LOKALIZOWANIE

punktów dostępowych oraz urządzeń w sieci bezprzewodowej Wi-Fi

podkom. Tomasz Boroń

Naczelnik Wydziału do Walki z Cyberprzestępczością
Komendy Wojewódzkiej Policji w Bydgoszczy

Niniejszy artykuł stanowi opis sieci bezprzewodowych. Autor przedstawia ich rozwój, typy oraz specyfikę działania. Ponadto omawia metody lokalizowania punktów dostępowych oraz urządzeń w sieci bezprzewodowej.

Zapewnienie bezpieczeństwa teleinformatycznego w obecnych czasach stawia przed Policją nowe wyzwania. Generalnie głównym zadaniem jest monitorowanie, przeciwdziałanie, ujawnianie i gromadzenie dowodów przestępstw dla organów procesowych, pomoc merytoryczna i techniczna podległym jednostkom. Cyberprzestępczość to nie tylko typowe przestępstwa komputerowe wskazane w kodeksie karnym, ale też inne przestępstwa, do których popełnienia zostały użyte urządzenia telekomunikacyjne oraz informatyczne.

Ogrom analizowanych danych, uzyskanych w trakcie ujawniania przestępstw komputerowych, wymusza na prowadzących sprawę poświęcenie większej ilości czasu potrzebnego do ustalenia sprawcy. Dodatkowym utrudnieniem jest brak ujednoliconego systemu, który by standaryzował otrzymane dane od operatorów.

Obecnie, żeby sprostać nowym wyzwaniom, trzeba nieustannie śledzić rozwój nowych technologii oraz nowe metody popełniania przestępstw.

Typowe obszary zagrożeń:

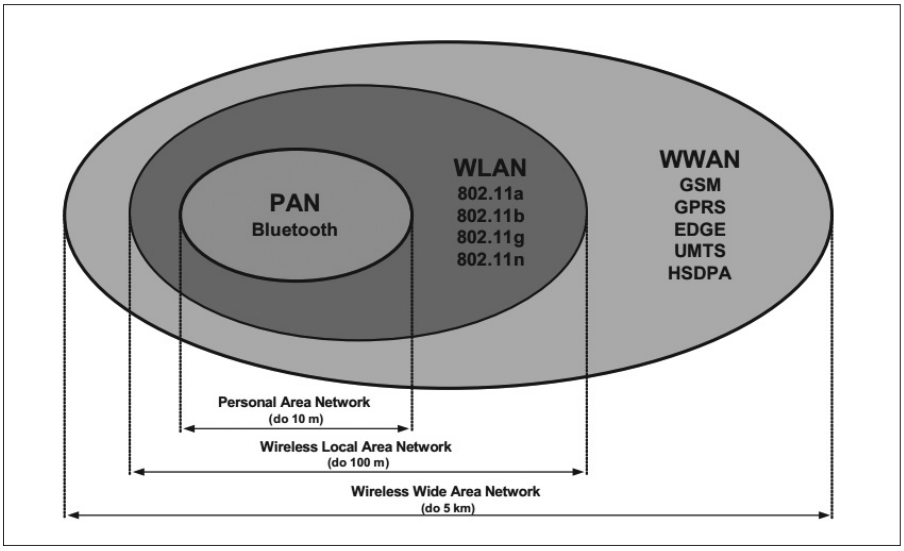
- pornografia dziecięca;
- propagowanie przemocy, nienawiści, zakazanych ideologii;
- przejmowanie tożsamości;
- przełamywanie zabezpieczeń kont pocztowych, kont bankowości elektronicznej, kont na portalach społecznościowych;
- szantaż;
- podrabianie dokumentów i pieniędzy;
- kradzież własności intelektualnych;
- e-handel zakazanymi produktami;
- oszustwa na portalach aukcyjnych;
- podsłuch elektroniczny;
- niszczenie, wykradanie danych;
- zakłócanie pracy serwerów/komputerów w sieci;
- wykorzystywanie komunikatorów do komunikowania się sprawców.

