

Piotr KOSZULIŃSKI, Grzegorz KOTOWSKI, Ziemowit NOWAK
Politechnika Wrocławska, Instytut Informatyki

ANALIZA STRUKTURY POŁĄCZEŃ W INTERNECIE NA POZIOMIE AUTONOMICZNYCH SYSTEMÓW

Streszczenie. Rozpatrzono strukturę Internetu na poziomie autonomicznych systemów. Opisano sposób pozyskania danych do analizy. Przedstawiono system do wyszukiwania i wizualizacji połączeń pomiędzy AS-ami. Zaprezentowano ciekawsze wyniki. Wskazano kierunki dalszych prac.

Słowa kluczowe: Internet, wizualizacja połączeń, wyszukiwanie połączeń, AS

STRUCTURE ANALYSIS THE INTERNET CONNECTIONS AT AUTONOMOUS SYSTEMS LEVEL

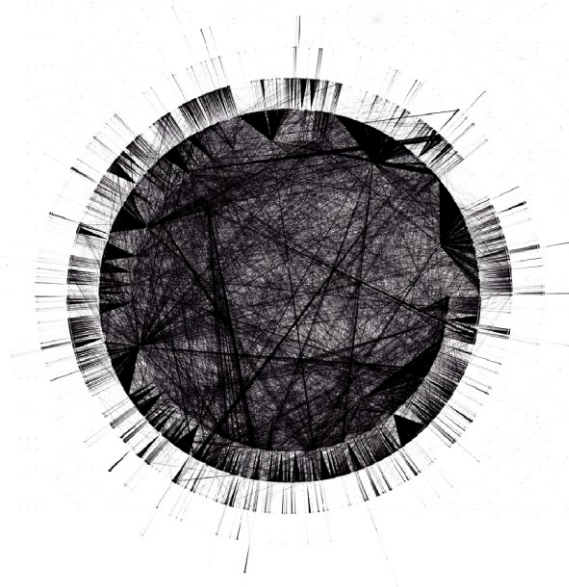
Summary. The structure of the Internet at the level of autonomous systems was examined. A method of obtaining data for analysis was described. A system for searching and visualizing the connections between the ASes was presented. More interesting results were shown. The direction for further work was laid out.

Keywords: Internet, connections' visualization, connections' searching, AS

1. Wprowadzenie w tematykę

Problematyka tomografii sieciowej – czyli uzyskiwania przekroju sieci na pewnym poziomie [1, 2] oraz wizualizacji dużych sieci – jest znana od dawna i wciąż podejmowana, w szczególności przez organizację CAIDA [3, 4]. Sieć połączeń w Internecie, z racji ich liczby, stanowi bardzo skomplikowaną strukturę. Z tego względu, jej analiza w czasie rzeczywistym nie jest możliwa. Można jednak przyjąć, że do analizy całej struktury połączeń wystarczają informacje pochodzące z autonomicznych systemów (*Autonomous System, AS*). Próbę zwizualizowania wszystkich połączeń przedstawiono na rys. 1.

Pod pojęciem autonomicznego systemu należy rozumieć wspólnie zarządzany zbiór adresów IP, względem którego stosuje się jasno zdefiniowany schemat routowania. Każdy autonomiczny system ma swój unikatowy numer ASN (*Autonomous System Number*).



Rys. 1. Próba wizualizacji połączeń pomiędzy wszystkimi AS-ami
Fig. 1. An attempt to visualize the connections between all ASes

System autonomiczny wykorzystuje jeden lub więcej protokołów z rodziny protokołów routowania danych wewnątrz systemu autonomicznego IGP (*Interior Gateway Protocol*). Do wymiany informacji o routowaniu pomiędzy systemami autonomicznymi służą zewnętrzne protokoły routowania z rodziny EGP (*Exterior Gateway Protocol*), m.in. BGP (*Border Gateway Protocol*) [5].

