rynku może odbywać się w sposób ciągły, sekwencyjny lub iteracyjny, a poszczególne funkcje systemu mogą działać w architekturze scentralizowanej lub rozproszonej (w szczególności cały system może być scentralizowany lub rozproszony). Na kształt architektury fizycznej systemu mają także wpływ wymagania dotyczące wydajności i niezawodności systemu, decydujące o potrzebie redundancji i zwielokrotnienia jego elementów. Różnorodność możliwych modeli handlowych wymaga zachowania dużej otwartości i elastyczności przyjętego modelu informacyjnego. Ten cel osiągnięto przez zastosowanie opartego na notacji **XML** języka modelowania **M³** (*Multicommodity Market Model*) [4]. Jest on zbiorem formalnych modeli opisujących dane i wymianę komunikatów na potrzeby wielotowarowych rynków infrastrukturalnych.

W pracach nad planowaną architekturą systemu uwzględniono zalecenia dotyczące budowy systemów **NGOSS** (*Next Generation Operation Support Systems*) opracowane przez TMForum, stanowiące model odniesienia dla systemów wspomagających różnego rodzaju operacje biznesowe w firmach z branży telekomunikacyjnej.

* * *

Prowadzone badania są odpowiedzią na istotne zmiany rynku telekomunikacyjnego, mające źródło w procesach liberalizacji. Podkreślają one wagę mechanizmów rynkowych w zarządzaniu zasobami sieci. Opracowywane w Zakładzie Teleinformatyki i Telekomutacji Instytutu Telekomunikacji modele oraz ich aplikacje wykorzystują techniki i narzędzia z pogranicza teorii gier, ekonomii i optymalizacji. Interdyscyplinarny charakter badań umożliwia uwzględnienie najnowszych trendów pojawiających się w tej dziedzinie. Wśród zaplanowanych celów badawczych znajduje się opracowanie modeli handlowych przeznaczonych dla konkretnych typów zasobów sieci oraz zaproponowanie koncepcji budowy rzeczywistego systemu informacyjnego wspierającego wymianę handlową na rynku zasobów sieci.

LITERATURA

[1] Stańczuk W., Lubacz J., Toczyłowski E.: *Giełdy przepustowości na rynku zasobów transportowych sieci telekomunikacyjnych*. Przegląd Telekomunikacyjny i Wiadomości Telekomunikacyjne, 8 – 9, 2007

[2] Stańczuk W., Lubacz J., Toczyłowski E.: *Trading links and paths on a communication bandwidth markets.* Journal of Universal Computer Science, 14(5), 2008

[3] Stańczuk W., Lubacz J.: *A Market Mechanism for Routing and Wavelength Assignment in WDM Optical Networks*, Proceedings of 16th Polish Teletraffic Symposium, Łódź, 2009

[4] *M³ – Multicommodity Market data Model*. http://www.openm3.org/

[5] Projekt badawczy zamawiany na lata 2008 – 2010 – *Usługi teleinformatyczne następnej generacji – aspekty techniczne, aplikacyjne i rynkowe.* https://pbz.itl.waw.p

