Implementación de un enfoque basado en teoría de juegos para contrarrestar amenazas persistentes avanzadas

Diego Esteban Quintero Rey

Modelos Estocásticos y Simulación en Computación y Comunicaciones

Jorge Eduardo Ortiz Triviño (Profesor Asociado)
Universidad Nacional de Colombia

Artículo de referencia

PLOS ONE

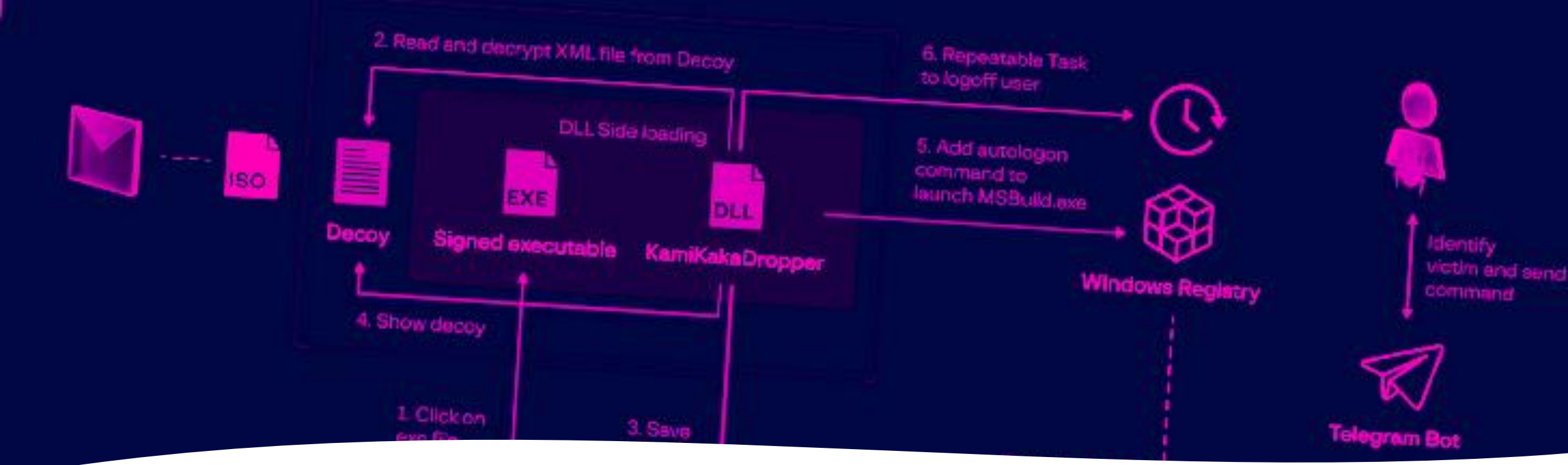
RESEARCH ARTICLE

Defending Against Advanced Persistent Threats Using Game-Theory

Stefan Rass[1]*, Sandra König[2], Stefan Schauer[2]

1 Universität Klagenfurt, Institute of Applied Informatics, Klagenfurt, Austria, **2** Austrian Institute of Technology, Safety & Security Department, Klagenfurt, Austria