BGP jest obecnie jedynym międzydomenowym protokołem routowania zewnętrznego wykorzystywanym przez współczesny Internet. Główną funkcją AS-a posługującego się protokołem BGP jest wymiana informacji o osiągalności sieci z innymi systemami, które gromadzone są w tzw. tablicach BGP. Informacja o osiągalności sieci zawiera również dane o systemach autonomicznych. Dane pochodzące z tablic BGP są wystarczające do zbudowania grafu, który odzwierciedla połączenia pomiędzy autonomicznymi systemami [6].

Szacuje się, że liczba aktywnych systemów autonomicznych wynosi 60 tys. spośród ok. 70 tys. zarejestrowanych. Sumaryczna liczba połączeń pomiędzy nimi wynosi ok. 120 tys., a obsługiwanych podsieci – ok. 200 tys.

Wyróżnia się 2 typy połączeń istniejących pomiędzy systemami autonomicznymi: wstępujące (*upstream*) oraz zstępujące (*downstream*). W niektórych przypadkach, dla ważniejszych węzłów komunikacyjnych (należących np. do dostawców Internetu lub firm telekomunikacyjnych), liczba połączeń zstępujących sięga 3000. Widoczne jest to np. na rys. 1 w postaci punktów skupiających wiele połączeń. Zależność liczby połączeń i węzłów od odległości od

punktu obserwacji przykładowych, autonomicznych systemów przedstawiono w tabeli 1. Dane poza zakresem analizatora połączeń zostały oznaczone kreską.

Tabela 1

Liczba węzłów i połączeń w zależności od odległości (głębokości)

Nazwa AS	Nr AS	I	II	III	IV	V	VI
KTH	5601	2	4	22	44	742	15649
WASK	8970	2	29	334	10647	30689	–
WP	12827	2	66	1164	20064	–	–
Onet	12990	3	375	4199	25227	–	–
Facebook	32934	4	1450	21129	–	–	–
Google	15169	13	2573	23477	–	–	–
Yahoo	10310	56	4385	27671	–	–	–
Cogent	174	2803	13264	32458	–	–	–

Należy zauważyć, że sieć połączeń pomiędzy systemami autonomicznymi nie jest tworzona dynamicznie, a raczej statycznie – na podstawie umów zawieranych pomiędzy organizacjami zarządzającymi odpowiednimi fragmentami sieci. Wykorzystując ten fakt możemy założyć, że, o ile zmiany wewnątrz systemów autonomicznych – leżące w gestii operatora/administradora – mogą być częste i dynamiczne, dostosowywane np. do natężenia ruchu sieciowego, o tyle zmiany w strukturze połączeń pomiędzy samymi systemami autonomicznymi są raczej rzadkie. Porównując tę strukturę do drogowej mapy świata możemy zauważyć następujące analogie: systemy autonomiczne to państwa, wewnątrz których sposób poruszania się określa sieć dróg oraz wewnętrzne przepisy, natomiast połączenia pomiędzy nimi to przejścia graniczne, ustalane na podstawie umów międzynarodowych. Można zatem przyjąć, że do analizy całej struktury połączeń wystarczą informacje na temat systemów autonomicznych.

2. Pozyskanie danych

Dane dotyczące systemów autonomicznych zostały pobrane z różnych baz funkcjonujących w Internecie (np. whois, www.cidr-report.org itp.). Do ich pozyskania wykorzystano autorskie narzędzia pozwalające na pobranie informacji, przetworzenie parserem, a następnie zapisanie ich w bazie danych. Powstały one z wykorzystaniem języka skryptowego Bash. Utworzona w ten sposób baza danych zawierała opisy połączeń pomiędzy systemami autonomicznymi: zarówno wstępujących, jak i zstępujących oraz przypisane do nich, obsługiwane podsieci. Dodatkowo, pobierane były dane dotyczące klasyfikacji systemów autonomicznych, mianowicie:

- wielcy dostawcy usług łączenia z Internetem (*Large ISPs*) – duże firmy z międzykontynentalnymi sieciami, które są dostawcami usług łączenia z Internetem,

