Projekt przejściowy

Temat: Problemy uwierzytelniania i bezpiecznej transmisji danych w sieciach WLAN 802.11.

Opracował : st. plut. pchor. Grzegorz Moranowski

Promotor : por. mgr inż. Mariusz Bednarczyk

1. Wprowadzenie

2. Mechanizmy bezpieczeństwa w IEEE 802.11
   2.1 SSID
   2.2 WEP

3. Uwierzytelnianie i asocjacja w IEEE 802.11
   3.1 Otwarte uwierzytelnianie
   3.2 Uwierzytelnianie za pomocą współdzielonego klucza
   3.3 Uwierzytelnianie na podstawie adresów MAC

4. Analiza mechanizmów bezpieczeństwa w IEEE 802.11
   4.1 Uwierzytelnianie na podstawie adresów MAC
   4.2 Jednokierunkowa autentykacja
   4.3 Słabość klucza WEP
   4.4 Zarządzanie kluczem

5. Uwierzytelnienie na podstawie specyfikacji IEEE 802.1x
   5.1 Uwierzytelnianie na podstawie protokołu EAP
   5.2 Uwierzytelnianie na podstawie protokołu LEAP

6. Wnioski

1. Wprowadzenie

Technologie umożliwiające transmisję danych drogą radiową są już znane od wielu lat. Ta forma przesyłania informacji ma szereg zalet:

- współużytkowanie zasobów sieci przez ograniczoną liczbę osób bez konieczności przemieszczania się wewnątrz pomieszczenia.
- swobodny dostęp do informacji w czasie rzeczywistym w dowolnym miejscu objętym zasięgiem radiowym sieci.
- prostota instalacji bez potrzeby prowadzenia okablowania przez ściany i sufity pomieszczeń, a więc niewielkie koszty instalacyjne.
- skalowalna struktura sieci, konfigurowalna w zależności od zastosowania; zmiana topologii sieci nie wymaga prac instalacyjnych.
- możliwość komunikacji z użytkownikami mobilnymi.
- elastyczność pracy i swoboda ruchu stacji mobilnych w terenie.
- łatwość zwiększania całkowitej przepustowości sieci przez tworzenie wielu komórek na tym samym obszarze.
- niski koszt utrzymania sieci
- wysoka niezawodność pracy sieci WLAN, szczególnie w przypadku istnienia w niej kilku punktów dostępu.
- szybkie wykrywanie nieprawidłowości w sieci.

Niestety mimo niezaprzeczalnych zalet, sieci bezprzewodowe posiadają również pewne wady;

- wrażliwość na zakłócenia elektromagnetyczne.
- wrażliwość na zakłócenia atmosferyczne.
- wrażliwość na celowe zakłócenia transmisji danych.
- niewystarczający poziom transmisji danych.

Mimo, że sieci bezprzewodowe znane są już od wielu lat, to jednak dopiero niedawno, wraz z przyjęciem specyfikacji IEEE 802.11 ustanowione zostały pierwsze standardy dotyczące tego sposobu przesyłania danych.

Standard IEEE 802.11 został zdefiniowany w 1997 roku i obecnie jest jednym z najpopularniejszych standardów transmisji bezprzewodowej. Określa on zasady pracy urządzeń do transmisji bezprzewodowej w sieciach lokalnych.

W standardzie przewidziano możliwość tworzenia dwóch konfiguracji sieci bezprzewodowych:

- ✓ sieć tymczasowa (*ad-hoc*) – nie posiadająca elementów stałych.
- ✓ sieć stacjonarna (*infrastructure*) – zawierająca pewne elementy stałe, w tym połączenie z siecią przewodową.

W warstwie fizycznej przewidziano dwie podwarstwy.

- niezależną od medium PLPC (*Phisical Layer Convergence Protocol*) – zapewniająca realizację mechanizmów typowych dla warstwy fizycznej.

- zależną od mediów PMD (*Phisical Medium Dependit*) – obejmującą zagadnienia takie jak modulacja czy kodowanie.

Przewidziano trzy warianty warstwy fizycznej:

- fale radiowe z rozpraszaniem widma metodą kluczowania bezpośredniego.
- fale radiowe z rozpraszaniem widma metodą przeskoków częstotliwości.
- fale optyczne z zakresu bliskiej podczerwieni.

Dla każdego rodzaju medium standard IEEE 802.11 zakłada prędkości 1 Mb/s oraz 2 Mb/s, przy czym większa szybkość transmisji stosowana jest opcjonalnie podczas przesyłania danych użytkowych; informacje sterujące w tym nagłówek ramek danych, przesyłane są zawsze z prędkością 1 Mb/s.

W przypadku fal radiowych z rozpraszaniem widma metodą kluczowania bezpośredniego przyjęto różnicową modulację fazy ze stałą prędkością 1 Mb/s. Oznacza to, że dla prędkości transmisji 1Mb/s stosowana jest modulacja binarna DBPSK (*Differential Binary Phase Shift Keying*), a dla prędkości 2 Mb/s – kwadraturowa DQPSK (*Differential Quadrature Phase Shift Keying*). Przebieg rozpraszający jest 11 bitowym ciągiem Barkera o prędkości 11 Mb/s. W przydzielonym paśmie 2,4 – 2,4835 GHz określono 13 kanałów częstotliwościowych szerokości 5 MHz.

W przypadku fal radiowych z rozpraszaniem widma metodą przeskoków częstotliwości FHSS (*Frequency Hopping Spread Spektrum*), przyjęto modulację częstotliwości z filtrem Gaussa ze stałą prędkością 1 Mbd. Oznacza to, że dla prędkości transmisji 1 Mb/s stosowana jest modulacja binarna 2-GFSK (*Gaussian Frequency Shift Keying*), a dla prędkości transmisji 2 Mb/s – kwadraturowa 4-GFSK. W przydzielonym paśmie 2,4 – 2,4835 GHz określono 79 kanałów o szerokości 1 MHz i 78 wzorców przeskoków.

W przypadku fal optycznych przyjęto rozproszoną emisję fal. Dla prędkości 1 Mbps stosuje się modulację 16-PPM (*Pulse Position Modulation*), a dla 2 Mb/s – 4-PPM.
Zasięg optyczny wynosi około 10m.

Jako sposób dostępu do medium, zdecydowano się zastosować protokół CSMA/CA (*Carier Sense Multiple Access with Collision Avoidance*), który polega na tym, że po skompletowaniu ramki stacja nadawcza sprawdza stan łącza, jeśli jest ono wolne to stacja rozpoczyna nadawanie, a jeśli zajęte to transmisja jest wstrzymywana do chwili zwolnienia łącza. W celu wykrycia kolizji lub innych błędów transmisji, stacja odbierająca musi wysłać potwierdzenie odebrania ramki. Ramki przekłamane są nadawane ponownie.
Ramka w standardzie IEEE 802.11 stanowi podstawową jednostkę informacji wymienianych pomiędzy stacjami, tym niemniej pełna jednostka protokołu może składać się z ciągu ramek.
Każda ramka zawiera następujące pola:

- nagłówek dopasowujący do wymagań warstwy fizycznej
- typ ramki (type field), określający czy w ramce stosowano kompresję bądź szyfrowanie oraz sposób dostępu do medium
- pole sterujące (control field)
- identyfikator protokolarnej jednostki danych
- adres odbiorcy i ewentualnie nadawcy wraz z identyfikatorem sieci
- elementy sterujące i zależne od typu ramki
- dane podwarstwy LLC
- sumę kontrolną CRC 8- lub 32- bitową, zależnie od typu ramki

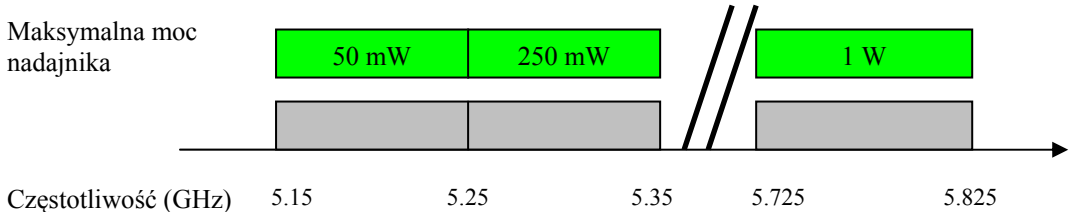
Standard IEEE 802.11 stał się punktem wyjścia do opracowania nowych standardów.
IEEE 802.11 opracowało dwa rozszerzenia standardu: IEEE 802.11a i IEEE 802.11b.
Standard IEEE 802.11b wykorzystując to samo pasmo co IEEE 802.11 zapewnia jednak transmisję danych z szybkością 11 Mbps.

