Warszawa, 2.06.2017r.

dr hab. inż. Andrzej Bęben
Instytut Telekomunikacji
Politechnika Warszawska

Recenzja rozprawy doktorskiej kpt. mgr inż. Krzysztofa Maślanki

Rozprawa doktorska kpt. mgr inż. Krzysztofa Maślanki, pt. "Zarządzanie konfiguracją ruterów brzegowych w taktycznych sieciach IP" została opracowana na Wydziale Elektroniki Wojskowej Akademii Technicznej w Warszawie. Promotorem pracy jest prof. dr hab. inż. Marek Amanowicz, a promotorem pomocniczym jest ppłk. dr inż. Jarosław Krygier. Rozprawa dotyczy opracowania nowatorskiego systemu autokonfiguracji ruterów brzegowych w taktycznych, wielodomenowych sieciach łączności bazujących na protokole IP (*Internet Protocol*), który zapewnia ciągłość działania systemu łączności w przypadku wystąpienia nieplanowanych zmian topologii sieci. Opracowany system, nazywany systemem SYBRA (*SYstem of Border Router Autoconfiguration*), umożliwia: 1) przechowywanie danych dotyczących konfiguracji sieci w ramach rozproszonej, odpornej na awarie/uszkodzenia bazy danych, wykorzystującej mechanizmy sieci p2p (*peer-to-peer*), 2) monitorowanie zmian topologii sieci przez analizę otoczenia ruterów brzegowych poszczególnych systemów autonomicznych, 3) realizację procedur automatycznego odtworzenia spójności wielodomenowej, taktycznej sieci łączności przez automatyczną rekonfigurację ruterów brzegowych, pomiędzy którymi istnieje możliwość wymiany danych. W szczególności, opracowany system SYBRA umożliwia realizację następujących scenariuszy: a) ustanowienie nowego połączenia pomiędzy współpracującymi systemami autonomicznymi, b) dołączenie izolowanego węzła do systemu łączności, c) podział (scalenie) systemu autonomicznego w wyniku utraty (odtworzenia) łączności pomiędzy węzłami danego systemu autonomicznego.

W ramach rozprawy przedstawiono: 1) krytyczną analizę aktualnego stanu badań dotyczących protokołów rutingu stosowanych w sieciach IP oraz taktycznych sieciach łączności. W szczególności, została przedstawiona analiza literatury dotycząca protokołu rutingu międzydomenowego BGP (*Border Gateway Protocol*) oraz proponowanych rozszerzeń wspierających mobilność sieci; 2) projekt systemu SYBRA umożliwiającego autokonfigurację ruterów brzegowych w taktycznych, wielodomenowych sieciach łączności, 3) implementację prototypu systemu SYBRA, 4) wyniki badań efektywności systemu SYBRA dotyczące oceny czasu rekonfiguracji sieci oraz wymaganego dodatkowego ruchu sygnalizacyjnego, oraz 5) wyniki oceny skalowalności systemu dotyczące wpływu topologii sieci oraz liczby ruterów brzegowych w systemie autonomicznym.

1. Cel badań (w odniesieniu do tez rozprawy)

Celem rozprawy jest opracowanie systemu automatycznej konfiguracji ruterów brzegowych w taktycznych, wielodomenowych sieciach łączności bazujących na protokole IP (*Internet Protocol*). Celem systemu jest zapewnienie ciągłości działania taktycznej sieci łączności w przypadku

wystąpienia nieplanowanych zmian topologii sieci. Cel rozprawy został zrealizowany przez zaprojektowanie systemu SYBRA, implementację jego prototypu oraz przeprowadzenie badań efektywności działania systemu w środowisku emulatora sieci. Ponadto, w rozprawie zamieszczono wyniki oceny skalowalności opracowanego systemu. Eksperymenty przeprowadzono w środowisku emulatora wielodomenowej, taktycznej sieci łączności, rozważając scenariusze zmiany topologii sieci, tj. a) ustanowienie nowego połączenia, b) dołączenie izolowanego węzła, c) podział (scalenie) systemu autonomicznego, które są charakterystyczne dla wielodomenowej sieci.

W rozprawie sformułowano tezę, iż "*wykorzystanie techniki peer-to-peer w ruterach brzegowych umożliwia skuteczną ich autokonfigurację w warunkach dynamicznych zmian struktury sieci*". Powyższą tezę udowodniono przez przeprowadzenie szerokiego zakresu eksperymentów wykorzystując zaimplementowany prototyp systemu SYBRA. Wnioski z przeprowadzonych eksperymentów potwierdziły, iż opracowany system umożliwia utrzymanie spójności sieci przez automatyczną konfigurację ruterów brzegowych w czasie zbliżonym do rzeczywistego. Ponadto, uzyskane wyniki potwierdziły słuszność sformułowanej tezy rozprawy.

