Z E S Z Y T Y N A U K O W E P O L I T E C H N I K I Ł Ó D Z K I E J
Nr 1154 ORGANIZACJA I ZARZĄDZANIE, z. 55 2013

ANNA SZMIT
Katedra Zarządzania
Politechnika Łódzka

MACIEJ SZMIT
Wydział Bezpieczeństwa IT dla Korporacji
Orange Labs Polska

O WYKORZYSTANIU MODELI EKONOMETRYCZNYCH DO PROGNOZOWANIA RUCHU SIECIOWEGO

Opiniodawca: **dr hab. Wojciech Czakon, prof. UE**

Akwizycja, analiza, modelowanie, prognozowanie i symulacja ruchu sieciowego są czynnościami prowadzonymi w sieciach teleinformatycznych zarówno dla potrzeb zarządzania jakością jak i zarządzania bezpieczeństwem. W szczególności w prognozowaniu ruchu sieciowego wykorzystuje się modele statystyczne, ekonometryczne, modele szeregów czasowych oraz metody zaliczane do sztucznej inteligencji. W artykule przedstawiono krótki przegląd metod prognozowania wykorzystywanych współcześnie w metodach NBAD (ang. Network Behavioral Anomaly Detection) w odniesieniu do rekomendacji Międzynarodowej Unii Telekomunikacyjnej (ITU).

1. Prognozowanie ruchu sieciowego – rekomendacje ITU-T

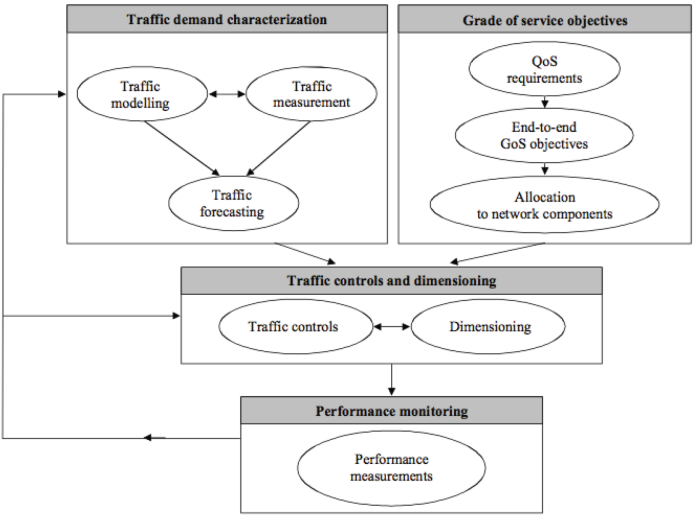
Akwizycja, analiza, modelowanie, prognozowanie i symulacja ruchu sięciowego są czynnościami prowadzonymi w sieciach teleinformatycznych zarówno dla potrzeb zarządzania jakością (na przykład wykrywanie „wąskich gardeł" transmisji, zaburzeń ruchu[1], czy w ramach testów obciążeniowych urządzeń sięciowych) jak i w ramach zarządzania bezpieczeństwem informatycznym[2] (na przykład detekcja anomalii czy analiza botnetów[3]). W szczególności w prognozowaniu

[1] Zjawisk takich jak na przykład "burst of updates" w protokole BGP – zob. np. [16] s. 248.
[2] Por. np. [10] str. 194 i nast.
[3] Botnet jest to grupa komputerów zainfekowanych złośliwym oprogramowaniem pozwalającym osobie, która je kontroluje na zdalne zarządzanie komputerami wchodzącymi w ramach botnetu

ruchu sieciowego wykorzystuje się modele statystyczne, ekonometryczne, modele szeregów czasowych oraz metody zaliczane do sztucznej inteligencji.

Inżynieria ruchu sieciowego (ang. Network Traffic Engineering) jest dyscypliną zajmującą się badaniem zjawisk i procesów zachodzących przy przesyłaniu informacji w sieciach teleinformatycznych. Historycznie pierwszymi sieciami, dla których prowadzono rozważania dotyczące inżynierii ruchu, były sieci telekomunikacyjne POTS (ang. Plain Old Telephone Services). Współcześnie rozważania dotyczące ruchu sieciowego prowadzi się głównie w odniesieniu do sieci komputerowych.

