International Journal of Engineering Trends and Technology
ISSN: 2231–5381 / https://doi.org/10.14445/22315381/IJETT-V71I5P220

Volume 71 Issue 5, 191-196, May 2023


*Original Article*

# Cyber Attack Link Formation in a Network

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: 18 February 2023 Revised: 07 May 2023 Accepted: 16 May 2023 Published: 25 May 2023

***Abstract*** *- The threat of cyber-attacks has become a major concern for organizations of all sizes. The linkage between different components is an important factor in detecting and mitigating cyber-attacks. An investigation of the link formation between cyber-attacks and a network is presented in this research article. This study analyzes the behaviour of attackers and the evolution of attack campaigns within a network and proposes a method for tracing the links between different components in an attack. Cyber-attacks are analyzed based on their characteristics, and the nature of them is revealed. The study results indicate that attackers often use multiple entry points and different attack methods to get into a target network. It has been observed that attackers tend to use infrastructure and techniques across campaigns, providing evidence of the existence of networks of attackers. Creating a link between the attack node and other nodes propagates a cyber-attack in a network. At equilibrium, cyber-attacks propagate through a centre-sponsored start network even though the choice of forming a link is probabilistic. A cyber-attack in a network is analyzed using probabilistic link formation in this paper for the formation of a centre-sponsored start network. This study will help organizations improve their cyber defences by improving their understanding of how cyber-attacks from their links.*

***Keywords*** *- Cyber-attack, Network, payoff, Equilibrium, Star network, Attack-link formation.*

## 1. Introduction

A majority of electronic devices are connected to cyberspace today, allowing human activity and interaction at different levels [1]. A connected system is comprised of information, sensitive infrastructure, and/or systems [2]. Cyber-security is still in its infancy at a time when cyberspace is developing at an accelerating pace [3-6]. It is currently being investigated how to analyze cyber threats in both qualitative and quantitative ways [7-9]. For analyzing cyber network systems, researchers are using attack trees, as well as their variants, and quantitative methods.

In a number of studies [13-15] to provide a framework for defence mechanisms while alleviating the attack problem, differential equation-based epidemic modelling has been used to study attacks and defences of malicious objects and their consequences on networks. In this way, attack trajectories can be analyzed in greater detail, leading to a better understanding of cyber-attack dynamics. In addition, the network's most vulnerable parts can be identified along with an evaluation of the defensive mechanism.

By understanding the attack dynamics, organisations can develop strategies to prevent future attacks and improve their security posture. Additionally, more efficient defence strategies can be implemented to protect the most vulnerable parts of the network.

There are no studies examining the link formation of cyber-attacks in a network, which is the research gap discussed in this article. Prior studies have analyzed the behaviour of attackers and the evolution of attack campaigns, but not specifically on how different components of an attack are linked. To improve the defence against cyber-attacks, organizations must understand the link formation of these attacks.

An important aspect of the article is that it emphasizes the growing concern of cyber-attacks for organizations of all sizes and the difficulties of detecting and mitigating them. When an attack involves multiple stages and different types of attacks, it can be difficult to identify and stop the root cause. It aims to provide insights into how organizations can better defend against cyber-attacks by investigating the link formation of cyber-attacks within a network.

Computer networks are dynamic environments in which malicious objects are propagated. An attack begins with the seed infecting the initial node and then propagates. Infectious payloads are shared between seed nodes and the nodes in their network that form an attack link. Node two similarly follows suit. This process results in the formation of a network attack link. A probabilistic dynamic process forms attack links in the network when nodes do not explicitly specify the next node. As the infection grows in a random order, all of the infected nodes form an equilibrium network

similar to the centre sponsored star network. In this study, it is found that cyberattack links are dynamic in nature and eventually converge to a minimally connected network. The network's final state is determined by the level of security of the nodes. By providing secure connections between nodes, the network can resist the attack. Consequently, it is essential to ensure the security of the node connections to protect the network from malicious attacks.

According to section II, propagation of attack through link formation produces a connected, star-centered network in a non-empty network at equilibrium. A simulation study was conducted in section III to demonstrate that attacks propagate in networks.

