Rozproszone mechanizmy sieciowe i paradygmat mikroekonomiczny

Jerzy Konorski
Wydział ETI Politechniki Gdańskiej

Nowe rodzaje ataków

intruz	*egoista*
oczekuje uczciwego przydziału zasobów dla szkodliwych celów	dąży do nieuczciwie wysokiego przydziału zasobów dla nieszkodliwych celów
wykorzystuje standardowy protokół komunikacyjny	modyfikuje standardowy protokół komunikacyjny

- *fałszywe tablice* (manipulacja mechanizmem przydziału)
- *wymuszanie pierwszeństwa* (agresywna strategia dostępu)
- *jazda na gapę* (konsumpcja bez współponoszenia kosztów)

Nowy rodzaj obrony

- ingerencje w standard – eliminacja prywatnych parametrów

  STOP firmware, instalacje zastane

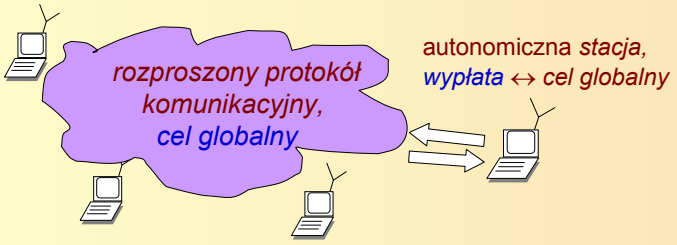
- środki administracyjne – IDS

  STOP uwierzytelnianie, potrzeba stacji zaufanych

- mechanizmy mikroekonomiczne
  egoizm powinien prowadzić do koooperacji, podejście teorii gier

ONE WAY samoregulacja, rozwiązania potencjalnie kosztowo efektywne

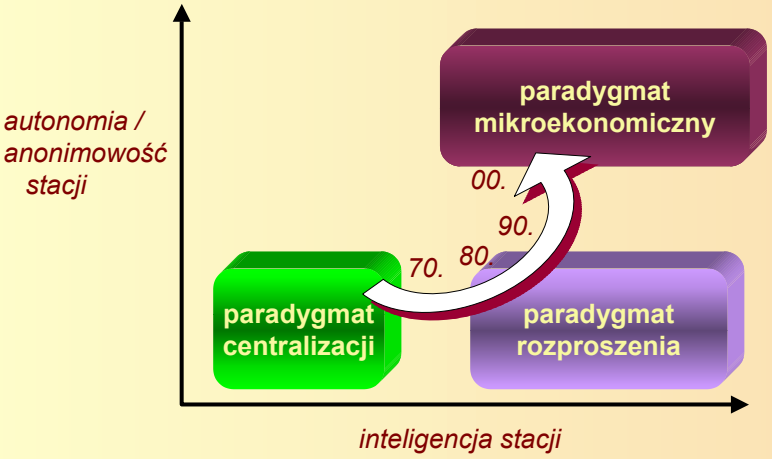
Modelowanie



Paradygmat kooperacyjny
- zachowania przedprogramowane, zgodne z "ustawieniami fabrycznymi"
- optymalizacja, dystrybucja wypłat

Paradygmat niekooperacyjny (mikroekonomiczny)
- zachowania autonomicznie racjonalne
- strategie maksymalizacji wypłat, równowaga Nasha

Modelowanie: trend



Gra: interaktywny proces decyzyjny

- $<\{1,...,N\}, S, u>$ – gracze, strategie, wypłaty
- wypłata gracza n : $u_n(s_1,\ldots,s_N) = u_n(s_n, \boldsymbol{s}_{-n})$
- punkt równowagi Nasha (NE) $(\hat{s}_1,...,\hat{s}_N)$

$$u_n(\hat{s}_n, \hat{\boldsymbol{s}}_{-n}) = \max_{s_n \in S} u_n(s_n, \hat{\boldsymbol{s}}_{-n}) \quad \forall n$$

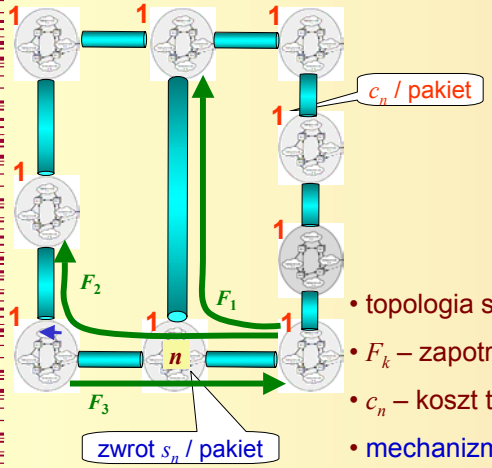
- gra powtarzalna, metastrategie – timing, horyzont wstecz i w przód:

$$s_n^k = \sigma_n(\boldsymbol{s}^{k-l},...,\boldsymbol{s}^{k-1}) \quad (l = 1..\infty\text{: reaktywne, behawioralne})$$

$$(1-\delta)\sum_{j=0}^{\infty}\delta^j u_n(s^{k+j}) \quad \text{(wsp. dyskonta } \delta = 0..1\text{: krótko-, dalekowzroczne)}$$

