POLITECHNIKA WARSZAWSKA
WYDZIAŁ ELEKTRONIKI I TECHNIK INFORMACYJNYCH
INSTYTUT TELEKOMUNIKACJI
ZAKŁAD TELEINFORMATYKI I TELEKOMUTACJI

STEGANOGRAFIA W BEZPRZEWODOWYCH SIECIACH LOKALNYCH

ROZPRAWA DOKTORSKA

Autor
mgr inż. Krzysztof Stanisław Szczypiorski

Promotor
prof. dr hab. Józef Lubacz

Warszawa, wrzesień 2006

False face must hide what the false heart doth know

William Shakespeare, *The Tragedy of Macbeth*

Streszczenie

W pracy przedstawiono i przeanalizowano system steganograficzny HICCUPS (*Hidden Communication System for Corrupted Networks*) przeznaczony dla bezprzewodowych sieci lokalnych (*Wireless Local Area Networks* – WLAN), zgłoszony do Urzędu Patentowego RP jako wynalazek. Opracowany przez autora rozprawy system HICCUPS wykorzystuje ramki z niepoprawnymi sumami kontrolnymi jako metodę na stworzenie dodatkowego, dostępnego na żądanie, pasma do ukrywania informacji. W pracy zaprezentowano dziedzinę steganografii sieciowej, która zrywa z pierwotnym paradygmatem steganografii, wiążącym się z wprowadzaniem w błąd wyłącznie zmysłów człowieka. Dla sieci WLAN, działających wg standardu IEEE 802.11, przedstawiono „ortogonalne" do zagadnień steganografii mechanizmy bezpieczeństwa, w tym WEP (*Wired Equivalent Privacy*), TKIP (*Temporal Key Integrity Protocol*) i CCMP (*CCM Protocol*). Opisano system HICCUPS dla sieci o współdzielonym medium, definiując warunki niezbędne do jego realizacji, a także architekturę oraz koncepcję jego działania. Poddano dyskusji kwestie związane z realizacją systemu HICCUPS w sieciach IEEE 802.11 zwracając uwagę na specyfikę metody dostępu do medium CSMA/CA (*Carrier Sense Multiple Access with Collision Avoidance*). Dokonano analizy właściwości systemu HICCUPS, w szczególności wyznaczono jego efektywność i „koszt" działania w WLAN. Analizę przeprowadzono z wykorzystaniem nowego, zaproponowanego w pracy, modelu CSMA/CA.

Składam serdeczne podziękowania Panu prof. dr. hab. Józefowi Lubaczowi za życzliwą i cierpliwą opiekę merytoryczną. Mam nadzieję, że dzięki naszej współpracy niniejsza rozprawa jest pierwszym, ale nie ostatnim owocem zmiany mojego myślenia.

Dziękuję również Kolegom z Zakładu Teleinformatyki i Telekomutacji IT PW, w szczególności: dr. inż. Krzysztofowi Brzezińskiemu, dr. inż Michałowi Jarocińskiemu i dr. inż. Sławomirowi Kuklińskiemu, a także mgr. inż. Romanowi Dygnarowiczowi z Ministerstwa Obrony Narodowej oraz Panu prof. dr. hab. Andrzejowi Dudzie z *École Nationale Supérieure d'Informatique et de Mathématiques Appliquées de Grenoble* (Francja).

Szczególne podziękowania składam mojej Rodzinie, w tym moim Dzieciom, Aleksandrowi oraz Matyldzie, za wiele wyrzeczeń oraz wyrozumiałość.

Spis treści

Lista tabel

Lista rysunków

1. Wprowadzenie

1.1 Wstęp

Słowo *steganografia* pochodzi z greckiego (*στεγανογραφία*) i oznacza dosłownie *osłonięte, zakryte pisanie* (*covered writing*), podczas gdy kryptografia (*κρυπτογραφία*) utożsamia *ukryte, tajne pisanie* (*secret*, *hidden writing*). Steganografia jest techniką przekazywania informacji bez ujawniania **istnienia informacji**, natomiast kryptografia chroni **treść informacji** przed wyjawieniem.

Cel użycia steganografii znakomicie ilustruje dylemat więźniów opisany przez G. Simmonsa w pracy [87]. Dwóch współwinnych zostaje osadzonych w oddzielnych, niesąsiadujących ze sobą, celach. Strażnik zezwala więźniom na komunikację za pomocą zaufanego sobie posłańca, jednak podejrzewa, że będą planować ucieczkę. Zatem aby wymiana informacji nie została uznana za spisek – wymieniane przez więźniów wiadomości nie mogą wyglądać podejrzanie. Więźniowie muszą użyć metody przekazywania informacji, która ukrywa istnienie tej komunikacji, a więc **steganografii**. Jeśli wysłana wiadomość będzie niezrozumiała dla posłańca (np. zabezpieczona przez kryptografię za pomocą szyfru), to komunikacja pomiędzy więźniami zostanie przerwana.

Jak wskazuje przykład dylematu więźniów, w przypadku otwartego kanału kryptografia zdradza tajną komunikację. Jednak dla ustalonego kanału utworzonego przez steganografię, kryptografia może ten kanał dodatkowo chronić.

Techniki steganograficzne są znane i używane od wielu wieków. Pierwsze metody zostały opisane prawie 2500 lat temu przez starożytnego historyka greckiego Herodota z Halikarnasu [57]. Herodot opisał m.in. użycie drewnianych tabliczek i wosku jako metody przekazywania informacji o planowanym ataku perskiego króla Kserksesa na Grecję, wysyłanie wiadomości w jamie brzusznej upolowanych zwierząt, tatuowanie wiadomości na głowie zaufanych więźniów i posyłanie ich z tak ukrytą informacją po odrośnięciu włosów. Innym klasycznym przykładem techniki steganograficznej jest użycie atramentu sympatycznego [57]. 2000 lat temu Owidiusz w „Sztuce miłości" („*Ars amatoria*") opisał użycie mleka do pisania w sposób niewidoczny. Odczyt tego typu **steganogramów** (wiadomości zawierających ukryte treści) polegał na posypaniu sadzą papieru i odzyskaniu informacji zapisanych uprzednio za pomocą mleka.

Historyczne przykłady można przytaczać bez końca, udowadniając pomysłowość i przebiegłość ludzkiego umysłu. Warto jednak podkreślić, że historycznym paradygmatem steganografii było ukrycie informacji przede wszystkim przed ludzkimi zmysłami. Współczesne prace badawcze z tej dziedziny koncentrują się na ukrywaniu informacji w multimediach (obrazy i dźwięk), co jest tożsame z „oszukiwaniem" ludzkich zmysłów (wzroku i słuchu).

W **steganografii sieciowej,** mamy do czynienia z technikami, które nie są związane z wprowadzaniem w błąd zmysłów człowieka, lecz z ukrywaniem informacji przed innymi

stacjami sieciowymi. W tym sensie steganografia sieciowa jest nowym trendem oderwanym od historycznego paradygmatu. Ze względu na to, że stacje sieciowe komunikują się za pomocą protokołów telekomunikacyjnych, istotą tej odmiany steganografii jest manipulowanie elementami protokołów, takimi jak opcjonalne pola, sekwencje wysyłanych wiadomości, kody transmisyjne i tym podobne.

Po atakach terrorystycznych na Stany Zjednoczone z 11 września 2001 roku notuje się wzmożone zainteresowanie omawianą dziedziną, w szczególności w zakresie rozpoznawania oraz zwalczania przekazów steganograficznych. Powodem tego zainteresowania jest postawiona, nie tylko w mediach, hipoteza ([66], [6]), że techniki ukrywania informacji mogły posłużyć do swobodnej komunikacji pomiędzy terrorystami przygotowującymi serię zamachów.

W ujęciu sieciowym przekazy steganograficzne mogą być dokonywane we wszystkich warstwach sieci [39]. Niniejsza rozprawa koncentruje się na ukrywaniu informacji w podwarstwie MAC (*Medium Access Control*) lokalnych sieciach bezprzewodowych (WLAN – *Wireless LANs*), działających wg standardu IEEE 802.11 ([44], [78]).

Przedstawiony i przeanalizowany w tej pracy system o akronimie **HICCUPS** (***Hi****dden* ***C****ommuni****c****ation System for Corr****up****ted Network****s***) jest pierwszym znanym w literaturze systemem steganograficznym dla sieci WLAN [63]. Istota systemu polega przede wszystkim na wykorzystaniu ramek z niepoprawnie stworzonymi sumami kontrolnymi jako środka umożliwiającego przesłanie steganogramów. Słowo ***hiccups*** oznacza w języku angielskim atak czkawki i w rozważanym przez nas przypadku ma obrazować sposób działania sieci, w której co pewien czas pojawiają się uszkodzenia (czkawka), wyglądające na efekt błędów w kanale. System HICCUPS może być zanurzony w środowisku sieciowym, które jest chronione za pomocą metod kryptograficznych. Metody ochrony informacji są „ortogonalne" w stosunku do steganografii i pełnią rolę „szumu" informacyjnego utrudniającego rozdzielenie steganogramów od zwykłych wiadomości.

System HICCUPS został zgłoszony przez Politechnikę Warszawską do Urzędu Patentowego RP, jako wynalazek pod tytułem *Sposób steganograficznego ukrywania i przesyłania danych dla sieci telekomunikacyjnych ze współdzielonym medium transmisyjnym oraz układ formowania ramek warstwy sterowania dostępem do medium* (zgłoszenie wynalazku nr 359660 z 11 kwietnia 2003 [97]). Zgłoszenie, którego głównym twórcą jest autor tej pracy, zawierało opis metody działania i schemat logiczny generycznej karty sieciowej realizującej system HICCUPS.

Po zgłoszeniu wniosku patentowego system HICCUPS został przedstawiony na kilku konferencjach poświęconych bezpieczeństwu sieciowemu (m.in. *Advanced Computer Systems* [100], Enigma [99], Krajowe Sympozjum Telekomunikacji [103]), także w kontekście stanu sztuki w tej dziedzinie (Krajowa Konferencja Bezpieczeństwa Biznesu [101], Krajowa Konferencja Bezpieczeństwa Sieciowego [102]).

Referat [100] doczekał się kilku cytowań, w tym najbardziej znaczącego [73] na uznawanej za najpoważniejszą w dziedzinie steganografii konferencji *7th Information*

Hiding Workshop w 2005 roku. W publikacji [63] z września 2006 stwierdzono, że system HICCUPS jest jedynym znanym do tej pory systemem steganograficznym dla sieci WLAN.

Poza Politechniką Warszawską [94] system HICCUPS był przedmiotem analiz na *Otto-von-Guericke-Universität* w Magdeburgu (Niemcy) [64] oraz na *University of Houston-Clear Lake* (Stany Zjednoczone) [86].

1.2 Cele i teza rozprawy

Celem niniejszej rozprawy jest przedstawienie i analiza systemu steganograficznego HICCUPS dla WLAN. Ogólny cel pracy zostanie osiągnięty poprzez:

- prezentację stanu sztuki w dziedzinie steganografii sieciowej,
- przedstawienie architektury i funkcji systemu HICCUPS w kontekście sieci o współdzielonym medium, a zwłaszcza WLAN,
- omówienie zagadnień bezpieczeństwa WLAN w kontekście systemu HICCUPS,
- analizę działania protokołu dostępu do medium CSMA/CA (*Carrier Sense Multiple Access with Collision Avoidance*) pod kątem użycia systemu HICCUPS,
- stworzenie modelu analitycznego 802.11 CSMA/CA bazującego na łańcuchach Markowa,
- zastosowanie zaproponowanego modelu do analizy systemu HICCUPS,
- analizę efektywności i „kosztu" działania systemu HICCUPS w WLAN.

Realizacja tak sformułowanych celów pozwala sformułować i obronić następującą tezę rozprawy:

Teza: System HICCUPS jest efektywną techniką steganograficzną dla bezprzewodowych sieci lokalnych wykorzystującą ramki z celowo niepoprawnie stworzonymi sumami kontrolnymi.

1.3 Układ pracy

Praca składa się z siedmiu rozdziałów.

W rozdziale 2 zaprezentowano bezpieczeństwo informacyjne sieci WLAN jako tło dla systemu HICCUPS.

W rozdziale 3 przedstawiono zagadnienia związane ze steganografią w ujęciu sieciowym.

W rozdziale 4 zawarto ogólny opis architektury i funkcji systemu HICCUPS.

W rozdziale 5 przedstawiono realizację systemu HICCUPS dla IEEE 802.11, w szczególności zaprezentowano współpracę systemu z protokołem dostępu do medium CSMA/CA.

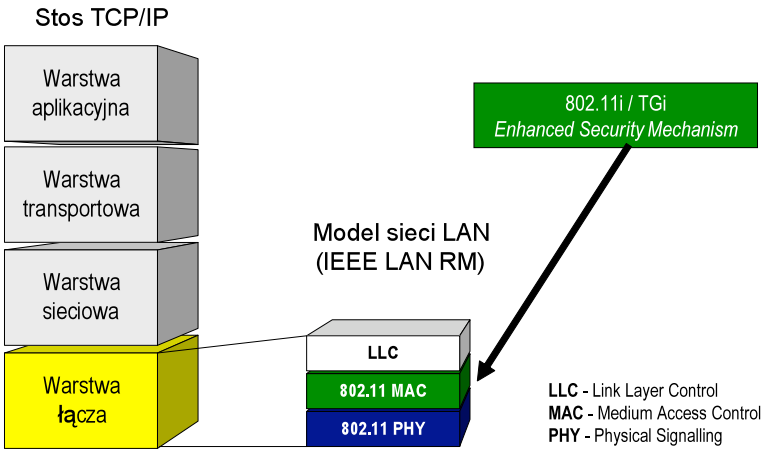
W rozdziale 6 zaproponowano model analityczny 802.11 CSMA/CA oparty na łańcuchach Markowa uwzględniający błędy w kanale oraz jego adaptację dla systemu HICCUPS. Następnie przeanalizowano efektywność i „koszt" działania systemu HICCUPS w WLAN.

W ostatnim rozdziale podsumowano pracę.

2. Bezpieczeństwo informacyjne bezprzewodowych sieci lokalnych[1]

2.1 Podstawowe cechy standardów WLAN

Bezprzewodowe sieci lokalne (znane także pod nazwami IEEE 802.11, Wi-Fi – *Wireless Fidelity*) są przykładem jednej z najbardziej innowacyjnych technologii ostatniego ćwierćwiecza. Obok sieci TCP/IP i telefonii IP można je śmiało uznać za jedno z najważniejszych dokonań we współczesnych technikach teleinformatycznych. Główną „chorobą wieku dziecięcego" sieci WLAN, podobnie jak wielu innych rozwiązań sieciowych, było nikłe ich bezpieczeństwo ([4], [15], [96], [98]). Obecnie oferowana przez rozszerzenie standardu IEEE 802.11 – IEEE 802.11i-2004 – ochrona informacji w sieciach WLAN jest już na przyzwoitym poziomie i eliminuje wiele dotychczasowych słabych punktów. Standard 802.11 stanowi rozwinięcie faworyzowanej przez producentów koncepcji *Ethernet everywhere* – jest naturalną bezprzewodową mutacją sieci Ethernet (IEEE 802.3 – [52]). WLAN odziedziczył po IEEE 802.3 podobną strukturę ramki i dostosowany do sieci bezprzewodowych protokół dostępu do medium CSMA/CA (*Carrier Sense Multiple Access with Collision Avoidance*) zamiast CSMA/CD (*Carrier Sense Multiple Access with Collision Detection*). Z tego też powodu sieci WLAN określane są mianem bezprzewodowego Ethernetu (*Wireless Ethernet*).



Rysunek 2-1 Warstwy sieci IEEE 802.11

Podobnie jak inne sieci lokalne, WLAN bazuje na modelu sieci IEEE LAN RM (RM – *Reference Model*) – Rysunek 2-1. Znamienna dla 802.11 jest warstwa 802.11 PHY (warstwa fizyczna – *Physical Signalling*) i podwarstwa 802.11 MAC. Bezpieczeństwo WLAN jest przeważnie realizowane w podwarstwie MAC (*Medium Access Control*).

[1] Niniejszy rozdział rozprawy został oparty na analizie bezpieczeństwa WLAN dokonanej przez autora w pracy [95] (rozdziały 1, 2 i 5).

Warstwa LLC jest wspólna dla wszystkich sieci zgodnych z IEEE LAN RM, a zatem nie jest specyficzna dla 802.11.

Powszechnie implementowaną odmianą standardu 802.11 jest standard 802.11b [46] pracujący w paśmie 2,4 GHz, wykorzystujący technikę DSSS (*Direct Sequence Spread Spectrum*), dający teoretyczną możliwość transferu w kanale radiowym z przepustowością do 11 Mbit/s. W 2003 zakończono prace nad rozszerzeniem 802.11b – standardem 802.11g [48] dającym możliwość transferu z przepustowością nawet pięciokrotnie większą. 802.11g stopniowo eliminuje z rynku rozwiązania 802.11b zachowując z nimi zgodność wstecz[2]. 802.11g cechuje się lepszymi własnościami związanymi z odpornością na zakłócenia głównie za sprawą metody rozpraszana widma OFDM (*Orthogonal Frequency Division Multiplexing*).

Kilka słów o blisko 10 letniej historii standardu 802.11 w kontekście bezpieczeństwa. Jego pierwsza wersja z 1997 roku traktowała zagadnienia ochrony informacji marginalnie i opcjonalnie, faworyzując skompromitowany w artykule [13] z 2001 roku algorytm WEP (*Wired Equivalent Privacy*). Druga wersja standardu 802.11 z 1999 (IEEE 802.11-1999), przygotowana pod kątem standaryzacji ISO/IEC (ISO/IEC 8802-11:1999), nie wniosła pod względem bezpieczeństwa żadnych innowacji. Ważnym wydarzeniem w 1999 roku było utworzenie stowarzyszenia *Wireless Ethernet Compatibility Alliance* (od 2002 znane jako *Wi-Fi Alliance*) promującego technologię WLAN, zajmującego się także standaryzowaniem profili zabezpieczeń znanych jako WPA (*Wi-Fi Protected Access* – [113], [114]).

Punkt zwrotny w dziedzinie bezpieczeństwa WLAN to rok 2000, w którym rozpoczęło się zainteresowanie świata akademickiego omawianą technologią, głównie za sprawą pierwszych prób implementacji WLAN w campusach czołowych amerykańskich uniwersytetów. Równolegle do wdrożeń na uczelniach, na jesieni 2000 roku została opublikowana pierwsza analiza w ramach IEEE podważająca bezpieczeństwo WLAN [111]. Dopiero kilka miesięcy później zaprezentowano pierwszą, spoza IEEE, krytykę bezpieczeństwa 802.11, opracowaną przez naukowców z *University of California* w Berkeley (Stany Zjednoczone) [13].

Rezultatem zmasowanej krytyki bezpieczeństwa 802.11 była decyzja IEEE o utworzeniu grupy zadaniowej TGi (*Task Group i*) w ramach prac standaryzacyjnych w komórce 802.11. Grupa ta powstała wiosną 2002 i skoncentrowała swoje prace na rozwoju podwarstwy MAC w kontekście opracowania skutecznych mechanizmów zabezpieczeń. Także w tym czasie IEEE postanowiło zrezygnować z płatnego dostępu do swoich standardów po sześciu miesiącach od ich publikacji. Działanie to miało za zadanie ułatwić dostęp środowiska naukowego do wdrażanych standardów sieciowych, a także wywołać szerszą dyskusję nad zaproponowanymi rozwiązaniami. Jesienią 2002 organizacja *Wi-Fi Alliance* ogłosiła pierwszy zbiór przejściowych zasad zwiększających bezpieczeństwo WLAN, znany jako WPA [113]. Ostatecznie standard IEEE 802.11i [49]

[2] Standard 802.11g ERP-OFDM tzw. "tylko g" (por. rozdział 5.3) nie jest zgodny z 802.11b.

został opublikowany w lipcu 2004. Do dnia dzisiejszego coraz więcej nowych urządzeń WLAN na rynku wykorzystuje IEEE 802.11i. Standardowi 802.11i odpowiada profil WPA2 [114].

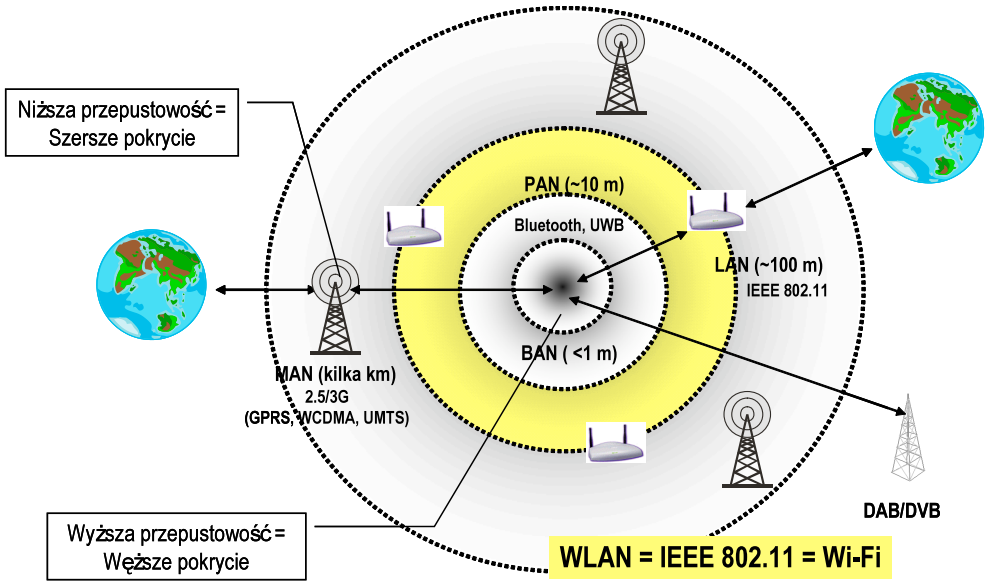
Z punktu widzenia bezpieczeństwa informacyjnego najistotniejsze cechy standardu 802.11 to:

– zasięg działania sieci WLAN,

– techniki modulacji w warstwie fizycznej (PHY),

– technika dostępu do medium CSMA/CA w podwarstwie MAC.

Zasięg WLAN jest uzależniony od wielu czynników, w tym: środowiska, czułości odbiornika, mocy doprowadzonej do anteny nadawczej. W zamkniętym obszarze biurowym można go oszacować na poziomie do 100 metrów (Rysunek 2-2), jednak w otwartej przestrzeni typowe urządzenia (takie jak klient i punkt dostępowy – *access point*) mogą komunikować się nawet na odległość 500 metrów. Zastosowanie anten kierunkowych o dużym zysku (np. anten parabolicznych) daje możliwość komunikacji na odległość do kilku kilometrów, głównie w zastosowaniach typu punkt-punkt lub punkt-wielopunkt. Rekordowa instalacja WLAN powstała w 2002 roku w Szwecji i miała zasięg (łącze punkt-punkt) 310 kilometrów [117].



Rysunek 2-2 Sieci WLAN a sieci BAN, PAN i MAN – na podstawie materiałów firmy Intel

Propagacja sygnału radiowego jest uzależniona od położenia i mocy nadajnika oraz charakterystyki i położenia anten. Na propagację wpływają także przestrzenne własności terenu i budynków, w tym grubości ścian i stropów, typ ich wypełnienia, przebieg różnych instalacji np. elektrycznej. Zasięg radiowy technologii WLAN w sposób naturalny może przekraczać granice budynków, przez co zwiększa się ryzyko podsłuchu transmisji danych dokonywanych przede wszystkim przez punkty dostępowe.

Jednym z najbardziej znanych z literatury ataków, który wykorzystuje wyciek sygnału radiowego z budynku, jest tzw. atak parkingowy (*parking lot attack*) [108].

Zastosowane wyrafinowane techniki rozpraszania widma, modulacji i kodowania (nie szyfrowania) w warstwie fizycznej (oparte na OFDM, DSSS) często są traktowane, jako metody ochrony przed podsłuchem przesyłanych danych. Jest to jedynie częściowo słuszne – struktura warstwy fizycznej PHY utrudnia wgląd w zawartość ramek, jednak model warstwowy daje możliwość abstrahowania od treści wymienianych w innych warstwach. Zatem większość istotnych informacji możemy uzyskać z poziomu podwarstwy MAC, która jest izolowana logicznie od komunikacji w warstwie fizycznej (implementowanej przez zwykłą bezprzewodową kartę sieciową). Traktowanie skomplikowanych technik modulacji i kodowania jako elementów ochrony informacji można śmiało określić mianem „mitu bezpieczeństwa warstwy fizycznej".

Skoro kluczowa dla podsłuchu informacji jest podwarstwa MAC, w której można odczytać strukturę ramek, a także w prosty sposób – poprzez analizę pól danych odtworzyć zawartość informacji z warstw wyższych, to szczególne znaczenie ma bezpieczeństwo tej podwarstwy, które zostanie omówione w dalszej części pracy, w rozdziale 2.3.

2.2 Ataki na sieci WLAN

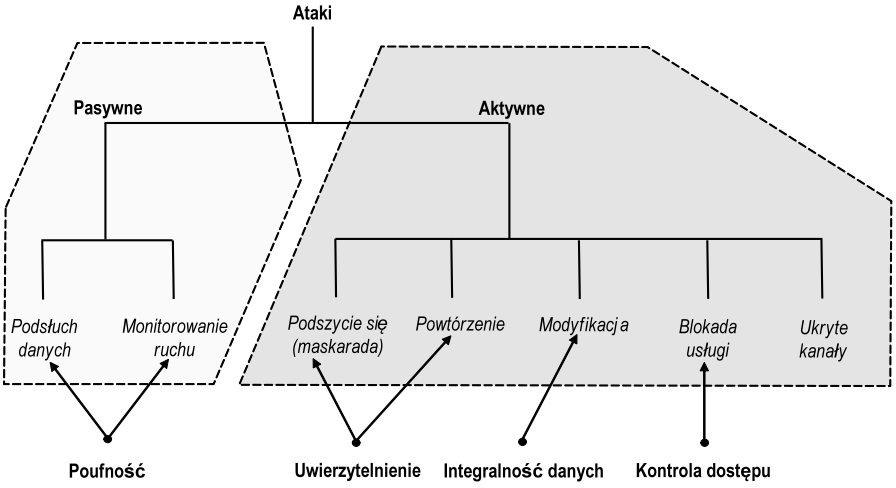
Ataki w sieciach WLAN można podzielić na dwie grupy (por. Rysunek 2-3, adaptacja z [60]):

pasywne – nieautoryzowana działalność, w której atakujący nie modyfikuje zawartości ramek, a jedynie biernie nasłuchuje transmisji w kanale:

- podsłuch danych – atakujący przechwytuje informacje wymieniane pomiędzy legalnymi użytkownikami,
- monitorowanie ruchu – intruz śledzi transmisje pomiędzy legalnymi użytkownikami, w celu analizy cech stacji i ich aktywności,

aktywne – nieautoryzowana działalność, w której atakujący czynnie bierze udział w transmisji w kanale:

- podszycie się (maskarada) – atakujący udaje legalnego użytkownika lub usługę sieciową,
- powtórzenie – włamywacz po przechwyceniu za pomocą podsłuchu informacji retransmituje ją, tak jak legalny użytkownik,
- modyfikacja – intruz kasuje, dodaje, zmienia wiadomość wysłaną przez legalnego użytkownika,
- blokada usługi – atakujący destabilizuje pracę sieci, uniemożliwiając poprawną komunikację,
- ukryte kanały – opisane w rozdziale 3. metody ukrywania informacji mogące doprowadzić do wycieku danych.



Rysunek 2-3 Taksonomia ataków na WLAN i usługi ochrony informacji

Ataki pasywne w większości przypadków są związane z brakiem uruchomionych mechanizmów zabezpieczeń na poziomie podwarstwy MAC. Jest to pierwotna przyczyna problemów związanych z **podsłuchem**. Wtórna, to użycie mechanizmów, które zostały skompromitowane, np. WEP (por. rozdział 2.3). Rozgłaszanie informacji o identyfikatorze sieci SSID (*Service Set IDentifier*) przez punkty dostępowe jest również przykładem wycieku informacji uwierzytelniającej przed siecią bezprzewodową. W sieciach WLAN podsłuch jest ułatwiony przez implementację w kartach sieciowych trybu monitorującego (*monitor mode*), umożliwiającego wysłanie do warstw wyższych ramek także uszkodzonych. Jest to odpowiednik trybu odbierania *promiscuous mode* znanego z przewodowych kart np. 802.3 (Ethernet). Tryb monitorujący umożliwia przeszukiwanie kanałów radiowych używanych do komunikacji pomiędzy urządzeniami bezprzewodowymi. **Monitorowanie ruchu** zdradza przede wszystkim aktywność stacji, a także, w przypadku braku zabezpieczeń w podwarstwie MAC, relacje pomiędzy stacjami.

Podszycie się (maskarada) i **powtórzenie** są możliwe w sytuacji, w której nie jest używane uwierzytelnienie w protokole 802.11 lub mechanizmy wymiany uwierzytelniającej zostały skompromitowane. Modyfikacja jest dość trudnym atakiem, a po uruchomieniu integralności bardziej wyrafinowanej niż CRC-32 (*Cyclic Redudancy Code*), czyli zwykłego kodu nadmiarowego, jest mocno utrudniona. Spotykanym atakiem jest też podszycie się na poziomie adresów podwarstwy MAC [118].

Specyficznym atakiem prowadzącym do **blokady usługi** [7] jest przede wszystkim zakłócanie (zagłuszanie) pracy punktu dostępowego lub innych stacji przez użycie tej samej częstotliwości radiowej. Może to być dokonywane przez włączenie konkurencyjnego punktu dostępowego lub urządzeń zakłócających pracę w paśmie WLAN (np. kuchenki mikrofalowe w przypadku 802.11b/g). Znane też są przypadki wysyłania masowych próśb o asocjację lub deasocjację, które również mogą prowadzić do „zawieszenia się" punktu dostępowego. Innym atakiem prowadzącym do blokady usługi może być „zapychanie" pasma radiowego, bądź celowe przerywanie transmisji –

powodowanie kolizji. Dość ciekawym atakiem, w kontekście omawianego w tej rozprawie systemu HICCUPS, jest „zalewanie" (*flooding*) punktu dostępowego ramkami z uszkodzonymi sumami kontrolnymi [67].

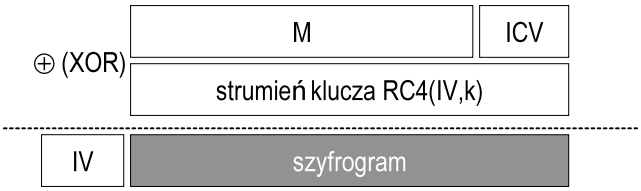
Ostatnią grupą ataków są ataki związane ze steganografią, w szczególności poprzez tzw. **ukryte kanały** tj. kanały komunikacyjne, które służą do wymiany informacji bez ujawniania istnienia tych kanałów. Przykładem tego typu ataków jest użycie systemu HICCUPS do wycieku informacji.

Zgodnie z ISO 7498-2:1989 [54] przed podsłuchem i monitorowaniem ruchu chroni poufność. Przed podszyciem się (maskaradą), podobnie jak powtórzeniem, chroni uwierzytelnienie. Przed modyfikacją – integralność danych, a przed blokadą usługi – kontrola dostępu. Przed ukrytymi kanałami nie chroni żadna ze znanych usług ochrony informacji.

2.3 Metody zapewnienia bezpieczeństwa informacji w WLAN (istotne z punktu widzenia systemu HICCUPS)

Metody kryptograficzne stosowane w WLAN do ochrony części użytkowej ramek tworzą „szum" informacyjny utrudniający rozróżnienie steganogramów od zwykłych wiadomości wymienianych w sieci. Podobnie jak w dylemacie więźniów (por. rozdział 1.1) w sieciach pozbawionych mechanizmów bezpieczeństwa wykorzystanie szyfrowania na potrzeby ochrony ukrytej komunikacji może zdradzać istnienie tej wymiany informacji.

Do ochrony pól użytkowych ramek służą w sieciach WLAN trzy algorytmy: **WEP** (*Wired Equivalent Privacy*), **TKIP** (*Temporal Key Integrity Protocol*) oraz **CCMP** (*Counter Mode with CBC-MAC Protocol*). Funkcję usługową dla algorytmów CCMP i TKIP pełnią metody zarządzania kluczami kryptograficznymi[3]. Z punktu widzenia systemu HICCUPS zarządzanie kluczami w WLAN jest drugorzędne, podobnie jak metody uwierzytelnienia stacji.



Rysunek 2-4 Schemat działania WEP

Celem przyświecającym twórcom **WEP** [44] było osiągnięcie bezpieczeństwa sieci przewodowych (w tym Ethernetu) za pomocą kryptografii. Sama nazwa algorytmu (dosłownie *odpowiednik przewodowej prywatności*) wskazuje na kierunek innowacji.

[3] Algorytm WEP jest praktycznie pozbawiony tej funkcji.

Jednak tego ambitnego zadania nie udało się zrealizować, chociaż przygotowany w połowie lat 90 „przepis na sukces" wydawał się dość prosty – miały go zapewniać:

- siła algorytmu WEP gwarantowana przez tajność klucza,
- samosynchronizacja algorytmu dostosowana do własności medium (duża stopa błędów w kanale – typowo 10^{-5}-10^{-6}, a nawet 10^{-4}),
- efektywność implementacji programowej (tym bardziej – sprzętowej),
- eksportowalność algorytmu poza Stany Zjednoczone,
- opcjonalność – implementacja i użycie WEP jako opcji.

WEP bazuje na szyfrze strumieniowym RC4 z kluczem 64-bitowym (efektywnie – 40-bitowym) lub 128-bitowym (efektywnie – 104-bitowym). Rozwiązania te noszą odpowiednio nazwy WEP-40 i WEP-104. W WEP nadawca i odbiorca współdzielą tajny klucz *k*. Wiadomość *M* – pole z danymi, oraz bazująca na CRC-32 suma kontrolna ICV (*Integrity Check Value*) są dodawane modulo 2 (XOR) do strumienia klucza (*key stream*) utworzonego przez RC4 – Rysunek 2-4. Strumień klucza jest ciągiem pseudolosowym wygenerowanym na podstawie jawnie przesyłanego wektora inicjalizującego (IV) o długości 24 bity i klucza *k* (RC4(IV,*k*)).

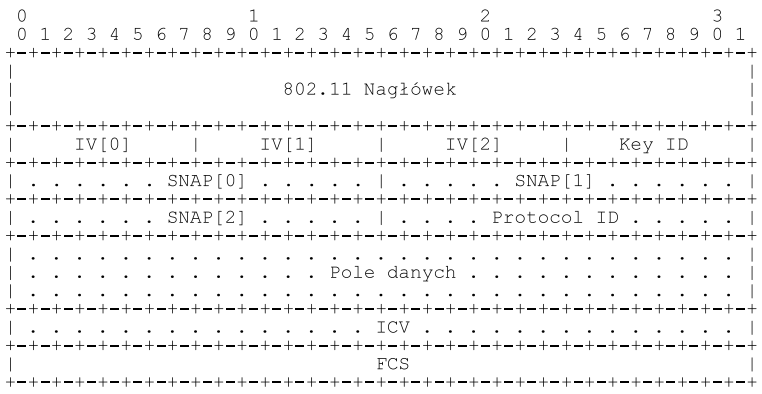
W najpopularniejszym wariancie działania WEP, tzw. *default keys,* wszystkie stacje współdzielą 4 klucze WEP. W drugim, rzadko implementowanym, tzw. *key mapping keys*, klucze są przydzielone w relacjach <TA,RA>, gdzie TA to adres nadajnika (*Transmiter Address*), a RA – adres odbiornika (*Receiver Address*).

Do głównych słabości WEP należy zaliczyć:

- zbyt krótkie, często statyczne lub przewidywalne, wartości wektorów IV,
- zbyt krótkie klucze kryptograficzne w WEP-40, co powoduje szczególną podatność na omówiony dalej atak typu *brute-force* (atak na zasadzie pełnego przeglądu),
- współdzielenie tych samych kluczy przez stacje w wariancie *default keys*,
- brak metod automatycznego odświeżania kluczy – w praktyce nieskończony czas życia klucza,
- niewłaściwe użycie RC4, tzw. *weak key schedule*, co powoduje szczególną podatność na omówiony dalej atak FMS [32],
- słaby niekryptograficzny mechanizm integralności, realizowany za pomocą CRC-32,
- brak uwierzytelnienia źródła danych.

Atak na WEP jest możliwy poprzez wykorzystanie słownika wyrazów do znalezienia właściwego klucza (tzw. atak słownikowy), bądź przez przeszukanie całej przestrzeni kluczy (atak typu *brute-force*). W 2001 roku przedstawiono w pracy [74] jeden z najefektywniejszych pod względem szybkości ataków typu *brute-force*. Niepoprawna struktura zdefiniowanego w standardzie generatora pseudolosowego PRNG inicjującego

szyfrowanie RC4 zmniejsza przestrzeń niepowtarzalnych kluczy z 2^{40} do jedynie 2^{21}. Atak dotyczy tylko niektórych implementacji WEP-40.



Rysunek 2-5 Ramka IEEE 802.11 zabezpieczona WEP

Atak FMS (od nazwisk twórców Fluhrer-Mantin-Shamir – por. [32], a także [93]) jest najczęściej implementowany przez hackerów (narzędzia *AirSnort, WEPcrack*). Atak wykorzystuje znajomość pierwszego bajtu strumienia klucza[4], na którym dla pewnych wartości wektorów IV, ukazać się może fragment współdzielonego klucza *k*. Atak został zoptymalizowany przez D. Hultona [43]. O ile atak typu *brute-force* można zrealizować na podstawie zebranych kilku ramek 802.11 (a nawet jednej), o tyle atak FMS ściśle zależy od szczęścia atakującego, tj. znalezienia odpowiednio słabych wartości wektora IV w odbieranych danych. Atak FMS jest niezależny od długości klucza RC4.

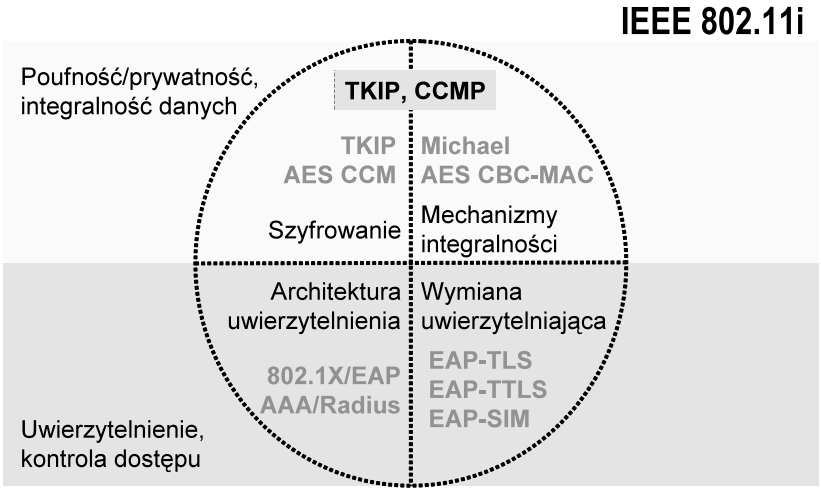
Perturbacje związane ze słabością WEP i podjęte w związku z tym prace standaryzacyjne doprowadziły do opublikowania w lipcu 2004 roku standardu IEEE 802.11i [49]. W standardzie zaproponowano nowe, solidne metody zwiększenia bezpieczeństwa zarówno w kontekście poufności jak i uwierzytelnienia (Rysunek 2-6) – por. [41], [110], [109]. Wprowadzona została koncepcja RSNA (*Robust Security Network Association*) zakładająca uzupełnienie dotychczasowych metod ochrony, w tym WEP o:

- rozszerzone uwierzytelnienie dla stacji bezprzewodowych,
- algorytmy zarządzania kluczami, w tym algorytmy ustanawiania kluczy,
- mechanizmy ochrony na poziomie MAC: TKIP oraz CCMP.