W dzisiejszych czasach urządzenia Wi-Fi opanowały większość gałęzi życia człowieka. W niektórych dziedzinach ich obecność jest niezbędna. Urządzenia te gromadzą i udostępniają duże ilości danych. Jednak, aby udostępniać nam swoje zasoby, muszą się między sobą porozumieć. Dlatego są one połączone w sieci komputerowe. Jedną z takich sieci jest bezprzewodowa sieć lokalna.

Rozwój sieci bezprzewodowych na świecie kształtował się w trzech etapach. Pierwszy etap to teoretyczna koncepcja badań i poszukiwań możliwych zastosowań. Drugi etap to projektowanie sprzętu i jego rozwój. Trzeci etap związany jest z promowaniem i upowszechnieniem komunikacji bezprzewodowej. Badania nad rozwojem sieci bezprzewodowych odbywały się w dwóch kierunkach, tj. w związku ze świadczeniem usług związanych z komunikacją głosową oraz wymianą danych.

Obecnie mamy dwa typy sieci bezprzewodowej, które ze względu na zasięg możemy podzielić na dwa rodzaje. Są to sieci lokalne o niewielkim zasięgu oraz sieci rozległe WAN, których zasięg wielokrotnie przekracza górną granicę możliwości sieci lokalnych.

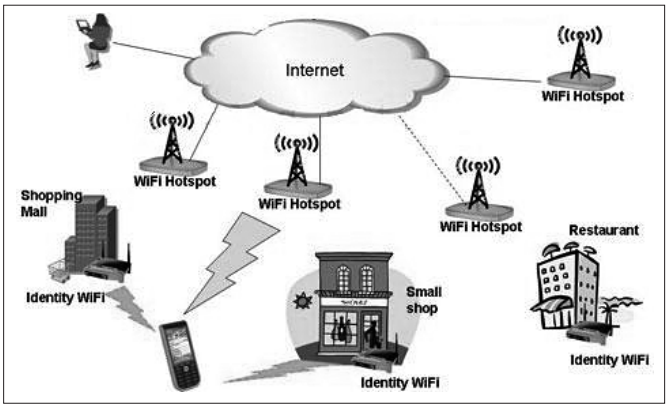
Teraz wystarczy połączenie z Internetem, aby móc dokonać zakupów w polskich i zagranicznych sklepach, wykonać szybkie i bezpośrednie płatności poprzez bankowe konta elektroniczne, wymieniać się danymi czy komunikować z ludźmi na całym świecie. Niskie ceny sprzętu komputerowego spowodowały, że komputer jest praktycznie w każdym gospodarstwie domowym, a łatwość jego konfiguracji sprawiła, że każdy po uruchomieniu systemu operacyjnego może połączyć się z globalną siecią.
Wprowadzanie nowych technologii dostępu do sieci oraz miniaturyzacja sprzętu komputerowego umożliwiają użytkownikom korzystanie z sieci bezprzewodowych, dzięki którym nie są ograniczeni długością „kabla" czy miejscem, w którym jest komputer.



Rys. 2. Typowy zasięg sieci bezprzewodowych.
Źródło: Sieci komputerowe, dr inż. Andrzej Opaliński, AGH Kraków, http://docplayer.pl/2951424-Sieci-komputerowe-sieci-bezprzewodowe-wydzial-inzynierii-metali-i-informatyki-przemyslowej-dr-inz-andrzej-opalinski-www-agh-edu.html.

