International Journal of Engineering Trends and Technology
ISSN: 2231–5381 / https://doi.org/10.14445/22315381/IJETT-V71I8P226

Volume 71 Issue 8, 295-303, August 2023

Original Article

Entropy of a Computer Network Under Propagation of Cyber-Attacks

Shiju Rawther[1], S. Sathyalakshmi[2]

[1,2]*Department of CSE, Hindustan Institute of Technology and Science, OMR, Padur, Chennai, Tamil Nadu, India.*

[1]*Corresponding Author : shiju.rawther@gmail.com*

Received: 19 May 2023 Revised: 29 July 2023 Accepted: 10 August 2023 Published: 15 August 2023

Abstract *- With the increasing reliance on computer networks for critical infrastructure and information exchange, the security of these networks has become a paramount concern. Cyber-attacks pose a significant threat, capable of exploiting vulnerabilities within a network and causing severe damage. Understanding the dynamics of cyber-attacks and their impact on the entropy of a computer network is crucial for developing effective defense mechanisms.*

In this research paper, the investigation is done on the entropy of a computer network during the propagation of cyber-attacks. This research paper also proposes a novel framework for modelling the network's entropy dynamics by integrating statistical measures and graph theory. By considering network attributes such as connectivity, traffic patterns, and attack vectors, through this study, a comprehensive approach is developed to quantify the changes in entropy caused by cyber-attacks through extensive simulations on realistic network topologies, analysis of the impact of various types of cyber-attacks on network entropy. The research findings reveal that successful cyber-attacks tend to increase the entropy of a network, indicating a higher degree of disorder and unpredictability. Furthermore, the study reveals that the entropy dynamics are influenced by factors such as attack intensity, attack duration, and the network's inherent resilience. Based on research analysis, it is concluded that an entropy-based metric for assessing network vulnerability to cyber-attacks. This metric allows network administrators to quantify the potential impact of an attack and prioritize security measures accordingly. Moreover, this study has also helped in developing a real-time monitoring system that leverages the entropy metric to detect and respond to ongoing cyber-attacks promptly.

This research paper contributes to the understanding of the complex relationship between cyber-attacks and network entropy. By exploring entropy as a measure of disorder in a network, This research paper provides valuable insights for designing resilient and secure computer networks. Ultimately, this work aims to enhance the overall security posture of computer networks and mitigate the risks associated with cyber-attacks. Using compartment labels Susceptible, Infectious, or Recovered, each computer network node can move between these compartments to simulate the propagation of cyber-attacks in a computer network. An attack on a computer network is predicted using a computer model. Propagation entropy can be measured to assess propagation uncertainties even when propagation choices are probabilistic. As part of this study, the compartmental epidemic model's capability has been adopted to prove the ability to predict entropy behaviour under cyber-attack.

Keywords *- Cyber-Attack propagation, Kermack-McKendrick model, Propagation entropy, Network security, Attack vectors.*

1. Introduction

In the ever-evolving landscape of an interconnected world, computer networks have emerged as the backbone of modern society, facilitating seamless communication, data exchange, and critical operations across diverse sectors. The proliferation of these networks has ushered in an era of unprecedented convenience and efficiency, revolutionizing the way we live and work. However, with this pervasive connectivity and dependence on digital infrastructure come significant risks, chief among them being the constant and insidious threat of cyber-attacks. Cyber-attacks represent a multifaceted menace that spans across the digital realm, exploiting vulnerabilities within network systems with malicious intent. These attacks can take various forms, such as malware infiltration, phishing scams, denial-of-service (DoS) attacks, ransomware, and more. Their motivations range from financial gain and data theft to ideological or

political agendas. Regardless of the attackers' motivations, the consequences of successful cyber-attacks can be devastating. They have the potential to compromise the integrity of sensitive data, disrupt critical services, impair functionality, and even lead to substantial financial losses and tarnished reputations for organizations and individuals alike.

As the reliance on computer networks intensifies across various industries, the imperative to secure these networks against cyber-attacks becomes paramount. A robust and comprehensive understanding of how cyber-attacks propagate within computer networks is crucial for developing effective strategies and techniques to defend against such threats. This understanding requires the exploration of the intricate dynamics underlying cyber-attack dissemination and the factors influencing their spread.

One fundamental concept that finds applications across diverse fields, including cybersecurity, is entropy. In information theory, entropy measures the uncertainty or randomness in a system. In the context of computer networks, the concept of entropy can be harnessed to assess the level of disorder and unpredictability induced by cyber-attacks. By quantifying the entropy of a computer network under the propagation of cyber-attacks, we can gain insights into the degree of chaos and uncertainty brought about by these malicious activities.

This research endeavor seeks to delve into the concept of entropy as it pertains to computer networks under the influence of cyber-attacks. We aim to explore how the entropy of a network evolves as cyber-attacks spread and how this entropy can be harnessed to assess the network's vulnerability and resilience in the face of such threats. By analyzing the entropy of a computer network under the propagation of cyber-attacks, we can gain valuable insights into the level of disorder and unpredictability introduced by these attacks, which, in turn, can inform the design of more effective defense mechanisms. We endeavor to shed light on the complex interplay between cyber-attack propagation and network entropy through comprehensive simulations and in-depth analysis. Our research findings will contribute to developing novel strategies for enhancing network security, incident response, and designing resilient computer systems. Moreover, this research seeks to expand the understanding of entropy's applicability in the realm of cybersecurity, forging new pathways for quantifying and mitigating the impact of cyber-attacks on computer networks.

