RELIABILITY OF ROUTING PROTOCOLS

NIEZAWODNOŚĆ PROTOKOŁÓW ROUTINGU

Rafał Polak, Dariusz Laskowski

Wojskowa Akademia Techniczna

e-mail: rafal.polak@wat.edu.pl, dlaskowski@wat.edu.pl

Abstract: The article refers to the impact of damage and dynamic variables on operation of routing protocols and consequently to the whole network. On this purpose, there was introduced the characteristic of the routing protocols and both an internal and an exterior gateway. Then, it was built the network architecture based on the TCP / IP stack. In the stack, there were created three autonomous systems and one of them was the backbone of the network. What is more, reliability tests, which have been performed, consisted of a resistance to physical damage to the network and dynamically changing parameters of the network as well as performance tests.

Keywords: reliability, routing, network protocols

Streszczenie: Artykuł porusza tematykę wpływu uszkodzeń i zmiennych dynamicznych na działanie protokołów routingu i w konsekwencji całej sieci. W tym celu zapoznano się z charakterystyką routingu oraz protokołów wewnątrz i międzydomenowych. Następnie zbudowano architekturę sieciową opartą o stos protokołów TCP/IP, w której utworzono trzy systemy autonomiczne, z wyróżnieniem szkieletu sieci. Wykonano testy niezawodnościowe polegające na odporności na narażenia fizyczne sieci i zmiany dynamiczne paramentów sieciowych oraz testy wydajnościowe.

Słowa kluczowe: niezawodność, routing, protokoły sieciowe

1. Wstęp

Podstawowym założeniem sieci teleinformatycznych jest wymiana danych między stacjami sieciowymi (tj. terminalami końcowymi, przełącznikami, routerami, serwerami, itp.). W ramach tej usługi wyróżnia się: komunikację między komputerami użytkowników, dostęp do zasobów sieci, transmisję danych i udostępnianie zasobów sprzętowych oraz usług pochodnych (tj. przeglądanie stron WWW, ftp, e-mail, itp.). Poprawność przesyłu danych wymaga wielodrożnego transportu pakietów w sieci. Urządzenia węzłowe (tj. routery) za pomocą protokołów trasowania zarządzają ruchem pakietów, wysyłając je oraz wskazując im optymalną drogę do adresata z punktu widzenia przyjętych determinant w metrykach.

Dynamicznie rozwijająca się techniki i technologie możliwe do implementacji w sieć teleinformatyczne są stymulantą przyczyniła się do ewolucji protokołów routingu pakietów. Docelowo istnieje możliwość zwiększenia efektywności i niezawodności przesyłu danych w warstwie sieci. Nowoczesne protokoły warstwy III wspierają również bezpieczeństwo i jakość danych.

2. Charakterystyka routingu

W obecnych czasach sieci teleinformatyczne znajdują szerokie zastosowanie praktyczne w wielu dziedzinach przedsiębiorczości ze względu na liczny zbiór usług. Głównym elementem sieci są agregatory ruchu, przełączniki warstwy II i III, i routery działające w warstwie III. Jednym z najważniejszych zadań routera jest wybór trasy przesyłu pakietów adekwatnie do trasowania statycznego lub dynamicznego. Każdy z tych sposobów wykorzystuje tablice routingu zawierające informacje o stanie interfejsów i zasobów transportowych sąsiadujących routerów. Poprawność uzupełniania tablic routingu są krytyczną determinantą wybierania i aktualizacji tras pakietów. Algorytmy funkcjonowania routera porównują adres docelowy z adresami sieci zawartymi w jego tablicy trasowania. Następnie wybierają optymalną trasę według zbioru zadanych i przyjętych do realizacji zasad - zwanych algorytmami trasowania.

