Kierunek:	Nazwa zajęć:	Ocena:
TIN	LABORATORIUM SIECI BEZPRZEWODOWYCH	

Nr. ćwiczenia:	Tytuł ćwiczenia:
5	Konfiguracja i badanie sieci bezprzewodowych standardu IEEE 802.11b i 802.11g

Termin:	Data wykonania ćwiczenia:	Nr. grupy:
Czwartek TN 13:15	07.12.2017 r.	1

Osoby wykonujące ćwiczenie:	Podpisy:
Łukasz Gielec	Łukasz Gielec
Marcin Kołodziej	Marcin Kołodziej
Igor Michalski	Igor Michalski

Sprawozdanie wykonał:	Igor Michalski
Data wykonania sprawozdania:	21.12.2017r.
Sprawozdanie sprawdził:	

Oświadczam, że zapoznałem/łam się ze niniejszym sprawozdaniem i uważam je za poprawnie wykonane:

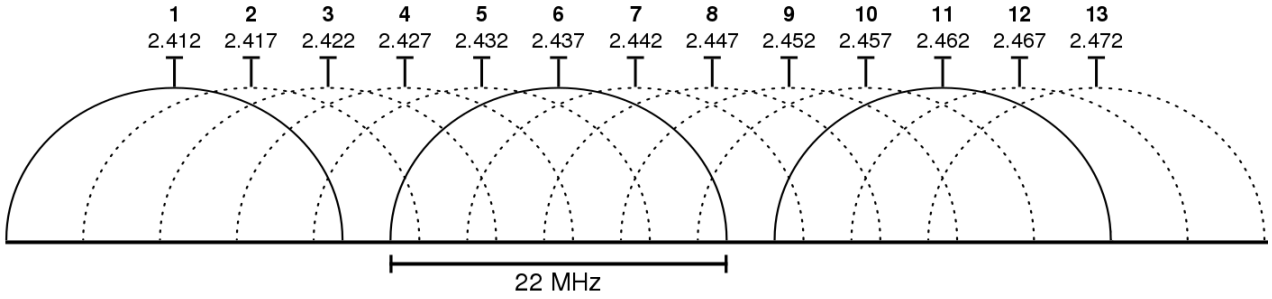
Marcin Kołodziej Łukasz Gielec

Oświadczam/y iż poniższe sprawozdanie zostało wykonane przeze mnie/nas samodzielnie:

Igor Michalski

1 Wstęp

Podczas laboratorium badane są przepustowości standardów IEEE 802.11b oraz 802.11g. Odnoszą się one do warstwy fizycznej (PHY) oraz podwarstwy kontroli dostępu do medium (MAC) w warstwie łącza modelu ISO OSI. Oba standardy zostały w pełni ukończone - ich rozwój nie jest kontynuowany, a obecnie pierwszy z nich praktycznie całkowicie odszedł z użycia. Dla 802.11b/g w Polsce zdefiniowano 13 kanałów w paśmie 2,4 - 2,4835 GHz. Każdy z kanałów ma szerokość 22 MHz. Częstotliwości środkowe kanałów przesunięte są względem siebie o 5 MHz, co powoduje nakładanie się wielu kanałów. Jedynie kanały 1, 6 oraz 11 są od siebie oddalone na tyle, że nie występuje ich nakładanie się, a nawet występuje odstęp 3 MHz pomiędzy granicznymi częstotliwościami kanałów.



Rysunek 1: Schemat kanałów dostępnych w Europie dla IEEE 802.11b/g.

IEEE 802.11b posiada dwie metody rozpraszania widma pozwalające na osiąganie różnych przepływności. Pierwsza z nich to DSSS (Direct Sequence Spread Spectrum), polegająca na mnożeniu sygnału przez szybkozmienny sygnał kodowy. Pozwala to na rozproszenie (poszerzenie) widma sygnału i tym samym uniknięcie zakłóceń wąskopasmowych. Przy DSSS stosowane są modulacje DBPSK pozwalająca osiągnąć przepływność 1 Mbps oraz DQPSK zwiększająca przepływność do 2 Mbps. Większe szybkości udało się osiągnąć poprzez zastosowanie CCK (Complementary Code Keying), które działa jak DSSS, jednak wykorzystuje sprawniejsze ciągi kodowe. Pozwala to na osiągnięcie 5.5 Mbps przy modulacji DBPSK oraz 11 Mbps dla DQPSK.

