

Antoni Masiukiewicz
Akademia Finansów i Biznesu Vistula – Warszawa

WYKORZYSTANIE ANALIZATORA TCPDUMP W SYMULATORZE NS-3 DO ANALIZY RUCHU W SIECIACH WI-FI

Streszczenie

Symulator NS-3 jest zaawansowanym narzędziem do analizy sieci. Pozwala na symulację szeregu sieci bezprzewodowych i posiada rozbudowany moduł dotyczący sieci Wi-Fi. Model do przeprowadzenia analizy danego zagadnienia musi być przygotowany indywidualnie. Do pozyskania informacji na temat ruchu w sieci w trakcie symulacji możliwe jest wykorzystanie analizatora *tcpdump*. Jest on przydatny również dlatego, że symulator NS-3 jest w zasadzie przeznaczony do pracy w środowisku Linux, a *tcpdump* jest domyślnie instalowany w systemach operacyjnych Linux. W artykule przetestowano możliwość wykorzystania *tcpdump* przy analizie zjawiska interferencji w modelu *wifi-simple-interference*.

Słowa kluczowe: interferencje, NS-3, symulator sieciowy, analizator pakietów.

Kody JEL: L86

Wstęp

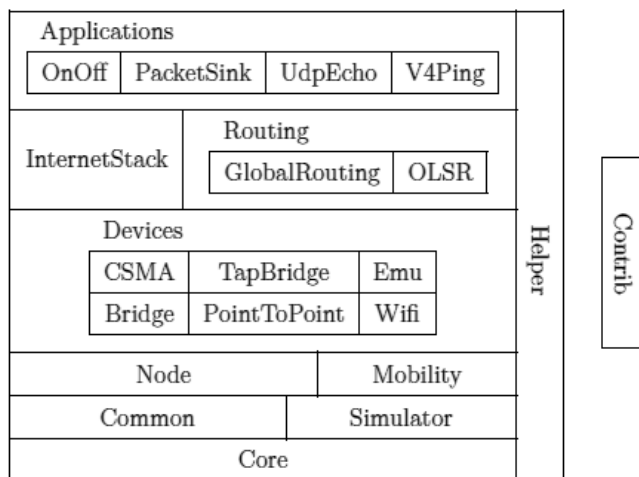
Symulator NS-3 to następca symulatora NS-2. Prace nad projektem rozpoczęto w 2006 roku, a pierwsza stabilna wersja została udostępniona w 2008 roku. Celem prac było stworzenie narzędzia spełniającego aktualne zapotrzebowania badawcze, przy czym rozwiązanie miało spełniać warunki *open-source* tak, aby umożliwić jego nieskrępowany rozwój. W symulatorze NS-3 zrezygnowano z możliwości tworzenia skryptów w języku OTcl pozostawiając jedynie opcje C++. W celu ułatwienia implementacji nowych modeli w strukturze symulatora jest ona w obszarze *hardware* i *software* jak najbardziej zbliżona do rozwiązań stosowanych w praktyce. Wprowadzono możliwość wykonywania obliczeń w sytuacji, gdy obok urządzeń wirtualnych pracują urządzenia fizyczne. Było to możliwe dzięki 100% zgodności struktury wykorzystywanych w symulacjach pakietów z rzeczywistymi pakietami. Korzystanie z NS-3 wymaga wiedzy w takich kwestiach, jak kolejgowanie, modelowanie i programowanie z wykorzystaniem skryptu. Powoduje to, że w zasadzie symulator NS można stosować do badań naukowych. Wersja NS3 jest rozpoznawana jako podstawowe narzędzie

do testowania sieci LAN, WAN i Wi-Fi (The NS-3 network Simulator 2016; Ryu i in. 2008).

Model ogólny zastosowany w symulatorze pokazany na schemacie 1 ma charakter warstwowy (Bingmann 2009). Modele opisujące poszczególne procesy są zawarte w warstwach Core, Common i Simulator. Warstwa Core jest wykorzystywana praktycznie we wszystkich projektach w ramach NS-3 i wykorzystuje obiekty umieszczone w bazie Object. Warstwa Common zajmuje się kreowaniem i zarządzaniem pakietami. Narzędzia są umieszczone w rozwiązaniach Header i Trailer. DataRate pozwala na sterowanie przepływnością. Moduł Simulator pozwala na realizację scenariuszy w ramach prowadzonych obliczeń. Istotnym elementem symulatora jest funkcja Time. Pozwala ona na precyzyjne taktowanie w trakcie symulacji, a rozdzielczość określenia czasu wynosi 1 nanosekundę.