- mali dostawcy usług łączenia z Internetem (*Small ISPs*) – regionalne firmy dostarczające Internet z małymi, miejskimi lub większymi, regionalnymi sieciami,
- klienci (*Customer ASes*) – firmy lub organizacje, które utrzymują własne sieci, ale nie dostarczają usług łączenia z Internetem (np. banki, szpitale, wojskowe sieci itp.),
- uniwersytety (*Universities*) – klasa ta została oddzielona od klasy „Klienci”, ponieważ uczelnie mają znacznie większe sieci, które obsługują tysiące hostów końcowych,
- punkty wymiany ruchu internetowego (*Internet Exchange points, IXPs*) – małe sieci, służące jako punkty wzajemnych połączeń dla członków pierwszych dwóch klas,
- centra informacji sieciowej (*Network Information Centers, NICs*) – sieci, które udostępniają ważną sieciową infrastrukturę, takie jak serwery root lub TLD (Top-Level Domain) [7].

Lokalna baza danych, w przeciwieństwie do „żywej” struktury, tworząc statyczną mapę połączeń daje niemal nieograniczone możliwości przeglądania struktury połączeń, bez ryzyka jej zakłócenia.

3. Wizualizacja połączeń

Do wizualizacji połączeń skonstruowany został dedykowany system w architekturze klient-serwer pod nazwą *ASvis*. Składa się on z dwóch części: *backendu*, czyli aplikacji działającej na serwerze i *frontendu* – aplikacji w przeglądarce internetowej. *Frontend* odpowiada za wyświetlanie graficznego interfejsu aplikacji. Żądania użytkownika realizuje wysyłając zapytania do *backendu*.

Podstawową funkcją *backendu* jest odpytywanie bazy danych o autonomicznych systemach, przetwarzanie otrzymanych wyników i realizacja zadania przeszukiwania grafu. Aby zapewnić wysoką wydajność systemu, zastosowano autorską implementację grafowej bazy danych pod nazwą *NodeDB*. Implementacja ta zapewnia bardzo szybki dostęp do struktury grafu i danych o połączeniach wierzchołków.

Komunikacja z *backendem* odbywa się poprzez interfejs wykorzystujący wzorzec architektury oprogramowania REST (*Representational State Transfer*). *Backend* odpowiada na następujące zapytania:

- GET */nodes/find/[number]* – wyszukuje AS-y o numerach pasujących do wzorca, zwraca ich listę posortowaną alfabetycznie,
- POST */nodes/meta* – zwraca metadane (takie, jak pulę adresów czy maskę sieciową) AS-ów o podanych numerach,
- GET */structure/graph/[node_number]/[depth]* – zwraca strukturę połączeń wokół AS-a do określonej głębokości, zwraca również listę numerów znalezionych AS-ów, posortowaną

wg liczby połączeń oraz listę numerów znalezionych AS-ów, posortowaną wg odległości od AS-a źródłowego,

- GET /structure/tree/[node_number]/[height]/[dir] – zwraca strukturę drzewa od AS-a o podanym numerze o danej wysokości i kierunku,
- GET /structure/path/[num_start]/[num_end]/[dir] – zwraca ścieżkę pomiędzy podanym AS-ami startowym i docelowym szukając w zadanym kierunku,
- GET /connections/meta/[num_for] – wyszukuje informacje na temat połączeń z podanego wierzchołka.

Aplikacja *frontendowa* napisana jest w języku JavaScript i do prezentacji wyników wykorzystuje HTML5 oraz CSS3. Do prawidłowego działania, *frontend* wymaga przeglądarki internetowej wspierającej WebGL oraz karty graficznej kompatybilnej z WebGL, co obecnie jest standardem niemal każdego komputera PC.