IEEE 802.11g można traktować jako rozwinięcie standardu 802.11b. Dostępne są szybkości 1, 2, 5,5, 11 Mbps realizowane jak w 802.11b oraz dzięki zastosowaniu Orthogonal Frequency Division Multiplexing (OFDM) i innych modulacji: 6, 9 Mbps z modulacją BPSK, 12, 18 Mbps z modulacją QPSK, 24, 36 Mbps modulowane z użyciem 16-QAM oraz 48 i 54 Mbps przy wykorzystaniu modulacji 64-QAM.

W trybie kompatybilności z 802.11b preambuła i nagłówek nadawane są z szybkością 1 Mbps. W trybie „g only" preambuła i nagłówek przesyłane są z szybkością 6 Mbps. Wpływ długości preambuły na przepływność podlega badaniu podczas laboratorium.

Oba standardy implementują Automatic Rate Fallback (ARF), co pozwala na automatyczną adaptację szybkości w zależności od minimalnej mocy odebranej. Zmniejszenie szybkości transmisji przy obniżeniu się poziomu mocy pozwala na utrzymanie stałej stopy błędów Bit Error Rate (BER) na poziomie 10^{-5}. W przypadku niskiego poziomu mocy i wymuszonej wysokiej szybkości transmisji, stopa błędów może ulec gwałtownemu wzrostowi, co obniży jakość transmisji i będzie wymuszało kolejne retransmisje obniżające rzeczywistą przepustowość.

W dalszej części laboratorium badany jest wpływ długości pakietu UDP na przepustowość. Na tym etapie szybkość ustawiona jest na maksymalną teoretyczną wartość równą 54 Mbps. Urządzenie po odebraniu określa czy otrzymany z wyższej warstwy pakiet może zostać przesłany w jednej ramce. Maksymalna długość wynosi 2 346 B. Jeśli nie, to następuje jego fragmentacja. Zgodnie z protokołem CSMA/CA i DCF - rozproszoną funkcją koordynującą (w praktyce jedynie ta jest im-

plementowana w urządzeniach powszechnego użytku) urządzenie zgłasza gotowość przez wysłanie pakietu Ready To Send (RTS). Jeśli po okresie Short Interframe Space (SIFS) otrzyma pakiet Clear To Send (CTS), to rozpoczyna transmisję ramek. Po każdej z nich, po odczekaniu SISF, oczekuje na potwierdzenie ACK od odbiorcy. Następnie po odczekaniu kolejnego SISF, wysyła następny fragment nie rywalizując ponownie o dostęp do medium. Po otrzymaniu ACK po ostatnim fragmencie czeka okres Distributed IFS (DIFS).

Podobne pomiary przeprowadza się dla wpływu fragmentacji warstwy MAC na przepustowość. Powyżej zadanego rozmiaru, każda ramka jest dzielona i przesyłana we fragmentach. Większa ilość przesyłanych ramek wymaga częstszego oczekiwania na potwierdzenie ACK. Jednak dzięki takiemu dzieleniu i ponownemu łączeniu po stronie odbiorcy można uzyskać mniejszą ilość błędów transmisji.

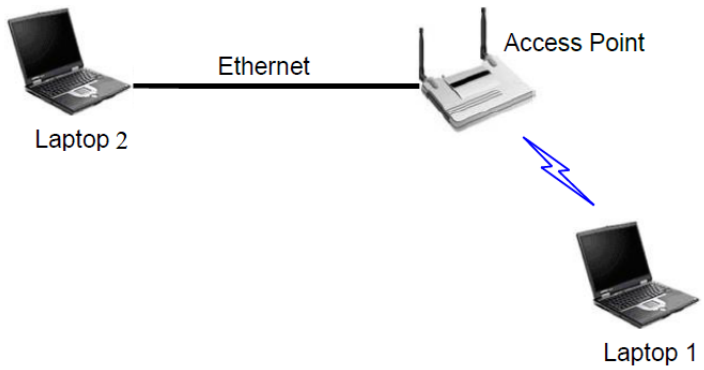
Badaniu podlega także wpływ procedury RTS/CTS na przepustowość. RTS jest wysyłany, kiedy stacja chce zacząć nadawać. Inne stacje w zasięgu wstrzymują się wtedy z rozpoczęciem transmisji, a nadawca oczekuje na CTS od adresata RTS. Odbiorca wysyłając CTS informuje stacje w swoim zasięgu o transmisji, którą będzie prowadził. Wykorzystanie RTS/CTS pozwala na uniknięcie zjawiska stacji ukrytej.

