

Fall 2022 | Lecture 11

Security Games

Ariel Procaccia | Harvard University

STACKELBERG GAMES

- Playing up is a dominant strategy for row player
- So column player would play left
- Therefore, (1,1) is the only Nash equilibrium outcome

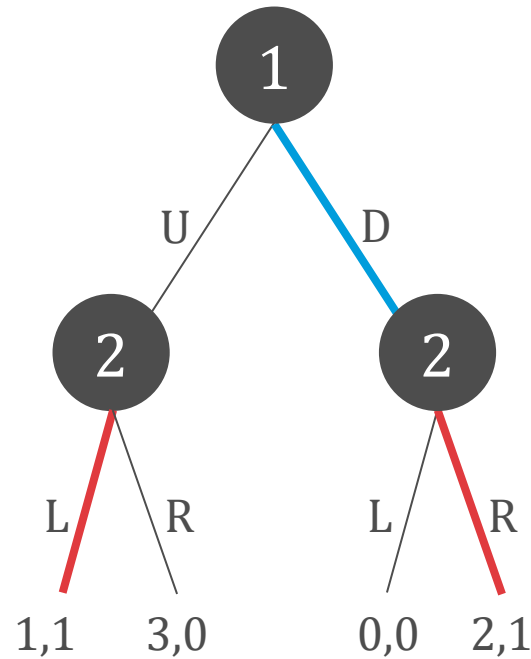
1,1	3,0
0,0	2,1

STACKELBERG GAMES

- A **Stackelberg game** is played as follows:
 - Row player (the **leader**) commits to playing a row
 - Column player (the **follower**) observes the commitment and chooses column
- The leader can commit to playing down!

1,1	3,0
0,0	2,1

STACKELBERG GAMES



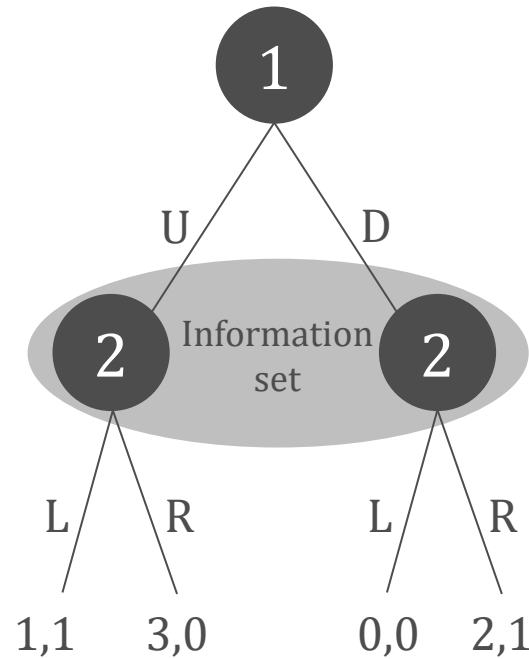
If the leader announces their commitment, the Stackelberg game can be rewritten as an extensive-form game of perfect information

STACKELBERG GAMES

- **Poll 1:** What reward can the leader get by committing to a mixed strategy? (Assume the follower breaks ties in favor of the leader)
 - 1
 - 1.5
 - 2
 - 2.5

1,1	3,0
0,0	2,1

STACKELBERG GAMES



Randomness helps the leader due to imperfect information

COMMITMENT IN REAL LIFE



<http://youtu.be/S0qjK3TWZE8>

STACKELBERG EQUILIBRIUM

- For a mixed strategy x_1 of the leader, define the best response set of the follower as

$$B_2(x_1) = \operatorname{argmax}_{s_2 \in S} u_2(x_1, s_2)$$

- In a **strong Stackelberg equilibrium** (SSE), the leader plays a mixed strategy in

$$\operatorname{argmax}_{x_1 \in \Delta(S)} \max_{s_2 \in B_2(x_1)} u_1(x_1, s_2),$$

where $\Delta(S)$ is the set of mixed strategies

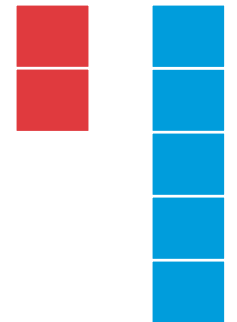
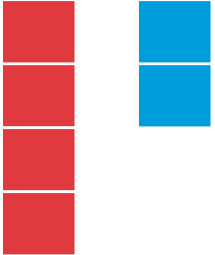
COMPUTING SSE

