BIULETYN INSTYTUTU AUTOMATYKI I ROBOTYKI
NR 33, 2012

Metodyka badań protokołów trasowania dla sieci ad-hoc

Tomasz MALINOWSKI

Instytut Teleinformatyki i Automatyki WAT,
ul. Gen. S. Kaliskiego 2, 00-908 Warszawa
t.malinowski@ita.wat.edu.pl

STRESZCZENIE: W artykule scharakteryzowano, jako przedmiot badań symulacyjnych, protokoły routingu dynamicznego dla sieci ad-hoc. Przedstawiono zasady przygotowania i realizacji eksperymentu symulacyjnego, służącego ocenie wpływu zastosowanego protokołu trasowania na funkcjonowanie sieci ad-hoc. Wyniki badań symulacyjnych, przeprowadzonych zgodnie z proponowanym planem eksperymentu symulacyjnego, pozwalają wskazać preferowany tryb uaktualniania tras w tablicach routingu węzłów sieci mobilnej o określonej wielkości i w zależności od szybkości przemieszczania się węzłów.

SŁOWA KLUCZOWE: sieci mobilne ad-hoc, protokoły routingu dynamicznego w sieciach ad-hoc, badania symulacyjne

1. Wprowadzenie

Mobilne sieci ad-hoc (Manet – Mobile Ad-hoc Networks) to bezprzewodowe sieci bez stałej, a'priori określonej infrastruktury, z przemieszczającymi się węzłami (mobilnymi urządzeniami komunikacji bezprzewodowej), zdolnymi do komunikowania się ze sobą. Sieć komunikacyjna ad-hoc charakteryzuje się zwykle brakiem stacjonarnych urządzeń dostępowych. Znaczący wpływ na rozwój technologii umożliwiających komunikowanie się mobilnych urządzeń ma potrzeba wyposażania na szeroką skalę komputerów przenośnych, tabletów i telefonów komórkowych w układy do bezprzewodowej komunikacji sieciowej.

Sieci ad-hoc znajdują zastosowanie wszędzie tam, gdzie konieczne jest szybkie zorganizowanie systemu łączności między rozproszonymi na pewnym

obszarze geograficznym węzłami. Poza oczywistym wykorzystaniem rozwiązań technicznych dla sieci ad-hoc w systemach komunikacji wojskowej, sieci mobilne znajdują zastosowanie w sytuacjach kryzysowych, gdy przykładowo konieczne jest zorganizowanie łączności na potrzeby ratownictwa medycznego, usuwania skutków powodzi, trzęsień ziemi, czy innych katastrof. Istotnym staje się krótki czas tworzenia infrastruktury sieciowej (samoorganizowanie się sieci), odporność systemu transmisji na awarie węzłów sieciowych i to, że nie jest z góry określona liczba węzłów (pojemność sieci). Węzły w takiej sieci są nie tylko odbiornikami informacji, ale również mogą pełnić funkcję urządzeń przesyłających dane do innych węzłów.

Przy potrzebie sprawnego organizowania systemów łączności bezprzewodowej, sieci ad-hoc stają się ważnym obszarem badań odkrywających możliwości rozwoju oraz praktycznego wykorzystania technicznych środków, służących realizacji systemów charakteryzujących się wysoką dostępnością i niezawodnością transmisji (unikanie izolowania węzłów sieciowych), pożądaną pojemnością sieci, dzięki której możliwe jest osiągnięcie wymaganej jakości transmisji, bez zakłóceń i interferencji pomiędzy węzłami, czy wysokim poziomem bezpieczeństwa transmisji [1], [2].

Wybrane cechy charakterystyczne sieci ad-hoc zebrane zostały w tab. 1.

Tab. 1. Cechy charakterystyczne sieci ad-hoc [3]

Cecha	Charakterystyka
Mobilność	Dynamicznie zmieniające się pozycje węzłów. Nieustalona liczba węzłów wchodzących w skład danej sieci.
Multihopping	Trasa od źródła do celu prowadzi przez kilka węzłów. Liczba przeskoków może się zmieniać w krótkim okresie czasu.
Samoorganizacja	Węzeł sieci ad-hoc musi niezależnie określić swoje parametry konfiguracyjne, takie jak routing, pozycja, kontrola zasilania.
Oszczędzanie energii	Wiele urządzeń tworzących sieci ad-hoc posiada ograniczone źródło zasilania. Wykorzystanie zoptymalizowanych pod kątem energetycznym protokołów pozwala wydłużyć czas pracy tych urządzeń.
Skalowalność	Charakter sieci ad-hoc pozwala na dynamiczne budowanie sieci, które zawierać mogą dużą liczbę węzłów.
Niski poziom bezpieczeństwa	Ze względu na swój charakter, sieci ad-hoc są jednym z najbardziej podatnych na ataki środowisk sieciowych.

Istotnym elementem systemu transmisji w sieciach ad-hoc jest podsystem trasowania pakietów, bazujący na określonym algorytmie organizowania tablic trasowania w węzłach sieciowych, umożliwiających efektywne przekazywanie pakietów do odległego węzła mobilnego przez szereg węzłów pośredniczących

w transmisji. Protokoły routingu dynamicznego stosowane w sieciach przewodowych nie są w stanie w krótkim czasie reagować na szybkie zmiany położenia węzłów sieciowych. Dodatkowo, sprawdzające się doskonale w sieciach przewodowych protokoły typu stanu łącza, wykonując szereg obliczeń w sieci o szybkozmiennej topologii konsumowałyby zbyt dużo zasobów energetycznych węzła, na co nie można sobie pozwolić, gdyż podstawowym założeniem jest zapewnienie jak najdłuższego czasu funkcjonowania węzła (z możliwością transmitowania i odbierania pakietów) [3].

Protokoły trasowania dla sieci ad-hoc powinny być jak najprostsze, szybkie i w sposób minimalny wykorzystujące zasoby sieci, zarówno węzła (procesor, pamięć, bateria), jak i na przykład dostępne pasmo transmisyjne. Przy projektowaniu protokołów trasowania powinna być uwzględniona duża dynamika reorganizowania topologii sieci (położenia węzłów), ograniczone pasmo transmisyjne, ograniczona „widzialność" węzła sieciowego, czy występowanie łączy jednokierunkowych (ang. *unidirectional link*), zwanych łączami z zerową przepustowością zwrotną.

W artykule przedstawiona została metodyka prowadzenia symulacyjnych badań porównawczych wybranych protokołów trasowania dla sieci ad-hoc. Badania przeprowadzone zostały z wykorzystaniem pakietu symulacyjnego OPNET, a szczegółowy ich przebieg i interpretacja uzyskanych wyników będą omówione w kolejnym artykule.

