Telekomunikacja Cyfrowa – Technologie i Usługi
Tom 9. Rok 2008/2009

Wykorzystanie informacji pomiarowych pochodzących z protokołu BGP do oceny struktury sieci Internet [1]

Marcin Malinowski, Jacek Nowak, Piotr Pacyna (e-mail: pacyna@kt.agh.edu.pl)
Katedra Telekomunikacji Akademii Górniczo-Hutniczej – Kraków

STRESZCZENIE

Niniejszy artykuł przybliża metody monitorowania i badania sieci Internet, pozwalające na uzyskanie informacji o jego strukturze, operatorach i połączeniach. Przedstawiono projekty i metody wykorzystujące dane pomiarowe z protokołu BGP, które umożliwiają nie tylko poznanie struktury sieci, lecz również obserwację dynamiki zachodzących w niej zmian. Przydatność metod zilustrowano na przykładzie analizy struktury połączeń sieci ACK CYFRONET AGH z innymi operatorami. W trakcie dyskusji poruszono także najważniejsze problemy dotyczące rozwoju sieci Internet.

ABSTRACT

Evaluation of Internet Structure Based on Measurement Information from BGP protocol

The paper presents methods for investigating topology of the contemporary Internet which jointly allow to learn its structure, discover operators and interconnections. The focus is on methods based on information available in BGP protocol which allows to learn dynamic properties of the Internet. Usability of the methods is presented in a case study of ACK CYFRONET AGH network.

1. Wprowadzenie

Przedstawienie struktury organizmu tak złożonego i niejednorodnego, jak współczesny Internet, jest zadaniem śmiałym lub wręcz niemożliwym. Wymaga ono zbudowania obrazu sieci Internet albo przynajmniej jej wybranego fragmentu. Zadanie to zostało podjęte w pracy [1]. Ponieważ wykorzystane metody przedstawiają dużą wartość użytkową dla organizacji nadzorujących funkcjonowanie Internetu, dla dostawców Internetu, a także dla instytucji i przedsiębiorstw korzystających z dostępu do Internetu, uzyskane wyniki zostały syntetycznie przedstawione w niniejszym artykule. Wykorzystując prezentowane metody, można monitorować własną sieć i jej pozycję w globalnej strukturze Internetu, w tym także np. osiągalności tej sieci z różnych punktów w Internecie lub przebieg tras prowadzących do niej, co w wielu przypadkach umożliwia wyciąganie wniosków na temat jakości połączeń i otwiera drogę do jej poprawy.

1.1. Struktura sieci Internet

Współczesny Internet jest strukturą połączonych ze sobą sieci komputerowych. Od strony administracyjnej, sieci te są zorganizowane w niezależne zarządzane obszary nazywane systemami autonomicznymi – AS (*Autonomous System*). Według klasycznej definicji system autonomiczny jest strukturą routerów i łączy pozostających pod wspólną władzą administracyjną, w której zastosowano ten sam protokół wewnątrzdomenowy doboru trasy i jednorodną metrykę dla określania jakości tych łączy [2].

Systemy autonomiczne połączone są ze sobą za pomocą wyznaczonych do tego celu routerów. Są to tzw. routery brzegowe lub graniczne (*border routers*). Połączenia mogą być bezpośrednie lub za pośrednictwem punktu wymiany danych – IXP (*Internet Exchange Point*), które są inicjatywą lokalnych operatorów internetowych. Rozbudową systemu autonomicznego zajmuje się operator będący właścicielem infrastruktury sieciowej systemu, podczas gdy utrzymanie połączeń pomiędzy systemami autonomicznymi leży w gestii zarządzających nimi operatorów, którzy zestawiają łącza bezpośrednie i ustanawiają tzw. *peering* albo korzystają w tym zakresie z pomocy wyspecjalizowanych instytucji utrzymujących tzw. punkty wymiany ruchu.

1.2. Kierowanie ruchem między domenami

Protokoły wewnątrzdomenowe, takie jak RIP (*Routing Information Protocol*), IGRP (*Interior Gateway Routing Protocol*), OSPF (*Open Shortest Path First*) i IS-IS (*Intermediate System-to-Intermediate System*), obejmują swym działaniem obszar pojedynczego systemu autonomicznego. W obrębie systemu autonomicznego często stosuje się równocześnie kilka protokołów wewnątrzdomenowych, ale w taki sposób, że inne obszary autonomiczne ‘postrzegają’ obszar jako wewnętrznie spójny plan przebiegu tras. Sieci znajdujące się w obrębie systemu są reprezentowane w sposób szczegółowy, podczas gdy sieci znajdujące się poza

obszarem są reprezentowane w sposób uogólniony [2]. Protokoły międzydomenowe służą do wymiany informacji pomiędzy routerami należącymi do różnych systemów autonomicznych. Powszechnie używanym protokołem jest BGP (*Border Gateway Protocol*).

Systemy autonomiczne identyfikowane są przez 16-bitowy numer – tzw. *Autonomous System Number* (ASN) – przydzielony przez jeden z rejestrów RIR (*Regional Internet Registry*), których zadaniem jest przydzielanie adresów IPv4, IPv6 i identyfikatorów ASN organizacjom oraz dostawcom usług internetowych. Dotychczas zostało przypisanych przeszło 41300 publicznych numerów ASN [3], w związku z czym rozważa się wprowadzenie 32-bitowej numeracji [4]. Informacja o 'publicznych' systemach autonomicznych dostępna jest w bazie *whois* [5].

1.3. Rodzaje systemów autonomicznych

Ze względu na charakter obsługiwanego ruchu można wprowadzić prostą klasyfikację systemów autonomicznych. Systemy autonomiczne typu *single-homed* (określane również jako *stub*) odpowiadają mniejszym sieciom i są połączone tylko z jedną domeną. Systemy autonomiczne typu *multi-homed non-transit* są przyłączone do co najmniej dwóch systemów autonomicznych, ale nie tranzytują ruchu pochodzącego z zewnątrz. Natomiast systemy autonomiczne typu *multi-homed transit* są przyłączone do co najmniej dwóch systemów autonomicznych i przekazują ruch tranzytowy. Ich głównym celem jest zapewnienie połączenia między domenami typu *single-homed* i *multi-homed non-transit* i właśnie na nich oparty jest główny szkielet Internetu [6].

Powyższy podział jest ogólny i nie przedstawia wszystkich możliwych sytuacji.

W Internecie dominuje około 12 największych dostawców usług internetowych [7]. Są to operatorzy tzw. warstwy 1 routingu (*tier-1*), ponieważ ich wzajemne połączenia dają im dostęp do większości tras w Internecie [7]. Operatorzy warstwy 2 wykupują usługę tranzytowania ruchu poprzez główny szkielet Internetu od operatorów warstwy 1 i tworzą połączenia między sobą: bezpośrednie lub za pomocą punktów wymiany ruchu [30]. Są to najczęściej operatorzy regionalni (narodowi) a ich liczba sięga kilku tysięcy [7], [30]. Dostawcy usług internetowych, którzy wykupują połączenia tranzytowe od operatorów warstwy 2, są zaliczani do warstwy 3. Obecnie, z uwagi na kratową strukturę Internetu (*mesh*), warstwa 3 ma znaczenie głównie historyczne, albowiem dostawca usług internetowych, mając bezpośrednie połączenia z warstwą 2 oraz warstwą 3, może wykupić dodatkowe łącza tranzytowe od operatorów warstwy 1 i warstwy 2 [30].

1.4. Rola protokołu BGP w rutingu międzydomenowym

Protokół BGP jest w praktyce standardem routingu między obszarami autonomicznymi. Został wprowadzony w 1989 roku. Obecnie powszechnie stosowana jest wersja oznaczona jako BGP-4 [2]. Głównym założeniem protokołu BGP było sprowadzenie topologii Internetu do postaci grafu, w którym węzły grafu reprezentują systemy autonomiczne, a krawędzie to ścieżki pomiędzy sąsiadującymi systemami, w których połączenia realizowane są poprzez routery obsługujące protokół BGP. Podstawową funkcją BGP jest wymiana informacji o dostępności sieci pomiędzy różnymi systemami BGP. Protokół BGP reprezentuje trasy przy pomocy tzw. wektora ścieżki (*path vector protocol*) [8], co oznacza, że definiuje trasę za pośrednictwem identyfikatora sieci docelowej i atrybutów ścieżki prowadzącej do tej sieci. Sieć docelowa identyfikuje urządzenia końcowe, których adresy IP objęte są adresem sieci przenoszonym w polu NLRI (*Network Layer Reachability Information*) wiadomości *Update*.

BGP-4 wprowadza szereg mechanizmów wspierających CIDR (*Classless Inter-Domain Routing*) i umożliwia agregowanie tras (*AS path*). Mechanizmy te pozwalają na rozgłaszanie sieci IP w formie tzw. prefiksów adresów IP.

1.5. Atrybuty ścieżki protokołu BGP

Wiadomości uaktualniające BGP są używane do przenoszenia informacji o ścieżkach pomiędzy systemami BGP. Informacje te mogą być wykorzystane do budowy grafu, który przedstawia relacje pomiędzy różnymi systemami autonomicznymi. Trasy otrzymane z protokołu BGP mają powiązane tzw. atrybuty, które są wykorzystane do określenia najlepszej ścieżki prowadzącej do miejsca docelowego, w przypadku gdy istnieje wiele prowadzących do niego ścieżek. Rodzaje atrybutów oraz ich semantyka jest szczegółowo opisana w standardzie [2] oraz skrótowo opisana w [1].

1.6. Wybór najlepszej ścieżki

Router BGP zwykle dysponuje kilkoma komunikatami informującymi o osiągalności określonej sieci, pochodzącymi z różnych źródeł. W takiej sytuacji musi on wybrać jedną ścieżkę, uważaną za najlepszą, i umieścić ją w tablicy routingu IP. Unikalną cechą protokołu BGP jest zdolność uwzględniania wielu atrybutów ścieżki (zarówno obowiązkowych, jak i opcjonalnych) jako kryteriów przy wyborze najlepszej ścieżki prowadzącej do odległej sieci. Wybór jest dokonywany przez tzw. *BGP decision process* [9]. W zależności od polityki operatora, wybrana ścieżka może być rozgłasza-

na do innych systemów autonomicznych, które wezmą ją pod uwagę w procesie decyzyjnym jako potencjalną ścieżkę dla tranzytowania ruchu.

