Hindawi
Security and Communication Networks
Volume 2019, Article ID 6803801, 14 pages
https://doi.org/10.1155/2019/6803801

Research Article

Dynamics on Hybrid Complex Network: Botnet Modeling and Analysis of Medical IoT

Mingyong Yin,[1,2] **Xingshu Chen**,[3,4] **Qixu Wang**,[3,4] **Wei Wang**,[4] **and Yulong Wang**[2,3]

[1]*College of Computer Science and Technology, Sichuan University, Chengdu 610065, China*
[2]*Institute of Computer Application, Mianyang 621900, China*
[3]*College of Cybersecurity, Sichuan University, Chengdu 610065, China*
[4]*Cybersecurity Research Institute, Sichuan University, Chengdu 610065, China*

Correspondence should be addressed to Qixu Wang; qixuwang@scu.edu.cn

Received 22 May 2019; Accepted 28 July 2019; Published 18 August 2019

Guest Editor: Kuan Zhang

Copyright © 2019 Mingyong Yin et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

With the rapid development of Internet of things technology, the application of intelligent devices in the medical industry has become ubiquitous. Connected devices have revolutionized clinicians and patient care but also made modern hospitals vulnerable to cyber attacks. Among the security risks, botnets are of particular concern, which can be used to control thousands of devices for remote data theft and equipment destruction. In this paper, we propose a non-Markovian spread dynamics model to understand the effects of botnet propagation, which can characterize the hybrid contagion situation in reality. Based on the Susceptible-Adopted-Recovered model, we introduce nonredundant memory spread mechanism for global propagation, as a tuner to adjust spreading rate difference. For describing the proposed model, we extend a heterogeneous edge-based compartmental theory. Through extensive numerical simulations, we reveal that the growth pattern of the final adoption size versus the information transmission probability is discontinuous and how the final adoption size is affected by hybrid ratio α, global scope control factor ϵ, accumulated received information threshold T, and other parameters on ER network. Furthermore, we give the theory and simulation result on BA network and also compare the two hybrid methods—single infection in one time slice and double infections in one time slice—to evaluate the influence on final adoption size. We found in SIOT hybrid contagion scenario the final adoption size shows the phenomenon of a decline followed by an increase versus different hybrid ratio, and it is both verified in theory and numerical simulation. Through validation by thousands of experiments, our developed theory agrees well with the numerical simulations.

1. Introduction

With the wide application of Internet of things (IoT) devices in the medical industry, security threats caused by limited computing power of devices, less security protection measures, and insufficient attention are also increasing, among which botnet is one of the biggest security threats. As is well known, most medical equipments have following security characters: always online, weak security protection, low cost of botnet attacks, and difficulty in clarifying the attribution of security responsibilities. With the control of medical IoT devices, botnet can be used to steal information and destroy devices according to hacker instructions. The security weaknesses of medical device can be manipulated to appropriate control over personal devices, hospital diagnostic machines, and other medical appliances. The work conducted by Jay Radcliffe in 2011 on weaknesses found in insulin pumps had aroused a lot of attention, he gave a live demonstration showing that it was possible to remotely deliver lethal doses of insulin to patients [1, 2].

Botnet, as a general bearing platform, has become the source of all kinds of network attacks. Botnet is evolved from traditional malicious code, which combines various attack methods, and has gradually become a highly efficient attack platform. Through botnet, the attacker implants botnet programs into the host in the network, controls the infected host, and establishes command and control channels. The biggest difference between botnet and traditional attacks is the one-to-many control structure, which enables attackers to control a large number of resources to serve them at a very low cost, which poses a huge

challenge to the security, confidentiality, and integrity of the medical industry network environment.

With the increasing threats of botnet, from antivirus companies to research institutions have conducted a large number of in-depth analysis and research on botnet, including botnet detection, tracking, defense, and countermeasures, and also, different defending mechanisms are introduced into IoT network [3–6]. The establishment of botnet propagation model is an effective tool to analyze and study the propagation characteristics of botnet, which is a necessary condition to understand the dynamics of the threat they pose. The recent frequent extortion of ransomware, such as Wannacry, Petya, etc., has caused great losses to individuals and enterprises. This kind of virus based on botnet can spread both on WAN and on LAN, and their propagation law also presents some new characteristics. It is a challenging problem to evaluate the influence of different information transmission channels on user adoption, the possibility of virus email sent by friends or strangers to be clicked and opened.

A mixture of local propagation and global propagation is typical in hybrid propagation mechanism, as depicted in Figure 1. For local propagation, where the infected node only infects a subset of the limited propagation target nodes, the infected node typically infects neighboring nodes [7]; for global propagation, the nodes are fully mixed, and the infected nodes can infect any other node [8, 9]. In fact, many epidemics use mixed transmission, which involves two or more combined transmission mechanisms. Also, the ransomware can scan a target computer on a local network or any computer randomly selected on the internet through a port scan. Among them, the local area network node is in the internal network environment which means the communication between internal nodes will not pass through firewall; also, to the node homogeneity, the probability of successful infection is higher in local spreading. Because the WAN node is not aware of the network environment of the target node, its success probability will be lower than the local success probability.

Another phenomenon we are interested in is when a host receives a number of disguised emails with viruses, the probability of computer infection will also increase because it is more likely to be misclicked; this memory effect makes the dynamics of social contagion non-Markovian.

