Modeling self-propagating malware with epidemiological models

Alesia Chernikova¹*, Nicolò Gozzi², Nicola Perra³, Simona Boboila¹, Tina Eliassi-Rad¹ and Alina Oprea¹

Abstract

Self-propagating malware (SPM) is responsible for large financial losses and major data breaches with devastating social impacts that cannot be understated. Well-known campaigns such as WannaCry and Colonial Pipeline have been able to propagate rapidly on the Internet and cause widespread service disruptions. To date, the propagation behavior of SPM is still not well understood. As result, our ability to defend against these cyber threats is still limited. Here, we address this gap by performing a comprehensive analysis of a newly proposed epidemiological-inspired model for SPM propagation, the Susceptible-Infected-Infected Dormant-Recovered (SIIDR) model. We perform a theoretical analysis of the SIIDR model by deriving its basic reproduction number and studying the stability of its disease-free equilibrium points in a homogeneous mixed system. We also characterize the SIIDR model on arbitrary graphs and discuss the conditions for stability of disease-free equilibrium points. We obtain access to 15 WannaCry attack traces generated under various conditions, derive the model’s transition rates, and show that SIIDR fits the real data well. We find that the SIIDR model outperforms more established compartmental models from epidemiology, such as SI, SIS, and SIR, at modeling SPM propagation.

Keywords: Self-propagating malware, Compartmental models, Epidemiology, Modeling, Dynamical systems

Introduction

Self-propagating malware (SPM) is one of today’s most concerning cybersecurity threats. Over past years, SPM resulted in huge financial losses and data breaches with high economic and societal impacts. For instance, the infamous WannaCry (Mike Azzara 2021) attack, first discovered in 2017 and still actively used by attackers nowadays, was estimated to have affected more than 200,000 computers across 150 countries worldwide, with economic damages ranging from hundreds of millions to billions of dollars. In May 2021, the Colonial Pipeline (Wikipedia 2023a) cyber-attack caused the shut down of the entirety of the Colonial gasoline pipeline system for several days. It affected consumers and airlines along the East Coast of the United States and was deemed a national security threat. Another remarkable worldwide SPM attack is Petya (Wikipedia 2023b), first discovered in 2016 when it started spreading through phishing emails. Petya represents
a family of various types of ransomware responsible for estimated economic damages of over 10 million dollars (Wikipedia 2023b).

Given the current cyber-crime landscape, with new threats emerging daily, tools designed for modeling SPM behavior become crucial. Indeed, a deep understanding of self-propagating malware characteristics provides us opportunities to identify threats, test control strategies, and design proactive defenses against attacks. A large body of research on the subject so far has been devoted to the design of methods to detect and mitigate self-propagating malware. Proposed techniques include network traffic signatures (Kim and Karp 2004; Kumar and Lim 2020; Ongun et al. 2021; Newsome et al. 2005) and host-level binary analysis (Chen and Bridges 2017; Ben Said et al. 2018) used to identify anomalous behavior, software-defined networking (SDN) for ransomware threat detection and mitigation (Akbanov et al. 2019; Alotaibi and Vassilakis 2021), as well as evasion-resilient methods for detecting adaptive worms (Li and Stafford 2014; Newsome et al. 2005; Ongun et al. 2021). However, less attention was dedicated to comparing and finding the most suitable models to capture SPM behavior. Additionally, the majority of existing works on SPM modeling focus on theoretical analyses of infection spreading (Guillén et al. 2017; Guillén and del Rey 2018; Mishra and Saini 2007; Martínez Martínez et al. 2021), lacking a thorough real-world evaluation of these models.

In this paper, we model the behavior of a well-known SPM attack, WannaCry, based on real-world attack traces. The similarities between the behavior of biological and computer viruses enable us to leverage compartmental models from epidemiology. We adopt a novel compartmental epidemic model called SIIDR (Chernikova et al. 2022), and conduct a thorough analysis to show that it can be used to accurately model SPM spreading dynamics.

First, we study the model assuming a homogeneous mixing of hosts and analytically derive its basic reproduction number $R_0$ (Dietz 1993; Kephart and White 1993; Van den Driessche and Watmough 2008). $R_0$ is the number of secondary cases generated by an infectious seed in a fully susceptible population. It describes the epidemic threshold, thus, the conditions necessary for a macroscopic outbreak ($R_0 > 1$) (Fraser et al. 2009; Van den Driessche and Watmough 2008). We also investigate equilibrium or fixed points of SIIDR as they provide insights on how to contain or suppress the spreading.

Additionally, computer networks are often represented as graphs, where nodes denote the hosts in the network and edges represent the communication links between them. In any static graph, the propagation of contagion processes depends not only on the transition rates of SPM but also on the spectral properties of the graph (Newman 2018). To discuss the important characteristics of SIIDR that illustrate the ability of SPM to successfully propagate through the network in these settings, we represent SIIDR model as a Non-Linear Dynamical System (NLDS) and relaxing the homogeneous mixing assumption.

Finally, we reconstruct the dynamics of WannaCry spreading analysing real traffic logs. We use the Akaike Information Criterion (AIC) (Akaike 1974) to compare how different compartmental models fit the derived epidemic traces. We show that SIIDR captures malware spreading better than classical epidemic models such as SI,
SIS, SIR. Indeed, the investigation of real WannaCry attacks showed that consecutive infection attempts originating from the same host are delayed by a variable time interval. This finding suggests the existence of “dormant” infected state, in which infected hosts temporarily cease to pass infection to their neighbors. Furthermore, calibrating the model to the real data via an Approximate Bayesian Computation technique we determine the transition rates (i.e., model parameters) that characterize WannaCry propagation.

To summarize, our contributions are the following:

- We derive the basic reproduction number of the SIIDR model (Chernikova et al. 2022) and discuss the stability conditions of the disease-free equilibrium points of the system of ODEs that represents SIIDR under a homogeneous mixing assumption.
- We derive the conditions for stability of the SIIDR disease-free equilibrium points on arbitrary graphs thus relaxing the homogeneous mixing assumption.
- We reconstruct the spreading dynamics of an actual SPM (WannaCry) using real-world traces obtained by running a vulnerable version of Windows in a virtual environment.
- We show that SIIDR outperforms several classical models in terms of capturing WannaCry behavior, and derive the model’s transition rates from actual attacks.

We organize the rest of the paper as follows: first, we provide background information about the WannaCry malware and the most common compartmental models of epidemiology. We also define the threat model and problem statement. Then we introduce the SIIDR model, discuss the derivation of $R_0$ and the stability of the disease-free equilibrium points. In addition, we present the experimental results that support the findings of the paper. Table 1 includes common terminology used in the paper.

| Notation | Meaning |
|----------|---------|
| $S$      | Number of susceptible individuals |
| $I$      | Number of infected individuals |
| $I_D$    | Number of infected dormant individuals |
| $R$      | Number of recovered individuals |
| SPM      | Self-propagating malware |
| ODE      | Ordinary differential equation |
| AIC      | Akaike information criterion |
| ABC      | Approximate Bayesian computation |
| ABC-SMC (SMC) | Sequential Monte-Carlo approach |
| ABC-SMC-MNN (SMC) | SMC when covariance matrix is calculated using $M$ nearest neighbors of the particle |
| SI       | Susceptible-infected model |
| SIS      | Susceptible-infected-susceptible model |
| SIR      | Susceptible-infected-recovered model |
| SEIR     | Susceptible-exposed-infected-recovered model |
| SIIDR    | Susceptible-infected-infected dormant-recovered model |
Background and problem statement

WannaCry malware

WannaCry is a self-propagating malware attack, which targets computers running the Microsoft Windows operating system by encrypting data and demanding ransom in Bitcoins. It automatically spreads through the network and scans for vulnerable systems, using the EternalBlue exploit to gain access, and the DoublePulsar backdoor tool to install and execute a copy of itself. WannaCry malware has a 'kill-switch' that appears to work like this: part of WannaCry's infection routine involves sending a request that checks for a web domain. If its request returns showing that the domain is alive or online, it will activate the 'kill-switch,' prompting WannaCry to exit the system and no longer proceed with its propagation and encryption routines. Otherwise, if the malicious program cannot connect to the domain, it encrypts the computer's data, then attempts to exploit the vulnerability of Server Message Block protocol to spread out to random computers on the Internet, and laterally to computers on the same network (Wikipedia 2023c).

Epidemiological models

Compartmental epidemiological models are used to model the spread of infectious diseases (Brauer 2008; Keeling and Rohani 2008). This approach segments the population into groups (compartments) describing the various stages of infection. The compartmental structure varies according to the disease under study and the application of the model. Following disease evolution, individuals can transition at specific rates among compartments. Generally speaking, these transitions can be either spontaneous (e.g., recovery process) or resulting from interactions (e.g., infection process). In their simplest formulation, compartmental models assume homogeneous mixing. Said differently, each individual is potentially in contact with everyone else (Vespignani 2012).

The most common compartmental models are the SI, SIS, SIR and SEIR models. In Appendix 1 we will briefly review the formulation of these models by neglecting demographic changes in the population (i.e., the number of individuals is assumed to be fixed). More in detail, we represent them as systems of Ordinary Differential Equations (ODEs). This is a common approach to model epidemics in continuous time, even though it approximates the number of individuals in different compartments as continuous functions.

Problem statement and threat model

The objective of our work is to provide a rigorous mathematical analysis of realistic SPM attacks, and thus lay down the foundation of efficient defense strategies against these prevalent threats. Several works propose models to capture the behavior of SPM (Guillén et al. 2017; Guillén and del Rey 2018; Mishra and Saini 2007; Martínez Martínez et al. 2021), however, the vast majority of them have only theoretical analysis and do not incorporate the information about real-world SPM traces. Thus, they lack validation in real-world scenarios. Additionally, it is hard to perform comparative analysis to other models without presenting their performance using real-world data. Existing work that uses actual malware traces for modeling SPM (Levy et al. 2020) leverages minimal
epidemiological models that, in their simplicity, fail to fully capture malware characteristics. To this end, here we use a more advanced compartmental model (called SIIDR) to describe epidemics resulting from SPM and apply it to real-world attack traces from a well-known malware, WannaCry.

Besides studying different epidemiological models according to their suitability to describe WannaCry epidemics, our second goal is to infer the parameters of the SIIDR epidemic model for different malware variants. Parameter inference is crucial for enabling attack simulations on real networks to measure the impact of the attack, as well as the effectiveness of defensive measures. Indeed, once the parameters of the attack are known, an analyst could estimate the basic reproduction number of the attack, and understand whether the attack might result in a macroscopic outbreak. Similarly, a defender might configure its network topology by performing edge or node hardening (Le et al. 2015; Tong et al. 2012; Torres et al. 2021), minimizing the leading eigenvalue of the graph to prevent the damage from self-propagating malware attacks, or using anomaly detection methods to detect the malware propagation (Ongun et al. 2021).

In this work, our focus is on modeling SPM propagation inside a local network (e.g., enterprise network, campus network) since we do not have global visibility on SPM propagation across different networks. We assume that the attacker gets a foothold inside the local network through a single initially infected host. From the ‘patient zero’ victim, the attack can propagate and infect other vulnerable machines in the subnet. We initially assume a homogeneous mixing model, meaning that every machine can contact all others. This is a valid assumption because in a subnet every machine is able to scan every other internal IP within the same subnet. We are assuming that none of the machines is immune to the exploited vulnerability at the beginning of the attack, thus, all of them may become infected during SPM propagation. Infectious machines become recovered when the malware is successfully detected and an efficient recovery process removes it. We assume that these machines cannot be reinfected again. We then relax the homogeneous mixing assumption and characterize the behavior of the model on arbitrary graph, considering that a contact between any two nodes in a network does not occur randomly with equal probabilities, but each node communicates with the particular subset of nodes in the network.