Routing statyczny i dynamiczny

Pierwszy typ trasowania danych to routing statyczny polegający na ręcznej konfiguracji interfejsów routera w tablicy routingu celem odzwierciedlenia pożądaných relacji sieciowych. Znajdując one zastosowanie w architekturze sieci zawierające „niewielką” liczbę routerów np. do kilkunastu sztuk. Jednak w przypadku złożonych sieciach, gdzie liczba terminali może być liczona w setkach lub tysiącach to utrzymanie stanu zdolności takiej sieci może być dość skomplikowane i czasochłonne. Kolejnym typem trasowania jest routing dynamiczny wykorzystujący zautomatyzowany proces ustalania i zmian tras pakietów na podstawie aktualizacji informacji o stanie osiągalności sąsiednich routerów.

W przypadku, gdy do jednej podsieci prowadzi wiele zasobów transportowych (łączy, ścieżek), to protokoły trasowania ustalają optymalną trasę w oparciu o metryki routingu. Metryka jest wartością na podstawie, której protokół ocenia trasę. Niektóre protokoły routingu oceniają trasę na podstawie jednego czynnika, którego metryka to liczba skoków (liczba routerów) między routerem źródłowym a docelowym. Inne protokoły do wyboru trasy korzystają z dwóch, trzech bądź nawet i pięciu czynników tj.: przepływność (szerokość pasma), opóźnienie i jego zmienność, obciążenie, niezawodność, liczbę skoków, koszt, itp. Niektóre z tych czynników (tj. pasmo czy opóźnienie) są statyczne, czyli pozostają takie same dla każdego interfejsu do momentu przekonfigurowania routera lub zmiany w topologii sieci. Natomiast inne czynniki (tj. obciążenie czy niezawodność) to czynniki dynamiczne przeliczalne dla każdego interfejsu przez router w czasie rzeczywistym. Uwzględniając szeroki zbiór zalet i stosunkowo niewiele wad zasadnym jest stwierdzenie, że routing dynamiczny znajduje powszechniejsze zastosowanie w praktycznie eksploatowanych środowiskach sieci teleinformatycznych [1].

Protokoły routingu dynamicznego dzieli się na dwie kategorie: protokoły wewnątrzdomenowe IGP (ang. *Interior Gateway Protocol*) stosowane wewnątrz jednego systemu autonomicznego i międzysystemowe EGP (ang. *Exterior Gateway Protocol*) wymieniające dane między różnymi systemami autonomicznymi.

Protokoły routingu wewnątrzdomenowe

Pierwszym protokołem wewnątrz domenowym jest protokół RIP (ang. *Routing Information Protocol*) znajduje on zastosowanie, jako klasyczna metoda wymiany danych między routerami [2]. Posługuje się on algorytmem wektora odległości wybierając trasę z najmniejszą liczbą skoków, jako najkorzystniejszą trasę. Tablice trasowania są budowane dzięki wymienianym danym od sąsiednich stacji sieciowych w postaci pełnych tablic routingu. W przypadku wysłania przez router żądania o dane, otrzymuje on odpowiedź z konkretnymi danymi identyfikacyjnymi stan interfejsów. Za pomocą mechanizmu RIP router może wysyłać okresowo dane o swojej obecności i dane o aktualnej zawartości tablicy routingu. Aktualizacja tablic routingu odbywa się w stałych odstępach czasu (np. domyślnie 30 sekund) lub w przypadku zmian w topologii. Router po otrzymaniu tablicy od sąsiedniego routera, porównuje jej zawartość ze posiadaną tablicą i jeśli stwierdzi, że nastąpiła zmiana to wówczas zmienia lub dodaje zapisy np. o nowej trasie. Natomiast w przypadku, gdy znajdzie taką samą trasę tylko z niższą metryką to dokonuje zamiany na krótszą trasę. Klasycznym wyznacznikiem optymalnej trasy jest wektor odległości. Poważnym ograniczeniem RIP jest to, że jego metryka jest ograniczona do 15 skoków dla protokołu adresacji IPv4 i do 255 skoków dla IPv6 [3]. Oznacza to, że stacje sieciowe oddalone od routera dalej odpowiednio 15 lub 256 skoków są nieosiągalne dla tego protokołu, gdyż po tych skokach zostaną pakiety zatrzymane i usunięte z sieci.