Rozszerzone uwierzytelnienie i zarządzanie kluczami w 802.11i opiera się na (niebędącym formalnie częścią tego standardu) protokole IEEE 802.1X ([53], [20]). Użycie protokołu 802.1X silnie wpływa na jakość tworzonych kluczy sesyjnych dla stacji WLAN. Istotna dla tego protokołu jest koncepcja użycia serwera uwierzytelniającego,

[4] Atakowane są IV postaci: (A + 3, N - 1, X); stwierdzenie, czy IV jest słabe następuje zaraz po kroku KSA (*Key Scheduling Algorithm*) algorytmu RC4: X = S{B + 3}[1] < B + 3, X + S{B + 3}[X] = B + 3.

która pozwala na wyniesienie inteligencji uwierzytelniania poza stacje i punkty dostępowe uczestniczące w tym procesie. Serwer uwierzytelniający (serwer AAA – *Authentication, Authorization and Accounting*) jest najczęściej realizowany za pomocą systemu RADIUS [84]. Sam proces uwierzytelnienia jest oparty na wywodzącym się z prac IETF (*Internet Engineering Task Force*) protokole EAP (*Extensible Authentication Protocol* – RFC 3748 [1]). EAP, pierwotnie określony dla protokołu PPP [12], jest generycznym nośnikiem specyficznej metody uwierzytelnienia. Znanych jest kilkadziesiąt jego realizacji tzw. metod EAP [92] (głównie standardów producenckich), jednak ze względu na zgodność z profilami WPA i WPA2 najpopularniejszymi są: EAP-TLS [2], EAP-TTLS/MSCHAPv2 [35], PEAPv0/EAP-MSCHAPv2 [58], PEAPv1/EAP-GTC, EAP-SIM [40].



Rysunek 2-6 Standard IEEE 802.11i – usługi ochrony informacji i mechanizmy zabezpieczeń

Po kompromitacji algorytmu WEP, został opracowany algorytm **TKIP,** jako przejściowa metoda zapewnienia bezpieczeństwa w sieciach 802.11. TKIP wykorzystuje WEP, w związku z tym w prosty sposób daje się zaimplementować w starych urządzeniach poprzez wymianę oprogramowania. Standard 802.11i traktuje TKIP jako opcję, jednak profil WPA [113] *Wi-Fi Consortium* nakłada obowiązek realizowania TKIP. Algorytm wykorzystuje klucze o długości 128 bitów.

Głównym celem stworzenia algorytmu TKIP była możliwość utworzenia unikalnego klucza dla WEP dla każdej ramki. Zmienność klucza ma na celu uodpornienie algorytmu TKIP na znane ataki na WEP, w tym FMS. W algorytmie TKIP klucz dla WEP jest funkcją adresu nadajnika (TA), numerów ramki (TSC – *TKIP Sequence Number*) oraz klucza tymczasowego (TK – *Temporary Key*). Algorytm tworzenia kodu integralności MIC (*Message Integrity Code*) – Michael – jest funkcją klucza MIC (o długości 64 bity), adresów źródła (SA) i przeznaczenia (DA), oraz zawartości ramki. Algorytm Michael jest zbudowany analogicznie do kryptograficznych funkcji skrótu – bazuje na prostych operacjach logicznych i bitowych.

W literaturze znane są ataki typu *brute-force* na TKIP, związane wyłącznie z użyciem klucza współdzielonego PSK (*Pre-Shared Key*) [104]. Metodą ochrony przed tymi atakami

jest stosowanie dobrej jakości kluczy współdzielonych, czyli dobrych haseł sieciowych. Do tej pory algorytm TKIP nie został uznany za niebezpieczny; rekomendowane jest jego użycie wyłącznie z kluczami dystrybuowanymi za pomocą protokołu 802.1X.

CCMP został opracowany jako docelowa metoda zapewnienia poufności w podwarstwie MAC sieci 802.11. CCMP nie wykorzystuje ani WEP, ani TKIP. Standard 802.11i wymaga zaimplementowania CCMP, podobnie jak profil bezpieczeństwa WPA2 [114] *Wi-Fi Consortium*.

CCMP bazuje na szyfrze blokowym AES (*Advanced Encryption Standard*) oraz na jego szczególnym trybie wiązania bloków CCM (*Counter mode with CBC-MAC*), w którym jest realizowana poufność (CTR – *Counter Mode*) i integralność (CBC-MAC – *CBC Message Authentication Code*). Zdefiniowany w FIPS PUB 197 ([77]) algorytm AES wykorzystuje na potrzeby CCMP klucze o długości 128 bitów i operuje na blokach o takiej samej długości. Algorytm AES został zaprojektowany jako następca legendarnego algorytmu DES (*Data Encryption Standard*).

Generyczny tryb pracy szyfru AES, o nazwie CCM, został określony w [112]; w przypadku sieci 802.11 CCM ma dwa parametry: $M = 8$ (MIC ma 8 oktetów), $L = 2$ (pole *długość* ma 2 oktety, co wystarcza, aby zakodować informację o długości ramki wyrażonej w oktetach). CCM wymaga świeżego tymczasowego klucza dla każdej sesji, a także unikalnej wartości tzw. numeru pakietu (PN – *Packet Number*) o długości 48 bitów dla każdej ramki.

Tryb pracy szyfru blokowego CTR cechuje się wiązaniem bloków ze strumieniem danych poprzez sumę modulo 2 (XOR) i jest zbliżony do podstawowego trybu pracy szyfrów blokowych ECB (*Electronic Code Book*) [24]. CBC-MAC (*CBC Message Authentication Code*) jest szyfrowaniem w trybie CBC (*Cipher-Block Chaining*), w którym ostatni blok szyfrogramu jest traktowany jako suma kontrolna MIC. Zaimplementowanie CCMP wymaga stosowania realizacji AES jedynie w części szyfrującej. Wariant deszyfrujący AES nie jest wykorzystywany, co daje oszczędność pamięci w implementacji sprzętowej.

CCMP jest uznawany za bezpieczny. Nie istnieją żadne informacje w literaturze dowodzące jego niebezpieczeństwa. Algorytm CCMP w trybie PSK, podobnie jak TKIP, może być podatny na atak typu *brute-force*. Metodą ochrony, podobnie jak w TKIP, jest stosowanie dobrych haseł sieciowych.

Podsumowując, z punktu widzenia bezpieczeństwa, bazujący na AES, algorytm CCMP jest najlepszym rozwiązaniem i w miarę możliwości powinien zastępować algorytmy TKIP oraz WEP.

Po wprowadzeniu standardu IEEE 802.11i uznaje się, że bezpieczeństwo sieci bezprzewodowych IEEE 802.11 jest względnie dobrze zapewnione. Niestety, stopień skomplikowania niektórych protokołów skojarzonych z IEEE 802.11i, w szczególności 802.1X i metod EAP, pozwala przypuszczać, że przez najbliższy czas będziemy zmagać się z błędami w ich architekturze [119]. Należy pamiętać, że mechanizmy bezpieczeństwa określone w ramach 802.11i zostały opracowane z myślą o użytkownikach komercyjnych

(tzw. *commercial grade security*). Mogą one jednak nie być wystarczające do zastosowań militarnych, bądź do przesyłania informacji niejawnych, których dotyczą najostrzejsze klauzule bezpieczeństwa.

Względnie stabilny stan 802.11i pozytywnie wpływa na kształtowanie się zabezpieczeń w innych rodzajach sieci bezprzewodowych. Jeden z nowych standardów PAN – IEEE 802.15.4 (ZigBee – [51]), stworzony z maksymalną prostotą i w celu ograniczenia kosztów, odziedziczył po 802.11i protokół CCMP w podwarstwie MAC. Jest to krok naprzód w stosunku do zastosowanego w IEEE 802.15.1 (Bluetooth – [50]) szyfru strumieniowego typu liniowego rejestru przesuwnego ze sprzężeniem zwrotnym (LFSR – *Linear Feedback Shift Registers* – [90], [91]).

Z rynku zostaną najprawdopodobniej wyeliminowane („śmierć moralna") produkty wspierające jedynie WEP. Faworyzowane przez *Wi-Fi Alliance* profile WPA i WPA2 oraz skorelowana z nimi certyfikacja, stanowią swego rodzaju wyznacznik klasy bezpieczeństwa nowych produktów. Należy podkreślić, że WPA2 jest z punktu widzenia bezpieczeństwa tożsamy z IEEE 802.11i.

Dzięki IEEE 802.1X umacnia się rola serwerów AAA (w szczególności RADIUS) w sieciach teleinformatycznych. Przez pewien czas, w szczególności w drugiej połowie lat 90., ich znaczenie stawało się dość marginalne, jednak wykorzystanie AAA w sieciach IEEE 802.11 jako strony odpowiedzialnej za uwierzytelnianie użytkowników podkreśla wagę tych rozwiązań. W najbliższych latach należy się spodziewać większego wzrostu zainteresowania rozwojem nowych systemów AAA – bezpieczniejszych i bardziej rozbudowanych pod kątem rozliczania użytkowników.

Pewien niepokój związany z IEEE 802.1X mogą wzbudzać metody EAP. Mnogość tych metod, hybrydowe użycie kilku z nich łącznie oraz brak standardowego wsparcia w systemach operacyjnych powoduje bałagan w praktycznych implementacjach 802.11i. Przy wyborze metod warto podążać ścieżką wyznaczoną przez *Wi-Fi Alliance* – preferować metody EAP zgodne z WPA i WPA2. Jedna z tych metod, EAP-SIM [40], pomimo podważania jej bezpieczeństwa [80], jest wygodnym sposobem na uwierzytelnianie użytkowników WLAN poprzez informacje dostępne w sieci GSM. Warto wspomnieć o metodzie EAP-AKA [5] zwiększającej elastyczność w wykorzystaniu sieci IEEE 802.11 jako interfejsów radiowych do sieci 3G (w tym do UMTS).

Wciąż trwają pracę nad trzema standardami mającymi bezpośredni wpływ na bezpieczeństwo WLAN: IEEE 802.11r (*Fast Roaming/Fast BSS Transition*), IEEE 802.11s (*ESS Mesh Networking*) i IEEE 802.11w (*Protected Management Frames*).

IEEE 802.11r odnosi się do problemów związanych z szybkim roamingiem. WPA2 wspiera już częściowo szybki roaming, jednak doświadczenia związane z obecnymi wdrożeniami szybkiego roamingu wskazują na duże obciążenie punktów dostępowych procesem uwierzytelnienia. W szczególności telefony IP bazujące na 802.11 istotnie degradują wydajność punktów dostępowych.

IEEE 802.11s związane jest z budową sieci o strukturze wieloboku zupełnego (*mesh topology*). Pojawiają się tu kwestie związane z routingiem między węzłami

i z jego bezpieczeństwem. Grupa TGs (*Task Group s*) została utworzona niedawno i dopiero w najbliższej przyszłości okaże się, jak kwestie bezpiecznego routingu w tego typu sieciach będą rozwiązane.

Ostatni standard IEEE 802.11w dotyczy bezpieczeństwa ramek zarządzających (*management frames*), w tym związanych z asocjacją i uwierzytelnieniem, wpływa także na postać innych standardów rodziny 802.11, w tym na wspomniany 802.11r oraz na 802.11u (*Interworking with External Networks*).

W najbliższej przyszłości warto wnikliwie śledzić informację o ewentualnych błędach znalezionych w architekturze bezpieczeństwa WLAN, w szczególności 802.11i. Pewien dystans należy zachować przy wykorzystaniu różnych metod EAP, w szczególności nowych, jako nie do końca stabilnych. Istotne jest także obserwowanie rozwoju tworzonych standardów 802.11r, 802.11s i 802.11w, jako bezpośrednio oddziaływujących na bezpieczeństwo WLAN.

Reasumując: zaprezentowane w tym rozdziale trzy metody zapewnienia poufności w podwarstwie MAC (WEP, TKIP i CCMP) tworzą „szum" informacyjny utrudniający rozróżnienie steganogramów systemu HICCUPS od zwykłych wiadomości wymienianych w sieci. Pozostałe elementy architektury bezpieczeństwa 802.11, w tym zarządzanie kluczami i uwierzytelnienie, są drugorzędne z punktu widzenia systemu HICCUPS.

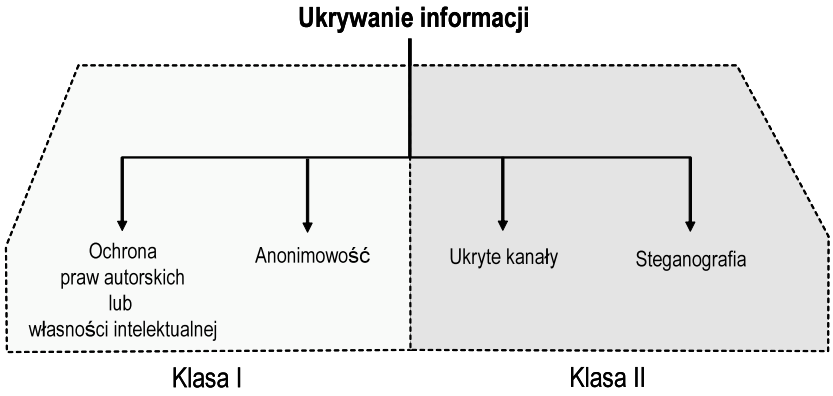
3. Steganografia sieciowa – pojęcia podstawowe i stan sztuki

3.1 Steganografia a ukrywanie informacji

Na pierwszej konferencji poświęconej steganografii *Information Hiding: First International Workshop*, która odbyła się w 1996 w Cambridge (Wielka Brytania), dokonano próby uporządkowania podstawowych pojęć dotyczących tej dziedziny [81], [25]. Krąg poszukiwań badawczych wokół steganografii i jej pochodnych technik przyjęto nazywać dziedziną **ukrywania informacji** (*information hiding*). Nazwa ta została użyta po raz pierwszy w 1972 roku przez D. Parnasa w pracy [79].

W przyjętej na wspomnianej konferencji propozycji wyróżniono cztery grupy technik (Rysunek 3-1):

- ochrona praw autorskich lub własności intelektualnej (*copyright marking*),
- anonimowość (*anonymity*),
- ukryte kanały (*covert channels*),
- steganografia (*steganography*).



Rysunek 3-1 Podział dziedziny ukrywania informacji zaproponowany w pracy [81]

Ochrona praw autorskich lub własności intelektualnej bazuje na dwóch technikach: na znakach wodnych (*watermarking*) i na skrótach danych (*fingerprinting*). Dzięki tym technikom można personalizować cyfrowe obiekty do identyfikowania właściciela stosownych praw bądź posiadacza cyfrowej kopii. Obiekty multimedialne są zbiorem bitów, który można powielać, zatem problem cyfrowego zarządzania prawami (DRM – *Digital Rights Management*) stał się istotny z punktu widzenia ochrony własności intelektualnej.

Technika zapewnienia **anonimowości** ma na celu ukrycie tożsamości komunikujących się podmiotów – zachowanie prywatności. W wielu sytuacjach zachowanie anonimowości jest uzasadnione, np. w przypadku ochrony danych

osobowych, jednak aspekt ukrywania tożsamości może prowadzić do konfliktu z polityką kontroli obywateli, prowadzonej przez rządy praktycznie wszystkich państw.

Ukryte kanały (pojęcie wprowadzone po raz pierwszy w [65]) są rozumiane jako kanały komunikacyjne, które służą do wymiany informacji bez ujawnienia istnienia tych kanałów. Ukryte kanały dzieli się na dwie podklasy ([107], [38]):

- kanały typu *storage* (*storage channels*) wykorzystujące wspólne dla wielu procesów lub podmiotów zbiory danych, np. pliki na dysku, nieużywane bity w przesyłanych pakietach,
- kanały typu *timing* (*timing channels*) wykorzystujące możliwość wpływania procesu lub podmiotu na zachowanie się systemu, np. wymuszenie ustalonej sekwencji opóźnień w wysłaniu ramki, ustalona kolejność odczytu danych ze wspólnej pamięci.

Definicja **steganografii** przyjęta na wspomnianej konferencji została zawężona do pozostałych technik, niewymienionych w omówionych powyżej trzech grupach, w szczególności do ukrywania informacji w treściach multimedialnych.

Techniki ukrywania informacji podzielono na dwie grupy:

- klasa I – techniki, w których, fakt istnienia ukrywania informacji **jest** powszechnie znany,
- klasa II – techniki, w których, fakt istnienia ukrywania informacji **nie jest** powszechnie znany.

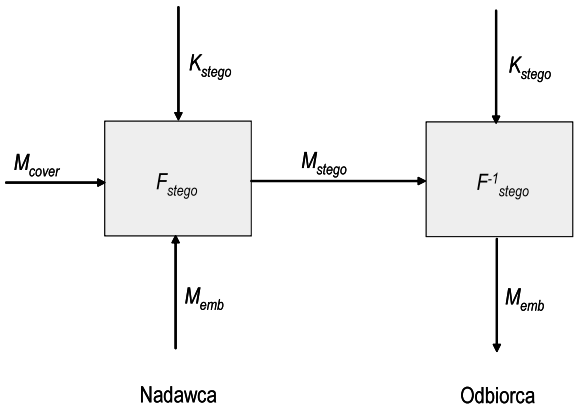
W niniejszej rozprawie (podobnie jak w wielu innych pracach) pojęcie **technik steganograficznych** jest utożsamiane ze wszystkimi technikami w dziedzinie ukrywania informacji, natomiast pojęcie **steganografia** – z technikami należącymi do klasy II.

Przez **steganografię sieciową** (*network steganography*) będziemy rozumieć grupę technik ukrywania informacji wykorzystujących strukturę protokołów sieciowych lub oddziaływanie na zachowanie tych protokołów. Elementami struktury protokołów są m.in. opcjonalne pola nagłówków, kody nadmiarowe. Oddziaływanie na zachowanie protokołów polega na realizacji konkretnego scenariusza bazującego np. na kolejności wymiany informacji, bądź uzyskaniu pożądanych opóźnień w reakcji na ustalone zdarzenie. Innym funkcjonującym w literaturze określeniem steganografii sieciowej jest *protocol steganography* (przez analogię do *image/audio/text steganography*).

3.2 Model systemu steganograficznego i miary jego jakości

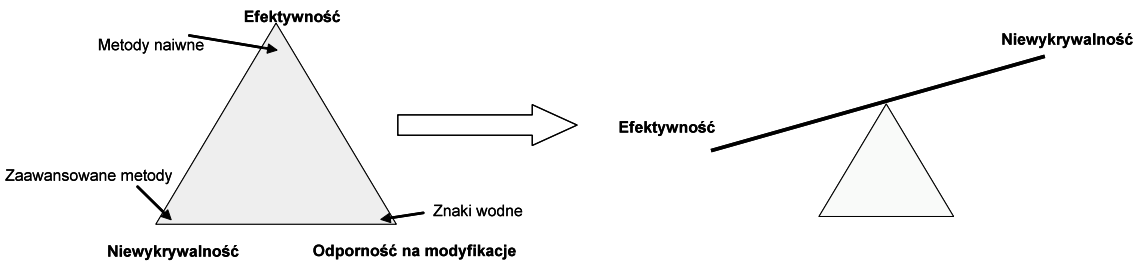
Na wspomnianej konferencji, w pracy [82] podsumowującej prowadzone podczas obrad dyskusje, został zaproponowany generyczny model systemu steganograficznego (Rysunek 3-2). Wiadomość do ukrycia (M_{emb}) jest umieszczana w wiadomości nośnej (M_{cover}) za pomocą przekształcenia steganograficznego $F_{stego.}$ Wynikiem tego przekształcenia jest steganogram (M_{stego}). Przez analogię do szyfrów symetrycznych, przekształcenie steganograficzne F_{stego} jest parametryzowane kluczem K_{stego}. Struktura

M_{cover} jest ściśle związana z cechami danego systemu steganograficznego; np. dla systemów sieciowych M_{cover} może być elementem struktury protokołu. Przekształceniem odwrotnym do F_{stego} jest F^{-1}_{stego}, pozwalające dokonać ekstrakcji M_{emb} z M_{stego}.



Rysunek 3-2 Generyczny model systemu steganograficznego

Istotnym z punktu widzenia tej pracy aspektem steganografii sieciowej jest jej **koszt** rozumiany w niniejszej pracy jako zmniejszenie przepustowości łącza dla wiadomości użytkowych. Koszt wynika z przeznaczenia części jednostek danych (M_{cover}) do ukrycia wiadomości (M_{emb}). Drugim interesującym nas aspektem będzie **efektywność** kanału utworzonego na bazie M_{cover}, rozumiana jako przepustowość dostępna dla systemu steganograficznego (w literaturze najczęściej określana jako *capacity*). Przedstawiony w tej pracy system HICCUPS będziemy utożsamiać z F_{stego}.



Rysunek 3-3 Klasyczny konflikt wymagań na system steganograficzny oraz jego interpretacja dla steganografii sieciowej

W pracy J. Fridricha [34] wyróżniono kilka istotnych cech ukrywania informacji, które pozwalają stworzyć kryteria oceny systemów steganograficznych. Autor, skupiając się przede wszystkim na steganografii w obrazach, zwrócił uwagę na konflikt (Rysunek 3-3) pomiędzy efektywnością (*capacity*), **niewykrywalnością** (*undetectability*) i odpornością na modyfikacje (*robustness*). Według autora, wysoka efektywność jest cechą metod naiwnych i stoi w sprzeczności z niewykrywalnością; te dwie cechy z kolei są sprzeczne z odpornością obiektu cyfrowego (i zawartego w nim steganogramu) na modyfikacje. Ponieważ odporność na modyfikacje jest pożądana

w zasadzie wyłącznie dla znaków wodnych, w sieciowych systemach steganograficznych cecha ta nie ma większego znaczenia. Stąd w steganografii sieciowej konflikt pomiędzy efektywnością a niewykrywalnością możemy zobrazować za pomocą huśtawki (Rysunek 3-3), mając jednocześnie świadomość, że dla niektórych metod (nie tylko sieciowych) istotny jest koszt, zdefiniowany jak powyżej. Należy podkreślić, że w wielu zastosowaniach osiągnięcie wysokiej efektywności nie jest głównym celem steganografii [72] – istotniejszym jest zapewnienie niewykrywalności.

3.3 Przegląd metod steganografii sieciowej

Jak wspomniano w rozdziale 1.1, steganografia sieciowa może być realizowana w każdej warstwie sieci [39]. Dla sieci LAN istnieje w literaturze jedynie kilka propozycji ([37], [116], [39], [22], [88]), w tym dwie dla WLAN ([100], [63]), a także jedna dla routingu w sieciach ad hoc [89]. Większość prac koncentruje się na warstwie sieciowej i transportowej, ze szczególnym akcentem na protokoły stosu TCP/IP [69].

A. Chmielewski w 1988 roku zaproponował ([18], [19]) w warstwie fizycznej użycie nietypowych wartości z przestrzeni kodu transmisyjnego AMI do stworzenia dodatkowego kanału przesyłania informacji.

Dla warstwy łącza danych C. G. Girling rozważył, w pracy [37] z 1987 roku, dwa kanały typu *storage* w LAN (pola adresowe w nagłówku i rozmiar ramki) oraz kanał typu *timing* (przesłanie „0” lub „1” poprzez odpowiedni dobór czasu pomiędzy transmisjami). Praca Girlinga jest pierwszą analizą dotyczącą użycia ukrytych kanałów w środowisku sieciowym.

M. Wolf, w artykule [116] z 1989 roku, rozwinął pracę Girlinga przedstawiając metody steganograficzne dla trzech protokołów podwarstwy MAC: 802.5 (Token Ring), 802.3 (Ethernet), 802.4 (Token Bus) oraz dla LLC (802.2). Wolf stwierdził, że szyfrowanie nie zapewnia ochrony przed wyciekiem informacji za pomocą ukrytych kanałów; uznał też, że wspólne medium w LAN jest kanałem typu *storage*. Zaproponowane przez Wolfa metody polegają na użyciu pól zarezerwowanych i pól uzupełnień (*PAD field*) w ramkach.

W 1996 T. Handel i M. Sandford w pracy [39] przedstawili steganografię sieciową w kontekście modelu odniesienia OSI. W warstwie drugiej zaproponowali protokół steganograficzny dla CSMA/CD [52], polegający na manipulacji czasem retransmisji po wykryciu kolizji – natychmiastowe powtórzenie ramki przyjęto jako „0”, a powtórzenie po maksymalnym czasie wyznaczonym przez standard 802.3, jako „1”.

T. Dogu i A. Ephremides, w artykule [22] z 1999, zaproponowali dwie techniki steganograficzne dla protokołów bazujących na algorytmach podziału (*splitting algorithms*) typu FCFS (*First Come First Served*). Autorzy doszli do wniosku, że zaproponowane techniki, bazujące na zwiększaniu liczby kolizji w medium, nadają się wyłącznie do mało przeciążonych kanałów. S. Li i A. Ephremides, w pracy [88] z 2005 roku, nieznacznie rozwinęli pracę [22], przedstawiając trzy uogólnione metody

ukrywania informacji dla całej klasy protokołów bazujących na algorytmach podziału. W innej pracy [89] z 2004, Li i Ephremides przedstawili propozycję systemu ukrywania informacji w protokole routingowym dla sieci ad hoc AODV (*Ad-hoc On-demand Distance Victor Routing*).

Autor niniejszej rozprawy, w artykule [100] z 2003 roku, zaproponował pierwszy znany w literaturze system steganograficzny dla WLAN – system HICCUPS – polegający na wykorzystaniu ramek z niepoprawnie stworzonymi sumami kontrolnymi, jako metody na stworzenie dodatkowego (dostępnego na żądanie) pasma dla systemu steganograficznego. W 2006 roku przedstawiona koncepcja została rozwinięta przez C. Krätzera, J. Dittmann, A. Langa i T. Kühne'a w pracy [63] (wykorzystującej [64]) poprzez wyróżnienie dwóch scenariuszy tworzących kanały typu *timing* i bazujących na modyfikacji oraz na zduplikowaniu ramek.

Dla warstwy sieciowej i transportowej C. Rowland, w pracy [85] z 1996, rozważył utworzenie trzech ukrytych kanałów na bazie: pola identyfikacji datagramu IP, pola zawierającego wartość inicjującą numer kolejny w TCP (ISN – *Initial Sequence Number*) oraz pól związanych z potwierdzeniami w TCP. Rowland przedstawił implementację zaproponowanych technik dla systemu Linux (wersja jądra 2.0).

Handel i Sandford, we wspomnianej powyżej pracy [39], zaproponowali użycie, jako kanału ukrywania informacji w warstwie sieciowej, 8-bitowego pola ToS (*Type of Service*) IP, natomiast w warstwie transportowej – 6 zarezerwowanych bitów protokołu TCP.

K. Ahsan i D. Mundur, w pracy [3] z 2002, rozwinęli pomysły Rowlanda z pracy [85], a także zaproponowali stworzenie kanału ukrywania informacji bazującego na zmianie kolejności wysyłania pakietów IPsec.

J. Giffin, R. Greenstadt, P. Litwack i R. Tibbetts, w pracy [36] z 2002, zaproponowali stworzenie kanału steganograficznego na bazie znaczników czasowych (*timestamps*) TCP, twierdząc, że najmłodsze bity w łączach o niskich przepustowościach mają charakter dość losowy i mogą posłużyć do ukrywania informacji.

G. Fisk, M. Fisk, C. Papadopoulosi i J. Neil, w pracy [31] z 2002, przeanalizowali metody eliminowania steganografii z ruchu IP poprzez zastosowanie aktywnych agentów (*wardens*) poprawiających struktury pakietów wyglądające anormalnie. Podobnie jak Fisk i in., S. Murdoch i S. Lewis, w pracy [73] z 2005, zaproponowali metody wykrywania ruchu steganograficznego w sieciach wykorzystujących mechanizmy opisane m.in. w pracach Rowlanda [85] oraz Handela i Sandforda [39].

Przykład stworzenia ukrytego kanału w warstwie aplikacji na bazie protokołu SSH przedstawili w 2004 N. Lucena, J. Pease, P. Yadollahpour oraz S. Chapin w pracy [71]. Przykład użycia protokołu HTTP do tworzenia kanału typu *timing* zaproponowali w 2006 H-G. Esser i F. Freiling w pracy [30].

Większość z powyższych prac rozważa efektywność, nie biorąc jednak pod uwagę kosztu użycia danej metody (por. rozdział 3.2). Koszt jest w zasadzie pomijalny tylko

w dwóch przypadkach: wtedy, gdy stworzony kanał jest oparty na polach opcjonalnych, bądź wtedy, gdy wpływ danej techniki ukrywania informacji na zachowanie protokołu nie prowadzi do spadku jego wydajności.

4. System steganograficzny HICCUPS – architektura i funkcje

4.1 Wstęp

Prezentowany w tym rozdziale system HICCUPS jest systemem steganograficznym wykorzystującym niedoskonałość środowiska, w którym działają sieci – zakłócenia kanałów transmisyjnych. Główna idea systemu polega na użyciu ramek z niepoprawnymi sumami kontrolnymi jako metody na stworzenie dodatkowego, dostępnego na żądanie, pasma do przesyłania steganogramów.

System HICCUPS może być zaimplementowany w środowisku sieciowym, w którym:

(1) dostęp do współdzielonego medium transmisyjnego (*shared medium*) umożliwia kopiowanie wszystkich ramek z kanału (np. sieć LAN o topologii szyny),

(2) istnieje kontrola poprawności ramek za pomocą sum kontrolnych (np. cyklicznych kodów nadmiarowych CRC – *Cyclic Redundancy Code*).

Wspólną własnością mechanizmów dostępu do wspólnego medium, takich jak np. CSMA/CD, CSMA/CA jest „nasłuchiwanie" medium transmisyjnego i wynikająca z tego możliwość podsłuchu wymienianych danych. Ramki uszkodzone podczas transmisji są odrzucane przez interfejs sieciowy, dzięki dokonywanej kontroli poprawności – przeważnie za pomocą cyklicznych kodów nadmiarowych.

Dodatkowo w sieciach, w których:

(3) istnieje mechanizm zapewniający poufność części użytkowej ramki,

można stworzyć „szum" informacyjny utrudniający rozróżnienie steganogramów od zwykłych ramek.

Cechy (1) i (2) są nieodzowne do działania systemu HICCUPS, cecha (3) jest opcjonalna.

Grupa stacji sieciowych stosujących system HICCUPS tworzy **ukrytą grupę**. Wymiana informacji w obrębie ukrytej grupy następuje przez **ukryte kanały**, przede wszystkim typu *storage*.

4.2 Architektura systemu

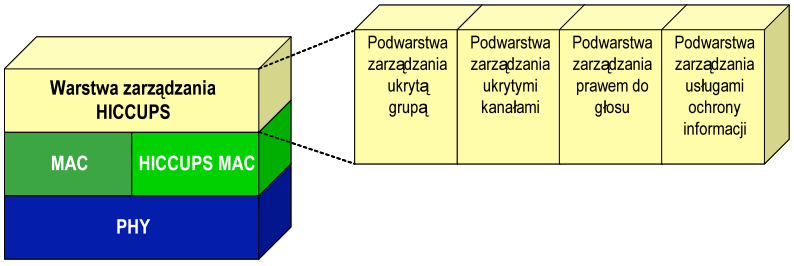
System składa się z następujących **czterech warstw** (Rysunek 4-1):

- warstwy zarządzania HICCUPS – odpowiedzialnej za sterowanie systemem, a w szczególności zarządzaniem ukrytymi kanałami, ukrytą grupą, prawem do głosu oraz usługami ochrony informacji,
- warstwy MAC – tożsamej z podwarstwą sterowania dostępem do medium do sieci dla danego protokołu LAN,

- warstwy HICCUPS MAC – zajmującej się formowaniem ramek zgodnie z potrzebami systemu HICCUPS,
- warstwy PHY – tożsamej z warstwą fizyczną danego protokołu LAN.

Warstwa zarządzania HICCUPS składa się **z czterech podwarstw**:

- podwarstwy zarządzania **ukrytą grupą**,
- podwarstwy zarządzania **ukrytymi kanałami**,
- podwarstwy zarządzania **prawem do głosu**,
- podwarstwy zarządzania **usługami ochrony informacji**.



Rysunek 4-1 Architektura proponowanego systemu

Podstawowymi **elementami** fizycznymi systemu są:

– interfejs sieciowy pracujący w danej technologii sieciowej np. IEEE 802.11g, umożliwiający modyfikację ukrytych kanałów, w tym pełne sterowanie polem użytkowym w ramce MAC,

– system zarządzania, zgodny z przedstawioną w tej części pracy architekturą systemu.

Interfejs sieciowy realizuje warstwy MAC, HICCUPS MAC i PHY. Natomiast system zarządzania realizuje warstwę zarządzania HICCUPS.

Warstwa zarządzania HICCUPS jest kluczowa dla działania całego systemu. Jej cztery podwarstwy omówiono w kolejnych podrozdziałach.

4.3 Zarządzanie ukrytą grupa

Za sterowanie członkostwem w ukrytej grupie odpowiada podwarstwa zarządzania ukrytą grupą. Główne operacje przeprowadzane przez tę podwarstwę to dołączanie i odłączanie użytkowników ukrytej grupy.

Zgodnie z definicją z [14]:

„Niech N będzie liczbą komponentów systemu. Pojedynczy (logicznie) akt komunikacji pociąga za sobą pojedynczy proces transmisji wiadomości do grupy procesów odbierających (GR). W zależności od liczności grupy odbiorczej ($|GR|$) mamy do czynienia z następującymi technikami komunikacji:

$|GR| = 1$ **unicast** (1 → 1), wiadomość jest przeznaczona dla unikatowego odbiorcy,

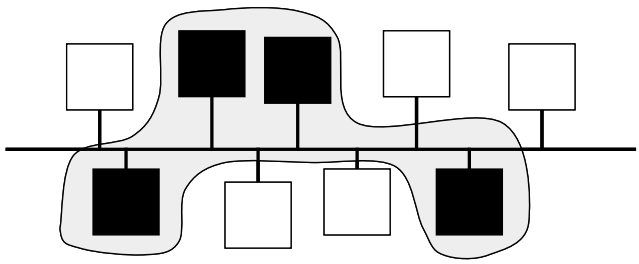
$|GR| = N$ **broadcast** (1 → wszyscy), wiadomość jest przeznaczona dla wszystkich procesów odbiorców,

$1 < |GR| < N$ **multicast**, także nazywany selektywnym broadcastem (1 → grupy, 1 → N), wiadomość jest przeznaczona dla podzbioru odbiorców".

W obrębie ukrytej grupy przyjmuje się notację:

- zdolność **jednego** procesu do wysyłania wiadomości do grupy: $1 \rightarrow N$,
- zdolność **wszystkich** procesów do wysyłania wiadomości: $N \rightarrow N$,
- zdolność **niektórych** procesów do wysyłania wiadomości: $M \rightarrow N$ $(M < N)$.

Fizycznie (transmisyjnie) system HICCUPS posiada funkcjonalność $N \rightarrow N$**,** jednak w zależności od konkretnych zastosowań może działać jako $1 \rightarrow N$ lub $M \rightarrow N$.



Rysunek 4-2 Przykładowa ukryta grupa składająca się z czterech stacji

Rysunek 4-2 ilustruje przykładową ukrytą grupę składającą się z czterech stacji. Grupa funkcjonuje pośród pięciu innych stacji nieposiadających wiedzy na temat działania systemu.

Należy podkreślić, że zdolność do wysyłania wiadomości nie jest warunkiem koniecznym do bycia członkiem grupy. Członek grupy może zachowywać się pasywnie tj. wyłącznie nasłuchiwać informacji przesyłanych w ukrytych kanałach.

4.4 Zarządzanie ukrytymi kanałami

Za sterowanie kontekstem użycia ukrytych kanałów w systemie HICCUPS odpowiada podwarstwa zarządzania ukrytymi kanałami. Główne operacje przeprowadzane przez tę podwarstwę to: sterowanie wymianą danych przy pomocy tych kanałów oraz zarządzanie trybami pracy systemu.

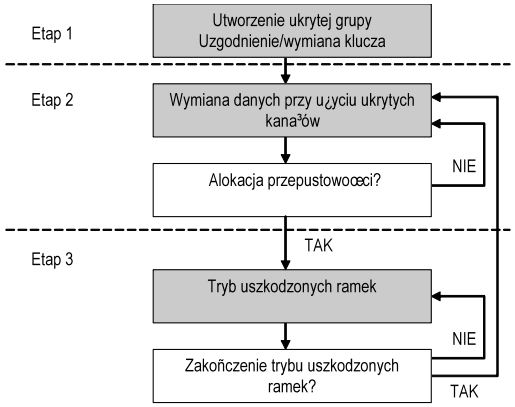
System HICCUPS wykorzystuje następujące **ukryte kanały**:

K1: kanał oparty na adresach sieciowych MAC (np. adresach źródła i przeznaczenia) lub innych polach nagłówka ramki MAC,

K2: kanał oparty na sumach kontrolnych,

K3: kanał oparty na polu użytkowym ramki.

Na potrzeby HICCUPS istnieje możliwość wykorzystania innych kanałów steganograficznych, w szczególności z warstw wyższych, zarówno typu *timing*, jak i *storage*.



Rysunek 4-3 Ogólny schemat działania proponowanego systemu

Ogólny schemat działania systemu (Rysunek 4-3) jest następujący:

Etap 1 (inicjacja systemu)

Stacje tworzące ukrytą grupę ustalają wspólny klucz (tzw. klucz grupowy) dla systemu steganograficznego. Do uzgodnienia klucza tajnej grupy może zostać użyty np. algorytm Diffie-Hellman [21] opcjonalnie z algorytmem podpisów cyfrowych DSS (*Digital Signature System* [76]), a do ochrony wymiany informacji pomiędzy użytkownikami tajnej grupy – szyfr AES. Wybór algorytmu uzgodnienia, bądź dystrybucji klucza, a także algorytmu chroniącego informacje w obrębie ukrytej grupy nie jest przedmiotem specyfikacji systemu. W szczególnym przypadku system może działać bez dodatkowego wsparcia ze strony technik kryptograficznych.

Etap 2 (podstawowy tryb działania)

Podstawowym trybem pracy jest przesyłanie komunikatów sterujących w polach adresowych MAC lub innych polach nagłówka – K1. Kanał K1 ma zwykle niską przepustowość. Oprócz informacji sterujących, K1 może być używany jako kanał transmisyjny dla danych wymienianych w obrębie ukrytej grupy. Ustalona przez stacje sekwencja wartości na polach adresowych MAC, bądź na innych polach nagłówka prowadzi do stanu, w którym stacje stanowiące ukrytą grupę przechodzą w tzw. **tryb uszkodzonych ramek** – tj. tryb z większą przepustowością, dzięki czemu dostępne stają się kanały K2 i K3. Ustalona przez stacje sekwencja wartości na polach adresowych MAC, bądź na innych polach nagłówka, stanowi wspólną wiedzę stacji i nie jest przedmiotem specyfikacji systemu.