Omawiane standardy pozwalają także na uwierzytelnianie kluczem współdzielonym Wired Equivalent Privacy (WEP). Jest to standard szyfrowania powstały w 1999 r. i obecnie bardzo prosty do złamania. Klucz 40 lub 104 bitowy łączony jest z 24 bitowym wektorem inicjującym. Tak otrzymany 64 lub 128 bitowy klucz podawany jest na wejście generatora liczb pseudolosowych, który na tej podstawie generuje pseudolosową sekwencję kluczową, która wykorzystywana jest do wykonania XOR zarówno z wektorem integralności jak i danymi. Metoda ta pozwala na otrzymanie 4 różnych kluczy.

2 Sprzęt i konfiguracja

Podczas laboratorium zestawiono sieć złożoną z:

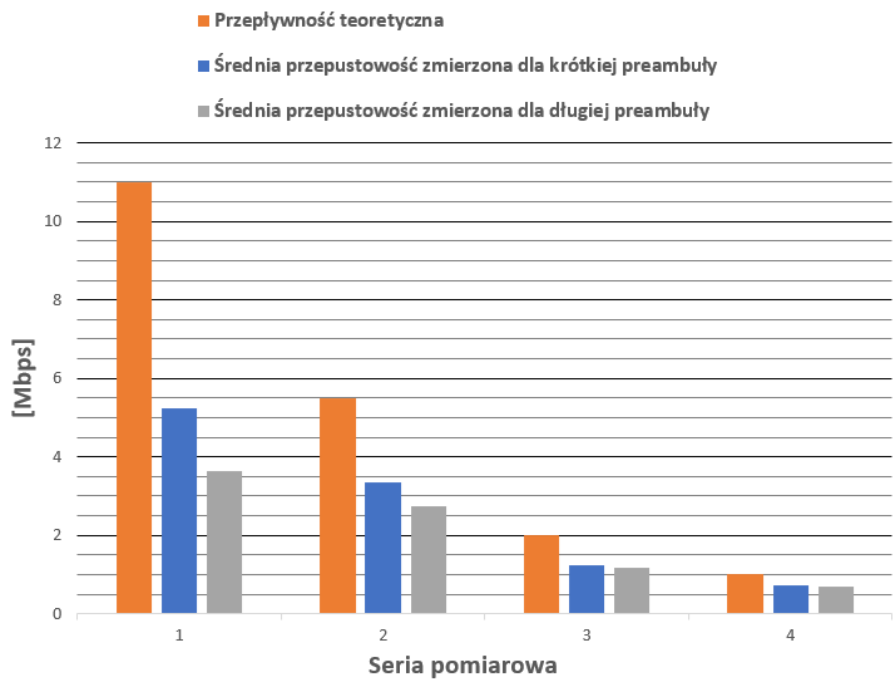
- laptopa (192.168.1.110/24) łączącego się bezprzewodowo z punktem dostępowym (AP),
- laptopa (192.168.1.4/24) połączonego kablem Ethernet z AP,
- AP (192.168.1.1/24).



Rysunek 2: Stanowisko laboratoryjne.

