Diego Esteban Quintero Rey
Modelos estocásticos y simulación en computación y comunicaciones
ME01
Proyecto Final: Implementación de un enfoque basado en teoría de juegos para contrarrestar amenazas persistentes avanzadas

MARCO TEÓRICO

AMENAZAS PERSISTENTES AVANZADAS Y TEORÍA DE JUEGOS

Las amenazas persistentes avanzadas (APTs) abarcan una variedad diversa de métodos de ataque, que van desde la ingeniería social hasta las explotaciones técnicas. La naturaleza variada y a menudo encubierta de las APTs plantea un desafío significativo para la seguridad práctica contemporánea del sistema. Esto se debe a que la información sobre los ataques, el estado actual del sistema o los motivos de los atacantes suele ser poco clara, incierta y, en ocasiones, completamente indisponible.

La teoría de juegos emerge como un marco natural para modelar el conflicto entre atacantes y defensores. Este estudio explora una clase generalizada de juegos de matriz como una herramienta para mitigar riesgos en la defensa contra amenazas persistentes avanzadas (APTs). A diferencia de la teoría de juegos y decisiones tradicional, nuestro modelo está diseñado específicamente para capturar y gestionar la completa incertidumbre inherente a las APTs. Esto incluye factores como desacuerdos entre evaluaciones de riesgos cualitativas de expertos, motivos adversarios desconocidos e incertidumbre sobre el estado actual del sistema (como la profundidad de la penetración del atacante en las capas protectoras del sistema).

En términos prácticos, los modelos de APT basados en la teoría de juegos pueden derivarse directamente de análisis de vulnerabilidad topológica, junto con evaluaciones de riesgos siguiendo estándares comunes como la familia ISO 31000. Teóricamente, estos modelos presentan propiedades distintas en comparación con los modelos clásicos de teoría de juegos. La solución técnica presentada en este trabajo puede tener significado independiente en el campo.

DESAFÍOS PARA CONTRARRESTAR AMENAZAS PERSISTENTES AVANZADAS

La creciente diversidad, conectividad y apertura de los sistemas de información actuales a menudo ofrecen a los ciberatacantes numerosas vías para infiltrarse en un sistema. Las medidas de seguridad actuales suelen depender de herramientas y técnicas semiautomáticas, como el análisis de vulnerabilidad topológica (TVA), para identificar y abordar vulnerabilidades. Sin embargo, este progreso se acompaña de la evolución simultánea y mejora de ataques relacionados. Las Amenazas Persistentes Avanzadas (APTs) se adaptan naturalmente a la creciente diversidad de medidas de seguridad ejecutando ataques sigilosos y diversos, con el objetivo de permanecer "bajo el radar" hasta que el sistema objetivo haya sido infiltrado, infectado y sea vulnerable al ataque previsto. Las contramedidas pueden ser demasiado tarde para ser efectivas una vez que se detecta el ataque, ya que el daño ya ha ocurrido.

Mitigar las APTs a menudo no es solo cuestión de precauciones técnicas, sino también de combatir a un oponente invisible e influencias externas en el sistema, principalmente debido a que la APT permanece oculta. Por lo tanto, la efectividad de cualquier medida de seguridad depende del estado actual del sistema y de cuán avanzada haya llegado a ser la APT. El aspecto económico se vuelve particularmente desafiante e incierto, ya que cuantificar el rendimiento de las inversiones en seguridad es casi imposible teniendo en cuenta diversos factores fuera de la influencia del oficial de seguridad.

AVANCES EN EL ESTUDIO DE LAS AMENAZAS PERSISTENTES AVANZADAS

En la última década, ha habido un rápido aumento en las Amenazas Persistentes Avanzadas (APTs), con numerosos incidentes de seguridad relacionados informados a nivel mundial. Una razón principal de este incremento es que las APTs no se centran en una única vulnerabilidad en un sistema, lo que facilitaría la detección y eliminación. En cambio, explotan una cadena de vulnerabilidades en diferentes sistemas para acceder a áreas de alta seguridad dentro de la red de una empresa. Los adversarios aprovechan la importancia de la protección perimetral, facilitando el movimiento dentro de la infraestructura de manera inadvertida. Superar la protección perimetral mediante ingeniería social, malware o siendo transportado inadvertidamente por personas legítimas (el problema del "trae tu propio dispositivo") son métodos comunes para vulnerar la seguridad.

