Bezprzewodowe sieci LAN

Autorzy: Jakub Lewicki, Jacek Mazur IVFDS

STRESZCZENIE

Sieci WLAN stale zyskują na popularności. Pierwsze urządzenia zgodne z normą 802.11b pojawiły się kilka lat temu. W tym roku firmy zaprezentowały pierwsze systemy 802.11a. W przyszłym roku oczekuje się pierwszych produktów zgodnych z 802.11g (Enterasys Networks już oferuje punkt dostępu zgodny z tą normą!). Dwie pierwsze normy nie są ze sobą kompatybilne. 802.11g będzie zgodna z 802.llb, ale nie z 802.11a. Najciekawsze, że tworzona norma IEEE 802.11g będzie uważana za następczynię popularnego standardu 802.11b. Urządzenia zgodne z nową normą umożliwią osiągnięcie przepływności dochodzącej do 54 Mb/s. Ale to jeszcze nie wszystko. Punkty dostępu 802.11g będą wspierały klientów 802.11b i odwrotnie. W ten sposób komputer wyposażony w kartę 802.11g będzie mógł uzyskać dostęp do punktów dostępu 802.11b i g. Pojawiają się też nieformalne zależności w rodzaju a/b > a+b. Wzór ten oznacza, że integracja obydwu norm w krzemie (a/b) jest lepsza od dwu kart w chassis (a+b). Ale świat sieci bezprzewodowych czeka też na dokończenie normy uniwersalnej 802.1X, która umożliwi identyfikowanie klientów przed udzieleniem im praw transmisji w LAN. Procedury identyfikacji przewidują teraz współuczestniczenie: urządzenia klienta, specjalnego serwera identyfikacyjnego RADIUS (obsługującego EAP) i punktu dostępu. Do tej pory bezpieczeństwo nie należało do silnych stron WLAN.

Luki w systemach bezpieczeństwa sieci stoją ciągle na przeszkodzie jeszcze szybszemu rozwojowi systemów IEEE 802.11. Jednak sytuacja nie przedstawia się już tak źle jak jeszcze kilka lat temu. Na rynku pojawiło się już kilka dosyć skutecznych środków chroniących transmisję w sieciach bezprzewodowych. Problem w tym, że są one relatywnie drogie, na ogół trudne w zarządzaniu, a nade wszystko niestandardowe.

W 2001 r. udowodniono słabość algorytmu WEP *(Wired Equivalent Privacy).*

SPIS TREŚCI

1. WSTĘP

WLAN (Wireless LAN) - bezprzewodowe sieci LAN - są elastycznym systemem komunikacyjnym, który może służyć do wymiany danych między komputerami przenośnymi lub stanowić uzupełnienie tradycyjnych sieci LAN - opartych na okablowaniu miedzianym (albo światłowodach), łącząc się z takim środowiskiem za pośrednictwem specjalnych urządzeń. Transmisja danych odbywa się za pośrednictwem fal elektromagnetycznych, a rolę okablowanie przejmują: interfejs bezprzewodowy i niewielka antena. Sieci WLAN oznaczają mobilność i możliwość zwiększenia efektywności pracy w wielu istotnych obszarach przemysłowych, w edukacji i służbach publicznych (np. w lecznictwie). Bezprzewodowe sieci LAN (WLAN) umożliwiają połączenia z systemem informatycznym przy użyciu fal radiowych, co eliminuje konieczność wykonywania podłączeń fizycznych sieci komputerowej czy gniazdka telefonicznego.

Poważnym problemem dotyczącym tego środowiska jest bezpieczeństwo pracy. Opracowano już stosowne protokoły kodujące dane i uwierzytelniające użytkowników dzięki czemu włamania do takich sieci nie są wcale takie łatwe.

Rozwój sieci WLAN jest dynamiczny, o czym może świadczyć fakt. że obroty na tym rynku wyniosły na świecie w 2000 r. 1,1 mld USD. a przewidywania na rok 2005 to kwota 3.2 mld USD. WLAN jest systemem telekomunikacyjnym pozwalającym przesyłać dane drogą radiową w trybie peer-to-peer (na przykład na linii PC-PC, PC-hub lub drukarka-hub) i w trybie point-point (na przykład LAN-LAN). Sieci WLAN umożliwiają poprawną pracę tradycyjnych aplikacji: transfer plików, e-mail, Internet czy dostęp do baz danych.

Sieci WLAN pracują w oparciu o dwa podstawowe elementy: karty sieciowe (wbudowywane najczęściej na stale do komputerów przenośnych) i punkty dostępu/mosty. Karty sieciowe gwarantują interfejs między końcowym urządzeniem użytkownika i anteną, która wysyła/odbiera dane do/z punktu dostępu. Punkty dostępu pełnią rolę nadajników/odbiorników między siecią bezprzewodową a siecią bezprzewodową. [1]

2. ZALETY SIECI WLAN

1. Mobilność – oznacza większą efektywność pracy, pozwala świadczyć lepsze usługi oraz dostęp do informacji przechowywanych w tradycyjnej sieci LAN funkcjonującej w przedsiębiorstwie.

2. Łatwość instalowania i prostota obsługi - sieci WLAN można łatwo i szybko instalować, nie przeciągając żadnych kabli przez ściany i sufity.

3. Elastyczność instalacji - technologia WLAN umożliwia rozbudowę sieci do tych miejsc, do których sieci kablowe nie mają dostępu.

4. Obniżenie kosztów posiadania – pomimo początkowych kosztów inwestycji związanych z zakupem sprzętu do sieci WLAN, które mogą przekroczyć inwestycje poniesione na tradycyjną sieć przewodową - całkowite koszty instalacji i utrzymania w ruchu mogą być jednak znacząco niższe.

5. Skalowalność – sieci WLAN umożliwiają zastosowanie różnych topologii - tak aby spełniały wymagania określonych aplikacji. Konfigurację sieci WLAN można szybko i łatwo zmienić, zastępując niewielką sieć, składającą się z kilkunastu użytkowników, rozbudowaną siecią obsługującą setki użytkowników i mającą dużo większy zasięg. [1]

3. SIECI WLAN A INNE TECHNOLOGIE BEZPRZEWODOWE

Użytkownicy sieci WLAN mogą budować zarówno niezależne sieci (komunikacja typu *peer-to-peer* między poszczególnymi komputerami przenośnymi), jak i sieci infrastrukturalne, oferujące wszystkie funkcje, jakie są dostępne w kablowych sieciach LAN. Rozwiązania bezprzewodowe punkt-punkt, takie jak mosty LAN-LAN czy połączenia PAN *(Personal Area Network),* mogą czasami obsługiwać te same aplikacje, które są uruchamiane w sieciach LAN.

Sieci WLAN oferując wszystkie funkcje realizowane przez tradycyjne sieci LAN eliminują jednocześnie konieczność instalowania skomplikowanego okablowania.

Most bezprzewodowy LAN-LAN jest alternatywą względem technologii kablowych, łącząc ze sobą dwa budynki. Bezprzewodowa sieć PAN o zasięgu kilku metrów wystarcza do wymiany danych między komputerem a lokalnymi urządzeniami peryferyjnymi. Należy pamiętać aby nie mylić sieci WLAN z sieciami WMAN *(Wireless* MAN) i z sieciami WWAN *(Wireless* WAN) realizującymi inne zadania. Sieci WMAN i WWAN do poprawnego funkcjonowania potrzebują wybudowania kosztownej infrastruktury, pracują przy tym dużo wolniej.

Tabela 1.

Rodzaj sieci	WLAN *(Wireless Local Area Network)*	WPAN *(Wireless Personal Area Network)*	Most LAN-LAN	WMAN *(Wireless Metropolitan Area Network)*	WWAN *(Wireless Witle Area Network)*
Zasięg	Pojedynczy budynek	2-3 m	Komunikacja miedzy budynkami	Sieci metropolitarne	Cale miasto, województwo lub większy obszar
Zastosowanie	Rozszerzenie sieci LAN lub zastąpienie jej siecią WLAN	Rozwiązanie alternatywne bez użycia kabli	Rozwiązanie alternatywne bez użycia kabli	Rozszerzenie sieci LAN	Rozszerzenie sieci LAN
Typowa przepustowość	1-10 Mb/s (i więcej)	0,1-4 Mb/s	2-1 00 Mb/s	10-1 00 kb/s	1-32 kb/s

RadioLAN - bez standardów, ale za to wydajnie

Ciekawym aspektem rozważań nad sieciami WLAN jest technologia RadioLAN – wyjątkowo wydajnie pracująca sieć, która nie spełnia wymagań stawianych przez standard 802.11. RadioLAN wykorzystuje nietypową częstotliwość (5.8 GHz) i może przesyłać pakiety z szybkością 10 Mb/s, czyli teoretycznie pięć razy szybciej niż sieci zgodne ze standardem 802.11. W praktyce sieć ta nie pracuje tak szybko, ale przy odległości 1.5 m (użytkownik-punkt dostępu) osiąga rzeczywiście przepustowość 4.39 Mb/s. Jednak wraz z wzrostem odległości między użytkownikiem a punktem dostępu przepustowość spada bardzo szybko. W odległości 11 m od punktu dostępu przepustowość spada do poziomu 1.88 Mb/s i tylko 30 procent ramek jest wtedy przesyłana od razu bezbłędnie. W technologii RadioLAN stosuje się bardzo duże anteny, co nie jest zgodne z ideą przenośności. Przepustowość ulega zmianie po zmianie kąta ustawienia anteny. Sieci RadioLAN działają przeciętnie około 50 proc. szybciej (przy założeniu odległości 11m), niż sieci standardu 802.11. Jeśli użytkownik zdecyduje się zainstalować dodatkowe punkty dostępu, odległość pomiędzy punktami ulegnie zmniejszeniu a przepustowość może osiągnąć poziom 4 Mb/s. Mimo stosowania tak dużych anten maksymalny zakres tej sieci wynosi 20 m. Z tego powodu rozwiązanie to nie nadaje się do implementowania w dużych budynkach, chyba że zainstalujemy wiele punktów dostępu,

jednak powoduje to wyższe koszty. Główną wadą sieci RadioLAN jest niewielki zasięg; natomiast najważniejszą zaletą duża przepustowość przy niewielkim oddaleniu użytkownika od punktu dostępu. RadioLAN może zatem stanowić dobre rozwiązanie na przykład dla niewielkiego biura. [1]

4. DROGA DO SZYBKICH SIECI BEZPRZEWODOWYCH

Litery po cyfrach wskazują na kolejność, w jakiej standardy były proponowane, a nie kolejność, w jakiej pojawiały się później na rynku - dlatego produkty 802.11b pojawiły się przed produktami 802.11a. Pierwszy standard dla sieci bezprzewodowych (802.11) został zaakceptowany przez organizację IEEE *(Institute of Electrical and Electronics Engineers)* w 1997 r. - pozwala przesyłać dane z szybkością do 2 Mb/s.

W 1999 r. IEEE zaaprobowała standardy: 802.11a i 802.11b.

Standard 802. l la to szybkość 54 Mb/s i częstotliwość 5 GHz. Metoda modulacji OFDM *(Orthogonal Frequency Dwision Multiplexing).*

Standard 802.11b (inna nazwa Wi-Fi) to szybkość do 11 Mb/s i częstotliwość 2.4 GHz. Metoda modulacji DSSS *(Direct Sequence Spread Spectrum).*

Metoda DSSS jest łatwiejsza do implementowania niż OFDM. Dlatego właśnie produkty 802.11b pojawiły się najpierw - pod koniec 1999 r. Produkty działające w standardzie 802.11b zaczęły się pojawiać w przedsiębiorstwach, w małych i domowych biurach (SOHO), w domach i w miejscach publicznych (tzw. *hot spot* Wi-Fi).