Related work
Numerous works propose to simulate and model malware propagation on different levels of fidelity and scalability (Perumalla and Sundaragopalan 2004). The research on modeling malware and worms propagation includes hardware testbeds (Vahdat et al. 2002; White et al. 2002), emulation systems (Durst et al. 1999; Wei et al. 2010), packet-level simulations (Riley et al. 2004; Szymanski et al. 2003), fully-virtualized environments (Perumalla and Sundaragopalan 2004), mixed abstraction simulations (Guo et al. 2000; Kiddle et al. 2003), and epidemic models. In our work we focus on this last line of research. Similarly, Mishra and Jha (Mishra and Jha 2010) introduce the SEIQRS (Susceptible-Exposed-Infectious-Quarantined-Recovered-Susceptible) model for viruses and study the effect of the quarantined compartment on the number of recovered nodes. In their paper, the authors focus on the analysis of the threshold that determines the
outcome of the disease. Mishra and Pandey (2014) introduce the SEIS-V model for viruses with a vaccinated state, while (Mishra and Saini 2007) study the SEIRS model to characterize the malicious objects’ free equilibrium, formulating the stability of the results in terms of the threshold parameter. Toutonji et al. (2012) propose a VEISV (Vulnerable-Exposed-Infectious-Secured-Vulnerable) model and use the reproduction rate to derive global and local stability. With the help of simulation, they show the positive impact of increasing security countermeasures in the vulnerable state on worm-exposed and infectious propagation waves. Guillén et al. (2019) introduce a SCIRAS (Susceptible-Carrier-Infectious-Recovered-Attacked-Susceptible) model. Authors study the local and global stability of its equilibrium points and compute the basic reproductive number. Ojha et al. (2021) develop a new SEIQRV (Susceptible-Exposed-Infected-Quarantined-Recovered-Vaccinated) model to capture the behavior of malware attacks in wireless sensor networks. In their work, authors obtain the equilibrium points of the proposed model, analyze the system stability under different conditions, and verify the performance of the model through simulations. Zheng et al. (2020) introduce the SLBQR (Susceptible-Latent-Breaking out-Quarantined-Recovered) model considering vaccination strategies with temporary immunity as well as quarantined strategies. The authors study the stability of the model, investigate a strategy based on quarantines aimed at suppressing the spread of the virus, and discuss the effect of the vaccination on permanent immunity. In order to verify their findings, the authors simulate the model exploring a range of temporary immune times and quarantine rates.

Recently, several attempts have been made to enhance the realism of the epidemic models. For instance, Guillén et al. (2017) study the SEIRS model with an improved incidence rate (i.e., new infected hosts per time unit). Additionally, the equilibrium points are computed and their local and global stability are studied. Finally, the authors derive the explicit expression of the basic reproductive number and propose efficient measures to control the epidemics. Martínez Martínez et al. (2021) introduce a dynamic version of SEIRS. The authors look at the performance of the model with different sets of parameters, propose optimal values, and discuss its applicability to model real-world malware. Gan et al. (2020) propose a dynamical SIP (Susceptible-Infected-Protected) model, find an equilibrium point, and discuss its local and global stability. Additionally, the authors perform the numerical simulations of the model to demonstrate the dependency on parameter values. Yao et al. (2018) present a time-delayed worm propagation model with variable infection rate. They analyze the stability of equilibrium and the threshold of Hopf bifurcation. The authors carry out the numerical analysis and simulation of the model.

Some papers explore malware propagation on networks comprised of different types of devices. For instance, Guillén and del Rey (2018) considers the special class of carrier devices whose operative systems are not targeted by malware (for example, iOS devices for Android malware); the authors introduce a new compartment (Carrier) to account for these devices, and analyze efficient control measures based on the basic reproductive number. Zhu et al. (2012) take into consideration the ability of viruses to infect not only computers, but also many kinds of external removable devices; in their model, internal devices can be in Susceptible, Infected, and Recovered states, while removable devices can be in Susceptible and Infected states.
None of these previous works perform model fitting to real-world malware scenarios, but only consider theoretical analyses of the proposed models. The closest to our work is Levy et al. (2020); the authors use real traces to fit malware propagation with SIR, a simplistic model that, as we have shown, performs poorly compared to SIIDR and fails to capture self-propagating malware dynamics.

**Analysis of the SIIDR model**

In this section, we introduce the main characteristics of WannaCry propagation dynamics, the proposed modeling framework (the SIIDR model), we discuss its basic reproduction number and the stability of disease-free equilibrium points. Table 2 includes common terminology used in this section.

**SPM modeling with the SIIDR model**

A detailed analysis of the WannaCry traces (Chernikova et al. 2022) revealed the following characteristics:

- The time interval $\Delta t$ between two consecutive malicious attempts from the same infected IP is not constant and has high variability. This intuition is supported by the results in Fig. 1 where we show the quartile coefficient of dispersion (QCoD) of these $\Delta t$ for different WannaCry variants. The QCoD is defined as $(Q_3 - Q_1)/(Q_3 + Q_1)$. As benchmark we show the hypothetical QCoD of exponentially distributed $\Delta t$ with the same mean observed in the data. We chose the exponential distribution since time intervals lapsing between Poisson-like events happening at constant rate follow this distribution. From the figure we see that the QCoD of $\Delta t$ obtained from the data is much higher ($\sim 50\%$ more across variants) than the one we would expect to see with constant frequency events.

![Fig. 1](image-url)  
**Fig. 1** Quartile coefficient of dispersion of $\Delta t$ between two consecutive malicious attempts from the same infected IP and of exponential distribution with same mean for different WannaCry variants
• The time interval $\Delta t$ between the last attack from an infected IP and the end of the collected trace is large. The average values of $\Delta t$ between two consecutive malicious attempts and $\Delta t$ between the last attack attempt from an infected IP and the end of the epidemics are shown in Fig. 2. The mean value of the $\Delta t$ in the second case are much larger then the $\Delta t$ between two consecutive attack attempts.

Based on the first observation, an infected dormant state $I_D$ is included to capture the heterogeneous distribution of time windows between two malicious attack attempts. Therefore, an infected node can become dormant for some period of time and resume its malicious activity later. The second observation supports the presence of a Recovered state: once nodes recover, they will not become infectious or susceptible again, at least within a certain observation period. The transition diagram corresponding to the SIIDR model is illustrated in Fig. 3. Interacting with the infectious, a susceptible node can become infected with rate $\beta$, and afterwards, it may either
recover with rate $\mu$, or move to the dormant state with rate $\gamma_1$. From the dormant state, it may become actively infectious again with rate $\gamma_2$.

The evolution of the system can be modeled through the following ODEs system:

$$\begin{align*}
\frac{dS}{dt} &= -\beta S \frac{I}{N} \\
\frac{dI}{dt} &= \beta S \frac{I}{N} - \mu I - \gamma_1 I + \gamma_2 ID \\
\frac{dID}{dt} &= \gamma_1 I - \gamma_2 ID \\
\frac{dR}{dt} &= \mu I
\end{align*}$$

with $N = S(t) + I(t) + ID(t) + R(t)$, where the total size of the population $N$ is constant. It is important to stress how the system of ODEs assumes an homogeneous mixing in the host population.

**SIIDR equilibrium points**

While modeling SPM we are interested in equilibrium states when the number of infected individuals equals to 0 and does not change over time (i.e., disease-free equilibrium points). Thus, we need to derive the constant solutions of the ODE system corresponding to SIIDR model (Perko 2013).

| Notation | Meaning |
|----------|---------|
| $\beta$  | Infection rate |
| $\tilde{\beta}$ | Infection probability |
| $\mu$    | Recovery rate |
| $\gamma_1$ | Transition rate from infected to infected dormant compartment |
| $\gamma_2$ | Transition rate from infected dormant to infected compartment |
| $\xi_i(t)$ | The probability of node $i$ of not getting infected at time step $t$ |
| $\alpha_{XY}$ | The probability of a node to transition from state $X$ to $Y$ |
| $\omega_{XX}$ | The probability of a node to stay in the state $X$ |
| DFE | Disease-free equilibrium point |
| $R_0$ | The basic reproduction number |
| $G$ | Next-generation matrix |
| $X$ | The vector of individual numbers in each compartment |
| $E^*$ | Equilibrium point for SIIDR as the system of ODEs |
| $L$ | Lyapunov function |
| $p$ | Each node's vector of probabilities to be in each compartment |
| $p^*$ | Equilibrium point for SIIDR as the NLDS |
| $g$ | Matrix form of SIIDR represented as the NLDS |
| $C$ | Linear part of SIIDR as the NLDS Matrix Form |
| $B$ | Non-Linear Part of SIIDR as the NLDS Matrix Form |
| $A$ | Graph adjacency matrix |
| $\lambda_A$ | The largest eigenvalue of the adjacency matrix $A$ |
| $d$ | Degree of the $d$-regular Graph |
Definition 1  An equilibrium point or fixed point of the system of ODEs \( \dot{x} = f(X) \) is a solution \( E^* \) that does not change with time, i.e., \( f(E^*) = 0 \).

For the SIIDR model we can find the equilibrium points by solving the following system:

\[
-\beta I \frac{S}{N} = 0 \\
\beta I \frac{S}{N} - \mu I - \gamma_1 I + \gamma_2 I_D = 0 \\
\gamma_1 I - \gamma_2 I_D = 0 \\
\mu I = 0
\]

given that \( S + I + I_D + R = N \).

Thus, we find disease-free equilibrium points of the SIIDR model as \( E^* = (S, 0, 0, R) \) where \( I = I_D = 0 \) and \( S + R = N \). The particular case is the beginning of the propagation process when the number of recovered individuals is 0: \( R = 0 \) or \( E^* = (N, 0, 0, 0) \).

Therefore, we perform further analyses of SIIDR model based on this equilibrium point. There exists no endemic equilibrium point when \( I = 0 \) for SIIDR model. It is present only when \( \mu = 0 \) (SIID model) and is equal to \( (0, I^*, \frac{\gamma_1 I^*}{\gamma_2}, 0) \).

The basic reproduction number

The basic reproduction number \( R_0 \) is the number of secondary cases generated by a single infectious seed in a fully susceptible population (Keeling and Rohani 2008). \( R_0 \) defines the epidemic threshold, that is the condition for a macroscopic outbreak. If \( R_0 > 1 \), on average, infected individuals are able to sustain the spreading. If \( R_0 < 1 \), on average, the disease will die out before any macroscopic outbreak.

