Analiza zagadnienia sprawiedliwego dostępu do kanału radiowego realizowanego za pomocą modyfikacji parametrów okna współzawodnictwa w sieciach ad-hoc standardu IEEE 802.11e[1]

Szymon Szott, Marek Natkaniec, Andrzej R. Pach (e-mail: {szott, natkaniec, pach}@kt.agh.edu.pl)
Katedra Telekomunikacji Akademii Górniczo-Hutniczej – Kraków

STRESZCZENIE

Niniejsza praca dotyczy problemu stacji oszukujących na oknie współzawodnictwa w sieciach ad-hoc. W pracy przedstawiono, jak takie nieuczciwe stacje mogą wpływać na wydajność sieci standardu IEEE 802.11e. Podano przyczyny, które powodują, że sieci tego standardu są bardziej narażone na nieuczciwe zachowania stacji niż sieci dotychczasowych wersji standardu 802.11. Analizę symulacyjną wydajności sieci z nieuczciwymi stacjami przeprowadzono dla kilku scenariuszy. Wyniki badań pokazały, że nieuczciwa stacja może znacząco pogorszyć pracę sieci. W związku z tym zaproponowano opracowanie mechanizmów, które pozwoliłyby ograniczyć skutki nieuczciwej modyfikacji okna współzawodnictwa przez stacje w sieci standardu IEEE 802.11e.

ABSTRACT

Analysis of Fairness in Channel Access when Modifying Contention Window Parameters in IEEE 802.11e MANETs

This paper is related to the problem of node misbehaviour. The presented work determines how contention window cheating can influence the performance of ad-hoc networks based on the new IEEE 802.11e standard. It is explained why such networks are more prone to misbehaviour than previous 802.11 (other WiFi) standards. A simulation analysis has been carried out for several distinct scenarios. The presented results show that a misbehaving node can significantly decrease the network performance. Therefore, countermeasures to this problem need to be developed.

1. Wstęp

U podstaw prawidłowej, niczym niezakłóconej i wydajnej pracy mobilnej sieci ad-hoc MANETs (*mobile ad-hoc networks*) leży zasada wzajemnej uczciwej współpracy wszystkich tworzących ją stacji, z których każda jest jednocześnie terminalem i ruterem. Wydajność sieci MANET zależy przede wszystkim od tego, jak dobrze stacje tworzące jej węzły współpracują ze sobą. Zagrożenie nieuczciwym zachowaniem stacji (węzła sieci) pojawia się wówczas, gdy stacja zdecyduje się, a dokładniej jej użytkownik, na zwiększenie, na przykład, swojej przepustowości lub czasu życia baterii kosztem współpracy z grupą. Wykrycie takiego zachowania któregoś z węzłów i następnie skuteczne przeciwdziałanie mu jest bardzo istotne dla całości pracy sieci ad-hoc.

Obecnie w sieciach MANET stosuje się najczęściej standardy rodziny IEEE 802.11. Zdefiniowana w tych standardach warstwa MAC zakłada wzajemną uczciwą współpracę wszystkich węzłów. Stacje w sieci MANET współzawodniczą ze sobą o dostęp do kanału radiowego wykorzystując okno współzawodnictwa CW (*Contention Window*). Jednak, jak zostanie pokazane, modyfikacja parametrów okna współzawodnictwa przez któregoś z użytkowników może doprowadzić do nieuczciwego zachowania się jego terminala w grupie stacji i w konsekwencji może stać się przyczyną znaczącego spadku wydajności transmisji danych w całej sieci MANET.

Standard IEEE 802.11e [4] opracowano w celu zapewnienia w warstwie MAC odpowiedniego poziomu usług QoS (*Quality of Service*). Wprowadzono nowy tryb dostępu do kanału radiowego EDCA (*Enhanced Distributed Channel Access*)[2], w którym ruch telekomunikacyjny został podzielony na cztery kategorie AC (*access categories*) o różnych priorytetach dostępu do kanału. Każda kategoria ma własny zestaw parametrów, z których najważniejsze dotyczą okna współzawodnictwa CW. Standard 802.11e pozwala na łatwą zmianę parametrów poszczególnych kategorii AC.

[1] Praca została wykonana w ramach grantu MNiSW nr N N517 4391 33.

[2] IEEE 802.11e definiuje również inny mechanizm dostępu: *HCF Controlled Channel Access* (HCCA). Mechanizm ten jest przeznaczony tylko dla sieci z infrastrukturą, których niniejsza praca nie dotyczy.

W praktyce może to być zrobione, na przykład, przy użyciu karty WLAN opartej na chipsecie Atheros i sterowniku madwifi [9]. Zatem każdy użytkownik, pracujący w sieci MANET, może wykorzystać możliwości karty WLAN do własnych, nie zawsze uczciwych celów. W standardach IEEE nie zaimplementowano żadnych mechanizmów nagradzających dobre zachowania stacji w sieciach ad-hoc. Zatem zakres złych, z punktu widzenia sieci MANET, działań którejś ze stacji może być naprawdę duży. Wystarczy, by nieuczciwy użytkownik danej stacji, na przykład, permanentnie ustawiał najniższą możliwą wartość okna współzawodnictwa.

Celem niniejszej pracy jest udzielenie odpowiedzi na szereg pytań, dotyczących problemu oszukiwania na oknie współzawodnictwa w sieciach MANET, opartych na standardzie IEEE 802.11e, z których najważniejsze to:

1. Jakich złych zachowań można oczekiwać od nieuczciwego użytkownika?
2. Czy nieuczciwe działania są korzystne dla użytkownika i łatwe do przeprowadzenia?
3. Jaki jest wpływ złych zachowań jednej ze stacji na jakość usług w całej sieci?
4. Czy korzyści użytkownika zachowującego się nieuczciwie zależą od protokołu warstwy transportowej i/lub od rozmiarów sieci?
5. Czy korzyści te są równie duże w łączu „w górę" (uplink), jak i „w dół" (downlink)?

