Rozproszone systemy teleinformatyczne: inteligencja, autonomia, racjonalność i bezpieczeństwo kooperacji

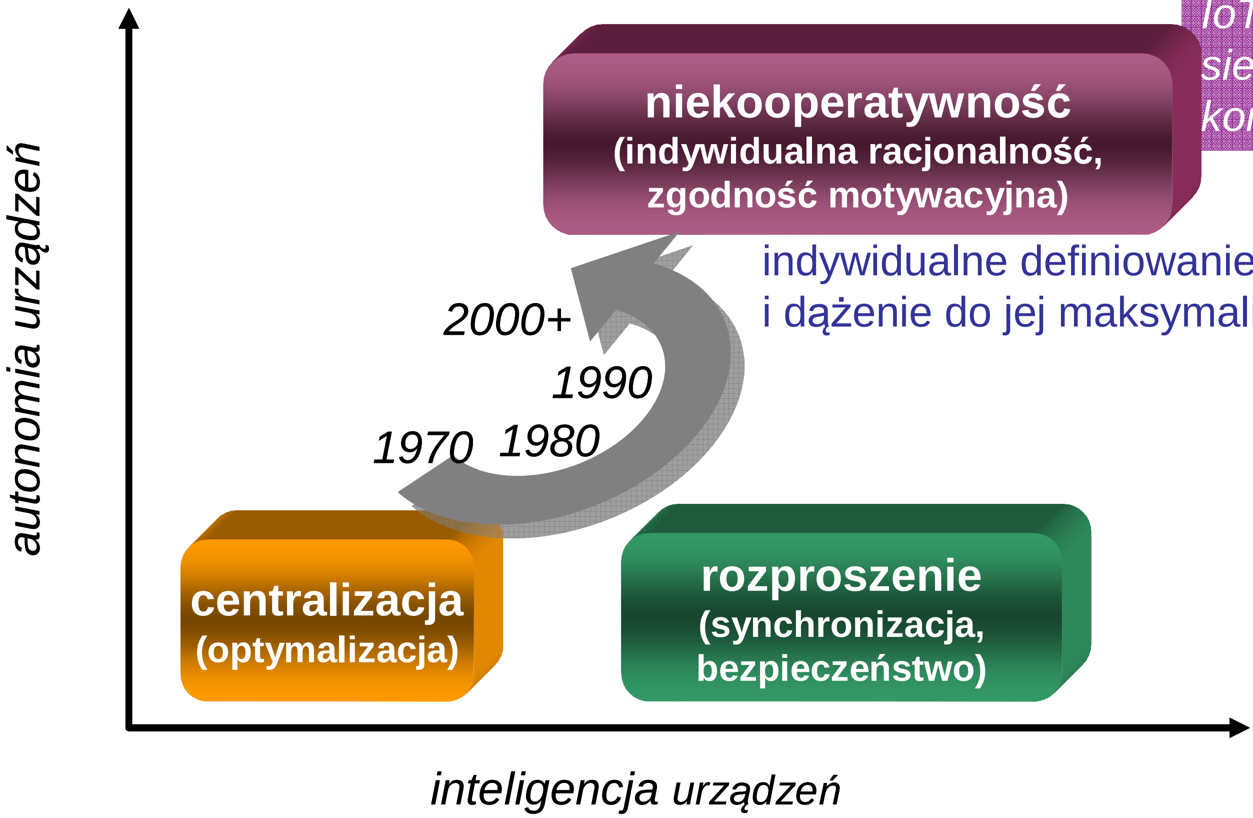
Jerzy Konorski

Politechnika Gdańska, Wydział ETI

- dr inż. 1984 IPI PAN Warszawa
- dr hab. inż. PG 2007
- > 100 samodzielnych i >25 współaut. prac opublik. w wyd. międzynarod.
- 2005-2012 kierownik 4 kraj i międzynarod. projektów naukowych, i kierownik zadania w 3 projektach
- współred. 2 tomów i 1 spec. wyd. Telecomm. J., stały czł. komitetów progr. >20 międzynar konf. nt. sieci komputer.
- liczne wykłady zaproszone w 12 krajach
- zainteresowania: systemy rozproszone, badania operacyjne, zastosowania teorii gier w sieciach bezprzewodowych

Paradygmaty projektowania i analizy systemów (tele)informatycznych

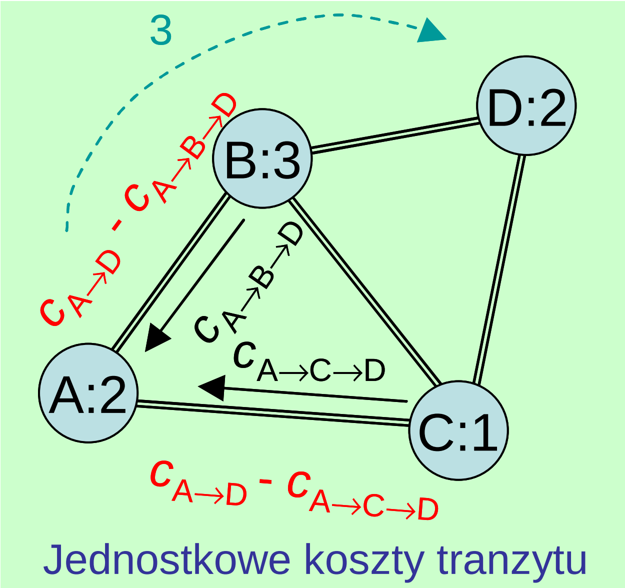
P2P, protokoły wieloagentowe, IoT, radio kognitywne, sieci ad hoc, sensorowe, komórkowe, mesh, self-X, IDS

