Konfigurowanie sieci bezprzewodowej w trybie ad hoc

1 Wprowadzenie

Wymagania wstępne: wykonanie ćwiczeń "Adresacja IP".

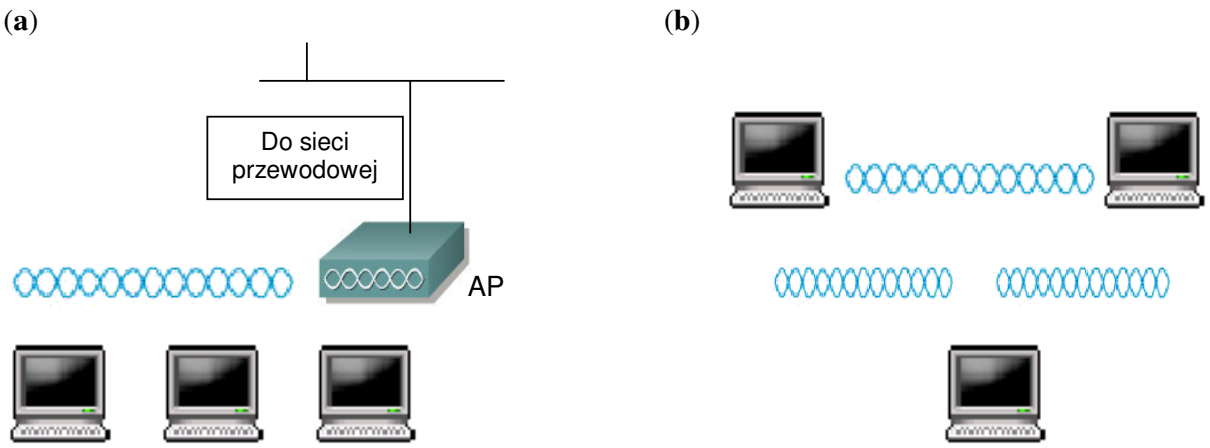
Bezprzewodowe sieci komputerowe stają się obecnie coraz popularniejsze, zarówno w zastosowaniach sieci lokalnych jak i do połączeń w sieciach MAN. Technologie te pozwalają na realizację sieci w różnych konfiguracjach – z wykorzystaniem punktów dostępowych, w architekturze ad hoc, czy też do połączeń mostowych – takie możliwości wpływają na wzrost ich znaczenia w praktycznych zastosowaniach. Sieci bezprzewodowe obecnie najczęściej realizowane są w oparciu o standardy 802.11; zestaw standardów IEEE dla sieci bezprzewodowych obejmuje m.in.:

- 802.11 – oryginalny standard obecnie oznaczany 802.11y, opublikowany w 1997 roku i wprowadzający dwie prędkości dla transmisji bezprzewodowej: 1 i 2 Mbps;
- 802.11b – obecnie najpopularniejszy standard sieci bezprzewodowych gwarantujący prędkość transmisji do 11 Mbps (jednak w praktyce sprawność protokołów obniża prędkość transmisji do około 5,5 Mbps); wykorzystuje pasmo 2,4 GHz podzielone na 14 kanałów – w Polsce wykorzystuje się ich jedynie 13 w paśmie od 2400,0 do 2483,5;
- 802.11a – prędkość transmisji do 54 Mbps w paśmie 5 GHz; pasmo dzielone jest na 12 kanałów: 8 do transmisji wewnątrz budynków i 4 do komunikacji pomiędzy budynkami (ang. *point-to-point*);
- 802.11g – standard wykorzystujący to samo pasmo co 802.11b (i zgodny z tym standardem) ale pozwalający na transmisję z prędkością do 54 Mbps;
- 802.11n – opracowywany od 2004 roku standard dotyczący rozległych sieci bezprzewodowych;
- 802.11c – dotyczy protokołów mostów (ang. *bridge*) bezprzewodowych.