Reprezentatywnym protokołem wewnątrz domenowym jest protokół OSPF (ang. *Open Shortest Path First*) i zawiera się on w grupie otwartych protokołów

trasowania typu „łącze-stan” [4]. OSPF cechuje się wysokim poziomem skalowalności. Routery korzystające z tego protokołu w przesyłanych komunikatach dostarczają sąsiadom dane o stanie swoich połączeń, następnie je przetwarzają porównując z aktualnymi i budują bazę danych stanów łącz na temat routerów znajdujących się w danym obszarze. Kolejnym etapem po zbudowaniu bazy danych jest utworzenie topologii sieci w postaci drzewa poprzez zastosowanie algorytmu SPF (ang. *Shortest Path First - Algorytm Dijkstry*). Wówczas to router tworzący jest korzeniem szkieletu sieci i optymalną trasę ustala się z uwzględnieniem kosztu, którym najczęściej jest szerokość pasma do sieci docelowego adresata danych. Routery budują relacje ze swoimi sąsiadami w celu efektywnego przekazywania danych o stanie swoich łącz. Protokół OSPF, jako metryki routingu używa kosztu podczas określania trasy. Koszt jest związany z przepływnością osiągalną na interfejsie routera i zależną od zewnętrznych danych dotyczących trasowania, oszacować go można na podstawie uogólnionej zależności (1):

$$\text{Metryka OSPF} = \frac{10^8}{\text{przepływność} \left[\frac{b}{s} \right]} \quad (1)$$

Możliwe jest także użycie innych metod konfiguracji kosztu. Im niższy koszt, tym większe jest prawdopodobieństwo, że interfejs będzie używany do przekazywania ruchu.

Konkurencyjnym dla protokołu OSPF jest protokół hybrydowy EIGRP (ang. *Enhanced Interior Gateway Routing Protocol*) wykorzystujący do metryki wektor odległości i posiłkuje się dodatkowo funkcje protokołów „łącze-stan”. Zaletą EIGRP jest możliwość jednoczesnej synchronizacji wszystkich routerów zaangażowanych w zmianę topologii sieci dzięki przeliczaniu tras poprzez zastosowanie algorytmu DUAL (ang. *Diffusing Update Algorithm*). To zapewnia szybką i efektywną konwergencję. Częściowe i skokowe uaktualnienia dotyczące zmian w tablicach wysyłane są tylko do tych routerów, które ich potrzebują. Dodatkowo nie są rozsyłane aktualizacje w cyklicznych odstępach czasu, tylko utrzymują kontakt za pośrednictwem pakietów *Hello*, to zapewnia minimalne zużycie dostępnej przepływności (szerokości pasma) podczas przesyłu danych w sieci. Do określenia optymalnych tras EIGRP stosuje metrykę zbiorczą ujmującą: przepływność (pasma), opóźnienie, niezawodność, obciążenie i rozmiar najmniejszej maksymalnej jednostki transmisyjnej danych obsługiwanej przez interfejsy routerów MTU (ang. *Maximum Transmission Unit*). Metryka ta jest możliwa do oszacowania z poniższej zależności (2):

$$\text{Metryka} = 256 \cdot \left(K1 \cdot \text{Przepływność} + \frac{K2 \cdot \text{Przepływność}}{256 - \text{Obciążenie}} + K3 \cdot \text{Opóźnienie} \right) \cdot \frac{K5}{\text{Niezawodność} + K4} \quad (2)$$

Wartości wskaźników KX są zmienne i zależne od wielu składowych zależnych od własności i architektury sieci. Domyślna metryka jest sumą przepływności i opóźnienia. Optymalną ścieżką jest ścieżka o najniższej wartości metryki tj. (3):

$$\text{Metryka EIGRP} = 256 \cdot (K1 \cdot \text{Przepustowość} + K3 \cdot \text{Opóźnienie}) \quad (3)$$

Przepływność i opóźnienie są liczone z wykorzystaniem przykładowych wartości:

- przepływność wynosi $10000000/(\text{najniższa przepływność [kbit/s]})$,
- opóźnienie wynosi sumę opóźnień występujących na ścieżce[μs]/10.

