza ten obszar o kolejne segmenty. Zastosowanie nieekranowanego kabla typu skrętka UTP (*ang. Unshielded Twisted Pair*) oraz wprowadzenie przełączników sieciowych znacznie usprawniło to rozwiązanie. Umożliwiło ono realizację komunikacji dwukierunkowej (*ang. full duplex*) opartej pierwotnie na dwóch niezależnych parach przewodów. Jednocześnie ze względu na fakt, iż przełączniki odbierają, buforują, analizują, a następnie dopiero wysyłają ramki doprowadziło to do ograniczenia wielkości domen kolizyjnych do ich pojedynczego portu. W związku z powyższym w obecnych sieciach

LAN opartych na przełącznikach problem kolizji został zupełnie wyeliminowany. Pomimo tego, iż w takim przypadku opisywany mechanizm CSMA/CD wydaje się być zbyteczny, jest on nadal realizowany dla zachowania standardu transmisji danych [28].

W swoich założeniach sieć bezprzewodowa IEEE 802.11 miała stanowić naturalne rozszerzenie sieci przewodowej IEEE 802.3. W związku z powyższym zastosowano w niej wiele mechanizmów znanych z dotychczasowych rozwiązań wykorzystywanych w transmisjach przewodowych. Ze względu na fakt, iż urządzenia do wspólnej komunikacji wykorzystują jedno wybrane pasmo radiowe sytuacja ta jest znacznie bardziej skomplikowana. Zastosowanie technologii wykorzystującej jeden współdzielony kanał radiowy oznacza, iż podobnie jak w pierwszych wersjach sieci Ethernet komunikacja będzie realizowana w trybie half duplex. Sytuacją, która ideowo najbardziej przypomina rozwiązanie stosowane w standardzie IEEE 802.3 jest sieć radiowa pracująca w topologii „ad hoc", stosowana w komunikacji pomiędzy dwoma urządzeniami. Tryb infrastruktury przewiduje możliwość podłączenia do sieci radiowej większej ilości urządzeń, co wymusza zastosowanie urządzenia pośredniczącego, którym jest punkt dostępowy. Jest on najczęściej podłączony do istniejącej sieci przewodowej, stanowiąc tym samym punkt graniczny pomiędzy dwoma technologiami. W odróżnieniu od mechanizmu **CSMA/CD** stosowanego w standardzie Ethernet urządzenia pracujące w standardzie IEEE 802.11 stosują rozwiązanie **CSMA/CA** (*ang. Carrier Sense Multiple Access with Collision Avoidance*). Oznacza to, iż podobnie jak w sieciach Ethernet urządzenie przed wysłaniem informacji musi sprawdzić dostępność wykorzystywanego kanału komunikacyjnego. Jednakże inaczej niż w sieci przewodowej, w takiej topologii możliwe jest, iż ze względu na usytuowanie urządzeń oraz tłumienie sygnału (np. przez ściany) dwie stacje klienckie mogą komunikować się z punktem dostępowym nie odbierając jednakże swoich bezpośrednich transmisji. W efekcie może prowadzić to do sytuacji, w której punkt dostępowy będzie równocześnie odbierał kilka interferujących ze sobą sygnałów, co spowoduje błędy w komunikacji. Sytuacja ta określana jako „problem ukrytego węzła" (*ang. hidden node*) powoduje, iż prosty mechanizm wykrywania kolizji musiał zostać zastąpiony znacznie bardziej zaawansowanym rozwiązaniem polegającym na unikaniu kolizji (Rys.1).



Rysunek 1. Podstawowa komórka sieci bezprzewodowej BSS ze zdefiniowaną nazwą sieci Firma (SSID), z widocznym identyfikatorem BSSID punktu dostępowego AP oraz identyfikatorami STAID trzech stacji klienckich (STA1, STA2, STA3). Stacja STA3 ze względu na moc swojego sygnału jest widoczna dla AP, natomiast nie jest widoczna dla stacji STA1 oraz STA2.

4. Ramki IEEE 802.11

Stosowanie zaawansowanych mechanizmów zarządzania pasmem radiowym wymaga dodatkowych funkcji realizowanych przez protokoły sieciowe, co wpływa na rozbudowanie pól stosowanych w odpowiednich datagramach. W przypadku sieci Ethernet ogólna postać wykorzystywanej ramki jest bardzo prosta, a przesyłane pakiety są po prostu opakowywane w ramki z wypełnionymi polami adresów MAC, typem protokołu oraz obliczoną sumą kontrolną. Zatem system pragnący przesłać jakąś informację, po sprawdzeniu czy kanał komunikacyjny jest wolny przystępuje do wysłania ramki. Samo przyłączenie urządzenia do sieci odbywa się zaś na poziomie warstwy pierwszej modelu OSI w momencie podłączenia kabla do interfejsu sieciowego. Ze względu na ciągły rozwój technologii, w obecnych sieciach IEEE 802.3 mamy do czynienia z kilkoma standardami przesyłania danych. Pierwotnie Ethernet został zaprojektowany do realizacji transmisji z prędkością 10 Mb/s opartej na kodowaniu Manchester. Wprowadzona technologia Fast Ethernet zmieniła sposób przesyłania i kodowania informacji (4B/5B z MLT3 lub NRZI) co zapewniło pasmo na poziomie 100 Mb/s. Obecnie możliwe jest realizowanie komunikacji w sieciach Ethernet

z prędkością 1 Gb/s oraz 10 Gb/s. Wymaga to zastosowania odpowiedniego kodowania sygnału, które może być realizowane w różny sposób w zależności od zastosowanego medium transmisyjnego. Oznacza to, iż urządzenie podłączone do sieci LAN musi posiadać informację w jakim standardzie będzie realizowana komunikacja. Skonfigurowanie nieodpowiedniego sposobu kodowania spowoduje brak możliwości odczytania przesyłanych danych. Problem ten dotyczy na przykład urządzeń wyposażonych w karty sieciowe wykorzystujące port RJ45 i obsługujące standardy transmisji 10/100/1000 Mb/s. W celu zapewnienia automatycznej kompatybilności takich urządzeń również ze starszymi typami interfejsów sieciowych stworzono funkcję autonegocjacji. Bazuje ona na wysyłaniu szeregu impulsów elektrycznych, za pomocą których ogłaszane są możliwe tryby pracy urządzenia oraz negocjowany jest najlepszy wspólnie obsługiwany standard kodowania. Rozwiązanie to dotyczy tylko i wyłącznie komunikacji między dwoma urządzeniami (np. komputer – komputer, komputer – przełącznik ethernetowy, przełącznik – router). Negocjacja ta realizowana jest w warstwie fizycznej modelu OSI, bez potrzeby angażowania wyższych warstw.

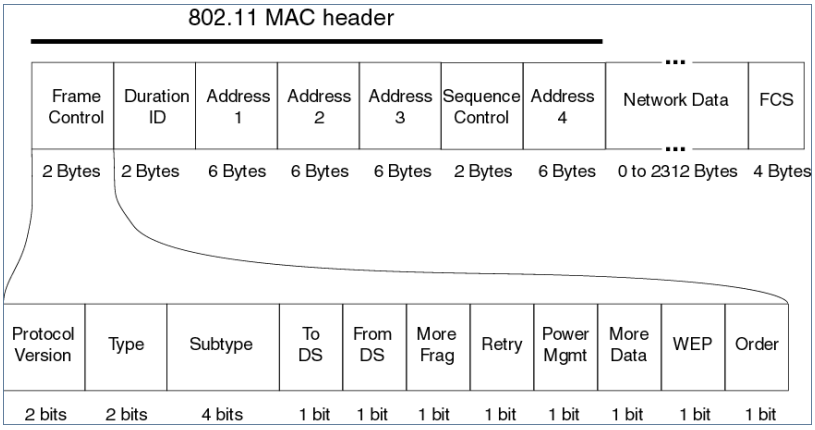
W sieciach bezprzewodowych nie mamy do czynienia z „bezpośrednim fizycznym" podłączeniem urządzenia do kanału komunikacyjnego. W związku z tym muszą zostać zastosowane w tym przypadku funkcje odpowiedzialne za logiczne podłączenie stacji klienckiej do systemu BSS. Ponadto ze względu na duże prawdopodobieństwo występowania zakłóceń oraz pojawiania się błędów podczas transmisji danych stosowany jest mechanizm potwierdzeń realizowanych na poziomie drugiej warstwy modelu OSI. Dodatkowo należy pamiętać, iż szybkość transmisji zależy od mocy odbieranego sygnału, co oznacza, iż urządzenia w trakcie nawiązywania połączenia muszą uzgodnić najlepszy możliwy sposób kodowania sygnału. W związku z powyższym w celu obsługi transmisji danych w sieciach bezprzewodowych IEEE 802.11 wykorzystuje się trzy typy ramek:

