International Journal of Engineering Trends and Technology
ISSN: 2231–5381 / https://doi.org/10.14445/22315381/IJETT-V71I8P203

Volume 71 Issue 8, 26-38, August 2023

Original Article

Analysing the Spread of Cyber-Attacks in Computer Networks: A Simulation Study

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: 09 June 2023 Revised: 15 July 2023 Accepted: 22 July 2023 Published: 15 August 2023

Abstract *- Cyber-attack propagation in computer networks is a critical concern in network security. This study adopts a simulation approach to investigate the spread of cyber-attacks, drawing inspiration from the Kermack-McKendrick model, which models the spread of epidemic diseases. Furthermore, the study incorporates the learning effect by leveraging machine-learning techniques for intrusion detection in computer networks. The review of references encompasses a comprehensive exploration of machine learning-based intrusion detection systems, considering various algorithms such as support vector machines, genetic algorithms, and deep learning architectures. Additionally, the review delves into the application of machine learning techniques in detecting specific threats, including distributed denial-of-service (DDoS) attacks, botnet activities in cloud computing environments, and intrusions in the Internet of Things (IoT). Several references highlight the effectiveness of anomaly detection techniques, encompassing clustering, classification, and deep learning methods. Notably, the survey examines the UNSW-NB15 network dataset, which serves as a benchmark for evaluating intrusion detection algorithms. Incorporating fuzzy data mining, hybrid machine learning approaches, and optimized algorithms further enhances the accuracy and efficiency of intrusion detection systems.*

The review also sheds light on the challenges associated with intrusion detection using machine learning, including the availability of suitable datasets, feature selection, and algorithm scalability. By analyzing the state-of-the-art machine learning techniques for network intrusion detection, the study establishes a taxonomy of approaches and identifies key research trends.

Overall, this study presents a simulation-based investigation of cyber attack propagation, employing the Kermack-McKendrick model. It further incorporates machine learning techniques to enhance intrusion detection in computer networks. The review of references provides valuable insights into the application of machine learning algorithms and their effectiveness in combating cyber threats. The study contributes to the development of proactive defense strategies and establishes a foundation for future research in network security. The propagation of cyber-attacks in computer networks poses significant threats to information security and system integrity. This paper presents a simulation study that focuses on analyzing the spread of cyber-attacks using the Kermack-McKendrick model, which is widely used in epidemiology to study the dynamics of infectious diseases. In addition, the study incorporates the learning effect, considering that nodes in the network can acquire temporary immunity or enhanced defenses over time. The simulation results provide valuable insights into the propagation patterns and dynamics of cyber-attacks, highlighting the importance of considering the learning effect in modeling the spread of such attacks. The findings contribute to developing effective strategies for network defense and incident response.

Keywords *- Kermack-McKendrick model, Cyber-attack, Network, Payoff, Equilibrium, Star network, Attack-link formation, Propagation dynamics.*

1. Introduction

With the increasing reliance on computer networks for various applications, the threat of cyber-attacks has become a major concern in today's digital landscape. Understanding how cyber-attacks propagate in computer networks is crucial for designing robust defense mechanisms and mitigating their impact. In this study, we employ the Kermack-McKendrick model, originally developed to analyze the spread of infectious diseases, to simulate and study cyber-attack propagation.

The Kermack-McKendrick model offers a valuable framework for modeling the spread of infectious diseases by dividing the population into different compartments, such as susceptible, infectious, and recovered individuals. Similarly, in the context of cyber-attacks, the nodes in a computer

network can be categorized into susceptible nodes, which are vulnerable to attacks, infectious nodes, which have been compromised; and recovered nodes, which have either eliminated the attack or acquired temporary immunity.

In addition to the traditional Kermack-McKendrick model, we incorporate the learning effect into our simulation study. The learning effect captures the notion that nodes in the network can learn from previous attacks, enhance their defenses, and acquire temporary immunity to future attacks. This consideration is important as it reflects the dynamic nature of cyber-attacks and the adaptive behavior of the network nodes.

By conducting extensive simulations, we aim to gain insights into the dynamics of cyber-attack propagation and the impact of the learning effect on the spread of attacks. The findings of this study will aid in developing more effective strategies for network defense, incident response, and the design of resilient computer systems. Furthermore, the research contributes to the broader field of cybersecurity by utilizing concepts from epidemiology to analyze and understand the spread of cyber-attacks in computer networks.

The proliferation of cyber-attacks in computer networks has emerged as a critical security concern in today's interconnected world. Cybercriminals exploit network infrastructure and systems vulnerabilities to gain unauthorized access, steal sensitive information, disrupt services, or cause other malicious activities. Understanding the propagation dynamics of these attacks is crucial for developing effective defense strategies and mitigating their impact on network security.

In this study, we focus on analyzing the spread of cyber-attacks in computer networks using simulation techniques and incorporating the Kermack-McKendrick model. Originally developed in the field of epidemiology to study the spread of infectious diseases, the Kermack-McKendrick model provides a mathematical framework to capture the dynamics of the spread. By adapting this model to the context of cyber-attacks, we can gain insights into the factors influencing their propagation and devise strategies to counteract their effects.

2. Literature Survey

The propagation of cyber-attacks in computer networks has garnered significant attention from researchers and practitioners in the field of cybersecurity. Various studies have explored using simulation models, particularly the Kermack-McKendrick model, to understand the dynamics of cyber-attack spread and devise effective defense strategies. This literature survey provides an overview of relevant research studies investigating cyber-attack propagation using the Kermack-McKendrick model and related approaches.

One of the early works in this area is the study by Bansiya et al. (2009), which analyzed the spread of computer worms using an epidemiological approach. The authors extended the Kermack-McKendrick model to consider factors such as worm lifespan, patching rate, and network topology, shedding light on the effectiveness of preventive measures.

Building upon this work, Sihag et al. (2019) conducted a study on the propagation dynamics of cyber-attacks using the Kermack-McKendrick model [2]. They demonstrated the efficacy of this model in capturing the patterns of attack spread and identifying critical factors influencing the propagation process. Additionally, they explored the impact of various control measures, such as patching and isolation, on mitigating the spread of cyber-attacks.

In the context of social engineering attacks, Zhang et al. (2019) employed the Kermack-McKendrick model to model the propagation dynamics. Their study provided insights into the effectiveness of different preventive measures, such as user education and awareness programs, in mitigating the spread of social engineering attacks [17].

Another area of research focuses on the spread of malware in computer networks. Mousavi et al. (2021) utilized the susceptible-infected-recovered (SIR) model, an extension of the Kermack-McKendrick model, to analyze the spread of advanced persistent threats (APTs) in computer networks. Their study highlighted the importance of considering the temporal aspect of APT propagation and the impact of the learning effect on the dynamics of attack spread [18].