Okno aplikacji podzielone jest na dwie części. Po lewej stronie wyświetlana jest trójwymiarowa reprezentacja połączeń pomiędzy AS-ami. Aktualnie wybrany AS jest oznaczony dużym czerwonym punktem. Trójwymiarowy graf można obracać i przemieszczać. Do grafu można się przybliżać i oddalać. Po wskazaniu kursorem dowolnego wierzchołka pojawia się „dymek” z numerem i nazwą AS-a. W menu „dymka” dostępne są polecenia:

- „pokaż z głębością” – powoduje przejście do danego AS-a i wyświetlenie jego otoczenia z wybraną głębością,
- „pokaż ścieżki” – powoduje wyszukanie i wyświetlenie ścieżek pomiędzy aktualnie wybranym (na czerwono) AS-em i AS-em zaznaczonym.

Po prawej stronie okna aplikacji *frontendowej* znajduje się panel prezentujący następujące informacje:

- aktualnie wybrany AS – jego podstawowe dane (nazwa, numer),
- połączenia aktualnego AS-a z innymi AS-ami wraz z następującymi oznaczeniami:
 - U (upstream) – AS docelowy znajduje się w tablicy routingu ponad obecnym,
 - D (downstream) – AS znajduje się poniżej,
 - B (both) – oznacza, iż AS znajduje się poniżej i powyżej jednocześnie (występuje dwukrotnie),
 - OK – połączenie skonfigurowane w jednym i drugim AS-ie,
 - Bad – jeśli w jednym jest skonfigurowane, a w drugim brak takowego wpisu,
- lista puli adresów IP przypisanych do bieżącego AS-a.

Panel pozwala również nawigować po połączeniach. Kliknięcie na numer AS-a z listy połączeń powoduje jego wybranie. W aplikacji *frontendowej* wprowadzono konwencję, że każdy numer poprzedzony znakiem # (np. #12312) stanowi skrót do wyświetlenia AS-a o danym nu-

merze wraz z jego otoczeniem. Ponadto, przytrzymanie kursora nad danym połączeniem powoduje oznaczenie tego połączenia na grafie czerwoną linią.

4. Operacje na grafie połączeń

4.1. Przeglądanie połączeń

Przeglądanie połączeń pomiędzy AS-ami polega na przeglądaniu wycinka całej sieci połączeń. Wycinek taki zorientowany jest wokół wybranego AS-a, nazywanego tutaj źródłowym. Połączenia wczytywane są w zależności od zadanej głębokości wyszukiwania.

Głębokość wyszukiwania jest parametrem określającym jak dalecy sąsiedzi AS-a źródłowego mają zostać pokazani. Głębokość 1 oznacza tylko bezpośrednich sąsiadów, bo tylko do nich można dotrzeć z AS-a źródłowego przechodząc po maksymalnie 1 połączeniu. Głębokość 2 wyszuka sąsiadów, do których można dotrzeć z AS-a źródłowego przechodząc po maksymalnie 2 połączeniach itd.

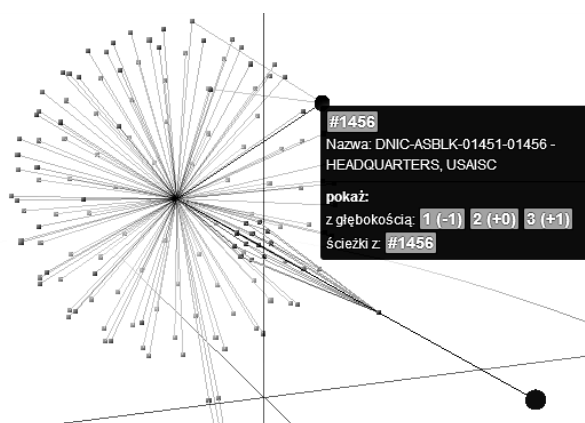
4.2. Wyszukiwanie drzew

Pod pojęciem drzewa kryje się struktura mająca korzeń, jednak nie musi być ona drzewem z matematycznego punktu widzenia. Strukturę taką należy rozumieć jako podsieć połączoną z resztą AS-ów jedynie przez zadany korzeń. Pomiędzy liśćmi i gałęziami mogą znajdować się połączenia, jeśli nie będą tworzyły dodatkowego kanału komunikacji poza obrębem tej podsieci.