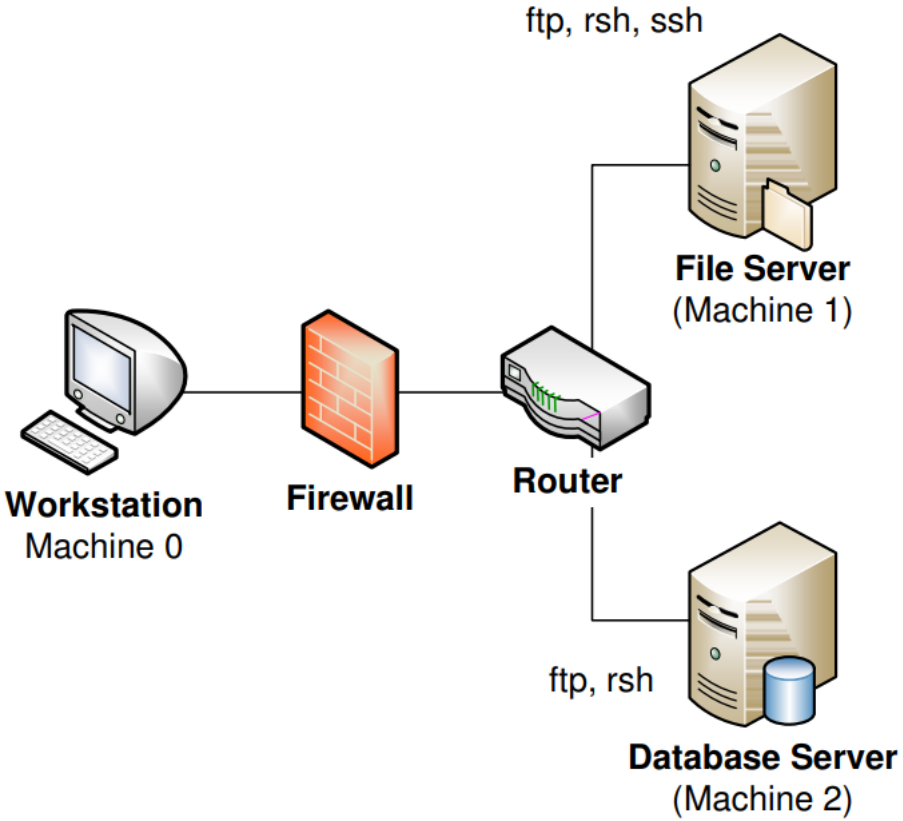
* stefan.rass@aau.at

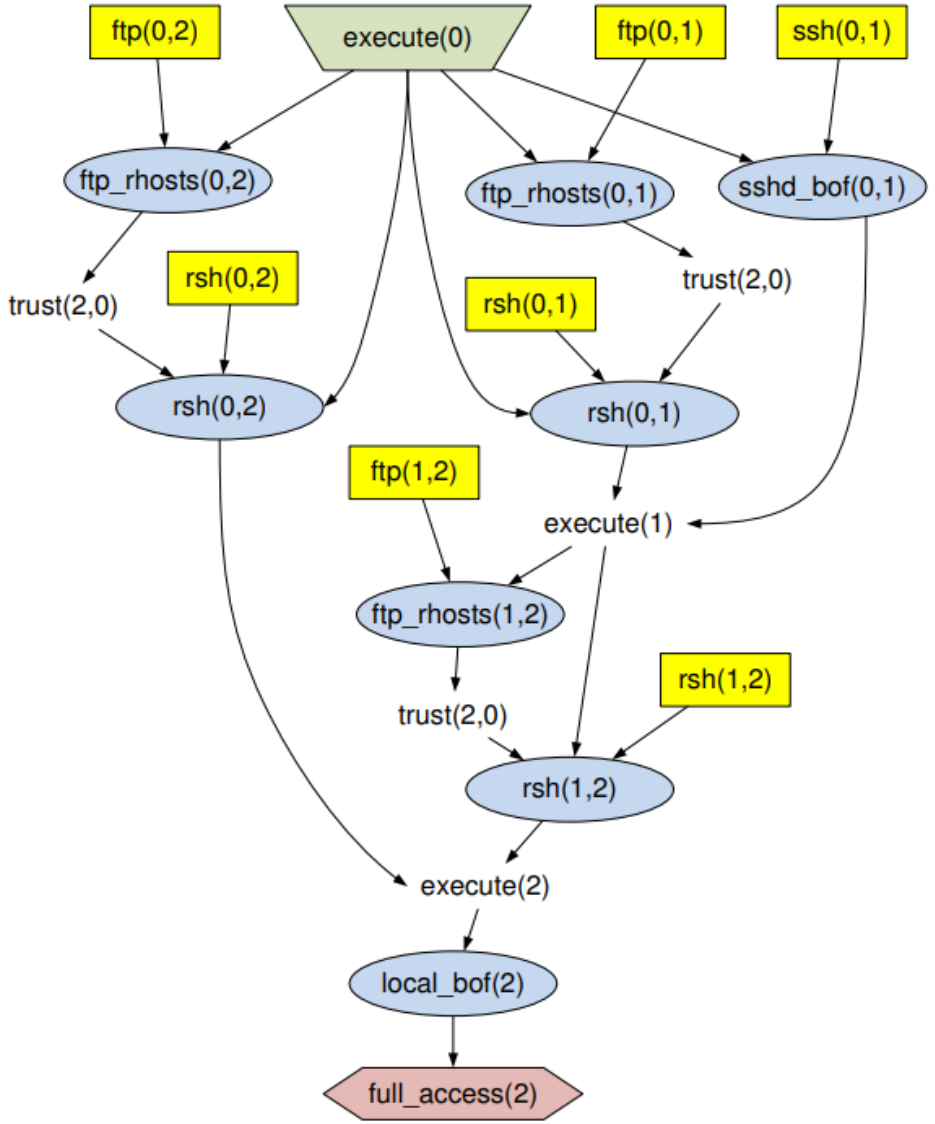


Amenaza Persistente Avanzada (APT)

Conjunto de procesos informáticos sigilosos orquestados por un tercero (organización, grupo delictivo, una empresa, un estado, ...) con la intención y la capacidad de atacar de forma avanzada (a través de múltiples vectores de ataque) y continuada en el tiempo, un objetivo determinado (empresa competidora, estado, ...).