Bezprzewodowe sieci lokalne

Historia sieci radiowych rozpoczęła się w okresie II wojny światowej. Pierwsze transmisje były przeprowadzane przez armię Stanów Zjednoczonych. Następnie na Uniwersytecie Hawajskim zbudowano pierwszą sieć bezprzewodową o nazwie „ALOHNET". Była to sieć o zasięgu lokalnym w topologii gwiazdy. Dziś większość dostępu do Internetu realizowana jest z udziałem komputerów przenośnych wyposażonych w kartę sieciową przeznaczoną do pracy w standardzie „802.11", który określa zasady pracy urządzeń. Technologia lokalnych sieci bezprzewodowych umożliwia transmisję danych w zależności od miejsca, od 30 do 300 m w terenie otwartym (rys. 1). Z wykorzystaniem anten kierunkowych odległość tę można zwiększyć do kilkunastu kilometrów. Aby osiągnąć tak duże odległości, muszą być zachowane pewne warunki, czyli pomiędzy antenami nie mogą występować żadne przeszkody w postaci np. murów, drzew. Jednakże wraz ze wzrostem odległości pogarsza się jakość sygnału, a szybkość transmisji danych maleje.



Rys. 1. Przykład zastosowania sieci bezprzewodowej.
Źródło: http://lejinternetplaza.com/what-is-wifi-and-how-to-use-it/.

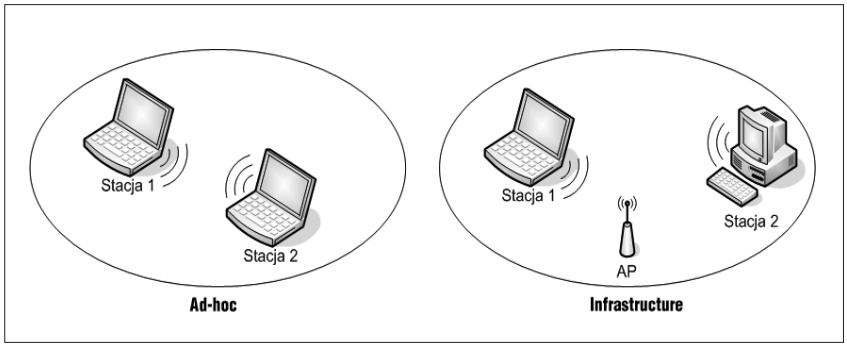
Standard 802.11

Obecnie istnieje wiele metod uzyskania połączenia bezprzewodowego – od łączy „IrDA" (podczerwień), poprzez „Bluetooth", sieci w standardzie „802.11", aż po bardzo drogie, wymagające profesjonalnego montażu, radiolinie. Jednakże ze względu na praktyczne zastosowanie, popularność i niedrogie urządzenia w tego typu połączeniach, standard „802.11" jest najczęściej wykorzystywany. Zasięg typowych sieci bezprzewodowych waha się w granicach: do 10 metrów – „Bluetooth", do 200 m – sieci w standardzie „802.11", aż po sieci „WWAN", które osiągają zasięg do 5 kilometrów (rys. 2).
Do chwili obecnej wykorzystywane były i są m.in. następujące wersje standardu „802.11" (tab. 1): „802.11", „802.11a", „802.11b", „802.11g", „802.11n".

Tabela 1. Porównanie standardów sieci bezprzewodowej 802.11.
Źródło: opracowanie własne.

	IEEE 802.11	IEEE 802.11a	IEEE 802.11b	IEEE 802.11g	IEEE 802.11n
Zasięg	60 m	75 m	100 m	100 m	200 m
Maksymalna szybkość transmisji	2 Mb/s	54 Mb/s	11 Mb/s	54 Mb/s	200/540 Mb/s
Wrażliwość na zakłócenia	średnia	średnia	mała	duża	mała
Długość fali / częstotliwość	2,4 GHz	5 GHz	2,4 GHz	2,4 GHz	2,4/5 GHz

