Diseño de una Estrategia Probabilística de Defensa de Objetivo Móvil para Manejar Ataques contra Nodos de Red con Múltiples Recursos

***Resumen*—Las estrategias de defensa de ciberseguridad tradicionales se basan en un enfoque lineal que consiste en detectar las amenazas, seleccionar las defensas y mitigar los ataques. Sin embargo, estas estratégias presentan limitaciones frente a amenazas emergentes, desconocidas y avanzadas. Uno de los enfoques para diseñar soluciones más robustas y que no requieran del conocimiento previo del adversario o del ataque específico que se está ejecutando es la Defensa de Objetivo Móvil (Moving Target Defense - MTD). En este estudio, presentamos una solución innovadora de MTD que busca desviar o minimizar los daños causados por los ataques, aprovechando la teoría bayesiana del juego de Stackelberg para establecer estrategias óptimas tanto para el defensor como para el adversario. Demostramos cómo el defensor puede reducir costes al alejar los ataques de los nodos de mayor criticidad. Validamos nuestro enfoque mediante simulaciones cuyos resultados superan a las estrategias anteriores. Este nuevo enfoque sienta las bases para el desarrollo de modelos más avanzados que puedan utilizar una representación más detallada de los recursos del sistema, optimizando aún más la ciberseguridad ante amenazas complejas y en constante evolución.**

Ciberseguridad, Defensa de Objetivo Móvil, Ciberdefensa, Teoría de Juegos, Modelo Lógico

I. Introducción

La ciberseguridad es un tema complejo, especialmente cuando los adversarios están motivados para explotar unos sistemas objetivo determinados. Los sistemas de defensa tradicionales enfrentan dificultades cuando los adversarios poseen cierto conocimiento del sistema y pueden eludir el enfoque básico de detección y mitigación del sistema. Para abordar estos ataques avanzados, la literatura científica ha introducido nuevos enfoques que obstaculizan los ataques en lugar de simplemente detenerlos, como es el caso de las Defensas de Objetivo Móvil (*Moving Target Defense* (MTD)). El MTD tiene sus orígenes en aplicaciones más antiguas, como las técnicas de salto de frecuencia de radio utilizadas durante la Segunda Guerra Mundial para evitar la interceptación. Este concepto central ha transicionado de manera fluida a la era digital, con el surgimiento de Internet en la década de 1990, mediante el desarrollo de técnicas MTD para asegurar la comunicación digital [16], [6], [4] y para abordar problemas de ciber-resiliencia asociados con sistemas críticos [15]. El MTD opera sin necesidad de conocimiento previo del adversario, basándose únicamente en información sobre el tipo de ataque esperado [20].

Las estrategias de MTD tienen como objetivo aumentar la ciber-resiliencia del sistema al incrementar la incertidumbre percibida por el adversario. Para lograrlo, mueven dinámicamente los nodos dentro del sistema (por ejemplo, cambiando direcciones IP). Mediante cambios periódicos, el sistema de defensa puede disminuir la probabilidad de éxito de los atacantes [8].

Este trabajo emplea la teoría de juegos, un marco matemático para analizar las interacciones estratégicas entre agentes [1], [10]. En este contexto, un juego representa una interacción con reglas que definen las acciones disponibles y sus resultados correspondientes [10]. En el caso de MTD entre el defensor y el adversario, la teoría de juegos explora cómo estos agentes toman decisiones estratégicas con objetivos contrapuestos [12]. Estas decisiones se fundamentan en funciones de utilidad que evalúan las posibles ganancias o pérdidas [12], buscando optimizar sus resultados.

Este artículo extiende la propuesta de Feng et. al [5] y proponer un nuevo modelo matemático para un juego defensor-adversario. El modelo considera un sistema con múltiples recursos y nodos y define estrategias para que el defensor reubique sus recursos para minimizar costos. El desarrollo de nuestro modelo, que constituye la principal contribución de este artículo, sigue una metodología estructurada que se detalla en la siguiente lista:

- Presentación de un modelo para un sistema compuesto por múltiples nodos y recursos.
- Definición de las ganancias para los dos jugadores en el juego.
- Resolución del problema y desarrollo de una estrategia teórica de juego para el defensor.
- Análisis de los resultados: comparaciones numéricas entre la estrategia propuesta y los trabajos relacionados.

El artículo está organizado de la siguiente manera. En la Sección II se revisan los trabajos relacionados. La Sección III presenta el método propuesto y algunos resultados analíticos. La Sección IV describe los escenarios óptimos para el adversario y el defensor. La Sección V ofrece resultados numéricos. Finalmente, la Sección VI concluye el artículo.

II. Estado del arte

Los enfoques existentes utilizan diversos modelos, como la teoría de juegos y el aprendizaje automático, para la toma de decisiones (p.e. qué modificar y cuándo). Los desencadenantes de activar una acción pueden estar basados en el tiempo o en eventos, e incluso pueden combinarse para un enfoque híbrido[3], [11]. Aunque estos métodos son robustos, presentan dificultades ante atacantes avanzados que utilizan modelos diversos e híbridos [19].

Yoon *et al*. proponen un enfoque de MTD basado en un grafo de ataque de tres niveles [18]. En este tipo de grafo cada nivel representa diferentes aspectos o etapas del ataque (entrada, intermedio, objetivo) y estos niveles se integran con MTD para reducir su impacto. El modelo emplea varios

métodos de protección y además usa el engaño para mejorar aún más la efectividad de la MTD.