Produkty, które mają logo Wi-Fi są zgodne ze standardem 802.11b i posiadają certyfikat wydawany przez stowarzyszenie WECA *(Wireless Ethernet Compatibility Alliance).*

Obecnie WECA pracuje nad certyfikatem zgodności dla produktów 802.11a. Produkty, które przejdą testy, będą traktowane jako zgodne z Wi-Fi5.

Amerykańska komisja do spraw telekomunikacji - FCC *(Federal Communications Commission)* - zapowiedziała nowe uregulowania zezwalające na dodatkowe modulacje w zakresie 2,4 GHz. Umożliwi to IEEE rozszerzenie specyfikacji 802.11b, tak aby można było stosować większe szybkości.

Powstanie standard 802.11g : szybkość do 54 Mb/s, częstotliwość 2,4 GHz i metoda modulacji OFDM, będzie się charakteryzować wsteczną zgodnością ze specyfikacją 802.11b. [1]

5. STANDARDY WLAN

Standard IEEE 802.11b wykorzystuje częstotliwość 2,4 GHz, tę samą co sieci HomeRF. Szybkość pezsyłu danych w sieci 802.11b wynosi 11 Mb/s, w HomeRF l Mb/s (z możliwością rozszerzenia do 10 Mb/s). Zauważalny jest jednak spadek obrotów na rynku HomeRF gdyż użytkownicy decydują się na standard 802.11b - sieci tego standardu są tańsze.

Rozwiązanie Bluetooth należy zaliczyć do sieci osobistych PAN *(Personal Area Network)* i nie traktować tej technologii jak standardu WLAN. Bluetooth zaprojektowano jako standard przesyłania danych na krótkie odległości (na przykład synchronizując dane między komputerami osobistymi i obsługując komunikację między komputerem osobistym a urządzeniami peryferyjnymi).

Wsparcie Windows 2000 i Windows XP dla sieci WLAN

Windows 2000 wspiera na różne sposoby bezprzewodowe sieci LAN. Windows 2000 wykrywa obecność sieci WLAN natomiast stos komunikacyjny TCP/IP zaprojektowano z myślą o użytkowniku aby ten mógł łatwiej przemieszczać się między punktami dostępu, nie tracąc połączenia *z* systemem. Interfejs NDIS systemu operacyjnego Windows 2000 NDIS obsługuje bezprzewodowe adaptery i ich sterowniki. System operacyjnym Windows 2000 zawiera kilka sterowników dla sieci WLAN, a większość bezprzewodowych urządzeń LAN jest dostarczana ze sterownikami dla systemu Windows 2000. Bezprzewodowe urządzenia wspierane przez system Windows 2000 są wyposażone w zabezpieczenia oparte na jakiejś postaci współdzielonego klucza lub na standardzie WEP *(Wired Equivalent Prńracy).*

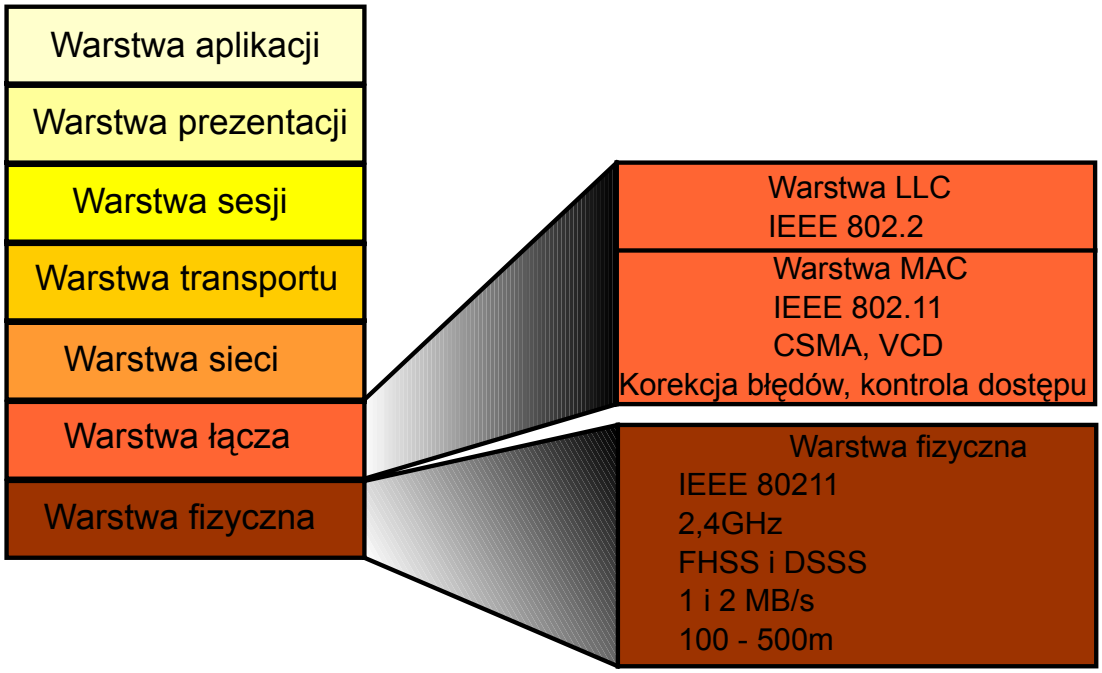
System operacyjny Windows XP ułatwia zarządzanie urządzeniami bezprzewodowymi, ponieważ zawiera wsparcie dla standardu IEEE 802.1X.

Wi-Fi

Wi-Fi(*wireless fidelity)* to inne określenie standardu IEEE 802.11b. WECA wymyśliła ten termin jako symbol handlowy ułatwiający identyfikację standardu. Dla dodatkowego porównania dodać można, że relacja między Wi-Fi a 802.11 jest taka sama jak między Ethernetem a standardem IEEE 802.3. Certyfikat Wi-Fi oznacza zgodność z wszystkimi innymi produktami mającymi taki certyfikat – niezależnie od producenta. Użytkownik, posiadając urządzenie Wi-Fi, może się łączyć z dowolnym punktem dostępu spełniającym wymogi Wi-Fi.

Standard 802.11

Standard 802.11 jest całą rodziną specyfikacji opracowanych przez IEEE. Opisuje technologie stosowane w środowisku bezprzewodowych sieci LAN. 802.11 określa sposób przesyłania danych za pomocą fal radiowych między bezprzewodowym klientem (np. notebookiem) a stacją bazową lub między dwoma bezprzewodowymi klientami. Standard 802.11 został zaakceptowany przez organizację IEEE w 1997 r.



Rys 5.1 Sieci bezprzewodowe LAN standardu IEEE 802.11 [1]

Standard 802.11 zawiera:

Specyfikacja 802.11 - opisuje działanie sieci WLAN przesyłających dane z szybkością l lub 2 Mb/s, używając częstotliwości 2,4 GHz i metod modulacji FHSS *(Frequency Hopping Spread Spectrum)* lub DSSS *(Direct Sequence Spread Spectrum}*.

Specyfikacja 802.11a - opisuje działanie sieci WLAN przesyłających dane z szybkością 54 Mb/s - wykorzystując częstotliwość 5 GHz.

802.11a używa techniki kodowania OFDM *(Orthogonal Frequency Division Muliplexing),* a nie FHSS czy DSSS. Standard 802.11a cechuje się dwiema podstawowymi zaletami w porównaniu ze standardem 802.11b: szybkość wzrasta do 54 Mb/s oraz wzrasta liczba nie zachodzących na siebie kanałów. W przypadku częstotliwości 5 GHz (pasmo UNII – *Unlicensed National Information Infrastructure)* mamy trzy subpasma:

UNII l (5.15-5.25 GHz),

UNII2 (5.25-5.35 GHz),

UNII3 (5725-5.825 GHz).

Używając UNII1 i UNII2 można uzyskać do ośmiu nie zachodzących na siebie kanałów.

W przypadku częstotliwości 2,4 GHz są to trzy kanały. Ogólna szerokość pasma dostępna przy 5 GHz jest też większa niż przy 2,4 GHz (przy 2,4 jest to 83,5 MHz, a przy 5 GHz - 300 MHz.

Jeżeli chodzi o zgodność i pokrywany obszar:

Ponieważ oba standardy pracują na innych częstotliwościach, produkty 802.11a i 802.11b nie są ze sobą zgodne. Punkt dostępu 2,4 GHz 802.11b nie może współpracować z kartą sieciową 5 GHz 802.11a. Oba standardy mogą być jednak stosowane w tym samym systemie informatycznym. Użytkownicy 802.11a i 802.11b mogą korzystać z różnych punktów dostępu, które są podłączone do tej samej sieci LAN.

Wyższa częstotliwość używana przez 802.11a oznacza mniejszy zasięg. Dlatego w przypadku standardu 802.11a. w porównaniu ze standardem 802.11, trzeba stosować więcej punktów dostępu, aby pokryć ten sam obszar. Standard 802.11a to jednak duży postęp. Testy wykazują, że sieci te pracują w typowych warunkach trzy razy wydajniej niż sieci 802.11b.

Specyfikacja 802.11b (802.11 *High Rate* lub Wi-Fi) - opisuje działanie sieci WLAN przesyłających dane z szybkością 11 Mb/s (z możliwością przechodzenia na niższe szybkości: 5.5, 2 lub l Mb/s), wykorzystując częstotliwość 2.4 GHz. Specyfikacja 802.11b używa tylko techniki DSSS i była ratyfikowana w 1999 r.

Specyfikacja 802.11g (w trakcie aprobowana) - opisuje działanie sieci WLAN pracujących z szybkością od 11 do 54 Mb/s (z wykorzystaniem częstotliwości 2.4 GHz). Standard 802.11g to wyższa szybkość i zgodność wsteczna z produktami 802.11b. Sieci 802.11g używają tej samej częstotliwości (2.4 GHz) i tej samej metody modulacji (DSSS) co sieci 802.11b.

Karta sieciowa 802.11g będzie pracować z punktem dostępu 802.11b, a punkt dostępu 802.11g będzie pracować z kartą sieciową 802.11b. przesyłając dane z szybkością do 11 Mb/s. Standard przewiduje też możliwość stosowania modulacji OFDM/CCK, zwiększając tym samym efektywność pracy instalacji 802.11g. Ta technologia pozwala przesyłać dane szybciej, ale ogólna dostępna szerokość pasma przy częstotliwości 2,4 GHz pozostaje taka sama ponieważ liczba kanałów w przypadku 802.11g jest ograniczona do trzech (przy 5 GHz dostępnych jest osiem kanałów).