Una vez que se ha violado el perímetro, los ataques internos se convierten en una amenaza aún mayor. Existen pautas para asegurar áreas internas, como la zona desmilitarizada (DMZ), pero la intensidad de la vigilancia es limitada. Herramientas especializadas para la detección o prevención de intrusiones requieren una administración y recursos humanos significativos. Las APTs emplean una combinación de métodos de ataque adaptados a la organización específica, la infraestructura de la red de TI y las medidas de seguridad existentes. La ingeniería social, especialmente en las etapas iniciales, permite a los atacantes eludir medidas técnicas como sistemas de detección y prevención de intrusiones, penetrando eficientemente la protección externa de la red de TI. Ataques APT prominentes, como Stuxnet en 2008, Operation Aurora, Shady Rat, Red October o MiniDuke, se han divulgado públicamente.

La detección de ataques APT ha sido objeto de una extensa investigación. Si bien las herramientas de protección perimetral pueden fallar ocasionalmente, se han explorado métodos de detección de anomalías, analizando archivos de registro recopilados de toda la red. Sin embargo, la detección de eventos excepcionales en los archivos de registro por sí sola es insuficiente, ya que a menudo las anomalías solo se hacen evidentes cuando los eventos se correlacionan. La naturaleza interconectada de los sistemas actuales y el sustancial intercambio de datos dificultan la evaluación de los archivos de registro.

Una herramienta como AECID (Correlación Automática de Eventos para la Detección de Incidentes) aplica listas blancas y monitorea eventos del sistema para detectar comportamientos anómalos. Nuestro enfoque es preventivo, estimando y minimizando el riesgo de un APT exitoso desde el principio. Se aplica la teoría de juegos para optimizar la defensa contra un invasor sigiloso, considerando un conjunto de rutas conocidas y la protección simultánea por parte del defensor. La falta y asimetría de información en los escenarios de ciberseguridad son desafíos abordados por modelos de teoría de juegos. El tiempo discreto para el defensor y el tiempo continuo para el atacante es un aspecto novedoso considerado en este trabajo, utilizando juegos de matriz para tener en cuenta resultados que dependen de acciones tomadas en diferentes momentos. Los modelos empíricos de teoría de juegos, que caen en la categoría de este trabajo, abordan la falta de comprensión y la dependencia de datos cualitativos o simulados para instanciar modelos de APT.

EL ENFOQUE PROPUESTO POR STEFAN RASS, SANDRA KÖNIG Y STEFAN SCHAUER

Los autores presentan un enfoque novedoso para capturar la incertidumbre en las ganancias dentro de modelos de teoría de juegos. Su desviación de los juegos estándar radica en medir los resultados del juego no en términos precisos, sino más bien como objetos de distribución de probabilidad completos. Esencialmente, la teoría de juegos se juega dentro del espacio abstracto de distribuciones por varias razones:

1. *Dificultad para Especificar Pérdidas y Ganancias:* Cuantificar los resultados de la defensa ante un ataque a menudo es un desafío para los jugadores. Surge la pregunta: ¿Se debe medir el número de máquinas infectadas o se debe considerar la pérdida monetaria? Las escalas categóricas tradicionales, como las utilizadas en los estándares de cuantificación de riesgos, presentan desafíos. Su enfoque permite que el juego sea definido por cualquier resultado ordenable, brindando flexibilidad.

2. *Asimetría en la Información del Jugador:* Los jugadores a menudo tienen información dispar. La estructura del juego en sí no es conocimiento común, y la jugabilidad varía para ambos jugadores, ya que los movimientos no son mutuamente observables y no ocurren simultáneamente.

3. *Compatibilidad con Procesos de Gestión de Riesgos:* Los modelos de teoría de juegos deben alinearse con los procesos de gestión de riesgos, abarcando la mitigación de APT. Sus juegos de APT están diseñados para ser compatibles con estos flujos de trabajo.

4. *Simplicidad del Modelo:* Mientras que los modelos estocásticos convencionales utilizan juegos bayesianos para capturar la incertidumbre, a menudo requieren especificar múltiples estructuras de juego posibles, complicando las cosas. Su enfoque trabaja directamente con datos empíricos, manteniendo los modelos de juego simples.