2. Literature Survey

Most electronic gadgets are currently connected through cyberspace, so human activities and interactions can occur on multiple levels through cyberspace [1]. Since the decarbonization of energy systems has presented previously unheard-of challenges in terms of system complexity and operational unpredictability, it is imperative to utilize cutting-edge technology to enable real-time, autonomous operation and control of the power systems [2]. In recent years, the traditional electrical system has evolved into a smart grid that utilizes both cyber and physical technologies simultaneously. However, attackers may construct well-coordinated attacks that have catastrophic results by exploiting physical or cyber-layer vulnerabilities [3]. A major segment of the Internet of Things is the smart grid, a rapidly expanding essential infrastructure featuring the integration of power plants and the Internet of Things (IoT). However, recent events illustrate how adversaries might develop attacks against SG by exploiting IoT device weaknesses [5,35].

Cyberspace is a way of linking sensitive infrastructure and/or systems along with critical information [6]. Despite the rapid development of cyber security, it is still in its infancy in modern cyberspace [7-10]. There are currently investigations into both quantitative and qualitative approaches to assessing cyber threats [12,13,37]. Cyber network systems are also being analyzed using quantitative techniques using attack trees and their variations [14–16]. A differential equation-based epidemic model has been used in recent years to investigate the effects of malicious objects on networks and the assault and defense of malicious objects [17-18]. As a result of this analysis, researchers were able to develop a framework for defensive mechanisms as well as reduce the vulnerability to Nodes that may be assigned to compartments, such as Susceptible (S), Infectious (I), and Recovered (R) nodes, allowing them to move among these compartments to simulate the transmission of cyber-attacks.

Entropy can be used to identify malicious injection of data in state vectors, which can cause temporal and spatial correlations to deviate from their normal behavior [19]. Information theory can be used to analyze cyber-security processes using entropy and mutual information metrics. According to recent studies [21,22,39], entropy measurement is crucial to analysing cyber-security challenges.

Li, H., Zhou, Q., & Dong, Q. (2021) present an entropy-based approach for detecting botnet attacks in Software-Defined Networking (SDN) [40]. The study focuses on analyzing network traffic entropy to identify malicious activities associated with botnets. Their approach demonstrates the effectiveness of entropy analysis in enhancing botnet detection mechanisms in SDN environments.

Mohsin, M., Ullah, A., & Jan, S. (2021) propose a framework for assessing network security using information entropy analysis. They emphasize the significance of entropy analysis as a metric for measuring network security and highlight its potential in quantifying the randomness and unpredictability of network traffic [27].

Song, Q., Zhang, Z., & Sun, Y. (2022) propose a novel approach for intrusion detection based on network traffic entropy analysis. They leverage entropy analysis to identify anomalies and potential intrusions in network traffic. Their work highlights the potential of entropy-based metrics in enhancing intrusion detection systems [28].

Li, W., & Zhang, X. (2022) investigate entropy analysis of dynamic network topology based on attack strategies. They propose an entropy-based approach to assess the security and resilience of dynamic networks under various attack scenarios. Their research emphasizes the importance of considering network topology dynamics in entropy analysis for effective security evaluations [29].

Luo, B., Li, M., & Zhang, T. (2022) present an entropy-based network anomaly detection algorithm that utilizes feature selection techniques. Their approach aims to improve the accuracy and efficiency of network anomaly detection by selecting relevant features based on entropy analysis. Their work demonstrates the potential of entropy-based feature selection in network security applications [30].

Peng, Y., Jiang, S., & Liu, H. (2022) conducted research on a network security situation awareness model based on network traffic entropy analysis. Their study focuses on developing a comprehensive model that utilizes entropy analysis to enhance network security situational awareness. They emphasize the importance of real-time network traffic analysis and entropy-based metrics for effective security monitoring [41].

Qiao, Y., Shi, R., & Chen, X. (2023) propose an entropy-based dynamic network security assessment model under cyber-attacks. They develop a framework that utilizes entropy analysis to assess network security and evaluate cyber-attacks' impact on network behavior [32]. All existing research aims to enhance the understanding of network security dynamics and provide insights for proactive defense strategies. Changing state of each compartment or node plays a crucial role in determining how cyberattacks spread.

Through differential equation-based modelling, the number of infected and uninfected nodes over time can be predicted. A compartmental epidemic model can also be used to investigate a node's transient immunity within a computer network. While spreading a virus can be viewed as a random process, modelling in a random environment shows certain patterns to the expansion of infected (and non-infected) nodes. The goal of this article is to demonstrate how assaults in a closed, random network follow the pattern of ODEs.

For malicious items to spread throughout a computer network, a sophisticated, dynamic procedure must be followed. The seed of an attack infects the first node, and from there, it spreads to other nodes. The seed node creates a link between itself and the neighborhood nodes closest to the network and distributes the virus payloads across it. As a result of the procedure, a network attack connection is created. As the infection spreads, all infected nodes create a network that resembles a center-sponsored star network once equilibrium is reached. By measuring entropy, we can measure how unpredictable a process is. Since cyber-attacks tend to be random, entropy may be used to quantify their uncertainty.

