WLAN 2: tryb infrastruktury

Plan

1. Terminologia
2. Kolizje pakietów w sieciach WLAN - CSMA/CA
3. Bezpieczeństwo - WEP/WPA/WPA2

Terminologia

Tryb infrastruktury / tryb ad-hoc

Tryb infrastruktury - (lub też tryb stacjonarny) wykorzystuje punkty dostępowe (AP); wszystkie urządzenia komunikują się tylko z AP, który spełnia funkcję bramy (do sieci przewodowej) i pośredniczy w komunikacji pomiędzy urządzeniami sieci bezprzewodowej (STA).

Ad-hoc - sieć bez AP, IBSS (independent BSS)

BSS, ESS, SSID

- BSS - Basic Service Set (AP + STAs)
- ESS - Extended Service Set - zbiór wielu BSS z tym samym SSID połączonych siecią dystrybucji (DS, distribution system)
- (E)SSID - Service Set identifier - słowna nazwa sieci

BSSID

- Basic Service Set Identifier
- Służy do rozróżnienia sieci o tym samym SSID
- W ad-hoc liczba bez specjalnego znaczenia (zwykle MAC jednego z pierwszych uczestników)
- W trybie infrastruktury adres MAC AP

Kolizje pakietów

Kolizje pakietów - przypomnienie dla Ethernet

CSMA/CD - carrier sense multiple access with collision **detection**

- Carrier sense
  - przed wysłaniem sprawdzamy czy nośna jest wolna
- Multiple access
  - wiele urządzeń korzysta z tego samego medium
- Detection
  - podczas wysyłania, karta sieciowa sprawdza czy napięcie na medium wzrosło do określonej wartości (kolizja)
  - Jeżeli kolizja została wykryta czekamy losowy czas

Dlaczego WLAN wymaga innego rozwiązania

- Z reguły bezprzewodowe karty sieciowe nie są zdolne do jednoczesnego wysyłania i odbierania pakietów.
- Nawet jeśli posiadałyby taką zdolność, sygnał radiowy emitowany podczas transmisji zagłuszyłby transmisje innych węzłów.

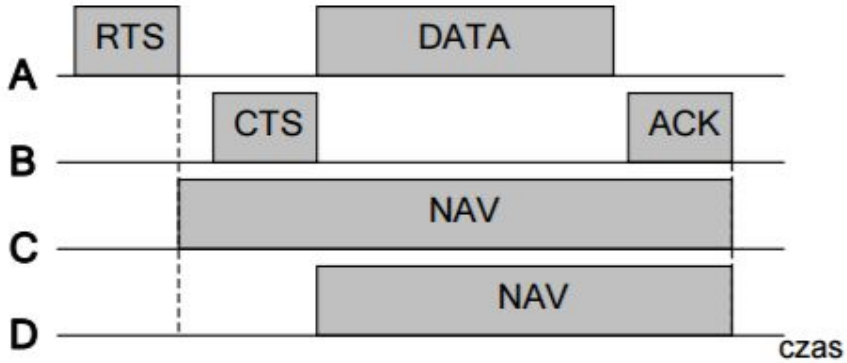
Kolizje pakietów - w sieciach WLAN

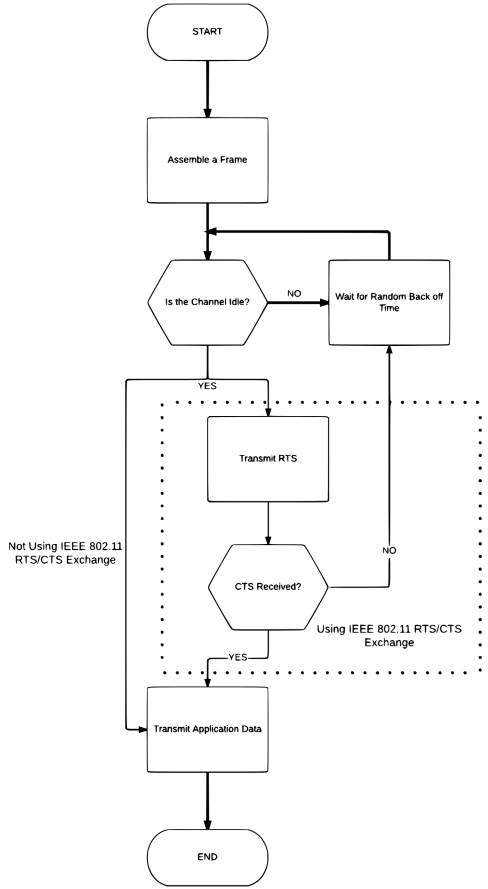
CSMA/CA - carrier sense multiple access with collision **avoidance**