Centrándose en resultados evaluados cualitativamente que pueden ser aleatorios, su pregunta central aborda el razonamiento bajo incertidumbre: Dadas las acciones potenciales, ¿cuál es la mejor opción si las consecuencias de una acción son intrínsecamente aleatorias? Demuestran cómo responder a esta pregunta modelando la aleatoriedad a través de distribuciones de probabilidad para los resultados. A diferencia de la optimización típica que maximiza una cantidad numérica derivada de la distribución de una variable aleatoria X, sus juegos optimizan la forma de la distribución en sí.

Para ilustrar estos conceptos, se puede considerar el ejemplo de la toma de decisiones con respecto a la protección de los derechos de propiedad intelectual (DPI). El robo de DPI puede desencadenar un APT. En este escenario, la elección óptima no es evidente debido a consecuencias imprevisibles. Proponen una relación de orden para determinar la pérdida menos probable de propiedad intelectual, permitiéndoles calcular de manera algorítmica la mejor opción entre las opciones disponibles.

ANÁLISIS DE VULNERABILIDADES TOPOLÓGICO

El análisis de vulnerabilidad topológica consiste en identificar sistemáticamente posibles ataques a un sistema mediante el análisis de su estructura, especialmente su topología de red. Este proceso generalmente implica crear una visión integral de la infraestructura, incorporando todos los detalles disponibles sobre sus componentes. Al modelar la topología del sistema como un grafo (no dirigido) $G(V, E)$ con un nodo objetivo especificado $v_0 \in V$, se pueden emplear algoritmos estándar de búsqueda de caminos para encontrar rutas desde el exterior de G hasta el nodo objetivo v_0. Una vez que el AVT revela la estructura, surge una pregunta crucial sobre la aplicación de patrones de ataque conocidos al modelo de infraestructura, de manera análoga a la búsqueda de patrones de virus en el software. Las técnicas de coincidencia de grafos surgen como una herramienta intrigante en este contexto.

Las vulnerabilidades o exploits asociados con los nodos en V, ya sean conocidos o sospechosos, determinan qué rutas teóricamente permiten el acceso a v_0 para atacar exitosamente el sistema. Estas rutas de ataque consisten en secuencias de vulnerabilidades, complementadas con las respectivas condiciones necesarias para explotar una vulnerabilidad, y representan el resultado principal de un AVT. Desde una perspectiva ligeramente simplificada, se puede percibir una Amenaza Persistente Avanzada (APT) como la totalidad de estas rutas de ataque, ejecutadas físicamente al avanzar secuencialmente a lo largo de una ruta elegida para evitar la detección en todas las etapas (permaneciendo sigilosa). Es

importante destacar que los riesgos prácticos provienen de la explotación de vulnerabilidades aún no conocidas, comúnmente denominadas exploits de día cero.

La incertidumbre sobre estas vulnerabilidades surge en parte debido a la naturaleza intrincada de la red, lo que hace que las medidas de entropía del grafo sean una herramienta potencial para cuantificar la probabilidad de que ocurran ataques a través de rutas pasadas por alto durante el análisis. Gestionar efectivamente este riesgo residual a menudo implica aprovechar el conocimiento del dominio, recopilar opiniones de expertos, basarse en la experiencia y la minería de información, en combinación con modelos matemáticos adecuados.

GRAFOS DE ATAQUE Y ÁRBOLES DE ATAQUE

El grafo de ataque, que abarca todas las vías de acceso a un sistema, incluyendo intersecciones y rutas alternativas en los caminos de ataque, constituye una representación conocida como el grafo de ataque. Este grafo es una representación basada en la topología del sistema G, donde los enlaces salientes de un nodo v se mantienen solo si un exploit específico en v facilita el acceso al vecino de v. Es esencial diferenciar un grafo de ataque de un árbol de ataque en términos de representación. Un árbol de ataque, a menudo un árbol AND/OR, representa posibles cadenas de exploits de una manera diferente. Sin embargo, independientemente de su disponibilidad, el punto focal de interés para este contexto es el conjunto de caminos de ataque, que corresponde directamente al conjunto de acciones del jugador 2 en los juegos de APT.