Żeby udzielić odpowiedzi na tak postawione pytania, w rozdziale 2 niniejszej pracy opisano standard IEEE 802.11 i metodę rywalizacji o dostęp do kanału radiowego, nazywaną oknem współzawodnictwa. Następnie, w rozdziale 3 dokonano przeglądu literatury analizowanego przedmiotu. Scenariusze eksperymentów symulacyjnych przedstawiono w rozdziale 4, a wyniki badań – w rozdziale 5. Rozdział 6 stanowi podsumowanie pracy i omawia propozycje przyszłych badań.

2. Standard IEEE 802.11

W standardzie IEEE 802.11 [3] zdefiniowano między innymi, oparty na CSMA/CA (*Carrier Sense Multiple Access/Collision Avoidance*), VCS (*Virtual Carrier Sense*) i NAV (*Net Allocation Vector*), mechanizm DCF (*Distributed Coordination Function*) dostępu do kanału radiowego w sieciach bezprzewodowych, w tym przede wszystkim w sieciach ad-hoc.

W sieciach ad-hoc stacje rywalizują o dostęp do kanału radiowego, wykorzystując metodę okna współzawodnictwa CW. W metodzie CW każda stacja abonencka, chcąc nadać swoje dane, prowadzi nasłuch, by sprawdzić, czy w kanale radiowym jest prowadzona transmisja. Jeśli stwierdzi, że kanał jest wolny, to rozpoczyna wysyłanie danych. W przeciwnym przypadku, jeżeli kanał radiowy jest zajęty, to stacja czeka przez czas DIFS (*DCF Inter Frame Space*) na jego zwolnienie. Następnie wybiera z przedziału [0, CW] losową wartość czasu oczekiwania na zwolnienie kanału, ustawia na nią swój licznik *backoff* i rozpoczyna jego zmniejszanie (odliczanie czasu). Wartość licznika wskazuje konkretną szczelinę czasową, w której stacja rozpocznie transmisję swoich danych. Takie postępowanie zmniejsza prawdopodobieństwo kolizji, czyli wystąpienia sytuacji, w której dwie lub więcej stacji zacznie jednocześnie nadawać swoje dane. Zmniejszanie wartości licznika *backoff* zawiesza się, gdy kanał jest zajęty. Z chwilą, gdy licznik osiągnie wartość zero, stacja rozpoczyna nadawanie swoich danych.

Zaraz po włączeniu się stacji do sieci ad-hoc, parametr okna CW ustawiany jest na wartość minimalną CWmin, a po każdej kolizji jego wartość jest podwajana, i tak do chwili, aż osiągnie ona wartość maksymalną CWmax. Z kolei każda udana transmisja powoduje ustawienie parametru CW ponownie na wartość CWmin.

Standard IEEE 802.11e [4] wprowadza nowy tryb dostępu do kanału radiowego EDCA, w którym ruch telekomunikacyjny jest dzielony na cztery kategorie, tak by można było zapewnić usługom wymagane QoS. Zaczynając od najwyższego priorytetu, kategorie te to: *voice* (Vo), *video* (Vi), *best effort* (BE) i *background* (BK). Każda z nich ma własny zestaw parametrów: AIFS (*Arbitration InterFrame Space*), TXOP (*Transmission Opportunity*), oraz CWmin i CWmax (tab. 1), które pozwalają zróżnicować dane przesyłane w sieci, z punktu widzenia ich dostępu do kanału radiowego.

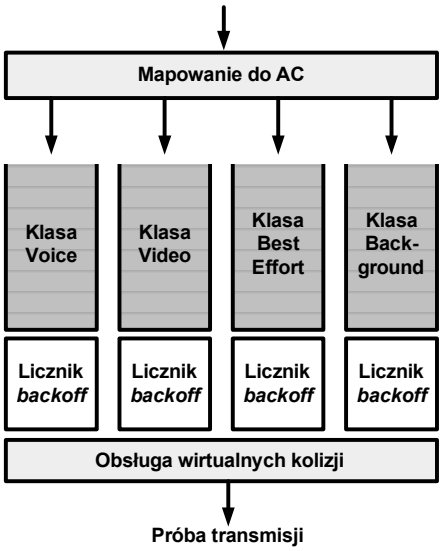
Tabela 1

Wartości parametrów CW w standardzie IEEE 802.11e

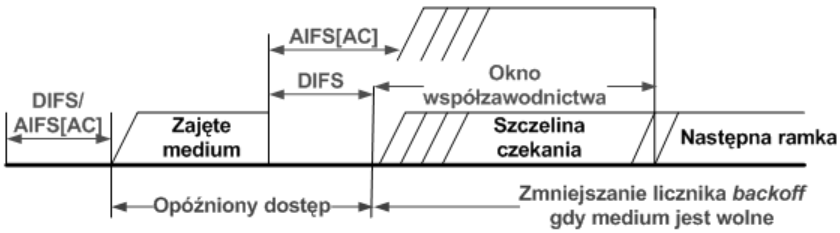
AC	CWmin	CWmax
Voice	7	15
Video	15	31
Best effort	31	1023
Background	31	1023

Podstawowe zasady dostępu do kanału radiowego w trybie EDCA są bardzo podobne do tych w DCF. Różnica polega jedynie na tym, że każda ramka przychodząca do warstwy MAC jest przydzielana, zgodnie ze swoim priorytetem, do odpowiedniej kategorii AC ruchu telekomunikacyjnego. Stąd w każdym węźle sieci mamy nie jedną, a cztery kolejki ruchu – jedna

kolejka dla każdej kategorii ruchu (rys. 1). Ponadto, stosowany w trybie DCF parametr DIFS został zastąpiony w EDCA nowym parametrem AIFS[AC] (rys. 2). W trybie EDCA mamy do czynienia z dwoma rodzajami kolizji. Wirtualna kolizja występuje wówczas, gdy w danej stacji więcej niż jedna kategoria AC wygrywa współzawodnictwo o dostęp do kanału radiowego. Natomiast kolizja w kanale ma miejsce, kiedy dwie lub więcej stacji rozpocznie nadawanie swoich ramek.