W zależności od szybkości przesyłania danych wykorzystywane są różne rodzaje modulacji.

Prędkość transmisji	Rodzaj modulacji
1	DBPSK (*Differential Binary Phase Shift Keying*)
2	DQPSK (*Differential Quadrature Phase Shift Keying*)
5,5	BPSK (*Binary Phase Shift Keying*)
11	QPSK (*Quadrature Phase Shift Keying*)

Rys.1. Prędkości transmisji dla IEEE 802.11b

Drugim standardem bazującym na IEEE 802.11 jest IEEE 802.11a, w odróżnieniu od IEEE 802.11b definiuje on mechanizmy bezprzewodowej transmisji danych w paśmie 5 GHz, maksymalną prędkością 54 Mbps. Standard ten definiuje trzy podpasma:
- pierwsze od 5,15 – 5,25 GHz z maksymalną mocą nadajnika 50 mW
- drugie od 5,25 – 5,35 GHz z maksymalną mocą nadajnika 250 mW
- trzecie od 5,725 – 5,825 z maksymalną mocą nadajnika 1 W

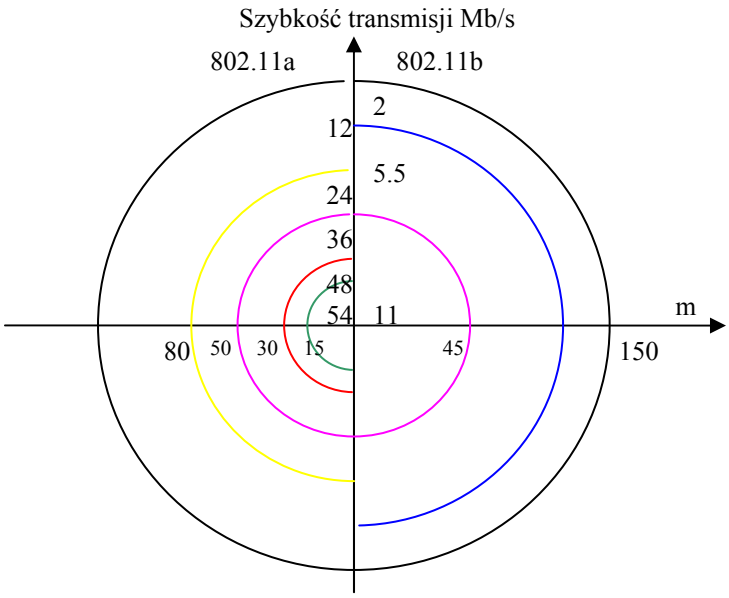


Rys.2. Pasmo częstotliwości wykorzystywanych przez IEEE 802.11a

W zależności od używanej prędkości transmisji danych używa się różnych metod modulacji.

Prędkość transmisji	Rodzaj modulacji
6	BPSK (*Binary Phase Shift Keying*)
9	BPSK
12	QPSK (*Quadrature Phase Shift Keying*)
18	QPSK
24	16-QAM (*Quadrature Amplitude Modulation*)
36	16-QAM
48	64-QAM
54	64-QAM

Zasięgi dla IEEE 802.11b i IEEE 802.11a przedstawia poniższy rysunek.



Rys.3. Szybkość transmisji informacji i odpowiadające im zasięgi transmisji

W Europie powstał inny standard transmisji bezprzewodowej, promowany przez ETSI - HiPeRLAN (*High Performance Radio Local Area Networ*k).

W ramach tego standardu zdefiniowano:

- warstwę fizyczną, w której określono min. pasma częstotliwości oraz sposób transmisji danych
- podwarstwę MAC – obejmującą:
    - dostęp do łącza
    - realizację funkcji mostu
    - transmisję wieloetapową
    - specyfikację jednostek danych
- podwarstwę CAC (*Channel Access Control*) obejmującą:
    - specyfikację protokołów dostępu do łącza
    - opisów typów ramek przesyłanych na poziomie podwarstwy

Podwarstwy MAC i CAC mogą współpracować z rozwiązaniami zgodnymi ze standardem IEEE 802.2. Ponadto standard zapewnia obsługę zgłoszeń asynchronicznych oraz z ograniczeniami czasowymi we wspólnym kanale. Na potrzeby standardu HiPeRLAN zarezerwowano w Europie pasma 5,15 – 5,3 GHz oraz 17,1 – 17,3 GHz. Oba pasma podzielone są na kanały o szerokości 25 MHz, a na granicach pasm znajdują się przedziały ochronne o szerokości 12,5 MHz. W niższym zakresie częstotliwości dostępnych jest zatem pięć kanałów, z których 3 są dostępne do transmisji, pozostałe są wykorzystywane opcjonalnie.

Transmisja ramek odbywa się z dwiema prędkościami.

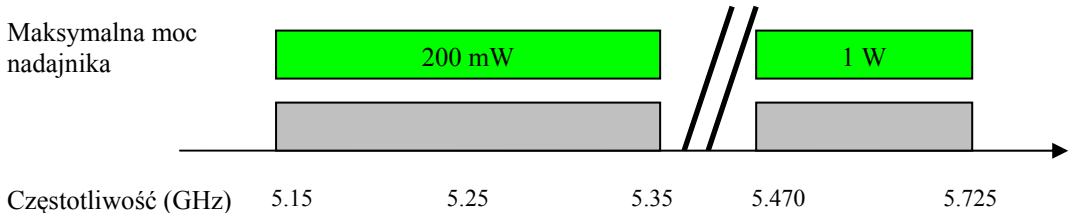
- mała LBR (*Low Bit Rate*) – wynosząca 1,4706 Mb/s ± 15 bps, z wykorzystaniem modulacji FSK (*Frequency Shift Keying*).
- duża HBR (*High Bit Rate*) – wynosząca 23,5294 Mb/s ± 235 bps, z wykorzystaniem modulacji GMSK (Gaussian Minimum Shift Keying) z parametrem BT=0,3.

Prędkość LBR stosuje się do wymiany danych sterujących natomiast prędkość HBR wykorzystywana jest do transmisji informacji użytkowych.

Maksymalny zasięg transmisji wynosi 50 m przy większej prędkości transmisji danych i 800m dla prędkości mniejszej. Dopuszcza się poruszanie stacji z prędkością do 10 m/s bez konieczności przerywania połączenia.

Standard ten definiuje protokół dostępu do łącza oparty na niewymuszonym, priorytetowym dostępie do łącza EY-NMPA (*Elimination Yield Non – preemptive Priority Multiple Access*). Protokół ten jest połączeniem mechanizmów wykrywania nośnej z algorytmami eliminacji i rozwiązywania konfliktów. Wydzielono w nim mechanizmy dostępu do kanału wolnego i zajętego oraz w przypadku tzw.; ukrytej eliminacji.

Podobnie jak standard IEEE 802.11 stał się podstawą do opracowania innych standardów, tak i HiPeRLAN ze względu na coraz to zwiększające się zapotrzebowanie na ilość przesyłanych informacji musiał ewoluować. Tak powstał jego następca HiPeRLAN 2. Pasmo częstotliwości dla Europy podzielone jest na dwa zakresy 5,15 – 5,35 i 5,470 – 5,725.



Rys.4. Zakres częstotliwości dla HiPeRLAN 2.