In a word, in order to effectively depict the dissemination of botnet, we need to be able to describe the heterogeneous credibility of information from different sources, the impact range of different masters in the dissemination model, and the mixture way of different propagation method in single time slice. This characteristic also exists widely in other information and behavior dissemination. Therefore, it is necessary to study this dissemination scenario in order to provide a theoretical basis for the prediction and control of bot dissemination.

This paper proposes a hybrid propagation dynamics theoretical model based on the SAR model and the edge compartmental theory that includes local and global propagation and can capture differences in its propagation capabilities, which contributes in the following areas:

(1) In order to describe the phenomenon of botnet mixed propagation through LAN and WAN, we propose a hybrid propagation model that supports the global spreading participation node range control, which can better reflect the reality that a target node is infected by a limited range of attack nodes because of the impact of time, space, and randomness. It is different from previous work regarding global spreading as the infected node will infect every node in the network.

(2) We introduce nonredundant memory features in global propagation process, by setting the parameter of cumulative information that needs to be received for triggering state change; the propagation rate can be modified flexibly.

(3) Theoretical analysis and simulation experiments verify the effects of different mixing ratios on the final propagation range and find that under a certain spreading rate, the final propagation range will present a wavy curve phenomenon versus hybrid ratio α.

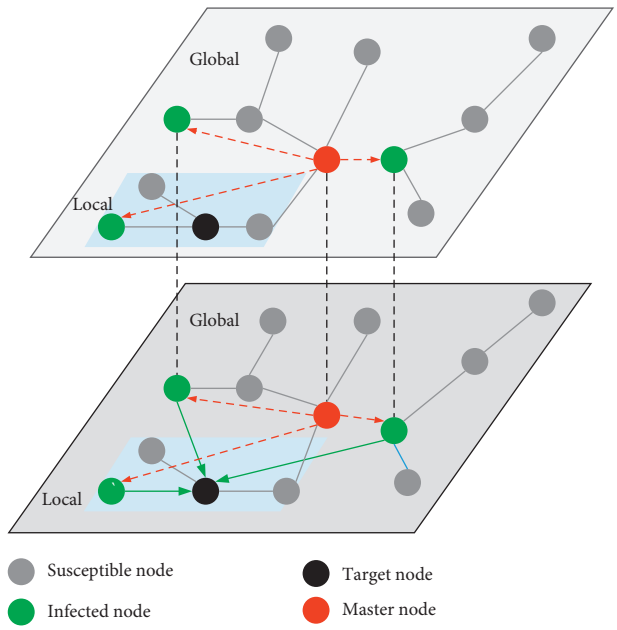


Figure 1: Illustration of hybrid propagation.

This paper is organized as follows. Section 2 gives a brief summary about related work on botnet propagation model. In Section 3, we abstract the scenes of different types of mixed propagation and present the model description. Based on the definition in Section 3, we give the theoretical derivation in Section 4. In Section 5, the correctness of the theory is verified by numerical simulation and program simulation, and the influence of different parameters on the final propagation range in the mixed propagation process is analyzed.

2. Related Work

2.1. Botnet Propagation Model. With the widespread use of IoT technology in the medical industry, ubiquitous smart

devices have greatly increased the attack surface while providing convenience for doctors and patients [10]. Among them, the malware infects the sensor and the terminal and is commanded and controlled by the external botnet master node, so the attacker initiates the attack to achieve purpose when the attacker needs it. These botnets composed of botnet devices have become the main threat to the network security and life safety in the medical industry, and they can breakthrough defense under heterogeneous network structure and different layers [11–14]. We need to perceive and understand the propagation process as early as possible to provide theoretical support for better control in different scenarios.

Botnet can generally be divided into infection, command and control, and attack phases. This article focuses on the infection phase of botnet. At this stage, attackers can spread bots in various ways, such as trojans, malicious emails, active scanning, passively inducing users to download and install bots, or proactively exploiting remote service vulnerabilities. After the attacker infects the target host, the hidden module is loaded, and the botnet program is hidden in the controlled host by techniques such as deformation and polymorphism. One of the most influential botnets is the Mirai botnet. Mirai uses worm-based propagation, which includes Internet of things cameras, routers, printers, and video recorders [1].

Modeling the botnet propagation based on the biological disease propagation model is a common method adopted by researchers. The propagation dynamics is used to model the propagation behavior and derive botnet spreading differential equations and then verify the worm propagation law with numerical simulation. They also try to solve the problem of how the network defender can prevent the formation of botnet by enhancing the security defense capability of the device under the condition that the network operation overhead is minimal [15–17].

Researchers have conducted extensive research on the propagation behavior of worms in wireless sensor networks. Representative work includes the Susceptible-Exposure-Infection-Recovery-Sensitivity Vaccination (SEIRS-V) model and the Susceptible-Exposure-Infection-Recovery-Vaccination (SEIRV) model. By capturing the spatiotemporal dynamics of the worm's propagation process, these models define equilibrium points using the basic reproductive number $R0$ and then assess the stability of the system at these points [18, 19].

Dagon et al. [20] discovered the law of botnet propagation affected by time and region based on the continuous monitoring of botnet and constructed a diurnal propagation model to characterize botnet infection. Todd Gardner et al. [21] researched botnet from the perspective of user behavior and found that we can mitigate the frequency of IoT botnet attacks with improved user information, which may positively affect user behavior; this can be used to predict user behavior after the botnet attack.