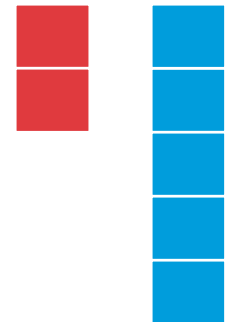
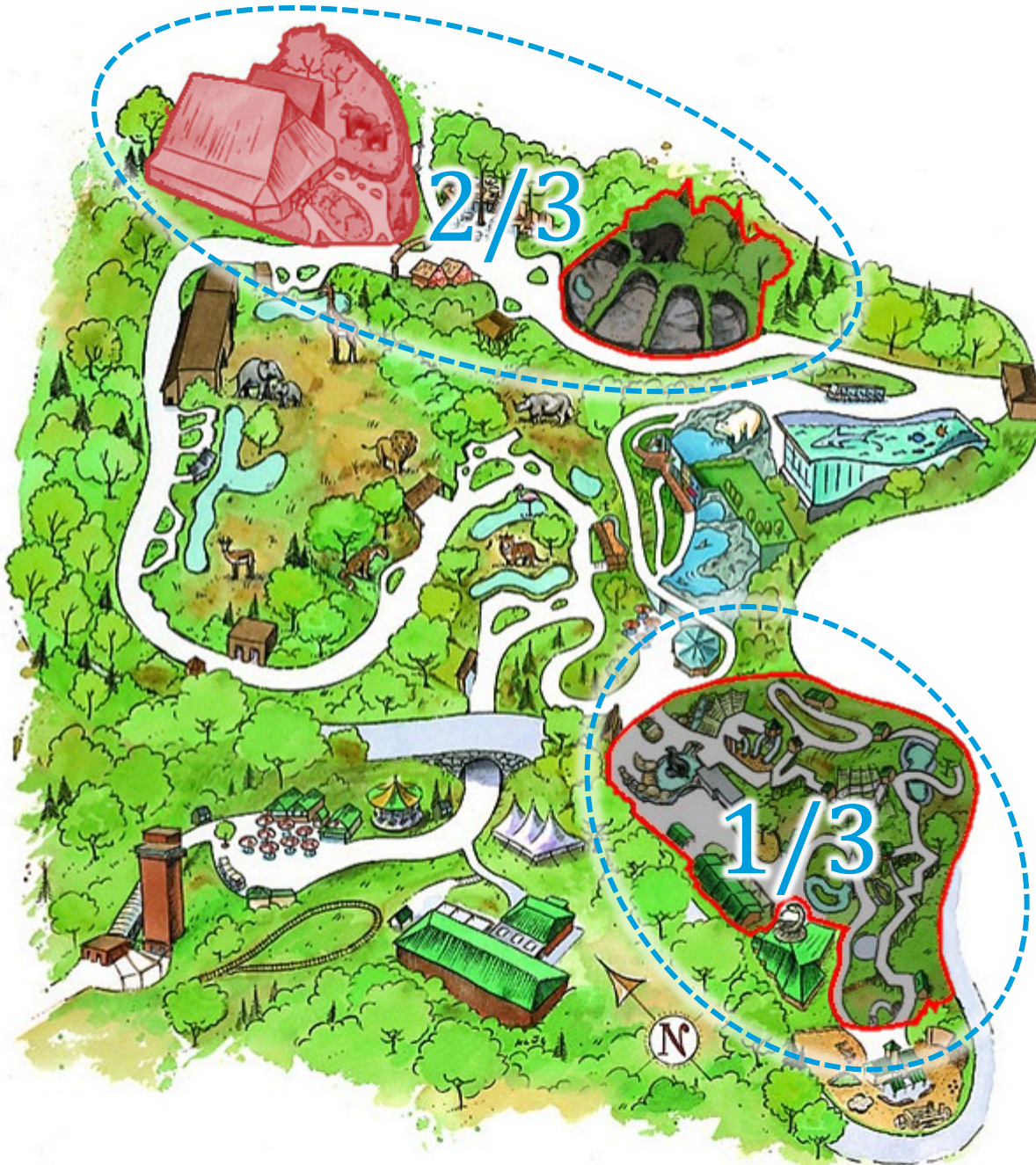
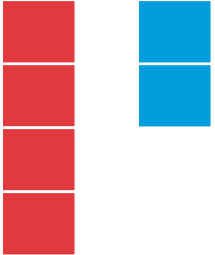
- In 2-player normal form games, an SSE can be computed in polynomial time through a linear program
- The leader's mixed strategy is defined by variables $x(s_1)$, which give the probability of playing each strategy $s_1 \in S$
- For each follower strategy s_2^* , we compute a strategy x for the leader such that
 - Playing s_2^* is a best response for the follower
 - Under this constraint, x is optimal