Komunikacja w sieci bezprzewodowej WLAN odbywa się za pomocą modulowanej fali radiowej o częstotliwości 2,4 GHz (802.11b/g) oraz 5 GHz (802.11a, 802.11n).
Zastosowany rodzaj techniki umożliwiający podział zasobów komunikacyjnych pozwala na sprawną wymianę danych. Podstawowa technika zgodna ze standardem 802.11g wykorzystuje podział czasu (TDMA). Użytkownicy korzystają z jednej częstotliwości, ale każdy nasłuchuje w innym czasie. Innym rozwiązaniem jest współdzielenie częstotliwości, czyli komunikowanie się w tym samym czasie na różnych częstotliwościach. Następne rozwiązanie to używanie sieci w tym samym czasie i na tej samej częstotliwości z wykorzystaniem kodowania ortogonalnego[1] pozwalającego wyodręb-



Rys. 3. Dwa różne tryby pracy: Ad-Hoc i Infrastructure. Źródło: https://pl.wikipedia.org/wiki/Punkt_dostępu.

nić transmisję wygenerowaną przez konkretnego użytkownika (CDMA). W nowszych rozwiązaniach zastosowano technikę unikalnego podziału czasu i częstotliwości dla danego użytkownika (OFDMA).
Sygnał radiowy dociera do odbiornika wieloma ścieżkami. Związane jest to z odbijaniem się fal od przeszkód znajdujących się w zasięgu sieci radiowej, dlatego do odbiornika dociera wiele wersji tego samego sygnału w różnych odstępach czasu. Opóźnienie sygnału może spowodować zakłócenia, w wyniku czego sygnał stanie się niezrozumiały dla odbiornika.

Architektura i topologia sieci w standardzie 802.11

Architektura sieci w standardzie „802.11" umożliwia połączenie sieci bezprzewodowych w dwóch trybach pracy (rys. 3):
- „Ad-hoc" – sieć tymczasowa,
- „Infrastructure" – sieć stacjonarna.

Sieci tymczasowe „Ad-hoc" wykorzystują komunikację „P2P" do przesyłania danych. W tym trybie pracy nie jest wymagany „Access Point"w celu zapewnienia fizycznego połączenia z siecią przewodową. Takie sieci tworzone są m.in. na potrzeby konferencji, zjazdów, spotkań. Wadą takiego rozwiązania jest niewielki zasięg.
Sieci stacjonarne „Infrastructure" zawierają element stały, tzw. „Access Point", który pośredniczy w transmisji danych pomiędzy siecią bezprzewodową a siecią przewodową. Cały ruch odbywa się za pośrednictwem „Access Point". Punkty dostępowe „Access Point" połączone są przewodem z siecią przewodową.
Najczęściej sieć bezprzewodowa jest uzupełnieniem tradycyjnej sieci przewodowej.
Obecnie wśród sieci bezprzewodowych można wyróżnić dwa typy topologii:
- **topologia gwiazdy** – najbardziej popularna; w celu komunikacji wykorzystuje jeden punkt dostępu („Access Point"); pakiet danych wysłany z węzła sieciowego jest odbierany w stacji centralnej i kierowany przez nią do odpowiedniego węzła; sieci budowane w tej topologii mają duże możliwości i są wydajne;
- **topologia kraty** – w sieciach kratowych poszczególne węzły (punkty „Access Point") nie komunikują się z innymi węzłami za pośrednictwem centralnych punktów przełączania, ale wymieniają z nimi dane bezpośrednio lub przez inne węzły wchodzące w skład kraty.

Działanie protokołu 802.11

Komputer z włączoną kartą bezprzewodową może się znajdować w trzech stanach pracy:
- stan początkowy – sieć nie jest uwierzytelniona i skojarzana z punktem dostępowym,
- uwierzytelniony,
- uwierzytelniony i skojarzony – sieć jest uwierzytelniona i skojarzona z danym punktem dostępowym.