Rys. 1. Mapowanie do kategorii AC [4]



Rys. 2. Dostęp do kanału według priorytetu danej kategorii AC

3. Przegląd literatury

Pierwsze prace poświęcone problemowi oszukiwania na oknie współzawodnictwa [7] i [8] dotyczyły kilku strategii niewłaściwego zachowania stacji w sieci, w tym między innymi wyboru jak najmniejszej wartości licznika *backoff* (z przedziału [0, CW/4]), ustawienia licznika *backoff* na stałe (1 szczelina) oraz niepodwajania wartości CW. Po raz pierwszy obniżoną przepustowość w sieciach 802.11 z infrastrukturą i niewłaściwie zachowującymi się stacjami stwierdzono w pracy [7]. Autorzy postanowili rozwiązać ten problem przy pomocy odbiorcy wiadomości, który miał wymusić na nadawcy jego poprawne zachowanie się w sieci. W zaproponowanym algorytmie to odbiorca, a nie nadawca, wybierał losową wartość licznika *backoff*. Wartość ta była następnie przekazywana nadawcy za pomocą ramek CTS lub ACK. Niewłaściwe zachowanie nadawcy miało miejsce wówczas, gdy używał on innej wartości licznika *backoff* niż przesłana mu przez odbiorcę. Karą za to było przyznanie większej wartości licznika *backoff* przez odbiorcę dla następnych ramek. Wadą tego rozwiązania było to, że wymagało ono zmian w standardzie 802.11. Ponadto nie nadawało się do sieci ad-hoc, w których odbiorcy nie można ufać. Dodatkowo, stacje ukryte również mogły utrudnić ustalenie odpowiedniego czasu *backoff*.

Kilka prac poświęconych temu zagadnieniu zostało opublikowanych przez Baras *et al*.: [1], [2] i [11]. W pracy [2] przedstawiono algorytm ERA-802.11, oparty na negocjacji wartości parametrów CW przez nadawcę i odbiorcę, który utrudniał oszukiwanie przez nadawcę przy wyborze wartości licznika *backoff*. Do monitorowania sąsiednich stacji zastosowany znany z [5] system. Rozwiązanie to nie było kompatybilne ze standardem 802.11, gdyż wprowadzało dodatkowe informacje sygnalizacyjne.

Możliwość wykrycia oszustwa na oknie współzawodnictwa w praktyce sprowadza się do obserwacji wartości licznika *backoff* wybranej stacji. Obserwacje te są utrudnione przez: interferencje pochodzące od innych transmisji, niezsynchronizowane zegary i niedeterministyczny dostęp do kanału. Problemem jest też wybór momentu zaprzestania obserwacji licznika i podjęcia decyzji. Problem ten omówiono w pracy [11], w której analizowano zachowanie złośliwego użytkownika, umiejącego adaptować się do zmieniających się warunków w sieci i dowiedziono, że istnieje optymalna reguła decyzyjna, która minimalizuje liczbę koniecznych obserwacji. Podobne wnioski znalazły się w pracy [13].

Protokołem odpornym na oszukiwanie na oknie współzawodnictwa jest ICMAC [1], protokół warstwy MAC, oparty na wielodostępie z podziałem czasowym TDMA (ang. *Time Division Multiple Access*). ICMAC korzysta z mechanizmu aukcji Vickreya, znanego z teorii gier, dzięki któremu stacje są motywowane do współpracy. Jednakże użycie wielodostępu TDMA znacząco utrudnia zastosowanie tego protokołu w środowisku sieci ad-hoc.

Z kolei DOMINO [12] to zaawansowana aplikacja zaprojektowana, by chronić publiczne punkty dostę-

powe do Internetu (ang. *hotspots*) przed chciwymi użytkownikami. Aplikacja ta monitoruje ruch, rejestruje informacje i analizuje je pod kątem występowania anomalii. DOMINO potrafi wykryć wiele rodzajów złośliwych i chciwych ataków, w tym oszukiwanie na oknie współzawodnictwa. Wykrywanie anomalii jest oparte na ciągłym śledzeniu zmian przepustowości (a nie – obserwowanej wartości *backoff*). Jednak autorzy pracy [12] stwierdzili, że nie jest to optymalne kryterium. Wprawdzie aplikacja DOMINO może być zintegrowana z punktami dostępu AP i jest zgodna ze standardami, jednak nie może być stosowana w sieciach ad-hoc.

Teoretyczne rozważania dotyczące oszukiwania za pomocą licznika *backoff* zostały opublikowane przez Konorskiego, w tym np. w [6], w której zastosowano podejście z teorii gier, by motywować stacje do współpracy. Zaproponowano też strategię, która zapewnia sprawiedliwe i efektywne wykorzystanie przepustowości w sieci.

Prezentowane w literaturze dotychczasowe wyniki badań sieci 802.11 koncentrowały się na wykrywaniu stacji oszukujących na oknie współzawodnictwa, pracujących w trybie infrastruktury. Sieci ad-hoc stanowią spore wyzwanie, ponieważ charakteryzują się dużym rozproszeniem i nie posiadają centralnego zarządzania. Z tego powodu, niewiele prac omawiało oszukiwanie na oknie wielodostępu w sieciach MANET. Jeszcze mniej z nich dotyczyło standardu 802.11e, który, jak zaznaczono wcześniej, pozwala na łatwą modyfikację parametrów MAC.