Node jest bardzo ważnym elementem NS-3. Za pomocą Node wprowadzamy obiekty, które mogą wytwarzać i odbierać różne komunikaty. Node zawiera oprócz odpowiednika fizycznego urządzenia nazywanego NetDevice zestaw narzędzi do komunikacji w postaci stosu podobnie jak w modelu ISO. Wyróżnia się dwie podstawowe warstwy – protokołów i aplikacji.

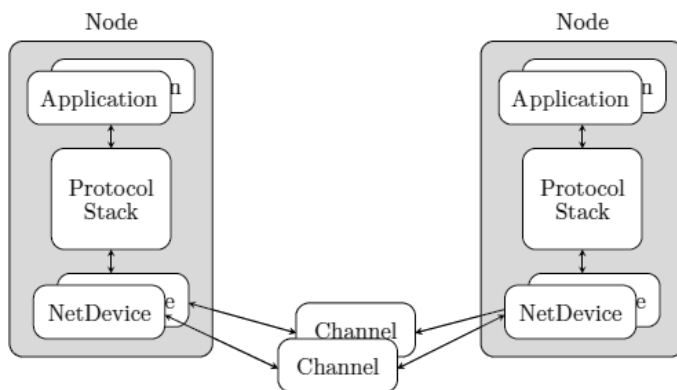
Schemat 1. Model warstwowy symulatora NS-3



Źródło: Bingmann (2009).

Urządzenia nawiązują kontakt na poziomie NetDevice z wykorzystaniem kanału komunikacyjnego przewodowego lub bezprzewodowego zgodnie ze schematem 2.

Schemat 2. Sposób komunikacji w NS-3



Źródło: jak w schemacie 1.

Funkcja Application inicjuje sesje komunikacyjne. Aby informacja mogła przemieszczać się w górę i w dół stosu konieczne było opracowanie odpowiednich interfejsów pomiędzy poszczególnymi warstwami. Interfejsy są podobne do stosowanych w praktyce. Obsługują one również funkcje kolejkowania. Interfejsy bazują na rozwiązaniu BSD sockets API. Trzy możliwości (PacketSocket, TCPSocket i UDPSocket) są wykorzystywane do transmisji pakietów. Cztery podstawowe aplikacje w NS-3 pozwalające na wysłanie pakietów to: OnOffApplication, UdpEchoClient i UdpEchoServer oraz V4Ping. Funkcja helper upraszcza projektowanie poprzez zastosowanie powielania raz zdefiniowanego urządzenia lub procesu. W symulatorze wbudowane są narzędzia typu helper, m.in.: WifiPhyStateHelper, InterferenceHelper (Lertpratchya 2017; Saeed 2017; Kostaros 2017).

Tcpdump jest analizatorem ruchu sieciowego, czasami dla tego typu oprogramowania używa się nazwy angielskiej sniffer (TCPDUMP 2017). *Tcpdump* służy do śledzenia komunikacji w sieciach. Pozwala na pełne lub selektywne przechwytywanie, wyświetlanie i zapisywanie do pliku pakietów TCP/IP oraz innych protokołów transmitowanych lub odbieranych w sieci. *Tcpdump* pracuje na większości platform uniksowych, jak np. Linux, Solaris, BSD, Mac OS X, HP-UX i AIX. Na tych systemach *tcpdump* opiera się na bibliotece libpcap, której funkcja pcap_loop() odpowiedzialna jest za przechwytywanie pakietów, a pcap_breakloop() zaterminację przechwytywania. Analizator jest domyślnie instalowany w większości dystrybucji Linuxa.

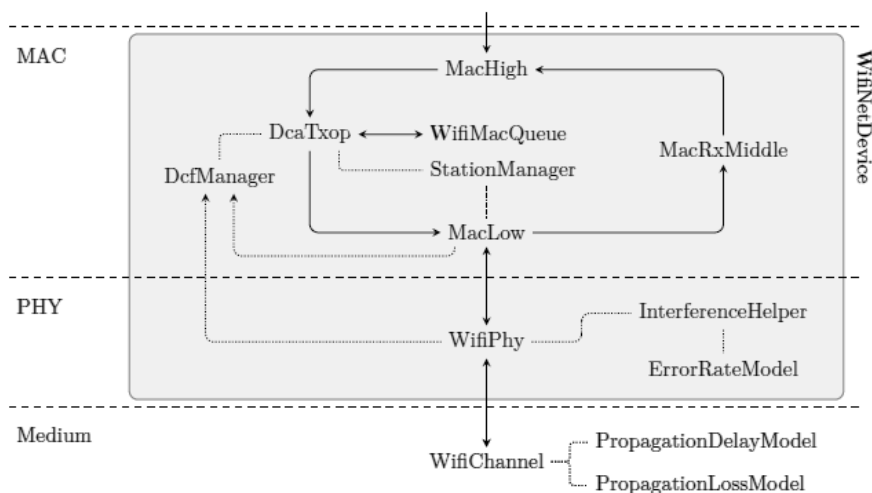
W artykule przetestowano możliwość wykorzystania *tcpdump* przy analizie zjawiska interferencji w modelu *wifi-simple-interference*.