Feng *et al.* [5] proponen un modelo basado en la teoría de juegos con engaño para la protección de recursos. Este modelo asume que el adversario tiene más conocimiento que el defensor. El defensor reubica estratégicamente los recursos para engañar al adversario y utiliza comunicación falsa, mientras que el adversario estudia el sistema para atacar la ubicación más probable de los recursos. El objetivo de los dos jugadores es maximizar las ganancias y minimizar las pérdidas. Una limitación del modelo es que no es aplicable a sistemas con múltiples recursos y no considera ciertos ataques como *Denial of Service* (DoS) que afectan nodos enteros.

Jia *et al.* introducen la conmutación de proxy en las estrategias de MTD para ataques de DoS[9], de manera que se asignan nodos no maliciosos a proxies seguros y se mezclan para identificar amenazas internas. Wright *et al.* amplían este trabajo con un nuevo modelo de compensación y estrategias adicionales de defensa[17]. Sus resultados demuestran la efectividad de la defensa proactiva.

Aunque en los últimos años ha habido un avance significativo en los sistemas MTD[2], existen limitaciones en como gestionar las redes con múltiples recursos. La separación de recursos correlacionados puede mejorar la eficiencia (ver SecciónV). La gestión efectiva de recursos se vuelve crucial cuando los adversarios poseen conocimiento previo. Este artículo propone un modelo para que los defensores gestionen múltiples recursos, minimizando costos de defensa e impacto de ataques. Se asume que todos los recursos tienen la misma criticidad.

III. Descripción del Modelo

En esta sección, describimos nuestro modelo de dos jugadores. El apartado III-A describe la estrategia MTD y el apartado III-B la estrategia del defensor.

Símbolo	Significado
π	Estrategia del adversario
n	Número de nodos
m	Número de recursos
c_a	Costo total del ataque del adversario
c_m	Costo de migración de recursos del defensor
i	Índice para recursos
k	Índice para nodos
R	Conjunto de recursos
r_i	Recurso i
$T_c(k)$	Criticidad del nodo k
$\alpha(i,k)$	Probabilidad de mover r_i al nodo k
$\mathbb{C}(k)$	Costo de defensa si el nodo k es atacado

Tabla I: Símbolos utilizados en el artículo.

III-A. Modelo de Defensa de Objetivo Móvil

Nuestro modelo de MTD trabaja con dos elementos: nodos interconectados ($n > 1$) y recursos esenciales ($m > 1$). Los recursos (*e.g.* aplicaciones) residen en nodos (*e.g.* computadoras) que permiten el movimiento de los recursos. Este marco analiza la gestión dinámica de recursos en redes.

Introducimos dos agentes inteligentes: un adversario que busca maximizar el daño y un defensor que quiere minimizar el costo de defensa. El costo de defensa incluye la implementación de la estrategia de protección de recursos (ver apartado III-B) mediante la reubicación de los múltiples recursos en diferentes nodos (ver Fig. 1) y el impacto del ataque.

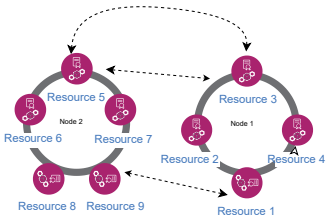


Figura 1: Modelo dinámico de dos nodos y nueve recursos.

El adversario selecciona estratégicamente los nodos a atacar teniendo en cuenta los costos del ataque (*e.g.* ataques DoS para deshabilitar nodos), y los beneficios que anticipa obtener. Este análisis costo-beneficio, incluyendo la estrategia de protección de recursos del defensor, moldea la estrategia de ataque del adversario.

III-A0a. Premisas: Como se mencionó anteriormente, tanto los adversarios como los defensores tienen un conjunto de conocimientos previos sobre los cuales basan su estrategia. Los adversarios y defensores operan con conjuntos de conocimientos distintos que influyen en sus estrategias. Los adversarios conocen el número total de nodos y recursos, pero carecen de información precisa sobre las ubicaciones de los recursos. Son conscientes de la estrategia MTD del defensor y pueden estimar los costos de los ataques, pero desconocen los detalles de la implementación del MTD. En contraste, los defensores tienen una imagen completa del sistema, incluyendo nodos y recursos. Pueden estimar los costos de los ataques del adversario y comprenden su proceso general de toma de decisiones. Sin embargo, los defensores no pueden predecir el momento exacto del ataque del adversario. Esta asimetría de conocimiento moldea las elecciones y estrategias de los dos agentes del MTD.

Debido al conocimiento limitado, los agentes evalúan sus estrategias a partir de probabilidades. El adversario utiliza observaciones pasadas para predecir la ubicación de los recursos. En estas condiciones de conocimiento mutuo limitado, los agentes pueden converger en estrategias que optimizan sus resultados individuales mientras siguen siendo aceptables para la otra parte. Este punto de convergencia, donde ambos agentes logran un resultado estable y mutuamente aceptable, corresponde al concepto de estado de equilibrio en teoría de juegos.

En resumen, el sistema comprende los siguientes componentes clave:

- Un agente defensor que intenta disminuir el costo de defensa y el impacto del ataque.
- Un agente adversario que intenta causar el mayor daño posible con el ataque.
- m recursos que se pueden mover libremente entre nodos con un costo determinado.
- n nodos interconectados, cada uno capaz de contener múltiples recursos.
- El impacto del ataque depende del número de recursos en el nodo atacado.