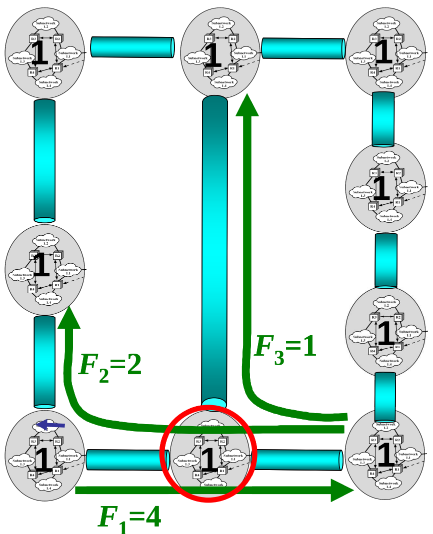


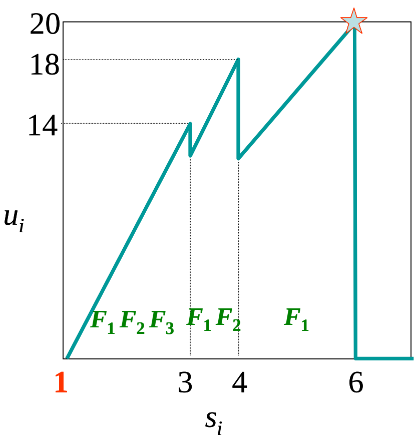
indywidualne definiowanie ***użyteczności*** (racjonalność) i dążenie do jej maksymalizacji (niekooperatywność)

Wyśledzić moment historyczny, w którym liczydło dosięgło Rozumu, jest równie trudno jak ów, co małpę przemienił w człowieka. [St. Lem 1981]

Routing: najtańszy tranzyt







- <u>centralizacja</u>: np. "mnożenie" macierzy

$$\begin{bmatrix} 0 & 0 & 0 & \infty \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ \infty & 0 & 0 & 0 \end{bmatrix} \underset{\text{min-plus}}{\otimes} \begin{bmatrix} 0 & 2 & 2 & \infty \\ 3 & 0 & 3 & 3 \\ 1 & 1 & 0 & 1 \\ \infty & 2 & 2 & 0 \end{bmatrix}^t$$

- <u>rozproszenie</u>: np. zasada optymalności

$$c_{\mathrm{A}\to\mathrm{D}} = \min\{c_{\mathrm{B}} + c_{\mathrm{A}\to\mathrm{B}\to\mathrm{D}},\, c_{\mathrm{C}} + c_{\mathrm{A}\to\mathrm{C}\to\mathrm{D}}\}$$

- <u>niekooperatywność</u>: nie da się zrealizować!
  deklarowane koszty jednostkowe $\boldsymbol{s} \neq \boldsymbol{c}$

użyteczność $u_i = (s_i - c_i) \cdot \sum_{k:\, i \in T_k(\boldsymbol{s})} F_k$

$\boldsymbol{s} = \boldsymbol{c}$ maksymalizuje użyteczności węzłów ⇔ przepływ k dopłaca węzłowi i koszt jednostkowy $= c(T_k(\boldsymbol{s})) - c(T_k(\infty, \boldsymbol{s}_{-i}))$ [Feigenbaum *et al*. 2005]

Główne podejścia

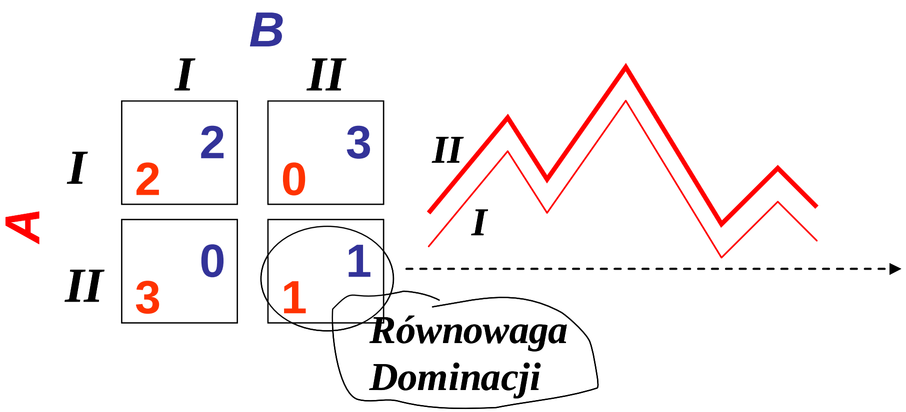
- Bezpieczeństwo kooperacji: uczciwy (kooperatywny) agent vs. racjonalny intruz

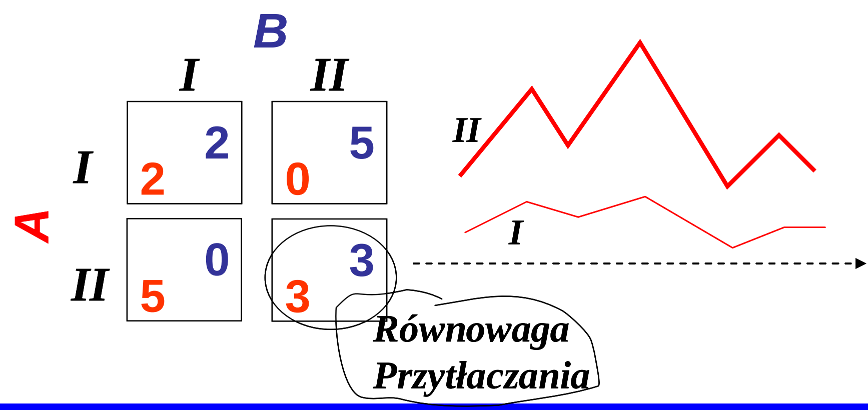
  - *Gapowicz*: udział w konsumpcji zasobów bez udziału w kosztach
  - *Pirat Drogowy*: łamanie zasad dostępu do zasobów
  - *Fałszywy Radiowóz*: uzurpacja przywilejów dostępu do zasobów

  Modyfikacja strategii uczciwego agenta ograniczająca użyteczność racjonalnego intruza bez naruszania własnej.

