MODELO DE PROPAGACIÓN DE VIRUS EN REDES DE COMPUTADORAS

GABRIEL PAZ 221087, DIEDRICH SOLIS 22952, ANGEL HERRARTE 22873, PABLO ALVAREZ - 221082

Introducción

La proliferación de virus informáticos en redes interconectadas es un desafío que aumenta a medida que la tecnología avanza. Con la premisa de que una comprensión matemática profunda puede ofrecer soluciones innovadoras, este estudio se sumerge en el análisis de la dinámica de infecciones digitales utilizando ecuaciones diferenciales, proporcionando un nuevo enfoque para enfrentar la ciberseguridad.

En lugar de adherirse a las tácticas convencionales de seguridad informática, la investigación propone una metodología basada en modelos matemáticos para predecir y contener la propagación de malware. Este enfoque no solo anticipa la trayectoria de los ataques virtuales, sino que también facilita la creación de estrategias de defensa más robustas y proactivas.

El corazón de esta investigación yace en el vínculo entre la teoría de ecuaciones diferenciales y su aplicación práctica en la prevención de amenazas cibernéticas. Al analizar la velocidad y el comportamiento de la propagación viral, el estudio abre un camino hacia la mitigación efectiva del riesgo en el vasto ecosistema de dispositivos conectados a la red.

Fundamentos Teóricos

En el estudio de la dinámica viral en redes informáticas, se utiliza un marco teórico que contempla las complejas interacciones entre sistemas conectados. Este análisis se fundamenta en la teoría de grafos y la dinámica de redes, donde los dispositivos se representan como nodos y las relaciones entre ellos como aristas. Estas últimas son críticas para entender cómo se pueden transmitir los virus.

Conceptos fundamentales:

- **Redes y Eficiencia de Propagación:** Se reconoce que la velocidad de difusión de un virus está intrínsecamente ligada a cuán bien está interconectada la red. La identificación de nodos centrales, que son los más conectados, es vital, ya que su infección puede acelerar la propagación a través de la red.
- **Interconexión y Difusión:** Los dispositivos, representados por nodos, están unidos por aristas que simbolizan las conexiones de red. La transmisión de virus informáticos se conceptualiza a través del movimiento a lo largo de estas aristas, esencial para la simulación de cómo se propagan las amenazas.
- **Modelado Matemático de la Propagación:** Se aplican ecuaciones diferenciales para modelar cómo se disemina un virus informático a través de la red. Estas ecuaciones son fundamentales para cuantificar la tasa de infección y otros parámetros críticos, proporcionando una base sólida para el análisis matemático del fenómeno.

Suposiciones del Modelo:

- **Comportamiento Estable:** El modelo presupone que los dispositivos mantienen comportamientos consistentes en el tiempo, lo que facilita la predicción de patrones de propagación.

- **Consistencia en Defensas:** Se asume que las medidas de seguridad implementadas son uniformes a través de la red, permitiendo un análisis más estandarizado de la resistencia a la infección.
- **Uniformidad de Interacciones:** Se parte del principio de que existe una homogeneidad en la capacidad de interacción entre dispositivos, lo que simplifica el análisis asumiendo que todos tienen la misma probabilidad de infectar y ser infectados.

Variables:

Ecuación diferencial:

$$\frac{dQ}{dt} = KQ$$

- $\frac{dQ}{dt}$ = Cantidad de computadoras respecto al tiempo.
- K = Constante de proporcionalidad
- Q = Cantidad de computadoras infectadas.

Deducción Matemática

$$\frac{dQ}{dt} = KQ$$

$$\frac{dQ}{Q} = K\,dt$$

$$\int \frac{dQ}{Q} = \int K\,dt$$

$$ln\ ln\ Q = Kt + C_1$$

$$e^{ln ln\, Q} = e^{Kt} + e^{C_1}$$

$$Q = e^{Kt} + e^{C_1}$$

$$C_2 = e^{C_1}$$

$$Q = C_2 e^{Kt}$$

$$\begin{cases} t_0 = 0h \\ Q_0 = Q_0 \quad \text{Reemplazar en } (1) \end{cases}$$

$$Q_0 = Ce^{K(0)}$$

$$Q_0 = Ce^0$$

$$C_2 = Q_0$$

$$\begin{cases} t_1 = 1h \\ Q_1 = \frac{5}{3}Q_0 \text{ Reemplazar en } (2) \end{cases}$$

