wizjonerzy

Bezpieczeństwo sieci bezprzewodowych

CONFidence 2005 // Kraków // Październik 2005

Agenda

- Sieci bezprzewodowe LAN
  - 802.11b/g
  - 802.11a
- Sieci bezprzewodowe PAN
  - Bluetooth
  - UWB
- Sieci bezprzewodowe PLMN
  - GSM/GPRS/EDGE
  - UMTS
- Operatorskie sieci bezprzewodowe
  - LMDS
  - PDH
  - SDH
- Bezprzewodowe sieci czwartej generacji
  - IEEE 802.16 (WiMAX)
  - IEEE 802.20

Przyszłość

wizjonerzy

Cyfrowo

Bezprzewodowo

Mobilnie

wizjonerzy

802.11a/b/g

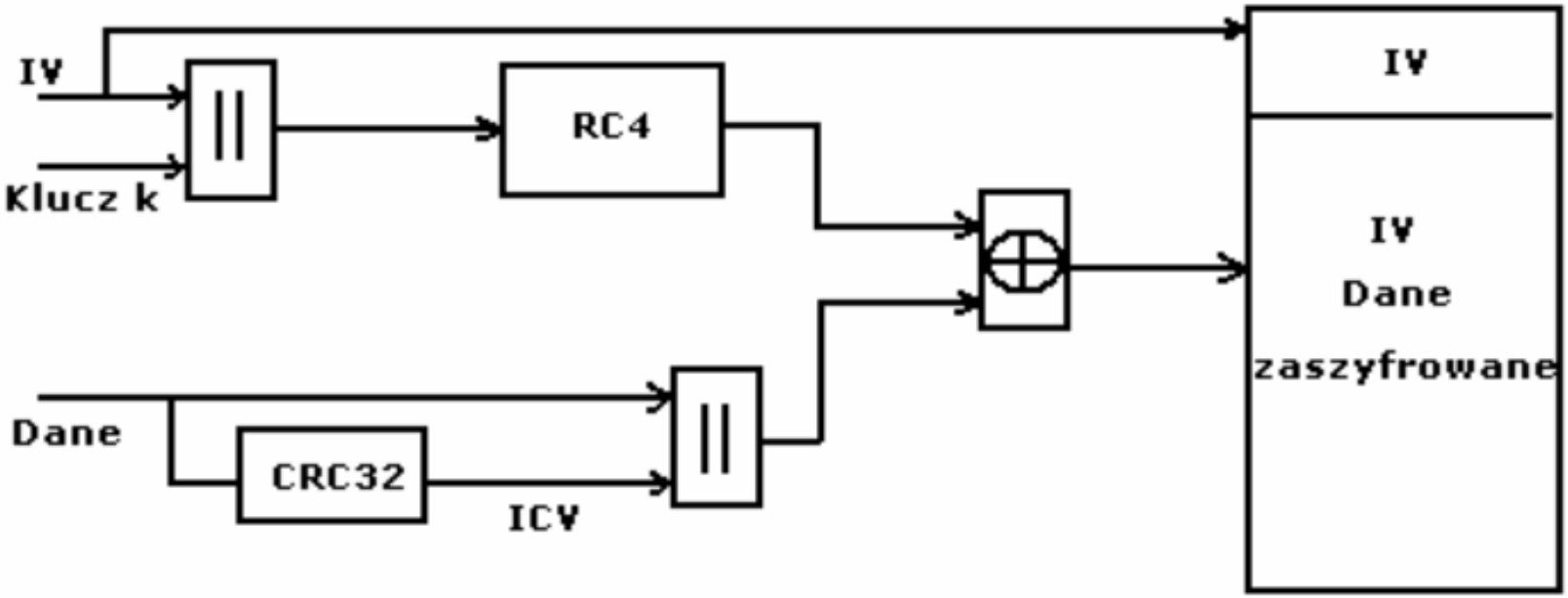
- Częstotliwość pracy 2,4 lub 5 GHz
- Modulacja sygnału CDMA DSSS/CCK, OFDM
- Dostępne protokoły zebezpieczające:

