Politechnika Białostocka

Wydział Elektryczny

Katedra Telekomunikacji i Aparatury Elektronicznej

Kierunek: Inżynieria biomedyczna

Instrukcja do zajęć laboratoryjnych

Temat ćwiczenia:

Konfiguracja i badanie sieci WLAN w technologii Wi-Fi

Numer ćwiczenia: 1

Laboratorium z przedmiotu: **Telematyka medyczna**

Kod przedmiotu: MKIB2S01005M

Instrukcję opracowali:

dr inż. Andrzej Zankiewicz
dr inż. Andrzej Holiczer

Białystok 2015

1. Ogólna charakterystyka ćwiczenia

Lokalne sieci bezprzewodowe (WLAN – *Wireles LAN*) zyskują obecnie bardzo dużą popularność m.in. ze względu na łatwość zestawienia połączenia (nie ma potrzeby układania kabli) oraz powszechną dostępność i stosunkowo niskie ceny odpowiedniego wyposażenia. Sieci te budowane są przede wszystkich na podstawie standardów rodziny IEEE 802.11 określanych komercyjną nazwą Wi-Fi. Do najczęściej spotykanych standardów tej serii należą:

- 802.11b (szybkość transmisji do 11Mb/s, pasmo 2,4GHz),
- 802.11g (szybkość transmisji do 54Mb/s, pasmo 2,4GHz),
- 802.11a (szybkość transmisji do 54Mb/s, pasmo 5GHz),
- 802.11n (szybkość transmisji do 600Mb/s (w praktyce do 450Mb/s), pasma 2,4GHz oraz 5GHz),
- 802.11ac (szybkość transmisji do 6,9GB/s (obecnie praktycznie do ok. 1Gb/s, pasmo 5GHz).

Celem ćwiczenia jest zapoznanie z praktycznymi zasadami zestawiania i konfiguracji sieci WLAN 802.11 oraz praktycznymi możliwościami obserwacji i analizy ruchu w sieciach Wi-Fi.

2. Przygotowanie do zajęć

Przed przystąpieniem do wykonywania ćwiczenia należy zapoznać się z następującymi materiałami:

- całość niniejszej instrukcji.
- podstawowe informacje o sieciach bezprzewodowych standardu 802.11.

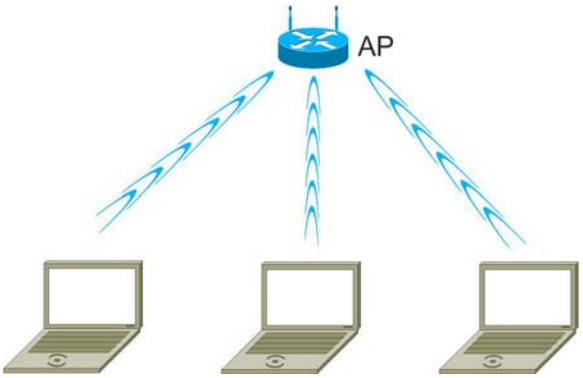
Informacje zawarte w podanych powyżej źródłach stanowią minimum wiedzy teoretycznej **niezbędnej** do przystąpienia i prawidłowego wykonania ćwiczenia.

3. Podstawowe informacje o sieciach Wi-Fi

Logiczna architektura sieci Wi-Fi

Sieci Wi-Fi mogą pracować w dwóch podstawowych trybach: Ad-Hoc oraz infrastrukturalnym. W trybie Ad-Hoc (formalnie określanym jako IBSS – *Independent Basic Service Set*) stacje sieciowe wyposażone w interfejsy radiowe Wi-Fi komunikują się bezpośrednio ze sobą. W trybie infrastrukturalnym (BSS – Basic Service Set) stacje sieciowe nawiązują połączenie poprzez osobne urządzenie określane jako punkt dostępowy (AP – *Access Point*). Punkt dostępowy pełni rolę koncentratora połączeń radiowych, zapewnia komunikację pomiędzy poszczególnymi stacjami przyłączonymi radiowo oraz zazwyczaj pozwala też na połączenie sieci radiowej z siecią przewodową (najczęściej w standardzie Ethernet). Rozszerzeniem trybu infrastrukturalnego jest tryb ESS (*Extended Service Set*), w którym sieć zawiera wiele punktów dostępowych komunikujących się poprzez sieć dystrybucyjną (DS – *Distribution System*), która w