Cechy HIPERLAN 2:

- **Duża szybkość transmisji** do 54 Mb/s w warstwie fizycznej zaś w warstwie 3 do 25 Mb/s.
- **Połączenia zorientowane**. W sieciach HIPERLAN 2 transmisja danych jest poprzedzona wcześniejszym zestawieniem połączenia pomiędzy stacją roboczą a punktem dostępu przy użyciu funkcji sygnalizacyjnych. Połączenia są multipleksowane w czasie. Wyróżnia się dwa typy połączeń: punkt - punkt oraz punkt - wielopunkt. Połączenia punkt - punkt są dwukierunkowe, natomiast punkt - wielopunkt jednokierunkowe, w kierunku stacji mobilnych. Dodatkowo może być wykorzystywany kanał dedykowany np. na czas trwania transmisji do wszystkich stacji.
- **Wspieranie QoS**. Połączeniowo Zorientowana natura HIPERLAN 2 pozwala na bezpośrednią implementację usług wspierających QoS. Każdemu połączeniu może być przydzielona specyficzna usługa QoS zależna od szerokości pasma, opóźnienia, bitowej stopy błędu itd. Jest również możliwe przydzielenie każdemu połączeniu priorytetu. Usługa QoS w połączeniu z dużą szybkością transmisji wspomaga równoczesną transmisję różnych typów danych np. wideo, głosu i danych.
- **Automatyczny przydział częstotliwości**. W HIPERLAN 2 nie ma potrzeby ręcznego planowania częstotliwości jak to jest w sieciach komórkowych takich jak GSM. Punkt dostępu ma wbudowaną funkcję automatycznego wyboru odpowiedniego kanału radiowego dla transmisji w danym obszarze pokrycia. Punkt dostępu nasłuchuje sąsiednie punkty dostępu jak również inne źródła nadawcze i wybiera właściwe kanały radiowe minimalizując jednocześnie interferencje.
- **Zapewnienie bezpieczeństwa transmisji**. Standard HIPERLAN 2 zapewnia autoryzację i utajnianie przesyłanej informacji. Zarówno punkt dostępu AP jak i stacja mobilna mogą dokonywać autoryzacji zapewniając dostęp do sieci (z punktu widzenia AP) lub zapewniając dostęp upoważnionym użytkownikom. Utajnianie przesyłanej informacji ma na celu zapewnienie zabezpieczenia informacji przed podsłuchem i przechwytem.

- **Zapewnienie mobilności abonentów**. Stacja mobilna utrzymuje łączność z tym AP, z którym będzie najlepsza wartość stosunku sygnał-szum. Podczas przemieszczania się stacja mobilna nasłuchuje i analizuje jakość transmisji różnych punktów dostępu. Na podstawie zbieranych charakterystyk sygnału jest wybierany punkt dostępu.
- **Niezależność sieci i aplikacji**. Zestaw protokołów HIPERLAN 2 charakteryzują się architekturą podatną na adaptację i integrację z różnymi sieciami zbudowanymi w oparciu o różne standardy. HIPERLAN 2 może być np. użyta jako ostatni etap bezprzewodowego segmentu przełączanego Ethernetu, ale może być także użyta w innej konfiguracji, np. jako dostęp do sieci komórkowych 3 generacji. Wszystkie aplikacje, które są wykorzystywane w stałych sieciach mogą być wykorzystywane w sieci HIPERLAN 2.
- **Tryb oszczędzania energii**. Mechanizm pozwala stacji mobilnej przejść w tryb oszczędzania energii. Bazuje on na mechanizmie negocjacji okresu czuwania. Stacja mobilna może zażądać w dowolnym czasie od AP przejścia w tryb czuwania. W czasie tego stanu, stacja szuka, co pewien okres czasu sygnału „pobudki" od AP. Jeżeli go nie ma, przechodzi dalej w stan czuwania. AP będzie buforować przychodzące dane do danej stacji mobilnej dopóki nie wygaśnie okres czuwania. Czasy trwania uśpienia są różne dla żądania przejścia w tryb oszczędzania energii i żądania krótkiej

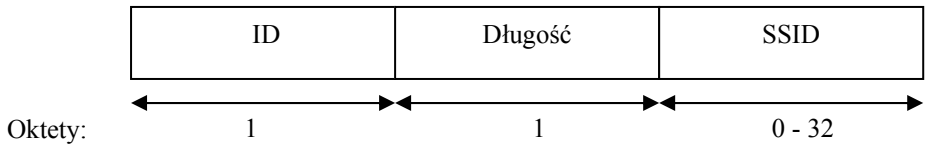
Standard	802.11	802.11b	802.11a	HiPeRLAN
Pasmo [GHz]	2,4	2,4	5	5
Prędkość transmisji danych [Mbps]	2	11	54	54
Protokół dostępu do łącza	CSMA/CA			TDMA/TDD
Tryb rozgłoszeniowy	Tak	Tak	Tak	Tak
Wspomaganie QoS	(PCF)	(PCF)	(PCF)	ATM/802.1/RSVP
Wybór częstotliwości	FHSS lub DSSS	DSSS	Pojedyncza fala nośna	Pojedyncza fala nośna z dynamicznym wyborem częstotliwości
Uwierzytelnianie	Nie	Nie	Nie	NAI/IEEE adres/X.509
Szyfrowanie	40-bit RC4	40-bit RC4	40-bit RC4	DES, 3DES
Obsługiwana sieć	Ethernet	Ethernet	Ethernet	Ethernet,IP,ATM,UMCS, FireWire,PPP
Zarządzanie	802.11MIB	802.11MIB	802.11MIB	HiperLAN/2 MIB
Kontrola jakości łącza	Nie	Nie	Nie	Adaptacja łącza

Rys.5. Porównanie wszystkich standardów.

2. Mechanizmy bezpieczeństwa w IEEE 802.11

2.1 SSID

SSID (*Service Set Identifier*) – jest informacją wykorzystywaną przez punkty dostępu AP (*Access Points*) do identyfikacji stacji mających uzyskać dostęp do sieci WLAN. Identyfikator SSID można porównać do wspólnej nazwy sieci, którą znają tylko punkty dostępu i uprawnieni użytkownicy, jest to więc pewien rodzaj hasła., jednak ponieważ stacje ruchome muszą rozpoznawać w zasięgu którego punktu dostępu aktualnie się znajdują, identyfikator SSID jest rozgłaszany przez AP w specjalnej ramce, w jawnej postaci.
Cecha ta może być w prosty sposób wykorzystana przez ewentualnego włamywacza, w związku z tym nie należy traktować SSID jako zabezpieczenia przed nieautoryzowanym dostępem do sieci WLAN.



Rys.6. Format SSID

Długość pola SSID zawiera się w granicach 0 -32 oktetów, jeśli wynosi 0 oznacza to SSID jest typu rozgłoszeniowego.

2.2 WEP

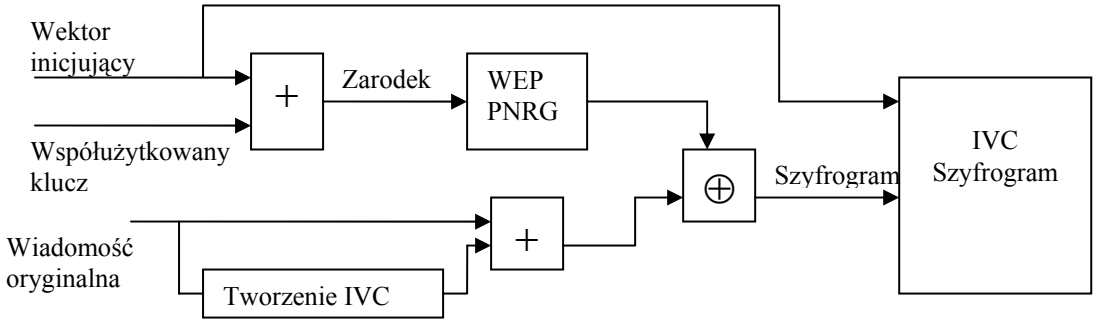
Ze względu na naturę fal radiowych, które rozprzestrzeniają się w sposób nieograniczony, transmisja bezprzewodowa jest łatwiejsza do przechwycenia niż transmisja w sieci przewodowej, w związku z tym do bezpiecznej transmisji danych zaproponowano wykorzystanie protokołu WEP (*Wired Equivalent Privacy*), zapewniającego bezpieczeństwo transmisji. Jest to rodzaj szyfrowania polegający na tym, że do zaszyfrowania i odszyfrowania stosowany jest ten sam klucz.
Własności WEP:

- jest protokołem samosynchronizującym się.
- łatwy w implementacji zarówno programowej jak i sprzętowej.
- jego zastosowanie jest opcjonalne

WEP wykorzystuje algorytm szyfrowania kluczem symetrycznym RC4 PRNG (*Ron's Code 4 Pseudo Random Number Generator*). Pod kontrolą WEP wszyscy klienci i punkty dostępu w sieci bezprzewodowej używają tego samego klucza do szyfrowania i odszyfrowania danych.