Aby wyszukać drzewo, należy wybrać korzeń (jedyne punkt komunikacji z resztą świata), maksymalną głębokość poszukiwań i kierunek połączeń. Na wynikowych grafach często będzie widać niezaznaczone AS-y, które mają więcej połączeń niż jedynie z korzeniem. Mogą się też zdarzyć połączenia między liśćmi.

4.3. Wyszukiwanie ścieżek

Wyszukiwanie ścieżek pozwala na znalezienie najkrótszych ścieżek łączących dane AS-y. Mając wybrany AS źródłowy (poprzez *Przeglądanie połączeń*) z menu należy wybrać wyszukiwanie ścieżek i wprowadzić nr docelowego AS-a.



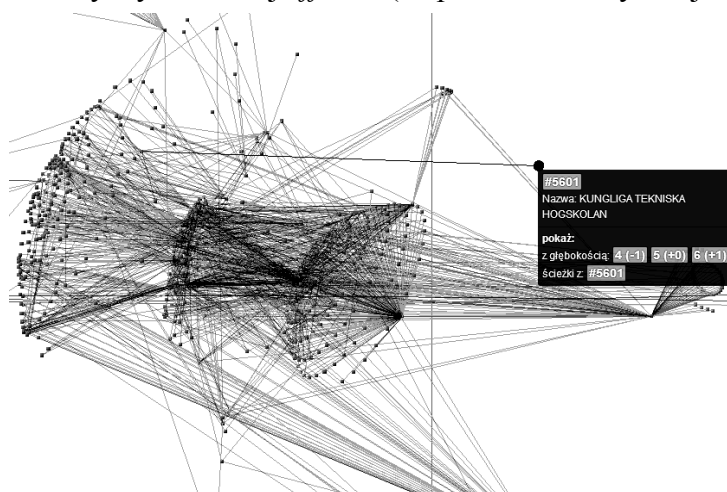
Rys. 2. Wynik poszukiwań ścieżki pomiędzy dwoma AS-ami

Fig. 2. Result search for a path between two Ases

W wyniku poszukiwań docelowy AS zostaje oznaczony dużym niebieskim punktem. Niebieskim kolorem zostaje również zaznaczona (i pogrubiona) znaleziona ścieżka lub więcej ścieżek, jeżeli jest ich więcej o tej samej długości (rys. 2).

5. Studium przypadków

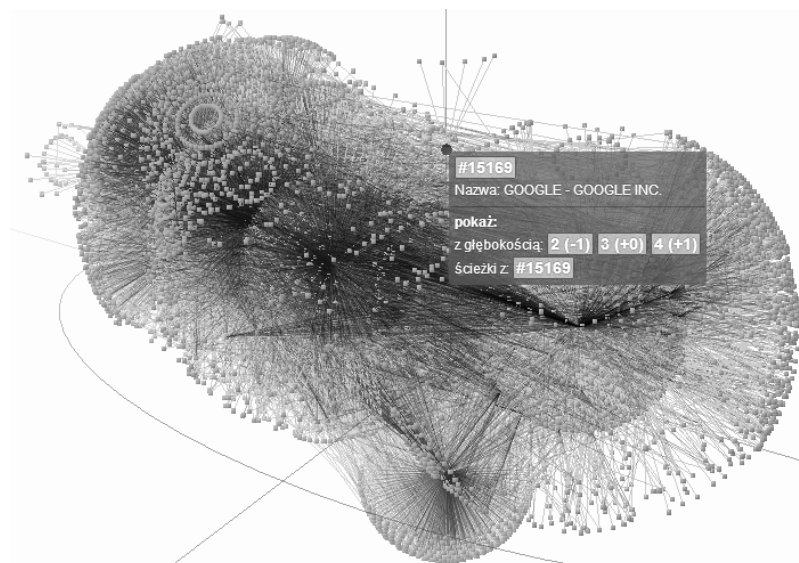
Podczas analizy sieci Internet informacje dotyczące systemów autonomicznych mogą mieć kluczowe znaczenie, ponieważ, dzięki nim, możliwe jest ograniczenie liczby koniecznych do obserwacji systemów, poprzez odrzucenie nieistotnych, z punktu widzenia eksperymentu, np. takich, które nie mają połączeń zstępujących lub stanowią ślepo zakończone rozwidlenia ścieżek głównych. Należy jednak mieć na uwadze, że trasa przejścia przez systemy autonomiczne, wyznaczona *on-line* (np. z użyciem sieciowych narzędzi diagnostycznych) może czasem różnić się od trasy wyznaczonej *off-line* (na podstawie statycznej mapy połączeń).