szczególności też może być bezprzewodowa (WDS – *Wireless Distribution System*). Na rysunku 1 przedstawiono strukturę sieci Wi-Fi w trybie BSS wykorzystywanym w ćwiczeniu.



Rys. 1. Połączenia w sieci Wi-Fi w trybie BSS.

Ramki w sieciach Wi-Fi

Technologia Wi-Fi obejmuje dwie pierwsze warstwy modelu OSI, czyli warstwę fizyczną oraz warstwę łącza danych. Warstwa fizyczna odpowiedzialna jest za utworzenie sygnału transmitowanego w medium i jest różna w poszczególnych standardach rodziny IEEE 802.11. Warstwa łącza danych zapewnia logiczną obsługę transmisji i definiuje m.in. format ramki wspólny dla wszystkich wariantów warstwy fizycznej. W sieciach Wi-Fi używane są trzy typy ramek: zarządzające, kontrolne oraz z danymi. Ramki zarządzające są wykorzystywane w procesie przyłączania stacji do sieci (operacje uwierzytelnienia i skojarzenia stacji) oraz do ogłaszania i uzyskiwania informacji o sieci. Ramki kontrolne używane są m.in. w procedurach zarządzania dostępem stacji do medium transmisyjnego oraz do potwierdzania odbieranych ramek. Ramki danych służą przede wszystkim do przesyłu informacji użytkownika, ale jednocześnie mogą zawierać też dane związane z kontrolą dostępu do nośnika (funkcja PCF). Każdy z trzech typów ramki zawiera wiele podtypów służących do przesyłania danych związanych w realizacją określonych funkcji. Przykładowo istnieje 11 podtypów ramek zarządzających służących np. do rozgłaszania informacji o sieci (ramka *Beacon*), żądania skojarzenia stacji, żądania likwidacji wykonanego skojarzenia itd. Jako przykład, na rysunku 2 przedstawiono format ramki z danymi (typ ramki: dane, podtyp: dane).

Kontrola ramki	Czas trwania	Adres docelowy	BSSID	Adres źródłowy	Kontrola sekwencji	Dane	Suma kontrolna
2B	2B	6B	6B	6B	2B	0 - 2312B	4B

Rys. 2. Struktura ramki danych stosowanej w sieciach Wi-Fi.

Pole „Kontrola ramki” (*Frame Control*, 2 bajty) jest wspólne dla wszystkich typów ramek i zawiera informacje m.in. o typie i podtypie ramki, czy ramka pochodzi lub jest przeznaczona dla systemu dystrybucyjnego oraz czy została zaszyfrowana za pomocą algorytmu WEP. Pole „Czas trwania” (*Duration*, 2 bajty) zawiera informację

o czasie wymiany ramek (wysłania danych i odebrania potwierdzenia) używaną przez algorytm kontroli dostępu do medium. Adresy docelowy i źródłowy są to 6 bajtowe adresy fizyczne (MAC) stacji odbierającej i wysyłającej ramkę. BSSID jest to adres MAC punktu dostępu (tryb BSS) lub wartość losowa wygenerowana przy tworzeniu sieci Ad-Hoc (tryb IBSS). Pole kontrola sekwencji (*Sequence control*, 2 bajty) jest wykorzystywane w procesie fragmentacji ramek (podziału większej ramki na kilka mniejszych w celu zwiększenia niezawodności przesyłu przez niepewny lub mocno obciążony nośnik) i zawiera numer fragmentu ramki. Suma kontrolna (FCS – *Frame Check Sequence*) ramki zawiera 32-bitową sumę kontrolną wyznaczoną algorytmem CRC-32.