2. Charakter rozprawy

Postawione w rozprawie zadanie, zaproponowane rozwiązanie oraz przeprowadzone badania mają charakter naukowy, a uzyskane wyniki mogą być zastosowane w praktyce. Należy zwrócić uwagę, iż autokonfiguracja sieci jest obecnie jednym z wymagań stawianym nowym rozwiązaniom sieciowych opracowywanym w ramach Internetu Przyszłości. Nowe rozwiązania powinny cechować się właściwościami samo-zarządzania (*self management*) oraz samo-konfiguracji (*self configuration*), tak aby istotnie uprościć działania operatora sieci. Z tego powodu, rozważane w rozprawie zagadnienie jest zgodne z aktualnymi kierunkami badań. Przedstawione rozwiązanie, wykorzystujące elementy techniki sieci p2p, należy uznać za nowatorskie.

3. Sposób przeprowadzenia analizy źródeł. Sposób sformułowania wniosków wynikających z analizy źródeł

Przedstawiona w rozprawie analiza stanu badań dotyczących protokołów rutingu międzydomenowego stosowanych w sieciach taktycznych zawiera odwołania do ponad 40 prac (w tym prac autora), które obejmują publikacje konferencyjne, artykuły z czasopism, oraz zalecenia standaryzacyjne, np. IETF oraz NATO. Analiza stanu badań jest wyczerpująca, gdyż obejmuje większość rozważanych obecnie rozwiązań dotyczących rozszerzenia protokołu BGP o funkcje wspierania mobilności węzłów sieci. Przedstawione wnioski z analizy świadczą o dobrej znajomości kierunków aktualnie prowadzonych badań dotyczących rutingu międzydomenowego w sieciach taktycznych, jak również trafnych spostrzeżeń dotyczących ograniczeń obecnie proponowanych rozwiązań. Przedstawiona w rozdziale 3, analiza stanu badań dotyczących sieci p2p obejmuje odwołania do ponad 30 publikacji. Jednakże, są to jedynie podstawowe rozwiązania, takie jak Chord, Kademlia, Pastry bazujące na jednowymiarowej przestrzeni adresowej. Wybór rozwiązania Kademlia jako podstawy dla budowy projektowanego systemu rozproszonej bazy danych jest dość arbitralny, bazujący jedynie na wynikach opublikowanych w pracach [59-62]. Niewątpliwie wartościowym byłoby przeprowadzenie eksperymentów umożliwiających ocenę efektywności rozważanych rozwiązań w oparciu o własne doświadczenia autora.

Pewnym mankamentem analizy źródeł jest brak analizy rozwiązań dla automatycznego wykrywania topologii sieci, np. NDP (*Neighbor Discovery Protocol*), LLDP (*Link Layer Discovery Protocol*), czy Bonjour. Analiza tych rozwiązań mogłaby być pomocna w projektowaniu mechanizmu rozpoznawania otoczenia w ruterze brzegowym.

4. Rozwiązanie przedstawionego zadania, właściwości przyjętych metod i założeń

Problem utraty spójności taktycznej, wielodomenowej sieci łączności w wyniku nieplanowanej zmiany topologii sieci rozwiązano przez zaprojektowanie systemu SYBRA i implementację jego prototypu. System SYBRA jest odpowiedzialny za identyfikację wystąpienia zmiany międzydomenowej topologii sieci przez analizę otoczenia ruterów brzegowych oraz określenie rodzaju występującej zmiany topologii, np. nowe połączenie pomiędzy domenami, dołączenie izolowanego węzła, podział lub scalenie systemu autonomicznego. Następnie, system automatyczne uaktualnia konfigurację ruterów brzegowych, aby uzyskać spójność sieci. Automatyczna konfiguracja jest realizowana wykorzystując informacje zawarte w rozproszonej bazie danych wykorzystującej struktury sieci p2p, co pozwala zachować prawidłowe działanie nawet w przypadku utraty znaczącej liczby węzłów.