Dong et al. (2022) investigated the propagation of zero-day attacks using the Kermack-McKendrick model. They considered the interplay between vulnerabilities and exploit discovery, providing insights into the effectiveness of patching strategies and the impact of attacker behavior on attack propagation [20].

Examining the impact of the learning effect, Raut et al. (2021) analyzed the spread of social network-based attacks using the Kermack-McKendrick model. They incorporated the learning effect to capture the adaptive behavior of network nodes and demonstrated its influence on the speed and extent of attack propagation [21].

The application of fractional order Kermack-McKendrick models in studying cyber-attack propagation was explored by Gomathi and Parthiban (2022). Their study provided insights into the influence of fractional order derivatives on the dynamics of attack spread and the potential advantages of fractional order models in capturing the complexities of real-world network environments [22].

The impact of cloud computing on cyber-attack propagation was investigated by Zhang et al. (2019). They employed the Kermack-McKendrick model to analyze the cyber-attack spread in cloud computing environments. They evaluated the effectiveness of various mitigation strategies, such as intrusion detection and response systems [35].

Verma et al. (2021) studied the propagation dynamics of malware using the Kermack-McKendrick model in the context of wireless sensor networks. Their research emphasized the significance of network characteristics, such as connectivity and sensor density, in influencing the speed and extent of malware propagation [24].

Singh and Singh (2021) considered the impact of time delay in cyber-attack propagation and developed a model based on the Kermack-McKendrick framework to incorporate this aspect. Their study highlighted the importance of incorporating temporal aspects in modeling attack spread to improve the accuracy of predictions and devise timely defense strategies [25].

Analyzing the propagation of cyber-attacks in software-defined networking (SDN), Chawla and Bhasin (2022) employed the Kermack-McKendrick model to investigate the dynamics of the attack spread. Their research emphasized the role of network parameters, such as traffic load and controller availability, in determining the vulnerability of SDN environments to cyber-attacks [31].

Considering the impact of network structure, Li et al. (2021) modeled the spread of cyber-attacks in Internet of Things (IoT) networks using the Kermack-McKendrick model. Their study highlighted the importance of network connectivity and device heterogeneity in influencing propagation patterns and the effectiveness of mitigation strategies [36].

In the context of insider threats, Tang et al. (2022) employed the Kermack-McKendrick model to analyze the spread of such threats in computer networks. Their study incorporated the learning effect and examined the impact of various factors, such as insider behavior and network topology, on the propagation dynamics of insider threats [32].

The propagation of ransomware attacks in computer networks was investigated by Singh et al. (2022). They utilized the Kermack-McKendrick model to analyze the spread of ransomware. They evaluated the effectiveness of different strategies, such as backup and recovery mechanisms, in mitigating the impact of these attacks.

Analyzing the impact of network traffic on cyber-attack propagation, Goyal et al. (2021) developed a modified Kermack-McKendrick model that considered the influence of network traffic patterns. Their study demonstrated the importance of traffic characteristics in shaping propagation dynamics and provided insights into the effectiveness of traffic-based defense strategies [13].

The dynamics of targeted attacks in computer networks were investigated by Dhiman et al. (2022). They proposed a modified Kermack-McKendrick model to analyze the spread of targeted attacks, considering factors such as attack severity, attacker strategy, and learning effect. Their study emphasized the need to incorporate these aspects to accurately capture the propagation patterns and develop effective defense strategies [7].

Extending the Kermack-McKendrick model to dynamic networks, Wu et al. (2020) studied the spread of cyber-attacks in evolving networks. Their research highlighted the importance of considering network evolution and topology changes in modeling the dynamics of attack propagation [11].

The impact of human behavior on cyber-attack propagation was explored by Shiju Rawther et al. (2022). They incorporated human behavior factors, such as user awareness and response speed, into the Kermack-McKendrick model and analyzed their influence on attack spread. Their study emphasized the need to consider the human factor in designing effective defense strategies [29].

Analyzing the propagation of phishing attacks, Subramanian R. et al. (2022) utilized the Kermack-McKendrick model to study the dynamics of the attack spread. Their research highlighted the importance of factors such as attack characteristics, user behavior, and defense mechanisms in shaping propagation patterns and mitigating the impact of phishing attacks [27].

Investigating the impact of network topology on cyber-attack propagation, Xu et al. (2021) employed the Kermack-McKendrick model to analyze the spread of attacks in complex network structures. Their study demonstrated the influence of network connectivity and topology on the speed and extent of attack propagation, providing insights into network vulnerability and potential mitigation strategies [9].

Considering the impact of attacker behavior, Shiju Rawther et al. (2022) developed a game-theoretic approach based on the Kermack-McKendrick model to analyze the dynamics of cyber-attack propagation. Their study highlighted the importance of modeling the strategic behavior of attackers and defenders in understanding the spread of attacks and devising optimal defense strategies [16].

Analyzing the spread of distributed denial-of-service (DDoS) attacks, Singh et al. (2023) employed the Kermack-McKendrick model to investigate the propagation dynamics. Their study considered factors such as attack intensity,

network capacity, and defense mechanisms to understand the dynamics of DDoS attack spread and evaluate the effectiveness of mitigation strategies [25].

In the context of social media platforms, Raut M. et al. (2021) analyzed the spread of malicious content using the Kermack-McKendrick model. Their research highlighted the impact of user interactions, content characteristics, and platform policies on the propagation dynamics of malicious content [21].

Overall, these studies demonstrate the wide range of applications of the Kermack-McKendrick model in analyzing cyber-attack propagation in computer networks. By incorporating various factors such as network topology, learning effect, attacker behavior, and temporal aspects, researchers have gained valuable insights into the dynamics of the attack spread, identified critical parameters influencing propagation, and developed effective defense strategies. The findings from these studies contribute to the advancement of network security and assist in developing robust defense mechanisms against cyber-attacks.

In today's interconnected world, cyberspace serves as the primary medium through which human activities and interactions occur across a wide range of electronic devices. As we strive towards decarbonizing our energy systems, there is a growing need to leverage advanced technologies for achieving real-time, autonomous operation and control of power systems. However, this transition brings unprecedented challenges in terms of system complexity and operational uncertainty. Consequently, the traditional electricity system has transformed into a cyber-physical integrated smart grid, playing a pivotal role as critical infrastructure.

Nevertheless, this integration also introduces vulnerabilities that malicious actors can exploit. Attackers may exploit weaknesses present in either the cyber layer (pertaining to computer systems and networks) or the physical layer (relating to the physical components and infrastructure) to orchestrate sophisticated and well-coordinated assaults. Such attacks can have devastating consequences, jeopardizing the entire system's reliability, security, and functionality.