- **Ramki zarządzające** (*ang. management frames*) – określające parametry połączenia oraz odpowiedzialne za podłączenie klienta do sieci radiowej,
- **Ramki kontrolne** (*ang. control frames*) – ramki potwierdzeń, oraz ramki pozwalające na zarządzanie czasem radiowym np. RTS/CTS,
- **Ramki danych** (*ang. data frames*) – niosące dane pochodzące z wyższych warstw modelu OSI,

Format ramki IEEE 802.11 został przedstawiony na Rysunku 2. Jak widać rozpoczyna się ona 2-bajtowym polem kontrolnym określającym typ ramki oraz liczne parametry komunikacji. W szczególności są to pola:

- **Version** – określające wersję protokołu 802.11 (2 bity),
- **Type** – typ ramki, sekwencja 00 oznacza ramkę zarządzającą, 01 ramkę kontrolną, 10 ramkę danych, 11 jest wartością zarezerwowana (2 bity),

- **Subtype** – podtyp ramki (4 bity), typowe kody typów i podtypów ramek przedstawiono w Tabeli 2,
- **ToDs, FromDS** – pola określające rodzaj ruchu z lub do systemu dystrybucyjnego DS, który najczęściej oznacza punkt dostępowy (1 bit),
- **More Fragments** – pole wykorzystywane w przypadku, gdy przed wysłaniem wymagany jest podział oryginalnych danych, co oznacza, iż przesyłane w niniejszej ramce informacje będą miały swoją kontynuację w kolejnej ramce (1 bit),
- **Retry** – pole retransmisji oznaczające, że pakiet został wysłany ponownie (1 bit),
- **Power Management** – pole zarządzania mocą, ustawiona wartość 1 oznacza, iż po zakończeniu transmisji interfejs przejdzie w stan oszczędzania energii (power save mode), 0 oznacza, iż interfejs będzie cały czas aktywny. Opcja ta wykorzystywana jest przez urządzenia mobilne oszczędzające energię (1 bit),
- **More Data** – pole to ma wartość 1, gdy urządzenie posiada zbuforowane kolejne dane oczekujące na wysłanie do stacji odbiorczej, pole to jest istotne dla urządzeń z włączoną opcją zarządzania energią (1 bit),
- **WEP** – pole ma ustawioną wartość 1, gdy dane zostały zaszyfrowane, pierwotnie dotyczyło to tylko klucza WEP (1 bit),
- **Order** – pole posiada wartość 1, gdy dane wymagają specjalnej obsługi np. VoIP (1 bit).



Rysunek 2. Format ramki IEEE 802.11 [22].

Jak widać powyższe pola mają głównie charakter informacyjny określający sposób obsługi przesyłanych danych.

Tabela 2. Typowe wartości określające typy i podtypy ramek 802.11 [11].

Typ wartość	Typ opis	Podtyp wartość	Podtyp opis	Interpretacja pola w Wireshark
00	Management	0000	Association Request	wlan.fc.type_subtype == 0x00
00	Management	0001	Association Response	wlan.fc.type_subtype == 0x01
00	Management	0010	Reassociation Request	wlan.fc.type_subtype == 0x02
00	Management	0011	Reassociation Response	wlan.fc.type_subtype == 0x03
00	Management	0100	Probe Request	wlan.fc.type_subtype == 0x04
00	Management	0101	Probe Response	wlan.fc.type_subtype == 0x05
00	Management	1000	Beacon	wlan.fc.type_subtype == 0x08
00	Management	1010	Disassociation	wlan.fc.type_subtype == 0x0A
00	Management	1011	Authentication	wlan.fc.type_subtype == 0x0B
00	Management	1100	Deauthentication	wlan.fc.type_subtype == 0x0C
01	Control	1011	RTS	wlan.fc.type_subtype == 0x1B
01	Control	1100	CTS	wlan.fc.type_subtype == 0x1C
01	Control	1101	ACK	wlan.fc.type_subtype == 0x1D
10	Data	0000	Data	wlan.fc.type_subtype == 0x20

Kolejnymi polami opisywanej ramki są:

- **Duration /ID** – pole określające czas w ciągu którego spodziewane jest otrzymanie następnej ramki, ID pojawia się w ramkach kontrolnych określając identyfikator asocjacji stacji określony przez punkt dostępowy,
- **Address 1, Address 2, Address 3, Address 4** – pola określające adresy fizyczne poszczególnych interfejsów radiowych, ich znaczenie zależy od typu

transmisji określonej polami ToDS oraz FromDS. Szczegółowe ich znaczenie przedstawiono w Tabeli 3. Opis Destination oznacza adres docelowego odbiorcy danych, Source jest adresem nadawcy danych, Receiver oznacza adres odbierającego urządzenia pośredniczącego, Transmitter adres pośredniczącego urządzenia wysyłającego dane, BSSID oznacza adres radiowy punktu dostępowego.

- **Sequence Control** – pozwala na filtrowanie ruchu i określenie poprawnej kolejności przesłanych danych np. podczas retransmisji,
- **Network Data** – przesyłane dane wyższych warstw,
- **FCS** – stanowi obliczoną sumę kontrolną.

Tabela 3. Znaczenie adresów w ramce IEEE 802.11 w zależności od wartości pól „ToDS i „FromDS".

To DS	From DS	Address 1	Address 2	Address 3	Address 4	Typ połączenia
0	0	Destination	Source	BSSID	N/A	ad hoc lub beacon z STA do STA
0	1	Destination	BSSID	Source	N/A	infrastructure z AP do STA
1	0	BSSID	Source	Destination	N/A	infrastructure z STA do AP
1	1	Receiver	Transmitter	Destination	Source	infrastructure AP do AP

5. Proces podłączania klienta bezprzewodowego

Wiedząc już jak wygląda postać ramki, warto prześledzić sam proces podłączania klienta do sieci radiowej. Istnieją dwa sposoby wyszukiwania sieci przez stację kliencką:

- **Połączenie pasywne** – polegające na skanowaniu przez stację kliencką kanałów radiowych w oczekiwaniu na **ramkę nawigacyjną (*ang. Beacon*)** wysyłaną cyklicznie typowo co 100 ms przez punkt dostępowy. W ramce tej znajdują się parametry obsługiwanej sieci takie jak: nazwa sieci SSID, zabezpieczenia czy wspierane prędkości transmisji. Po odebraniu ramki nawigacyjnej system klienta sprawdza czy nie posiada zapisanego profilu konfiguracji związanego z odczytaną nazwą sieci. Jeżeli taki istnieje, to stacja kliencka próbuje połączyć się z

rozgłaszaną siecią, jeżeli nie to oczekuje na decyzję użytkownika. Jest to domyślny sposób podłączania użytkownika do sieci radiowej.

- **Połączenie aktywne** – polegające na wysyłaniu przez stację kliencką **ramki sondującej (*ang. Probe Request*)** zdefiniowanej na podstawie zapisanego profilu sieci. Ramka ta jest rozgłaszana kolejno po dostępnych kanałach pasma radiowego. Aby uruchomić ten tryb połączenia należy w profilu sieciowym systemu operacyjnego klienta skonfigurować opcję wymuszającą połączenie z siecią, która nie emituje swojej nazwy w ramkach nawigacyjnych. Ukrycie sieci obsługiwanej przez punkt dostępowy oznacza, iż w wysyłanych ramkach nawigacyjnych nie ma określonego identyfikatora sieci SSID.

Ostatecznie po uzyskaniu informacji o parametrach sieci stacja kliencka wysyła do punktu dostępowego ramkę Probe Request oczekując na zwrotną informację o parametrach sieci zawartą w ramce **Probe Response**. Po tym etapie następuje proces autentykacji, który jest realizowany poprzez przesyłanie ramek **Authentication Request** oraz **Authentication Response**. Jak widać z przedstawionej struktury ramki, pierwotnie standard IEEE 802.11 przewidywał dwa warianty autentykacji:

- otwartą – oznaczającą brak autentykacji klienta i szyfrowania danych,

W przypadku otwartej autentykacji interfejs radiowy wysyła ramkę autentykacji do punktu dostępowego, który odpowiada ramką autentykacji zawierającą akceptację lub odrzucenie żądania klienta.