## 2. Formation of a Center-Sponsored Star Topology

Let $N = \{1,2,3,\dots,n\}$ the cyber-attack policy can be considered at a node when there are a number of nodes as $c_i = (c_{i1}, c_{i2}, \dots, c_{ii-1}, 0, c_{ii+1} \dots \dots, c_{in})$, where $c_{ij} \in \{0,1\}$ for each $j \in N\backslash\{i\}$. If $c_{ij} = 1$, Attack links are formed between nodes i and j. Cyber-attack profiles can be displayed for all nodes in a network Attack links may be directed or undirected, depending on the type of network. Visualization tools can be used to display attack profiles and other important characteristics of the network as $c = (c_1, c_2, \dots \dots, c_n)$. Let $N_i(c) = \{j \in N | c_{ij} = 1\}$ represent the nodes with which node $i$ forms a link. Let $N_i(c) = \{j \in N | c_{ij} = 1\}$ be the nodes to which *i* has a direct path in a directed network. Because the node can access itself, the number of nodes accessed by $i$ is $m_i \equiv |N_i| + 1$. In cyber-attack of a network, the infected node creates an attack link with the other nodes in such a way that the payloads can be delivered through the link. The payoff function for creating the attack link depends on the directed network in which the node has a direct path, and the attack link the node forms with the other nodes (access to nodes). Hence, let's define the payoff function of node *i* as

$$\pi_i = \frac{|N_i(c)|}{|N|} \qquad (1)$$

Here $m_i$ is the number of network nodes *i* can access, and $|N_i(c)|$ is responsible for the cost of delivering payloads of the virus from node *i*. Here we can consider that the payoff function increases with the number of nodes that *i* access in the network. Since payloads are distributed to all nodes in which node I form an attack link, we can assume the payoff function is decreasing function in $N_i(c)$.

Hence we can assume,

***Assumption 1:*** *The payoff function φ can be a strictly increasing function in $m_i$ and decreasing function in $N_i(c)$.*

Here we have to find how node *i* forms an attack link in the network. Using the above assumption, we can consider the following two lemmas,

***Lemma 1:*** *Let the payoff given by (1) satisfies assumption 1, then at equilibrium, cyber-attack creates a minimally connected network.*

Proof: It is easy to see that a minimally connected network at equilibrium cannot exist in a network with a cycle; since, in a cycle, a node can delete a link gaining access to all nodes

Considering a network *G* be non-empty, let's assume G is a non-connected network if possible. Since *G* is non-empty, there exists a component *H* in *G* with |*H*|>1. Without loss of generality, we can consider $i \in H$, and it is obvious that $|N_i(G)| \geq 1$. Hence, we can state, $\varphi(x,1) \geq \varphi(x,|N_i(G)|) = \varphi(m_i(G),|N_i(G)|) = \pi_i(G)$. Since, according to our initial assumption, *G* is a non-empty, non-connected network, it can be stated that, $\pi_i(G) \geq \pi_i(G_{-i}) = \varphi(m_i(G_{-i}),0) \geq \varphi(1,0)$, where $G_{-i}$ represents the *G* having no links formed by node *i*. Hence $\varphi(x,1) \geq \varphi(1,0)$. Since *G* is not connected, there exists a node $j \notin H$.

Now, let's consider that another node *j* creates a singleton component, and using assumption 1, we can state that,

$$\varphi(x+1,1) > \varphi(x,1) \geq \varphi(1,0) = \pi_j(G)$$

However, this contradicts the hypothesis that node *j* is selecting the best response.

Now, let $i \in H'$ where |*H*'|>1. Let $|H'| \leq x$ and $|N_j(G)| > 1$. Here if node *j* deletes all his links and creates a link with node *i*, we can state that $\varphi(x+1,1) > \varphi(|H'|,1) \geq \pi_j(G)$ which contradicts the hypothesis that *j* is in foremost response.

Considering two cases of $j \notin H$, we can state that if *G* is non-empty, *G* is connected.