Rys. 3. Wizualizacja grafu o głębokości 5 dla KTH w Sztokholmie (AS174)

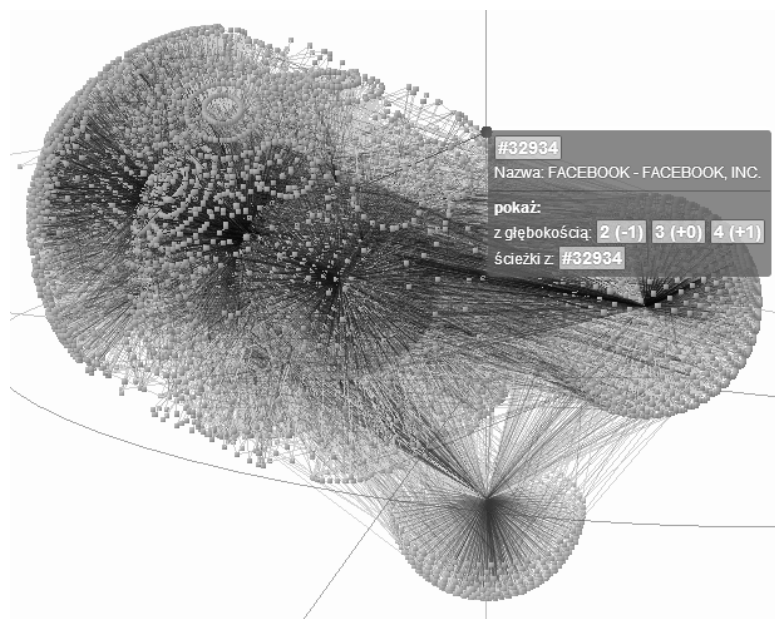
Fig. 3. Graph visualization of depth 5 for KTH in Stockholm (AS174)

Zaprezentowane przypadki pokazują, jak różne mogą być struktury połączeń, tworzone na zadaną odległość od określonego punktu. W przypadku przykładowej uczelni w Szwecji, znanej z silnie rozwiniętej sieci (AS174 Kungliga Tekniska Hogskolan KTH – Sztokholm) graf zaczyna się komplikować dopiero przy odległości 5 przeskoków na poziomie AS-ów (rys. 3). Natomiast w przypadku popularnych, komercyjnych przedsiębiorstw (Google, Facebook) można zaobserwować bardzo skomplikowaną sieć już przy odległości równej 3 przeskoki (rys. 4 i 5).



Rys. 4. Wizualizacja grafu o głębokości 3 dla Google (AS15169)
Fig. 4. Graph visualization of depth 3 for Google (AS15169)

Co ciekawe, AS15169 (Google) oraz AS32934 (Facebook), pomimo ich różnego umiejscowienia w sieci połączeń, tworzą bardzo zbliżone „wizualnie” struktury.



Rys. 5. Wizualizacja grafu o głębokości 3 dla Facebook (AS32934)
Fig. 5. Graph visualization of depth 3 for Facebook (AS32934)

6. Podsumowanie i kierunki dalszych prac

Przeważającą większość spośród wszystkich systemów autonomicznych stanowią te, które zawierają treści (lub mieszane: zawierające treści i przesyłowe), dlatego też redukcja struktury o przesyłowe systemy autonomiczne nie daje wystarczającego rezultatu – liczba pozostałych systemów autonomicznych jest nadal zbyt duża, a ich obserwacja wciąż niewykonalna. Konieczne jest zatem wykonanie kolejnych kroków, które pozwolą na uproszczenie struktury do akceptowalnego poziomu, w którym możliwa jest obserwacja w trybie rzeczywistym. Przykładem takiego podejścia jest proces agregacji systemów autonomicznych opisany w [8], który zakłada grupowanie systemów autonomicznych na podstawie podobieństwa charakterystyk, np. RTT, czasu nawiązania połączenia TCP, czasu pobrania zasobu itp.