Etap 3 (tryb uszkodzonych ramek)

W trybie uszkodzonych ramek informacje są przesyłane w części użytkowej ramek (K3) z celowo niepoprawnie stworzonymi sumami kontrolnymi (K2). W ten sposób może być wykorzystana w pełni, przez pewien czas, dostępna przepustowość. Pozostałe stacje niebędące członkami ukrytej grupy odrzucają ramki z niepoprawnymi sumami kontrolnymi. Sposób tworzenia niepoprawnych sum kontrolnych stanowi wspólną wiedzę stacji i nie jest przedmiotem specyfikacji. Określona sekwencja na kanałach (K1-K3) powoduje powrót do stanu wyjściowego. Sekwencja ta stanowi wspólną wiedzę stacji i nie jest przedmiotem specyfikacji. W sieciach WLAN praca interfejsów sieciowych przesyłających dane z uszkodzonych ramek do warstw wyższych, wymaga trybu monitorującego karty sieciowej (por. rozdział 2.2).

Dopóki nie istnieje podejrzenie, że uszkodzone ramki są tworzone celowo, działanie systemu HICCUPS pozostaje niewidoczne. W niektórych przypadkach, przy częstym alokowaniu dodatkowej przepustowości, sieć, w której działa proponowany system, będzie mieć znacznie wyższą ramkową stopę błędów (**FER** – *Frame Error Rate*) niż sieć działająca bez systemu HICCUPS. Stąd też HICCUPS powinien być rozbudowany o mechanizm śledzenia aktualnej ramkowej stopy błędów, aby móc w sposób elastyczny sterować jej obniżeniem. Rozdział 4.6 zawiera opis tego mechanizmu, zrealizowanego w podwarstwie zarządzania prawem do głosu.

Przy wdrażaniu systemu HICCUPS należy zdecydować, czy wykorzystywany przez HICCUPS protokół komunikacyjny w ramach ukrytej grupy ma być **protokołem zawodnym** (*unreliable*), czy też nie. Przez **protokół niezawodny**, będziemy rozumieć protokół, w którym stacja nadawcza posiada wiedzę, czy przesłane dane zostały odebrane poprawnie przez stację odbiorczą. Informacja o udanej transmisji może być wywnioskowana, np. na podstawie mechanizmu potwierdzeń (pozytywnych, bądź negatywnych). Brak potwierdzenia pozytywnego lub uzyskanie potwierdzenia negatywnego najczęściej prowadzi do sytuacji, w której dochodzi do retransmisji danych. Przez **protokół zawodny** będziemy rozumieć protokół, w którym stacja nadawcza wysyła dane bez troski o uzyskanie informacji o tym, czy przesłane dane zostały odebrane poprawnie.

W dalszej części niniejszej rozprawy przyjęto, że protokół komunikacyjny w ramach ukrytej grupy jest **protokołem zawodnym** i w związku z tym nie posiada mechanizmów potwierdzeń, ani retransmisji. Brak tych mechanizmów wpływa na zwiększenie niewykrywalności systemu HICCUPS – hipotetyczny atak na system HICCUPS polegający na niszczeniu steganogramów nie implikuje żadnego zachowania protokołu. W przypadku protokołu niezawodnego, w zależności od ustalonego mechanizmu potwierdzeń: atakujący niszcząc steganogramy mógłby zaobserwować bądź pojawienie się negatywnych potwierdzeń, bądź zanik pozytywnych. Z kolei w przypadku retransmisji, ze względu na to, że ramki z celowo uszkodzonymi sumami kontrolnymi wpływają na FER sieci, atakujący mógłby obserwować wzrost FER po zaprzestaniu niszczenia steganogramów.

Aby jednak odbiorcy mogli zweryfikować poprawność steganogramów, zakładamy, że istnieje wewnętrzny **mechanizm integralności** w wiadomościach przesyłanych

w obrębie ukrytej grupy w trybie uszkodzonych ramek. Dzięki temu mechanizmowi, system HICCUPS jest w stanie wykryć przekłamania wynikające z błędów w kanale.

4.5 Zarządzanie usługami ochrony informacji

Za sterowanie bezpieczeństwem ukrytej grupy odpowiada podwarstwa zarządzania usługami ochrony informacji. Główne operacje przeprowadzane przez tę podwarstwę to:

- uzgodnienie/wymiana klucza grupowego (por. Etap 1 – inicjacja systemu),
- odświeżanie klucza grupowego,
- renegocjacja klucza grupowego.

W bezpieczeństwie ukrytej grupy można wydzielić dwa obszary związane z zastosowanymi usługami ochrony informacji:

- realizacja podstawowych usług ochrony informacji dla ukrytej grupy,
- zarządzanie kluczami kryptograficznymi.

W ukrytej grupie przeważnie zapewnia się [54]: poufność, integralność danych, uwierzytelnienie źródła danych oraz uwierzytelnienie grupy. **Poufność** jest realizowana poprzez zaszyfrowanie danych wymienianych pomiędzy nadawcą a odbiorcami za pomocą **klucza grupowego**. Uwierzytelnienie źródła danych jest realizowane najczęściej wraz z integralnością danych. Uwierzytelnienie grupy jest poświadczeniem, że dane zostały utworzone podczas sesji przez grupę.

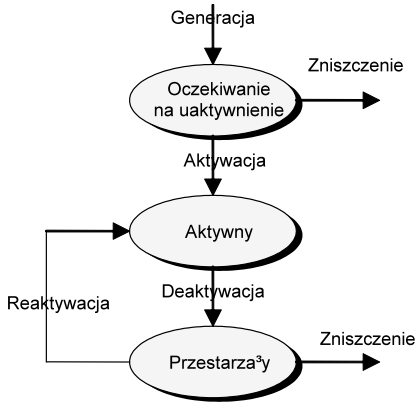
Zarządzanie kluczami kryptograficznymi jest związane z zarządzaniem materiałem klucza, informacjami o stanie kluczy, w tym informacją o ich przynależności.

Klucze kryptograficzne przechodzą przez serię stanów, które określają ich cykl życia [55]. Trzy podstawowe **stany** to:

- **oczekiwanie na uaktywnienie** – klucz nie jest używany do ochrony żadnej informacji,
- **stan aktywny –** klucz jest używany do kryptograficznej ochrony informacji;
- **stan przestarzały** – klucz służy jedynie do odszyfrowania lub weryfikacji.

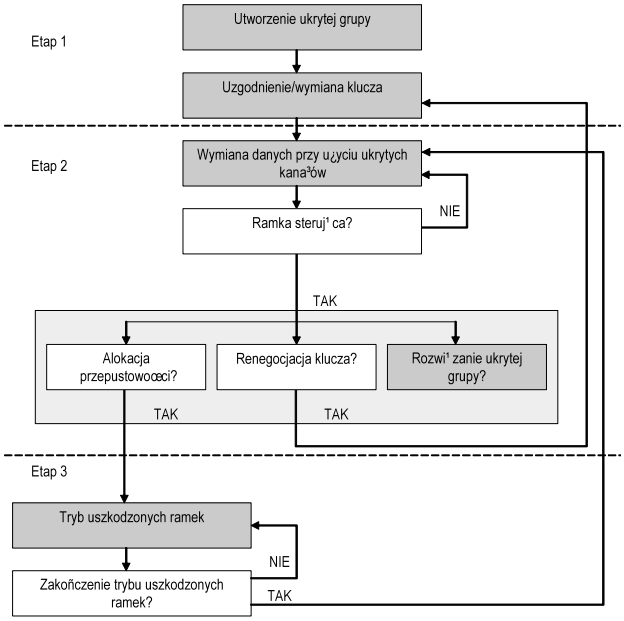
Następujące **procesy** odpowiadają za przejścia pomiędzy stanami:

- **generacja –** proces generacji klucza,
- **aktywacja –** proces umożliwiający użycie klucza,
- **deaktywacja –** proces ograniczający użycie klucza,
- **reaktywacja –** proces umożliwiający ponowne użycie przestarzałego klucza,
- **zniszczenie –** zakończenie życia klucza.



Rysunek 4-4 Cykl życia klucza kryptograficznego

Rysunek 4-5 zawiera schemat działania proponowanego systemu, uszczegółowiony pod kątem czasu życia ukrytej grupy.



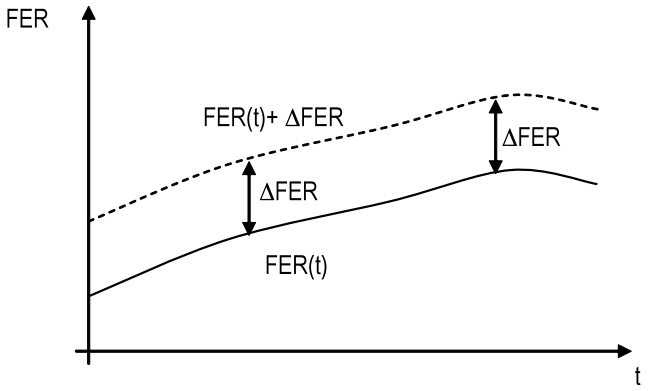
Rysunek 4-5 Uszczegółowiony schemat działania proponowanego systemu

4.6 Zarządzanie prawem do głosu

Podwarstwa zarządzania prawem do głosu steruje możliwością nadawania informacji w trybie uszkodzonych ramek. Główne operacje przeprowadzane przez tę podwarstwę to:

- badanie aktualnej ramkowej stopy błędów w sieci użytkowej,
- tworzenie dodatkowego ruchu w przypadku niewystarczającej aktywności stacji.

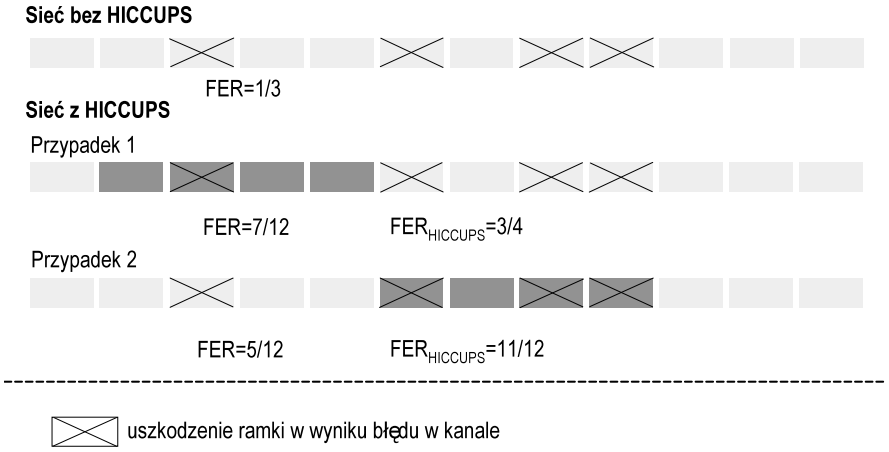
Przyjmijmy, że system HICCUPS, pracujący w trybie uszkodzonych ramek, pogarsza ramkową stopę błędów sieci użytkowej o stałą wartość Δ*FER* (Rysunek 4-6). Wielkość Δ*FER* będziemy traktować jako parametr omawianej podwarstwy. Ramkowa stopa błędów, jako miara jakościowa, mówi jedynie o proporcji pomiędzy ramkami odebranymi niepoprawnie, a ramkami wysłanymi. Zatem parametr Δ*FER* wpływa bezpośrednio na górne ograniczenie przepustowości (czyli efektywności) uzyskiwanej przez system HICCUPS. W sieci, w której jest wymienianych stosunkowo mało danych użytkowych np. w wyniku małej aktywności stacji, system HICCUPS powinien zapewnić dodatkowy ruch użytkowy tak, aby osiągnąć pożądaną efektywność.



Rysunek 4-6 Wpływ systemu HICCUPS na ramkową stopę błędów sieci użytkowej

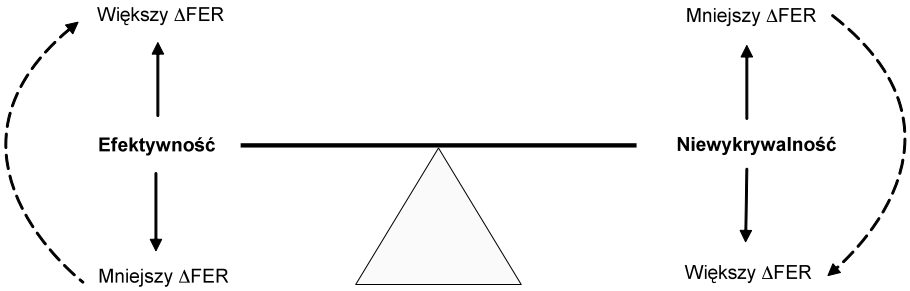
Z punku widzenia analizy właściwości systemu HICCUPS, która zostanie dokonana w rozdziale 6, istotne jest uwypuklenie różnicy pomiędzy ramkową stopą błędów obserwowaną w sieci użytkowej, a ramkową stopą błędów obserwowaną w systemie HICCUPS ($FER_{HICCUPS}$).

W rozważanej sytuacji weźmiemy pod uwagę dwanaście ramek (Rysunek 4-7). Załóżmy, że *FER* w sieci bez HICCUPS wynosi 1/3, czyli średnio co trzecia ramka jest tracona w wyniku błędów w kanale. Załóżmy, że system HICCUPS wprowadza cztery ramki z uszkodzonymi sumami kontrolnymi, w miejsce ramek z poprawnymi sumami. Rozważmy dwa przypadki z tym samym rozkładem błędów w kanale. W pierwszym przypadku, tylko jedna z ramek wprowadzonych przez system HICCUPS zostaje uszkodzona, w drugim przypadku – trzy. W pierwszym przypadku *FER* sieci użytkowej wynosi 7/12 (czyli Δ*FER*=1/4), natomiast $FER_{HICCUPS}$ wyniesie 3/4 (czyli 1-Δ*FER*). W drugim przypadku – *FER* sieci użytkowej wynosi 5/12 (czyli Δ*FER*=1/12), a $FER_{HICCUPS}$=11/12 (czyli 1-Δ*FER*). Reasumując, na wielkość $FER_{HICCUPS}$ wpływa wyłącznie liczba ramek z nieuszkodzonymi steganogramami.



Rysunek 4-7 Ramkowa stopa błędów (FER) obserwowana w sieci użytkowej, a ramkowa stopa błędów w systemie HICCUPS

Wybór Δ*FER*, jako parametru podwarstwy zarządzania prawem do głosu, istotnie wpływa na niewykrywalność systemu HICCUPS. Rysunek 4-8 ilustruje konflikt pomiędzy efektywnością a niewykrywalnością w systemie HICCUPS (por. rozdział 3.2). Przyjmując dużą wartość Δ*FER* w stosunku do ramkowej stopy błędów *FER* ryzykujemy wykryciem obecności systemu, równocześnie zyskując na efektywności. Przyjmując małą wartość Δ*FER* – osiągamy większe bezpieczeństwo systemu, kosztem efektywności. W praktyce, wybór wartości Δ*FER* powinien wynikać z pragmatycznej oceny jakości i skuteczności działania systemu HICCUPS w konkretnym środowisku sieciowym.



Rysunek 4-8 Konflikt pomiędzy efektywnością a niewykrywalnością w HICCUPS

5. System HICCUPS w sieciach IEEE 802.11

5.1 Cechy podstawowe

Sieci WLAN działające wg standardu IEEE 802.11 [44] posiadają wszystkie cechy niezbędne do realizacji systemu HICCUPS (por. rozdział 4.1), w szczególności:

- metodę dostępu do wspólnego medium CSMA/CA dającą możliwość kopiowania wszystkich ramek z kanału,
- kontrolę poprawności ramek (mechanizm FCS – *Frame Check Sequence*) za pomocą sum kontrolnych – CRC-32,
- opcjonalnie: mechanizm zapewniający poufność części użytkowej ramki (WEP, TKIP, CCMP).

Istotną własnością sieci bezprzewodowych jest duża podatność kanału radiowego na błędy ([23], [26]), które wynikają m.in. z utraty mocy sygnału wraz z odległością pomiędzy nadajnikiem a odbiornikiem, szumu i interferencji od innych sieci lub urządzeń (w przypadku pasma 2.4 GHz interferencji od kuchenek mikrofalowych i urządzeń Bluetooth), szybkich zaników (*fast fading*) związanych z ruchem stacji i propagacją wielodrogową, wolnych zaników (*slow fading*) związanych z ruchem pomiędzy dużymi przeszkodami. Część z powyższych zjawisk, w szczególności szumy i interferencje, ma charakter zmienny i w wielu przypadkach nieprzewidywalny.

W sieciach IEEE 802.11 możemy wyróżnić następujące ukryte kanały:

– K1**:** kanał oparty na adresach sieciowych MAC (maksymalnie 4 pola adresowe po 48-bitów) oraz innych polach nagłówka, np. pole *Frame Control* o wielkości 16 bitów,

– K2**:** kanał oparty na sumach kontrolnych CRC-32 o wielkości 32 bity,

– K3**:** kanał oparty na polu użytkowym ramki o maksymalnej wielkości 18432 bitów (2304[5] oktetów).

W przypadku użycia mechanizmu WEP istnieje możliwość wykorzystania w ramach kanału K1 pól inicjujących wektory IV (o wielkości 24 bity).

Sieci IEEE 802.11 zostały zaprojektowane do transmisji typu unicast i są wyposażone w mechanizm pozytywnych potwierdzeń (ACK). Stacje będące w zasięgu radiowym mogą odbierać wszystkie informacje wymieniane w medium, jednak w protokole 802.11 nie istnieje możliwość potwierdzenia faktu odbioru danych przez stacje, do których dane te nie były kierowane. Należy jednak zauważyć, że przejście do trybu z uszkodzonymi ramkami HICCUPS jest potwierdzane przez stację odbierającą przez wysłanie ramki ACK.

[5] Jest to wielkość pola użytkowego przed użyciem mechanizmu szyfrowania np. przy zastosowaniu WEP maksymalny rozmiar to 2312 oktetów ([44], [49]).

Tryb uszkodzonych ramek systemu HICCUPS zastosowany do sieci 802.11 jest ściśle powiązany z mechanizmem retransmisji. Stacje należące do ukrytej grupy przesyłając ramki z celowo uszkodzonymi sumami kontrolnymi zachowują się tak jak stacje, które nie otrzymują pozytywnego potwierdzenia, a więc ponawiają transmisję. W sieci bez HICCUPS kolejne retransmitowane ramki są pod względem zawartości takie same. Aby system HICCUPS był niewykrywalny istotne jest zbadanie rzeczywistego wpływu zniekształceń na ramkę (podobnie jak w pracy [115]), w szczególności rozkładu błędów i ewentualnej korelacji pomiędzy nimi. Taka analiza mogłaby doprowadzić do stworzenia algorytmu upodabniającego do siebie kolejne ramki wysyłane przez system HICCUPS (w jednym cyklu retransmisyjnym 802.11) zgodnie z fizycznymi własnościami kanału radiowego. Zwiększenie niewykrywalności poprzez upodobnienie do siebie ramek prowadzi do spadku efektywności systemu (por. rozdział 3.2).

Rozważmy sytuację działania systemu HICCUPS w trybie infrastrukturalnym 802.11 – IBSS (*Independent Basic Service Set*). Punkt dostępowy jest mostem (*bridge*) pośredniczącym w wymianie danych pomiędzy stacjami i nie przekazuje dalej (*forwarding*) ramki z niezgodną sumą kontrolną. W sytuacji, gdy wszystkie stacje ukrytej grupy są w zasięgu radiowym, obecność punktu dostępowego nie jest istotna, gdyż członkowie ukrytej grupy mogą nasłuchiwać wszystkich transmisji. W przypadku, gdy nie wszystkie stacje są w zasięgu, jedyna metoda łączności następuje przez punkt dostępowy, który powinien być członkiem ukrytej grupy. Aby zwiększyć niewykrywalność systemu HICCUPS punkt dostępowy powinien buforować transmisje w trybie uszkodzonych ramek, aż do momentu przekazania tych danych dalej. Tak określony schemat działania prowadzi do nieuchronnych opóźnień i wymaga użycia dodatkowej pamięci na buforowanie danych. W dalszej części pracy omówiono przypadek, w którym wszystkie stacje są w zasięgu radiowym. Brak istotnej roli punktu dostępowego w omawianej sytuacji pozwala sprowadzić nasze rozważania do trybu ad hoc – BSS (*Basic Service Set*).

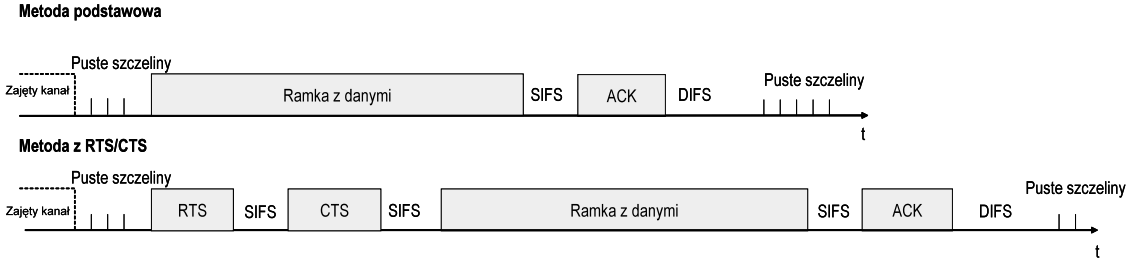
5.2 Cechy protokołu CSMA/CA (istotne z punktu widzenia zastosowania systemu HICCUPS)

Realizacja systemu HICCUPS jest ściśle związana z metodą dostępu do medium. Używany przez sieci 802.11 protokół CSMA/CA bazuje na ulepszonej wersji protokołu MACA [59] – MACAW [8]. Protokół CSMA/CA jest określony w standardzie mianem DCF (*Distributed Coordination Function*) i używa procedury wykładniczego odczekiwania (*backoff*) w celu unikania kolizji. W dalszej części pracy będzie stosowane określenie ***procedura backoff***.

Drugą metodą dostępu w podwarstwie MAC określoną w standardzie IEEE 802.11 [44], jest metoda PCF (*Point Coordination Protocol*) polegająca na przepytywaniu (*polling*). Protokół PCF jest wolny od kolizji i jest przeznaczony dla aplikacji czasu rzeczywistego. Praktyczne użycie tej metody dostępu jest jednak marginalne, w związku z tym w dalszej części pracy ograniczymy się do rozważania DCF.

Wyróżnia się dwa warianty działania CSMA/CA (Rysunek 5-1):

- **metodę podstawową** (*basic metod, 2-way-handshake*) – bez rezerwacji kanału,
- **metodę z RTS/CTS** (*RTS/CTS method, 4-way handshake*) – z rezerwacją kanału.

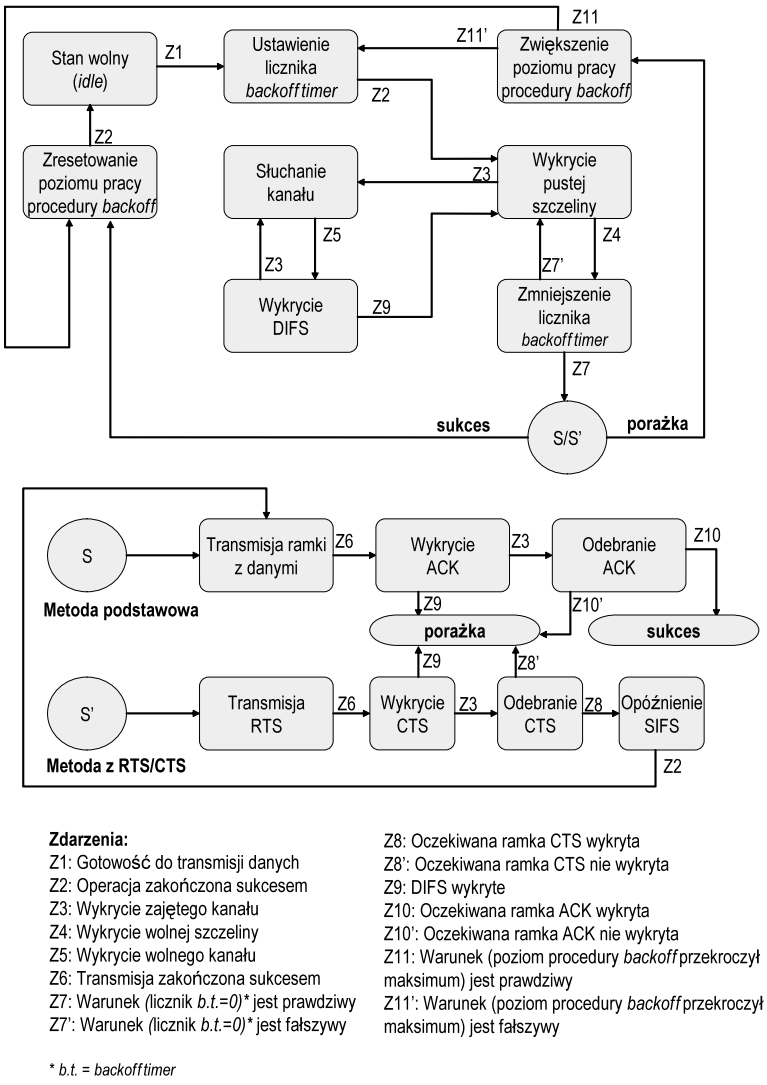


Rysunek 5-1 Dwie metody dostępu w CSMA/CA: podstawowa i z RTS/CTS

W metodzie podstawowej stacja, która chce wysłać ramkę z danymi, nasłuchuje kanał transmisyjny (Rysunek 5-2). W celu uniknięcia kolizji stacja korzysta z **licznika *backoff timer***. Po wykryciu, że kanał jest wolny (*idle*) przez czas **DIFS** (*DCF IntreFrame Space*), licznik *backoff timer* jest inicjowany liczbą losową *X*. Wartość licznika jest zmniejszana o jeden przy każdym wykryciu pustej szczeliny (*slot*), natomiast gdy kanał jest zajęty (*busy*) przez inną transmisję, wartość licznika nie jest zmieniana. Wznowienie pracy licznika może nastąpić po zakończonej transmisji, tj. po wykryciu DIFS. Gdy wartość licznika osiągnie 0, stacja może rozpocząć transmisję. Wartość licznika *X* jest liczbą całkowitą losowaną z przedziału $X \in [0, CW]$, gdzie *CW* to wartość tzw. okna niezgody (*Contention Window*). Początkowo *CW* jest ustawione na CW_{min}; po każdym nieskutecznym wysłaniu ramki wielkość okna jest podwajana[6], aż do osiągnięcia wartości CW_{max} (Rysunek 5-3). Jest to tzw. **zwiększenie poziomu procedury *backoff***, które możemy utożsamiać z kolejnymi próbami transmisji. W przypadku udanej transmisji ramki z danymi, wielkość okna dla kolejnej ramki jest ustawiana na CW_{min}.

Aby stacja nadająca mogła stwierdzić, że transmisja powiodła się, protokół wykorzystuje pozytywne potwierdzenia. Stacja odbierająca ramkę po stwierdzeniu jej poprawności wysyła do stacji nadającej ramkę ACK. ACK jest wysyłane po czasie **SIFS** (*Short InterFrame Space*). Jeśli potwierdzenie nie zostanie odebrane po czasie SIFS, stacja nadająca traktuje transmisję jako nieudaną i uznaje, że powinna nastąpić retransmisja. W takim przypadku kolejna transmisja w kanale będzie mogła nastąpić po czasie **EIFS** (*Extended InterFrame Space*) liczonym od momentu zakończenia transmisji ramki z danymi.

[6] Ponieważ określona w standardzie 802.11 wielkość okna jest liczbą nieparzystą, w istocie jest to podwajanie i dodanie liczby 1.

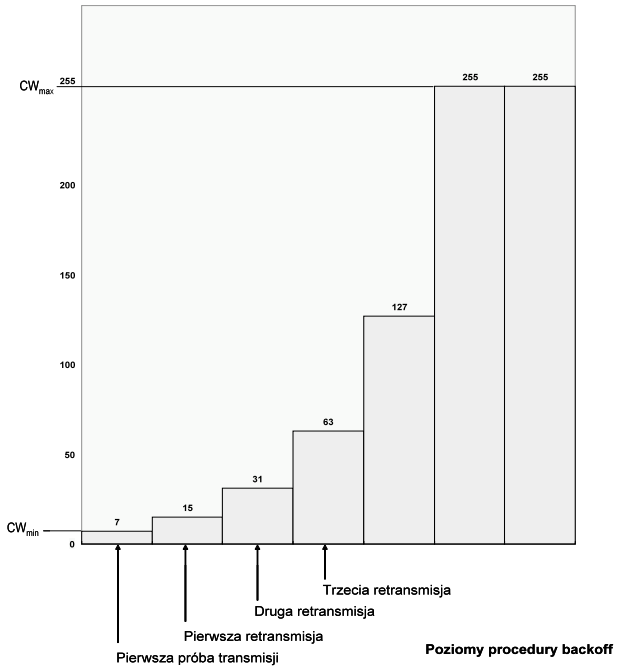


Zdarzenia:
Z1: Gotowość do transmisji danych
Z2: Operacja zakończona sukcesem
Z3: Wykrycie zajętego kanału
Z4: Wykrycie wolnej szczeliny
Z5: Wykrycie wolnego kanału
Z6: Transmisja zakończona sukcesem
Z7: Warunek *(licznik b.t.=0)** jest prawdziwy
Z7': Warunek *(licznik b.t.=0)** jest fałszywy
Z8: Oczekiwana ramka CTS wykryta
Z8': Oczekiwana ramka CTS nie wykryta
Z9: DIFS wykryte
Z10: Oczekiwana ramka ACK wykryta
Z10': Oczekiwana ramka ACK nie wykryta
Z11: Warunek (poziom procedury *backoff* przekroczył maksimum) jest prawdziwy
Z11': Warunek (poziom procedury *backoff* przekroczył maksimum) jest fałszywy

* *b.t. = backoff timer*

Rysunek 5-2 Automat skończony prezentujący przejścia pomiędzy stanami w CSMA/CA – na podstawie [33]

W przypadku metody z RTS/CTS (Rysunek 5-2), która funkcjonalnie jest rozszerzeniem metody podstawowej, zanim stacja rozpocznie transmisję ramki z danymi, wysyła do odbiorcy krótką ramkę RTS (*Request to Send*) w celu rezerwacji kanału. Jeśli odbiorca jest w stanie odebrać ramkę, tj. nie jest zaangażowany w inną transmisję, wysyła po czasie SIFS do nadawcy ramkę potwierdzającą rezerwację – CTS (*Clear to Send*). Po prawidłowym odbiorze ramki CTS nadawca zachowuje się tak jak przy metodzie podstawowej. W przypadku odebrania ramki CTS wysyłana ramka z właściwymi danymi nie ulegnie kolizji – tylko pierwsza wysyłana ramka (RTS) może wejść w kolizję z inną ramką. Metoda z RTS/CTS ma szczególne zastosowanie w sytuacji, gdy w sieci WLAN istnieją ukryte terminale (*hidden terminals*), czyli stacje, które są poza zasięgiem niektórych stacji z komunikującej się grupy.



Rysunek 5-3 Przykład wykładniczego zwiększania okna niezgody – poziomy procedury *backoff*

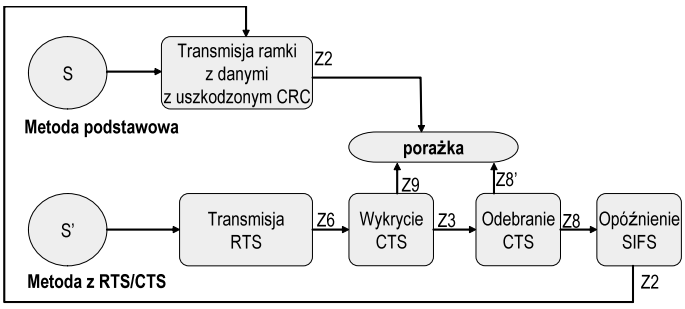
W przypadku metody podstawowej, po nieudanej transmisji, ramka jest retransmitowana maksymalnie 4 razy (tzw. ograniczenie *LongRetryLimit*). W przypadku metody z RTS/CTS ramka z RTS jest retransmitowana maksymalnie 7 razy (tzw. ograniczenie *ShortRetryLimit*). Liczniki powtórzeń skojarzone z ograniczeniami *LongRetryLimit* i *ShortRetryLimit* (odpowiednio SLRC – *STA Long Retry Counter* i SSRC – *STA Short Retry Counter*) są niezależne. Obydwa liczniki są początkowo ustawione na 0. Nieodebranie prawidłowego CTS powoduje zwiększenie licznika o jeden; poprawne odebranie powoduje wyzerowanie licznika SSRC. Analogicznie dla SLRC: brak poprawnego odebrania ACK zwiększa licznik o jeden, poprawne – zeruje. Brak odebrania CTS, jak i ACK, wymusza zwiększenie okna niezgody, aż do maksymalnego rozmiaru. Jak wspomniano wcześniej, dopiero w przypadku udanej transmisji ramki z danymi wielkość okna dla kolejnej ramki jest ustawiana na CW_{min}.

Wielkości:

- czas trwania pustej szczeliny (a*SlotTime* [44]) – oznaczany dalej σ,
- czas SIFS (T_{SIFS}),
- czas DIFS (T_{DIFS}),
- czas EIFS (T_{EIFS}),
- CW_{min} oraz CW_{max}

są uzależnione od warstwy fizycznej 802.11 PHY i są specyfikowane przez standard (por. rozdział 5.3, Tabela 5-3).

System HICCUPS w trybie uszkodzonych ramek wykorzystuje mechanizm retransmisji 802.11 (por. rozdział 5.1). W konsekwencji, jedynej modyfikacji w automacie skończonym ulega proces wysyłania ramek z danymi (Rysunek 5-4). Stacja nadawcza celowo przekłamuje CRC w ramce i wykorzystuje do transmisji kolejne stany procedury *backoff*. Ponieważ podstawowa wymiana informacji systemu HICCUPS dokonuje się na kanałach z poprawnymi ramkami, odebranie ramki sygnalizującej przejście w tryb uszkodzonych ramek jest potwierdzane przez ACK. Zgodnie z założeniami z rozdziału 4.4, w trybie uszkodzonych ramek system HICCUPS zachowuje się jak protokół zawodny, tj. żadne potwierdzenia nie są przysyłane do nadawcy, jednak odbiorca jest w stanie zweryfikować integralność steganogramu.



Rysunek 5-4 Zmodyfikowana część automatu skończonego prezentującego przejścia pomiędzy stanami w CSMA/CA w systemie HICCUPS w trybie uszkodzonych ramek (oznaczenia zdarzeń – por. Rysunek 5-2)

5.3 Parametry warstwy fizycznej 802.11a, 802.11g (ERP-OFDM) i 802.11-1999 DSSS

Parametry warstwy fizycznej (PHY) są istotne z punktu widzenia analizy ilościowej systemu HICCUPS, która zostanie przedstawiona w następnym rozdziale i będzie dotyczyć technik bazujących na OFDM (*Orthogonal Frequency Division Multiplexing*). W części symulacyjnej (związanej z weryfikacją modelu protokołu DCF) zostanie uwzględniona także warstwa fizyczna 802.11-1999 DSSS działająca z **szybkością transmisji danych *R*** (*data rate* – [44]) 1 Mbit/s.

W sieciach WLAN zgodnych z 802.11a [45] i 802.11g [48] wykorzystywana jest metoda rozpraszania widma OFDM. W celu dostosowania warstwy fizycznej do różnych warunków działania sieci, w szczególności do różnych wartości współczynnika sygnał-sum (SNR – *Signal-to-Noise Ratio*), w 802.11a i 802.11g wprowadzono różne schematy modulacji (Tabela 5-1) tj.:

- BPSK (*Binary Phase Shift Keying*),
- QPSK (*Quadrature Phase Shift Keying*),
- *M*-QAM (*M-Quadrature Amplitude Modulation*), gdzie $M=16$ i 64,

oraz różne stopnie kodowania nadmiarowego (1/2, 2/3, 3/4) do korygowania błędów transmisyjnych.

Tabela 5-1 Charakterystyki modulacji sygnału OFDM w 802.11a i 802.11g

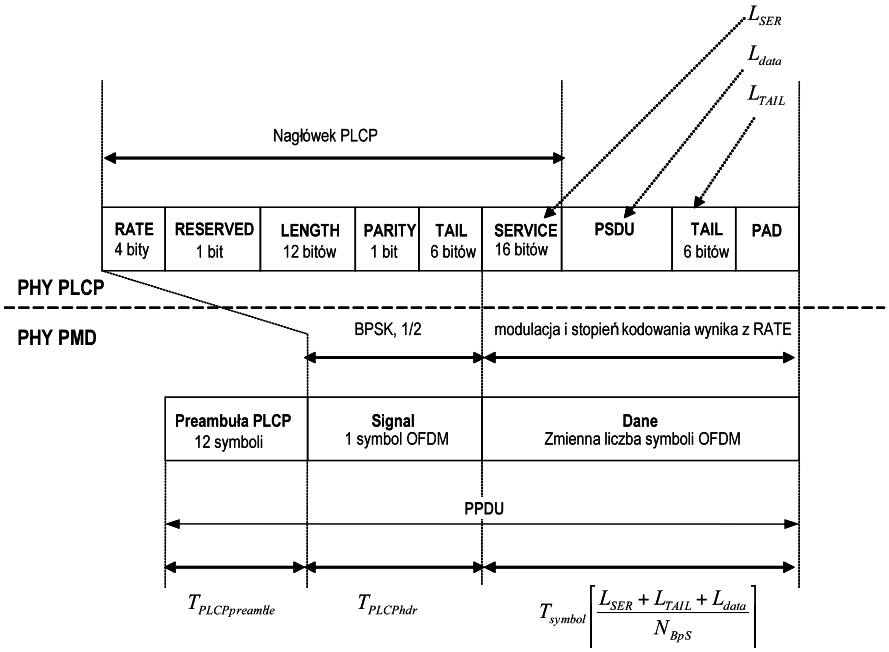
Szybkość transmisji danych – *R* [Mbit/s]	Rodzaj modulacji	Współczynnik kodu	Liczba bitów na symbol – N_{BpS}
6	BPSK	½	24
9	BPSK	¾	36
12	QPSK	½	48
18	QPSK	¾	72
24	16-QAM	½	96
36	16-QAM	¾	144
48	64-QAM	⅔	192
54	64-QAM	¾	216

Każdy symbol modulacji może być zakodowany ustaloną liczbą bitów N_{BpS} (*number of encoded bits per symbol*) – Tabela 5-1.

Warstwa fizyczna PHY 802.11 składa się z dwóch podwarstw:

- *PHY Layer Convergence Procedure* (PLCP), która odpowiada za wymianę ramek pomiędzy warstwą PHY a podwarstwą MAC,
- *PHY Medium-Dependent* (PMD), która prowadzi fizyczną transmisję w medium bezprzewodowym.

Przed każdą transmisją ramka MAC, czyli PSDU (*PLCP Service Data Unit*), jest enkapsulowana w jednostkę danych warstwy PLCP, czyli PPDU (*PLCP Protocol Data Unit*).



Rysunek 5-5 Jednostka danych PPDU dla 802.11a i 802.11g (ERP-OFDM)

Czas trwania jednego symbolu OFDM w 802.11a i 802.11g to 4μs. Każda ramka na poziomie warstwy PHY jest poprzedzona preambułą składającą się z 12 symboli treningowych (10 „krótkich" po 0,8 μs i 2 „długie" po 4 μs). Preambuła trwa zatem 16 μs. Nagłówek PLCP, za wyjątkiem 16-bitowego pola SERVICE, jest kodowany na jednym symbolu OFDM za pomocą modulacji BPSK z współczynnikiem kodu nadmiarowego 1/2 (a więc z szybkością 6 Mbit/s). Pole SERVICE nagłówka PLCP, jednostka danych PSDU (czyli ramka MAC), 6 bitów zakończenia (pole TAIL), a także niezbędne bity uzupełnienia (PAD), są kodowane za pomocą wybranej modulacji z właściwym współczynnikiem kodu nadmiarowego (Tabela 5-1). Informacja o rodzaju modulacji i współczynniku kodu nadmiarowego jest przekazywana w polu RATE nagłówka PLCP.