  WEP Wired Equivalent Privacy
  Algorytm RC4
  Klucze 64, 128, 256 bitów

  802.1x
  Mechanizmy uwierzytelniania i dystrybucji kluczy
  EAP, TKIP

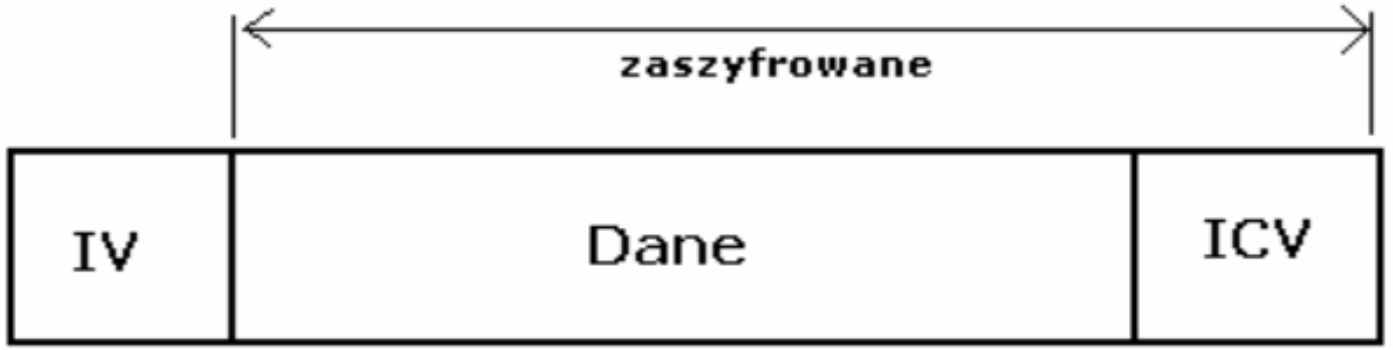
  802.11i
  Algorytm szyfrujący AES

WEP



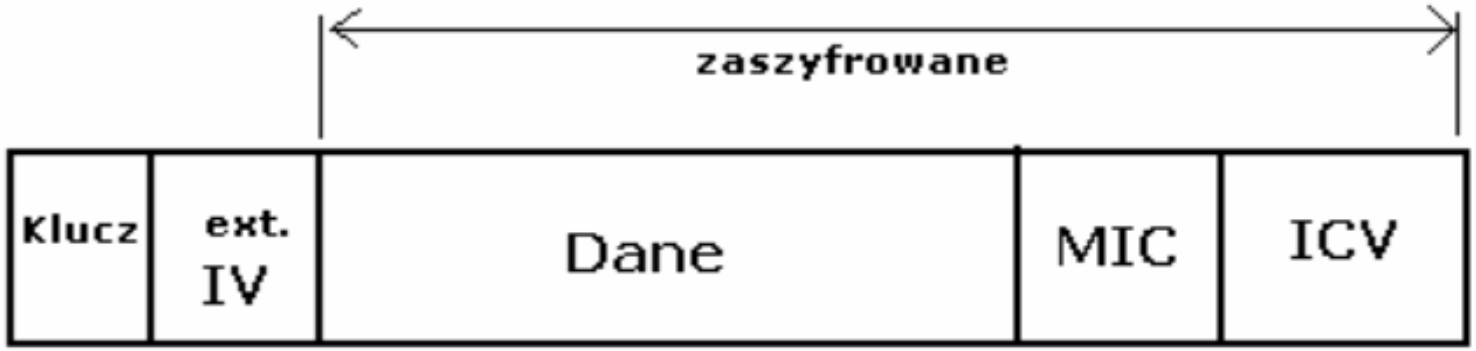
Rys. 1 Schemat blokowy procesu szyfrowania WEP.

WEP



Rys. 2 Ramka zaszyfrowana przy pomocy WEP.

TKIP



Rys. 3 Ramka protokołu TKIP.

wizjonerzy

Porównanie protokołów

Protokół	802.11/WEP	WPA/TKIP	802.11i/CCMP
Szyfr	RC4	RC4	AES
Rozmiar klucza [bity]	40/104	128	128
Czas życia klucza [bity]	24	48	48
Integralność danych	CRC32	Michael	CCM
Integralność nagłówka	-	Michael	CCM
Zarządznie kluczami	-	802.1x	802.1x
Wzajemne uwierzytelnianie	-	802.1x	802.1x
Bajty protokołu na ramkę	8	20	16
Skalowalność	Nie	Tak	tak

Tabela 1. Porównanie protokołów.