2. Metody pomiarowe

Struktura Internetu jest ważną cechą, którą interesują się projektanci systemów sieciowych, aplikacji, urządzeń, oraz osoby odpowiedzialne za ustanawianie polityki obsługi ruchu na styku swojego systemu autonomicznego z innymi systemami. Informacje o strukturze Internetu można pozyskać, analizując dane pochodzące z protokołu BGP. Dla tego typu informacji stosowane jest reprezentowanie struktury Internetu na poziomie systemów autonomicznych AS. Służy to przedstawieniu Internetu z perspektywy połączeń międzydomenowych, a na dalszy plan odsuwa wewnątrzdomenową strukturę systemów autonomicznych.

Nawet tylko przy wykorzystaniu tak uproszczonego modelu, analiza struktury Internetu jest zadaniem trudnym. Poza samym rozmiarem globalnej sieci mierzonym ilością systemów autonomicznych, kolejnym problemem są ograniczenia natury administracyjnej w zakresie dostępu do informacji o strukturze sieci. Brak centralnego nadzoru w zakresie planowania, rozwoju sieci i polityki obsługi ruchu w środowisku wielooperatorskim utrudnia także weryfikację danych i uniemożliwia znalezienie punktu, z którego należałoby prowadzić pomiary [6]. Dlatego wyznaczanie topologii sieci na podstawie danych pomiarowych jest niełatwe, czasochłonne, pochłania znaczne zasoby obliczeniowe i skłania do poszukiwania nowych metod pozyskiwania i archiwizowania danych.

2.1. Kolektory tras projektu RIPE RIS

Kolektor tras BGP[1] to urządzenie sieciowe nawiązujące sesje BGP (*peering*) z wieloma komercyjnymi dostawcami usług internetowych, w celu gromadzenia informacji pochodzących z BGP, które jednak samo nie rozgłasza żadnych prefiksów. Tabela rutingu BGP kolektora tras jest okresowo archiwizowana, dzięki czemu uzyskuje się obraz zmian zachodzących w sieci. Kolektory stanowią zwykle główne źródło danych przy analizie problemów i zmian obserwowanych w Internecie.

Punkty pomiarowe, których elementem jest kolektor, lokuje się zazwyczaj tak, by nawiązywały sesję z tzw. routerami decyzyjnymi [13], które aktywnie rozstrzygają, dokąd kierować dane przeznaczone dla systemów autonomicznych innych niż ten, do którego należy router decyzyjny. Dane pochodzące z takich routerów dotyczą zwykle kluczowych punktów globalnej sieci, w których najczęściej można zaobserwować zmiany. Są więc bardzo istotne dla uzyskania poprawnego i całościowego obrazu sieci [13].

Kolektor może nawiązać sesje z dużą liczbą maszyn BGP i w ten sposób rekonstruować bardziej szczegółową bazę informacji o rutingu (RIB – *Routing Information Base*). Każdy węzeł, z którym nawiązano sesję, przechowuje kopię własnego obrazu globalnej sieci, a im więcej obrazów otrzyma kolektor, tym dokładniejsza będzie jego własna tablica BGP. Rozmiar pojedynczej tablicy jest zwykle bardzo duży (powyżej 260000 rekordów [10]). Ciągły przyrost ich rozmiaru ilustruje jeden z głównych problemów protokołu BGP.

Istnieją różne implementacje systemu opartego na kolektorach. Projekt RIS (*Routing Information Service*) jest utrzymywany przez Europejski Rejestr Internetowy. Sesje nawiązywane są z bezpośrednimi sąsiadami lub z urządzeniami oddalonymi o kilka systemów autonomicznych (tzw. sesje *multihop*). Zgromadzone informacje o trasach wysyłane są do węzła centralnego, gdzie są archiwizowane w binarnym formacie MRT.

Projekt RIS rozróżnia dwa rodzaje sesji i dwa typy punktów pomiarowych. Sesje w trybie *multihop* są nawiązywane przez centralny kolektor z ważnymi dostawcami usługi internetowej. W ramach projektu skonfigurowano 12 tzw. zdalnych kolektorów tras RRC (*Remote Route Rollector*) umiejscowionych w pobliżu istotnych punktów w topologii sieci. Sesje *multihop* występują tylko dla punktu centralnego.

Zwykle zadaniem kolektora jest tylko odtworzenie i zapisanie tablicy rutingu. Takie podejście ma jednak pewną istotną wadę, mianowicie zachowuje jedynie chwilową strukturę Internetu. Tabela rutingu, zrekonstruowana przez kolektor, zawiera tylko te trasy do prefiksów, które są w danej chwili preferowane i pomija trasy nadmiarowe i zastępcze. By uzyskać pełny obraz połączeń pomiędzy systemami autonomicznymi, należy analizować nie tylko samą bazę RIB, ale również rozgłoszenia, wycofania i zmiany tras (*advertisment*, *withdrawal*, *update*).

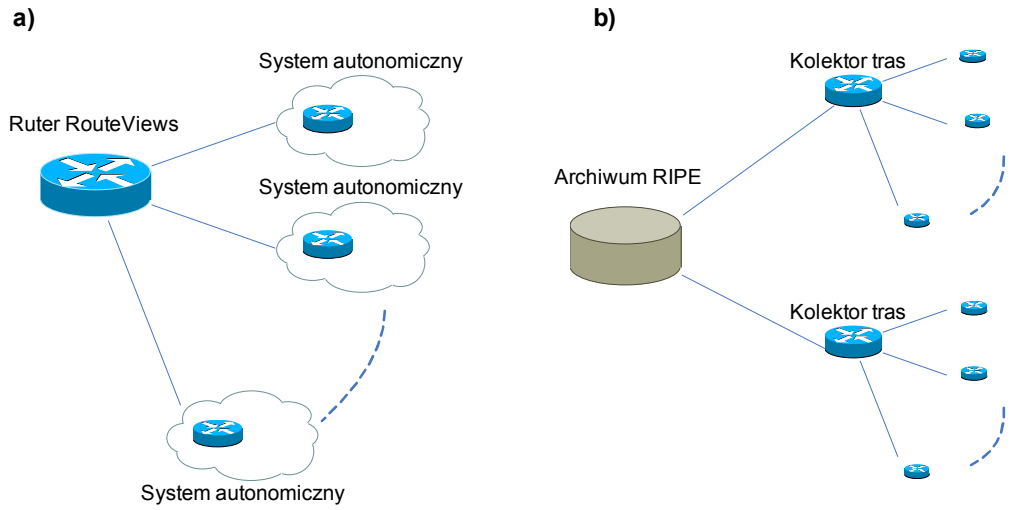
Pełna analiza danych z protokołu BGP pozwala na odkrycie zmian wynikających np. z awarii łącza lub polityki rutingu i uwidacznia systemy autonomiczne i połączenia, których nie ma w obrazie chwilowym. Z przeprowadzonych badań wynika, że można w ten sposób wykryć o 38% więcej połączeń niż w obrazie chwilowym i o 3% więcej systemów autonomicznych [11].

2.2. Projekt RouteViews

W ramach projektu RouteViews [12], stworzono system pozwalający na badanie Internetu w trybie rzeczywistym z kilku punktów pomiarowych. Podobnie jak RIS, RouteViews korzyta z BGP, ale nie używa zdalnych kolektorów tras. Routery RouteViews na-

[1)] W literaturza anglojęzycznej zdalny kolektor tras oznaczany jest często skrótem RRC (*Remote Route Colector*).

wiązują sesję posługując się numerem AS6447 (same nie rozgłaszają żadnych prefiksów ani w żaden sposób nie przekazują ruchu wzdłuż uzyskanych w ten sposób tras BGP). Na rysunku 1 zilustrowano obydwie architektury.



Rys. 1. Architektura projektu RouteViews (a) i RIPE RIS (b)

Lista routerów i ich lokalizacja jest dostępna w [13]. Na serwerach przechowywane są także dane archiwalne: tablice RIB zapisywane są co dwie godziny, a komunikaty BGP odświeżane co 15 minut. Route Views odpowiada taże za jeden z tzw. impulsów BGP (*BGP beacon*) [14]. Jest to niewykorzystywany prefiks 192.135.183.0, rozgłaszany i wycofywany co dwie godziny. W ten sposób można obserwować, jak globalna sieć reaguje na zmiany.

2.3. Usługa zwierciadła

Usługa zwierciadła (*Looking Glass*) oferuje interfejs użytkownika, za pomocą którego można wykonać ograniczony zestaw komend na wybranych routerach BGP. Polecenia konfigurujące są zablokowane, jednak udostępnione komendy pozwalają na przykład na sprawdzenie trasy prowadzącej do danego prefiksu, chociaż zapisanie całej tablicy rutingu jest zwykle niemożliwe. Niekiedy udostępniane jest polecenie *show ip bgp summary*. Na podstawie wyniku zapytania można odtworzyć topologię sieci w najbliższym otoczeniu routera, do którego skierowano zapytanie.

Interfejs zwierciadła pozwala zazwyczaj na kierowanie komend do wielu routerów, często niewidocznych dla większości kolektorów tras. Strona www [15] utrzymuje aktualną listę dostawców udostępniających tę usługę, obejmującą około 170 systemów autonomicznych. Chociaż pojedynczy Looking Glass nie może dostarczyć niektórych użytecznych informacji, to jednak uzyskane z nich dane są często ważnym uzupełnieniem danych z kolektorów tras.