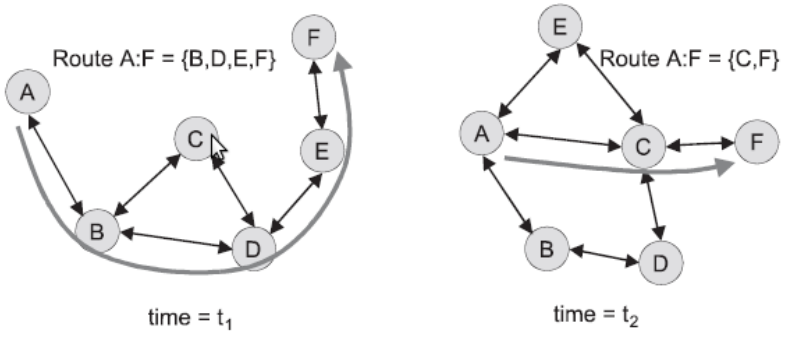
2. Protokoły trasowania w sieciach ad-hoc jako przedmiot badań porównawczych

Pierwotnie, badania nad sieciami ad-hoc prowadzone były pod kątem ich wykorzystania w obszarze militarnym. Rosnące zapotrzebowanie na system komunikacji urządzeń nie będących w bezpośrednim zasięgu nadajników sieci szkieletowej zaowocowało powołaniem przy organizacji IETF grup MANET oraz NEMO (*Network Mobility*). Zadaniem obu grup jest badanie i standaryzacja protokołów trasowania pakietów IP pod kątem ich użycia w sieciach o topologii stałej jak i dynamicznie zmieniającej się, zbudowanych z różnych odmian sprzętu wykorzystującego komunikację bezprzewodową [3], [4].

Trasa pakietu w środowisku sieci ad-hoc może przebiegać przez jeden lub więcej węzłów, przy czym topologia sieci podlega dynamicznym zmianom, często w sposób nieprzewidywalny. Protokół trasowania w sieci ad-hoc powinien być automatycznie uruchamiany, gdy zaistnieje taka potrzeba i wyznaczać wolną od pętli trasę do żądanego punktu docelowego. W warunkach często zmieniającej się topologii sieci, powinien zapewniać krótki

czas osiągania stanu ustalonego (ang. *convergence time*), w którym wszystkie węzły sieciowe mają aktualne i właściwe, wolne od nieprawidłowych wpisów tablice routingu. Ponadto, protokół powinien charakteryzować się jak najmniejszym zapotrzebowaniem na pasmo transmisyjne i zasoby sprzętowe węzła sieciowego [5].

W sieciach ad-hoc każdy węzeł należący do sieci może brać udział w przekazywaniu pakietów. Rys. 1 przedstawia prostą sieć ad-hoc, zmieniającą w czasie swoją topologię, w której w celu przesłania pakietów z węzła A do F wykorzystywany jest protokół trasowania dynamicznego.



Rys. 1. Proces dynamicznego wyznaczania trasy w sieci o zmieniającej się topologii [1]

W czasie t_1 najkrótsza trasa od węzła A do F wiedzie przez węzły B, D i E. W czasie t_2 topologia ulega zmianie, co powoduje konieczność ponownego wyznaczenia trasy dla pakietów przesyłanych od źródła A do celu F. Najkrótsza trasa, która powinna zastąpić w tablicy routingu węzła A trasę {B,D,E,F}, wiedzie tym razem przez węzeł C ({C,F}).

Podobnie jak w przypadku sieci przewodowych, protokół trasowania ma za zadanie wyznaczenie „najlepszej" (zgodnie z ustalonym kryterium oceny jakości) trasy dla pakietów z węzła źródłowego do docelowego. Biorąc jednak pod uwagę wymienione wcześniej cechy i ograniczenia sieci ad-hoc, w szczególności dużą dynamikę zmian topologii i nieprzewidywalność połączeń między węzłami, realizacja tego zadania jest innym wyzwaniem, omawianym w szeregu publikacji, w tym w [6], [7].

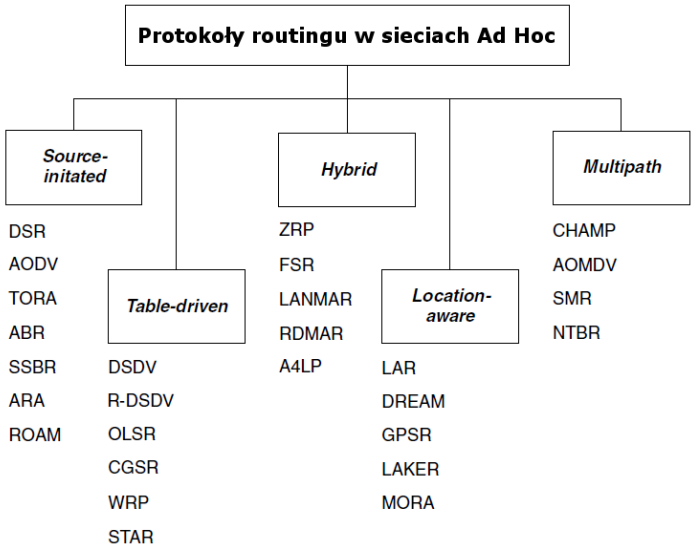
Do chwili obecnej opracowano szereg różnych protokołów trasowania, które w zależności od potrzeb i wymagań mogą być implementowane w sieciach mobilnych. Protokoły te klasyfikowane są jako [4]:

1. Protokoły proaktywne (ang. *proactive*), nazywane również protokołami *table-driven*, charakteryzują się tym, że w każdym węźle tablice trasowania są wyznaczane na drodze odbierania i interpretowania cyklicznie

odbieranych od innych węzłów sieciowych aktualizacji. Stosowanie tych protokołów nie jest zalecane w rozbudowanych (z dużą liczbą węzłów) i z szybko zmieniającą się topologią środowisk sieciowych ad-hoc. Zasadniczą wadą protokołów z tej grupy jest powodowanie dużego obciążenia sieci cyklicznie rozsyłanymi pakietami aktualizacyjnymi. Reprezentantami tej grupy protokołów są np.: WRP (*Wireless Routing Protocol*) i DSDV (*Highly Dynamic Destination-Sequenced Distance Vector Routing Protocol*), powstałe na bazie algorytmu Bellmana-Forda i protokołu RIP, czy OLSR (*Optimized Link State Routing Protocol*) z koncepcją węzłów pośredniczących w transmisji (tzw. *Multipoint relays*).