Reasumując protokół OSPF oferuje liczniejszy zbiór funkcjonalności i jest powszechnie stosowanym protokołem wewnątrz domenowym. Uzupełnienie przesyłu danych w relacji ent-2-end jest wykorzystanie protokołu BGP dla międzydomenowego ruchu pakietów [5]. Mniejsze wykorzystanie znajduje protokół EGP służącym do wymiany danych między systemami autonomicznymi, gwarantując wybór ścieżek wolnych od pętli uważany za standard internetowy [6]. BGP w odróżnieniu od protokołów IGP nie korzysta z metryk do wyboru ścieżek, tylko podejmuje decyzję na podstawie przyjętych zasad strategii sieciowych. Do wymiany aktualizacji BGP korzysta z protokołu transportowego TCP (ang. *Transmission Control Protocol*) na porcie 179, dzięki czemu dziedziczy właściwości niezawodności protokołu TCP. Gwarancja wyboru tras bez pętli jest zapewniona dzięki procedurze tworzenia przez protokół BGP wykresu systemów autonomicznych bazując na danych o sąsiadach. Połączenia dwóch systemów autonomicznych stanowią ścieżkę, a zbiór ścieżek prowadzących do miejsca docelowego tworzy sekwencje numerów systemów autonomicznych, przez które przechodzą ścieżki. Po ustanowieniu połączenia między dwoma routerami, stają się one routerami równoważnymi. Wymieniają się one danymi o trasach i wysyłają częściowe aktualizacje związane ze zmianami stanu interfejsów i zasobów transportowych w sieci.

Przedstawione powyżej zasadnicze własności protokołów odpowiedzialnych za przesył danych między nadawcą i adresatem informacji został poddany sprawdzeniu w zakresie identyfikacji cech budujących wiedzę o niezawodności szkieletu sieci. Na podstawie ogólnie znanych zasad prowadzenia badań diagnostycznych

i przy wykorzystaniu treści przedstawionych w literaturze [7,8] opracowano szczegółową metodykę badawczą zawierającą:

- 1) zapotrzebowania na realizację przesyłu danych odwzorowane poprzez w postaci generatorów usług,
- 2) rzeczywisty ruch strumienia osiągnięty w wyniku procesu trasowania pakietów,
- 3) analizator zdarzeń i monitor ruchu, itp.

Badania zawierały wiele aspektów związanych z przesyłem danych, jednym z nich było zebranie dostatecznej liczby powtarzalnych danych umożliwiających wiarygodne wypowiedzenie się o niezawodności szkieletu sieci teleinformatycznej na podstawie identyfikacji:

- 1) dostępności do zasobów sieci i nieosiągalności zadeklarowanych usług dla OSPFv2 i EIGRP oraz BGPv4,
- 2) uogólnionej wydajności z punktu widzenia klienta (np. uprawnionego użytkownika dysponującego terminalem PC2 w domenie AS200);
- 3) poprawności funkcjonowania tablic trasowania routerów w domenach AS100 i AS200 podczas występowania (emulacji) zmiennej w czasie i liczbie anomalii (niezdatności) z wykorzystaniem cząstkowych wyników zaprezentowanych w publikacjach [9÷11].

3. Architektura sieci i testbed

Budowa środowiska testowego (testbed-u) dla sieci teleinformatycznych w rzeczywistych warunkach jest procesem złożonym i wymagającym dużych nakładów czasowo przestrzennych i finansowych. Jednak przy odpowiedniej analizie i planowaniu oraz projektowaniu architektury sieci można znacząco ograniczyć liczbę elementów sieciowych i typy relacji z punktu widzenia głównego celu badań. Dlatego też postanowiono, że testbed składać się będzie z trzech domen, z pośród których jedna to szkielet sieci a zasadniczy stos protokołów to TCP/IPv4 (Rys. 1).