One way to derive the basic reproduction number is to use the next-generation matrix approach (Diekmann et al. 1990, 2010; Blackwood and Childs 2018). This states that the basic reproduction number is the largest eigenvalue of the next-generation matrix. The method takes into consideration the dynamics of compartments linked to new infections. For example the number of infected individuals in compartment \( i \), \( i \in \{1, \ldots, k\} \), where \( k \) is the number of compartments with infected individuals, changes as follows:

\[
\frac{df_i(X)}{dt} = F_i(X) - V_i(X)
\]

where \( F_i(X) \) is the rate of appearance of new infections in compartment \( i \) by all other means, \( V_i(X) = [V_i^-(X) - V_i^+(X)] \). \( V_i^+(X) \) is the rate of transfer of individuals into compartment \( i \) and \( V_i^-(X) \) represents the rate of transfer of individuals out of compartment. If \( E^* \) is a disease-free equilibrium, then we can define a next-generation matrix:

\[
G = FV^{-1}
\]

where:
In the case of SIIDR model, the matrix $G$ can be represented at one of the disease-free equilibrium points $DFE = (N, 0, 0, 0)$ as follows:

$$G = \begin{bmatrix} \beta & 0 \\ 0 & \mu + \gamma_1 & -\gamma_2 \\ 0 & -\gamma_1 & \gamma_2 \end{bmatrix}^{-1} = \begin{bmatrix} \frac{\beta}{\mu} & \frac{\beta}{\mu} \\ \frac{\beta}{\mu} & 0 \\ 0 & 0 \end{bmatrix}$$ (2)

Let $\tilde{v}$ be an eigenvector of the matrix $G$, and $\lambda$ its corresponding eigenvalue. The eigenvalue equation is (Bhatia 1997):

$$G\tilde{v} = \lambda \tilde{v},$$

where $\tilde{v}$ is a nonzero vector, therefore $det(\lambda I - G) = 0$. Using $G$ from equation 2, we obtain:

$$det(\lambda I - G) = \lambda \left( \lambda - \frac{\beta}{\mu} \right) = 0,$$

which results in: 1) $\lambda = 0$ or 2) $\lambda = \beta/\mu$. According to the next-generation matrix method (Diekmann et al. 1990, 2010; Blackwood and Childs 2018), the reproduction number $R_0$ is the largest eigenvalue of the next-generation matrix $G$, hence, $R_0 = \frac{\beta}{\mu}$, which is the same definition of $R_0$ of the SIR model. In other words, the introduction of the new compartment $I_D$ does not alter the conditions for a macroscopic outbreak. We note that, in general, the disease free equilibrium might contain individuals already immune to the disease, i.e., $E^* = (N - R, 0, 0, R)$. This might be due to wave of infections caused by previous introductions of the virus. In this more general case we have: $R_0 = \frac{\beta}{\mu} \left( 1 - \frac{R}{N} \right)$, where in parenthesis we have the fraction of the susceptible population.

**Stability analysis of SIIDR equilibrium points**

A particularly important characteristic of a disease-free equilibrium point is its stability (Hirsch and Smale 1974), which indicates whether the system will be able to return to the equilibrium point after small perturbations. For example, a small perturbation can be a slight increase in the number of initially infected nodes.

Let us consider the system of ODEs that captures the dynamics of our SIIDR model (see Eqs. 1), governed by:

$$\dot{X} = f(X), X \in \mathbb{R}^n$$

Let $X = E^*$ be a fixed point of $f(X)$, that is, $f(E^*) = 0$. Furthermore, let us assume that the system’s initial state at $t = 0$ is $X = X^0$. In this context, the stability of $E^*$ can be obtained answering to the following question: if the system starts near $E^*$, how close will it remain to $E^*$? Beside this intuition, stability is more formally defined as follows (Hirsch and Smale 1974):
Definition 2  The equilibrium point $E^*$ is stable if for any $\epsilon > 0$, there exists a $\delta > 0$ such that: if the system’s initial state $X^0$ lies in the ball of radius $\delta$ around $E^*$ (i.e., $||X^0 - E^*|| < \delta$), then solutions $X^t$ exist for all $t > 0$, and they stay in the ball of radius $\epsilon$ around $E^*$ (i.e., $||X^t - E^*|| < \epsilon$).

In addition:

Definition 3  We say that $E^*$ is locally asymptotically stable if it is stable and the solutions $X^t$ with initial state $X^0$ in the ball of radius $\delta$ converge to $E^*$ as $t \to \infty$.

And:

Definition 4  We say that $E^*$ is stable in the sense of Lyapunov (i.e., Lyapunov stable) when there exists the continuously differentiable function $L(X)$ such that:

\begin{equation}
\dot{L}(X) = \frac{dL}{dx} f_i(X) \leq 0, \dot{L}(E^*) = 0
\end{equation}

If $\dot{L}(X) < 0$ and $\dot{L}(X) = 0$ only when $X = E^*$, then $E^*$ is locally asymptotically stable.

We next analyze the stability of the SIIDR disease-free equilibrium points and show that they are Lyapunov stable, if the reproduction number $R_0$ is smaller or equal to one. We formally state and prove it in the following theorem:

Theorem 1  If $R_0 \leq 1$ the disease-free equilibrium point $E^*$ of the SIIDR system of ODEs is Lyapunov stable.

Proof  Let $L(X) = I + I_D$, where $L$ is the valid Lyapunov function as long as it is non-negative continuously differentiable scalar function which equals 0 at the disease-free equilibrium point ($I = I_D = 0$). The time-derivative of $L$ is the following:

\begin{equation}
\dot{L} = \frac{dL}{dt} = \frac{d(I + I_D)}{dt} = \beta_S \frac{I}{N} - \mu I,
\end{equation}

where we used Eqs. 1 that describe the evolution of $I$ and $I_D$. Therefore, $\dot{L} \leq 0$ (Eq. 4) when:

\begin{equation}
I \left( \frac{\beta S}{\mu N} - 1 \right) \leq 0
\end{equation}

Given the basic reproduction number $R_0 = \frac{\beta S}{\mu N}$, we obtain:

\begin{equation}
I(R_0 - 1) \leq 0
\end{equation}

Eq. 5 holds when $R_0 \leq 1$. Hence, $\dot{L} \leq 0$ when $R_0 \leq 1$. Furthermore, $\dot{L}(E^*) = 0$ (since $I = 0$ when $X = E^*$), which concludes the proof that $E^*$ is a Lyapunov stable disease-free equilibrium point.
Note that $\dot{L}(X) = 0$ when $I = 0$, even if $X \neq E^*$ (for instance, if $I_D \neq 0$). Thus, $E^*$ is not locally asymptotically stable (see Definition 4). □

SIIDR analysis on arbitrary graphs

Our analysis in previous sections was performed under the homogeneous-mixing assumption (Bansal et al. 2007; Vespignani 2012). In this limit, all hosts are well-mixed and potentially in contact. The homogeneous approximation might be a good representation of the contact dynamics in a local subnet where each machine can contact anyone else. However, the contact patterns in larger networks are complex. Indeed, many real networks (including the Internet) feature, among other properties, a heterogeneous connectivity distribution consisting of a few highly-connected ‘hubs’, while the vast majority of nodes have much lower connectivity (Albert and Barabási 2002; Pastor-Satorras et al. 2015). In this section, we analyze the epidemiological dynamics of the SIIDR model on arbitrary graphs that capture heterogeneity in host contact patterns. In this case, the propagation of malware can be modeled with a discrete-time Non-Linear Dynamical System (Chakrabarti et al. 2008; Prakash et al. 2011).

A NLDS system is specified by the vector of probabilities at time step $t + 1$ as $P_{t+1} = g(P_t)$, where $g$ is non-linear continuous function operating on a vector $P_t$. We define the system equations based on the transition diagram of the model (Fig. 3).

First, we are computing the probability of node $i$ of not getting infected at time step $t$: $\zeta_{i,t}(I)$, which happens when: (1) none of its neighbors are in state $I$, or (2) a neighbor is in state $I$ but fails to infect $i$ with probability $(1 - \tilde{\beta})$, where $\tilde{\beta}$ is the attack transmission probability over a contact-link. We note how $\tilde{\beta}$ is generally different than the infection rate $\beta$ introduced above. Indeed we can approximate $\beta = \tilde{\beta} \langle k \rangle_t$ where $\langle k \rangle_t$ is the average contact rate per unit time. Hence:

$$\zeta_{i,t}(I) = \prod_{j \in \text{Neigh}(i)} [(1 - P_{I_d,i,t}) + P_{I_d,i,t} \cdot (1 - \tilde{\beta})] = \prod_{j \in 1..N} (1 - \tilde{\beta} A_{ij} P_{I_d,i,t})$$ (6)

Next, we develop the equations for probabilities $P$ of node $i$ to be in each of the possible states ($S, I, I_D, R$) at time step $t + 1$.

For generality and clarity, we denote by $\alpha_{XY}$ the probability of a node to transition from state $X$ to $Y$, while $\alpha_{XX}$ is the probability of a node to remain in state $X$. With this notation, the probability equations for each state are as follows:

**State S**: A node $i$ is in state $S$ at time $t + 1$ if it was in state $S$ at time $t$ and it did not get infected:

$$P_{S,i,t+1} = P_{S,i,t} \cdot \zeta_{i,t}(I)$$ (7)

**State I**: A node $i$ is in state $I$ at time $t + 1$ if either: 1) it was in state $S$ at time $t$ and was successfully infected, or 2) it was in state $I$ at time $t$ and it remained there (i.e., it did not transition to states $R$ or $I_D$), or 3) it was in state $I_D$ at time $t$ and transitioned to state $I$.

$$P_{I,i,t+1} = P_{S,i,t} \cdot (1 - \zeta_{i,t}(I)) + P_{I,i,t} \cdot \alpha_{II} + P_{I_D,i,t} \cdot \alpha_{I_D I}$$ (8)
State ID: A node \( i \) is in state ID at time \( t + 1 \) if either: 1) it was in state I at time \( t \) and transitioned to state ID, or 2) it was in state ID at time \( t \) and it remained there.

\[
P_{ID,i,t+1} = P_{I,I} \cdot \alpha_{ID} + P_{ID,I} \cdot \alpha_{ID}
\]

State R: We can compute \( P_{R,i,t} \) using the relation:

\[
\forall i, t : P_{S,i,t} + P_{I,i,t} + P_{ID,i,t} + P_{R,i,t} = 1
\]

Now we can write down the system of equations for SIIDR using Eqs. 7–10 to define \( P_t \), the probability vector that completely describes the evolution of the system at any time step \( t \):

\[
\begin{align*}
P_{S,i,t+1} &= P_{S,i,t} \cdot \xi_{I,I}(I) \\
P_{I,I,t+1} &= P_{S,I,I} \cdot (1 - \xi_{I,I}(I)) + P_{I,I} \cdot \alpha_{II} + P_{ID,I} \cdot \alpha_{ID} \\
P_{ID,I,t+1} &= P_{I,I} \cdot \alpha_{ID} + P_{ID,I} \cdot \alpha_{ID} \\
P_{R,I,t+1} &= 1 - P_{S,I,I} - P_{ID,I} \cdot (\alpha_{ID} + \alpha_{II}) - P_{I,I} \cdot (\alpha_{II} + \alpha_{ID})
\end{align*}
\]

Stability analysis
The next step in our analysis of the SIIDR propagation on complex networks represented as arbitrary graphs is to define the disease-free equilibrium points and analyze their stability.

Definition 5 An equilibrium point of NLDS is the probability vector \( P^* \) that satisfies \( P_{t+1} = P_t = P^* \) for any \( t \) (Verhulst 2006). Thus, for the SIIDR model we can define the disease-free equilibrium point as follows:

\[
P^* = [P_S, 0, 0, P_R]^T, \text{ where } P_R + P_S = 1
\]

One way to analyze the stability of the equilibrium point of a non-linear dynamical system is to approximate its dynamics at that point as a linear dynamical system (i.e., linearization) (Sayama 2015). In this case, the system behavior in an infinitesimally small area about the equilibrium point is approximated with a Jacobian matrix.

The largest eigenvalue \( \lambda_j \) of the Jacobian matrix indicates whether the equilibrium point of the system is stable or not. Since we are considering the time as discrete, if \( |\lambda_j| < 1 \), the equilibrium point is asymptotically stable; even if small perturbations occur, the system asymptotically goes back to the equilibrium point. If \( |\lambda_j| > 1 \), the system is unstable and diverges away from the equilibrium point. If \( |\lambda_j| = 1 \), then the system may either diverge from, or converge to the equilibrium point (Bof et al. 2018; Dahleh et al. 2004; Haddad and Chellaboina 2011; Sayama 2015).