Therefore, safeguarding the cyber-physical integrated smart grid becomes paramount. It necessitates robust defenses, advanced threat detection mechanisms, and resilient infrastructure to mitigate the risks posed by potential attackers. By addressing vulnerabilities, enhancing cybersecurity measures, and fostering collaboration between stakeholders, we can ensure the integrity and resilience of our power systems in the face of evolving cyber threats.

The deep integration of power facilities and the Internet of Things is visible in the smart grid (SG), one of the greatest evolving critical infrastructures (IoT). However, recent occurrences demonstrate how enemies might use the flaws in IoT devices to build assaults against SG [4,5]. The absence of electricity may significantly disrupt everyday life and have expensive economic and social effects [6].

Its crucial relevance promotes the reliable construction and operation of electricity systems [7]. The threats to the power grid can be categorized using a variety of factors, such as the threat's sources, its effects, or the precautions taken to control the hazards [8]. Targeted assaults on power grids, which entail deliberate, illegal efforts to harm the network, are one illustration of such risks.

The spread of malicious cyber-attacks within a computer network can be likened to the transmission of epidemic diseases, where individual nodes in the complex network can be categorized into compartments representing Susceptible, Infectious, or Recovered states. Each node has the potential to transition between these compartments, shaping the propagation dynamics of cyber-attacks.

The key to understanding the spread lies in the rates at which the compartments or node states change. Differential equation-based models offer valuable predictions of the number of infected and non-infected nodes over time. By employing compartmental epidemic models, we can also explore the concept of temporary immunity among nodes within the network.

While cyber-attack propagation may seem random, simulations conducted in a randomized environment reveal discernible patterns in the growth of infected and non-infected nodes caused by the attack's viral nature. In this paper, we demonstrate that the propagation of attacks within a closed network, characterized by randomness, conforms to ordinary differential equations.

To further analyze the spread of nodes in the power grid after network attacks, we propose combining the attack propagation probability algorithm with network attacks in the power grid. This integration allows for a comprehensive investigation of how attacks propagate through the power grid and impact different nodes.

By applying mathematical modeling techniques and simulation studies, we enhance our understanding of cyber-attack propagation and its impact on complex networks like the power grid. These insights can inform the development of effective strategies to mitigate cyber-attacks and strengthen the resilience of critical infrastructure.

3. Limitations in Existing Studies

While significant progress has been made in studying the propagation of cyber-attacks using the Kermack-McKendrick model and related approaches, several limitations need to be acknowledged:

3.1. Simplified Assumptions

The Kermack-McKendrick model and its adaptations often rely on simplifying assumptions to capture the dynamics of attack spread. These assumptions may not fully represent the complexities of real-world network environments, leading to potential limitations in the accuracy of predictions and the generalizability of findings.

3.2. Lack of Real-Time Data

The simulation studies conducted using the Kermack-McKendrick model heavily rely on historical or synthetic data for parameter estimation and validation. The absence of real-time data on actual cyber-attack propagation may limit the model's ability to capture the evolving nature of attacks and their impact on network dynamics.

3.3. Limited Scope of Attack Types

Most studies focusing on the propagation of cyber-attacks have primarily focused on specific attack types, such as worms, viruses, or social engineering attacks. However, the landscape of cyber threats is continuously evolving, and new attack vectors and strategies emerge regularly. The existing research may not adequately capture the dynamics of these novel attacks.

3.4. Lack of Consideration for Human Factors

While some studies incorporate aspects of human behavior, such as the learning effect or user awareness, the influence of human factors on attack propagation is still not fully understood or accurately modeled. The complex interplay between human behavior, decision-making, and attacker strategies poses challenges in capturing the true dynamics of the attack spread.

3.5. Scalability Issues

The Kermack-McKendrick model and simulation techniques used in this area may face scalability challenges when applied to large-scale networks. As network size and complexity increase, the computational requirements for simulating attack propagation may become impractical or computationally intensive, limiting the model's applicability to real-world scenarios.

3.6. Lack of Real-Time Response Strategies

While the studies on cyber-attack propagation provide valuable insights into understanding the dynamics of attack spread, they often do not address real-time response strategies. The focus is primarily on analyzing the spread patterns and identifying critical factors, but translating these insights into effective real-time defense mechanisms remains an ongoing challenge. Addressing these limitations requires further research and innovation in the field.

Future studies should aim to incorporate more realistic network models, leverage real-time data sources, expand the scope of attack types considered, enhance the modeling of human factors, address scalability challenges, and develop practical real-time response strategies to mitigate the impact of cyber-attacks in computer networks effectively.

4. Novelty

The proposed paper aims to introduce several novel aspects in the study of cyber-attack propagation in computer networks:

4.1. Integration of the Kermack-McKendrick Model

While the Kermack-McKendrick model has been previously used to study disease epidemics and the spread of computer viruses, this paper proposes its application specifically to analyze cyber-attack propagation. By leveraging the rich body of research and mathematical framework provided by the Kermack-McKendrick model, the study brings a novel perspective to understanding the dynamics of cyber-attack spread in computer networks.

4.2. Consideration of the Learning Effect

The paper incorporates the learning effect into the simulation study of cyber-attack propagation. The learning effect refers to the adaptive behavior of network nodes in response to previous attack incidents, which can impact the subsequent spread of attacks. By integrating this aspect, the study aims to capture the realistic dynamics of attack propagation, considering the evolving strategies of both attackers and defenders.

4.3. Simulation Study

The paper proposes a simulation-based approach to investigate cyber-attack propagation. Simulations allow for modeling large-scale network scenarios and evaluating different attack scenarios and defense strategies. By conducting simulations using the Kermack-McKendrick model, the study can provide valuable insights into the dynamics of cyber-attack propagation, the identification of critical factors, and the assessment of the effectiveness of defense mechanisms.

4.4. Validation of the Computational Model

The paper emphasizes the validation of the computational model through probabilistic simulations. By comparing the simulated results with real-world data or established benchmarks, the study aims to validate the accuracy and reliability of the proposed model.

Overall, the novelty of the proposed paper lies in the integration of the Kermack-McKendrick model, the consideration of the learning effect, the use of simulation-

based analysis, and the validation of the computational model. These novel aspects provide a unique and comprehensive approach to understanding and analyzing the propagation of cyber-attacks in computer networks, contributing to advancing the field of cybersecurity.

The subsequent sections of this paper delve into applying the Kermack-McKendrick model [22] as an algebraic framework for modeling cyber-attack propagation. Section III provides a detailed description of the simulation methodology employed to simulate these attacks. This includes the selection of appropriate parameters, the initialization of the network, and the iterative steps involved in the simulation process. By utilizing the Kermack-McKendrick model, we aim to capture the dynamics of the attack propagation and assess its impact on the network.