2.2. Dynamics on Complex Network. With the development of complex networks and communication dynamics, many phenomena in the fields of computer science, biology, sociology, and economics are characterized by "propagation dynamics on complex networks," and the methods to reveal their propagation laws are widely used [22–24].

In the field of Internet, the recent frequent extortion of ransomware, such as Wannacry, Petya, Scarab, etc., has caused great losses to individuals and enterprises [25–27]. For rumor spreading, ordinary users often receive opinions from opinion leaders and people they are familiar with; it is a challenging problem to evaluate the influence of different information spreading ways on user adoption. Therefore, it is necessary to conduct research on this hybrid propagation phenomenon and understand its law of transmission so as to further take effective countermeasures.

Research on social contagion mechanism and corresponding control strategies is one of the hotspots of current research. At present, scholars have carried out a lot of research on the impact of the heterogeneity of individual adoption behavior, heterogeneity of network structure, memory of individual adoption behavior, nonredundant contagion, and incomplete neighborhood spreading on social propagation. In reality, memory usually plays an important role on adoption enhancement for social contagion. For instance, when someone hears a message from many people, it is believed that the credibility of information will be greatly improved. When receiving a number of disguised emails with viruses, the probability of computer infection will also increase because it is more likely to be misclicked. This memory effect makes the dynamics of social contagion non-Markovian. Considering the memory effect, a modeling method based on non-Markov model is proposed in [28–30]. Generally speaking, a node can receive the cumulative information about specific social behavior either in a redundant or nonredundant manner [31], where the former allows a pair of individuals to successfully transmit information many times, but for the latter, repetitive transmission is prohibited. Previous studies on nonredundant information transmission characteristics of society have been relatively few [30, 32, 33]. It is of great significance to understand the dynamics of transmission with nonredundant information memory effect in hybrid spreading situation.

3. Model Descriptions

In this section, we give the model of botnet propagation in hybrid spreading scenario, to characterize the comprehensive effect on target node. It can reflect the fact that medical devices can be infected by local area nodes or internet terminals with different impacts. For the network G composed of N nodes, the average degree is $\langle k \rangle$ and the degree of node i is k_i. The nodes participate in one of the propagations with a certain probability in each time slice. For node i, during each round of propagation, it will involve in local propagation or global propagation with probability α; we note this kind of propagation as single in one time slice (SIOT). Correspondingly, for the situation that node i can receive messages from both local and global propagation, we name it as double in one time slice (DIOT).

In order to describe the heterogeneous credibility of information received from the local and the global sources in the case of mixed propagation, we assume that the local

propagation threshold and the global propagation threshold are different and the global propagation information is received as a nonredundant memory process; each node information can only be passed once to the target node. As shown in Figure 1, the target node (black) can receive information from the local neighbor infected nodes (green) and global infected nodes.

In the case of local propagation, nodes are more likely to adopt corresponding ideas or infect similar viruses, so we set the threshold of local contagion to 1. The infected neighbor node j infects node i with probability lambda; that is, the probability of accepting information from local propagation per round is $\lambda_L = \alpha\lambda$. Similarly, node i participates in global propagation with probability $1-\alpha$, and the rate is $\lambda_G = (1-\alpha)\lambda$. Due to the large number of nodes in the whole network, we introduce the global parameter ϵ to control the node scale in propagation; the global node participating in the propagation of i is $N\epsilon$, and the number of participating global nodes can be adjusted by the parameter ϵ. In the global propagation situation, the Internet attack node randomly scans the target user for botnet propagation and randomly sends the message for propagation.

Compared with local propagation, the information credibility from global channel is less trustworthy. Therefore, we set the threshold as T, and it is satisfied that each node receives broadcast information of other nodes no more than once. In addition, since the number of global nodes is much larger than that of local nodes, in the modeling process, to simplify processing, the global propagation node includes neighbor nodes of node i.

For the dynamic modeling of network propagation process, this paper references the SAR (Susceptible-Adopted-Recovered) model. At any time, any node in the network is in one of these three states, as shown in Figure 2. S represents susceptible state, indicating that a node in the network can be infected; A represents infected state, indicating that a node in the network has been infected; and R represents recovery state, indicating that the infected node in the network has changed to a recovery state and can no longer participate in the follow-up process.

In each propagation round, we assume that one node can participate in either global or local contagion one time if the node state is S; for nodes in A state, it can try once for recovering to R state by sampling γ. For the mixed propagation of different intensity propagation sources, we are concerned about the outbreak threshold characteristics, especially the first-order phase transition. We further investigate the impact on the final adoption size under different hybrid ratios of mixed propagation, various transmission rates, and initial seed ratio during the propagation process.

4. Theory

4.1. SIOT. In this section, we make use of generalized heterogeneous edge-based compartmental theory, based on the previous work in [34–36] to describe our model and characterize the hybrid propagation process based on edge-based compartmental theory for the analysis. Although the system in [35] was proposed to analyze single-mechanism-based spreading for the continuous time case, it can be modified to be suitable for our model with hybrid propagation for discrete time and nonredundant information memory characteristic. We calculate the probability that a random test node u is in each state: susceptible $S(t)$, infected $A(t)$, and recovered $R(t)$.