HiperLAN2

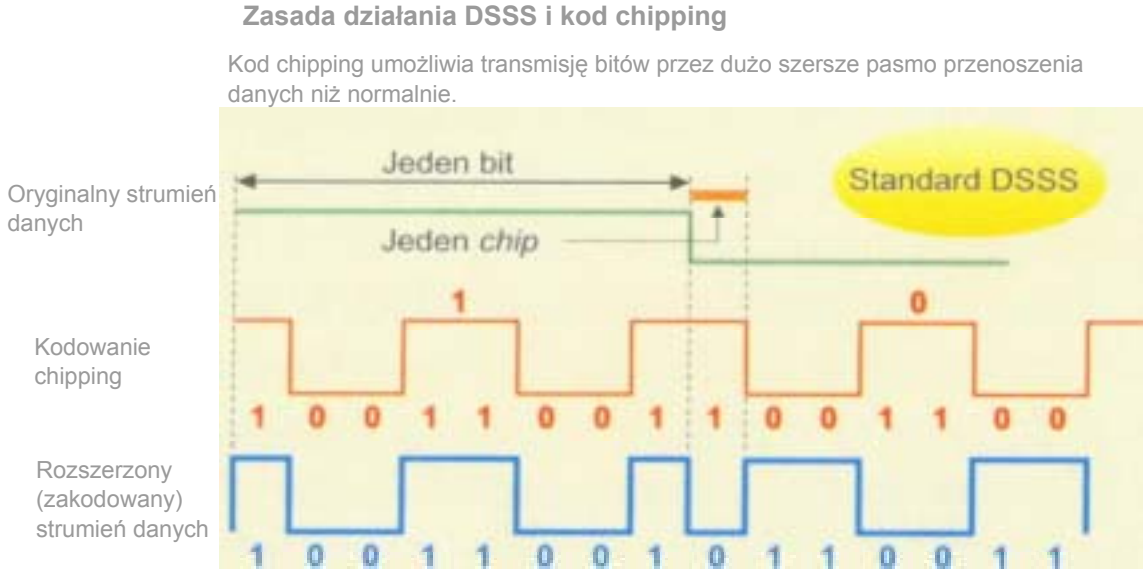
Standard HiperLAN/2 jest promowany przez ETSI *(Eumpean Telecommunications Standards Institute)*. Ponieważ standard HiperLAN/2.s wspiera technologię ATM, sieci HiperLAN/2.s mogą współpracować z sieciami trzeciej generacji (3G) – tego nie potrafią sieci WLAN 802.11a. HiperLAN2 jest jednym ze standardów nowej generacji, które obsługują zarówno dane asynchroniczne jak i usługi krytyczne, jeśli chodzi o czas (pakiety zawierające głos i wideo), wymagające przestrzegania reguł QoS. Jeśli chodzi o warstwę fizyczną, standard HiperLAN2 jest bardzo podobny do standardu 802.11 - aby osiągnąć odpowiednią szybkość, oba używają technologii OFDM. Warstwa MAC *(Media Access Control)* jest już jednak całkowicie inna, jeśli chodzi o sposób, w jaki są formowane pakiety i jak są adresowane urządzenia. Od strony technicznej standard 802.11 to rzeczywisty bezprzewodowy Ethernet, natomiast HiperLAN2 to raczej bezprzewodowy ATM *(Asynchronous Transfer Modę)*. HiperLAN2 współdzieli kanały o szerokości 20 MHz wykorzystując częstotliwość 5 GHz i używając technologii TDMA *(Time Dwision Muttiple Access),* udostępniając w ten sposób usługi QoS za pomocą mechanizmu podobnego do ATM. Główną zaleta tego standardu (w porównaniu ze standardem 802.11h) jest możliwość zagwarantowania wybranym użytkownikom określonej przepustowości.

Standard HiperLAN2 opiera się na topologii stosowanej w telefonach komórkowych i obsługuje dwa podstawowe tryby pracy: scentralizowany i bezpośredni. Tryb scentralizowany jest stosowany w telefonii komórkowej, gdzie każda komórka radiowa jest kontrolowana przez punkt dostępu pokrywający określony obszar geograficzny. W tym trybie mobilny terminal komunikuje się z innym mobilnym terminalem lub ze szkieletem sieci przez punkt dostępu. Ten tryb jest stosowany głównie przez aplikacje biznesowe, które muszą działać na większych geograficznie obszarach. Tryb bezpośredni jest stosowany do tworzenia *ad-hoc* topologii sieciowej - głównie chodzi o środowisko domowe - gdy komórka radiowa pokrywa cały obszar. W tym trybie mobilne terminale zlokalizowane w obszarze jednej komórki mogą wymieniać między sobą dane bezpośrednio. [1]

6. METODY MODULACJI

Modulacja DSSS *(Direct Sequence Spread Sprectrum)* jest technologią rozszerzonego widma z bezpośrednim szeregowaniem bitów. Strumienie danych są tu rozdzielane przy transmitowaniu z wykorzystaniem specjalnych bitów (zwanych bitami szumów), a odbiornik musi dysponować układem deszyfrującym (który wykorzystuje tzw. *chipping code,* interpretując w odpowiedni sposób poszczególne strumienie danych).

Proces polega na rozbiciu informacji na wiele „pod-bitów" (pod-bit to *chip,* nazwany tak od wspomnianego powyżej mechanizmu szyfrowania). Taka operacja umożliwia transmisję pakietów przy użyciu dużo szerszego pasma przenoszenia danych niż w przypadku normalnej transmisji. Standard wymaga, aby współczynnik poszerzenia wynosił 1:10.



Rys 6.1 Tak pracuje DSS i kog chipping [1]

Modulacja FHSS *(Frequency Hopping Spread Spectrum)* polega na tym, że strumienie danych są przełączane z jednej częstotliwości na drugą, pozostając na każdej z nich (przy czym każda taka częstotliwość to oddzielny kanał komunikacyjny) nie dłużej niż 100 ms.

Modulacja OFDM *(Ortbogonal Frequency Diuision Multiplexing)* została zoptymalizowana, pod kątem transmisji danych w środowiskach pełnym zakłóceń, takich jak zatłoczone obszary miejskie. Właśnie dlatego OFDM pracuje niezawodnie i nie ma tych ograniczeń i wad (chodzi o odległości, odporność na zakłócenia, łatwość instalowania i rozmiary anteny), które towarzyszą innym systemom łączności bezprzewodowej).

Rozważania o częstotliwościach

Urządzenia WLAN transmitują i odbierają dane przy użyciu fal radiowych. Jednocześnie może przebiegać wiele transmisji i żadna z nich nie interferuje z inną, jeśli fale radiowe są transmitowane na różnych częstotliwościach zwanych kanałami. W celu wyodrębnienia danych, odbiornik radiowy dostraja się do jednego kanału, odrzucając wszystkie inne sygnały radiowe. Produkty WLAN korzystają z określonych pasm częstotliwości (np. 2,4 GHz w

przypadku standardu 802.11 b i 5 GHz w przypadku 802.11 a). Aby przesyłać informacje przez fale radiowe, urządzenia WLAN muszą nakładać transmitowane dane na falę radiową, zwaną falą nośną, ponieważ jest ona nośnikiem danych – tutaj następuje proces modulacji. Opracowano różne metody modulacji a każda ma swoje wady oraz zalety. Modulacje DSSS są używane przez standard 802.11 b, a modulacje OFDM przez standard 802.11 a. Częstotliwości i metody modulacji definiuje warstwa fizyczna (PHY) standardu IEEE. [1]

7. JAK PRACUJĄ SIECI WLAN?

Sieci WLAN to transmisji danych używają fal elektromagnetycznych (radiowych lub z zakresu podczerwieni). W ten sposób bez konieczności zaprzątania sobie głowy fizycznymi połączeniami dane są przenoszone z jednego punktu do drugiego. Fale radiowe są często określane jako nośnik radiowy, gdyż pełnią proste zadanie - dostarczają energię do odległego odbiornika. Dane gotowe do transmisji są nakładane na nośną radiową, tak aby mogły być dokładnie wyodrębnione przez stację końcową. Ten proces nosi nazwę modulacji nośnej przez transmitowaną informację. Gdy dane zostaną nałożone na nośną radiową, sygnał radiowy zajmuje więcej niż pojedynczą częstotliwość, ponieważ częstotliwość lub szybkość bitowa zmodulowanej informacji dodaje się do nośnej.

W przypadku gdy fale radiowe są transmitowane w tym samym obszarze na różnych częstotliwościach, w tym samym czasie możemy mieć do czynienia z wieloma nośnymi radiowymi, a żadna z nich nie zakłóca pozostałych nośnych. Poprawne wyodrębnienie danych przez odbiornik wymaga wyboru jednej częstotliwości, odrzucając wszystkie inne sygnały na innych częstotliwościach. Typowa konfiguracja WLAN nadajnik/odbiornik (nazywany punktem dostępu) łączy się z siecią kablową, używając standardowego okablowania ethernetowego. Wówczas rola punktu dostępu to: odbieranie, buforowanie i transmitowanie danych między siecią WLAN a siecią kablową. Pojedynczy punkt dostępu może obsługiwać niewielką grupę użytkowników i może wysyłać sygnały na odległość 30-500 m. Użytkownicy końcowi uzyskują dostęp do sieci WLAN za pomocą bezprzewodowych adapterów LAN instalowanych w komputerach przenośnych.

Bluetooth

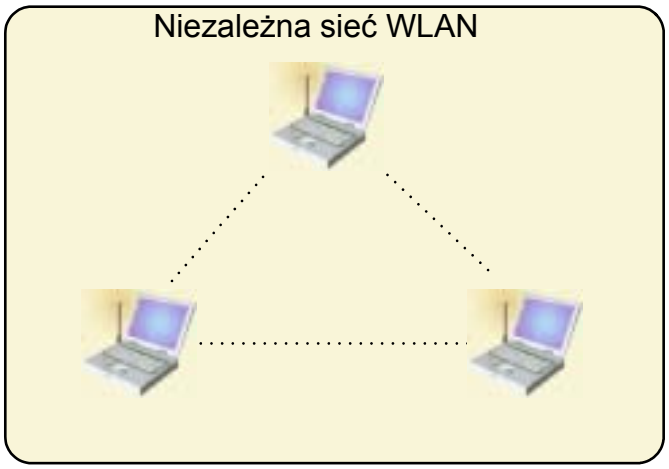
Jest to technologia używana do budowania sieci WPAN *(Wireless PersonalArea Network).* Zyskuje ona ostatnio na popularności i jest stosowana w wielu urządzeniach ponieważ jej zaletą jest współpraca sieci WPAN z większością rozwiązań LAN. Systemy bezprzewodowe oparte na specyfikacji Bluetooth przesyłają dane z szybkością 1Mb/s. Bluetooth to idealne zastosowanie w projektowaniu tanich radiowych systemów bezprzewodowych, które mogą być używane do łączenia ze sobą komputerów przenośnych i innych przenośnych urządzeń. [1]

8. KONFIGURACJE SIECI

Niezależne sieci WLAN

Podstawowa konfiguracja sieci WLAN to niezależna sieć WLAN (*peer-to-peer)* łącząca grupę komputerów osobistych bezprzewodowymi adapterami. Zzwsze gdy dwa lub więcej bezprzewodowych adapterów znajduje się w tym samym obszarze wzajemnego oddziaływania, to komputery takie mogą utworzyć niezależną sieć WLAN. Sieci takie (nazwijmy je *on demand)* nie wymagają przeważnie administrowania czy też wstępnego konfigurowania.

Punkty dostępu rozszerzają zasięg działania sieci peer-to-peer pełniąc rolę repeatera – podwajając odległość, na jaką się mogą komunikować ze sobą bezprzewodowe komputery osobiste.