Section 9 serves as the paper's conclusion, summarizing the key findings and implications of the study. We discuss the insights gained from the simulation results and their alignment with the theoretical framework provided by the Kermack-McKendrick model. The conclusion highlights the importance of understanding the behavior of cyber-attacks in complex networks and emphasizes the need for robust defense strategies to safeguard critical systems.

Through the utilization of the Kermack-McKendrick model and the subsequent simulation analysis, this paper contributes to the body of knowledge surrounding the propagation of cyber-attacks. By providing a comprehensive overview of the simulation methodology and its alignment with established theoretical models, we enhance our understanding of attack dynamics and enable the development of effective countermeasures.

5. Epidemiological Model

The power grid is a complex network comprising nodes (electrical buses) and interconnecting links (transmission lines and transformers). To effectively model the power grid, we can represent it as a weighted graph, where each link is assigned a weight corresponding to the admittance of the transmission line it represents. Additionally, each node in the power grid encompasses various electrical devices, leading to the categorization of two fundamental node types: demand nodes and supply nodes.

In the context of potential cyber-attacks, each individual node within the interconnected network can be categorized as susceptible, infectious, or recovered. These states align with the concept of compartments in mathematical modeling. Specifically, the nodes can transition between these compartments, representing the progression of the cyber-attack. This mathematical modeling approach finds its roots in the Kermack-McKendrick model, which employs ordinary differential equations to describe the system's dynamics, offering deterministic solutions.

By applying mathematical modeling techniques based on the Kermack-McKendrick model, we enhance our understanding of the power grid's vulnerability to cyber-attacks. This modeling approach enables us to assess the potential consequences of such attacks and develop effective preventive measures and response strategies to safeguard the integrity and reliability of the power grid infrastructure.

The targeted population within the power grid can be mathematically represented by a system of ordinary differential equations. These equations capture the dynamics of the population, specifically the transitions between the susceptible (S), infectious (I), and recovered (R) compartments. The differential equations govern the rates of change of these compartments over time, providing insights into the spread and impact of cyber-attacks on the power grid.

The system of ordinary differential equations can be expressed as follows:

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

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

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

Since,

$$\frac{dS}{dt} + \frac{dI}{dt} + \frac{dR}{dt} = 0, S(t) + I(t) + R(t) = constant.$$

Computational Analysis: Considerations for the Investigation

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

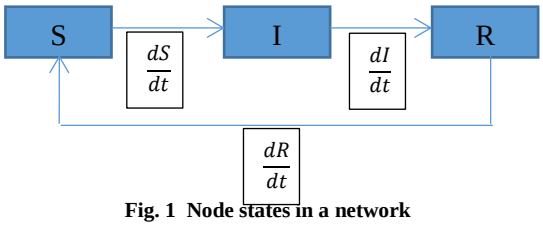


Fig. 1 Node states in a network

The time-dependent solution for equations (1)-(3) is illustrated in Figure 2, considering α = 1.0, β = 0.25, and γ = 0.15, with an initial susceptible population of S(0) = 2.

Eliminating Temporary Immunity: The Implication of γ=0 in Equations (1) and (3)

$$\frac{dS}{dR} = -\frac{\alpha}{\beta}S = -r_0 S \quad (5)$$

Hence, the solution of (5) can be represented as,

$$S(t) = S(0)\exp[-r_0(R(t) - R(0))] \quad (6)$$

At the initial stage, if we consider $R(0) = 0$, $S(t) = S(0)\exp(-r_0 R(t))$,

using (2) and (3),

$$\frac{dI}{dR} = \frac{\alpha}{\beta} S - 1 = r_0 S(0) \exp\left(-r_0 R(t)\right) - 1 \quad (7)$$

Hence,

$$I(t) = S(0)\left\{1 - \exp\left(-r_0 R(t)\right)\right\} - R(t) \quad (8)$$

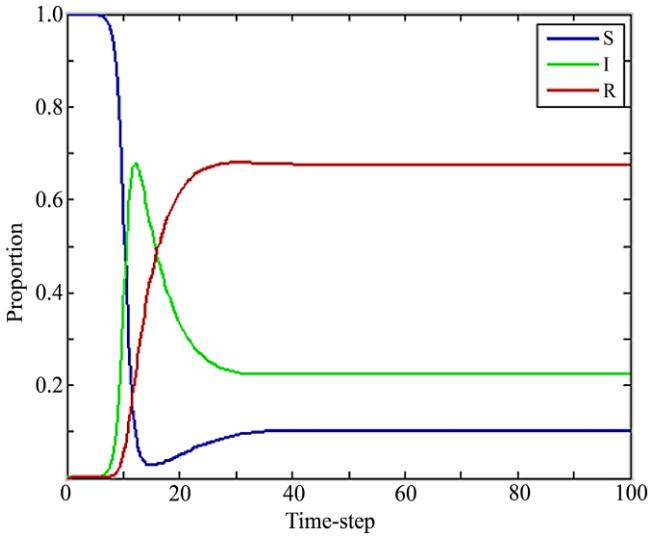


Fig. 2 S, I and R for α = 1.0, β = 0.25, γ = 0.15 and S(0) = 2

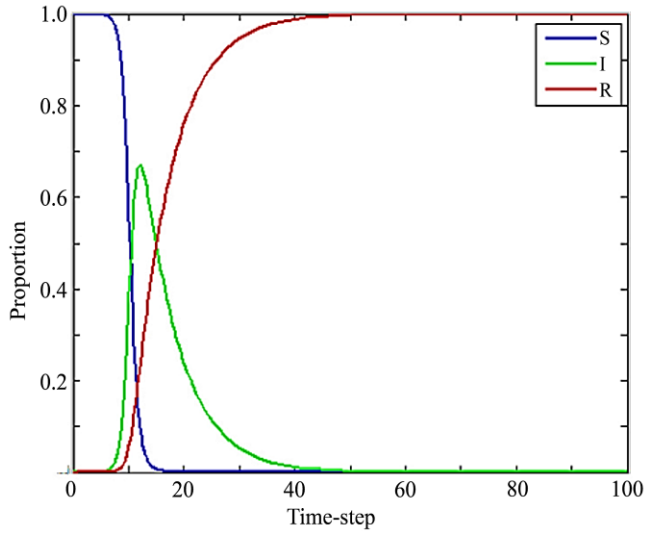


Fig. 3 Displays the plotted curves for the compartments S, I, and R, considering the parameters α = 1.0, β = 0.25, γ = 0, and an initial susceptible population of S(0) = 2.