The study of entropy in computer networks has gained significant attention in the context of analyzing network dynamics under cyber-attacks. One approach to investigating the propagation of cyber-attacks and their impact on network security is through the application of mathematical models. In this regard, the Kermack-McKendrick model, originally developed to study infectious disease spread, can be adapted to capture the cyber-attack spread in a computer network. This research aims to explore the entropy of a computer network under the propagation of cyber-attacks using the Kermack-McKendrick model.

2.1. Past Work

Previous research has focused on applying mathematical models to study cyber-attack propagation and assess network security. For instance, Pastor-Satorras et al. (2015) explored epidemic processes in complex networks, providing insights into the spread of attacks and vulnerabilities. Xynos et al. (2017) developed a bi-virus competing spreading model to analyze the behavior of different infection rates in a network. These studies provide valuable foundations for studying the propagation of cyber-attacks using mathematical models.

2.2. Novelty

This research is novel in the application of the Kermack-McKendrick model to the analysis of the entropy of a computer network that is subjected to malicious cyber-attacks. The simulation of cyber-attacks within the network and observations of the entropy changes during propagation can be carried out by modifying this model. Cyber-attacks are dynamic and impact network security in different ways. This approach allows us to understand them better. In this study, we are looking at how the spread of attacks impacts the entropy of the network, potentially resulting in increased vulnerabilities for the network or the need to mitigate them. The results of this research will be useful for developing better solutions and strategies for protecting networks against cyber-attacks by understanding the relationship between cyber-attack spread and entropy changes.

Section III of this paper defines the propagation entropy of cyber-attacks using the Kermack-McKendrick model [18]. A cyber-attack simulation is described in Section IV of the study, as well as how entropy increases in the system in the simulation environment, and the study concludes in Section V.

3. Propogation Entropy using Compartmental Model

The interconnected nodes within a network can be categorized into three distinct states concerning an actual cyber-attack: susceptible (S), infectious (I), or recovered (R). Each node can be analogously viewed as a compartment transitioning between these stages. This mathematical modeling approach finds its roots in the Kermack-McKendrick model [19], a framework based on ordinary differential equations with deterministic solutions. Key parameters of this model include the contact rate between nodes, the infection rate, and the recovery rate. Leveraging the Kermack-McKendrick model offers a valuable tool for predicting and comprehending the spread of cyber-attacks within a network.

The model enables a holistic view of the dynamics of attack propagation, facilitating the identification of vulnerable points within the network. By studying the interactions and transitions of nodes between susceptible, infectious, and recovered compartments, the model grants insights into cyber-attack progression. Armed with this understanding, network administrators can strategically deploy preventive measures and allocate resources to safeguard the network.

Furthermore, the Kermack-McKendrick model empowers administrators to gauge the effectiveness of countermeasures implemented to thwart cyber-attacks. Administrators can assess their efficacy in mitigating the spread of attacks by adjusting the model's parameters to represent the impact of countermeasures such as patching vulnerable nodes or implementing firewalls.

In essence, the Kermack-McKendrick model, represented by ordinary differential equations, serves as a powerful analytical tool to evaluate the dynamics of cyber-attack propagation and assess the network's vulnerability. This mathematical framework equips network administrators with the ability to proactively identify high-risk nodes and devise preventive measures accordingly, enhancing the overall resilience of the network against potential cyber threats. Additionally, the model aids in measuring the effectiveness of defensive strategies, allowing administrators to fine-tune their approaches and continuously improve the network's security posture. Ultimately, by leveraging the insights offered by the Kermack-McKendrick model, network administrators can safeguard their systems against cyber-attacks and promote a safer and more secure digital environment. The following is a representation of an ordinary differential equation:

$$\frac{dS}{dt} = -\alpha SI + \gamma R \qquad (1)$$

$$\frac{dI}{dt} = \alpha SI - \beta I \qquad (2)$$

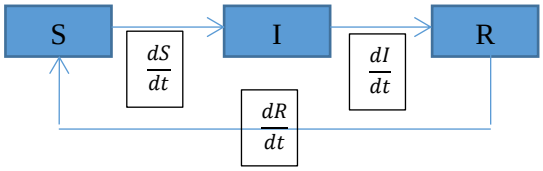


Fig. 1 States of nodes of a network

$$\frac{dR}{dt} = \beta I - \gamma R \qquad (3)$$

Since,

$$\frac{dS}{dt} + \frac{dI}{dt} + \frac{dR}{dt} = 0$$

$$S(t) + I(t) + R(t) = \text{constant}.$$

Hence, for the computational analysis, we can consider,

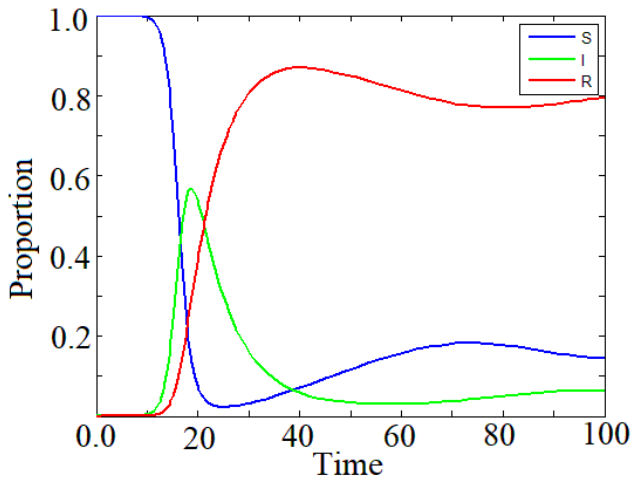
$$S(t) + I(t) + R(t) = 1 \qquad (4)$$

In terms of propagation entropy at t, the system can be described by,

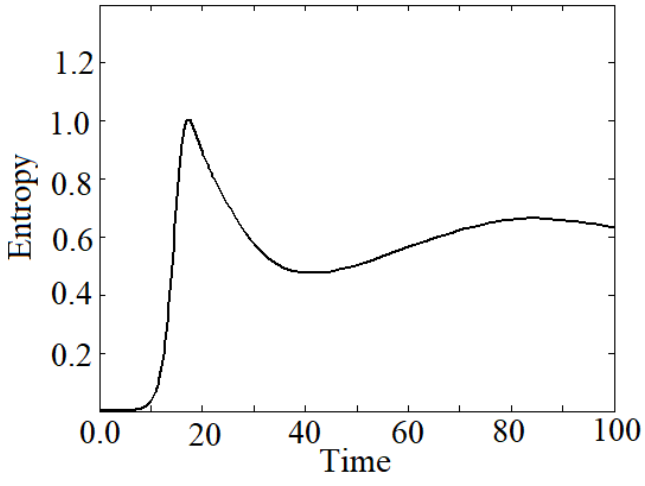
$$H(t) = -S(t)\log S(t) - I(t)\log I(t) - R(t)\log R(t) \qquad (5)$$

The propagation of cyber-attacks within a network can introduce a degree of uncertainty akin to entropy, which encompasses the overall unpredictability and disorder in the network. This entropy can serve as a valuable metric for estimating the network's uncertainty and potential security risks. By comprehending this uncertainty, network administrators gain a powerful tool to promptly identify and respond to threats posed by malicious activities or security breaches. Leveraging the concept of network entropy, administrators can proactively safeguard the network from malevolent actors. For instance, by monitoring the network's entropy levels, administrators can swiftly detect abnormal patterns or spikes indicative of malicious traffic attempting to infiltrate the system. Armed with this knowledge, they can promptly implement measures to block such intrusions, preventing potential harm and data compromise.

Furthermore, network administrators can utilize detailed activity logs to monitor and analyze network behavior over time. The information gleaned from these logs can be instrumental in identifying any suspicious activity that may signify a security breach. Armed with an understanding of the network's entropy and the potential security threats it faces, administrators can promptly respond to and mitigate the impact of such breaches, minimizing the damage caused. Moreover, the insights derived from monitoring the network's entropy can expedite the diagnosis and resolution of existing problems within the network. Administrators can swiftly detect and address anomalies or vulnerabilities by continuously monitoring entropy levels before they escalate into more significant issues. This proactive approach ensures a higher level of network stability and resilience.

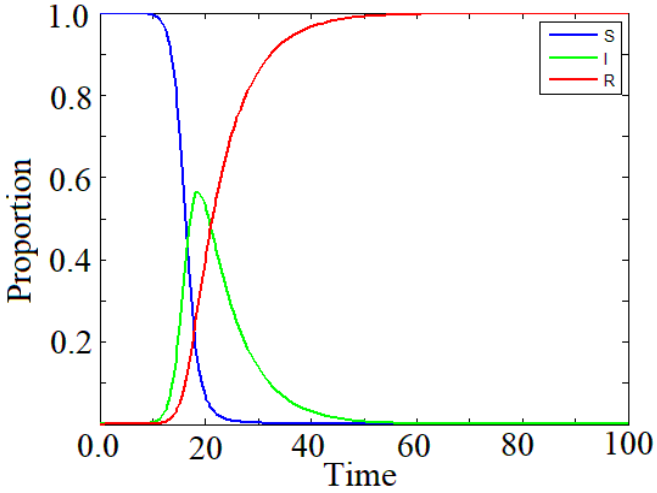


(a)

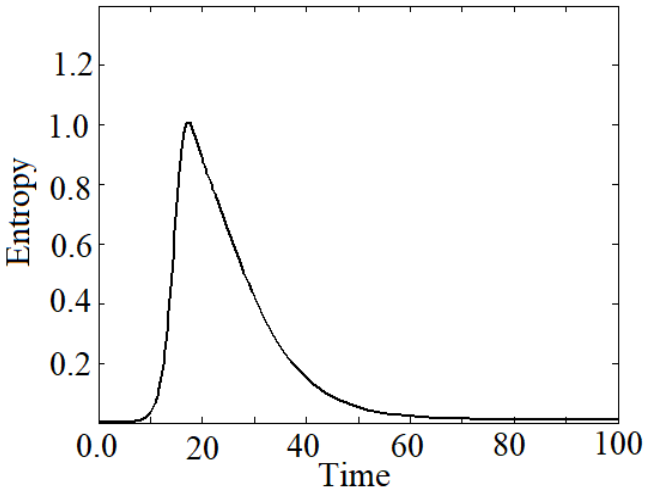


(b)

Fig. 2 (a) S, I and R for α = 1.0, β = 0.15, γ = 0.01 and S(0) = 1 and (b) the propagation entropy of the network due to cyber-attack



(a)



(b)

Fig. 3 (a) S, I and R for α = 1.0, β = 0.15, γ = 0 and S(0) = 1 and 3 (b) the propagation entropy of the network due to cyber-attack

The time-dependent solution for the system of equations (1)-(4) is depicted in Figure 2(a) for specific parameter values of α = 1.0, β = 0.15, γ = 0.01, and an initial value of S(0) = 1. This representation offers a visual understanding of how the system evolves over time and how the nodes transition between susceptible, infectious, and recovered compartments under the influence of cyber-attack propagation.