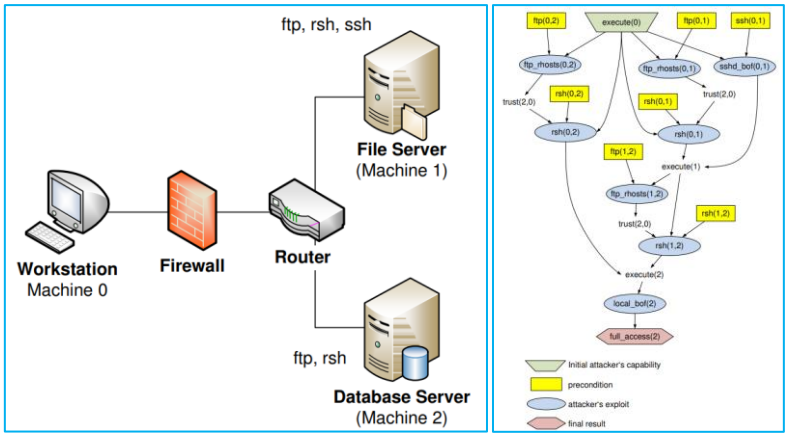

Figura 1 - Topología de un sistema (izquierda) y un grafo de ataque (derecha) para un par de nodos

JUEGOS EN FORMA EXTENSIVA

Al desarrollar un modelo de teoría de juegos para Amenazas Persistentes Avanzadas (APTs), se emplea un enfoque que utiliza juegos de forma extensiva (EFGs, por sus siglas en inglés). Aunque la definición formal de EFG es intrincada, una breve descripción destaca su semejanza con las APTs. Formalmente, los EFGs se representan mediante un árbol $T(V_T, E_T)$ con un nodo raíz designado que simboliza el punto de inicio del juego. En el contexto de las APTs, la raíz corresponde a un punto hipotético que representa el exterior del grafo de red G. El EFG involucra a dos jugadores y un jugador hipotético llamado "chance", que representa movimientos aleatorios. Cada nodo $v \in V_T$ en el árbol del juego lleva información sobre el jugador que está realizando un movimiento en ese momento, con movimientos indistinguibles recopilados en el conjunto de información del jugador, reflejando la incertidumbre desde la perspectiva del oponente. En un modelo de APT, los conjuntos de información

corresponderían a ubicaciones potenciales donde podría estar el atacante sigiloso. El EFG se completa asignando vectores de resultados a los nodos hoja en el árbol del juego.

Al ver una APT como un EFG, se vuelve necesario especificar los daños y las ganancias para el adversario al alcanzar el nodo objetivo v_0. Sin embargo, determinar la ganancia del adversario presenta desafíos prácticos debido a la incertidumbre causada no solo por los movimientos del atacante sino también por influencias externas. Declarar esta incertidumbre en el nodo de "chance" en la descripción del EFG se considera inviable, dada su dependencia de las acciones y movimientos de ambos jugadores.

Dada la naturaleza de información imperfecta de los EFGs, definir conjuntos de información se vuelve desafiante, especialmente cuando los jugadores tienen conocimientos diferentes sobre la etapa actual del juego. Describir estas hipótesis implica distribuciones de probabilidad en conjuntos de información, a menudo disponibles en términos cualitativos como "bajo", "medio" o "alto" riesgo.

Para abordar estos desafíos, se propone reemplazar las ganancias del atacante con las pérdidas del defensor, asumiendo una competencia de suma cero. Este enfoque busca superar las incertidumbres en las ganancias al enmarcar el juego como un evento único, donde ambos jugadores eligen estrategias y las ganancias se determinan por esas elecciones. En este contexto, una APT se modela como un juego con información completa pero con ganancias inciertas, representadas como distribuciones de probabilidad completas en lugar de números específicos.

MODELADO DE LA INCERTIDUMBRE PARA LA TOMA DE DECISIONES

En la búsqueda de modelar la incertidumbre para el soporte de decisiones, el enfoque implica lidiar con resultados inciertos o incluso aleatorios de las acciones. El método propuesto consiste en recopilar datos disponibles y opiniones de expertos, entre otra información, para luego construir una distribución de probabilidad basada en estos datos y encapsular la incertidumbre en las evaluaciones. Aunque esto preserva toda la información disponible en el objeto de distribución, el proceso de trabajar con ello se vuelve más intrincado, representando una contribución técnica central en este trabajo.

En casos en los que las evaluaciones están consistentemente alineadas, se puede definir un representante razonable, como la evaluación promedio. Sin embargo, en otros casos, la distribución podría ser multimodal, indicando diversas respuestas plausibles con sus propias justificaciones. Encontrar la mejor acción generalmente implica asignar valores de utilidad a las acciones y buscar la utilidad máxima tanto para el defensor como para el atacante.