III-B. Estrategia de Movimiento de Recursos

El defensor utiliza una estrategia de MTD para proteger el sistema mediante una reubicación de recursos que dificulte los ataques por parte del adversario. El defensor, consciente que el adversario va adquiriendo conocimiento del sistema, procede a mover los recursos entre nodos. Por su parte, el adversario busca anticiparse a los movimientos del defensor y planificar su plan de ataque consecuentemente. Esto da lugar a un juego de Stackelberg bayesiano de dos jugadores [14]. El Stackelberg bayesiano es uno de los modelos clásicos de teoría de juegos que intenta establecer estrategias realistas para los jugadores, donde cada uno elige su acción anticipando la respuesta del otro jugador y teniendo en cuenta la incertidumbre en el sistema.

Definimos el conjunto de recursos del sistema como $R = \{r_1, r_2, \ldots, r_m\}$. Estos recursos R son la principal preocupación del defensor y del adversario. El adversario construye un modelo probabilístico de la ubicación de cada recurso, p.e. a través de nodos internos o escuchas. A lo largo del documento, todos los costos y valores se normalizan en relación con el costo del recurso.

El adversario elige una estrategia de ataque π (Ec. 1) basada tanto en la ganancia esperada (impactando recursos) como en el costo del ataque c_a.

$$\pi = \begin{cases} 1, & \text{si } c_a < \text{ganancia esperada del ataque} \\ 0, & \text{en caso contrario} \end{cases} \tag{1}$$

Antes de llevar a cabo un ataque, el adversario establece una matriz de probabilidad posicional A, donde $\alpha(i,k)$ es la probabilidad de que el recurso r_i esté en el nodo k, como se muestra a continuación:

$$A = \begin{pmatrix} \alpha(1,1) & \alpha(2,1) & \ldots & \alpha(m,1) \\ \alpha(1,2) & \alpha(2,2) & \ldots & \alpha(m,2) \\ \vdots & \vdots & \ddots & \vdots \\ \alpha(1,n) & \alpha(2,n) & \ldots & \alpha(m,n) \end{pmatrix} \tag{2}$$

donde $\sum_{k=1}^{n} \alpha(i,k) = 1$. Para cada nodo k, el adversario puede calcular T_c como la suma de los elementos de la fila k en la matriz A multiplicada por el costo de cada recurso. Dado que el modelo está normalizado con respecto al costo de los recursos, reemplazamos ese valor con 1 para formar el impacto del costo del ataque como $T_c(k) = \sum_{i=1}^{m} \alpha(i,k)$. Sea $U_a(k)$ la ganancia esperada del adversario, es decir, la función de utilidad si el ataque se dirigirse al nodo k. Definimos la utilidad del adversario de la siguiente manera:

$$U_a(k) = (T_c(k) - c_a) \cdot \pi \tag{3}$$

El defensor establece de manera similar $\mathbb{C}(k)$ como el costo esperado en la implementación de la estrategia de defensa. Lo definimos de la siguiente manera:

$$\mathbb{C}(k) = (T_c(k) \cdot \pi) + c_m \sum_{i=1}^{m} (1 - \alpha(i, Position(i)))^2 \tag{4}$$

donde c_m es el costo de movimiento para el defensor y $Position(i)$ denota la ubicación de r_i antes de que el defensor tome alguna acción. Dado que el defensor utiliza un enfoque uniforme para mover recursos y todos los recursos tienen igual importancia, mover cualquier recurso incurre en el mismo costo para el defensor. El costo de mover recursos difiere solo entre diferentes redes y configuraciones del sistema con distintos costos de recursos. Dada la naturaleza discreta del modelo, la probabilidad de movimiento de recursos se calcula como uno menos la probabilidad de no mover el recurso. Por lo tanto, $1 - \alpha(i, Position(i))$ es la probabilidad de que r_i sea reubicado.

El costo del defensor, como se muestra en la Ec. (4), se forma a partir de la pérdida esperada debido a un ataque y el costo de la estrategia del defensor. En este contexto, el defensor reasigna los recursos del sistema para generar un estado que minimiza la utilidad del adversario. De manera similar, el adversario apunta al nodo con la mayor criticidad (es decir, mayor $T_c(k)$). Nuestro modelo de costo tiene similitudes con el presentado en [5], pero a diferencia de este, permite gestionar sistemas con múltiples recursos y no solo uno. El sistema busca penalizar que el movimiento se realice siempre sobre un mismo recurso, ya que esto llevaría a que este recurso esté frecuentemente no disponible y siendo todos los recursos en R críticos, el sistema completo podría detenerse mientras espera que el recurso no disponible vuelva a la funcionalidad normal. Por eso el costo del defensor toma en consideración el valor cuadrado de la probabilidad de mover un recurso, $1 - \alpha(i, Position(i))$, en lugar de dividir el movimiento entre múltiples recursos. Por lo tanto, es más ventajoso para el defensor mover múltiples recursos.

IV. Escenario Óptimo

En esta sección discutimos la estrategia preferida de MTD del defensor. En el apartado IV-A presentamos la metodología del defensor. En IV-B aplicamos la metodología para encontrar la solución general. En IV-C discutimos los escenarios y destacamos algunas observaciones importantes.

IV-A. Derivación de la Matriz

Basándonos en el modelo presentado en el apartado III-A, la estrategia del defensor se define por dos restricciones. La primera se centra en minimizar la probabilidad de mover nodos; un valor alto de α para un recurso indica una menor probabilidad de movimiento. La segunda restricción busca minimizar es el impacto del ataque en todos los nodos, es decir, $T_c(k)$. Este problema de optimización puede verse como una variación del problema de la suma de subconjuntos [13], donde el conjunto de números es la matriz de probabilidad A, y la suma de cada fila está determinada por los escenarios del defensor $\frac{m}{n}$.