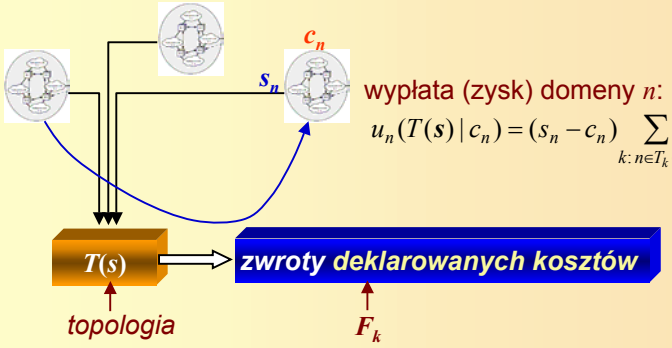
- typowe problemy:
  - "cena anarchii" w NE, identyfikacja / zmniejszanie
  - metastrategia zapewniająca zbieżność do "dobrych" NE

Fałszywe tablice: routing międzydomenowy



- topologia sieci, domeny $n = 1,...,N$
- F_k – zapotrzebowanie przepływu k
- c_n – koszt tranzytu/pakiet w domenie n
- mechanizm routingowy (np. BGP):
  - zbiera s_n – deklarowane koszty tranzytu/pakiet
  - znajduje najtańsze trasy $T_k(\boldsymbol{s})$
  - realizuje zwrot deklarowanych kosztów

Wypłaty domen i koszt sieci



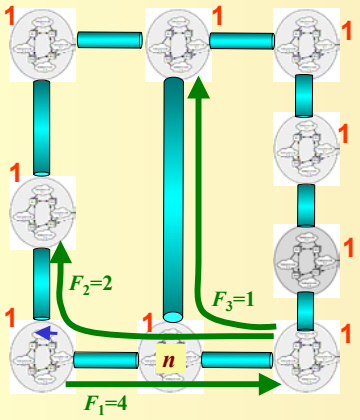
wypłata (zysk) domeny n:

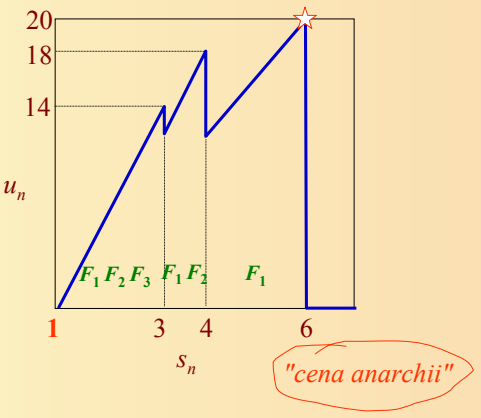
$$u_n(T(\boldsymbol{s}) \mid c_n) = (s_n - c_n) \sum_{k:\, n \in T_k(\boldsymbol{s})} F_k$$

- koszt sieci: $V(T(\boldsymbol{s})) = \sum_{n=1}^{N} c_n \sum_{k:\, n \in T_k(\boldsymbol{s})} F_k$ minimum (z definicji) dla $\boldsymbol{s} = \boldsymbol{c}$

STOP $s_n = c_n$ na ogół nie maksymalizuje u_n (motywacja zawyżania kosztów!)

Maksymalizacja wypłaty





? Jak wymusić najtańsze trasy?

Błędne koło – tylko mechanizm oparty o s_n, lecz przy jego znajomości domeny deklarują $s_n \neq c_n$, by maksymalizować u_n!

Strategioodporny routing VCG: płatności

- zysk domeny n = płatność – koszt:

$$p_n - c_n \sum_{k:\, n \in T_k(\boldsymbol{s})} F_k = u_n'(T(s_n, \boldsymbol{s}_{-n}) \mid c_n) = -V(T(\boldsymbol{s})) + h(\boldsymbol{s}_{-n})$$