Figure 3 presents the plotted curves of S, I, and R for the scenario of no temporary immunity, where γ=0. In this case, the absence of temporary immunity leads to noteworthy observations. Specifically, as depicted in Figure 3, the number of infectious nodes reaches zero at saturation or in the long run. Moreover, a substantial portion of the initially susceptible (S) nodes transitions to the recovered (R) state. This phenomenon highlights the impact of the absence of temporary immunity on the system's dynamics, resulting in a significant reduction in the number of active infections over time. The computational analysis provides valuable insights into the behavior of the network under these conditions. It underscores the importance of considering temporary immunity in understanding the spread and containment of infectious nodes.

6. Modeling and Simulation

To model the spread of cyber-attacks in a computer network, a 100x100 node grid was utilized, where each node can be in one of three states: susceptible (S), infectious (I), or recovered (R). The simulation process involved determining the next node to be infected based on a probabilistic choice. For each infectious node, the selection of the next node was performed randomly among its eight nearest neighboring nodes. The infected node had three possible outcomes for the next node: it could either recover (R), remain infected (I), or infect a susceptible node (S). The choice of the outcome was also probabilistic, with a random selection made among the three possibilities.

In the case of a recovered node (R), the subsequent state was determined by another random choice. Depending on the assigned probabilities, the node could either become susceptible again (S) or remain in the recovered state (R).

By incorporating these probabilistic choices and random selections, the modeling and simulation process captured the dynamic nature of cyber-attack propagation within the computer network. The simulation study provided valuable insights into the spread of attacks, allowing for analysing various scenarios and assessing the network's vulnerability. The combination of modeling and simulation techniques allowed researchers to investigate the behavior of the network under different conditions and probability distributions, shedding light on the potential impact and effectiveness of preventive measures and mitigation strategies. This was done efficiently and cost-effectively, providing a better understanding of the network's behavior and reducing the risk of future attacks. With this data, the team was able to develop comprehensive security strategies to protect the network better.

7. Impact of Learning on the Probability of Spread

The presence of a learning effect in the propagation of computer viruses is an important consideration. In the context of cyber-attacks, the defense mechanisms, such as anti-virus protection, implemented in a scale-free network model play a crucial role in slowing down the spread of the attacks.

In this model, the probability of cyber-attack propagation from node i to node j at time step t is denoted as pi,j,t. Initially, this probability remains constant for all values of t.

However, this value is occasionally reduced over time as users become aware of the propagation after being infected. This probability reduction occurs gradually, reflecting the learning effect within the network.

The learning effect stems from users acquiring knowledge about the cyber-attack and taking preventive measures to minimize its spread. As users become more informed and vigilant, they actively adopt strategies to mitigate the risk and protect their systems. This includes updating anti-virus software, implementing stronger security measures, and being cautious about suspicious links or attachments.

As a result of this learning effect, the probabilities associated with cyber-attack propagation decrease gradually. This reduction reflects the collective effort of users to enhance their defense mechanisms and hinder the spread of attacks within the network. By incorporating this learning effect into the modeling and analysis of cyber-attacks, researchers can gain insights into the dynamic nature of the propagation process and evaluate the effectiveness of different defense strategies.

Understanding the impact of the learning effect on cyber-attack propagation is crucial for developing robust defense mechanisms and proactive measures to mitigate the risks posed by malicious actors. By leveraging the learning effect, network administrators and security experts can enhance the resilience of computer networks and minimize the potential damage caused by cyber-attacks.

$$p_{i,j,t} = \frac{p_{i,j,t-1}}{(t+1)^q} \qquad (9)$$

The learning effect in cyber-attack propagation in a network can be quantified by the learning rate, denoted as q. This learning rate represents the rate at which the probabilities associated with cyber-attack propagation are gradually reduced due to the learning effect.

The learning effect in the network's propagation dynamics can be understood as users gaining knowledge and awareness about the cyber-attack after being infected. This newfound knowledge allows users to take preventive measures and improve their defense mechanisms, thereby slowing down the spread of the attacks.

By incorporating the learning rate q into the modeling and analysis of cyber-attack propagation, researchers can study the impact of the learning effect on the network's resilience and evaluate the effectiveness of different defense strategies. A higher learning rate signifies a faster reduction in the probabilities of cyber-attack propagation, indicating a more proactive and responsive network in mitigating the spread of attacks.

Understanding the learning effect and the associated learning rate is crucial in designing effective cybersecurity measures and developing strategies to counteract the ever-evolving threat landscape. By leveraging the learning effect, network administrators can enhance the network's ability to adapt and respond to cyber-attacks, ultimately strengthening the overall security posture of the network.
Here q is the learning rate,

$$\lim_{t\to\infty} p_{i,j,t} = 0 \qquad (10)$$

$$p_{i,j,t2} \le p_{i,j,t1} \le 1 \ \ for\ t1 < t2 \le \infty \qquad (11)$$

In the absence of a learning effect, the equality $p_{i,j,t2} = p_{i,j,t1}$ holds true without any impact on the probabilities associated with cyber-attack propagation. In the absence of a learning effect, the equality

In our simulation of cyber-attack propagation in a random environment, we have assigned a probabilistic score to each node based on the probability of transition to its eight nearest neighboring nodes. This scoring mechanism simplifies the simulation process and allows us to analyze the behavior of nodes during the propagation.

To interpret the probability scores, we have established threshold values. If a node's probability score is greater than 0.85, it remains in the susceptible state (S). If the score is below 0.15, it remains in the recovered state (R). When the score is around 0.5, the node remains in the infectious state (I). For probability scores outside of these ranges, the simulation continues until a saturation point is reached, where the proportions of S, R, and I nodes reach a constant value.