wizjonerzy

Bluetooth

- Pasmo pracy: 2400-2483 MHz;
- Metoda wielodostępu: CDMA FHSS
- Kanały: 78 niezachodzących kanałów 1MHz;
- Parametry FHSS: 1600 skoków/s
- Modulacja:GFSK;
- Moc nadajnika: 1-100mW

Bluetooth™

wizjonerzy

Bezpieczeństwo Bluetooth

- Krótki zasięg
- Wykorzystanie szyfru strumieniowego E0
  (podatny na ataki mniej kosztowne niż bruteforce)
- Konieczność każdorazowego uzgadaniania klucza sesji (PIN)
- Możliwość zestawienia połączenia nieszyfrowanego
- Problemy z algorytmem wymiany kluczy
- Jakość klucza inicjalizacyjnego wynika wprost z jakości PINu
  (w dużej ilości urządzeń domyślnie 0000)

Bluetooth™

wizjonerzy

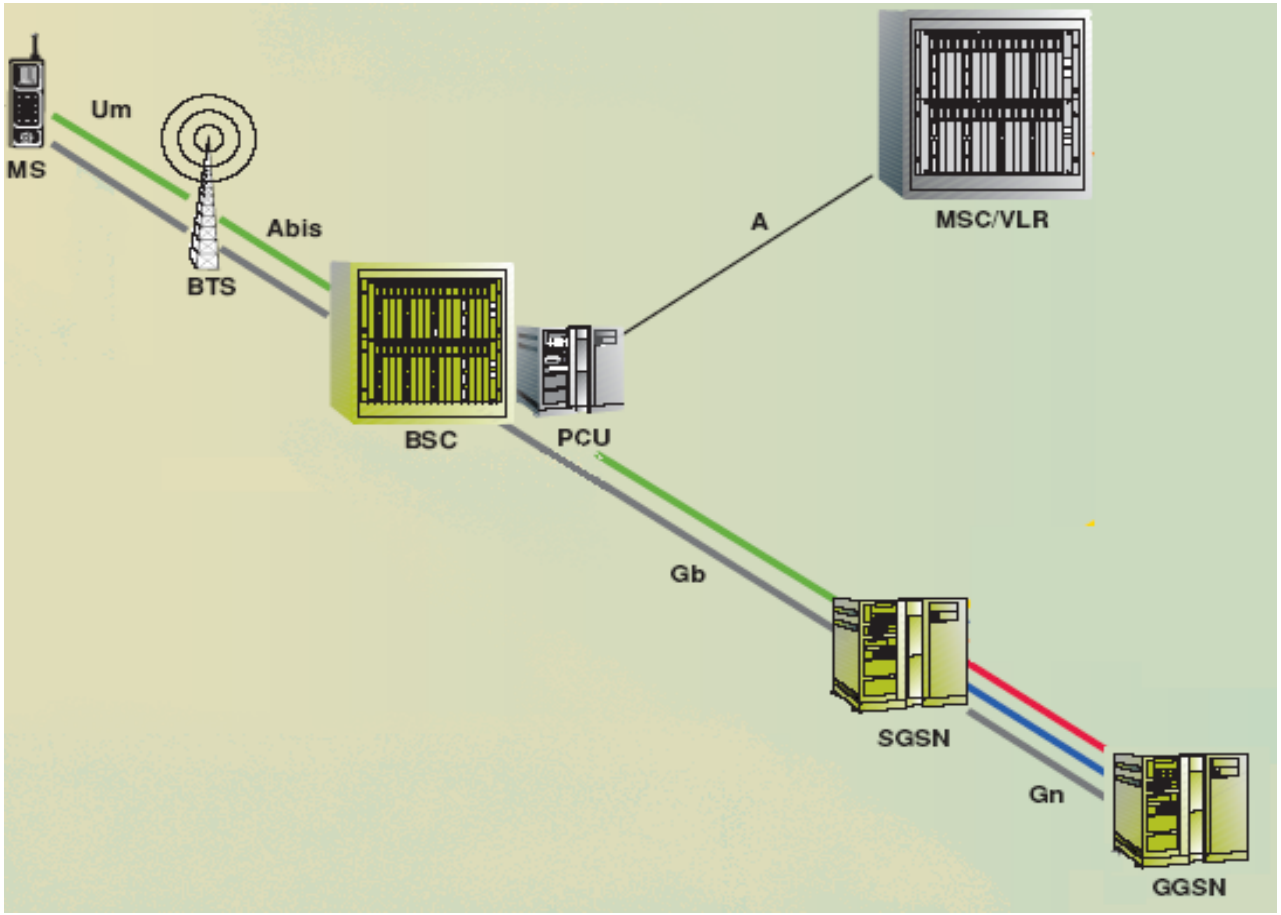
Ultra Wide Band (UWB)