- $<\{1,\ldots,N\}, \mathbf{R}^+, u'>$ jest grą potencjałową

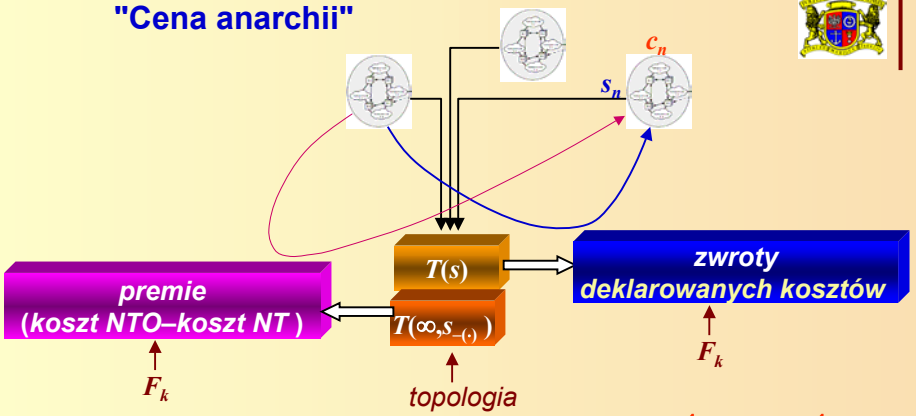
strategie gracza B

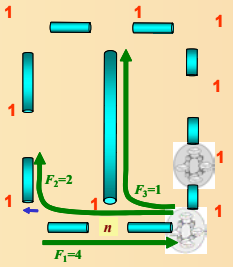
strategie gracza A

5 6	1 4
3 2	2 3

- NE pokrywa się z minimum V, tj. maksimum zysku dla $s_n = c_n$
- metastrategia reaktywna → NE
- $s_n = \infty \Rightarrow h(\boldsymbol{s}_{-n}) = V(T(\infty, \boldsymbol{s}_{-n}))$ – najtańsze trasy obejściowe (bez domeny n)

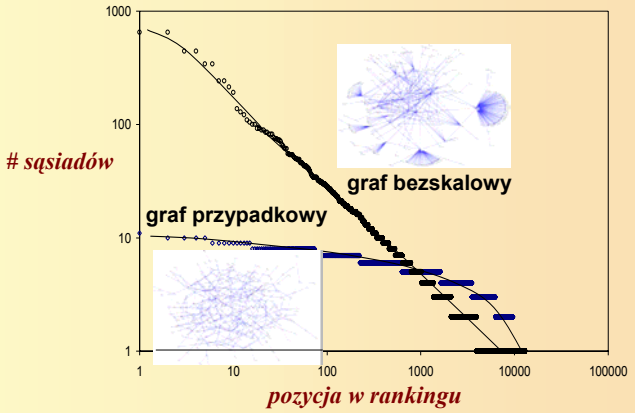
"Cena anarchii"





- zysk/koszt domeny n = $^{(4\cdot5+2\cdot3+1\cdot2)}/_{1\cdot(4+2+1)}$ = 300%
- zyski domen = "cena anarchii"
- czy to poważny problem w rdzeniu Internetu?

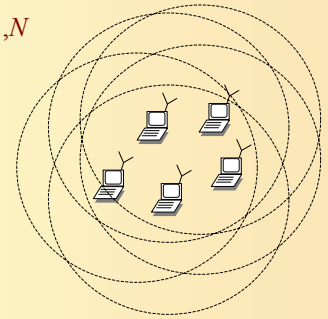
Zyski domen i ranking sąsiedztwa



- średni zysk domeny powiązany z kształtem rankingu sąsiedztwa
- 1997..obecnie: 4000→25000 domen, nachylenie ∈ [–0.80, –0.87]
- średni zysk ∈ [40%, 50%], ok. 60% domen bez zysku

Wymuszanie pierwszeństwa: rywalizacja MAC

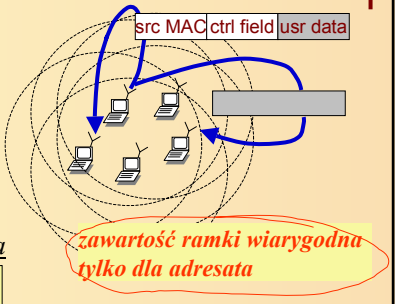
- ad hoc WLAN, stacje $1,\ldots,N$
- wzajemna słyszalność



- stacja n kontroluje prywatny parametr rywalizacji $s_n \in S$
  ($s' > s$: stochastycznie częstsze próby transmisji ramek)
- $u_n(s_1,\ldots,s_N)$ – wypłata stacji n (przepływność = udział pasma)

MAC: warunki ataku egoistycznego

- $u_n(s_n,\boldsymbol{s}_{-n})$ obserwowalne tylko dla stacji n



- $<\{1,\ldots,N\}, S, u>$ – Dylemat Więźnia

strategie gracza A \ strategie gracza B	*kooperacyjna*	*egoistyczna*
kooperacyjna	**1 1**	**-1 2**
egoistyczna	**2 -1**	**0 0**

