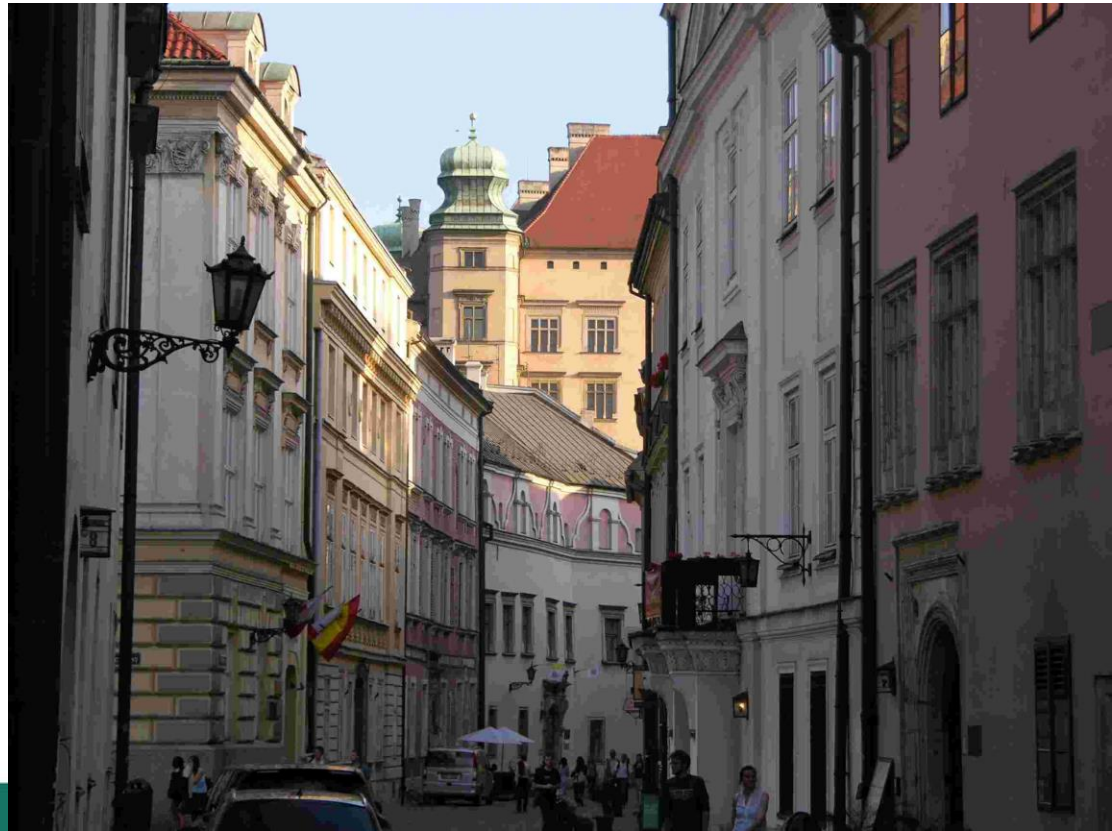
AKADEMIA GÓRNICZO HUTNICZA
IM. S. STASZICA W KRAKOWIE

Prace naukowe prowadzone w Katedrze Telekomunikacji AGH



Wrzesień 2015

Al. Mickiewicza 30, 30-059 Kraków
Tel. +48 12 6345582
Fax +48 12 6342372
E-mail: kt@agh.edu.pl

Plan

- Akademia Górniczo-Hutnicza
- Katedra Telekomunikacji — podstawowe dane
- Katedra Telekomunikacji — obszary badawcze
- Działalność standaryzacyjna
- Wcześniejsze doświadczenia — wybrane projekty europejskie
- Dydaktyka
- Zakończenie

Akademia Górniczo-Hutnicza

- Data otwarcia: 1919
- Liczba studentów (2014): ~ 35 000
- Liczba pracowników (2014): ~ 4 200

Akademia Górniczo-Hutnicza (2)

Tematyka badawcza w AGH

- Techniki informacyjne
- Środowisko i zmiany klimatu
- Górnictwo
- Nauki ścisłe i nauki o ziemi
- Nowe materiały i technologie
- Energia i jej źródła
- Inżynieria elektryczna i mechaniczna
- Nauki społeczno-ekonomiczne i humanistyczne

Katedra Telekomunikacji

Pracownicy

- 5 profesorów tytularnych
- 50 pracowników naukowo-dydaktycznych
- 25 doktorantów
- 120 studentów II stopnia rocznie

Katedra Telekomunikacji
Obszary badawcze

- **Bezpieczeństwo i niezawodność**
  - Bezpieczeństwo i ochrona danych
  - Zarządzanie bezpieczeństwem w systemach 4G
  - Niezawodność sieci i ich odporność na uszkodzenia
  - Sieci odporne na uszkodzenia z uwzględnieniem zagadnień ryzyka
  - Ochrona infrastruktur krytycznych
  - Znaki wodne
- **Inteligentne monitorowanie i wymiana informacji związana z bezpieczeństwem obywateli**

Katedra Telekomunikacji
Obszary badawcze (2)

- **Usługi społeczeństwa informacyjnego**
  - Systemy i aplikacje multimedialne
  - Postrzegana jakość obsługi (QoE)
  - Rozwiązania telemedyczne
  - Informatyczne wsparcie diagnostyki i terapii medycznych
- **Architektury i projektowanie sieci**
  - Sieci zorientowane na przepływy
  - Sieci nakładkowe
  - Sieci przyjazne środowisku
  - Dynamiczne zarządzanie ruchem
  - Sieci bezprzewodowe

Bezpieczeństwo i ochrona danych

Obszary zainteresowań:

- Kryptografia (szyfratory, funkcje mieszające, kryptografia kwantowa)
- Ochrona w systemach SCADA (wykrywanie zagrożeń, monitorowanie)
- Weryfikacja bezpieczeństwa (ocena ryzyka, testy penetracyjne)
- Detekcja szkodliwego oprogramowania (podejście heurystyczne)
- Zapewnianie bezpieczeństwa przeciw atakom wewnętrznym w sieciach Wi-Fi

SCADA (*Supervisory Control and Data Acquisition*)

Bezpieczeństwo i ochrona danych (2)

Kryptografia

- Nowe algorytmy kryptograficzne (np. szyfr IBC — struktura algorytmu zależna od klucza)
- Implementacje programowe i sprzętowe
- Środowisko OpenSSL (integracja nowych szyfrów i trybów szyfrowania danych)
- Weryfikacja algorytmów kryptograficznych (nieliniowość, lawinowość, dyfuzyjność, itd.)

Kryptografia kwantowa

- Symulator protokołów kryptografii kwantowej — weryfikacja i ewaluacja protokołów
- Sterowanie bezpieczeństwem i wydajnością kwantowej dystrybucji kluczy kryptograficznych

Bezpieczeństwo i ochrona danych(3)

- UE Horizon 2020 project **SCISSOR** no. 644425 "Security In trusted SCADA and smart-grids"
- Udział AGH
  - Mechanizmy pozyskiwania i transmisji danych wizyjnych z wielu kamer różnych typów (CCTV, podczerwień)
  - Automatyczne rozpoznawanie obiektów, ich charakterystyk i pozycji
  - System analizy zdarzeń — opracowanie wymagań i metod analizy danych oraz podejmowania decyzji z uwzględnieniem integracji informacji pochodzącej z wielu źródeł
  - Ochrona prywatności przetwarzanych i przesyłanych danych cyfrowych z użyciem cyfrowych znaków wodnych
  - System analizy zdarzeń — integracja algorytmów; implementacja i ewaluacja modułu generowania danych do wizualizacji i podejmowania decyzji
  - Zintegrowany system przetwarzania i przechowywania danych

Bezpieczeństwo i ochrona danych(4)

Wybrane publikacje:

- M. Niemiec, A. Pach, „Management of security in quantum cryptography”, *IEEE Communications Magazine*, vol. 51, no. 8, 2013
- M. Niemiec, P. Machnik, „Authentication in virtual private networks based on quantum key distribution methods”, *Multimedia Tools and Applications*, 2014
- T. Kurek , M. Niemiec, A. Lason, „Taking back control of privacy: a novel framework for preserving cloud-based firewall policy confidentiality”, *International Journal of Information Security*, 2015

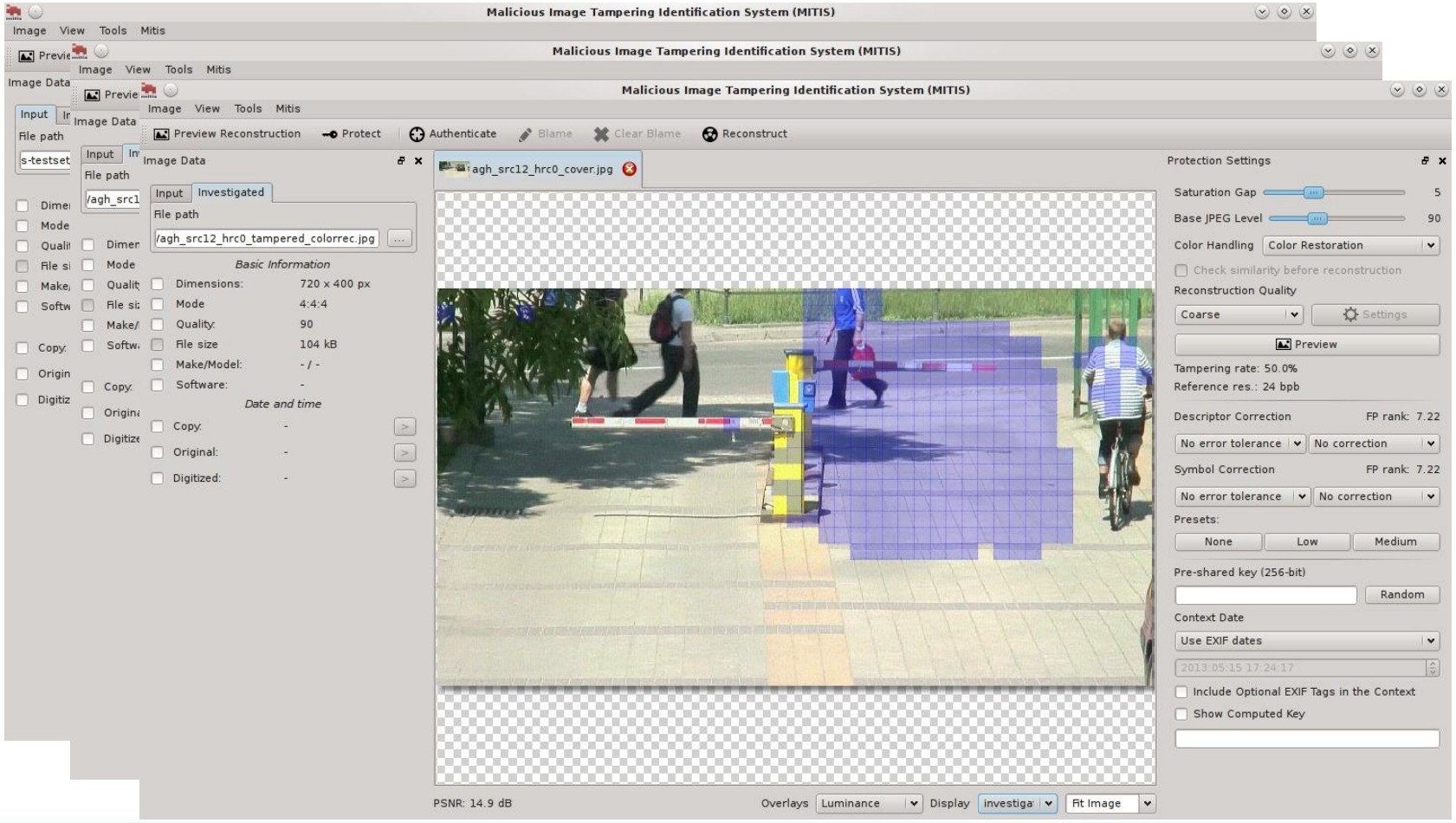
Cyfrowe znaki wodne w ochronie prywatności i danych

