

Шести семинар
„Математика и примени“

17 март 2023

Институт за математика
Природно-математички факултет
Универзитет „Св. Кирил и Методиј“ Скопје

СТАКЕЛБЕРГ ИГРИ ВО БЕЗБЕДНОСТА

Невена Серафимова



СОДРЖИНА

- Што е игра?
- Стакелберг игри
- Безбедносни игри
- Решенија и алгоритми
- Отворени прашања





1



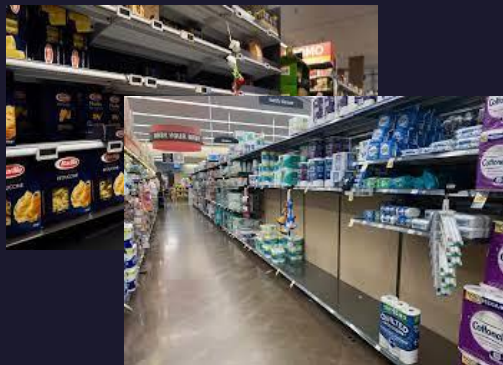
2



3



4



5

(1 – веројатност за одбрана) * добивка од успешен напад

6



ШТО Е ИГРА?

Научна метафора за поширок опсег на меѓучовечки интеракции

Интерфејс помеѓу математиката и процесите на одлучување

Исходите зависат од интерактивните стратегии на две или повеќе лица

Спротивставени, или во најдобар случај мешани мотиви

Комплетна / некомплетна информација

Рационалност

Соработка (коалиции) или агресивност (лична добивка)

Повторување на играта – што е различно во однос на еднократните средби?

ШТО Е ИГРА? ИНФОРМАЦИИ

Комплетна информација: ако играчите ги знаат не само сопствените стратегии и добивки, туку и оние на другите играчи, како и дека сите останати го знаат истото.

НЕКОМПЛЕТНА ИНФОРМАЦИЈА:

ако не е со комплетна информација

Доколку играта се повторува, вообичаено е играчот со **УЧЕЊЕ** да ги открива информациите кои не му се достапни.

Совршена информација: ако при секој потег, играчите ги знаат претходните потези на другите играчи т.е. можат да ги набљудуваат дејствата.

НЕСОВРШЕНА ИНФОРМАЦИЈА:

ако не е со совршена информација

Тогаш, играчот треба да претпоставува кои дејства ги преземале останатите учесници.

ШТО Е ИГРА? СОРАБОТКА

КООПЕРАТИВНИ ИГРИ:
стратегиски игри во кои
интересите на играчите се
совпаѓаат

НЕКООПЕРАТИВНИ ИГРИ:
во кои постои конфликт на
интереси т.е. се стриктно
КОМПЕТИТИВНИ

(Сигнална игра) Два автомобили кои возат во спротивна насока се среќаваат на тесен пат и се во опасност да се судрат. Секој од нив има по три стратегии: оди лево, оди десно и оди право.

Исходот зависи од одлуката и на двата возачи, и во нивни интерес е да го избегнат сударот. За таа цел, барем еден од нив треба да ги сигнализира своите намери на другиот возач.

(0-сума игра) Неколку големи добавувачи се присутни на зеднички пазар. Секој треба да одлучи дали да ги намали своите цени, без да знае што одлучиле останатите.

Под претпоставка дека потрошувачката се зголемува кога цените паѓаат, различни стратегиски комбинации ќе резултираат со добивка или загуба за едните или другите.

Но, порастот на клиенти кај едниот добавувач, значи загуба кај другиот.

НОРМАЛНА ИГРА

- Сите играчи дејствуваат истовремено
- Нешов еквилибриум = стабилни исходи
- Секој играч го бира најдобриот одговор на стратегиите на сите други играчи

	КОЛ 1	КОЛ 2
РЕД 1	(1,1)	(3,0)
РЕД 2	(0,0)	(2,1)

СТАКЕЛБЕРГ ИГРА

Играчите дејствуваат последователно.