Modelado de una APT



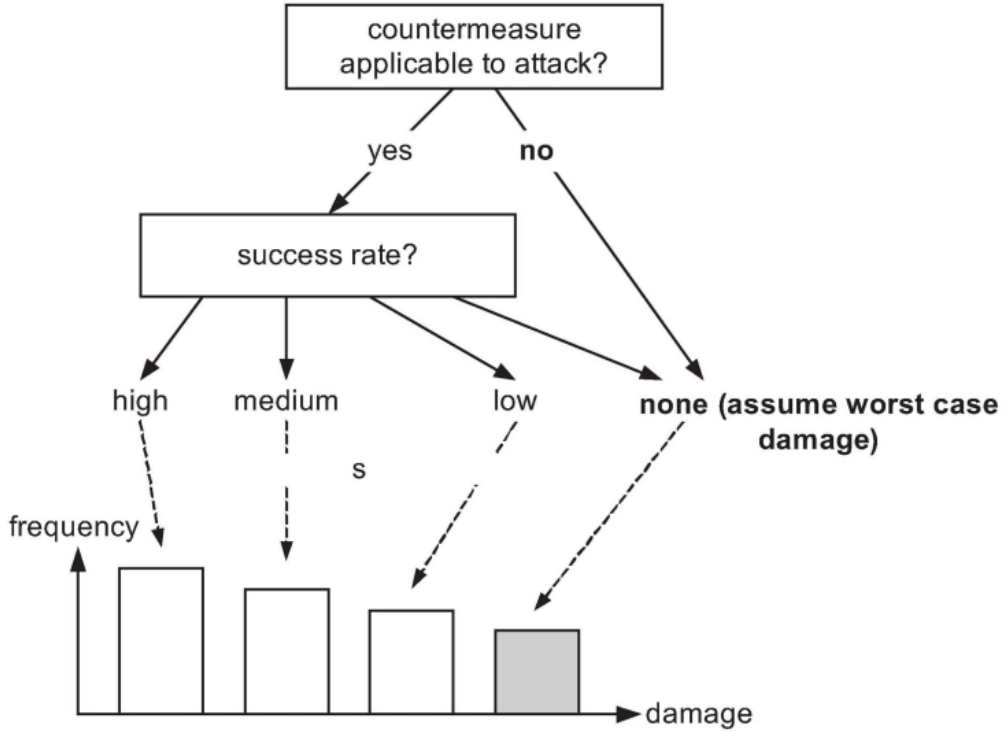


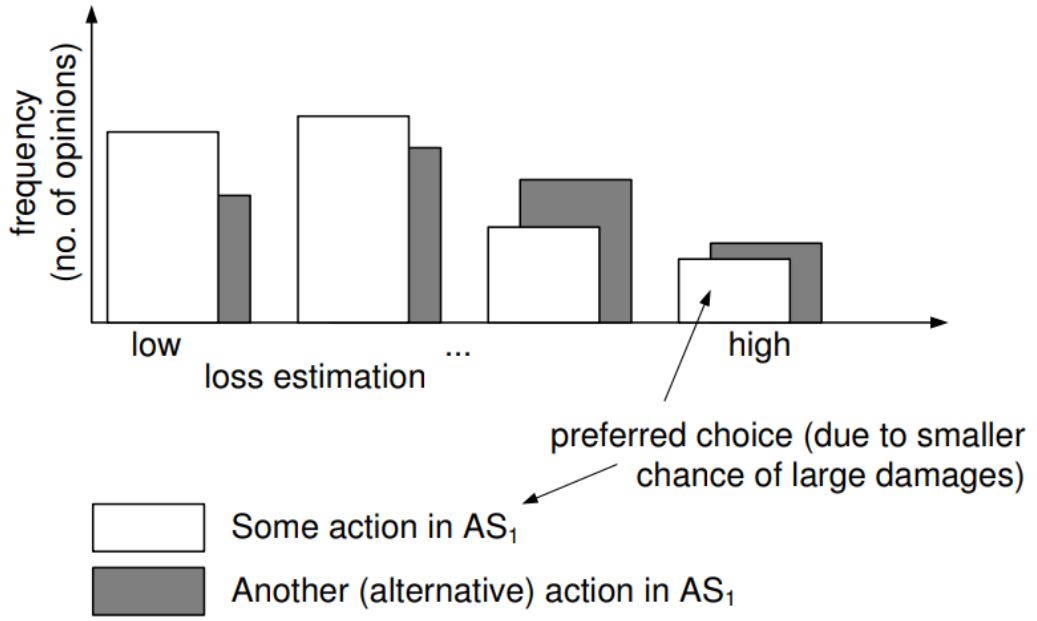
Modelado de una APT

Table 3. APT scenarios (adversary's action set AS_2, based on Fig 2)

1	execute(0) → ftp_rhosts(0,1) → rsh(0,1) → ftp_rhosts(1,2) → rsh(1,2) → local_bof(2) → full_access(2)
2	execute(0) → ftp_rhosts(0,1) → rsh(0,1) → rsh(1,2) → local_bof(2) → full_access(2)
3	execute(0) → ftp_rhosts(0,2) → rsh(0,2) → local_bof(2) → full_access(2)
4	execute(0) → rsh(0,1) → ftp_rhosts(1,2) → rsh(1,2) → local_bof(2) → full_access(2)
5	execute(0) → rsh(0,1) → rsh(1,2) → local_bof(2) → full_access(2)
6	execute(0) → rsh(0,2) → local_bof(2) → full_access(2)
7	execute(0) → sshd_bof(0,1) → ftp_rhosts(1,2) → rsh(1,2) → local_bof(2) → full_access(2)
8	execute(0) → sshd_bof(0,1) → rsh(1,2) → local_bof(2) → full_access(2)

Controles y la variable aleatoria pérdida L_{ij}





El juego APT

Table 4. Correspondence of Attack Trees/Graphs and Extensive Form Games.

Extensive form game	Attack tree/graph
start of the game	root of the tree/graph
stage of the gameplay	node in the tree/graph
allowed moves at each stage (for the adversary)	possible exploits at each node
end of the game	leaf node (attack target)
strategies	paths from the root to the leaf (= attack vectors)
information sets	uncertainty in the attacker's current position and move

doi:10.1371/journal.pone.0168675.t004

- Atacante: Invisible (Sigiloso, puede o no estar presente)
- Defensor: Omnisciente (Tiene acceso a todo el sistema)

Matriz del juego APT

AS_1 : controles → globales

AS_2 : ataques (caminos) → vectores de ataque (puntuales)