2. Protokoły reaktywne (ang. *reactive*) – znane również jako protokoły trasowania na żądanie (ang. *on-demand*) lub protokoły typu *source-initiated*. Jest to klasa protokołów, w których trasa wyznaczana jest w momencie, gdy węzeł źródłowy chce przesłać pakiety do określonego celu. Proces trasowania uruchamiany jest na żądanie węzła źródłowego. Sieć zalewana jest z inicjatywy węzła źródłowego specjalnymi pakietami żądania wyznaczenia trasy. Po zakończeniu procedury wyznaczania trasy, trasa jest utrzymywana w tablicy routingu do momentu zakończenia jej wykorzystywania. Do tej grupy protokołów należą między innymi AODV (*Ad-hoc On-demand Distance Vector*) czy DSR (*Dynamic Source Routing*).
3. Protokoły hybrydowe (ang. *hybrid*) – protokoły te łączą właściwości protokołów proaktywnych i reaktywnych. W większości przypadków protokołów z tej grupy ich działanie bazuje na podziale sieci na mniejsze obszary, a węzły utrzymują tablice tras dla tych wydzielonych obszarów. Procedura utrzymywania i uaktualniania tablic trasowania dla obszarów o ograniczonej rozpiętości jest podobna do stosowanej np. w sieciach z protokołem OSPF. Reprezentantem tej grupy jest np. protokół ZRP (*Zone Routing Protocol*).
4. Protokoły wielościeżkowe (ang. *multipath*), umożliwiające wyznaczenie wielu ścieżek od źródła do celu i tym samym realizację równoważenia obciążenia łączy oraz natychmiastowe skierowanie pakietów na łącza alternatywne w przypadku zaniku połączenia podstawowego (odporność na awarie). Protokoły tej grupy, jako szczególnie użyteczne w sieciach o dużej „gęstości" węzłów, są obecnie przedmiotem wielu badań.
5. Protokoły routingu bazujące na danych GPS o położeniu węzłów (ang. *location-aware*) – w przypadku tych protokołów do wyznaczenia efektywnej trasy do węzła docelowego może być wykorzystywana informacja nie tylko o aktualnym położeniu węzła docelowego, ale również o szybkości i kierunku w jakim węzeł się porusza, co może być podstawą wyznaczenia położenia węzła z pewnym wyprzedzeniem.

Klasyfikację protokołów (wraz z nazwami wybranych protokołów należących do danej klasy) przedstawia rys. 2. Szczegółową charakterystykę wymienionych tutaj grup znaleźć można np. w [4], [5].



Rys. 2. Podział protokołów trasowania w sieciach ad-hoc [4]

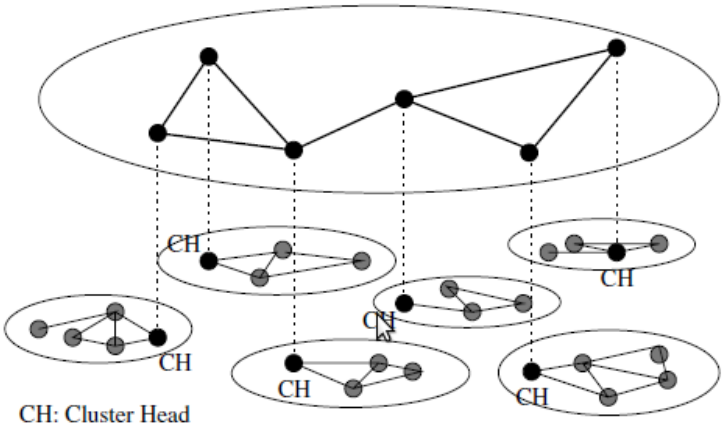
Biorąc pod uwagę sposób rozsyłania do innych węzłów aktualizacji, protokoły trasowania można sklasyfikować jako:

- unicastowe protokoły trasowania – protokoły przesyłające aktualizacje do każdego węzła z osobna,
- multicastowe protokoły trasowania – protokoły przesyłające informacje do grupy odbiorców jednocześnie.

Architektura trasowania w samoorganizujących się sieciach ad-hoc może być płaska lub hierarchiczna. W płaskiej architekturze każdy węzeł sieciowy postrzegany jest jako autonomiczny router, identyfikowany przez adres sieciowy. Nie zakłada się hierarchicznego podziału węzłów, a każdy węzeł realizuje identyczne zadania związane z wyznaczaniem tras. Przykładowe protokoły stosowane w sieciach płaskich to *Destination-Sequenced Distance Vector* (DSDV) i *Wireless Routing Protocol* (WRP). Węzły z tymi protokołami w swoich tablicach trasowania utrzymują trasy do wszystkich węzłów danej sieci. Niestety, stosowanie tych protokołów sprawdza się jedynie w sieciach o niewielkim rozmiarze, w których dynamika zmian topologii jest nieduża. Powodem jest ograniczona skalowalność protokołu, co oznacza, że w przypadku przyłączania się do sieci kolejnych węzłów wzrasta czas osiągania stanu

ustalonego. W przypadku dużych sieci powinien zatem zostać zastosowany protokół bazujący na hierarchicznym modelu trasowania.

Ideą trasowania hierarchicznego (rys. 3) jest łączenie węzłów w grupy zwane klastrami. Jeden z węzłów wyznaczany jest na węzeł główny, przechowujący informacje o przynależności węzłów do klastra. Brzegowy węzeł klastra stanowi bramę prowadzącą do innych klastrów i jest odpowiedzialny za obsługę ruchu międzyobszarowego.



Rys. 3. Hierarchiczna infrastruktura trasowania [7]

Brzegowy węzeł klastra, nazywany również stacją czołową, wybierany jest spośród węzłów funkcjonujących w danym obszarze. Wszystkie węzły pozostające w zasięgu transmisji stacji czołowej tworzą klaster. Po uformowaniu klastra każdy węzeł klastra utrzymuje tablicę zawierającą informację o innych węzłach w klastrze i stacji czołowej klastra. Routowanie pakietów poza klaster odbywa się z wykorzystaniem stacji czołowej klastra.

Ważnym aspektem procesu wyznaczania tras jest stopień wykorzystywania zasobów energetycznych węzła sieciowego. Duża aktywność protokołu routingu może znacząco wpływać na szybsze rozładowanie baterii węzła. Do technik służących oszczędzaniu energii zaliczyć można na przykład:

- wysyłanie aktualizacji z wykorzystaniem trybu transmisji multicast,
- unikanie retransmisji danych,
- wykorzystywanie protokołów reaktywnych, wprowadzających, w porównaniu z protokołami proaktywnymi, mniejsze obciążenie sieci pakietami aktualizacyjnymi, a więc pakietami o charakterze informacyjnym (sygnalizacyjnym).

Interesującym obszarem badań nad sieciami ad-hoc jest badanie skutków ataków sieciowych przy zastosowaniu określonego protokołu routingu

dynamicznego. Jako jedna z krytycznych usług w sieci, trasowanie jest częstym celem ataków [2]. Wszystkie węzły w sieci muszą ze sobą współpracować i wymieniać informacje w celu wyznaczania i utrzymywania tras. Fakt ten oraz łatwość prowadzenia podsłuchu sprawiają, że ochrona sieci przed atakami z wykorzystaniem podatności protokołów routingu jest trudna. Infrastruktura ad-hoc w większym stopniu niż sieć przewodowa podatna jest na typowe ataki związane z blokowaniem usług, „wstrzykiwaniem" fałszywych tras, podmianą pakietów, czy innymi działaniami związanymi z nieautoryzowanym badaniem topologii i właściwości urządzeń działających w sieci [2].