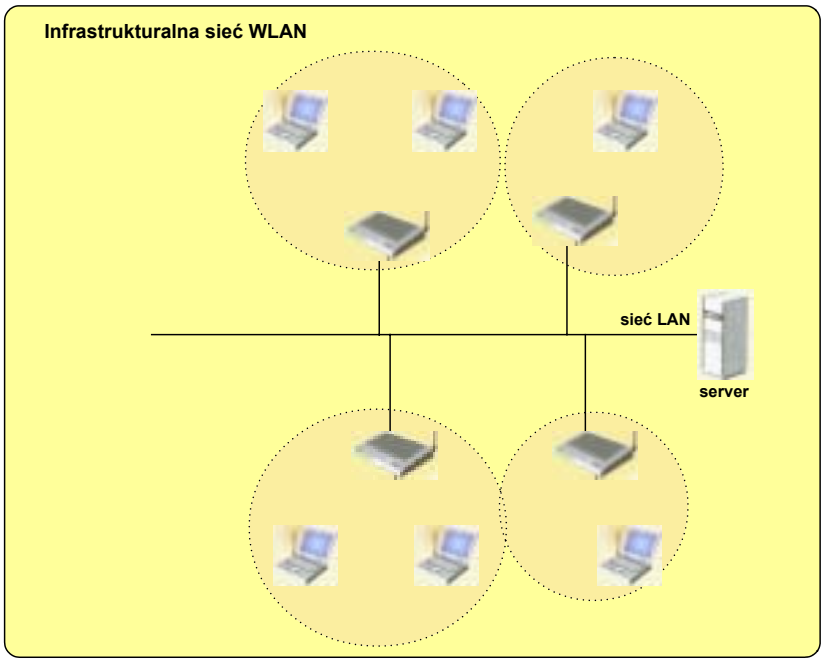


Rys 8.1 Niezależna sieć WLAN [1]

Rys 8.2 Niezależna sieć WLAN z punktem dostępu [1]

Infrastrukturalne sieci WLAN

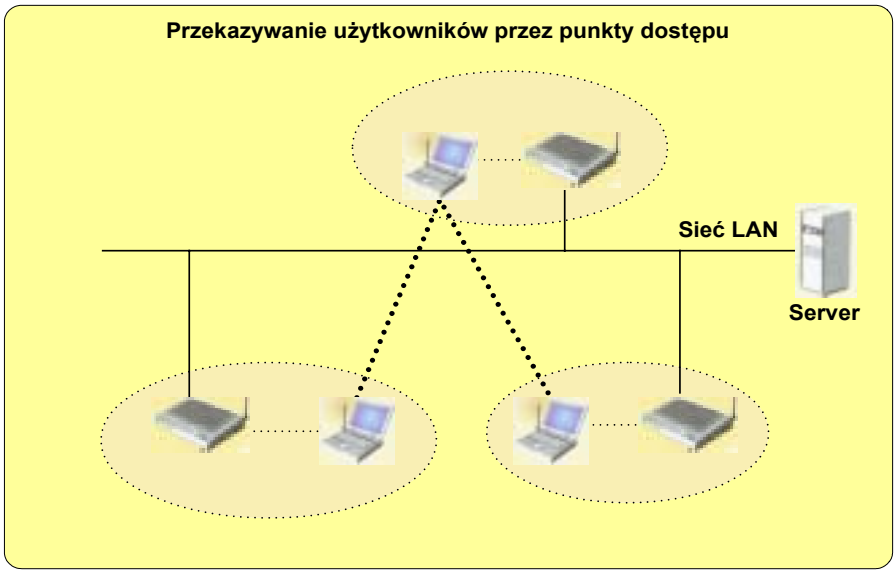
Sieci WLAN w konfiguracji infrastrukturalnej łączą sieć WLAN z siecią kablową przy pomocy wielu punktów dostępu. Użytkownicy komputerów przenośnych mogą wtedy korzystać ze wszystkich zasobów kablowej sieci LAN, a punkty dostępu pozwalają łączyć się z siecią LAN z dowolnego miejsca budynku, biura czy przedsiębiorstwa.



Rys 8.3 Infrastrukturalna sieć WLAN [1]

Mikrokomórki i mobilność

To co cechuje komunikację mobilną to zasięg zależny od tego na jaką odległość można transmitować sygnały dysponując określoną mocą nadawczą. Sieci WLAN używają komórek nazywanych mikrokomórkami działających podobnie jak te w systemach telefonii bezprzewodowej. Przenośny komputer z adapterem WLAN komunikuje się z jednym punktem dostępu, który działa w obszarze określonej mikrokomórki. Indywidualne mikrokomórki zachodzą na siebie, dzięki czemu komputer przenośny będący w ruchu nigdy nie traci łączności z kablową siecią LAN. Jeśli komputer jest przenoszony poza obszar działania jednego punktu dostępu (mikrokomórka), pieczę nad nim przejmuje następny punkt dostępu.



Rys 8.4 Przekazywanie użytkowników przez punkty dostępu [1]

9. BEZPIECZEŃSTWO

Ponieważ ogólnodostępne narzędzia, takie jak AirSnort czy WEPcrack pozwalają włamać się do sieci bezprzewodowej tak samo jak do każdej innej sieci LAN, dlatego bardzo ważną kwestią jest bezpieczeństwo sieci WLAN.

WEP – skrót ten oznacza *Wired Equivalent Privacy ,* jest to protokół bezpieczeństwa opracowany dla bezprzewodowych sieci LAN, wchodzący w skład standardu 802.l1b. Protokół ten został tak zaprojektowany, aby zapewnić sieciom WLAN taki sam poziom bezpieczeństwa, jaki jest stosowany w tradycyjnych sieciach LAN. Jednak sieci LAN są z natury chronione lepiej, ponieważ są sieciami kablowymi i aby się do nich dostać, trzeba sforsować ich strukturę fizyczną lub podłączyć się do nich. Sieci WLAN natomiast wykorzystują fale radiowe. WEP zapewnia bezpieczeństwo poprzez szyfrowanie danych przesyłanych drogą radiową. Nie zapewnia on jednak stuprocentowego bezpieczeństwa. WEP operuje w dwóch najniższych warstwach modelu OSI (warstwa fizyczna i warstwa łącza danych), dlatego nie jest w stanie zapewnić bezpieczeństwa *end-to-end.*

Protokół WEP posiada wiele słabych punktów, m. in.:

- słabe szyfrowanie:

Grupa robocza 802.11 ograniczyła długość klucza WEP do 40 bitów. Pozwala to na ograniczony poziom szyfrowania; zabezpieczenie można łatwo złamać. Haker używający statystycznych narzędzi analizy może przechwycić klucz WEP z bezprzewodowej sieci LAN w czasie krótszym niż 24 godz.

- statyczne klucze:

Klucze WEP są stosowane w kartach instalowanych w komputerach i w punktach dostępu w tej samej bezprzewodowej sieci LAN i nie są zmieniane automatycznie zgodnie z wcześniej ustalonymi zasadami. Co gorsza, standard WEP nie dopracował się metody dystrybucji kluczy. Gdy klucze zostaną skonfigurowane dla każdego użytkownika, bardzo trudno jest je zmienić. Administratorzy bardzo niechętnie modyfikują klucze WEP, ponieważ to pociąga za sobą konieczność dokonania zmian u końcowego użytkownika. Tak więc aktualna wersja standardu WEP nie chroni efektywnie danych. Większość aplikacji wymaga silniejszego, dynamicznego szyfrowania i mechanizmu uwierzytelniania.

EAP - skrót od słów *Extensible Authentication Protocol,* jest to protokół, wspierający wiele metod uwierzytelniania, takich jak np. Kerberos, Token Ring, certyfikaty czy tzw. inteligentne karty *(smart card).* Standard IEEE 802.lX określa, jak informacje EAP powinny być enkapsulowane w ramkach LAN. W sieciach bezprzewodowych wykorzystujących protokół EAP użytkownik łączy się z punktem dostępu, który chcąc potwierdzić tożsamość użytkownika transmituje odpowiednie informacje do serwera uwierzytelniania, takiego jak RADIUS. Protokół EAP jest zdefiniowany w RFC 2284. [1]

Standard IEEE 802. IX.

Standard ten jest wspierany przez większość producentów punktów dostępowych. Zawiera on mechanizm dystrybucji i potwierdzania tożsamości. IEEE 802.IX potrafi dynamicznie alokować klucze szyfrowania. Głównym elementem standardu jest protokół EAP. Wymiana informacji pomiędzy dwiema stronami odbywa się z wykorzystaniem serwera uwierzytelniania.

Jedną stroną stanowi klient (karta sieciowa 802.11), natomiast drugą punkt dostępowy.

Standard 802.1X uwierzytelnia użytkownika

Rys. 9.1 Standard 802.1X uwierzytelnia użytkownika [1]

Standard 802. IX oparty na protokole EAP pracuje w następujący sposób:

1. Klient próbuje połączyć się z punktem dostępowym, zaczyna działać protokół EAP, który uzgadnia wstępne procedury.
2. Punkt dostępowy wybiera port, który posłuży wyłącznie do obsługi ruchu EAP, następnie prosi klienta o identyfikację.
3. Klient odpowiada.
4. Punkt dostępu żąda uwierzytelnienia od serwera.
5. Po zakończonej sukcesem operacji uwierzytelnienia punkt dostępowy akceptuje ruch.

Rola serwera uwierzytelniania polega na zezwoleniu lub zabronieniu. Serwery uwierzytelnienia występują w postaci rozwiązań *Remote Authentication Dial-In User Service* i *Kerberos*. Podczas próby połączenia klienta z punktem dostępu, punkt ten wyznacza port, który będzie obsługiwał ruch EAP. Punkt ten posiada dane identyfikujące klienta i celem jego uwierzytelnienia komunikuje się z serwerem. Jeśli proces uwierzytelniania zakończy się sukcesem, punkt dostępowy zaczyna obsługiwać inne protokoły {takie jak *Dynamie Host Configuration Protocol. Post Office Protocol 3* i *Simple Mail Transfer Protocol}*. Gdy klient wyloguje się, punkt dostępowy wyłącza porty obsługujące tego klienta. System bezpieczeństwa wymaga też zaimplementowania jednej z metod uwierzytelniania, takiej jak LEAP *(Lightweight Extensible Authentication Protocol)* lub EAP-TLS *(EAP Transport Layer Security)*. Obie metody są oparte na mechanizmie obopólnego uwierzytelniania między klientem a punktem dostępu. Metoda LEAP jest stosowana w sieciach WLAN Cisco, gdzie dynamicznie generuje klucze WEP. Metoda EAP-TLS wymaga, aby klienci i punkty dostępu dysponowały certyfikatami cyfrowymi, które pozwalają na dynamiczną dystrybucję kluczy WEP przez bezpieczne połączenia. Metodę EAP-TLS wspiera system operacyjny Windows XP oraz wielu producentów sieci WLAN. Problem z produktami 802. IX polega na tym. że używają one ciągle szyfrowania WEP, które jest stosunkowo słabe. Jednak 802.IX zmienia klucze na tyle często, że minimalizuje niebezpieczeństwo włamań. Administrator może tak skonfigurować system, aby klucze były zmieniane co parę minut, co godzinę, co tydzień lub po

zakończeniu każdej sesji.