The Jacobian matrix of SIIDR modeled as NDLS and an analysis of its eigenvalues is presented in Appendix 3. We show that one of the eigenvalues of the Jacobian has value 1. This result is particularly significant. Asymptotic stability requires all the eigenvalues of the Jacobian matrix to be less than 1 in absolute values. Since the Jacobian matrix has at least one eigenvalue of value 1, the equilibrium point of the NLDS system cannot be asymptotically stable. However, the equilibrium point can still be Lyapunov stable.
We show that the equilibrium points of SIIDR are indeed Lyapunov stable using Lyapunov’s second stability criterion.

**Definition 6** The equilibrium point \( P^* \) of \( P_{t+1} = g(P_t) \) NLDS is **Lyapunov stable** if there exists a continuous function \( L \), such that for any \( t \):

\[
L(P) > 0, L(P^*) = 0
\]

\[
L(P_{t+1}) - L(P_t) \leq 0
\]

**Theorem 2** The equilibrium points of SIIDR represented as NLDS of the form (11) are Lyapunov stable if:

\[
\lambda_A \beta \mu \leq 1
\]

where \( \lambda_A \) is the largest eigenvalue of the adjacency matrix, \( \beta \) and \( \mu \) are probabilities of infection and recovery respectively.

The proof of Theorem 3 is presented in Appendix 4.

**Experimental results**

In this section, we present the reconstruction of WannaCry dynamics from network logs captured with Zeek monitoring tool (The Zeek Project 2023). Additionally, we show supporting results that confirm that the SIIDR model fits WannaCry traces best. We also present our experiments for parameter estimation, providing the statistics from the posterior distribution of SIIDR transition rates. These results expand the results presented in our previous work where we introduced SIIDR model (Chernikova et al. 2022). Moreover, we study the basic reproduction number \( R_0 \) of the reconstructed attacks to understand its correlation with SPM dynamics (in particular, its propagation speed). We also discuss the issue of structural and practical identifiability of SIIDR parameters which is common in epidemiological modeling. Finally, we experimentally demonstrate that the condition for Lyapunov stability of the disease-free equilibrium point holds when the networks are modeled as arbitrary graphs relaxing homogeneous mixing assumption.

**WannaCry malware traces**

We obtained realistic WannaCry attack traces by running the malware in a controlled virtual environment consisting of 51 virtual machines, configured with a version of Windows vulnerable to the EternalBlue SMB exploit. The external traffic generated by the VMs was blocked to isolate the environment and prevent external malware spread. The infection started from an initial victim IP, and then the attack propagated through the network as the infected IPs began to scan other IPs. In these experiments, WannaCry varied the number of threads used for scanning, which were set to 1, 4 or 8, and the time interval between scans, which was set to 500ms, 1 s, 5 s, 10 s or 20 s. Using the
combination of these two parameters resulted in 15 WannaCry traces. While running WannaCry with this setup, the log traces were collected with the help of the open source Zeek network monitoring tool.

WannaCry reconstruction

To reconstruct the WannaCry dynamics we are using Zeek communication logs where we consider only communication between internal IPs. Since WannaCry attempts to exploit the SMB vulnerability, we label as malicious all the attempts of connections on destination port 445. The first attempt to establish the malicious connection is considered to be the start of the epidemics, and the end corresponds to the last communication event in the network. Each IP trying to establish a malicious connection for the first time at time $t$ is considered infected at time $t$. The cumulative number of infected IPs through time represents the curve of the WannaCry epidemics.

WannaCry dynamics

We show the dynamics of WannaCry variants characterized by different numbers of scanning threads and time between scans in Fig. 4. These dynamics represent the cumulative number of infected nodes during the epidemic time. The trace which corresponds to 1 thread and 20s sleeping time wc_1_20s has unusual behavior in the dynamics. It has a very small number of infected nodes until the end of the attack, when the infections rapidly increase to the 7 infected nodes at once. For all other WannaCry variants we observe that the attack reaches the maximum number of infected nodes quickly and is not able to infect any other nodes for a large time window before the end of the epidemic. These graphs confirm the fact that after an IP enters a recovered state it no longer has an opportunity to get back to susceptible or infected nodes. For modeling and parameter estimation experiments we exclude the time windows after which the number

![Graph showing WannaCry dynamics](image-url)
of infections does not change. Additionally, we present the number of contacted and infected IPs in Table 3. Interestingly, the overall percentage of infected nodes is small (around 25% on average) for all variants. The possible reason for this is the fact that some of the machines that do not get infected may have immunity to the malware.

### Model selection

We select the model that fits WannaCry traces best among several representative compartmental epidemiological models: SI, SIS, SIR, SEIR and SIIDR assuming an homogeneous mixing of machines. These models have different number of parameters and, therefore, different a-priori explaining power. The SIIDR model is also the one that has the largest number of parameters. To allow for a fair comparison among models, we considered the Akaike Information Criterion (AIC) as a metric to measure their performance. The AIC is calculated based on the maximum likelihood estimate and the number of free model parameters, thus, allowing comparison of models with different number of parameters. More information about AIC criteria can be found in “Model selection” section in Appendix 5. We perform model selection for all WannaCry traces. The lowest AIC score corresponds to the best model. We run the experiments on an uniform grid of model parameter values between 0 and 1. We select the lowest AIC score for each WannaCry trace and each compartmental model. The results are illustrated in Table 4. In bold, we highlight the minimum AIC value across all models for each WannaCry trace. The SIIDR model has the lowest AIC score for all traces except for wc_1_20s. For instance, the AIC score associated with the SEIR model for wc_8_5s WannaCry trace is equal to -87, the SIS model score is 104, the SIR model score is -35, whereas for the SIIDR model the AIC is the lowest and has the value of -121. This trend is valid for all other WannaCry traces except for wc_1_20s where the SEIR model provides the best

| WannaCry variant | # Contacted IPs | # Infected IPs | Fraction of infected IPs |
|------------------|----------------|---------------|--------------------------|
| wc_1_500 s       | 37             | 8             | 0.22                     |
| wc_1_1 s         | 37             | 8             | 0.22                     |
| wc_1_5 s         | 37             | 8             | 0.22                     |
| wc_1_10 s        | 34             | 10            | 0.29                     |
| wc_1_20 s        | 35             | 7             | 0.20                     |
| wc_4_500 ms      | 34             | 5             | 0.15                     |
| wc_4_1 s         | 35             | 8             | 0.23                     |
| wc_4_5 s         | 36             | 9             | 0.25                     |
| wc_4_10 s        | 35             | 7             | 0.20                     |
| wc_4_20 s        | 35             | 5             | 0.14                     |
| wc_8_500 ms      | 35             | 7             | 0.20                     |
| wc_8_1 s         | 35             | 7             | 0.20                     |
| wc_8_5 s         | 35             | 5             | 0.14                     |
| wc_8_10 s        | 36             | 6             | 0.17                     |
| wc_8_20 s        | 35             | 9             | 0.26                     |
However, this variant is an outlier. Therefore, we can conclude that, among the four epidemiological models, the SIIDR model fits the WannaCry attack traces best.

For each compartmental model and each WannaCry trace, we plot the reconstruction curve of the number of infected nodes using the parameters corresponding to the lowest AIC score along with the true dynamics of infected nodes. The results are shown in Fig. 5. In the case of the SIS model, the orange line (representing the simulated dynamics of the number of infected nodes) is far from the blue one, which illustrates the empirical dynamic for all malware traces. In the case of the SIR and SEIR models the numbers of simulated infections are closer to the real ones, however, the SIIDR and actual dynamics curves are the closest.

Parameter estimation

We approximated the posterior distribution of SIIDR transition rates using the ABC-SMC-MNN technique (Filippi et al. 2013). The details of this technique are described in “Posterior distribution of transition rates” in Appendix 5. The mean values and standard deviation of the posterior distribution of SIIDR transition rates ($\beta$, $\mu$, $\gamma_1$, $\gamma_2$) are represented in Table 5. The parameter $dt$ is the integration step, which is calculated as: $dt = (t_N - t_0)/T$, where $t_N$ is the last timestamp, $t_0$ is the first timestamp, and $T$ is
the number of timestamps in WannaCry traces. \( dt \) differs by variant due to the different propagation speeds. The attack transmission probability \( \tilde{\beta} \) is related to attack transmission rate \( \beta \) as follows: \( \beta = \tilde{\beta}(k) \), where \( (k) \) is the average contact rate per unit time. In the WannaCry traces we have one communication or contact per \( dt \), hence, the transmission probability \( \tilde{\beta} \) over a contact-link also equals \( \beta \).

Based on estimated values of transition rates we calculated the basic reproduction number \( R_0 \) for all WannaCry traces. We also calculate the SPM propagation speed for all WannaCry traces as the average number of new infections per 100 s. The results are illustrated in Fig. 6. As expected, we observe that higher SPM propagation speed corresponds to a higher basic reproduction number \( R_0 \).

**Table 5** Statistics from posterior distribution of SIIDR parameters estimated with the ABC-SMC-MNN method

| WannaCry variant | \( \beta \) (mean, std) | \( \mu \) (mean, std) | \( \gamma_1 \) (mean, std) | \( \gamma_2 \) (mean, std) | \( dt \) |
|------------------|-------------------------|-----------------------|--------------------------|--------------------------|--------|
| wc_1_500 ms      | (0.16, 0.10)            | (0.11, 0.11)          | (0.79, 0.15)             | (0.06, 0.07)             | 0.09   |
| wc_1_1 s         | (0.16, 0.11)            | (0.11, 0.10)          | (0.80, 0.15)             | (0.06, 0.06)             | 0.06   |
| wc_1_5 s         | (0.05, 0.03)            | (0.04, 0.03)          | (0.82, 0.12)             | (0.02, 0.01)             | 0.16   |
| wc_1_10 s        | (0.13, 0.08)            | (0.08, 0.07)          | (0.80, 0.15)             | (0.05, 0.04)             | 0.09   |
| wc_1_20 s        | (0.22, 0.20)            | (0.63, 0.24)          | (0.46, 0.28)             | (0.51, 0.29)             | 0.99   |
| wc_4_500 ms      | (0.45, 0.26)            | (0.66, 0.24)          | (0.53, 0.28)             | (0.47, 0.29)             | 0.05   |
| wc_4_1 s         | (0.17, 0.13)            | (0.11, 0.13)          | (0.79, 0.17)             | (0.07, 0.07)             | 0.05   |
| wc_4_5 s         | (0.14, 0.10)            | (0.09, 0.08)          | (0.76, 0.18)             | (0.07, 0.07)             | 0.07   |
| wc_4_10 s        | (0.20, 0.17)            | (0.23, 0.20)          | (0.74, 0.20)             | (0.07, 0.08)             | 0.10   |
| wc_4_20 s        | (0.43, 0.26)            | (0.65, 0.24)          | (0.50, 0.29)             | (0.51, 0.29)             | 0.14   |
| wc_8_500 ms      | (0.17, 0.14)            | (0.16, 0.16)          | (0.79, 0.15)             | (0.07, 0.08)             | 0.03   |
| wc_8_1 s         | (0.17, 0.14)            | (0.16, 0.16)          | (0.76, 0.17)             | (0.09, 0.09)             | 0.03   |
| wc_8_5 s         | (0.45, 0.27)            | (0.63, 0.24)          | (0.47, 0.28)             | (0.48, 0.29)             | 0.07   |
| wc_8_10 s        | (0.47, 0.26)            | (0.63, 0.24)          | (0.49, 0.29)             | (0.46, 0.29)             | 0.06   |
| wc_8_20 s        | (0.14, 0.10)            | (0.09, 0.09)          | (0.80, 0.15)             | (0.07, 0.06)             | 0.07   |

**Fig. 6** The basic reproduction number \( R_0 \) calculated by using estimated values of transition rates compared to the speed of SPM propagation. Higher propagation speed corresponds to higher \( R_0 \). We exclude the results for the wc_1* traces.
The mean values of the parameters’ posterior distribution can be further used to simulate SPM with the SIIDR model. This provides an opportunity to create synthetic, but realistic, WannaCry scenarios and evaluate whether existing defenses are successful in preventing and stopping the malware from propagation in the networks. However, we notice that some of the WannaCry attack variants affect only a small number of nodes. For example, the wc_8_5s trace has only 4 infected nodes at the end of the trace which constitutes 14% of all nodes. Consequently, ABC-SMC-MNN is expected to perform worse in the estimation of transition rates for such traces. Thus, parameters estimated from the traces with higher numbers of infections are more reliable.