Trzy główne grupy zagadnień inżynierii ruchu sieciowego w ujęciu ITU[4] stanowią: pomiary ruchu (ang. traffic measurements), modelowanie ruchu (ang. traffic modelling) oraz prognozowanie ruchu (ang. traffic forecasting) – zob. Rys. 1. Głównymi metodami badawczymi inżynierii ruchu sieciowego[5] są modelowanie i symulacja obliczeniowa[6].



Rys. 1. Traffic engineering tasks
Źródło: [9, s. 2].

(tzw. komputerami zombie). W skład botnetu może wchodzić duża liczba urządzeń. Na przykład botnet o nazwie Virut, którego polskie domeny 17 stycznia 2013 zostały zablokowane przez administratorów NASK, miał pod prawdopodobnie kontrolą ponad 300 tys. urządzeń – w samej Polsce.

[4] ang. International Telecomunication Union, Międzynarodowa Unia Telekomunikacyjna.

[5] Przegląd rekomendacji ITU dotyczących inżynierii ruchu sieciowego zebranych w rekomendacji [9] został omówiony w referacie [25].

[6] W szczególności rodzajem symulacji obliczeniowej może symulacja komputerowa (ang. a computer simulation). W odniesieniu do ruchu sieciowego należałoby jednak rozróżnić symulację komputerową, wykorzystywaną np. do empirycznych testów wydajności urządzeń sieciowych a polegającą na generowaniu czy preparowaniu ruchu sieciowego i „symulację obliczeniową", będącą badaniem nieempirycznym (teoretycznym) w której komputer wykorzystywany jest do prowadzenia obliczeń.

W szczególności rekomendacja [9] zaleca[7] stosowanie do predykcji ruchu modeli, wśród których wymienia jako przykładowe modele z trendem (liniowym, parabolicznym, wykładniczym, logistycznym,danym funkcją Gompertza), modele z wygładzaniem (prostym wygładzaniem wykładniczym, podwójnym wygładzaniem wykładniczym, regresję ważoną, modele Holta, modele Holta-Wintersa), modele autoregresji (modele autoregresji linowej AR, scałkowane modele autoregresji i średniej ruchomej ARIMA), modele przestrzeni stanów z filtrem Kalmana, modele regresji liniowej z egzogenicznymi zmiennymi objaśniającymi.

Warto zwrócić uwagę na rozróżnienie, jakie rekomedacja [ITU-T E.490.1] czyni pomiędzy modelowaniem a prognozowaniem. Rzeczywiście, o ile do modelowania i symulacji zachowań systemów sieciowych stosuje się stosunkowo często modele generatywne (takie jak: modele Markova czy procesy Poissona), o tyle do prognozowania warto stosować wspomniane wyżej modele dyskryminacyjne.

Z uwagi na złożoność i wielość procesów zachodzących we współczesnych sieciach komputerowych, aby zbudować model opisowy trzeba dysponować rzeczywiście szczegółową analizą zjawisk zachodzących w konkretnej sieci, co zazwyczaj wymaga dłuższych analiz ruchu rzeczywistego, podobnie model generatywny nie może ograniczyć się do modelowania jednego zjawiska czy technologii sieciowej, bowiem w sieciach rzeczywistych funkcjonuje najczęściej wiele zjawisk i procesów, często powiązanych ze sobą. Z tego też względu rozsądne jest wykorzystanie modeli szeregów czasowych (ang. Time Series Models), operujących na historycznych danych endogenicznych, w tym również modeli adptacyjnych, czy metod zaliczanych tradycyjnie do dziedziny sztucznej inteligencji (ang. Artificial Intelligence, AI), takich jak drzewa decyzyjne, rozproszone sztuczne sieci neuronowe, algorytmy immunologiczne czy logika rozmyta[8].

Inżynieria ruchu sieciowego, dyscyplina „czysto informatyczna", jest więc dziedziną, w której – dość niespodziewanie – zastosowanie znajdują metody i formalizmy znane i wypracowane w naukach ekonomicznych, w tym naukach o zarządzaniu.