Modelowanie sieci Wi-Fi w NS-3

Jednym z najważniejszych NetDevice w NS-3 jest urządzenie typu Wi-Fi. Stanowi ono największy moduł w NS-3. WifiNetDevice implementuje rozwiązania standardu IEEE 802.11. Pozwala na wykonanie symulacji z różnymi wersjami MAC i PHY.

Architektura standardu IEEE 802.11 zaimplementowana w NS-3 została wykonana na podstawie rozwiązania zastosowanego w symulatorze YANS (Yet Another Network Simulator) przez Mathieu Lacagei Toma Hendersona (Lacage, Henderson 2006). Model zastosowany w NS-3 jest bardzo rozbudowany i zawiera 75 elementów i funkcji. Uproszczona struktura modelu została pokazana na schemacie 3.

Schemat 3. Architektura modelu Wi-Fi w symulatorze NS-3



Źródło: The ns-3 network simulator (2016).

W modelu możemy wyróżnić trzy podstawowe warstwy: medium, PHY, MAC (NS-3 Model Library 2017). Na schemacie pokazano drogę przesyłania pakietu za pomocą linii ciągłej. Linie przerywane wskazują funkcje dodatkowe współpracujące z submodułami. Budowa analizatora ma charakter modułowy, w związku z czym twórcy symulatora często wykorzystują określenie moduł, przy czym trzeba pamiętać, że moduły mogą leżeć na różnych poziomach. Przedstawiony proces jest uproszczony i nie zawiera wszystkich procedur i funkcji. W pierwszej kolejności pakiet jest przekazywany z warstwy aplikacji do modułu MacHigh umieszczonego w warstwie MAC WifiNetDevice przez standardowy interfejs. MacHigh Nazywana również WifiMac odpowiada za testowanie kanału i połączenie z AP. W ramach MacHigh można wyróżnić trzy

funkcje: AdhocWifiMac, staWifiMac i apWifiMac, odpowiedzialne za zarządzanie różnymi procesami. staWifiMac odpowiada za bezprzewodowe stacje STA nie obsługujące opcji QoS które wysyłają komunikaty żądania połączenia z AP. AP są symulowane przez apWifiMac, który kontroluje również grupę stacji połączonych z danym AP. Z kolei adhocWifiMac pozwala na tworzenie sieci bez udziału punktów dostępowych. Wszystkie wymienione procesy warstwy MacHigh kierują pakiety do jednego modułu DcaTxop. Moduł ten, wspierany przez funkcje DcfManager implementuje zasady dostępu zgodne z algorytmem DCF standardu 802.11 zaimplementowanym w warstwie MAC. DcaTxop zawiera licznik czasu T_{BO} (*back off time*), który pozwala na generowanie wartości Contention Window wykorzystywanych do zarządzania kolejną stacją oczekujących na dostęp. Żądanie dostępu jest wysuwane przez funkcje DcfManager. Po otrzymaniu dostępu do kanału pakiet jest przesyłany przez warstwę MacLow po otrzymaniu numeru nadawanego przez MacTxMiddle i przechodzi proces fragmentacji wtedy, gdy jest to konieczne. StationManager wspierający DcaTxop obsługuje proces segmentacji oraz mechanizm RTS/CTS. DcaTxop obsługuje jeden pakiet od początku aż do przesłania dalej. W tym czasie inne pakiety, które nadeszły są przechowywane w WifiMacQueue. Station Manager kontroluje i przechowuje parametry dotyczące takich transmisji, jak: szybkość transmisji, komunikaty RTS/CTS, liczniki krótkich i długich retransmisji, sygnalizacja błędów w odebranych pakietach. Informacja o błędach jest uwzględniana przy wyborze prędkości transmisji z wykorzystaniem różnych dostępnych w NS-3 algorytmów. Oprócz stałej przepływności i managera wykorzystującego warunki teoretyczne mamy do dyspozycji takie algorytmy, jak: ARF, AARF, AMRR, Onoe i RRAA. Wybrane warunki transmisji są udostępniane DcaTxop i MacLow na żądanie.