***Lemma 2:*** At equilibrium, if (1) and assumption 1 is true, then the network is a center-sponsored star network.

*This means that the center node takes control of the network, and all other nodes must comply with the center node's rules in order to remain part of the network. The center node is responsible for maintaining the network and governing its operations.*

*The following proof is given:* Let G be a nonempty connected network, then Gij=1 for all pairs of nodes i and j. *For all pairs of nodes j and k, Gj,k = 0.*

The payoffs of node i would remain the same if it was not true. The hypothesis that G is connected is contradicted by this observation. This means that any node linked to node i cannot be linked to any other node.

Due to G's connectivity, node i must also be able to access everyone directly. In the above argument, if Glj = 1, then node L can switch links and still retain the same payoffs. As a result, the equilibrium principle is violated.

if $\varphi(n, n-1) > \varphi(x+1, x)$ for all $x \in \{0,1,2, \ldots., n-2\}$, then it follows that a center-sponsored star is in equilibrium. On other hand suppose there is some $x \in \{0,1,2, \ldots., n-2\}$ such that $\varphi(x+1, x) \gg \varphi(n, n-1)$. Then the central node in a center-sponsored star *G* can delete all but x links and at least as well so that *G* cannot be at equilibrium.

Using the proposed lemmas [21], we can say that the propagation of cyber-attacks can be viewed as a dynamic process in a finite state Markov chain and that the dynamic process will converge to a minimally connected network with positive probability starting from any network.

## 3. Creating a Simulation

A 100-by-100-node network was designed to simulate cyber-attacks on a computer network by infecting its neighboring nodes with infected or malicious objects. Probability-based selection determined which of its eight closest neighbors to infect with the infectious node. Based on the simulation, an infectious node will select the next neighbor at random from its eight neighbors nearby. Through the propagation of the attack, infected nodes formed a network that resembled a center-connected star. Initial attack links were random, as illustrated in Figure 1. An initial attack on the star network was clearly performed at the node at its center. By spreading rapidly, the attack significantly damaged the network during the simulation. Simulations show that an attack can be contained by cutting off the central node, limiting its spread. The central node is critical for the survival of the entire network, which is why it is important to monitor the central node in a star network. It is also important to ensure that the other nodes in the network are secure to prevent the attack from spreading.

## 4. Learning Effect on Spread Probability

Computer viruses propagate pragmatically due to the learning effect. The scale-free model uses an anti-virus defense mechanism to slow the propagation of cyber-attacks. If pi,j,t is the probability that a cyber-attack propagates from node i to node j at step t, then pi,j,t remains constant regardless of t. The value of pi,j,t is occasionally reduced after the propagation has become apparent to the users. As a result, probabilities gradually reduce with learning, as shown by the following relation [17, 18]. This slow-down of the spread of cyber-attacks helps to reduce the amount of damage they cause. The scale-free model can also be used to prevent cyber-attacks from occurring in the first place by predicting their likelihood of success.

Additionally, it can be used to identify malicious actors in the network.

$$p_{i,j,t} = \frac{p_{i,j,t-1}}{(t+1)^q} \quad (2)$$

Here, q represents the learning rate. It can be stated that the learning effect in network propagation is as follows: q determines the magnitude of the weight changes during each iteration of the training process. The larger the q value, the greater the weight changes and the faster the network learns. On the other hand, if q is too small, the network will take longer to learn.

$$\lim_{t \to \infty} p_{i,j,t} = 0 \quad (3)$$

$$p_{i,j,t2} \leq p_{i,j,t1} \leq 1 \ \ for\ t1 < t2 \leq \infty \quad (4)$$

A learning effect $p_{i,j,t2} = p_{i,j,t1}$ is not present in this case, so equality holds. This means that the same amount of effort will yield the same result. There is no need to repeat the same task again and again to get better performance. It can be concluded that this method is efficient and time-saving.