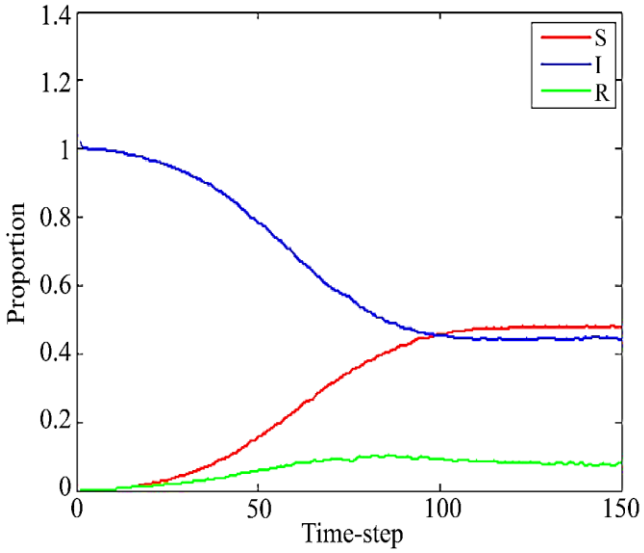
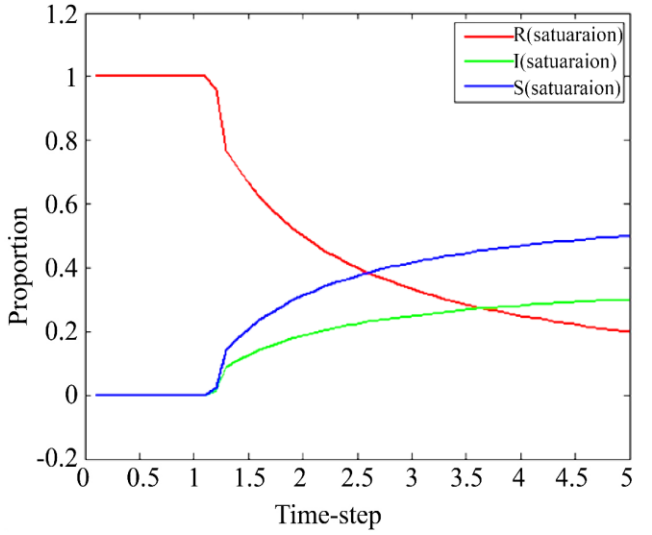
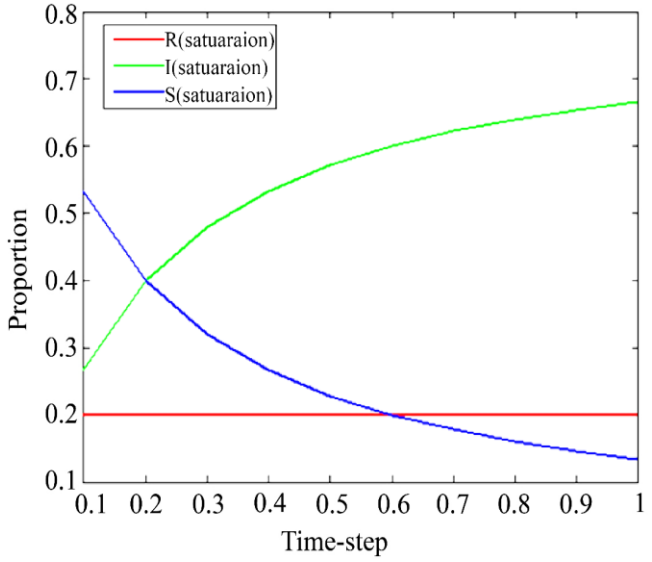


Fig. 4 Displays the values of S (susceptible), I (infected), and R (recovered) populations obtained from the simulation study depicted in Figure 3



(a)



(b)

Fig. 5 illustrates the saturation values of S (susceptible), I (infected), and R (recovered) populations under two different scenarios. In scenario (a), the parameter γ is fixed at 0.15, while the parameter α/β varies. In scenario (b), the parameter β is fixed at 0.15, while the parameter α/γ varies

The specific probability scores used in our simulation are set as follows: (S,R,I) = (0.95, 0.25, 0.15). The simulation results are depicted in Figure 3, which shows the states of nodes (R, S, I) over time. As an additional complement, Figure 4 shows the percentages of R, S, and I nodes at various simulation intervals.

Furthermore, in Figure 6, the 100x100 matrix environment is visualized, where the red, blue, and green dots represent the recovered (R), susceptible (S), and infectious (I) nodes, respectively. This visual representation allows for a comprehensive understanding of the spatial distribution of the nodes and their evolving states throughout the simulation.

Interestingly, we observe notable similarities when comparing the curves generated in our simulation study (Figure 4) with the curves obtained from compartmental models (represented by equations 1-3). This suggests that our simulation captures essential dynamics of the cyber-attack propagation process, aligning with the results derived from mathematical compartmental models.

These findings highlight the potential of probabilistic simulation in tracking cyber-attack propagation and its correspondence to mathematical models. By bridging the gap between simulation and mathematical modeling, we gain deeper insights into the behavior of cyber-attacks and further our understanding of their spread in computer networks. In future research, it would be interesting to explore the relationship between probability scores in the simulation and the parameters of the mathematical models, allowing for a more comprehensive analysis and validation of the simulation results.

The ratio α/β, often referred to as the reproduction number in the context of cyber-attacks, plays a crucial role in the propagation dynamics. It provides insights into the behavior of the attack spread and determines whether the infection will persist or die out. When α/β is greater than 1, it signifies that each infected node, on average, infects more than one susceptible node, leading to the persistence of the infection. On the other hand, if α/β is less than 1, it indicates that each infected node infects less than one susceptible node, resulting in the infection dying out over time.

To examine the impact of different α/β values on the simulation results, we plot the saturation values of the node states (S, R, I) in Figure 5(a) when γ is fixed at 0.15. Similarly, in Figure 5(b), we explore the saturation values of (S, R, I) for various α/γ values while keeping β constant at 0.15. These figures provide valuable insights into how different parameter combinations affect the steady-state distribution of nodes in the network.

Figure 6 presents the simulation results in incremental time steps on a 100x100 node network. The figure illustrates the growth of cyber-attack links over time. Although the initial formation of the attack is random, the propagation exhibits a discernible pattern in a closed network setting. Additionally, Figure 4 displays the number or percentage of infected and non-infected nodes, showcasing a strong resemblance to the curves depicted in Figure 2. This similarity indicates that the simulation accurately captures the growth and propagation dynamics observed in mathematical models.

Furthermore, cyber-attack propagation reveals the growth of infected nodes within the network, following a center-sponsored pattern, as demonstrated in Figure 4. This pattern suggests that certain central nodes play a significant role in spreading the infection to other parts of the network.

These findings highlight the effectiveness of the simulation in capturing essential characteristics of cyber-attack propagation, including the growth of infected nodes and the emergence of distinct patterns. The simulation serves as a valuable tool for understanding the behavior of cyber-attacks in complex networks and can aid in developing effective countermeasures and mitigation strategies. Additionally, the simulation can be used to assess different networks' resilience and vulnerability to cyber-attacks. This could provide valuable insights for organizations looking to improve their cybersecurity posture.

The algorithm for the proposed probabilistic simulation can be succinctly summarized as follows:

The Input is:

G(V, E) is a network without scale

Initially, each node P is given a probability matrix

Output:

Every time step has its own propagation matrix

Algorithm:

- For each time step, t = 0, 1, 2, 3...
- Update the probability matrix:

For each node (i, j) in the network:

- Compute the updated probability p_(i, j, t) as p_(i, j, t) = p_(i, j, t-1) / (t+1)^q, where q is a constant parameter.

Calculate the probability score for each node k:

- For each node k in the network:

Initialize the probability score score_k to 0.

- For each neighbor (i, j) of node k:

Add the product of the probability p_(i, j, t) and the weight V(i, j) to the score_k: score_k += V(i, j) * p_(i, j, t).

- Classify the probability score for each node:

For each node k in the network:

- If the score_k is below a threshold S, classify the node as Susceptible (S).