La gestión cuantitativa de riesgos a menudo emplea el daño esperado como valor de utilidad, calculado como el producto del daño y la probabilidad. Sin embargo, esta convención tiene limitaciones, ya que la media no proporciona información sobre posibles variaciones. La introducción de la varianza como el siguiente valor natural ayuda a abordar esta limitación. Una distribución puede describirse con mayor precisión utilizando más momentos.

Una representación que involucra una secuencia de momentos como un número hiperreal permite una "ordenación natural" en las distribuciones, existiendo en el espacio hiperreal $(*\mathbb{R}, \leq)$. Este enfoque dota al modelo de una aritmética completa aplicable a distribuciones aleatorias de pagos y una ordenación estocástica, facilitando la definición de "optimalidad" de decisiones.

Es fundamental reconocer de dónde provienen estas distribuciones de pérdidas. El grafo de ataque, que describe todos los escenarios de APT y se trata como una descripción de juego EFG, se convierte en la forma normal del juego, una matriz. La matriz de variables aleatorias describe los resultados en el juego APT, donde cada variable representa la pérdida aleatoria al tomar una estrategia de mitigación en relación con el movimiento desconocido del adversario.

La Sección 4.2 de [1] discute la decisión práctica de las preferencias $\succcurlyeq$.Si la distribución de pérdida es continua, diversas distribuciones de gestión de riesgos como la distribución de valores extremos o la distribución estable pueden aproximarse definiendo un umbral de aceptación de riesgos. Si L_1, L_2 tienen el mismo soporte compacto $[1, a] \subseteq \mathbb{R}$ y sus respectivas funciones de densidad son continuas, las preferencias pueden decidirse en función de las funciones de densidad de la variable aleatoria. Si la distribución es discreta, $\succcurlyeq$ se reduce a una ordenación lexicográfica cuando las pérdidas tienen distribuciones categóricas.

La Sección 4.3 de [1] aborda el significado práctico de las preferencias $\succcurlyeq$, concluyendo que $L_1 \succcurlyeq L_2$ si las grandes pérdidas son más probables bajo L_2 que bajo L_1. Una decisión $\succcurlyeq$-mínima minimiza las posibilidades de que ocurran grandes pérdidas. Esto concuerda con el enfoque de la gestión de riesgos en eventos extremos, destacando la naturaleza aversa al riesgo de la relación $\succcurlyeq$.

TOMA DE DECISIONES EN LA PRÁCTICA

Al abordar el ejemplo de mitigación de APT, la persona o entidad está considerando la implementación de medidas de seguridad persistentes, como firewalls adicionales, controles de acceso y protección física, como estrategia inicial. También se podrían contemplar modificaciones organizativas, como se discutió anteriormente. Sin embargo, la efectividad de estas medidas sigue siendo incierta, y la relación $\succcurlyeq$ se vuelve fundamental para navegar esta incertidumbre.

En un contexto general y abstracto, el proceso de toma de decisiones implica los siguientes pasos:

- Un conjunto de opciones (por ejemplo, precauciones de seguridad) representadas por $d_1, d_2, \ldots, d_n \in AS_1$ está disponible, cada una asociada con una consecuencia o efecto aleatorio capturado por pérdidas aleatorias $L_1, L_2, \ldots, L_n$.
- Identificar el mínimo $\succcurlyeq$ entre las distribuciones de $L_1, L_2, \ldots, L_n$ permite la selección de una decisión óptima en medio de la incertidumbre.

Un desafío constante es determinar la fuente de las pérdidas, un tema que se volverá a abordar varias veces en [1].

Los enfoques más simples para construir distribuciones de pérdidas que cumplen con la definición de pérdida aleatoria son:

- Recopilar datos disponibles y compilar una distribución empírica basada en ellos.
- Definir la distribución de pérdidas directamente según la experiencia, si es aplicable, por ejemplo, cuando la pérdida incurrida por una acción sigue una distribución conocida.

El último escenario es poco frecuente en situaciones prácticas, a menos que la amenaza específica haya sido estudiada extensamente (por ejemplo, distribuciones de valores extremos para la gestión de desastres o escenarios de valor en riesgo). En casos que involucran a un adversario racional como competidores comerciales o hackers, la inteligencia de amenazas y la experiencia desempeñan un papel fundamental en la medición de la pérdida. Las evaluaciones a menudo se realizan en términos cualitativos debido a los desafíos inherentes:

- El razonamiento humano tiende a ser no numérico, y los expertos pueden encontrar más conveniente proporcionar evaluaciones como "alto riesgo" en lugar de especificar cifras precisas.