- Pasmo pracy: 3.1 – 10.6 GHz;
- Modulacja: OFDM;
- Zasięg: około 10m
- Przepustowość liczona w setkach Mbps

  (do około 800Mbps, bezprzewodowe USB/bezprzewodowe FireWire)
- Zgodność ze starszymi standardami (Bluetooth)
- Opracowywany standard (IEEE 802.15)

Sieci bezprzewodowe PLMN

GSM/GPRS/EDGE



Sieci bezprzewodowe PLMN

GSM

- Interfejs radiowy szyfrowany
  - Specyfikacja protokołu nie jest ogólnie dostępna
- Pozostałe interfejsy standardowo nie są szyfrowane
  - Dysponując odpowiednio zaawansowanym sprzętem, przechwytywanie sygnalizacji jak i ruchu głosowego nie stanowi problemu.

GPRS/EDGE

- Wszystkie interfejsy szyfrowane
  - Przechwytywanie ruchu GPRS/EDGE jest możliwe na interfejsie Gn pomiędzy SGSN a GGSN. W praktyce oznacza to konieczność uzyskania fizycznego dostępu do SGSN/GGSN ponieważ zwykle są to zintegrowane węzły sieci.

wizjonerzy

UMTS

- **Interfejs radiowy WCDMA**
  Technologia z natury jest niezwykle trudna w podsłuchu, problemem może być nawet sama detekcja obecności sygnału.

- **Wszystkie interfejsy UMTS są szyfrowane**
  Szyfrowane są zarówno dane użytkownika jak i sygnalizacja.

- **Nowe algorytmy szyfrujące**
  Zastosowano znacznie mocniejsze algorytmy szyfrujące niż w GSM.

wizjonerzy

Local Multipoint Distribution System (LMDS)

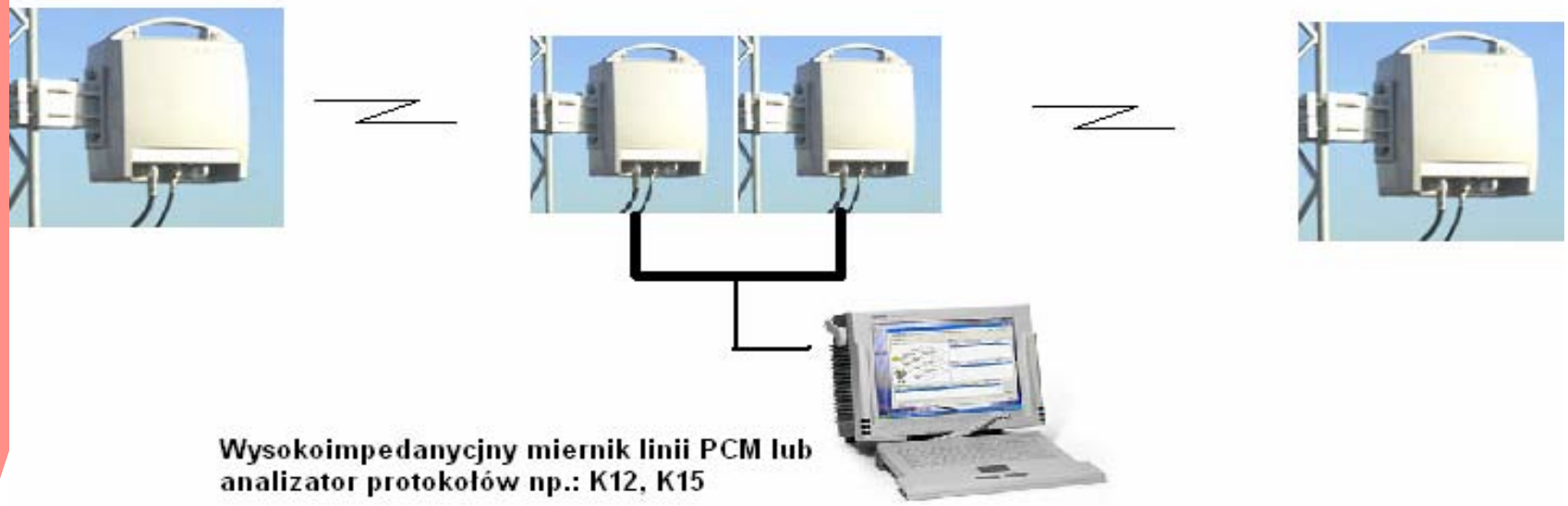
- Częstotliwość 10 – 40Ghz
- Modulacja: QPSK, x-QAM
- Zasięg: do 8km.
- Technologia LOS
- Przepustowość: ok. 34-36Mbps
- Autentykacja i enkrypcja wynikająca z adaptacji protokołu DOCSIS (DOCSIS+)
- Certyfikaty X.509, klucze RSA
- 3DES