Imaginemos 5 recursos y 3 nodos. El defensor desea minimizar el impacto del ataque y maximizar la probabilidad de movimiento. Cada columna de la matriz representa un recurso, y cada fila representa un nodo. Inicialmente, los recursos se distribuyen equitativamente entre los nodos para minimizar el costo del ataque. El defensor puede intercambiar recursos entre nodos para reducir la probabilidad de movimiento sin afectar el impacto del ataque. Este enfoque es similar a modelos de asignación de recursos como [7]. Alternativamente, el defensor puede distribuir el costo de movimiento entre varios recursos dentro de un nodo (en lugar de enfocarse en uno) dividiendo igualmente la probabilidad total de movimiento. Aplicando estos dos enfoques que hemos definido, el defensor

puede optimizar el costo de defensa como se muestra en las matrices de a continuación:

$$A = \begin{pmatrix} \frac{1}{3} & \frac{1}{3} & \frac{1}{3} & \frac{1}{3} & \frac{1}{3} \\ \frac{1}{3} & \frac{1}{3} & \frac{1}{3} & \frac{1}{3} & \frac{1}{3} \\ \frac{1}{3} & \frac{1}{3} & \frac{1}{3} & \frac{1}{3} & \frac{1}{3} \end{pmatrix} \rightarrow \begin{pmatrix} \frac{5}{6} & \frac{5}{6} & 0 & 0 & 0 \\ 0 & 0 & \frac{5}{6} & \frac{5}{6} & 0 \\ \frac{1}{6} & \frac{1}{6} & \frac{1}{6} & \frac{1}{6} & 1 \end{pmatrix}$$

IV-B. Estrategia Preferida del Defensor

Utilizando la metodología del apartado IV-A, establecemos un modelo matemático novedoso para definir la solución general para el defensor, que diferenciamos para tres escenarios: ataque, ataque optimizado y sin ataque. La solución tiene en cuenta que el adversario prefiere atacar el nodo k con el mayor $T_c(k)$, y que el máximo valor de $T_c(k)$ no puede ser inferior al promedio, y por lo tanto $T_c(k) \geq \frac{m}{n}$.

IV-B1. Escenario de Ataque: Este escenario es la solución general para el ejemplo en el apartado IV-A cuando el adversario planea atacar ($c_a < T_c(k)$). Si $c_a < \frac{m}{n}$, el defensor no puede asignar r_i a los nodos de manera que evite un ataque. Así, inicialmente prioriza minimizar $T_c(k)$ dividiendo los recursos equitativamente entre los nodos, $T_c(k) = \frac{m}{n}$, y luego maximiza α lo que le lleva a la Matriz 2.

$$\begin{array}{c} \overbrace{\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad}^{m} \\ \left(\begin{array}{ccccccccccccccc} \overbrace{\qquad\qquad\qquad}^{\lceil \frac{m}{n} \rceil} & & & & & & & & & & & \overbrace{\qquad\qquad\qquad\qquad}^{\lfloor \frac{m}{n} \rfloor (n-m \bmod n)} & & & \\ \frac{m}{n\lceil \frac{m}{n} \rceil} & \cdots & \frac{m}{n\lceil \frac{m}{n} \rceil} & \cdots & 0 & 0 & 0 & 0 & 0 & 0 \ldots 0 & \ldots & 0 & & & \\ \vdots & & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \ddots \vdots & \ddots & \vdots & & & \\ 0 & \ldots & 0 & \ldots & \frac{m}{n\lceil \frac{m}{n} \rceil} & \cdots & \frac{m}{n\lceil \frac{m}{n} \rceil} & 0 & 0 & 0 \ldots 0 & \ldots & 0 & & & \\ \frac{1}{n\lceil \frac{m}{n} \rceil} & \cdots & \cdots & \cdots & \cdots & \cdots & \frac{1}{n\lceil \frac{m}{n} \rceil} & 1 & \ldots 1 & \ldots 0 & \ldots & 0 & & & \\ \vdots & & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \ddots \vdots & \ddots & \vdots & & & \\ \frac{1}{n\lceil \frac{m}{n} \rceil} & \cdots & \cdots & \cdots & \cdots & \cdots & \frac{1}{n\lceil \frac{m}{n} \rceil} & 0 & 0 & 0 \ldots 1 & \ldots & 1 & & & \end{array}\right) \begin{array}{l} \Big\} m \bmod n \\ \Big\} n - m \bmod n \end{array} \end{array}$$

Figura 2: Matriz A cuando el adversario planea atacar.

donde $\lfloor \frac{m}{n} \rfloor$ es el valor redondeado hacia abajo de $\frac{m}{n}$ y $\lceil \frac{m}{n} \rceil$ es el redondeo hacia arriba.La matriz muestra que el impacto esperado del ataque es $\frac{m}{n}$ y que $\lfloor \frac{m}{n} \rfloor (n - m \bmod n)$ recursos no se mueven mientras que $(m \bmod n)\lceil \frac{m}{n} \rceil$ recursos tienen una probabilidad de no moverse de $\frac{m}{n\lceil \frac{m}{n} \rceil}$. Actualizamos $\mathbb{C}(k)$ con el valor calculado como se muestra en la Ec. 1.

$$\mathbb{C}(k) = \frac{m}{n} + c_m(m \bmod n)\lceil \frac{m}{n} \rceil (1 - \frac{m}{n\lceil \frac{m}{n} \rceil})^2 \qquad (5)$$

IV-B2. Escenario de Ataque Optimizado: $\mathbb{C}(k)$ puede reducirse aún más aumentando $T_c(k)$ más allá de $\frac{m}{n}$ para disminuir el costo de mover nodos. Designamos δ como el incremento del impacto del ataque para reducir la probabilidad de mover recursos. Planteamos el problema de optimización $\mathbb{C}(k) = \frac{m}{n} + \delta(m \bmod n)\lceil \frac{m}{n} \rceil + c_m(m \bmod n)\lceil \frac{m}{n} \rceil (1 - \frac{m}{n\lceil \frac{m}{n} \rceil} - \delta)^2$.