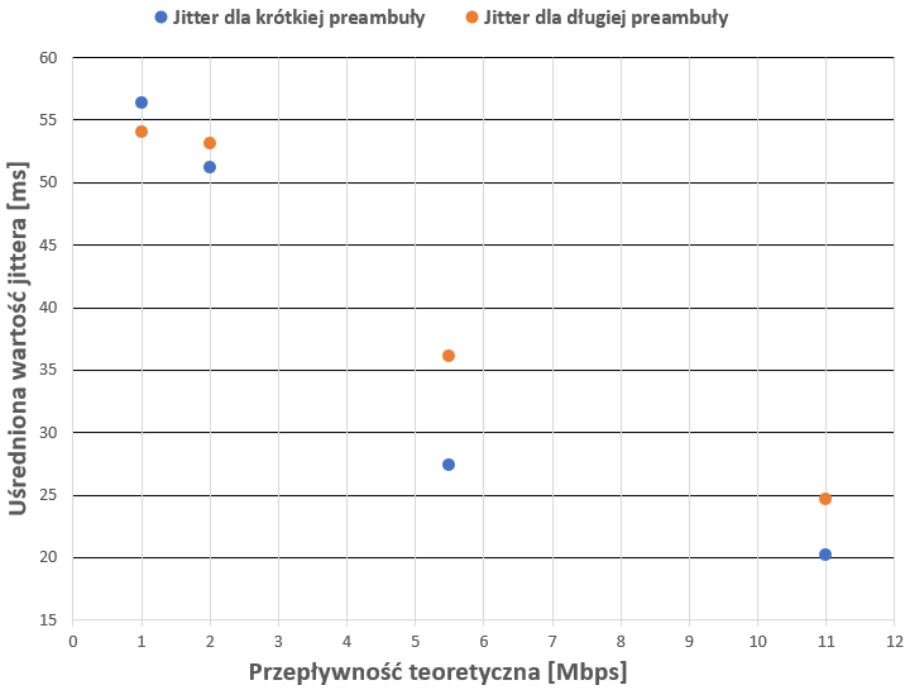
3 Wyniki pomiarów

3.1 Badanie wpływu długości preambuły



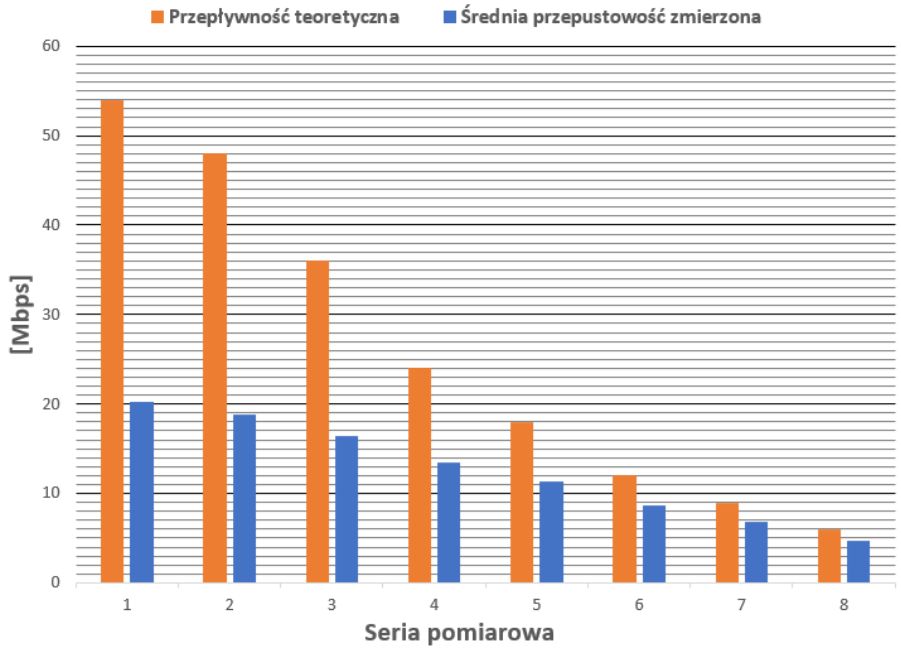
Rysunek 3: Porównanie dla 802.11b przepływności teoretycznej z osiągniętą dla niej średnią przepustowością dla trzech pomiarów w każdej z serii przy zastosowaniu kolejno krótkiej i długiej preambuły.

Z rys. 3 jednoznacznie wynika, że zwiększanie długości preambuły zmniejsza przepustowość łącza. Wynik ten jest obserwowany wyraźniej dla większych przepływności bitowych i prawie niezauważalny dla przepływności poniżej 2 Mbps.