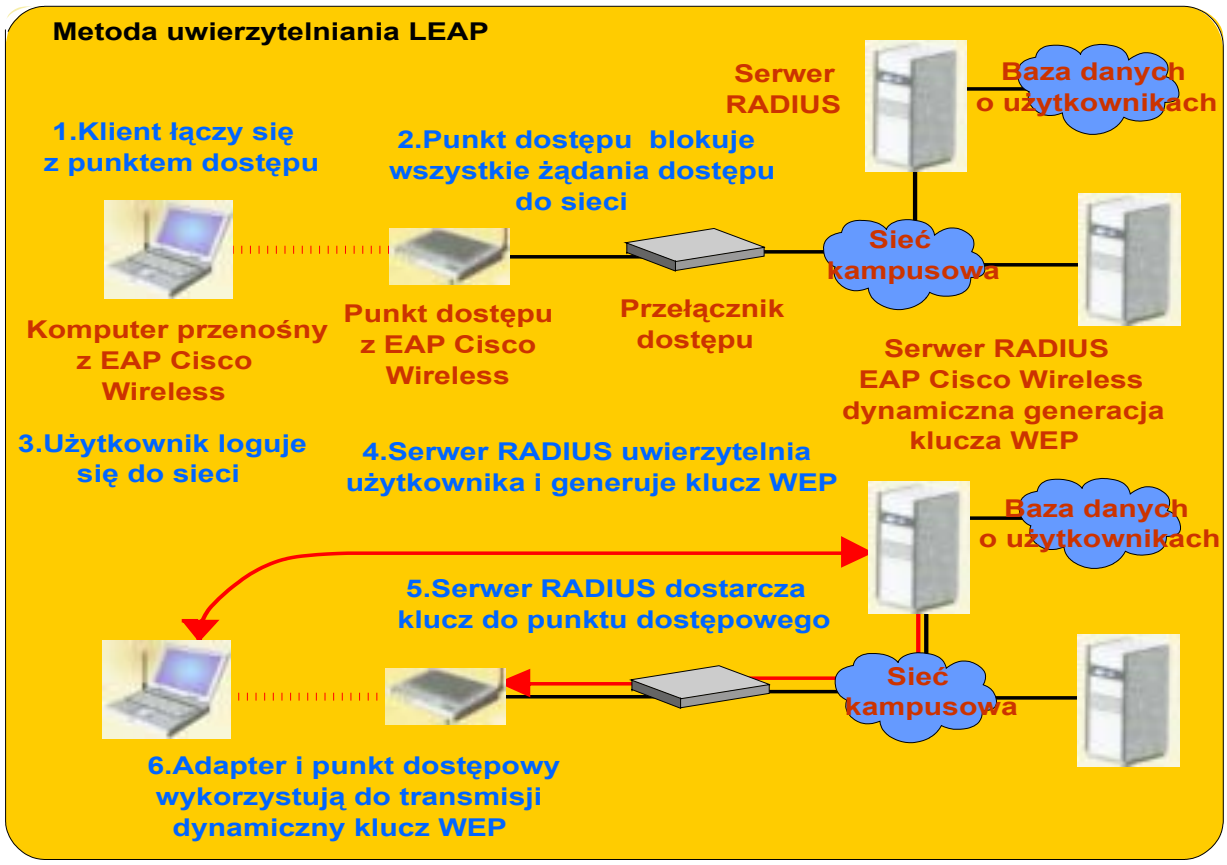
Firma Cisco Systems opracowała metodę uwierzytelniania 802.1X, która nosi nazwę EAP Cisco Wireless lub Cisco LEAP (*Lightweight EAP*). Za pomocą metod uwierzytelniania

802.1X, takich jak Cisco LEAP i EAP-TLS, są implementowane systemy uwierzytelniania między klientem a serwerem RADIUS *(Remote Authentication Dial-ln User Senrice).* Dane dotyczące uwierzytelniania, takie jak podawanie hasła, nie są nigdy transmitowane przez sieć bezprzewodową bez szyfrowania.

Metoda uwierzytelniania LEAP

LEAP to metoda uwierzytelniania 802.1 X opracowana przez Cisco. LEAP jest częścią zestawu Cisco Wireless Security Suite. Produkty Aironet firmy Cisco wspierają standard Cisco LEAP i wszystkie metody uwierzytelniania 802.1X, w tym EAP *Transport Layer Security* (EAP-TLS). Metody uwierzytelniania 802.1 X, takie jak Cisco LEAP i EAP-TLS pozwalają implementować systemy uwierzytelniania między klientem a serwerem RADIUS *(Remote Authentication Dial-ln User Senrice).* Dane dotyczące uwierzytelniania, takie jak podawanie hasła, nie są nigdy transmitowane przez sieć bezprzewodową bez szyfrowania.

Gdy proces uwierzytelniania zakończy się sukcesem wówczas punkt dostępu zaczyna obsługiwać inne protokoły (takie jak *Dynamic Host Configuration Protocol. Post Office Protocol 3* i *Simple Mail Transfer Protocol).* Po wylogowaniu klienta, punkt dostępu wyłącza porty obsługujące tego użytkownika. EAP nie definiuje wszystkich technik zabezpieczania połączeń bezprzewodowych. System bezpieczeństwa wymaga też zaimplementowania jednej z metod uwierzytelniania, mianowicie LEAP *(Lightweight Extensible Authentication Protocol)* lub EAP-TLS *(EAP Transport Layer Security).*



Rys. 9.2 Metoda uwierzytelniania LEAP [1]

Powyższe metody są oparte na mechanizmie obopólnego uwierzytelniania między klientem a punktem dostępu. LEAP jest stosowany w sieciach WLAN Cisco dynamicznie generując klucze WEP. Metoda EAP-TLS wymaga od klientów i punktów dostępu aby dysponowały certyfikatami cyfrowymi, które pozwalają na dynamiczną dystrybucję kluczy WEP przez bezpieczne połączenia. Metoda EAP-TLS jest wspierana przez system operacyjny Windows XP oraz przez wielu producentów sieci WLAN. Wadą produktów 802. 1X jest to, że używają one ciągle szyfrowania WEP, które jest stosunkowo słabe. Zaznaczyć jednak należy, że 802.1X zmienia klucze na tyle często, że minimalizuje niebezpieczeństwo włamań. Administrator może tak skonfigurować system, aby klucze były zmieniane co parę minut, co godzinę, co tydzień lub po zakończeniu każdej sesji.

802.11i – krok ku zwiększeniu bezpieczeństwa

IEEE 802.11i jest podgrupą, nazywaną również Task Group l (TGi), która chce zmodyfikować specyfikację 802.11 *Media Access Control Layer,* wprowadzają do niej mechanizmy 802.1X. Standard 802.11i zakłada częste zmiany klucza i wzmocnienie procesu szyfrowania. 802.11i pomoże pozbyć się dwóch głównych problemów trapiących protokół WEP: statyczne klucze i słabe szyfrowanie. [1]

10. DLACZEGO WLAN?

Rosnąca popularność sieci bezprzewodowych związana jest z potrzebą dostępu do Internetu i do innych sieci IP z dowolnego miejsca . Taką możliwość stwarza technologia bezpiecznych sieci IP VPN, pozwalająca łączyć się z siecią z dowolnego miejsca na całym świecie. Istnieje wiele obszarów zastosowań sieci WLAN, spośród nich warto wymienić między innymi:

- **Służba zdrowia –** potrzeba szybkiego uzyskania informacji o pacjentach niezależnie od miejsca przebywania.
- **Edukacja -** głównie centra szkoleniowe przedsiębiorstw a także używanie sieci WLAN przez studentów uniwersytetów do wymiany i zdobywania informacji oraz zdalnej nauki.
- **Handel hurtowy/detaliczny i produkcja -** usprawnienie procesów produkcyjnych oraz lepsze prowadzenie gospodarki magazynowej przez przedsiębiorstwa.

Wśród innych zastosowań sieci WLAN wymienić należy np. biura oddziałowe, sale konferencyjne, biblioteki - administratorzy mogą szybko wdrażać tam technologie bezprzewodowe.

Sieci WLAN najprawdopodobniej zrewolucjonizują sposób komunikacji z Internetem i z sieciami korporacyjnymi. Duże znaczenie w tym procesie ma fakt, że sieci bezprzewodowe są w stanie zagwarantować wszystkie możliwości oferowane przez tradycyjne systemy informatyczne. Do usług oferowanych przez sieci WLAN zaliczyć można usługi takie, jak: ftp, e - mail czy http. [1]

11. WDRAŻANIE ROZWIĄZAŃ WLAN

Wprowadzenie na dużą skalę rozwiązań sieci WLAN może w znacznym stopniu przyczynić się do w zrostu wydajności pracy wielu przedsiębiorstw. Jednak z implementacją sieci WLAN oraz urządzeń bezprzewodowych związana jest pewna trudność – otóż należy wszystko zaplanować i zaimplementować na tyle dokładnie, żeby zapewnić poprawne działanie takiej sieci. Sieć bezprzewodową można skonfigurować dwojako: albo będzie to stanowiła ona

architekturę niezależną (tzw. konfiguracje *peer-to-peer,)* albo rozbudowaną architekturę w postaci sieci infrastrukturalnej (tzn. składającą się z wielu punktów dostępu). Obecnie są już dostępne urządzenia bezprzewodowe różnego rodzaju, tak więc każdy użytkownik może znaleźć takie urządzenie, które najbardziej mu odpowiada. Projektując sieć WLAN należy kierować się następującymi uwarunkowaniami:

- **Jakość i solidność usług** (możliwość skalowania, przepustowość, niezawodność)

Użytkownicy oczekują, że jakość usług świadczonych przez sieć WLAN będzie taka sama, jak tradycyjnych sieci LAN, z czasem też prawdopodobnie zaistnieje potrzeba uruchomienia w sieci bardziej wymagających usług.

- Szybkość

WLAN opiera się na technologii współdzielonego widma. Dostępne widmo dzielone jest między użytkowników, którzy często wykorzystują jedynie część dostępnej teoretycznie przepustowości 11 Mb/s. Praca sieci WLAN podobna była do pracy hubów LAN (współdzielony dostęp do medium), zanim do użytku nie weszły przełączniki.

- Zasięg

Zasięg sieci bezprzewodowych jest ograniczony (do 100 m wewnątrz budynków i do 500 m w otwartej przestrzeni), dlatego, aby zbudować sieć WLAN na przykład w dużym banku, potrzebne będą setki punktów dostępu. Wewnątrz budynków istnieje wiele przeszkód dla fal radiowych, takich jak ściany, czy nawet znajdujący się w pomieszczeniach ludzie. Mimo to fale radiowe są wykorzystywane ponieważ mogą one penetrować wewnętrzne ściany i powierzchnie. Dzięki mikrokomórkom i punktom dostępu zasięg sieci WLAN można zwiększyć tak, aby mogła ona obsługiwać nawet duże bardzo duże przedsiębiorstwo czy szpital.

- Zakłócenia

Zakłócenia powodowane np. przez urządzenia korzystające z komunikacji bezprzewodowej Bluetooth mogą w skrajnych przypadkach spowodować spadek przepustowości sieci WLAN z 11Mb/s do 1Mb/s.

- Bezpieczeństwo

Przy implementowaniu technologii bezprzewodowych należy bacznie przyjrzeć się kwestii bezpieczeństwa. Należy rozważyć, jakie są wymagania dotyczące bezpieczeństwa i czy dane rozwiązanie jest w stanie tym wymaganiom sprostać. Bezpieczeństwo sieci jest szczególnie ważne w instytucjach, takich jak banki czy ministerstwa. W ostatnich latach stwierdzono wiele słabych punktów standardu WEP *(Wired Eąiwalent Priwacy)* stosowanego powszechnie w większości sieci WLAN 802.1 Ib. Może np. dochodzić do ataków przez zakłócanie sygnałów radiowych używanych do transmitowania danych. Pod pewnymi względami okazuje się jednak, że sieci WLAN są bezpieczniejsze od tradycyjnych sieci LAN – przechwycenie danych przesyłanych drogą radiową wymaga więcej zachodu, a nawet jeśli się to uda, to dane te są często zaszyfrowane.