- Фокус на двајца играчи: „лидер“ и „следбеник“
- Лидерот прво се обврзува да игра (евентуално мешана) стратегија x_1

Лидерот комуницира x_1 со следбеникот.

- Не може подоцна да се повлече од обврската

Следбеникот го избира најдобриот одговор x_2 .

- Следбеникот мора да верува дека посветеноста на лидерот е веродостојна

! Може да се претпостави дека е чиста стратегија.

- Дали обврзувањето пред почеток на играта може да биде штетно?
- Дали лидерот може да изгуби во Стакелберг еквилибриум во споредба со Нешовиот еквилибриум?

СТРОГ СТАКЕЛБЕРГ ЕКВИЛИБРИУМ

L – лидер S - следбеник

SSE (l^*, s^*) :

1) Лидерот игра најдобар одговор

$$U_L(l^*, s^*) \geq U_L(l, R(l)), \forall l \in L$$

2) Следбеникот игра најдобар одговор

$$U_S(l^*, s^*) \geq U_S(l^*, s), \forall s \in S$$

3) Следбеникот прекршува во корист на лидерот

$$U_L(l^*, s^*) \geq U_L(l^*, s'), \forall s' \in \operatorname{argmax}_{s \in S} U_S(l^*, s)$$

0-СУМА ИГРИ: $A + B = 0$

Секој чист NE е максимин решение.

$$\max_{x_1} \min_{x_2} (x_1)^T A x_2 = \min_{x_2} \max_{x_1} (x_1)^T A x_2$$

- Што ќе направи Играч 1 ако е прв на потег?
- Што ќе направи Играч 2 потоа?

ОПШТА СУМА ИГРИ: $A + B \neq k \cdot I$

$$\max_{x_1} (x_1)^T A f(x_1)$$

$$f(x_1) = \max_{x_2} (x_1)^T B x_2$$

БЕЗБЕДНОСНИ ИГРИ

КОНТЕКСТ

B. Von Stengel, S. Zamir. Leadership games with convex strategy sets. *Games and Economic Behavior*, 69(2):446-457, 2010

V. Conitzer, T. Sandholm. Computing the optimal strategy to commit to. In *Proceedings of the 7th ACM conference on Electronic commerce*, 82-90, 2006

- Бранителот (лидер) има k идентични патролни единици (ресурси).
- Бранителот сака да одбрани множество C составено од n цели.
- Користејќи чиста стратегија, секој ресурс на бранителот може да заштити подмножество од цели $S \subseteq C$ од вкупната колекција на цели \mathcal{S} .
- Секоја цел се смета за покриена, ако е заштитена со барем еден ресурс.
- Напаѓачот сака да избере цел за напад.

БЕЗБЕДНОСТА е од критично значење за разни домени од секојдневието: заштита на аеродроми, пристаништа, критична инфраструктура, луѓе и добра, на живиот свет, и подразбира спречување на несреќи, напади, криумчарење или илегална трговија со оружје, луѓе, дрога или пари, а системите кои ги третира се протегаат од физички па до сајбер-физички.

Во безбедносните проблеми, РЕСУРСИТЕ со кои се располага се ограничени, па треба внимателно да се распоредат, земјаќи ги предвид целите, приоритетите, дејствата/случувањата, неизвесноста, способностите и знаењето.

БЕЗБЕДНОСНИ ИГРИ

СТРАТЕГИИ И ДОБИВКИ

Добивки

- За секоја цел, бранителот и напаѓачот имаат две добивки: една ако целта е покриена, една ако не е.
- Добивката зависи од тоа дали поединечните цели се бранети или не.
- Бранителот се обврзува на мешана стратегија;
- Напаѓачот следи со избирање на цел за напад.

	БРАНИТЕЛ		НАПАЃАЧ	
	покриена	непокриена	покриена	непокриена
ЦЕЛ 1	10	0	-1	1
ЦЕЛ 2	0	-10	-1	1
...				

П: Бидејќи ова е игра на Стакелберг со 2 играчи, дали може само да ја пресметаме оптималната стратегија за бранителот во полиномно време...?