We can calculate a probabilistic score for each node based on the probability of transition in each of its 8 directions (since nodes have eight neighbour nodes). Those with a probability score over 0.85 are classified as S, those with a probability score below 0.15 are classified as R, and those with a probability score around 0.5 are classified as I. For other probability scores, simulations are run until saturation of S, R, and I reaches a constant value. Below Figure 2 is a graph showing the percentages of R, S, I for different simulation times for the case of (S, R, I) =(1.5,0.1.0,0.5). Several thousand iterations are needed for the system to stabilize.

S and I contribute a greater fraction of the system's energy to the steady state compared to R. This illustrates the convergent behavior of the system.

Probabilistic simulation using the proposed algorithm is expressed as follows:

**Input**: A network with no scale constraints G(V, E) G(V, E) is a graph with vertices V and edges E. It has no restrictions on the graph size and can contain an arbitrary number of nodes and edges.

Each node P starts with a probability matrix. The goal is to find the most efficient path from one node to another. The probability matrix helps to determine the likelihood of each edge being used in the shortest path. The result is the shortest path with the highest probability.

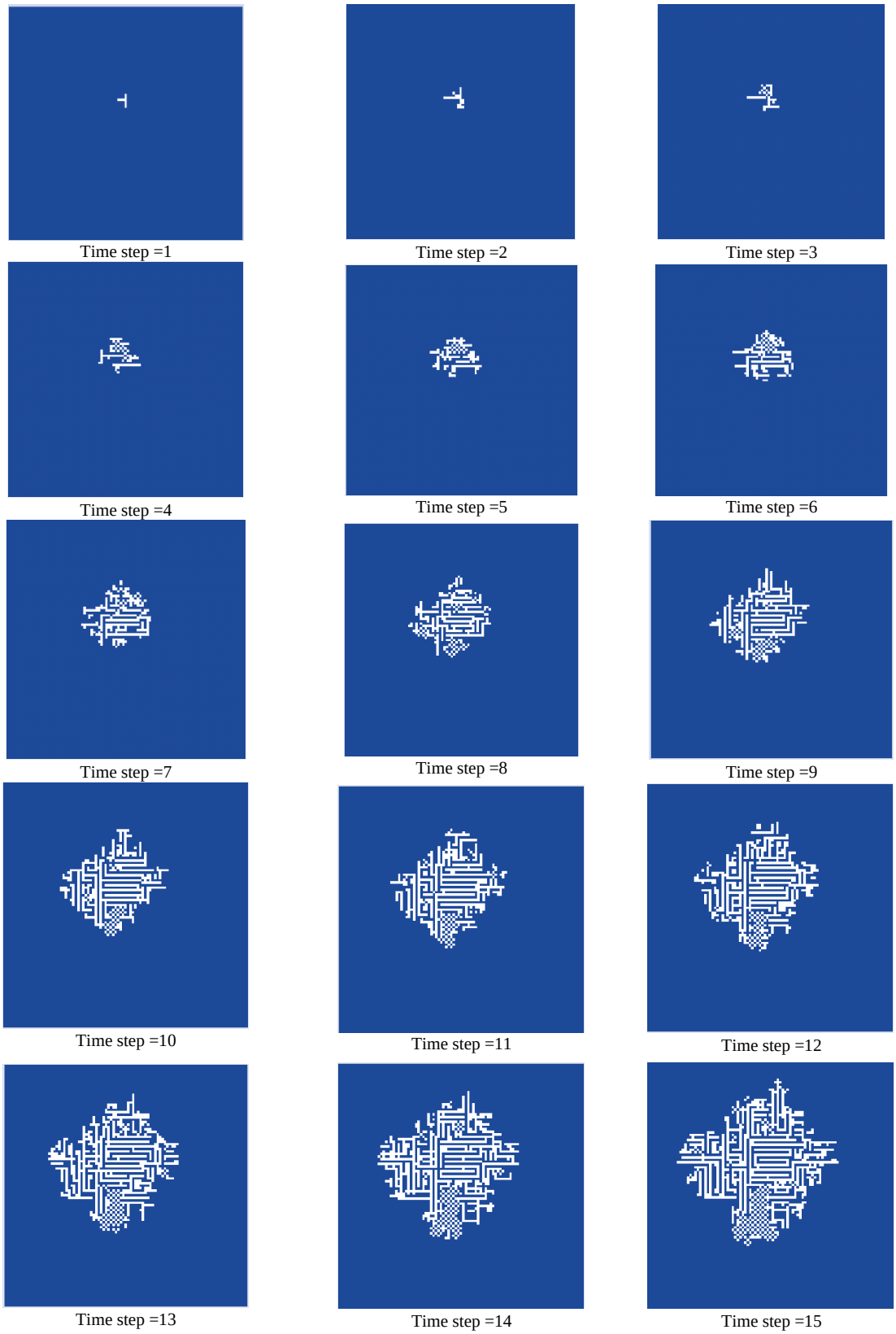


**Fig. 1 An incremental simulation of 100X100 nodes resulted in the following result. It begins with randomly placing an infectious object in the top left subplot**

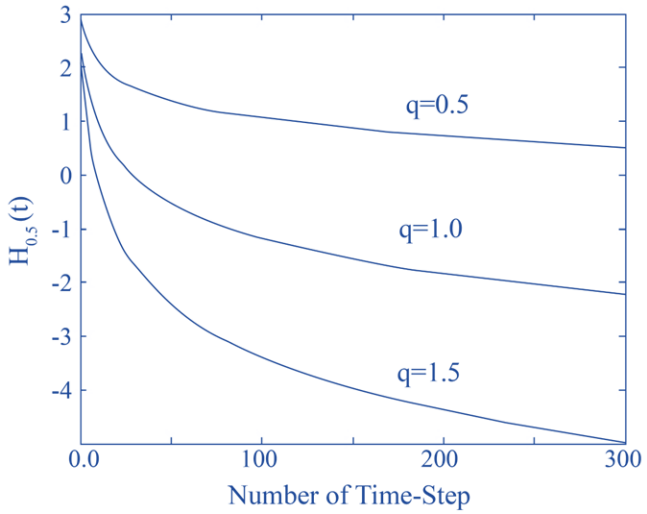


**Fig. 2 Graph with the percentages of R, S, I for different simulation times**

**Output:** At each time step, the propagation matrix is displayed. The propagation matrix is used to update the probability matrix for each node. The new probability matrix is then used to compute the shortest path with the highest probability.

At the end, the shortest path is displayed. You can adjust the time step from 0,1,2,3,... and so on.

A new matrix of probabilities has been generated using $p_{i,j,t} = \frac{p_{i,j,t-1}}{(t+1)^q}$

1. Each node k has a probability score calculated as :
$$\sum_{(i,j) \in Neighbour of\ k} V(i,j) p_{i,j,t}$$