2.4. Pomiary makroskopowe

Wykorzystanie publicznie dostępnych tablic BGP jest powszechną metodą oceny struktury sieci Internet, jednak przydatność tych danych jest ograniczona. Ich istotną wadą jest to, że nie odzwierciedlają tego, jak w rzeczywistości kierowany jest ruch do sieci docelowej. Nie ujawniają krótkich, okresowych zmian ścieżek pomiędzy systemami autonomicznymi oraz wyrównywania obciążeń (*load balancing*) pomiędzy nimi. W celu wyeliminowania tych ograniczeń powstało narzędzie pomiarowe o nazwie *skitter* [16]. Jego działanie jest podobne do narzędzia systemowego *traceroute*. *Skitter* wysyła komunikat żądania echa (*echo request*) protokołu ICMP i oczekuje na komunikat o przekroczeniu czasu życia pakietu (*time exceeded*).

Uzyskana na podstawie tych danych topologia ma pewne ograniczenia, które są związane z metodologią pomiarów [17]. Sukces pomiarów zależy od punktu docelowego oraz od związanych z nim węzłów pośredniczących, przez które wraca odpowiedź ICMP *echo reply*. Narzędzie *skitter* także nie jest w stanie odwzorowywać ścieżek adresów IP, które znajdują się za zaporami ogniowymi (*firewall*) lub w sieciach, w których zastosowano translację adresów NAT (*Network Address Translation*).

Uzyskane ścieżki nie odwzorowują całej topologii Internetu z uwagi na jego rozmiar. Obecne cele projektu mają na celu zbadanie osiągalności przynajmniej jednego (dowolnego) hosta w każdej sieci o długości prefiksu /24. Potencjalnie istnieje takich sieci ponad 16 milionów, z czego około 4 miliony adresów sieci IP są routowalne [17]. Na całym świecie rozmieszczone są 22 działające punkty pomiarowe [18] i każdy z nich wysyła próbne pakiety do miejsc docelowych, które

znajdują się na liście celów. Zbiór ten ciągle maleje z uwagi na stosowanie zapór oraz zmianę adresów IP, dlatego też lista sondowanych hostów musi być aktualizowana. Obecnie stosowana lista została utworzona 1 stycznia 2004 roku. Zawiera 971054 adresów IPv4, które reprezentują końcowe hosty, serwery stron www, routery i inne urządzenia sieciowe. Zbiór tych adresów obejmuje 62,6% półglobalnych prefiksów oraz 917529 adresów z zakresu o długości maski /24. Półglobalny prefiks jest to prefiks rozgłoszony przez co najmniej 22 z 41 uczestników projektu RouteViews dnia 9 grudnia 2003 roku. Liczba tych prefiksów wyniosła wtedy 127209. Przy tworzeniu listy starano się zawrzeć co najmniej jedno miejsce docelowe w każdym zakresie adresów o wielkości /24, który odpowiadał na zapytania ICMP, oraz co najmniej dwa hosty w każdym półglobalnym prefiksie. Znajdowanie miejsc docelowych w każdym zakresie adresów o wielkości /24 jest bardzo ważne, gdyż zapewnia proporcjonalną reprezentację większych prefiksów np. o wielkości /8 [13].

3. Metody zaawansowane i korekcja błędów

Każda topologiczna mapa Internetu z natury rzeczy jest uogólniona, bez względu na to, jaką metodą posłużono się do jej zbudowania. Z jednej strony wynika to z ogromnej liczby urządzeń i połączeń, które musiałyby zostać zidentyfikowane i zapisane przez system pomiarowy, z drugiej jednak same metody również wnoszą margines błędu. Dzieje się tak, ponieważ stosowana metodyka pomiarów często prowadzi do błędnej interpretacji wyników lub też samo narzędzie pomiarowe nie jest w stanie wykryć wszystkich istotnych obiektów należących do badanego fragmentu sieci. Aby temu zapobiec i tym samym zwiększyć dokładność pomiarów, metody podstawowe są modyfikowane przy pomocy algorytmów korygujących. Poniżej przedstawiono wybrane rozszerzenia do metodyki gromadzenia danych, najlepiej udokumentowane błędy, przyczyny ich występowania oraz sposoby ich zwalczania.

3.1. Mapy rozszerzone

Podstawowym problemem metod korzystających z protokołu BGP jako źródła informacji jest niekompletność informacji. Teoretycznie, każda tabela rutingu BGP powinna pokrywać całą przestrzeń adresową Internetu. W rzeczywistości, ze względu na politykę rutingu i konieczność wyboru optymalnej trasy, pojedyncza tabela stanowi zaledwie fragment obrazu globalnej sieci. Częściowo problem niekompletności można rozwiązać, stosując łączenie tabel pochodzących z wielu routerów BGP, ale jak pokazują analizy [11], metoda ta nie gwarantuje kompletności danych. Alternatywą jest zastosowanie tzw. rozszerzonych map – opartych na wielu źródłach danych.

Do stworzenia mapy rozszerzonej można np. wykorzystać dane pochodzące z czterech źródeł: z tabeli rutingu projektów RouteViews, projektu RIPE, serwerów *Looking Glass* i z serwerów tras (*route servers*), czyli z routerów publicznie udostępniających polecenie *show ip bgp*. Podstawą mapy są wtedy tablice rutingu BGP. Każda z nich zawiera chwilowy obraz sieci (*snapshot*). Uzyskana „migawka" powinna pokazać aktywne w chwili pomiaru węzły (systemy autonomiczne) i połączenia między nimi. By zwiększyć wykrywalność połączeń i węzłów, można zastosować agregację danych z wielu tablic rutingu. Daje to przyrost wykrywalności połączeń rzędu 19% i 0,9% węzłów [11]. Wartości te można dalej poprawić przez zastosowanie innych metod, na przykład opartych na danych z komunikatów *update* BGP i danych z Regionalnych Rejestrów Internetowych. Analiza komunikatów, jeżeli jest prowadzona przez dłuższy okres, pozwala ponadto wykryć zapasowe połączenia, awarie łączy, zmiany topologii i polityki rutingu, których nie można dostrzec w pojedynczej migawce[2]. Ostatnim typem źródła danych mapy rozszerzonej jest Regionalny Rejestr Internetowy, a konkretnie informacje zgłaszane do RIR przez dostawców usług internetowych. Do weryfikacji wiarygodność tych informacji można stosować kryteria z [19], dotyczące systemów autonomicznych, które określają, które systemy autonomiczne znalezione w bazie danych RIR należy odrzucić jako mało wiarygodne [11].

3.2. Rozpoznawanie aliasów

Routery dysponują wieloma interfejsami, a każdy z nich to odrębne połączenie z sąsiednim urządzeniem i każdy z nich musi mieć odrębny adres IP [6]. Jednym z problemów interpretacji wyników uzyskanych na drodze aktywnego próbkowania, np. z wykorzystaniem aplikacji *traceroute*, jest kwestia rozpoznawania interfejsów routera (*interface resolution problem*).

By przeciwdziałać takim sytuacjom, projekty oparte na aktywnej metodzie *traceroute* stosują zwykle dodatkowe narzędzie do tzw. rozpoznawania aliasów (*alias resolution tool*). Jego zadaniem jest wysyłanie pakietów do nieużywanego portu na interfejsie routera. Ponieważ port jest niedostępny, router odpowiada komunikatem o błędzie, który zostaje wysłany przez aktywny interfejs. Jeżeli interfejs, z którego otrzymano odpowiedź, jest inny niż ten, na który wysłano zapytanie, to oznacza to, że obydwa interfejsy należą do tego samego routera i powinny być reprezentowane przez jeden punkt na mapie. By zwiększyć skutecz-

[2] Dlatego projekty badawcze oparte na BGP, jak RouteViews czy RIPE RIS, gromadzą i udostępniają archiwalne dane pomiarowe.

ność tej metody, zapytania wysyłane są regularnie, z różnych punktów pomiarowych.

Przykładem narzędzia do rozpoznawania adresów jest *iffinder*, używany w projekcie CAIDA. Więcej informacji na ten temat można uzyskać w [1], [19] oraz [20].

3.3. Wykrywanie tras rezerwowych

W procesie analizy struktury Internetu istotny jest także rodzaj grafu generowanego na podstawie pomiarów. Jeżeli głównym wykorzystywanym narzędziem byłaby aplikacja *traceroute* i jeżeli dysponowalibyśmy tylko jednym punktem pomiarowym, to w efekcie, zamiast oczekiwanego grafu silnie połączonego, otrzymalibyśmy drzewo rozpinające *spanning tree*. Wynika to z faktu, że stosowana metoda (jeden punkt pomiarowy) nie wykrywa połączeń pomiędzy punktami na różnych „ścieżkach" sondowanych przez aplikację. Taki obraz sieci nazywany jest również „widokiem ptolemejskim" [6], ponieważ w centrum mapy znajduje się punkt, z którego prowadzono pomiary.

Ograniczenie tego efektu było istotne między innymi dla projektu Mercator, w którym użyto tylko jednego punktu pomiarowego. Zaproponowano kilka metod służących do wykrycia brakujących połączeń. Najbardziej oczywista z nich polega na sondowaniu sieci przez dłuższy okres. Dzięki temu wykrywane są ścieżki zapasowe (*backup path*), które nie są domyślnie wykorzystywane przy rutingu, a które mogą przybliżyć faktyczną strukturę połączeń.

Polityka routingu wpływa również na trasę pakietów generowanych przez aplikację *traceroute*, dzięki czemu możliwe jest uzyskanie bardziej reprezentatywnego obrazu połączeń między routerami. Inne rozwiązanie polega na próbkowaniu tras w oparciu o tzw. routery źródłowe (*source-route path probing*). Routery źródłowe pozwalają na wysyłanie pakietów sondujących tak, jakby były dodatkowymi punktami pomiarowymi, choć w rzeczywistości nie stanowią części systemu pomiarowego (takich routerów jest jednak stosunkowo niewiele i nie mogą być silnie obciążane).

Niestety, żadna z tych technik nie gwarantuje dobrych rezultatów, więc znacznie lepszym podejściem jest sondowanie z użyciem wielu punktów pomiarowych. Taka metoda nazywana jest „tomografią internetową" i jest stosowana w projekcie CAIDA (narzędzie *skitter*) [16].