Zagadnienia bezpieczeństwa w sieciach Wi-Fi

W sieciach Wi-Fi, podobnie jak w innych technologiach radiowych, fizyczna kontrola dostępu do nośnika transmisyjnego praktycznie nie jest możliwa. Każdy znajdując się w zasięgu działania sieci może rejestrować przesyłany w tej sieci sygnał radiowy w sposób praktycznie niewidoczny. Dlatego w takich sieciach szczególnie istotne są zagadnienia bezpieczeństwa obejmujące ochronę przesyłanych danych przed nieupoważnionym dostępem oraz kontrolę dostępu do sieci.

Już w pierwszej wersji standardu 802.11 został uwzględniony mechanizm WEP (*Wire Equivalent Privacy*) realizujący szyfrowanie przesyłanych danych oraz uwierzytelnienie użytkowników. Obie te operacje bazują na wspólnym kluczu skonfigurowanym we wszystkich urządzeniach (stacje użytkowników, punkty dostępowe). Wraz w biegiem czasu odkrywane były kolejne słabości mechanizmu WEP, a w 2004 roku zostały zaprezentowane metody ataków KoreKa oraz Arbaugha pozwalające na wyznaczenie klucza WEP w ciągu kilku-kilkunastu minut na podstawie zarejestrowanych poniżej 500 000 ramek (w rzeczywistości w tym przypadku wystarczą fragmenty ramek zawierające tzw. wektory inicjujące IV). Po opublikowaniu tych metod mechanizm WEP stał się zupełnie nieskuteczny i pomimo iż jest on ze względów formalnych implementowany nawet w najnowszych urządzeniach, nie powinien być już wykorzystywany do zabezpieczania sieci Wi-Fi.

W czerwcu 2004r. został zatwierdzony standard IEEE 802.11i stanowiący kompleksowy system zabezpieczenia sieci Wi-Fi obejmujący uwierzytelnianie, integralność oraz poufność danych. Szerzej jest on znany pod handlową nazwą WPA (*Wi-Fi Protected Access*) wykreowaną przez Wi-Fi Alliance. Od strony technicznej 802.11i zawiera dwa mechanizmy zabezpieczeń: TKIP oraz CCMP. TKIP (*Temporal Key Integrity Protocol*) stanowi modyfikację protokołu WEP (zachowany został ten sam generator szyfru RC4) głównie poprzez wprowadzenie generacji indywidualnego klucza szyfrującego dla każdej wysyłanej ramki. Z kolei CCMP (*Counter-mode/CBC MAC Protocol*) jest już zupełnie inną metodą, bazująca na algorytmie szyfrującym AES. Mechanizm CCMP określany jest w wielu przypadkach jako WPA2.

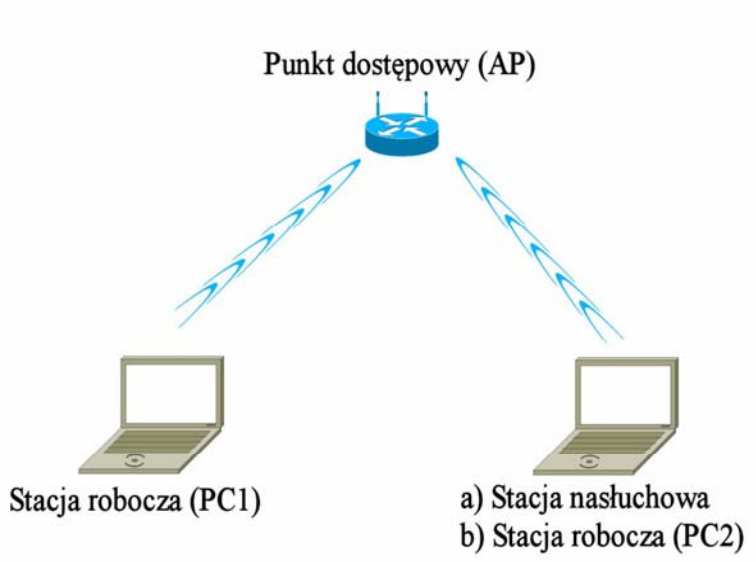
Standard IEEE 802.11i umożliwia wzajemne uwierzytelnienie użytkowników i sieci za pomocą serwera zawierającego bazę użytkowników (w praktyce jest to system uwierzytelniania na porcie 802.1x oraz serwer uwierzytelniający RADIUS). Dla mniej wymagających zastosowań zdefiniowano też wersje WPA ze współdzielonym