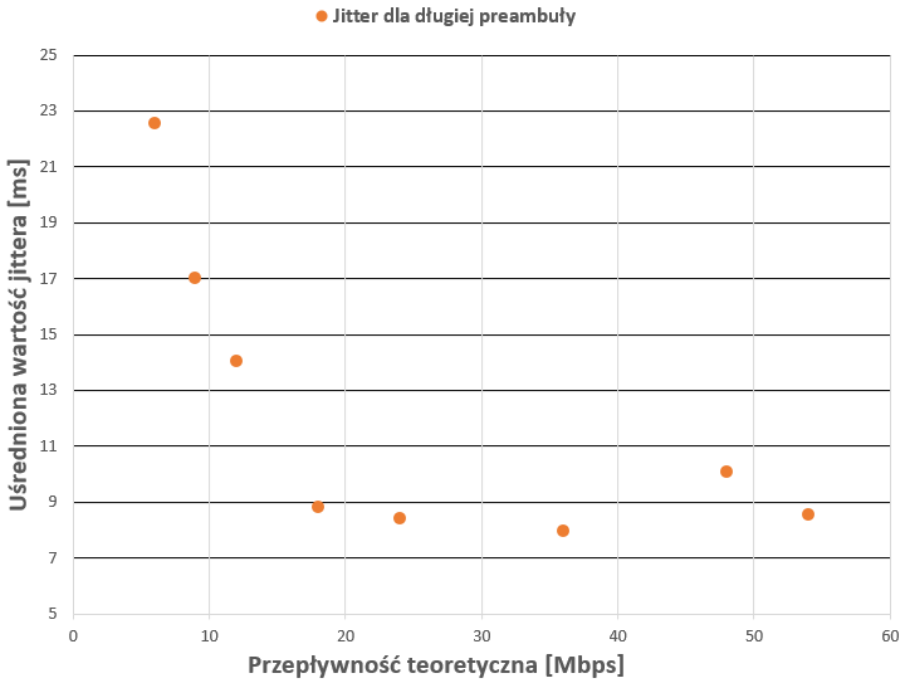
Rysunek 4: Porównanie wartości jittera dla 802.11b przy różnych przepływnościach, dla krótkiej i długiej preambuły.

Wartości jittera dla niskiej przepływności są większe o 2 ms dla preambuły krótkiej, po czym dla pozostałych badanych przepływności przyjmują wartości mniejsze, niż wartości jittera przy wykorzystaniu długiej preambuły.



Rysunek 5: Porównanie dla 802.11g przepływności teoretycznej z osiągniętą dla niej średnią przepustowością dla trzech pomiarów w każdej z serii przy zastosowaniu długiej preambuły.

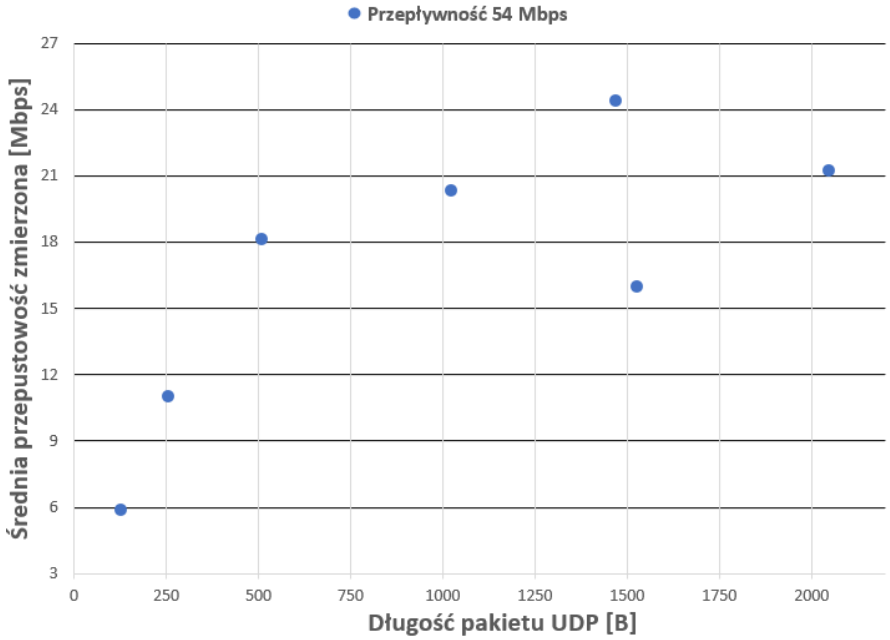
Wartości przepustowości na rys. 5 są znacząco niższe niż przepływność. Różnica ta maleje wraz ze zmniejszaniem przepływności w kolejnych seriach pomiarowych.



Rysunek 6: Wartości jittera dla 802.11g przy różnych przepływnościach, dla długiej preambuły.