Identifiability of SIIDR transition rates
As long as the goals of modeling with SIIDR include inferences about the underlying propagation process, we are interested in the estimation of SIIDR parameter distribution corresponding to model outputs that best fit the observed data. However, parameters’ estimation can only produce robust results if the model is identifiable meaning that it is possible to obtain a unique solution for all unknown parameters given the model structure and output. On the other hand, if parameters are not identifiable their similar values may yield considerably different model outputs (Chis et al. 2011; Tuncer and Le 2018).

The common problem of data uncertainty forces the issue of parameter identifiability to appear relevant in epidemiological modeling (Chowell 2017; Gallo et al. 2022; Weitz and Dushoff 2015; Valdez et al. 2015). The lack of identifiability in the model parameters may prevent reliable predictions of the epidemic dynamics. Therefore, it becomes crucial to investigate the parameter identifiability, and its limitations and propose solutions to improve it.

There exist notions of structural and practical identifiability. Structural identifiability is a property of the model structure itself given that the model is error-free and the observed data has no noise. Practical identifiability is connected to the quality of data leveraged for parameter estimation. It measures whether there is enough information to infer the transition rates (Dankwa et al. 2022).

We addressed the structural SIIDR parameters identifiability using the method of differential algebra (Chis et al. 2011; Miao et al. 2011) with the help of DAISY (Bellu et al. 2007) and SIAN (Hong et al. 2020; Ilmer et al. 2021) software and achieved the following result:

**Theorem 3** All parameters of the SIIDR model are globally structurally identifiable when incidence represents the output of the model and the size of population $N$ is known. Otherwise, parameters $N$ and $\beta$ appear to be structurally non-identifiable while $\mu$, $\gamma_1$ and $\gamma_2$ remain identifiable.

Therefore, we consider the SIIDR model to be structurally identifiable as long as the size of the computer networks is usually known. More information about SIIDR structural identifiability along with the results from DAISY software can be found in Appendix 2.

However, even when the model parameters are structurally identifiable, they may still be non-identifiable in practice due to the limited number of observed variables,
the quality of data used for estimation, and the complexity of the model (the number of parameters that are jointly estimated).

To investigate practical identifiability we looked at the joint posterior distribution of SIIDR parameters. The plots can be found in “Joint posterior distributions of SIIDR parameters” in Appendix 2. For some of the WC variants, there exists a correlation between parameters $\beta$ and $\mu$. Additionally, some of the joint posterior distributions possess multimodality. Although on average the issue of non-identifiability is not dominant, it might appear in some parts of the phase space of the SIIDR model. One reason for this behavior is that the incidence represents the output of the fitted model and appears to be insufficient to characterize the whole model’s dynamic. On the other hand, SIIDR has four parameters estimated jointly, therefore, it may contain multiple sets of parameters that lead to the same output of the model. Hence, measuring the data about other states rather than just the number of infected nodes as a function of time to characterize the system dynamics more extensively, should improve the practical SIIDR identifiability.

Threshold evaluation
In this section, we evaluate the conditions of SIIDR model equilibrium points to satisfy the Lyapunov stability. Specifically, we are interested in the equilibrium point which corresponds to the start of epidemics, when all nodes in the network have the following probability vector to appear in all of the states of SIIDR model $P^* = \{1, 0, 0, 0\}$. We study the stability of this point after the infection of the initial node by SPM (i.e., the system initial state $P_0$ lies in the ball of radius $\delta$ around $P^*$) by looking at the density of recovered nodes w.r.t to the stability threshold $s$ and associated infection propagation dynamics $P_t$.

We evaluate stability conditions on the variety of synthetic and real-world networks described in the following subsection.

**Graphs characteristics**
We consider synthetic networks generated with Barabási-Albert (BA) (Barabási and Albert 1999), Erdős-Rényi (ER) (Erdős and Rényi 1959), Watts-Strogatz (WS) (Watts and Strogatz 1998), Configuration Model (CM) (Newman 2003), and Scale-free (SF) (Barabási 2009) models along with three real-world graphs (Leskovec et al. 2005; Leskovec and Mcauley 2012; Leskovec et al. 2007). Real-world graphs include networks generated using Facebook data (Facebook), autonomous systems peering information inferred from Oregon route views (Oregon), and anonymized traffic data about incoming and outgoing emails between members of the European research institution (Email). All synthetic graphs have 1000 nodes and different topological characteristics. Thus, ER graphs have different leading eigenvalues that range from 11 to 999, BA networks have the leading eigenvalue between 35 and 508, and WS graphs - between 10 and 900. ER, BA, and WS networks have only one connected component. They have a larger diameter and average path length, and smaller density and transitivity in the graphs with smaller leading eigenvalues. CM and SF networks have more connected components and the values of other topological characteristics are similar to ER, BA, and WS graphs with small leading eigenvalues.

More details about the topological characteristics of considered networks are presented in Table 6.
Phase transition

To illustrate the results of Theorem 2 we plot the final number of recovered nodes in the network with respect to the threshold values \( s = \lambda_A \beta / \mu \) in the range from 0 to 2. We achieve these results by fixing the transition rates \( \mu = 0.5, \gamma_1 = 0.5, \gamma_2 = 0.5 \) and changing the value of \( \beta \). For ER, BA and WS graphs infection propagation starts from one
Initially infected node, for SF, CM and real-world networks the fraction of infected nodes at \( t = 1 \) is 0.05. We average results over 100 stochastic realizations that we run considering 50 different seeds. Resulting phase transition plots are illustrated in Figs. 7, 8, 9, and 10.

For all types of graphs, the total fraction of recovered nodes is negligible for values of \( s < 1 \). As predicted by the theory, the epidemic threshold is \( s \sim 1 \). In the case of SF, CM, and real networks (see Fig. 10), the threshold appears to be for \( s < 1 \). However, we note how in order to obtain macroscopic outbreaks in these graphs, we started the simulations with 5\% of initially infected seeds, instead of a single one as done for the other networks. Hence, also for these networks, the phase transition takes place for \( s \sim 1 \).
In general, networks with larger diameters and average path lengths, smaller density, and transitivity have a smaller fraction of recovered nodes during the infection propagation.

These results demonstrate that for all \( t \) the solution \( P_t \) stays in some ball of radius \( \epsilon \) from the starting equilibrium point \( P^* = P_0 \) when \( s < 1 \), therefore, it is Lyapunov stable. Moreover, we see that SIIDR behaves the same as the SIR model in terms of the stability of equilibrium points: when the threshold \( s \) is less than one the SIIDR system solution converges to DFE when \( t \) tends to infinity. It can be explained by the fact that SIIDR model is very similar to a SIR model except for the particular configuration of transition rates.

**Conclusions**

We performed a comprehensive analysis of a new compartmental model, SIIDR, that captures the behavior of self-propagating malware. We showed that SIIDR fits real-world WannaCry traces much better than existing compartmental models such as SI, SIS, SIR, and SEIR (which were previously studied in the literature). Additionally, we estimated the posterior distribution of the model’s parameters for real attack traces and showed how they characterize the WannaCry behavior. We also analytically derived the conditions when SPM is expected to become an epidemic and discussed the stability of model’s disease-free equilibrium points. Our work demonstrates the impact of modeling the propagation of SPM, simulating real attacks on networks, and evaluating defensive techniques.

**Appendix 1 Compartmental models of epidemiology**

**SI model**

The SI model is used to describe diseases where infection is permanent. It features two compartments and one transition. The susceptible compartment \( S \) represents healthy
individuals that interacting with infectious individuals in the compartment $I$ can get infected ($S + I \rightarrow 2I$). It can be translated in the following system of ODEs:

\[
\begin{align*}
\frac{dS}{dt} &= -\beta \frac{S}{N}I \\
\frac{dI}{dt} &= \beta \frac{S}{N}I - \mu I
\end{align*}
\]

Due to the homogeneous mixing assumption, the per capita rate at which susceptible individuals get infected can be written as the probability of interacting with an infected individual ($I/N$) times the transmission rate of the disease $\beta$. The state diagram for the SI model is shown in Fig. 11.

**SIS model**

The SIS model features two compartments and two transitions. Beside the infection process as in the SI model, SIS models have also a recovery process: infected individuals spontaneously recover at rate $\mu$ becoming susceptible to the disease again ($I \rightarrow S$). Hence SIS models are used for diseases that can infect individuals multiple times. The system of ODEs associated with SIS model is:

\[
\begin{align*}
\frac{dS}{dt} &= -\beta \frac{S}{N}I + \mu I \\
\frac{dI}{dt} &= \beta \frac{S}{N}I - \mu I
\end{align*}
\]

Note how, differently from infection, the recovery process is spontaneous and does not require any interaction. Hence, each infected individual has an average duration of infection of $\mu^{-1}$. The state diagram for SIS model is shown in Fig. 12.
The SIR model describes diseases that give permanent (or long-lasting) immunity. It features three compartments and two transitions. Differently from SIS models, within the SIR framework infected individuals that are no longer infectious transition to the recovered compartment $R$. The system of differential equations corresponding to the SIR model is the following:

\[
\begin{align*}
\frac{dS}{dt} &= -\beta S \frac{I}{N} \\
\frac{dI}{dt} &= \beta S \frac{I}{N} - \mu I \\
\frac{dR}{dt} &= \mu I
\end{align*}
\]

The state diagram for the SIR model is represented in Fig. 13.

The SEIR model describes diseases where susceptible individuals $S$ remain exposed $E$ after interaction with infected $I$ individual before becoming infectious themselves. It features four compartments and three transitions. The system of differential equations corresponding to the SEIR model is the following:

\[
\begin{align*}
\frac{dS}{dt} &= -\beta S \frac{I}{N} \\
\frac{dE}{dt} &= \beta S \frac{I}{N} - \gamma E \\
\frac{dI}{dt} &= \gamma E - \mu I \\
\frac{dR}{dt} &= \mu I
\end{align*}
\]

The state diagram for the SEIR model is represented in Fig. 14.
Appendix 2 Identifiability of SIIDR transition rates

SIIDR model can be represented as follows:

\[
\begin{align*}
\text{SIIDR} &:= \begin{cases} 
\dot{X}(t) = f(X(t), \theta) \\
Y(t) = g(X(t), \theta) \\
X_0 = X(t_0)
\end{cases}
\end{align*}
\] 

where \( t_0 \leq t \leq T \), \( \dot{X}(t) \) is a system of ODEs, \( X(t) \) is a vector of time-varying diseases states and the unique solution to the system \( \dot{X}(t), \theta \in \Theta \) is a vector of constant unknown model parameters, \( Y(t) \) is a vector of time-dependent model outputs, \( g \) is the measurement equation which defines the relationship between \( X(t), \theta \) and \( Y \), and \( X_0 \) is a vector of the known initial conditions.