- Dependiendo de datos estadísticos confiables, hay pocos tipos de incidentes disponibles y tener grandes cantidades de datos sobre ataques de APT en incidentes generales de ciberseguridad puede ser irrealista (y también indeseable si los incidentes se refieren a uno mismo).

En la práctica, la evaluación de acciones basada en sus resultados a menudo se basa en encuestas a expertos, donde las respuestas pueden tomar formas cualitativas. Agregar numerosas opiniones en una distribución empírica $\tilde{L}$ sobre el rendimiento de una precaución puede dar lugar a formas unimodales o multimodales, según el nivel de consenso o desacuerdo entre las opiniones. Independientemente del resultado, la relación de preferencia $\succcurlyeq$ proporciona un medio elegante para lidiar con este tipo de incertidumbre.

JUEGOS Y EQUILIBRIO

En el contexto de un escenario defensivo contra un ataque, donde las probabilidades de resultado están descritas por una distribución de probabilidad L_{ij}, y estas distribuciones están totalmente ordenadas según$\succcurlyeq$, la definición de juegos y equilibrios de matrices sigue un enfoque directo. Sin embargo, es importante señalar que los conceptos resultantes pueden no reflejar con precisión los equilibrios clásicos en todos los aspectos, como se detalla más adelante en esta discusión. Para mayor claridad, se presentan aquí conceptos y definiciones esenciales de la teoría clásica de juegos.

Consideremos los espacios de acción AS_1 y AS_2 para los jugadores 1 y 2, respectivamente, con cardinalidades n y m. Sea $A = \left(L_{ij}\right)^{n,m}$ una matriz de variables aleatorias, todas soportadas en el mismo conjunto compacto $\Omega = [1, a]$ Sea F_{ij} la función de distribución de la pérdida aleatoria L_{ij}.

En cada ronda del juego, el resultado aleatorio R depende de las acciones elegidas por el jugador 1 y el jugador 2, con una distribución $R \sim L_{ij}$ si el jugador 1 elige la acción $i \in AS_1$ y el jugador 2 elige la acción $j \in AS_2$.

Las reglas de elección aleatoria $p = (p_1, \ldots, p_n) \in S(AS_1)$ y $q = (q_1, \ldots, q_n) \in S(AS_2)$ describen las probabilidades de las acciones tomadas por cada jugador. En este caso, el resultado aleatorio tiene una distribución $R \sim F(p, q)$ calculada a partir de la ley de probabilidad total.

El objetivo del juego no es maximizar los ingresos promedio, como en la teoría de juegos tradicional, sino dar forma de manera óptima a la distribución de resultados $F(p, q)$ hacia la $\succcurlyeq$-minimalidad. En una competencia de suma cero, los jugadores buscan elegir acciones para minimizar/maximizar la probabilidad de eventos extremos. El jugador 1 busca desplazar la masa de la distribución hacia daños menores, mientras que el jugador 2 se esfuerza por poner más probabilidad en daños mayores. Este proceso técnico se alinea con nuestras estrategias de mitigación de riesgos APT basadas en la teoría de juegos, que logran una optimalidad similar a un equilibrio de Nash lexicográfico. En el caso unidimensional, esto es equivalente a un equilibrio de Nash estándar.

Similar a los equilibrios estándar, un equilibrio lexicográfico penaliza desviaciones unilaterales, pero abre la puerta para que el segundo jugador mejore sus ingresos en otro objetivo. Los hechos teóricos sobre equilibrios de Nash de valores reales se extienden a términos hiperreales a través del principio de transferencia. Sin embargo, surgen diferencias prácticas en términos de computabilidad, ya que las defensas obtenidas algorítmicamente en juegos sobre distribuciones de pérdidas se derivan de equilibrios lexicográficos. La distinción entre equilibrios de Nash estándar y equilibrios de Nash lexicográficos es crucial.

Para juegos estándar, el valor del punto de silla $V(A)$ es invariable entre diferentes equilibrios de Nash estándar. Los equilibrios definidos con respecto a $\succcurlyeq$ existen y se pueden generalizar a equilibrios de Nash estándar en juegos de n personas.