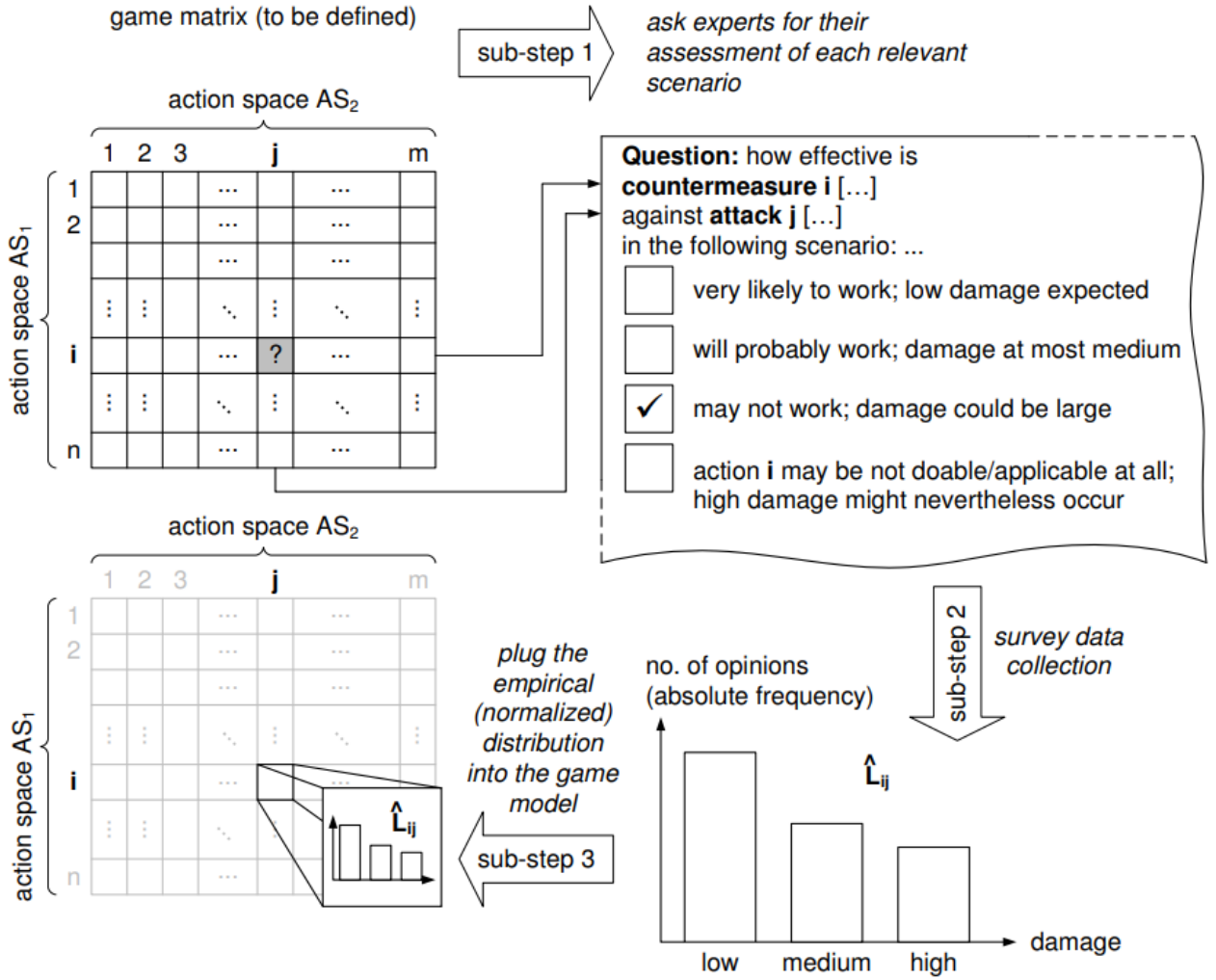
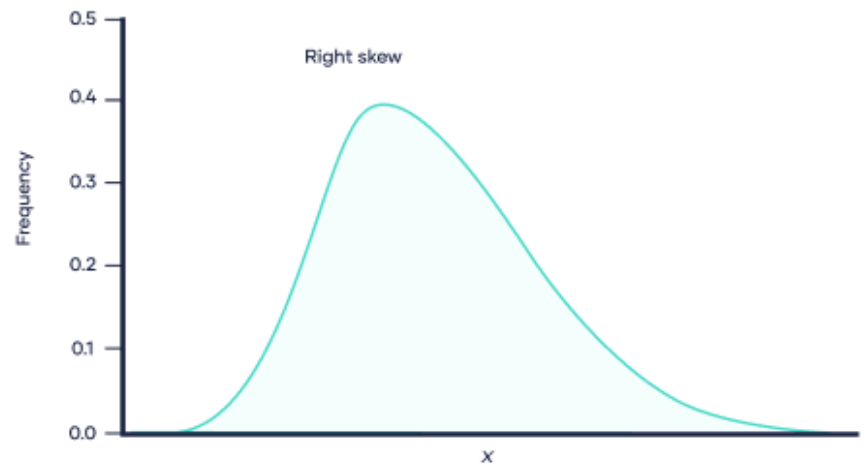


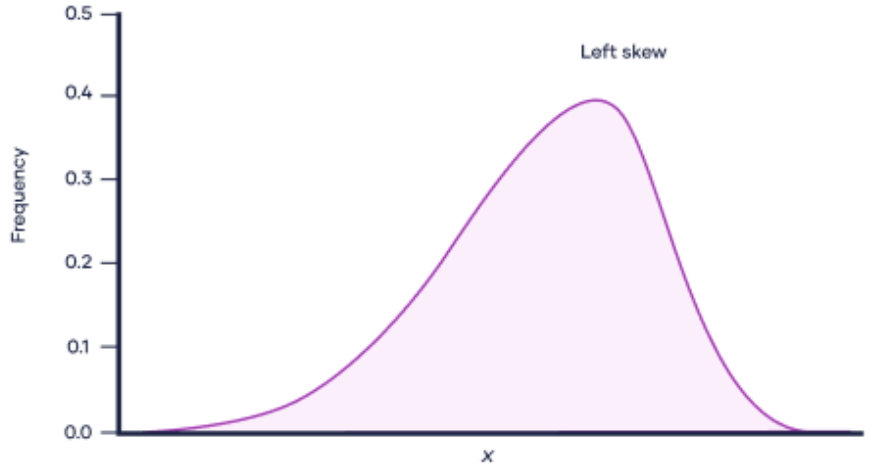
Fig. 7. Specification of an APT Game (Example Workflow Snapshot)