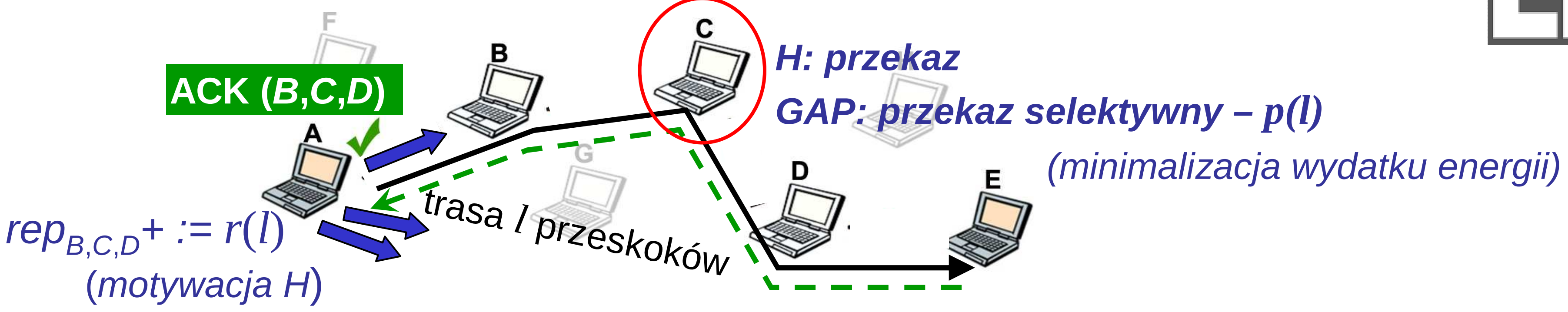
> *We have always known that heedless self-interest was bad morals; we know now that it is bad economics.* [FDR 1933]

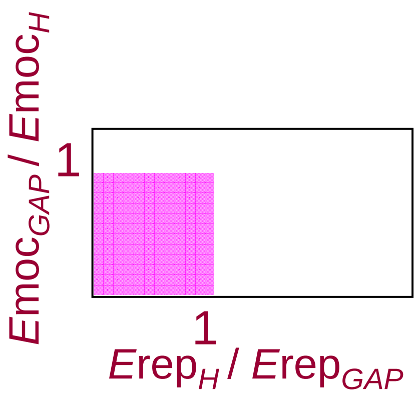
- Gra niekooperatywna: predykcja wyniku interakcji racjonalnych agentów & mechanizmy zgodności motywacyjnej ich użyteczności i celów globalnych.

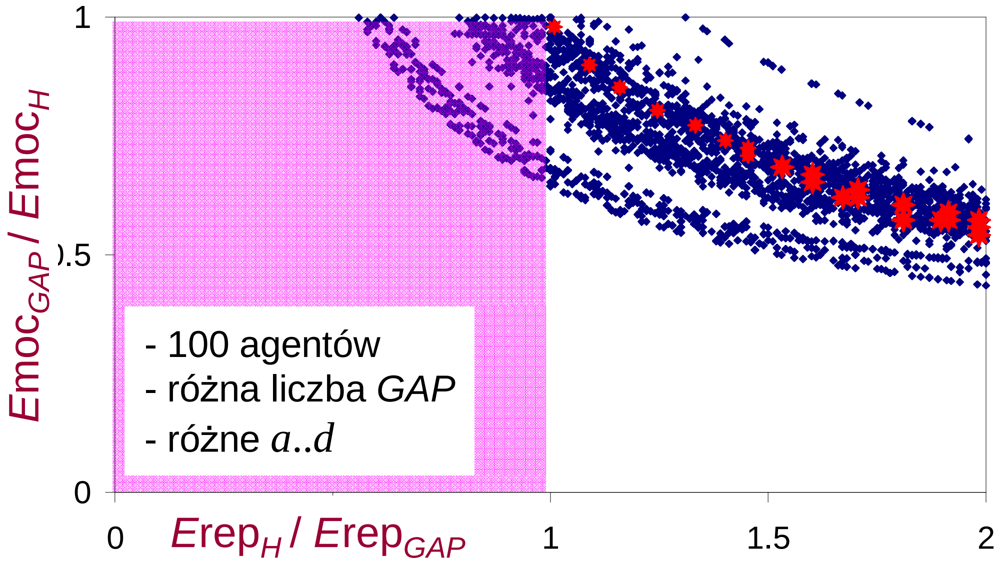




System reputacyjny vs. Gapowicze







$$r(l)=\begin{cases}0, & l=1\\ l^a, & l>1\end{cases}$$

$$p(l)=\begin{cases}1, & l=1\\ cl^b, & 0<l\le d\\ 0, & l>d\end{cases}$$

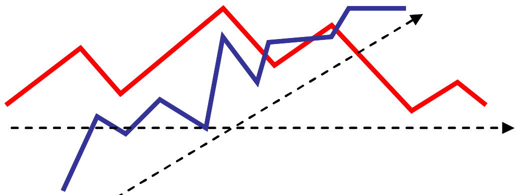
H jest strategią przytłaczającą (zakazany region nie zostaje naruszony niezależnie od liczby *GAP*) $\Leftrightarrow$ $r(1) = 0$ i $p(l) = const.$ dla $l > 1$. [J.K. 2011]

Równowaga Nasha

Bez dodatkowych mechanizmów motywacyjnych nie istnieje nawet protokół zapewniający dominację *H*. [Zhong *et al*. 2007]

Mniej (lecz dalej bardzo) przekonująca predykcja wyniku gry:

A \ B	I	II
I	2, 1	0, 0
II	0, 0	1, 2



Równowaga Nasha (NE)

$$\boldsymbol{s} \ \text{ jest NE gdy } \ s_i \in \arg\max_{z \in S_i} u_i(z, \boldsymbol{s}_{-i}) \ \ \forall i$$

Na ogół niezbędna jest wspólna wiedza agentów
o racjonalności i funkcjach użyteczności (założenie dość silne).