- zamkniętą – z wykorzystaniem uwierzytelnienia opartego na współdzielonym kluczu WEP, w tym przypadku transmisja przesyłana przez sieć jest kryptowana,

Przy wykorzystaniu współdzielonego klucza WEP, interfejs radiowy wysyła inicjującą ramkę autentykacji do punktu dostępowego. Punkt dostępowy odpowiada ramką autentykacji zawierającą tekst (challenge text), który musi zostać zaszyfrowany przez stację kliencką za pomocą posiadanego klucza WEP, a następnie wysłany do punktu dostępowego. Punkt dostępowy deszyfruje przesłany tekst przy pomocy swojego klucza WEP sprawdzając czy otrzymany ciąg znaków jest identyczny z wysłanym tekstem do stacji klienckiej. Na tej podstawie punkt dostępowy wysyła ramkę autentykacji informując klienta o wyniku procesu autentykacji.

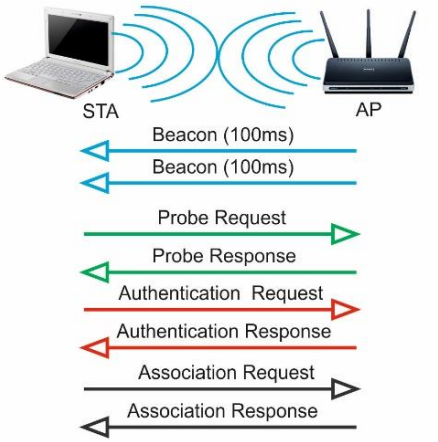
Ze względu na ograniczenia związane z eksportowaniem technologii kryptograficznych poza obszar USA rozwiązanie WEP pierwotnie stosowało 40-bitowy klucz (nazywany WEP-40), tworząc w połączeniu z 24-bitowym wektorem inicjalizującym (IV) klucz RC4 o długości 64 bitów. Stosowany algorytm RC4 jest symetrycznym szyfrem strumieniowym z poufnym kluczem zwanym inaczej strumieniem klucza, który wykorzystywany jest do szyfrowania przesyłanych danych. W celu odkodowa-

nia wiadomości, odbiorca wykorzystuje ten sam strumień klucza. Po zniesieniu restrykcji zgodnie ze standardem, klucz został określony jako 40 lub 104-bitowy tworząc z 24-bitowym wektorem IV odpowiednio 64 lub 128-bitowy klucz RC4. Wydłużenie strumienia klucza w naturalny sposób zwiększyło bezpieczeństwo przesyłanych danych. Obecnie w rozwiązaniach niektórych producentów pojawiają się implementacje pozwalające na stosowanie również 152 i 256-bitowych kluczy RC4 [6].

Po autentykacji następuje etap przyłączenia klienta do obszaru BSS. W celu realizacji tego procesu stacja kliencka wysyła do punktu dostępowego ramkę **Association Request.** Zawiera ona informacje o interfejsie radiowym (np. listę wspieranych prędkości) oraz identyfikator sieci (SSID), do której klient chce się przyłączyć. Po otrzymaniu żądania punkt dostępowy analizuje je i w przypadku akceptacji rezerwuje odpowiedni obszar pamięci przeznaczony do obsługi klienta oraz ustanawia dla niego identyfikator przyłączenia AID (*ang. association ID*). Następnie wysyła do klienta ramkę **A*ssociation Response*** zawierającą odpowiedź na otrzymane żądanie klienta (akceptację lub odrzucenie). W przypadku akceptacji punkt dostępowy wysyła klientowi jego identyfikator przyłączenia AID. Po otrzymaniu wszystkich informacji klient radiowy może korzystać z punktu dostępowego w celu realizowania komunikacji z innymi hostami.Po poprawnym przeprowadzeniu całego procesu (Rys. 3) klient może rozpocząć realizację kolejnych funkcji np. związanych z uzyskaniem konfiguracji interfejsu w oparciu o protokół DHCP [24].

W celu sprawowania pełnej kontroli nad obsługą klienta w sieci bezprzewodowej wykorzystywane są również inne ramki zarządzające. Jako przykład można wymienić tutaj **ramkę deautentykacji (*ang. Deauthentication Frame*)** wysyłaną przez stację nadawczą do innej stacji (punktu dostępowego) w celu zakończenia bezpiecznego połączenia. **Ramka rozłączenia (*ang. Disassociation Frame*)** wysyłana jest zaś przez stację do punktu dostępowego, gdy chce ona zakończyć swoje przyłączenie. Punkt dostępowy po jej otrzymaniu zwalnia przydzieloną dla klienta pamięć oraz usuwa go z tablicy asocjacyjnej. W przypadku, gdy interfejs radiowy utraci połączenie z dotychczasowym punktem dostępowym, lub moc odbieranego sygnału spadnie poniżej minimalnej wartości pozwalającej na realizację połączenia (typowo - 80 dBm), przechodzi on w stan skanowania oczekując na nowe ramki nawigacyjne. Po odebraniu ramki nawigacyjnej od innego punktu dostępowego, ale z tym samym identyfikatorem sieci SSID, klient wysyła do niego ramkę **żądania ponownego przyłączenia (*ang. Reassociation Request Frame*).** W rozwiązaniach opartych na kontrolerach WLAN, po akceptacji połączenia nowy punkt dostępowy może kontynuować przesyłanie danych znajdujących się w buforze poprzedniego punktu dostępowego czekającego na uruchomienie transmisji do stacji klienckiej. Aby to jednak nastąpiło nowy punkt dostępowy musi poinformować stację kliencką o przyłączeniu wysyłając

ramkę odpowiedzi na żądanie ponownego przyłączenia (ang. R*eassociation Response Frame).* Podobnie jak w procesie typowego przyłączenia, ramka może zawierać akceptację lub odrzucenie żądania. Pozytywna odpowiedź zawiera informacje takie jak wspierane prędkości transmisji danych oraz identyfikator przyłączenia AID.

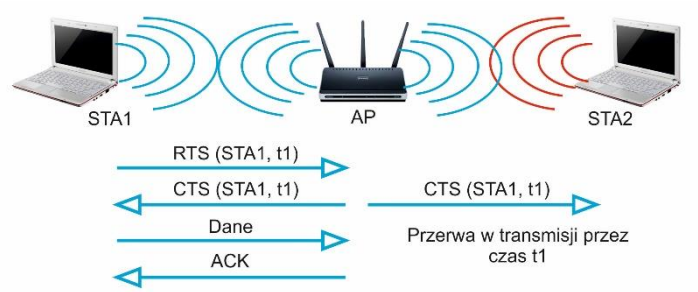


Rysunek 3. Etapy przyłączania klienta do sieci bezprzewodowej.

6. Ramki kontrolne

W odróżnieniu od komunikacji realizowanej w ramach większości sieci przewodowych, transmisja realizowana w standardzie IEEE 802.11 jest transmisją wymagającą potwierdzeń. Wynika to z dużej zawodności, która może towarzyszyć przesyłaniu danych w niechronionym środowisku radiowym. W związku z powyższym po przesłaniu ramki danych urządzenie nadawcze oczekuje potwierdzenia. Po otrzymaniu ramki danych stacja odbiorcza weryfikuje jej sumę kontrolną i w przypadku zgodności z obliczoną wartością wysyła do nadawcy **ramkę potwierdzenia ACK** (***ang. Acknowledgement Frame)***. Stacja nadawcza, która nie otrzymała potwierdzenia odbioru ponownie wysyła tą samą ramkę jednocześnie odnotowując ten fakt w polu kontrolnym ramki. Jak już wcześniej opisywano w sieciach bezprzewodowych ze względu na parametry fizyczne transmisji może dochodzić do problemu tzw. ukrytego węzła (Rys. 1). W takiej sytuacji, aby uniknąć kolizji może zostać zastosowany mechanizm zarządzania pasmem RTS/CTS. Polega on na wysłaniu przez stację nadawczą **ramki RTS (*ang. Request to Send)*** do punktu dostępowego, co stanowi pierwszy etap dwu-stronnego nawiązania połączenia (*ang. 2-way handshake*), które