Zastosowanym protokołem między domenowym służącym do wymiany danych między systemami autonomicznymi był protokół BGPv4, a protokołami do wymiany danych wewnątrz systemów autonomicznych zastosowanymi w szkielecie sieci były protokoły OSPFv2, EIGRP i RIPv2. Dodatkowo w krańcowych systemach autonomicznych zostały umieszczone przełączniki 3COM Baseline 2226 Plus oraz serwery HP ProLiant DL380p Gen8 E5-2640. Poniżej przedstawiono zbudowaną architekturę wraz z adresacją.

Opracowana metodyka badań składała się z dwóch części: analitycznej (sprawdzającej poprawności i wariantowość konfiguracji w aplikacjach symulacyjnych) oraz walidacyjnej w badaniach miejscowych na fizycznie istniejących urządzeniach platformy sprzętowo-programowej testbed-u [7,8]. Realizacja zasadniczych przedsięwzięć metodyki badań dotyczyła zarówno adekwatności konfiguracji sprzętu i implementacji protokołów, systemów operacyjnych i aplikacji użytecznych oraz narzędzi testowych jak i dokładności zestawienia łańcuchów diagnostycznych. Dlatego też w pierwszej kolejności skonfigurowano protokół OSPF w szkielecie sieci i protokół BGP między domenami. Następnie zrealizowano scenariusze badawcze i przeprowadzono zaplanowane do wykonania testy. W kolejnym etapie protokół OSPF w szkielecie sieci został zamieniony na protokół EIGRP i ponownie zostały zrealizowane scenariusze testowe.

Rys. 1 Architektura testowa.

Protokoły OSPF i EIGRP zostały zastosowane w szkieletcie sieci ze względu na posługiwanie się najbardziej rozbudowanymi metrykami przy wyborze tras. OSPF wybierając trasy pakietów posługuje się kosztem, który jest oceną stanu łącza obliczaną na podstawie przepustowości (chwilowej przepływności).

W testach z zastosowaniem protokołu EIGRP uwzględniano złożoność stosowanych metryk tj. pasmo, opóźnienie, niezawodność, obciążenie i MTU. Dodatkowo sprawdzeniu podlegać będzie szybkość konwergencji i aktualizacji tablic trasowania w przypadku zaistnienia anomalii (awarii) na łączach. Dokładniejsza identyfikacja środowiska testowego została przedstawiona w publikacjach [7-11].

Testy

Testy rozpoczęto od analizy działania protokołu OSPFv2 w przypadku niezdatności kilku podsieci i porównanie wyników z otrzymanymi podczas przeprowadzenia identycznych testów dla protokołu EIGRP. Pierwszym krokiem była analiza trasy pakietów z komputera PC1 znajdującego się w AS100 do terminala PC2 znajdującego się w AS200 w sieci działającej bez żadnych uszkodzeń.

Następnie po kolei wyłączano fizycznie porty w podsieci 192.168.1.0, 192.168.7.0 i 192.168.3.0 celu pozyskania danych do analizy zachowania protokołu w przypadku zaistnienia uszkodzenia – nieosiągalności interfejsów. Czas konwergencji osiągnięty przez sieć był zadowalający (poniżej teoretycznych wartości), ponieważ sieć nawet na chwile nie przestała działać i cały czas realizowane było połączenie oraz przesyłanie danych. Jest to bardzo dużą zaletą dynamicznego protokołu routingu. Podczas tego testu dokonywano obniżenia zdadności zasobów transportowych poprzez emulowanie uszkodzeń łącz w ten sposób, aby znacznie dłuższą trasą niż początkowo trasą były przekazywane dane. Następnie zmieniono konfigurację protokołów w szkieletowych routerach sieci, implementując protokół EIGRP zamiast OSPF i przeprowadzono testy przy zachowaniu pozostałych determinant scenariuszy badawczych jak poprzednio. Okazało się, że protokół EIGRP zapewnił przesył danych na poziomie porównywalnym do protokołu OSPF.

W ostatniej fazie pierwszej grupy testów zaimplementowano protokół RIP do szkieletu sieci i również przeprowadzono testy. Wyniki nie były już tak zadowalające jak dla OSPF i EIGRP, ponieważ w tym przypadku sieć uzyskiwała konwergencję po czasie bliskim 30 sekund. Poniżej przedstawiono rysunek obrazujący dobór tras podczas testów (Rys. 2.).