- Carrier sense
  - przed wysłaniem sprawdzamy czy nośna jest wolna
- Multiple access
  - wiele urządzeń korzysta z tego samego medium
- **Avoidance**
  - Przed wysłaniem danych wysyłany jest pakiet “ostrzegawczy”
  - Odebranie pakietu ostrzegawczego jest potwierdzane
  - Odebranie pakietu ostrzegawczego powoduje wstrzymanie wysyłania swoich danych aż do odebrania danych od węzła, który wysłał pakiet ostrzegawczy
  - Jeżeli nadawca nie otrzymał ack od odbiorcy, to spróbuje ponownie po pewnym czasie

CSMA/CA dla 802.11.x

- RTS - request to send
  - nadawca do odbriocy - zazwyczaj AP
- CTS - clear to send
  - Odbiorca do wszystkich w jego zasięgu (którzy mogliby przeszkodzić w transmisji)

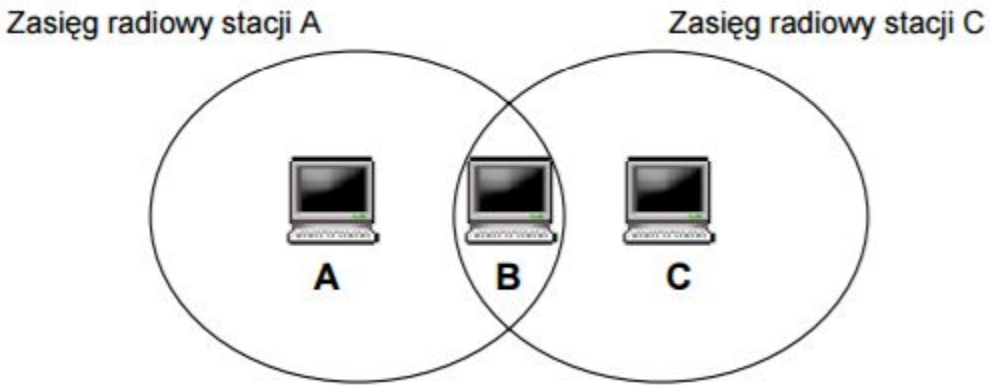




Źródło: https://en.wikipedia.org/wiki/Carrier_sense_multiple_access_with_collision_avoidance#/media/File:Csma_ca.svg