musi zostać zrealizowane przed wysłaniem danych. W odpowiedzi punkt dostępowy wysyła do wszystkich podłączonych stacji **ramkę CTS (*ang. Clear to Send*)**. Zawiera ona identyfikator AID stacji żądającej wolnego pasma oraz wartość czasu, przez który będzie odbywała się transmisja. Stacje, których identyfikator AID jest różny od zawartego w ramce odbierając ten komunikat przerywają wysyłanie danych przez określony w ramce czas. Jednocześnie stacja żądająca wolnego pasma po odebraniu takiej informacji przystępuje niezwłocznie do nadawania danych. Proces ten realizowany jest przez czas określony w ramce CTS. Następnie punkt dostępowy potwierdza otrzymanie danych standardową ramką ACK (Rys. 4). Rozwiązanie to wpływa na zmniejszenie ilości kolizji spowodowanych wystąpieniem „problemu ukrytych węzłów", co skutkuje zwiększeniem efektywnego pasma klienta. Należy zauważyć, iż funkcja ta generuje dodatkowe ramki obsługujące niniejszą komunikację. W związku z tym jest ona włączana wyłącznie w sytuacji występowania dużej ilości błędów w transmitowanych danych lub w przypadku przesyłania dużych pakietów, dla których wzrasta prawdopodobieństwo pojawienia się zakłócenia. Włączenie mechanizmu RTS/CTS w sytuacji gdy nie występuje „problem ukrytego węzła" może spowodować zmniejszenie pasma dostępnego dla podłączonych stacji klienckich.



Rysunek 4. Działanie mechanizmu Request to Send/Clear to Send.

W przypadku sieci radiowej prawdopodobieństwo wystąpienia błędu transmisji wzrasta wraz ze zwiększającą się wielkością przesyłanego pakietu opakowanego w ramkę. W związku z powyższym w celu optymalizacji transmisji w sieci radiowej punkt dostępowy po otrzymaniu ramki z sieci przewodowej może podjąć decyzję o podziale zawartych w niej danych i przesłaniu ich niezależnie w kilku ramkach. Jednocześnie informuje on odbiorcę o zaistniałej sytuacji ustawiając odpowiednie wartości w polach kontrolnych przesyłanych ramek. Najczęściej funkcja ta realizowana jest automatycznie dla pakietów o wielkości większej niż określona wartość graniczna definiowana jako Fragmentation Threshold. Funkcja ta wpływa na generowanie większej ilości przesyłanych ramek danych, jednakże nie wymaga stosowania dodatkowych ramek kontrolnych poza standardowymi ramkami ACK.

7. Bezpieczeństwo w sieciach bezprzewodowych

Przedstawiony na Rysunku 3 schemat komunikacji dotyczy tylko obowiązkowych etapów przyłączania. W praktyce może okazać się, iż ze względu na stosowane rozwiązania dotyczące bezpieczeństwa będzie ich znacznie więcej. Wynika to z faktu, iż zastosowany pierwotnie sposób kryptowania danych okazał się mało odporny na ataki, co było impulsem do kontynuowania badań nad innymi formami zabezpieczeń. Prace te były realizowane zarówno przez firmy produkujące urządzenia sieciowe (np. protokół LEAP firmy Cisco) jak i konsorcjum Wi-Fi Alliance oraz organizację IEEE. Ostatecznie spowodowało to pojawienie się nowych standardów zabezpieczeń, które pierwotnie nie były masowo wdrażane we wszystkich urządzeniach, co skutkowało problemami z ich wzajemną komunikacją. Proponowane rozwiązania miały opierać się na opisanym już standardzie ramki IEEE 802.11. W wyniku implementacji nowych standardów zmieniono interpretację pola „WEP" znajdującego się w polu kontrolnym, które obecnie opisywane jest jako „protected", co oznacza, że przesyłane dane zostały zaszyfrowane. Podczas prac nad nowym standardem bezpieczeństwa IEEE 802.11i stwierdzono, iż ze względu na wysoki stopień złożoności nie będzie on mógł być w prosty sposób zastosowany w starszych urządzeniach. W związku z powyższym w 2003 roku konsorcjum Wi-Fi Alliance wprowadziło swój tzw. przejściowy standard WPA (*ang. Wi-Fi Protected Access*). Rozwiązywał on główne problemy związane ze stosowaniem klucza WEP wymagając wyłącznie implementacji programowej. Zawierał on tylko wybrane rozwiązania proponowane w specyfikacji Draft 802.11i, dlatego też późniejszą implementację pełnego standardu IEEE 802.11i opisuje się jako WPA2 lub RSN (*ang. Robust Security Network*).

Do największych problemów związanych z kluczem WEP można zaliczyć:

- bezpieczeństwo współdzielonego klucza – klucz WEP stanowi jedyny element bezpieczeństwa, jest zapisany w konfiguracji wszystkich urządzeń podłączonych do sieci, w efekcie cały ruch szyfrowany jest w ten sam sposób,
- stałość klucza – brak mechanizmów pozwalających na automatyczną zmianę klucza, podczas przesyłania danych, w przypadku gdy istnieje obawa, iż klucz dostał się w niepowołane ręce należy „ręcznie" dokonać zmiany klucza we wszystkich urządzeniach,
- jeden typ uwierzytelniania – brak wsparcia dla zaawansowanego uwierzytelniania takiego jak indywidualne klucze, certyfikaty, hasła.

Badania nad algorytmem szyfrowania danych z wykorzystaniem klucza WEP doprowadziły do wniosków, iż jest on stosunkowo łatwy do złamania poprzez analizę przesyłanych danych. W efekcie pojawiły się narzędzia umożliwiające automatyczne

rozszyfrowanie klucza WEP, czego przykładem jest AirSnort oraz Aircrack-ng [2]. W kwietniu 2007 roku grupa osób z Darmstadt University of Technology opublikowała artykuł przedstawiając nową metodę ataku o nazwie PTW, która umożliwia uzyskanie klucza WEP z podsłuchiwanych danych w czasie krótszym niż 60 sekund, co ostatecznie pokazało słabość tego rozwiązania [7].

Wprowadzony standard IEEE 802.11i rozwiązuje te problemy wprowadzając dwa nowe protokoły: 4-Way Handshake oraz Group Key Handshake odpowiedzialne za wymianę i aktualizację kluczy. Wykorzystują one standard IEEE 802.1x sprawujący kontrolę dostępu do sieci bezprzewodowej z wykorzystaniem protokołu EAP (*ang. Extensible Authentication Protocol* [16,17]. Standard ten obejmuje również stosowanie protokołów TKIP (*ang. Temporal Key Integration Protocol*) wraz z MIC (*ang. Message Integrity Check*) oraz CCMP wykorzystujący szyfrowanie AES (*ang. Advanced Encryption Standard*) [8]. Wspomniany tutaj protokół TKIP stanowi rozszerzenie mechanizmu szyfrowania opartego na kluczu WEP. W związku z powyższym jego wdrożenie było możliwe poprzez aktualizację oprogramowania i jako taki stał się rozwiązaniem zaimplementowanym w standardzie WPA. Jest on odpowiedzialny za szyfrowanie każdego pakietu innym 128-bitowym kluczem, co rozwiązuje jeden z problemów związanych ze stałością klucza WEP. Szczegółowy opis procesów związanych z autentykacją realizowaną w ramach standardu WPA i WPA2 wykracza stanowczo poza zakres niniejszego opracowania. Dodatkowe informacje na ten temat można znaleźć w innych źródłach [5,10]. Powyższy opis miał na celu jedynie ogólne zarysowanie całego procesu wskazując na jego olbrzymią złożoność.