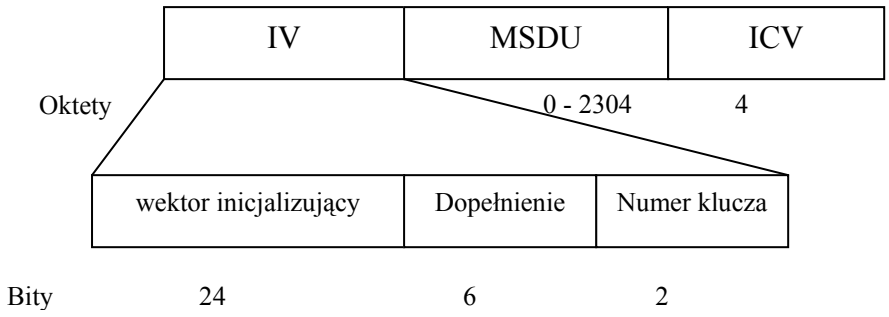
Klucz rezyduje w komputerze klienta i w każdym punkcie dostępu w sieci. W 802.11 nie określono protokołu zarządzania kluczem, tak więc klucze WEP w sieci muszą być zarządzane ręcznie. Wsparcie dla WEP jest standardowe w nowych kartach i punktach dostępu 802.11. System bezpieczeństwa WEP jest też dostępny w konfiguracji ad-hoc.
WEP specyfikuje użycie klucza szyfrującego 40-bitowego, a także 104-bitowego.

Ponieważ klucz szyfrujący jest łączony z 24-bitowym wektorem inicjalizującym IV, w rezultacie otrzymuje się 64- i 128-bitowy klucz. Otrzymana sekwencja jest używana do szyfrowania transmitowanych danych.



Rys.7. Mechanizm szyfrowania WEP

Do wygenerowania sekwencji szyfrującej przez RC4 niezbędne są dwa ciągi bitów: poufny klucz, taki sam zarówno dla AP, jak i dla stacji użytkownika, oraz wektor inicjujący. Poufny klucz przydzielany jest ręcznie lub za pomocą specjalnych protokołów przesyłania kluczy, natomiast wektor inicjujący przesyłany jest w sposób jawny wraz z zaszyfrowanymi danymi. Do tak utworzonego niezaszyfrowanego ciągu danych dodawany jest współczynnik integralności (ICV), zapewniający integralność danych podczas odbioru.
Sekwencja szyfrująca sumowana jest następnie modulo 2 z wiadomością niezaszyfrowaną.



Rys.8. Ramka danych WEP

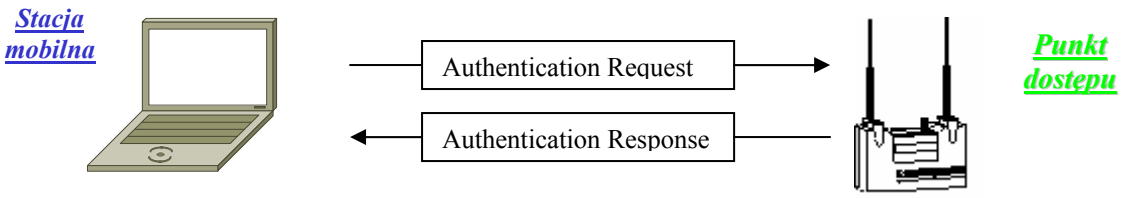
Pierwsze 24 bity ramki nazywane są wektorem inicjalizującym z zapewniają unikatową postać ramki. Łatwo policzyć że pole to może przyjmować 16,777,216 możliwych wartości.
W polu numer klucza określony mamy wybór jednego z czterech możliwych wartości klucza wykorzystywanego do deszyfrowania ramki.
MSDU - Medium Access Control (MAC) Service Data Unit – jest to informacja przenoszona pomiędzy dwoma warstwami MAC.
ICV - Integrity Check Value - współczynnik integralności, zapewniający integralność danych podczas odbioru.

3. Uwierzytelnianie i asocjacja w 802.11

Celem uwierzytelniania jest sprawdzanie wiarygodności stacji ruchomej, która ma być obsługiwana przez sieć WLAN.
W Standardzie IEEE 802.11 zdefiniowano kilka mechanizmów uwierzytelniania.
Zaliczamy do nich:

3.1 Otwarte uwierzytelnianie – polega na tym, że cały proces wymiany informacji uwierzytelniającej przed dopuszczeniem stacji ruchomej do korzystania z sieci odbywa się w sposób jawny. Każda stacja może więc pozytywnie przejść proces uwierzytelnienia i utworzyć skojarzenie z punktem dostępu, nawet wówczas jeśli nie będzie miała poprawnego klucza WEP. Jednak w przypadku braku klucza WEP nie będzie mogła nadawać i odbierać żadnych danych.

Otwarte uwierzytelnienia odbywa się w dwóch krokach. W pierwszym kroku wysyłana jest sekwencja od stacji mobilnej do punktu dostępu z żądaniem uwierzytelnienia (Authentication Request). W drugim kroku punkt dostępu zezwala na uwierzytelnienie (Authentication Response).

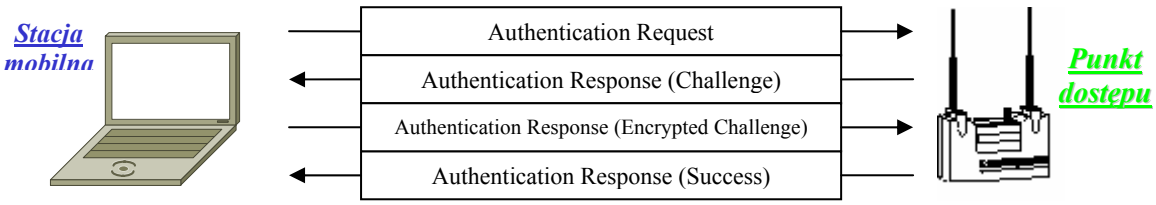


Rys.9. Fazy występujące przy otwartym uwierzytelnianiu

W pierwszym kroku w ramce przesyłane są informacje;
- typ wiadomości: zarządzanie
- podtyp wiadomości: uwierzytelnianie
- elementy wiadomości:
  - Identyfikacja algorytmu uwierzytelniania = ‘Uwierzytelnianie Otwarte’
  - Identyfikacja stacji (adres przenoszony w polu SA nagłówka)
  - Numer ramki = 1
  - Informacja zależna od algorytmu uwierzytelniania, przy otwartym uwierzytelnianiu ustawiana wartość 0
- kierunek przepływu wiadomości: Od stacji inicjującej do stacji uwierzytelniającej.

W ramce zezwalającej na uwierzytelnienie przesyłane są informacje;
- typ wiadomości: zarządzanie
- podtyp wiadomości: uwierzytelnianie
- elementy wiadomości:
    - Identyfikacja algorytmu uwierzytelniania = ‘Uwierzytelnianie Otwarte’
    - Numer ramki = 2
    - Informacja zależna od algorytmu uwierzytelniania
    - Informacja o zgodzie na uwierzytelnianie, wartość ustawiana na 0
- kierunek przepływu wiadomości: Od stacji uwierzytelniającej do stacji inicjującej.

3.2 Uwierzytelnianie za pomocą współdzielonego klucza – podczas uwierzytelniania stacja, która ma się włączyć do sieci, wysyła do punktu dostępu żądanie przyznania dostępu do sieci WLAN. W odpowiedzi AP wysyła do stacji mobilnej tzw. pakiet-wyzwanie(*Challenge*). Stacja mobilna musi w odpowiedzi przesłać zaszyfrowany pakiet za pomocą współużytkowanego klucza WEP i odesłać go z powrotem do punktu dostęp. Jeżeli wysłany pakiet został prawidłowo odszyfrowany przez punkt dostępu to, zostaje utworzone skojarzenie, o czym stacja jest powiadamiana w odpowiedzi zwrotnej na żądanie, zarówno uwierzytelnianie jak i skojarzenie są realizowane wyłącznie w warstwie łącza danych. Punkt dostępu nie ma żadnych wiadomości na temat użytkownika, któremu pozwolił włączyć się do sieci.



Rys.10. Fazy uzyskiwania uwierzytelniania z użyciem współdzielonego klucza.