Ataki skierowane na protokoły trasowania charakteryzują się różną złożonością działań napastnika i rozmiarem skutków ataków. Zachowania napastnika są klasyfikowane jako służące:

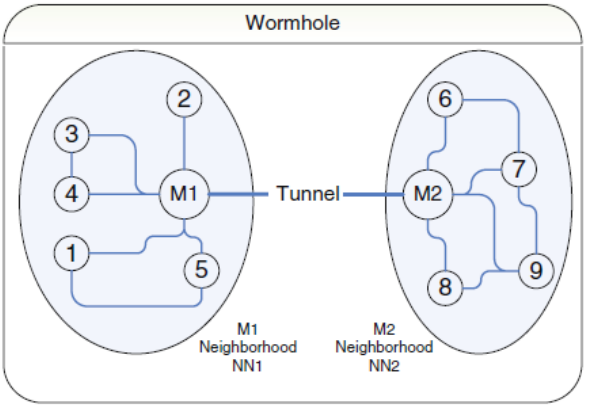
- podglądaniu tras,
- modyfikowaniu tras,
- uszkadzaniu tras.

Przy aktywnych atakach na mechanizmy trasowania celem może być nie tylko zmodyfikowanie lub zablokowanie procesu trasowania, ale również takie wpłynięcie na jego działanie, aby możliwe stało się przeprowadzenie ataku w wyższych warstwach modelu ISO/OSI. Pasywne ataki mogą mieć na celu między innymi podsłuchanie sieci w celu lokalizacji danego węzła, co dla przykładu w rozwiązaniach militarnych może mieć krytyczne znaczenie. Ataki pasywne są znacznie trudniejsze do wykrycia i wyeliminowania.

Typowe i szczególnie szkodliwe ataki na sieć ad-hoc to [4]:

1. Atak typu „czarna dziura" (ang. *black hole*) – w ataku tego typu pakiety są przekierowywane do nieistniejące punku docelowego, gdzie znikają. Można wyróżnić dwie odmiany ataku typu „czarna dziura". W pierwszej odmianie cały ruch jest kierowany do nieistniejącego węzła, w drugim natomiast osoba manipulująca trasami pakietów dokonuje przekierowania jedynie określonego strumienia pakietów do punktu pełniącego rolę „czarnej dziury".
2. Atak typu „tylne wejście" (ang. *wormhole*) – atak ten polega na stworzeniu tunelu pomiędzy dwoma zaatakowanymi węzłami granicznymi różnych obszarów sieci ad-hoc. Rys. 4 przedstawia sieć, w której pomiędzy węzłami M1 i M2 został stworzony tunel będący jedynym łącznikiem komunikacyjnym dla węzłów sąsiadujących z M1 oraz M2. Wskutek manipulacji trasami węzły należące do obu sieci posiadają informacje, że droga z jednej sieci do drugiej wiedzie przez tunel (trasa pakietów wymienianych między węzłami z różnych obszarów wiedzie przez zaatakowane węzły M1 i M2). Stworzenie takiego środowiska przez atakującego daje mu możliwości przeprowadzenia pasywnego lub aktywnego ataku, polegającego na monitorowaniu i analizie ruchu

sieciowego w celu określenia lokalizacji poszczególnych węzłów lub modyfikacji przesyłanych danych. Jest to jeden z trudniejszych do wykrycia ataków.



Rys. 4. Tunel między atakowanymi węzłami przy ataku *wormhole* [2]

3. Atak typu „podział sieci" (ang. *network partitioning*) – atak ma na celu odizolowanie części sieci poprzez usunięcie tras odnoszących się do tego obszaru.
4. Atak typu „zatruwanie pamięci podręcznej" (ang. *cache poisoning*) – atak ten polega na manipulacji informacjami o trasach znajdującymi się w pamięci podręcznej danego węzła.
5. Atak typu „uśpienie węzła" (ang. *sleep deprivation*) – atak ten ma na celu wyeliminowanie danego węzła poprzez pozbawienie go źródła zasilania. Sieć ad-hoc składa się głównie z mobilnych urządzeń wyposażonych w baterie, mające ograniczone czasowo możliwości dostarczania energii. W trakcie ataku tego typu, jeden z węzłów sieci, będący pod kontrolą atakującego, przesyła do innego węzła błędne informacje związane z trasowaniem. Informacje te są cały czas analizowane przez zaatakowany węzeł, co może znacznie skrócić czas jego działania.

Jedną z metod mających podnieść bezpieczeństwo procesu trasowania w sieciach ad-hoc jest dołączanie do istniejących protokołów trasowania rozszerzenia SRP (*Secure Routing Protocol)*. Opiera się ono na negocjacji tajnego klucza podczas procedury nawiązywania połączenia pomiędzy węzłami. Przykładem protokołu posiadającego wbudowane mechanizmy zabezpieczeń oparte na certyfikatach jest protokół ARAN (*Authenticated Routing for Ad-hoc Network*). Posiada on nie tylko mechanizmy uwierzytelniania, ale również zapewnia integralność przesyłanych między węzłami informacji [2].

3. Modelowanie i metodyka badań porównawczych protokołów trasowania dla sieci ad-hoc

W punkcie omówione zostanie przygotowanie uporządkowanego eksperymentu symulacyjnego, służącego porównaniu wybranych protokołów routingu dynamicznego dla sieci ah-hoc. Założono wykorzystanie pakietu symulacyjnego OPNET Modeler.

Symulacja komputerowa postrzegana jest jako skuteczna technika komputerowa służąca badaniu wydajności sieci komputerowych i analizie jej działania. Pakiet symulacyjny OPNET stanowi uznane narzędzie programowe do modelowania sieci i przeprowadzania badań symulacyjnych. Zawiera szczegółowe modele urządzeń sieciowych, przewodowych i bezprzewodowych, wiodących producentów sprzętu sieciowego. Umożliwia również własnoręczne modelowanie zachowania węzłów sieciowych, korzystających ze znanych lub modelowanych w środowisku OPNET protokołów.

Zasadnicze etapy eksperymentu symulacyjnego to:

- określenie celu badań;
- modelowanie środowiska sieciowego;
- wybór istotnych obserwowanych parametrów i wyznaczanych na ich podstawie charakterystyk;
- przeprowadzenie symulacji;
- zebranie i analiza wyników.

Ostatnim, szczególnie istotnym etapem badania symulacyjnego jest ocena adekwatności modelu i wiarygodności uzyskanych wyników [8]. W większości przypadków badań symulacyjnych z wykorzystaniem pakietu OPNET zakłada się adekwatność modeli urządzeń sieciowych i innych elementów dostępnych w bibliotece OPNET, a więc tym samym adekwatność modelu sieci zbudowanego z tychże urządzeń [9], [10], [11], [12]. Oczywiście w przypadku własnoręcznego modelowania od podstaw urządzenia sieciowego i procesów zachodzących z modelowanym środowisku, etap ten nie może być pominięty. Obalenie hipotezy o adekwatności modelu skutkuje zwykle powrotem do etapu modelowania. Wiarygodność uzyskanych wyników, związana z adekwatnością modelu i powtarzalnością eksperymentu, może być oceniona z użyciem odpowiednich testów statystycznych [8], [15].

Metodyka przygotowania i prowadzenia badań symulacyjnych wybranych protokołów trasowania zilustrowana została na drodze omówienia eksperymentu służącego zbadaniu jaki wpływ na funkcjonowanie sieci ma zastosowany protokół routingu dynamicznego przy różnej liczbie węzłów sieciowych i różnej szybkości poruszania się węzłów. Przedmiotem badań były: proaktywny protokół OLSR i dwa protokoły z grupy protokołów reaktywnych - AODV i DSR [14].