4. Scenariusze symulacyjne

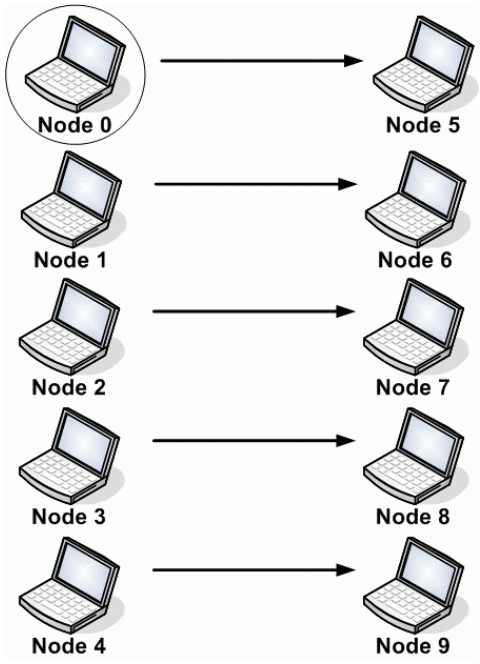
Przedmiotem badań symulacyjnych była ocena wpływu stacji oszukujących na oknie współzawodnictwa (CW) na wydajność sieci ad-hoc. W tym celu określono dla protokołów UDP i TCP potencjalne korzyści, jakie może odnieść nieprawidłowo zachowująca się stacja w łączach *uplink* i *downlink*.

Tabela 2
Parametry symulacyjne

Parametr	Wartość
Protokół MAC	802.11b + 802.11e
Szybkość transmisji	11 Mb/s
Szybkość podstawowa	1 Mb/s
Protokół rutingu	Brak
Protokół transportowy	UDP i TCP
Rozmieszczenie stacji	Losowe
Generator ruchu	CBR
Wielkość ramki	1000 B
Wymiana ramek	DATA-ACK

Analiza symulacyjna została przeprowadzona za pomocą symulatora ns2 wykorzystującego tryb EDCA, opracowany przez TKN [14]. Stacje badanej sieci znajdowały się we wzajemnym zasięgu radiowym. Parametry użyte w badaniach symulacyjnych przedstawiono w tabeli 2.

Dla transmisji w łączach *uplink* i *downlink* rozważono dwie różne topologie sieciowe. W analizach małej, średniej i dużej sieci w scenariuszach symulacyjnych dla łącza *uplink* przyjęto, że liczba jednakowych stacji w sieci ad-hoc, transmitujących dane, wynosiła odpowiednio 5, 25 i 100. Ruch generowany przez każdą stację zmieniał się od 64 kbit/s do 8 Mbit/s. Wszystkie stacje były we wzajemnym zasięgu radiowym. Przykładowa topologia dla 5 stacji pokazana jest na rysunku 1.

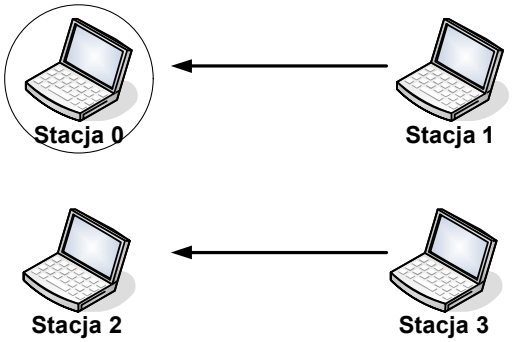


Rys. 3. Przykładowa topologia sieci (scenariusz *uplink*)

W każdym scenariuszu transmisji w łączu *uplink* była dokładnie jedna źle zachowująca się stacja, np. na rysunku 1 była to stacja obwiedziona kołem. Wszystkie stacje pracowały z priorytetem *best effort*. Stacje poprawnie zachowujące się (*dobre*) miały niezmieniane parametry okna współzawodnictwa: CWmin = 31, CWmax=1023. Parametry źle zachowującej się stacji (*złej*) były znacząco mniejsze: CWmin = 1, CWmax = 5. Zatem można było przypuszczać, że źle zachowująca się stacja przyjmowała tak małe (lub mniejsze) wartości parametrów CWmin i Cwmax, by zmaksymalizować swój zysk.

Nieco inna topologia sieci została wzięta pod uwagę w scenariuszu transmisji dla łącza *downlink* (rys. 4). Wszystkie cztery stacje były we wzajemnym zasięgu

radiowym i tylko jedna z nich źle się zachowywała (rysunek 4 – stacja obwiedziona kołem). W analizowanej sytuacji pomiar ruchu UDP był bezcelowy, gdyż źle zachowująca się stacja nie miała żadnej możliwości wpływania na szybkość wysyłania danych w łączu *downlink*. Natomiast w przypadku ruchu TCP *zła* stacja wysyłała pakiety TCP-ACK, a więc wpływała na szybkość przesyłanych danych. Tak więc w tym scenariuszu przepustowość była mierzona z włączonym i wyłączonym złym zachowaniem się *złej* stacji.

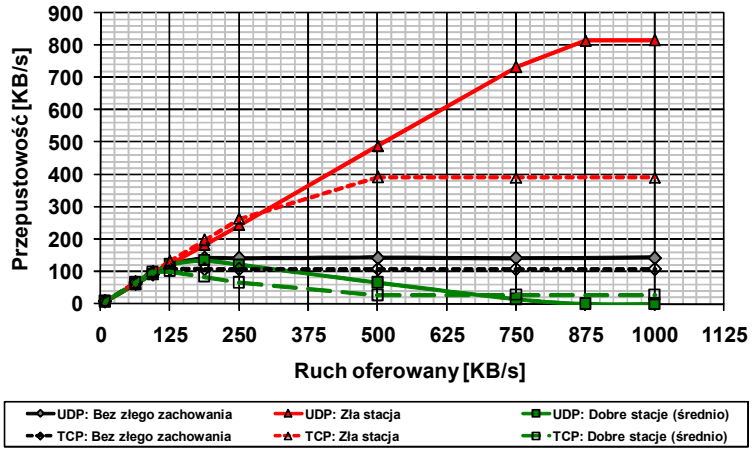


Rys. 4. Topologia sieci (scenariusz *downlink*)