Objetivo de los jugadores

- Defensor: Escoger las defensas i que minimizan la pérdida L_{ij}
- Atacante: Escoger los ataques j que maximizan la pérdida L_{ij}



defensor



atacante

Suma cero: lo que uno pierde el otro lo gana

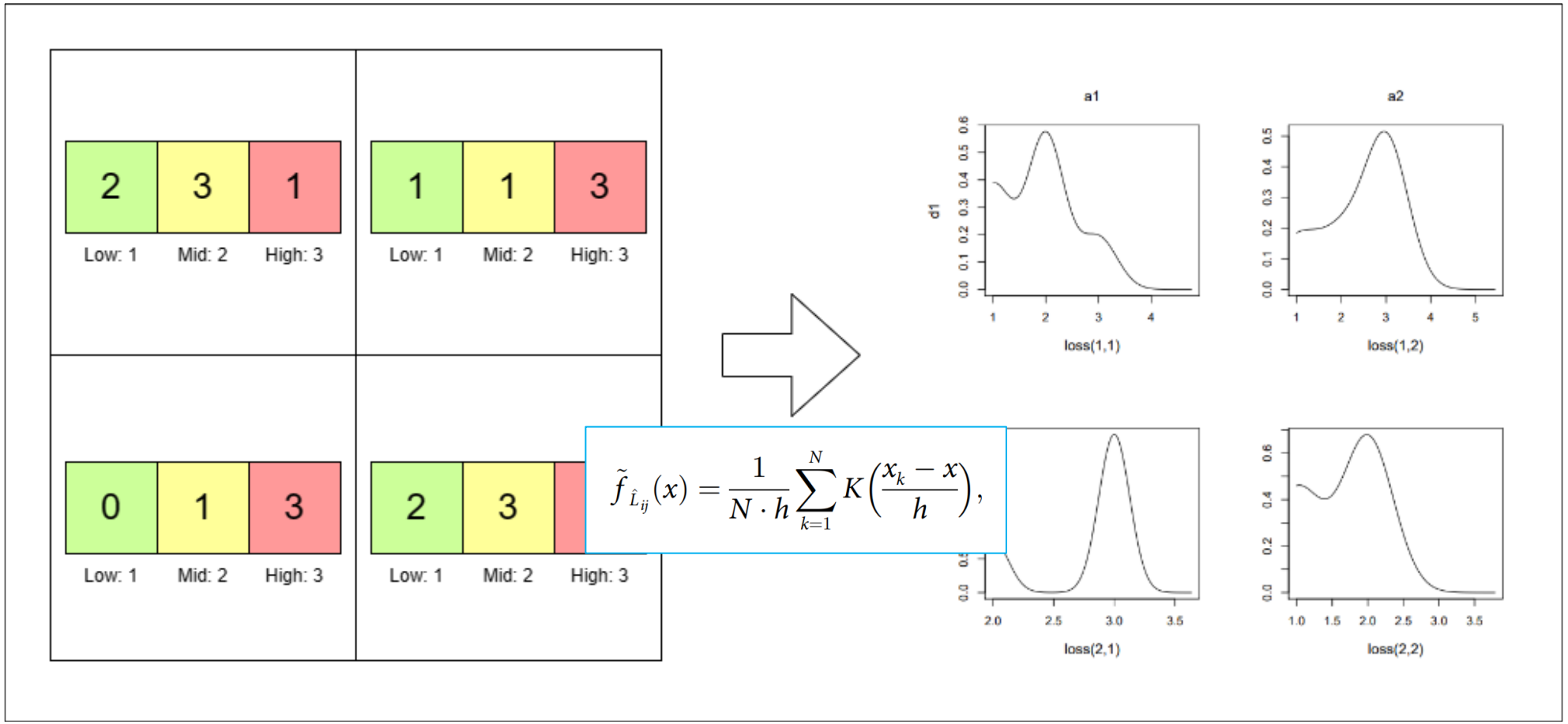
Cálculo del equilibrio y comparación de distribuciones

- El cálculo del equilibrio se hace con el algoritmo de juego ficticio.

- La matriz del juego es una matriz de distribuciones, no una matriz de números.