Moduł Wireless pakietu OPNET umożliwia modelowanie bezprzewodowych sieci mobilnych z uwzględnieniem protokołów warstwy MAC, warstwy sieci, transportowej i aplikacji. Umożliwia generowanie losowych trajektorii ruchu węzłów, zgodnie z wybranym rozkładem prawdopodobieństwa.

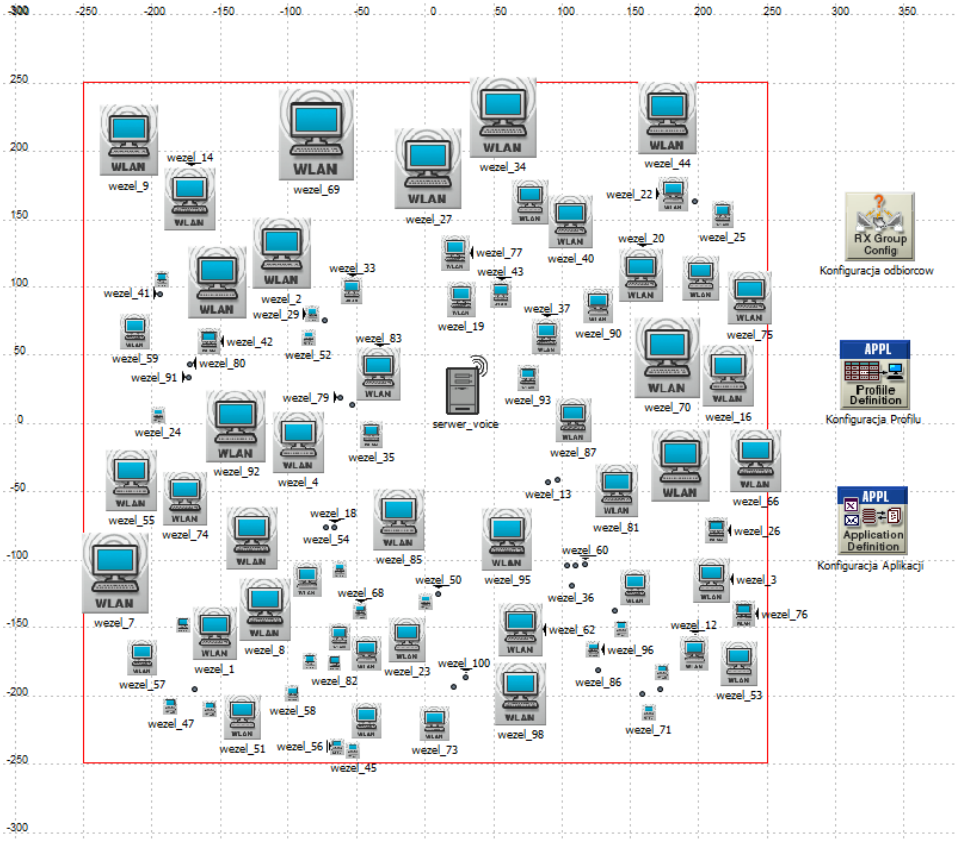
Podstawowym zadaniem modelowania komunikacji bezprzewodowej jest określenie maksymalnego zasięgu komunikacji między węzłami sieciowymi wyposażonymi w nadajnik i odbiornik radiowy. Komunikacja między węzłami sieciowymi jest możliwa wtedy, gdy węzeł X jest w stanie odebrać i zdekodować sygnał wysłany przez węzeł Y. Obowiązuje tu prosta zasada mówiąca, że transmisja dojdzie do skutku gdy moc sygnału odebranego przez węzeł X będzie większa od progu czułości jego odbiornika. Kluczowym staje się znalezienie modelu współczynnika utraty mocy sygnału w określonym środowisku sieciowym. W pracach badawczych, w zależności od celu badań, wykorzystywany jest jeden z trzech modeli tego współczynnika: model zmian dużej skali (ang. *path-loss*), model efektów średniej skali (ang. *shadowing*) i model efektów małej skali (ang. *fading*) [13]. Niestety, większość dostępnych symulatorów umożliwia skorzystanie z uproszczonego modelu *path-loss*.

Model *path-loss*, dostępny w środowisku OPNET, zakłada, że utrata mocy przesyłanego sygnału uzależniona jest od odległości euklidesowej między nadawcą i odbiorcą sygnału. Model *shadowing* jest modelem wolnych, losowych zmian mocy nadanego sygnału, wynikających z ukształtowania terenu, warunków atmosferycznych, niesymetrycznych wzmocnień anteny, itp. Model efektów małej skali zakłada z kolei szybkie, losowe zmiany amplitudy sygnału przy małej zmianie położenia węzła i/lub czasu symulacji [13].

Inne, ważne parametry modelu opisującego działanie węzła mobilnego, to:

- użyty standard sieci bezprzewodowej (np. 802.11g),
- moc nadawanego sygnału (zależna od charakterystyki użytej anteny),
- czułość odbiornika,
- mechanizm sterowania wymianą ramek (np. RTS/CTS),
- liczba prób retransmisji pakietu,
- wykorzystywane aplikacje i protokoły transportowe,
- wykorzystywany protokół routingu dynamicznego,
- obszar w jakim porusza się węzeł (obszar symulacji np. 1 km^2 = 1000 m x 1000 m),
- inne dane, typu ograniczenie maksymalnej szybkości transmisji węzła.

Model sieci wykorzystywany w omawianych badaniach przedstawiony został na rys. 5 [14].



Rys. 5. Model sieci ad-hoc zawierającej 100 węzłów [14]

Charakterystyczne dla symulacyjnych badań porównawczych jest manipulowanie wybranymi parametrami modelu symulacyjnego sieci. Zmiana parametrów modelu, jak np. zmiana liczby węzłów sieciowych, szybkości poruszania się węzłów, rozpiętości sieci, wykorzystywanego protokołu routingu, rodzi wiele scenariuszy symulacyjnych. Wyniki symulacji zgodnych z określonymi scenariuszami są podstawą oceny danego rozwiązania [11], [12].

Omawiana tutaj metodyka i wykonane zgodnie z nią badania bazują na uproszczonym modelu środowiska sieciowego, nie uwzględniającym topografii terenu, mającej zwykle istotny wpływ na zasięg transmisji węzła sieciowego, interferencje, zakłócenia sygnału, odbicia od różnych przeszkód, itp.

Scenariusze związane z przedstawionym modelem zakładały stacjonarność węzłów, użycie aplikacji VoIP (komunikowanie się węzłów z serwerem o nazwie *serwer_voice*) oraz zastosowanie różnych protokołów routingu. W scenariuszach symulacyjnych zmianie podlegała również liczba

węzłów sieciowych. Ten etap badań (przy stacjonarności węzłów) miał na celu wskazanie protokołu routingu, który w najmniejszym stopniu obciąża aktualizacjami sieć i tym samym nie wpływa znacząco na komunikację głosową w sieci (w przypadku transmisji VoIP znaczenie ma dostępne pasmo transmisyjne, wpływające na opóźnienie w dostarczaniu pakietów, jitter, wyrażający zmienność opóźnienia, czy liczba utraconych pakietów).