We define the probability that a node has degree k is $p(k)$; it means the number of neighbors of node u for local spreading is k. The generating function of degree distribution $p(k)$ is defined as $g(x) = \sum_k p(k)x^k$, where $p_n(k)$ means the probability that, for a random neighbor of u, it has k edges. We assume the degrees of the two end nodes of each edge are independent.

In an uncorrelated network $p_n(k) = kp(k)/\langle k\rangle$, where $\langle k\rangle$ is the average degree of the network, we denote θ_t as the probability that a random neighbor v has not infected u through local path. Let ϑ_t be the probability that global node w has not infected u through global path.

Suppose u has k neighbors, the probability that it is susceptible is decided by local and global spreading result. For local propagation, we assume the infection threshold is 1, i.e., whenever node u receives one message from neighbors, it will be infected, so we can get $S_L(\overrightarrow{k}, t) = \theta_t^k$ for nodes which have degree k. For global propagation, influenced by the factors like low trust and environment heterogeneity, we assume the infection threshold is T, and T is greater than or equal to 1; at time t, the probability of node u not infected through global spreading is

$$S_G(\overrightarrow{k}, t) = \binom{N-1}{m}\vartheta_t^{N-1-m}(1-\vartheta_t)^m, \tag{1}$$

where n is the number of nodes attending in the propagation. So, at time t, the probability that node u is in the susceptible state can be written as

$$S(\overrightarrow{k}, t) = \theta_t^k \sum_{m=0}^{T-1}\binom{N-1}{m}\vartheta_t^{N-1-m}(1-\vartheta_t)^m. \tag{2}$$

Then, by averaging $S(\overrightarrow{k}, t)$ over all degrees, the initial ratio of nodes in adopted state is ρ_0, and we have

$$S(t) = (1-\rho_0)\sum_k p(k)\theta_t^k \sum_{m=0}^{T-1}\binom{N-1}{m}\vartheta_t^{N-1-m}(1-\vartheta_t)^m. \tag{3}$$

A neighbor of individual u may be in one of susceptible, adopted, or recovered states. We can thus further express θ_t as

$$\theta_t = \phi_S(t) + \phi_A(t) + \phi_R(t), \tag{4}$$

where $\phi_S(t), \phi_A(t), \phi_R(t)$ is the probability that a neighbor of the individual u, is in the state of susceptible, adopted, or recovered, and has not transmitted the information to

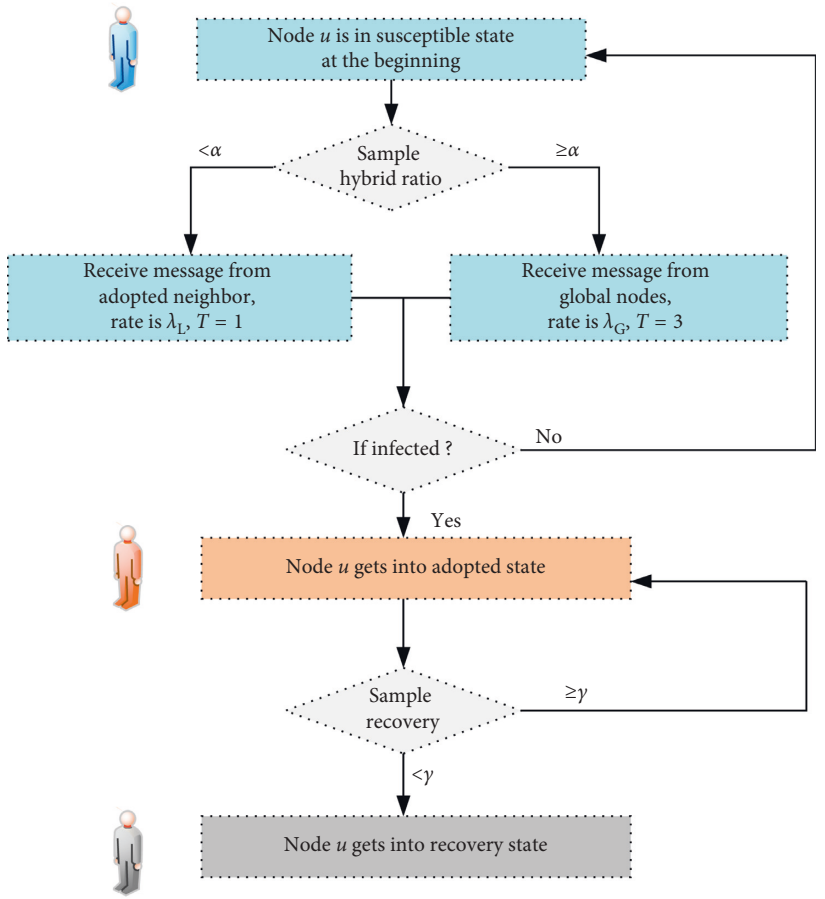


FIGURE 2: The flow chart of node state transferring; in each spread phase, a node will act in either local or global propagation according to the sample result.

individual u by time t. We need to seek the solution of three possibilities. Assume a neighboring individual v of u is in the susceptible state at start point; it cannot transmit the information to u. Individual v can get the information from its other neighbors, since u is in a cavity state. Neighbor v cannot be infected by u and itself; then,

$$\phi_S(t) = (1-\rho_0)\sum_k kp(k)\theta_t^{k-1}\binom{N-2}{m}\sum_{m=0}^{T-1}\vartheta_t^{N-2-m}\frac{(1-\vartheta_t)^m}{\langle k\rangle}. \tag{5}$$