4. Analiza struktury połączeń metropolitalnej sieci ACK CYFRONET AGH

Omówione wcześniej metody gromadzenia danych zostały wykorzystane do zbadania struktury miejskiej sieci komputerowej ACK CYFRONET AGH [1]. Jest to sieć dosyć duża, posiada własne systemy autonomiczne i jednocześnie stanowi niewielki wycinek Internetu – stosunkowo łatwy do analizy i zaprezentowania wyników. Przeprowadzono analizę połączeń na poziomie routerów IR (*Internet Router level*) oraz na poziomie systemów autonomicznych (*Autonomous System level*). Podstawę badań stanowiły dane uzyskane z narzędzia *skitter*. Właścicielem tych danych jest organizacja CAIDA, która po rozpatrzeniu wniosku autorów udostępniła je w celach badawczych. Analiza opierała się również na danych z projektu organizacji RIPE (kolektory tras) oraz RouteViews (tablice BGP). Dzięki temu odtworzono strukturę sieci na podstawie tego, jak jest ona widziana z Internetu, nie znając jej rzeczywistej budowy.

W celu przedstawienia dokładnej struktury sieci ACK CYFRONET AGH prace przebiegały następującymi etapami:

- wyszukanie systemów autonomicznych należących do ACK CYFRONET AGH,
- wyszukanie adresów IP rozgłaszanych przez te systemy autonomiczne,
- prezentacja struktury połączeń na poziomie routerów,
- prezentacja struktury połączeń na poziomie systemów autonomicznych,
- wyszukanie sąsiadów systemów autonomicznych na podstawie danych projektu RIPE RIS i wyszczególnienie najważniejszych elementów tej struktury.

4.1. Analiza na podstawie danych organizacji CAIDA

W pierwszej kolejności zostały wyszukane systemy autonomiczne, które należą do ACK CYFRONET AGH. Do tego wykorzystano informacje pochodzące z bazy *whois* Regionalnych Rejestrów Internetowych [5]. Interesujące systemy autonomiczne to: AS8267 i AS8323.

Do wyszukania adresów IP rozgłaszanych przez te systemy autonomiczne wykorzystano informacje z kolektorów tras projektu RIPE RIS. Dane te (tab. 1) stanowiły dla nas podstawę do znalezienia adresów IP z listy miejsc docelowych *skittera*. Przedział czasu, którego dotyczyło zapytanie do bazy [21], to okres od 15 lipca do 15 sierpnia 2006 roku.

Tabela 1
Prefiksy rozgłaszane przez AS należące do ACK CYFRONET AGH [21]

ASN	Prefiksy
8267	192.245.169.0 /24
	195.150.224.0 /19
	149.156.0.0 /16
8323	193.193.64.0 /19
	195.150.0.0 /16
	195.150.11.0 /24
	194.8.45.0 /24
	194.8.46.0 /24
	193.193.75.0 /24

Warto tu zwrócić uwagę na błąd w konfiguracji routera w systemie autonomicznym AS8323. Niepotrzebnie rozgłaszany jest prefiks 193.193.75.0 /24, który zawiera się w prefiksie 193.193.64.0 /19. Podobnie jest z prefiksem 195.150.11.0 /24 zawartym w 195.150.0.0 /16. Błędy te zostały zgłoszone do administratora ACK CYFRONET AGH, a następnie zostały one poprawione. Nie są już rozgłaszane adresy o zakresie 193.193.75.0 /24 oraz 195.150.11.0 /24. Narzędzia tego typu [21] mogą (i powinny) być wykorzystane do sprawdzenia poprawności konfiguracji routerów.

W celu przedstawienia struktury połączeń na poziomie routerów wykorzystano dane z narzędzia *skitter*. Wybrano punkt pomiarowy, który znajduje się w Cambridge w Anglii, o nazwie *cam*. Z bazy danych pobrano pliki z pomiarami wykonanymi w okresie od 2 do 5 sierpnia 2006 roku. Zawartość tego pliku po konwersji na postać znaków ASCII [16] i obejmuje:

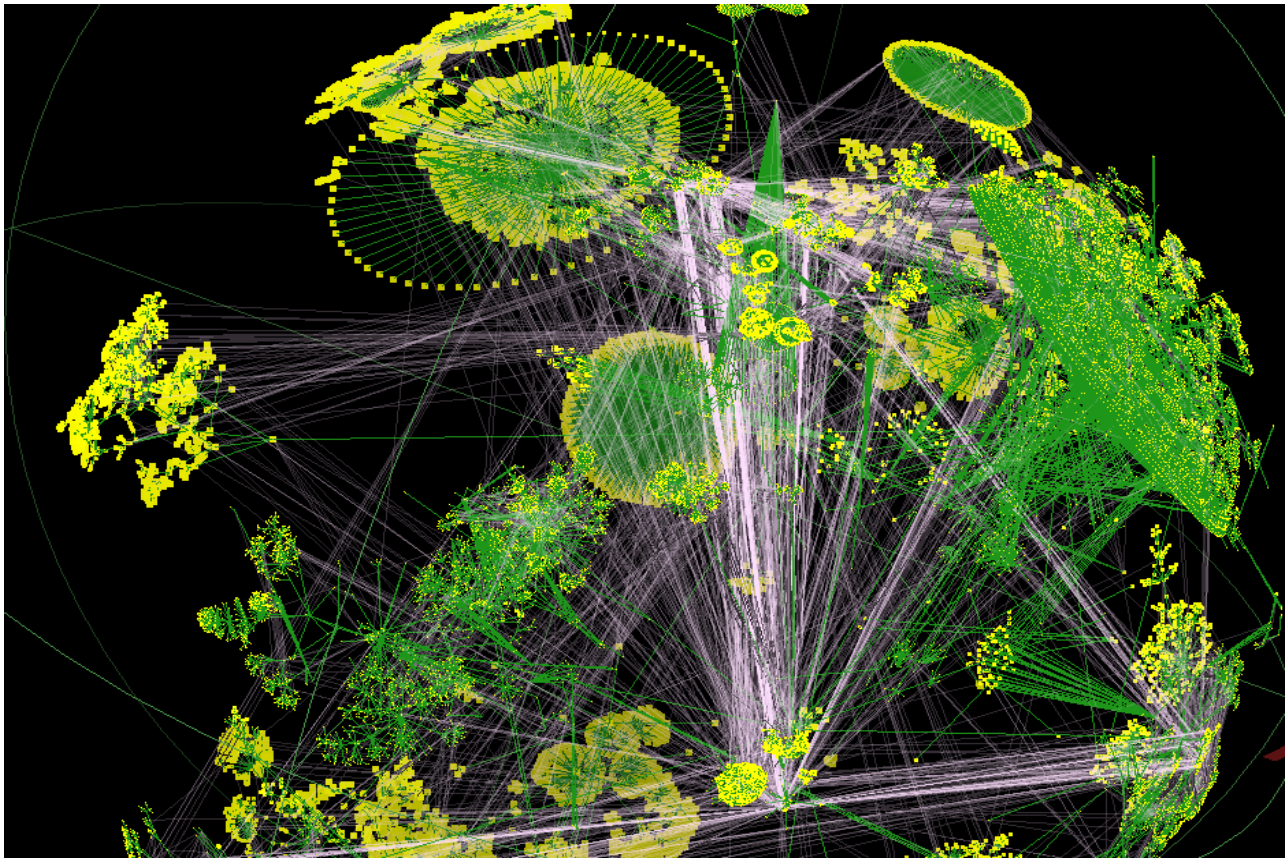
- informacje na temat ścieżki,
- adres IP punktu pomiarowego (*skittera*),
- adres IP miejsca docelowego, czyli ostatniego punktu pomiarowego na ścieżce,
- czas, kiedy *skitter* wysłał pierwsze zapytanie do miejsca docelowego,
- RTT – czas w milisekundach od wysłania pakietu ze *skittera* do pojawienia się pierwszej odpowiedzi od miejsca docelowego na wejściu *skittera*,
- TTL – reprezentuje liczbę „skoków” od punktu pomiarowego do docelowego,

Pozostałe kolumny zawierają adresy IP kolejnych węzłów znajdujących się na ścieżce od źródła do celu.

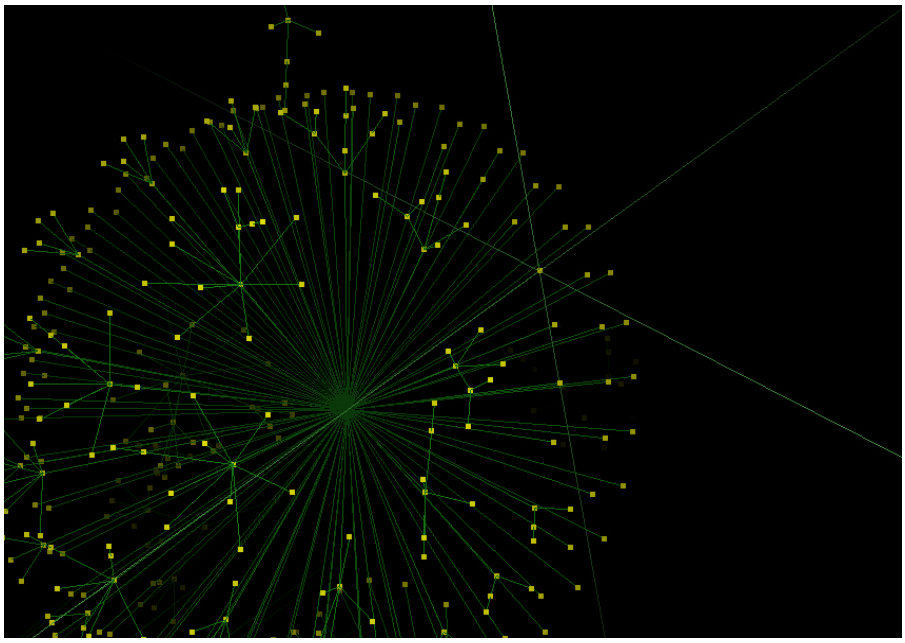
4.2. Mapa struktury na poziomie routerów

Do prezentacji graficznej grafu służy program *Walrus* [22], który tworzy strukturę grafu na podstawie informacji zawartych w pliku [16]. Rysunek tworzony jest wewnątrz sfery (rys. 2). Punkty znajdujące się blisko jej środka są powiększane, a znajdujące się w pobliżu zewnętrznej krawędzi – pomniejszane. Stopień powiększenia maleje stopniowo od środka sfery w kierunku krawędzi aż do momentu, gdy ostatnie obiekty zostaną zredukowane do zera (powierzchnia sfery reprezentuje nieskończoność).