W(x) = Z(x) ^ Z^2(x) ^ …

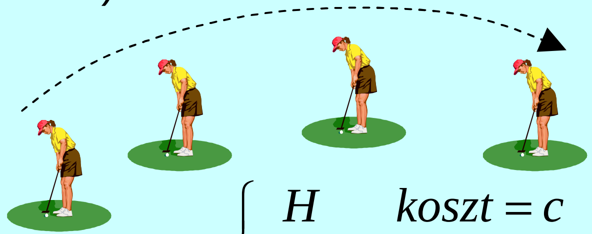
Operator vs. Gapowicze: pokusa nadużycia

Należy zapewnić NE przy $\boldsymbol{s} = \boldsymbol{H}$.

zadanie (dostarczenie pakietu)

$W\,|_{\boldsymbol{s}} \in \{+,-\}$

u_i^+ lub u_i^-



$$s_i = \begin{cases} H & koszt = c \\ GAP & koszt = 0 \end{cases}$$

Model niezawodności i interakcji agentów $\Rightarrow$ $W\,|_{s_i,\boldsymbol{H}_{-i}} = \begin{cases} - & \phi \\ V\,|_{s_i,\boldsymbol{H}_{-i}} & 1-\phi \end{cases}$

Przy $\boldsymbol{s} = \boldsymbol{H}$ dla każdego agenta i opłacalne jest:

- (IR) przyjęcie kontraktu $\phi \cdot u_i^- + (1-\phi) \cdot \left(\underset{V|_{H,\boldsymbol{H}_{-i}}}{E} u_i^v - c \right) \geq 0$
- (ZM) wybór H w warunkach kontraktu $\underset{V|_{H,\boldsymbol{H}_{-i}}}{E} u_i^v - c \geq u_i^-$

W punkcie NE $\boldsymbol{s} = \boldsymbol{H}$, przy równych kosztach i niezawodności *end-to-end*, dłuższe trasy są zawsze tańsze dla Operatora! [Feldman *et al*. 2007]

NE i informacja agenta

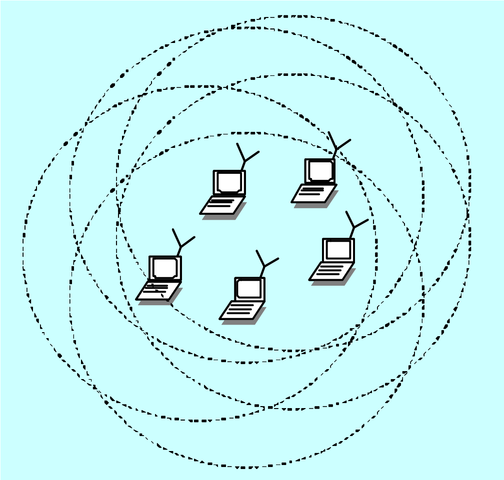
Wersje NE zależą od rodzaju informacji dostępnej w grze.
Strategia agenta i jest funkcją $X_i \to S_i$ posiadanej informacji.

Jeśli każdy agent posiada informację prywatną, a wspólna wiedza dotyczy jedynie jej charakterystyk probabilistycznych, to NE $\to$ równowaga bayesowska (BE).

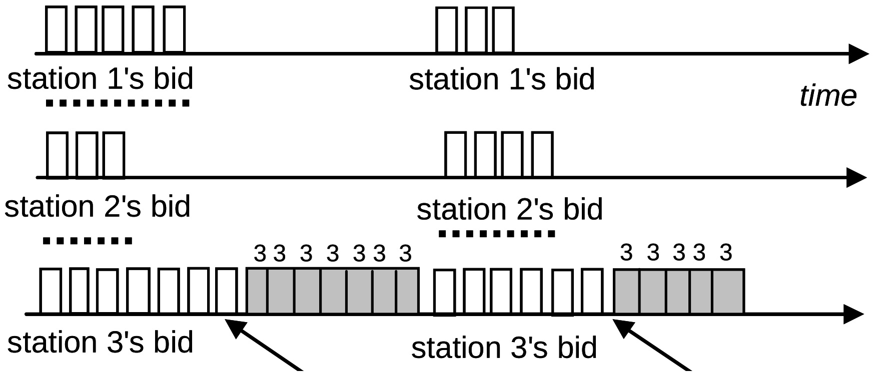
$$\boldsymbol{s} \text{ jest BE, gdy } s_i(x) \in \arg\max_{z \in S_i} \mathop{E}_{\boldsymbol{x}_{-i}} u_i(x, z, \boldsymbol{s}_{-i}(\boldsymbol{x}_{-i})) \quad \forall x \in X_i$$

W systemach teleinformatycznych pojęcie BE jest przydatne, gdy x_i opisuje lokalne warunki ruchowe, konfigurację protokołu, jakość transmisji, fazy rywalizacji o zasoby, percepcję jakości usług, stan zasilania, lokalizację itp.

Aukcja pasma dla Piratów Drogowych



H: standardowy MAC
PIR: agresywny



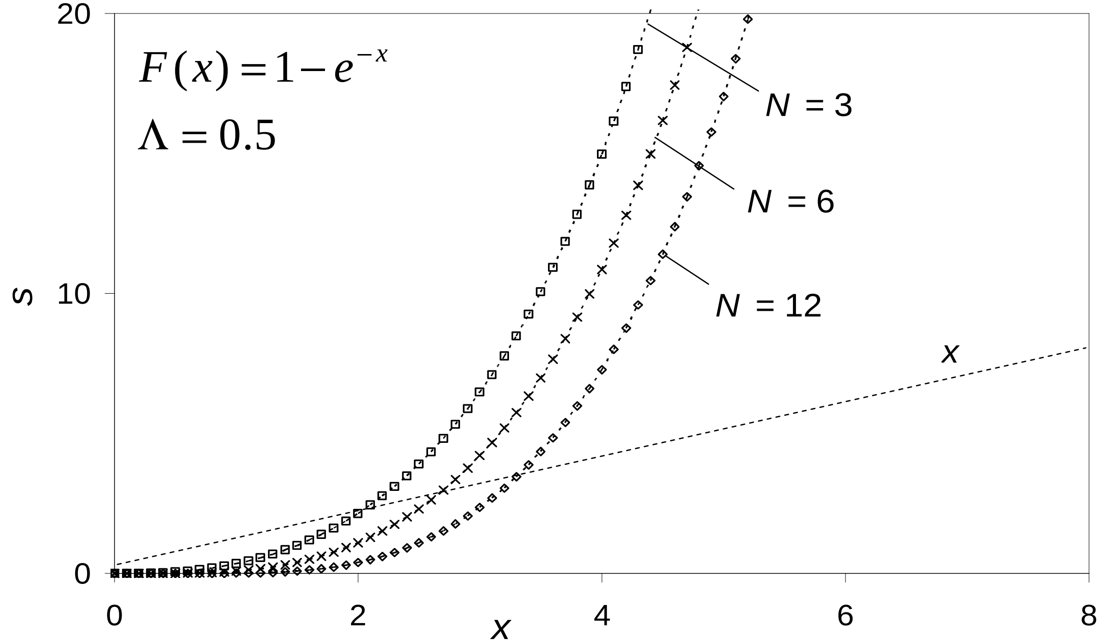
- strategia agenta jest funkcją $X \to S$ odwzorowującą długość transferu ruchu na długość sekwencji licytującej
- użyteczność u_i = |transfer| - |sekwencja licytująca|
- x – prywatna informacja agenta, dystrybuanta $F(x)$ – wspólna wiedza