Inne scenariusze symulacyjne, rejestrowane w trakcie i wyliczane po zakończeniu eksperymentu symulacyjnego charakterystyki oraz hipotezy badawcze wyszczególnione zostały w rozdziale 4.

4. Założenia i przebieg eksperymentu symulacyjnego

Przedmiotem badań były: proaktywny protokół OLSR i dwa protokoły z grupy protokołów reaktywnych - AODV i DSR. Implementacje tych protokołów są najczęściej spotykane we współczesnych sieciach ad-hoc, a ich ocena często stanowi punkt odniesienia przy ocenianiu nowych, eksperymentalnych rozwiązań [9], [10], [11], [12].

Celem badań było porównanie wpływu wymienionych protokołów na funkcjonowanie sieci ad-hoc, w zależności od liczby oraz szybkości przemieszczania się węzłów sieciowych.

Zasadna wydawała się ocena [14]:

- prawdopodobieństwa dostarczenia pakietu do odbiorcy (ang. *packet delivery fraction* – PDF), mierzonego stosunkiem liczby odebranych pakietów przez wszystkie węzły sieciowe do liczby wysłanych pakietów przez wszystkie węzły źródłowe,
- obciążenia sieci wprowadzanego przez proces routingu (ang. *normalized routing load* – NRL), wyrażanego stosunkiem średniej liczby wysłanych pakietów przez proces routingu do średniej liczby odebranych pakietów danych przez węzły sieci ad-hoc,
- liczby odrzuconych przez węzły sieciowe pakietów (ang. *packets dropped*), nie wliczając pakietów kontrolnych (generowanych przez proces routingu),
- średniego czasu transmisji pakietów (ang. *delay*),
- średniej, dostępnej przepustowości sieci (szybkości przesyłania danych w sieci (ang. *throughput*)).

Wartości parametrów „*packets dropped*”, „*throughput*” i „*delay*” dostępne są natychmiast po zakończeniu symulacji (automatyczne zliczanie w trakcie symulacji), natomiast PDF i NRL wyliczone zostały na podstawie:

- liczby wysyłanych pakietów przez proces routingu,

- liczby wysyłanych przez węzły pakietów danych,
- liczby odebranych pakietów danych przez wszystkie węzły sieciowe.

Przed rozpoczęciem symulacji sformułowano hipotezy, które miały być potwierdzone przez wyniki symulacji. Hipotezy te są następujące [14]:

- wraz ze wzrostem liczby węzłów, niezależnie od wybranego protokołu routingu w sieciach ad-hoc:
  - zmniejsza się prawdopodobieństwo dostarczenia pakietów,
  - zwiększa się obciążenie sieci przez proces routingu oraz opóźnienie w dostarczaniu pakietów;
- wraz z przyrostem szybkości poruszania się węzłów w sieci ad-hoc, niezależnie od wybranego protokołu routingu:
  - zmniejsza się prawdopodobieństwo dostarczenia pakietów oraz szybkość przesyłania danych,
  - zwiększa się obciążenie sieci przez proces routingu, liczba odrzucanych pakietów oraz opóźnienie w dostarczaniu pakietów;
- w sieciach z protokołami reaktywnymi DSR i AODV, w porównaniu z sieciami z protokołem OLSR, występują większe opóźnienia ze względu na wymianę wiadomości kontrolnych przed wysyłaniem pakietów;
- obciążenie sieci wprowadzane przez protokół OLSR jest większe w porównaniu z obciążeniem sieci pakietami kontrolnymi generowanymi przez protokoły reaktywne DSR i AODV (w związku z okresową aktualizacją informacji o topologii sieci);
- w sieciach z protokołem OLSR szybkość przesyłania danych jest największa ze względu na implementację węzłów *multipoint relays;*
- szybkość przesyłania danych w sieciach z zaimplementowanym protokołem DSR jest najmniejsza z powodu czasowego wykorzystywania zdezaktualizowanych ścieżek (ang. *stale routes*) z tablicy *route cache*;
- protokół DSR jest efektywniejszym od AODV protokołem wyszukiwania tras w sieciach o dużej szybkości przemieszczania się węzłów.

Po sformułowaniu hipotez określone zostały parametry modelu sieci. Tab.2 prezentuje istotne parametry ogólne, parametry węzłów sieciowych i serwera VoIP używanych w eksperymencie symulacyjnym.

W określonych scenariuszach symulacyjnych węzły mogły przemieszczać się poza obszar sieci ad-hoc, stąd obszar objęty symulacją (1km2) jest większy od obszaru sieci (0,25km2).

Tab. 2. Zestawienie elementów wykorzystanych w symulacji [14]

Ustawienia ogólne	Symulowane protokoły	OLSR, AODV, DSR
	Czas symulacji	60 sekund
	Obszar symulacji	1 km^2
	Rozpiętość sieci ad-hoc	0,25km^2
	Standard sieci bezprzewodowej	802.11g
	Warstwa fizyczna sieci	Extended Rate PHY (802.11g)
	Liczba węzłów sieciowych	25, 50, 75, 100
	Szybkość przemieszczania się węzłów	1m/s, 5m/s, 10m/s, 15m/s
	Generowany ruch sieciowy	VoIP
Konfiguracja węzłów	Maksymalna szybkość transmisji pojedynczego węzła	1 Mb/s
	Moc nadawanego sygnału	0,5 mW
	Czułość odbiornika	-95 dBm
	Pojemność bufora WLAN (ang. WLAN buffer)	64000 bitów (6250 kb)
	Akcja podejmowana przy przekroczeniu przez ramki maksymalnej wielkości	Odrzucanie
	Mechanizm wymiany ramek RTS/CTS	Wyłączony
	Mechanizm CTS-to-self	Włączony
	Liczba prób retransmisji pakietu	7
Konfiguracja serwera głosowego	Liczba serwerów	1
	Szybkość poruszania się serwera	Serwer nie przemieszcza się
	Maksymalna szybkość transmisji danych	54 Mb/s
	Moc nadawanego sygnału	0,1 W
	Czułość odbiornika	-95 dBm
	Bufor WLAN	1024000 bitów (1000 kb)
	Akcja podejmowana przy przekroczeniu przez ramki maksymalnej wielkości warstwy WLAN MAC	Odrzucanie
	Mechanizm wymiany ramek RTS/CTS	Wyłączony
	Mechanizm CTS-to-self	Włączony
	Liczba prób retransmisji pakietu	7