- Zgodność między urządzeniami przenośnymi i istniejącymi już sieciami LAN

Wprowadzenie w przedsiębiorstwie sieci bezprzewodowej stwarza niebezpieczeństwo, że istniejące już systemy informatyczne i nowe urządzenia sieci WLAN nie będą w stanie ze sobą współpracować.

- Zarządzanie sieciami WLAN

Zastosowanie nowych rozwiązań bezprzewodowych wymaga użycia coraz lepszych narzędzi do zarządzania sieciami WLAN. Systemy zarządzania wpływają bezpośrednio na takie elementy, jak ogólny koszt posiadania sieci (TCO) i zwrot inwestycji (ROI). Zarządzanie siecią bezprzewodową polega na monitorowaniu, sprawdzaniu konfiguracji i kontrolowania przepustowości poszczególnych elementów wchodzących w skład sieci: punktów dostępu, mostów i innych elementów sieciowych.

- Cena

Koszt implementacji sieci bezprzewodowej obejmuje koszty infrastruktury (punkty dostępu) oraz koszty ponoszone przez klientów (bezprzewodowe adaptery). Koszty infrastruktury uwarunkowane są głównie liczbą punktów dostępu, która z kolei zależy od tego, jak duży obszar chcemy pokryć naszą siecią i jaka będzie liczba użytkowników, którym będziemy świadczyć usługi. Ceny punktów dostępu wahają się od 800 do 2000 USD, bezprzewodowe adaptery LAN natomiast od 200 do 700 USD. Koszty związane z instalacją i utrzymywaniem w ruchu sieci WLAN są zasadniczo niższe niż koszty ponoszone w przypadku tradycyjnej sieci LAN. Przyczyny tego stanu rzeczy są dwie: po pierwsze odpadają koszty okablowania, po drugie w sieciach WLAN pracują użytkownicy mobilni, nie wymagający tak dużych nakładów pracy związanych z ich administrowaniem. [1]

12. HOT SPOT CZYLI PUBLICZNY DOSTĘP BEZPRZEWODOWY

Publiczny dostęp bezprzewodowy związany jest ze skrótem WISP *(Wireless Internet Service Provider).* Są to usługodawcy, którzy oferują dostęp do publicznych bezprzewodowych sieci LAN w miejscach odwiedzanych przez mobilnych pracowników czy innych użytkowników, którzy np. podróżują z notebookiem. Miejsca takie to np. porty lotnicze, centra konferencyjne, hotele czy restauracje. Przy użyciu notebooka czy komputera PDA użytkownik może uzyskać dostęp do Internetu, czy też zalogować się do swojej sieci przy wykorzystaniu technologii VPN *(Virtual Prwate Network}.* Miejsca takie, oferujące publiczny dostęp nazywane są popularnie *hot spot.* Usługodawcy umieszczają w miejscach *hot spot* punkty dostępu . Punkt dostępu komunikuje się z komputerem użytkownika (dokładnie rzecz biorąc z zainstalowanym w nich interfejsem bezprzewodowym). Użytkownik może zalogować się używając strony logowania wyświetlonej przez przeglądarkę sieci web. Zasięg między punktem dostępu a użytkownikiem wynosi najczęściej od 50 do 150 m. Szybkość połączenia to 11 Mb/s przy zastosowaniu technologii IEEE 802.1 Ib (znanej jako Wi-Fi).

Czasem dostęp jest bezpłatny, jednak z reguły użytkownik musi płacić - za jednokrotny dostęp, za minutę, za dzień. Może też wykupić np. miesięczną subskrypcję.

Aby uregulować problem płatności, organizacja WECA (*Wireless Ethernet Compatibility Alliance),* w skład którego wchodzą Cisco Systems. IBM, Intel. 3Com i Microsoft, pracuje nad utworzeniem standardu, który miałby byś stosowany przez usługodawców WISP. [1]

13. WSZYSTKO O STANDARDACH WLAN

Zaaprobowane standardy zgodnie ze stanem na maj 2002:

1. IEEE 802.11 (sieci WLAN pracujące z szybkością do 2 Mb/s i wykorzystujące

częstotliwość 2.4 GHz, zastosowanie w nauce, przemyśle i służbach publicznych).

Data akceptacji - lipiec 1997.

2. IEEE 802.11a (sieci WLAN pracujące z szybkością do 54 Mb/s i wykorzystujące częstotliwość 5 GHz, zastosowanie w nauce, przemyśle i służbach publicznych).

Data akceptacji -wrzesień 1997. Pierwsze produkty weszły na rynek na początku 2002 r

3. IEEE 802.11b (sieci WLAN pracujące z szybkością do 11 Mb/s i wykorzystujące częstotliwości 2.4 GHz, zastosowanie w nauce, przemyśle i służbach publicznych).

Data akceptacji - lipiec 1997. Pierwsze produkty weszły na rynek na początku 2000 r.

Tabela 2.

Standardy IEEE WLAN	802.11	802.11a	802.11 b	802.11 g
Data akceptacji standardu	Lipiec 1997	Wrzesień 1999	Wrzesień 1997	Faza „draft" ma być ukończona jeszcze w 2002 r.
Dostępna szerokość pasma (MHz)	83,5	300	83,5	83,5
Częstotliwość (GHz) i metoda modulacji	2,4-2,4835 DSSS, FHSS	5,15-5,35 OFDM 5,725-5,825 OFOM	2,4-2,4835 DSSS	2,4-2,4835 DSSS, OFDM
Liczba nie zachodzących na siebie kanałów	3 (w sieciach wewnętrznych/ zewnętrznych)	4 w sieciach wewnętrznych (pasmo UNII1*) 4 w sieciach wewnętrznych/ zewnętrznych (pasmo UNII2) 4 w sieciach zewnętrznych (pasmo UNII3)	3 (w sieciach wewnętrznych/ zewnętrznych)	3 (w sieciach wewnętrznych/ zewnętrznych)
Szybkość przesyłania danych na kanał (Mb/s)	2,1	54; 48; 36; 24, 18; 12; 9; 6	11; 5,5; 2,1	54; 36; 33; 24; 22; 12; 11; 9; 6; 5,5; 2
Zgodność ze specyfikacją	802.11	WI-R5	Wi-Fi	

Standardy znajdujące się w fazie rozpatrywania:

1. IEEE 802.11g- rozszerzenie standardu 802.11b, pozwalające przesyłać dane z szybkością do 54 Mb/s z wykorzystaniem częstotliwości 2.4 GHz. Standard został wstępnie przyjęty (faza *draft)* pod koniec 2001 r. Pełna ratyfikacja spodziewana pod koniec 2002 lub na początku 2003.

2. IEEE 802.15.1. *Standard Wireless Personal Area Network* (osobiste bezprzewodowe

sieci komputerowe) oparty na specyfikacji Bluetooth. Sieci będą pracować z wykorzystaniem częstotliwości 2.4 GHz. Został warunkowo zaaprobowany 21 marca 2002 r.

Standardy znajdujące się ciągle w fazie opracowywania:

1. Grupa robocza IEEE 802.11e. Pracuje nad udoskonaleniem 802.11 MAC *(Medam Access Control)* celem lepszego zarządzania *Quality o f Service,* udostępnienia nowych klas i poprawienia bezpieczeństwa oraz usprawnienia mechanizmów uwierzytelniania. Usprawnienia te powinny zapewnić jakość, jaka jest wymagana przy takich usługach jak telefonia IP i przesyłanie strumieni wideo.
2. Grupa robocza IEEE 802.11f. Pracuje nad protokołem IAPP *(Inter-Access Point Protocol),* który udostępni funkcje niezbędne do tego, aby punkty dostępu produkowane przez różnych producentów były ze sobą zgodne.
3. Grupa robocza IEEE 802.l1h. Pracuje nad usprawnieniem standardów 802.11 MAC *(Media Access Control)* i 802.11a PHY *(High Speed Physical Layer),* tak aby produkty IEEE 802.11a były zgodne z wymaganiami rynku europejskiego.
4. Grupa robocza IEEE 802.111. Pracuje nad usprawnieniem 802.11 MAC *(Media Access Control),* tak, aby można było poprawić bezpieczeństwo mechanizmy uwierzytelniania.
5. Grupa robocza IEEE 802.15 TG2. Pracuje nad rozwiązaniami, dzięki którym sieci WPAN *(Wireless Personal Area Networks)* (802.15) i sieci WLAN 802.11 będą mogły ze sobą współpracować.
6. Grupa robocza IEEE 802.15 TG3. Pracuje nad nowym standardem dla sieci WPAN, które będą pracować z szybkością 20 Mb/s i większą.

Organizacje zajmujące się promowaniem i propagowaniem standardów dla sieci bezprzewodowych:

1. Wireless Ethernet CompatibilityAlliance (WECA); http://www.wi-fi.org:

Przymierze certyfikuje zgodność produktów IEEE 802.11 i wspiera sieci Wi-Fi.

2. Bluetooth Special Interest Group; http://www.bluetooth.com:

Grupa wspiera specyfikację Bluetooth i promuje standard IEEE 802.15.

3. OFDM Forum; http://www.ofdm-forum.org:

Forum koncentruje się na standardzie OFDM *(Orthogonal Frequency Division Multiplexing)*;

4. HomeRF: http://www.homerf.org:

Organizacja zajmuje się specyfikacjami dla bezprzewodowych technologii stosowanych w domu i promuje standard HomeRF Protocol.

5. HIPERLAN Alliance; http://www.hiperlan.com:

Przymierze wspiera standard HiperLAN/1.

6. HiperLAN2 Global Forum: http://www.hiperlan2.com:

Forum wspiera standard HiperLAN2 jako globalną technologię bezprzewodową wykorzystującą częstotliwość 5 GHz.

7. Wireless LAN Association (WLANA): http://www.wlana.org:

Stowarzyszenie edukacyjne promujące sieci WLAN i technologie bezprzewodowe *(Wireless Local Area Networks,* publiczne, ogólnodostępne sieci WLAN. mosty LAN-LAN i sieci *Persona/ Area Networks}*.