Para encontrar la solución óptima en un escenario de ataque, calculamos el mínimo de la ecuación anterior variando δ. El defensor utiliza la misma matriz A de la Fig. 2 pero cambia los recursos que se mueven (parte izquierda de la matriz). Nótese que $-\frac{m}{n\lceil \frac{m}{n} \rceil} \leq \delta \leq 1 - \frac{m}{n\lceil \frac{m}{n} \rceil}$ ya que la probabilidad no puede ser negativa ni exceder 1. La resolución del problema da $\delta = 1 - \frac{m}{n\lceil \frac{m}{n} \rceil} - \frac{1}{2c_m}$. Sustituyendo δ en la Ec. (5) obtenemos el costo optimizado para el defensor como:

$$\mathbb{C}(k) = \frac{m}{n} + (m \bmod n)\lceil \frac{m}{n} \rceil (1 - \frac{m}{n\lceil \frac{m}{n} \rceil} - \frac{1}{4c_m}) \qquad (6)$$

IV-B3. Escenario Sin Ataque: Si $c_a \geq \frac{m}{n}$, el defensor puede distribuir los recursos de manera que evite el ataque. En este escenario, el defensor minimiza el costo de defensa maximizando $\alpha(i, Position(i))$ y evitando el ataque (es decir, $T_c(k) = c_a$). Es importante señalar que cuando c_a es igual a $\lceil \frac{m}{n} \rceil$ (donde $\lceil \frac{m}{n} \rceil$ representa el valor redondeado hacia arriba de $\frac{m}{n}$), el defensor puede asignar recursos estáticamente ($\alpha = 1$) a los nodos, evitando así el ataque al mantener $T_c(k)$ por debajo de c_a. Más allá de este umbral $\lceil \frac{m}{n} \rceil$, el modelo del defensor no muestra cambios.

Basta con resolver el rango $\frac{m}{n} \leq c_a \leq \lceil \frac{m}{n} \rceil$ para minimizar costos y cumplir las restricciones dadas. Para ello, mientras se optimizan los gastos, la estrategia óptima del defensor se define en la Matriz 3.

$$\begin{array}{c} \overbrace{\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad}^{m} \\ \left(\begin{array}{ccccccccccccccc} \overbrace{\qquad\qquad\qquad}^{\lceil c_a \rceil} & & & & & & & & & & & \overbrace{\qquad\qquad\qquad\qquad}^{\lfloor c_a \rfloor (n-N_m)} & & & \\ \frac{c_a}{\lceil c_a \rceil} & \cdots & \frac{c_a}{\lceil c_a \rceil} & \cdots & 0 & 0 & 0 & 0 & 0 & 0 \ldots 0 & \ldots & 0 & & & \\ \vdots & & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \ddots \vdots & \ddots & \vdots & & & \\ 0 & \ldots & 0 & \ldots & \frac{c_a}{\lceil c_a \rceil} & \cdots & \frac{c_a}{\lceil c_a \rceil} & 0 & 0 & 0 \ldots 0 & \ldots & 0 & & & \\ \frac{\lceil c_a \rceil - c_a}{\lceil c_a \rceil (n-N_m)} & \cdots & \cdots & \cdots & \cdots & \cdots & \frac{\lceil c_a \rceil - c_a}{\lceil c_a \rceil (n-N_m)} & 1 & \ldots 1 & \ldots 0 & \ldots & 0 & & & \\ \vdots & & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \ddots \vdots & \ddots & \vdots & & & \\ \frac{\lceil c_a \rceil - c_a}{\lceil c_a \rceil (n-N_m)} & \cdots & \cdots & \cdots & \cdots & \cdots & \frac{\lceil c_a \rceil - c_a}{\lceil c_a \rceil (n-N_m)} & 0 & 0 & 0 \ldots 1 & \ldots & 1 & & & \end{array}\right) \begin{array}{l} \Big\} N_m \\ \Big\} n - N_m \end{array} \end{array}$$

Figura 3: Matriz A cuando el adversario no planea atacar.

donde $\lfloor c_a \rfloor$ es el valor redondeado hacia abajo de c_a y $N_m = m - n\lfloor c_a \rfloor$ es el número de nodos con solo recursos móviles. El adversario no planea atacar, por lo tanto, el impacto del ataque es cero. $N_m\lceil c_a \rceil$ recursos tienen una probabilidad de no moverse de $\frac{c_a}{\lceil c_a \rceil}$. Nótese que N_m es estrictamente positivo y cuando c_a excede $\lceil \frac{m}{n} \rceil$, el defensor no necesita mover recursos ($N_m = 0$). $\mathbb{C}(k)$ se muestra en la Ec. 7

$$\mathbb{C}(k) = c_m \cdot N_m\lceil c_a \rceil (1 - \frac{c_a}{\lceil c_a \rceil})^2 \qquad (7)$$

IV-C. Discusión

La Ec. (7) presenta una situación en la que el defensor se enfrenta a dos estrategias conflictivas. Por un lado, optimizar la colocación de r_i para minimizar la migración reduce los costos. Por otro, disminuir la migración incrementa la atracción del adversario a atacar. Este aumento en la atracción está relacionado con el costo del ataque c_a y el número de nodos involucrados. Cuando c_a supera a $\frac{m}{n}$, el adversario ya no ve atractivo atacar.