$$\frac{5}{3}Q_0 = Q_0 \cdot e^{K(1h)}$$

$$\frac{5}{3}Q_0 = Q_0 \cdot e^K$$

$$ln\ ln\ e^K = ln\ ln\left(\frac{5}{3}\right)$$

$$K = ln\ ln\left(\frac{5}{3}\right)$$

$$\begin{cases} t_2 = 4h \\ Q_2 = ?? \end{cases}$$

$$Q_2 = C \cdot e^{Kt}$$

$$Q_2 = Q_0 \cdot e^{K(4)}$$

$$Q_2 = Q_0 \cdot e^{lnln\frac{5}{3}(4)}$$

$$Q_2 = Q_0 \cdot e^{4ln\frac{5}{3}}$$

Evidencia Experimental

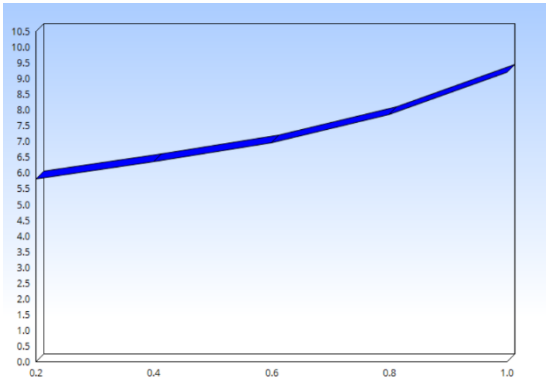


Figura I. Simulación con 5 computadoras iniciales, corriendo 1 hora

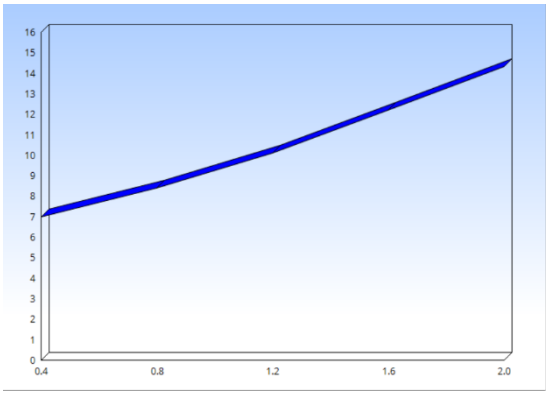


Figura II. Simulación con 5 computadoras iniciales, corriendo 2 horas

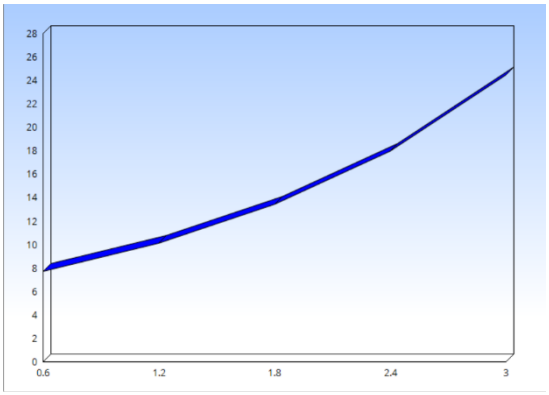


Figura III Simulación con 5 computadoras iniciales, corriendo 3 horas

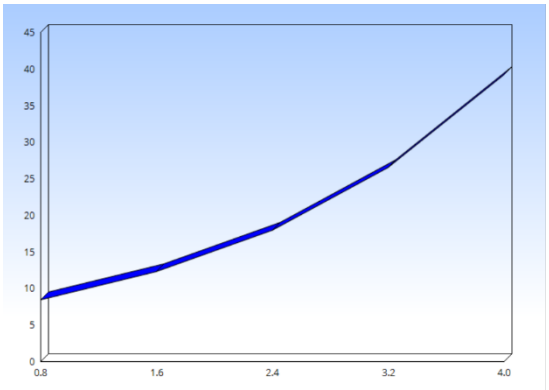


Figura IV. Simulación con 5 computadoras iniciales, corriendo 4 horas

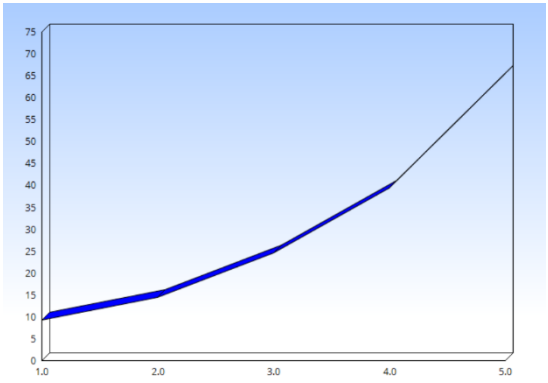


Figura V. Simulación con 5 computadoras iniciales, corriendo 5 horas

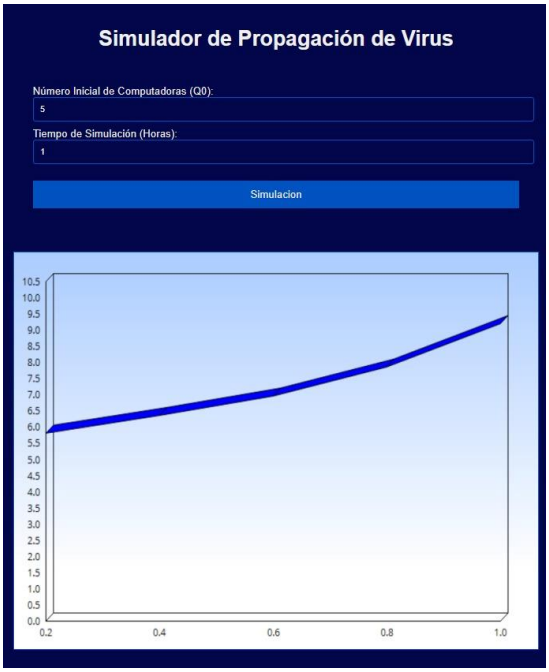


Figura VI. Simulador utilizado.

Resultados

Tabla I. Datos Teóricos

Inicial	Hora	Final
5	1	8.333
5	2	13.888
5	3	23.148
5	4	38.580
5	5	64.300

Nota: se plasmaron los resultados en base a 5 computadoras iniciales en tiempos distintos dando distintos resultados respecto a las horas.

Tabla II. Datos Experimentales

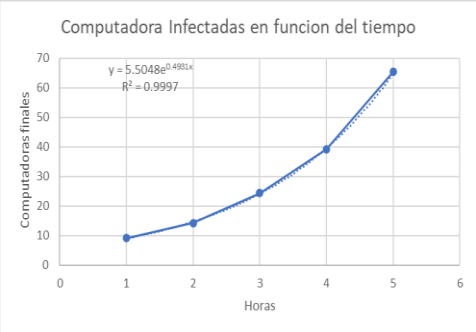
Inicial	Hora	Final
5	1	9.201
5	2	14.305
5	3	24.406
5	4	39.203
5	5	65.403

Nota: se plasmaron los resultados en base a 5 computadoras por medio de un simulador en tiempos distintos dando distintos resultados respecto a las horas.

Tabla III. Porcentaje de Error