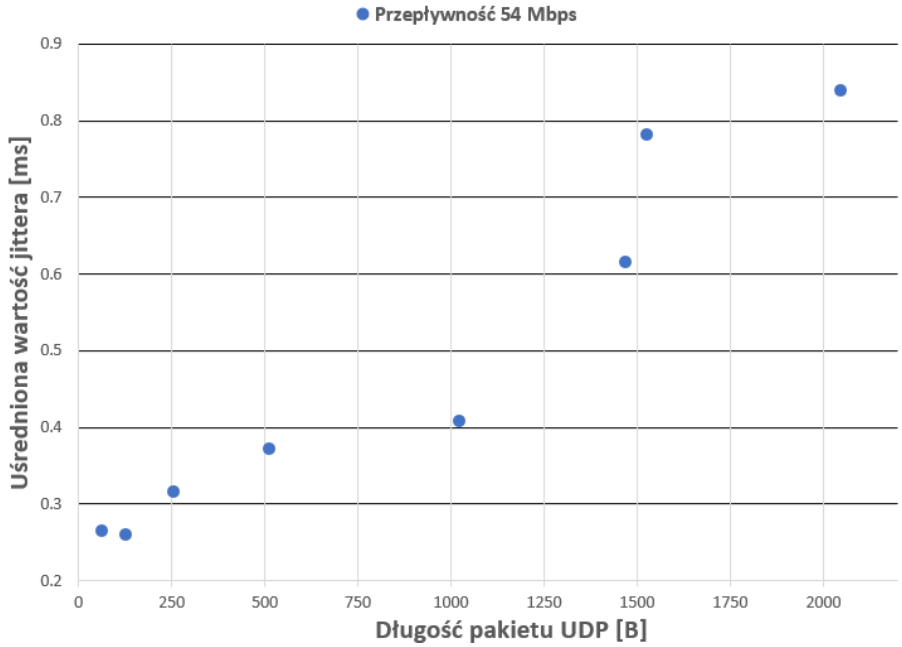
Wartości jittera najwyższe są dla najniższej przepływności. Po zwiększeniu przepływności do 17,5 Mbps, jitter zaczyna oscylować wokół wartości 9 ms. Ten stan utrzymuje się do końca zakresu pomiarowego.

3.2 Badanie wpływu fragmentacji pakietów UDP na przepustowość (802.11g)



Rysunek 7: Średnia wartość przepustowości w funkcji długości pakietu UDP, przy ustalonej przepływności 54 Mbps.

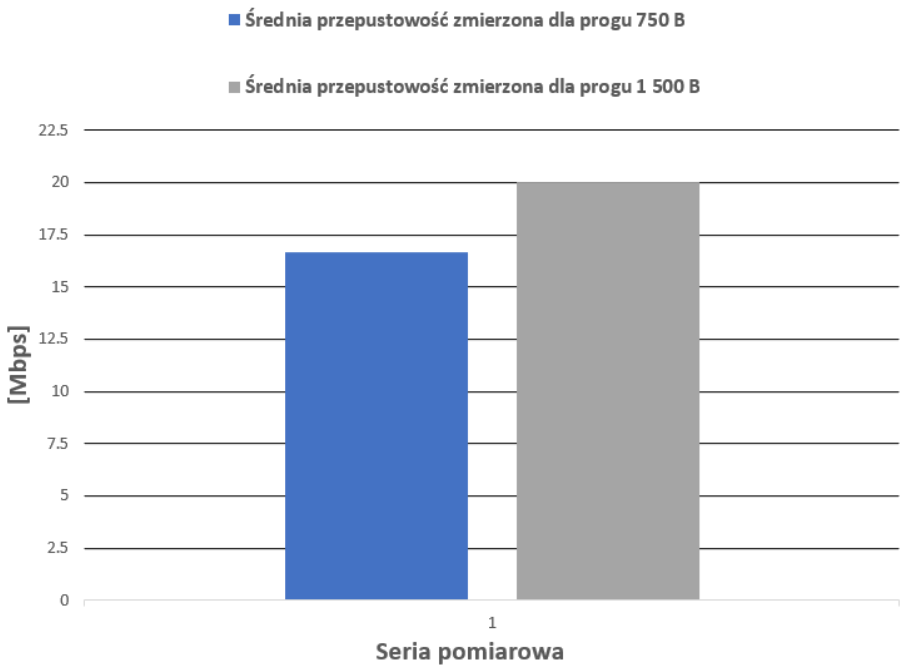
Przepustowość w kanale rośnie wraz ze wzrostem długości pakietu UDP do momentu, w którym następuje fragmentacja (pakiet UDP przekracza 1470 B). Obniża to przepustowość o 9 Mbps, po czym znów obserwowany jest wzrost, który trwać będzie do przekroczenia kolejnej wielokrotności dopuszczalnej długości pakietu.