Zbigniew KOTULSKI, Łukasz KUCHARZEWSKI*, Igor MARGASIŃSKI**

Bezpieczeństwo w sieciach telekomunikacyjnych

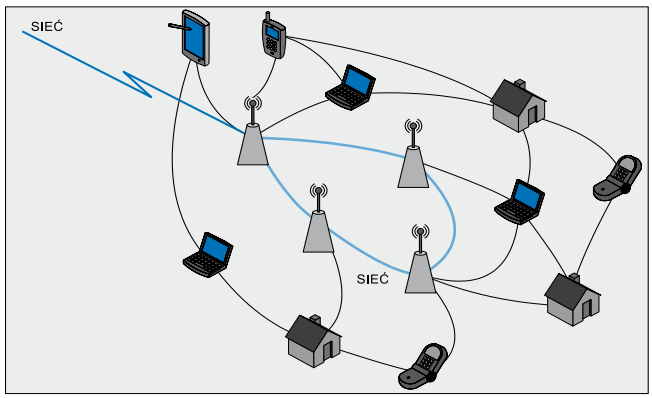
BEZPIECZEŃSTWO I PRYWATNOŚĆ W SIECI INTERNET

Bezpieczeństwo oraz prywatność będą odgrywały zasadniczą rolę w tworzonym na naszych oczach Internecie przyszłości. Popularyzacja wielu zastosowań sieci Internet, takich jak handel elektroniczny, platformy społecznościowe, wybory przez Internet i innych, jest wciąż ograniczona ze względu, obawy dotyczące bezpieczeństwa. W znacznej mierze odnoszą się one do zagrożeń związanych z utratą prywatności oraz dotyczą braku zaufania do innych uczestników komunikacji sieciowej. Internet, stając się we wszystkich wymiarach systemem rozproszonym, będzie rozwijał się w kierunku jeszcze bliższej interakcji z użytkownikami w zakresie wzrastającej liczby nowych, wirtualnie wydzielonych usług, jak również w odniesieniu do zadań o zakresie globalnym. Tzw. aplikacje brzegowe (*edge-based applications*) oraz aplikacje oparte na treściach udostępnianych bezpośrednio przez użytkowników (*user-contributed content applications*) dominują już dziś i potwierdzają, że zjawisko decentralizacji staje się podstawowym trendem w rozwoju Internetu. W przyszłości to użytkownik będzie znajdował się w centrum tworzenia nowych usług, a jego bezpieczna identyfikacja oraz ochrona prywatnych danych będzie decydować o sukcesie wdrożenia nowych funkcji sieciowych.

W badaniach prowadzonych przez Zakład Teleinformatyki i telekomunikacji (ZTiT) w znacznym zakresie prace poświęcono rozwojowi technik prywatności sieciowej. Szczególną uwagę zwrócono na praktyczne aspekty wdrożenia i użytkowania sieci zapewniających prywatność, ze szczególnym uwzględnieniem ich wydajności ruchowej oraz odporności na zmiany w sieciach dużej skali. Wyniki tych badań są obiecujące i pokazują, że możliwa jest budowa sieci anonimowych, konkurujących w dziedzinie szybkości działania z obecnymi rozwiązaniami. Aktualnie stosowane techniki ochrony prywatności, budowane na podstawie koncepcji Mix-net, Onion Routing i TOR, a także Mix-ring, kształtują ruch anonimowy w trudne do śledzenia ścieżki lub pierścienie wielu węzłów pośredniczących. W dziedzinie anonimowości zjawisko zbiorowości jest szczególnie istotne do realizacji skutecznych mechanizmów ochrony prywatności, a transport anonimowego ruchu za pośrednictwem ścieżek złożonych z wielu węzłów pośredniczących wpływa korzystnie na poziom anonimowości. Jednak te szeroko stosowane techniki ukrywania powiązań pomiędzy uczestnikami ruchu telekomunikacyjnego stanowią źródło duzych opóźnień w transporcie danych.

Wirtualizacja Internetu oraz praktyczne możliwości,umożliwiające dziś realizację heterogenicznych sieci nakładkowych o ogólnoświatowym zasięgu, zachęcają do opracowywania nowych architektur sieciowych dostosowanych do konkretnych potrzeb i usług sieciowych. Do takich nowych koncepcji należy **P2Priv** (*peer-to-peer direct and anonymous distribution overlay*) [2,3]. Sieć P2Priv jest obecnie przedmiotem wniosku patentowego na rzecz Politechniki Warszawskiej. P2Priv rozdziela zadania anonimizacji sieciowej od transportu danych użytkowych. Artykuł prezentujący tę koncepcję został bardzo dobrze przyjęty w międzynarodowym środowisku naukowym oraz został umieszczony w czołowej międzynarodowej liście bibliograficznej z dziedziny anonimowości (*FreeHaven.net/anonbib*). W odniesieniu do transportu danych sieć P2Priv angażuje taką samą liczbę wirtualnych łączy nadmiarowych jak w przypadku klasycznych sieci anonimowych. Jednakże architektura P2Priv umożliwia organizowanie anonimowych łączy w sposób równoległy, a nie jak w sieciach klasycznych kaskadowo. Sieć P2Priv nie wymaga przesyłu

*** Instytut Telekomunikacji, Wydział Elektroniki i Technik Informacyjnych Politechniki Warszawskiej,**
e-mail: kotulsk@tele.pw.edu.pl, igor@tele.pw.edu.pl