R – ресурси, T - цели

	цел 1	цел 2	...	цел t-1	цел t	цел t+1	...	цел n
ресурс 1	1	0	...	0	1	1	...	1
ресурс 2	1	1	...	1	0	1	...	0
ресурс 3	0	0	...	1	1	0	...	0
...			...					
ресурс k	0	1		0	1	0		1

 Групен распоред j на ресурс 3 над T

 Покриеност на цел t

$$P_{3t} = 1$$

J – достапни групни распореди на ресурсите
 веројатносни распределби над J = мешани стратегии на лидерот
 веројатносни распределби над T = мешани стратегии на следбеникот

Очекувани добивки

$$U_L(x, a) = \sum_{t \in T} a_t [c_t U_L^+(t) + (1 - c_t) U_L^-(t)]$$

$$U_S(x, a) = \sum_{t \in T} a_t [c_t U_S^+(t) + (1 - c_t) U_S^-(t)]$$

$$c_t = \sum_{j \in J} P_{jt} x_j$$

маргинална
веројатност за
покривање на t

$$\max_a U_L(x, a)$$

МОДЕЛ I

Ограничувања:

- $\sum_i x_i = 1$ ← стратегија на L
- $\sum_j a_j = 1$ ← стратегија на S
- $a \in BR(x)$ ← одговор
- J ← распореди

R – ресурси, T - цели

	цел 1	цел 2	...	цел t-1	цел t	цел t+1	...	цел n
ресурс 1	1	0	...	0	1	1	...	1
ресурс 2	1	1	...	1	0	1	...	0
ресурс 3	0	0	...	1	1	0	...	0
...			...					
ресурс k	0	1		0	1	0		1

 Групен распоред j на ресурс 3 над T

 Покриеност на цел t

$$P_{3t} = 1$$

J – достапни групни распореди на ресурсите
 веројатносни распределби над J = мешани стратегии на лидерот
 веројатносни распределби над T = мешани стратегии на следбеникот

Очекувани добивки

$$U_L(x, a) = \sum_{t \in T} a_t [c_t U_L^+(t) + (1 - c_t) U_L^-(t)]$$

$$U_S(x, a) = \sum_{t \in T} a_t [c_t U_S^+(t) + (1 - c_t) U_S^-(t)]$$

$$c_t = \sum_{j \in J} P_{jt} x_j$$

маргинална веројатност за покривање на t

$$\max_c U_L(BR(x)|c) \quad \text{МОДЕЛ 2}$$

Ограничувања:

- $c_t = \sum_{r \in R, t \in J(r)} c_{r,t} \leq 1, \forall t \in T$
- $\sum_{t \in J(r)} c_{r,t} \leq 1, \forall r \in R$
- $U_S(t|c) \leq U_S(t^*|c), \forall t \in T$

БЕЗБЕДНОСНИ ИГРИ

Инфраструктурни игри



(a) LAX Checkpoint



(b) LAX Canine Patrol

Карактеристики на апликацијата:

- заштита на инфраструктурата, како што се пристаништа, аеродроми, возови, летови итн.;
- целта е помагање на агенциите ангажирани во борбата против тероризмот;
- статичност – мали промени (на пр., аеродромот може да има нова градба еднаш во 2-3 или повеќе години);
- активностите во инфраструктурата се регулирани со добро воспоставени распореди на движење на луѓе или стоки;
- целите што се заштитени често имаат дискретна структура, на пример, терминали на аеродром, индивидуални летови, индивидуални возови итн.

Севкупни карактеристики на играта:

- еднократна игра;
- лидерот се обврзува на мешана стратегија;
- еден напад од страна на противникот ја завршува играта.

Карактеристики на противникот:

- внимателно планирање и надзор
- напади со високи последици

Карактеристики на бранителот:

- не ги ажурира постојано стратегиите

БЕЗБЕДНОСНИ ИГРИ

Зелени игри



Карактеристики на апликацијата:

- заштита на животната средина, вклучувајќи ги шумите, рибите и дивиот свет;
- целта е помагање на безбедносните агенции против ловокрадците, нелегалните рибари или незаконска сеча;
- динамичност –животните или рибите кои се заштитени може да се движат наоколу во географскиот простор, воведувајќи нови димензии на сложеност;
- целите што се заштитени се распоредени на огромни отворени географски простори.