Ochrona prywatności

- Ochrona wrażliwych części obrazu
- Ochrona przed manipulacją (sprawdzanie oryginalności)
- Monitorowanie dostępu

Cyfrowe znaki wodne w ochronie prywatności i danych (2)

MITIS: Malicious Image Tampering Identification System



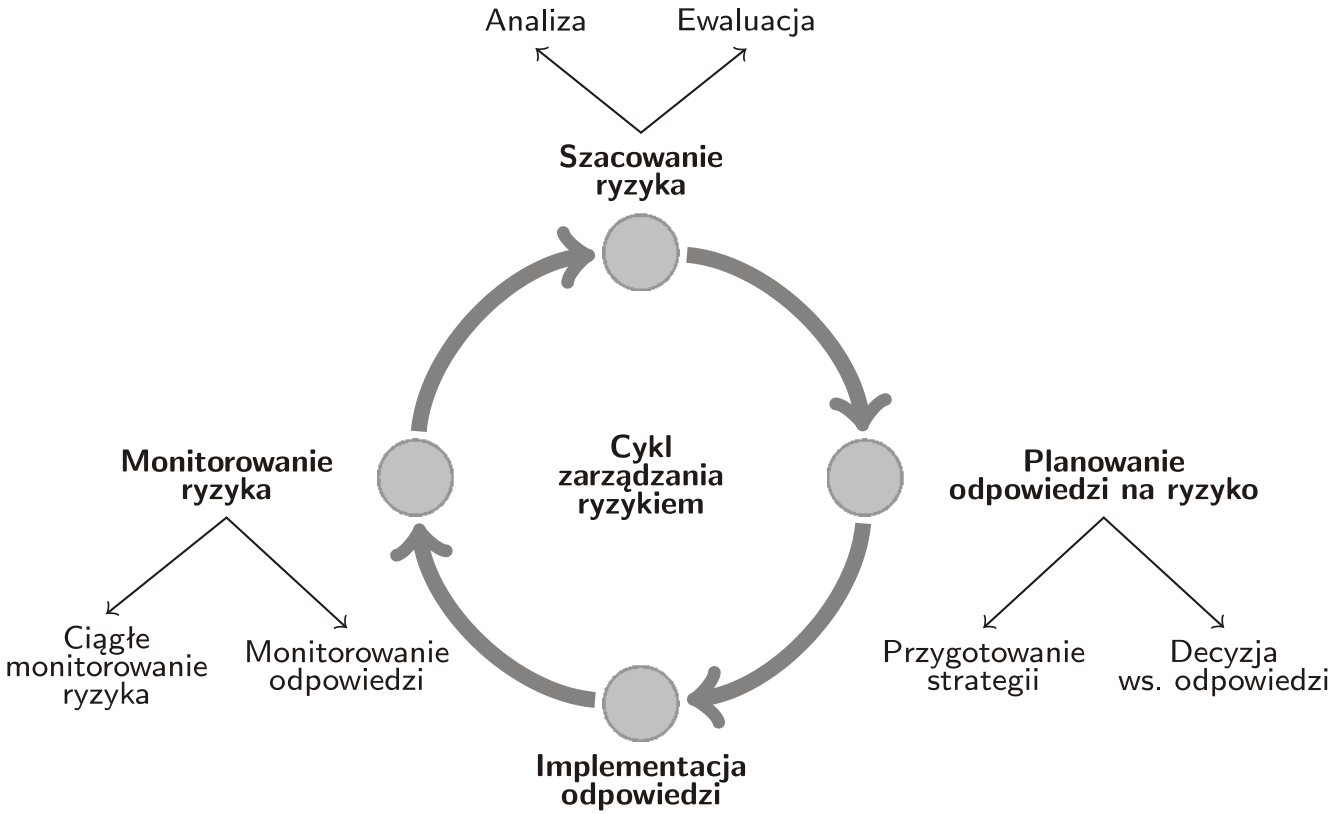
Cyfrowe znaki wodne w ochronie prywatności i danych (3)

Wybrane publikacje:

- P. Korus, J. Białas, A. Dziech, „Towards Practical Self-Embedding for JPEG-compressed Digital Images, *IEEE Transactions on Multimedia*, vol. 17, no. 2, 2015
- P. Korus, A. Dziech, „Adaptive Self-Embedding Scheme with Controlled Reconstruction Performance," *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 2, 2014
- P. Korus, A. Dziech, „Efficient Method for Content Reconstruction with Self-Embedding," *IEEE Transactions on Image Processing*, vol. 22, no. 3, 2013