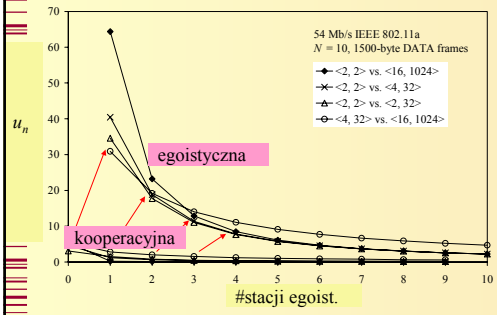
Uogólniony N-DW:

(i) $u_n(s_n,\boldsymbol{s}_{-n})$ rośnie w funkcji s_n (jednostronna opłacalność)
(ii) $u_n(s_n,\boldsymbol{s}_{-n})$ maleje w funkcji $\boldsymbol{s}_{-n}$ (zewnętrzna uciążliwość)
(iii) $u_n(s',\ldots,s') < u_n(s,\ldots,s)$ dla $s' > s$ ("tragedia dobra publicznego")

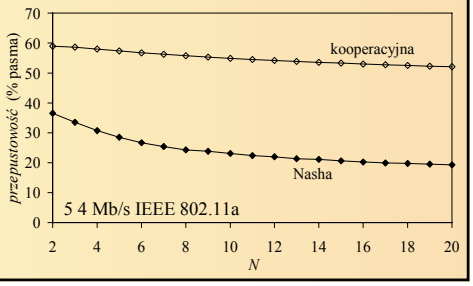
IEEE 802.11: gra CSMA/CA

$s \sim (CW_{\min}, CW_{\max})$ np. (16,1024),…,(2,2)

W zakresie nasycenia ruchem zachodzi (i).
W zakresie rywalizacji (gdy u_n rośnie w funkcji prawdop. udanej transmisji) zachodzi także (ii), (iii).



• metastrategia reaktywna
→ NE = $(s^*,\ldots,s^*)$ ($s^* = \sup S$)



• "cena anarchii" rzędu 50%!

Jak wymusić kooperację

...na autonomicznych stacjach, przy anonimowych ramkach, bez ingerencji w standard MAC?

• dalekowzroczne metastrategie behawioralne σ_n, $\delta \to 1$

• $s_n^k = \sigma_n(x^1,\ldots,x^{k-1})$, $x^k = \#s^*$ "zgrubnie" obserwowalne w grze CSMA/CA)

• "ludowe twierdzenie teorii gier":
przy $\delta \to 1$ metastrategia behawioralna może zapewnić zbieżność do NE z dowolnymi wypłatami powyżej minimaksowych (selektywne kary za odstępstwo)

STOP problem – stacje anonimowe

Σ = SPELL

Naprzemienna gra kooperacyjna ($s^o = \inf S$) i egoistyczna ($s^* = \sup S$), stochastycznie wydłużające się okresy gry egoistycznej.

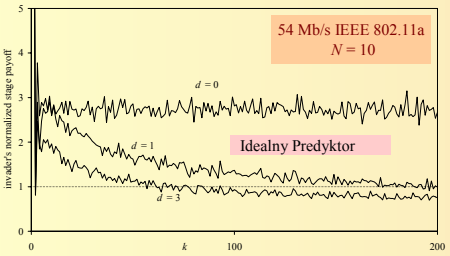
Przy odpowiednim doborze stochastycznego wzrostu,

$$(s_1^k,\ldots,s_N^k) \xrightarrow[k\to\infty]{(\sigma,\Sigma,\ldots\Sigma)} (s^*,\ldots,s^*) \qquad \forall\sigma(\#\text{odstępstw od } \Sigma = \infty)$$

$$(s_1^k,\ldots,s_N^k) \xrightarrow[k\to\infty]{(\Sigma,\ldots\Sigma)} (s^o,\ldots,s^o)$$

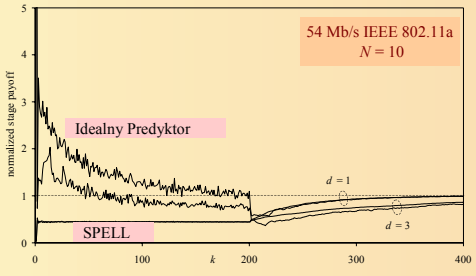
w sensie l.i.p., $\forall\ (x^1,\ldots,x^{k-1})$.

SPELL *vs.* Idealny Predyktor



bez wzrostu stochastycznego...

powrót do SPELL...



Podsumowanie

- Rozwiązania samoregulacyjne, kosztowo efektywne, odpowiednie dla środowisk autonomicznych / anonimowych
- Modelowanie: od klasycznej inżynierii (optymalizacja, przedprogramowanie) do teorii konfliktu
- Problemy: "cena anarchii" w NE, metastrategie zbieżności do "dobrych" NE
- Korzyści poznawcze
  - analiza: identyfikacja bardziej realistycznych punktów pracy
  - synteza: wymuszanie kooperacji poprzez zgodność motywacyjną