DcfManager zarządza wieloma DcaTxop i nadzoruje proces udzielania dostępu do medium zgodnie z zasadami obowiązującymi w standardzie 802.11. Warstwa MacLow po otrzymaniu pakietu inicjuje sesje RTS/CTS i oczekuje na ACK, jeżeli jest taka konieczność. W warstwie PHY model WifiPhy ustala parametry odbiornika/nadajnika pracującego w kanale bezprzewodowym. Korzystając z YansWifiPhy możliwa jest ocena poziomu szumu białego (AWGN - Average White Gaussian Noise), a InterferenceHelper pozwala na ocenę szumu/interferencji pochodzących od innych stacji. Do kanału radiowego w warstwie Medium jest dołączonych szereg warstw WifiPhy od stacji skojarzonych z danym punktem dostępowym. Dwie funkcje wbudowane w WifiChannel, a mianowicie PropagationDelayModel i PropagationLossModel wspomagają symulację opóźnienia w kanale i rozkładu mocy w kanale. W symulatorze zaimplementowano 15 modeli propagacji (NS-3 Model Library 2017), m.in. takich jak: Cost231PropagationLossModel, FixedRssLossModel, FriisPropagationLossModel itd. (Freeman 2007).

Dane dotyczące obu wymienionych parametrów są przechowywane w WifiPhy każdej stacji. Poziom mocy odebranej pozwala na ocenę przez WifiPhy możliwości poprawnego odbioru pakietu. Proces wspiera funkcja ErrorRateModel, która przetwarza dane dotyczące stanu kanału radiowego, rozkładu mocy i szumów/interferencji dla każdej stacji (Proakis 2001). Bezbłędnie odebrane pakiety są przechowywane przez MacLow. MacLow po otrzymaniu komunikatu RTS wysyła potwierdzenie CTS po upływie odcinka czasu SIFS. Pakiety danych oraz ramki zarządzające są następnie przesyłane z MacLow do MacRxMiddle, gdzie są usuwane duplikaty oraz następuje defragmentacja. Po tych zabiegach gotowe pakiety są przesyłane do MacHigh, a następnie do warstwy aplikacji. Dokładny opis symulatora znajduje się w dokumentacji oraz w szeregu tutoriali na stronie <http://www.nsnam.org>. Najnowszy tutoriali pochodzi z 2017 roku (NS-3 Library 2017).

Funkcjonalność analizatora tcpdump

Tcpdump jest popularnym analizatorem sieciowym. Pozwala na analizę komunikacji w sieci oraz przechwytywanie pakietów nadawanych i odbieranych. Pakiety mogą być odbierane na wybranym lub wszystkich interfejsach. Możliwe jest zwracanie wyników działań analizatora bezpośrednio do wiersza poleceń lub po odpowiedniej konfiguracji do pliku. Istotną zaletą *tcpdump* jest możliwość konstruowania filtrów. Analizator po zakończeniu przechwyty pakietów raportuje następujące statystyki: liczbę przechwyconych pakietów, liczbę pakietów wynikających z zastosowanej filtracji oraz liczbę pakietów odrzuconych przez kernel np. z powodu wyczerpania bufora. Uruchomienie analizatora *tcpdump* następuje z wiersza poleceń. Polecenie *tcpdump* ma następująca składnie:

```
tcpdump [ -AbDDefhHIJKILnNOpqStuUvxX# ] [ -B buffer_size ] [ -c count ]
[ -C file_size ] [ -G rotate_seconds ] [ -F file ]
[ -i interface ] [ -j tstamp_type ] [ -m module ] [ -M secret ] [ --number ]
[ -Q in|out|inout ] [ -r file ] [ -V file ] [ -s snaplen ]
[ -T type ] [ -w file ] [ -W filecount ] [ -E spi@ipaddr algo:secret,... ]
[ -y datalinktype ] [ -z postrotate-command ] [ -Z user ]
[ --time-stamp-precision=tstamp_precision ] [ --immediate-mode ] [ --version ]
[ expression ]
```

Za pomocą liter oznaczono większość dostępnych funkcji. W tabeli 1 przedstawiono wybrane atrybuty analizatora.