Czas trwania transmisji T ramki o długości L_{data} wynosi zatem (por. Rysunek 5-5 i [75]):

$$T = T_{PHYhdr} + T_{symbol}\left\lceil \frac{L_{SER} + L_{TAIL} + L_{data}}{N_{BpS}} \right\rceil, \tag{5-1}$$

gdzie T_{PHYhdr} to czas trwania preambuły i nagłówka PLCP bez pola SERVICE:

$$T_{PHYhdr} = T_{PLCPpreamble} + T_{PLCPhdr} = 16 + 4 = 20\,[\mu s], \tag{5-2}$$

a T_{symbol} to wynoszący $4\ \mu s$ czas trwania symbolu OFDM. $\lceil x \rceil$ oznacza część całkowitą z x powiększoną o liczbę 1. Długość pola SERVICE L_{SER} wynosi 16 bitów, a długość pola SERVICE L_{TAIL} 6 bitów. Natomiast wartość N_{BpS} wynika z ustalonej metody modulacji oraz współczynnika kodu i jest powiązana z szybkością transmisji danych R w następujący sposób:

$$R = \frac{\mathrm{N_{BpS}}}{T_{symbol}}. \tag{5-3}$$

W sieciach WLAN zgodnych z 802.11-1999 DSSS [44] wykorzystywana jest technika rozpraszania widma DSSS (*Direct Sequence Spread Spectrum*). Preambuła (tzw. długa preambuła) i nagłówek są transmitowane z szybkością 1 Mbit/s. Użyte modulacje dla danych to DBPSK (*Differential Binary Phase Shift Keying*) dla szybkości 1 Mbit/s oraz DQPSK (*Differential Quadrature Phase Shift Keying*) dla 2 Mbit/s.

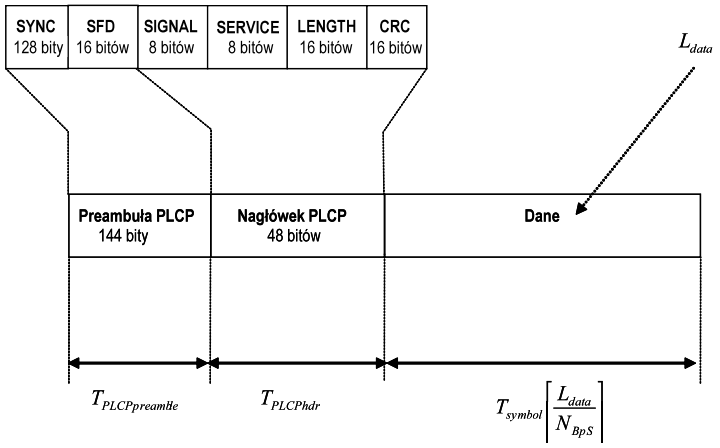
Czas trwania symbolu DSSS T_{symbol} wynosi 1 μs, zatem każdy bit preambuły i nagłówka trwa 1 μs. Czas trwania transmisji T ramki o długości L_{data} wynosi (Rysunek 5-6):

$$T = T_{PHYhdr} + T_{symbol}\left\lceil \frac{L_{data}}{N_{BpS}} \right\rceil, \tag{5-4}$$

gdzie T_{PHYhdr} to czas trwania preambuły i nagłówka PLCP:

$$T_{PHYhdr} = T_{PLCPpreamble} + T_{PLCPhdr} = 144 + 48 = 192\,[\mu s]. \tag{5-5}$$

Wartość N_{BpS}, podobnie jak dla OFDM, wynika z ustalonej metody modulacji (Tabela 5-2).



Rysunek 5-6 Jednostka danych PPDU dla 802.11-1999 DSSS

Tabela 5-2 Charakterystyki modulacji sygnału DSSS w 802.11-1999 DSSS

Szybkość transmisji danych – *R* [Mbit/s]	**Rodzaj modulacji**	**Liczba bitów na symbol – N_{BpS}**
1	DBPSK	1
2	DQPSK	2

Tabela 5-3 zestawia omówione (częściowo także w rozdziale 5.2) parametry rozważanych warstw PHY.

Tabela 5-3 Parametry 802.11a, 802.11g (ERP-OFDM) i 802.11-1999 DSSS

	802.11a	**802.11g**	**802.11-1999 DSSS**
T_{PHYhdr}[μs]	20		192
T_{symbol} [μs]	4		1
CW_{min}	15		31
CW_{max}	1023		
σ [μs]	9		20
T_{SIFS}[μs]	16	10	
T_{DIFS} [μs]	34	28	50

Wymieniony w rozdziale 5.2 czas T_{EIFS} jest zdefiniowany w standardzie 802.11 jako:

$$T_{EIFS}=T_{SIFS}+T_{PLCPpreamble}+T_{PLCPhdr}+T_{ACK}+T_{DIFS}, \qquad (5\text{-}6)$$

gdzie T_{ACK} to czas trwania ramki ACK (bez T_{PHYhdr}, por. zależność (6-3)).

6. Analiza właściwości systemu HICCUPS

6.1 Cele, założenia i etapy analizy

W niniejszym rozdziale przedstawiamy analizę właściwości systemu HICCUPS, w szczególności określimy (por. rozdział 3.2):

- **koszt użycia systemu HICCUPS (κ)** rozumiany jako utrata przepustowości użytkowej w sieci 802.11 wynikająca z działania systemu HICCUPS w trybie uszkodzonych ramek,
- **efektywność systemu HICCUPS (ε)** rozumiana jako przepustowość systemu HICCUPS w trybie uszkodzonych ramek.

Czynnikami istotnie wpływającymi na osiąganą faktycznie przepustowość sieci LAN są: błędy w kanale, metoda dostępu do medium i nadmiar informacyjny związany z nagłówkami. Miarą efektywnej przepustowości sieci w stanie, gdy każda ze stacji posiada niepustą kolejkę z oczekującymi do wysłania ramkami, jest **ruch przenoszony w warunkach nasycenia** (*saturation througput*) oznaczany dalej przez **RPN**. Warunki nasycenia (*saturated conditions*) są granicznym stanem sieci, w którym wszystkie stacje rywalizują o medium. RPN określa maksymalną szybkość wysyłania danych użytkowych przez protokół komunikacyjny, czyli jego maksymalną wydajność.

Aby wyznaczyć koszt κ, porównamy RPN sieci WLAN dla rzeczywistej ramkowej stopy błędów z RPN sieci WLAN dla stopy wynikającej z nałożenia się pracy systemu HICCUPS w trybie uszkodzonych ramek. Rzeczywista ramkowa stopa błędów (FER – *Frame Error Rate*) jest związana przede wszystkim z własnościami fizycznymi kanału, w szczególności z bitową stopą błędów (BER – *Bit Error Rate*). System HICCUPS wprowadzając swoje własne ramki z uszkodzonymi sumami kontrolnymi pogarsza ramkową stopę błędów sieci WLAN (por. rozdział 4.6). Warto podkreślić, że w sieci WLAN nie są rozróżniane ramki uszkodzone przez HICCUPS od ramek zniekształconych w wyniku błędów w kanale.

Aby określić efektywność ε systemu HICCUPS wyznaczymy jego RPN w stanie, który wynika z własności fizycznych (BER), jak i z liczby ramek uzyskanych w wyniku działania trybu uszkodzonych ramek.

W analizie przyjęto następujące założenia:

Założenie 1: O medium rywalizuje n stacji; każda ze stacji ma niepustą kolejkę (warunki nasycenia). Przypadek graniczny dla n=1 będziemy utożsamiać z sytuacją, gdy medium przejmuje jedna stacja poprzez transmisje danych do innej stacji, która z kolei może wysyłać wyłącznie potwierdzenia.

Założenie 2: Błędy w kanale pojawiają się losowo. Wszystkie stacje mają tą samą bitową stopę błędów (BER). Losowy rozkład błędów jest najgorszym przypadkiem, jeśli chodzi o wpływ na ramkową stopę błędów (FER).

Założenie 3: Wszystkie stacje są w zasięgu, czyli nie ma ukrytych stacji (por. rozdział 5.1). Zatem dostęp do medium może być zrealizowany za pomocą metody podstawowej, czyli bez RTS/CTS (por. rozdział 5.2) i stacje mogą komunikować się bezpośrednio, bez punktu dostępowego; stąd też rozważymy tryb ad hoc – BSS (*Basic Service Set*) – por. rozdział 5.1.

Założenie 4: Stacje używają tej samej warstwy fizycznej, pracującej z identyczną szybkością transmisji danych. W części analitycznej rozważono OFDM (por. rozdział 5.3), a w obliczeniach numerycznych przyjęto parametry standardu 802.11g 54 Mbit/s ERP-OFDM („tylko g"). 802.11g jest obecnie najpopularniejszym standardem WLAN w Europie, natomiast 54 Mbit/s to jego największa szybkość.

Założenie 5: Ramki z danymi mają stałą długość. Poza ramkami z danymi i potwierdzeniami ACK, nie są transmitowane żadne inne ramki.

Założenie 6: Ramki, które ulegają kolizji, są traktowane jako błędne. Jest to typowe założenie upraszczające dla modeli analitycznych. W rzeczywistych warunkach, pod pewnymi warunkami, istnieje możliwość poprawnego odebrania ramki, która uległa kolizji (tzw. *capture effect*) [61].

Założenie 7: Rozważany jest wariant pracy systemu HICCUPS, w którym wszystkie stacje dokonują transmisji w trybie uszkodzonych ramek. Jest to najgorszy przypadek, jeśli chodzi o rywalizację o medium stacji wspierających system HICCUPS. Konsekwencją tego założenia jest uzyskanie równomiernego wzrostu FER w sieci WLAN (por. rozdział 4.6).

Założenie 8: W trybie uszkodzonych, ramek system HICCUPS wykorzystuje do komunikacji w obrębie ukrytej grupy protokół zawodny (por. rozdział 4.4). System HICCUPS ma możliwość zweryfikowania integralności steganogramu (por. rozdział 4.4).

Założenie 9: W trybie uszkodzonych ramek dla każdej ramki zawartość pola użytkowego jest inna (por. rozdział 5.1). Założenie to pozwala oszacować maksymalną efektywność systemu HICCUPS w trybie uszkodzonych ramek.

Analizę właściwości systemu HICCUPS, której ostatecznym celem jest wyznaczenie kosztu κ (rozdział 6.7) i efektywności ε (rozdział 6.8), podzielono na pięć etapów:

Etap 1: Analiza krytyczna znanych z literatury modeli zachowania protokołu 802.11 CSMA/CA (DCF) w warunkach nasycenia (rozdział 6.2), której celem jest stworzenie ulepszonego modelu.

Etap 2: Propozycja ulepszonego modelu zachowania protokołu 802.11 CSMA/CA (DCF) w warunkach nasycenia w zastosowaniu do wyznaczania RPN (rozdział 6.3).

Etap 3: Ocena ulepszonego modelu przedstawionego w Etapie 2 (rozdział 6.4).

Etap 4: Wyznaczenie RPN dla systemu HICCUPS w trybie uszkodzonych ramek przy użyciu ulepszonego modelu (rozdział 6.5).

Etap 5: Analiza RPN na podstawie Etapu 2 i Etapu 4 (rozdział 6.6).

W dalszej części pracy zaproponowany ulepszony model zachowania protokołu 802.11 CSMA/CA (DCF) w warunkach nasycenia będzie nazywany **modelem NM (nowy model)**.

6.2 Analiza znanych z literatury modeli zachowania protokołu 802.11 CSMA/CA (DCF) w warunkach nasycenia

Jeden z pierwszych modeli zachowania protokołu 802.11 CSMA/CA (DCF) w warunkach nasycenia został zaproponowany przez G. Bianchiego w pracach [9] i [11]. Model Bianchiego składa się z dwóch komponentów: opartego na łańcuchach Markowa modelu procedury *backoff* dla CSMA/CA oraz uzależnionego od warstwy fizycznej modelu stanów w kanale.

H. Wu, Y. Peng, K. Long, S. Cheng, S. i J. Ma w pracy [120] zmodyfikowali model Bianchiego poprzez usunięcie niezgodnej ze standardem 802.11 nieskończonej liczby retransmisji. Oprócz wprowadzenia maksymalnej liczby poziomów procedury *backoff*, Wu i in. uwzględnili fakt, że okno niezgody powiększa się tylko do pewnego poziomu procedury.

E. Ziouva i T. Antonakopoulos w pracy [123], a za nimi M. Ergen w pracy [29] (a później w [28]), zmodyfikowali model Bianchiego, aby uwzględnić stan zawieszenia licznika *backoff timer* na czas wykrycia innej transmisji. Ziouva i Antonakopoulos, niezgodnie ze standardem 802.11, przyjęli, że po każdej udanej transmisji stacja może przejąć medium bez inicjowania procedury *backoff*. Rozwiązanie łańcucha Markowa z prac Ergena ([29], [28]) jest błędne.

Modele analityczne procedury *backoff* dla CSMA/CA zaproponowane przez Bianchiego, Ergena oraz Wu i in. odwołują się jedynie do prawdopodobieństwa kolizji – zakładają kanał transmisyjny bez błędów.

W pracy [17] P. Chatzimisios, A. Boucouvalasi i V. Vitsas oraz (najprawdopodobniej niezależnie) dwa lata później w pracy [75] Q. Ni, T. Li, T. Turletti i Y. Xiao rozszerzyli model Wu i in. poprzez uwzględnienie prawdopodobieństwa uszkodzenia ramki wynikającego z błędów w kanale. W pracy [17], w odróżnieniu od [75], nie uwzględniono jednak możliwości przekłamania ramki z potwierdzeniem (ACK).

W pracach Bianchiego [9], Ergena [29] oraz Wu i in. [120] rozważono zarówno metodę podstawową, jak i z RTS/CTS. We wspomnianych pracach, w przypadku metody z RTS/CTS, autorzy nie rozpatrywali dwóch niezależnych liczników powtórzeń SLRC i SRRC (por. rozdział 5.2). W pracy Wu i in. [120], wprowadzając maksymalną liczbę poziomów procedury *backoff,* zignorowano odmienny przebieg procesu retransmisji dla obydwu metod (por. rozdział 5.2). Nieuwzględnienie liczników SLRC i SRRC

przy metodzie z RTS/CTS powoduje, że zaproponowane w pracach [9], [29], [120] modele nie dają się przekształcić w dobre jakościowo modele dla kanałów z błędami. Prace Ni i in. [75] oraz P. Chatzimisiosa i in. [17] skupiają się na metodzie podstawowej.

W pracach Bianchiego [9], Wu i in. [120] oraz Chatzimisiosa i in. [17] niesłusznie przyjęto, że czas oczekiwania po uszkodzeniu ramki to DIFS. Zgodnie ze standardem jest to EIFS, co zauważono w pracy Ergena [29] oraz Ni i in. [75].

Na bazie modelu Bianchiego [9] powstało wiele modeli dla standardu 802.11e [47] (EDCF – *Enhanced DCF*): [121], [122], [27], [62]. Ciekawy jest model Y. Xiao z artykułu [122] uwzględniający zawieszenie licznika *backoff timer* na czas innej transmisji.

Część wspomnianych prac rozważa także pracę sieci WLAN w warunkach braku nasycenia ([29], [28], [27]).

Oprócz modeli zachowania protokołu 802.11 CSMA/CA wywodzących się z pracy Bianchiego [9], istnieją inne, które bazują m.in. na wartościach średnich ([105], [68]), na modelach dostępu p-trwałe (*p-persistent*) [16], na prawdopodobieństwach zależnych [10].

Tabela 6-1 zawiera porównanie cech wybranych modeli zachowania protokołu 802.11 CSMA/CA w warunkach nasycenia: modeli Bianchiego [9], Wu i in. [120], P. Chatzimisiosa i in. [17], Ergena [29] oraz Ni i in. [75].

Tabela 6-1 Porównanie cech wybranych modeli zachowania protokołu 802.11 CSMA/CA

Autor/ Autorzy	**Poziomy *backoff* zgodne z 802.11**	**Błędy w kanale**	**Zawieszenie licznika *backoff timer***	**EIFS**	**Uwagi**
G. Bianchi	-	-	-	-	pierwszy model procedury *backoff* oparty na łańcuchach Markowa
H. Wu i in.	+	-	-	-	spostrzeżenie, że model Bianchiego nie jest zgodny ze standardem – wprowadza nieskończoną liczbę transmisji
P. Chatzimisios i in.	+	+	-	-	rozszerzenie modelu Wu i in. o błędy w kanale, jednak bez zwrócenia uwagi na możliwość przekłamania ACK
M. Ergen	-	-	+	+	spostrzeżenie, że model Bianchiego nie uwzględnia zawieszenia licznika *backoff timer* na czas innej transmisji; niepoprawne rozwiązanie łańcucha Markowa
Q.Ni i in.	+	+	-	+	rozszerzenie modelu Wu i in. o błędy w kanale

Zaproponowany w następnym rozdziale model NM uwzględnia ulepszenia modelu Bianchiego wprowadzone przez Wu i in. oraz Ergena, a także rozszerzenie Ni i in. oraz Chatzimisios i in. dotyczące uwzględnienia błędów w kanale. Jednocześnie zawiera analizę stanów kanału zgodną ze standardem 802.11, tak jak w pracy Ni i in. [75].

Zaproponowany model koncepcyjnie jest najbardziej zbliżony do modelu Xiao z pracy [122], jednak w pracy tej rozważono kanał bez błędów, skupiono się jedynie na standardzie 802.11e (EDCF) i nie podano rozwiązań analitycznych.

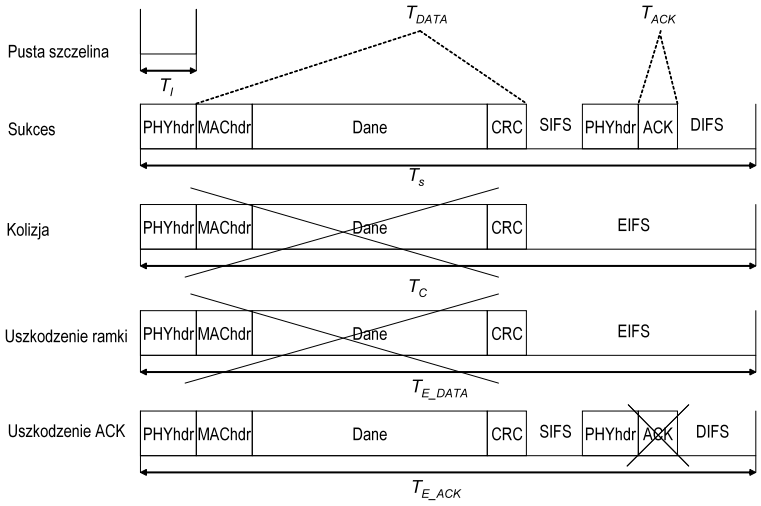
6.3 Analiza RPN dla WLAN – RPN_{WLAN}

6.3.1 Wyznaczenie RPN

RPN dla WLAN (RPN_{WLAN}) określimy analogicznie do pracy [9] (a także [29], [120], [75], [17]) jako:

$$RPN_{WLAN} = \frac{E[DATA]}{E[T]}, \tag{6-1}$$

gdzie $E[DATA]$ to oczekiwana liczba poprawnie przesłanych danych użytkowych, a więc danych z pola użytkowego ramki, a $E[T]$ to wartość oczekiwana czasu trwania wszystkich stanów w kanale.



Rysunek 6-1 Pięć możliwych stanów w kanale w trakcie pracy sieci WLAN

Czasy trwania poszczególnych stanów oznaczone są następująco (por. Rysunek 6-1):

T_I – czas trwania pustej szczeliny,

T_S – czas trwania transmisji zakończonej sukcesem,

T_C – czas trwania transmisji, podczas której doszło do kolizji,

T_{E_DATA} – czas trwania transmisji, podczas której uszkodzeniu uległa ramka z danymi w wyniku zakłóceń w kanale,

T_{E_ACK} – czas trwania transmisji, podczas której uszkodzeniu uległa ramka z potwierdzeniem (ACK) w wyniku zakłóceń w kanale.

Rysunek 6-1 obrazuje czas trwania poszczególnych stanów T_I, T_S, T_C, T_{E_DATA}, T_{E_ACK} w zależności od $T_{PHYhdr}, T_{DATA}, T_{ACK}, T_{SIFS}, T_{DIFS}, T_{EIFS}$.

T_{DATA} to czas trwania ramki z danymi (bez T_{PHYhdr}), a T_{ACK} to czas trwania ramki ACK (również bez T_{PHYhdr}). Podobnie jak w [75] i [29] przyjęto, zgodnie ze standardem 802.11, że po kolizji, bądź uszkodzeniu ramki z danymi, czas liczony od wysłania ramki to EIFS, a nie DIFS (jak założono błędnie w [9] i [120]).

Wobec tego:

$$\begin{cases} T_I = \sigma \\ T_S = 2T_{PHYhdr} + T_{DATA} + 2\delta + T_{SIFS} + T_{ACK} + T_{DIFS} \\ T_C = T_{PHYhdr} + T_{DATA} + \delta + T_{EIFS} \\ T_{E\_DATA} = T_{PHYhdr} + \delta + T_{DATA} + T_{EIFS} \\ T_{E\_ACK} = T_S \end{cases} \tag{6-2}$$

gdzie δ oznacza opóźnienie propagacji. Natomiast zgodnie z rozważaniami przeprowadzonymi w rozdziale 5.3 (por. zależność (5-1) i Rysunek 5-5) T_{ACK} i T_{DATA} wynoszą:

$$T_{ACK} = T_{symbol}\left\lceil \frac{L_{SER} + L_{TAIL} + L_{ACK}}{N_{BpS}} \right\rceil, \tag{6-3}$$

$$T_{DATA} = T_{symbol}\left\lceil \frac{L_{SER} + L_{TAIL} + L_{data}}{N_{BpS}} \right\rceil. \tag{6-4}$$

Parametry $\sigma, T_{PHYhdr}, T_{SIFS}, T_{DIFS}, T_{EIFS}, T_{symbol}, N_{BpS}, L_{SER}$ i L_{TAIL} są określone w standardzie IEEE 802.11 i zostały omówione w rozdziale 5.2.

Analogicznie jak w [75] wprowadzimy następujące prawdopodobieństwa wystąpienia poszczególnych stanów w kanale:

P_I – prawdopodobieństwo, że szczelina jest pusta,

P_S – prawdopodobieństwo, że transmisja zakończyła się sukcesem,

P_C – prawdopodobieństwo, że podczas transmisji nastąpiła kolizja,

P_{E_DATA} – prawdopodobieństwo, że ramka z danymi uległa uszkodzeniu w wyniku zakłóceń w kanale,

P_{E_ACK} – prawdopodobieństwo, że ramka z potwierdzeniem (ACK) uległa uszkodzeniu w wyniku zakłóceń w kanale.

Niech τ oznacza prawdopodobieństwo transmisji ramki, a p_{e_data} i p_{e_ACK} odpowiednio prawdopodobieństwo uszkodzenia ramki z danymi i prawdopodobieństwo

uszkodzenia ramki z ACK. Prawdopodobieństwa wystąpienia poszczególnych stanów w kanale związane z τ, p_{e_data} i p_{e_ACK} mają postać [75]:

$$\begin{cases} P_I = (1-\tau)^n \\ P_S = n\tau(1-\tau)^{n-1}(1-p_{e\_data})(1-p_{e\_ACK}) \\ P_C = 1-(1-\tau)^n - n\tau(1-\tau)^{n-1} \\ P_{E\_DATA} = n\tau(1-\tau)^{n-1} p_{e\_data} \\ P_{E\_ACK} = n\tau(1-\tau)^{n-1}(1-p_{e\_data}) p_{e\_ACK} \end{cases} \tag{6-5}$$

Zgodnie z przyjętymi założeniami (por. rozdział 6.1) rozważane ramki z danymi mają stałą długość. Zatem (podobnie jak w [75]):

$$RPN_{WLAN} = \frac{P_S L_{pld}}{T_I P_I + T_S P_S + T_C P_C + T_{E\_DATA} P_{E\_DATA} + T_{E\_ACK} P_{E\_ACK}}, \tag{6-6}$$

gdzie L_{pld} to długość danych w ramce MAC i $L_{pld} = L - L_{MAChdr}$, natomiast L_{MAChdr} to długość nagłówka warstwy MAC i pola FCS. RPN_{WLAN} jest wyrażone w bit/s. Miarę tę można znormalizować do szybkości transmisji danych R (por. rozdział 5.3):

$$\overline{RPN}_{WLAN} = \frac{RPN_{WLAN}}{R}. \tag{6-7}$$

Ponieważ RPN_{WLAN} jest wyrażone poprzez τ, p_{e_data} i p_{e_ACK}, przejdźmy do wyznaczenia tych prawdopodobieństw.

6.3.2 Wyznaczenie prawdopodobieństwa transmisji ramki τ

Niech $S(t)$ będzie zmienną losową o wartościach ze zbioru $\{0, 1, 2,\ldots, m\}$ określającą poziom procedury *backoff* dla 802.11 CSMA/CA (por. rozdział 5.2) w chwili t. Niech $B(t)$ będzie zmienną losową o wartościach ze zbioru $\{0, 1, 2,\ldots, W_i - 1\}$ określającą stan licznika *backoff timer* (por. rozdział 5.2) w chwili t. Zmienne losowe $S(t)$ i $B(t)$ nie są niezależne, bowiem maksymalna wartość stanu licznika *backoff timer* zależy od poziomu procedury *backoff*. W_i wynosi (por. [120]):

$$W_i = \begin{cases} 2^i W_0, & dla\ i \le m' \\ 2^{m'} W_0 = W_m, & dla\ i > m' \end{cases} \tag{6-8}$$

gdzie W_0 to wartość początkowa okna niezgody, określona w standardzie (por. rozdziały 5.2, 5.3), a m' oznacza określoną w tym standardzie maksymalną liczbę podwojeń okna W_0. Należy podkreślić, że m' może być mniejsze, równe lub większe od m.

Dla okna niezgody obowiązują następujące zależności (por. rozdziały 5.2, 5.3):

$$W_0 = CW_{\min} + 1, \tag{6-9}$$

$$W_{m'} = CW_{\max} + 1 = 2^{m'} W_0 . \tag{6-10}$$

Dwuwymiarowy proces ($S(t)$, $B(t)$) będzie analizowany poprzez włożony łańcuch Markowa z czasem dyskretnym, w momentach zmiany stanu pracy sieci WLAN (por. rozdział 6.3.1 i Rysunek 6-1). Rozważamy łańcuch w stanie ustalonym – stacjonarnym.

Stan łańcucha będzie oznaczany przez (i,k), a prawdopodobieństwo stanu przez $b_{i,k}$. Prawdopodobieństwo przejść pomiędzy stanami będzie oznaczane przez $P = (\bullet,\bullet\,|\,\bullet,\bullet)$.

Niech p_f oznacza prawdopodobieństwo nieudanej transmisji ramki, a p_{coll} oznacza prawdopodobieństwo kolizji ramki. Niezerowe prawdopodobieństwa przejść pomiędzy stanami rozważanego łańcucha Markowa są związane z p_f , p_{coll}, W_0 i W_i w następujący sposób:

$$\begin{aligned}
&(1)\ P(i,k\,|\,i,k+1) = 1 - p_{coll}, && dla\ 0 \le i \le m,\ 0 \le k \le W_i - 2\\
&(2)\ P(i,k\,|\,i,k) = p_{coll}, && dla\ 0 \le i \le m,\ 1 \le k \le W_i - 1\\
&(3)\ P(0,k\,|\,i,0) = (1 - p_f)/W_0, && dla\ 0 \le i \le m-1,\ 0 \le k \le W_0 - 1\\
&(4)\ P(i,k\,|\,i-1,0) = p_f / W_i, && dla\ 1 \le i \le m,\ 0 \le k \le W_i - 1\\
&(5)\ P(0,k\,|\,m,0) = 1/W_0, && dla\ 0 \le k \le W_0 - 1
\end{aligned} \tag{6-11}$$

Uzasadnienie powyższych związków jest następujące:

Ad (1): Zmiana stanu licznika *backoff timer* z wartości *k+1* na wartość *k* (przy ustalonym poziomie *i* procedury *backoff*), co oznacza, że wykryto pustą szczelinę, a więc że kanał jest wolny. Prawdopodobieństwo tego zdarzenia jest równe *Pr{kanał wolny}=1-Pr{nadaje co najmniej jedna stacja}*. Ponieważ z założenia (por. rozdział 6.1) rozważamy warunki nasycenia, więc zdarzenie „nadaje co najmniej jedna stacja" jest równoważne zdarzeniu zajścia kolizji, a zatem równe p_{coll}.

Ad (2): Brak zmiany stanu licznika *backoff timer* (przy ustalonym poziomie *i* procedury *backoff*) oznacza, że stacja wykryła zajęty kanał. Wobec uzasadnienia związku (1), prawdopodobieństwo tego zdarzenia jest równe p_{coll}.

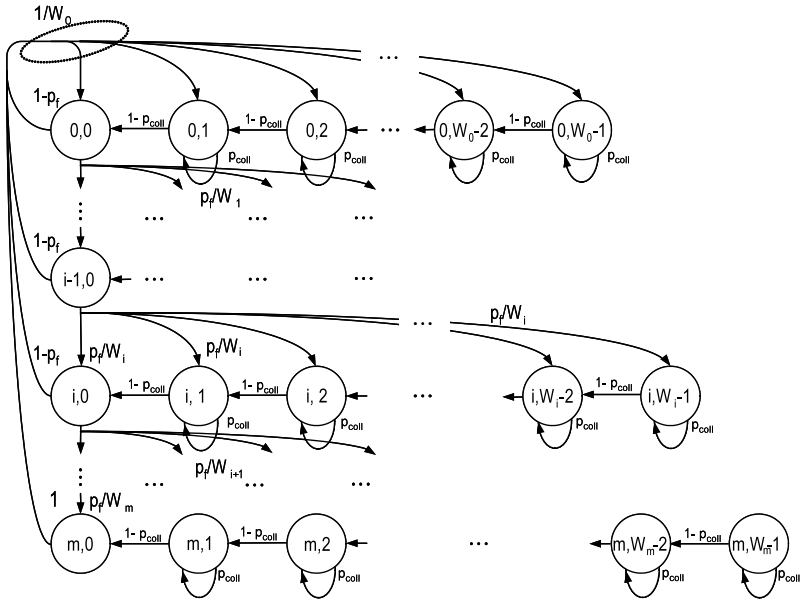
Ad (3): Zmiana stanu licznika *backoff timer* z wartości 0 na wartość *k*, przy jednoczesnej zmianie poziomu procedury *backoff* z *i* na 0, oznacza, że stacja dokonała udanej transmisji, powróciła do początkowego stanu procedury *backoff* i wylosowała liczbę *k* do zainicjowania licznika *backoff timer*. Prawdopodobieństwo tego zdarzenia można wyrazić przez prawdopodobieństwa dwóch niezależnych zdarzeń: *Pr{udana transmisja ramki i wylosowanie liczby k z poziomu 0 procedury backoff} = Pr{udana transmisja ramki}·Pr{wylosowanie liczby k z poziomu 0 procedury backoff}*. Prawdopodobieństwo zdarzenia „udana transmisja ramki" wynosi $1\text{-}p_f$,

a prawdopodobieństwo zdarzenia „wylosowanie liczby *k* z poziomu 0 procedury *backoff*" jest równe $1/W_0$.

Ad (4): Zmiana stanu licznika *backoff timer* z wartości 0 na wartość *k*, przy jednoczesnej zmianie poziomu procedury *backoff* z *i*-1 na *i*, oznacza, że stacja dokonała nieudanej transmisji, zwiększyła poziom procedury *backoff* i wylosowała liczbę *k* do zainicjowania licznika *backoff timer*. Prawdopodobieństwo tego zdarzenia można wyrazić przez prawdopodobieństwa dwóch niezależnych zdarzeń: *Pr{nieudana transmisja ramki i wylosowanie liczby k z poziomu 'i' procedury backoff} = Pr{nieudana transmisja ramki}·Pr{wylosowanie liczby k z poziomu 'i' procedury backoff}*. Prawdopodobieństwo zdarzenia „nieudana transmisja ramki" wynosi p_f, a prawdopodobieństwo zdarzenia „wylosowanie liczby *k* z poziomu *i* procedury *backoff*" jest równe $1/W_i$.

Ad (5): Zmiana stanu licznika *backoff timer* z wartości 0 na wartość *k*, przy jednoczesnej zmianie poziomu procedury *backoff* z maksymalnego poziomu *m* na 0, oznacza, że stacja dokonała transmisji (udanej bądź nie), powróciła do początkowego stanu procedury *backoff* i wylosowała liczbę *k* do zainicjowania licznika *backoff timer*. Wobec uzasadnienia (3) prawdopodobieństwo zdarzenia „wylosowanie liczby *k* z poziomu 0 procedury *backoff*" jest równe $1/W_0$.

Przy powyższych związkach oraz ich uzasadnieniach, graf stanów i przejść w rozważanym łańcuchu Markowa można przedstawić jak na poniższym rysunku (Rysunek 6-2):



Rysunek 6-2 Graf stanów i przejść dla procedury *backoff* w rozważanym łańcuchu Markowa

Zaproponowana analiza uwzględnia: maksymalną liczbę stanów procedury *backoff*, zawieszenie licznika *backoff timer* na czas innych transmisji, a także uwzględnia prawdopodobieństwo uszkodzenia ramki (bez ograniczania się wyłącznie do kolizji).

Zaprezentowana analiza jest ulepszeniem znanych do tej pory modeli literaturowych bazujących na łańcuchach Markowa (por. rozdział 6.2).

Poniżej przedstawiono rozwiązanie zaproponowanego łańcucha Markowa. Dla $i \neq 0$:

$$b_{i,k} = \begin{cases} b_{i-1,0} \cdot \dfrac{p_f}{W_i} + b_{i,1} \cdot (1 - p_{coll}), & dla\ k = 0 \\ \dfrac{b_{i-1,0} \cdot \dfrac{p_f}{W_i} + b_{i,k+1} \cdot (1 - p_{coll})}{1 - p_{coll}}, & dla\ 0 < k < W_i - 1 \\ \dfrac{b_{i-1,0} \cdot \dfrac{p_f}{W_i}}{1 - p_{coll}}, & dla\ k = W_i - 1 \end{cases} \tag{6-12}$$

Natomiast dla $i=0$

$$b_{0,k} = \begin{cases} b_{m,0} \cdot \dfrac{1}{W_0} + \dfrac{1 - p_f}{W_0} \sum_{j=0}^{m-1} b_{j,0} + b_{0,1}(1 - p_{coll}), & dla\ k = 0 \\ \dfrac{b_{m,0} \cdot \dfrac{1}{W_0} + \dfrac{1 - p_f}{W_0} \sum_{j=0}^{m-1} b_{j,0} + b_{0,k+1}(1 - p_{coll})}{1 - p_{coll}}, & dla\ 0 < k < W_i - 1 \\ \dfrac{b_{m,0} \cdot \dfrac{1}{W_0} + \dfrac{1 - p_f}{W_0} \sum_{j=0}^{m-1} b_{j,0}}{1 - p_{coll}}, & dla\ k = W_i - 1 \end{cases} \tag{6-13}$$

Na podstawie (6-12) otrzymujemy:

$$b_{i,0} = p_f \cdot b_{i-1,0}, \tag{6-14}$$

skąd (przez indukcję):

$$b_{i,0} = p_f^{\,i} \cdot b_{0,0}. \tag{6-15}$$

Dla $k \neq 0$:

$$b_{i,k} = \begin{cases} \dfrac{W_i - k}{W_i (1 - p_{coll})} [(1 - p_f) \sum_{j=0}^{m-1} b_{j,0} + b_{m,0}], & dla\ i = 0 \\ \dfrac{W_i - k}{W_i (1 - p_{coll})} p_f b_{i-1,0}, & dla\ 0 < i \leq m \end{cases} \tag{6-16}$$

Dla $p_f < 1$ (przypadek $p_f = 1$ rozważono w rozdziale 6.5.2)

$$\sum_{i=0}^{m} b_{i,0} = b_{0,0} \frac{1 - p_f^{\,m+1}}{1 - p_f}. \tag{6-17}$$

Wobec tego

$$\sum_{i=0}^{m-1} b_{i,0} = b_{0,0} \frac{1 - {p_f}^{m+1}}{1 - p_f} - b_{m,0} . \tag{6-18}$$

Zatem

$$(1 - p_f) \sum_{i=0}^{m-1} b_{i,0} + b_{m,0} = b_{0,0} . \tag{6-19}$$

Ostatecznie dla $0 \le i \le m$

$$b_{i,k} = \begin{cases} \dfrac{W_i - k}{W_i (1 - p_{coll})} {p_f}^i \cdot b_{0,0}, & dla\ 0 < k \le W_i - 1 \\ {p_f}^i \cdot b_{0,0}, & dla\ k = 0 \end{cases} \tag{6-20}$$

Korzystając z warunku normalizacyjnego:

$$\sum_{i=0}^{m} \sum_{k=0}^{W_i - 1} b_{i,k} = 1 \tag{6-21}$$

oraz zależności (6-8), (6-17) i (6-20) otrzymujemy:

$$\begin{aligned} 1 &= \sum_{i=0}^{m} \sum_{k=1}^{W_i - 1} b_{i,k} + \sum_{i=0}^{m} b_{i,0} = \\ &= \frac{b_{0,0}}{1 - p_{coll}} \sum_{i=0}^{m} p_f^i \sum_{k=1}^{W_i - 1} \frac{W_i - k}{W_i} + b_{0,0} \frac{1 - {p_f}^{m+1}}{1 - p_f} = \frac{b_{0,0}}{1 - p_{coll}} \sum_{i=0}^{m} p_f^i \frac{W_i - 1}{2} + b_{0,0} \frac{1 - {p_f}^{m+1}}{1 - p_f} . \end{aligned} \tag{6-22}$$

Po przekształceniach:

$$\begin{aligned} {b_{0,0}}^{-1} &= \frac{1}{1 - p_{coll}} \sum_{i=0}^{m} p_f^i \frac{W_i - 1}{2} + \frac{1 - {p_f}^{m+1}}{1 - p_f} = \\ &= \begin{cases} \dfrac{(1 - p_f) W_0 (1 - (2p_f)^{m+1}) - (1 - 2p_f)(1 - {p_f}^{m+1})}{2(1 - 2p_f)(1 - p_f)(1 - p_{coll})} + \dfrac{1 - {p_f}^{m+1}}{1 - p_f}, & dla\ m \le m' \\ \dfrac{\Psi}{2(1 - 2p_f)(1 - p_f)(1 - p_{coll})} + \dfrac{1 - {p_f}^{m+1}}{1 - p_f}, & dla\ m > m' \end{cases} \end{aligned} \tag{6-23}$$

gdzie

$$\Psi = (1 - p_f) W_0 (1 - (2p_f)^{m'+1}) - (1 - 2p_f)(1 - {p_f}^{m+1}) + W_0 2^{m'} p_f^{m'+1} (1 - 2p_f)(1 - {p_f}^{m-m'}) . \tag{6-24}$$

Na podstawie zależności (6-17) i (6-23) prawdopodobieństwo transmisji ramki τ jest równe prawdopodobieństwu zdarzenia „licznik *backoff timer* jest równy 0” i może zostać wyrażone następująco:

$$\tau = \sum_{i=0}^{m} b_{i,0} =$$

$$= \begin{cases} \left(\dfrac{(1-p_f)W_0(1-(2p_f)^{m+1}) - (1-2p_f)(1-p_f{}^{m+1})}{2(1-2p_f)(1-p_f)(1-p_{coll})} + \dfrac{1-p_f{}^{m+1}}{1-p_f} \right)^{-1} \dfrac{1-p_f{}^{m+1}}{1-p_f}, & dla\ m \le m' \\ \left(\dfrac{\Psi}{2(1-2p_f)(1-p_f)(1-p_{coll})} + \dfrac{1-p_f{}^{m+1}}{1-p_f} \right)^{-1} \dfrac{1-p_f{}^{m+1}}{1-p_f}, & dla\ m > m' \end{cases} \quad (6\text{-}25)$$

Warto zauważyć, że dla $p_{coll} = 0$ otrzymamy to samo rozwiązanie, co w pracy [75], w której nie rozważano zawieszenia licznika *backoff timer* na czas innej transmisji.