$$\max \sum_{s_1 \in S} x(s_1) u_1(s_1, s_2^*)$$

$$\text{s.t. } \forall s_2 \in S, \sum_{s_1 \in S} x(s_1) u_2(s_1, s_2^*) \geq \sum_{s_1 \in S} x(s_1) u_2(s_1, s_2)$$
$$\sum_{s_1 \in S} x(s_1) = 1$$

- Take the x resulting from the “best” s_2^*



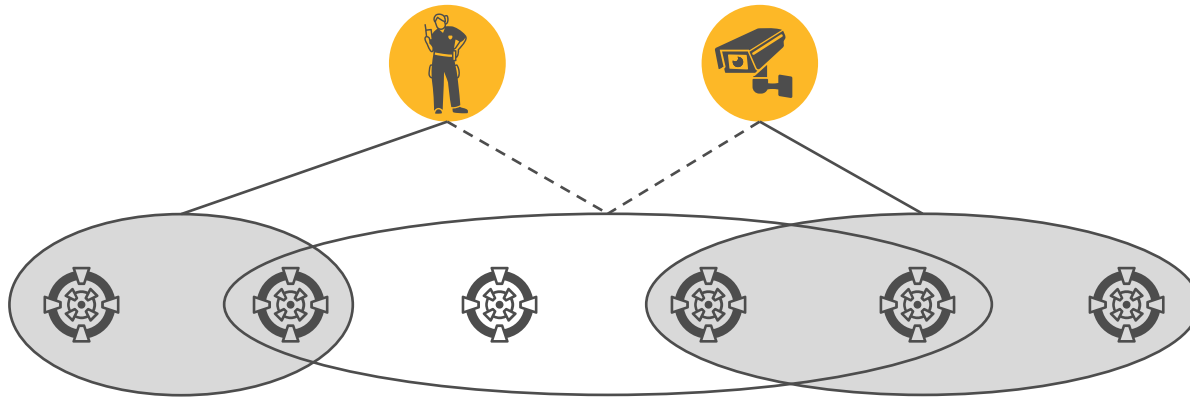


SECURITY GAMES



Milind
Tambe

SECURITY GAMES: MODEL



- Set of **targets** $T = \{1, \dots, n\}$
- Set of m security **resources** Ω available to the defender (leader)
- Set of **schedules** $\Sigma \subseteq 2^T$
- Resource ω can be assigned to one of the schedules in $A(\omega) \subseteq \Sigma$
- Attacker chooses one target to attack

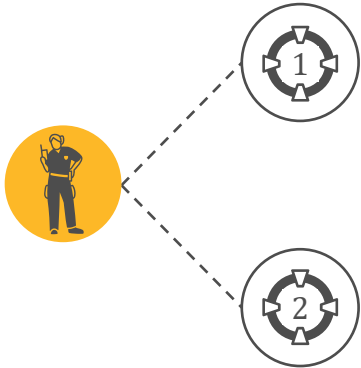
SECURITY GAMES: MODEL

- For each target t , there are four numbers:
 $u_d^+(t) \geq u_d^-(t)$ and $u_a^+(t) \leq u_a^-(t)$
- Mixed defender strategy induces **coverage probabilities** $\mathbf{c} = (c_1, \dots, c_n)$
- The utilities to the defender/attacker under \mathbf{c} if target t is attacked are