8. Badanie ramek

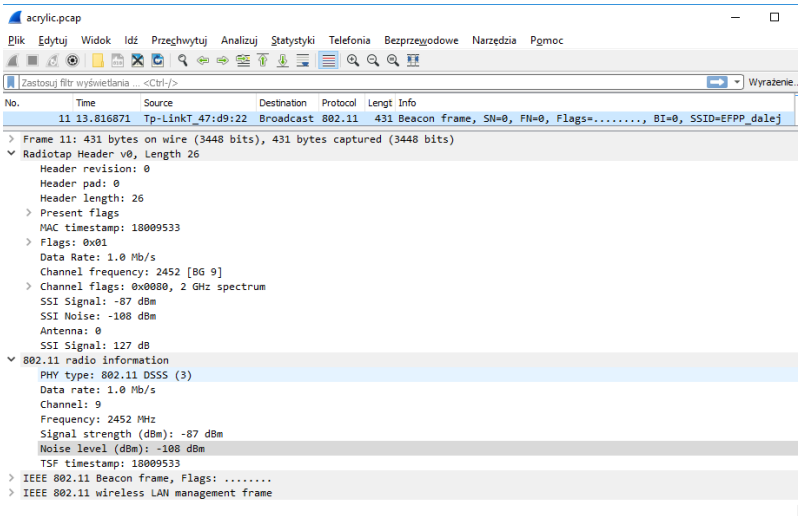
Analizowanie opisywanych procesów realizowanych w sieciach bezprzewodowych wymaga możliwości obserwacji ramek docierających do interfejsu bezprzewodowego. W tym celu można wykorzystać komercyjnie dostępne przystawki umożliwiające śledzenie wybranego kanału radiowego i pełną analizę danych docierających do interfejsu [21]. W przypadku gdy nie chcemy ponosić dodatkowych kosztów można zastosować również zwykły interfejs radiowy komputera. Niestety w dużej ilości przypadków napotkamy na problemy wynikające z samego standardu IEEE 802.11, a mianowicie założenia, iż urządzenie może odbierać i analizować dane dopiero po przejściu procesu podłączenia do punktu dostępowego. Oznacza to, że w celu dokonywania pełnej analizy danych musimy zmienić tryb pracy interfejsu, który jest niezgodny z opisywanym standardem. W popularnym programie do analizy danych sieciowych Wireshark odpowiedzialna jest za to opcja przechwytywania ramek „Monitor mode" [26]. Po jej włączeniu interfejs sieciowy analizuje wszystkie ramki docierające do niego na wybranym kanale radiowym, niezależnie od

określonego w nich identyfikatora sieci SSID. Ten nietypowy tryb pracy interfejsu musi być wspierany przez kartę oraz jej sterownik, co jak się okazuje często stanowi problem. W takim przypadku nasłuchiwanie ramek nie będzie możliwe, co więcej po podłączeniu urządzenia do sieci radiowej i analizie odbieranych danych program Wireshark będzie interpretował je jako ramki IEEE 802.3, co może budzić duże zdziwienie. Obecnie znacznie więcej sterowników dających takie możliwości dostępnych jest dla systemów Linux niż Windows, a zatem czasami rozwiązaniem może być uruchomienie programu Wireshark pod innym systemem operacyjnym. Co więcej po przechwyceniu i zapisaniu danych można je później poprawnie analizować nawet w systemie, który nie wspiera trybu monitoringu sieci radiowej. W pewnych przypadkach rozwiązaniem może być także instalacja innego oprogramowania posiadającego wbudowane odpowiednie uniwersalne sterowniki do kart sieciowych. Przykładem takiej aplikacji może być Acrylic Wi-Fi Proffesional Scanner [12]. Na Rysunku 5 przedstawiono okno tego programu z widocznymi zarejestrowanymi ramkami nawigacyjnymi. Wskazana ramka dotyczy sieci o identyfikatorze SSID „EFPP_dalej", która jak widać pracuje na kanale 9 w pasmie 2,4 GHz wykorzystując 40 MHz kanał.

Rysunek 5. Okno programu Acrylic Wi-Fi Professional z analizowanymi ramkami nawigacyjnymi.

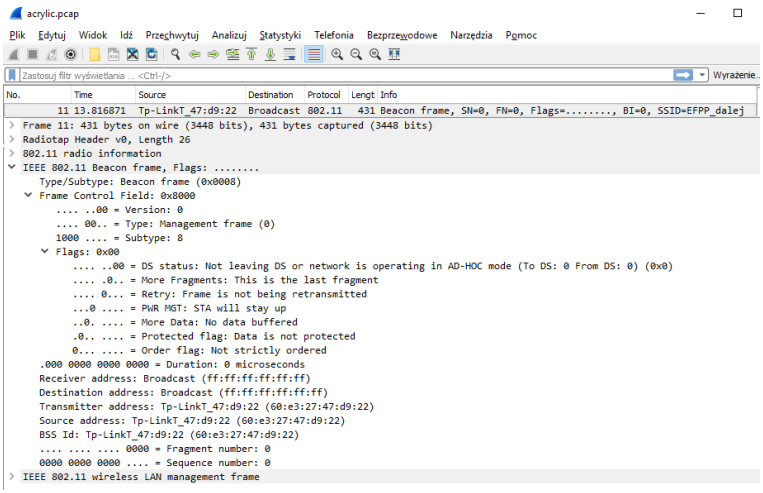
W przekonaniu autora znacznie lepiej niniejsze dane interpretowane są przez program Wireshark. Na Rysunku 6 przedstawiono informacje warstwy fizycznej dotyczące odebranej ramki nawigacyjnej. Jak widać ramki nawigacyjne transmitowane są z najniższą dozwoloną prędkością (1 Mb/s), aby były one widoczne dla wszystkich stacji radiowych. Dane został odebrane na kanale 9 w pasmie 2,4 GHz, co oznacza częstotliwość centralną 2452 MHz. Poziom odbieranego sygnału wynosił -87 dBm, przy poziomie szumu -108 dBm, wykorzystany typ modulacji to DSSS. Wszystkie te

dane wynikają z parametrów fizycznych odczytanych przez interfejs radiowy odbiorcy.



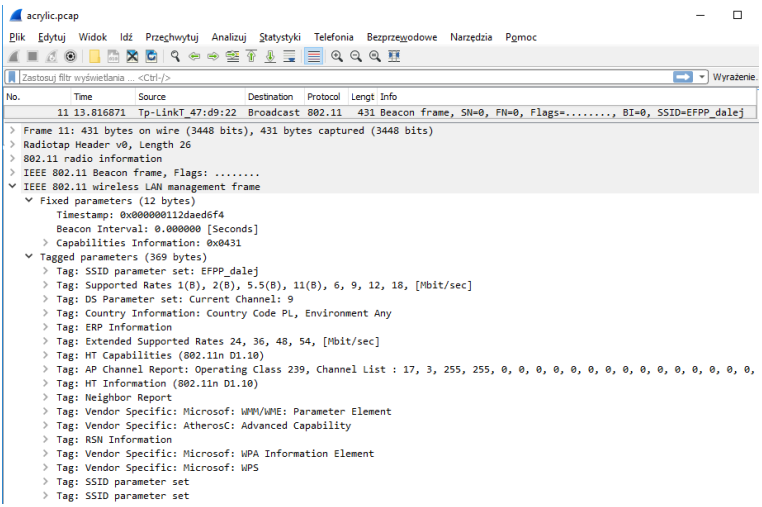
Rysunek 6. Ramka nawigacyjna interpretowana w programie Wireshark (informacje opisujące warstwę fizyczną).

Znacznie ciekawsze informacje z naszego punktu widzenia znajdują się w samej ramce wysłanej przez punkt dostępowy. Na Rysunku 7 widoczny jest nagłówek przechwyconej ramki. Jest to ramka zarządzająca (typ 00), pełniąca funkcję nawigacyjną (podtyp 1000 Beacon). Obie flagi ToDs oraz FromDS posiadają wartość 0, co oznacza, iż źródłem tej ramki jest punkt dostępowy, a ma ona trafić do stacji klienckiej. W związku z powyższym pierwszy adres jest adresem urządzenia docelowego (w tym przypadku jest to rozgłoszenie ff:ff:ff:ff:ff:ff), drugi adres oznacza stację nadawczą (adres 60:e3:27:47:d9:22 interpretowany jako TP-LinkT_), trzeci zaś określa BSSID, który w tym przypadku jest tożsamy z adresem punktu dostępowego (60:e3:27:47:d9:22). Ze względu na charakter tej ramki pozostałe pola przyjmują wartość 0.



Rysunek 7. Ramka nawigacyjna interpretowana w programie Wireshark (pola ramki IEEE 802.11).