- Los autores encontraron que al comparar lexicográficamente las derivadas de las KDE de las distribuciones, se logra convergencia con juego ficticio y además se obtiene un orden de preferencia $\succcurlyeq$ donde $L_1 \succcurlyeq L_2$ si L_2 genera menos pérdidas

Frecuencias a KDEs



Derivadas de las KDEs y Serie de Taylor

$$f^{(k)}(x) = \frac{1}{N\sqrt{\pi}} \frac{(-1)^k}{(h \cdot \sqrt{2})^{k+1}} \times \sum_{j=1}^{n} \left[H_k\left(\frac{x - x_j}{h\sqrt{2}}\right) \cdot \exp\left(-\frac{(x - x_j)^2}{2h^2}\right) \right]$$

$$\tilde{f}_{\hat{L}_{ij}} \simeq \left((-1)^k f^{(k)}_{\hat{L}_{ij}}(a) \right)_{k=0}^{\infty} = (y_0, y_1, y_2, \ldots) \in \mathbb{R}^{\infty},$$

Pila de matrices de derivadas

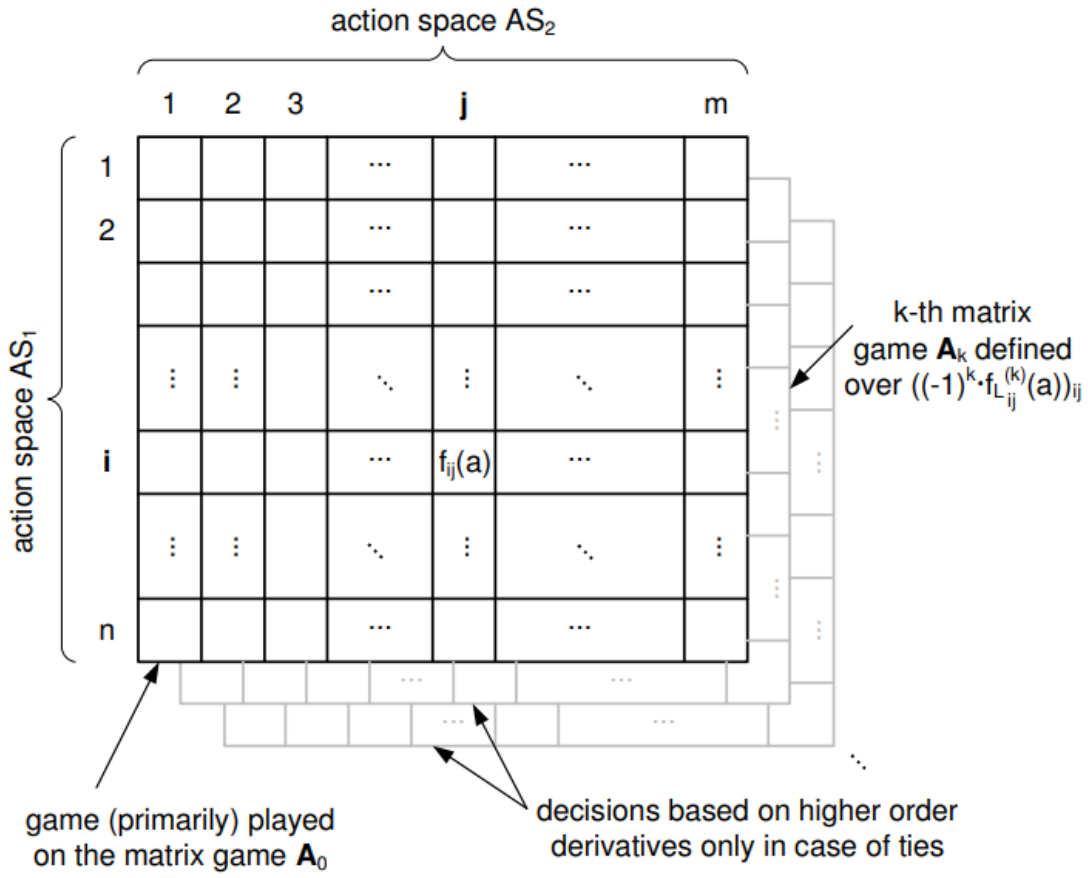


Fig. 8. Applying Fictitious Play

Juego Ficticio en “Paralelo”

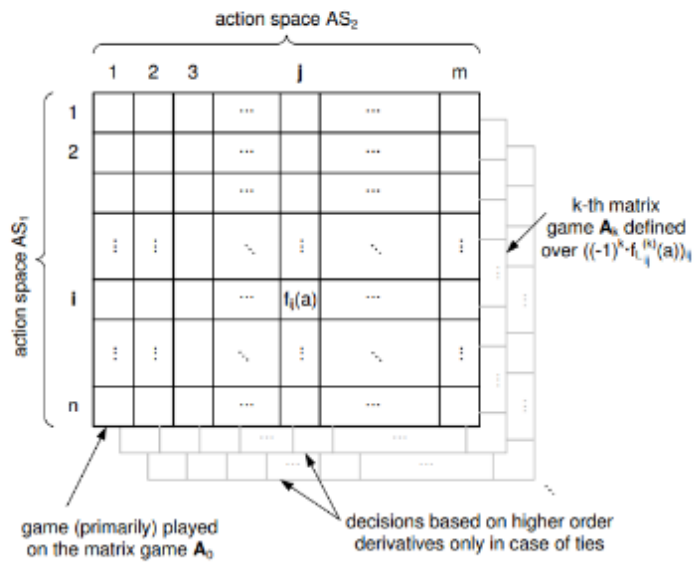
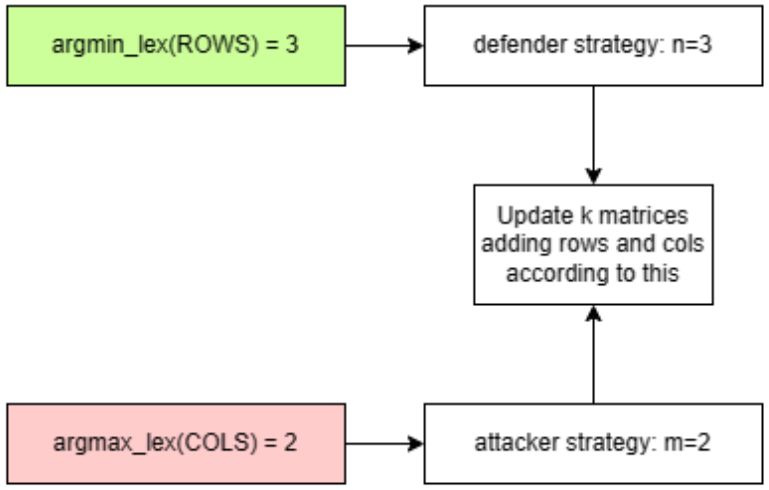