Przez obiekt o nazwie *„Konfiguracja odbiorców”* (rys. 5) zostało wprowadzone ograniczenie maksymalnej odległości węzłów, przy której

transmisja dochodzi do skutku (500m). Standardem bezprzewodowym wykorzystanym przez stacje jest 802.11g z rozszerzeniem warstwy fizycznej Extended Rate PHY (ERP)[1]. Dzięki wykorzystaniu tego rozszerzenia możliwe było ustawienie maksymalnej szybkości transmisji danych dla serwera do 54Mb/s. Węzły nadawały sygnał o mocy 0,5mW, przy czułości odbiornika -95dBm. Serwer nie przemieszczał się podczas symulacji i nadawał sygnał o mocy 0,1W. Bufor WLAN (występujący w warstwie MAC) służy do przechowywania pakietów danych odebranych od warstw wyższych. Maksymalny rozmiar bufora dla węzłów to 64000 bitów, dla serwera 1024000 bitów. W momencie przepełnienia bufora, pakiety danych dostarczone z warstw wyższych są odrzucane. W każdym scenariuszu występował jeden serwer, a pojemność jego bufora była dwukrotnie większa od pojemności bufora innych węzłów. Środowisko OPNET ogranicza maksymalną wielkość danych, która może być przetransmitowana przez warstwę WLAN MAC do 18432 bitów (2304 bajtów). W sytuacji, gdy wielkość danych odbieranych z warstw wyższych przekracza maksymalną, dane te są odrzucane. Wymiana ramek RTS/CTS została wyłączona ze względu na działanie mechanizmu CTS-to-self. W przypadku pakietów odrzuconych podejmowanych było do 7 prób retransmisji.

Ruch w sieci ad-hoc generowany był przez aplikację głosową VoIP (ang. *Voice over Internet Protocol*). Aplikacja ta wykorzystywała kodek (koder/dekoder) mowy G.723.1[2], który wymagał pasma sieci 5,3 kb/s. Na jeden przekazywany pakiet przypadało 7 ramek głosowych. Przekazywanie pakietu głosowego obarczone zostało dodatkowym opóźnieniem wynoszącym 0,02 sekundy, wynikającym z kompresji i dekompresji tegoż pakietu.

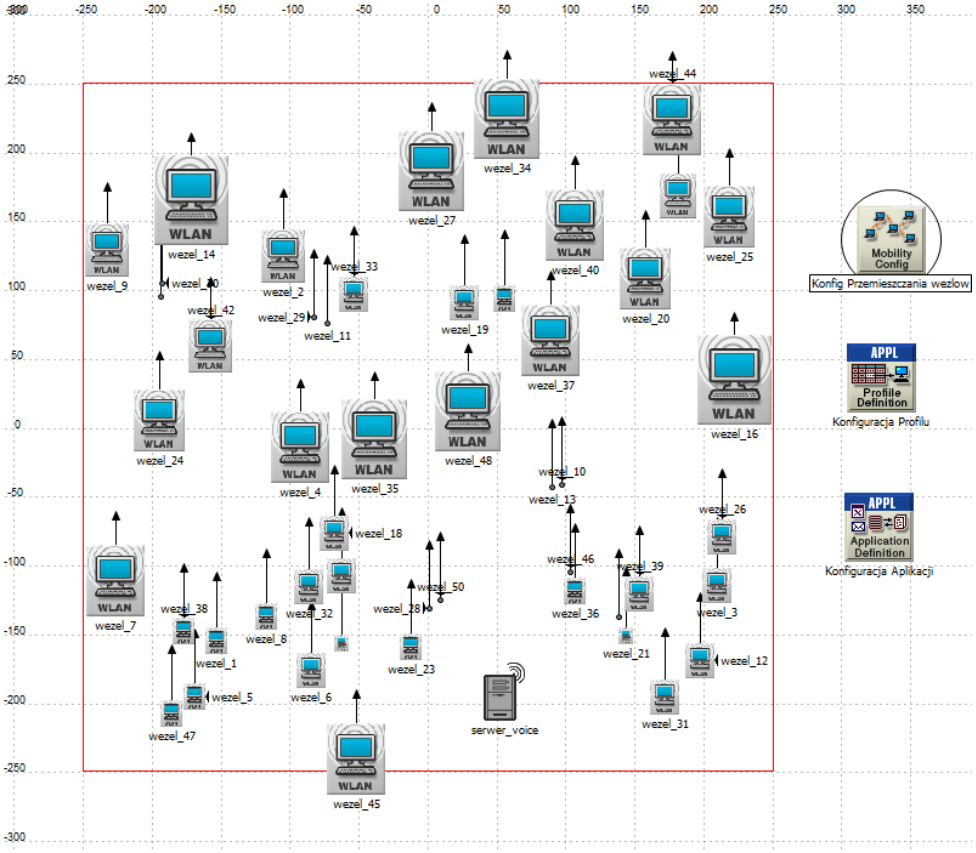
Scenariusze symulacyjne z badanymi protokołami routingu, objęte nazwą „Liczba węzłów", zawierały 25, 50, 75, 100 węzłów i jeden serwer. Obiekt „*Konfiguracja Aplikacji*" definiował aplikację głosową. Zdefiniowana aplikacja skojarzona była z profilem o nazwie *„Konfiguracja Profilu"* (rysunek 5). Profil ten został przypisany każdemu węzłowi oraz serwerowi.

Jak podano wcześniej w scenariuszach „Liczba węzłów" węzły i serwer nie poruszały się.

Rys. 6 ilustruje model sieci dla scenariuszy o nazwie „Mobilność".

[1] Extended Rate PHY (ERP) – rozszerzenie warstwy fizycznej WLAN dla standardu 802.11g. Wprowadza wsteczną kompatybilność ze standardem 802.11a, tym samym wspiera podobne szybkości transmisji: 6, 9, 12, 18, 24, 36, 48 i 54Mb/s.

[2] G.723.1 – koder/dekoder używany w komunikacji cyfrowej wykorzystujący modulację PCM. Częstotliwość próbkowania wynosi 8kHz z rozdzielczością 16 bitów na próbkę. G.723.1 oferuje przesyłanie sygnału w trybie full-duplex i half-duplex.



Rys. 6. Model sieci z liczbą 50 węzłów dla scenariuszy „Mobilność" [14]

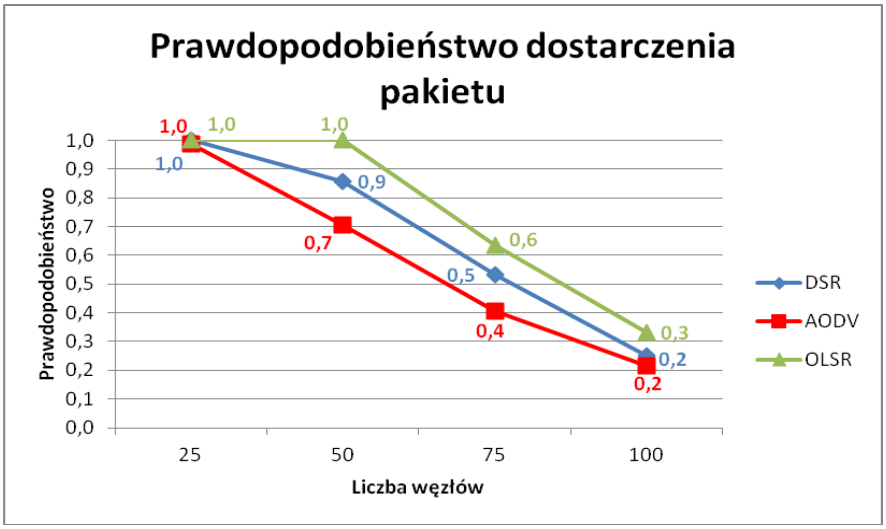
Sieć zawierała 50 węzłów i serwer. Wprowadzony został dodatkowy obiekt „Konfiguracja przemieszczania węzłów", definiujący sposób poruszania się węzłów. Wszystkie węzły, oprócz serwera, podlegały losowemu przemieszczeniu się (sposób przemieszczania był zgodny z modelem *Random Mobility Model*[3]*).* W modelu zastosowano stałą szybkość transmisji (tab. 2).