W pierwszym kroku w ramce zawarte są informacje:
- typ wiadomości: zarządzanie
- podtyp wiadomości: uwierzytelnianie
- elementy wiadomości:
    - Identyfikacja stacji (adres przenoszony w polu SA nagłówka ramki)
    - Identyfikacja algorytmu uwierzytelniania = ‘Uwierzytelnianie przy pomocy współdzielonym kluczem’
    - Numer ramki = 1
    - Informacja zależna od algorytmu uwierzytelniania, ustawiana wartość 0
- kierunek przepływu wiadomości: Od stacji inicjującej do stacji uwierzytelniającej.

W drugim kroku w ramce zawarte są informacje:
- typ wiadomości: zarządzanie
- podtyp wiadomości: uwierzytelnianie
- elementy wiadomości:
    - Identyfikacja algorytmu uwierzytelniania = ‘Uwierzytelnianie z współdzielonym kluczem’
    - Numer ramki = 2
    - Informacja zależna od algorytmu uwierzytelniania = wynik uwierzytelnienia
    - Odpowiedz na żądanie uwierzytelniania zaszyfrowana współużytkowanym kluczem.
- kierunek przepływu wiadomości: Od stacji uwierzytelniającej do stacji inicjującej.

W trzecim kroku w ramce zawarte są informacje:
- typ wiadomości: zarządzanie
- podtyp wiadomości: uwierzytelnianie
- elementy wiadomości:
    - Identyfikacja algorytmu uwierzytelniania = ‘Uwierzytelnianie z współdzielonym kluczem’
    - Numer ramki = 3
    - Informacja zależna od algorytmu uwierzytelniania = zaszyfrowany pakiet przez stacje żądającą uwierzytelnienia
    - Odpowiedz na żądanie uwierzytelniania zaszyfrowana współużytkowanym kluczem.
- kierunek przepływu wiadomości: Od stacji inicjującej do stacji uwierzytelniającej.

W czwartym kroku w ramce zawarte są informacje:
- typ wiadomości: zarządzanie
- podtyp wiadomości: uwierzytelnianie
- elementy wiadomości:
    - Identyfikacja algorytmu uwierzytelniania = ‘Uwierzytelnianie z współdzielonym kluczem’
    - Numer ramki = 4
    - Odpowiedz punktu dostępu o zgodzie bądź odrzucenie żądania uwierzytelnienia
- kierunek przepływu wiadomości: Od stacji uwierzytelniającej do stacji inicjującej.

3.3 Uwierzytelnienie na podstawie adresów MAC – producenci urządzeń bezprzewodowych wprowadzają możliwość wydzielenia ograniczonego zbioru adresów MAC, które jednoznacznie identyfikują stacje ruchome. Punkt dostępu sprawdza w swoich zasobach czy posiada adres fizyczny urządzenia żądającego dostępu do sieci, jeśli wynik jest pozytywny to stacja mobilna uzyskuje dostęp do zasobów sieci, jeśli nie jego prośba jest odrzucana.

4. Analiza mechanizmów bezpieczeństwa w IEEE 802.11

4.1 Uwierzytelnianie na podstawie adresów MAC.

Ten typ uwierzytelniania opiera się na sprawdzeniu przez AP adresu MAC stacji mobilnej. Jeśli adres ten zgadza się z adresem który jest znany przez AP, to stacja mobilna dostaje zgodę na pracę w sieci. W przeciwnym przypadku decyzja jest odmowna. Taki proces uwierzytelniania nie jest zbyt bezpieczny ponieważ, wystarczy że włamywacz zdobędzie w dowolny sposób adres MAC urządzenia mającego zgodę na pracę w sieci, podszyje się pod niego i uzyska natychmiastowy dostęp do sieci WLAN.

4.2 Jednokierunkowa autentykacja.

W sieciach w WLAN stosowany jest proces jednokierunkowej autentykacji polegający na tym, że sprawdzana jest tożsamość tylko stacji mobilnej za pośrednictwem punktu dostępu. Słabość takiego rozwiązania polega na możliwości podszycia się wrogiego klienta pod punkt dostępowy tuż po zakończeniu fazy uwierzytelniania i wygenerowania błędnego komunikatu o pomyślnym zakończeniu procesu. Tak „oszukany" klient nieświadomie przesyła wszystkie dane prosto do komputera intruza.

4.3 Słabości klucza WEP.

Podstawowym mechanizmem wykorzystywanym do zabezpieczenia transmisji w sieciach bezprzewodowych jest szyfrowanie za pomocą protokołu WEP (Wired Equivalent Privacy) bazującego na algorytmie RC4 stworzonym przez naukowców z RSA Data Security Inc. RC4 jest algorytmem symetrycznym, co oznacza, ze ten sam klucz używany jest zarówno do szyfrowania, jak i odszyfrowania informacji. Ze względu na wprowadzone przez USA ograniczenia eksportu technologu kryptograficznych długość klucza została zdefiniowana na poziomie 40 bitów. Jednak wielu producentów szybko doszło do wniosku, ze jest to niewystarczające i do pełnego zabezpieczenia transmisji potrzebne są klucze 128-bitowe. Zmiana ta nie rozwiązała jednak wszystkich problemów. Okazało się bowiem, ze w zasadzie bez względu na długość zastosowanego klucza, WEP jest bardzo podatny na ataki polegające na próbie wyekstrahowania klucza z pakietów o znanej zawartości, np. zawierających zapytania DHCP. Metoda ta bazuje na pewnych niedociągnięciach implementacji wektora inicjującego (ang. Initialization Vector) w skrócie nazywanego IV. Wektor inicjujący to 24-bitowa wartość, którą tworzy zmienną część klucza szyfrującego w algorytmie WEP. Wektor inicjujący wydaje się być bardzo potrzebny, gdyż powinien zapobiec wystąpieniu dwóch ramek o identycznej zawartości (po zaszyfrowaniu). Ponieważ popularne usługi, jak DHCP czy DNS, wykorzystują komunikaty w standardowych formatach, istnieje duże ryzyko wystąpienia takich ramek. Klucz WEP jest symetryczny i niezmienny, dzięki przechwyceniu kilku takich zaszyfrowanych pakietów można wydzielić z nich zastosowany klucz w stosunkowo krótkim czasie. Zmienny wektor IV, który jest dodawany do statycznego klucza bazowego w celu utworzenia unikatowego klucza wynikowego, ma zapobiec takim sytuacjom. Sama wartość IV jest przesyłana otwartym tekstem wraz z numerem zastosowanego klucza oraz dopełnieniem.

Wydawać by się mogło, ze dzięki takiemu mechanizmowi mamy pełną gwarancję unikatowości zaszyfrowanych ramek. 24-bitowe pole umożliwia nam wykorzystanie 16 777 216 różnych wartości wektora, dzięki czemu teoretycznie możliwe jest zapewnienie unikatowego klucza efektywnego tej samej liczbie ramek.

Niestety, większość spotykanych obecnie implementacji wykorzystuje do tworzenia IV algorytm pseudolosowy, który generuje jedynie pewien podzbiór wszystkich możliwych kombinacji bitów. Ponadto algorytm RC4, który wykorzystuje KSA (Key Scheduling Algorithm) do generacji IV, jako podstawy do jego utworzenia używa wartości klucza bazowego. W efekcie wartość IV może się dość często powtarzać i dodatkowo zawierać elementy klucza bazowego, co powoduje tzw. kolizje IV, czyli powtórne wykorzystanie tego samego IVz tym samym kluczem bazowym. Można więc założyć, ze po odpowiednio długim czasie śledzenia ruchu w sieci bezprzewodowej włamywacz będzie w stanie wychwycić odpowiednią liczbę identycznych ramek i na ich podstawie odtworzyć wartość klucza bazowego.

Protokół WEP nie zapewnia ochrony przed modyfikacją transmitowanej wiadomości. Możliwa jest jej zmiana bez detekcji i naruszania mechanizmów bezpieczeństwa. Wykorzystana do tego zostaje własność sumy kontrolnej polegająca na tym, że suma kontrolna w protokole WEP jest liniową funkcją wiadomości. Oznacza to, że sumę kontrolną można rozdzielić poprzez operację XOR. Konsekwencją powyższej własności jest to, że możliwa staje się kontrolowana modyfikacja zaszyfrowanej wiadomości bez zmiany sumy kontrolnej. Załóżmy sytuację, kiedy zaszyfrowana wiadomość *C (nieznana wiadomość M)* zostanie przechwycona przed dostarczeniem jej do miejsca przeznaczenia. Możliwe jest znalezienie nowej zaszyfrowanej wiadomości *C'*. Wykorzystana do tego zostanie własność systemu kodowania RC4,polegająca na ponownym wykonaniu operacji XOR. Oznacza to, że można stworzyć dowolne modyfikacje zaszyfrowanej wiadomości bez obawy o wykrycie tego faktu. W związku z powyższym, pole sumy kontrolnej protokołu WEP nie nadaje się do ochrony integralności danych.