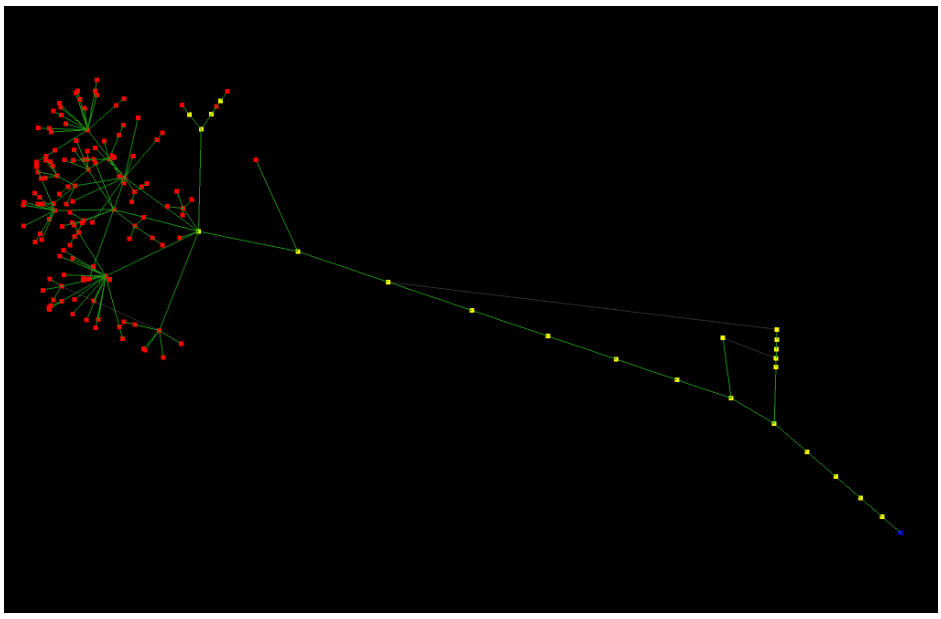
Użytkownik może wybrać dowolny fragment grafu i umieścić go w punkcie centralnym (rys. 3). Dzięki temu można szczegółowo oglądnąć mały wycinek grafu niezależnie od jego rozmiarów. Program generuje układ graficzny węzłów i kanałów na podstawie algorytmu drzewa rozpinającego (*spanning tree*). Graf jest skierowany od punktu pomiarowego do węzłów



Rys. 3. Struktura połączeń na poziomie routerów



Rys. 3. Widok po wybraniu dowolnego węzła jako środka grafu



Rys. 4 Struktura połączeń na poziomie IR dla AS8267

reprezentujących adresy IP, które znajdują się na liście miejsc docelowych.

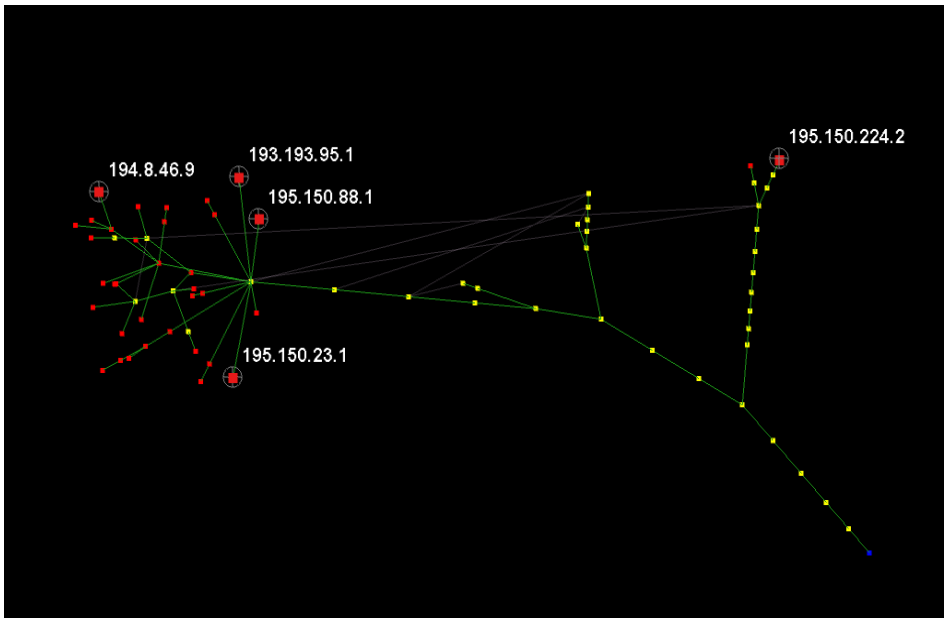
Ponieważ dane z narzędzia *skitter* zawierają wszystkie węzły znajdujące się na liście miejsc docelowych (rys. 2), przeprowadzono filtrację i wyszukano jedynie te, które znajdują się w tabeli 1. Graficzna struktura połączeń na poziomie routerów została przedstawiona osobno dla obydwu systemów autonomicznych (rys. 4 i rys. 5) oraz na rysunku zbiorczym przedstawiającym całą strukturę ACK CYFRONET AGH (rys. 6).

Kanały reprezentujące strukturę drzewa rozpinającego narysowano kolorem zielonym, pozostałe – kolorem szarym. Węzły grafu przedstawiono w 3 kolorach:

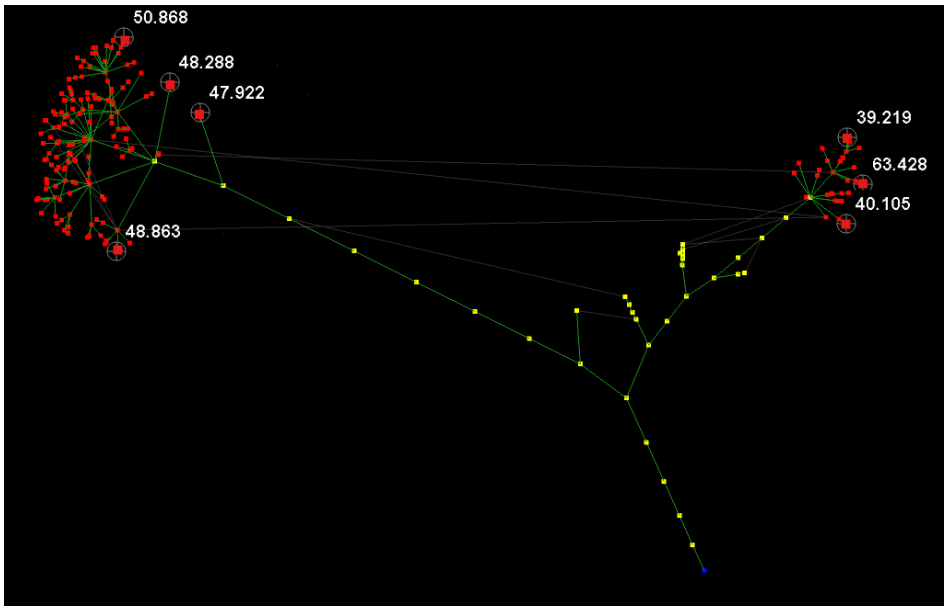
1. zielonym – adresy IP należące do ACK CYFRONET AGH,
2. niebieskim – adres IP punktu pomiarowego (128.232.97.8),
3. żółtym – adresy znajdujące się na ścieżce od punktu pomiarowego do miejsc docelowych.

Wszystkie węzły przedstawione w grafie reprezentują pojedyncze urządzenia, tzn. router z wieloma interfejsami jest reprezentowany jako jeden węzeł.

System autonomiczny AS8267 zawiera 73978 potencjalnie dostępnych adresów IP. Obliczono je na podstawie tabeli 1 po odjęciu adresów z ustawionymi



Rys. 5. Struktura połączeń na poziomie IR dla AS8323



Rys. 6. Struktura połączeń na poziomie IR dla AS8267 i AS8323

bitami ID hosta na 0 (ID sieci) oraz adresów z ustawionymi bitami ID hosta na 1 (adres rozgłoszeniowy danej sieci). Z narzędzia *skitter* uzyskano 137 dostępnych adresów IP należących do tego systemu autonomicznego. Należy podkreślić, że *skitter* wykrywa jedynie te adresy, które znajdują się na liście miejsc docelowych. Poza tym nie wiadomo, jaka część adresów z dostępnej puli jest zagospodarowana, ani jaka ich część jest aktywna.

Program *Walrus* umożliwia wyświetlenie adresu IP dla każdego węzła grafu (rys. 6). Aby rysunek był czytelny adresy pokazano tylko dla kilku punktów. System autonomiczny AS8323 zawiera 74232 potencjalnie dostępnych adresów. Z narzędzia *skitter* uzyskano 36 dostępnych adresów IP.

Przy pomocy tego programu można również przedstawić czas drogi okrężnej RTT dla pakietu kontrolnego dla każdego węzła, który reprezentuje miejsce docelowe (rys. 6). Nie ma możliwości prezentacji wartości RTT dla węzłów znajdujących się na ścieżce do miejsca docelowego. Systemy autonomiczne AS8267 i AS8323 zawierają 140.020 potencjalnie dostępnych adresów IP. Część z nich jest rozgłaszana zarówno przez AS8267 (195.150.224.0 /19), jak i AS8323 (195.150.0.0 /16). Z narzędzia *skitter* uzyskano 173 dostępne adresy IP.