En la Ec. (5), el defensor asume que el adversario intenta atacar, ya que el beneficio del ataque supera los costos. Aquí, el defensor puede reposicionar r_i para confundir al adversario, incurriendo en costos de migración, o distribuir r_i equitativamente entre varios nodos, evitando un ataque altamente impactante.

En la Fig. 4, se muestran las variaciones de costo de los tres enfoques del defensor, con $m = 4$ y $n = 3$. La figura ilustra que el costo óptimo del ataque es casi tan eficiente como el óptimo matemático. Además, la curva indica si la estrategia sin ataque es deseable según el valor de c_m.

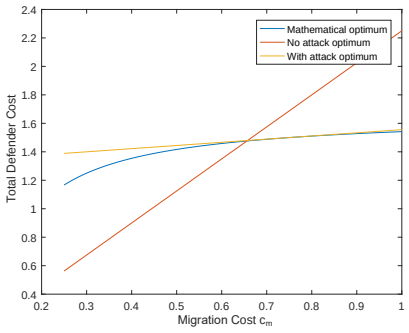


Figura 4: Comparación de $\mathbb{C}$ con los tres modelos de este artículo a medida que varía c_m. Con $m = 4$ y $n = 3$.

V. Simulación Numérica

En esta sección, validamos los resultados presentados en este artículo utilizando como referencia el trabajo de Feng et al. [5]. Realizamos simulaciones numéricas para calcular diversos valores y generar gráficos que respaldan nuestros hallazgos.

V-A. Modelo de Simulación

El sistema se configura según lo descrito en el apartado III-A. Calculamos $\mathbb{C}(k)$ utilizando la definición proporcionada en este trabajo y en [5]. Luego, dividimos $\mathbb{C}(k)$ por m para obtener el costo por recurso. Exploramos seis escenarios distintos que examinan el efecto de variar c_m, c_a, m y n de la siguiente manera:

1. $m = 1$, $n = 2$, $c_a = \frac{1}{3}$ con $c_m \in [0{,}1 \dots 2]$ (Fig. 5(a)).
2. $m = 13$, $n = 5$, $c_a = \frac{1}{3}$ con $c_m \in [0{,}1 \dots 1]$ (Fig. 5(b)).
3. $m = 13$, $n = 5$, $c_m = \frac{3}{2}$ con $c_a \in [0{,}1 \dots 1]$ (Fig. 5(c)).
4. $m = 20$, $c_a = \frac{1}{3}$, $c_m = \frac{1}{5}$ con $n \in [2 \dots 50]$ (Fig. 5(e)).
5. $m = 20$, $c_a = \frac{1}{3}$, $c_m = \frac{1}{50}$ con $n \in [2 \dots 50]$ (Fig. 5(f)).
6. $n = 5$, $c_m = \frac{1}{5}$, $c_a = \frac{1}{3}$ con $m \in [2 \dots 50]$ (Fig. 5(d)).

V-B. Discusión

Nuestra nueva estrategia (Fig. 5(a)) alcanza la misma efectividad en defensa que los enfoques anteriores $(m = 1)$ pero con menor costo (ver figuras siguientes). Por ejemplo, en la Fig. 5(b) se observa cómo el costo de defensa del modelo de Feng aumenta rápidamente con el incremento del costo de movimiento c_m. Este aumento se desacelera cuando los defensores cambian de estrategia en $c_m = \frac{n}{2(n-1)}$. Nuestro modelo logra reducir este costo utilizando otros recursos para mantener el mismo nivel de defensa mientras se disminuye el costo de movimiento. En contraste, el modelo de Feng trata los recursos de manera independiente, lo que resulta en mayores costos de defensa.

La Fig. 5(c) explora el impacto del modelo de Feng [5] en el costo del defensor. Se definen dos enfoques: *Separado* donde los recursos se tratan de forma independiente, y *Combinado* donde todos los recursos se consideran juntos. La asignación separada de recursos puede llevar al defensor a adoptar una estrategia que no se alinea con la estrategia del adversario, lo que resulta en una defensa ineficiente y picos de costo, como se observa en la figura. Estos ejemplos subrayan posibles problemas de implementaciones ineficaces en los trabajos relacionados.

La ventaja de nuestra estrategia se hace más evidente con el incremento de m y n, hasta un umbral, como se muestra en las Figures 5(d) to 5(f). Esto se debe a que nuestro enfoque permite una asignación de recursos más flexible en comparación con simplemente mover recursos constantemente.