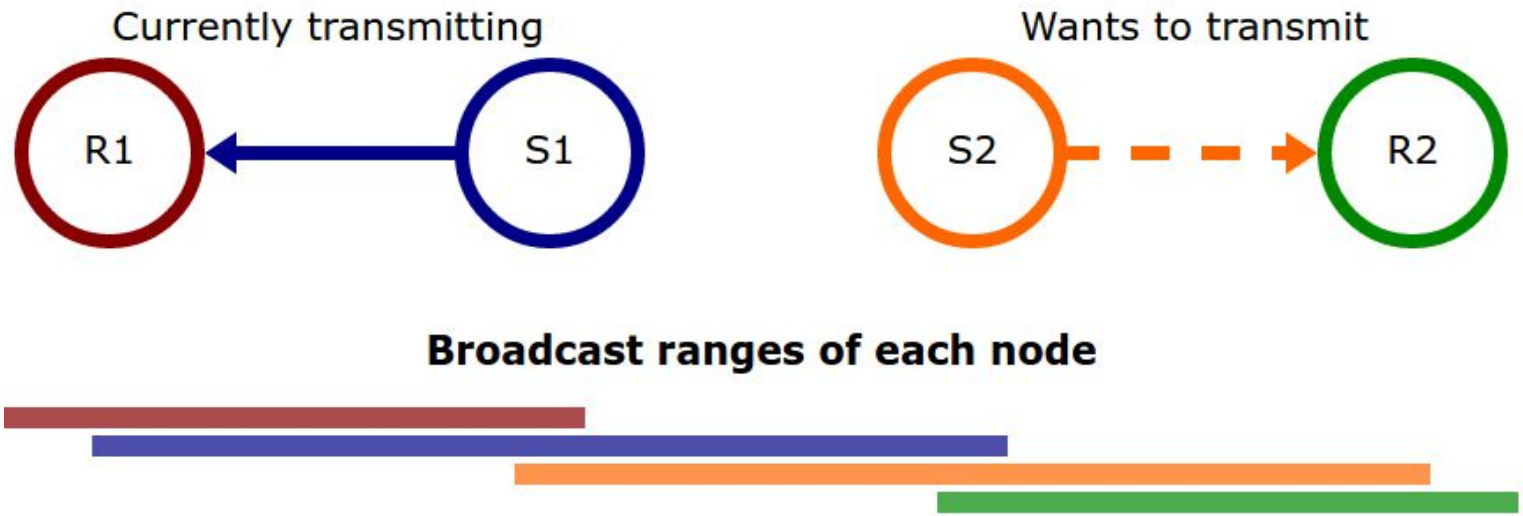
Problem ukrytego węzła (hidden node/station)

Dwie stacje widzą Access Point, ale nie widzą siebie nawzajem



Problem odkrytego węzła (exposed node/station)

S2 błędnie zakłada, że nie powinno transmitować do R2.



https://en.wikipedia.org/wiki/File:Exposed_terminal_problem.svg

Bezpieczeństwo

WEP

- Pre-shared key o stałej długości 40(64) albo 104(128) bitów
- RC4 - strumieniowy algorytm szyfrujący
  - Konkatenacja wektora inicjalizującego (przesyłany jawnie) i klucza
  - Dziurawy
- Dopuszczalne powtórne wykorzystanie tego samego IV
- Brak uwierzytelnienia źródła danych

WPA

- Klucz do 256 bit (w praktyce 128 wystarczy)
- Tymczasowe rozwiązanie kompatybilne ze sprzętem wspierającym WEP
- Głównie TKIP - też RC4, ale:
  - Zamiast konkatenacji - połączenie => brak ścisłego ograniczenia na długość hasła
  - Częsta zmiana klucza
  - + inne ulepszenia
- Opcjonalnie CCMP (AES)
  - Nie RC4 - fundamentalnie różny
  - Do tej pory nie udowodniono słabości

WPA2

- Opcjonalne TKIP (kompatybilność z WPA)
- Głównie CCMP (AES)

WPA uwierzytelnianie

- PSK (personal)
- EAP, EAPOL (enterprise)
  - PSK
  - TLS
  - PEAP, TTLS
- Scentralizowane uwierzytelnianie przez RADIUS

WPA3

- Uniemożliwia znane ataki na WPA2
  - Odkryto już nowe ataki na WPA3
- Silniejsza kryptografia
- Naprawia niektóre wady WPA2
- Nie zezwala na użycie starych metod (np. WEP, TKIP)

Zadania

Zadania

- Skonfigurować sieć bezprzewodową z użyciem mikrotik i co najmniej 2 komputerów z kartą bezprzewodową
- Dodać szyfrowanie WPA (po stronie klientów - wpa_supplicant)
- Skonfigurować port ethernet na mikrotiku i dodać dostęp do internetu
- Filtry MAC