**Definition 7**  A parameter \( \theta \) is structurally globally identifiable if \( \forall \theta^* \in \Theta \):

\[
\text{SIIDR}(\theta^*) = \text{SIIDR}(\theta) \Rightarrow \theta^* = \theta
\]

**Definition 8**  A parameter \( \theta \) is structurally locally identifiable if \( \forall \theta^* \in \Theta \), there exists a neighbourhood \( \Omega(\theta) \) such that

\[
\theta^* \in \Omega(\theta) \Rightarrow \text{SIIDR}(\theta^*) = \text{SIIDR}(\theta) \Rightarrow \theta^* = \theta
\]

A variety of methods exists to evaluate the structural and practical identifiability of parameters. In our work, we leveraged the method of differential algebra implemented in DAISY (Bellu et al. 2007) and SIAN (Hong et al. 2020; Ilmer et al. 2021) software to address the structural identifiability of SIIDR. We looked at the joint posterior distribution of SIIDR parameters to address the issue of practical identifiability. We discuss SIIDR identifiability results in the following subsections.

**Differential algebra approach for structural identifiability**

In this section, we show the results for structural identifiability of SIIDR parameters achieved with the differential algebra approach implemented in DAISY software. Figures 15, 16 represent the input and output of the DAISY software when the number of infected nodes is the output variable \( Y(t) \). Figures 17, 18 show the results from DAISY software in the situation when the sum of infected, infected dormant, and recovered nodes is the output variable. When the size of the population \( N \) is known, we can exclude it from the ODE equations and consider \( \beta = \beta/N \) to be the unknown parameter. In both cases all parameters of the SIIDR model are globally structurally identifiable. Figures 19, 20 show the results when the \( N \) is the unknown parameter. In this situation, parameters \( \beta \) and \( N \) are not identifiable, however, \( \mu, \gamma_1, \gamma_2 \) remain identifiable.
Joint posterior distributions of SIIDR parameters

In this subsection, we illustrate the joint posterior distribution for SIIDR parameters. The plots for wc_4_500ms variant are in Figs. 21, 22. In this case, joint posterior distribution has multiple modes which means that the parameters value are not uniquely identifiable. The results for wc_8_20s are illustrated in Figs. 23, 24. In this situation, $\beta$ and $\mu$ parameters are correlated. In Figs. 25, 26 we show the results for wc_1_5s variant. The posterior joint distribution of $\beta$ and $\mu$ parameters are not correlated and there is no multimodality.
Fig. 17 Input for DAISY to evaluate the SIIDR structural identifiability of parameters when output is the sum of infected, infected dormant and recovered individuals.

MODEL ALGEBRAICALLY OBSERVABLES$
PARAMETER VALUES$
b2_ := \{\beta=2, \mu=3, \gamma_1=5, \gamma_2=7\}$

MODEL PARAMETER SOLUTION(S)$
g_ := \{\{\beta=2, \gamma_1=5, \gamma_2=7, \mu=3\}\}$$

MODEL GLOBALLY IDENTIFIABLES$

Fig. 18 SIIDR structural identifiability of parameters achieved with DAISY when output is the sum of infected, infected dormant and recovered individuals.

MODEL NOT ALGEBRAICALLY OBSERVABLES$
PARAMETER VALUES$
b2_ := \{\beta=2, \mu=3, \gamma_1=5, \gamma_2=7, n=11\}$

MODEL PARAMETER SOLUTION(S)$
g_ := \{\{\gamma_1=5, \mu=3, n=(11+\beta)/2, \gamma_2=7\}\}$

MODEL NON IDENTIFIABLES$

Fig. 19 SIIDR structural identifiability of parameters achieved with DAISY when output is the sum of infected, infected dormant and recovered individuals and the size of population $N$ is unknown.
MODEL ALGEBRAICALLY OBSERVABLES

PARAMETER VALUES

\[ b_2 := \{\text{beta}=2, \text{mu}=3, \text{gamma1}=5, \text{gamma2}=7, n=11\} \]

MODEL PARAMETER SOLUTIONS

\[ g_\gamma := \{\text{beta}=(2*n)/11, \text{gamma1}=5, \text{gamma2}=7, \text{mu}=3\} \]

MODEL NON IDENTIFIABLES

Fig. 20 SIIDR structural identifiability of parameters achieved with DAISY when output is the sum of infected, infected dormant and recovered individuals and the size of population \( N \) is unknown.

Fig. 21 Joint posterior distribution for SIIDR parameters for wc_4_500ms variant.

(a) \( \beta \) and \( \gamma_1 \)  
(b) \( \beta \) and \( \gamma_2 \)  
(c) \( \beta \) and \( \mu \)

Fig. 22 Joint posterior distribution for SIIDR parameters for wc_4_500ms variant.

(a) \( \gamma_1 \) and \( \gamma_2 \)  
(b) \( \mu \) and \( \gamma_1 \)  
(c) \( \mu \) and \( \gamma_2 \)

Fig. 23 Joint posterior distribution for SIIDR parameters for wc_8_20s variant.

(a) \( \beta \) and \( \gamma_1 \)  
(b) \( \beta \) and \( \gamma_2 \)  
(c) \( \beta \) and \( \mu \)
Appendix 3 Linearization of SIIDR as NLDS

The Jacobian matrix $\mathcal{J}$ at the equilibrium point $P^*$ is defined as:

$$\mathcal{J} = \nabla g(P^*),$$

where $\mathcal{J}_{i,j} = \left[\nabla g(P^*)\right]_{i,j} = \frac{\partial g_i}{\partial p_j} \big|_{p=P^*}$.

We calculate the partial first order derivatives of our equation system and obtain the Jacobian matrix:

Fig. 24 Joint posterior distribution for SIIDR parameters for wc_8_20s variant

Fig. 25 Joint posterior distribution for SIIDR parameters for wc_1_5s variant

Fig. 26 Joint posterior distribution for SIIDR parameters for wc_1_5s variant

\begin{align*}
\text{(a) } & \gamma_1 \text{ and } \gamma_2 \\
\text{(b) } & \mu \text{ and } \gamma_1 \\
\text{(c) } & \mu \text{ and } \gamma_2 \\
\text{(a) } & \beta \text{ and } \gamma_1 \\
\text{(b) } & \beta \text{ and } \gamma_2 \\
\text{(c) } & \beta \text{ and } \mu \\
\text{(a) } & \gamma_1 \text{ and } \gamma_2 \\
\text{(b) } & \mu \text{ and } \gamma_1 \\
\text{(c) } & \mu \text{ and } \gamma_2
\end{align*}
The size of the Jacobian matrix is $4N \times 4N$, where $N$ is the number of nodes in the graph. Every row has 4 elements of size $N \times N$. We use the following notation: $I$ is the identity matrix of size $N \times N$ and $O$ is a matrix of size $N \times N$ with all zeros. $A$ is the adjacency matrix of the network represented as a graph, of size $N \times N$.

The first row is a linear combination of the other rows, thus:

$$J = \begin{bmatrix}
O & -I & -\left(\alpha_{I_pI_d} + \alpha_{I_dI_p}\right)I & -\left(\alpha_{IIi} + \alpha_{II_i}\right)I \\
O & I & O & -xS\tilde{\beta}\tilde{A} \\
O & O & \alpha_{I_pI_d}I & \alpha_{II_i}I \\
O & O & \alpha_{I_dI_p}I & xS\tilde{\beta}\tilde{A} + \alpha_{II_i}I
\end{bmatrix}$$

(17)

Let us represent the Jacobian matrix as follows:

$$J = \begin{bmatrix} Q_1 & Q_2 \\
O & Q_3 \end{bmatrix}$$

(19)

where $Q_1$, $Q_2$, $Q_3$, $O$ are matrices of size $N \times N, 2N \times N, 2N \times 2N, 2N \times N$ respectively:

$$Q_1 = I, \quad Q_2 = \begin{bmatrix} O & -xS\tilde{\beta}\tilde{A} \end{bmatrix}, \quad Q_3 = \begin{bmatrix} \alpha_{I_pI_d}I & \alpha_{II_i}I \\
\alpha_{I_dI_p}I & xS\tilde{\beta}\tilde{A} \end{bmatrix}$$

(20)

Let $\tilde{v}$ of size $3N \times 1$ and $\lambda_i$ be the eigenvector and the eigenvalue of $J$ respectively. Then we can define $\tilde{v}$ to be composed of $\tilde{v}_1$ of size $N \times 1$ and $\tilde{v}_2$ of size $2N \times 1$:

$$\tilde{v} = \begin{bmatrix} \tilde{v}_1 \\
\tilde{v}_2 \end{bmatrix}$$

(21)

$\tilde{v}$ and $\lambda_i$ satisfy the following equation:

$$J\tilde{v} = \lambda_i\tilde{v}$$

(22)

which results in:

$$\begin{bmatrix} Q_1 & Q_2 \\
O & Q_3 \end{bmatrix} \begin{bmatrix} \tilde{v}_1 \\
\tilde{v}_2 \end{bmatrix} = \lambda_i \begin{bmatrix} \tilde{v}_1 \\
\tilde{v}_2 \end{bmatrix}$$

(23)

Eq. 23 implies that:

$$Q_1 \cdot \tilde{v}_1 + Q_2 \cdot \tilde{v}_2 = \lambda_i \cdot \tilde{v}_1$$

(24)

$$Q_3 \cdot \tilde{v}_2 = \lambda_i \cdot \tilde{v}_2$$

(25)

From Eq. 25 we have:

1. $\tilde{v}_2 = \tilde{0}$, or
2. $\tilde{v}_2$ is the eigenvector of $Q_3$ and $\lambda_i$ is the eigenvalue of $Q_3$. 
We look at the first case into more detail: if $v_2 = 0$, from Eq. 24, we obtain that $Q_1 \cdot \tilde{v}_1 = \lambda_j \cdot \tilde{v}_1$. That means either: (a) $\tilde{v}_1 = 0$, which is not feasible, because in this case $\tilde{v} = \tilde{0}$, or (b) $\lambda_j$ is the eigenvalue of $Q_1$.

Thus, the eigenvalues of the Jacobian matrix can be represented as eigenvalues of matrix $Q_1$ (when $v_2 = 0$) and eigenvalues of matrix $Q_3$. Given the structure of $Q_1$ (i.e., identity matrix of size $N \times N$), the eigenvalues of $Q_1$ are equal to $I$. Thus, we can conclude that the Jacobian matrix has at least one eigenvalue equal to 1.

**Appendix 4 SIIDR stability as the system of NLDS**

**Theorem 4** The equilibrium points of SIIDR represented as NLDS of the form (11) are Lyapunov stable if:

$$\lambda_A \frac{\tilde{\beta}}{\mu} \leq 1$$  \hspace{1cm} (26)

where $\lambda_A$ is the largest eigenvalue of the adjacency matrix, $\tilde{\beta}$ and $\mu$ are probabilities of infection and recovery respectively.