Organizacje zajmujące się standaryzacją:

1. Institute for Electrical and Electronics Engineers(IEEE);
http://www.ieee.org:
Organizacja zajmuje się wszystkimi standardami 802.11 i 802.15.
2. European Telecommunications Standards Institute (ETSI);
http://www.etsi.org:
Organizacja opracowuje standardy telekomunikacyjne dla Europy (HiperLAN/1 i HiperLAN/2). [1]

14. INTEGRACJA WLAN Z GPRS\UMTS

Działania operatorów zmierzające w kierunku nowych usług, większego pasma, nowej jakość telefonii komórkowej oraz stworzenia systemu IP dla abonentów mobilnych to wdrożenie systemów WAP i GPRS. Z wiadomych przyczyn ich atrakcyjność dla przeciętnego użytkownika jest niewielka, szczególnie jeśli idzie o WAP. Systemy te miały być pomostem do 3G, zapowiedzią nowych możliwości.
3G dla Europy to UMTS *(Universal Mobile Telecommunication System).* UMTS już na początku napotykał na poważne problemy - techniczne, implementacyjne. Jednak największym problemem okazały się licencje, a dokładnie ich koszt. Właśnie to było powodem przesunięcia terminu komercyjnych wdrożeń.
Istnieje jednak spore zapotrzebowanie na bezprzewodowy dostęp do Internetu, a brak jeszcze docelowej infrastruktury. Właśnie dlatego można wykorzystać już tę istniejąca, a taką właśnie zapewniają WLAN *(Wireless Local Aren Nctwork).* WLAN, czyli bezprzewodowe sieci lokalne, pojawiły się dosyć dawno, ale początkowo produkty różnych firm nie współpracowały ze sobą. Dlatego też wprowadzono standardy, m.in. takie jak IEEE 802.11 czy HiperLAN - określały zasady pracy urządzeń do transmisji bezprzewodowej. Rozwiązania WLAN zyskały na popularności, a dostępne przepustowości są coraz większe (np. najpopularniejszy standard 802.11b - do 11 Mb/s w paśmie 2,4 GHz). Jest to bardzo dobry wynik, nawet przy uwzględnieniu zależność przepustowości od odległości. Chociaż systemy takie działają na bardzo ograniczonym obszarze (typowo na otwartej przestrzeni ok. 150 m od punktu dostępowego, a w zamkniętej ok. 30 m - dane dla przepustowości 11 Mb/s), to należy pamiętać, iż zależy nam przede wszystkim na niezawodnej usłudze mobilnego Internetu w istotnych punktach. Bierzemy pod uwagę centra miast, poczekalnie na lotniskach, hotele - tzw. hotspots. Właśnie takie miejsca zapewniłyby użytkownikowi korzystanie z publicznej sieci WLAN.
Poza siecią dostępową WLAN jest natomiast GPRS, problemem jest więc zapewnienie mechanizmów przełączania pomiędzy sieciami oraz mechanizmów autoryzacji. Docelowo zaproponowane rozwiązania mają zapewnić pełną integrację dla kombinacji WLAN-GSM/GPRS oraz WLAN-UMTS. Ciekawym rozwiązaniem dla integracji WLAN z GSM/GPRS jest architektura zaproponowana przez firmę Ericsson. Rozwiązanie nazwane Ericsson Mobile Operator WLAN Release zakłada brak konieczności ingerencji w istniejącą architekturę GSM/GPRS.
System wykorzystuje nakładkowe tworzenie wysp dostępu WLAN w istniejącej sieci GPRS. Ta ostatnia zapewnia dostęp do Internetu prawie wszędzie, ale dysponujemy wówczas stosunkowo niewielkim pasmem. Dostęp przez WLAN jest zapewniany tylko w specyficznych miejscach (hotspots), wówczas dostępna jest przepustowość jak w systemie 802.11b, a więc teoretyczna maksymalna przepływność to 11 Mb/s. Celem jest zapewnienie roamingu WLAN-GPRS.
Takie rozwiązanie wymaga jedynie pewnej rozbudowy istniejącej już infrastruktury dla sieci GSM/GPRS o dodatkowe elementy funkcjonalne. Istotne są mechanizmy identyfikacji i

autoryzacji użytkowników systemu. Uwzględniono możliwość identyfikacji przy użyciu jednorazowego hasła dostępu, które przy logowaniu jest dostarczane w postaci SMS konkretnemu abonentowi GSM. Inny mechanizm polega na dostarczeniu abonentowi stałego hasła dostępu które przy wykorzystaniu SSL umożliwia identyfikację.
Architektura systemu wyróżnia dwa podstawowe moduły funkcjonalne: segment dostępowy oparty na rozwiązaniu WLAN oraz system zarządzania dostępem (Access *Management System).*
Punkty dostępowe AP (Access *Points),* funkcjonujące w standardzie IEEE 802.11b, zapewniają dostęp do usług na określonym obszarze - obszar zależy od liczby AP oraz charakteru obiektu (np. czy w budynku jest dużo ścian). Zespół AP jest podłączony przez sieć Ethernet do węzła ASN (Access *Serving Node). Z* kolei ASN jest podłączony do sieci szkieletowej IP. Funkcjonalność ASN jest zbliżona do serwera dostępowego usług. Jego główne zadania to autoryzacja użytkowników korzystających z dostępu oraz gromadzenie informacji o ilości przesłanych danych. ASN jest odpowiedzialny również za utrzymanie parametrów odpowiadających danym profilom użytkowników (profil użytkownika w szczegółowy sposób definiuje parametry serwisu - umożliwia to różnicowanie usług). ASN wraz z instalacją AP tworzy segment dostępowy.
Access *Management System* zawiera następujące elementy funkcjonalne:

- SCS *(Senńcc Control Sewer)* - wspiera funkcjonalność ASN. Dla bezpieczeństwa każdy ASN połączony jest z dwoma SCS. Za każdym razem, gdy użytkownik loguje się do sieci, ASN przesyła żądanie autoryzacji do SCS przy wykorzystaniu protokołu RADIUS *(Remote Authentication Dial in User Service).* SCS odpowiada natychmiast (dla użytkowników *prepaid)* lub działa jako RADIUS proxy przy komunikacji z serwerem AS *(Authentication Server)* albo zewnętrznym serwerem RADIUS (dla użytkowników *postpaid).*
- AS *(Authentication Server)* - realizuje identyfikację przez jednorazowe hasło przesyłane abonentowi w postaci SMS. Gdy AS otrzymuje żądanie autoryzacji od ASN, odnajduje użytkownika w bazie danych *(WLAN subscriber data-base)* i komunikuje się z SMS-C (SMS *Center),* aby dostarczyć jednorazowe hasło dostępu. Jeśli wprowadzone przez użytkownika hasło jest zgodne z wygenerowanym przez AS, dostęp zostaje zatwierdzony.
- SAS *(Statistics and Accounting Sewer)* - jest serwerem realizującym gromadzenie zbiorczych statystyk dla systemu billingowego. SAS agreguje dane ze wszystkich ASN i wysyła to GSM/GPRS BGW *(Billing Gateway).*
- CABS *(Custoincr Administration and Billing Server)* -- odpowiedzialny za stworzenie interfejsu zarządzania dla użytkowników *prepaid.*
- APIS *(Application Program Interface Sewer)* - zadaniem jego jest przechowywanie informacji o profilach użytkowników oraz danych dla użytkowników *prepaid* (hasła, limity itp.). Dane użytkowników *postpaid są* przechowywane w AS lub bazie danych serwera RADIUS. Przechowywane dane to kopie informacji z HLR operatora. Wszyscy użytkownicy *postpaid* korzystający z WLAN, oprócz standardowego zestawu danych, takich jak MSISDN, muszą mieć dodatkowe pole opisujące status subskrypcji usługi WLAN oraz profil subskrypcji.
- WLAN manager - centralny element *zarządzania* dla wszystkich podległych systemów WLAN.

Nokia *(Nokia Operator Wireless LAN Solution*) jest również dostawcą rozwiązań opartych na technologiach WLAN. System Nokii również wykorzystuje standard 802.11b. Przykładowe rozwiązanie może wykorzystywać punkty dostępowe AO32 Nokia, które komunikują się z kontrolerem P022 *(access controller).* Podstawowe funkcje kontrolera to monitorowanie ruchu i gromadzenie danych billingowych. Identyfikację użytkownika realizowana jest w oparciu o typowy mechanizm wykorzystywany w sieci GSM - użytkownik posiada kartę SIM *(Subscriber Ideu-tity Module), z* którą jest skojarzony kod PIN. Ta technika identyfikacji pozwala na pełne wykorzystanie zalet międzynarodowego roamingu już zaimplementowanego

w sieciach GSM. Nokia Operator Wireless LAN Solution gwarantuje również wsparcie dla standardu RADIUS. Użytkownicy bez karty SIM mają możliwość osobnej identyfikacji przy wykorzystaniu pary: nazwa użytkownika i hasło, co z kolei stwarza możliwość wykorzystania architektury systemu przez bezprzewodowych dostawców Internetu (WISP). Abonenci GSM/GPRS korzystający z dostępu WLAN otrzymują jeden wspólny rachunek uwzględniający taryfikację za połączenia w *hotspots.*
Nokia jest również dostawcą terminali dla potencjalnych użytkowników systemu. Za przykład rozwiązań mogą posłużyć: przeznaczona do laptopów karta Wireless LAN C110/111 - karta umożliwia korzystanie z publicznej sieci WLAN dla abonentów GSM/GPRS (wewnątrz karty znajduje się interfejs dla karty SIM) oraz karta Nokia D211 (dostępna także w Polsce) - jest to pracująca w wielu trybach karta radiowa umożliwiająca dostęp do sieci przez GPRS, HSCSD lub bezprzewodowy LAN.

Do tej pory dostawcy europejscy oferują tylko opisane powyżej rozwiązania. Wspomnieć jednak należy również o produkcie firmy Siemens. Proponowane przez Siemensa 1250 Access Gateway oraz seria produktów I-Gate (punkty dostępowe oraz karty WLAN) tworzą infrastrukturę umożliwiającą WISP świadczenie usługi publicznego dostępu przez WLAN. Funkcjonalność 1250 Access Gateway zapewniają m.in.:
- wykorzystanie mechanizmów opartych na SMS do celów autoryzacji i uwierzytelniania;
- zróżnicowanie stosowanych modeli billingo-wych;
- wykorzystanie RADIUS (stworzenie możliwości budowania prostych interfejsów do innych WISP).

Ciekawostką jest fakt, iż 5 sierpnia 2002 wiodąca na rynku w USA firma Mobility Network Systems oraz operator sieci GSM/GPRS Rogers AT&T Wireless przeprowadziły pilotową instalację systemu integracji WLAN-GSM/GPRS. Instalacja zakończyła się powo-dzeniem, a całość wykonano w ciągu 24 godzin!
Rozwiązanie firmy Mobility Network Systems wyróżnia następujące moduły funkcjonalne:
- RAC *(Radio Access Controller)* - moduł działający jako brama uwierzytelniająca dla bazy danych sieci komórkowej (HLR lub AAA); w rozwiązaniu tym nie są wymagane żadne modyfikacje w strukturze HLR.
- RLM *(Radio Link Manager)* - moduł zainstalowany w *Iwtspot,* jego zadaniem jest kontrolowanie punktów dostępowych (wykorzystywany jest *Advanced En-cryption Standard).*
- MLC *(Multi-Link Clicnl Software)* - moduł zainstalowany po stronie użytkownika, zapewnia usługę uwierzytelniania przy wykorzystaniu karty SIM lub pary użytkownik/hasło.
Oprogramowanie współpracuje z dowolnym typem karty WLAN pracującej w standardzie 802.11b lub a.

Odpowiedzią na problemy rozwoju rynku usług 3G jest inicjatywa standaryzacji dla integracji WLAN/UMTS zaproponowana przez 3GPP. Przewidziano integrację przez ewolucyjne modyfikacje architektury. Każda zmiana pozwala osiągnąć dany poziom integracji systemów, przy czym każdy kolejny poziom zawiera możliwość funkcjonalności poprzednich.
Przewidziano sześć etapów integracji:
- etap 1: wspólny billing, ale niezależne dla obu sieci mechanizmy i poziom autoryzacji;
- etap 2: autoryzacja realizowana przez system 3GPP - użytkownik nie widzi istotnych różnic w sposobie dostępu dla obu sieci. Dzięki takiej funkcjonalności operator systemu 3GPP może w łatwy sposób przekształcić swoich dotychczasowych abonentów w abonentów systemu mieszanego (3GPP-WLAN), dla których procedury utrzymaniowe i obsługi pozostają bez zmian - możliwość rozszerzenia oferty usług o dostęp przez WLAN;
- etap 3: zapewnienie dostępu przez WLAN dla podsystemu PS *(Packet Switched)* 3GPP - możliwość korzystania z pewnych serwisów opartych na podsystemie PS (np. usługi lokalizacyjne);

- etap 4: zapewnienie ciągłości serwisów wyróżnionych w etapie 3 przy konieczności zmiany typu sieci (przełączenie pomiędzy WLAN i 3GPP);
- etap 5: rozszerzenie funkcjonalności etapu 4 o minimalizację czasu przełączenia oraz obsługę ewentualnych sytuacji wyjątkowych;
- etap 6: dostęp do podsystemu GS *(Circuit Switched)* 3GPP.