6.3.3 Wyznaczenie prawdopodobieństwa nieudanej transmisji ramki p_f i prawdopodobieństwa kolizji ramki p_{coll}

Powyższa analiza doprowadziła do określenia zależności τ od p_f i p_{coll}. Przystąpmy do wyliczenia tych prawdopodobieństw.

Ponieważ rozważamy działanie sieci w warunkach nasycenia, przy każdej próbie transmisji ramka ma stałe prawdopodobieństwo nieudanej transmisji. Nieudana transmisja następuje w przypadku zajścia jednego z dwóch niezależnych zdarzeń: „nastąpiła kolizja ramki" i „ramka została uszkodzona w wyniku błędu w kanale". W związku z tym (podobnie jak w [17] i [75]):

$$p_f = 1 - (1 - p_{coll})(1 - p_e), \quad (6\text{-}26)$$

gdzie p_e oznacza prawdopodobieństwo wystąpienia błędu w ramce z danymi lub ramce ACK. Wobec przyjętego modelu błędów w kanale (por. rozdział 6.1), zdarzenia „wystąpił błąd w ramce z danymi" i „wystąpił błąd w ramce z ACK" są niezależne, a więc:

$$p_e = 1 - (1 - p_{e\_data})(1 - p_{e\_ACK}), \quad (6\text{-}27)$$

gdzie p_{e_data} to prawdopodobieństwo uszkodzenia ramki z danymi, p_{e_ACK} to prawdopodobieństwo uszkodzenia ramki ACK. Prawdopodobieństwa te są funkcjami BER. Wobec przyjętego modelu błędów w kanale (por. rozdział 6.1) można zastosować zależność pozwalającą obliczać prawdopodobieństwo $p_{err}(q,L)$ wystąpienia q błędów w bloku L-elementowym [56]:

$$p_{err}(q, L) = \binom{L}{q} (1 - p_b)^{L-q} p_b{}^q, \quad (6\text{-}28)$$

gdzie p_b jest bitową stopą błędu (BER), a L jest wyrażone w bitach. Interesuje nas sytuacja, w której nie ma żadnych błędów. Wobec tego, że $\sum_{i=0}^{L} p_{err}(i, L) = 1$, prawdopodobieństwo uszkodzenia ramki wynosi:

$$\sum_{i=1}^{L} p_{err}(i,L) = 1 - p_{err}(0,L) = 1 - (1 - p_b)^L . \tag{6-29}$$

Zatem:

$$\mathrm{p}_{\mathrm{e\_data}} = 1 - (1 - p_b)^{L_{data}} , \tag{6-30}$$

$$\mathrm{p}_{\mathrm{e\_ACK}} = 1 - (1 - p_b)^{L_{ACK}} , \tag{6-31}$$

gdzie L_{data} to długość ramki z danymi, a L_{ACK} to długość ramki ACK; obydwie długości są wyrażone w bitach. p_{e_data} i p_{e_ACK} to odpowiednio FER dla ramki z danymi i FER dla ACK (tzw. AER – *ACK Error Rate*). Zatem:

$$p_e = 1 - (1 - p_b)^{L_{data} + L_{ACK}} . \tag{6-32}$$

Prawdopodobieństwo p_b jest zależne od własności fizycznych kanału. Dla niektórych typów kanałów można określić analitycznie p_b z parametrów kanału. Przykładowo dla modulacji QPSK i BPSK (stosowanych w 802.11a/g) p_b można zapisać zależnością ([83], [75]):

$$p_b = Q\left(\sqrt{2\frac{E_b}{N_0}}\right), \tag{6-33}$$

gdzie $\frac{E_b}{N_0}$ jest współczynnikiem bitowej energii do szumu, a

$$Q(x) = \int_x^{\infty} \frac{1}{\sqrt{2\pi}} e^{\frac{-t^2}{2}} dt . \tag{6-34}$$

Natomiast dla modulacji *M*-QAM (w 802.11a/g *M* wynosi 16 albo 64):

$$p_b \approx 4(1 - \frac{1}{\sqrt{M}})Q\left(\sqrt{\frac{3E_b}{(M-1)N_0}}\right). \tag{6-35}$$

Dla modulacji DBPSK (stosowanej w 802.11-1999 DSSS 1 Mbit/s):

$$p_b = \frac{1}{2} e^{-\frac{E_b}{N_0}} . \tag{6-36}$$

Przejdźmy do wyznaczenia p_{coll}. Ponieważ zachowania stacji są wzajemnie niezależne, można założyć, że każda ramka może ulec kolizji ze stałym prawdopodobieństwem. Wobec tego:

$$p_{coll} = 1 - (1 - \tau)^{n-1} . \tag{6-37}$$

Zatem na podstawie równań (6-26) i (6-37) otrzymujemy:

$$p_f = 1 - (1 - p_{coll})(1 - p_e) = 1 - (1 - \tau)^{n-1}(1 - p_e). \quad (6\text{-}38)$$

Równania (6-25) i (6-38) stanowią układ równań nieliniowych z dwiema niewiadomymi τ i p_f, który został rozwiązany za pomocą metod numerycznych w rozdziale 6.6.

6.4 Ocena zaproponowanego modelu NM

Zaproponowany w poprzednim rozdziale model NM, służący do wyznaczania RPN, ocenimy przez porównanie z wynikami symulacji. Dla *BER*=0 wykorzystano symulator *ns-2* (*network simulator*) [106]. Ze względu na to, że symulator *ns-2* nie ma wbudowanego przyjętego w niniejszej rozprawie modelu błędów (por. rozdział 6.1), dla *BER*≠0 wykorzystano wyniki otrzymane przez A. Dudę i in. w pracy [70] za pomocą niedostępnego powszechnie symulatora, opracowanego na *Universitat Politècnica de Catalunya* z Barcelony (Hiszpania). Symulacje z artykułu [70] zostały przeprowadzone przy tych samych założeniach, co przyjęte w tej pracy (por. rozdział 6.1 – Założenia 1-6). Wyniki dla *BER*=0 porównamy także z rezultatami uzyskanymi w innej pracy tych samych autorów [42]. Do obliczeń wykorzystano pakiet *Mathematica 5.2* firmy *Wolfram Research* dla systemu MS Windows – uzyskane dzięki tym obliczeniom wyniki (dla ustalonego modelu analitycznego) są nazywane w dalszej części pracy ***wynikami analitycznymi***.

Do oceny zaproponowanego modelu w *BER*=0 użyto symulatora *ns-2* w wersji 2.29 (dystrybucja *ns-2-snapshot-20050907-14.2*[7], system operacyjny: Linux RedHat). Ponieważ w standardowym *ns-2* nie jest zaimplementowany model OFDM, parametry symulacji przyjęto jak dla IEEE 802.11-1999 DSSS 1 Mbit/s (por. rozdział 5.3).

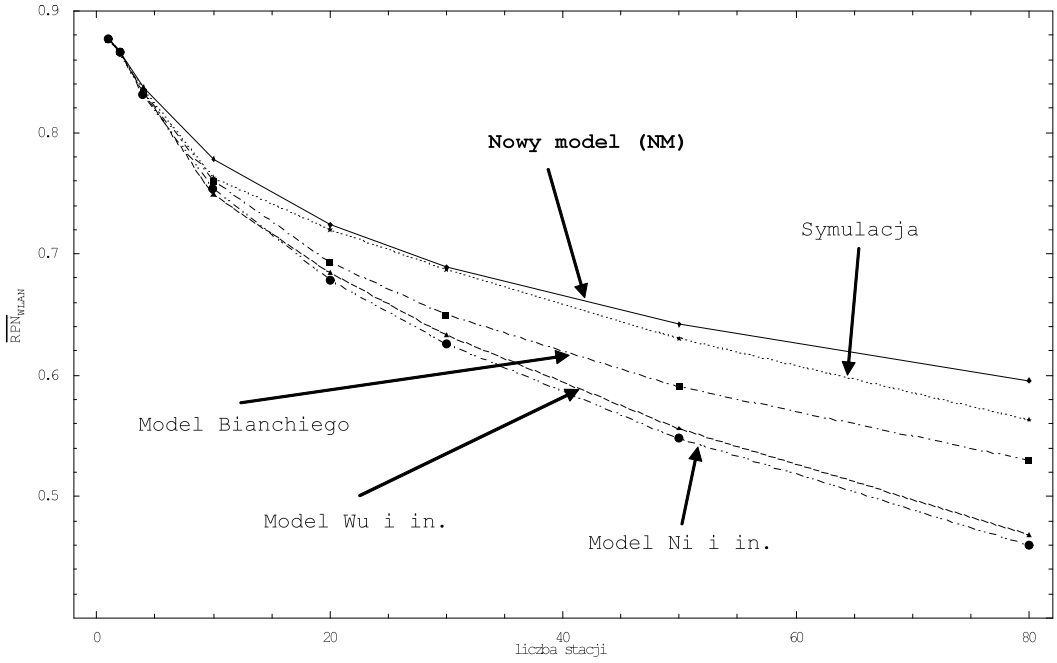
Zgodnie z założeniami przyjętymi w rozdziale 6.1 ramki uczestniczące w kolizji odrzucano, a także wyłączono mechanizm RTS/CTS. Stacje rozmieszczono na obszarze 100 m^2 tak, aby wszystkie były w zasięgu i tak, aby zapewnić na tyle silny sygnał by nie dochodziło do błędów w kanale. Symulowano sieć w warunkach nasycenia. Przebiegi symulacyjne były na tyle długie, aby rozrzut statystyczny wyników symulacji był praktycznie pomijalny. Ruch CBR (*Constant Bit Rate*) generowano w warstwie sieciowej poprzez protokół UDP (*User Datagram Protocol*) tak, aby uzyskać w podwarstwie MAC ramki o długości *L*=1000 bajtów. Zapewniono, aby kolejki stacji były niepuste. Użyto statycznego routingu tworzonego za pomocą wbudowanego w *ns-2* agenta *DumbAgent*.

[7] Dystrybucja ta zawiera także konkurencyjną, ale niestety nieudokumentowaną implementację 802.11, w tym różnych warstw PHY; w niniejszej rozprawie wykorzystano standardową implementację 802.11 z *ns-2*.

Tabela 6-2 zawiera zestawienie wyników symulacji oraz wyników analitycznych RPN dla modeli: Bianchiego [9], Wu i in. [120], Ni i in. [75] (por. rozdział 6.2) i modelu NM (por. rozdział 6.3). Przy *BER*=0, model Wu i in. jest tożsamy z modelem Chatzimisios i in. [17]. Model Wu i in. [120] różni się przy *BER*=0 od modelu Ni i in. [75] brakiem uwzględnienia czasu EIFS po nieudanej transmisji (por. rozdział 6.2). Model Ergena z pracy [29] nie został rozważony ze względu na niepoprawne rozwiązanie łańcucha (por. rozdział 6.2).

Tabela 6-2 Znormalizowane wartości RPN_{WLAN} – wyniki analityczne i wyniki symulacji w *ns-2* – dla *BER*=0 i dla *L*=1000 bajtów

n	Model Bianchiego z pracy [9]	Model Wu in. z pracy [120]	Model Ni in. z pracy [75]	Model NM	Symulacja *ns-2* (średnia)	Odchylenie standardowe dla symulacji *ns-2*
1	0,8769	0,8769	0,8769	**0,8769**	0,8780	0,000
2	0,8666	0,8666	0,8657	**0,8661**	0,8635	0,000
4	0,8329	0,8329	0,8306	**0,8367**	0,8354	0,003
10	0,7602	0,7586	0,7540	**0,7779**	0,7625	0,005
20	0,6929	0,6846	0,6783	**0,7238**	0,7200	0,002
30	0,6497	0,6330	0,6258	**0,6891**	0,6872	0,004
50	0,5904	0,5558	0,5477	**0,6421**	0,6303	0,003
80	0,5297	0,4684	0,4599	**0,5955**	0,5633	0,004



Rysunek 6-3 Znormalizowane wartości RPN_{WLAN} – wyniki analityczne i wyniki symulacji w *ns-2* – dla *BER*=0 i dla *L*=1000 bajtów

Wyniki otrzymane analitycznie dla modelu NM są zbieżne z wynikami otrzymanymi za pomocą symulatora *ns-2* (por. Rysunek 6-3). Wartości RPN_{WLAN} otrzymane analitycznie są nieznacznie wyższe od wyników RPN_{WLAN} uzyskanych w symulacji.

W symulacji zaobserwowano stosunkowo niewielką liczbę ramek wykorzystywanych przez protokół ARP (*Address Resolution Protocol*); nie ma to jednak istotnego wpływu na obniżenie wyników. Dla $n \leq 10$ otrzymane wyniki symulacyjne i analityczne dla wszystkich modeli są zbliżone. Dla $n>10$ można zaobserwować przewagę modelu NM, który uwzględnienia wstrzymanie licznika *backoff timer* na czas transmisji przez inne stacje. Analizując wyniki dla modelu Wu i in. oraz Ni. in. można dostrzec różnicę wynikającą z przyjęcia różnych czasów po niepoprawnej transmisji, odpowiednio DIFS i EIFS. Ponieważ czas DIFS jest krótszy od czasu EIFS, przyjęcie DIFS zamiast EIFS podwyższa RPN_{WLAN}.

Przed omówieniem wyników dla $BER \neq 0$, porównamy wyniki analityczne uzyskane dla modelu NM z wynikami symulacyjnymi dla $BER=0$ zamieszczone w pracy [42]. Wyniki te otrzymano dla metody podstawowej, $L=1500$ bajtów i dla dwóch różnych warstw fizycznych: 802.11b 11 Mbit/s (z długą preambułą)[8] oraz 802.11g 54 Mbit/s ERP-OFDM. Wyniki symulacyjne potwierdziły dobrą jakość modelu NM (por. Tabela 6-3). Zgodnie ze sposobem prezentacji wyników za artykułu [42], zamieszczone w tabeli wyniki RPN_{WLAN} wyrażono w Mbit/s i podzielono przez liczbę stacji n (tzw. niezagregowany RPN_{WLAN}). Wyniki analityczne i symulacyjne pokrywają się dość dobrze, jednak należy wziąć pod uwagę fakt, że prezentacja wartości RPN_{WLAN} w formie niezagregowanej, z dokładnością do dwóch miejsc po przecinku, jest mało precyzyjna dla dużej liczby stacji.

Tabela 6-3 Niezagregowane wartości RPN_{WLAN} – wyniki analityczne i wyniki symulacji z pracy [44] – dla $BER=0$ i dla $L=1500$ bajtów

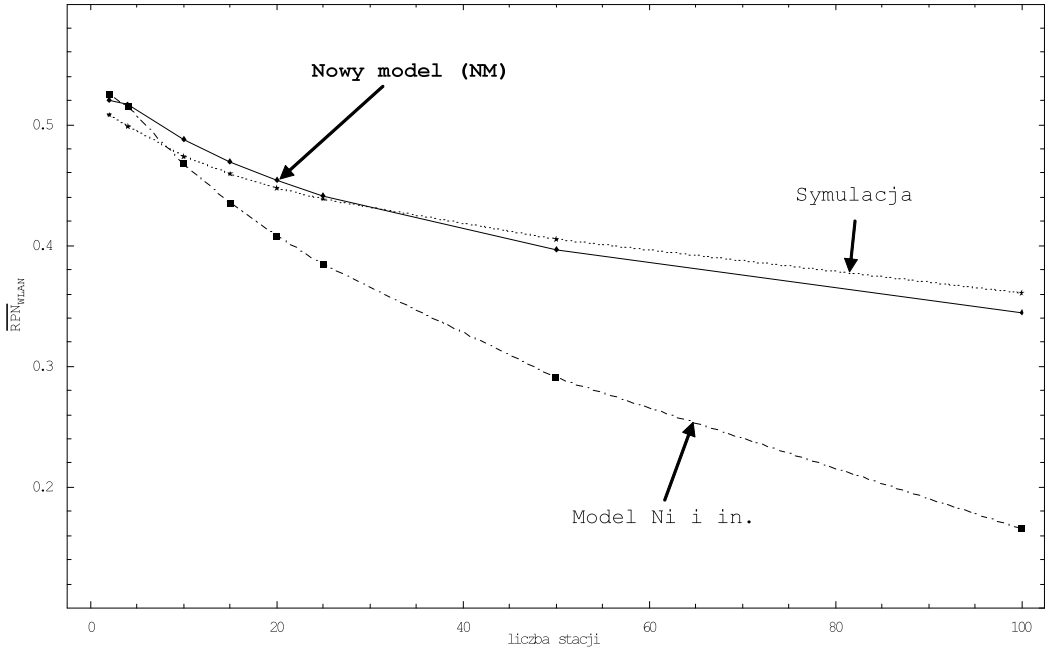
n	Symulacja z pracy [42]	Model NM	Symulacje z pracy [42]	Model NM
	802.11b 11 Mbit/s		802.11g 54 Mbit/s	
1	6,39	**6,34**	31,79	**31,36**
2	3,35	**3,33**	16,18	**16,05**
4	1,67	**1,67**	7,85	**7,86**
10	0,63	**0,63**	2,92	**2,93**
15	0,41	**0,41**	1,87	**1,88**
20	0,29	**0,30**	1,36	**1,36**
25	0,23	**0,23**	1,06	**1,06**
50	0,10	**0,11**	0,49	**0,47**
100	0,05	**0,05**	0,22	**0,21**

Przejdźmy do omówienia wyników dla $BER \neq 0$. Z rozważanych modeli z literatury, tylko w dwóch pracach rozważono błędy w kanale: [75], [17]. Autorzy pracy [17] nie wzięli pod uwagę możliwości uszkodzenia ramki z ACK, a także nie uwzględnili

[8] Parametry jak dla 802.11-1999 DSSS za wyjątkiem $T_{symbol} = 1/1{,}375\ \mu s$ i $N_{BpS} = 8\ bitów$.

czasu EIFS po niepoprawnej transmisji. W dalszej części oceny modelu NM uwzględniono w celach porównawczych jedynie model Ni i in. [75].

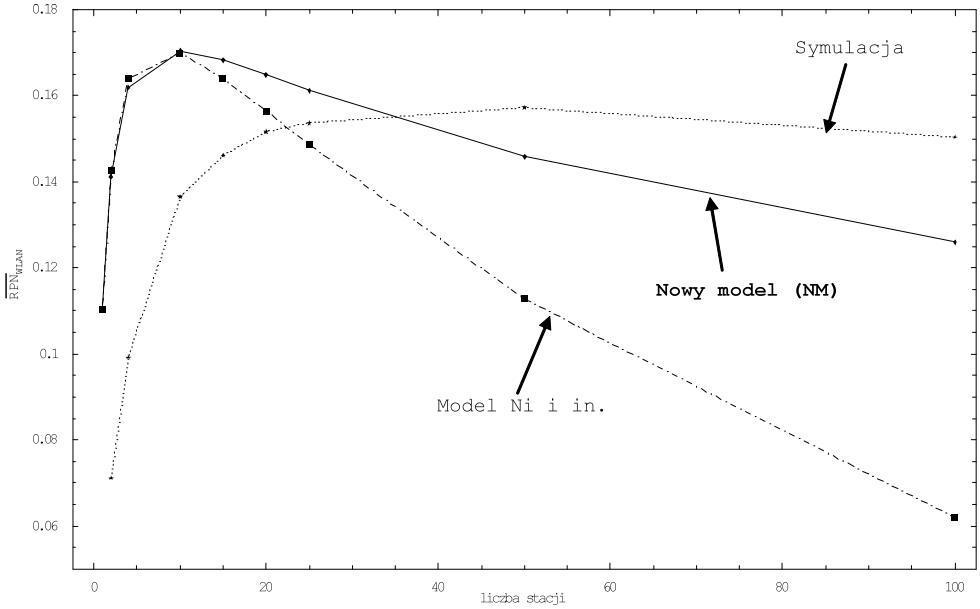
Dla $BER=10^{-5}$ porównano wyniki analityczne dla modelu NM oraz modelu Ni i in. [75] z wynikami symulacji zamieszczonymi w pracy [70]. Wyniki symulacji otrzymano bezpośrednio od autorów pracy. Symulacje przeprowadzono dla metody podstawowej, dla L=1500 bajtów i dla 802.11g 54 Mbit/s ERP-OFDM. Wyniki potwierdziły bardzo dobrą jakość zaproponowanego modelu (Rysunek 6-4). Wyniki analityczne dla modelu Ni i in. [75] wykazały dużą rozbieżność dla $n \geq 15$ zarówno z wynikami symulacji, jak i z wynikami analitycznymi uzyskanymi dla modelu NM.



Rysunek 6-4 Znormalizowane wartości RPN_{WLAN} – wyniki analityczne i wyniki symulacji z pracy [70] – dla $BER=10^{-5}$ i dla L=1500 bajtów

Na zakończenie procesu oceny rozważono $BER=10^{-4}$ dla metody podstawowej, dla L=1500 bajtów i dla 802.11g 54 Mbit/s ERP-OFDM. Wyniki potwierdziły poprawność modelu NM, jednak wykresy RPN_{WLAN}, uzyskane analitycznie i symulacyjnie, przebiegają odmiennie (Rysunek 6-5). Krzywa symulacyjna ma charakter narastający do n=50, natomiast analityczna dla modelu NM ma maksimum dla n=10, a następnie łagodnie opada. Nie zmienia to jednak faktu, że poziom RPN_{WLAN} jest podobny. Wyniki analityczne dla modelu Ni i in. [75] wykazały dużą rozbieżność dla $n \geq 25$ zarówno z wynikami symulacji, jak i z wynikami analitycznymi uzyskanymi dla modelu NM.

Reasumując, zaproponowany w niniejszej rozprawie model NM można uznać za dobre narzędzie analityczne do wyznaczania RPN.

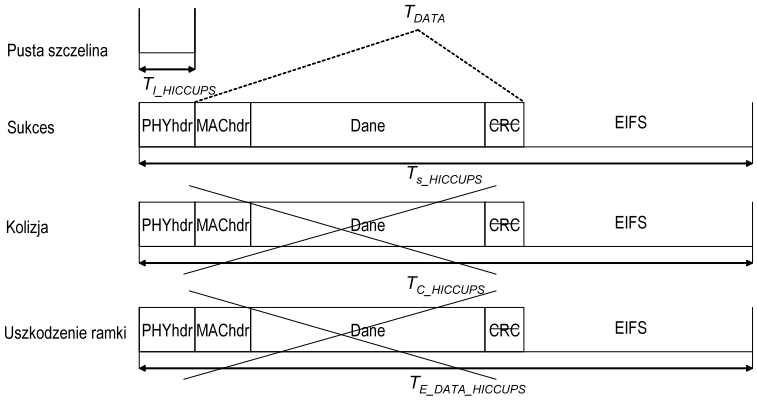


Rysunek 6-5 Znormalizowane wartości RPN_{WLAN} – wyniki analityczne i wyniki symulacji z pracy [70] – dla BER=10^{-4} i dla L=1500 bajtów

6.5 Analiza RPN dla systemu HICCUPS w trybie uszkodzonych ramek – $RPN_{HICCUPS}$

6.5.1 Wyznaczenie RPN

W tym rozdziale dokonamy analizy RPN dla systemu HICCUPS w trybie uszkodzonych ramek ($RPN_{HICCUPS}$). Analiza zostanie przeprowadzona analogicznie, jak w rozdziale 6.3.



Rysunek 6-6 Cztery możliwe stany w kanale w trakcie pracy systemu HICCUPS w trybie uszkodzonych ramek

Rysunek 6-6 przedstawia cztery stany w kanale, które mogą wystąpić w trakcie działania systemu HICCUPS. W związku z tym, że system HICCUPS w trybie uszkodzonych ramek wpisuje nieprawidłową sumę kontrolną CRC-32 w polu FCS (por. rozdział 5.2), nie występują ramki z potwierdzeniami ACK, a zatem nie istnieje

stan „uszkodzenie ACK” (por. Rysunek 6-1). Należy podkreślić, że sukces w transmisji systemu HICCUPS, jest inaczej zdefiniowany niż dla sieci WLAN bez HICCUPS. Transmisja, która zakończyła się sukcesem z punktu widzenia systemu HICCUPS, to transmisja, w której spełnione są dwa warunki: nie doszło do kolizji i nie nastąpiło uszkodzenie ramki w wyniku zakłóceń w kanale. Zgodnie z rozważaniami przeprowadzonymi w rozdziale 4.4 istnieje możliwość weryfikacji integralności steganogramu.

Czasy trwania poszczególnych stanów są oznaczane następująco (Rysunek 6-6):

$T_{I\_HICCUPS}$ – czas trwania pustej szczeliny,

$T_{S\_HICCUPS}$ – czas trwania transmisji zakończonej sukcesem,

$T_{C\_HICCUPS}$ – czas trwania transmisji, podczas której doszło do kolizji,

$T_{E\_DATA\_HICCUPS}$ – czas trwania transmisji, podczas której uszkodzeniu uległa ramka z danymi w wyniku zakłóceń w kanale.

Zatem:

$$\begin{cases} T_{I\_HICCUPS} = \sigma \\ T_{S\_HICCUPS} = T_{PHYhdr} + T_{DATA} + \delta + T_{EIFS} \\ T_{C\_HICCUPS} = T_{S\_HICCUPS} \\ T_{E\_DATA\_HICCUPS} = T_{S\_HICCUPS} \end{cases} \tag{6-39}$$

Wprowadzimy następujące prawdopodobieństwa wystąpienia poszczególnych stanów w kanale:

$P_{I\_HICCUPS}$ – prawdopodobieństwo, że szczelina jest pusta,

$P_{S\_HICCUPS}$ – prawdopodobieństwo, że transmisja zakończyła się sukcesem,

$P_{C\_HICCUPS}$ – prawdopodobieństwo, że podczas transmisji nastąpiła kolizja,

$P_{E\_DATA\_HICCUPS}$ – prawdopodobieństwo, że ramka z danymi uległa uszkodzeniu w wyniku zakłóceń w kanale.

Niech $\tau_{HICCUPS}$ oznacza prawdopodobieństwo transmisji ramki w systemie HICCUPS, a p_{e_data} prawdopodobieństwo uszkodzenia ramki z danymi (zgodne z zależnością (6-30)).

Prawdopodobieństwa poszczególnych stanów w kanale wyrażone przez $\tau_{HICCUPS}$ i p_{e_data} przyjmują postać (por. zależność (6-5)):

$$\begin{cases} P_{I\_HICCUPS} = (1-\tau_{HICCUPS})^n \\ P_{S\_HICCUPS} = n\tau_{HICCUPS}(1-\tau_{HICCUPS})^{n-1}(1-p_{e\_data}) \\ P_{C\_HICCUPS} = 1-(1-\tau_{HICCUPS})^n - n\tau(1-\tau_{HICCUPS})^{n-1} \\ P_{E\_DATA\_HICCUPS} = n\tau_{HICCUPS}(1-\tau_{HICCUPS})^{n-1} p_{e\_data} \end{cases} \quad (6\text{-}40)$$

Zgodnie z założeniami (por. rozdział 6.1), rozpatrujemy wyłącznie ramki z danymi o stałej długości, a więc ostatecznie $RPN_{HICCUPS}$ możemy określić zależnością (analogicznie do (6-6)):

$$RPN_{HICCUPS} = \frac{P_{S\_HICCUPS} L_{pld\_HICCUPS}}{T_{I\_HICCUPS} P_{I\_HICCUPS} + T_{S\_HICCUPS} P_{S\_HICCUPS} + T_{C\_HICCUPS} P_{C\_HICCUPS} + T_{E\_DATA\_HICCUPS} P_{E\_DATA\_HICCUPS}}, \quad (6\text{-}41)$$

gdzie $L_{pld\_HICCUPS}$ to długość danych w ramce MAC wraz z polem FCS, z pominięciem danych generowanych przez wewnętrzny mechanizm integralności systemu HICCUPS (por. rozdział 4.4). W dalszej części przyjmiemy, że wspomniany mechanizm integralności wykorzystuje tyle samo bitów, co mechanizm CRC-32 w WLAN, zatem $L_{pld\_HICCUPS} = L_{pld}$.

$RPN_{HICCUPS}$ jest wyrażone w bit/s. Miarę tę można znormalizować do szybkości transmisji danych R (por. zależności (6-7) i (5-3)):

$$\overline{RPN}_{HICCUPS} = \frac{RPN_{HICCUPS}}{R}. \quad (6\text{-}42)$$

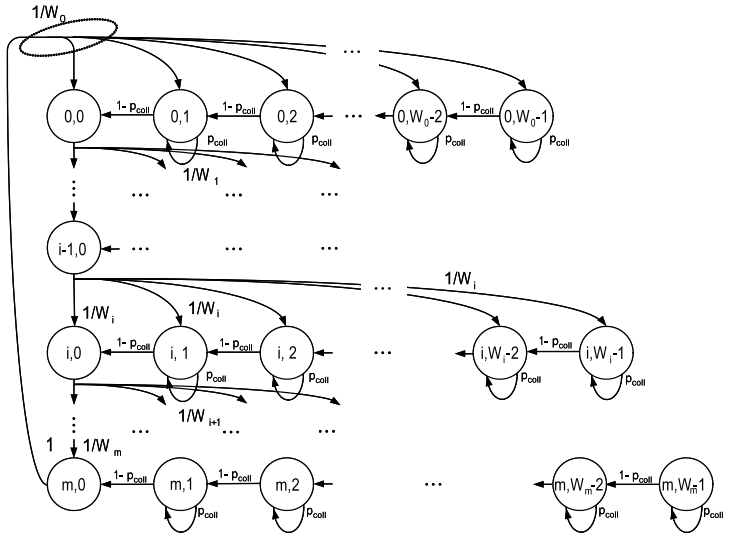
6.5.2 Wyznaczenie prawdopodobieństwa transmisji $\tau_{HICCUPS}$

Bazując na modelu wprowadzonym w rozdziale 6.3 rozważymy model procedury *backoff* uwzględniający funkcjonowanie systemu HICCUPS w trybie uszkodzonych ramek. Z punktu widzenia logiki działania sieci WLAN komunikacja w ukrytej grupie (por. rozdział 4.3) za pomocą ramek z celowo uszkodzonymi sumami kontrolnymi jest transmisją, która nie kończy się sukcesem. Stąd też (por. rozdział 5.2), w systemie HICCUPS transmisja steganogramów jest dokonywana w kolejnych poziomach procedury *backoff*. W związku z tym możemy analizować zachowanie systemu HICCUPS za pomocą łańcucha Markowa (jak w rozdziale 6.3) przy $p_f = 1$ (zależność (6-11)).

Niezerowe prawdopodobieństwa przejść pomiędzy stanami rozważanego łańcucha Markowa są związane z p_{coll}, W_0 i W_i w następujący sposób:

$$\begin{cases} P(i,k \mid i,k+1) = 1-p_{coll}, & dla\ 0 \le i \le m, 0 \le k \le W_i - 2 \\ P(i,k \mid i,k) = p_{coll}, & dla\ 0 \le i \le m, 1 \le k \le W_i - 1 \\ P(i,k \mid i-1,0) = 1/W_i, & dla\ 0 \le i \le m, 0 \le k \le W_i - 1 \\ P(0,k \mid m,0) = 1/W_0, & dla\ 0 \le k \le W_0 - 1 \end{cases} \quad (6\text{-}43)$$

Przy powyższych związkach oraz uzasadnieniach jak w rozdziale 6.3, graf stanów i przejść w rozważanym łańcuchu Markowa przedstawia Rysunek 6-7. Zwróćmy uwagę, że dostosowany do systemu HICCUPS graf stanów i przejść różni się, od grafu przedstawionego w rozdziale 6.3, brakiem powrotu do stanów $(0,k)$ dla $0 \le k \le W_0-1$ ze stanów $(i,0)$ dla $0 \le i \le m-1$, co odpowiada sytuacji, w której transmitowane ramki są uszkodzone z punktu widzenia logiki działania WLAN.



Rysunek 6-7 Graf stanów i przejść dla procedury *backoff* w rozważanym łańcuchu Markowa dla systemu HICCUPS w trybie uszkodzonych ramek

Rozwiązanie łańcucha dla $0 \le i \le m$ jest następujące:

$$b_{i,k} = \begin{cases} \dfrac{W_i - k}{W_i(1-p_{coll})} b_{0,0}, & dla\ 0 < k \le W_i - 1 \\ b_{0,0}, & dla\ k = 0 \end{cases} \tag{6-44}$$

Skoro

$$\sum_{i=0}^{m} b_{i,0} = b_{0,0}(m+1) \tag{6-45}$$

to z warunku normalizacyjnego i (6-45) otrzymujemy:

$$1 = \sum_{i=0}^{m} \sum_{k=1}^{W_i-1} b_{i,k} + \sum_{i=0}^{m} b_{i,0} = \frac{b_{0,0}}{1-p_{coll}} \sum_{i=0}^{m} \frac{W_i - 1}{2} + b_{0,0}(m+1)\,. \tag{6-46}$$

Stąd:

$$b_{0,0}^{-1} = \begin{cases} \dfrac{W_0(2^{m+1}-1)-(m+1)}{2(1-p_{coll})} + (m+1), & dla\ m \le m' \\ \dfrac{W_0(2^{m'+1}-1)-(m+1)+(m-m')W_0 2^{m'}}{2(1-p_{coll})} + (m+1), & dla\ m > m' \end{cases} \tag{6-47}$$

Mając $b_{0,0}$ możemy wyznaczyć (analogicznie jak w (6-25)) prawdopodobieństwo transmisji ramki $\tau_{HICCUPS}$:

$$\tau_{HICCUPS} = \sum_{i=0}^{m} b_{i,0} =$$

$$= \begin{cases} \left(\dfrac{W_0(2^{m+1}-1)-(m+1)}{2(1-p_{coll})} + (m+1) \right)^{-1} (m+1), & dla\ m \le m' \\ \left(\dfrac{W_0(2^{m'+1}-1)-(m+1)+(m-m')W_0 2^{m'}}{2(1-p_{coll})} + (m+1) \right)^{-1} (m+1), & dla\ m > m' \end{cases} \tag{6-48}$$

Prawdopodobieństwo p_{coll}, analogicznie do (6-37), wynosi:

$$p_{coll} = 1 - (1 - \tau_{HICCUPS})^{n-1}. \tag{6-49}$$

Zależności (6-48) i (6-49) stanowią układ równań z dwiema niewiadomymi $\tau_{HICCUPS}$ i p_{coll}, który został rozwiązany za pomocą metod numerycznych w rozdziale 6.6.

6.6 Analiza wyników RPN

Do obliczeń wykorzystano pakiet *Mathematica 5.2* firmy *Wolfram Research* dla systemu MS Windows. Zgodnie z założeniami (por. rozdział 6.1) przyjęto parametry jak dla IEEE 802.11g 56 Mbit/s ERP-OFDM:

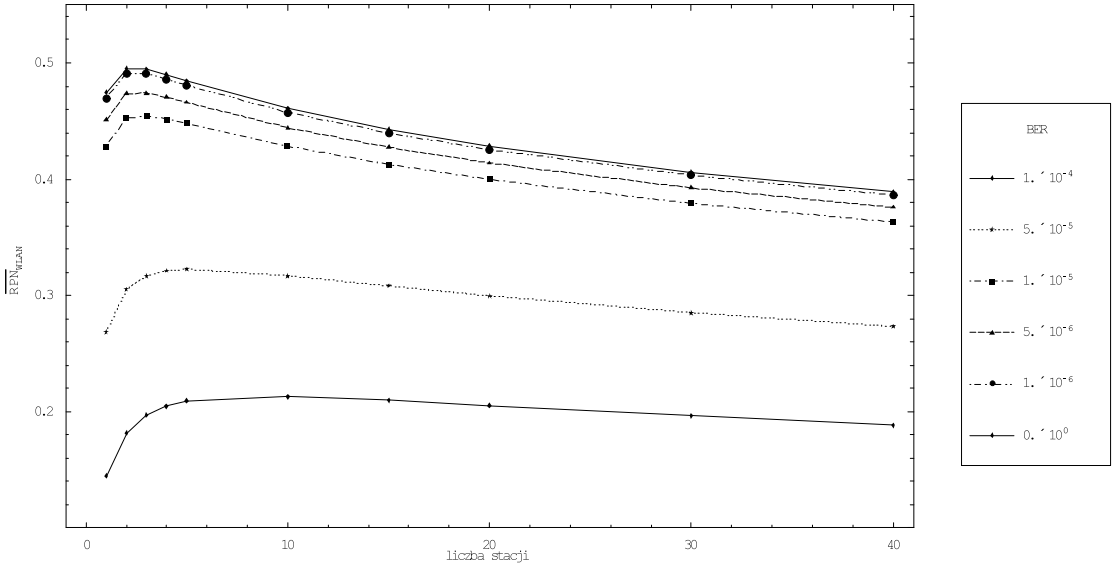
- m=4,
- m'=6,
- R=54 Mbit/s,
- N_{BpS}=24 bity,
- W_0=16,
- σ=9 μs,
- T_{SIFS}=10 μs,
- T_{DIFS}=28 μs,
- T_{symbol}=4 μs,
- T_{PHYhdr}=20 μs,
- L_{ack}=112 bitów,
- L_{MAChdr}=224 bity,
- L_{SER}=16 bitów,
- L_{TAIL}=6 bitów.

Założono stałe opóźnienie propagacji δ=1 μs dla wszystkich stacji.

6.6.1 Zależność RPN od liczby stacji

Na wykresach przedstawiono znormalizowane wartości RPN w funkcji n (zgodnie z wzorami (6-7) dla WLAN i (6-42) dla HICCUPS). Wszystkie obliczenia wykonano dla $n \in \{1, 2, 3, 4, 5, 10, 15, 20, 30, 40\}$. Obliczenia dla ramki o długości L=1000 bajtów wykonano dla $BER \in \{10^{-4}, 5\cdot10^{-5}, 10^{-5}, 5\cdot10^{-6}, 10^{-6}, 0\}$. Obliczenia dla $L \in \{100, 250, 500, 1000, 1500, 2000\}$ bajtów wykonano dla $BER \in \{0, 10^{-5}, 10^{-4}\}$.

Rysunek 6-8 przedstawia znormalizowane wartości RPN_{WLAN} w funkcji n, dla stałej długości ramki L=1000 bajtów oraz dla różnych wartości *BER* (Tabela 6-4). Wraz ze wzrostem wartości *BER* maleje RPN, przesuwa się także maksimum z n=2 (dla dwóch najmniejszych *BER* 0 i 10^{-6}), przez n=3 dla *BER* $5{\cdot}10^{-6}$ i 10^{-5}, n=5 dla $5{\cdot}10^{-5}$, aż do n=10 dla $BER=10^{-4}$. Wraz ze wzrostem *BER* przedstawione krzywe są coraz bardziej płaskie. Spadek wartości RPN_{WLAN} przy ustalonej wartości *BER* wraz ze wzrostem liczby stacji ma związek ze zwiększaniem się liczby kolizji w medium. Zmniejszenie RPN_{WLAN} pomiędzy BER=0 a $BER=10^{-6}$ jest niewielkie.