We further investigate $\phi_R(t)$; it should satisfy the definition that an adopted neighbor has not transmitted the information to u via its connection and with probability γ the adopted neighbor to be recovered. According to the analysis above, we get

$$\frac{d\phi_R(t)}{dt} = \gamma(1-\lambda_L)\phi_A(t). \tag{6}$$

At time t, the rate of change in the probability that a random edge has not transmitted the information is equal to the rate at which the adopted neighbors transmit the information to their susceptible neighboring individuals through edges. Thus, we get

$$\frac{d\theta(t)}{dt} = -\lambda_L\phi_A(t). \tag{7}$$

Combining equations (6) and (7), we obtain

$$\phi_R(t) = \frac{\gamma(1-\theta(t))(1-\lambda_L)}{\lambda_L}. \tag{8}$$

$$\frac{d\theta(t)}{dt} = -\lambda_L(\theta(t)-\phi_S(t)-\phi_R(t)). \tag{9}$$

Substitute equations (8) and (5) into equation (7). Doing so, we can rewrite equation (6) as

$$\frac{d\theta(t)}{dt} = \lambda_L\sum_k\frac{kp(k)}{\langle k\rangle}\theta_t^{k-1}\binom{N-2}{m}\sum_{m=0}^{T-1}\vartheta_t^{N-2-m}(1-\vartheta_t)^m + \gamma(1-\theta(t))(1-\lambda_L) - \lambda_L\theta(t). \tag{10}$$

We can write ϑ_t as

$$\vartheta_t = \varphi_S(t) + \varphi_A(t) + \varphi_R(t). \tag{11}$$

In the same way with local spreading, for global propagation, we take into account the weak relationship with global nodes; the threshold for state change from

susceptible state to adopted state is T, that is, a node should at least receive T messages from global spreading and then it can trigger state change. Then, $\varphi_S(t)$ can be written as

$$\varphi_S(t) = (1-\rho_0)\sum_K p(k)\theta_t^k \binom{N-2}{m} \sum_{m=0}^{T-1} \vartheta_t^{N-2-m}(1-\vartheta_t)^m. \tag{12}$$

So $\varphi_R(t)$ is

$$\varphi_R(t) = \frac{\gamma(1-\vartheta(t))(1-\lambda_G)}{\lambda_G}. \tag{13}$$

Then, we can get

$$\frac{d\vartheta(t)}{dt} = \lambda_G \sum_K p(k)\theta_t^k \binom{N-2}{m} \sum_{m=0}^{T-1} \vartheta_t^{N-2-m}(1-\vartheta_t)^m + \gamma(1-\vartheta(t))(1-\lambda_G) - \lambda_G\vartheta(t). \tag{14}$$

We know $S(t) + A(t) + R(t) = 1$ at time t, note that the rate $dA(t)/dt$ is equal to the rate at which $S(t)$ decreases because all the individuals moving out of the susceptible state must move into the adopted state minus the rate at which adopted individuals become recovered. We have

$$\frac{dA(t)}{dt} = -\frac{dS(t)}{dt} - \gamma A(t), \tag{15}$$

$$\frac{dR(t)}{dt} = \gamma A(t). \tag{16}$$

According to the deduction above, we can have the general description of social contagion dynamics so that we can calculate the probability that node u has not received enough messages for state changing.

$$\theta(\infty) = \sum_k \frac{kp(k)}{\langle k\rangle}\theta_{(\infty)}^{k-1} \binom{N-2}{m} \sum_{m=0}^{T-1} \vartheta_{(\infty)}^{N-2-m}(1-\vartheta_\infty)^m + \frac{\gamma(1-\theta(\infty))(1-\lambda_L)}{\lambda_L}, \tag{17}$$

$$\vartheta(\infty) = \sum_k p(k)\theta_\infty^k \binom{N-2}{m} \sum_{m=0}^{T-1} \vartheta_\infty^{N-2-m}(1-\vartheta_\infty)^m + \frac{\gamma(1-\vartheta(\infty))(1-\lambda_G)}{\lambda_G}. \tag{18}$$

Now, we analyze the critical information transmission probability. Since we have already assumed that $T > 1$ to study the memory reinforcement, a vanishingly small fraction of seeds cannot trigger a global behavior adoption. In this situation, $\theta_x(\infty) = 1$ is not a solution of the following equation:

$$\frac{\partial f_L(\theta(\infty),\vartheta(\infty))}{\partial\theta(\infty)} \frac{\partial f_G(\theta(\infty),\vartheta(\infty))}{\partial\vartheta(\infty)} = 1. \tag{19}$$

From theory analysis, we can capture first-order phase transition at the critical point, where the condition is fulfilled. We assume $A(\infty) = 0$, then $R(\infty) = 1 - S(\infty)$; we can calculate $R(\infty)$ as final adoption size.

4.2. DIOT. For the theory introduced above, it assumes that a node can participate in only one type of spreading in each time slice, either local or global propagation. In reality, different propagation may act on nodes at the same time, so we also carry out research on this scenario.

In alternative hybrid contagion, the spreading rate for local and global propagation is $\lambda_L = \alpha\lambda$ and $\lambda_G = (1-\alpha)\lambda$, respectively, while $\lambda_L + \lambda_G = \lambda$. Different from alternative hybrid contagion, the spreading rate of parallel hybrid contagion does not have such constraints, and λ_L and λ_G are isolated.