**Proof** System (11) can be reduced to the first three equations because of linear dependency of $P_{R, i, t+1}$ on other equations, and has the following representation in the matrix form:

$$g(P_{t+1}) = CP_t + P_i^TBP_t$$

where matrices $C$ and $P_i^TBP_t$ of size $3N \times 3N$ correspond to the linear and non-linear part of the system, respectively. $P^T = \{P_1^T, P_2^T, P_3^T\}$ is a $3N \times 9N$ matrix, where $P_i^T$ is a $3N \times 3N$ matrix with non-zero $i_{th}$ row $P_S, P_t, P_D$:

$$P_i^T = \begin{bmatrix} 0 & 0 & 0 \\
                        P_S & P_t & P_D \\
                        0 & 0 & 0 \end{bmatrix}$$

$B = \{B_i\}_{i=1}^3$ is a $9N \times 3N$ matrix where $B_i = \{b_{kl}\}_{k,l=1}^3$ has the size of $3N \times 3N$. Based on our system representation (11) matrix $C$ is the following:

$$C = \begin{bmatrix} I & 0 & 0 \\
                        0 & \alpha_{H} & \alpha_{I} \\
                        0 & \alpha_{D} & \alpha_{P} \end{bmatrix}$$

and matrix $B$ is:
where $\mathbf{A}$ is the adjacency matrix of the corresponding graph.

Let $L$ be the continuous function equal to $P^T K$, where $K$ is the $3N \times 1$ matrix:

$$
K = \begin{bmatrix}
0 \\
1 \\
1 
\end{bmatrix}
$$

Then

$$
L(P) = \begin{bmatrix}
P_S & P_I & P_{I_d}
\end{bmatrix}
\begin{bmatrix}
0 \\
1 \\
1 
\end{bmatrix} = \sum_{i=1}^{N} (P_I + P_{I_d})_i
$$

$L$ is positive definite because it is equal to the sum of probabilities of all nodes in the graph be infected or infected dormant. The finite difference (13) in this case is equal to:

$$
L(P_{t+1}) - L(P_t) = P_{t+1}^T K - P_t^T K = [CP_t + P_t^T BP_t]^T K - P_t K = P^T [C^T K + B^T P^T K - K]
$$

where:

$$
C^T K = \begin{bmatrix}
\mathbb{1} & 0 & 0 \\
0 & \alpha_{II} \mathbb{1} + \alpha_{II_d} \mathbb{I} & \alpha_{II_d} I \\
0 & \alpha_{I_d} I \mathbb{1} + \alpha_{I_d} I \mathbb{I} & \alpha_{I_d} I \mathbb{I}
\end{bmatrix}
\begin{bmatrix}
0 \\
\mathbb{1} \\
\mathbb{1}
\end{bmatrix}
$$

and

$$
\begin{bmatrix}
\mathbb{1} - \mu \mathbb{1} \\
\mathbb{1}
\end{bmatrix}
$$
Thus, which results in the condition:

\[
\begin{bmatrix}
\begin{array}{ccc}
\text{0} & \text{0} & \text{0} \\
-\hat{\beta}A & \text{0} & \text{0} \\
\text{0} & \text{0} & \text{0} \\
\text{0} & \hat{\beta}A & \text{0} \\
\text{0} & \text{0} & \text{0} \\
\text{0} & \text{0} & \text{0}
\end{array}
\end{bmatrix}
+ \begin{bmatrix}
\text{0} & \text{0} & \text{0} \\
\text{0} & \text{0} & \text{0} \\
\text{0} & \text{0} & \text{0} \\
\text{0} & \text{0} & \text{0} \\
\text{0} & \text{0} & \text{0} \\
\text{0} & \text{0} & \text{0}
\end{bmatrix}
\begin{bmatrix}
P_I \\
P_S \\
P_I \\
P_{ID} \\
P_I \\
P_I
\end{bmatrix}
\begin{bmatrix}
\text{0} \\
1
\end{bmatrix}
\]

\[
= \begin{bmatrix}
\text{0} \\
\text{0} \\
\text{0} \\
\text{0} \\
\text{0} \\
\text{0}
\end{bmatrix}
\]

Thus,

\[
C^T K + B^T P^T K = \begin{bmatrix}
\text{0} \\
-\mu I + \hat{\beta}P_S A
\end{bmatrix}
\]

which results in the condition:

\[
\begin{bmatrix}
P_S & P_I & P_{ID}
\end{bmatrix}
\begin{bmatrix}
\text{0} \\
-\mu I + \hat{\beta}P_S A
\end{bmatrix} \leq 0
\]

or

\[
P_I [\hat{\beta}P_S A - \mu I] \leq 0 \quad (27)
\]

where \(P_I\) is the \(1 \times N\) vector of node probabilities to be infected, \(P_S\) is the \(1 \times N\) vector of node probabilities to be susceptible, and \(A\) is the adjacency matrix of the corresponding graph. Expression (27) means that the sum of probabilities of nodes to recover should be greater than the sum of probabilities of nodes to become infected at each time step for the equilibrium points of the system (11) to be Lyapunov stable.

As long as the maximum value of probabilities in the vector \(P_S\) is 1, it is true that:

\[
\hat{\beta}P_S A \leq \hat{\beta} 1_A
\]

(28)

So if we prove that:

\[
P_I [\hat{\beta} 1_A - \mu I] \leq 0 \quad (29)
\]

the condition (27) will be satisfied.

This condition can also be formulated by incorporating the nodes’ degrees as follows:

\[
P_I [\hat{\beta} D - \mu I] \leq 0 \quad (30)
\]
where $\mathbf{D}$ is the $1 \times N$ vector where each element $d_i$ is equal to the degree of the node $i$ in the graph.

As long as the maximum value of probabilities in the vector $P_I$ is 1, it is true that:

$$P_I \tilde{\beta} \mathbf{D} \leq 1 \tilde{\beta} \mathbf{D}$$

(31)

So if we prove that:

$$\tilde{\beta} \mathbf{D} - \mu 1 \leq 0$$

(32)

the condition (27) will be satisfied. Condition 32 can be rewritten as follows:

$$\tilde{\beta} \frac{\sum_{i} d_i}{N \mu} \leq 1$$

(33)

or

$$\frac{\beta d_{ave}}{\mu} \leq 1$$

(34)

It is known that the largest eigenvalue $\lambda_A$ has the following lower bound in the case of an arbitrary graph:

$$d_{ave} \leq \lambda_A$$

(35)

where $d_{ave}$ is the average degree of the graph. Therefore it is true that

$$\frac{\beta d_{ave}}{\mu} \leq \frac{\beta \lambda_A}{\mu}$$

(36)

Hence if the following condition:

$$\frac{\beta \lambda_A}{\mu} \leq 1$$

(37)

is satisfied, then the DFE equilibrium point will be Lyapunov stable on an arbitrary graph. □

**Appendix 5 Model fitting and parameter estimation**

In this section, we present the methodology used to compare different epidemic models in reproducing real WannaCry attack traces. Our method leverages the Akaike Information Criterion (AIC) Akaike (1974) to select the model that best fits the spreading caused by WannaCry malware. We also discuss how we estimate the posterior distribution of the SIIDR transition rates using an Approximate Bayesian Computation approach based on Sequential Monte Carlo (ABC-SMC) Filippi et al. (2013), McKinley et al. (2018), Toni et al. (2009).
Model selection
We use the AIC as guiding criterion to compare SIIDR to other epidemiological models, namely SI, SIS, SIR. The AIC is calculated based on the number of free parameters $k$ and the maximum likelihood estimate of the model $L$ as follows:

$$AIC = 2k - 2 \ln L$$

(38)

The first term introduces a penalty that increases with the number of parameters and thus discourages overfitting. The second term rewards the goodness of fit that is assessed by the likelihood function. For the likelihood function, we use the least squares estimation. The best model is the one with the lowest AIC. In the case of the least squares estimation, the AIC can be expressed as:

$$AIC = 2k + n \ln \hat{\sigma}^2$$

where:

$$\hat{\sigma}^2 = \frac{\sum_{t=1}^{T} \hat{\epsilon}_t^2}{T}$$

(39)

and $\hat{\epsilon}_t$ are the estimated residuals:

$$\hat{\epsilon}_t = I_{t}^{\text{sim}} - I_{t}^{\text{real}}$$

with $I_{t}^{\text{sim}}$ being the cumulative number of infected nodes from model simulations, and $I_{t}^{\text{real}}$ the cumulative number of infected nodes from real-world observations, at time interval $t$.

We use stochastic simulations (Higham 2001) to obtain a numerical approximation of the propagation process described by the system of ODEs. Generally, statistical methods such as stochastic simulations are a good approximation for larger systems, while in the case of smaller systems stochastic fluctuations become more important. The transitions among compartments are implemented through chain binomial processes (Abbey 1952).

At step $t$ the number of entities in compartment $X$ transiting to compartment $Y$ is sampled from a binomial distribution $Pr^{\text{Bin}}(X(t), p_{X \rightarrow Y}(t))$, where $p_{X \rightarrow Y}(t)$ is the transition probability. If multiple transitions can happen from $X$ (e.g., $X \rightarrow Y$, $X \rightarrow Z$), a multinomial distribution is used (e.g., $Pr^{\text{Mult}}(X(t), p_{X \rightarrow Y}(t), p_{X \rightarrow Z}(t))$).

The model selection methodology is summarized in Algorithm 1. We start by creating a uniform grid of possible parameter values (lines 2-5). For each model and each set of parameter values $p = (\beta, \mu, \gamma_1, \gamma_2)$ we perform several stochastic experiments simulating the model dynamics (the run_stochastic_avg procedure). Each stochastic realization consists of a time series, where $S(t), I(t), I_D(t), R(t)$ represent the number of nodes in each state at time interval $t$ during the simulation. The cumulative infection $I_{t}^{\text{sim}}$ consists of the total number of nodes in states $I, I_D$, and $R$, and is also a time series across all time intervals $dt$. Next, we compute the AIC using equation (38) by comparing the simulated to the actual dynamic. We select the minimum AIC score for each model; the best model is the one with the minimum AIC score overall.
Algorithm 1: SPM model selection

1. procedure MODEL_SELECTION
2. \( \beta \leftarrow 20 \) equidistant values in \((0, 1)\)
3. \( \mu \leftarrow 20 \) equidistant values in \((0, 1)\)
4. \( \gamma_1 \leftarrow 10 \) equidistant values in \((0, 1)\)
5. \( \gamma_2 \leftarrow 10 \) equidistant values in \((0, 1)\)
6. for each model \( m \in \{SI, SIS, SIR, SIIDR\} \) do
7. \quad for each set \( p = (\beta, \mu, \gamma_1, \gamma_2) \) do
8. \quad \quad \( S_i, I_i, ID_i, R_i = \text{run\_stochastic\_avg}(p, h) \)
9. \quad \quad \( I_{sim} = I_i + ID_i + R_i \)
10. \quad \quad \( \text{aic} = \text{AIC}(I_{sim}, I_{real}) \)
11. \quad end for
12. \quad \text{aic}_{\text{min}}^{m} \leftarrow \text{min}_i \text{aic}
13. end for
14. \text{aic}_{\text{min}} \leftarrow \text{min}_m \text{aic}
15. \( M \leftarrow \) model that corresponds to \text{aic}_{\text{min}}
16. return \( M \)
17. end procedure

SIIDR Parameters associated with the best AIC score

In Table 7 we show the SIIDR parameters associated with the minimum AIC score for all WC variants.