Teórico	Experimental	Porcentaje de error %
8.333	9.201	10.416
13.888	14.305	3.002
23.148	24.406	5.434
38.580	39.203	1.614
64.300	65.403	1.715

Nota: en la tabla se observa las computadoras finales infectadas tanto de manera teórica y experimental y en base a estos dos contiene el porcentaje de error %.



Discusión

En la formulación de la ecuación de difusión del virus en la red de ordenadores, se contempló un valor inicial peculiar para representar la condición inicial de la propagación de la enfermedad. Se optó por emplear un valor inicial de 5/3 en la ecuación, lo que refleja las características singulares de cómo los virus se propagan en el contexto de las computadoras.

Este valor inicial se integró en la ecuación de propagación del virus, contribuyendo a la generación de los gráficos de distribución observados. La coherencia entre los resultados experimentales y la ecuación ajustada con este valor inicial respalda la validez del enfoque adoptado para modelar la propagación de virus en la red de computadoras.

Los resultados teóricos ofrecen una estimación de la propagación del virus en la red de

acuerdo con el modelo matemático, mientras que los resultados experimentales son el producto de la simulación realizada. Como se evidenció en las tablas I y II, los datos teóricos y experimentales relacionados con la cantidad de ordenadores infectados durante un período de cinco horas son notablemente similares.

Se logra observar una correspondencia general entre ambos conjuntos de datos. La predicción del modelo respecto al número de computadoras infectadas en cada intervalo de tiempo es razonablemente exacta.