Rys. 1. Bezprzewodowe sieci typu mesh wg standardu 802.11 i 802.16

danych przez kaskadę węzłów pośredniczących. Dzięki temu, szybkość przesyłu danych z zapewnieniem usługi prywatności w sieci P2Priv jest kilkakrotnie wyższa, niż w klasycznych anonimowych sieciach małych opóźnień. Przedstawione techniki są dalej rozwijane. Sieć P2Priv jest przeznaczona do anonimizacji wymiany danych dużej objętości w architekturze *peer-to-peer*. W uzupełnieniu do tak zdefiniowanego celu, w ubiegłym roku, na forum Identity and Privacy in the Internet Age, NordSec 2009, została przedstawiona architektura sieci zapewniającej prywatność w komunikacji ogólnego przeznaczenia. Nowe rozwiązanie (**NetPriv** – *Network Privacy Preserving Parallel Topology*), przenosząc czasochłonne techniki anonimizacji sieciowej do warstwy sygnalizacyjnej, łączy ogólną zasadę zrównoleglenia transportu P2Priv ze specyficznymi funkcjami sieciowych serwerów pośredniczących (*proxy*), a także z innymi podrozwiązaniami [1]. Celem tej nowej architektury hybrydowej jest zarządzanie anonimowością z uwzględnieniem zarówno dostępu do sieciowych usług rozproszonych jak i usług scentralizowanych realizowanych w architekturze klient-serwer (np. **WWW**). W szczególności badania te koncentrują się na opracowaniu platformy anonimizującej dla tych aplikacji sieciowych, w których są wymagane zarówno prywatność, jak i niskie opóźnienia transmisji.

Nowe techniki są obecnie przedmiotem analiz, testów praktycznych oraz integracji z innymi nowatorskimi rozwiązaniami sieciowymi, m.in. z zakresu rutingu. Została nawiązana współpraca międzynarodowa, a także współpraca krajowych ośrodków naukowo-badawczych w ramach rozwoju sieci eksperymentalnych (*testbeds*), umożliwiających badania nowatorskich rozwiązań „na żywym organizmie". Współtworzy sie sieć testową **GpENI** (*Great Plains Environment for Network Innovation*), obejmującą ośrodki naukowe w Stanach Zjednoczonych i Europie oraz krajową sieć eksperymentalną w ramach projektu *inżynieria Internetu przyszłości*, w programie *Innowacyjna Gospodarka.*

BEZPIECZEŃSTWO W HETEROGENICZNYCH SIECIACH BEZPRZEWODOWYCH ORAZ SIECIACH SENSORYCZNYCH

Jednym z obszarów badań prowadzonych w zakresie bezpieczeństwa w Zakładzie Teleinformatyki i Telekomutacji są heterogeniczne sieci bezprzewodowe. Sieci takie, w których nośnikiem sygnału są fale radiowe, funkcjonują w wyniku współdziałania jednego z wielu dostępnych standardów transmisji (np. 802.11, 802.16, **GSM, UMTS, LTE, Bluetooth, ZigBee**). Różnią się między sobą częstotliwością pasma, technikami modulacji oraz zaimplementowanymi protokołami bezpieczeństwa.

Poszczególne urządzenia klienckie (802.11, 802.16) mogą stanowić sieć powiązanych ze sobą węzłów, tworząc sieć kratową (*Wireless Mesh Network*). Każdy węzeł może komunikować się z innym węzłem w sposób bezpośredni lub przez sąsiadujące z nim węzły pośredniczące. Model taki możemy zobrazować jako *mesh cloud* do wymiany informacji, w której są realizowane zaawansowane metody rutingu, zarządzania pasmem, wydajnością oraz jakości transmisji danych.