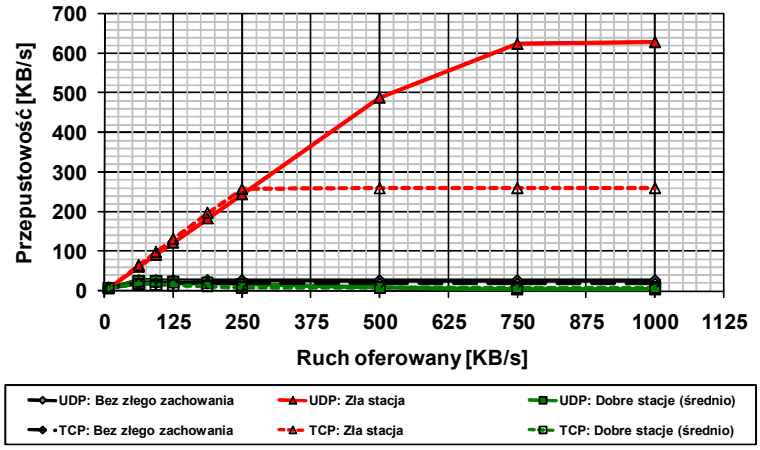
5. Wyniki

Wyniki symulacji komputerowych dla łącza *uplink* przedstawiono na rysunkach od 5 do 8. Dla poziomu ufności 95% błąd względny estymatorów średnich wartości przepustowości i opóźnienia nie przekraczał $\pm 2\%$. Na rysunkach 5, 6 i 7 przedstawiono średnie przepustowości wybranych stacji wyrażone w funkcji ruchu oferowanego w sieci złożonej z 5, 25 i 100 stacji. Porównano ze sobą: średnią przepustowość źle zachowującej się stacji ze średnią przepustowością *dobrych* stacji oraz średnią przepustowością stacji w sieci, w której nie ma *złych* stacji. Średnie opóźnienie ramek zaprezentowano jedynie dla małej sieci (rys. 8), gdyż dla większych opóźnienia te były bardzo do siebie zbliżone.

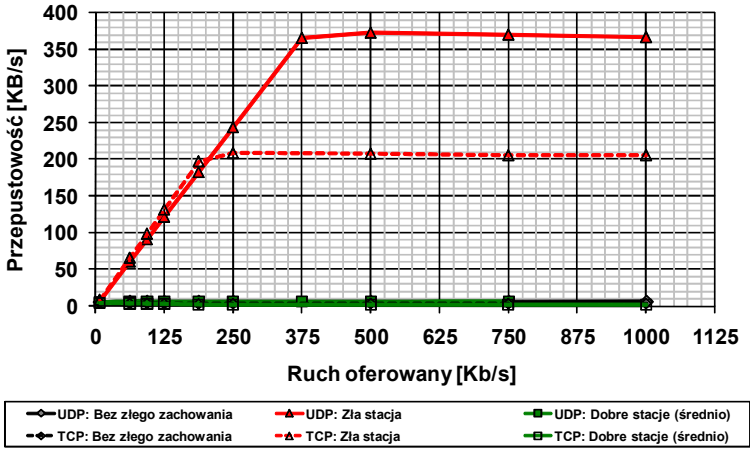
Z analizy rysunków 5 do 8 wynika, że źle zachowująca się stacja może zdominować pracę całej sieci, jeśli chodzi o przepustowość i opóźnienie. Dzieje się tak, gdy w sieci panuje natłok, bowiem wzrost ruchu oferowanego powoduje wzrost średniej przepustowości *złej* stacji, przy jednoczesnym spadku średniej



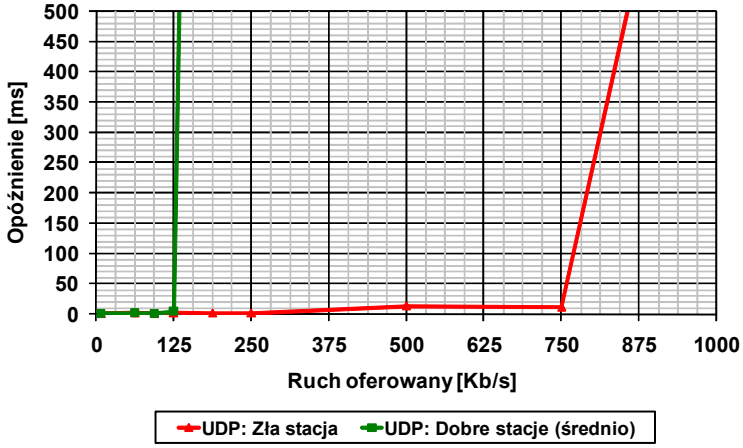
Rys. 5. Porównanie średnich przepustowości 4 *dobrych* i 1 *złej* stacji z przepustowością sieci złożonej z 5 *dobrych* stacji



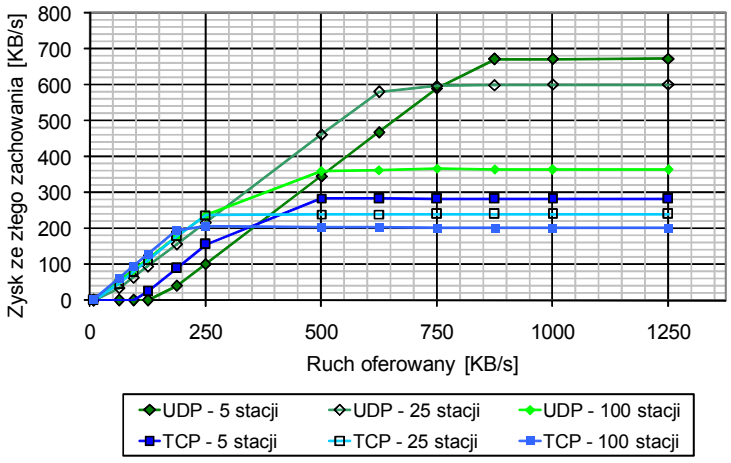
Rys. 6. Porównanie średnich przepustowości 24 *dobrych* i 1 *złej* stacji z przepustowością sieci złożonej z 25 *dobrych* stacji



Rys. 7. Porównanie średnich przepustowości 99 *dobrych* i 1 *złej* stacji z przepustowością sieci złożonej z 100 *dobrych* stacji



Rys. 8. Porównanie średnich opóźnień 4 *dobrych* i 1 *złej* stacji z opóźnieniem sieci złożonej z 5 *dobrych* stacji



Rys. 9. Zysk przepustowości dla stacji źle zachowującej się

przepustowości *dobrych* stacji. Przy braku natłoku, obecność *złej* stacji jest niezauważalna w sieci. Po jego wystąpieniu, *zła* stacja zwiększa swoją przepustowość kosztem *dobrych* stacji, aż do wystąpienia w sieci stanu nasycenia. Wyniki dla ruchu UDP i TCP różnią się jedynie pod względem ilościowym. Ruch TCP uzyskuje mniejszą przepustowość niż ruch UDP ze względu na kontrolę przeciążeń oraz mechanizm potwierdzania pakietów. Natomiast liczba stacji w sieci wpływa głównie na przepustowość, jaką *zła* stacja uzyskała w stanie nasycenia sieci.