4.3. Mapa struktury na poziomie systemu autonomicznego

Na podstawie tablicy BGP z projektu RouteViews wykonano konwersję adresów IP na systemy autonomiczne. Ponieważ tablice BGP zapisywane są do pliku co dwie godziny, a pomiary narzędziem *skitter* trwały kilka dni, wybrana została pierwsza tablica BGP z dnia (i godziny), w którym zakończono pomiary. Konwersja adresów IP na systemy autonomiczne przebiega według odpowiednio przygotowanego pliku (rys. 7). Został on utworzony przez program dostarczony w pakiecie *CoralReef* [23] na podstawie tablicy BGP routera CISCO. Wyodrębniono z niego wszystkie miejsca docelowe (prefiksy) osiągane z tego routera i przyporządkowane do nich numery systemów autonomicznych.

```
Adres sieci          maska  ASN
149.152.0.0          16     22742
149.153.0.0          16     1213
149.155.0.0          16     786
149.156.0.0          16     8267
149.157.0.0          16     1213
195.150.0.0          16     8323
195.150.11.0         24     8323
195.150.224.0        19     8267
```

Rys. 7. Prefiksy z numerami ich systemów autonomicznych (fragment pliku)

Pierwsza kolumna określa adres sieci, a druga jej maskę. W trzeciej kolumnie są numery systemów autonomicznych przyporządkowane do danego prefiksu. Adresy IP znajdujące się w pliku oraz wszystkie pozostałe, znajdujące się na ścieżce od punktu pomiarowego, zamienione zostały na odpowiadające im numery systemów autonomicznych i utworzono z nich graf skierowany od punktu pomiarowego do miejsc docelowych [16].

Graficzną strukturę połączeń na poziomie systemów autonomicznych prezentują rysunki 8 (AS8267), 9 (AS8323), 10 (AS8267 i AS8323). Przy każdym węźle podany jest numer ASN. Punkt pomiarowy umieszczony jest w AS786.

Ponieważ w każdym z dwóch systemów autonomicznych należących do ACK CYFRONET AGH znajduję się grupa adresów IP, które reprezentują miejsca docelowe, to program Walrus umożliwia przedstawienie trzech wartości czasu RTT:

1. wartości maksymalnej dla systemu autonomicznego;
2. mediany dla systemu autonomicznego;
3. wartości minimalnej dla systemu autonomicznego.

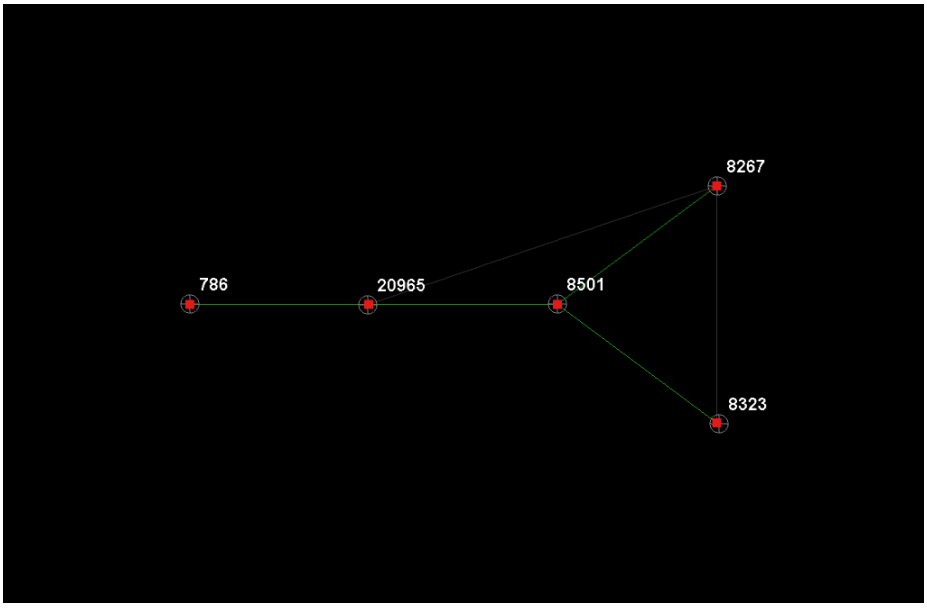
Czas podróży pakietu ICMP dla AS8267 wynosi: 157,529 ms (wartość maksymalna), 48,676 ms (mediana) i 44,375 ms (wartość minimalna).

Czas podróży pakietu ICMP dla AS8323 wynosi: 51,524 ms (wartość maksymalna), 40,105 ms (mediana), 38,866 ms (wartość minimalna).

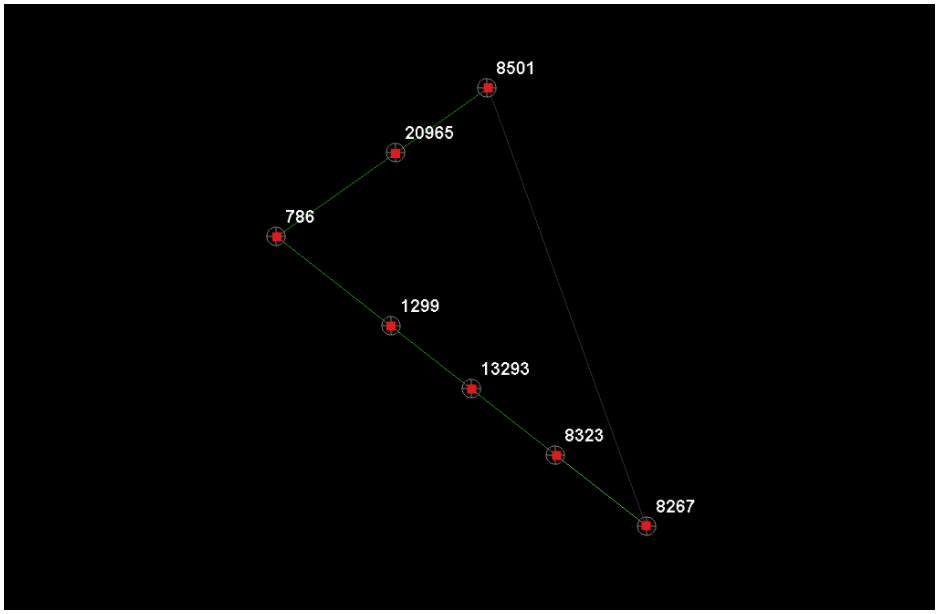
W tym miejscu uwidacznia się niedoskonałość programu *Walrus*. Na rysunku 10 nie widać wyraźnie bezpośredniego połączenia AS20965 z AS8267 w porównaniu do rysunku 8. Wynika to z tego, że program narysował w tej samej płaszczyźnie połączenia między AS20965 z AS8501 z AS8267 (kolor zielony) oraz bezpośrednie połączenie AS20965 z AS8267 (kolor szary). Połączenia te pokrywają się.

4.4. Analiza na podstawie danych RIPE RIS

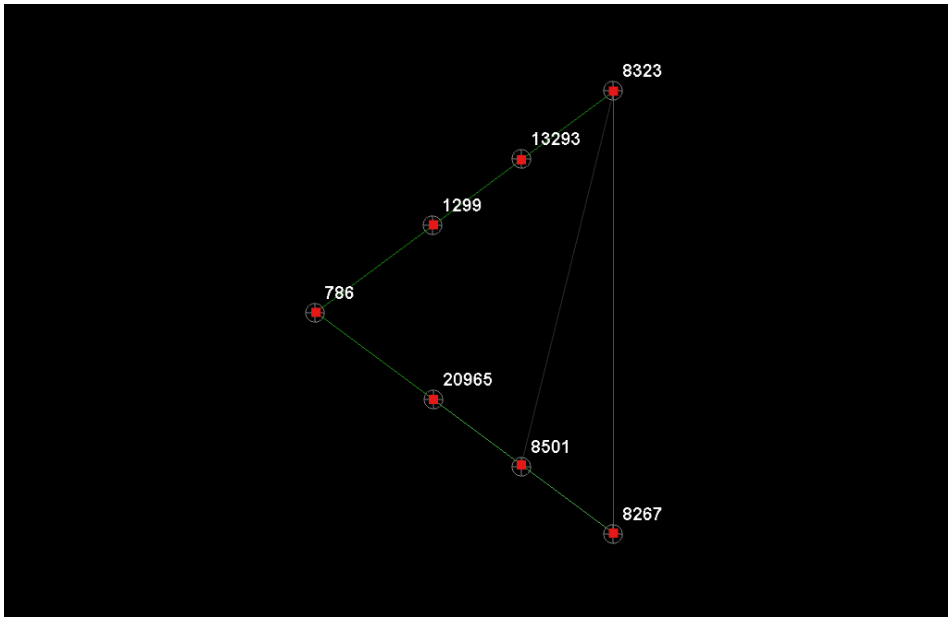
Zaprezentowana w poprzednim rozdziale analiza struktury sieci ACK CYFRONET AGH polegała na przekształceniu topologii routerów na strukturę systemów autonomicznych przy wykorzystaniu informacji



Rys. 8. Struktura połączeń na poziomie systemów autonomicznych dla AS8267



Rys. 9. Struktura połączeń na poziomie systemów autonomicznych dla AS8323



Rys. 10. Struktura połączeń na poziomie AS dla AS8267 i AS8323

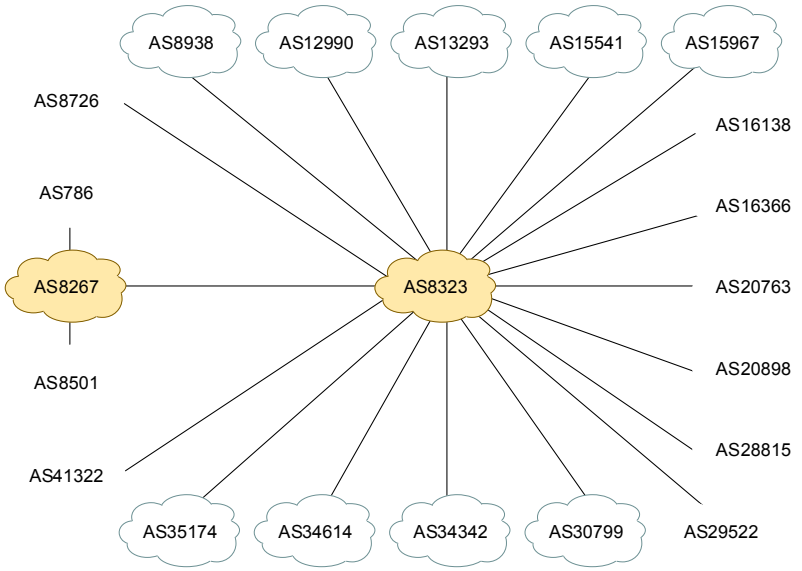
z protokołu BGP. Uzyskane wyniki zostaną teraz porównane z danymi uzyskanymi z projektu RIPE RIS, który wykorzystuje wyłącznie informacje z BGP.