Prawidłowe działanie zaprojektowanego systemu zostało zweryfikowane eksperymentalne, w środowisku emulatora taktycznej sieci łączności. Przeprowadzone eksperymenty dotyczyły oceny efektywności działania systemu oraz oszacowania skalowalności systemu. W ramach testów efektywności zbadano czas rekonfiguracji sieci oraz ruch sygnalizacyjny generowany przez system SYBRA w odpowiedzi na zmianę topologii. W eksperymentach rozważono wszystkie scenariusze zmian topologii przyjęte w założeniach na system. Uzyskane wyniki potwierdziły, iż we wszystkich rozważanych przypadkach opracowany system umożliwił odtworzenie spójności sieci łączności, a czas rekonfiguracji sieci oraz generowany dodatkowy ruch sygnalizacyjny był akceptowalny z punktu widzenia wymagań sieci taktycznych. Eksperymenty dotyczące skalowalności systemu wykazały, że czas rekonfiguracji ruterów brzegowych jedynie w niewielkim stopniu zależy od liczby i topologii sieci. Czas uzyskania zbieżności rutingu jest dość silnie zależny od liczby ruterów oraz topologii, co wynika bezpośrednio z własności protokołu BGP. Istotnym elementem ograniczającym skalowalność rozwiązania jest znaczący wzrost ruchu sygnalizacyjnego obserwowany wraz ze wzrostem liczby ruterów brzegowych. Niewątpliwie wartościowym byłoby zdefiniowanie dodatkowym mechanizmów ograniczających ruch sygnalizacyjny.

Założenia przyjęte na etapie projektowania systemu oraz sposób weryfikacji w postaci przeprowadzonych eksperymentów z prototypem systemu badanym w środowisku emulatora sieci zasadniczo są poprawne. Pewnym mankamentem jest przyjęcie w wiadomości *Net_Address_Set* (Rys. 21c) wartości adresu maski jako pola o długości 4 bajtów, podczas gdy wystarczające jest zastosowanie pola o rozmiarze 5 bitów do przesłania rozmiaru maski sieciowej. Ponadto, w zależnościach (3-5) przyjęto stałą wartość M, podczas gdy wydaje się iż wartość M dotyczy danej relacji, zatem powinna być również indeksowana.

W przypadku przeprowadzonych badań nie porównano wyników uzyskanych w eksperymentach z wartościami odniesienia, np. wartościami teoretycznymi uzyskanymi z analizy systemu bądź wartościami uzyskanymi z symulacji. Ponadto, niewątpliwym wzbogaceniem części eksperymentalnej byłby przeprowadzenie wybranych eksperymentów w rzeczywistych warunkach (lub co najmniej modelu sieci) wykorzystujących fizyczne rutery stosowane w sieci taktycznej.

5. Oryginalność rozprawy, samodzielny dorobek autora, pozycja rozprawy w stosunku do stanu wiedzy (poziom techniki) prezentowanego w literaturze światowej

Zaproponowane rozwiązanie problemu utraty spójności taktycznej, wielodomenowej sieci łączności w wyniku nieplanowanej zmiany topologii sieci, bazujące na autokonfiguracji ruterów brzegowych inicjowanej przez opracowany protokół odkrywania otoczenia ruterów brzegowych jest zgodne z aktualnymi kierunkami badań dotyczącymi opracowania samo-konfigurowalnych sieci. W mojej ocenie proponowane rozwiązanie stanowi istotne rozszerzenie rozważanych obecnie rozwiązań dla protokołu BGP. Przedstawione rozwiązanie jest szczególnie istotne dla sieci taktycznych, charakteryzujących się znaczą dynamiką zmian topologii sieci wynikającą z prowadzonych działań. Niewątpliwie oryginalnym rozwiązaniem jest realizacja rozproszonej bazy danych przechowującej informację o konfiguracji domeny w postaci sieci nakładkowej wykorzystującej technikę sieci p2p.

Samodzielnym dorobkiem autora jest: 1) opracowanie analizy stanu badań dotyczących protokołów rutingu w taktycznych sieciach łączności, 2) zaprojektowanie systemu autokonfiguracji ruterów brzegowych w taktycznych, wielodomenowych sieciach łączności, obejmujące opracowanie protokołu analizy otoczenia ruterów brzegowych, opracowanie rozproszonej bazy danych bazującej na strukturze sieci p2p, oraz metody konfiguracji ruterów brzegowych, 3) implementacji prototypu systemu, 4) przeprowadzenie badań efektywności systemu oraz 5) ocena skalowalności systemu.

6. Poprawność przedstawienia uzyskanych wyników (zwięzłość, jasność, umiejętność przekonywania, poprawność redakcyjna).

Przeprowadzone eksperymenty oraz uzyskane wyniki zostały przedstawione w sposób zwięzły, logiczny i klarowny. Przeprowadzone eksperymenty wskazują zarówno pozytywne strony proponowanego rozwiązania, jak również pewne niekorzystne cechy (np. istotny wzrost ruchu sygnalizacyjnego w sieciach o dużej liczbie ruterów brzegowych), co pozwala na określenie warunków stosowalności proponowanego rozwiązania.