2. S, I, and R probability scores should be classified according to their probability.
3. Formulate the propagation matrix.

In Fig. 1, an incremental time step simulation is shown for 100X100 nodes. 1. Cyber-attacks become more prevalent over time as links between them grow. In spite of the fact that the formation of a closed network is considered random, a definite pattern of propagation can be observed. An attack propagation pattern involving infected nodes growing in the network can be seen in Figure 1. Infected nodes form a center-connected star network as the attack spreads, whereas the attack link is initially random. For example, each node in the attack path is connected to the central node, so the attack seed spreads uniformly outward from the center of the star network. In this way, the attacker has better control over the attack and can increase its effectiveness. Detection and stopping the attack become more difficult as the attack propagates. In this manner, it is evident that the attack seed plays a critical role in the overall attack strategy.

## 5. Conclusion & Future Work

In this paper, the authors focus on understanding the formation of center-connected star networks when cyber-attacks propagate in a network. The study shows that cyber-attacks create an attack link in the network, forming a minimally connected network at equilibrium. The authors propose a theoretical analysis of this attack-link formation and use simulation to confirm their findings.

A 100 x 100 node network simulation shows that an infectious object can spread to neighboring nodes. A probability-based approach is used to select one of the eight closest neighbors randomly among the infected nodes. A network of infected nodes becomes connected as the attack spreads, resembling a centre-connected star network. A network of attack links appears random initially, but as it crosses borders, it becomes more connected, similar to a star network. According to the authors, cyber-attacks have an impact on network connectivity by forming attack links in connected networks. Using the study as an example, the authors examine how center-connected star networks form and the importance of the initial attack node in creating the network's center.