Wyszukano wszystkie systemy sąsiadujące z systemami autonomicznymi AS8267 i AS8323, które były widziane w ciągu ostatnich trzech miesięcy (rys. 11[3]).

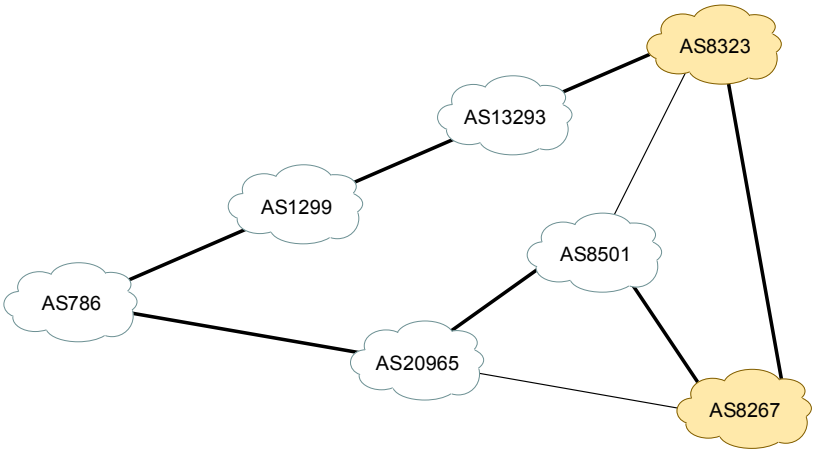
W porównaniu ze strukturą uzyskaną za pomocą narzędzia *skitter* (rys. 10) system autonomiczny AS8323 ma znacznie więcej sąsiadów. Różnice te wynikają z innej metody pomiarowej oraz z tego, że dane ze *skittera* uzyskano tylko z jednego punktu pomiarowego, natomiast dane z projektu RIPE RIS zostały zebrane z wielu punktów pomiarowych. Uwagę zwraca to, że *skitter* wykrył połączenia, których nie ma na rysunku 11. Są to np. połączenia systemu autonomicznego AS8501 z AS8323 oraz AS8267 z AS20965. Strukturę połączeń, uzyskaną z narzędzia *skitter* (rys. 10) w odniesieniu do struktury uzyskanej z danych RIPE RIS, przedstawiono na rysunku 12.

Połączenia między systemami autonomicznymi, które uzyskano ze *skittera* oraz z RIPE RIS [24], narysowano linią pogrubioną, cienką linią narysowano te, których nie wykryły kolektory tras. Celem tego porównania było potwierdzenie struktury uzyskanej z narzędzia *skitter*, dlatego na rysunku 12 nie przedstawiono pozostałych sąsiadów systemów autonomicznych.

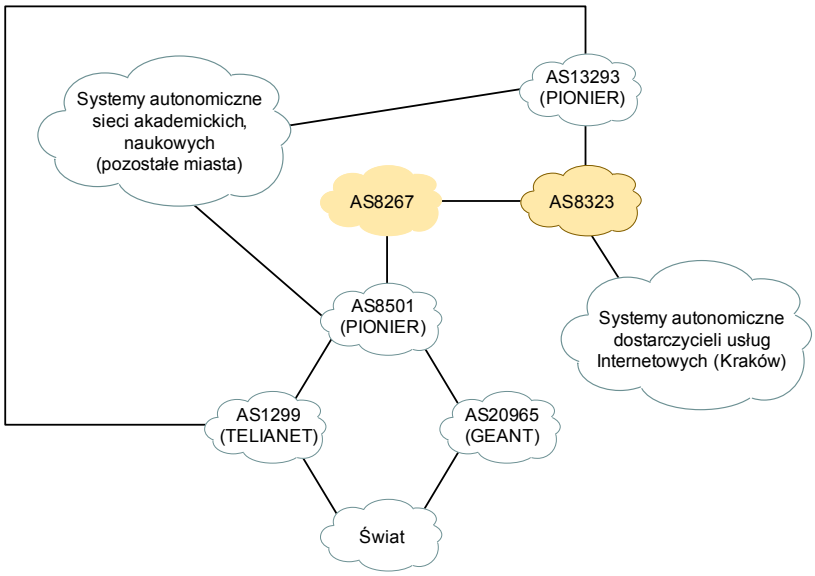
[3] Zapytanie do bazy danych [25], z której otrzymano informacje o sąsiadujących systemach autonomicznych, wykonano 26 sierpnia 2006 roku.



Rys. 11. Połączenia systemów autonomicznych Cyfronetu i ich sąsiadów



Rys. 4.12. Porównanie struktury na poziomie AS dla dwóch metod pomiarowych



Rys. 4. 13. Najważniejsze elementy struktury sieci ACK CYFRONET AGH

Aby wyjaśnić problem połączeń systemu autonomicznego AS8267 z AS20965 i AS8323 z AS8501, które nie zostały wykryte przez kolektory tras, należy najpierw przedstawić strukturę połączeń dalszych sąsiadów sieci ACK CYFRONET AGH (rys. 13). Informacje o poszczególnych systemach autonomicznych uzyskano na podstawie [24], [5].

Sieć ACK CYFRONET AGH jest częścią sieci naukowej PIONIER [25]. Systemy autonomiczne AS8501 i AS13293 są punktami centralnymi, które łączą sieci z całej Polski. PIONIER jest częścią sieci GEANT. Jest to ogólnoeuropejska sieć badawcza, która łączy ośrodki naukowe w Europie oraz posiada połączenia ze Stanami Zjednoczonymi, Ameryką Południową oraz Azją [26], [27]. Sieć PIONIER połączona jest również z systemem autonomicznym AS1299, należącym do dostawcy usług internetowych *TeliaSonera International Carrier*. Jest to operator międzynarodowy, należy do warstwy 1 [28]. Do systemu autonomicznego AS8323 podłączeni są krakowscy dostawcy usług internetowych.

Z listy miejsc docelowych narzędzia *skitter* zostało wyszukane to, którego odwzorowanie adresów IP na poziom systemów autonomicznych utworzyło połączenie AS8501 z AS8323. Jest to adres IP 149.156.10.34. Utworzona ścieżka połączeń jest kompletna, tzn. miejsce docelowe oraz wszystkie pośrednie węzły w ścieżce odpowiedziały na zapytania. Kolejność połączeń od punktu pomiarowego do miejsca docelowego przedstawiono w tabeli 2. Ponieważ punkt pomiarowy znajduje się w Anglii, to zapytania protokołu ICMP przeszły przez sieć GEANT (AS20965), a następnie przez sieć PIONIER (AS8501).

Podczas odtwarzania struktury sieci z dokładnością do routerów oraz do

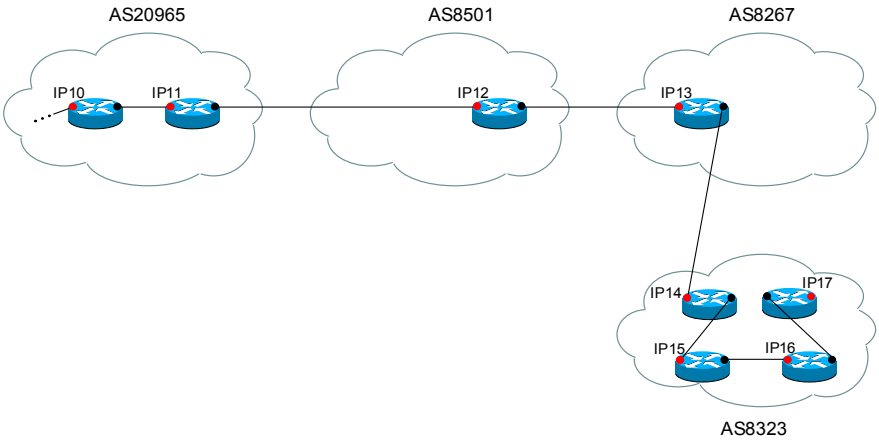
systemów autonomicznych (rys. 14) założono, że struktura połączeń z dokładnością do systemów autonomicznych, uzyskana z narzędzi RIPE RIS, jest prawidłowa. Informacje te zostały potwierdzone przez administratora systemów autonomicznych AS8267 i AS8323. Uzyskano także informację, że adres IP13 (patrz tab. 2) jest przypisany do routerze w systemie autonomicznym AS8267 a adres IP17 do routera w systemie autonomicznym AS8323. Na tej podstawie możliwe stało się odtworzenie wewnętrznej struktury połączeń w systemach autonomicznych na poziomie routerów (rys. 14).