According to Fig 3 (a), temporary immunity does not exist, and the S, I, and R curves show no relationship. According to Figure 3(a), nodes cease to be infectious when temporary immunity reaches saturation or after a long period of time. Over time, however, the most susceptible nodes (S) become recovered nodes (R). There is an equilibrium state known as the basic reproductive number (R0) between the susceptible (S), infected (I), and recovered (R) nodes. High R0 indicates a higher risk of infection since it determines how far the malware spreads.

The disease cannot spread once there are zero I nodes, and the S and R nodes are in equilibrium due to the dynamic balance between S, I, and R nodes. This equilibrium state is known as the basic reproductive number (R0), which is determined by the number of susceptible (S) and recovered (R) nodes. A higher R0 means a greater risk of infection. The entropy of the system is illustrated in Figure 3(b).

4. Simulation

In a 100X100 node network, a single cyber-attack can affect multiple subsequent nodes, allowing an analysis of cyber-attacks on computer networks. The attack is modeled as a random variable with an independent and identical distribution based on the probability of selection. In order for an attack to succeed, it must affect a large number of nodes. It is determined which node will be selected next using simulations to estimate the probability of success. Our model assumes that infected nodes (I) will choose their subsequent

neighbours randomly among their eight nearest neighbors. Three outcomes are possible when a node is affected: recovery (R), maintenance (I), and spread (S).

Consequently, our probability-based decision included considering three possible outcomes at random. A node can become susceptible (S) or remain susceptible (R) once the random choice has been recovered (R). There is the option to set different probabilities for each of the three options (R, I, S). With this approach, the model is able to incorporate the different rates of recovery, maintenance, and spread into the equation. To determine whether the decision-making process was effective, the model's results are analyzed.

4.1. Learning Effect on Spread Probability

The impact of computer viruses on learning is pragmatic. Unlike conventional models, scale-free models have an anti-virus defense mechanism that helps prevent cyberattacks from spreading quickly. In terms of cyberattack spread probability, we can calculate pi,j,t as the probability that a cyberattack will spread from node I to node j at time step t, with pi,j,t remaining constant over all time steps. This amount can occasionally decrease due to infection-related propagation, which users acknowledge. As a consequence, the probability decreases steadily due to the learning effect [23,24].

$$p_{i,j,t} = \frac{p_{i,j,t-1}}{(t+1)^q} \tag{6}$$

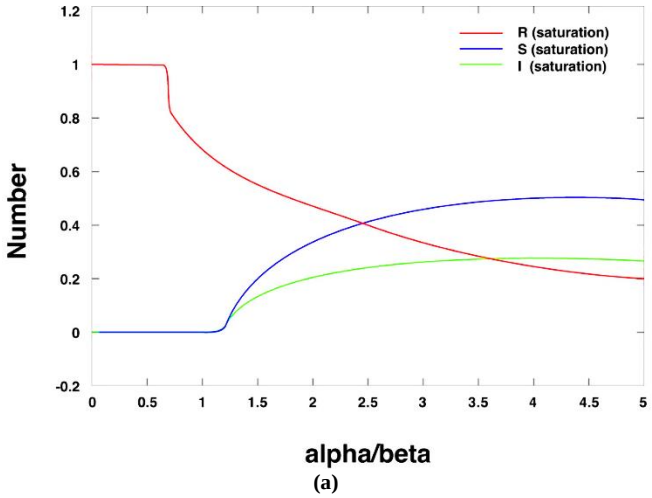
The rate of learning is represented by q in this case. As a result of looking at the learning effect, it is possible to conclude:

$$\lim_{t\to\infty} p_{i,j,t} = 0 \tag{7}$$

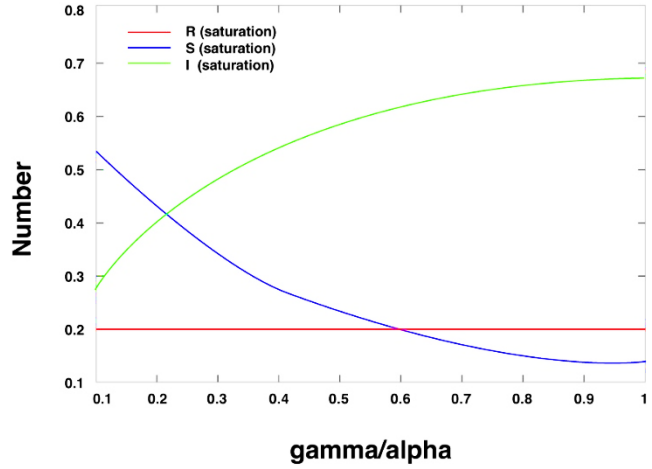
$$p_{i,j,t2} \le p_{i,j,t1} \le 1 \quad \text{for} \quad t1 < t2 \le \infty \tag{8}$$

Here the equality $p_{i,j,t2} = p_{i,j,t1}$holds without any learning effect.