Protokół WEP nie zapewnia także ochrony przed kontrolą dostępu. Wynika to z następującej własności pola sumy kontrolnej protokołu WEP, mianowicie suma kontrolna w protokole WEP jest niekluczowalną funkcją wiadomości. W konsekwencji powyższego, pole sumy kontrolnej może być obliczone w sposób odwrotny przez kogoś kto zna wiadomość. Jeżeli potencjalny włamywacz przechwyci pełną treść niezaszyfrowanej wiadomości odpowiadającą kilku transmitowanym ramkom, będzie on zdolny wprowadzić dowolne wiadomości do sieci.

Rozważmy teraz protokół WEP z punktu widzenia potencjalnego włamywacza. Protokół WEP używa strumienia cyfr do zapewnienia ochrony przesyłanych wiadomości (RC4), tak więc bezpośredni atak kryptografa jest bezcelowy. Jest jednak miejsce gdzie atak taki może być przeprowadzony jest to punkt dostępu. W każdym protokole kryptograficznym, uprawniony algorytm szyfrowania musi zawsze posiadać sekretny klucz szyfrujący. Celem naszym może więc będzie oszukanie punktu dostępu nakazujące mu odszyfrowanie dla nas kilku wiadomości. Jeżeli zostanie to zrobione, modyfikacja transmitowanych pakietów będzie pozwalała na wykorzystanie punktu dostępu do dwóch celów:

- przekierowanie IP;
- prowadzenia ataków bazujących na reakcji odbiorcy.

4.3.1 Przekierowanie IP

Atak ten może być użyty gdy punkt dostępu działa jak router IP. W tym wypadku, celem jest sniffing zaszyfrowanych pakietów w powietrzu i użycie techniki zmieniającej miejsce przeznaczenia takiego pakietu. Punkt dostępu odszyfrowuje taki pakiet i przesyła go do nowego miejsca przeznaczenia, gdzie potencjalny włamywacz może go teraz przeczytać już w postaci jawnej. Należy zauważyć, że zmodyfikowany pakiet będzie podróżował poczynając od środowiska bezprzewodowego do przewodowego, przechodząc przez wiele firewali, które wcale nie będą mu przeszkadzać.

Najłatwiejszym sposobem modyfikacji miejsca przeznaczenia pakietu jest rozpracowanie oryginalnego docelowego adresu IP, a następnie zastosowanie techniki stosowanej przy modyfikacji wiadomości. Rozpracowanie oryginalnego adresu przeznaczenia nie jest sprawą trudną, zwłaszcza gdy całość przychodzącego ruchu np. będzie przeznaczone do podsieci bezprzewodowej, którą to można łatwo określić.

Zaraz po tym, jak przychodzący ruch zostanie rozszyfrowany, adres IP miejsca przeznaczenia zostanie ujawniony i wychodzący ruch może być zaszyfrowany w ten sam sposób.

4.3.2 Ataki bazujące na reakcji odbiorcy

Jest również inny sposób manipulacji punktem dostępu i złamania szyfrowania transmisji przy pomocy protokołu WEP, dające się zastosować w miejscach gdzie protokół WEP jest używany do ochrony ruchu TCP/IP. Atak taki nie wymaga podłączenia do sieci Internet i może być użyty nawet wówczas, gdy atak przekierowania IP jest niemożliwy. Jest to jednak możliwe tylko w stosunku do ruchu TCP, inne protokoły IP nie mogą być odszyfrowane przy pomocy tego ataku. Atak ten polega na monitorowaniu reakcji odbiorcy pakietu TCP i użyciu tego co zostało zaobserwowane do wnioskowania informacji o wiadomości. Atak wykorzystuje fakt, że tylko te pakiety TCP są akceptowane, które maj ą poprawną sumę kontrolną i w odpowiedzi przesyłany jest pakiet potwierdzający. Pakiet potwierdzający jest łatwo identyfikowalny poprzez jego rozmiar, nie jest więc wymagane jego odszyfrowanie. Zatem reakcja odbiorcy będzie ujawniała czy w odebranym pakiecie pole sumy kontrolnej było poprawne. Powyższy atak będzie przebiegał następująco. Przechwytujemy zaszyfrowaną wiadomość C o nieznanym sposobie szyfrowania. Zamieniamy kilka bitów w wiadomości C i korygujemy CRC tak, aby otrzymać nową zaszyfrowaną wiadomość C' *z* poprawną sumą kontrolną WEP. Następnie transmitujemy wiadomość C' w sfałszowanym pakiecie do punktu dostępu. Obserwujemy czy ewentualny odbiorca przesyła pakiet potwierdzenia TCP ACK. Należy zauważyć, że można zamienić dowolne bity w wiadomości *C*. Poprzez odpowiedni wybór bitów do zamiany, możemy zapewnić, że pole sumy kontrolnej TCP nie zmieni się. Obecność lub brak pakietu ACK będzie ujawniał jedno bitową informację o nieznanej jawnej postaci wiadomości. Powtarzanie ataków dla wielu wyborów *i*, można dowiedzieć się prawie wszystkiego o jawnej postaci wiadomości, a wtedy dedukując o kilku pozostałych nieznanych bitach będzie można łatwo zastosować klasyczne techniki.

4.4 Zarządzanie kluczem

Standard IEEE 802.11 nie specyfikuje jak ma być dokonywana dystrybucja klucza. Liczy on na zewnętrzne mechanizmy, które będą wypełniać wspólnie dzieloną tablicę
4 kluczy. Każda wiadomość zawiera pole identyfikujące umiejscowienie w tablicy użytego klucza. Standard uwzględnia także tablice, które kojarzą klucz z każdą stacją mobilną, ale ta opcja nie jest rozpowszechniona. W praktyce większość instalacji używa pojedynczego klucza w całej sieci.

Praktyka ta poważnie wpływa na zmniejszenie bezpieczeństwa systemu, ponieważ sekret dzielony pomiędzy wielu użytkowników nie może być dobrze ukryty. Niektórzy administratorzy sieci próbują rozwiązać ten problem nie ujawniając sekretu użytkownikom końcowym i samemu konfigurując ich komputery. Nie daje to jednak pełnego rozwiązania problemu, gdyż klucze te są w dalszym ciągu przechowywane na komputerach użytkowników końcowych.

Zagrożeniem jest także duża liczba użytkowników, gdyż wzrastają wówczas szanse na kolizje. Co gorsza zerowanie wektorów inicjujących po każdym restarcie kart PCMCIA, powoduje ponowne użycie strumienia kluczowego odpowiadającego niskim wartościom wektora inicjującego.

Zastąpienie natomiast rozszyfrowanych kluczy innymi jest trudne do wykonania przy dużej liczbie użytkowników. Wymaga to bowiem rekonfiguracji sterowników sieci bezprzewodowych.