Rysunek 5 pokazuje wzrost przepustowości stacji źle zachowującej się w porównaniu do sytuacji, w której zachowuje się ona tak, jak robią to inne *dobre* stacje.

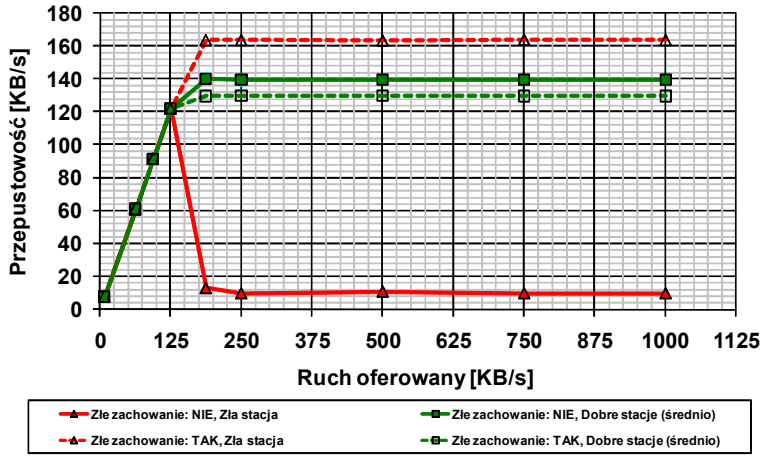
Przepustowość, przy której dochodzi do nasycenia, jest uzależniona od protokołu transportowego (TCP, UDP) i liczby stacji w sieci (5, 25, 100). Niewątpliwie niewłaściwe zachowanie stacji przynosi jej korzyści – stacja, która oszukuje, zawsze może liczyć na większą niż inne stacje szybkość transmisji.
W poprzednich symulacjach, źle zachowująca się stacja używała następujących parametrów okna *backoff*: CWmin = 1, CWmax = 5. W celu sprawdzenia, jak wartość CWmax wpływa na przepustowość stacji źle zachowującej się, przeprowadzono badania symulacyjne, których wyniki przedstawiono w tabeli 3.

Tabela 3

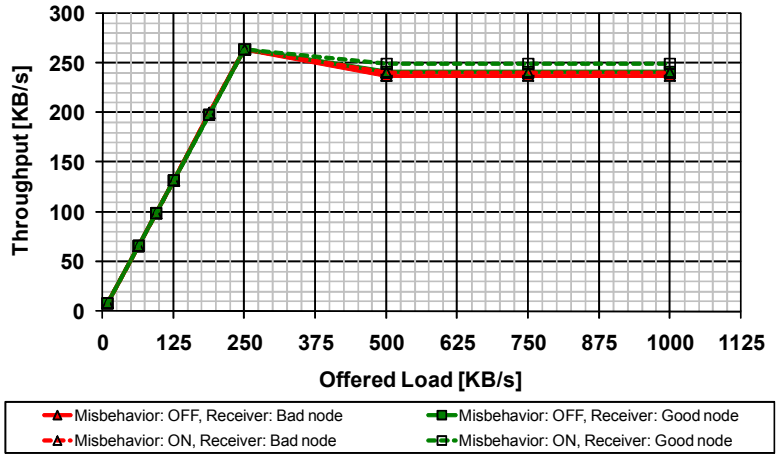
Wpływ CWmax na średnią przepustowość źle zachowującej się stacji (w KB/s)

Liczba stacji	CWmax		
	1	5	31
5	763	755	754
25	676	623	604
100	507	367	265

Zwiększanie parametru CWmax (do 31) wpływa znacząco na przepustowość *złej* stacji jedynie w przypadku dużych sieci. Można przypuszczać, że stacja źle zachowująca się będzie wybierała najmniejszą możliwą wartość parametru CWmax, żeby zmaksymalizować swój zysk. By sprawdzić tę dolną granicę, przeprowadzono symulację dla CWmax = 1. Spowodowało to wzrost przepustowości *złej* stacji. Największy wzrost przepustowości miał ponownie miejsce w sieci o dużej liczbie stacji. Jak wspomniano wcześniej, standard 802.11 nie zawiera żadnych mechanizmów, które sprawdzałyby, czy dana stacja zachowuje się poprawnie.
Istotnym problemem jest wpływ złego zachowania na ruch o wysokim priorytecie. Czy stacja, która oszukuje w zakresie kategorii dostępu o niskim priorytecie (np. *best effort*), może odebrać przepustowość stacji wysyłającej ruch o wyższym priorytecie (np. *voice*)? By odpowiedzieć na to pytanie, zbadano zmodyfikowaną wersję scenariusza z 5 stacjami (rys. 3). Cztery *dobre* stacje wysyłały ruch o najwyższym priorytecie (*voice*). Stacja źle zachowująca się używała priorytetu *best effort*. Przebadano dwa przypadki –



Rys. 10. Średnia przepustowość stacji w funkcji ruchu oferowanego (priorytety BE i Vo)