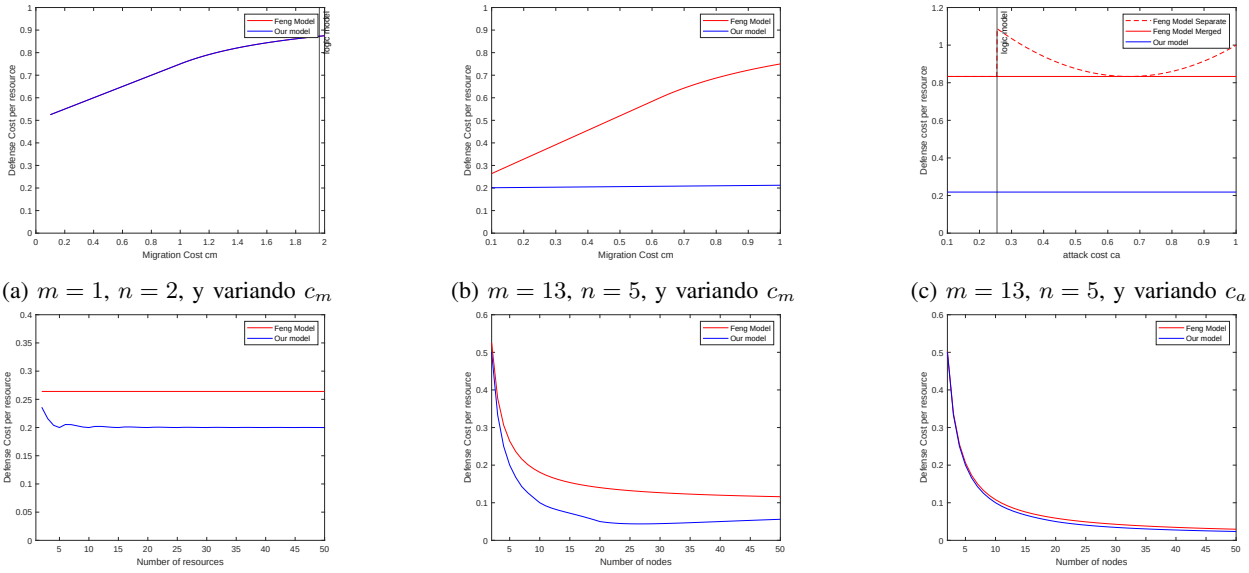
Finalmente, el parámetro c_m juega un papel crucial al influir en la diferencia entre nuestro modelo y trabajos previos, como se observa en las Figures 5(c) and 5(f). Un aumentar de c_m amplía la brecha entre el rendimiento de nuestro modelo y los enfoques existentes. En un escenario ideal con c_m muy bajo, el defensor puede mover recursos infinitamente sin incurrir en ningún costo, lo que hace que el costo del defensor dependa únicamente del número de recursos y nodos, independientemente de la estrategia elegida o del enfoque de MTD utilizado.

Nuestra estrategia propuesta ofrece evidentes ahorros de costos en comparación con las estrategias existentes, especialmente con un mayor número de recursos y nodos. Al comprender el impacto de diferentes variables, los defensores pueden aprovechar esta estrategia para crear sistemas de defensa más eficientes. Dado que c_m no se puede controlar, se utiliza este valor para evaluar si MTD es una estrategia de defensa rentable. Por otro lado, el defensor puede controlar m y n mediante la variación del diseño del sistema, permitiéndole construir redes más favorables.. Finalmente, c_a ayuda al defensor a establecer un límite del costo óptimo de defensa.

VI. Conclusiones

En el dinámico campo de la ciberseguridad, las estrategias tradicionales de defensa estática han demostrado ser insuficientes ante amenazas emergentes, no identificadas y sofisticadas. Esto ha llevado a los investigadores a explorar enfoques innovadores que puedan asegurar redes sin conocimiento previo del adversario o del ataque específico en curso. Entre estos enfoques, MTD ofrece una vía prometedora. En lugar de detener los ataques abruptamente, MTD busca dificultarlos distribuyendo los objetivos del adversario en la red sin introducir entidades adicionales. Al expandir los puntos potenciales de ataque, la confianza del adversario en ejecutar el ataque se debilita, lo que a menudo resulta en retrasos en sus acciones.La implementación periódica de MTD en intervalos específicos puede llevar a los adversarios a un estado de demora continua, esperando un momento oportuno, lo que efectivamente disuade los ataques. Además, en caso de que se inicie un ataque, el defensor puede minimizar las pérdidas desviando el impacto lejos de las partes más críticas del sistema.

En este trabajo presentamos una nueva estrategia de MTD para asegurar nodos segmentados, donde el principal objetivo son los recursos distribuidos en estos nodos. Utilizando la teoría de juegos de Stackelberg bayesiana, establecimos escenarios óptimos tanto para el defensor como para el adversario, analizando cómo el defensor puede reducir costos moviendo recursos de manera eficiente entre nodos y al mismo tiempo disminuir la probabilidad de ataques. Nuestros resultados de simulación muestran que esta estrategia logra un menor costo para el defensor cuando hay múltiples recursos presentes. También evidencian que la eficacia de la estrategia mejora aún más con el incremento en el número de nodos y recursos. Basados en estos resultados numéricos, consideramos que la



(a) $m = 1$, $n = 2$, y variando c_m (b) $m = 13$, $n = 5$, y variando c_m (c) $m = 13$, $n = 5$, y variando c_a

(d) $n = 5$, $c_m = \frac{1}{10}$, y variando m (e) $c_m = \frac{1}{10}$, $m = 20$, y variando n (f) $c_m = \frac{1}{100}$, $m = 20$, y variando n

Figura 5: $\mathbb{C}(k)$ por recurso para los modelos definidos. El cambio de escenario indica el límite sobre el cual el defensor cambia del ataque a la no-ataque escenario o viceversa.

estrategia presentada tiene un gran potencial para mejorar la seguridad de las redes en comparación con contribuciones anteriores. Como trabajo futuro, planeamos extender el modelo para abordar escenarios con múltiples adversarios y mejorar la definición de la criticidad de los recursos y las restricciones relacionadas con los tamaños de los nodos.