Sin embargo, no todas las propiedades se heredan directamente, y una característica computacional central de los juegos de suma cero está ausente en este contexto. La Proposición 8 de [1], que demuestra la no convergencia del juego ficticio en ciertos juegos de matriz de suma cero.

EL JUEGO APT

En el desarrollo de un modelo de juego de matriz para Amenazas Persistentes Avanzadas (APTs), se centra en especificar los resultados de escenarios de ataque/defensa. Para abordar la incertidumbre intrínseca, se emplea una evaluación cualitativa, y las distribuciones de pérdidas, según la definición 2, describen las pérdidas potenciales en cada escenario (i, j) dentro de los espacios de acción $AS_1 \times AS_2$. Para manejar escenarios sin una distribución clara, se considera un enfoque pesimista, que implica posiciones fijas, acciones de defensa y suposiciones de distribución uniforme. El proceso de decisión, representado como un árbol de decisiones, se repite para todos los escenarios, y las distribuciones empíricas se recopilan a partir de evaluaciones, formando una matriz de juego. El juego, diseñado para minimizar pérdidas, se alinea con los principios de gestión de riesgos, simplificando el modelado en comparación con los enfoques clásicos. El enfoque es subjetivo pero se alinea bien con los procesos estándar de gestión de riesgos, brindando ventajas detalladas en la Tabla 6 de [1]. Este método se adapta a las incertidumbres en la cuantificación del nivel de riesgo y contribuye a mantener a los adversarios a distancia de sus objetivos. La dependencia de la experiencia y el esfuerzo manual, al integrarse en marcos de gestión de riesgos establecidos, ofrece una solución simplificada a diversos desafíos de modelado.

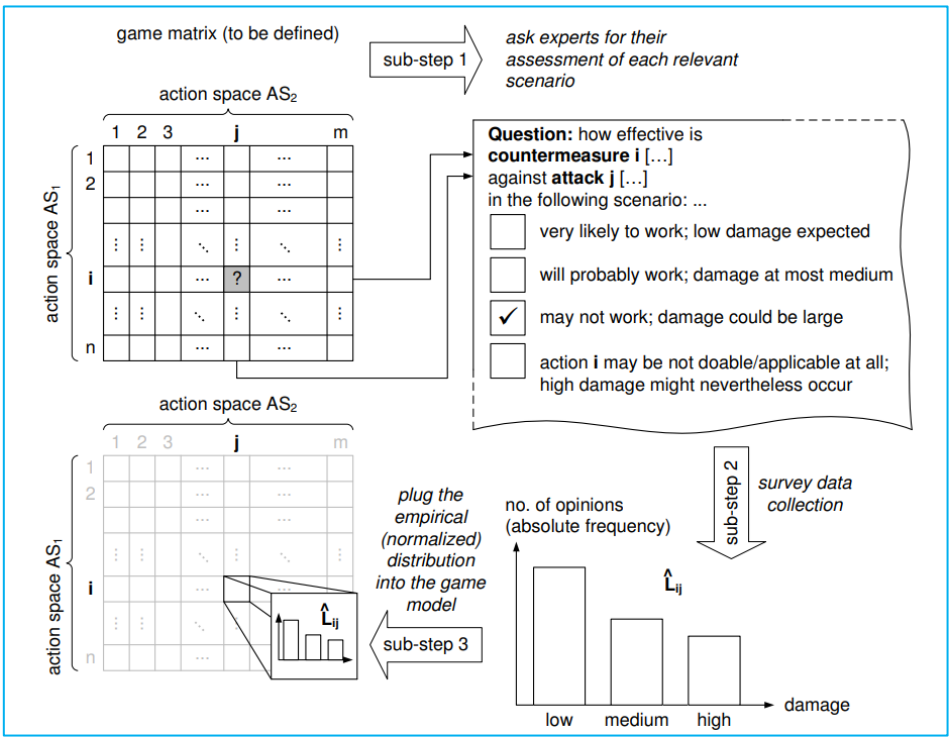

Figura 2 - Esquema para construir la matriz del juego APT

CÁLCULO DEL EQUILIBRIO

Para calcular el equilibrio lexicográfico del juego APT se deben seguir los siguientes pasos:

Se construye la distribución empírica $\tilde{L}_{ij}$ ya sea consultando a expertos, por medio de simulaciones o de acuerdo con la literatura. Se asume que esta distribución es categórica, aunque no necesariamente. El caso continuo se discute en la última sección 10 de [1]. A esta distribución empírica se le aplica un estimador de densidad de kernel (KDE) gaussiano:

$$\tilde{f}_{L_{ij}}(x) = \frac{1}{Nh}\sum_{k=1}^{N} K\left(\frac{x_k - x}{h}\right)$$

Donde K es la función gaussiana estándar:

$$K = \frac{1}{\sqrt{2\pi}}\exp\left(-\frac{1}{2}x^2\right)$$

Y $h > 0$ es el parámetro de ancho de banda calculado con una regla estadística estándar. En este caso se utiliza la regla de Silverman.

Se trunca esta función de densidad estimada en el dominio $[1, a]$ donde a que es el umbral de riesgo puede ser el valor máximo de las observaciones de pérdida obtenidas, aunque no necesariamente.

Usando la expansión de Taylor sobre esta función de densidad estimada, se obtiene la expresión para las derivadas de orden k:

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

De esta manera la función de densidad estimada puede aproximarse con la expansión de Taylor como una secuencia de sus derivadas con signos alternantes así:

$$\tilde{f}_{L_{ij}} \cong \left((-1)^k f_{L_{ij}}^{(k)}(a)\right)_{k=0}^{\infty} = (y_0, y_1, y_2, \dots) \in \mathbb{R}^{\infty}$$

En este caso se evalúa la secuencia en a, pues al ordenar lexicográficamente esta secuencia se logra una equivalencia con el orden de preferencia $\succcurlyeq$ de los hiperreales.

Al comparar estas secuencias lexicográficamente se están comparando las distribuciones $\tilde{L}_{ij}$, lo cual es suficiente para poder aplicar el algoritmo de juego ficticio y encontrar el equilibrio de Nash del juego APT.

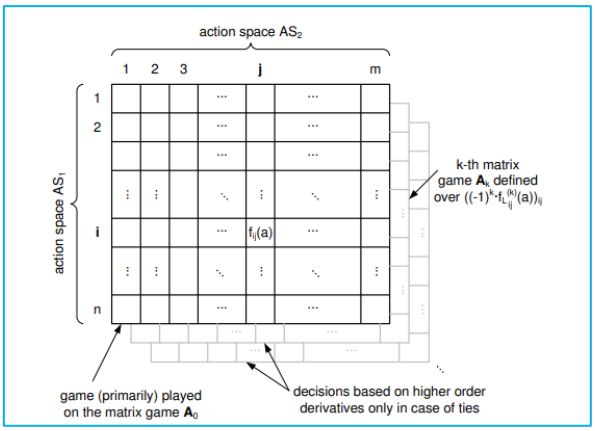

Figura 3 - Juego Ficticio para el juego APT

El juego ficticio se aplica sobre la matriz de las derivadas de orden cero, es decir la función de densidad estimada evaluada en a. En caso de que haya un empate al momento de intentar definir un mínimo un

máximo, se construye la matriz de derivadas de orden uno. Se juega en dicha matriz usando las mismas estrategias que se usaron en la matriz de orden cero hasta llegar a la iteración en la que se presentó el conflicto y se define cuál es el máximo o el mínimo de acuerdo con el valor de esta derivada. Si hay un empate nuevamente, se repite el proceso con la matriz de derivadas de orden dos y así sucesivamente. Pero siempre las estrategias utilizadas en cada matriz de orden superior son las mismas que se utilizan en la matriz principal (de orden cero).

De esta manera, las matrices de orden superior se generan a demanda cuando se presenta un conflicto, y una vez se crean se sigue jugando el juego en ellas en paralelo con las estrategias de la matriz inicial.

El resultado del algoritmo de juego ficticio es un vector para cada jugador denominados $\mathbf{p}^*$ y $\mathbf{q}^*$ que contiene las frecuencias óptimas o probabilidades esperadas de las estrategias de cada jugador.

El algoritmo de juego ficticio estándar puede consultarse en [2].

REFERENCIAS

[1] Rass S, König S, Schauer S (2017) Defending Against Advanced Persistent Threats Using Game-Theory. PLOS ONE 12(1): e0168675. https://doi.org/10.1371/journal.pone.0168675

[2] Washburn, A. (2001), A new kind of fictitious play . Naval Research Logistics, 48: 270-280. https://doi.org/10.1002/nav.7