PDH (Plesiochronous Digital Hierarchy)

- Częstotliwość 7 – 40 GHz;
- Modulacja zależna od przepustowości;
- Wąska wiązka radiowa;
- Zasięg do 50km;
- Konieczna przejrzystość strefy Fresnela;
- Opóźnienia na łączu zwykle ok. 2-3 ms;
- Topologia punkt-punkt

PDH

Przykładowy schemat przechwytywania strumienia PDH



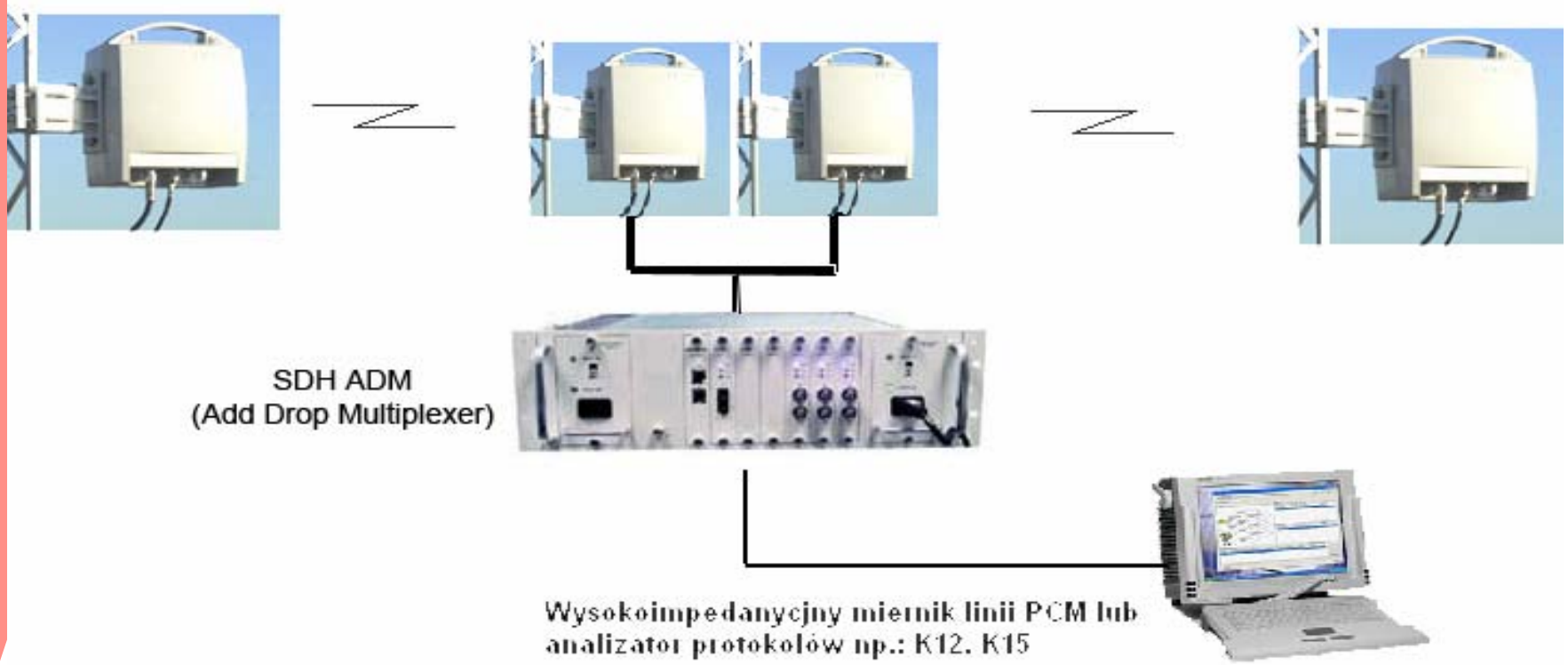
wizjonerzy

SDH (Synchronous Digital Hierarchy)