Rys 2. Zobrazowanie uszkodzeń sieci.

Kolejne testy ukierunkowano na sprawdzenie wydajności sieci i wykonano je na podstawie generacji danych z komputera PC1 znajdującego się w AS100 do komputera PC2 znajdującego się w AS200. Jeden komputer został uruchomiony w postaci serwera, zaś drugi, jako klient. Użyte do testów oprogramowanie Iperf przesyła strumień danych między użytkownikami umożliwiając pomiar maksymalnej wartości jednostek transmisji danych (ang. *bandwidth*), procentu utraconych pakietów (ang. *packet lost*) oraz ich zmienności (ang. *jitter*'a) w jednostkowych przedziałach czasu rzeczywistego (ang. *Real Time*). Pomiarzy zostały dokonane na poziomie warstwy transportu z wykorzystaniem protokołów TCP i UDP. W obu przypadkach otrzymane wyniki były zbliżone w zakresie wartości i tolerancji ich zmian. W celu zwiększenia wiarygodności testów oprócz przesyłania pojedynczego strumienia sprawdzono zachowanie sieci w trybie równoczesnego przesyłu dla obu kierunków (ang. *full duplex*). Wariantowość ta nie zobrazowała zmian wartości przepływności, która podczas wszystkich testów oscylowała w granicy wartości 94 Mb/s. Jest to zadowalający wynik biorąc pod uwagę specyfikację komponentów sieciowych wykorzystujących standard 100BASE-TX.

Realizacja trzeciego zbioru scenariuszy badawczych polegała na sprawdzeniu i przeanalizowaniu poprawności zapisów tablic routingu zbudowanych dzięki protokołowi OSPF w szkieletcie sieci, tras z systemu autonomicznego 100 do systemu autonomicznego 200, następnie ograniczono przepustowość do 10 Mb/s na interfejsach, przez które była wyznaczona trasa pakietów. Protokół szybko wymienił informację i uaktualnił trasę na nową nieprzebiegającą przez łącza o ograniczonej zdolności. W kolejnym etapie zwiększono opóźnienie kolejnych łącz znajdujących się na drodze przesyłu pakietów, celem detekcji dalszej reakcji protokołów trasowania i dynamiki zmian zapisów w tablicach. Według oczekiwań – protokoły trasowania „stosunkowo szybko” wybierały nowe trasy z mniejszymi metrykami. Następnie, po uwzględnieniu zawartości tablic, dobierana była konfiguracja oferująca dwie trasy z możliwie najmniejszymi i zbliżonymi do siebie wartościami metryki, ale z różną liczbą skoków między routerami. Wtedy protokoły wybierały trasę z mniejszą liczbą skoków koniecznych do przesyłu danych. Po zakończeniu fazy testowej w szkieletcie sieci zmieniono konfigurację protokołu na EIGRP i przeprowadzono identyczne testy. Okazało się, że protokół OSPF był niewrażliwy na zmiany wartości opóźnienia w wybranych zasobach transportowych, natomiast miało to odczuwalny wpływ na dobór trasy poprzez protokół EIGRP. Następnie w szkieletcie sieci zaimplementowano protokół RIPv2 i przeprowadzono te same testy. Zachowanie tego protokołu odbiegało znacząco od wcześniejszych, ponieważ okazało się, że protokół RIP jest niewrażliwy na zmiany dynamiczne sieci i w każdym przypadku pakiety były kierowane tą samą trasą.

4. Wnioski

Sieć teleinformatyczna integrująca zasoby klasycznie rozumianej telekomunikacji i urządzenia informatyczne stała się już nieodzownym komponentem każdego typu organizacji i przedsiębiorstwa. Powszechność stosowania tego typu złożonego obiektu technicznego wynika z szerokiej palety usług oferowanych dla uprawnionych jej użytkowników niezależnie od ich dyslokacji. Nie mniej jednak złożoność relacji i powiązań wewnątrz domen i między domenami sieci wymaga wysokiego poziomu wiedzy teoretycznej i praktycznych umiejętności jej zastosowania w procesie eksploatacji (użytkowania i obsługiwanie).