Based on the likelihood of transition in each node's 8 directions, we can create a probability score for each node since we simulated attacks spreading in a random environment (since every node has 8 nearest neighbour nodes). During simulation, we decided that nodes that have a probability score greater than 0.85 stay S, nodes that have a probability score less than 0.15 remain R and nodes that are still around 0.5 stay I. During saturation, S, R, and I reach constant values for various probabilities. A simulation's outcome is depicted in Figure 4 along with a probability score for (S, R, I) = (0.85,0.15,0.5), and Figure 5 shows the proportion of R, S, I over time.



(a)



(b)

Fig. 4 (a) Probability Score (b) Simulation's Outcome

As shown in Fig.4 On the 100X100 matrix, the red, blue, and green curves represent the Recovered (R), Susceptible (S), and Infectious (I) nodes. Figure 5 illustrates how the curves produced by simulation research resemble those produced by compartmental models (1-3).

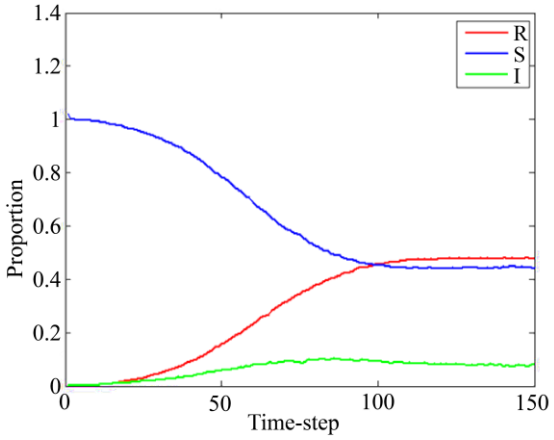
The results suggest that simulations can be used to accurately estimate the spread of infectious disease, as the results are in agreement with those produced by compartmental models. This lends credibility to the simulation approach for predicting the spread of infectious diseases.

For instance, researchers in the field of infectious diseases have found that simulations of the spread of the 2019-nCoV coronavirus were in agreement with compartmental models, lending credibility to the simulation approach. This means that the simulations can be used to predict the spread of the virus accurately and also to develop strategies for containing it.

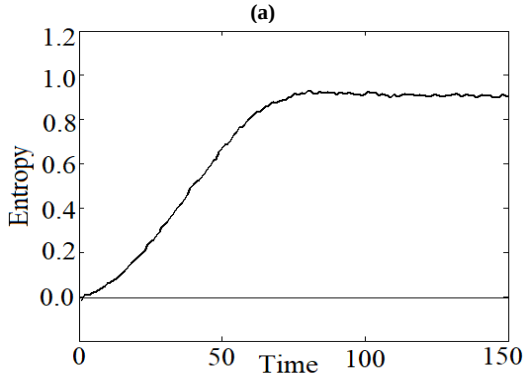
The simulations can also be used to identify areas where the virus is likely to spread and to develop preventative measures. For example, the simulations can be used to identify the populations most at risk of contracting the virus and to develop targeted strategies aiming at reducing the risk for these populations.

Figure 4 illustrates the outcome of a simulation based on incremental time steps of 100 nodes. Although cyber-attacks are supposed to be random, closed networks show specific patterns. Figure 4(a) shows the number (or percentage) of infected and uninfected nodes. In Figures 2(a) and 3(a), you can see how many (or how many%) of the nodes are infected.

A cyberattack affects the propagation entropy of 100X100 nodes at different time steps, as shown in Fig 4(b). Figure 4 shows that cyber-attacks spread by increasing the number of affected nodes and following a center-sponsored pattern. This indicates that cyber-attacks are not as random as they may appear; rather, they can be traced to specific sources and follow specific patterns. This is due to the fact that cyber-attacks tend to spread from a single source and then spread outwards from there. These patterns can be observed in the figures as the number of affected nodes and the propagation entropy increase as the attack progresses.



(a)



(b)

Fig. 5 (a) S, I and R for the simulation study shown in Fig 5 and (b) Propagation Entropy of the 100X100 nodes is shown in different time steps due to cyber-attack

Here is an expression of the algorithm in the proposed probabilistic simulation:

Ingestion: A network of nodes G(V, E) that is scale-free
Each node P has an initial probability matrix
Result: At every time step, the propagation matrix
In this case, the Time step considered = 0.0, 0.1,0.2,0.3….

1. Update probability matrix using $p_{i,j,t} = \frac{p_{i,j,t-1}}{(t+1)^q}$
2. Assume that node k has a probability score of $\sum_{(i,j)\in Neighbour\,of\,k} V(i,j)p_{i,j,t}$
3. S, I, and R probability scores should be classified
4. Produce a matrix for propagation

5. Conclusion & Scope for Future Work

In this study, it is demonstrated how compartmental models and simulation study findings are identical when it comes to cyber-attack propagation. Simulating the transmission of harmful objects in a computer network is a good way of tracing the transmission of harmful objects because there is no evidence of actual data-driven cyber-attacks. The proposed study examines the cyber-attack process by measuring the randomness of cyber-attacks in a closed network using propagation entropy. While the spread of a cyber-attack may appear random, some patterns can be identified.