- Częstotliwość 7 – 40 GHz;
- Modulacja zależna od przepustowości;
- Wąska wiązka radiowa;
- Zasięg do 50km;
- Konieczna przejrzystość strefy Fresnela;
- Opóźnienia na łączu zwykle ok. 2-3 ms;
- Topologia punkt-punkt
- Niektóre produkty implementują proste metody szyfrowania (najczęściej bazowane na DES)

SDH

Przykładowy schemat przechwytywania strumienia SDH



Sieci bezprzewodowe IV generacji

WiMAX jest standardem dla MAN (Metropolitan Area Network)

Historycznie bazuje na założeniach standardów LMDS.

Jego historia zaczęła się w 2001 roku, za sprawą publikacji IEEE.

Początkowo przewidziano dwie wersje systemu:

802.16 pracujący w paśmie 10-66GHz (LOS)

802.16a pracujący w paśmie 2-11GHz (NLOS)

802.16 wspiera zarówno ATM jak i IP.

Sieci bezprzewodowe IV generacji

wizjonerzy

	802.11a	802.11b	802.11g	802.16d
Peak Data Rate	54Mbps	11Mbps	54Mbps	75Mbps
Frequency Band(s)	5GHz	2.4GHz	2.4GHz	2-66GHz
Range	50m	100m	100m	50km
Channel Size(s)	20 MHz	20 MHz	20 MHz	1.5-20MHz
Spectral Efficiency	2.7bps/Hz	0.6bps/Hz	2.7bps/Hz	5bps/Hz
Modulation[1]	OFDM	DSSS	OFDM	OFDM
Quality of Service	No	No	No	Yes
IEEE Certification	1999	1999	2003	2004E

[1]OFDM: Orthogonal Freq. Division Multiplexing, DSSS: Direct Sequence Spread Spectrum.
Source: IEEE, WiMAX Forum, Merrill Lynch.

Sieci bezprzewodowe IV generacji

wizjonerzy

	UMTS	802.20	802.16e
Peak Data Rate	384kbps-2+Mbps	16Mbps @5Mhz[1]	70Mbps @14Mhz
Frequencies	1.8- 2.1GHz	Licensed <3.5Ghz	Licensed 2-6Ghz
Mobility	NA	Up to 250 km/h	20-100 km/h
Channel Size(s)	5MHz	1.25 and 5Mhz	1.5-20MHz
Efficiency	<0.5bps/Hz	3.2bps/Hz	5bps/Hz
Modulation[2]	QPSK	OFDM	OFDM
Certification	2000	2005/6E	2005E

[1] 3.2Mbps @1.25MHz
[2] QPSK: Quadrature Phase Shift Keying
Source: WiMAX Forum.

wizjonerzy

Bezpieczeństwo WiMAX

WiMAX FORUM

- Implementacja DOCSIS (DOCSIS+)
- Obligatoryjne wykorzystanie CCMP

  (Counter Mode with Cipher Block Chaining Message Authetication Code Protocol)
- Szyfrowanie AES
- Większość obecnych na rynku urządzeń zapewnia podstawowe zabezpieczeń w warstwie Ethernet (VLAN, ACL)
- Autentykacja end-to-end z wykorzystaniem EAP (Extensible Authetication Protocol (TLS))

wizjonerzy

Konsekwencje

- Konwergencja ma dwa końce
- Wszystko w IP ułatwia sprawę
- Dużo haseł – jedno hasło
- Kryptografia to nie bezpieczeństwo
- Większe przepustowości - droższe bezpieczeństwo
- Synchronizacja – również zagrożeń
- Konsekwencje dla prywatności

Nadzieja

- Większe przepustowości – mniejszy problem z naddatkami wynikającymi z kryptografii
- Większa wydajność obliczeniowa – możliwość stosowania silniejszej kryptografii
- Słabsze jednostki muszą zginąć ;-)

wizjonerzy

Pytania?

wizjonerzy

Dziękujemy za uwagę!