Севкупни карактеристики на играта:

- повторена игра;
- бранителот се обврзува на мешана стратегија;
- напаѓачот игра повеќе пати;
- по извесно време, бранителот повторно планира и игра нова мешана стратегија.

Карактеристики на бранителот:

- голем број на податоци
- постојано ажурирање на стратегиите

Карактеристики на противникот:

- ограничена рационалност и надзор
- напади со помали последици

БЕЗБЕДНОСНИ ИГРИ

Опортунистички криминал



Карактеристики на апликацијата:

- заштита на јавноста од опортунистички криминал;
- целта е помагање на безбедносните агенции во заштитата на приватниот имот;
- динамичност – човечки толпи се движат наоколу врз основа на закажаните активности;
- целите што се заштитени се распоредени во специфични ограничени географски области.

Севкупни карактеристики на играта:

- еднократна игра;
- бранителот се обврзува на мешана стратегија;
- напаѓачот игра повеќе пати;
- повеќе напаѓачи може да бидат активни истовремено.

Карактеристики на бранителот:

- ажурирањето на стратегиите е отворено прашање

Карактеристики на противникот:

- ограничена рационалност и надзор
- напади со помали последици
- опортунизам, флексибилност

БЕЗБЕДНОСНИ ИГРИ

Сајбер криминал



Карактеристики на апликацијата:

- заштита на мрежната инфраструктура од сајбер напади;
- целта е помагање на мрежните администратори во заштитата на компјутерските системи и спречување на прекин на услугите;
- големи компјутерски мрежи со повеќе компјутери со различно значење.
- целите што се заштитени се распоредени во специфични ограничени географски области.

Севкупни карактеристики на играта:

- различни цели на напаѓачот (контрола, компромитирање, кражба);
- бранителот (администратор или систем) сака да го идентификува и спречи натрапникот со избирање на пакети за проверка, и последователно да го спречи нападот;
- компромитираните системи се користат за понатамошни напади;
- поширока цел на бранителот: спречување на противникот да стекне контрола над системите во мрежата.

Карактеристики на бранителот:

- оптимална распределба на ресурсите за избор и инспекција на пакети за откривање на потенцијалните закани
- отворен проблем

Карактеристики на противникот:

- варијабилност по домени

АПЛИКАТИВНИ РЕШЕНИЈА

	ПРОБЛЕМ	ДОМЕН	РЕШЕНИЈА
СКАЛАБИЛНОСТ	Голем одбранбен стратегиски простор	Национални полициски сили	ASPEN – генерирање на стратегии
	Големи одбранбени и напаѓачки простори	Заштита на патната мрежа	RUGGED – оракл со двојна прецизност
	Мобилни ресурси и движечки цели	Заштита на бродови	CASS – компактно претставување на стратегии
	Повеќе рационално ограничени напаѓачи	Заштитата на рибарството	MIDAS – пристап на пресечна рамнина
	Детална просторна информација	Заштита на риболовот во дивниот свет	Хиерархиско моделирање
НЕИЗВЕСНОСТ	Унификација на неизвесноста	Безбедност на аеродроми	URAC – мултидимензионална редукција, подели и владеј
	Неизвесност при динамичко извршување	Безбедност на транспортните системи	Маркови процеси на одлучување
Ограничена напаѓачка рационалност, ограничено надгледување	Учење на напаѓачкото однесување	Заштита на риболовот во дивниот свет	Бихевиорални модели, експериментирање со човечки субјекти

Шести семинар

„Математика и примени“

17 март 2023

Институт за математика

Природно-математички факултет

Универзитет „Св. Кирил и Методиј“ Скопје

СТАКЕЛБЕРГ ИГРИ ВО БЕЗБЕДНОСТА

Невена Серафимова

nevena.serafimova@gmail.com

nevena.serafimova@ugd.edu.mk