W każdym scenariuszu „Mobilność" węzły zaczynały się przemieszczać w losowym kierunku w 10 sekundzie trwania symulacji. W 30 sekundzie węzły zatrzymywały się na losowy okres czasu, po czym, jeżeli nie upłynął czas symulacji, ponownie podlegały przemieszczaniu.

[3] Random Mobility Model – opracowany przez Davida *Johnsona* i Davida *Maltz'a* model losowego przemieszczania się węzłów wykorzystywany w celach symulacyjnych protokołów routingu dynamicznego w sieciach MANET. Model ten określa losowy schemat poruszania, położenia i prędkości węzłów (stacji) w sieci.

Po udanym przeprowadzeniu symulacji opartych o różne scenariusze zebrano wyniki niezbędne do porównania protokołów. Wyniki zilustrowano na wykresach generowanych w środowisku OPNET oraz wykresach opracowanych z wykorzystaniem Microsoft Excel.

Wynik przykładowego eksperymentu ze scenariuszami zakładającymi stacjonarność węzłów przedstawiony został na rys. 7.



Rys. 7. Prawdopodobieństwo dostarczenia pakietu w zależności od liczby węzłów sieci ad-hoc [14]

Wykres ilustruje jaki wpływ na prawdopodobieństwo dostarczenia pakietu do odbiorcy (nie bez znaczenia w sieciach VoIP) ma zastosowany protokół routingu dynamicznego i potwierdza tezę, że w sieciach stacjonarnych węzłów korzystniejsze jest stosowanie protokołów proaktywnych, takich jak np. protokół OLSR.

5. Podsumowanie

W artykule omówiono proces przygotowania i realizacji badań symulacyjnych wybranych protokołów routingu dynamicznego dla sieci urządzeń mobilnych. Wybranym aspektem badań, warunkującym kształt modeli i scenariuszy symulacyjnych, była ocena wpływu zastosowanego protokołu na funkcjonowanie sieci (jakość transmisji w sieci ad-hoc).

Szczególnego znaczenia dla powodzenia eksperymentu symulacyjnego i uzyskania miarodajnych wyników nabiera dostępność programowych pakietów symulacyjnych, takich jak OPNET Modeler. Zastosowanie pakietu OPNET pozwoliło w krótkim czasie przygotować eksperyment zgodnie z wybraną metodą realizacji zadania i założonym programem badań.

Omówiony przebieg przykładowego eksperymentu zakładał użycie dostępnych w OPNET implementacji trzech wybranych protokołów (OLSR, AODV i DSR). Niestety, również w przypadku rozbudowanego pakietu OPNET, badania nad nowymi rozwiązaniami wymagają włożenia znacznego wysiłku w przygotowanie modeli węzłów sieciowych funkcjonujących zgodnie z założeniami badacza.

Szczegółowe wyniki badań symulacyjnych implementacji protokołów routingu dla sieci ad-hoc zawarte są w [14] i zostaną przedstawione w przyszłym artykule.

Literatura

[1] SARKAR S. K., BASAVARAJU T. G., PUTTAMADAPPA C., *Ad Hoc Mobile Wireless Networks Principles, Protocols, and Applications*, Taylor & Francis Group, 2007.

[2] NATO Research and Technology Organisation, Awareness of Emerging Wireless Technologies: Ad-hoc and Personal Area Networks Standards and Emerging Technologies, Online, 2007.

[3] MISRA S., MISRA S. C., WOUNGANG I., *Guide to Wireless Ad Hoc Networks,* Springer-Verlag, London, 2009.

[4] MOHAPATRA P., KRISHNAMURTHY S. V., *Ad Hoc networks (Technologies and Protocols),* Springer, 2005.

[5] BOUKERCHE A., *Handbook of Algorithms for Wireless Networking and Mobile Computinng,* Chapman & Hall, 2006.

[6] BASAGNI S., CONTI M., GIORDANO S., STOJMENOVIC I., *Mobile Ad Hoc Networking,* IEEE Press, New Jersey.2004.

[7] PIERRE S., BARBEAU M., KRANAKIS E., *Ad Hoc , Mobile and Wireless Networks,* Springer, Montreal, 2003.

[8] *Symulacja sieci komputerowych,*(red. M.Nowak) IITiS PAN, Gliwice, 2009.

[9] GUPTA S. K., SADAWARTI H., VERMA A. K., *Performance Analysis of AODV, DSR & TORA Routing Protocols,* IACSIT International Journal of Engineering and Technology, Vol.2, No.2, April, 2010, pp. 226-231.

[10] MAKKAR A., BHUSHAN B., TANEJA S., *Behavioral Study of MANET Routing Protocols,* International Journal of Innovation, Management and Technology, Vol. 2, No. 3, June, 2011, pp. 201-216.

[11] SRIKANTH T., NARSIMHA V. B., *Simulation-based approach to performance study of routing protocols in MANETs and ad-hoc Networks*, IJCSNS International Journal of Computer Science and Network Security, VOL.11 No.9, September ,2011, pp. 111-115.

[12] SAJJAD A., ASAD A., *Performance Analysis of AODV, DSR and OLSR in MANET,* Department of Electrical Engineering with emphasis on Telecommunication Blekinge Institute of Technology, Sweden, 2009.

[13] SIKORA A., *Modelowanie, symulacja i przykładowe zastosowania mobilnej bezprzewodowej sieci typu ad-hoc,* Zeszyty Naukowe WSInf Vol 7, Nr 1, 2008, str. 98-114.

[14] PIERSA K., *Badania symulacyjne protokołów routingu dynamicznego w sieciach ad hoc,* praca dyplomowa, Wydział Cybernetyki, Wojskowa Akademia Techniczna, Warszawa, 2012.

[15] KAMYS B., *Statystyczne metody opracowania pomiarów,* Instytut Fizyki UJ, users.uj.edu.pl/~ufkamys/BK/smop1N_h.pdf .

Research methodology of routing protocols for ad hoc networks

ABSTRACT: This paper describes dynamic routing protocols for ad hoc networks as a matter of simulation. The principles of preparation and implementation of a simulation experiment were presented. An example of the experiment was to illustrate the impact of the used routing protocol on the functioning of ad hoc networks. Results of the simulation will indicate the preferred mode of updating routes in routing tables of the mobile nodes of a certain size network and various speed of nodes.

KEYWORDS: mobile ad hoc networks, dynamic routing protocols, simulation studies

Praca wpłynęła do redakcji: 30.10.2012