Tabela 1. Wybrane atrybuty analizatora *tcpdump*

Atrybut	Opis
-C <i>file_size</i>	Pozwala na dopasowanie rozmiaru pliku do objętości pobranych pakietów.
-D --list-interfaces	Pokazuje listę interfejsów sieciowych dostępnych w systemie, na których może odbierać pakiety <i>tcpdump</i> .
-e	Pokazanie nagłówków związanych z linkiem w sieciach 802.11.
-F <i>file</i>	<i>file</i> pozwala na umieszczenie wyrażenia pozwalającego na filtrację wyników.
-h --help	Polecenia <i>tcpdump</i> i <i>libpcap</i> .
-i <i>interface</i> --interface=interface	Nasłuch na wybranym interfejsie. Domyślnie wybiera najniższy numer. Opcja <i>any</i> powoduje przechwytywanie na wszystkich interfejsach.
-I --monitor-mode	Ustawia interfejs w tryb <i>monitor mode</i> dostępny jedynie w wybranych systemach operacyjnych dla sieci w standardzie 802.11.
-j <i>tstamp_type</i> --time-stamp-type=tstamp_type	Ustawia typ znacznika czasu.
-J --list-time-stamp-types	Pokazuje listę znaczników czasu dostępnych dla danego interfejsu.
--time-stamp-precision=tstamp_precision	Ustawia dokładność atrybutu <i>tstamp_precision</i> . Dokładność szczególnie na poziomie nsek. Jest uzależniona od parametrów oprogramowania i urządzeń. Możliwe jest ustawienie micro dla rozdzielczości na poziomie mikrosekund i nano dla nanosekund.
-n	Nie przekształca adresów w nazwy.
-r <i>file</i>	Czyta informacje z pliku <i>file</i> .
-T <i>type</i>	Wymusza zastosowanie wybranego gotowego filtra z listy np.: <i>aodv</i> , <i>carp</i> , <i>pgm</i> , <i>rtp</i> , <i>snmp</i> itd.
-tt	Wstawia znacznik czasu do każdej linii w sekundach i częściach ułamkowych sekundy.
-ttt	Wstawia różnicę czasu pomiędzy kolejnymi liniami z rozdzielczością mikrosekund.
-w <i>file</i>	Zapisuje do pliku <i>file</i> .
<i>expression</i>	Pozwala na filtrację pakietów zgodnie z zadaną formułą.

Źródło: TCPDUMP... (2017).

W trakcie symulacji z wykorzystaniem NS-3 pakiety są zapisywane do pliku, a po jej zakończeniu można je przesłać na terminal korzystając z polecenia *tcpdump -r [nazwa_pliku]*. Analizator pozwala na uzyskanie informacji o poziomach mocy sygnałów nadawanych, poziomie szumów, adresach IP, protokołach oraz stempli czasowych tzn. identyfikuje czas rozpoczęcia nadawania oraz czas nadawania pakietów.

Model wifi-simple-interference

Do przeprowadzenia symulacji i analiz wykorzystano model *wifi-simple-interference.cc* dostępny w zasobach na stronie <http://www.nsnam.org> (www1).

Model zawiera trzy węzły w sieci bezprzewodowej w standardzie 802.11b. Jednym z węzłów jest Access Point dwa pozostałe stanowią stacje robocze. Jedna ze stacji komunikuje się z AP druga jest stacja zakłócająca, która nie widzi stacji pierwszej. Jest to sytuacja związana z wystąpieniem stacji ukrytej (*hidden terminal*). Szereg atrybutów modelu może być zmienianych adekwatnie do potrzeb symulacji. Lista wszystkich możliwych do zmiany atrybutów jest przesyłana na konsolę po uruchomieniu następującego polecenia:

```
./waf --run „wifi-simple-interference --help”
```

i zawiera parametry, które zestawiono w tabeli 2.

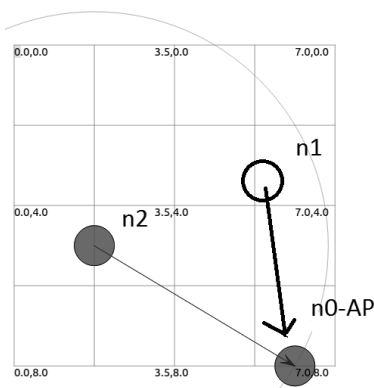
Tabela 2. Argumenty modelu wifi-simple-interference

Argument	Opis	Wartość domyślna
--phyMode [Mb/sek.]	Przepływność	DsssRate2Mbps
--Prss [dBm]	Moc odebrana sygnału n2	-80
--Irss [dBm]	Moc odebrana sygnału n1	-95
--delta [mikrosekundy]	Odstęp czasu pomiędzy wysłaniem sygnałów ze stacji n1 i n2 $\text{delta} = t1 - t2$	0
--PpacketSize [bit]	Rozmiar pakietu wysłanego ze stacji n2	1000
--IpacketSize [bit]	Rozmiar pakietu wysłanego ze stacji n12	1000
--verbose [false, true]	Lista wszystkich operacji wykonanych przez symulator	false

Źródło: (www1).

Stacje są rozłożone wzdłuż osi x zgodnie ze schematem 4.