2. Modelowanie w NBAD

Zaburzenia zachowań ruchu sieciowego są ważne z punktu widzenia jakości usług sieciowych, a powodowane mogą być przez uszkodzenia (celowe – na przykład na skutek działania cyberprzestępców, bądź przypadkowe – na przykład na skutek błędnej konfiguracji czy uszkodzenia sprzętu sieciowego). W przypadku działań celowych zarządzanie jakością wiąże się z zarządzaniem bezpieczeństwem.

[7] Jakkolwiek jest to rekomendacja – z punktu widzenia tempa rozwoju wysokich technologii – zdecydowanie wiekowa, ma ona ciągle status obwiązujący.

[8] Przegląd metod sztucznej inteligencji stosowanych w detekcji intruzów zawiera artykuł [14].

Do wykrywania i analizowania takich zjawisk wykorzystuje się systemy zaliczane do grupy IDS/IPS/UTM. Systemy IDS (ang. Intruder Detection Systems) są rozwiązaniami sprzętowymi bądź programowymi, których zadaniem jest wykrywanie prób włamań do zabezpieczanej sieci lub hosta. W celu realizacji tego zadania monitorują ruch w sieci, użycie zasobów chronionego systemu komputerowego lub logi systemowe w celu wychwycenia podejrzanych zdarzeń i następnie podjęcia odpowiedniego działania (zazwyczaj wygenerowania komunikatu o wykrytym zagrożeniu). Rozwinięciem koncepcji systemów IDS stały się systemy z aktywną odpowiedzią (ang. Active Response System) realizowane najczęściej w postaci połączenia systemu IDS z pracą zapory sieciowej za pomocą odpowiedniego programu pośredniczącego oraz samodzielne systemy przeciwdziałania włamaniom IPS. Systemy te współpracują z zaporą sieciową (ang. Firewall) bez żadnych aplikacji pośredniczących, dzięki czemu czas potrzebny na reakcję staje się zdecydowanie krótszy. Ponadto systemy IPS oferują wiele innych możliwości, mogą na przykład uruchomić przygotowany wcześniej skrypt, wylogować użytkownika lub zablokować jego konto. IPS może równie poinformować administratora o zaistniałej sytuacji poprzez wysłanie e-maila, czy wiadomości tekstowej na telefon komórkowy.

Kolejną generacją urządzeń zabezpieczających są tzw. UTMy (ang. Unified Threat Management), które integrują – oprócz tradycyjnego IPSa – również mechanizmy takie jak bramkę antywirusową (ang. Gateway Antivirus), bramkę antyspamową (ang. Gateway Antispam), filtrowanie zawartości (ang. Content Filtering, Parent Control, PC), równoważenie obciążeń (ang. Load Balancing, Bandwidth Management) oraz moduł raportowania (on-appliance reporting), przy czym oczywiście nie w każdym systemie UTM muszą by zaimplementowane wszystkie mechanizmy, o których mowa powyżej.

Innym rodzajem wyspecjalizowanych rozwiązań z zakresu bezpieczeństwa, które mogą być implementowane w systemach UTM bądź też występować samodzielnie są systemy ochrony przed wyciekiem informacji (znane pod kilkoma anglojęzycznymi nazwami: Data Loss Prevention, Data Leak Prevention, DLP, Information Leak Prevention, Information Loss Prevention, ILP).

Biorąc pod uwagę sposób wykrywania ataków w systemach wykrywania włamań, można wyodrębnić: systemy z detekcją nadużyć (ang. misuse detection), systemy oparte na weryfikacji integralności (ang. integrity verification) i systemy z detekcją anomalii (ang. anomalny detection).

Weryfikacja integralności jest prostą i skuteczną metodą wykrywania działań napastnika w chronionym systemie komputerowym, jako że jakakolwiek akcja podjęta przez włamywacza musi znaleźć swoje odzwierciedlenie bądź to w plikach podsystemu pamięci masowej bądź też – rzadziej – co najmniej w strukturach danych znajdujących się w pamięci RAM[9]. Podobne rozwiązania

[9] Mowa o na przykład łataniu jądra systemu operacyjnego w trakcie jego pracy (bez restartu), jak ma to miejsce w przypadku niektórych włamań, a również i narzędzi pozwalających nanosić

stosuje się też w informatyce śledczej[10] oraz inżynierii odwrotnej (ang. reverse engineering).