W skład radiowej sieci komputerowej wchodzą bezprzewodowe stacje klienckie (STA – ang. *STAtion*) oraz punkty dostępowe (AP – ang. *Access Point*). Sieć składającą się z co najmniej dwóch takich urządzeń określa się jako BSS (ang. *Basic Service Set*); natomiast połączone ze sobą sieci BSS nazywa się ESS (ang *Extended Service Set*). Wszystkie urządzenia działające w ramach BSS muszą posiadać identyczną wartość identyfikatora SSID (ang. *Service Set Identifier*) – najczęściej jest to nazwa określająca przeznaczenie lub właściciela sieci – oraz muszą pracować na tym samym kanale radiowym

Istnieją dwa tryby pracy sieci bezprzewodowych (rysunek nr 1):

- tryb **ad hoc** – (nazywany także *peer-to-peer*) w tym wypadku wszystkie urządzenia sieci komunikują się ze sobą bezpośrednio (jeśli pozwala na to zasięg radiowy) – nie wykorzystuje się punktów dostępowych;
- tryb **infrastruktury** – (lub też tryb stacjonarny) wykorzystuje punkty dostępowe (AP); wszystkie urządzenia komunikują się tyko z AP, który spełnia funkcję bramy (do sieci przewodowej) i pośredniczy w komunikacji pomiędzy urządzeniami sieci bezprzewodowej (STA).



Rysunek nr 1. Dwa tryby pracy sieci bezprzewodowej: (a) tryb infrastruktury, (b) tryb ad hoc.

1.1 Typy ramek i ich funkcje w sieciach 802.11x

Wyróżnia się trzy typy ramek: (i) **ramki zarządzające** (pozwalające na nawiązanie połączenia i zarządzanie komunikacją): *beacon*, *probe request*, *probe response*, *authentication request*, *authentication respose*, *deauthentication request*, *association request*, *associacion response*, *disassociacion request*; (ii) **ramki kontrolne** (wspomagające przekazywanie danych): *RTS*, *CTS*, *ACK*; (iii) **ramki danych**. Ramki zawierają m.in. następujące informacje: typ ramki, status szyfrowania, adresy MAC, nr kolejny ramki, przesyłane dane oraz suma kontrolna.

Główne funkcje jakie realizuje warstwa MAC to: skanowanie, uwierzytelnianie, przyłączanie oraz szyfrowanie.

- **Skanowanie** – polega na wyszukaniu przez stację dostępnych sieci bezprzewodowych (sieci będących w zasięgu radiowym). Wyróżnia się dwa rodzaje skanowania pasywne i aktywne. Skanowanie pasywne polega na przeglądaniu przez stację wszystkich kanałów w poszukiwaniu wysyłanych okresowo ramek zarządzających typu *beacon* – odebranie takiej ramki pozwala na ustalenie identyfikatora SSID, kanału pracy, obsługiwanych prędkości oraz poziomu sygnału radiowego dostępnej sieci bezprzewodowej. Skanowanie aktywne polega na wysłaniu przez stację ramki rozgłoszeniowej typu *probe request*; odpowiedzią na takie żądanie jest ramka *probe response* – nie ma wówczas konieczności oczekiwania na pojawienie się ramki typu *beacon*.
- **Uwierzytelnianie** – istnieją dwie metody dokonania weryfikacji tożsamości stacji: uwierzytelnianie otwarte (ang. *open*) i z kluczem dzielonym (ang. *restricted*). W przypadku systemu otwartego stacja ubiegająca się o uwierzytelnienie wysyła ramkę zarządzającą typu *authentication request*, na którą wysyłana jest odpowiedź typu *authentication response*, z informacją o przyznaniu dostępu lub o odmowie dostępu. W przypadku uwierzytelniania w oparciu o klucz dzielony, wszystkie węzły sieci bezprzewodowej posiadają wspólny klucz szyfrowania WEP (ang. *Wired Equivalent Privacy*). Schemat postępowania jest następujący: (i) stacja wysyła ramkę *authentication request*; (ii) węzeł uwierzytelniający (np. AP) w odpowiedzi wysyła ramkę *authentication response* z testowym ciągiem znaków; (iii) stacja szyfruje odebrany ciąg znaków z wykorzystaniem algorytmu WEP oraz klucza i odsyła zakodowany ciąg kolejną ramką; (iv) po odebraniu tej ramki węzeł uwierzytelniający szyfruje ciąg testowy własnym kluczem i porównuje oba zaszyfrowane ciągi – jeśli ciągi się zgadzają następuje odpowiedź (*authentication response*), a w przeciwnym razie wysyłana jest odpowiedź *deauthentication resquest* ■.
- **Przyłączanie** – następuje po fazie uwierzytelniania i wymaga wysłania ramki *association*

request ze wskazanie identyfikatora SSID. W celu obsługi połączenia tworzony jest tzw. identyfikator połączenia (ang. *association ID*), dostarczany wraz z ramką *association response*.