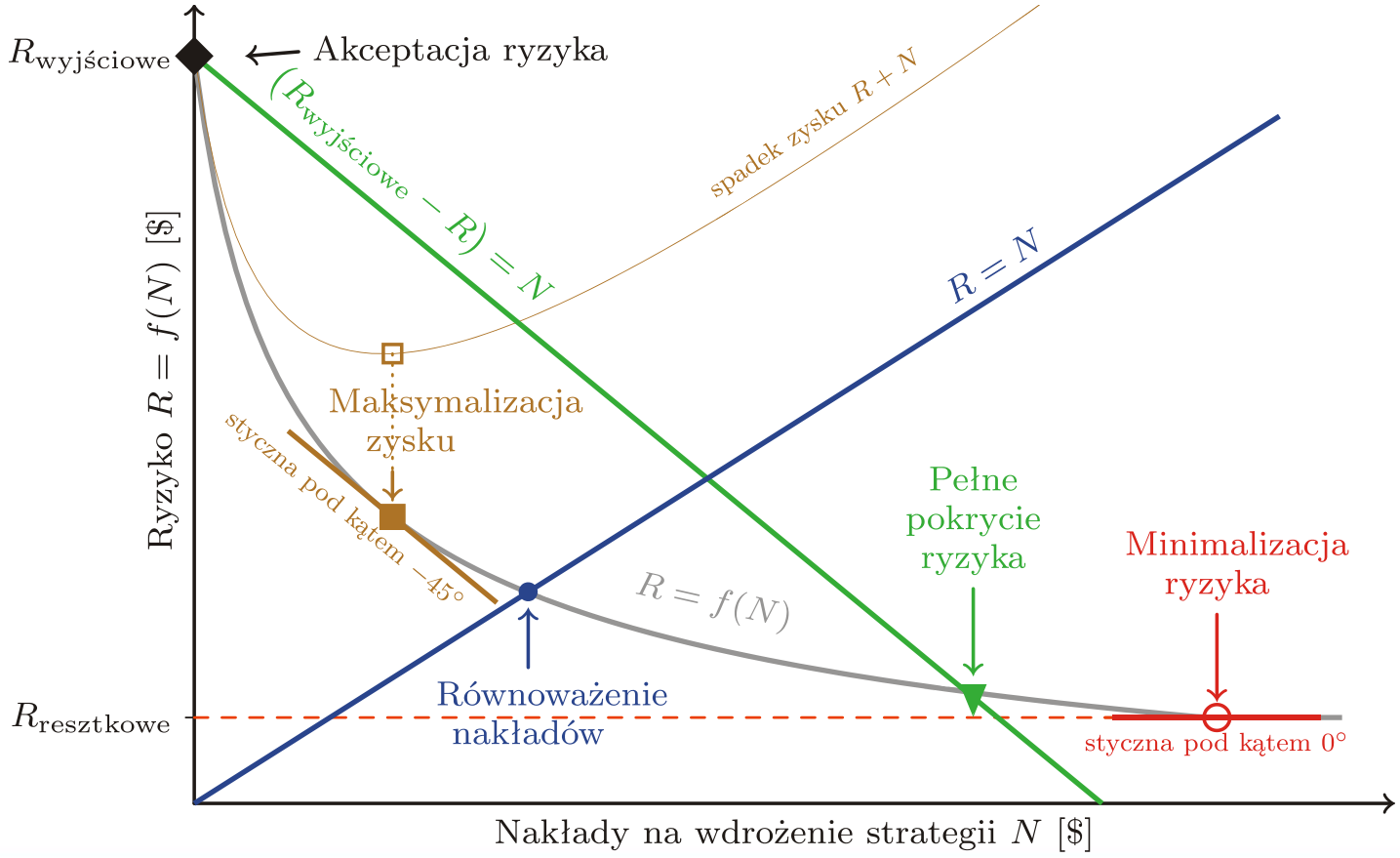
Projektowanie sieci odpornych na uszkodzenia z uwzględnieniem ryzyka

- Przystosowanie cyklu zarządzania ryzykiem do potrzeb projektowania sieci odpornych na uszkodzenia



Projektowanie sieci odpornych na uszkodzenia z uwzględnieniem ryzyka (2)

- Odpowiedź na ryzyko oparta na zorientowanych biznesowo strategiach ich minimalizowania



Projektowanie sieci odpornych na uszkodzenia z uwzględnieniem ryzyka (3)

- Analiza ryzyka w sieciach odpornych na uszkodzenia — modelowanie z metrykami zorientowanymi biznesowo
- Zastosowania w sieciach efektywnych energetycznie

Wybrane publikacje:

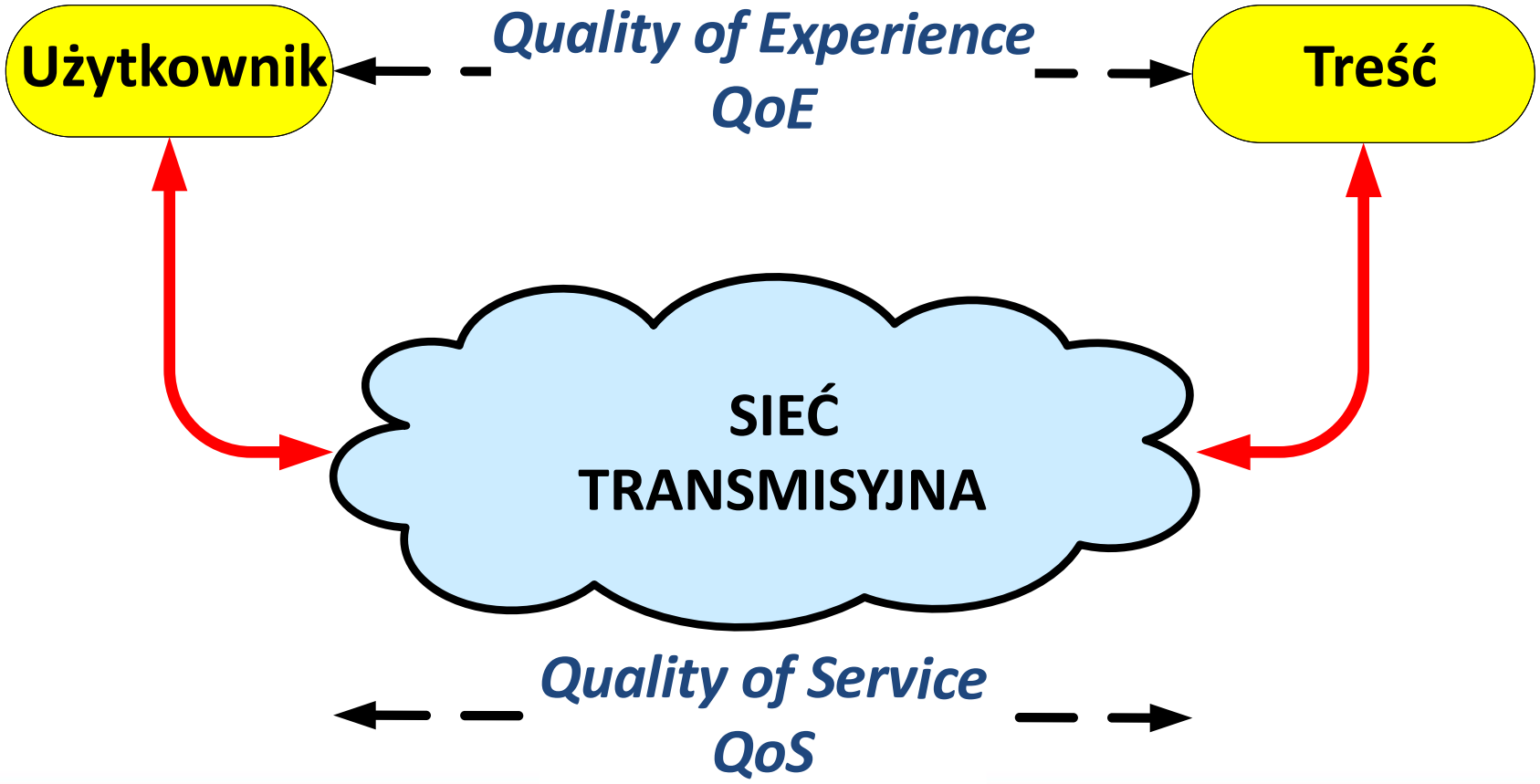
- P. Chołda, P. Jaglarz, „Energy-efficiency versus resilience: risk awareness view on dimensioning of optical networks with a sleep mode," *Photonic Network Communications*, March 2015
- P. Chołda, P. Jaglarz, „Optimization/simulation-based risk mitigation in resilient green communication networks," *Journal of Network and Computer Applications* (w druku)
- P. Chołda, E. L. Følstad, B. E. Helvik, P. Kuusela, M. Naldi, I. Norros, „Towards risk-aware communications networking," *Reliability Engineering and System Safety*, vol. 109, 2013
- A. Kamisiński, P. Chołda, A. Jajszczyk, „Assessing the structural complexity of computer and communication networks," *ACM Computing Surveys*, vol. 47 no. 4, 2015

Inteligentne monitorowanie i wymiana informacji związana z bezpieczeństwem obywateli

- Wykrywanie niebezpiecznych obiektów i sytuacji

Ocena QoE (*Quality of Experience*)

$$QoE = f(QoS;\ użytkownik,\ treść)$$



Ocena QoE (2)