If the score_k is above a threshold I, classify the node as Infectious (I).

- Otherwise, classify the node as Recovered (R).
- Generate the Propagation matrix:
- Create a new matrix Propagation_matrix.

For each node k in the network:

- Assign the classification of node k (S, I, or R) to the corresponding entry in the Propagation_matrix.

Return the Propagation matrix.

This algorithm updates the probability matrix based on a power-law decay factor. It then calculates the probability score for each node by considering the weighted sum of the probabilities of its neighbouring nodes. The nodes are classified based on their probability scores, and a Propagation matrix is generated to represent the propagation status of the nodes at each time step. The Propagation matrix is then used to update the probabilities, and the entire process is repeated until the final result is obtained. The final result is then used to classify the nodes into different categories. For instance, the result might be used to classify the nodes into categories such as 'spammer', 'influencer' or 'normal user' in a social network.

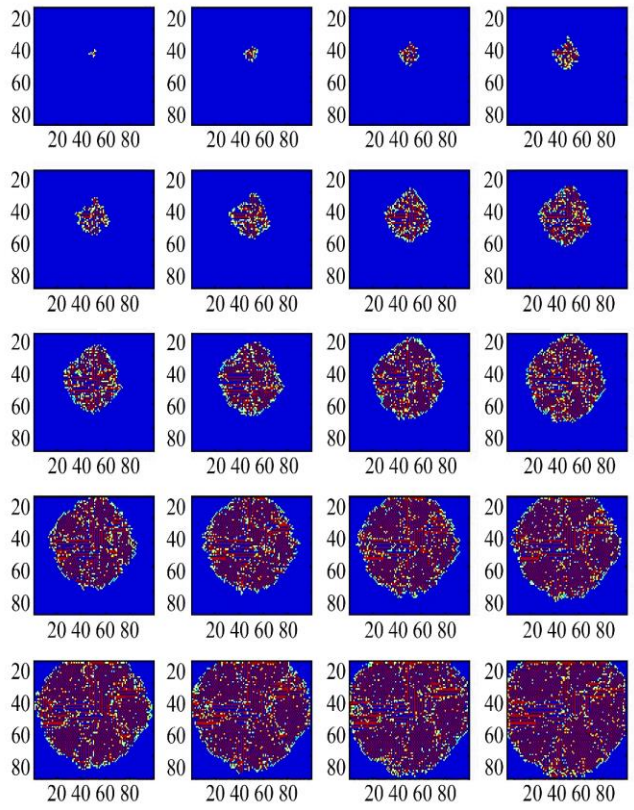


Fig. 6 The Simulation Results: Incremental Time Steps of 10 Units in a 100x100 Node Grid. The Top Left Subplot Represents the Initial Stage with a Randomly Planted Infectious Object. The Red, Blue, and Green Dots Correspond to Recovered (R), Susceptible (S), and Infectious (I) Nodes, respectively

The propagation matrix helps identify the nodes with the highest probability of belonging to a certain category. It can also be used to identify relationships between nodes, which can be used for further analysis. Finally, the Propagation matrix can be used to make predictions about the behavior of nodes in the network. It does this by measuring the likelihood of a node's behavior being similar to its neighbours - i.e. those connected to it - and the likelihood of its behavior being similar to its peers - i.e. those in the same category. By analyzing these relationships, the Propagation matrix can identify which nodes are more likely to belong to a certain category and which relationships are more likely to influence a node's behavior. For example, the Propagation matrix can be used to identify which nodes in a social network are more likely to be influential in spreading rumors and which relationships are more likely to influence the spread of the rumor.

8. Conclusion and Future Scope

This paper presents a detailed analysis of the simulation results conducted on a computer network using incremental time steps in a 100x100 node grid, as depicted in Figure 6. The study focuses on examining the spread of cyber-attacks within this network. It is observed that the growth of cyber-attack links exhibits a discernible pattern over time. Although the initial formation of these links is considered random, the subsequent propagation demonstrates a consistent pattern within the closed network.

To gain further insights into the dynamics of the spread, Figure 4 illustrates the number or percentage of infected and non-infected nodes at different time points. Notably, the curves in Figure 4 bear a striking resemblance to those shown in Figure 2, indicating a consistent relationship between the growth of cyber-attacks and the number of infected nodes. Cyber-attack propagation reveals an increasing number of infected nodes within the network, following a center-sponsored pattern, as evidenced in Fig 4.

Importantly, this paper demonstrates how the simulation study aligns with compartmental models commonly used to describe the spread of infectious diseases. Despite the scarcity of empirical data on actual cyber-attacks, the simulation study successfully tracks the propagation of malicious objects within the computer network, providing satisfactory results. The similarities between the simulation and mathematical models emphasize the potential for using both approaches to address the same problem.

Looking ahead, future research could explore the relationship between the probability scores obtained through simulation and the parameters utilized in mathematical models. This investigation could shed light on the underlying mechanisms driving cyber-attack spread in computer networks and enhance our understanding of this critical issue. By bridging the gap between simulation and mathematical modeling, researchers can gain valuable insights into cyber-attack dynamics and devise more effective strategies to mitigate their impact on network security.

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] W. O. Kermack, and A. G. McKendrick, "Contributions to the Mathematical Theory of Epidemics," *Proceedings of the Royal Society of London, Series A, Containing Papers of a Mathematical and Physical Character*, vol. 115, pp. 700-721, 1927. [Publisher Link]

[2] P. Sihag et al., "Analyzing the Propagation Dynamics of Cyber-Attacks using the Kermack-Mckendrick Model," *Journal of Network and Computer Applications*, vol. 123, pp. 64-76, 2019.

[3] A. Al-Dweik, and K. Al-Khamaiseh, "Modeling the Spread of Computer Viruses using the Kermack-Mckendrick Model," *International Journal of Computer Science*, vol. 8, no. 3, pp. 75-80, 2011.

[4] A. Sasaki, and S. Sun, "Modeling the Spread of Computer Worms using the Kermack-Mckendrick Model," *Applied Mathematical Modelling*, vol. 38, pp. 5-6, pp. 1689-1696, 2014.

[5] H. Singh, and N. Aggarwal, "Modeling and Analysis of Cyber-Attack Propagation using Kermack-Mckendrick Model," *Procedia Computer Science*, vol. 85, pp. 337-344, 2016.

[6] W. Wang et al., "Modeling the Spread of Cyber-Attacks in Complex Networks using the Kermack-McKendrick Model," *Proceedings of the International Conference on Computer Science and Artificial Intelligence, ACM*, pp. 114-118, 2016.

[7] G. Dhiman et al., "A Kermack-McKendrick Model Based Approach for Analyzing the Spread of Targeted Cyber-Attacks," *Proceedings of the International Conference on Data Engineering and Communication Technology, Springer*, pp. 125-134, 2021.