Aby komputer mógł się połączyć z daną siecią, musi dokonać najpierw skanowania. Najprostszą metodą wykrywania sieci jest skanowanie pasywne. Każdy punkt dostępowy wysyła co jakiś określony czas ramkę informacyjną. Ramka ta dostarcza informacje, dzięki którym nasłuchujący komputer może podjąć próbę podłączenia się do punktu dostępowego. W przypadku wielu punktów dostępowych komputer wybiera sobie punkt dostępowy o największej sile nadawania.
Dalej następuje proces przyłączania realizowany w całości przez komputer do punktu dostępowego wybranego w procesie skanowania.
Następnie realizowane jest uwierzytelnianie tylko przez komputer. Punkt dostępowy w tym momencie traktowany jest jako wiarygodny.
Po uwierzytelnieniu komputer kojarzony jest z punktem dostępowym. Proces ten polega na przydzieleniu numeru AID (Association ID), który służy do identyfikowania komputera w procesie buforowania ramek przez punkt dostępowy.

Warstwa fizyczna IEEE 802.11

Sieć IEEE 802.11 wykorzystuje obszar ISM w paśmie 2,4 GHz (od 2400 do 2485 MHz).

Tabela 2. Standardy sieci WLAN.
Źródło: opracowanie własne.

Standard	Pasmo	Zasięg w pomieszczeniu	Zasięg w przestrzeni otwartej
802.11a	5 GHz	30–35 m	75 m
802.11b	2,4 GHz	50 m	120 m
802.11g	2,4 GHz	35 m	~ 100 m
802.11n	2,4 / 5 GHz	70 m	~ 100 m

Tabela 3. Kanały i częstotliwości.
Źródło: https://pl.wikipedia.org/wiki/IEEE_802.11.

Kanał	Dolna częstotliwość [GHz]	Środkowa częstotliwość [GHz]	Górna częstotliwość [GHz]
1	2	3	4
1	2,401	2,412	2,423
2	2,406	2,417	2,428
3	2,411	2,422	2,433

1	2	3	4
4	2,416	2,427	2,438
5	2,421	2,432	2,443
6	2,426	2,437	2,448
7	2,431	2,442	2,453
8	2,436	2,447	2,458
9	2,441	2,452	2,463
10	2,446	2,457	2,468
11	2,451	2,462	2,473
12	2,456	2,467	2,478
13	2,461	2,472	2,483
14	2,473	2,484	2,495

Propagacja[2] fali radiowej w pomieszczeniu

Propagacja fali radiowej w budynku jest specyficzna, ponieważ napotyka na różne przeszkody, które tłumią sygnał. Do obliczenia tłumienia sygnału w pomieszczeniu wykorzystywany jest np. model „Multi-Wall".
Polega na badaniu poziomu sygnału po jego przejściu przez różnego rodzaju przeszkody. Model ten bazuje na obliczeniu różnicy mocy sygnału przebiegającego w linii prostej od nadajnika do odbiornika, natrafiającego na różnego typu przeszkody (sygnał jest osłabiany o daną wartość charakterystyczną dla tej przeszkody).

Tabela 4. Charakterystyka tłumienia wg modelu „Multi Wall". Źródło: Ł. Jasiński, *Pomiar tłumienia ścian i innych elementów charakterystycznych dla środowiska wewnątrzbudynkowego w paśmie 2,4 GHz,* Wrocław 2011.

Nazwa elementu	Materiał	Grubość [cm]	Tłumienie [dB]
Ściana wewnętrzna	Cegła	10	7
Ściana zewnętrzna	Cegła	3	9
Ściana działowa	Rigips i wełna szklana	7	2
Strop	Beton	30	11
Okno	Szkło	szyba x 2 + przerwa 1 cm	4,5
Drzwi	Drewno	4	2,5

Wady sieci radiowych

Korzystanie z sieci radiowych wiąże się z występowaniem następujących zakłóceń:
- ściany budynku obniżają szybkość przesyłu danych,
- urządzenia elektryczne zakłócają fale radiowe,
- rozproszenie energii,
- zakłócenia zewnętrzne,
- wzajemne zakłócanie się urządzeń bezprzewodowych.