As a measure of randomness, propagation entropy can quantify attack propagation's unpredictable nature. Mathematics and probabilistic simulations of a similar issue were used to demonstrate similarities between the solutions. There will be great interest in studying the relationship between cyber-attack transmission entropy and simulation likelihood scores for computer networks. This research can help identify new vulnerabilities in existing computer networks and strengthen defences to reduce the risk of cyber-attacks. It can also help to develop strategies to mitigate the spread of cyber-attacks and protect critical systems and data. These strategies can be implemented in real-world situations to protect data and critical systems from cyber-attacks.

Additionally, this research can help inform and educate users on the importance of cybersecurity measures. For example, this research could help to create guidelines and protocols to ensure that users are aware of the necessary security measures to protect their data, such as using strong passwords and updating software regularly. In addition, the research can provide insights on the best practices for implementing security measures, such as educating users on the importance of using secure networks, encrypting data, and using two-factor authentication. This research can also help to identify potential weak points in existing security systems and suggest ways to strengthen them.

References

[1] Gholamreza Aghajani, and Noradin Ghadimi, "Multi-Objective Energy Management in a Micro-Grid," *Energy Reports*, vol. 4, pp. 218-225, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[2] Lanting Zeng et al., "Physics-Constrained Vulnerability Assessment of Deep Reinforcement Learning-based SCOPE," *IEEE Transactions on Power Systems*, vol. 38, no. 3, pp. 2690-2704, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[3] Zhenyong Zhang et al., "SPMA: Stealthy Physics-Manipulated Attack and Countermeasures in Cyber-Physical Smart Grid," *IEEE Transactions on Information Forensics and Security*, vol. 18, pp. 581-596, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[4] N. Priyanka, and V. Vetriselvi, "Penetration Testing for Software Defined Networks against DOS Attack," *SSRG International Journal of Computer Science and Engineering*, vol. 3, no. 8, pp. 10-13, 2016. [CrossRef] [Publisher Link]

[5] Zhenyong Zhang et al., "Security Enhancement of Power System State Estimation with an Effective and Low-Cost Moving Target Defense," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 53, no. 5, pp. 3066–3081, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[6] Olalekan Adeyinka, "Internet Attack Methods and Internet Security Technology," *Modeling & Simulation*, pp. 77-82, 2008. [CrossRef] [Google Scholar] [Publisher Link]

[7] G.A. Marin, "Network Security Basics," *Security & Privacy, IEEE*, vol. 3, no. 6, pp. 68-72, 2005. [CrossRef] [Google Scholar] [Publisher Link]

[8] P.W. Dowd, and J.T. McHenry, "Network Security: It's Time to Take it Seriously," *Computer*, vol. 31, no. 9, pp. 24-28, 1998. [CrossRef] [Google Scholar] [Publisher Link]

[9] Amirreza Zarrabi, and Alireza Zarrabi, "Internet Intrusion Detection System Service in a Cloud," *International Journal of Computer Science Issues*, vol. 9, no. 5, pp. 308-315, 2012. [Google Scholar] [Publisher Link]

[10] F. L. Greitzer et al., "Predictive Modeling for Insider Threat Mitigation," PNNL Technical ReportPNNL-SA-65204, Richland, WA: Pacific Northwest National Laboratory, 2009. [Google Scholar]

[11] Shiju Rawther, and S. Sathyalakshmi, "Cyber Attack Link Formation in a Network," *International Journal of Engineering Trends and Technology*, vol. 71, no. 5, pp. 191-196, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[12] Roger G. Johnston, "Changing Security Paradigms," *Journal of Physical Security*, vol. 4, no. 2, pp. 35-47, 2010. [Google Scholar] [Publisher Link]

[13] M. Dacier, Y. Deswarte, and M. Kaâniche, "Models and Tools for Quantitative Assessment of Operational Security," *Information Systems Security*, Chapman & Hall, Ltd. London, pp. 177-186, 1996. [CrossRef] [Google Scholar] [Publisher Link].

[14] Davide Balzarotti, Mattia Monga, and Sabrina, "Assessing the Risk of Using Vulnerable Components," *Quality of Protection: Security Measurements and Metrics, Springer Science Business Media, LLC*, pp. 65-77, 2006. [Google Scholar] [Publisher Link]

[15] Elizabeth LeMay et al., "Model-based Security Metrics using ADversary VIew Security Evaluation (ADVISE)," *Proceedings of the 8th International Conference on Quantitative Evaluation of SysTems, Aachen, Germany*, pp. 191-200, 2011. [CrossRef] [Google Scholar] [Publisher Link]

[16] Romualdo Pastor-Satorras et al., "Epidemic Processes in Complex Networks," *Reviews of Modern Physics*, vol. 87, no. 3, 2015. [CrossRef] [Google Scholar] [Publisher Link]

[17] Lu-Xing Yang, Xiaofan Yang, and Yuan Yan Tang, "A Bi-Virus Competing Spreading Model with Generic Infection Rates," *IEEE Transactions on Network Science and Engineering*, vol. 5, no. 1, pp. 2-13, 2017. [CrossRef] [Google Scholar] [Publisher Link].