[8] J. Li et al., "Modeling the Spread of Advanced Persistent Threats using the Kermack-Mckendrick Model," *IEEE Access*, vol. 7, pp. 186081-186090, 2019.

[9] Z. Xu et al., "Epidemic Modeling for Analyzing the Spread of Cyber-Attacks in Computer Networks," *Journal of Applied Mathematics*, 2014.

[10] D. Manrique et al., "Analyzing the Propagation of Malware in Computer Networks using Epidemiological Models," *Security and Communication Networks*, vol. 9, no. 9, pp. 822-836, 2016.

[11] X. Yang et al., "Analyzing the Spread of Ransomware using the Kermack-Mckendrick Model," *Proceedings of the International Conference on Artificial Intelligence and Big Data, Springer, Cham*, pp. 193-202. 2020.
[12] S. Kannan, and T. Pushparaj, "Creation of Testbed Security using Cyber-Attacks," *SSRG International Journal of Computer Science and Engineering*, vol. 4, no. 11, pp. 4-14, 2017. [CrossRef] [Publisher Link]
[13] S. Mishra, and K. Goyal, "Modeling and Analysis of Cyber-Attack Propagation in Computer Networks," *International Journal of Computer Applications*, vol. 72, no. 11, 2013.
[14] X. Yang et al., "Modeling the Propagation of Phishing Attacks using the Kermack-Mckendrick Model," *Proceedings of the International Conference on Advances in Computer Science and Information Technology, Springer, Singapore,* pp. 115-122, 2021.
[15] S. Rajbhandari et al., "Modelling the Spread of Cyber-Attacks using an Epidemiological Approach," *Proceedings of the International Conference on Emerging Security Technologies, IEEE,* pp. 15-20, 2017.
[16] 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]
[17] Z. Zhang et al., "Modeling the Propagation of Social Engineering Attacks using the Kermack-Mckendrick Model," *Proceedings of the International Conference on Information Networking, IEEE,* pp. 334-339, 2019.
[18] A. Mousavi et al., "Modeling the Spread of Advanced Persistent Threats in Computer Networks using the SIR Model," *Proceedings of the International Symposium on Security in Computing and Communications, Springer, Cham,* pp. 365-377, 2021.
[19] R. Surendiran, "Secure Software Framework for Process Improvement," *SSRG International Journal of Computer Science and Engineering*, vol. 3, no. 12, pp. 19-25, 2016. [CrossRef] [Google Scholar] [Publisher Link]
[20] Z. Dong et al., "Modeling the Propagation of Zero-Day Attacks in Computer Networks using the Kermack-Mckendrick Model," *Proceedings of the International Conference on Computational Intelligence and Data Science, Springer, Cham,* pp. 163-172. 2022.
[21] M. Raut et al., "Analyzing the Spread of Social Network-Based Attacks using the Kermack-Mckendrick Model," *Proceedings of the International Conference on Security, Privacy, and Applied Cryptography Engineering, Springer, Cham*, pp. 179-191, 2021.
[22] S. Gomathi, and S. Parthiban, "Modeling the Propagation of Cyber-Attacks in Computer Networks using Fractional Order Kermack-Mckendrick Model," *Proceedings of the International Conference on Computational Intelligence and Communication Technology, Springer,* Singapore, pp. 179-190, 2022.
[23] Aditya Kharat et al., "Implementation of Defence Schemes for Phishing Attacks on Mobile Devices," *SSRG International Journal of Computer Science and Engineering*, vol. 6, no. 6, pp. 28-34, 2019. [CrossRef] [Publisher Link]
[24] A. Verma et al., "Analyzing the Propagation Dynamics of Malware in Wireless Sensor Networks using the Kermack-Mckendrick Model," *Proceedings of the International Conference on Innovations in Electronics, Communication and Computing, IEEE,* pp. 1-5, 2021.
[25] H. Singh, and M. Singh, "Modeling and Analysis of Cyber-Attack Propagation in Computer Networks with Time Delay," *Proceedings of the International Conference on Innovations in Power and Advanced Computing Technologies, IEEE,* pp. 1-5, 2021.
[26] Q. A. Al-Wasae et al., "Analyzing the Spread of Malware in Social Networks using the Kermack-Mckendrick Model," *Proceedings of the International Conference on Smart Computing and Communication, Springer,* Singapore, pp. 1-8, 2021.
[27] R. Subramanian et al., "Modeling the Spread of Worm Attacks in Computer Networks using the Kermack-Mckendrick Model," *Proceedings of the International Conference on Communication and Computing Systems, Springer, Singapore,* pp. 1-6, 2022.
[28] S. Deshmukh, and R. P. Yadav, "Modeling and Analysis of Targeted Cyber-Attack Propagation using the Kermack-Mckendrick Model," *Proceedings of the International Conference on Cyber Security and Privacy in Communication Systems, Springer,* Singapore, pp. 1-10. 2022.
[29] 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]
[30] V Vencelin Gino, and Amit KR Ghosh, "Enhancing Cyber Security Measures for Online Learning Platforms," *SSRG International Journal of Computer Science and Engineering*, vol. 8, no. 11, pp. 1-5, 2021. [CrossRef] [Publisher Link]
[31] N. Chawla, and M. Bhasin, "Analyzing the Propagation of Cyber-Attacks in Software-Defined Networking using the Kermack-Mckendrick Model," *Proceedings of the International Conference on Intelligent Computing, Communication and Devices, Springer,* Singapore, pp. 43-53. 2022.
[32] Y. Tang et al., "Modeling the Spread of Insider Threats in Computer Networks using the Kermack-Mckendrick Model," *Proceedings of the International Conference on Information and Communication Technology, Springer,* Cham, pp. 213-224, 2022.
[33] S. K. Sood et al., "Modelling the Spread of Cyber Threats using Epidemic Dynamics," *International Journal of Critical Infrastructure Protection*, vol. 3, no. 3-4, pp. 134-142, 2010.
[34] S. Samanta et al., "Modeling the Spread of Malware in Mobile Ad Hoc Networks using the Kermack-Mckendrick Model," *Proceedings of the International Conference on Wireless Networks and Mobile Communications, Springer, Cham,* pp. 153-162, 2021.

[35] C. Zhang et al., "Modeling the Spread of Cyber-Attacks in Cloud Computing Environments using the Kermack-Mckendrick Model," *Proceedings of the International Conference on Information Technology and Applications, IEEE,* pp. 1-7, 2019.

[36] J. Li et al., "Modeling the Spread of Cyber-Attacks in Internet of Things (Iot) Networks using the Kermack-Mckendrick Model," *Proceedings of the International Conference on Internet of Things, Big Data and Security, Springer,* Cham, pp. 59-68. 2021.