Pewnym mankamentem jest brak przedstawienia na wykresach przedziałów ufności, pomimo iż opis eksperymentów zakładał wyznaczenie 95% przedziałów ufności. Zamieszczenie przedziałów ufności jest szczególnie istotne w przypadku rys. 37, na którym prezentowane wartości są mocno zbliżone, a zatem istnieje obawa, iż prezentowane wyniki są statystycznie tożsame.

Ponadto, wnioski z eksperymentu przedstawione na str. 64, tj. ".. zwiększenie czasu Ts, powoduje wzrost wolumenu ruchu.." są niezrozumiałe. W szczególności, że wyniki przedstawione na rys. 29, których dotyczą przedstawione wnioski wskazują, iż zależność jest odwrotna, tj. większa wartość czasu Ts, a zatem mniejsza częstotliwość wysyłania wiadomości sygnalizacyjnych, skutkuje mniejszym obciążeniem ruchem sygnalizacyjnym.

Niestety autor nie uniknął drobnych uchybień językowych, np., str. 53 "plikowa baza danych", str. 67 "Na podstawie przedstawione powyżej wyników", „występują w trasie do wybranego prefiksu”, oraz błędów redakcyjnych, np. błędne odwołania str. 21 [33] a powinno być [34], rys. 19 jest kopią rys. 18, natomiast zamieszczony opis dotyczy innego, niezamieszczonego w rozprawie rysunku.

Powyższe uchybienia nie mają jednak istotnego wpływu na wartość merytoryczną pracy.

7. Słabe strony rozprawy i jej główne wady.

Do słabych stron rozprawy zaliczam:

1. Brak zastosowania modeli analitycznych do oceny efektywności proponowanego rozwiązania. Niewątpliwie, opracowanie modeli analitycznych dotyczących czasów konfiguracji oraz oszacowania ruch sygnalizacyjnego znacząco wzbogaciłoby pracę. Ponadto, wyniki uzyskane z analizy systemu (choćby analizy granicznych przypadków) umożliwiłby porównanie i ocenę wyników uzyskanych w przeprowadzonych eksperymentach.

2. Pominięcie analizy źródeł dotyczących rozwiązań dla automatycznego wykrywania topologii sieci, np. protokołów NDP (*Neighbor Discovery Protocol*), LLDP (*Link Layer Discovery Protocol*), czy Bonjour.

3. Brak przeprowadzenia eksperymentów w rzeczywistych warunkach sieci taktycznej (lub modelu sieci wykorzystującym fizyczne rutery. Przeprowadzenie takiego eksperymentu potwierdziłoby możliwość działania systemu w sieci taktycznej oraz umożliwiłoby porównanie wyników uzyskanych w środowisku emulatora sieci.

4. Niewielka liczba publikacji autora dotyczących tematyki rozprawy.

8. Przydatność rozprawy dla nauk technicznych, przemysłu, obronności kraju, itp.

Przedstawione w rozprawie rozwiązanie umożliwiające autokonfigurację ruterów brzegowych w taktycznej sieci łączności stanowi istotne rozszerzenie rozważanych obecnie rozwiązań dla protokołu BGP. Przedstawione rozwiązanie jest szczególnie istotne dla sieci taktycznych, charakteryzujących się znaczą dynamiką zmian topologii sieci wynikającą z prowadzonych działań. Opracowane rozwiązanie może mieć bezpośredni wpływ na przemysł i obronność kraju.

9. Podsumowanie (czy rozprawa spełnia wymagania przez obowiązujące przepisy)

Przedstawiony w rozprawie projekt systemu autokonfiguracji ruterów brzegowych w taktycznych, wielodomenowych sieciach łączności bazujących na protokole IP (*Internet Protocol*), który zapewnia ciągłość działania systemu łączności w przypadku wystąpienia nieplanowanych zmian topologii sieci stanowi oryginalne rozwiązanie problemu, które spełnia warunki stawiane rozprawom doktorskim zgodnie z "Ustawą o Stopniach Naukowych i Tytule Naukowym oraz o Stopniach i Tytule w Zakresie Sztuki", z dnia 14 marca 2003 roku wraz z późniejszymi zmianami, w części dotyczącej stopnia doktora, i po spełnieniu innych warunków formalnych wnoszę o jej publiczną obronę.