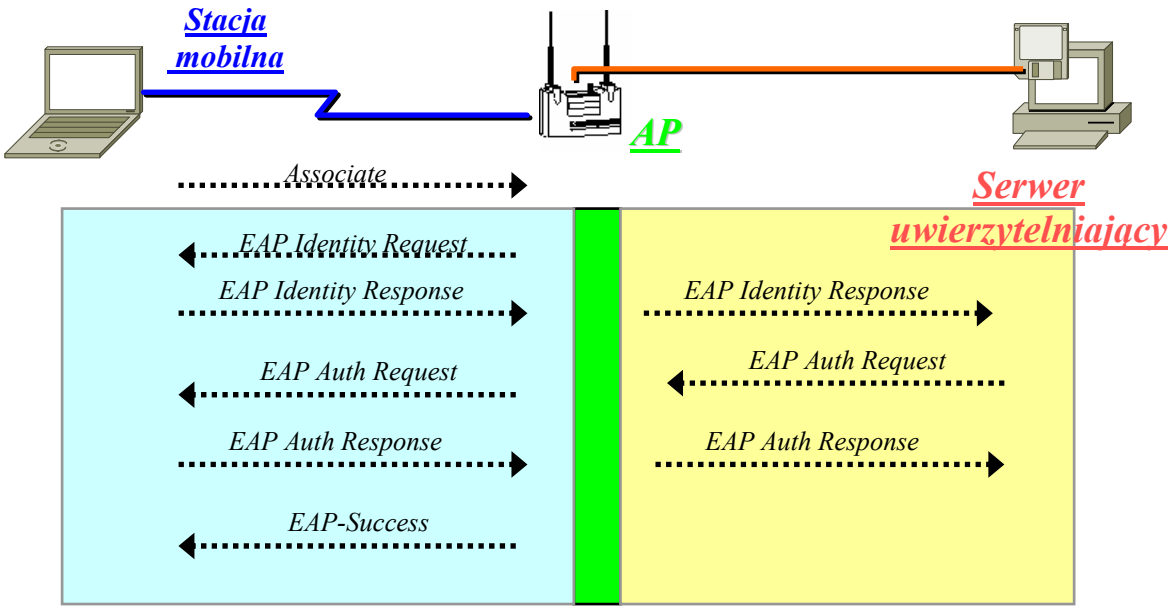
Z praktyki należy się spodziewać, że upłyną miesiące użytkowania kluczy zanim zostaną zastąpione nowymi. Pozwoli to potencjalnemu włamywaczowi na dokładną analizę ruchu i poszukiwanie momentów ponownego użycia klucza.

5. Uwierzytelnienie na podstawie specyfikacji IEEE 802.1x

W związku z niedoskonałościami protokołu WEP w zakresie zapewniania bezpieczeństwa podczas przesyłania informacji w sieciach bezprzewodowych, zaproponowano specyfikację IEEE 802.1x, mający za zadanie usunięcie wad protokołu WEP.

5.1 Uwierzytelnianie na podstawie protokołu EAP.

Mechanizm uwierzytelniania wykorzystywany przez protokół EAP (*Extensible Authentication Protocol*), polegający na wykorzystaniu serwera uwierzytelniającego, który ma za zadanie sprawdzenie tożsamości stacji mobilnej za pośrednictwem punktu dostępu.



Rys.11. Uwierzytelnienie z wykorzystaniem protokołu EAP

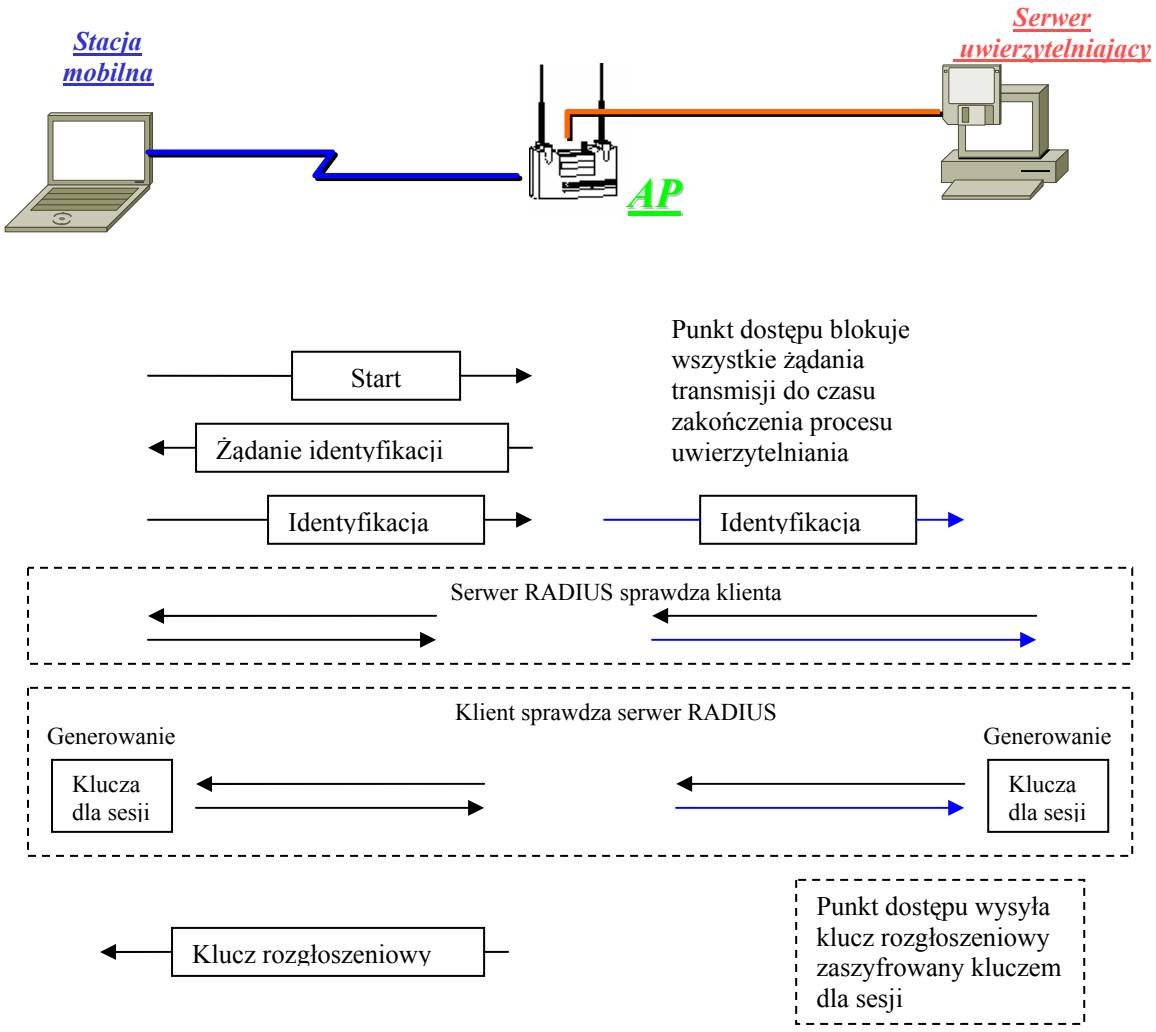
Podczas uwierzytelnienia z wykorzystaniem protokołu EAP, można wyróżnić następujące fazy:
- stacja mobilna zostaje skojarzona z punktem dostępu
- punkt dostępu wysyła do stacji mobilnej pakiet wyzwania z żądaniem podania tożsamości
- stacja mobilna wysyła do punktu dostępu pakiet identyfikujący
- pakiet ten przekazywany jest do serwera uwierzytelniającego
- z serwera uwierzytelniającego wysyłany jest pakiet żądania uwierzytelnienia, który jest przesyłany poprzez punkt dostępu do stacji mobilnej
- w odpowiedzi przesyłany jest pakiet odpowiedzi, który jest przekazywany do serwera i na jego podstawie wykonywany jest proces uwierzytelniania
- zgoda na uwierzytelnienie przekazywana jest poprzez punkt dostępu do stacji mobilnej

5.2 Uwierzytelnianie protokołem LEAP

Mechanizm wykorzystujący protokół LEAP (*Lighwieght Extensible Authentiction Protocol*), polega na wykorzystaniu mechanizmu wzajemnego uwierzytelniania, oznacza to, że wymagane jest potwierdzenie tożsamości klienta za pośrednictwem punktu dostępu jak i potwierdzenie tożsamości serwera uwierzytelniającego za pośrednictwem punktu dostępu względem klienta. Mechanizm ten zabezpiecza przed podszyciem się potencjalnego włamywacza pod punkt dostępu i serwer uwierzytelniający.