To further explore the contribution of two spreading methods in hybrid propagation, we introduce globe spreading rate control factor ζ; let $\lambda_G = \lambda_L/\zeta$; by doing this, we can get the variety of final adoption size versus different global transmission rate. So, equations (17) and (18) can be written as

$$\theta(\infty) = \sum_k \frac{kp(k)}{\langle k\rangle}\theta_{(\infty)}^{k-1} \binom{N-2}{m} \sum_{m=0}^{T-1} \vartheta_{(\infty)}^{N-2-m}(1-\vartheta_\infty)^m + \frac{\gamma(1-\theta(\infty))(1-\lambda)}{\lambda}, \tag{20}$$

$$\vartheta(\infty) = \sum_k p(k)\theta_\infty^k \binom{N-2}{m} \sum_{m=0}^{T-1} \vartheta_\infty^{N-2-m}(1-\vartheta_\infty)^m + \frac{\gamma(1-\vartheta(\infty))(1-\lambda/\zeta)}{\lambda/\zeta}. \tag{21}$$

5. Simulation

5.1. Simulation Method. Based on the theory analysis of the botnet spreading progress, we perform numerical simulations to study our proposed hybrid contagion model, using Erdos–Renyi (ER) network model [37] and Barabasi–Albert (BA) network with power-law degree distribution for our simulations [8]. For medical IoT, the medical equipment or sensors are always deployed in diagnosis and treatment room or datacenter; in general, it is hard to infect them by email attachments as commonly seen in computer. The most possible attack vector is wired or wireless network intrusion and hardware addition by human intervention, which can be categorized as local propagation; we can model these possible propagation channels with hybrid spreading model. An overview of the proposed numerical simulation program is shown in

Algorithm 1. In initiation phase, ER network generation and parameter settings need to be handled first. We use the open-source package NetworkX [38] to produce network ER network G, the network size is 10,000 network nodes, and the average degree is $\langle k \rangle = 10$.

We randomly set 5 nodes in adopted state, $\rho_0 = 5/10^4$. At each experiment, according to the variable that needs to be investigated, parameters like local propagation probability λ_L, global propagation probability λ_G, threshold T, recovery rate γ, hybrid ratio α, and globe scope controller ϵ are set respectively. In most cases, we set the scope parameter $\epsilon = 0.004$, that is, in each transmission, node u will receive messages from 40 global nodes. For each experiment, we repeat a thousand times and take the average value as simulation result.

5.2. SIOT in ER Network. We first study the effects of hybrid ratio α on social contagions in ER networks. As shown in Figure 3, the hybrid ratio changes the growth pattern of the final behavior adoption size $R(\infty)$ versus the information transmission probability λ. From the figure, we can see that when $\lambda = 0.1$, the final adoption size $R(\infty)$ is varied with α increments. When α value is small, the local propagation contributes less, and it is hard to outbreak when initial seeds are few. Nonetheless, when α gets higher, more chances are there for the node to receive message from neighbors; as we aforementioned, the threshold is 1, so it will promote the probability of nodes in susceptible state to get into adopted state. When more nodes are in adopted state, for global propagation, it is much easier to receive more messages than threshold for state changing. Furthermore, when α keeps on augmenting larger than the outbreak value, the final adoption size will gradually decline and ascend afterwards. Our theoretical predictions agree well with the numerical results. The differences between the theoretical and numerical predictions are caused by the strong dynamical correlations among the states of neighbors.

We further identify the outbreak threshold by the variability measure, which is a standard measure to determine the critical point in equilibrium phase on magnetic system, to reflect the fluctuation of the outbreak size for different α:

$$\delta = \frac{\sqrt{R^2 - \langle R \rangle^2}}{\langle R \rangle}. \tag{22}$$

When we fix the hybrid ratio α, the growth pattern of $R(\infty)$ versus transmission rate λ can be observed Figure 4.

We further investigate the relation between hybrid ratio α and final adoption size $R(\infty)$'s variation law; by calculating the relative change rate of $R(\infty)$, we can derive the variation pattern. It can be seen from Figure 5 that with the increase of α, the burst threshold decreases, indicating that local propagation still plays a dominant role in the mixed propagation process. The variability exhibits a peak over a wide range of λ. In our model, we introduce parameter ϵ to control the size of nodes joining in global propagation; the reason behind this is although node u can receive message from any node in the global

```
Initialization:
(1)  Network generation
(2)  Parameters initialization
     begin:
(1)  newState[]<- hisState[]
(2)  for: any node n_i in N
(3)    if node state is susceptiblesample propagation
       method with α;
(4)    if local:
(5)      get neighbor nodes list from G and node state
         from hisState[];
(6)      for: any node in neighbor[]
(7)        if node state is infected, then:
(8)          infect node n_i with λ_L;
(9)          if count > 1, update newState[];
(10)   else if global:
(11)     get Nϵ global nodes global[] from G and
         node state from hisState[];
(12)     for: any node in global[]
(13)       if node state is infected:
(14)         infect node n_i with λ_G and update count of
             received messages;
(15)         if count > T, update newState[];
(16)   else if node state is infected:
(17)     to recover with probability γ;
(18)     update newState[];
(19)   hisState[]<- newState[];
       calculate R, and refresh loop parameters.
(20) end
     Output: final adoption size R
```

Algorithm 1: Numerical simulation pseudocode.