Rysunek 8 przedstawia dane niesione w ramce nawigacyjnej opisującej parametry rozgłaszanej sieci. Widoczny jest tutaj identyfikator SSID (EFPP_dalej), deklarowane są również wspierane prędkości obligatoryjne: 1 Mb/s, 2 Mb/s, 5,5 Mb/s, 11 Mb/s kompatybilne ze standardem IEEE 802.11b oraz prędkości 6 Mb/s, 9 Mb/s,12 Mb/s,18 Mb/s. Dodatkowo opcjonalnie klient może wykorzystywać prędkości 24 Mb/s, 36 Mb/s, 48 Mb/s i 54 Mb/s (Extended Supported Rates). Warunkiem podłączenia klienta do sieci jest wspieranie przez niego wszystkich deklarowanych prędkości obowiązkowych. Podczas łączenia się z siecią klient wybiera najlepsze kodowanie (największą wspieraną prędkość) możliwe do zastosowania przy odbieranym poziomie sygnału. W ramce widoczne są również informacje dotyczące kodu kraju, który jest istotny ze względu na regulacje prawne dotyczące nielicencjonowanego pasma (PL), numer wykorzystywanego kanału radiowego (9) oraz typ standardu sieci (802.11n). Jak widać szczegółowa analiza otrzymywanych danych przynosi wiele istotnych informacji, które nie tylko mają aspekt edukacyjny, ale mogą pozwolić na optymalizację sieci radiowej.

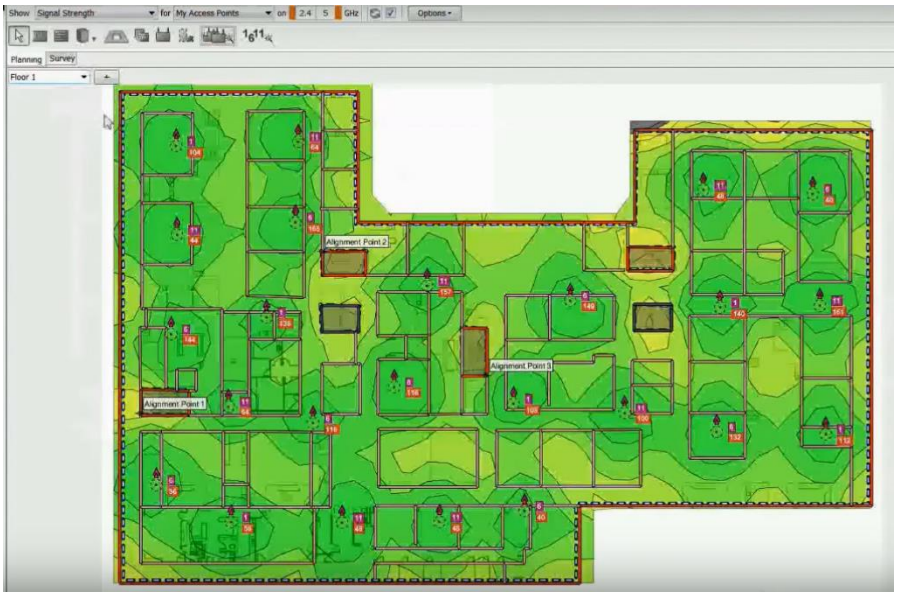


Rysunek 8. Ramka nawigacyjna interpretowana w programie Wireshark (informacje dotyczące rozgłaszanej sieci radiowej).

9. Zasięg sieci i moc nadawcza

Założenie dotyczące wykorzystania nielicencjonowanego pasma niesie ze sobą liczne problemy związane z faktem, iż te same częstotliwości mogą być wykorzystywane w tym samym czasie przez różne urządzenia. Dotyczy to zarówno innych sieci bezprzewodowych pracujących w standardzie IEEE 802.11 jak i komunikacji w standardzie Bluetooth (802.15.1 pasmo 2,4 GHz) [13] oraz zupełnie innych urządzeń takich jak układy zdalnego sterowania czy nianie elektroniczne. Ostatecznie skutkuje to znacznym zaszumieniem wykorzystywanego kanału radiowego, co negatywnie wpływa na maksymalną prędkość transmisji danych. Pewnym rozwiązaniem tego problemu mogłoby być zwiększenie mocy nadawczej wykorzystywanego urządzenia, jednakże między innymi ze względu na bezpieczeństwo regulacje prawne precyzyjnie określają maksymalną moc nadawania dla określonej częstotliwości. W przypadku 2,4 GHz wynosi ona 100 mW, a dla 5 GHz aż 1 W. W związku z powyższym technologie Wi-Fi przystosowane są głównie do pracy na małych odległościach (typowo do 100 m) w środowisku typu „indoor", czyli wewnątrz budynków. Nie oznacza to, że nie mogą być one stosowane na zewnątrz budynków, ale w takich przypadkach urządzenia te muszą spełniać również surowe normy dotyczące odporności na różne warunki atmosferyczne. Z powyższych rozważań jasno wynika, iż wewnątrz budynków na jakość przesyłanego sygnału oprócz zakłóceń wpływa również tłumienność obiektów przez które ma przechodzić fala elektromagnetyczna (ściany, drzwi , okna).

Poszczególne współczynniki absorbcji zależą zarówno od materiału, z którego wykonano poszczególne elementy jak i wykorzystywanej częstotliwości. Typowo ich wartości są większe dla wyższej częstotliwości pasma radiowego. W związku z powyższym analiza dotycząca dostępności sygnału radiowego dla klienta w obrębie konkretnej lokalizacji nie jest rzeczą trywialną. Na rynku istnieje wiele programów mających na celu ułatwienie projektowania oraz zarządzania sieciami radiowymi. Pozwalają one stworzyć plan budynku wraz z określeniem typu ścian oraz ich tłumienności, a także mocy nadajników. Następnie na podstawie dostarczonych danych program w sposób automatyczny jest w stanie określić teoretyczny zasięg projektowanej sieci radiowej. Ponadto po zrealizowaniu tej sieci w praktyce i dokonaniu odpowiednich pomiarów (badanie typu Site Survey) możliwe jest uwzględnienie zmierzonych wartości, a następnie zastosowanie algorytmów optymalizujących rozmieszczenie punktów dostępowych. Na Rysunku 9 przedstawiono przykładowy plan budynku wykonany w programie Ekahau wraz z szacowanym pokryciem sieci radiowej przy odpowiednio zdefiniowanych punktach dostępowych [14].



Rysunek 9. Plan budynku wykonany w programie Ekahau wraz z szacowanym pokryciem sieci radiowej przy odpowiednio zdefiniowanych punktach dostępowych [14].

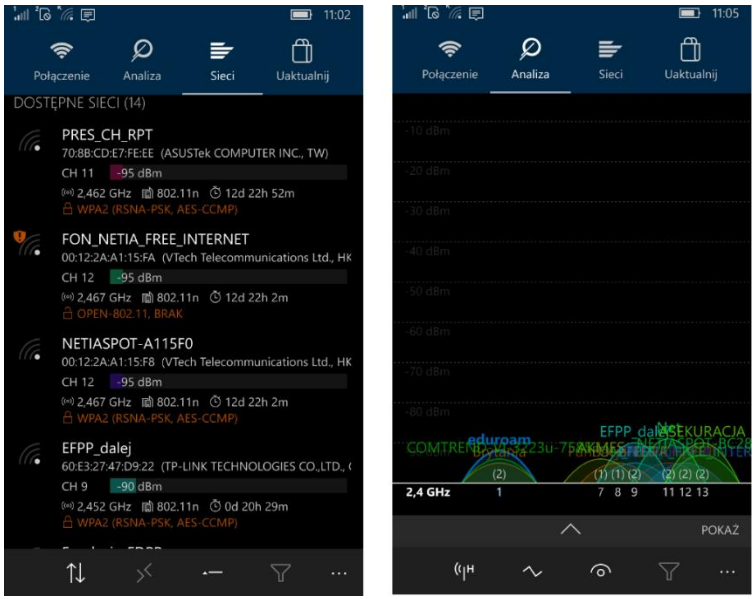
Zarówno na etapie planowania jak i optymalizacji sieci radiowej warto posłużyć się narzędziami umożliwiającymi w praktyce zbadanie jakości sygnału docierającego do odbiornika. W tym celu można wykorzystać profesjonalne analizatory widma lub

oprogramowanie, które zamieni komputer lub smartfon w prosty analizator sieci radiowych. Przykładem takiego oprogramowania może być InSSIDer firmy Metageek uruchomiony na komputerze PC (Rys. 10) lub WiFiAnalyzer uruchomiony na smartfonie wyposażonym w interfejs bezprzewodowy (Rys. 11).