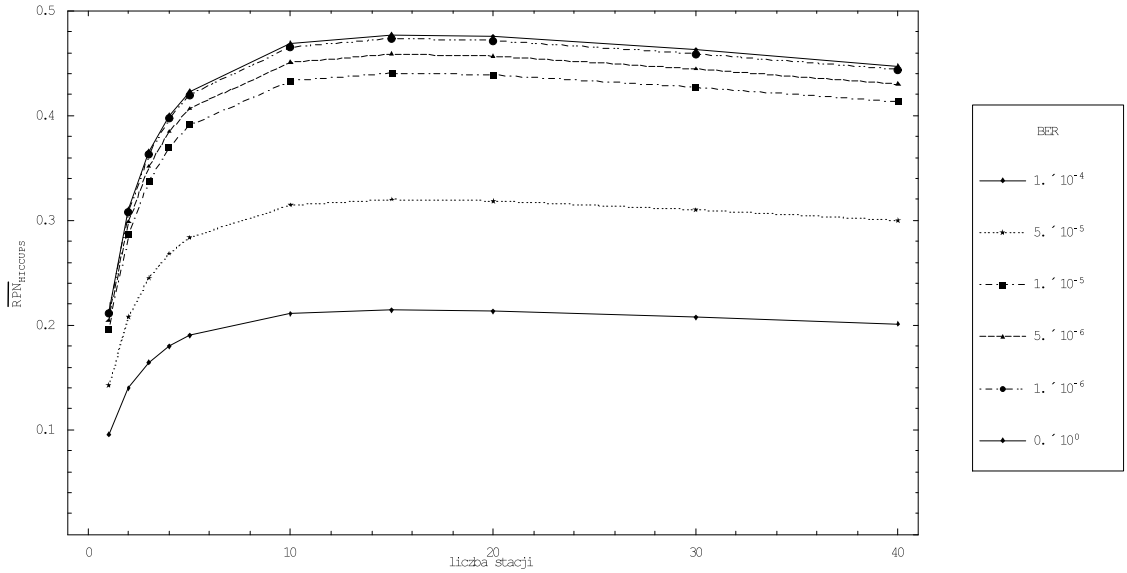


Rysunek 6-8 Znormalizowane wartości RPN_{WLAN} w funkcji n – dla L=1000 bajtów i dla różnych *BER*

Tabela 6-4 Znormalizowane wartości RPN_{WLAN} w funkcji n – dla L=1000 bajtów i dla różnych *BER*

BER / ***n***	**10^{-4}**	**$5{\cdot}10^{-5}$**	**10^{-5}**	**$5{\cdot}10^{-6}$**	**10^{-6}**	**0**
1	0,1446	0,2688	0,4281	0,4510	0,4697	0,4745
2	0,1816	0,3054	0,4521	0,4734	0,4909	0,4953
3	0,1971	0,3170	0,4542	0,4740	0,4904	0,4945
4	0,2050	0,3213	0,4517	0,4705	0,4860	0,4899
5	0,2092	0,3226	0,4479	0,4660	0,4808	0,4845
10	0,2131	0,3171	0,4285	0,4443	0,4574	0,4607
15	0,2097	0,3082	0,4126	0,4275	0,4396	0,4427
20	0,2052	0,2998	0,3997	0,4138	0,4254	0,4284
30	0,1963	0,2853	0,3792	0,3925	0,4034	0,4061
40	0,1885	0,2735	0,3631	0,3758	0,3863	0,3889

Rysunek 6-9 przedstawia znormalizowane wartości $RPN_{HICCUPS}$ w funkcji n dla stałej długości ramki L=1000 bajtów oraz dla różnych wartości BER (por. Tabela 6-5). Podobnie jak RPN_{WLAN} (por. Rysunek 6-8), $RPN_{HICCUPS}$ maleje wraz ze wzrostem BER. Maksimum (n=16) jest niezależne od BER, gdyż błędy w kanale nie wpływają na procedurę *backoff*. Po osiągnięciu maksimum krzywe są płaskie. Niewielki spadek wartości $RPN_{HICCUPS}$ przy ustalonej wartości BER wraz ze wzrostem liczby stacji ma związek ze zwiększaniem się liczby kolizji w medium. Zmniejszenie $RPN_{HICCUPS}$ pomiędzy BER=0 a BER=10^{-6} jest niewielkie.

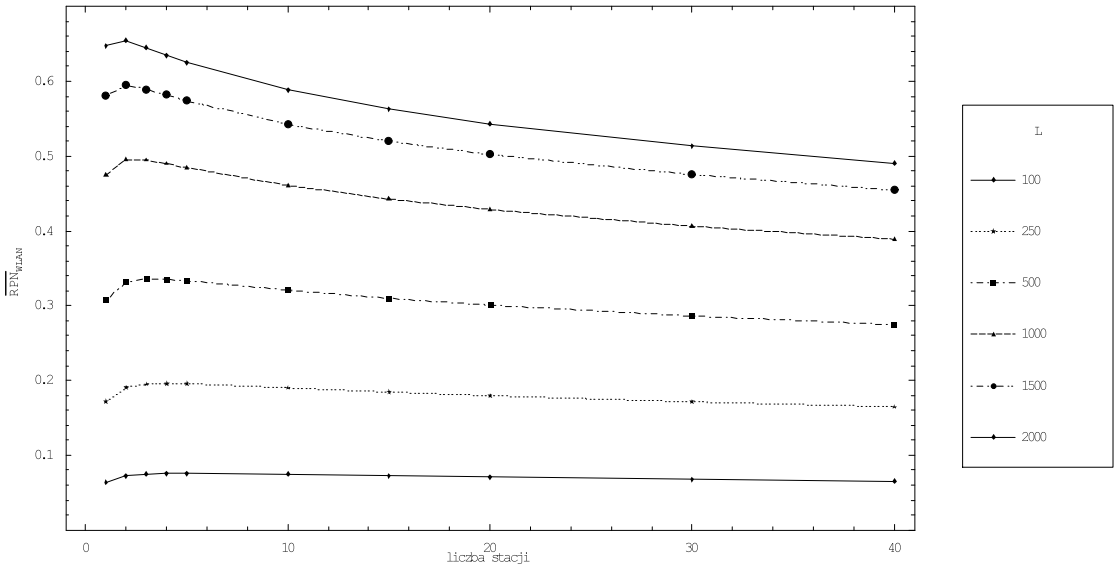


Rysunek 6-9 Znormalizowane wartości $RPN_{HICCUPS}$ w funkcji n – dla L=1000 bajtów i dla różnych BER

Tabela 6-5 Znormalizowane wartości $RPN_{HICCUPS}$ w funkcji n – dla L=1000 bajtów i dla różnych BER

BER / ***n***	**10^{-4}**	**$5\cdot10^{-5}$**	**10^{-5}**	**$5\cdot10^{-6}$**	**10^{-6}**	**0**
1	0,0954	0,1424	0,1961	0,2041	0,2107	0,2124
2	0,1395	0,2082	0,2867	0,2984	0,3081	0,3105
3	0,1643	0,2451	0,3376	0,3513	0,3628	0,3657
4	0,1798	0,2682	0,3694	0,3845	0,3970	0,4001
5	0,1901	0,2836	0,3906	0,4065	0,4197	0,4231
10	0,2107	0,3144	0,4330	0,4506	0,4653	0,4690
15	0,2144	0,3199	0,4405	0,4585	0,4734	0,4772
16	0,2145	0,3199	0,4406	0,4586	0,4735	0,4773
20	0,2135	0,3185	0,4386	0,4565	0,4714	0,4752
30	0,2078	0,3099	0,4268	0,4443	0,4587	0,4624
40	0,2010	0,2998	0,4129	0,4297	0,4437	0,4473

Rysunek 6-10 przedstawia znormalizowane wartości RPN_{WLAN} w funkcji n dla różnych długości ramki oraz dla BER=0 (por. Tabela 6-6). Dla ustalonego n, wraz ze wzrostem długości ramki rośnie wartość RPN_{WLAN}. W zależności od liczby stacji maksimum przypada w przedziale [2;5].

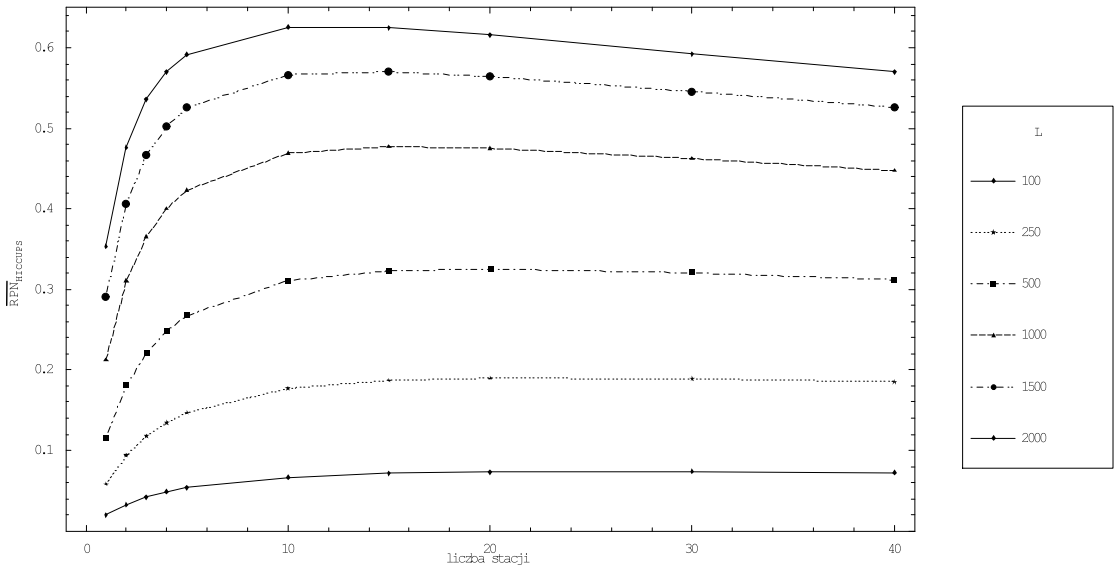


Rysunek 6-10 Znormalizowane wartości RPN_{WLAN} w funkcji n – dla różnych L i dla BER=0

Tabela 6-6 Znormalizowane wartości RPN_{WLAN} w funkcji n – dla różnych L i dla BER=0

L / *n*	100	250	500	1000	1500	2000
1	0,0637	0,1717	0,3074	0,4745	0,5808	0,6471
2	0,0723	0,1904	0,3319	0,4953	0,5949	0,6541
3	0,0748	0,1949	0,3360	0,4945	0,5896	0,6450
4	0,0756	0,1958	0,3354	0,4899	0,5817	0,6346
5	0,0758	0,1954	0,3334	0,4845	0,5738	0,6249
10	0,0744	0,1899	0,3208	0,4607	0,5422	0,5880
15	0,0725	0,1842	0,3098	0,4427	0,5197	0,5626
20	0,0708	0,1793	0,3008	0,4284	0,5021	0,5430
30	0,0678	0,1712	0,2862	0,4061	0,4751	0,5132
40	0,0653	0,1646	0,2747	0,3889	0,4544	0,4905

Rysunek 6-11 przedstawia znormalizowane wartości $RPN_{HICCUPS}$ w funkcji n dla różnych długości ramki oraz dla BER=0 (por. Tabela 6-7). Analogicznie jak dla RPN_{WLAN} (por. Rysunek 6-10), dla ustalonego n, wraz ze wzrostem długości ramki rośnie $RPN_{HICCUPS}$. W zależności od n maksimum przypada w przedziale [10;30].

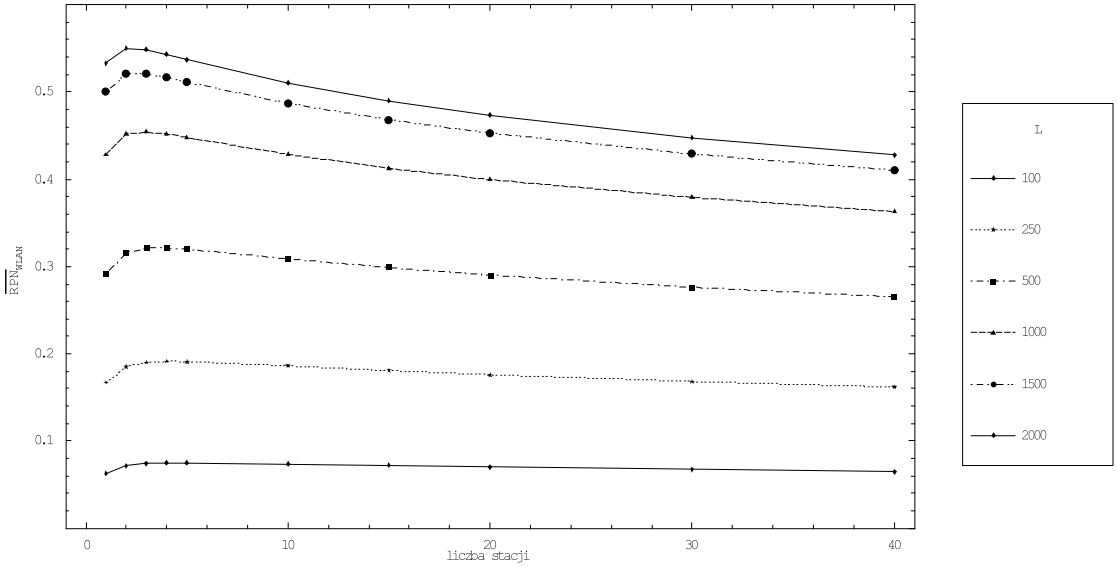


Rysunek 6-11 Znormalizowane wartości $RPN_{HICCUPS}$ w funkcji n – dla różnych L i dla BER=0

Tabela 6-7 Znormalizowane wartości $RPN_{HICCUPS}$ w funkcji n – dla różnych L i dla BER=0

L / *n*	100	250	500	1000	1500	2000
1	0,0197	0,0581	0,1162	0,2124	0,2908	0,3537
2	0,0327	0,0938	0,1807	0,3105	0,4065	0,4764
3	0,0418	0,1176	0,2211	0,3657	0,4668	0,5363
4	0,0485	0,1345	0,2483	0,4001	0,5025	0,5704
5	0,0536	0,1468	0,2675	0,4231	0,5253	0,5913
10	0,0667	0,1770	0,3111	0,4690	0,5665	0,6253
15	0,0715	0,1868	0,3230	0,4772	0,5701	0,6245
20	0,0734	0,1899	0,3253	0,4752	0,5642	0,6155
30	0,0738	0,1890	0,3205	0,4624	0,5455	0,5926
40	0,0727	0,1851	0,3121	0,4473	0,5259	0,5700

Rysunek 6-12 przedstawia znormalizowane wartości RPN_{WLAN} w funkcji n dla różnych długości ramki oraz dla $BER=10^{-5}$ (por. Tabela 6-8). Dla ustalonego n, wraz ze wzrostem długości ramki rośnie RPN_{WLAN}. W zależności od n, maksimum przypada w przedziale [2;5]. Ze względu na pojawienie się błędów w kanale osiągane wartości RPN_{WLAN} są mniejsze niż dla $BER=0$.

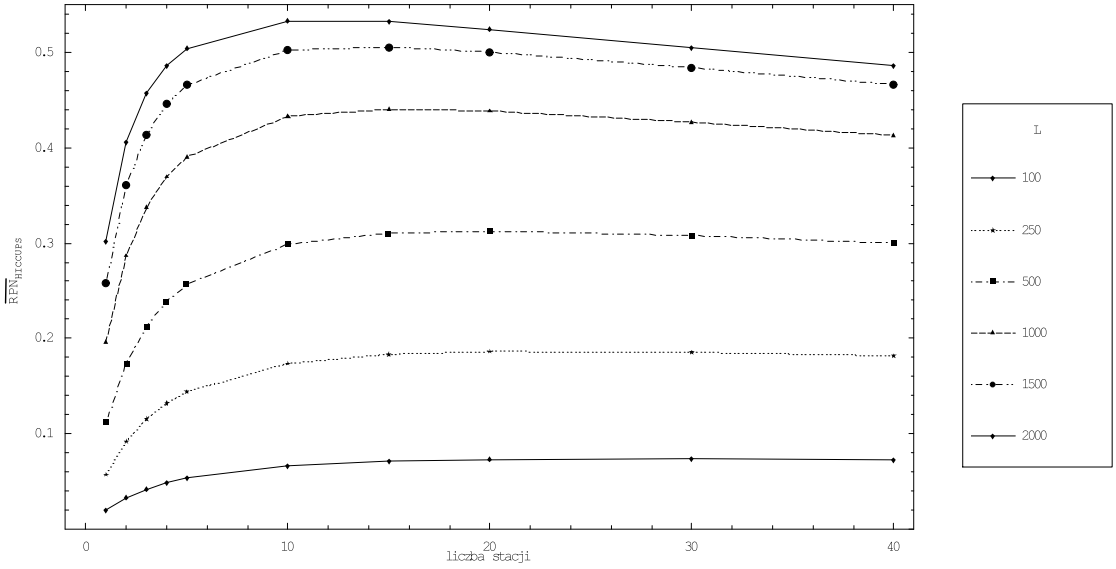


Rysunek 6-12 Znormalizowane wartości RPN_{WLAN} w funkcji n – dla różnych L i dla $BER=10^{-5}$

Tabela 6-8 Znormalizowane wartości RPN_{WLAN} w funkcji n – dla różnych L i dla $BER=10^{-5}$

L / *n*	100	250	500	1000	1500	2000
1	0,0629	0,1668	0,2909	0,4281	0,5004	0,5330
2	0,0715	0,1855	0,3162	0,4521	0,5211	0,5502
3	0,0740	0,1902	0,3212	0,4542	0,5208	0,5484
4	0,0749	0,1914	0,3213	0,4517	0,5166	0,5431
5	0,0751	0,1912	0,3199	0,4479	0,5114	0,5372
10	0,0738	0,1862	0,3089	0,4285	0,4872	0,5105
15	0,0719	0,1808	0,2988	0,4126	0,4682	0,4900
20	0,0702	0,1760	0,2902	0,3997	0,4529	0,4736
30	0,0673	0,1681	0,2763	0,3792	0,4289	0,4480
40	0,0648	0,1617	0,2652	0,3631	0,4103	0,4281

Rysunek 6-13 przedstawia znormalizowane wartości $RPN_{HICCUPS}$ w funkcji n dla różnych długości ramki oraz dla $BER=10^{-5}$ (por. Tabela 6-9). Dla ustalonego n, wraz ze wzrostem długości ramki rośnie $RPN_{HICCUPS}$. W zależności od n maksimum przypada w przedziale [10;30]. Ze względu na pojawienie się błędów w kanale osiągane wartości $RPN_{HICCUPS}$ są mniejsze niż dla $BER=0$.

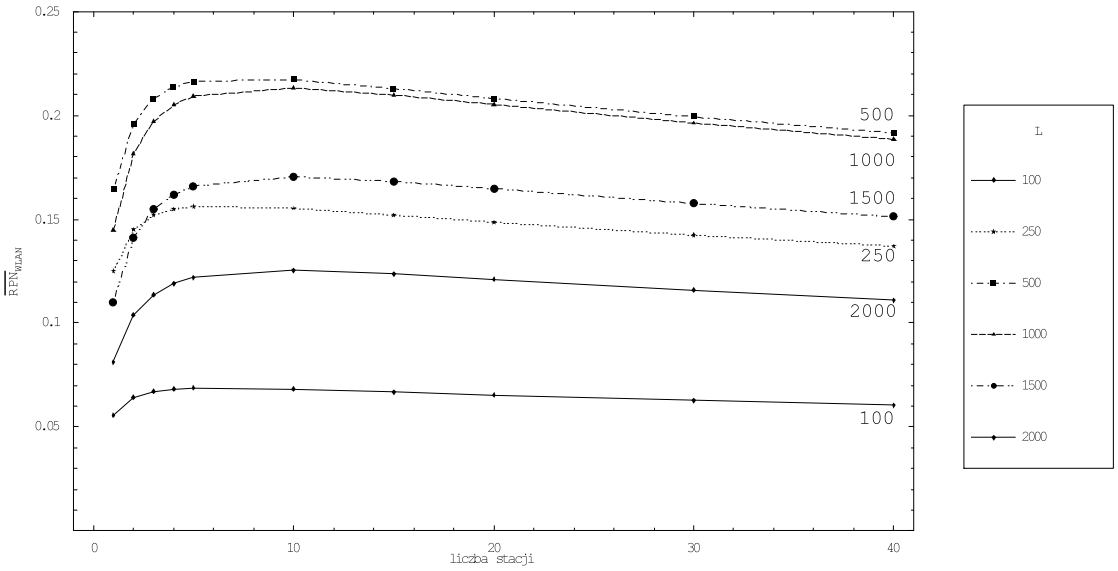


Rysunek 6-13 Znormalizowane wartości $RPN_{HICCUPS}$ w funkcji n – dla różnych L i dla $BER=10^{-5}$

Tabela 6-9 Znormalizowane wartości $RPN_{HICCUPS}$ w funkcji n – dla różnych L i dla $BER=10^{-5}$

L / *n*	100	250	500	1000	1500	2000
1	0,0195	0,0570	0,1116	0,1961	0,2579	0,3014
2	0,0324	0,0919	0,1736	0,2867	0,3606	0,4060
3	0,0415	0,1153	0,2124	0,3376	0,4140	0,4570
4	0,0481	0,1318	0,2385	0,3694	0,4457	0,4860
5	0,0531	0,1439	0,2570	0,3906	0,4659	0,5039
10	0,0662	0,1735	0,2989	0,4330	0,5024	0,5329
15	0,0710	0,1831	0,3104	0,4405	0,5056	0,5321
20	0,0728	0,1861	0,3126	0,4386	0,5004	0,5245
30	0,0732	0,1853	0,3079	0,4268	0,4838	0,5050
40	0,0721	0,1814	0,2999	0,4129	0,4664	0,4857

Rysunek 6-14 przedstawia znormalizowane wartości RPN_{WLAN} w funkcji n dla różnych długości ramki oraz dla $BER=10^{-4}$ (por. Tabela 6-10). Dla ustalonego n, wartości RPN_{WLAN} rosną wraz z długością ramki tylko do określonego poziomu; dla ramek dłuższych niż 500 bajtów i dla $n \geq 3$ wartość RPN_{WLAN} spada. Wpływ na to ma wzrost wartości FER wraz z długością ramki (por. zależność (6-30)).

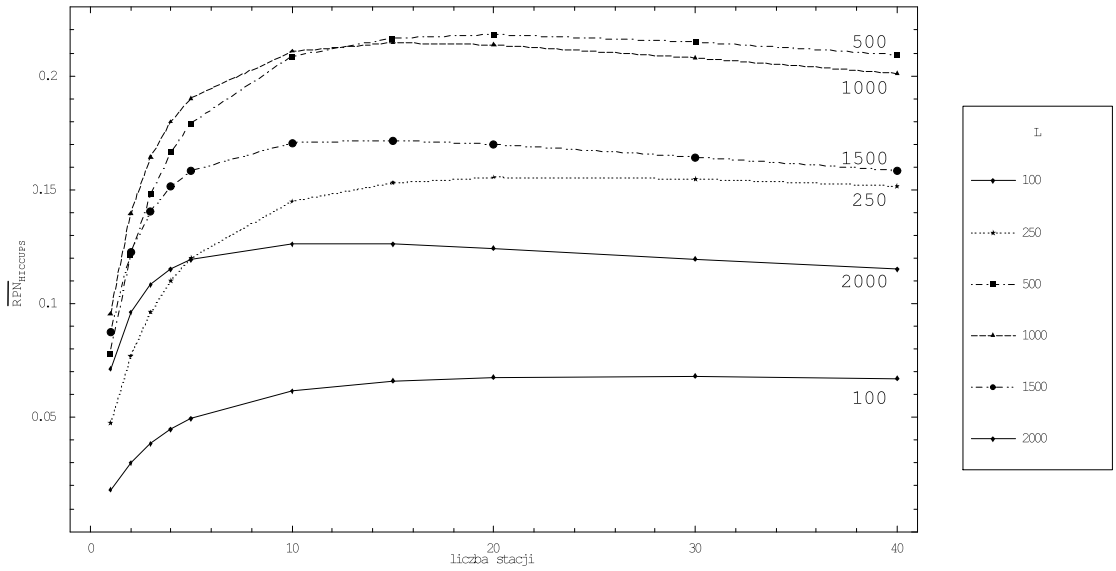


Rysunek 6-14 Znormalizowane wartości RPN_{WLAN} w funkcji n – dla różnych L i dla $BER=10^{-4}$

Tabela 6-10 Znormalizowane wartości RPN_{WLAN} w funkcji n – dla różnych L i dla $BER=10^{-4}$

L / *n*	100	250	500	1000	1500	2000
1	0,0556	0,1251	0,1643	0,1446	0,1103	0,0812
2	0,0643	0,1450	0,1960	0,1816	0,1412	0,1038
3	0,0671	0,1519	0,2081	0,1971	0,1548	0,1137
4	0,0682	0,1549	0,2137	0,2050	0,1619	0,1190
5	0,0687	0,1561	0,2165	0,2092	0,1659	0,1219
10	0,0682	0,1553	0,2172	0,2131	0,1705	0,1254
15	0,0667	0,1520	0,2129	0,2097	0,1682	0,1237
20	0,0652	0,1485	0,2081	0,2052	0,1647	0,1212
30	0,0626	0,1423	0,1992	0,1963	0,1576	0,1159
40	0,0604	0,1370	0,1916	0,1885	0,1512	0,1111

Rysunek 6-15 przedstawia znormalizowane wartości $RPN_{HICCUPS}$ w funkcji n dla różnych długości ramki oraz dla $BER=10^{-4}$ (por. Tabela 6-11). Podobnie jak dla RPN_{WLAN} (por. Rysunek 6-14) dla ustalonego n, wartości $RPN_{HICCUPS}$ rosną wraz z długością ramki tylko do określonego poziomu; dla ramek dłuższych niż 500 bajtów i dla $n \geq 15$ wartość $RPN_{HICCUPS}$ spada. Wpływ na to ma wzrost wartości FER wraz z długością ramki (zależność (6-30)).

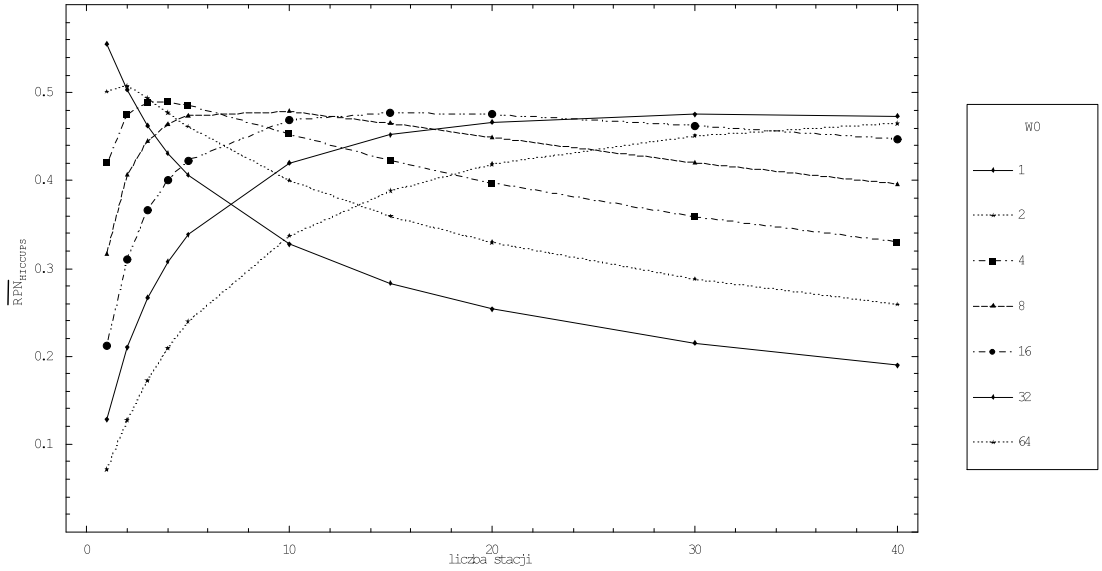


Rysunek 6-15 Znormalizowane wartości $RPN_{HICCUPS}$ w funkcji n – dla różnych L i dla $BER=10^{-4}$

Tabela 6-11 Znormalizowane wartości $RPN_{HICCUPS}$ w funkcji n – dla różnych L i dla $BER=10^{-4}$

L / *n*	100	250	500	1000	1500	2000
1	0,0182	0,0476	0,0779	0,0954	0,0876	0,0714
2	0,0302	0,0768	0,1211	0,1395	0,1224	0,0962
3	0,0386	0,0963	0,1482	0,1643	0,1406	0,1083
4	0,0448	0,1101	0,1664	0,1798	0,1513	0,1151
5	0,0495	0,1202	0,1793	0,1901	0,1582	0,1194
10	0,0616	0,1449	0,2085	0,2107	0,1706	0,1262
15	0,0660	0,1529	0,2165	0,2144	0,1717	0,1261
20	0,0677	0,1555	0,2181	0,2135	0,1699	0,1243
30	0,0681	0,1547	0,2148	0,2078	0,1643	0,1196
40	0,0671	0,1515	0,2092	0,2010	0,1584	0,1151

Rysunek 6-16 prezentuje znormalizowane wartości $RPN_{HICCUPS}$ w funkcji n dla stałej długości ramki L=1000 bajtów przy dla BER=0 dla różnych wartości okna niezgody. Dla W_0=1 (natychmiastowa transmisja bez procedury *backoff*) krzywa osiąga maksimum przy n=1, dla pozostałych W_0 zmniejsza się wartość maksimum, a także jest ono osiągane dla coraz większych n (por. Tabela 6-12).



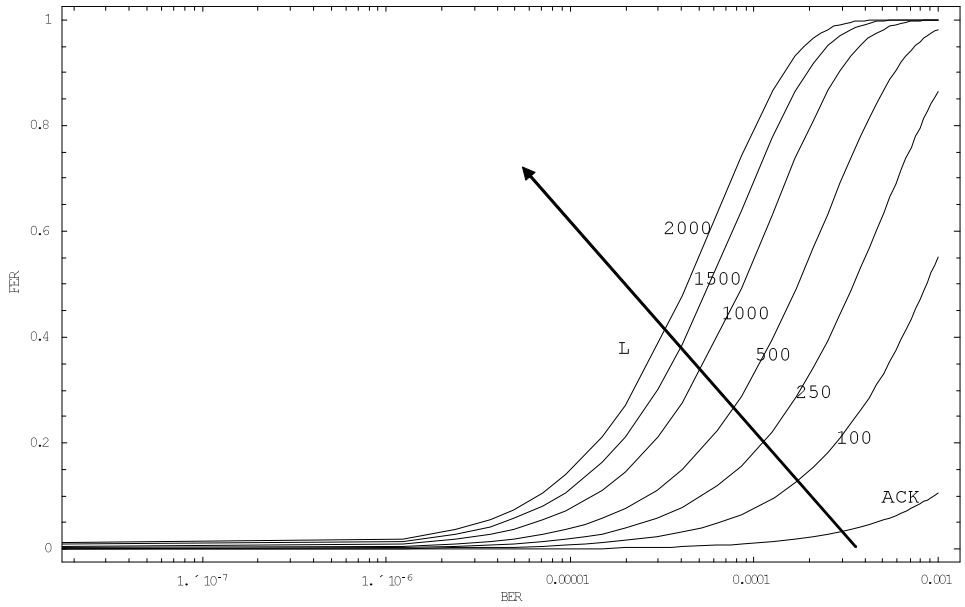
Rysunek 6-16 Znormalizowane wartości $RPN_{HICCUPS}$ w funkcji n – dla L=1000 bajtów, dla BER=0 i dla różnych wartości okna niezgody

Tabela 6-12 Znormalizowane wartości $RPN_{HICCUPS}$ w funkcji n – dla L=1000 bajtów, dla BER=0 i dla różnych wartości okna niezgody

W_0 / n	1	2	4	8	16	32	64
1	0,5551	0,5012	0,4197	0,3167	0,2124	0,1281	0,0714
2	0,5032	0,5079	0,4754	0,4064	0,3105	0,2100	0,1273
3	0,4626	0,4938	0,4886	0,4449	0,3657	0,2665	0,1721
4	0,4312	0,4773	0,4895	0,4640	0,4001	0,3076	0,2088
5	0,4061	0,4614	0,4857	0,4739	0,4231	0,3386	0,2393
10	0,3275	0,4000	0,4530	0,4786	0,4690	0,4202	0,3371
15	0,2834	0,3592	0,4225	0,4649	0,4772	0,4522	0,3883
20	0,2537	0,3294	0,3973	0,4492	0,4752	0,4666	0,4187
30	0,2147	0,2878	0,3588	0,4202	0,4624	0,4752	0,4509
40	0,1893	0,2591	0,3302	0,3961	0,4473	0,4735	0,4654

6.6.2 Zależność RPN od ramkowej stopy błędów (FER)

Zależność (6-30) wyraża związek pomiędzy bitową a ramkową stopą błędów. Ramkowa stopa błędów istotnie zależy od długości ramki – dla ustalonego *BER* zwiększa się wraz ze wzrostem długości ramki (Rysunek 6-17). Wartość *AER* (*FER* dla ACK) jest stosunkowo niewielka ze względu na małą długość ramki z potwierdzeniem (112 bitów).



Rysunek 6-17 Zależność pomiędzy BER i FER; długości ramek podano w bajtach, długość ramki ACK wynosi 112 bitów

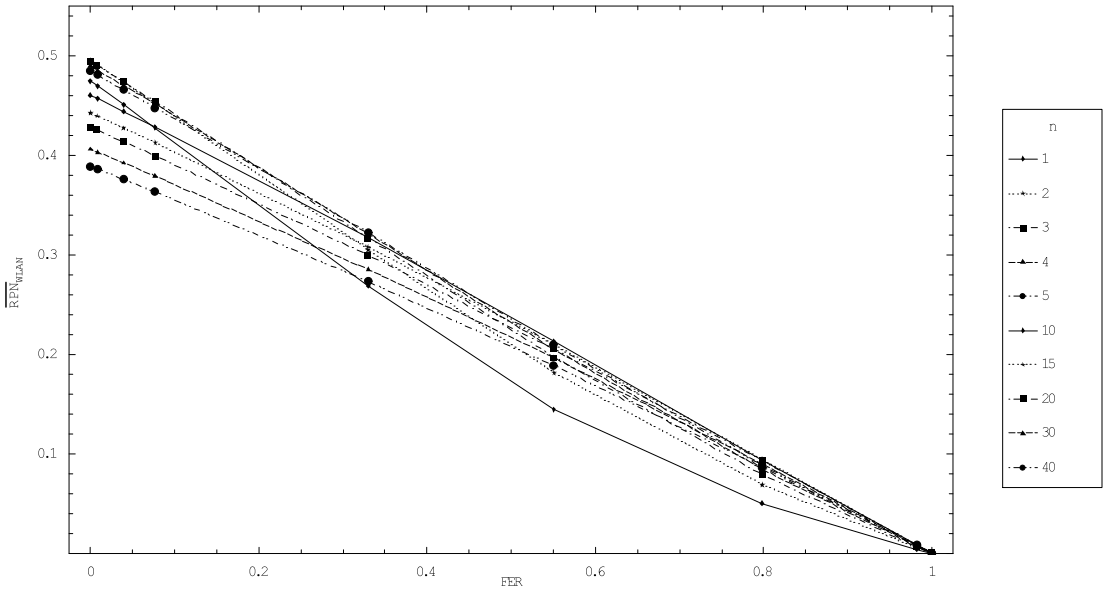
Na zamieszczonych w dalszej części tego podrozdziału wykresach przedstawiono znormalizowane wartości RPN_{WLAN} w funkcji *FER* (zgodnie z zależnością (6-7)). Wszystkie obliczenia wykonano dla *FER* wynikających z $BER \in \{10^{-3}, 5\cdot10^{-4}, 2\cdot10^{-4}, 10^{-4}, 5\cdot10^{-5}, 10^{-5}, 5\cdot10^{-6}, 10^{-6}, 0\}$ zgodnie z zależnością (6-30).

Rysunek 6-18 przedstawia znormalizowane wartości RPN_{WLAN} w funkcji *FER* dla stałej długości ramki L=1000 bajtów i dla $n \in \{1, 2, 3, 4, 5, 10, 15, 20, 30, 40\}$. Na wykresach można zaobserwować nieliniowość zależności RPN_{WLAN} od *FER*, w szczególności dla przypadku n=1. Brak liniowości dla ustalonego n wynika z faktu, że ramkowa stopa błędów wpływa na przebieg procedury *backoff*. FER wpływa na prawdopodobieństwo uszkodzenia ramki p_f (por. rozdział 6.3.2), co z kolei wpływa na nieliniową zmianę prawdopodobieństwa transmisji ramki τ (por. zależność (6-25)).

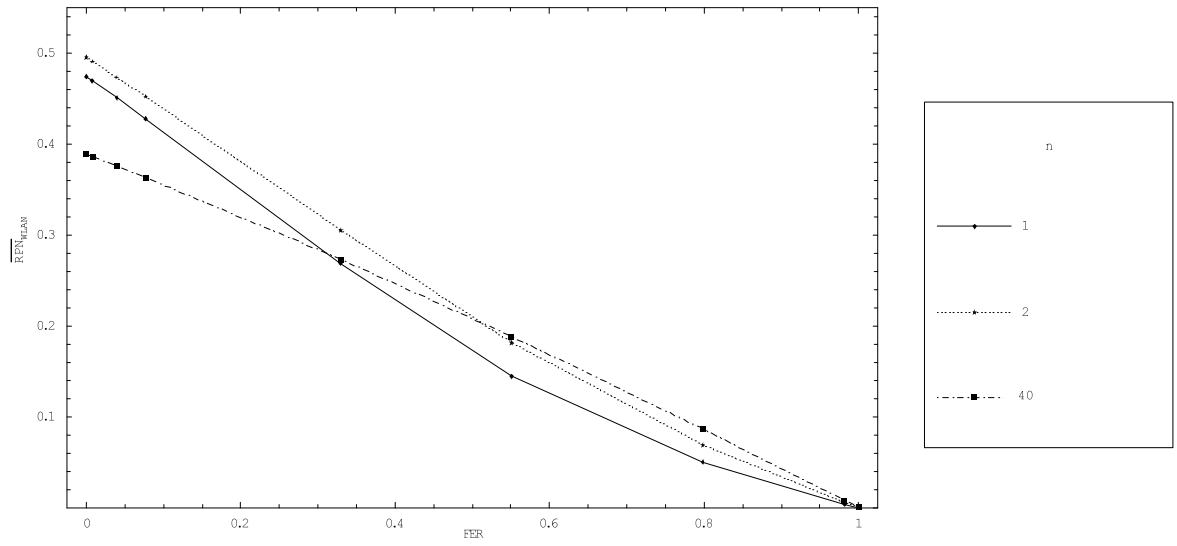
Rysunek 6-19 zawiera wykresy dla $n \in \{1, 2, 40\}$, a Rysunek 6-20 dla $n \in \{5, 10, 20, 40\}$. W porównaniu z n=1, wykres (Rysunek 6-19) dla n=2 zdecydowanie wygładza się. Wyniki analityczne przedstawia Tabela 6-13; w pierwszym wierszu tabeli (obok *FER*) podano w nawiasie wartość *AER*.