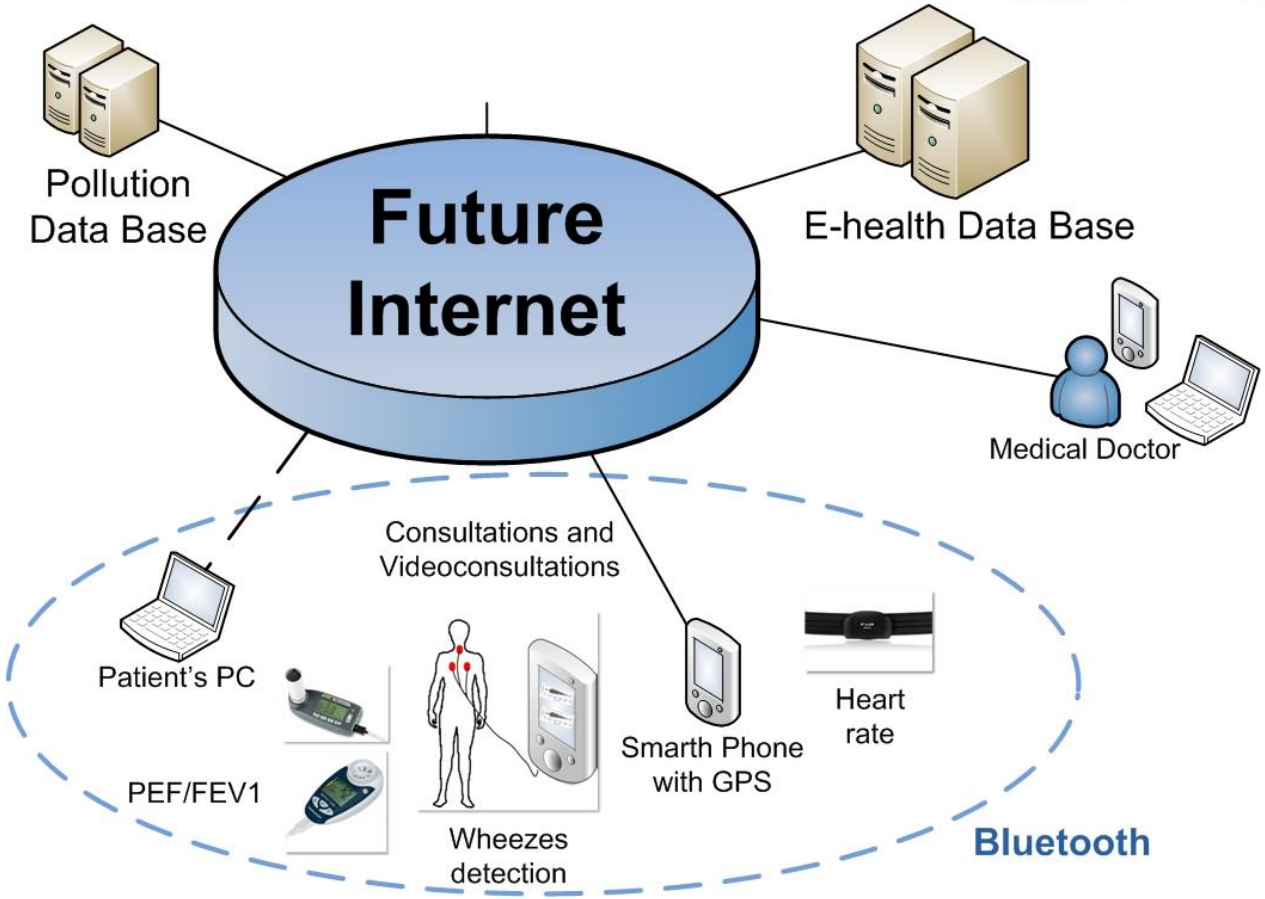
- Analiza QoE aplikacji wizyjnych z obiektywnego i subiektywnego punktu widzenia. Uzyskane wyniki obejmują obiektywne metryki jakości sygnałów wizyjnych uwzględniające różne rodzaje zniekształceń związanych z pozyskiwaniem, kodowaniem, transmisją i wyświetlaniem zawartości wizyjnej (HD, 3D)
- Wiele lat doświadczeń z prowadzeniem eksperymentów z oceną subiektywną
- Uznanie za: *Independent Laboratory of Video Quality Expert Group*

Ocena QoE (3)

Wybrane publikacje:

- M. H. Pinson, L. Janowski, Z. Papir, „Video quality assessment: subjective testing of entertainment scenes," *IEEE Signal Processing Magazine*, vol. 32 no. 1, 2015
- M. Leszczuk, K. Kowalczyk, L. Janowski, Z. Papir, „Lightweight implementation of No-Reference (NR) perceptual quality assessment of H.264/AVC compression," *Signal Processing: Image Communication*; in print 2015
- M. Leszczuk, „Optimising task-based video quality: a journey from subjective psychophysical experiments to objective quality optimisation," *Multimedia Tools and Applications*, vol. 68, 2014

Telemedycyna — Monitorowanie astmy



- M. Wiśniewski, T. P. Zieliński, „Joint Application of Audio Spectral Envelope and Tonality Index in an E-Asthma Monitoring System,” *IEEE J. of Biomedical and Health Informatics*, vol. 19, no. 3, 2015

Sieci zorientowane na przepływy (FAN)

- FAN: Architektura QoS zaproponowana w 2004
  - Ruch tworzony przez przepływy
  - Przepływy klasyfikowane pośrednio na dwie klasy ruchu

Porównanie z IntServ:

- Brak sygnalizacji
- Brak oznaczania pakietów
- Brak rezerwacji ścieżki

Porównanie z DiffServ:

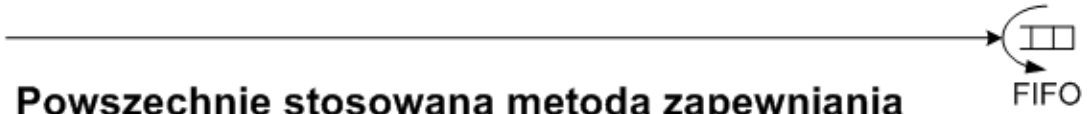
- Brak kontraktów ruchowych
- Brak oznaczania pakietów
- Tylko dwie klasy ruchu

Publikacja:

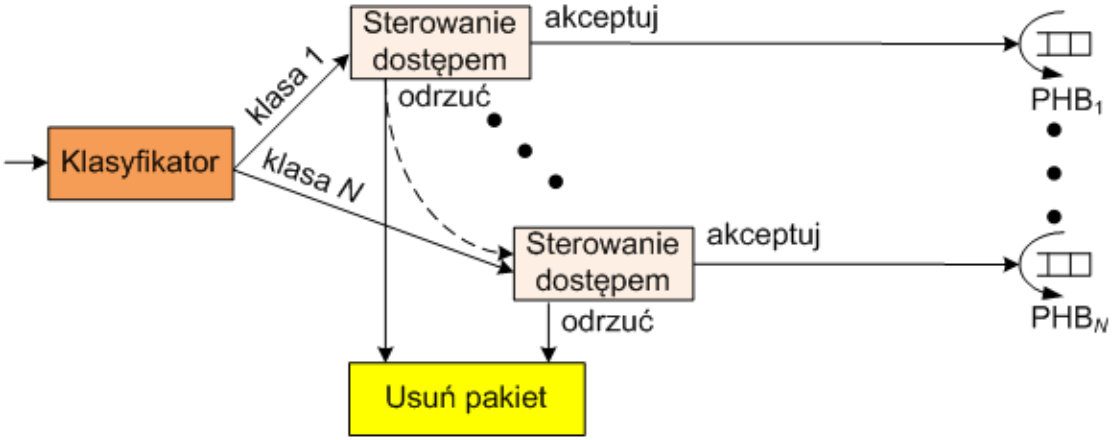
- R. Wójcik, A. Jajszczyk, "Flow oriented approaches to QoS assurance," *ACM Computing Surveys*, vol. 44, no. 1, 2012