Sprzęt do transmisji bezprzewodowej

Sieć bezprzewodowa do wysyłania i odbierania danych używa fal elektromagnetycznych (radiowych lub podczerwonych). Transmitowane dane nakładane są na nośnik radiowy (fale radiowe), które to później odbierane są przez punkt odbiorczy.
W dziedzinie sprzętu stosowanego do transmisji danych w sieciach bezprzewodowych panuje ogromna różnorodność. Istnieje wiele rozwiązań, różniących się przeznaczeniem, parametrami technicznymi i ceną.
Do budowy lokalnych sieci bezprzewodowych wykorzystywane są najczęściej następujące urządzenia:
- bezprzewodowe karty sieciowe,
- punkt dostępowy i router,
- anteny.

Bezprzewodowe karty sieciowe

Każdy komputer, aby mógł pracować w sieci, musi być wyposażony w bezprzewodową kartę sieciową. Jest ona podstawowym elementem każdej sieci. Karty te mają identyczne przeznaczenie jak karty sieci przewodowych. Wyróżniamy karty PCI, karty wbudowane w komputerze przenośnym, karty na USB i inne. Takie karty zawierają nadajnik radiowy.
Wybór bezprzewodowej karty sieciowej jest bardzo istotny, bowiem występują znaczne różnice pomiędzy dostępnymi kartami sieciowymi. W celu wyboru jak najlepszej karty sieciowej należy zwrócić uwagę na:
- rodzaj chipsetu znajdującego się na karcie,
- moc wyjściową i możliwości jej dowolnej zmiany,
- czułość odbiornika,
- obecność anten zewnętrznych,
- obsługa standardu „802.11".

Punkt dostępowy i router

Bezprzewodowy punkt dostępowy („Access Point") jest to urządzenie, które zapewnia komputerom dostęp do zasobów sieci. Punkty dostępowe mogą komunikować się ze sobą, co umożliwia budowę bardzo rozległych sieci bezprzewodowych.
Bezprzewodowy router pełni rolę węzła komunikacyjnego, służącego do rozdzielania sygnału i rozgałęzienia połączeń sieciowych.

Anteny wykorzystywane w sieciach bezprzewodowych

Urządzenia wykorzystujące łączność bezprzewodową nie mogą obejść się bez anten. Dzięki nim możemy zwiększyć zasięg poprzez skupienie sygnału radiowego oraz szerokość

wiązki promieniowania. Anteny charakteryzuje się za pomocą dwóch głównych parametrów: zysku i szerokości wiązki. Czasami pod uwagę bierze się strefę pokrycia i polaryzację. Anteny charakteryzują się następującymi parametrami:

- promieniowanie,
- kąt promieniowania,
- zysk,
- polaryzacja.

Ateny dzielimy na trzy podstawowe kategorie:

- antena dookólna,
- antena sektorowa,
- antena kierunkowa.

Antena dookólna

Może być instalowana na maszcie, na podstawie, na płaszczyźnie masy lub do sufitu. Emituje sygnał równomiernie we wszystkich kierunkach, w płaszczyźnie poziomej, okrywając kąt 360 stopni. Wykorzystywana jest w celu zwiększenia zasięgu sieci. Typowym zastosowaniem anten dookólnych jest połączenie punkt – wielopunkt z centralnym punktem dostępowym obsługującym wielu klientów, a czasami inne punkty dostępowe korzystające z anten kierunkowych.

Antena sektorowa

Emituje sygnał w sektorze określonym za pomocą kąta od 90 do 200 stopni. Anteny tego typu najczęściej wykorzystywane są w połączeniach poprzez ulicę albo w celu pokrycia długiego holu lub korytarza. Anteny sektorowe rozmieszczone dookoła, co pewien kąt, mogą zastąpić anteny dookólne.

Antena kierunkowa

Emituje najwęższy sygnał (sygnał jest skupiony) i dzięki temu antena tego typu ma największy zysk energetyczny. Stosowana jest w przypadku połączeń na duże odległości.