kluczem (*preshared key*), nie wymagające serwera Radius (oznaczane są one jako WPA-PSK lub WPA Personal).

Wewnętrzne działanie zabezpieczeń sieci Wi-Fi w rzeczywistości jest dość złożone, zwłaszcza w metodach WPA/WPA2. Od strony praktycznej należy brać pod uwagę, że metoda WEP nie zapewnia aktualnie praktyczne żadnej ochrony i nie powinna być stosowana, pomimo iż jest ona implementowana nawet w najnowszych urządzeniach. Obecnie system WPA/WPA2 uznawany jest za bardzo skuteczne zabezpieczenie, jednak w przypadku wersji z kluczem współdzielonym (PSK) istnieje możliwość wyszukiwania wspólnego klucza poza systemem (*off-line*) na podstawie zarejestrowanych informacji znajdujących się w dwóch pierwszych ramkach wymienianych przy podłączaniu użytkownika do sieci. Ponieważ przeszukiwanie to może odbywać się z wykorzystaniem bardzo szybkich maszyn równoległych (w Internecie można znaleźć oferty wyszukiwania klucza WPA-PSK na maszynach z kilkuset procesorami za stosunkowo niewielką opłatą) stosowane klucze PSK powinny stanowić losowe ciągi zawierające co najmniej 20 znaków (w tym znaki specjalne).

4. Opis stanowiska laboratoryjnego

Stanowisko laboratoryjne służące do badania sieci składa się z trzech urządzeń: dwóch komputerów klasy PC oraz routera z wbudowanym punktem dostępowym sieci Wi-Fi. Stacja PC1 zawsze pracuje jako stacja robocza i służy do generowania ruchu sieciowego z punktem dostępowym. Stacja PC2 natomiast będzie zmieniała swoje funkcje w trakcie wykonywania ćwiczenia. W pierwszej części nie będzie połączona z żadną siecią bezprzewodową i będzie jedynie nasłuchiwać i przechwytywać ramki (Rys. 3a). W dalszej części będzie pracowała jako stacja robocza, a dokładniej mówiąc jako klient usługi FTP służącej do wyznaczania rzeczywistej prędkości transmisji danych pomiędzy PC1 i PC2 (Rys. 3b).



Rys. 3. Urządzenia wykorzystywane w ćwiczeniu.

Punkt dostępowy (AP) po przywróceniu ustawień fabrycznych może być skonfigurowany za pośrednictwem przeglądarki internetowej. Adres IP oraz domyślny login i hasło znajdują się na obudowie routera. Konfiguracji routera dokonujemy za pośrednictwem stacji PC1 po udanym połączeniu się z siecią rozgłaszaną przez router w trybie domyślnym.

W programie WireShark istnieje możliwość tworzenia filtrów ramek, tak aby odczytywane były jedynie te nas interesujące. Oprócz standardowych filtrów dotyczących protokołu TCP/IP można również stosować filtry do niższych warstw modelu OSI w tym do warstwy łącza danych standardu 802.11a/b/g/n. Poniżej przedstawiono kilka przykładowych wyrażeń (ich składnia jest zbliżona do języka C), które mogą okazać się przydatne podczas realizacji ćwiczenia:

- wyświetlanie całego ruchu, poza ramkami *beacon*: **`!wlan.fc.subtype==8`**,
- wyświetlanie jedynie ramek z danymi: **`wlan.fc.subtype==2,`**
- określenie adresu źródłowego lub docelowego: **`wlan.addr`**,
- określenie adresu nadajnika: **`wlan.ta`**,
- określenie adresu źródłowego: **`wlan.sa`**,
- określenie adresu odbiornika: **`wlan.ra`**,
- określenie adresu docelowego: **`wlan.da`**,
- określenie nazwy sieci: **`wlan.bssid`**.