$$u_d(t, \mathbf{c}) = u_d^+(t) \cdot c_t + u_d^-(t)(1 - c_t)$$

$$u_a(t, \mathbf{c}) = u_a^+(t) \cdot c_t + u_a^-(t)(1 - c_t)$$

SECURITY GAMES: EXAMPLE

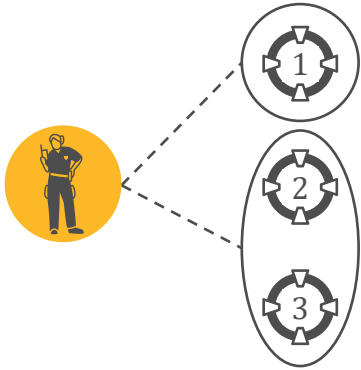


	Attacker		Defender	
Target	Covered	Uncovered	Covered	Uncovered
1	0	$1/2$	0	-1
2	0	1	0	-1

Poll 2: What is the defender's utility in an SSE?

- 0
- $-1/3$
- $-1/2$
- $-2/3$

SECURITY GAMES: EXAMPLE



	Attacker		Defender	
Target	Covered	Uncovered	Covered	Uncovered
1	0	4	0	-2
2	0	3	0	-1
3	0	2	0	-5

Poll 3: What is the defender's utility in an SSE?