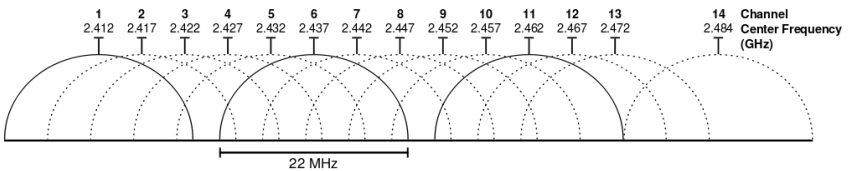
Rysunek 10. Ekran programu InSSIDer przedstawiający dostępne sieci radiowe [20].

W obu przypadkach programy wyświetlają informacje na temat dostępnych sieci radiowych pracujących na różnych częstotliwościach, których sygnały odbierane są z różną mocą. Aby w pełni zrozumieć informacje uzyskiwane z tego typu programów należy przypomnieć, iż w przypadku standardu IEEE 802.11 dostępne nielicencjonowane pasmo 2,4 GHz zostało podzielone na 22 MHz kanały, których częstotliwości główne oddzielone są o 5 MHz. Ze względu na różne regulacje prawne pasmo opisywane jako 2,4 GHz ma w rzeczywistości różną szerokość, co ostatecznie wpływa na różną liczbę kanałów dostępnych w różnych państwach. W USA dostępnych jest 11 kanałów, w Polsce oraz większej część Europy 13, a w Japonii aż 14. Szczegółowy podział kanałów został przedstawiony na Rysunku 12, z którego wynika, iż w całym dostępnym pasmie 2,4 GHz istnieją tylko trzy zupełnie niezakłócające się kanały. Oznacza to, iż na jednym obszarze mogą pracować maksymalnie 3 niezakłócające się punkty dostępowe. Podczas projektowania sieci bezprzewodowej ścisłe przestrzeganie tego warunku spowodowałoby, iż pełne pokrycie siecią bezprzewodową dużego budynku byłoby praktycznie niemożliwe. W efekcie stosuje się kanały pośrednie dbając o to, aby wykorzystujące je punkty dostępowe były jak najbardziej oddalone od siebie, przez co wzajemne zakłócenia będą jak najmniejsze. W trakcie

rozwoju standardu od wersji 802.11g zdecydowano się na zmianę szerokości kanałów na 20 MHz, co nie wpłynęło na ich ilość, a na lepszą separowalność. Ponadto standard IEEE 802.11n umożliwia wykorzystanie 40 MHz pasma wynikającego z połączenia ze sobą dwóch kanałów (np. 5 i 9) co pozwala na zwiększenie szybkości transmisji danych (Rys 10).



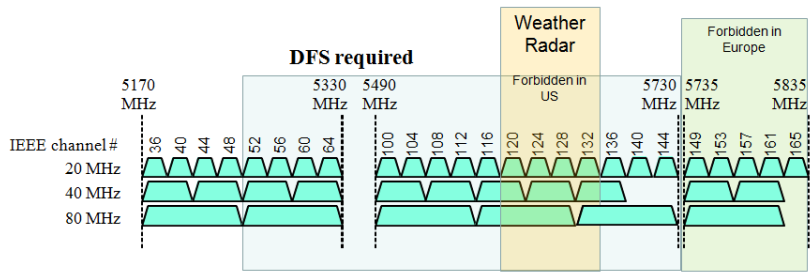
Rysunek 11. Ekran programu WiFiAnalyzer przedstawiający dostępne sieci radiowe [18].



Rysunek 12. Graficzna reprezentacja przydziału kanałów dla standardu 802.11b dla pasma 2,4 GHz [4].

W przypadku pasma 5 GHz problem wzajemnych zakłóceń jest znacznie mniejszy, gdyż kanały o szerokości 20 MHz są od siebie w pełni izolowane (Rys. 13). Jednakże ze względu na wykorzystanie tego pasma przez systemy radarowe urządzenia pracujące w górnych kanałach rozpoczynając od numeru 52 muszą być wyposażone w mechanizm DFS (*ang. Dynamic Frequency Selection*). Rozwiązanie to

oznacza, iż po wykryciu sygnału radarowego urządzenie ma obowiązek zmienić kanał komunikacyjny. W praktyce w pasmie 5 GHz mamy do dyspozycji tylko 4 kanały, których nie dotyczy to rozwiązanie (36, 40, 44, 48). Wykorzystując pozostałe kanały należy liczyć się z sytuacją, w której urządzenie sieciowe będzie musiało przełączyć się na inną częstotliwość. Wysoka czułość pogodowych stacji radarowych TDWR (*ang. Terminal Doppler Weather Radar*) sprawia, iż sytuacja ta może występować nawet, gdy są one oddalone nawet o 30 km od anteny nadawczej punktu dostępowego. Problemy tego typu pojawiają się w przypadku technologii typu „outdoor". W przypadku sieci bezprzewodowych zlokalizowanych wewnątrz budynków wysoka tłumienność ścian w większości rozwiązuje ten problem.



Rysunek 13. Organizacja pasma 5 GHz [19].

Jak wynika z Tabeli 1 oraz Rysunku 13 w przypadku pasma 5 GHz technologie IEEE 802.11n oraz IEEE 802.11ac przewidują zwiększenie prędkości transmisji poprzez łączenie kanałów tworząc 40 MHz, 80 MHz a nawet 160 MHz kanały komunikacyjne.

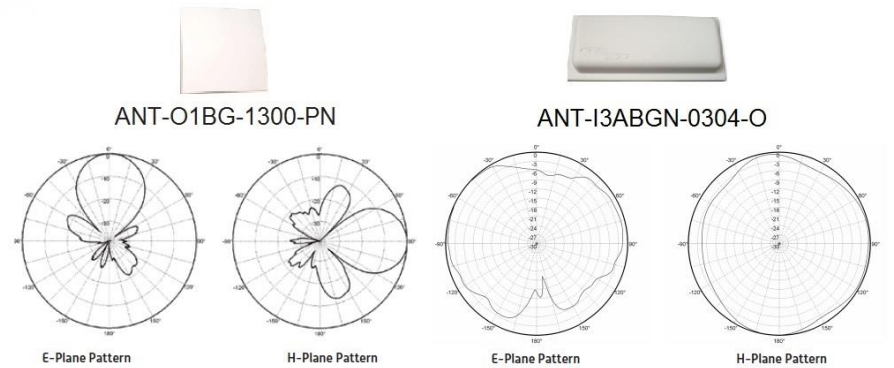
Programy umożliwiające analizę parametrów rozgłaszanych sieci oprócz ich identyfikatorów SSID, adresów interfejsów radiowych punktów dostępowych, standardów zastosowanych zabezpieczeń podają również informacje o jakości odbieranego sygnału (Rys. 10 i 11). W przypadku sieci bezprzewodowych moc sygnału wyrażania jest w jednostkach dBm i obliczana zgodnie z poniższym wzorem

$$P[dBm] = 10log_{10}\left(\frac{P_m[mW]}{1[mW]}\right), \quad (1)$$

gdzie P_m oznacza zmierzoną moc odbieranego sygnału, a wartością referencyjną jest 1 mW. W efekcie przy odbieranym sygnale o mocy 1 mW uzyskamy moc odbiorczą wynoszącą 0 dBm.

Jakość odbieranego oraz wysyłanego sygnału będzie uzależniona nie tylko od stosowanej mocy nadawczej, ale również od typu zastosowanej anteny. Obecnie na rynku dostępnych jest wiele rodzajów anten, które optymalizowane są pod kątem

różnych zastosowań. Podstawowym parametrem anteny jest jej wzmocnienie wyrażone w jednostkach dBi, które określa zysk anteny w stosunku do teoretycznej anteny izotropowej. Zatem w zależności od wyboru anteny można wpływać na kątowy rozkład natężenia generowanego pola elektromagnetycznego, zapewniając duże wzmocnienie w jednym kierunku przy jednoczesnym osłabieniu w innym. W typowych zastosowaniach „indoor" wykorzystuje się tzw. anteny dookólne, zbliżone parametrami do anteny izotropowej (Rys.14).



Rysunek 14. Rozkłady natężenia pola elektromagnetycznego przy częstotliwości 2,4 GHz dla zewnętrznej anteny kierunkowej ANT-O1BG-1300-PN o wzmocnieniu 13 dBi oraz anteny dookólnej ANT-I3ABGN-0304-O o wzmocnieniu 3 dBi.