Rysunek 8: Wartości jittera przy stałej przepływności 54 Mbps i zmiennej długości pakietu UDP.

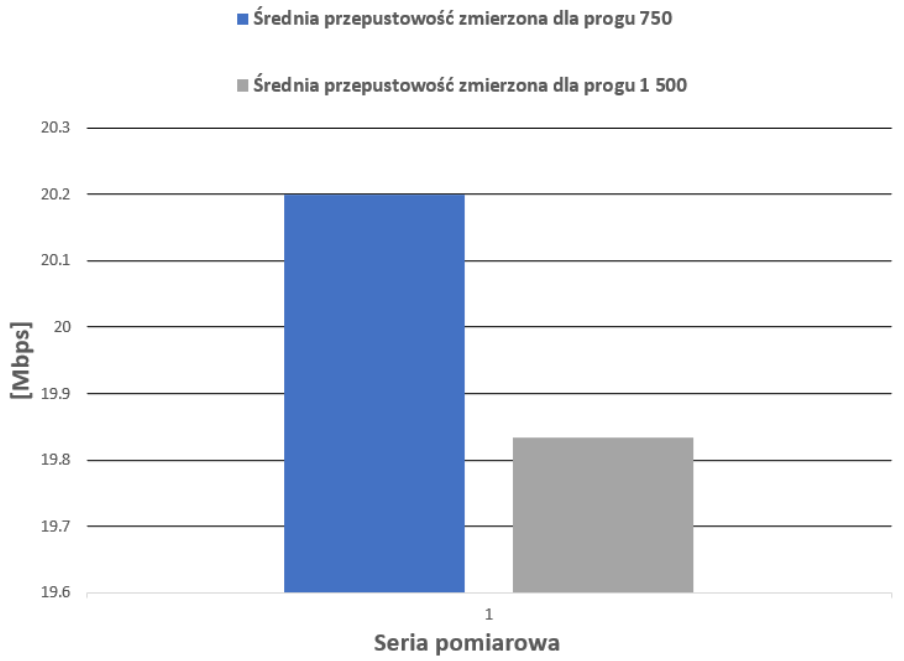
Wraz ze wzrostem długości pakietu jitter powolnie rośnie. Nagły wzrost wartości jittera obserwowany jest, gdy dochodzi do fragmentacji pakietu, po czym następuje jego dalszy powolny wzrost, który będzie trwał, aż do przekroczenia kolejnej wielokrotności 1470 B.

4 Badanie wpływu fragmentacji MAC na przepustowość (802.11g)



Rysunek 9: Średnia wartość przepustowości dla dwóch wartości progu fragmentacji warstwy MAC przy stałej przepływności równej 54 Mbps.