Rys. 11. Przepustowość w kierunku *downlink*

z niewłaściwym zachowaniem włączonym i wyłączonym. Rysunek 10 przedstawia uzyskaną przepustowość w funkcji ruchu oferowanego. Jeśli w sieci niewłaściwe zachowanie jest wyłączone (linie ciągłe), *dobre* stacje (*voice*) zajmują większość pasma, natomiast przepustowość *złej* stacji jest znacznie zredukowana. Wynika to z mechanizmu EDCA i wartości parametrów dostępu do kanału radiowego dla kategorii dostępu *voice* i *best effort*. Linie przerywane na rysunku 10 przedstawiają przypadek, kiedy *zła* stacja modyfikuje swoje parametry CW podobnie jak w poprzednich scenariuszach (tj., CWmin = 1, CWmax = 5). Stacja ta może teraz osiągnąć znacznie większą przepustowość niż poprzednio, wyższą nawet niż osiąganą przez priorytet *voice*. Różnica między tym a poprzednim scenariuszem jest taka, że źle zachowująca się stacja nie może zdominować kanału, tak jak poprzednio, w obecności stacji korzystających z priorytetu *voice*. Można wnioskować, że stacja niewłaściwie zachowująca się zawsze zwiększy swoją przepustowość, niezależnie od tego, w zakresie której kategorii dostępu oszukuje. Taka właściwość sieci może wpłynąć na decyzje podejmowane przez potencjalnie złośliwie zachowującą się stację w celu skorzystania z przewagi, jaką daje jej niewłaściwe zachowanie.

W scenariuszu transmisji dla łącza *downlink* mierzono tylko ruch TCP. Stacja niewłaściwie zachowująca się mogła wpłynąć tylko na wysyłanie pakietów TCP-ACK poprzez zmianę parametrów CW (CWmin = 1, CWmax = 5). Rysunek 11 przedstawia wykres przepustowości dla włączonego i wyłączonego niewłaściwego zachowania stacji.

Wyniki badań symulacyjnych wskazują, że przepustowość *złej* stacji zwiększa się w sposób nieznaczny. Szybsze wysyłanie pakietów TCP-ACK zwiększa liczbę kolizji w kanale, ale nie daje w zamian znaczącego wzrostu przepustowości. Jest to sytuacja, w której niewłaściwe zachowanie stacji nie przynosi jej znaczących zysków.

6. Wnioski

Niniejszy artykuł prezentuje, jak oszukiwanie przez stacje na oknie współzawodnictwa wpływa na pracę sieci ad-hoc typu *single-hop*. Za pomocą symulacji komputerowych zbadano przepustowość i opóźnienie dla ruchu TCP i UDP. Symulacji dokonano dla dwóch scenariuszy, zależnie od kierunku transmisji ruchu w sieci: *uplink* i *downlink*.

Główny wniosek jest następujący: oszukiwanie na oknie współzawodnictwa prowadzi do znaczącej niesprawiedliwości w przydziale pasma w kierunku *uplink*. Źle zachowująca się stacja potrafi zdominować ruch w łączu w górę zarówno pod względem przepustowości, jak i opóźnienia, zyskując na swoim złym zachowaniu. Niewłaściwe zachowanie jest zawsze korzystne, a uzyskana przepustowość jest wyższa dla UDP niż dla TCP i bardziej znacząca w małych sieciach. Dominująca rola stacji niewłaściwie zachowującej się naraża całą sieć ad-hoc na spadek wydajności, ponieważ pozostałe stacje otrzymują niską przepustowość. Takie zachowanie stacji powoduje również występowanie w sieci stacji jawnych (ang. *exposed stations*), które mogą stanowić istotny problem dla sieci typu *multi-hop*.

Zauważono, że wzrost przepustowości *złej* stacji występuje tylko w stanie natłoku w sieci. Zatem każda analiza dotycząca problemu oszukiwania przez stacje na oknie współzawodnictwa powinna być ograniczona tylko do takich sytuacji. W sieciach, w których nie mamy do czynienia z natłokiem, niewłaściwe zachowanie się stacji, choć teoretycznie obserwowalne, nie ma żadnego wpływu na sąsiadów stacji i jest przez to niegroźne.

Standard IEEE 802.11e jest bardzo podatny na niewłaściwe zachowanie stacji – pozwala na łatwą modyfikację parametrów MAC i nie daje żadnej motywacji do poprawnego zachowania się. Złośliwy użytkownik może wybrać najniższe możliwe wartości parametrów CWmin i Cwmax, by osiągnąć największą przepustowość.

W artykule pokazano, że standard IEEE 802.11e nie wspiera QoS, gdy któraś ze stacji oszukuje na oknie współzawodnictwa. Niewłaściwe zachowanie pozwala stacji, która oszukuje w zakresie kategorii dostępu o niskim priorytecie (np. *best effort*), odebrać przepustowość stacji wysyłającej ruch o wyższym priorytecie (np. *voice*).

Badania przeprowadzono także dla kierunku *downlink*. Pokazały one, że *zła* stacja nie może znacząco wpłynąć na przepustowość innych stacji, nawet w przypadku ruchu TCP. Stwierdzono zatem, że w niektórych przypadkach niewłaściwe zachowanie może nie przynosić korzyści, co jest istotną obserwacją. Celem złośliwego użytkownika może być zwiększenie szybkości pobieranych danych (np. w przypadku transferu FTP), jednakże żadna znacząca korzyść nie może być osiągnięta z oszukiwania na oknie współzawodnictwa.

Przyszłe prace skoncentrują się na bardziej skomplikowanych scenariuszach, występujących w rzeczywistych środowiskach i z wykorzystaniem rzeczywistych aplikacji (np. typu *peer-to-peer* dla sieci ad-hoc). Zostanie wzięta pod uwagę większa liczba niewłaściwie zachowujących się stacji w sieci. Na podstawie badań będzie można stwierdzić, jakich form niewłaściwego zachowania należy się spodziewać ze strony nieuczciwych użytkowników. Będą rozważone proste, jednakże przynoszące istotne korzyści zachowania, które mogą być wykorzystane przez zwykłego użytkownika, a nie tylko eksperta.

Ostatecznym celem badań będzie zaprojektowanie architektury przeciwdziałającej niewłaściwemu zachowaniu w sieciach 802.11e. Właściwa architektura sieci pozwoli wykrywać niewłaściwe zachowania się stacji.