Interfejs każdego routera ma przypisany adres IP (tab..2). Interfejsy, które odpowiedziały na zapytania *skittera,* zostały zaznaczone kolorem czerwonym. W celu zachowania przejrzystości rysunku, graf połączeń rozpoczęto od skoku o numerze 10. W większości przypadków, zestawiając połączenie między

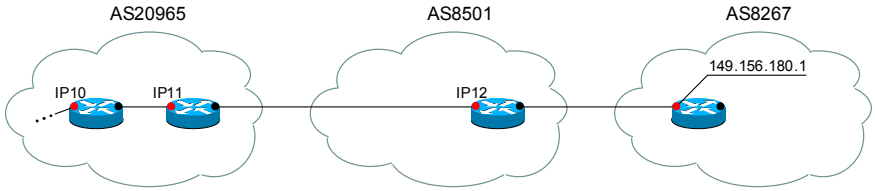
Tabela 2

Ścieżka połączeń na poziomie IR od punktu pomiarowego do ASN8267

Numer kolejnego skoku	Adres IP	Oznaczenie	System autonomiczny (ASN)
0	128.232.97.8	IP0	786
1	128.232.97.3	IP1	786
2	131.111.2.126	IP2	786
3	192.153.213.193	IP3	786
4	146.97.40.49	IP4	786
5	146.97.35.9	IP5	786
6	146.97.33.30	IP6	786
7	146.97.35.98	IP7	786
8	62.40.124.197	IP8	20965
9	62.40.112.137	IP9	20965
10	62.40.112.57	IP10	20965
11	62.40.112.62	IP11	20965
12	62.40.124.182	IP12	20965
13	212.191.224.70	IP13	8501
14	195.150.1.170	IP14	8323
15	195.150.1.238	IP15	8323
16	195.150.1.194	IP16	8323
17	149.156.10.34	IP17	8267



Rys. 14. Struktura połączeń na poziomie IR oraz AS dla Cyfronetu



Rys. 15. Struktura połączeń na poziomie IR oraz AS dla Cyfronetu, c.d.

dwoma systemami autonomicznymi, do interfejsów routerów brzegowych przydziela się zakres czterech adresów IP o masce /30 [29]. W takiej sytuacji router brzegowy może mieć przydzielone do interfejsów adresy IP, które należą do różnych systemów autonomicznych (sąsiadujących ze sobą). Interfejs routera brzegowego systemu autonomicznego AS8267 ma przypisany adres IP13 z puli adresów należących do systemu autonomicznego AS8501. Dlatego bezpośrednie odwzorowanie adresów IP13 oraz IP14 w systemy autonomiczne daje błędne połączenie AS8501 z AS8323.

Połączenie systemów autonomicznych AS20965 z AS8267 (rys. 12) otrzymano dla ścieżki o docelowym adresie IP 149.156.180.1. Kolejność połączeń routerów i adresów IP jest taka sama, jak w tabeli 2 do skoku o numerze 12. Ponieważ interfejs routera brzegowego systemu autonomicznego AS8501 ma przypisany adres IP12 (rys. 15) z puli adresów należących do systemu autonomicznego AS20965, to bezpośrednie odwzorowanie adresów IP12 i 149.156.180.1 daje błędne połączenie AS20965 z AS8267.

Tak więc bezpośrednie odwzorowanie struktury na poziomie routerów na poziom systemów autonomicznych może prowadzić do błędnych wniosków. Wykorzystanie do tego celu tablic rutingu BGP wydaje się być lepszym rozwiązaniem.

5. Podsumowanie

W niniejszym artykule przedstawiono kilka ważnych metod badania struktury Internetu bazujących głównie na informacjach pochodzących z protokołu BGP. Metody te korzystały ze statycznych informacji pochodzących z różnych źródeł. Właściwości dynamiczne, aczkolwiek niezwykle ważne, zostały w niniejszym artykule pominięte, albowiem na ogół wiążą się z koniecznością wiązania różnych rodzajów informacji pochodzących z różnych źródeł, których dostępność jest ograniczona.

Ogólnie można powiedzieć, że badanie struktury Internetu jest zadaniem złożonym. Wymaga skoordynowania działań wielu organizacji i dostarczycieli usług internetowych. Jeżeli chodzi o zasięg działania przedstawionych projektów, można wyciągnąć następujące wnioski:

- Z Regionalnych Rejestrów Internetowych (RIR) jedynie organizacja RIPE prowadzi projekt RIS. Pozostałe jednostki organizacyjne nie uczestniczą w tym projekcie. Dlatego struktura i dynamika uzyskana z protokołu BGP dobrze przedstawia jedynie obszar Europy.
- Projekt Routeviews obejmuje swoim zasięgiem obszar Ameryki Północnej i uzupełnia brakujące informacje o topologii projektu RIPE RIS.

Osobnym zagadnieniem jest kwestia przetwarzania i przechowywania uzyskanych danych. Ponieważ jest ich bardzo dużo, do ich analizy wymagane są spore zasoby obliczeniowe.

W artykule pokazano, że struktura, otrzymana na poziomie systemów autonomicznych z metody opartej na analizie tablic BGP, jest dokładniejsza niż struktura uzyskana po konwersji poziomu IR na AS, oraz że metody te wzajemnie się uzupełniają. Pomiary na poziomie makroskopowym przedstawiają wewnętrzną strukturę systemów autonomicznych. Dzięki niej można oszacować opóźnienia pakietów (z punktu widzenia punktu pomiarowego).

Analiza struktury sieci Internet jest bardzo potrzebna, gdyż umożliwia określenie trendów rozwoju Internetu w skali globalnej. Dostarcza również niezbędnych danych do tworzenia modeli Internetu w celu jego symulowania na przykład podczas opracowywania nowych, lepszych protokołów routingu międzydomenowego. W praktycznych zastosowaniach przez ISP umożliwia weryfikację poprawności konfiguracji routerów i wykrywanie awarii. Przedstawiono narzędzia, które służą do analizy i wizualizacji danych pomiarowych i wyjaśniono ich zastosowanie w zależności od tego, jakie informacje o strukturze sieci są przedmiotem badania.

Literatura

[1] Malinowski M., Nowak J.: *Wykorzystanie informacji pochodzących z protokołu BGP do oceny struktury sieci Internet*. Praca Magisterska, Kraków 2006

[2] Rekhter Y., Li T., Hares S.: *A Border Gateway Protocol 4* (*BGP-4)*. RFC 4271, 01/2006

[3] CIDR Report, http://www.cidr-report.org/autnums.html

[4] Vohra Q., Chen E.: *BGP Support for Four-octet AS Number Space.* Draft-ietf-idr-as4bytes-12.txt, 11/2005

[5] RIPE whois database, http://www.ripe.net/whois

[6] Pastor-Satorras R., Vespignani A.: *Evolution and Structure of the Internet. A Statistical Physics Approach*. Cambridge University Press, Cambridge 2004, ISBN 0 521 82698 5

[7] Labovitz C., Ahuja A., Arbor A., Jahanian F.: *Experimental Study of Internet Stability and Wide-Area Backbone Failures*. Proceedings of The Twenty-Ninth Annual International Symposium on Fault-Tolerant Computing, Madison, WI, USA, 06/1999

[8] Estrin D., Rekhter Y., Hotz S.: *A Unified Approach to Inter-Domain Routing*. RFC 1322, 05/1992

[9] Cisco BGP Documentation, http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/bgp.htm#wp1020647

[10] BGP Potaroo, http://bgp.potaroo.net/as1221/bgp-active.html

[11] Zhang B., Liu R., Massey D., Zhang L.: *Collecting the Internet AS-level Topology.* ACM SIGCOMM Computer Communication Review, 01/2005, vol. 35, no. 1, s. 53-61

[12] University of Oregon Route Views Project, http://www.routeviews.org/

[13] Réseaux IP Européens (RIPE), http://www.ripe.net

[14] BGP Beacon Info, http://psg.com/~zmao/BGPBeacon.html

[15] BGP4.net, http://www.bgp4.net/wiki/doku.php?id=tools:ipv4_looking_glasses

[16] CAIDA skitter, http://www.caida.org/tools/measurement/skitter/

[17] CAIDA Macroscopic Topology Analysis, http://www.caida.org/analysis/topology/macroscopic/

[18] CAIDA Topology Monitors, http://sk-status.caida.org/cgi-bin/main.pl

[19] Zhang B., Liu R., Massey D., Zhang L.: *Collecting the Internet AS-level Topology*. ACM SIGCOMM Computer Communication Review, 01/2005, vol. 35, no. 1, s. 53-61

[20] Pansiot J.-J., Grad D.: *On routes and multicast trees in the Internet*. ACM SIGCOMM Computer Communication Review, 01/1998, vol. 28, no. 1, s. 41-50

[21] RIPE RIS Search, http://www.ris.ripe.net/perl-risapp/risearch.html

[22] CAIDA Walrus, http://www.caida.org/tools/visualization/walrus/

[23] CAIDA CoralReef, http://www.caida.org/tools/measurement/coralreef/

[24] RIPE RIS AS in use, http://www.ris.ripe.net/perl-risapp/asinuse.html

[25] PIONIER-POLSKI INTERNET OPTYCZNY, http://www.pionier.gov.pl/siec/index.htm

[26] GÉANT, http://www.geant.net/server/show/nav.153

[27] Poznańskie Centrum Superkomputerowo Sieciowe. Rocznica powstania sieci GÉANT2, 30/06/2006, http://www.man.poznan.pl/pcss/public/komunikaty/index.html?lang=pl

[28] Réseaux IP Européens (RIPE), http://www.ripe.net

[29] Lucas W. M.: *Routery CISCO. Efektywne zarządzanie*. Wydawnictwo Helion, Gliwice 2005, ISBN 83 7361 858 9

[30] RIPE BGP cheat sheet, http://www.ripe.net/projects/ris/docs/bgpcheat.html#20

Niniejsza praca została wykonana w ramach grantu N N517 228135 finansowanego przez Ministerstwo Nauki i Szkolnictwa Wyższego.

Piotr Pacyna ukończył Informatykę na Wydziale Elektrotechniki, Automatyki i Elektroniki Akademii Górniczo-Hutniczej w Krakowie. w 2005 roku uzyskał stopień doktora nauk w dziedzinie Telekomunikacja. Obecnie pracuje w Katedrze Telekomunikacji AGH, gdzie prowadzi prace naukowe oraz zajęcia z przedmiotu Nowoczesne Sieci IP. Przebywał na stażach naukowych, m.in. w Loracom we Francji oraz w CNET France Telecom. Zainteresowania naukowe obejmują problematykę projektowania i użytkowania sieci IP: routing w sieciach stałych i w sieciach ad-hoc, wsparcie mobilności terminali ruchomych w sieci IP, bezpieczeństwo i sygnalizację. Jest aktywnie zaangażowany w międzynarodowe programy naukowo-badawcze ACTS oraz IST. Brał udział w pracach badawczych na zlecenie operatorów i firm telekomunikacyjnych. Organizował konferencję Protocols for Multimedia Systems PROMS2000. Jest współautorem czterech książek i autorem kilkunastu publikacji naukowych.