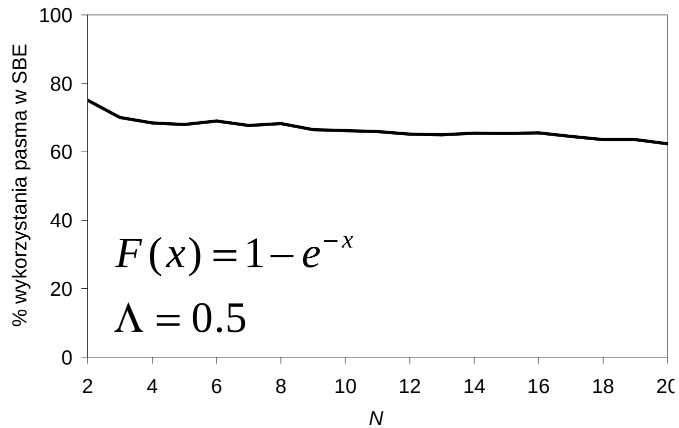
$$\underset{\boldsymbol{x}_{-i}}{E}\, u_i(x, z, \boldsymbol{s}_{-i} \equiv \sigma) = -z\big(1 - F^{N-1}(\sigma^{-1}(z))\big) + \int_0^z (x - y + \Lambda y)\, dF^{N-1}(\sigma^{-1}(y))$$

Symetryczny BE: dla $x \in X_i$ rodzina z dających maksimum pokrywa się z funkcją σ.

Aukcja pasma: strategia BE

W punkcie BE: $$s(x) = \int_0^x y \cdot \exp\left(\Lambda \cdot \int_y^x \mu_{F^{N-1}}(v)dv \right) \cdot \mu_{F^{N-1}}(y)dy$$ [J.K. 2009]





Nieintuicyjna licytacja w BE:
- możliwa powyżej wartości transferu!
- ostrożniejsza przy dużej liczbie rywalizujących stacji!
- bardziej agresywna przy wzroście Λ, lecz bez wpływu na Eu_i!

mixNE i wybór sieci

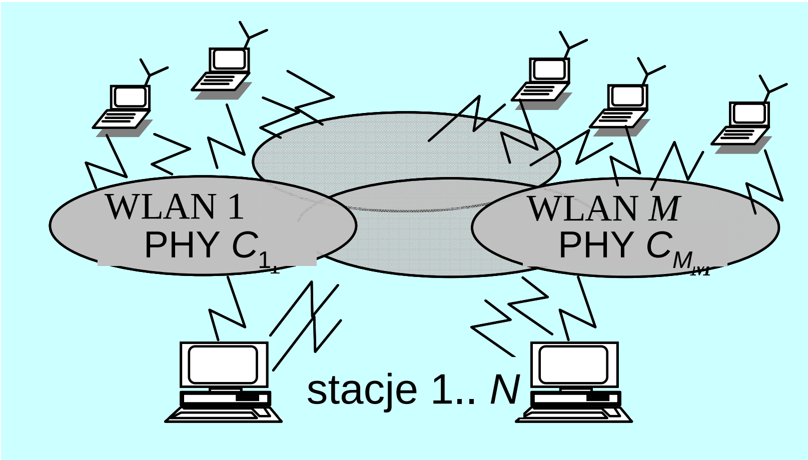
Rozszerzenie S_i na $\Delta(S_i)$ – <u>miksty</u>:

$$\boldsymbol{s} \text{ jest mixNE, gdy } s_i \in \arg\max_{z\in\Delta(S_i)} \underset{\boldsymbol{s}_{-i}}{E}\, u_i(z,\boldsymbol{s}_{-i}) \quad \forall i$$

Przy wielu asymetrycznych NE symetryczny mixNE jest bardziej przekonywującą koncepcją rozwiązania gry.

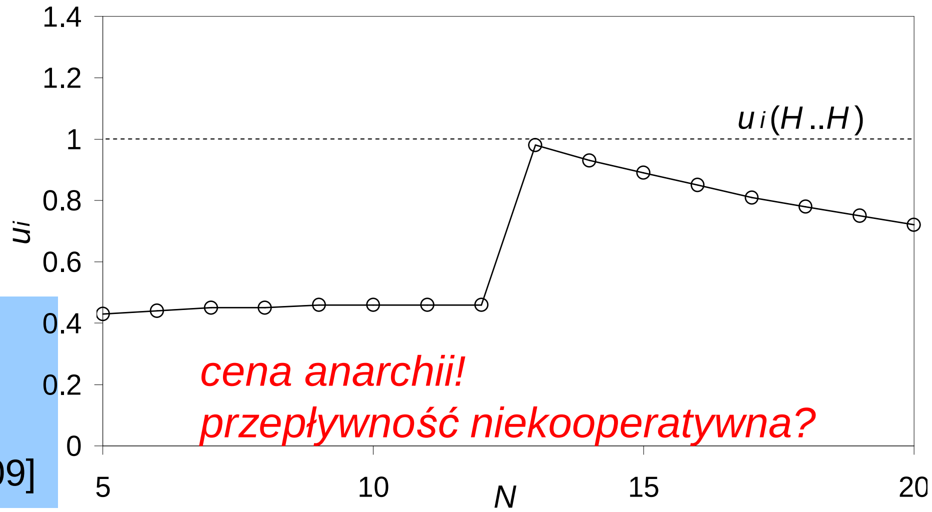
A \ B	*I*	*II*
I	2, 1	0, 0
II	0, 0	1, 2

mixNE = $^2/_3 * \boldsymbol{I} + ^1/_3 * \boldsymbol{II}$



- ***H*: standardowy MAC, równomierny wybór sieci**
- ***PIR*: agresywny MAC, preferencja dla szybkich sieci**