Szczególnie trudnym jest dotrzymanie zdolności technicznej i funkcjonalnej bezpośrednio budującej niezawodność sieci. To właśnie poprawności doboru i działania protokołów trasowania pakietów odpowiedzialnych za przesył danych między stacjami sieciowymi jest krytyczną determinantą analizowanego obszaru tematycznego. Liczność konfiguracji interfejsów sieciowych i ich adekwatność do potrzeb wymusza konieczność przeprowadzenia wieloaspektowej analizy atrybutów protokołów tj. RIP, BGP, OSPF czy też EIGRP, itp.

Uwzględniając wagę tych zagadnień autorzy postanowili poddać badaniu wpływu anomalii (uszkodzeń) i zmiennych dynamicznych związanych z ruchem sieciowym na działanie protokołów routingu i w konsekwencji sieci w ujęciu kompleksowym. Wybrano reprezentatywne protokoły trasowania, testbed z systemy autonomiczne odzwierciedlający rzeczywiste warunki eksploatacji a następnie przeprowadzono testy niezawodnościowe zgodnie z przyjętymi scenariuszami, w metodyce badań, polegające na odporności na narażenia fizyczne sieci i zmiany dynamiczne paramentów sieciowych oraz testy wydajnościowe.

Zasadnym wydaje się być stwierdzenie, że optymalnymi protokołami wewnątrz domenowymi są protokoły OSPFv2 i EIGRP, które we wszystkich testach wykazały się wysoką niezawodnością i osiągały niemalże identyczne wyniki. Największą różnicą między nimi jest fakt, że EIGRP jest protokołem komercyjnym, możliwym do zaimplementowania tylko na sprzęcie firmowym. Natomiast protokół OSPF jest protokołem otwartym i możliwym do zastosowania również w open source'owych rozwiązaniach.

W przypadku rozbudowanej architektury sieci opartej o kilka systemów autonomicznych bardzo dobrym rozwiązaniem jest wspólne zastosowanie protokołów wewnątrz domenowych tj. OSPFv2 lub EIGRP wraz z protokołem między domenowym BGPv4 z wyszczególnieniem szkieletu sieci będącym rdzeniem topologii. Zaletą protokołów OSPFv2 i EIGRP jest częsta wymiana danych (a więc i informacji), co przekłada się na „szybszą” reakcję sieci i „szybsze” osiągnięcie zbieżności routerów. Pozwala to na efektywne wykorzystanie łącz, „szybką” konwergencję w przypadku zaistnienia stanu niezdatności (uszkodzenia, awarii). Protokół RIPv2 ze względu na swoje ograniczenia nie nadaje się do rozbudowanych sieci, ponieważ ma „bardzo wolny” czas reakcji i ograniczenie w liczbie skoków do 15 węzłów.

Metoda badawcza zastosowana w artykule ze względu na wielodrogowość w szkieletach sieci i zastosowanie wielu systemów autonomicznych oraz współpracę protokołów wewnątrz i między domenowymi pozwala wiernie odzwierciedlić złożoność usługowych struktur sieciowych. Uwzględnia też ona wszystkie aspekty wpływające nie tylko na niezawodność, lecz także na pozwala wypowiadać się o jakości realizowanego połączenia (tj. metryka, natężenie ruchu oraz liczba skoków), to z kolei umożliwia dokonanie walidacji i oceny kryteriów warunkujących oczekiwany stan transportu danych w sieci. Biorąc pod uwagę fakt, że w różnych domenach (podsieciach) są implementowane różne protokoły można stwierdzić, że u różnych dostawców usług (tj. Internet) mogą mieć różny wpływ inne dynamiczne czynniki (tj. wartość opóźnienia i jego zmienność, dostępna przepływność, stopa błędów, itp.). Dlatego też, wybrane rekomendacje zostały już fragmentarycznie poddane procesowi wybiórczej analizy i w dedykowanych warunkach środowiskowych przebadane, a wyniki zaprezentowano w publikacjach [12–15].