Referencias

[1] A Petrosyan, L.a.: Recent advances in game theory and applications. Springer, Heidelberg, Germany (2016)

[2] Charpentier, A., Neal, C., Boulahia-Cuppens, N., Cuppens, F., Yaich, R.: Real-time defensive strategy selection via deep reinforcement learning. In: Proceedings of the 18th International Conference on Availability, Reliability and Security. ARES '23, Association for Computing Machinery, New York, NY, USA (2023). https://doi.org/10.1145/3600160.3600176

[3] Colbaugh, R., Glass, K.: Predictability-oriented defense against adaptive adversaries. In: 2012 IEEE international conference on systems, man, and cybernetics (SMC). pp. 2721–2727. IEEE, IEEE, Piscataway, NJ 08854 (2012), https://ieeexplore.ieee.org/document/6378159

[4] Douligeris, C., Mitrokotsa, A.: Ddos attacks and defense mechanisms: a classification. In: Proceedings of the 3rd IEEE International Symposium on Signal Processing and Information Technology (IEEE Cat. No. 03EX795). pp. 190–193. IEEE, IEEE, Piscataway, NJ 08854 (2003). https://doi.org/10.1109/ISSPIT.2003.1341092

[5] Feng, X., Zheng, Z., Cansever, D., Swami, A., Mohapatra, P.: A signaling game model for moving target defense. In: IEEE INFOCOM 2017 - IEEE Conference on Computer Communications. pp. 1–9. IEEE, Piscataway, NJ 08854 (May 2017). https://doi.org/10.1109/INFOCOM.2017.8057200

[6] Ghosh, A., Pendarakis, D., Sanders, W.: Moving target defense co-chair's report-national cyber leap year summit 2009. Tech. rep., Federal NITRD Program, Washington, DC, USA (2009), https://www.nitrd.gov/nitrdgroups/images/b/bd/National_Cyber_Leap_Year_Summit_2009_CoChairs_Report.pdf

[7] Gil Herrera, J., Botero, J.F.: Resource Allocation in NFV: A Comprehensive Survey. IEEE Transactions on Network and Service Management **13**(3), 518–532 (Sep 2016). https://doi.org/10.1109/TNSM.2016.2598420

[8] Gonzalez-Granadillo, G., Dubus, S., Motzek, A., Garcia-Alfaro, J., Alvarez, E., Merialdo, M., Papillon, S., Debar, H.: Dynamic risk management response system to handle cyber threats. Future Generation Computer Systems **83**, 535–552 (2018). https://doi.org/10.1016/j.future.2017.05.043

[9] Jia, Q., Sun, K., Stavrou, A.: MOTAG: Moving Target Defense against Internet Denial of Service Attacks. In: 2013 22nd International Conference on Computer Communication and Networks (ICCCN). pp. 1–9. IEEE, Piscataway, NJ 08854 (Jul 2013). https://doi.org/10.1109/ICCCN.2013.6614155, iSSN: 1095-2055

[10] John, v.N.H., Oskar, M.: The Theory of Games and Economic Behaviour. Princeton University Press, 41 William Street Princeton, USA (1944)

[11] Keromytis, A.D., Geambasu, R., Sethumadhavan, S., Stolfo, S.J., Yang, J., Benameur, A., Dacier, M., Elder, M., Kienzle, D., Stavrou, A.: The meerkats cloud security architecture. In: 2012 32nd International Conference on Distributed Computing Systems Workshops. pp. 446–450. IEEE, IEEE, Piscataway, NJ 08854 (2012). https://doi.org/10.1109/ICDCSW.2012.42

[12] Kiennert, C., Ismail, Z., Debar, H., Leneutre, J.: A survey on game-theoretic approaches for intrusion detection and response optimization. ACM Computing Surveys (CSUR) **51**(5), 1–31 (2018)

[13] Kleinberg, J., Tardos, E.: algorithm design (2003)

[14] Paruchuri, P., Pearce, J.P., Marecki, J., Tambe, M., Ordonez, F., Kraus, S.: Efficient algorithms to solve bayesian stackelberg games for security applications. In: AAAI. pp. 1559–1562. AAAI, Washington, DC, U.S. (2008)

[15] Segovia-Ferreira, M., Rubio-Hernan, J., Cavalli, A.R., Garcia-Alfaro, J.: Cyber-resilience approaches for cyber-physical systems (2023). https://doi.org/10.48550/arXiv.2302.05402

[16] Sengupta, S., Chowdhary, A., Sabur, A., Alshamrani, A., Huang, D., Kambhampati, S.: A survey of moving target defenses for network security. IEEE Communications Surveys & Tutorials **22**(3), 1909–1941 (2020). https://doi.org/10.1109/COMST.2020.2982955

[17] Wright, M., Venkatesan, S., Albanese, M., Wellman, M.P.: Moving Target Defense against DDoS Attacks: An Empirical Game-Theoretic Analysis. In: 3rd ACM Workshop on Moving Target Defense. pp. 93–104. ResearchGate, Berlin, Chausseestraße 20, Germany (Oct 2016). https://doi.org/10.1145/2995272.2995279

[18] Yoon, S., Cho, J.H., Kim, D.S., Moore, T.J., Free-Nelson, F., Lim, H.: Attack Graph-Based Moving Target Defense in Software-Defined Networks. IEEE Transactions on Network and Service Management **17**(3), 1653–1668 (Sep 2020). https://doi.org/10.1109/TNSM.2020.2987085

[19] Zhang, H., Zheng, K., Wang, X., Luo, S., Wu, B.: Efficient strategy selection for moving target defense under multiple attacks. IEEE Access **7**, 65982–65995 (2019). https://doi.org/10.1109/ACCESS.2019.2918319

[20] Zscaler: What is Deception Technology? Importance & Benefits| Zscaler (2023), https://www.zscaler.com/resources/security-terms-glossary/what-is-deception-technology