Metody lokalizacji

Urządzenia bezprzewodowe można lokalizować za pomocą metod tradycyjnych, takich jak pomiar kąta nadejścia sygnału (AoA), pomiar czasu, w jakim sygnał pokonuje drogę od nadajnika do odbiornika (ToA), a także za pomocą siły odbieranego sygnału (RSS).

Najbardziej rozpowszechnione metody lokalizowania to:

- trilateracja,
- triangulacja,
- Radio Frequency Fingerprinting.

Trilateracja

Metoda polegająca na obliczeniu odległości z co najmniej trzech punktów. Bieżące położenie urządzenia to miejsce, gdzie nakładają się trzy okręgi ze środkami w punktach orientacyjnych, a promienie okręgów wyznaczane są przez odległości od poszczególnych punktów orientacyjnych.

Triangulacja

Metoda polegająca na wyznaczaniu w terenie współrzędnych punktu. Punkt dostępu, który odbiera sygnał, wyznacza okręg. Bieżące położenie urządzenia to miejsce, gdzie nakładają się trzy okręgi ze środkami w punktach orientacyjnych, a promienie okręgów wyznaczane są przez odległości od poszczególnych punktów orientacyjnych.

Radio Frequency Fingerprinting

System do pomiaru częstotliwości radiowej jest skalibrowany poprzez pomiar siły odbieranego sygnału w określonych miejscach.

Dane te są wysyłane do bazy danych. W momencie próby znalezienia urządzenia bezprzewodowego, każdy punkt dostępu odpowiada. Następnie system śledzenia lokalizacji bierze informacje uzyskane z punktów dostępu i tworzy model środowiska radiowego.

Podsumowanie

W obecnych czasach nastąpił gwałtowny rozwój cyberprzestępczości. Sprawcy tego typu przestępstw mają coraz większą wiedzę z dziedziny informatyki, a co za tym idzie – potrafią również zacierać ślady swojej działalności przestępczej.

Dowodem działalności przestępczej może być ruch w sieci, zachowane dane w urządzeniach sieciowych, w urządzeniach pamięci masowej, urządzeniach przenośnych, zapisy w historii przeglądarek internetowych, wpisy w rejestrze po stronie klienta, jak i po stronie serwera.

Namierzanie użytkownika w otwartym terenie z rozproszoną zabudową nie sprawia większych problemów. Duży problem stanowi wskazanie dokładnego miejsca przy zabudowie zwartej.

Idea powstania urządzenia umożliwiającego lokalizowanie urządzeń pracujących w standardzie „802.11" pozwoli identyfikować użytkowników korzystających z sieci Wi-Fi, którzy za jej pomocą popełniają przestępstwa. Będzie również stanowić pomoc w ratownictwie, poszukiwaniu osób zaginionych oraz skradzionego sprzętu teleinformatycznego.

[1] Ortogonalność (z gr. *ortho* – prosto, prosty, *gonia* – kąt) – uogólnienie pojęcia prostopadłości znanego z geometrii euklidesowej na abstrakcyjne przestrzenie z określonym iloczynem skalarnym, jak np. przestrzenie unitarne (w tym przestrzenie Hilberta) czy przestrzenie ortogonalne. Pojęcie ortogonalności bywa uogólnianie również na przestrzenie unormowane, w których nie ma naturalnej struktury iloczynu skalarnego (ortogonalność w sensie Pitagorasa, ortogonalność w sensie Jamesa, ortogonalność w sensie Birkhoffa, T-ortogonalność). Źródło: https://pl.wikipedia.org/wiki/Ortogonalno%C5%9B%C4%87 [dostęp: 13.12.2017 r.].

[2] https://pl.wikipedia.org/wiki/Propagacja_fal_radiowych acji [dostęp: 13.12.2017 r.].

Summary

Locating access points and devices in the Wi-Fi wireless network

The present article constitutes the description of wireless networks. The author presents their development, types and specificity of action. Moreover he discusses methods of locating access points and devices in the wireless network.

Tłumaczenie: Joanna Łaszyn