Detekcja nadużyć dokonuje się poprzez wykrywanie zdefiniowanych zachowań, np. uzyskanie możliwości zapisu do chronionego zasobu, przesłanie pliku zawierającego znany kod wirusa bądź eksploita, detekcja anomalii natomiast zakłada istnienie pewnego wzorca zachowań[11], odchylenia od którego interpretowane są jako zdarzenie mogące, z pewnym prawdopodobieństwem, świadczyć o zaatakowaniu chronionego systemu. Tak więc, system detekcji anomalii modeluje zachowania chronionego systemu w oparciu o statystyczną idealizację obserwacji z przeszłości i obserwacji bieżących. W odniesieniu do zagadnień wykrywania anomalii pracujących w oparciu o analizę zachowań sieci komputerowych odpowiednia grupa metod nosi nazwę behawioralnego wykrywania anomalii sieciowych, ang. Network Behavior Anomaly Detection, NBAD[12] (komplementarną grupą metod są metody analizujące zachowania pojedynczych hostów – HBAD)[13]. Podczas analizy zachowań systemów sieciowych można przyjmować dwa punkty widzenia: analizę pojedynczych pakietów[14], bądź analizę przepływów sieciowych (ang. flow analysis), której elementem jest analiza ruchu sieciowego (ang. traffic analysis). Przez "analizę przepływów" rozumie się analizę metadanych dotyczących komunikacji sieciowej zebranych za pomocą telemetrii sieciowej[15]. Analizowane informacje dotyczą różnych aspektów komunikacji (np. jakie hosty komunikowały się z jakimi, jakich używały do tego celu portów, jakie wartości przyjmowały flagi TCP itd.).

Analiza ruchu sieciowego jest częścią analizy przepływów i zajmuje się metadanymi dotyczącymi natężenia poszczególnych rodzajów ruchu, jest więc tylko jednym z elementów analizy przepływów. Jeśli analiza ruchu prowadzona jest w celu znalezienia wzorca ruchu i wykrywania sytuacji od tego wzorca odbiegających, mówi się o detekcji anomalii ruchu sieciowego.

---

poprawki do jądra systemu na działającym serwerze bez naruszania jego ciągłości działania, np. Uptrack firmy KSplice. Zob: [11].

[10] W szczególności akwizycją i analizą dowodów elektronicznych zajmuje się dyscyplina zwana computer evidence, w której – obok klasycznej analizy zapisów na zabezpieczonych procesowo nośnikach pamięci masowej wyróżnia się – ostatnimi czasy coraz bardziej popularną – analizę zawartości komputerów w trakcie ich pracy tzw. live forensic (określeniem „Computer Forensic" nazywa się samą informatykę śledczą – w języku polskim funkcjonuje też określenie „informatyka sądowa").

[11] Tzw. wzorca predykowanego. Por. np. [26], str. 419 i nast.

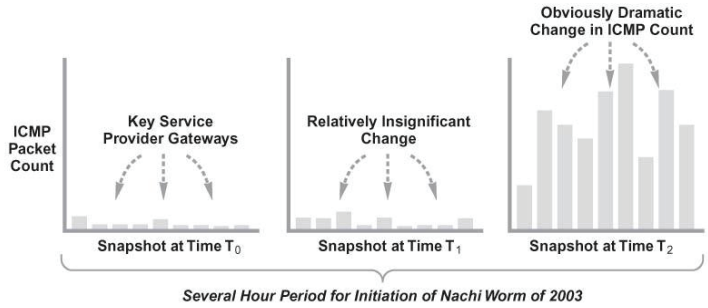
[12] Pewną trudnością w stosowaniu takiego podejścia jest konieczność apriorycznego ustalenia co jest anomalią, żeby móc później ocenić czy zastosowana metoda te anomalie wykryła – w artykule [14] mówi się o paradoksie systemów detekcji anomalii. Budzącą pewne wątpliwości metodologiczne – acz dość powszechnie stosowaną – metodą jest "manualne" generowanie anomalii (por. np. [4]).