Schemat 4. Lokalizacja stacji, gdzie n0-AP, n2-stacja nadająca, n1- stacja zakłócająca

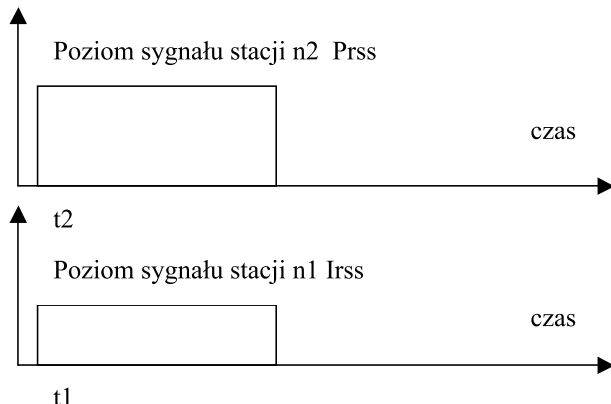


Źródło: opracowanie własne.

Możliwe jest przeprowadzenie analizy odbioru pakietów w funkcji poziomu mocy odebranej, stosunku sygnał szum oraz rozkładu pakietów na osi czasu.

Domyślnie pakiety są wysyłane w tym samym momencie. Na wykresie 1 pokazano układ startowy pakietów.

Wykres 1. Układ startowy pakietów



Źródło: opracowanie własne.

W oprogramowaniu modelu umieszczono polecenie pozwalające na śledzenie pakietów, *wifiPhy.EnablePcap* („*wifi-simple-interference*”, *devices*); w związku z powyższym możliwe jest odczytanie danych zawartych w pliku *wifi-simple-interference-o-o.pcap* przy wykorzystaniu komendy:

```
tcpdump -r wifi-simple-interference-0-0.pcap -nn -tt
```

Wyniki symulacji

W modelu, oprócz parametrów wymienionych w tabeli 2, ustawiono domyślnie m.in.: kanał nr 1, minimalny poziom stosunku sygnał/szum, który umożliwia odbiór pakietu równy 5 dB (Proakis 2001) oraz adres sieci 10.1.1.0. Przypisano następujące numery IP do poszczególnych węzłów: n0-10.1.1.1, n2-10.1.1.2 i n1-10.1.1.3. W trakcie symulacji zmieniano poziomy mocy Prss, Irss oraz odstęp pomiędzy pakietami na osi czasu. W zależności od poziomów mocy uzyskano trzy różne stany. Poniżej pokazano wyniki symulacji oraz informacje przechwycone przez analizator pakietów.

W pierwszej grupie symulacji zmieniano poziom mocy Prss w zakresie od -80 dBm do -97 dBm, pozostawiając poziom Irss=-95 dBm. W zakresie poziomu mocy Prss od -80 do -95 dBm możemy zaobserwować w kanale tylko 1 pakiet zidentyfikowany przez analizator jako pakiet pochodzący od stacji n2 o numerze IP 10.1.1.2. przy czym stosunek sygnał szum wynosi odpowiednio od 21dB do 6 dB.

```
antoni@antoni-VirtualBox:~/workspace/ns-allinone-3.25/ns-3.25$ ./waf --run
„wifi-simple-interference”
```

Primary packet RSS=-80 dBm and interferer RSS=-95 dBm at time offset=0 ms

Received one packet! Socket: 10.1.1.1 port: 80

```
antoni@antoni-VirtualBox:~/workspace/ns-allinone-3.25/ns-3.25$ tcpdump -r
wifi-simple-interference-0-0.pcap -nn -tt
```

reading from file wifi-simple-interference-0-0.pcap, link-type IEEE802_11_RADIO (802.11 plus radiotap header)

10.008704 10008704us tsft 1.0 Mb/s 2412 MHz 11b -80dB signal -101dB noise IP 10.1.1.2.49153 > 10.1.1.255.80: UDP, length 1000

```
antoni@antoni-VirtualBox:~/workspace/ns-allinone-3.25/ns-3.25$ ./waf --run
“wifi-simple-interference --Prss=-95”
```

Primary packet RSS=-95 dBm and interferer RSS=-95 dBm at time offset=0 ms

Received one packet! Socket: 10.1.1.1 port: 80

```
antoni@antoni-VirtualBox:~/workspace/ns-allinone-3.25/ns-3.25$ tcpdump -r
wifi-simple-interference-0-0.pcap -nn -tt
```

reading from file wifi-simple-interference-0-0.pcap, link-type IEEE802_11_RADIO (802.11 plus radiotap header)

10.008704 10008704us tsft 1.0 Mb/s 2412 MHz 11b -95dB signal -101dB noise IP 10.1.1.2.49153 > 10.1.1.255.80: UDP, length 1000