Agregacji takiej można dokonywać na całej strukturze bądź jej fragmentach. W tym celu należy również wybrać reprezentantów, aby wykonać pomiary charakterystyk. Następnie, należy określić charakterystykę pojedynczego systemu autonomicznego, będącą wypadkową charakterystyk pojedynczych hostów przynależnych do AS-ów.

Podziękowania

Autorzy dziękują inż. Maciejowi Bańskiemu oraz Pawłowi Kościukowi za pomoc przy realizacji systemu *ASvis*.

BIBLIOGRAFIA

1. Rabbat M., Coates M., Nowak R.: Multiple Source Internet Tomography, *IEEE Journal on Selected Areas in Communications*, 24, 2006, no. 12, pp. 2221-2234.
2. Karzelek U., Nowak Z.: Automatyczne wykrywanie źródeł przeciążeń w sieciach lokalnych, *Śląskie Wiadomości Elektryczne*. 2011, nr 4, ss. 39-43.
3. Huffaker B., Fomenkov M., claffy k.: Influence Maps - a novel 2-D visualization of massive geographically distributed data sets, *Internet Protocol Forum*, 2008.
4. King A., Dainotti A., Huffaker B., claffy k.: A Coordinated View of the Temporal Evolution of Large-scale Internet Events, *Computing*, 2013.
5. Hawkinson J., Bates T.: Guidelines for creation, selection, and registration of an Autonomous System, RFC 1930, *Internet Engineering Task Force*, 1996.
6. Rekhter Y., Li T., Hares S.: A border gateway protocol 4, RFC 4271, *Internet Engineering Task Force*, 2006.

7. Dimitropoulos X., Krioukov D., Riley G., claffy k.: Revealing the Autonomous System Taxonomy: The Machine Learning Approach, PAM Workshop, Adelaide 2006.
8. Kotowski G., Gąsior D.: Application of non-probabilistic descriptions of uncertainty for evaluation of approximate performance parameters in autonomous systems aggregation, ISAT: Advances in Web-Age Information Systems, Wrocław 2009, s. 59-68.

Wpłynęło do Redakcji 29 marca 2013 r.

Abstract

The authors defined the concept of an autonomous system. Pointed out the relevance of examining the structure of the Internet AS-level. They attempted to visualize the connections between all ASes (Fig. 1). The dependence of the number of connections and nodes on the distance from the point for examples of autonomous systems is shown (Tab. 1).

The authors described a method of obtaining data for analysis. A tool for searching and visualizing the connections between the ASes is presented. Available operations on the graph were listed. The result search for a path between two ASes is shown (Fig. 2).

Interesting case studies were presented: graph visualization of depth 5 for KTH in Stockholm (Fig. 3), graph visualization of depth 3 for Google (Fig. 4) and Facebook (Fig. 5). The presented cases show similarities and differences in the structures of connections depending on the distance from the specified point.

In conclusion, the authors pointed out directions for future work that will help to simplify the structure of connections to an acceptable level.

Adresy

Piotr KOSZULIŃSKI: Politechnika Wrocławska, Instytut Informatyki, Wybrzeże Wyspiańskiego 27, 50-370 Wrocław, Polska, piotrek@koszulinski.pl

Grzegorz KOTOWSKI: Politechnika Wrocławska, Instytut Informatyki, Wybrzeże Wyspiańskiego 27, 50-370 Wrocław, Polska, grzegorz.kotowski@pwr.wroc.pl

Ziemowit NOWAK: Politechnika Wrocławska, Instytut Informatyki, Wybrzeże Wyspiańskiego 27, 50-370 Wrocław, Polska, ziemowit.nowak@pwr.wroc.pl