Gra "wybór sieci" $<\{1..N\}, \{H, PIR\}, u>$
posiada wiele NE z jednakową liczbą *PIR* = K
i unikalny mixNE, zależny od K. [J.K. 2009]



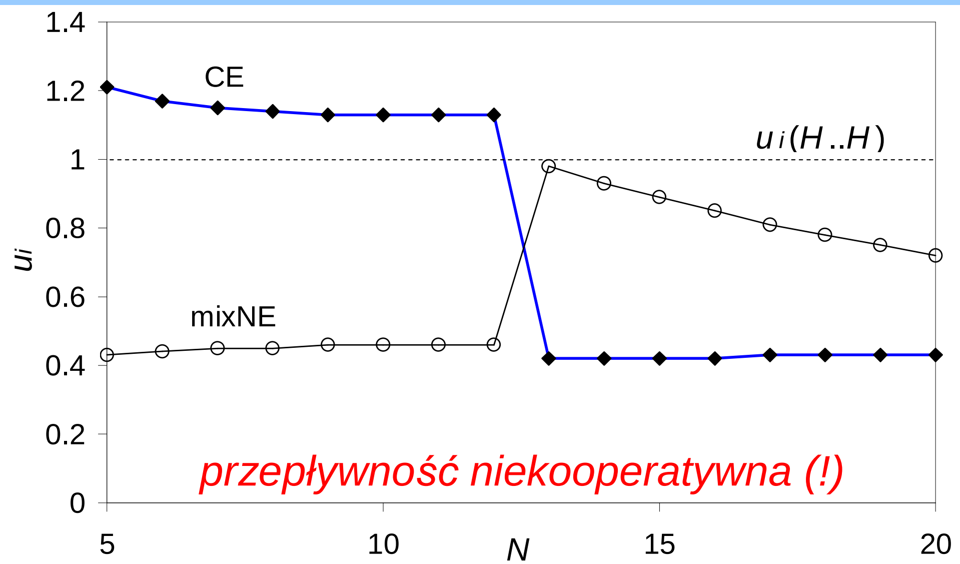
CE i wybór sieci

<u>Możliwa jest autonomiczna korelacja strategii agentów</u>!
Zewnętrzny mechanizm losuje $\boldsymbol{r} \in S_1\times\ldots S_N$, każdemu agentowi i rekomenduje r_i.
Agent we własnym interesie przyjmuje rekomendację.

$$\Pi \in \Delta(S_1 \times \ldots \times S_N) \text{ jest CE, gdy } r_i \in \arg\max_{z \in S_i} \mathop{E}_{\Pi(\boldsymbol{s}_{-i}|r_i)} u_i(z, \boldsymbol{s}_{-i}) \ \forall i$$

NE $\rightarrow$ równowaga korelowana (CE).

Gra "wybór sieci" $<\{1..N\}, \{H, PIR\}, u>$ posiada unikalny symetryczny CE, zależny od K i łatwy do rozproszonej implementacji. [J.K. 2009]

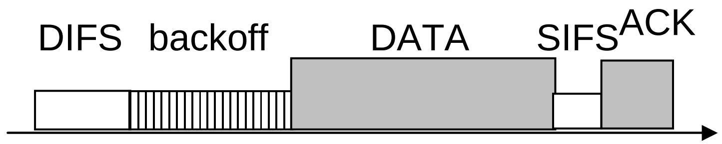


Uczenie NE: czy można?

Analiza introspektywna i wynikowa postać NE niekiedy b. skomplikowane.
Czy proste protokoły / urządzenia to potrafią?

Czy NE można się "nauczyć" w grze wieloetapowej, tj. $\boldsymbol{s}^{t+1} = \omega\left((\boldsymbol{s},\boldsymbol{u})^1;\ldots;(\boldsymbol{s},\boldsymbol{u})^t\right)$?

- IEEE 802.11 DCF robi to bezwiednie!



$$s_i^{t+1} = \begin{cases} s_{\max} & P_{succ,i}(\boldsymbol{s}^t) \\ s_i^t/2 & P_{coll,i}(\boldsymbol{s}^t) \\ s_i^t & 1-s_i^t \end{cases} \quad = \quad s_i^t + \frac{\partial u_i}{\partial s_i}\Big|_{\boldsymbol{s}^t} + \aleph$$

gdzie $\aleph$ – szum

$$u_i(\boldsymbol{s}) = \alpha \cdot P_{succ,i}(\boldsymbol{s}) - \beta \cdot P_{coll,i}(\boldsymbol{s})$$

Gra "DCF" $<\{1..N\}, [0..s_{\max}], u>$ posiada NE, do którego ww. schemat jest zbieżny!

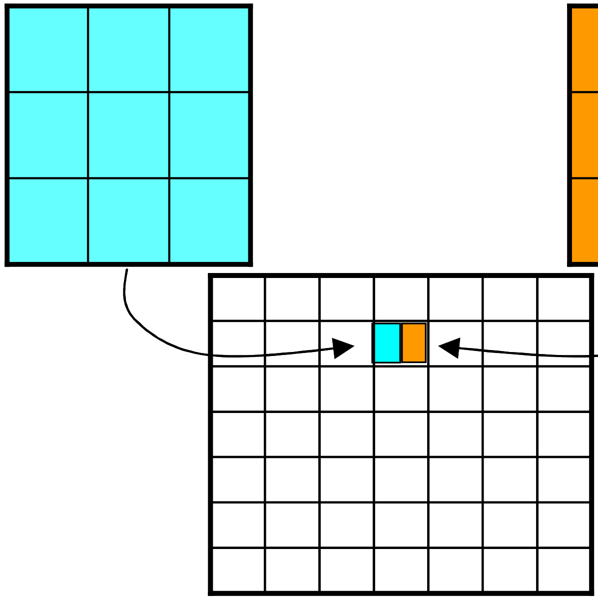
Po odpowiednim przeskalowaniu: $s_i^{t+1} \in \arg\max_z u(z, \boldsymbol{s}_{-i}^t)$, tj. DCF jest schematem najlepszej odpowiedzi!