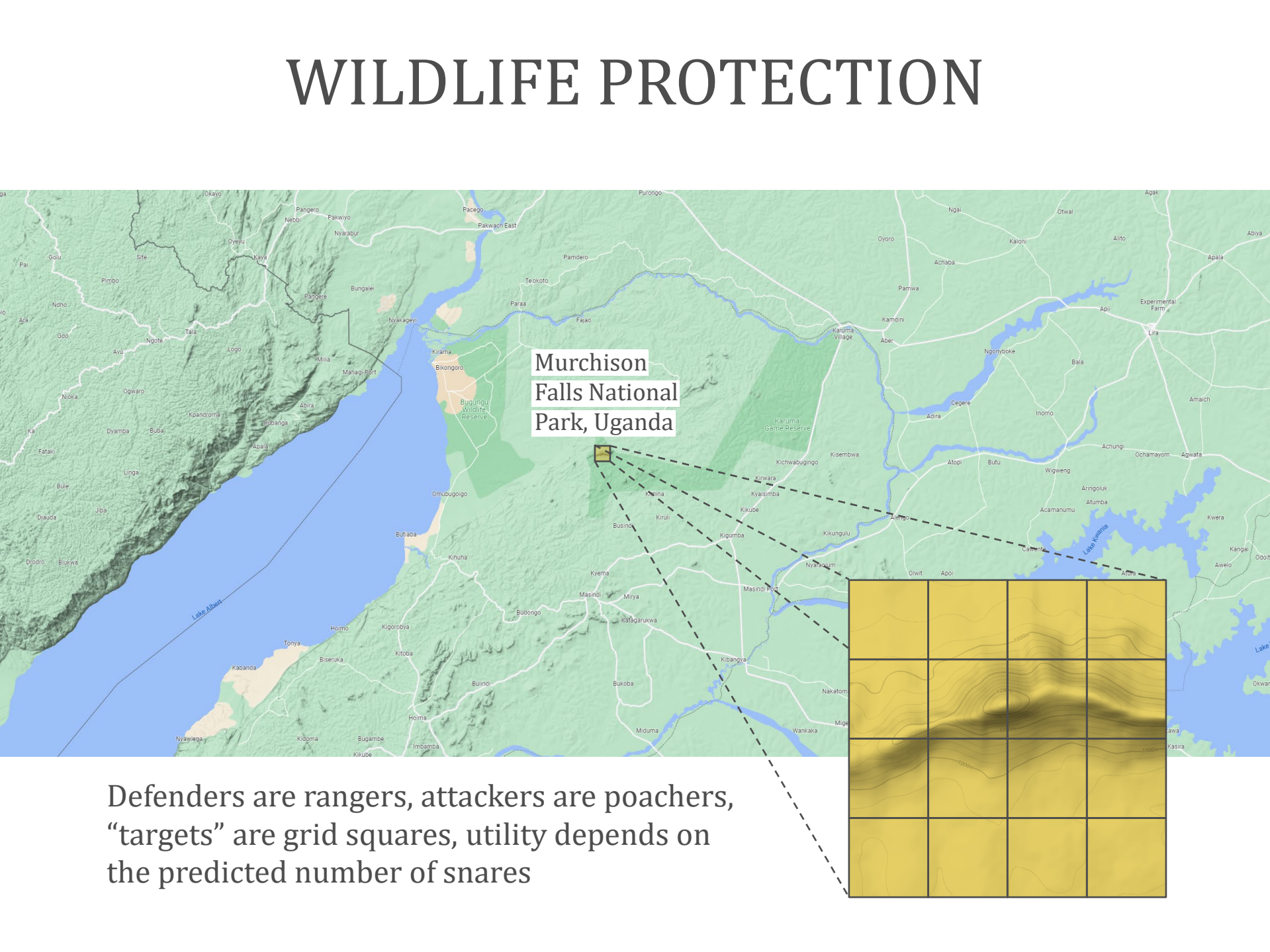
- $-3/7$
- $-4/7$
- $-3/4$
- $-4/3$

WILDLIFE PROTECTION

The image displays a topographic map of Murchison Falls National Park in Uganda. The park's boundary is outlined in black. A grid of dashed lines is overlaid on the map, with a small yellow square highlighting a specific area. A dashed line connects this yellow square to a larger, zoomed-in view of the same area in the bottom right corner. This zoomed-in view shows a 4x4 grid of yellow squares, with a black line indicating a path or boundary. The map includes various geographical features such as Lake Albert, Lake Kyoga, and Lake Kyoga, and is labeled with numerous place names and coordinates.

Defenders are rangers, attackers are poachers, “targets” are grid squares, utility depends on the predicted number of snares

WILDLIFE PROTECTION



Murchison Falls National Park, Uganda

Defenders are rangers, attackers are poachers, “targets” are grid squares, utility depends on the predicted number of snares

LIMITATIONS OF SECURITY GAMES



- **Poll 4 (brainstorm):** What are some of the gaps between the security games model and reality?

Sat, Jun 11, 2022

LOGIN

SUBSCRIBE FOR \$1 >

U.S. | World | Tech & Science | Culture | Autos | Rankings | Health | Life | Opinion | Experts | Education | Podcasts | Vantage Search 🔍

WORLD

Random Security: LAX's ARMOR System

BY **ANDREW MURR** ON 10/13/07 AT 11:32 AM EDT

SHARE



WORLD



Listen to this article now



Powered by Trinity Audio

00:00



02:28



1.0x

Security officials at Los Angeles International Airport now have a new weapon in their fight against terrorism: randomness. Anxious to thwart future terror attacks in the early stages while plotters are casing the airport, security patrols have begun using a computer program called ARMOR (Assistant for Randomized Monitoring of Routes) to make the placement of security checkpoints completely unpredictable. Now all airport security officials have to do is press a button labeled RANDOMIZE, and they can throw a sort of **digital cloak of invisibility** over where they place the cops' antiterror checkpoints on any given day.

THE DEBATE



Our Economic House Is on Fire

BY VERONIKA DOLAR

VS

The Fed Created the Next Recession

BY ALFIE MEEK



OPINION



I've Seen Kate Middleton With Her Children, She Doesn't Deserve Trolling

BY LULU SINCLAIR



WTO Cannot Continue as Barrier to COVID-19 Medicines

BY JOSEPH E. STIGLITZ AND LORI WALLACH



Zelensky is Betting Time is on Ukraine's Side

BY DANIEL R. DEPETRIS



MAGA Madness Was on Full Display at Jan. 6 Committee Hearing



Antipoaching patrols like this team at the Lewa Wildlife Conservancy in Kenya may soon use AI technology to stay one step ahead of criminals.