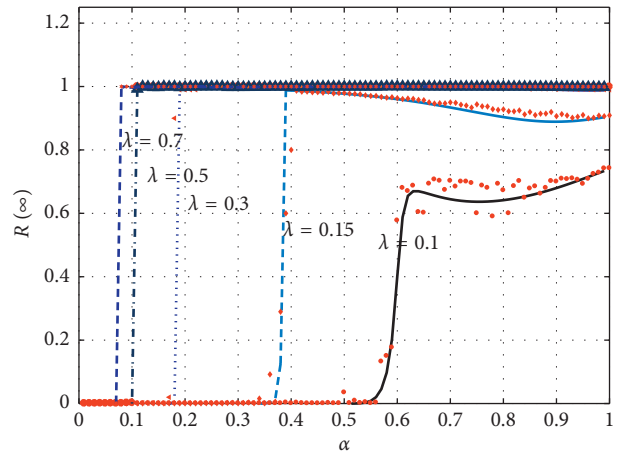


Figure 3: Propagation with fixed λ. The final behavior adoption size $R(\infty)$ versus the hybrid ratio α with fixed information transmission probability, $\lambda = 0.1, 0.15, 0.3, 0.5, 0.7$, respectively. The lines are the theoretical predictions and the dots are the simulation results.

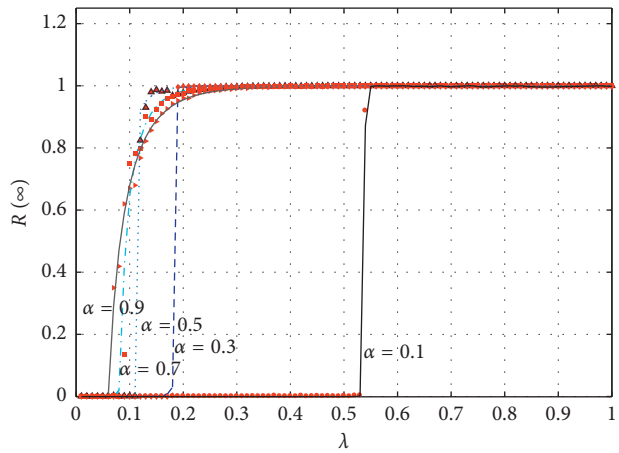


FIGURE 4: The final behavior adoption size $R(\infty)$ versus the information transmission probability λ, with fixed hybrid ratio, $\alpha = 0.1, 0.3, 0.5, 0.7, 0.9$, respectively. The lines are the theoretical predictions and the dots are the simulation results.

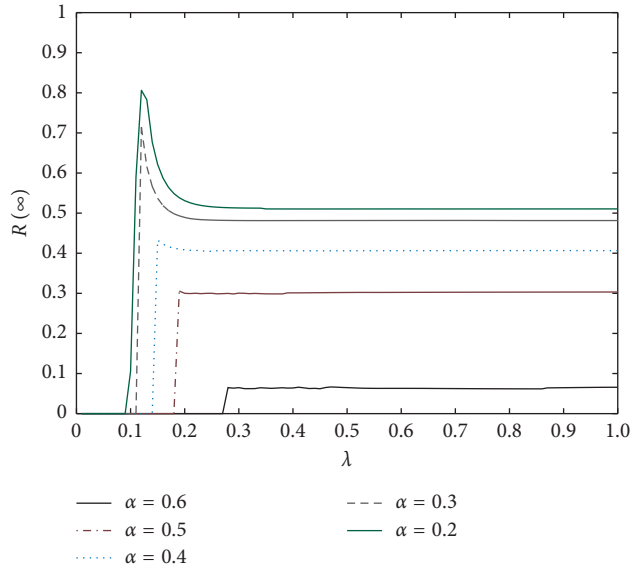


FIGURE 5: The variation of final adoption size $R(\infty)$ versus different λ with different hybrid ratio α.

method, in each round, it can be affected by only a few of them.

As shown in Figure 6, as ϵ increases, it is faster to reach the outbreak threshold value. In the same way, we further study the effects of γ on the spreading behavior. By setting $\alpha = 0.5$ and $\epsilon = 0.004$, we can investigate how the recovery rate γ influences final adoption size R, as shown in Figure 7. It visually demonstrated the change of outbreak threshold of λ; larger γ means slower outbreaks. Finally, we focus on the impact of the different memory threshold T on the propagation range. In our model, we use parameter T to adjust the information credibility, which means for large T value, more information needs to be received to change its status, as shown in Figure 8.

5.3. SIOT in BA Network. The BA network is one of the classical scale-free networks whose degree distribution follows a power law. The first scale-free model, the BA model, has a linear preferential attachment $\prod(k_i) = k_i/\sum_j k_j$ and adds one new node at every time step. Thus, in general, $\prod(k)$ has the form $\prod(k) = A + k^{\alpha}$, where A is the initial attractiveness of the node. We also set the network scale as 10,000 nodes, $\langle k \rangle = 10$, and $\rho = 5/10^4$. Other parameters are set as follows: threshold $T = 3$ for global contagion, recovery rate is $\gamma = 0.5$, and globe scope controller is $\epsilon = 0.004$.