5. Plan wykonywania ćwiczenia laboratoryjnego

1. Posługując się oprogramowaniem analizatora sieci określić jakie sieci bezprzewodowe Wi-Fi widoczne są pomieszczeniu laboratorium. Dla każdej z nich określić kanał częstotliwościowy na której pracuje, identyfikator SSID, poziom sygnału oraz rodzaj zabezpieczenia.
2. Skonfigurować punkt dostępowy AP (*Access Point*) do pracy na wybranym kanale częstotliwościowym z identyfikatorem SSID „Lab3”.
3. Przyłączyć stację PC1 do sieci bezprzewodowej „Lab3”. Sprawdzić konfigurację sieci z interfejsem bezprzewodowym (*ipconfig /all)*. Zapisać adresy IP oraz MAC stacji roboczej PC1 oraz adres bramy domyślnej (tylko adres IP). Za pomocą polecenia *ping* sprawdzić stan połączenia z bramą domyślną.
4. Korzystając ze stacji PC2 i posługując się oprogramowaniem analizatora sieci określić strukturę ramek nawigacyjnych (*beacon*) wysyłanych przez punkt dostępowy.
5. W linii poleceń stacji PC1 wykonać ponownie test połączenia PC1 <–> AP za pomocą komendy *ping* z dodatkowymi parametrami *–t –l 100*. Na stacji PC2 powtórzyć pkt. 4 z tą różnicą, że odfiltrować jedynie protokół ICMP (w polu filtra wystarczy wpisać *icmp*). Zaobserwować, czy dane przesyłane pomiędzy PC1, a AP mogą zostać odczytane przez stację nasłuchową (PC2).
6. Włączyć w punkcie dostępowym szyfrowanie transmisji zgodnie ze standardem WEP. Jako hasło ustawić 1234567890. Ponownie wykonać punkt 5. W programie WireShark ustawić filtr tak, aby były widoczne jedynie ramki wysyłane przez stację PC1. W tym celu należy w polu filtra wpisać polecenie: *wlan.sa == <adres MAC PC1>*. Adres MAC stacji PC1 wpisujemy zgodnie z pkt. 3.

7. Skomentować różnice pomiędzy zawartościami ramek odczytanymi w pkt 6 i 5.
8. Za pomocą programu klienta FTP zainstalowanego na stacji PC2 połączyć się z serwerem FTP działającym na stacji PC1 i sprawdzić szybkość pobierania pliku o rozmiarze 500MB dla następujących trybów pracy sieci bezprzewodowej: 802.11b, 802.11g oraz 802.11n. Zmian należy dokonywać poprzez stronę konfiguracyjną routera za pośrednictwem stacji PC1. Skomentować ewentualne różnice pomiędzy rzeczywistą prędkością transmisji, a wynegocjowaną przez kartę sieciową. Wynegocjowana prędkość transmisji karty bezprzewodowej należy sprawdzić w: Panel sterowania -> Sieć i Internet -> Połączenia sieciowe wybierając stan połączenia karty bezprzewodowej.

W sprawozdaniu należy zamieścić wyniki uzyskane przy wykonywaniu poszczególnych części ćwiczenia.

5. Literatura

1. Roshan P., Leary J.: *Bezprzewodowe sieci LAN 802.11. Podstawy*. Wydawnictwo PWN-MIKOM, Warszawa, 2006.
2. Balinsky A., Miller D., Sankar K., SundaralingamS.: *Bezpieczeństwo sieci bezprzewodowych. Ochrona sieci 802.11. Porady eksperta*. Wydawnictwo PWN-MIKOM, Warszawa, 2005.
3. http://standards.ieee.org/about/get/802/802.11.html