[Lee *et al*. 2007]

Uczenie NE: czy warto?

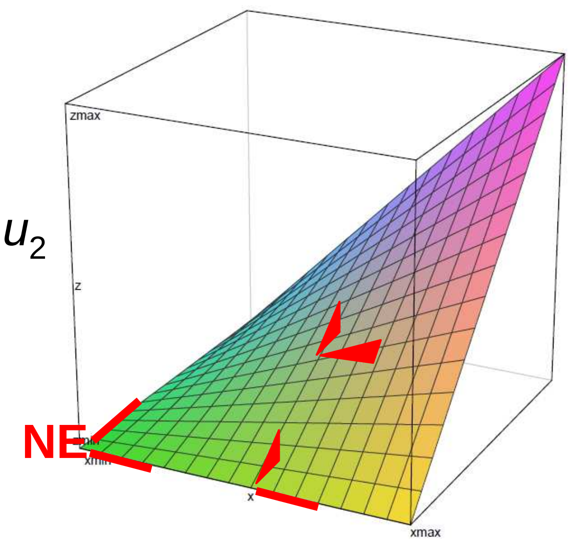
baza adresów agenta 1 – prefiksy
rozmiar $\in$ [0, ∞)

baza adresów agenta 2 – sufiksy
rozmiar $\in$ [0, ∞)



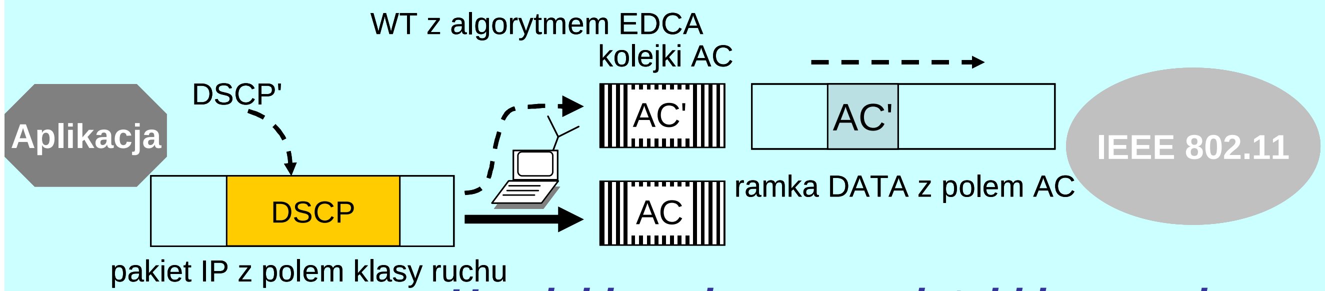
u_i = rozmiar przestrzeni adresowej

u_1, u_2



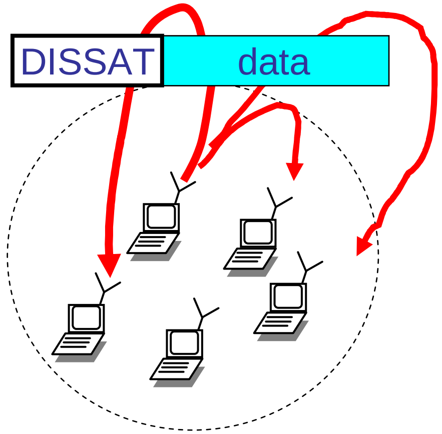
Jedyny NE = (0, 0) daje najgorszy możliwy wynik!
Jak się go uczyć – schemat najgorszej odpowiedzi?!

Fałszywe Radiowozy w EDCA



***H:* deklaracja rzeczywistej klasy ruchu**
***FR:* deklaracja klasy ruchu odwzorowanej na wyższą kategorię dostępu**

<u>Wiarygodna groźba</u> wykrycia *FR*:
emisja DISSAT przez nieusatysfakcjonowane stacje *H*
⇒ penetracja zawartości i zagłuszanie ramek



Użyteczność stacji i: $u_i(\mathbf{s}) = sat_i(\mathbf{s}) - ex_i(\mathbf{s}) \in \{-1,0,1\}$

- wymagania stacji
- dostępne pasmo

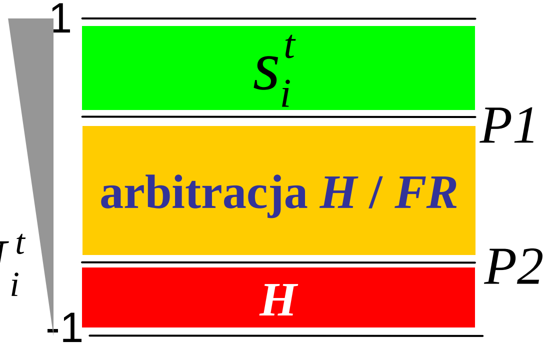
narażenie na wykrycie FR

- gra "EDCA" $<\{1..N\}, \{H, FR\}, \boldsymbol{u}>$
- pożądany NE: "równowaga satysfakcji", tj. $\boldsymbol{u}(\boldsymbol{s}^*) = \mathbf{1}$
- nie zawsze dopuszczalny przez $\boldsymbol{sat}(\cdot)$

Wieloetapowa gra EDCA: schemat uczenia

2-progowy wybór strategii w funkcji ruchomej średniej własnej użyteczności:

$$s_i^{t+1} =$$



$$s_i^{t+1} = f_{P1,P2}\left((s_i, U_i)^t\right)$$

$$U_i^{t+1} = \overline{U_i^t, u_i(s_i^{t+1})} \quad \Rightarrow \quad (\mathbf{s}, \mathbf{U})^{t+1} = \omega(\mathbf{s}, \mathbf{U})^t$$