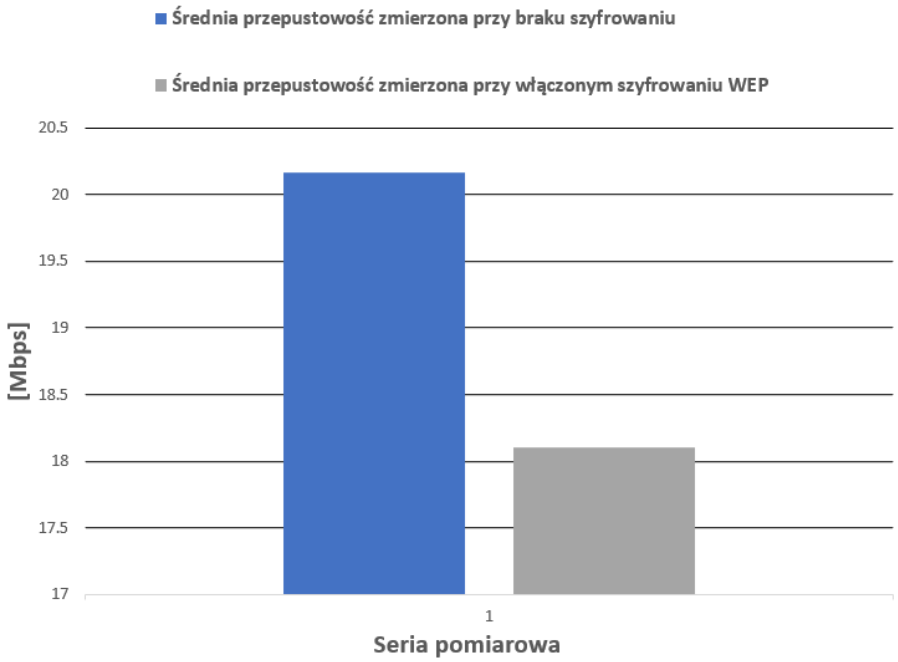
Zwiększenie progu fragmentacji zwiększa przepustowość kanału. Jest to spowodowane rzadszymi przerwami w nadawaniu, w których nadajnik oczekuje na potwierdzenie ACK.



Rysunek 10: Średnia wartość przepustowości dla dwóch wartości progu RTS/CTS przy stałej przepływności równej 54 Mbps.

Wartości przepustowości są bardzo zbliżone. Różnica wynosi zaledwie niecała 0,4 Mbps.

4.1 Badanie wpływu szyfrowania WEP na przepustowość

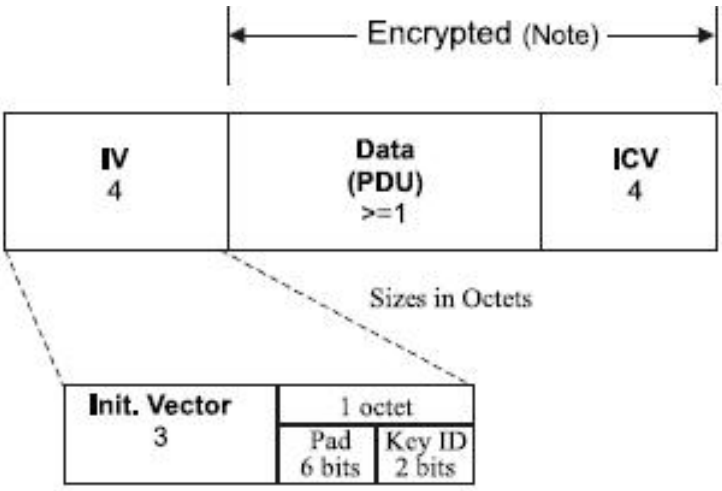


Rysunek 11: Średnia wartość przepustowości z wyłączonym oraz włączonym szyfrowaniem WEP przy stałej przepływności równej 54 Mbps.

Włączenie szyfrowania powoduje spadek przepustowości o 2 Mbps. Związane jest to z koniecznością przesyłania dodatkowych danych w każdej ramce.

5 Wnioski

- Wszystkie wartości średnie brane były z trzech pomiarów.
- Przepustowości zawsze są niższe od przepływności, jednak różnica jest tym większa, im większa jest przepływność.
- Stosowanie krótkiej preambuły poprawia przepustowość oraz obniża jitter.
- Zwiększanie przepływności powoduje zmniejszenie wartości jittera.
- Długość pakietu jest optymalna, kiedy jest równa maksymalnej długości ramki lub jej całkowitej wielokrotności. Dla tych długości również jitter przyjmuje wartości optymalne. Podczas laboratorium wymuszono fragmentację dla pakietów o długości większej niż 1 470 B.
- Zwiększenie progu fragmentacji w warstwie MAC pozwala na zwiększenie przepustowości.
- Dla badanych wartości progowych RTS/CTS zauważono znikomą różnicę przepustowości. Wynosiła ona niecałe 0,4 Mbps na korzyść progu 750.
- Włączenie szyfrowania WEP obniżyło przepustowość. Wiąże się to z koniecznością przesyłania większej ilości danych (struktura danych w ramce szyfrowanej przedstawiona na rys. 12).



Rysunek 12: Struktura ramki 802.11 z wektorem inicjującym (IV) i zaszyfrowanym polem danych.