Aspekt bezpieczeństwa w takich sieciach jest bardzo istotny z punktu widzenia prowadzonych w ZTiT badań. Przy przyjętych ograniczeniach, związanych z zapewnieniem funkcjonalności sieci, są stosowane odpowiednie mechanizmy, gwarantujące poufność transmisji, autentyczność pakietów (np. [4]), wzajemne uwierzytelnienie urządzeń klienckich i realizujące protokoły dostarczania tajnych kluczy, a także zapewniające niezbędną prywatność i anonimowość użytkowników sieci. W ramach prac realizowanych w Zakładzie projektowane są nowe protokoły wymiany kluczy oraz analizowane różne scenariusze dostępu do sieci. Nowym standardem, który będzie bezpośrednio dotyczył bezprzewodowych sieci kratowych, jest 802.11s. Definiuje on działanie takiej sieci oraz zapewnia prawidłową komunikację z innymi sieciami standardu 802.11. Podsystem bezpieczeństwa uwzględnia jednocześnie wszystkie sprawdzone rozwiązania oraz modyfikacje w toku ewolucji standardu 802.11.

Równoległym tematem, badań w Zakładzie są bezprzewodowe sieci sensoryczne. Sieć taka składa się z grupy autonomicznych urządzeń sensorycznych, które realizują funkcje komunikacyjne, pomiarowe i wstępnego przetwarzania danych. Komunikacja pomiędzy sensorami wyposażonymi w mikrokontroler, pamięć, własne zasilanie również odbywa się za pomocą fal radiowych. Rosnąca liczba ataków na ten rodzaj sieci wymaga wprowadzenia restrykcyjnej polityki bezpieczeństwa. Prawidłowe działanie sieci sensorycznej może być zakłócone przez zagłuszanie transmisji w sieci, wstrzykiwanie do niej zainfekowanych danych oraz ataki na metody trasowania. Podsłuchiwanie, powtarzanie podsłuchanych pakietów czy dokonywanie modyfikacji wykonywanych pomiarów to również elementy zagrożeń dla sieci sensoryczne.

Mając na uwadze powyższe rozważania, w Zakładzie prowadzi się badania ukierunkowane przede wszystkim na problem bezpieczeństwa w takich sieciach, wykorzystując przy tym matematyczne aspekty kryptologii (por. [5]).

Oprócz zagadnień bezpieczeństwa sieci, są prowadzone również prace w zakresie kryptografii. Ich efektem jest na przykład zgłoszenie (jedyne z Polski) projektu kryptograficznej funkcji skrótu *StreamHash* (autorstwa mgr. Michała Trojnary) na konkurs SHA-3. Funkcja ta nie przeszła wprawdzie poza pierwszy etap konkursu, jednak trwają prace nad jej rozwojem i badaniem jej bezpieczeństwa. Prowadzone są też prace nad innymi algorytmami kryptograficznymi, np. nad konstrukcją nowych szyfrów wykorzystujących chaos do zabezpieczania obrazów cyfrowych [6]. Opracowywane są też nowe metody wyszukiwania krytycznych luk w oprogramowaniu, zagrażających jego bezpieczeństwu, umożliwiających realizowanie ukrytych funkcji lub przesyłanie ukrytych komunikatów. Prace te są przedmiotem przygotowywanych rozpraw doktorskich.

LITERATURA

[1] Margasinski I.: *A parallelism-based approach to network anonymization*. In: A. Josang, T. Maseng and S.J. Knapskog (Eds.): Identity and Privacy in the Internet Age, Springer LNCS 5838 (2009)

[2] Margasinski I., Pioro M.: *A concept of an anonymous direct p2p distribution over-lay system*. In: Proceedings of IEEE 22nd International Conference on Advanced Information Networking and Applications (AINA), pp. 590–597. IEEE Computer Society Press, Ginowan, Okinawa, Japan 2008

[3] Margasinski I., Pioro M.: *Low-latency parallel transport in anonymous peer-to-peer overlays*. In: Akar, et al. (eds.), IP Operations and Management 2008, Springer LNCS 5275 2008

[4] Ksiezopolski B., Kotulski Z., Szalachowski P.: *Adaptive Approach to Network Security*, in: A. Kwiecień, P. Gaj, and P. Stera (Eds.): CN 2009, Communications in Computer and Information Science 39, Springer, Berlin 2009

[5] Szalachowski P., Ksiezopolski B., Kotulski Z.: *CMAC, CCM and GCM/GMAC: Advanced modes of operation of symmetric block ciphers in wireless sensor networks,* Information Processing Letters, doi:10.1016/j.ipl.2010.01.004

[6] Jastrzębski K., Kotulski Z.: *On improved image encryption scheme based on chaotic map lattices*, Engineering Transactions, 57 (2) 2009. ISSN 0867-888X.