Powyższa analiza produktów oraz tendencji rynkowych nasuwa wniosek, iż najbliższą przyszłość mobilnego Internetu będą tworzyćrozwiązania oparte na technice integracji WLAN z dotychczasowymi systemami. Przyczynami tej tendencji jest niski koszt rozwiązań WLAN. [2]

15. WYKAZ SKRÓTÓW I AKRONIMÓW

ACK - Acknowledgement
AP - Access Point
BER - Bit Error Rate
BPSK - Binary Phase Shift Keying
CCK - Complementary Code Keying
DSSS - Direct Sequence Spread Spectrura
EAP - Extensible Authentication Protocol
ESS - Extended Service Set
ETSI - European Telecommunications Standards Institute
FCC - Federal Communications Commission
FHSS - Frequency Hopping Spread Spectrum
IBSS - Independent Basic Service Set
IEEE - Institute of Electrical and Electronics Engineers
IETF - Internet Engineering Task Force
LAN - Local Area Network
MAC - Media Access Control
MAN - Metropolitan Area Network
MB/s - megabajty na sekundę
Mb/s - megabity na sekundę
OFDM - Orthogonal Frequency Division Multiplexing
OFDM/CCK - Orthogonal Freąuency Division Multiplexing/Complimentary Code Keying
OSI - Open System Interconnection
PAN - Personal Area Network
PBCC - Packet Binary Convolution Coding
PHY - Physical (Layer)
QAM - Quadrature Amplitude Modulation
QoS - Quality of Service
QPSK - Quadrature Phase Shift Keying
RADIUS - Remote Authentification Dial-In User Service
RF - Radio Frequency

UNII - Unlicensed National Information Infrastructure
WAN - Wide Area Network
WECA - Wireless Ethernet Compatibility Alliance
WISP - Wireless Internet Service Provider
WLAN - Wireless LAN [1]

16. SŁOWNIK PODSTAWOWYCH POJĘĆ

Bezprzewodowy węzeł - komputer wyposażony w bezprzewodowy interfejs *(adapter}*.

Brama - węzeł w sieci, który pełni rolę bramki umożliwiającej dostęp do innej sieci.

CSMA/CA *(Carrier Sense Multiple Access/Collision Avoidance)* - metoda dostępu do medium stosowana w sieciach WLAN zgodna z IEEE 802.11. Jest to metoda „posłuchaj, zanim zaczniesz rozmawiać". Metoda minimalizuje - ale nie eliminuje - liczbę kolizji przez jednoczesne transmitowanie sygnałów przez wiele nadajników radiowych. Standard IEEE 802.11 to unikanie, a nie wykrywanie kolizji, ponieważ mamy tu do czynienia z pracą w trybie półdupleksu. Inaczej niż w przypadku kablowego Ethernetu stacja WLAN nie może podczas transmitowania sygnału wykrywać kolizji. Jeśli pojawi się kolizja, stacja transmitująca nie odbierze pakietu ACK *(Acknowledgement}* od stacji docelowej. Dlatego w tym środowisku pakiety ACK mają wyższy priorytet niż wszystkie inne. Po zakończeniu transmisji stacja docelowa wysyła od razu pakiet ACK. zanim inny węzeł zacznie wysyłać nowe pakiety z danymi. Jeśli pakiet ACK nie zostanie odebrany, stacja nadająca czeka na kolejną możliwość transmitowania danych.

DSSS *(Direct-Sequencing Spread-Spectrutn}* - technika *spread-spectrum,* wykorzystująca fale radiowe dostępne w tzw. nie licencjonowanym paśmie ISM *(industrial, scientific, medicai.* przemysł, nauka, medycyna). Metoda DSSS używa nadajnika radiowego do transmitowania pakietów z danymi w ramach stałego zakresu częstotliwości.

EAP *(Extensible Authentication Protocol}* - jeden
z protokołów uwierzytelniania użytkowników w sieciach
LAN wspierający różne metody uwierzytelniania.

ETSI *(European Telecommunications Standards Institute)* - organizacja opracowuje standardy telekomunikacyjne dla Europy: HiperLAN/li HiperLAN/2 (www.etsi.org).

FHSS *(Frequency Hopping Spread Spectrum}* - metoda modulacji, w której transmitowany sygnał przeskakuje
w określonych odstępach czasu między kilkoma częstotliwościami, unikając w ten sposób interferencji.

IEEE *(Institute of Electrical and Electronics Engineers)* -organizacja zrzeszająca inżynierów, naukowców i studentów zajmujących się szeroko pojętą elektroniką. IEEE liczy obecnie 300 tyś. członków i zajmuje się głównie ustalaniem standardów dla przemysłu komputerowego oraz telekomunikacyjnego (www.ieee.org).

IEEE 802.xx - zestaw specyfikacji dla sieci LAN opracowywanych przez IEEE. Większość sieci kablowych pracuje zgodnie ze specyfikacją 802.3, specyfikacją Ethernet opartą na CSMA/CD lub IEEE 802.5 (sieci *Token Ring}*. Standard IEEE 802.11 definiuje sieci WLAN oparte na trzech niekompatybilnych technologiach: FHSS *(frequency Hopping Spread Spectrum),* DSSS *(Direct Seąuence Spread Spectrum]* i podczerwień.

IETF *(Internet Engineering Task Force)* - organizacja zajmująca się rozwojem Internetu i standaryzacją aplikacji systemowych usprawniających jego funkcjonowanie,

Klient - dowolny komputer podłączony do sieci (kablowej lub bezprzewodowej), korzystający ze świadczonych przez nią usług.

LEAP *(Lightweight Extensible Authentication Pmtocol)* -implementacja protokołu EAP dokonana przez Cisco Systems zapewniająca wzajemne uwierzytelnianie z użyciem prywatnych i publicznych kluczy.

MAC *(Media Access Control]* - protokół kontrolujący pracę nadajnika/odbiornika radiowego. Metoda MAC dostępu do medium odpowiada w modelu ISO warstwie łącza danych *(Data Link).* Standard IEEE 802.11 określa działania protokołu MAC dla metody współdzielonego dostępu do medium, formaty pakietów, adresowanie i wykrywanie błędów.

Mikrokomórka - określony obszar fizyczny, który obsługuje znajdujące się w nim bezprzewodowe komputery. Mikrokomórki zachodzą na siebie, tak aby przy wychodzeniu użytkownika komputera przenośnego z obszaru obsługiwanego przez jeden punkt dostępu do obszaru obsługiwanego przez kolejny punkt dostępu sieć WLAN świadczyła bez przerwy swoje usługi,

NAT *(Network Address Translation)* - translacja adresów IP używanych w obszarze jednej sieci LAN na adresy IP, które są znane w innej zewnętrznej sieci. Jedna sieć jest zaprojektowana jako wewnętrzna, a druga jako zewnętrzna. Sieć wewnętrzna jest postrzegana przez świat zewnętrzny jako jeden zasób. W przypadku sieci WLAN z zewnętrznym połączeniem do Internetu. NAT pozwala współdzielić jedno połączenie internetowe między wszystkimi komputerami bezprzewodowymi.

OFDM *(Orthogonal frequency Dwision Multiplexing)* -metoda modulacji tak zoptymalizowana, aby interfejs bezprzewodowy mógł transmitować dane w środowiskach pełnych zakłóceń, takich jak zatłoczone obszary miejskie. Dlatego OFDM pracuje niezawodnie i nie ma tych ograniczeń i wad (chodzi o odległości, odporność na zakłócenia, łatwość instalowania i rozmiary anteny), które towarzyszą innym systemom łączności bezprzewodowej).

PHY *(Physical Layer)* - najniższa warstwa w modelu OSI odpowiedzialna za transmitowanie strumieni bitów przez fizyczne medium transportujące pakiety. PHY definiuje parametry, takie jak szybkość transmitowania danych, metoda modulacji, parametry sygnałów, synchronizacja

nadajnika/odbiornika. W stosowanych obecnie implementacjach WLAN warstwa PHY odpowiada za przetwarzanie sygnałów radiowych.

Punkt dostępu - urządzenie, które dla bezprzewodowych klientów pełni rolę huba i zapewnia im dostęp do kablowej sieci LAN. Punkt dostępu podwaja zasięg bezprzewodowych klientów (sieci WLAN składające się z wielu punktów dostępu i mikrokomórek mogą obejmować swym zasięgiem największe przedsiębiorstwo) i zawiera mechanizmy zwiększające bezpieczeństwo sieci WLAN.

RADIUS *(Remote Autbentification Dial-ln User Service)* - protokół zdalnej weryfikacji tożsamości użytkowników oraz zdalnego dostępu do serwerów sieci, zaakceptowany przez IEFT. Definiuje on m.in. sposób wymiany danych między serwerem ochrony danych a serwerem zdalnego dostępu, przypisując temu ostatniemu rolę klienta.

Roaming - proces przemieszczania się z obszaru pokrywanego przez jedną komórkę do obszaru pokrywanego przez inną. Z mobilnością mamy do czynienia w przypadku infrastrukturalnych sieci bezprzewodowych, wykorzystujących wiele punktów dostępu. Mówiąc inaczej, jest to przemieszczanie się od jednego punktu dostępu do następnego, nie tracąc ani na chwilę łączności z systemem.

Sieć infrastrukturalna - bezprzewodowa sieć, w której centralnymi punktami topologii są punkty dostępu, W takich sieciach punkty dostępu zapewniają dostęp do kablowej sieci LAN oraz sterują ruchem pakietów wraz z przemieszczaniem się użytkowników.

Sieć niezależna - sieć, która zapewnia połączenia typu *peer-to-peer.*

Tryb *Ad-Hoc* - takie skonfigurowanie klienta, które zapewnia w bezprzewodowej sieci LAN niezależne połączenie *peer-to-peer* (niezależna sieć WLAN). Alternatywna konfiguracja występuje wtedy, gdy komputery komunikują się między sobą przez punkty dostępu (infrastrukturalna sieć WLAN).

Tryb infrastrukturalny - konfiguracja, w której klient komunikuje się z punktem dostępu (patrz: Tryb Ad-Hoc). Punkt dostępu nie tylko uzgadnia cały ruch bezprzewodowy, ale zapewnia komunikacją z kablową siecią LAN.

WEP *(Wired Equivalent Prwacy)* - protokół zdefiniowany w ramach standardu 802.1, dotyczący szyfrowania danych, tak aby włamywacze nie mogli ich przechwytywać. WEP pozwala administratorowi definiować zestaw kluczy szyfrowania dla każdego użytkownika sieci bezprzewodowej, wykorzystując tzw. *Key String.* generowany przez algorytm szyfrowania WEP. Jeśli użytkownikowi nie został przypisany taki klucz, nie uzyska on dostępu do sieci WLAN.

Wielościeżkowość - występuje wtedy, gdy sygnały radiowe są transmitowane między nadajnikiem a odbiornikiem przez wiele ścieżek. [1]

LITERATURA

[1] Networld „Kompedium Wiedzy o Sieciach Bezprzewodowych LAN”

[2] Networld „Integracja WLAN z GPRS/UMTS”