Kolejne dwa rysunki (Rysunek 6-21 i Rysunek 6-22) przedstawiają znormalizowane wartości RPN_{WLAN} w funkcji FER odpowiednio dla dwóch n (n=5 i n=10) i przy różnych

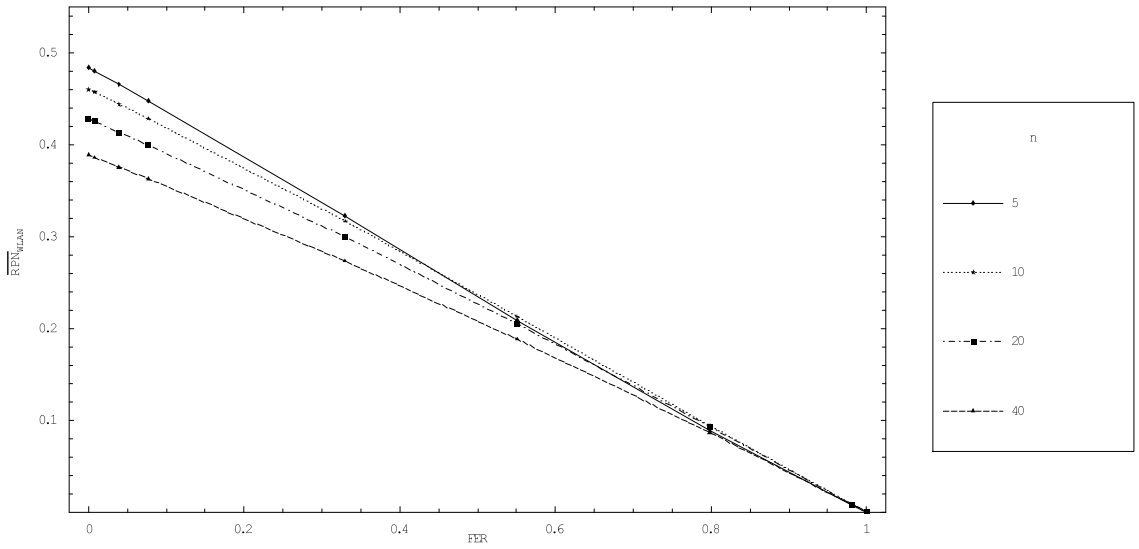
długościach ramki $L \in \{100, 250, 500, 1000, 1500, 2000\}$ bajtów. Na rysunkach można zaobserwować wzrost RPN_{WLAN} wraz ze wzrostem długości ramki.



Rysunek 6-18 Znormalizowane wartości RPN_{WLAN} w funkcji FER – dla L=1000 bajtów i dla różnych n



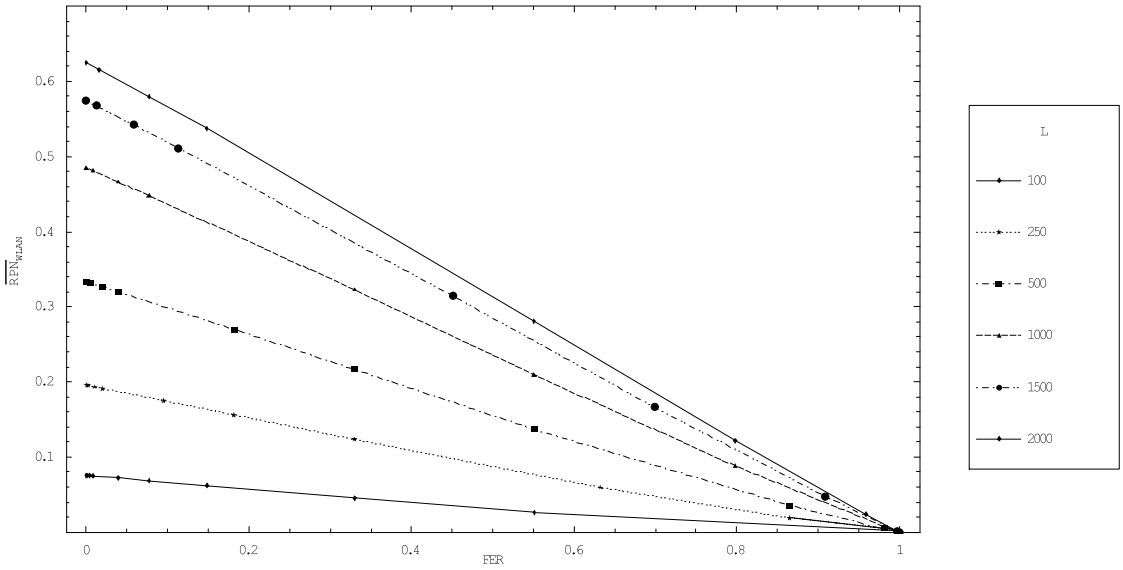
Rysunek 6-19 Znormalizowane wartości RPN_{WLAN} w funkcji FER – dla L=1000 bajtów i dla $n \in \{1, 2, 40\}$



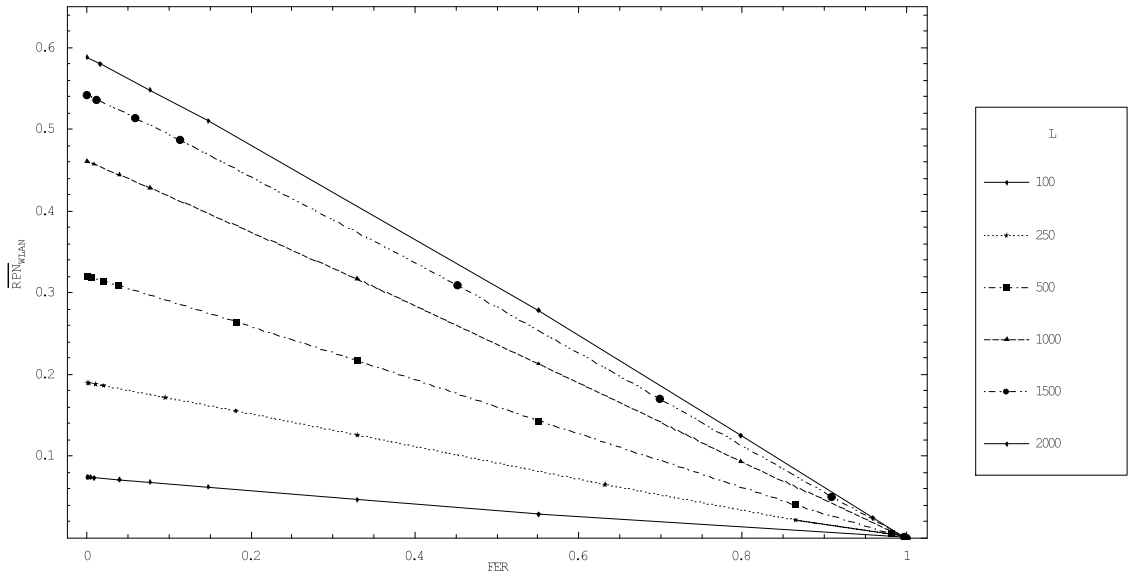
Rysunek 6-20 Znormalizowane wartości RPN_{WLAN} w funkcji *FER* – dla *L*=1000 bajtów i dla $n \in \{5, 10, 20, 40\}$

Tabela 6-13 Znormalizowane wartości RPN_{WLAN} w funkcji *FER* – dla *L*=1000 bajtów i dla różnych *n*

FER *(AER)* ***n***	**0** (0)	**0,0080** (0,0001)	**0,0392** (0,0006)	**0,0769** (0,0011)	**0,3297** (0,0056)	**0,5507** (0,0111)	**0,7981** (0,0222)	**0,9817** (0,0545)	**0,9997** (0,1060)
1	0,4745	0,4697	0,4510	0,4281	0,2688	0,1446	0,0497	0,0037	0,00006
2	0,4953	0,4909	0,4734	0,4521	0,3054	0,1816	0,0689	0,0054	0,00009
3	0,4945	0,4904	0,4740	0,4542	0,3170	0,1971	0,0787	0,0064	0,00011
4	0,4899	0,4860	0,4705	0,4517	0,3213	0,2050	0,0843	0,0070	0,00012
5	0,4845	0,4808	0,4660	0,4479	0,3226	0,2092	0,0879	0,0074	0,00013
10	0,4607	0,4574	0,4443	0,4285	0,3171	0,2131	0,0940	0,0081	0,00014
15	0,4427	0,4396	0,4275	0,4126	0,3082	0,2097	0,0942	0,0083	0,00014
20	0,4284	0,4254	0,4138	0,3997	0,2998	0,2052	0,0930	0,0082	0,00014
30	0,4061	0,4034	0,3925	0,3792	0,2853	0,1963	0,0898	0,0080	0,00014
40	0,3889	0,3863	0,3758	0,3631	0,2735	0,1885	0,0865	0,0077	0,00013



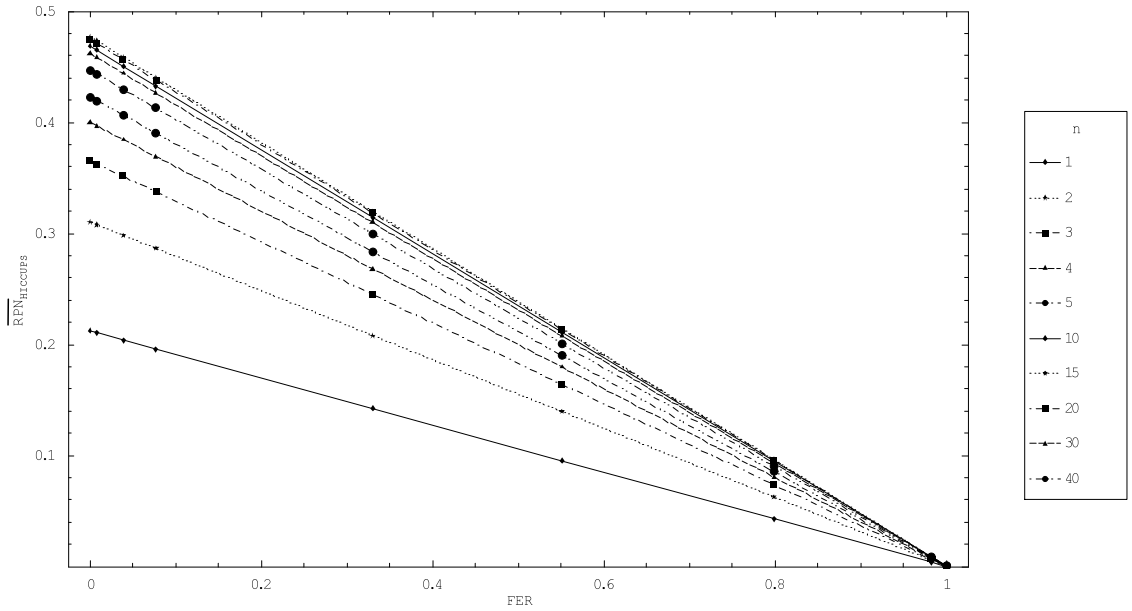
Rysunek 6-21 Znormalizowane wartości RPN_{WLAN} w funkcji *FER* – dla *n*=5 i dla różnych *L*



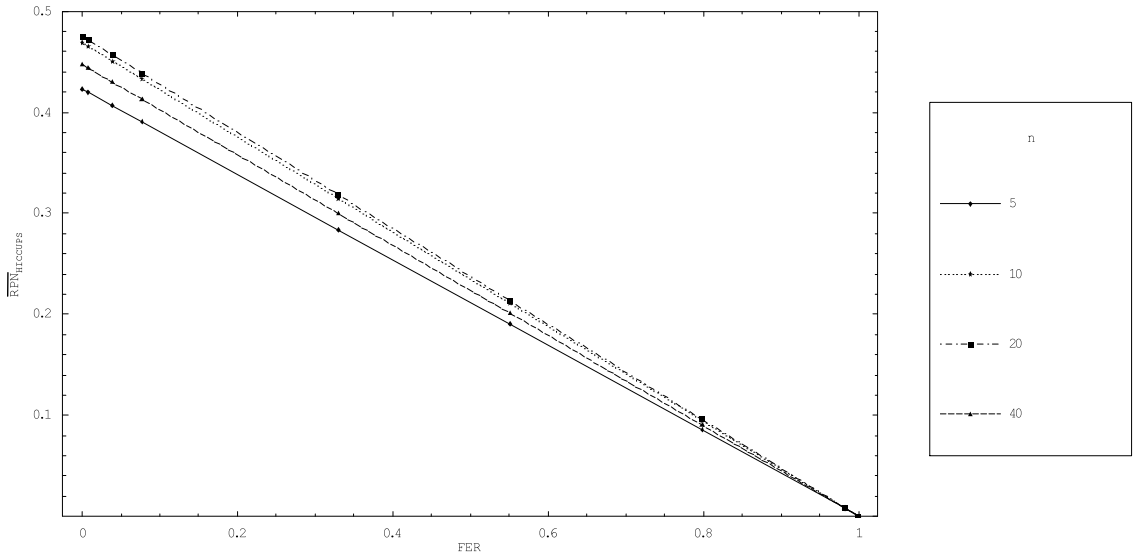
Rysunek 6-22 Znormalizowane wartości RPN_{WLAN} w funkcji *FER* – dla *n*=10 i dla różnych *L*

Rysunek 6-23 przedstawia znormalizowane wartości $RPN_{HICCUPS}$ w funkcji *FER* dla stałej długości ramki L=1000 bajtów i $n \in \{1, 2, 3, 4, 5, 10, 15, 20, 30, 40\}$. Na wykresach można zaobserwować liniową zależność pomiędzy *FER* a $RPN_{HICCUPS}$, która wynika z braku wpływu prawdopodobieństwa uszkodzenia ramki na przebieg procedury *backoff* (por. rozdział 6.5.2). Rysunek 6-24 przedstawia sytuację dla $n \in \{5, 10, 20, 40\}$. Wyniki analityczne, które posłużyły jako źródło do powyższych wykresów, przedstawia Tabela 6-14.

Ostatnie dwa rysunki (Rysunek 6-25 i Rysunek 6-26) przedstawiają znormalizowane wartości $RPN_{HICCUPS}$ w funkcji *FER* odpowiednio dla dwóch *n* (*n*=5 i *n*=10) i przy różnych długościach ramki $L \in \{100, 250, 500, 1000, 1500, 2000\}$ bajtów. Na rysunkach można zaobserwować wzrost $RPN_{HICCUPS}$ wraz ze wzrostem długości ramki.



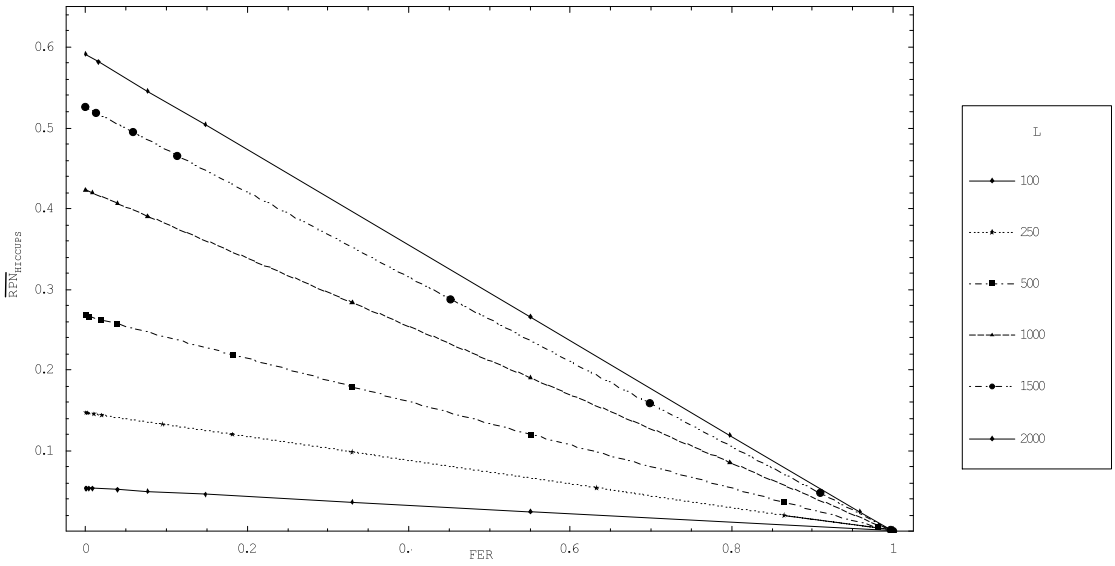
Rysunek 6-23 Znormalizowane wartości $RPN_{HICCUPS}$ w funkcji *FER* – dla *L*=1000 bajtów i dla różnych *n*



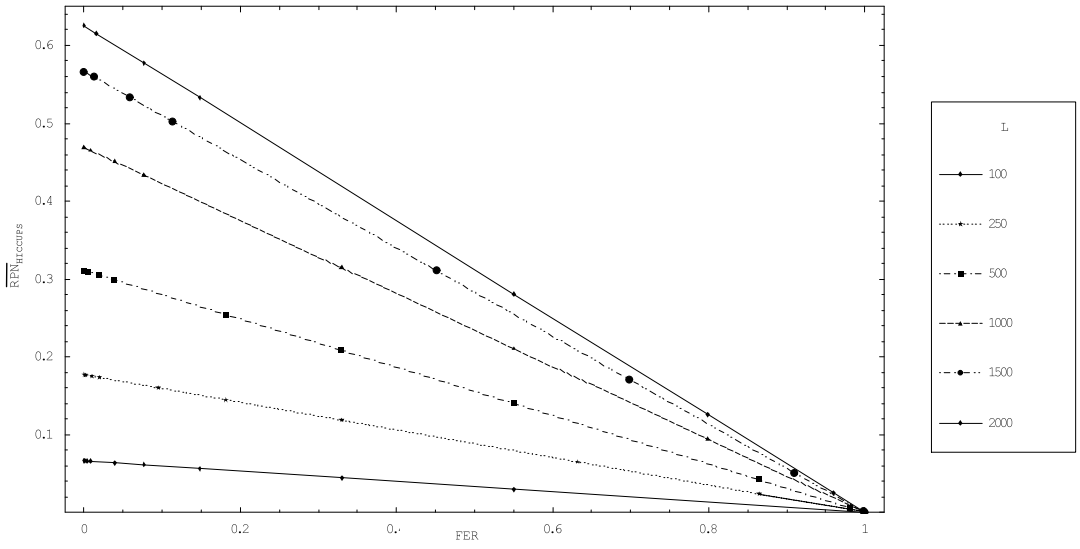
Rysunek 6-24 Znormalizowane wartości $RPN_{HICCUPS}$ w funkcji *FER* – dla *L*=1000 bajtów i dla $n \in \{5, 10, 20, 40\}$

Tabela 6-14 Znormalizowane wartości $RPN_{HICCUPS}$ w funkcji *FER* – dla *L*=1000 bajtów i dla różnych *n*

FER / ***n***	**0**	**0,0080**	**0,0392**	**0,0769**	**0,3297**	**0,5507**	**0,7981**	**0,9817**	**0,9997**
1	0,2124	0,2107	0,2041	0,1961	0,1424	0,0954	0,0429	0,0039	0,00007
2	0,3105	0,3081	0,2984	0,2867	0,2082	0,1395	0,0627	0,0057	0,00010
3	0,3657	0,3628	0,3513	0,3376	0,2451	0,1643	0,0738	0,0067	0,00012
4	0,4001	0,3970	0,3845	0,3694	0,2682	0,1798	0,0808	0,0073	0,00013
5	0,4231	0,4197	0,4065	0,3906	0,2836	0,1901	0,0854	0,0077	0,00014
10	0,4690	0,4653	0,4506	0,4330	0,3144	0,2107	0,0947	0,0086	0,00016
15	0,4772	0,4734	0,4585	0,4405	0,3199	0,2144	0,0963	0,0087	0,00016
20	0,4752	0,4714	0,4565	0,4386	0,3185	0,2135	0,0959	0,0087	0,00016
30	0,4624	0,4587	0,4443	0,4268	0,3099	0,2078	0,0933	0,0085	0,00015
40	0,4473	0,4437	0,4297	0,4129	0,2998	0,2010	0,0903	0,0082	0,00015



Rysunek 6-25 Znormalizowane wartości $RPN_{HICCUPS}$ w funkcji *FER* – *n*=5 i dla różnych *L*



Rysunek 6-26 Znormalizowane wartości $RPN_{HICCUPS}$ w funkcji *FER* – *n*=10 i dla różnych *L*

6.6.3 Wnioski

Na podstawie przeprowadzonej w rozdziałach 6.6.1 i 6.6.2 analizy RPN można sformułować następujące wnioski. Wartość RPN (zarówno RPN_{WLAN}, jak i $RPN_{HICCUPS}$) istotnie zależy od bitowej stopy błędów – im mniejsza wartość *BER*, tym, dla ustalonej liczby stacji *n* i długości ramki *L*, RPN jest większe. Jest to związane z wpływem błędów w kanale na liczbę efektywnie przesłanych danych.

Zwiększenie liczby stacji powoduje wzrost prawdopodobieństwa kolizji. Kolizje wpływają degradująco na wartość RPN. W systemie HICCUPS w trybie uszkodzonych ramek podwojenie okna w każdym kolejnym poziomie procedury *backoff* sprawia, że zanim dojdzie do kolejnej transmisji, system musi „przepuścić" średnio dwa razy większą liczbę pustych szczelin niż na poprzednim poziomie. W sieci WLAN działającej bez HICCUPS przejście do kolejnego poziomu procedury *backoff* następuję z prawdopodobieństwem p_f – dla $p_f << 1$ rzadko są osiągane najwyższe poziomy procedury *backoff*. Z powyższych obserwacji, a także z odmiennej definicji sukcesu transmisji w sieci WLAN bez HICCUPS i w systemie HICCUPS, przebieg krzywych RPN_{WLAN} jest inny niż przebieg $RPN_{HICCUPS}$. RPN przy ustalonej długości ramki *L* i ustalonej licznie stacji *n*, jest w dużym stopniu uzależniony od wielkości okna niezgody W_0 – zostało to dokładnie zbadane dla systemu HICCUPS.

Wartość RPN istotnie zależy od ramkowej stopy błędów, gdyż FER jest funkcją zarówno bitowej stopy błędów, jak i długości ramki *L* zgodnie z zależnością (6-30). Zatem przy ustalonej wartości *BER* i ustalonej liczbie stacji *n*, wartość RPN zależy od długości ramki *L*. Przy ustalonym FER i ustalonej liczbie stacji *n*, im większa długość ramki *L*, tym większa wartość RPN.

Zależność RPN_{WLAN} w funkcji *FER* przy ustalonym *n* (za wyjątkiem *n*=1) jest zbliżona do liniowej. W przypadku systemu HICCUPS jest liniowa. Wpływ

na liniowość ma związek FER z przebiegiem procedury *backoff*. W przypadku HICCUPS ten związek nie występuje.

6.7 Koszt działania systemu HICCUPS – κ

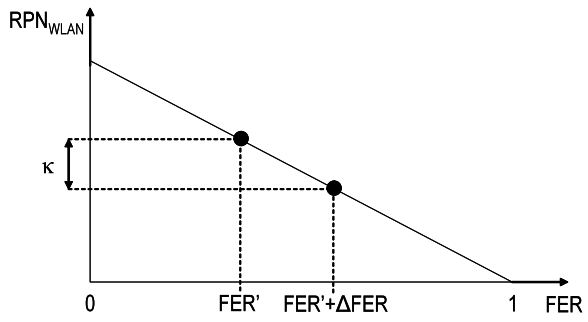
Zgodnie z definicją kosztu wprowadzoną w rozdziale 6.1 wyznaczenie kosztu (κ) sprowadza się do porównania RPN_{WLAN} dla rzeczywistej ramkowej stopy błędów z RPN_{WLAN} dla ramkowej stopy błędów wynikającej z nałożenia się pracy systemu HICCUPS w trybie uszkodzonych ramek. Inaczej mówiąc koszt κ jest oszacowaniem utraty RPN_{WLAN} związanej z użyciem przez HICCUPS ukrytych kanałów K3 i K2 (por. rozdział 5.1). W zależności od przyjętego mechanizmu przechodzenia w tryb uszkodzonych ramek i czasu pozostawania w tym stanie, użycie kanału K1 może mieć wpływ na koszt κ. Wpływ ten jest pomijalny w dwóch przypadkach (por. rozdział 3.3): wtedy, gdy stworzony kanał jest oparty na polach opcjonalnych, bądź wtedy, gdy ukryty kanał jest typu *timing* i jego użycie nie prowadzi do spadku przepustowości. W dalszych rozważaniach pominiemy wpływ użycia kanału K1 na koszt κ.

Zgodnie z rozważaniami przeprowadzonymi w rozdziale 4.6 efektem działania systemu HICCUPS jest zwiększenie *FER* sieci użytkowej o ustaloną wartość ΔFER, która jest parametrem podwarstwy zarządzania prawem głosu. Przyjmijmy, że ramkowa stopa błędów sieci bez systemu HICCUPS wynosi *FER'*. Zauważmy, że $0 \leq \Delta FER \leq 1\text{-}FER'$. W związku z tym koszt κ możemy określić następująco:

$$\kappa = RPN_{WLAN}(FER') - RPN_{WLAN}(FER'+\Delta FER) \tag{6-50}$$

lub w postaci znormalizowanej do szybkości transmisji danych *R* (por. zależność (5-3)):

$$\overline{\kappa} = \frac{\kappa}{R}. \tag{6-51}$$



Rysunek 6-27 Graficzna interpretacja kosztu κ

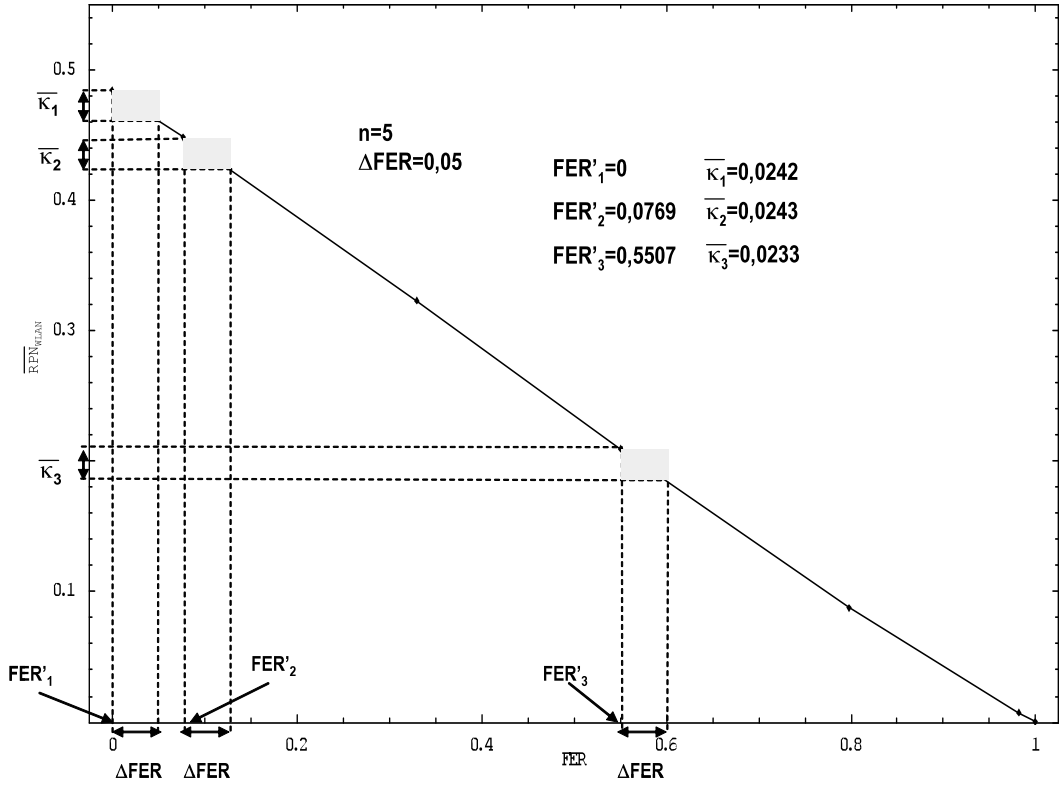
Krzywe kosztu bazują na omawianej w rozdziale 6.6.2 zależności RPN_{WLAN} w funkcji *FER*. Pomimo, że RPN_{WLAN} nie zachowuje się w pełni liniowo (por. Rysunek 6-18) dla małych ΔFER możemy korzystać ze wzoru przybliżonego (Rysunek 6-27):

$$\kappa \approx \frac{\Delta FER}{1 - FER'} RPN_{WLAN}(FER'). \tag{6-52}$$

W poniższych tabelach (Tabela 6-15 i Tabela 6-16) przedstawiono znormalizowane wartości kosztu κ dla dwóch wybranych parametrów n (n=5 i n=10). Wyniki otrzymano korzystając ze wzoru przybliżonego (6-52) i przy założeniu ramki o stałej długości L=1000 bajtów. Przyjęto trzy różne punkty pracy WLAN: $FER' \in \{0; 0{,}0769; 0{,}5507\}$ (odpowiadające pracy w BER $0, 10^{-5}, 10^{-4}$). Dla tak przyjętych warunków rozważono pięć wartości ΔFER (0,01; 0,02; 0,03; 0,04; 0,05). Rysunek 6-28 przedstawia graficzną interpretację przypadku dla n=5 i ΔFER=0,05.

Tabela 6-15 Znormalizowane wartości kosztu κ (w nawiasie podano wartości bezwzględne) – dla n=5 i dla L=1000 bajtów

ΔFER / FER'	**0,01**	**0,02**	**0,03**	**0,04**	**0,05**
0	0,0048 (0,26 Mbit/s)	0,0097 (0,52 Mbit/s)	0,0145 (0,78 Mbit/s)	0,0194 (1,05 Mbit/s)	0,0242 (1,31 Mbit/s)
0,0769	0,0049 (0,26 Mbit/s)	0,0097 (0,52 Mbit/s)	0,0146 (0,79 Mbit/s)	0,0194 (1,05 Mbit/s)	0,0243 (1,31 Mbit/s)
0,5507	0,0047 (0,25 Mbit/s)	0,0093 (0,50 Mbit/s)	0,0140 (0,75 Mbit/s)	0,0186 (1,01 Mbit/s)	0,0233 (1,26 Mbit/s)



Rysunek 6-28 Graficzna interpretacja kosztu κ – dla n=5, dla L=1000 bajtów i dla ΔFER=0,05

Tabela 6-16 Znormalizowane wartości kosztu κ (w nawiasie podano wartości bezwzględne) – dla n=10 i dla L=1000 bajtów

ΔFER / FER'	**0,01**	**0,02**	**0,03**	**0,04**	**0,05**
0	0,0046 (0,25 Mbit/s)	0,0092 (0,50 Mbit/s)	0,0138 (0,75 Mbit/s)	0,0184 (1,00 Mbit/s)	0,0230 (1,24 Mbit/s)
0,0769	0,0046 (0,25 Mbit/s)	0,0093 (0,50 Mbit/s)	0,0139 (0,75 Mbit/s)	0,0186 (1,00 Mbit/s)	0,0232 (1,25 Mbit/s)
0,5507	0,0047 (0,26 Mbit/s)	0,0095 (0,51 Mbit/s)	0,0142 (0,77 Mbit/s)	0,0190 (1,02 Mbit/s)	0,0237 (1,28 Mbit/s)

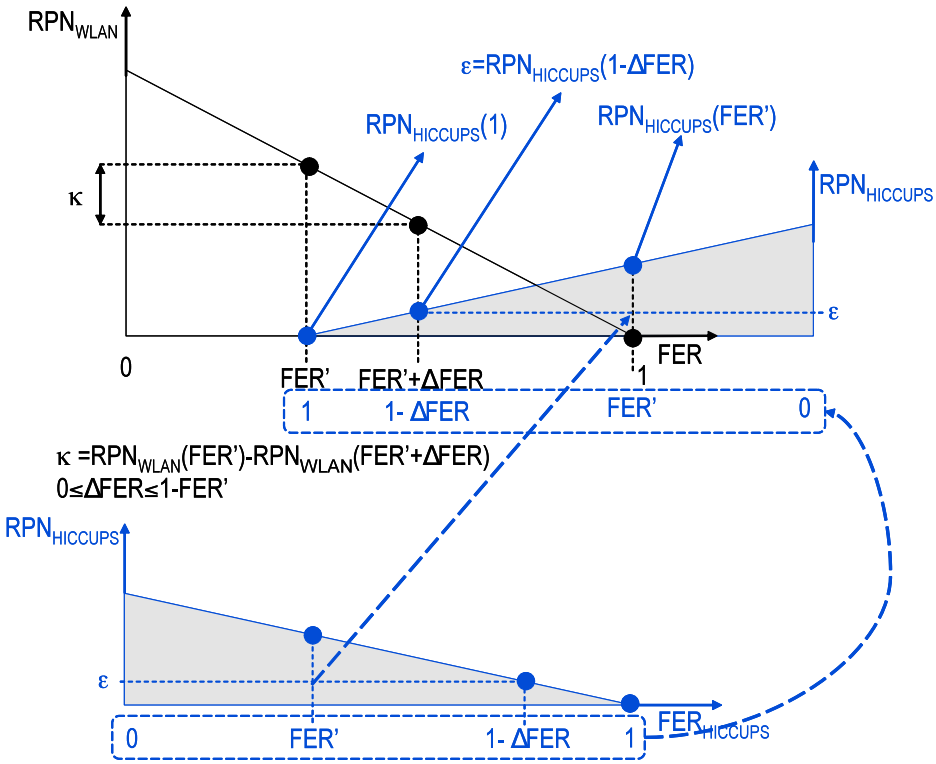
Reasumując: funkcja kosztu działania systemu HICCUPS jest pochodną zależności RPN_{WLAN} w funkcji FER i może zostać zaproksymowana liniowo. Dla ustalonego n i L koszt istotnie zależy od przyjętego ΔFER.

6.8 Efektywność systemu HICCUPS – ε

Zgodnie z definicją kosztu wprowadzoną w rozdziale 6.1, aby wyznaczyć efektywność systemu HICCUPS ε określimy jego RPN w stanie, który wynika z własności fizycznych (BER), jak i z liczby ramek uzyskanych w wyniku działania trybu uszkodzonych ramek.

W rozważanym w rozdziale 6.5 modelu, zgodnie z działaniem systemu HICCUPS i cechami 802.11 CSMA/CA, wraz z transmisją kolejnej ramki zwiększany jest poziom procedury *backoff*, aż do osiągnięcia maksimum. Model nie ujmuje sytuacji, w której przesłana ramka może być poprawna z punktu widzenia logiki działania WLAN, jednak dotyczy przypadku granicznego, dzięki, któremu można określić maksymalną wydajność systemu HICCUPS. W sieci WLAN z systemem HICCUPS tryb uszkodzonych ramek pojawia się co pewien czas. W sytuacji krańcowej stacje mogą przebywać w tym trybie przez cały czas, wtedy RPN_{WLAN} w funkcji FER wynosi 0 (gdyż $RPN_{WLAN}(1) = 0$), a RPN dla HICCUPS wynosi $RPN_{HICCUPS}(FER')$. Ponieważ $0 \leq \Delta FER \leq 1\text{-}FER'$, w omawianej sytuacji $\Delta FER = 1\text{-}FER'$. W innym skrajnym przypadku, gdy system HICCUPS nie jest używany, RPN dla HICCUPS wynosi 0 (gdyż $RPN_{HICCUPS}(1) = 0$), a RPN dla WLAN – $RPN_{WLAN}(FER')$. W tym przypadku $\Delta FER = 0$.

Mając na względzie powyższe rozważania wyznaczmy hipotetyczny „punkt pracy" systemu HICCUPS dla ($FER'+\Delta FER$) poprzez złożenie translacji (przesunięcia) i symetrii zwierciadlanej (Rysunek 6-29). Krzywa $RPN_{HICCUPS}$ w funkcji FER zostaje poddana symetrii zwierciadlanej i przesunięta w dziedzinie FER dla WLAN, tak aby punkt $RPN_{WLAN}(1) = 0$ odpowiadał punktowi $RPN_{HICCUPS}(FER')$, a punkt $RPN_{WLAN}(FER')$ – punktowi $RPN_{HICCUPS}(1) = 0$. Z rozwiązania graficznego wynika, że $FER_{HICCUPS} = 1\text{-}\Delta FER$ (por. rozdział 4.6).



Rysunek 6-29 Graficzna interpretacja efektywności ε

W związku z powyższym efektywność systemu HICCUPS ε możemy określić następująco:

$$\varepsilon = RPN_{HICCUPS}(1 - \Delta FER) \tag{6-53}$$

lub w postaci znormalizowanej do szybkości transmisji danych R (por. zależność (5-3)):

$$\overline{\varepsilon} = \frac{\varepsilon}{R}. \tag{6-54}$$

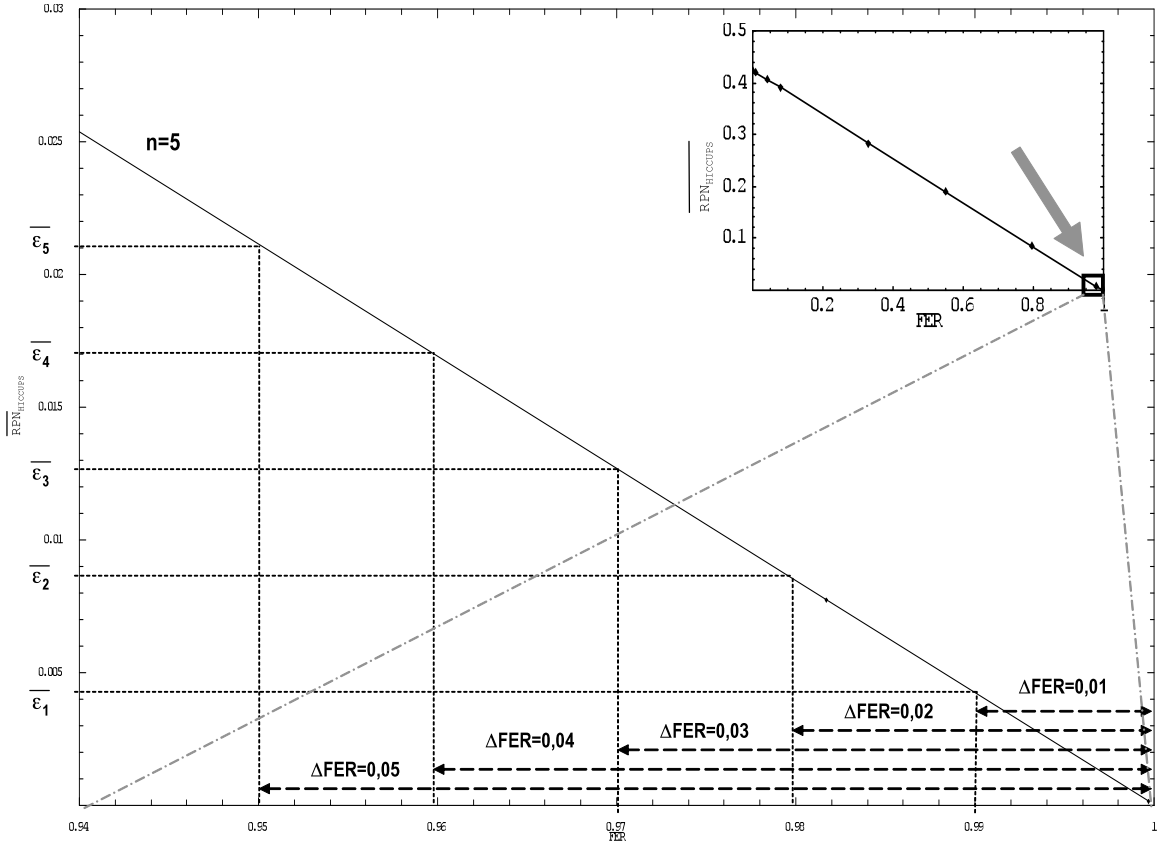
Efektywność zależy wyłącznie od ΔFER i nie jest bezpośrednio zależna od FER'. Ten pozorny paradoks wynika z tego, że ramki uszkodzone w sieci w wyniku warunków fizycznych (BER) są stratą dla WLAN jak i systemu HICCUPS w trybie uszkodzonych ramek, natomiast wprowadzone przez system HICCUPS ramki zmieniają FER sieci użytkowej o ΔFER (por. rozdział 6.7).