[13] Zob. np. [3], [5], [13].

[14] W literaturze używa się pojęć „packet inspection" w odniesieniu do analizy nagłówków pakietów (np. w zaporach przeciwogniowych) oraz „deep packet inspection" (DPI) w odniesieniu do analizy zawartości poszczególnych pakietów (pola danych).

[15] Zob. np. [7] str. 47 i nast.

Analiza ruchu sieciowego nie musi być prowadzona w odniesieniu wyłącznie do sumarycznej liczby pakietów. Wydaje się wręcz wskazane zróżnicowanie co najmniej poszczególnych protokołów. Róże protokoły pełnią bowiem różną rolę w komunikacji sieciowej. Na przykład jedną z ról protokołu ICMP jest zapewnianie informacji o błędach, analiza ruchu ICMP musi więc być – z punktu widzenia detekcji anomalii – szczególnie interesująca. Na rysunku poniżej przedstawiono schematycznie zmiany natężenia ruchu ICMP w początkowym okresie aktywności MP aktywności robaka Nachi[16] w 2003 roku.



Rys. 2. Ruch ICMP w początkowym okresie aktywności MP aktywności robaka Nachi w 2003 roku
Źródło: opracowanie na podstawie [2].

Jak już wspomniano stosowane współcześnie modele ruchu sieciowego są znacznie bardziej złożone niż wymienione w powołanych wcześniej rekomendacjach ITU-T. Odpowiednio również mechanizmy wykrywania sytuacji anomalnych nie są oparte tylko na prostej obserwacji zwiększonego natężenia ruchu. W naszych dotychczasowych badaniach[17] posługiwaliśmy się dotychczas modelami takimi jak: modele Holta-Wintersa oraz modele Holta-Wintersa z podwójną sezonowością (modele Taylora), opisowe modele ze zmiennymi zero–jedynkowymi, modele z autoregresją liniową (AR) z parametrami estymowanymi metodą najmniejszych kwadratów oraz modele AR z parametrami estymowanymi metodą najmniejszych odległości (Last Absolute Deciation), modele SARIMA oraz sztucznymi sieciami neuronowymi – perceptronem wielowarstwowym oraz sieciami z radialną funkcją bazową.

[16] Robak Nachi (znany też pod nazwą Welchia) do rozprzestrzeniania się wykorzystywał lukę w zabezpieczeniach RPC (Remote Procedure Call) a jego działanie polegało na usunięciu z zainfekowanego systemu robaka Blaster (jeśli ten był w nim obecny), zainstalowaniu szeregu poprawek, a następnie autodestrukcji samego robaka. Welchia była więc nietypowym przypadkiem robaka o – w zamierzeniu – pozytywnym działaniu. Niestety, z powodu błędów w kodzie, robak powodował niestabilne działanie zainfekowanych systemów. Nietypowe działanie robaka stało się kanwą opowiadania zawartego w [15].
[17] zob. [18], [19], [20], [21], [22], [23], [24].

3. Problemy

Jednym z zasadniczych problemów związanym z modelowaniem ruchu sieciowego jest ilość danych, które należałoby przetworzyć[18]. Są to ilości wręcz niewyobrażalne[19]: w samych tylko Stanach Zjednoczonych wykonuje się prawie 4 mld rozmów telefonicznych na dobę, współczesne sieci szkieletowe mają przepustowość rzędu dziesiątek i setek gigabitów na sekundę. Magazynowanie takiej ilości ruchu wymaga pamięci masowych o ogromnych pojemnościach: żeby przechwycić cały ruch z sieci 10 Gbps potrzeba 105 terabajtów na każde 24 godziny. Analiza takich ilości danych w czasie rzeczywistym wymagałaby niewyobrażalnie wielkich zasobów sprzętowych. O ile stosunkowo prosto jest wdrożyć „podsłuch" (czy raczej obserwację)[20] danych przesyłanych przez konkretne urządzenie (na przykład telefon GSM), o tyle szczegółowe badanie całości ruchu w większych sieciach jest niemożliwe inaczej niż przez administrację państwową w krajach totalitarnych bądź autorytarnych, dysponującą ogromnymi środkami finansowymi i prawnymi[21].