PHOTOGRAPH BY AMI VITALE, NATIONAL GEOGRAPHIC CREATIVE

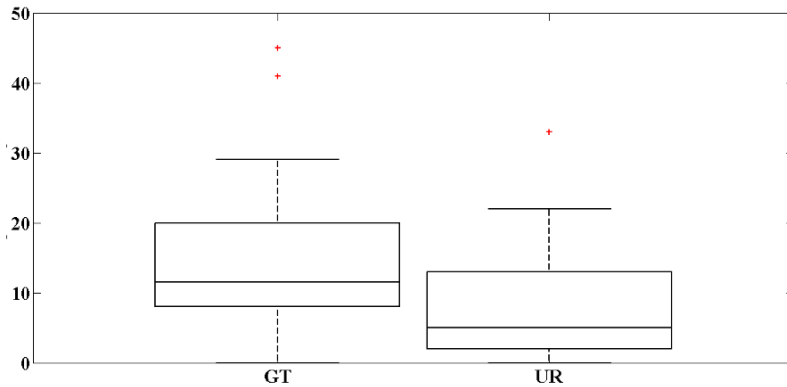
| WILDLIFE WATCH |

Rangers Use Artificial Intelligence to Fight Poachers

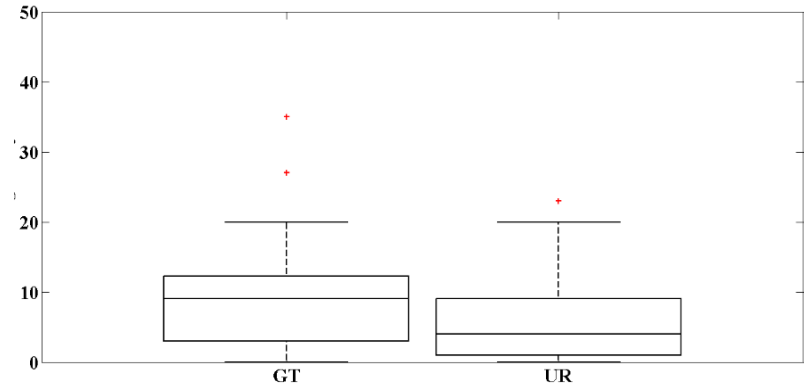
Emerging technology may help wildlife officials beat back traffickers.

PAWS, which stands for Protection Assistant for Wildlife Security, is a newly developed AI that takes data about previous poaching activities and outputs routes for patrols based on where poaching is likely to occur. These routes are also randomized to keep poachers from learning patrol patterns. Using machine learning, a branch of AI, PAWS can continually find new insights as more data is added.

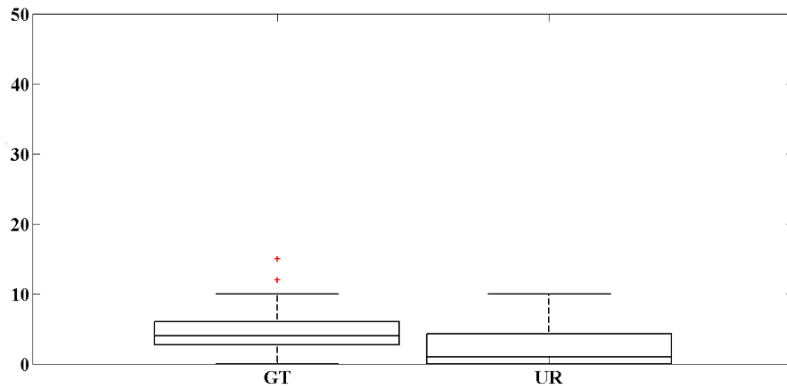
DOES THIS WORK?



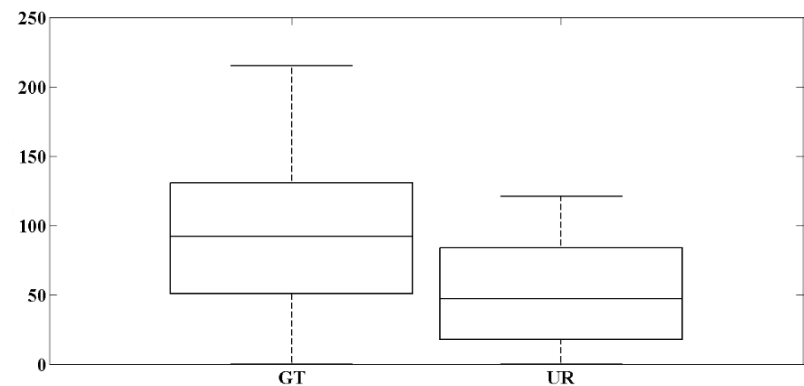
Captures (every 30 min.)



Warnings (every 30 min.)



Violations (every 30 min.)



Passengers (every 30 min.)

Game theory (GT) vs. uniform random (UR) in the LA metro
[Delle Fave et al., 2014]