Implementacja Cisco LEAP składa się z 3 komponentów:
- klienta sieci
- punktu dostępu z odpowiednim oprogramowaniem
- Serwera uwierzytelniającego LEAP

Proces uwierzytelniania i dystrybucji klucza można podzielić na trzy fazy:
- Start.
- Uwierzytelnianie.
- Zakończenie



Rys.12. Proces uwierzytelniania protokołem LEAP

W pierwszej kolejności klient sieci wysyła pakiet zgłoszeniowy do punktu dostępu. W tym momencie punkt dostępu blokuje wszystkie żądania transmisji do czasu zakończenia procesu uwierzytelniania. Następnie wysyła pakiet wyzwanie (*Challenge*) z żądaniem identyfikacji do klienta sieci. W odpowiedzi uzyskuje pakiet identyfikacji. W tym momencie punkt dostępu przekazuje pakiet identyfikacji pochodzący od klienta sieci do serwera uwierzytelniającego. Na jego postawie następuje sprawdzenie tożsamości klienta sieci.
W kolejnym kroku serwer jest sprawdzany przez klienta sieci, i tworzone są klucze sesyjne przez oprogramowanie zaimplementowane u klienta sieci i serwerze.
Zastosowanie protokołu LEAP nie ogranicza się tylko do sprawdzania tożsamości. Definiuje on również sposób tworzenia i dystrybucji kluczy szyfrujących. W celu zapewnienia maksymalnej ochrony przesyłanej informacji zastosowane zostały dwa rodzaje kluczy szyfrujących: sesyjne, służące do szyfrowania transmisji między pojedynczym klientem a punktem dostępu, oraz rozgłoszeniowe, stosowane w przypadku transmisji typu broadcast lub multicast. Klucz sesyjny jest używany przez jednego konkretnego klienta i komunikujący się z nim punkt dostępu wyłącznie w określonym przedziale czasu. Dzięki takiemu rozwiązaniu poznanie klucza szyfrującego przez osobę niepowołaną nie ma większego wpływu na bezpieczeństwo całego systemu – w przeciwieństwie do sieci w których wartości kluczy bazowych są nie zmieniane i jednakowe dla wszystkich użytkowników oraz punktów dostępu.
Ważnym i ciekawym procesem jest sam proces tworzenia i dystrybucji kluczy bazowych. Aby zachować maksimum bezpieczeństwa, klucze sesyjne w żadnym momencie nie są transmitowane za pośrednictwem sieci bezprzewodowej, są natomiast generowane za pomocą specjalnego algorytmu zaimplementowanego w oprogramowaniu klienta i serwera uwierzytelniającego. Jedną z wielu wartości zmiennych używanych do wygenerowania klucza sesyjnego są pakiety typu challenge, mające zastosowanie w fazie uwierzytelniania.
Po pomyślnym wygenerowaniu klucza sesyjnego przez obie strony i dostarczeniu jego wartości do bezprzewodowego punktu dostępu bezpiecznym połączeniem kablowym (Ethernet) przez serwer uwierzytelniający, mamy zapewniony chroniony kanał transmisyjny od i do klienta. Dopiero za pośrednictwem tak przygotowanego połączenia punkt dostępu może wysłać do klienta informacje o kluczu rozgłoszeniowym kanałem bezprzewodowym. Oczywiście klucze rozgłoszeniowe również są pewien czas wymieniane, aby zapobiec występowaniu kolizji wektora inicjującego.

6. Wnioski

W prezentowanej pracy omówiłem stosowane obecnie protokoły i przedstawiłem problemy występujące podczas, przesyłania informacji w sieciach bezprzewodowych.

Głównym niebezpieczeństwem podczas korzystania z sieci bezprzewodowych w zakresie bezpieczeństwa są luki w stosowanym protokole WEP. Protokół ten powinien zapewnić zgodnie z przyjętymi założeniami trzy główne zabezpieczenia w zakresie:
- poufności – zapobieganie przypadkom podsłuchu
- kontrola dostępu – zabezpieczenie infrastruktury sieci bezprzewodowej
- integralności danych – zapobieganie manipulacjom wiadomości przez osoby niepowołane

Niestety w podstawowej swej wersji wymagania te nie są spełnione.
Jednakże, w odpowiedzi na wykryte luki w protokole WEP firmy zajmujące się opracowywaniem urządzeń wykorzystywanych w sieciach bezprzewodowych, zaczęły wprowadzać pewne modyfikacje w celu zwiększenia bezpieczeństwa podczas transmisji informacji. Pierwszy krok uczyniła w tym kierunku firma Cisco, w której to produktach do generowania wektora inicjującego stosowany jest algorytm liniowy, który wykorzystuje wszystkie możliwe wartości wektora inicjującego. Dla przykładu w najbardziej pesymistycznym wariancie, tzn. w sytuacji, gdy przez bezprzewodowy punkt dostępowy będą przepływały ramki o długości 64 bitów z prędkością ok. 2300 ramek na sekundę, kolizja IV nastąpi co około 2 godziny. Aby zapobiec powstawaniu identycznych ramek po zaszyfrowaniu za pomocą algorytmu WEP, specjaliści z Cisco zdecydowali się na wprowadzenie nie tylko częstszej zmiany IV (dla każdego pakietu), ale również wymiany samych kluczy bazowych, które dotychczas byty elementem stałym, zmienianym ręcznie przez administratora. Dzięki temu, jeżeli założymy, ze klucz bazowy zmieni się, zanim wyczerpie się „pojemność" wektora inicjującego, możemy być prawie pewni, ze efekt pojawienia się identycznych ramek nie wystąpi Dodatkowym zabezpieczeniem jest haszowanie klucza bazowego połączonego z wektorem inicjującym. Takie rozwiązanie praktycznie uniemożliwia ekstrakcję klucza bazowego z zaszyfrowanej ramki nawet w przypadku znajomości IV i zawartości samej ramki. Dzięki tej metodzie urządzenia bezprzewodowe są całkowicie odporne na ataki dokonywane za pomocą takich narzędzi jak linuksowy Airsnot, gdyż jak wiadomo, niemożliwe jest odszyfrowanie czegokolwiek, co zostało przeliczone przez jednostronną funkcję haszującą. Wprowadzenie dynamicznych kluczy WEP nie jest jednak rozwiązaniem wszystkich słabości zabezpieczania transmisji bezprzewodowej.
Równie ważnym zagadnieniem jak samo szyfrowanie jest uwierzytelnianie użytkowników oraz punktów dostępowych. Brak takiego mechanizmu lub tylko częściowa implementacja może narazić sieć bezprzewodową na ataki polegające na podszywaniu się intruza pod legalnego użytkownika lub punkt dostępu. Luką w systemie zabezpieczeń jest bez wątpienia anonimowość użytkowników. Aby wyeliminować wpływ tych niedociągnięć specjaliści z Cisco zaczęli implementować w urządzeniach protokół EAP oraz w późniejszym czasie wprowadzany obecnie na szeroką skalę protokół LEAP opierający się na wykorzystaniu serwera uwierzytelniającego RADIUS oraz wzajemnym uwierzytelnianiu.
Zaletą takiego rozwiązanie jest nie tylko możliwość łatwego uzyskania spójnych informacji uwierzytelniających wszystkich użytkowników, ale również rejestracja zdarzeń o znaczeniu krytycznym, takich jak nieudane logowanie, mogących świadczyć o próbach włamania. Za jego pomocą zostało wyeliminowane niebezpieczeństwo podszycia się intruza pod legalnie działającą stację mobilną jak i pod punkt dostępu. Omówione dotychczas mechanizmy nie są jedynymi w walce z atakami polegającymi na przechwytywaniu sesji.

Konieczne stało się również wprowadzenie dodatkowego mechanizmu kontroli integralności zawartości zaszyfrowanych ramek. Poleganie wyłącznie na sumie kontrolnej
(pole ICV w ramce WEP) generowanej przy użyciu algorytmu CRC-32, będącego częścią standardowej implementacji WEP, wydaje się niewystarczające, gdyż słabości tego algorytmu są powszechnie znane. W tym celu dodane zostało pole MIC (Message Integrity Check), którego wartość jest funkcją adresu nadawcy, odbiorcy oraz zawartości ramki. Wartość końcowa uzyskiwana jest jako efekt przeliczenia powyższych informacji za pomocą funkcji haszującej. Samo MIC umieszczone jest wewnątrz ramki i jest szyfrowane za pomocą algorytmu WEP.
W celu sprawdzenia wiarygodności ramki oraz samego nadawcy odbiorca po rozpakowaniu oblicza wartości pola MIC. Jeżeli uzyskany wynik różni się od wartości otrzymanej, ramka jest odrzucana.
Należy się spodziewać, że w miarę rozpowszechniania się technologii sieci bezprzewodowych będzie ujawnianych coraz to więcej luk w mechanizmach opowiadających za bezpieczeństwo, jednocześnie będą tworzone coraz to skuteczniejsze metody blokowania ataków na sieci.

Podsumowując należy stwierdzić, że sieci bezprzewodowe są bardzo ciekawą alternatywą na dzisiejszym rynku technologii sieciowych i pomimo pewnych niedociągnięć w mechanizmach bezpieczeństwa będą zjednywać sobie coraz to większą liczbę użytkowników.