The novelty of this research paper lies in its focus on understanding the formation of centre-connected star networks in the context of cyber-attacks. The study provides a new perspective on cyber-attack's impact on network connectivity, which has not been extensively studied in previous research.

The authors' use of simulation-based analysis to study the propagation of cyber-attacks in a 100 x 100 node network is also a unique approach to the problem. Their proposed theoretical analysis of the attack-link formation due to cyber-attacks in a connected network provides a theoretical framework for understanding the phenomenon.

Furthermore, the study's findings highlight the importance of the initial attack node in creating the center of the network, which can have significant implications for network security. The research can be useful in developing more effective strategies to mitigate the impact of cyber-attacks and improve network security.

This research article provides a foundation for future work in several areas. One possible direction for future research is to investigate how different attack scenarios and strategies affect attack-link formation and the resulting network structure. Another area for further study is exploring network topology's impact on attack propagation and the formation of center-connected star networks. Additionally, future research could focus on developing more sophisticated attack propagation models that consider factors such as the dynamic nature of network traffic and the behavior of

network users. Finally, the findings of this study could be applied to developing more effective strategies for network security and mitigating the impact of cyber-attacks.

Overall, this paper contributes to the understanding of cyber-attacks in a connected network and the formation of center-connected star networks. The findings of this study can be useful for improving network security and developing more effective strategies to mitigate the impact of cyber-attacks.

## Funding Statement

Any external parties have not funded this research; all contribution was made by authors as part of the research program for higher studies.

## 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] Hossein Akhavan-Hejazi, and Hamed Mohsenian-Rad, "Power Systems Big Data Analytics: An Assessment of Paradigm Shift Barriers and Prospects," *Energy Reports*, vol. 4, pp. 91-100, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[3] Olalekan Adeyinka, "Internet Attack Methods and Internet Security Technology," *Second Asia International Conference on Modeling & Simulation*, 2008. [CrossRef] [Google Scholar] [Publisher Link]

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

[5] 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]

[6] 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]

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

[8] Konstantinos Xynos et al., "Penetration Testing and Vulnerability Assessments: A Professional Approach," *International Cyber Resilience Conference*, Edith Cowan University, 2010. [Google Scholar] [Publisher Link]

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

[10] M. Dacier, Y. Deswarte, and M. Kaâniche, "Models and Tools for Quantitative Assessment of Operational Security," *Information systems security*, pp. 177-186, 1996. [CrossRef] [Google Scholar] [Publisher Link]

[11] Davide Balzarotti, Mattia Monga, and Sabrina Sicari, "Assessing the Risk of Using Vulnerable Components," *Quality of Protection: Advances in Information Security*, pp. 65-77, 2006. [CrossRef] [Google Scholar] [Publisher Link]

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

[13] Romualdo Pastor-Satorras et al., "Epidemic Processes in Complex Networks," *Reviews of Modern Physics*, vol. 87, no. 3, p. 925, 2015. [CrossRef] [Google Scholar] [Publisher Link]

[14] 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]

[15] Lu-Xing Yang, Xiaofan Yang, and Yingbo Wu, "The Impact of Patch Forwarding on the Prevalence of Computer Virus: A Theoretical Assessment Approach," *Applied Mathematical Modelling*, vol. 43, pp. 110- 125, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[16] 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]

[17] Venkatesh Bala, and Sanjeev Goyal, "A Noncooperative Model of Network Formation," *Econometrica-Journal of the Econometric Society*, vol. 68, no. 5, pp. 1181-1229, 2000. [CrossRef] [Google Scholar] [Publisher Link]

[18] 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] [Publisher Link]

[19] 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]

[20] Adel Rajab et al., "Cryptography Based Techniques of Encryption for Security of Data in Cloud Computing Paradigm," *International Journal of Engineering Trends and Technology*, vol. 69, no. 10, pp. 1-6, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[21] 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, 1927. [CrossRef] [Google Scholar] [Publisher Link]