5. Literatura

- [1] Laskowski D., Lubkowski, P.: Confidential transportation of data on the technical state of facilities, *Advances in Intelligent Systems and Computing* 286, pp. 313-324, 2014.
- [2] Dokument IEFT: RFC 1058: Routing Information Protocol, RFC 1723: RIP Version 2.
- [3] Dokument IEFT: RFC 1812: Requirements for IP Version 4 Routers.
- [4] Dokument IEFT: RFC 2328: OSPF Version 2.
- [5] Dokument IEFT: RFC 4271: A Border Gateway Protocol 4 (BGPv4).
- [6] Dokument IEFT: RFC 1771: A Border Gateway Protocol 4 (BGP-4).
- [7] Bajda, A., Laskowski, D., Wrazen M.: Diagnostics the quality of data transfer in the management of crisis situation, *Przegląd Elektrotechniczny* 87 (9 A), pp. 72-78, 2011.
- [8] Lubkowski P., Laskowski D.: The end-to-end rate adaptation application for real-time video monitoring, *Advances in Intelligent Systems and Computing* 224, pp. 295-305, 2013.
- [9] Lubkowski P., Laskowski D., Pawlak E. Provision of the reliable video surveillance services in heterogeneous networks, *Safety and Reliability: Methodology and Applications - Proceedings of the European Safety and Reliability Conference, ESREL 2014* pp. 883-888, 2015.
- [10] Lubkowski P., Laskowski D.: Test of the multimedia services implementation in information and communication networks, *Advances in Intelligent Systems and Computing* 286, pp. 325-332, 2014.
- [11] Lubkowski P., Laskowski D.: The selected issues of reliable identification of object in transport systems using video monitoring services, *Communication in Computer and Information Science* 0471, pp. 59-68, 2014.

- [12] Laskowski D., Lubkowski P., Kwasniewski M.: Identification of suitability services for wireless networks, *Przegląd Elektrotechniczny* 89 (9), pp. 128-132, 2013.
- [13] Bylak M., Laskowski D.: Assessment of network coding mechanism for the network protocol stack 802.15.4/6LoWPAN, *Advances in Intelligent Systems and Computing* 224, pp. 75-82, 2013.
- [14] Bylak M., Laskowski D.: Diagnosis coding efficiency of network coding mechanism for wireless networks, *Przegląd Elektrotechniczny* 89 (9), pp. 133-138, 2013.
- [15] Laskowski D., Lubkowski P., Pawlak E., Stańczyk P.: Anthro-po-technical systems re-liability, *Safety and Reliability: Methodology and Applications - Proceedings of the European Safety and Reliability Conference, ESREL 2014*, pp. 399-407, 2015.

Mgr inż. Rafał Polak jest zatrudniony w firmie Transbit Sp. z o.o. na stanowisku specjalisty ds. Sieci Teleinformatycznych, w 2014r. ukończył Wydział Elektroniki Wojskowej Akademii Technicznej. Zajmuje się analizą zjawisk zachodzących podczas trasowania danych w złożonych strukturach systemowych wykorzystujących nowoczesne i perspektywiczne techniki i technologie w sieciach teleinformatycznych. Zasadnicze obszary zainteresowania to efektywność i niezawodność obiektów technicznych w aspekcie ich praktycznego zastosowania w sieciach teleinformatycznych.

Dr hab. inż. Dariusz Laskowski ukończył Wydział Elektroniki Wojskowej Akademii Technicznej, gdzie obecnie pracuje. Zajmuje się wieloaspektową analizą zjawisk determinujących poprawność realizacji usług w heterogenicznych systemach i sieciach oferujących przesył danych. Główne obszary zainteresowania to niezawodność, bezpieczeństwo, jakość i przeżywalność obiektów technicznych w aspekcie ich praktycznego zastosowania w sieciach heterogenicznych.