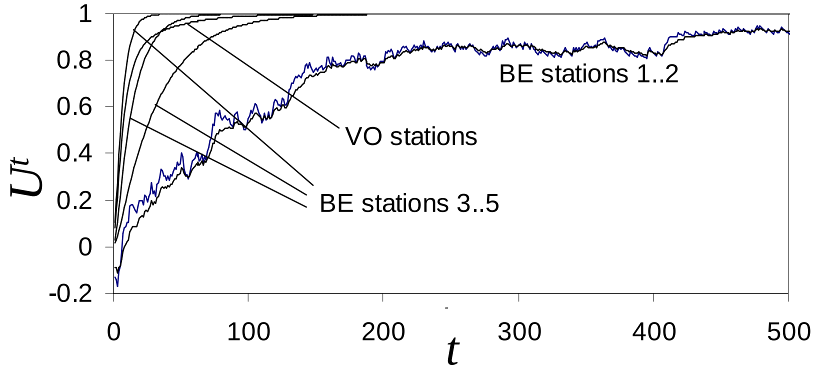
Jeżeli - $\boldsymbol{sat}(\cdot)$ dopuszcza $\boldsymbol{s}^*$,
- $P2 < 0 < P1$,
- arbitracja H / FR jest uczciwa,

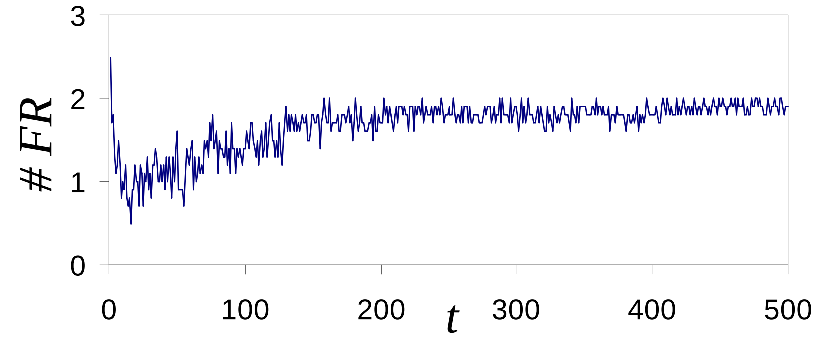
to ω gwarantuje osiągalność $\boldsymbol{s}^*$ z dowolnego stanu (s, U) w skończonej liczbie etapów.

???: ω jest NE gry wieloetapowej $<\{1..N, \Omega, U\}>$, tj. *FR* jest nieefektywny lub nieszkodliwy.

[J.K. & Szott 2012]

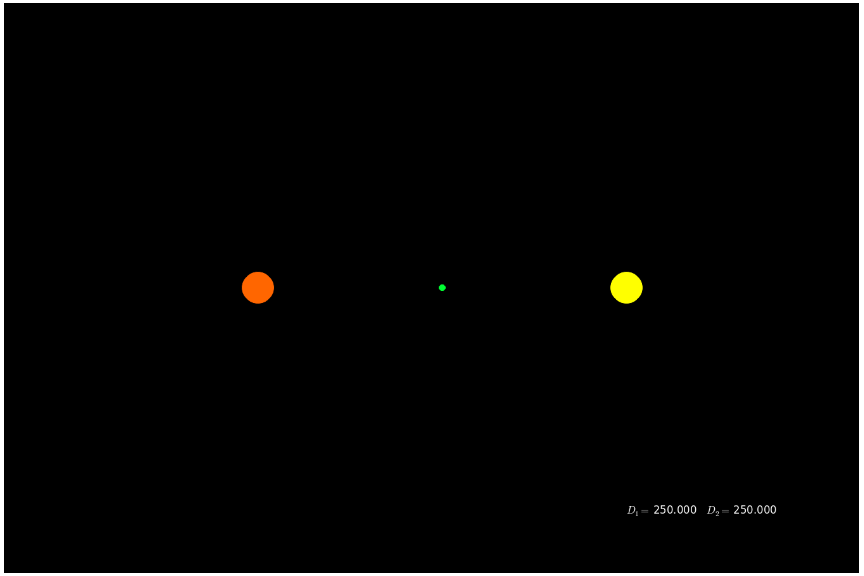
- stacje generują Voice i best-effort
- wysokie wymagania stacji b-e 1 i 2 powodują uporczywe ataki *FR*

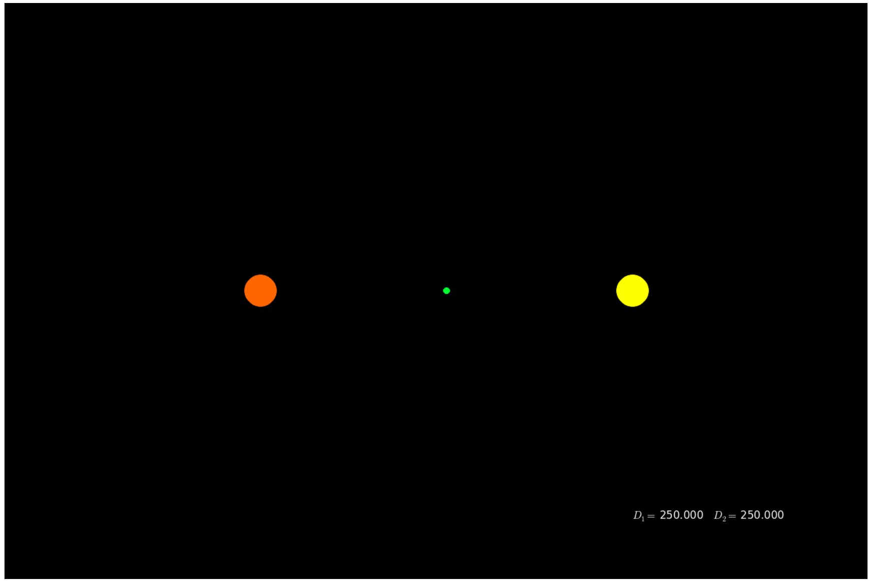




Podsumowanie

- Predykcje punktów pracy w paradygmacie niekooperatywności – często mniej optymistyczne, przeważnie mniej intuicyjne
- …znacznie mocniejsze (zgodność motywacyjna).!
- Dobre strategie – introspekcja, schematy uczenia, ewolucja, akwizycja?
- Cena anarchii, ignorancji, koegzystencji z agentami nieracjonalnymi?





Dziękuję za uwagę,

jekon@eti.pg.gda.pl