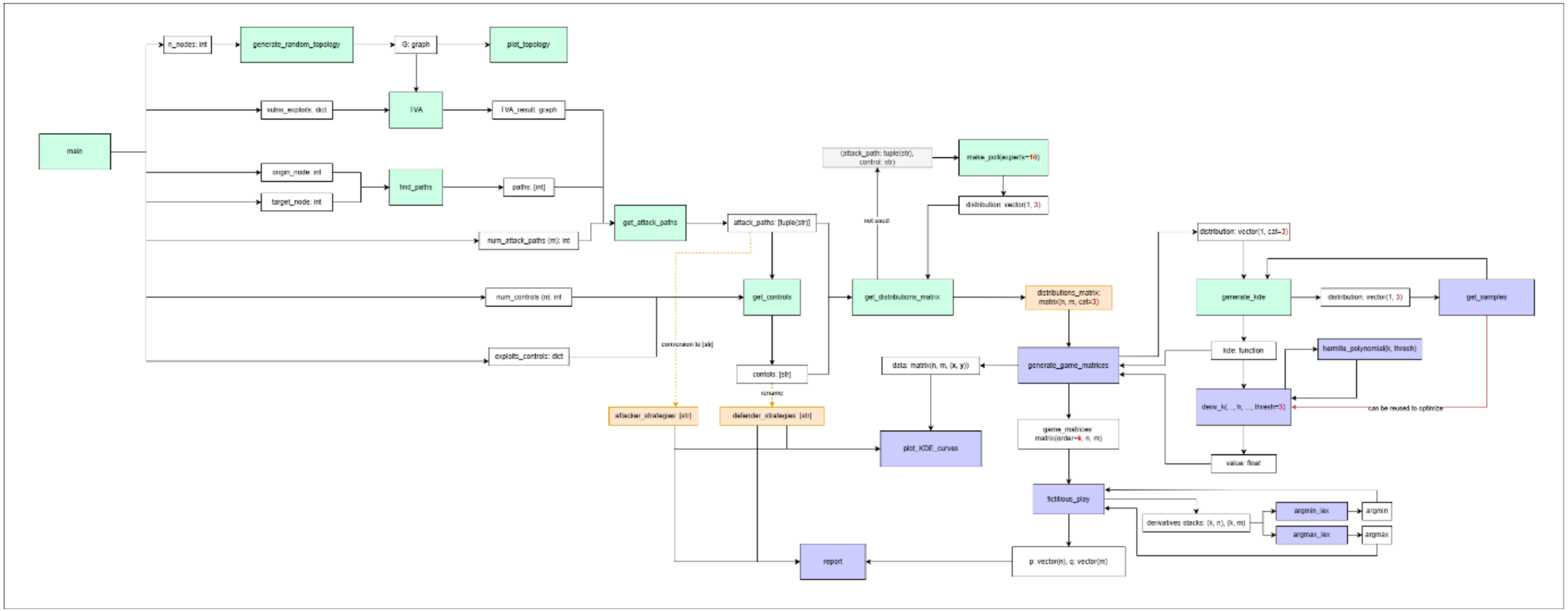
Fig. 8. Applying Fictitious Play

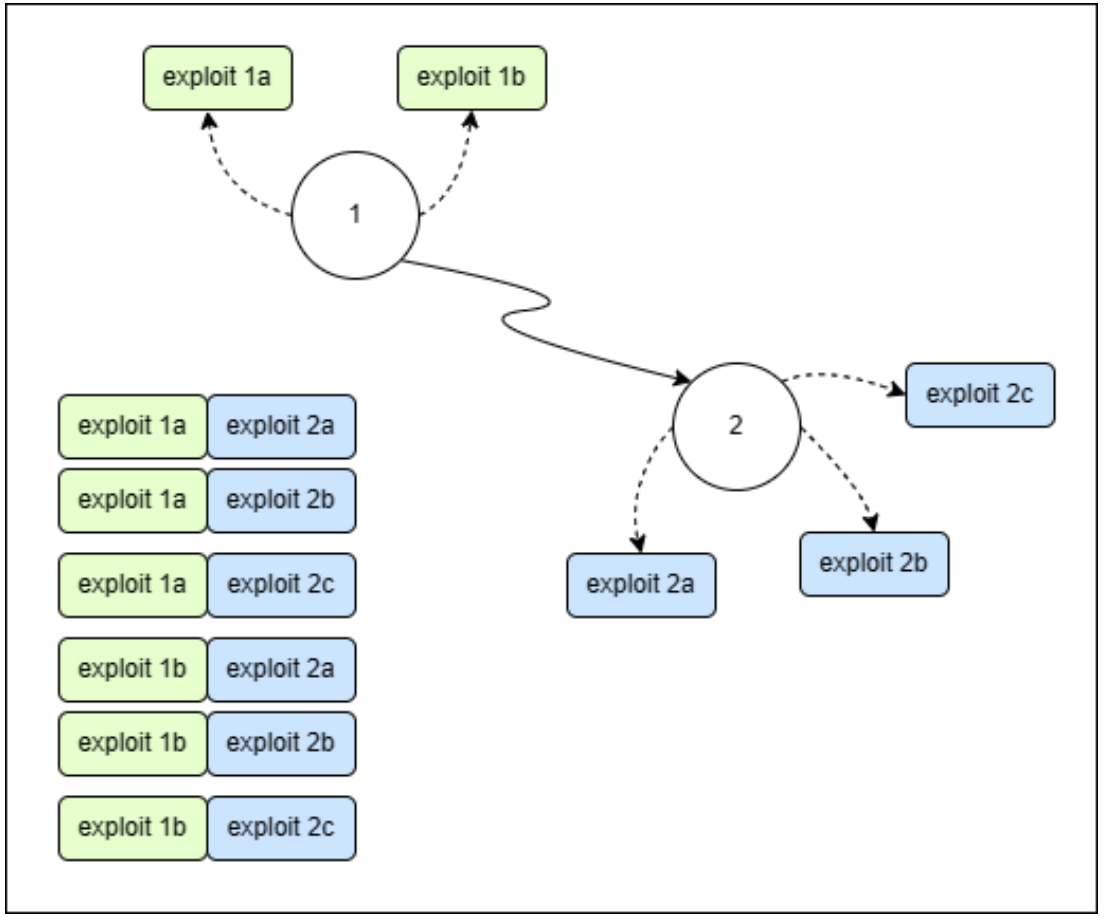
	1	2	3	n=4
k=0	3	3	3	4
k=1	4	6	2	5
k=2	5	7	1	6