Drugą grupą problemów dla wdrażania i rozwijania systemów opartych o analizę ruchu sieciowego są zagadnienia dotyczące prawnej strony akwizycji danych (można wymienić tu przepisy prawa, kwestie dotyczące poszanowania prywatności i tajemnicy korespondencji, zagadnienia związane z transgranicznością Internetu itd.).

Pewnym problemem jest również brak jednolitego standardu zbierania danych związanych z ruchem sieciowym. W zasadzie istnieją dwa sposoby reprezentacji danych: rodzina standardów netflow (z najnowszą wersją 9 i bazującym na niej standardem IP Flow Information Export, IPFIX) oraz pcap (packet capture) służący do przechowywania „surowych" danych odebranych przez interfejs sieciowy, niemniej konkretne rozwiązania sprzętowe i programowe korzystają czasami z innych formatów, co oczywiście utrudnia opracowanie jednolitych narzędzi czy prowadzenie testów porównawczych.

---

[18] W kontekście zarzadzania jakością i bezpieczeństwem konieczne jest przetwarzanie tych danych na bieżąco, w miarę ich napływania (ang. in real time) bądź z niewielkimi opóźnieniami (ang. near real-time).

[19] Więcej o ilości informacji we „wszechświecie cyfrowym" zob.: [6], [8], [12], [17].

[20] W odniesieniu do obserwacji, gromadzenia i analizy ruchu zleconej przez organy prowadzące postępowania przygotowawcze bądź sądowe używa się terminu lawful interception (zob. np. [1])

[21] tego rodzaju „kontrolę internetu", a w zasadzie kontrolę dostępu doń i rozpowszechniania w nim treści powadzą między innymi Chiny, Kazachstan i Iran, niemniej z uwagi na architekturę Internetu oraz dostępność współczesnych narzędzi szyfrujących nie jest to kontrola w pełni szczelna. Oczywiście w sieciach organizacji gospodarczych, prowadzona w etyczny sposób analiza przepływów sieciowych, prowadzona jest nie w celu inwigilacji pracowników (choć i takie przypadki się niestety zdarzają) ale w celu wykrycia zagrożeń, takich jak aktywność wirusów czy obecność koni trojańskich.

4. Podsumowanie

Usługi związane z transmisją danych w sieciach teleinformatycznych są oczywiście usługami z grupy „wysokich technologii", a więc zapewnienie odpowiedniego poziomu ich jakości i bezpieczeństwa wymaga zastosowania wyspecjalizowanych urządzeń i oprogramowania. Oprogramowanie to korzysta niejednokrotnie z zaawansowanych algorytmów, w tym z algorytmów opartych na modelach matematycznych powstałych pierwotnie do modelowania zupełnie innych zjawisk i dziedzin życia. W tym przypadku – inaczej niż w tradycyjnie rozumianej „informatyce i ekonometrii" to nie informatyka dostarcza narzędzi dla badania zjawisk ekonomicznych, ale ekonometria dostarcza narzędzi do badania systemów informatycznych.