Sieci zorientowane na przepływy (2)

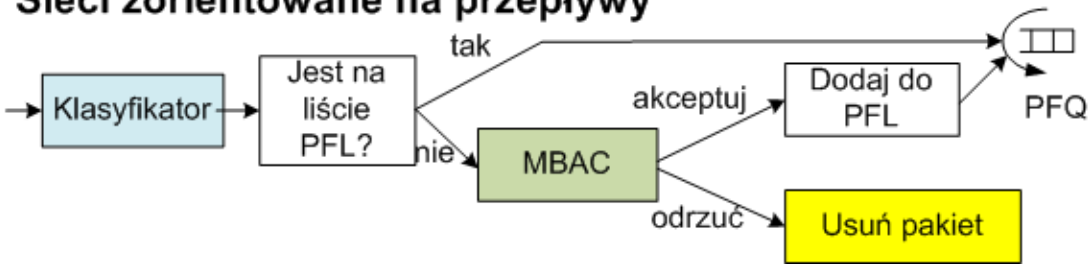
Best effort



Powszechnie stosowana metoda zapewniania gwarancji jakości obsługi



Sieci zorientowane na przepływy



Sieci zorientowane na przepływy (3)

Projekt: „ Niezawodna transmisja o wysokiej jakości w wielowarstwowych sieciach optycznych z zastosowaniem koncepcji Flow-Aware Networking”; finansowanie: NCN

Wyniki:

- Flow-Aware Multi-Topology Adaptive Routing
- Autonomic Hidden Bypasses

Publikacje:

- J. Domżał *et al*., „A survey on methods to provide multipath transmission in wired packet networks,” *Computer Networks*, vol. 77 , Feb. 2015
- J. Domżał, R. Wójcik, V. Lopez, J. Aracil, A. Jajszczyk, „EFMP– a new congestion control mechanism for flow-aware networks,” *Transactions on Emerging Telecommunications Technologies*, vol. 25, no. 11, Nov. 2014

Sieci zorientowane na przepływy (4)

Projekt: „ Zorientowany na przepływy adaptacyjny ruting oparty na wielu topologiach”; finansowanie: NCBR

Wyniki:

- Mechanizm rozwiązujący problem pętli pojawiających się po wystąpieniu awarii w sieciach z mechanizmem FAMTAR
- Implementacja rutera realizującego koncepcję FAMTAR

Publikacje:

- R. Wójcik, J. Domżał, Z. Duliński, P. Gawłowicz, „Loop resolution mechanism for Flow-Aware Multi-Topology Adaptive Routing,” *IEEE Communications Letters*, vol. PP, no. 99, June 2015
- R. Wójcik, J. Domżał, Z. Duliński, „Flow-aware multi-topology adaptive routing,” *IEEE Communications Letters*, vol. 18, no. 9, July 2014

Dynamiczne zarządzanie ruchem (DTM)

- Zawartość nie jest dostępna lokalnie
- Koszt ruchu „w dół” zależy od taryfy używanej w łączu międzydomenowym
- Część ruchu nakładkowego c (np. ruchu między centrami danych) jest zarządzalna: ISP może go rozpoznać i wybrać ścieżkę międzydomenową
- Optymalizacja całkowitego kosztu ruchu międzydomenowego (przez wpływanie na rozdział ruchu międzydomenowego między dwa lub więcej łączy o różniących się kosztach)
- DTM zawiera:
  - Algorytm optymalizacji
  - Procedurę kompensacji
  - Składnik pomiarowy

Dynamiczne zarządzanie ruchem (2)

Zaangażowanie AGH w projekt SmartenIT (*Socially-aware Management of New Overlay Application Traffic combined with Energy Efficiency in the Internet*), FP7

- Definiowanie scenariuszy i przypadków użycia
- Projektowanie i specyfikacja mechanizmu DTM
- Przygotowanie ram symulacji DTM
- Implementacja wybranych modułów systemu oraz jego integracja
- Zaproponowanie rozwiązań praktycznej realizacji wybranych funkcjonalności mechanizmu DTM w ICC (*Inter-Cloud Communication*)
- DTM++: integracja DTM i wybranych funkcjonalności ICC
- Kierowanie ewaluacją systemu i zadaniami oceny
- Zdefiniowanie środowiska testowego dla DTM i DTM++
- Przeprowadzenie eksperymentów dla DTM i DTM++

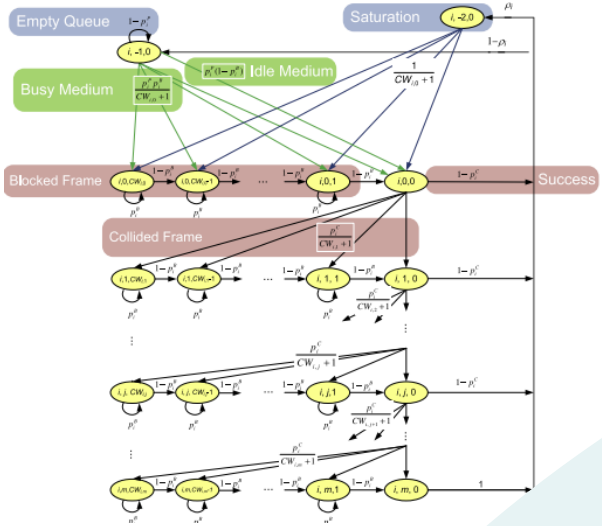
Sieci bezprzewodowe

Obszary badań:

- Rozszerzenia standardu 802.11
  - Analiza i poprawa wydajności 802.11ac, 802.11ax itd.
- Sieci spontaniczne (*ad-hoc*) i kratowe (*mesh*)
  - Dostęp do kanału radiowego i ruting
- Zastosowanie nowych koncepcji sieciowych do Wi-Fi
  - SDN, wirtualizacja, autonomizacja
- Łączność kooperatywna z wykorzystaniem łączy stratnych
- Zapewnianie bezpieczeństwa przeciw atakom wewnętrznym w Wi-Fi

Sieci bezprzewodowe (2)

Organizowanie dostępu do kanału radiowego w sieciach Wi-Fi



Eksperymenty rzeczywiste

Symulacje

Modelowanie

Sieci bezprzewodowe (3)

Wybrane publikacje:

- J. Konorski, S. Szott, „Discouraging Traffic Remapping Attacks in Local Ad Hoc Networks," *IEEE Transactions on Wireless Communications* , vol. 13, no. 7, 2014
- S. Szott, „Selfish insider attacks in IEEE 802.11s wireless mesh networks," *IEEE Communications Magazine*, vol. 52 no. 6, 2014
- K. Kosek-Szott, „A comprehensive analysis of IEEE 802.11 DCF heterogeneous traffic sources," *Ad Hoc Networks*, vol. 16, 2014

Działalność standaryzacyjna

WLAN

- IEEE 802.11 Working Group
  - „Potential voting member”
  - Udział od 2014
- ETSI NTECH AFI (od 2013)
  - Network Technology (NTECH) Working Group: Evolution of Management towards Autonomic Future Internet (AFI)
  - Wcześniej AFI ISG (2009-2013)

Działalność standaryzacyjna (2)

Internet engineering

- IETF (Internet Engineering Task Force), ALTO (Application-Layer Traffic Optimization) working group
- Prace koncentrują się na projektowaniu i standaryzowaniu nowych rozszerzeń protokołu ALTO

Działalność standaryzacyjna (3)

Dokumenty standaryzacyjne:

- T. B. Meriem, S. Szott, et al., „Autonomic network engineering for the self-managing Future Internet (AFI): Scenarios, Use Cases and Requirements for Autonomic/Self-Managing Future Internet”, ETSI Group Specification AFI 001, June 2011
- L. Ciavaglia, S. Szott, et al., „Autonomic network engineering for the self-managing Future Internet (AFI): Generic Autonomic Network Architecture (An Architectural Reference Model for Autonomic Networking, Cognitive Networking and Self-Management)”, ETSI Group Specification AFI 002, April 2013

Wybrane wcześniejsze projekty europejskie

- **4th Framework Programme ACTS** (1995 – 2001)
  - BBL (Broad-Band Loop)
  - BTI (Broadband Trial Integration)
  - BIDS (Broadband Infrastructures for Digital Television and Multimedia Services)
- **5th Framework Programme IST** (1998 – 2002)
  - LION (Layers Interworking in Optical Networks)
  - MOBY DICK (Mobility and Differentiated Services in a Future IP Network)
- **6th Framework Programme IST** (2002 – 2006)
  - NOBEL, NOBEL 2 (Next Generation Optical Network for Broadband in Europe)
  - DAIDALOS, DAIDALOS 2 (Designing Advanced Network Interfaces for the Delivery and Administration of Location Independent Optimised Personal Services)
  - Networks of Excellence: E-NEXT, EuroNGI, e-Photon/One
  - STREP: Calibrate

Wybrane wcześniejsze projekty europejskie (2)

- **7th Framework Programme ICT** (2007-2013)
  - INDECT (Intelligent Information System Supporting Observation, Searching and Detection for Security of Citizens in Urban Environment)
    AGH coordinated this project, which was the largest IP 7th FP project in Europe, coordinated by academia
  - Networks of Excellence: EuroNF, BONE
  - STREPs: CARMEN, SmoothIT, NI2S3
- **EUREKA CELTIC** project: DESYME
- **European Defense Agency** projects: MEDUSA, HECTOR
- **COST** project: COST2100 Action: Pervasive Mobile and Ambient Wireless Communications
- **eCONTENT+** project: GAMA

Dydaktyka
w Katedrze Telekomunikacji

- **Studia pierwszego i drugiego stopnia**
  - Elektronika i Telekomunikacja
  - Electronics and Telecommunications (po angielsku)
  - Teleinformatyka
- **Studia doktoranckie**
  - Elektronika
  - Informatyka
  - Telekomunikacja

Dodatkowe informacje

- Akademia Górniczo-Hutnicza
  http://www.agh.edu.pl
- Katedra Telekomunikacji:
  http://www.kt.agh.edu.pl
- Katedra Telekomunikacji, badania:
  http://www.kt.agh.edu.pl/badania_naukowe_lp
- **Adres:**
  Katedra Telekomunikacji
  Akademia Górniczo-Hutnicza im. S. Staszica w Krakowie
  Al. Mickiewicza 30, 30-059 Kraków
  Tel. +48 12 6345582
  Fax +48 12 6342372
  E-mail: kt@agh.edu.pl

Dziękuję bardzo za uwagę