Analogicznie do rozważań dotyczących kosztu κ prowadzonych w rozdziale 6.7 dla dwóch wartości n (n=5 i n=10) obliczono efektywność ε przy założeniu ramki o długości L=1000 bajtów. Rozpatrzono pięć wartości ΔFER (0,01; 0,02; 0,03; 0,04; 0,05). Wyniki przedstawiono w tabeli 6-17.

Tabela 6-17 Znormalizowane wartości efektywności ε (w nawiasie podano wartości bezwzględne) – dla n=5 i n=10 oraz dla L=1000 bajtów

ΔFER / n	0,01	0,02	0,03	0,04	0,05
5	0,0042 (0,23 Mbit/s)	0,0085 (0,46 Mbit/s)	0,0127 (0,69 Mbit/s)	0,0169 (0,91 Mbit/s)	0,0212 (1,14 Mbit/s)
10	0,0047 (0,25 Mbit/s	0,0094 (0,51 Mbit/s)	0,0141 (0,76 Mbit/s)	0,0188 (1,01 Mbit/s)	0,0235 (1,27 Mbit/s)

Dla n=5 i ΔFER=0,01 efektywność ε wynosi ok. 0,23 Mbit/s, co oznacza ok. 46 kbit/s w przeliczeniu na jedną stację. Ze względu na liniową zależność pomiędzy ramkową stopą błędów, zwiększając ΔFER do 0,05 uzyskujemy 5 razy większą efektywność, tj. ok. 1,14 Mbit/s, co oznacza ok. 228 kbit/s w przeliczeniu na jedną stację. W pierwszym przypadku, przy FER'=0 i FER'=0,0769, koszt κ (por. Tabela 6-15) wynosi ok. 0,26 Mbit/s, a przy FER'=0,5507 – 0,25 Mbit/s, podczas gdy w drugim przypadku odpowiednio ok. 1,31 Mbit/s i ok. 1,26 Mbit/s. Rysunek 6-30 przedstawia graficzną interpretację efektywności dla n=5 i parametrów przedstawionych w powyższej tabeli.



Rysunek 6-30 Graficzna interpretacja efektywności ε – dla n=5 i dla L=1000 bajtów

Dla n=10 i ΔFER=0,01 efektywność ε wynosi ok. 0,25 Mbit/s, co oznacza ok. 25 kbit/s w przeliczeniu na jedną stację. Zwiększając ΔFER do 0,05 uzyskujemy

5 razy większą efektywność, tj. ok. 1,27 Mbit/s, co oznacza ok. 127 kbit/s w przeliczeniu na jedną stację. W pierwszym przypadku przy *FER'*=0 i *FER'*=0,0769, koszt κ (por. Tabela 6-16) wynosi ok. 0,25 Mbit/s, a dla *FER'*=0,5507 – 0,26 Mbit/s, podczas gdy w drugim przypadku odpowiednio ok. 1,25 Mbit/s i ok. 1,28 Mbit/s.

Reasumując: funkcja efektywności systemu HICCUPS jest pochodną zależności $RPN_{HICCUPS}$ w funkcji *FER* i jest liniowa. Dla ustalonego *n* i *L* efektywność zależy wyłącznie od ΔFER. Dla omawianych przykładów (dla *n*=2 i *n*=10 oraz stosunkowo niewielkiej wartości ΔFER=0,05) efektywność wynosi ponad 1,1 Mbit/s, a koszt poniżej 1,3 Mbit/s.

7. Podsumowanie

Przedstawiony i przeanalizowany w niniejszej pracy system steganograficzny HICCUPS wykorzystuje ramki z niepoprawnymi sumami kontrolnymi jako metodę na stworzenie dodatkowego, dostępnego na żądanie, pasma do ukrywania informacji.

W rozprawie sformułowano warunki niezbędne do realizacji zaproponowanego systemu, a następnie przedstawiono jego architekturę oraz koncepcję działania. Poddano dyskusji kwestie związane z realizacją systemu HICCUPS w sieciach 802.11 zwracając uwagę na specyfikę metody dostępu do medium CSMA/CA. Dokonano analizy właściwości prezentowanego systemu, w szczególności wyznaczono jego efektywność oraz koszt realizacji w WLAN wyrażony przez spadek przepustowości użytkowej. Analizę przeprowadzono z wykorzystaniem nowego, zaproponowanego w pracy, modelu CSMA/CA bazującego na łańcuchach Markowa.

W pracy wykazano, że niewykrywalność systemu HICCUPS silnie zależy od ustalonego poziomu ramkowej stopy błędów wnoszonej do sieci użytkowej przez działanie systemu. Stwierdzono, że funkcja kosztu działania systemu HICCUPS jest pochodną zależności ruchu przenoszonego w warunkach nasycenia dla sieci WLAN w funkcji ramkowej stopy błędów i jest w przybliżeniu liniowa. Dla ustalonej liczby stacji i długości ramki, koszt istotnie zależy od poziomu ramkowej stopy błędów wnoszonej do sieci użytkowej przez działanie systemu HICCUPS. Wykazano, że funkcja efektywności systemu HICCUPS jest liniowa i jest pochodną zależności ruchu przenoszonego w warunkach nasycenia dla HICCUPS w trybie uszkodzonych ramek w funkcji ramkowej stopy błędów. Dla ustalonej liczby stacji i długości ramki efektywność zależy wyłącznie od poziomu ramkowej stopy błędów wnoszonej do sieci użytkowej przez działanie systemu HICCUPS.

Dokonana w rozprawie analiza właściwości systemu HICCUPS dotyczyła warunków nasycenia w sieci WLAN. W dalszych badaniach należałoby rozważyć warunki braku nasycenia, w szczególności dla różnych modeli napływu zgłoszeń, a zatem różnego przebiegu procesu rywalizacji o medium. Zaprezentowany w rozprawie nowy model CSMA/CA może zostać rozbudowany tak, aby uwzględniać warunki braku nasycenia.

W pracy rozważano model kanału, w którym błędy pojawiają się w sposób losowy, podczas gdy w rzeczywistości błędy są skorelowane. W dalszych badaniach należałoby poddać analizie rzeczywisty rozkład błędów w ramce oraz korelacje pomiędzy nimi, a następnie stworzyć algorytm upodabniający do siebie ramki wysyłane przez system HICCUPS w jednym cyklu retransmisyjnym WLAN. W rozprawie przeanalizowano metodę podstawową działania CSMA/CA tj. bez rezerwacji kanału; aby rozważyć metodę z rezerwacją kanału – z RTS/CTS, należy stworzyć nowy model procedury *backoff* uwzględniający dwa liczniki powtórzeń – SLRC i SSRC.

W pracy skoncentrowano się na pracy sieci WLAN w trybie ad hoc, w którym wszystkie stacje są w zasięgu. Zgodnie z rozważaniami przeprowadzonymi w pracy, komunikacja poprzez punkt dostępowy, w trybie infrastrukturalnym, wymaga

wprowadzenia w nim buforów opóźniających transmisję. Przy dużym ruchu steganograficznym buforowanie danych może stanowić wąskie gardło, zatem celem dalszych analiz powinno być zbadanie wpływu tego ograniczenia na efektywność systemu HICCUPS.

W rozprawie przeanalizowano wariant pracy systemu, w którym wszystkie stacje dokonują transmisji w trybie uszkodzonych ramek. Kolejnym celem poznawczym powinno być przeanalizowanie sytuacji, w której steganogramy są wysyłane przez podzbiór stacji.

Ze względu na złożoność sieci 802.11, w realizacji niektórych ze sformułowanych powyżej celów, w praktyce konieczne będzie zastosowanie metod symulacyjnych, gdyż wyprowadzenie zależności analitycznych wydaje się mało realne.

Na zakończenie warto wskazać kilka potencjalnych kierunków badawczych związanych z dziedziną steganografii sieciowej w ogóle. Istotnym zagadnieniem jest analiza wadliwych zachowań protokołów sieciowych, które mogą być związane z ukrytą komunikacją. Dzięki detekcji tego typu anomalii można wykrywać niesprawiedliwe (*unfair*) zachowanie stacji, w tym m.in. chciwe przejmowanie zasobów, czy też umyślne zakłócanie transmisji. Innym interesującym zagadnieniem badawczym jest stworzenie koncepcji „steganograficznego routera" przenoszącego informacje pomiędzy różnymi, nie tylko sieciowymi, systemami steganograficznymi. Ważny jest również rozwój technik ukrywania informacji dla szerszej klasy sieci bezprzewodowych, w tym dla sieci sensorowych oraz WiMax.

Bibliografia

[1] Aboba, B., Blunk, L., Vollbrecht, J. i in..: *Extensible Authentication Protocol (EAP)*. IETF Request for Comments: 3748. Czerwiec 2004

[2] Aboba, B., Simon, D.: *PPP EAP TLS Authentication Protocol*. IETF Request for Comments: 2716. Październik 1999

[3] Ahsan, K., Kundur, D.: *Practical Data Hiding in TCP/IP*. Materiały: ACM Workshop on Multimedia and Security. 2002

[4] Arbaugh, W., Shankar, N.: *Your 802.11 Wireless Network has No Clothes*. Materiały: First IEEE International Conference on Wireless LANs and Home Networks. Grudzień 2001. str. 131-144

[5] Arkko, J., Haverinen, H.: *Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA)*. IETF draft. Grudzień 2004

[6] Bagnall, R.: *Reversing the Steganography Myth in Terrorist Operations: The Asymmetrical Threat of Simple Intelligence Dissemination Techniques Using Common Tools*. SANS Information Security Reading Room. 31 października 2003. URL: http://www.sans.org/reading_room/whitepapers/stenganography/556.php

[7] Bellardo, J., Savage, S.: *802.11 Denial-of-Service Attacks: Real Vulnerabilities and Practical Solutions*. Materiały: USENIX Security Symposium. Waszyngton (Stany Zjednoczone). Sierpień 2003

[8] Bharghavan, V., Demers, A., Shenker, S., Zhang, L.: *MACAW: A Media Access Protocol for Wireless LANs*. Materiały: ACM SIGCOMM 1994. str. 212-225

[9] Bianchi, G.: *Performance Analysis of the IEEE 802.11 Distributed Coordination Function*. IEEE Journal on Selected Areas in Communications, Vol. 18, No. 3. Marzec 2000. str. 535-547

[10] Bianchi, G., Tinnirello, I.: *Remarks on IEEE 802.11 DCF Performance Analysis*. IEEE Communications Letters, Vol. 9. Sierpień 2005. str. 765-767

[11] Bianchi, G.: *IEEE 802.11: Saturation Throughput Analysis*. IEEE Communications Letters, Vol. 2. Grudzień 1998. str. 318-320

[12] Blunk, L., Vollbrecht, J.: *PPP Extensible Authentication Protocol (EAP)*. IETF Request for Comments: 2284. Marzec 1998

[13] Borisov, N., Goldberg, I., Wagner, D.: *Intercepting Mobile Communications: The Insecurity of 802.11*. Materiały: 7th Annual International Conference on Mobile Computing and Networking. Rzym (Włochy). 2001

[14] Brzeziński, K.: *Broadcast and Multicast in the Design and Programming of Large Distributed Systems*. Rozprawa doktorska. Politechnika Warszawska. Wydział Elektroniki i Technik Informacyjnych. 1995

[15] Cabaj, K., Szczypiorski, K.: *Systemy wykrywania włamań dla sieci bezprzewodowych Wi-Fi*. Materiały: Secure 2004 – VII Konferencja IT. Warszawa. 20-21 października 2004

[16] Cali, F., Conti, M., Gregori, E.: *Dynamic Tuning of the IEEE 802.11 Protocol to Achieve a Theoretical Throughput Limit*. IEEE/ACM Trans. Networking, Vol. 8, No. 6. Grudzień 2000. str. 785-799

[17] Chatzimisios, P., Boucouvalas, A., Vitsas, V.: *Influence of Channel BER on IEEE 802.11 DCF*. IEE Electronics Letters. Vol. 39 No. 23. 13 listopada 2003

[18] Chmielewski, A.: *Urządzenie do wytwarzania dodatkowego kanału cyfrowego*. Zgłoszenie wynalazku nr P 245442. Politechnika Warszawska. 1985

[19] Chmielewski, A.: *Wykorzystanie nadmiarowości kodu transmisyjnego do przesyłania dodatkowego strumienia danych*. Rozprawa doktorska. Politechnika Warszawska. 1988

[20] Craiger, J.: *802.11, 802.1X, and Wireless Security*. Sans InfoSec Reading Room. Czerwiec 2002
[21] Diffie, W., Hellman, M.: *New Directions in Cryptography*. IEEE Transactions on Information Theory, V. IT-22, n. 6. Czerwiec 1977
[22] Dogu, T., Ephremides, A.: *Covert Information Transmission through the Use of Standard Collision Resolution Algorithms*. Materiały: Third International Workshop on Information Hiding. Drezno (Niemcy). 1999. str. 419-433
[23] Duchamp, D., Reynolds, N.: *Measured Performance of a Wireless LAN*. Materiały: IEEE 17th Conference on Local Computer Networks. Wrzesień 1992. str. 494-499
[24] Dworkin, M.: *Recommendation for Block Cipher Modes of Operation*. NIST Pub 800-38A. Grudzień 2001
[25] Dygnarowicz, R.: *Steganografia*. IV Krajowa Konferencja Zastosowań Kryptografii Enigma 2000. Warszawa. Maj 2000
[26] Ebert, J-P., Willig, A.: *A Gilbert-Elliot Bit Error Model and the Efficient Use in Packet Level Simulation*. TKN Technical Reports Series of Technical University Berlin, TKN-99-002. Marzec 1999
[27] Engelstad, P., Østerbø, O.: *Queueing Delay Analysis of IEEE 802.11e EDCA*. Materiały: IFIP WONS 2006 – The Third Annual Conference on Wireless On demand Network Systems and Services. Les Ménuires (Francja). 18-20 stycznia 2006
[28] Ergen, M., Varaiya, P.: *Throughput Analysis and Admission Control in IEEE 802.11a*. Springer Mobile Networks and Applications, vol. 10, no. 5. Październik 2005. str. 705-706
[29] Ergen, M.: *I-WLAN: Intelligent Wireless Local Area Networking*. Rozprawa doktorska. University of California, Berkeley. Grudzień 2004
[30] Esser, H-G., Freiling, F.: *Kapazitätsmessung eines verdeckten Zeitkanals über HTTP*. Materiały: Sicherheit 2006. Magdeburg (Niemcy). 20-22 lutego 2006
[31] Fisk, G., Fisk, M., Papadopoulos, C., Neil, J.: *Eliminating Steganography in Internet Traffic with Active Wardens*. Materiały: Information Hiding 2002. LNCS 2578
[32] Fluhrer, S., Mantin, I., Shamir, A.: *Weaknesses in the Key Scheduling Algorithm of RC4*. Cisco Systems Inc. i The Weizmann Institute. Sierpień 2001
[33] Foh, C.: *Performance Analysis and Enhancement of MAC Protocols*. Rozprawa doktorska. University of Melbourne. Department of Electrical and Electronic Engineering. 2002
[34] Fridrich, J.: *Applications of Data Hiding In Digital Images*. Materiały: ISPACS'98 Conference. Melbourne (Australia). Tutorial. 4-6 listopada 1998
[35] Funk, P., Blake-Wilson, S.: *EAP Tunneled TLS Authentication Protocol (EAP-TTLS)*. IETF draft. Czerwiec 2004
[36] Giffin, J., Greenstadt, R., Litwack, P., Tibbetts, R.: *Covert Messaging through TCP Timestamps*. Materiały: Privacy Enhancing Technologies 2002. LNCS 2482, 2003. str. 194-208
[37] Girling, C.: *Covert Channels in LAN's*. IEEE Transactions on Software Engineering. Luty 1987
[38] Gligor, V.: *A Guide to Understanding Covert Channel Analysis of Trusted Systems*. National Computer Security Center. Maryland (Stany Zjednoczone). Tech. Rep. NCSC-TG-030. Listopad 1993
[39] Handel, T., Sandford, M.: *Hiding Data in the OSI Network Model*. Materiały: First International Workshop on Information Hiding. 30 maja-1 czerwca 1996. LNCS 1174. str. 23-38
[40] Haverinen, H., Salowey, J.: *Extensible Authentication Protocol Method for GSM Subscriber Identity Modules (EAP-SIM)*. IETF draft. Grudzień 2004

[41] He, C., Mitchell, C.: *Security Analysis and Improvements for IEEE 802.11i*. Materiały:12th Annual Network and Distributed System Security Symposium. San Diego (Stany Zjednoczone). Luty 2005
[42] Heusse, M., Rousseau, F., Guillier, R., Duda, A.: *Idle Sense: An Optimal Access Method for High Throughput and Fairness in Rate Diverse Wireless LANs*. Materiały: SIGCOMM'05 Conference on Applications, Technologies, Architectures and Protocols for Computer Communications. Filadelfia (Stany Zjednoczone). 22-26 sierpnia 2005. str. 121-132
[43] Hulton, D.: *Practical Exploitation of RC4 Weaknesses in WEP Environments*. 22 lutego 2002. URL: http://www.dachb0den.com/projects/bsd-airtools/wepexp.txt
[44] IEEE 802.11-1999 (8802-11: 1999) IEEE Standards for Information Technology – Telecommunications and Information Exchange between Systems – Local and Metropolitan Area Network – Specific Requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. 1999
[45] IEEE 802.11a-1999 (8802-11:1999/Amd 1:2000(E)) IEEE Standard for Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications – Amendment 1: High-speed Physical Layer in the 5 GHz band. 1999
[46] IEEE 802.11b-1999 Supplement to 802.11-1999, Wireless LAN MAC and PHY specifications: Higher speed Physical Layer (PHY) extension in the 2.4 GHz band. 1999
[47] IEEE 802.11e-2005 IEEE Standard for Information Technology – Telecommunications and Information Exchange Between Systems – LAN/MAN Specific Requirements – Part 11 Wireless Medium Access Control (MAC) and Physical Layer (PHY) specifications: Medium Access Control (MAC) Quality of Service (QoS) Enhancements
[48] IEEE 802.11g-2003 Standard for Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications – Amendment 4: Further Higher-Speed Physical Layer Extension in the 2.4 GHz Band. 2003
[49] IEEE 802.11i-2004 Standard for Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications Amendment 6: Medium Access Control (MAC) Security Enhancements. 2004
[50] IEEE 802.15.1-2002 Standard for Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements Part 15.1: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Wireless Personal Area Networks (WPANs). Czerwiec 2002
[51] IEEE 802.15.4-2003 Standard for Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks Specific requirements Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low Rate Wireless Personal Area Networks (LR-WPANs). Październik 2003
[52] IEEE 802.3 Standard for Information Technology – Telecommunications and Information Exchange between Systems – Local and Metropolitan Area Network – Specific requirements Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications. 2005

[53] IEEE Standard 802.1X-2001. IEEE Standard for Local and metropolitan area networks – Port-Based Network Access Control. Czerwiec 2001
[54] ISO 7498-2:1989 – Information processing systems – Open Systems Interconnection – Basic Reference Model – Part 2: Security Architecture. 1989
[55] ISO/IEC 11770-1:1996, Security Techniques – Key Management – Part 1: Framework. 1996
[56] Jarociński, M.: *Błędy w transmisji danych*. Pomoce dydaktyczne. Zeszyt 37. Instytut Telekomunikacji PW. 1980
[57] Kahn, D.: *The Codebreakers. The Comprehensive History of Secret Communication from Ancient Times to the Internet*. The Macmillan Company. Nowy Jork. 1967
[58] Kamath, V., Palekar, A., Wodrich, M.: *Microsoft's PEAP version 0 (Implementation in Windows XP SP1)*. IETF draft. Lipiec 2002
[59] Karn, P.: *MACA – A New Channel Access Method for Packet Radio*. Materiały: ARRL/CRRL Amateur Radio 9th Computer Networking Conference. 1990. str. 134-140
[60] Karygiannis, T., Owens, L.: *Wireless Network Security. 802.11, Bluetooth and Handheld Devices*. NIST Pub 800-48. Listopad 2002
[61] Kochut, A., Vasan, A., Shankar, A., Agrawala, A.: *Sniffing Out the Correct Physical Layer Capture Model in 802.11b*. Materiały: 12th IEEE International Conference on Network Protocols (ICNP 2004). Berlin (Niemcy). 5-8 października 2004
[62] Kong, Z., Tsang, D., Bensaou, B., Gao, D.: *Performance Analysis of IEEE 802.11e Contention-Based Channel Access*. IEEE Journal on Selected Areas in Communications, Vol. 22, No. 10. Grudzień 2004. str. 2095-2106
[63] Krätzer, C., Dittmann, J., Lang, A., Kühne, T.: *WLAN Steganography: a First Practical Review*. Materiały: 8th ACM Multimedia and Security Workshop. Genewa (Szwajcaria). 26-27 września 2006
[64] Kühne, T.: *Design und Implementierung von Steganographie in WLANs.* Otto-von-Guericke-Universität Magdeburg, praca magisterska (Diplomarbeit). 2006
[65] Lampson, B.: *A Note on the Confinement Problem*. Communications of the ACM, 16:10. Październik 1973. str. 613-615
[66] Lau, S.: *An Analysis of Terrorist Groups' Potential Use of Electronic Steganography*. SANS Security Essentials GSEC Practical Assignment. Version 1.3. 18 lutego 2003. URL: http://www.sans.org/reading_room/whitepapers/stenganography/554.php
[67] Liang, S., Ming-Yi, W.: *Protecting IEEE 802.11 Wireless LANs against the FCS False Blocking Attack*. Materiały: 11th International Conference on Parallel and Distributed Systems (ICPADS'05). Fukuoka (Japonia). Lipiec 2005. str. 723-729
[68] Lin, Y., Wong, V.: *Saturation Throughput of IEEE 802.11e EDCA Based on Mean Value Analysis*. Materiały: IEEE Wireless Communications and Networking Conference (WCNC). Las Vegas (Stany Zjednoczone). Kwiecień 2006
[69] Llamas, D., Allison, C., Miller, A.: *Covert Channels in Internet Protocols: A Survey.* Materiały: 6th Annual Postgraduate Symposium about the Convergence of Telecommunications, Networking and Broadcasting. Czerwiec 2005
[70] Lopez-Aguilera, E., Heusse, M., Rousseau, F., Duda, A., Casademont, J.: *Evaluating Wireless LAN Access Methods in Presence of Transmission Errors*. Materiały: IEEE INFOCOM. Barcelona (Hiszpania). 23-29 kwietnia 2006
[71] Lucena, N., Pease, J., Yadollahpour, P., Chapin, S.: *Syntax and Semantics-Preserving Application-Layer Protocol Steganography*. Materiały: 6th Information Hiding Workshop. Toronto (Kanada). 23-25 maja 2004
[72] Moskowitz, I., Chang, L., Newman, R.: *Capacity is the Wrong Paradigm*. Materiały: NSPW 2002 – New Security Paradigms Workshop. Virginia Beach (Stany Zjednoczone). 23-16 września 2002. str.114-126

[73] Murdoch, S., Lewis, S.: *Embedding Covert Channels into TCP/IP*. Materiały: 7th Information Hiding Workshop, Barcelona (Hiszpania). 6-8 czerwca 2005. LNCS 3727. str. 247-261
[74] Newsham, T.: *Cracking WEP Keys*. Materiały: BlackHat 2001
[75] Ni, Q., Li, T., Turletti, T., Xiao, Y.: *Saturation Throughput Analysis of Error-Prone 802.11 Wireless Networks*. Wiley Journal of Wireless Communications and Mobile Computing (JWCMC), Vol. 5, Issue 8. Grudzień 2005. str. 945-956
[76] NIST FIPS PUB 186-2: *Digital Signature Standard*. National Institute of Standards and Technology, U.S. Department of Commerce. 27 stycznia 2000
[77] NIST FIPS PUB 197: *Advanced Encryption Standard (AES)*. National Institute of Standards and Technology, U.S. Department of Commerce. 26 listopada 2001
[78] Nowicki, K., Woźniak, J.: *Przewodowe i bezprzewodowe sieci LAN*. Oficyna Wydawnicza Politechniki Warszawskiej. Warszawa. 2003
[79] Parnas, D.: *On the Criteria to Be Used in Decomposing Systems Into Modules*. Communications of the ACM. Grudzień 1972
[80] Patel, S.: *Analysis of EAP-SIM Session Key Agreement*. Lista pocztowa EAP. 29 maja 2003. URL: http://www.drizzle.com/~aboba/EAP/AnalyisOfEAP.pdf
[81] Petitcolas, F., Anderson, R., Kuhn, M.: *Information Hiding – A Survey*. Materiały: IEEE Special Issue on Protection of Multimedia Content. Lipiec 1999
[82] Pfitzmann, B.: *Information Hiding Terminology – Results of an Informal Plenary Meeting and Additional Proposals*. Materiały: First International Workshop on Information Hiding. 30 maja-1 czerwca 1996, LNCS 1174. str. 347-350
[83] Rappaport, T.: *Wireless Communications: Principles & Practice – 2nd edition*. Prentice Hall. 2002
[84] Rigney, C., Willens, S. i in.: *Remote Authentication Dial In User Service (RADIUS)*. IETF Request for Comments: 2865. Czerwiec 2000
[85] Rowland, C.: *Covert Channels in the TCP/IP Protocol Suite*. Tech. Rep. 5. FirstMonday, Peer-Reviewed Journal on the Internet. Lipiec 1997
[86] Sbrusch, R.: *Network Covert Channels: Subversive Confidentiality*. University of Houston-Clear Lake. Maj 2006
[87] Simmons, G.: *The Prisoners' Problem and the Subliminal Channel*. Materiały: Crypto'83. 1984. str 51-67
[88] Song, L., Ephremides, A.: *A Covert Channel in MAC Protocols Based on Splitting Algorithms*. Materiały: IEEE WCNC 2005 – Wireless Communications and Networking Conference. Nowy Orlean (Stany Zjednoczone). 13-17 marca 2005. str. 1168-1173
[89] Song, L., Ephremides, A.: *A Network Layer Covert Channel in Ad-hoc Wireless Networks*. Materiały: IEEE SECON 2004 – First Annual IEEE Communications Society Conference. Santa Clara (Stany Zjednoczone). 4-7 października 2004. str. 88-96
[90] Specification of the Bluetooth System Version 1.2. 5 listopada 2003
[91] Specification of the Bluetooth System Version 2.0 + EDR [vol 0]. 4 listopada 2004
[92] Stanley, D., Walker, J., Aboba, B.: *Extensible Authentication Protocol (EAP) Method Requirements for Wireless LANs*. IETF Request for Comments: 4017. Marzec 2005
[93] Stubblefield, A., Ioannidis, J., Rubin, A.: *Using the Fluhrer, Mantin, and Shamir Attack to Break WEP*. AT&T Labs Technical Report TD-4ZCPZZ. Revision 2. Sierpień 2001
[94] Szafran, P.: *Steganografia w lokalnych sieciach bezprzewodowych*. Praca magisterska (pod kierunkiem K. Szczypiorskiego). Politechnika Warszawska. Wydział Elektroniki i Technik Informacyjnych. 2004
[95] Szczypiorski, K., Cabaj, K., Margasiński, I.: *Analiza zagrożeń i ochrona danych w sieciach bezprzewodowych*. Instytut Telekomunikacji PW na zlecenie Instytutu

Łączności w ramach Programu Wieloletniego – Rozwój telekomunikacji i poczty w dobie społeczeństwa informacyjnego. Raport Techniczny. Listopad 2005

[96] Szczypiorski, K., Margasiński, I.: *Trendy zabezpieczeń w bezprzewodowych sieciach lokalnych*. Materiały: VIII Krajowa Konferencja Zastosowań Kryptografii Enigma'2004. Warszawa. 10-13 maja 2004. str. 245-257

[97] Szczypiorski, K., Szafran, P.: *Sposób steganograficznego ukrywania i przesyłania danych dla sieci telekomunikacyjnych ze współdzielonym medium transmisyjnym oraz układ formowania ramek warstwy sterowania dostępem do medium*. Zgłoszenie wynalazku nr P 359660. Politechnika Warszawska. 2003

[98] Szczypiorski, K.: *Bezpieczeństwo lokalnych sieci bezprzewodowych IEEE 802.11*. Materiały: VI Krajowa Konferencja Zastosowań Kryptografii Enigma'2002. Warszawa. 15-17 maja 2002. str. 173-181

[99] Szczypiorski, K.: *HICCUPS – system ukrytej komunikacji dla "zepsutych" sieci*. Materiały: VII Krajowa Konferencja Zastosowań Kryptografii Enigma'2003. Warszawa. 12-14 maja 2003. str. 247-253

[100] Szczypiorski, K.: *HICCUPS: Hidden Communication System for Coruppted Networks*. Materiały: The Tenth International Multi-Conference on Advanced Computer Systems ACS'2003. Międzyzdroje. 22-24 października 2004. str. 31-40

[101] Szczypiorski, K.: *Steganografia sieciowa: ukryte kanały czy anomalie?*. Materiały: III Krajowa Konferencja Bezpieczeństwa Biznesu. Warszawa. 22-23 listopada 2004

[102] Szczypiorski, K.: *Steganografia w sieciach TCP/IP*. Materiały: VI Krajowa Konferencja Bezpieczeństwa Sieciowego. Warszawa. 15-16 października 2003. str. 8-13

[103] Szczypiorski, K.: *System steganograficzny dla sieci o współdzielonym medium*. Materiały: Krajowe Sympozjum Telekomunikacji KST 2003. Bydgoszcz. 10-12 września 2003. Tom B. str. 199-205

[104] Takahashi, T.: *WPA Passive Dictionary Attack Overview*. 2004. URL: http://www.tinypeap.com/docs/WPA_Passive_Dictionary_Attack_Overview.pdf

[105] Tay, Y., Chua, K.: *A Capacity Analysis for the IEEE 802.11 MAC Protocol*. Wireless Networks, Vol. 7, No. 2. Marzec 2001. str. 159-171

[106] The Network Simulator – *ns-2*. URL: http://nsnam.isi.edu/nsnam/index.php/Main_Page

[107] US Department of Defence. *Trusted Computer System Evaluation Criteria (Orange Book)*. DOD 5200.28-STD. 26 grudnia l985

[108] VanBelleghem, D.: *No Parking Anytime – Protecting Your WAP from War Driving*. Materiały: Netsec 2003. Listopad 2003

[109] Walker, J., Chaplin, C., Qi, E., Ptasinski, H., Li, S.: *802.11i Overview*. Dokument IEEE 802.11-04/0123r1. Luty 2005

[110] Walker, J.: *IEEE 802.11i Standard Improves Wireless LAN Security*. Technology@Intel Magazine. Maj 2005

[111] Walker, J.: *Unsafe at Any Key Size; An Analysis of the WEP Encapsulation*. Dokument IEEE 802.11-00/362. Październik 2000

[112] Whiting, D., Housley, R., Ferguson, N.: *Counter with CBC-MAC (CCM)*. IETF Request for Comments: 3610. Wrzesień 2003

[113] Wi-Fi Alliance. WPA Home Page. URL: http://www.wi-fi.org/OpenSection/protected_access_archive.asp

[114] Wi-Fi Alliance. WPA2 Home Page. URL: http://www.wi-fi.org/OpenSection/protected_access.asp

[115] Willig, A., Kubisch M., Hoene, C., Wolisz, A.: *Measurements of a Wireless Link in an Industrial Environment using an IEEE 802.11-Compliant Physical Layer*. IEEE Transactions on Industrial Electronics, Vol. 43, No. 6. Grudzień 2002. str. 1265-1282

[116] Wolf, M.: *Covert Channels in LAN Protocols*. Materiały: LANSEC'89 – Workshop on Local Area Network Security. 1989. str. 91-101
[117] *World's Longest Wi-Fi Connection Made by The Swedish Space Corporation*. Informacja dla prasy. URL: http://www.alvarion.com/presscenter/pressreleases/3171/
[118] Wright, J.: *Detecting Wireless LAN MAC Address Spoofing*. Styczeń 2003. URL: http://www.rootsecure.net/content/downloads/pdf/wlan_macspooof_detection.pdf
[119] Wright, J.: *Weaknesses in LEAP Challenge/Response*. Materiały: Defcon 2003
[120] Wu, H., Peng, Y., Long, K., Cheng, S., Ma, J.: *Performance of Reliable Transport Protocol over IEEE 802.11 Wireless LAN: Analysis and Enhancement*. Materiały: IEEE INFOCOM`02. Czerwiec 2002
[121] Xiao, Y.: *A Simple and Effective Priority Scheme for IEEE 802.11*. IEEE Communication Letters Vol. 7 No. 2. Luty 2003
[122] Xiao, Y.: *Performance Analysis of IEEE 802.11e EDCF under Saturation Conditions*. Materiały: IEEE ICC. Paryż (Francja). Czerwiec 2004. str. 170-174
[123] Ziouva, E., Antonakopoulos, T.: *CSMA/CA Performance under High Traffic Conditions: Throughput and Delay Analysis*. Computer Communications, Vol. 25, Luty 2002. str. 313-321

Data ostatniego korzystania z podanych w bibliografii URL: 15 sierpnia 2006.

Wykaz skrótów

3G	*Third Generation*
AAA	*Authentication, Authorization and Accounting*
ACK	*Acknowledgment*
AER	*ACK Error Rate*
AES	*Advanced Encryption Standard*
AKA	*Authentication and Key Agreement*
AMI	*Alternate Mark Inversion*
AODV	*Ad-hoc On-Demand Distance Vector Routing*
ARP	*Address Resolution Protocol*
BAN	*Body Area Network*
BER	*Bit Error Rate*
BPSK	*Binary Phase Shift Keying*
BSS	*Basic Service Set*
CBC	*Cipher-Block Chaining*
CBC-MAC	*CBC Message Authentication Code*
CBR	*Constant Bit Rate*
CCM	*Counter mode with CBC-MAC*
CCMP	*CCM Protocol*
CRC	*Cyclic Redundancy Code*
CSMA	*Carrier Sense Multiple Access*
CSMA/CA	*Carrier Sense Multiple Access with Collision Avoidance*
CSMA/CD	*Carrier Sense Multiple Access with Collision Detection*
CTR	*Counter Mode*
CTS	*Clear To Send*
CW	*Contention Window*
DA	*Destination Address*
DBPSK	*Differential Binary Phase Shift Keying*
DCF	*Distributed Coordination Function*
DES	*Data Encryption Standard*
DIFS	*DCF InterFrame Space*
DQPSK	*Differential Quadrature Phase Shift Keying*
DRM	*Digital Rights Management*
DSS	*Digital Signature Scheme*
DSSS	*Direct Sequence Spread Spectrum*
EAP	*Extensible Authentication Protocol*
ECB	*Electronic Code Book*
EDCF	*Enhanced Distributed Coordination Function*
EIFS	*Extended InterFrame Space*
ERP	*Extended Rate PHY*
ESS	*Extended Service Set*
FCFS	*First Come First Served*
FCS	*Frame Check Sequence*
FER	*Frame Error Rate*
FHSS	*Frequency Hopping Spread Spectrum*
FIPS	*Federal Information Processing Standards*
FMS	*Fluhrer-Mantin-Shamir*
GPRS	*General Packet Radio Service*
GSM	*Global System for Mobile Communication*

GTC	*Generic Token Card*
HICCUPS	*Hidden Communication System for Corrupted Networks*
HTTP	*Hypertext Transfer Protocol*
IBSS	*Independent Basic Service Set*
ICV	*Integrity Check Value*
ID	*Identifier*
IEC	*International Electrotechnical Commission*
IEEE	*Institute of Electrical and Electronics Engineers*
IETF	*Internet Engineering Task Force*
IP	*Internet Protocol*
IPsec	*IP Security*
IR	*Infrared*
ISN	*Initial Sequence Number*
ISO	*International Organization for Standardization*
IT	Instytut Telekomunikacji
IV	*Initialization Vector*
KSA	*Key Scheduling Algorithm*
LAN	*Local Area Networks*
LEAP	*Lightweight EAP*
LFSR	*Linear Feedback Shift Register*
LLC	*Link Layer Control*
MAC	1: *Medium Access Control* 2: *Message Authentication Code*
MACA	*Multiple Access with Collision Avoidance*
MACAW	*Multiple Access with Collision Avoidance for Wireless*
MAN	*Metropolitan Area Network*
MIC	*Message Integrity Code*
M-QAM	*M-Quadrature Amplitude Modulation*
MS	*Microsoft*
MSCHAP	*Microsoft Challenge Handshake Authentication Protocol*
NACK	*Negative-acknowledgment*
NIST	*National Institute of Standards and Technology*
NM	nowy model
ns-2	*Network Simulator version 2*
OFDM	*Orthogonal Frequency Division Multiplexing*
OSI	*Open System Interconnection*
PAN	*Personal Area Network*
PCF	*Point Coordination Function*
PEAP	*Protected EAP*
PHY	*Physical Sygnalling*
PLCP	*PHY Layer Convergence Procedure*
PMD	*PHY Medium-Dependent*
PMK	*Pairwise Master Key*
PN	*Packet Number*
PPDU	*PLCP Protocol Data Unit*
PPP	*Point-to-Point Protocol*
PRF	*Pseudo-Random Function*
PRNG	*Pseudo-Random Number Generator*
PSDU	*PLCP Service Data Unit*
PSK	*Pre-Shared Key*

PUB	*Publication*
PW	Politechnika Warszawska
QPSK	*Quadrature Phase-Shift Keying*
RA	*Receiver Address*
RADIUS	*Remote Authentication Dial In User Service*
RC4	*Ron's Code 4*
RFC	*Request for Comments*
RM	*Reference Model*
RP	Rzeczpospolita Polska
RPN	ruch przenoszony w warunkach nasycenia
RSA	*Rivest Shamir Adleman*
RSNA	*Robust Security Network Association*
RTS	*Request to Send*
SA	*Source Address*
SIFS	*Short InterFrame Space*
SIM	*Subscriber Identity Module*
SLRC	*Station Long Transmission Retry*
SNR	*Signal-to-Noise Ratio Signal-to-Noise Ratio*
SSH	*Secure Shell*
SSID	*Service Set IDentifier*
SSRC	*Station Short Transmission Retry*
STA	*STAtion*
TA	*Transmitter Address*
TCP	*Transport Control Protocol*
TG	*Task Group*
TK	*Temporary Key*
TKIP	*Temporal Key Integrity Protocol*
TLS	*Transport Layer Security*
ToS	*Type of Service*
TSC	*TKIP Sequence Counter*
TTLS	*Tunneled TLS*
UDP	*User Datagram Protocol*
UMTS	*Universal Mobile Telecommunications System*
URL	*Uniform Resource Locator*
UWB	*Ultra Wideband*
WCDMA	*Wideband Code Division Multiple Access*
WEP	*Wired Equivalent Privacy*
Wi-Fi	*Wireless Fidelity*
WLAN	*Wireless LAN*
WPA	*Wi-Fi Protected Access*
WPA2	*Wi-Fi Protected Access 2*
XOR	*Exclusive OR*