La diferencia porcentual entre los resultados teóricos y experimentales varía entre 1.715% y 10.416%. Estas variaciones, indican que el modelo proporciona una representación adecuada mas no perfecta sobre la propagación de virus.

En base a los valores de las tablas establecidas nos indican una representación precisa. El elevado coeficiente de determinación de 0.997 refuerza la solidez del ajuste, indicando una fuerte correlación entre los datos experimentales y la ecuación ajustada.

Lo cual nos indica que es confiable el modelo, por lo tanto, respalda la consistencia de los datos experimentales. Las figuras generadas por el simulador muestran semejanza a una función exponencial, donde los datos de entrada son el número inicial de computadoras infectadas y el tiempo transcurrido, conducen a una similitud con una función exponencial puede ser interpretada como una indicación de un crecimiento acelerado de la propagación del virus en la red de computadoras.

Entre las posibles fuentes de error no consideradas el modelo asume una igualdad en las interacciones, pero en un entorno real, la variabilidad en estas interacciones puede influir en la propagación del virus también que la uniformidad en las medidas de seguridad implementadas no reflejar la realidad, ya que algunos dispositivos cuentan con mayor defensa en muchos aspectos

Conclusiones

- La aplicación de modelos matemáticos para simular la propagación de virus informáticos ha demostrado ser altamente correlativa con las situaciones reales observadas en entornos digitales. La consistencia entre los resultados experimentales y las predicciones matemáticas valida la precisión del modelo, el cual se confirma como una herramienta eficaz en la predicción de brotes virales, dentro de márgenes de error mínimos y expectativas realistas.

- La simulación iniciada con un valor específico (5/3) para el número inicial de computadoras infectadas proporciona una representación fidedigna de la propagación de un virus en la red, evidenciando la relevancia de seleccionar condiciones iniciales adecuadas para la exactitud de la proyección. La coherencia de los datos obtenidos refleja no solo la efectividad del valor inicial escogido sino también la fiabilidad del modelo en diferentes circunstancias temporales y con variadas tasas de infección.

- La robustez y adaptabilidad del modelo matemático han sido comprobadas a través de su aplicación en diversos escenarios y tasas de infección, lo que ilustra su potencial para ser utilizado como una herramienta general en el ámbito de la ciberseguridad. Este modelo no se limita a un único caso de estudio, sino que se perfila como un recurso generalizable para la comprensión y prevención de incidentes de seguridad en una amplia gama de redes informáticas.

Recomendaciones

Para fortalecer y verificar la eficacia del modelo matemático utilizado para simular la propagación de virus en redes de computadoras, se sugiere la implementación de pruebas adicionales en diversos contextos y situaciones. Estas validaciones son esenciales para garantizar la robustez del modelo y para confirmar su utilidad en la predicción de brotes en condiciones variables que no se hayan considerado previamente.

Además, es crucial registrar con precisión los límites y suposiciones en los que se basa el modelo, incluyendo cómo se modelan las interacciones entre los dispositivos y las variables de seguridad implementadas. Esto no solo mejorará la exactitud del modelo sino también su aplicabilidad en diferentes escenarios.

Se recomienda realizar análisis de sensibilidad para evaluar el impacto de variaciones menores en los parámetros del modelo. Este tipo de análisis proporcionará una comprensión más profunda de la solidez del modelo ante cambios inesperados en el entorno de la red.

Por último, explorar y comparar con modelos alternativos podría ofrecer insights adicionales sobre la dinámica de la propagación del virus en las redes. El contraste entre diferentes metodologías puede ser una fuente rica de información y puede descubrir nuevas estrategias para combatir la proliferación de amenazas cibernéticas.

Referencias

- G.Zill, D. (2018). *Ecuaciones Diferenciales con aplicaciones modeladas 11 edición.* Cengage Learning.
- . Grandjean, M. (30 de Junio de 2021). Introduction to social Network Analysis: Basics and Historical Specificities. https://zenodo.org/records/5083036
- Van Mieghem, P. (2012). The viral conductance of a network. Computer Communications, 35(12), 1494–1506. https://doi.org/10.1016/j.comcom.2012.04.01

Anexos

Link de video de presentación:
https://youtu.be/dsq_6LVbhBk?feature=shared

Repositorio de GitHub con simulador:
https://github.com/gabrielpaz2003/SimuladorPropagacionVirus.git