Gdy poziom mocy odebranej ze stacji n2 przez AP (n0) spada ponizej -95dBm analizator nie rejestruje zadnych pakietow.

```
antoni@antoni-VirtualBox:~/workspace/ns-allinone-3.25/ns-3.25$ ./waf --run
„wifi-simple-interference --Prss=-96”
```

Primary packet RSS=-96 dBm and interferer RSS=-95 dBm at time offset=0 ms

```
antoni@antoni-VirtualBox:~/workspace/ns-allinone-3.25/ns-3.25$ tcpdump -r
wifi-simple-interference-0-0.pcap - nn -tt
```

reading from file wifi-simple-interference-0-0.pcap, link-type IEEE802_11_RADIO (802.11 plus radiotap header)

Sytuacja ulega zmianie, gdy spadkowi mocy Prss towarzyszy wzrost mocy Irss. Jezeli Irss > Prss oraz spełnione są dwa warunki dotyczące stosunku sygnał szum : Prss/Pnoise < 5dB i Irss/Pnoise > 5dB. Wtedy pakiet pochodzący od n2 nie zostaje odebrany, natomiast analizator rejestruje pakiet pochodzący od n1 o numerze IP 10.1.1.3.

```
antoni@antoni-VirtualBox:~/workspace/ns-allinone-3.25/ns-3.25$ ./waf --run
„wifi-simple-interference --Prss=-98” --Irss=-90”
```

Primary packet RSS=-98 dBm and interferer RSS=-90 dBm at time offset=0 ms

```
antoni@antoni-VirtualBox:~/workspace/ns-`@antoni-VirtualBox:~/workspace/
ns-allinone-3.25/ns-3.25$
antoni@antoni-VirtualBox:~/workspace/ns-allinone-3.25/ns-3.25$ tcpdump -r
wifi-simple-interference-0-0.pcap -nn -tt
reading from file wifi-simple-interference-0-0.pcap, link-type IEEE802_11_RA-
DIO (802.11 plus radiotap header)
10.008704 10008704us tsft 1.0 Mb/s 2412 MHz 11b -90dB signal -100dB noise IP
10.1.1.3.49153 > 10.1.1.255.49000: UDP, length 1000
```

W tabeli 3 zestawiono wyniki symulacji.

Tabela 3. Wyniki symulacji

Pakiety przechwycone przez analizator (IP stacji nadającej)	Warunki: moc nadawania, stosunek sygnał/szum
10.1.1.2 (n2)	Prss>Irss, Prss/Pnoise* >5 dB
10.1.1.3 (n1)	Irss>Prss, Prss/Pnoise < 5dB, Irss/Pnoise>5 dB
brak	1/ Prss/Pnoise < 5 dB i Irss/Pnoise < 5 dB 2/ Prss=Irss

*Pnoise poziom mocy szumu w danym kanale radiowym

Źródło: opracowanie własne.

Jeżeli w symulacji zmienimy moment wysłania pakietu ze stacji n1 na osi czasu, to w stosunku do możliwych scenariuszy pokazanych w tabeli 3 pojawia się układ, w który oba pakiety są rejestrowane przez analizator, jak to pokazano poniżej.

```
antoni@antoni-VirtualBox:~/workspace/ns-allinone-3.25/ns-3.25$ ./waf --run
„wifi-simple-interference --delta=8705”
Primary packet RSS=-80 dBm and interferer RSS=-95 dBm at time offset=8705
ms
Received one packet! Socket: 10.1.1.1 port: 80
antoni@antoni-VirtualBox:~/workspace/ns-allinone-3.25/ns-3.25$ tcpdump -r
wifi-simple-interference-0-0.pcap -nn -tt
reading from file wifi-simple-interference-0-0.pcap, link-type IEEE802_11_RA-
DIO (802.11 plus radiotap header)
10.008704 10008704us tsft 1.0 Mb/s 2412 MHz 11b -80dB signal -101dB noise IP
10.1.1.2.49153 > 10.1.1.255.80: UDP, length 1000
10.017409 10017409us tsft 1.0 Mb/s 2412 MHz 11b -95dB signal -101dB noise IP
10.1.1.3.49153 > 10.1.1.255.49000: UDP, length 1000
```

W tabeli 4 zestawiono możliwe scenariusze po uwzględnieniu uzmiennienie parametru *delta*.

Tabela 4. Scenariusze przechwyty pakietów dla zmiennego parametru *delta*

Pakiety przechwycone przez analizator (IP stacji nadającej)	Warunki: moc nadawania, stosunek sygnał/szum	Warunki : delta [μsek.]
10.1.1.2 (n1)	Prss>Irss, Prss/Pnoise >5 dB	0-∞
10.1.1.2 (n1) i 10.1.1.3 (n2)	Prss/Pnoise > 5dB, Irss/Pnoise>5 dB	>8704+1*
brak	1/ Prss/Pnoise < 5 dB i Irss/Pnoise < 5 dB 2/ Prss=Irss	0-∞
10.1.1.3 (n2)	1/Irss>Prss, Prss/Pnoise < 5dB, Irss/Pnoise>5 dB 2/ Irss/Pnoise>5 dB, Prss/Pnoise < 5dB	0-8704 >8705

*8704 μsek. – czas na przesłanie pakietu o długości 1000 bitów z prędkością 1Mb/sek.