[18] William Ogilvy Kermack, and A. G. McKendrick, "A Contribution to the Mathematical Theory of Epidemics," *Proceedings of the Royal Society A*, vol. 115, no. 772, pp. 700–721, 1927. [CrossRef] [Google Scholar] [Publisher Link]

[19] Moslem Dehghani et al., "Cyber Attack Detection Based on Wavelet Singular Entropy in AC Smart Islands: False Data Injection Attack," *IEEE Access*, vol. 9, pp. 16488-16507, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[20] Nguyen Huy Binh, and Le Trung Kien, "Counteraction Against Digital Data Leak: Open Source Software for Intrusion Detection and Prevention," *International Journal of Engineering Trends and Technology*, vol. 69, no. 3, pp. 17-22, 2021. [Google Scholar] [Publisher Link]

[21] Ke Liu et al., "Detection and Localization of Cyber Attacks on Water Treatment Systems: An Entropy-Based Approach," *Front Frontiers of Information Technology & Electronic Engineering*, vol. 23, pp. 587–603, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[22] Mohammad Irshaad Oozeer, and Simon Haykin, "Cognitive Risk Control for Mitigating Cyber-Attack in Smart Grid," *IEEE Access*, vol. 7, pp. 125806-125826, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[23] Shiju Rawther, and S. Sathyalakshmi, "Entropy Analysis of Cyber-Attack Propagation in Network," *13th International Conference on Computing Communication and Networking Technologies*, pp. 1-4, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[24] Mina Youssef, and Caterina Scoglio, "Optimal Network-Based Intervention in the Presence of Undetectable Viruses," *IEEE Communications Letters*, vol. 18, no. 8, pp. 1347-1350, 2014. [CrossRef] [Google Scholar] [Publisher Link]

[25] John C Lang et al., "Analytic Models for Sir Disease Spread on Random Spatial Networks," *Journal of Complex Networks*, vol. 6, no. 6, pp. 948–970, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[26] Varanasi Usha Bala, Akhil Karrothu, and B. Sanat Kumar, "Network Packet Capturing and Incidence Response Planning to Avoid Ransomware," *SSRG International Journal of Computer Science and Engineering*, vol. 5, no. 5, pp. 1-5, 2018. [CrossRef] [Publisher Link]

[27] H. Li, Q. Zhou, and Q. Dong, "An Entropy-based Approach for Detecting Botnet Attacks in Software-Defined Networking," *Computers & Security*, vol. 107, 2021.

[28] M. Mohsin, A. Ullah, and S. Jan, "Towards Assessing Network Security Using Information Entropy Analysis," *Computers, Materials & Continua*, vol. 68, no.1, pp. 851-867, 2021.

[29] Q. Song, Z. Zhang, and Y. Sun, "A Novel Approach for Intrusion Detection Based on Network Traffic Entropy Analysis," *Future Internet*, vol. 14, no. 1, 2022.

[30] W. Li, and X. Zhang, "Entropy Analysis of Dynamic Network Topology based on Attack Strategy," *Wireless Personal Communications*, pp. 1-14, 2022.

[31] I. Lakshmi, "Security Analysis in Internet of Things Using Ddos Mechanisms," *SSRG International Journal of Mobile Computing and Application*, vol. 6, no. 1, pp. 19-24, 2019. [CrossRef] [Publisher Link]

[32] Y. Peng, S. Jiang, and H. Liu, "Research on Network Security Situation Awareness Model Based on Network Traffic Entropy Analysis," *Security and Communication Networks*, 2022.

[33] Alex Mathew, "Cyber-security: Identity Deception Detection on Social Media," *International Journal of Engineering Trends and Technology*, vol. 67, no. 9, pp. 55-57, 2019. [CrossRef] [Publisher Link]

[34] Y. Qiao, R. Shi, and X. Chen, "Entropy-Based Dynamic Network Security Assessment Under Cyber-Attacks," *Journal of Network and Computer Applications*, vol. 197, 2023.

[35] Zhenyong Zhang et al., "A Double-Benefit Moving Target Defense Against Cyber–Physical Attacks in Smart Grid," *IEEE Internet of Things Journal*, vol. 9, no. 18, pp. 17912-17925, 2022. [CrossRef] [Google Scholar] [Publisher Link].

[36] Animesh Kumar, Sandip Dutta, and Prashant Pranav, "A Comparative Study of DDoS Attack in Cloud Computing Environment," *SSRG International Journal of Electronics and Communication Engineering*, vol. 10, no. 7, pp. 87-96, 2023. [CrossRef] [Publisher Link]

[37] Konstantinos Xynos et al., "Penetration Testing and Vulnerability Assessments: A Professional Approach," *Proceedings of the 1st International Cyber Resilience Conference*, Edith Cowan University, Perth Western Australia, pp. 23-24, 2010. [Google Scholar] [Publisher Link]

[38] Richa Kunal Sharma, and Nalini Kant Joshi, "Security and Privacy Problems in Cloud Computing," *International Journal of Computer and Organization Trends*, vol. 9, no. 4 pp. 30-39, 2019. [CrossRef] [Publisher Link]

[39] Ghaith Husari et al., "Using Entropy and Mutual Information to Extract Threat Actions from Cyber Threat Intelligence," *IEEE International Conference on Intelligence and Security Informatics*, pp. 1-6, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[40] S. Li, C. Chen, and X. Chen, "Entropy Analysis of Network Traffic for Detecting Stealthy Covert Channels," *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 2754-2769, 2021.

[41] B. Luo, M. Li, and T. Zhang, "Entropy-based Network Anomaly Detection Algorithm using Feature Selection," *Journal of Information Security and Applications*, vol. 65, 2022.