Ostatecznie określając jakość sygnału nadawczego należy wziąć pod uwagę zarówno moc nadawczą interfejsu radiowego, wzmocnienie anteny oraz straty na ewentualnych kablach. W związku z powyższym w takich przypadkach należy posłużyć się parametrem EIRP (*ang. Effective Isotropical Radiated Power*), określającym równoważną efektywną moc promieniowania izotropowego naszego nadajnika zgodnie ze wzorem

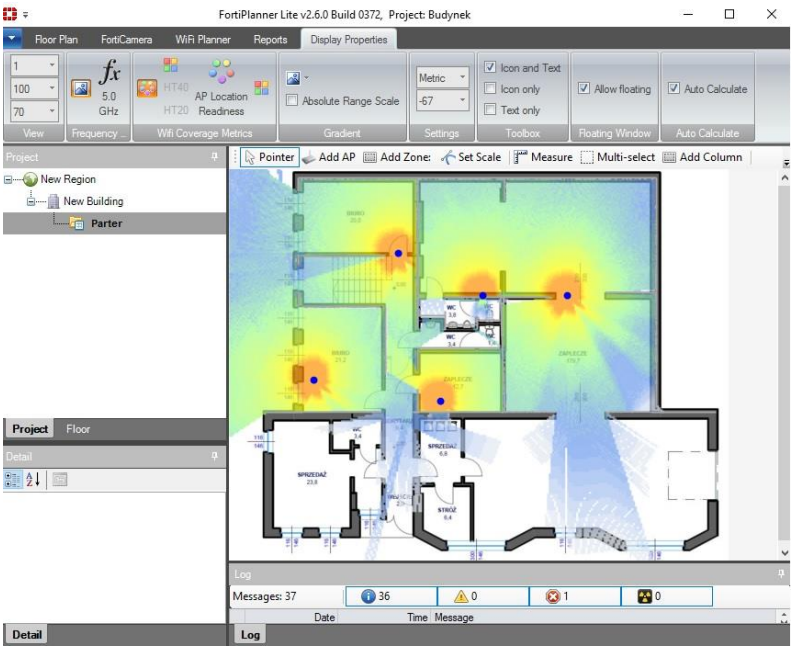
$$EIRP = P - Tk + Gi, \tag{2}$$

gdzie *P* jest mocą nadajnika (w dBm), *Tk* oznacza tłumienie kabla, a *Gi* zysk anteny. Przykładowo dla nadajnika o mocy 50 mW podłączonego do anteny kierunkowej o zysku 12 dBi kablem o tłumienności 0,55 dB/m i długości 18 metrów otrzymamy

$$EIRP = 10log_{10}\left(\frac{50mW}{1mW}\right) - 18 * 0{,}55 + 12 = 19{,}1[dBm] \tag{3}$$

W przypadku rozwiązań typu „indoor" punkt dostępowy najczęściej jest zintegrowany z anteną, co minimalizuje straty wynikające z wykorzystania długich kabli doprowadzających.

Jak widać podczas projektowania pokrycia budynku siecią radiową istotne jest również uwzględnienie parametrów fizycznych samych urządzeń. W związku z powyższym niektórzy producenci sprzętu udostępniają oprogramowanie, które oprócz możliwości definiowania w budynku obszarów obsługiwanych przez sieć radiową pozwala na wybór odpowiednich konkretnych urządzeń oraz zoptymalizowanie ich położenia i parametrów konfiguracyjnych w celu uzyskania jak najlepiej działającej sieci (Rys.15). W przypadku dużych sieci bezprzewodowych wykorzystujących dziesiątki punktów dostępowych niezbędne staje się zastosowanie rozwiązań opartych na kontrolerach WLAN. Pozwalają one na konfigurację i zarządzanie punktami dostępowymi, automatyczne planowanie obszaru pokrycia sieci radiowej, optymalizację pasma radiowego oraz kontrolę użytkowników [29].



Rysunek 15. Plan budynku wykonany w programie FortiPlanner wraz z szacowanym pokryciem sieci radiowej [15].

10. Podsumowanie

Proces projektowania, a następnie wdrożenia sieci radiowej jest bardzo skomplikowany. Wymaga on uwzględnienia wielu aspektów wynikających z założeń dotyczących topologii sieci jak i aspektów fizycznych związanych z dostępnością wolnych

kanałów radiowych w obsługiwanych pasmach, pojawiających się zakłóceń oraz parametrów fizycznych ścian budynków. Ostatecznie na podstawie wszystkich zebranych informacji należy przystąpić do wyboru odpowiednich punktów dostępowych, zaplanować ich rozlokowanie oraz wykonać konfigurację i uruchomienie sieci. Niniejsze opracowanie miało na celu przybliżenie zagadnień związanych ze standardem IEEE 802.11, co w efekcie powinno ułatwić proces tworzenia sieci bezprzewodowych oraz rozwiązywania napotkanych problemów.

Literatura

1. Ashton Kevin, That 'Internet of Things' Thing, http://www.rfidjournal.com/articles/view?4986
2. http://en.wikipedia.org/wiki/Aircrack-ng
3. http://en.wikipedia.org/wiki/Carrier_sense_multiple_access_with_collision_detection
4. http://en.wikipedia.org/wiki/IEEE_802.11
5. http://en.wikipedia.org/wiki/IEEE_802.11i-2004
6. http://en.wikipedia.org/wiki/Wired_Equivalent_Privacy
7. http://eprint.iacr.org/2007/120.pdf
8. http://ioeassessment.cisco.com/learn
9. http://pl.wikipedia.org/wiki/Advanced_Encryption_Standard#cite_note-Rijndael-ammended.pdf-2
10. http://sekurak.pl/bezpieczenstwo-sieci-wi-fi-czesc-4-standard-802-11i-czyli-wpa-i-wpa2/
11. http://supportforums.cisco.com/document/52391/80211-frames-starter-guide-learn-wireless-sniffer-traces
12. http://www.acrylicwifi.com
13. http://www.bluetooth.org/en-us
14. http://www.ekahau.com/products/ekahau-site-survey
15. http://www.fortinet.com/products/wlan-switching/wireless-lan/forti-planner.html
16. http://www.ietf.org/rfc/rfc2284.txt,

17. http://www.ietf.org/rfc/rfc3748.txt
18. http://www.matthafner.com/wifianalyzer
19. http://www.merunetworks.com
20. http://www.metageek.com
21. http://www.metageek.com/products/wi-spy
22. http://www.wildpackets.com/resources/compendium/wireless_lan/wlan_packets#wp1000868
23. http://www.wi-fi.org
24. Piwiński M., Automatyczna konfiguracja interfejsu sieciowego, czyli protokół DHCP w praktyce, Uczyć się będąc połączonym, 235-247, Teksty wystąpień, red. M. Sysło, A. B. Kwiatkowska, X Konferencja "Informatyka w Edukacji" 2013, Wydawnictwa Naukowe UMK, ISBN 978-83-231-3105-2, Toruń, 2013, http://repozytorium.umk.pl/handle/item/1729
25. Piwiński. M, Internet - wybrane aspekty bezpieczeństwa, Informatyka w Edukacji, Monografia naukowa, red. A.B. Kwiatkowska, Wydawnictwa Naukowe UMK, 2013, http://repozytorium.umk.pl/handle/item/1712
26. Piwiński M., Praktyczna analiza sieci komputerowych z wykorzystaniem programu Wireshark, „Informatyka w Edukacji, V", A.B. Kwiatkowska, M. Sysło, (2008) 277 285, http://repozytorium.umk.pl/handle/item/1686
27. Piwiński M., Sieci komputerowe, konfiguracja i bezpieczeństwo, Informatyka w Edukacji, Nauczyciel przewodnik i twórca, Monografia naukowa, red. A.B. Kwiatkowska, M.M. Sysło, Wydawnictwo Naukowe UMK, ISBN 978-83-231-3411-4, Toruń, 85-99, (2015) https://repozytorium.umk.pl/handle/item/2759
28. Piwiński M., „Uczniowie i komputery w sieci...", „Komputer w Szkole", nr 5, (2003), s 38, https://repozytorium.umk.pl/handle/item/1667
29. Piwiński M., Marczak G., Sieci bezprzewodowe wykorzystujące technologie wirtualnej komórki i wirtualnego portu na przykładzie Meru Networks, Informatyka w Edukacji, Informatyka dla wszystkich od najmłodszych lat, A.B. Kwiatkowska, M. Sysło, (2014) 978-83-231-3251-6 https://repozytorium.umk.pl/handle/item/2101