Źródło: jak w tabeli 3.

Podsumowanie

Zastosowanie analizatora jako narzędzia wspierającego analizę wyników symulacji w symulatorze NS-3 pozwala na uwzględnienie w analizie dodatkowych parametrów, takich jak adresy IP stacji i AP, poziomy mocy, poziomy szumu i stosunki sygnał szum. Dodatkowo możliwe jest przeanalizowanie zdarzeń na osi czasu. W zależności od wybranej opcji możliwe jest zastosowanie znaczników czasu w różnym formacie, a analiza zjawisk na osi czasu zwiększa liczbę możliwych scenariuszy symulacji. Oczywiście, wiele funkcji można zaimplementować pisząc odpowiednie oprogramowanie, trzeba jednak pamiętać że *tcpdump* jest gotowym narzędziem o dużej funkcjonalności, a próba implementacji podobnej funkcjonalności doprowadziłaby do bardzo znaczącej rozbudowy modeli w NS-3.

Bibliografia

- Bingmann T. (2009), *Accuracy Enhancements of the 802.11 Model and EDCA QoS Extensions in ns-3*, Diploma Thesis at the Institute of Telematics Faculty of Computer Science University of Karlsruhe, Karlsruhe.
- Freeman R.L. (2007), *Radio System Design for telecommunications*, Wiley Interscience, John Wiley & Sons, New York.
- Kostaros K. (2017), *Introduction to NS-3*, <http://personal.ee.surrey.ac.uk/Personal/K.Katsaros/media/NS-3-Presentation-2013.pdf> [dostęp: 02.2017].
- Lertpratchya D. (2017), *WiFi Module in NS-3*, <https://www.nsnam.org/tutorials/consortium14/ns-3-training-session-5.pdf> [dostęp: 02.2017].
- Lacage M., Henderson T.R. (2006), *Yet another network simulator. In WNS2'06: Proceeding from the 2006 Workshop on ns-2: the IP network simulator*, ACM, New York.
- NS-3 Network Simulator, NS-3 Model Library, Release ns-3 dev, NS-3 Project (2017), February 01., <http://www.nsnam.org> [dostęp: 02.2017].

- Proakis J.G. (2001), *Digital Communications*, McGraw-Hill, New York.
- Ryu J., Lee J., Sung-Ju Lee, Kwon T. (2008), *Revamping the IEEE 802.11a PHY simulation models*. In *MSWiM '08: Proceedings of the 11th International Symposium on Modeling, Analysis and Simulation of Wireless and Mobile Systems*, ACM, New York.
- Saeed S.A.A. (2017), *NS-3 WiFi*, http://www.cs.ucr.edu/~ycao009/Teaching_files/Module%20Modification.pdf [dostęp: 02.2017].
- The ns-3 network simulator* (2016), <http://www.nsnam.org> [dostęp: 10.2016]
- TCPDUMP Section: User Commands (1) Updated: 2 February 2017 (2017), <http://www.tcpdump.org> [dostęp: 02.2017].
- (www1) https://www.nsnam.org/doxygen/hwif-simple-interference_8cc_source.html [dostęp: 02.2017].

Using TCPDUMP Analyzer in the NS-3 Simulator for Traffic Analysis in Wifi Networks

Summary

The NS-3 Simulator is a powerful tool for network analysis. It enables simulation of a number of wireless networks and has a developed module for Wi-Fi networks. In order to analyze the issue, the model must be prepared individually. To obtain information about the network traffic during the simulation it is possible to use the *tcpdump* packet analyzer. It is also useful because the NS-3 simulator is basically designed to work in a Linux environment, and *tcpdump* is installed by default on Linux operating systems. In this article, the author has tested the possibility of using *tcpdump* when analyzing the interference in the *wifi-simple-interference* model.

Key words: interference, NS-3, network simulator, packet analyzer.

JEL codes: L86

Artykuł nadesłany do redakcji w lutym 2017 roku.

© All rights reserved

Afiliacja:

dr Antoni Masiukiewicz

Akademia Finansów i Biznesu Vistula

Wydział Inżynierski

ul. Stokłosa 3

02-787 Warszawa

e-mail: a.masiukiewicz@vistula.edu.pl