Literatura

[1] European Council Resolution of 17 January 1995 on the lawful interception of telecommunications, EUR-Lex - 31996G1104 - EN .
[2] **Amoroso E.G.:** Cyber Attacks: Protecting National Infra-structure. Butterworth-Heinemann 2011.
[3] **ByungRae C.:** Host anomaly detection preformance analysis based on system call of Neuro-Fuzzy using Soundex algorithm and N-gram technique, Proceedings of the 2005 Systems Communications (ICW'05), IEEE 2005.
[4] **Callegari C., Gazzarrini L., Giordano S., Pagano M., Pepe T.:** A Novel Multi Time-Scales PCA-based Anomaly Detection System, [v:] IEEE International Symposium on Performance Evaluation of Computer and Telecommuni-cation Systems, Ottawa 2010, pp 1-5.
[5] **Dubendorfer T., Wagner A., Plattner B.:** A Framework for Real-Time Worm Attack Detection and Backbone Monitoring, Proceedings of the First IEEE International Workshop on Critical Infrastructure Protection IEEE Computer Society Washington, 2005.
[6] Digital Universe http://www.emc.com/leadership/programs/digital-universe.htm
[7] **Fry C., Nystrom M.:** Monitoring i bezpieczeństwo sieci, Helion O'Reilly, Gliwice 2010.
[8] IDC Whitepaper: The Diverse and Exploding Digital Universe. An Updated Forecast of Worldwide Information Growth Through 2011.
[9] ITU-T E.507 Models for Forecasting International Traffic.
[10] **Korzeniowski L.F.:** Podstawy nauk o bezpieczeństwie, Diffin, Warszawa 2012.
[11] Strona firmy KSplice poświęcona programowi Uptrack http://www.ksplice.com/
[12] **Lyman P., Varian H.R., Dunn J., Strygin A., Swearingen K.:** How Much Information 2000? University of Berkeley Raport, 2000.
[13] **Minarik P., Krmicek V., Vykopal J.:** Improving Host Profiling With Bidirectional Flows. In 2009 International Conference on Computational Science and Engineering. Vancouver, Canada : IEEE Computer Society, 2009, pp. 231-237.
[14] **Palmieri F., Fiore U.:** Network anomalny detection though nonlinear analysis, [w:] Computers and Security 29/2010 s. 737-755.

[15] **Russell R., Mullen T., FX, Kaminsky D., Grand J., Pfeil K., Durbrawsky I., Burnett M., Craig P.:** Stealing the Network: How to Own the Box, Syngres Publishing 2003.
[16] **Rybarczyk P.:** Podręcznik inżynierii Internetu, PLJ, Warszawa 1999.
[17] **Swearingen K. (ed.):** How Much Information 2003? University of Berkeley Raport, 2003.
[18] **Szmit M.:** Využití nula-jedničkových modelů pro behaviorální analýzu síťového provozu, [w:] Internet, competitiveness and organizational security, Tomas Bata University Zlín 2011, s. 266-299.
[19] **Szmit M., Szmit A.:** Use of Holt-Winters method in the analysis of network traffic. Case study, Springer Communications in Computer and Information Science vol. 160, 18th Conference Computer Networks, 2011, s. 224-231.
[20] **Szmit M., Szmit A.:** Usage of Modified Holt-Winters Method in the Anomaly Detection of Network Traffic: Case Studies, Journal of Computer Networks and Communications, vol. 2012.
[21] **Szmit M., Szmit A.:** Usage of Pseudo-estimator LAD and SARIMA Models for Network Traffic Prediction. Case Studies, Communications in Computer and Information Science, 2012, Volume 291, s. 229-236.
[22] **Szmit M., Szmit A., Adamus S., Bugała S.:** Usage of Holt-Winters Model and Multilayer Perceptron in Network Traffic Modelling and Anomaly Detection, Informatica Vol. 36, Nr 4, pp. 359-368.
[23] **Szmit M., Adamus S., Bugała S., Szmit A.:** Anomaly Detection 3.0 for Snort(R), [w:] SECURITATEA INFORMAŢIONALĂ 2012, pp. 37-41, Laboratorul de Securitate Informaţională al ASEM, Chişinău 2012.
[24] **Szmit M., Adamus S., Bugała S., Szmit A.:** Implementation of Brutlag's algorithm in Anomaly Detection 3.0, Proceedings of the Federated Conference on Computer Science and Information Systems, pp. 685-691, PTI, IEEE, Wrocław 2011.
[25] **Villén-Altamirano M.:** Overview of ITU Recommendations on Traffic Engineering, Paper presented in the ITU/ITC workshop within 17th ITC.
[26] **Pieprzyk J., Hardjono T., Seberry J.:** Teoria bezpieczeństwa systemów komputerowych, Helion, 2005.

ABOUT USAGE OF ECONOMETRIC MODELS IN NETWORK TRAFFIC PREDICTION

Summary

Acquisition, analysis, modeling, forecasting and simulation of network traffic are activities carried in communication networks, both for the quality management and the stress testing, as well as in information security management. The prediction of network traffic uses among others statistical models, econometric time series models and methods included in the artificial intelligence. The article presents a brief overview of forecasting methods used in the methods of Network Behavioral Anomaly Detection according to the recommendations of the International Telecommunication Union.