- **Szyfrowanie** – wykonywane jest z wykorzystaniem algorytmu WEP. Szyfrowanie ramki danych *DF* składa się z następujących etapów: (i) na koniec ramki dodawana jest suma kontrolna *ICV* (ang. *Integrity Check Value*) jawnej zawartości ramki wyznaczona przy pomocy algorytmu **CRC-32**; uzyskujemy: *DF=DF.ICV(DF)*; (ii) generator liczb pseudolosowych wyznacza 24-bitowy tzw. wektor inicjalizacyjny *IV* (ang. *Initialization Vector*); (iii) do wektora *IV* dołączany jest klucz szyfrowania *K*; uzyskujemy: *IV.K*; (iv) wektor *IV.K* jest szyfrowany algorytmem strumieniowym **RC4**; uzyskujemy pseudolosową sekwencję *RC4(IV.K)*; (v) wykonywana jest funkcja logiczna XOR na zaszyfrowanym wektorze *RC4(IV.K)* i jawnej ramce *DF*; uzyskujemy zaszyfrowaną ramkę *CDF=(DF.ICV(DF) XOR (RC4(IV.K))*; (vi) wektor *IV* jest dodawany na początku zaszyfrowanej ramki *CDF* w postaci jawnej; ostatecznie uzyskujemy ramkę: *IV.CDF* ■.

1.2 Tryb ad hoc

Większość operacji i ramek standardów 802.11x jest wspólna dla trybów infrastruktury i ad hoc; praca w trybie ad hoc nie wymaga modyfikacji działań w warstwie fizycznej. Natomiast wymagane są pewne modyfikacje w warstwie MAC. Pierwszy uruchomiony węzeł sieci BSS – tutaj nazywanej IBSS (ang. *Independent Basic Service Set)* – rozpoczyna od nadawania ramek typu *beacon*, wymaganych do odpowiedniej synchronizacji pozostałych stacji (w trybie infrastruktury tylko AP rozsyła tego typu ramki). Pozostałe stacje mogą dołączyć do IBSS po odebraniu ramki *beacon*. Każda stacja sieci jest zobowiązana do nadawania okresowo własnych ramek typu *beacon*, jeśli taka ramka nie zostanie odebrana po określonym czasie. Czas oczekiwania na kolejną ramkę *beacon* jest (dla każdego węzła) losowy – ma to na celu zminimalizowanie ilości ramek tego typu transmitowanych w sieci.

2 Organizacja, wymagany sprzęt, oprogramowanie

- Zadanie wykonywane jest przez parę studentów;
- sprzęt: 2 komputery z bezprzewodowymi kartami sieciowymi (802.11b);
- oprogramowanie: pakiet **`wireless`**, **Cisco Aironet Client Utilities** (**ACU**).

3 Zadania

- Przy pomocy programu **`iwlist`** należy sprawdzić: dostępne sieci bezprzewodowe, kanały, prędkości transmisji, klucze szyfrowania oraz AP.
- Wykorzystując dwa komputery należy skonfigurować bezprzewodową sieć w trybie ad hoc – stosując polecenia **`iwconfig`** oraz **`ifconfig`**.
- Należy wprowadzić do skonfigurowanej sieci szyfrowanie WEP (powtórzyć ćwiczenie z kluczami o różnej długości i wprowadzanych w różnej formie – jako znaki ASCI lub przy pomocy kodów szesnastkowych).
- Wyświetlić statystyki narzędziem **`iwspy`**.
- Powtórzyć powyższe ćwiczenia z wykorzystaniem programu **Cisco Aironet Client Utilities**; sprawdzić jakość połączenia przy pomocy **Site Survey** oraz **Link Status Meter**.

4 Pytania sprawdzające

1. Jakie są wady szyfrowania WEP? -- czy możliwe jest złamanie tego zabezpieczenia?

2. Czy w sieciach ad hoc można stosować tradycyjny routing?
3. Jakie są wady i zalety bezprzewodowych sieci w architekturze ad hoc?
4. Na czym polega problem ukrytej stacji i jak jest on rozwiązywany przy pomocy protokołu RTS/CTS?

5 Literatura

1. Podręcznik systemowy **`man`**: polecenia **`iwconfig`**, **`iwspy`**, **`iwlist`**.
2. "Understanding Ad Hoc Mode", Jim Geier, http://www.wi-fiplanet.com/tutorials/article.php/10724_1451421_1 .
3. "802.11 Wireless LAN Fundamentals", Pejman Roshan, Jonathan Leary.