Posterior distribution of transition rates

To find the best set of parameters for the SIIDR model we can approximate the posterior distribution of the parameters using Approximate Bayesian Computation (ABC) techniques (Minter and Retkute 2019). These techniques are based on the Bayes rule for determining the posterior distribution of parameters given the data:
where \( P(\theta) \) is the prior distribution of parameters that represents our belief about them and \( P(D|\theta) \) is the likelihood function, i.e., the probability density function of the data given the parameters. Marginal likelihood of the data \( P(D) \) does not depend on \( \theta \), and therefore the posterior distribution \( P(\theta|D) \) is proportional to the numerator in (40).

ABC methods are useful when the likelihood function is unknown or is not feasible to estimate analytically. The simplest version of ABC techniques is called rejection algorithm and is illustrated in Algorithm 2. Despite its simplicity, the rejection algorithm is generally slow at converging. Indeed, each iteration is independent from the previous ones and the prior distribution from which parameters are sampled is never updated. Furthermore, it is often difficult to decide, a priori, a reasonable threshold value \( \epsilon \) that guarantees both fast convergence and accurate results.

In alternative to the rejection algorithm, we use here a more advanced ABC technique that leverages Sequential Monte Carlo (ABC-SMC) (Toni et al. 2009; McKinley et al. 2018). The ABC-SMC approach iteratively constructs generations of prior distributions by decreasing the rejection threshold over time. At the first generation, a given number of parameter sets (i.e., particles) is accepted from the starting prior distribution, while each prior distribution used in following generations is obtained as a weighted sample from the previous generation \( \theta^* \) perturbed through a kernel \( K(\theta|\theta^*) \).

Common choices for the kernel are the uniform and multivariate normal distributions. A kernel with a large variance will prevent the algorithm from being stuck in the local modes, but will result in a huge number of particles being rejected, which is inefficient. Therefore, we use the multivariate normal distribution, where the covariance matrix is calculated considering \( M \) nearest neighbors (MNN) of the particles from the previous generation (Filippi et al. 2013). The ABC-SMC-MNN algorithm is illustrated in Algorithm 3.
Algorithm 3 SIIDR parameters estimation

Require: \( G \) - number of generations, \( N \) - number of particles, \( M \) - number of nearest neighbors, \( \epsilon_1 > \epsilon_2 > \epsilon_3 > \cdots > \epsilon_G \) - sequence of decreasing tolerance values for each generation of the particles

1. Set \( g = 0 \)
2. Set \( j = 0 \)
3. If \( g = 0 \), sample particle \( \theta^{**} \) from prior distribution \( P(\theta) \). Otherwise, sample \( \theta^* \) from the previous generation of particles \( \{\theta_{g-1}\} \) with weights \( \{w_{g-1}\} \) and perturb to obtain \( \theta^{**} \sim K(\theta|\theta^*) \)
4. Generate \( n \) model simulations \( D^{**}_i \) using \( \theta^* \) and calculate \( \hat{P}(D|D^{**}) = 1/n \sum_{l=1}^{n} I(d(D, D^{**}_l) < \epsilon_g) \)
5. If \( \hat{P}(D|D^{**}) = 0 \), return to step 4
6. Set \( \theta^*_j \) and calculate weights for the particle:
   \[
   w^j_g = \begin{cases} 
   \frac{\hat{P}(D|D^{**}) P(\theta^{**}), g = 1}{\sum_{l=1}^{N} w^l_{g-1} K(\theta^*_j|\theta^*_{g-1})}, g > 1 
   \end{cases}
   \]
7. If \( j < N \), increment \( j \) and go to step 4
8. Normalize weights: \( \sum_{j=1}^{N} w^j_g = 1 \)
9. If \( g < G \), increment \( g \) and go to step 3

Acknowledgements
We acknowledge Jason Hiser and Jack W. Davidson from University of Virginia for providing us access to the WannaCry attack traces.

Author contributions
NG and NP proposed the SIIDR model. AC, NG, and NP contributed to the methodology of the paper. AC and NG performed the experiments. All authors contributed to the discussion and writing of the paper, and approved the final manuscript.

Funding
Open access funding provided by Northeastern University Library This research was sponsored by the U.S. Army Combat Capabilities Development Command Army Research Laboratory under Cooperative Agreement Number W911NF-13-2-0045 (ARL Cyber Security CRA). The views and conclusions contained in this document are those of the authors and should not be interpreted as representing the official policies, either expressed or implied, of the Combat Capabilities Development Command Army Research Laboratory or the U.S. Government. The U.S. Government is authorized to reproduce and distribute reprints for Government purposes notwithstanding any copyright notation hereon.

Availability of data and materials
The datasets supporting the conclusions of this article are available in the github repository: https://github.com/achernikova/siidr/. WannaCry data is available from the corresponding author on reasonable request.

Code availability
The code is available in the github repository: https://github.com/achernikova/siidr/.

Declarations

Competing interests
The authors declare that they have no competing interests.

Received: 9 June 2023   Accepted: 3 August 2023
Published online: 18 August 2023

References
Abbey H (1952) An examination of the Reed-Frost theory of epidemics. Hum Biol 24(3):201–33
Akaike H (1974) A new look at the statistical model identification. IEEE Trans Autom Control 19(6):716–723. https://doi.org/10.1109/TAC.1974.1100705
Akbanov MV, Vassilakis VG, Logothetis MD (2019) Ransomware detection and mitigation using software-defined networking: the case of WannaCry. Comput Electr Eng 76:111–121. https://doi.org/10.1016/j.compeleceng.2019.03.012
Kiddle C, Simmonds R, Williamson C et al (2003) Hybrid packet/flow network simulation. In: Seventeenth workshop on parallel and distributed simulation, 2003. (PADS 2003). Proceedings. IEEE, pp 143–152

Kim HA, Karp B (2004) Autograph: toward automated, distributed worm signature detection. In: 13th USENIX security symposium (USENIX Security 04). USENIX Association, San Diego, CA

Kumar A, Lim TJ (2020) Early detection of MiRaI-like botnets in large-scale networks through sub-sampled packet traffic analysis. In: Advances in information and communication: proceedings of the 2019 future of information and communication conference (FICC), vol 2. Springer, pp 847–867

Le LT, Eliassi-Rad T, Tong H (2015) MET: a fast algorithm for minimizing propagation in large graphs with small eigen-gaps. In: Proceedings of the 2015 SIAM International conference on data mining (SDM), pp 694–702

Leskovec J, McAuley J (2012) Learning to discover social circles in ego networks. Adv Neural Inf Process Syst 25

Leskovec J, Kleinberg J, Faloutsos C (2005) Graphs over time: densification laws, shrinking diameters and possible explanations. In: Proceedings of the eleventh ACM SIGKDD international conference on Knowledge discovery in data mining, pp 177–187

Leskovec J, Kleinberg J, Faloutsos C (2007) Graph evolution: densification and shrinking diameters. ACM Trans Knowl Discov Data (TKDD) 1(1):2–es

Levy N, Rubin A, Yom-Tov E (2020) Modeling infection methods of computer malware in the presence of vaccinations using epidemiological models: an analysis of real-world data. Int J Data Sci Anal 10(4):349–358

Li J, Stafford S (2014) Detecting smart, self-propagating Internet worms. In: IEEE Conference on communications and network security, pp 193–201. https://doi.org/10.1109/CNS.2014.6997486

Martinez Martinez I, Florián Quitián A, Díaz-López D et al (2021) MalSEIRS: Forecasting malware spread based on compartmental models in epidemiology. Complexity

McKinley DJ, Vernon I, Andrianiak L et al (2018) Approximate Bayesian computation and simulation-based inference for complex stochastic epidemic models. Stat Sci 33(1):4–18

Miao H, Xia X, Perelson AS et al (2011) On identifiability of nonlinear ode models and applications in viral dynamics. SIAM Rev 53(1):3–39

Minter A, Retkute R (2019) Approximate Bayesian computation for infectious disease modelling. Epidemics 29:100368

Mishra BK, Jha N (2010) SEIQRS model for the transmission of malicious objects in computer network. Appl Math Model 34(3):710–715

Mishra BK, Pandey SK (2014) Dynamic model of worm propagation in computer network. Appl Math Model 38(7–8):2173–2179

Mishra BK, Saini D (2007) SEIRS epidemic model with delay for transmission of malicious objects in computer network. Appl Math Comput 188(2):1476–1482

Newman MEJ (2003) The structure and function of complex networks. SIAM Rev 45(2):167–256. https://doi.org/10.1137/s003614450342480

Newcombe J, Karp B, Song D (2005) Polyscope: automatically generating signatures for polymorphic worms. In: IEEE Symposium on security and privacy (SP), pp 226–241. https://doi.org/10.1109/SP.2005.15

Öhla RP, Srivastava PK, Sanyal G et al (2021) Improved model for the stability analysis of wireless sensor network against malware attacks. Wirel Pers Commun 116(3):2525–2548

Ongun T, Spohngellert O, Miller BA et al (2021) PORTFILER: port-level network profiling for self-propagating malware detection. In: Proceedings of the 9th IEEE conference on communications and network security (CNS), pp 182–190

Pastor-Satorras R, Castellano C, Van Mieghem P et al (2015) Epidemic processes in complex networks. Rev Mod Phys 87:925–979. https://doi.org/10.1103/RevModPhys.87.925

Perko L (2013) Differential equations and dynamical systems, vol 7. Springer Science & Business Media, New York

Perumalla KS, Sundaragopalan S (2004) High-fidelity modeling of computer network worms. In: 20th Annual computer security applications conference. IEEE, pp 126–135

Prakash B, Chakrabarti D, Faloutsos M et al (2011) Threshold conditions for arbitrary cascade models on arbitrary networks. Knowl Inf Syst 33:537–546

Riley GF, Ammar MH, Fujimoto RM et al (2004) A federated approach to distributed network simulation. ACM Trans Model Simul (TOMACS) 14(2):116–148

Sayama H (2015) Introduction to the modeling and analysis of complex systems. Open SUNY, New York

Szymanski BK, Liu Y, Gupta R (2003) Parallel network simulation under distributed genesis. In: Seventeenth workshop on parallel and distributed simulation, 2003. (PADS 2003). Proceedings. IEEE, pp 143–152
Watts DJ, Strogatz SH (1998) Collective dynamics of 'small-world' networks. Nature 393(6684):440–442
Wei S, Hussain A, Mirkovic J et al (2010) Tools for worm experimentation on the deters testbed. Int J Commun Netw
Distrib Syst 5(1–2):151–171
Wertz JS, Dushoff J (2015) Modeling post-death transmission of Ebola: challenges for inference and opportunities for
control. Sci Rep 5(1):8751
White B, Lepeau J, Stoller L et al (2002) An integrated experimental environment for distributed systems and networks.
ACM SIGOPS Op Syst Rev 36(SI):255–270
Wikipedia (2023a) Colonial Pipeline ransomware attack. URL https://en.wikipedia.org/wiki/Colonial_Pipeline_ransomware_attack. Accessed 7 May 2022
Wikipedia (2023b) Petya and NotPetya. URL https://en.wikipedia.org/w/index.php?. Accessed 7 May 2022
Wikipedia (2023c) WannaCry ransomware attack. URL https://en.wikipedia.org/w/index.php?title=WannaCry_ransomware_attack&oldid=1086034703, accessed 7-May-2022
Yao Y, Fu Q, Yang W et al (2018) An epidemic model of computer worms with time delay and variable infection rate. Secur Commun Netw 2018
Zheng Y, Zhu J, Lai C (2020) A SEIQR model considering the effects of different quarantined rates on worm propagation
in mobile internet. Math Prob Eng
Zhu Q, Yang X, Ren J (2012) Modeling and analysis of the spread of computer virus. Commun Nonlinear Sci Numer Simul
17(12):5117–5124

Publisher’s Note
Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.