Literatura

[1] BenAmmar N., Baras J.S.: *Incentive compatible medium access control in wireless networks*. Proceedings from the 2006 Workshop on Game theory For Communications and Networks (GameNets '06), Piza, Włochy, październik 2006

[2] Cardenas A.A., Radosavac S., Baras J.S.: *Detection and Prevention of MAC Layer Misbehavior for Ad Hoc Networks*. Technical Report, 2004

[3] IEEE 802.11: *IEEE Standard for Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*. New York, USA, 12 czerwca 2007

[4] IEEE 802.11e: *IEEE Standard for Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, Amendment 8: Medium Access Control (MAC) Quality of Service Enhancements*. New York, USA, 11 październik 2005

[5] Grega M., Szott Sz., Pacyna P.: *Collaborative Networking with Trust and Misbehavior – A File Sharing Case*. First Workshop on Operator-assisted (Wireless Mesh) Community Networks, 18-19 września 2006, Berlin, Niemcy

[6] Konorski J.: *A Game-Theoretic Study of CSMA/CA Under a Backoff Attack*. IEEE/ACM Transactions on Networking, vol.14, no.6, pp.1167-1178, grudzień 2006

[7] Kyasanur P., Vaidya N.H.: *Detection and Handling of MAC Layer Misbehavior in Wireless Networks.* 2003 International Conference on Dependable Systems and Networks (DSN'03), 2003

[8] Kyasanur P., Vaidya N.H.: *Selfish MAC Layer Misbehavior in Wireless Networks*. IEEE Transactions on Mobile Computing, Volume 4, Number 5, wrzesień/październik 2005

[9] MADWiFi – Multiband Atheros Driver for WiFi, http://madwifi.org

[10] M. Raya, I. Aad, J.P. Hubaux, A. El Fawal: *DOMINO: Detecting MAC Layer Greedy Behavior in IEEE 802.11 Hotspots.* IEEE Transactions on Mobile Computing, grudzień 2006

[11] Radosavac S., Baras J.S., Koutsopoulos I.: *A Framework for MAC Protocol Misbehavior Detection in Wireless Networks*. In Proc. 4th ACM Workshop on Wireless Security (WiSe), Cologne, Germany, wrzesień 2005

[12] Raya M., Hubaux J., Aad I.*: DOMINO: a system to detect greedy behavior in IEEE 802.11 hotspots*. Proceedings of the 2nd International Conference on Mobile Systems, Applications, and Services (MobiSys '04), Boston, MA, USA, czerwiec, 2004

[13] Rong Y., Lee S.-K., Choi H.-A.: *Detecting Stations Cheating on Backoff Rules in 802.11 Networks Using Sequential Analysis*. INFOCOM 2006. 25th IEEE International Conference on Computer Communications. Proceedings , kwiecień 2006

[14] Wiethölter S., Emmelmann M., Hoene C., Wolisz A.: *TKN EDCA Model for ns-2*. Technical Report TKN-06-003, Telecommunication Networks Group, Technische Universität Berlin, czerwiec 2006

Szymon Szott ukończył studia na wydziale Elektrotechniki, Automatyki, Informatyki i Elektroniki Akademii Górniczo-Hutniczej w Krakowie w roku 2006. Obecnie jest w trakcie studiów doktoranckich w Katedrze Telekomunikacji AGH. Jego zainteresowania koncentrują się przede wszystkim na problemach dotyczących bezprzewodowych sieci lokalnych (w tym sieci ad-hoc). W szczególności obejmują zagadnienia związane z bezpieczeństwem oraz zapewnieniem odpowiedniej jakości usług w tych sieciach. Realizuje bądź realizował następujące projekty europejskie: DAIDALOS II, CONTENT, CARMEN, MEDUSA, jak również granty Ministerstwa Nauki i Szkolnictwa Wyższego. Jest autorem lub współautorem ponad 20 artykułów naukowych oraz rozdziału książki.

Marek Natkaniec otrzymał tytuł magistra inżyniera oraz doktora telekomunikacji na Wydziale Elektrotechniki Automatyki i Elektroniki Akademii Górniczo-Hutniczej w Krakowie w latach 1997 i 2002. Obecnie pracuje jako adiunkt w Katedrze Telekomunikacji Akademii Górniczo-Hutniczej. Jego zainteresowania obejmują: lokalne sieci bezprzewodowe, projektowanie protokołów komunikacyjnych, zagadnienia QoS, usługi multimedialne, modelowanie oraz analiza wydajności pracy sieci teleinformatycznych. Pracuje aktywnie w projektach europejskich. Uczestniczy również w realizacji projektów badawczych finansowanych przez Ministerstwo Nauki i Szkolnictwa Wyższego. Marek Natkaniec jest współautorem czterech książek oraz ponad sześćdziesięciu publikacji.

Andrzej Ryszard Pach ukończył Wydział Elektrotechniki, Automatyki i Elektroniki AGH w roku 1975, w r. 1977 doktoryzował się na AGH, a w roku 1990 uzyskał stopień doktora habilitowanego na Wydziale Elektroniki Politechniki Warszawskiej. Zatrudniony jest obecnie na stanowisku profesora zwyczajnego w Katedrze Telekomunikacji AGH, w której pełni funkcję kierownika. Wcześniej był prodziekanem Wydziału EAiE.

Główne zainteresowania naukowe związane są z sieciami telekomunikacyjnymi oraz systemami informacyjnymi. Autor ponad stu publikacji naukowych z zakresu protokołów komunikacyjnych, modelowania i analizy sieci komputerowych, sieci szerokopasmowych z integracją usług. Aktywnie uczestniczy w projektach europejskich IST, ACTS, COST i COPERNICUS. Członek komitetów programowych konferencji międzynarodowych. Konsultant firm państwowych i prywatnych w zakresie nowoczesnej telekomunikacji.

Współzałożyciel i wiceprezydent Fundacji Postępu Telekomunikacji, przewodniczący IEEE Communications Society Chapter.