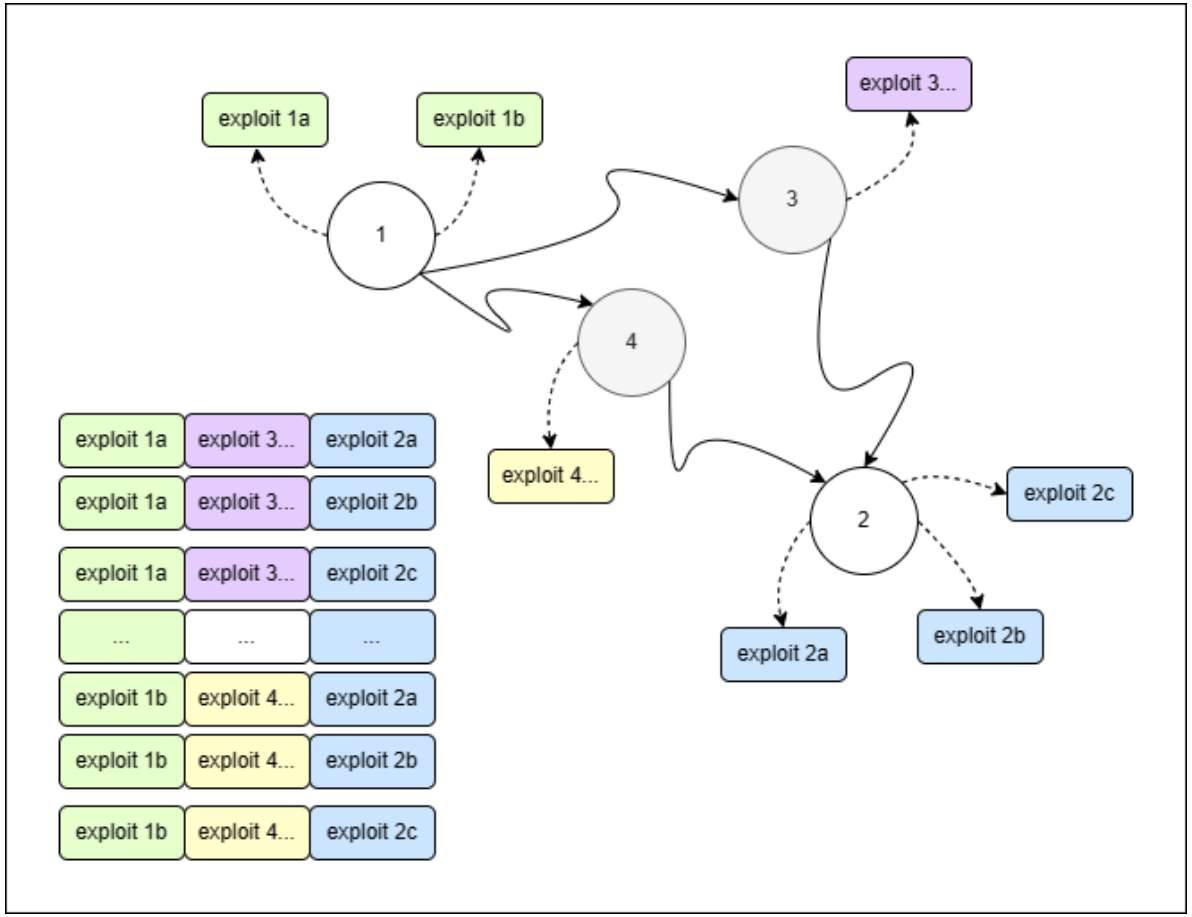
	1	2	3	m=4
k=0	1	2	2	2
k=1	2	5	5	4
k=2	4	8	7	4



Arquitectura de la solución







Complejidad en experimentos dependientes de la topología