Firstly, we can find in Figure 9 that nodes propagate faster in the BA network than in the ER network in the case of same average degree. Because BA network has unbiased degree distribution, large degree nodes have more neighbors to foster information propagation. We also find the phenomenon that final adoption size changes from decline to rise as α increases. Compared with the ER network, the BA network has 30% decrease when it reached the peak value; when $\lambda = 0.1$, greater amplitude of oscillation was caused by difference in degree

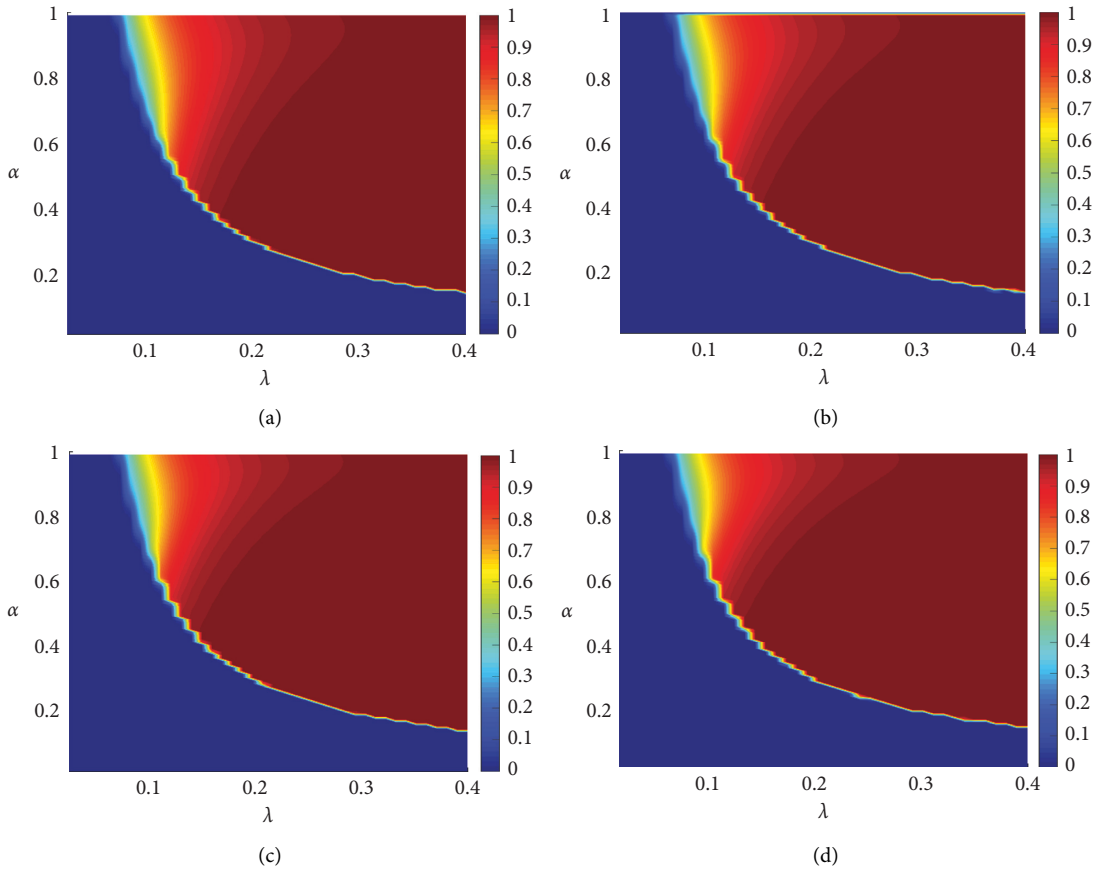


Figure 6: Final adoption size varied with ϵ. ϵ value is 0.0035, 0.004, 0.0045, and 0.005, respectively, from (a) to (d).

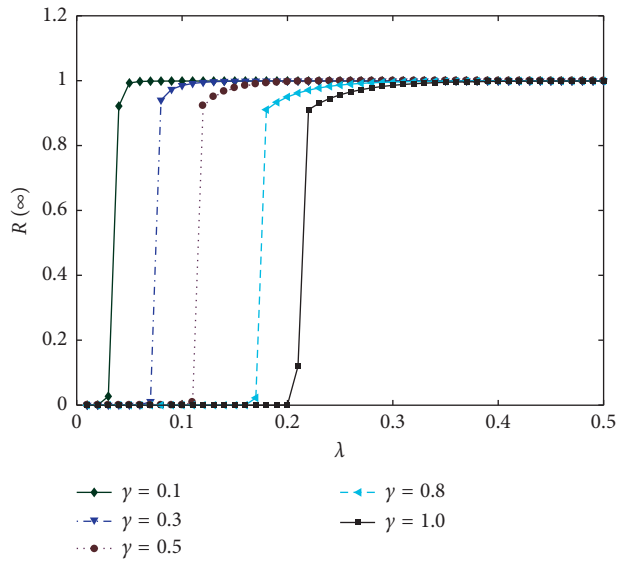


Figure 7: Final adoption size varied with γ while keeping other parameters unchanged.

distribution. Generally, the BA network can reach the burst threshold much faster than the ER network under the same lambda condition, as shown in Figure 10. In the same way, we fixed hybrid ratio α and observed the change of final adoption size with spreading rate; from Figure 11, it can be seen that when global propagation dominates, it spreads faster than the ER network, but when the local propagation ratio increases, the difference between these two network gets smaller.

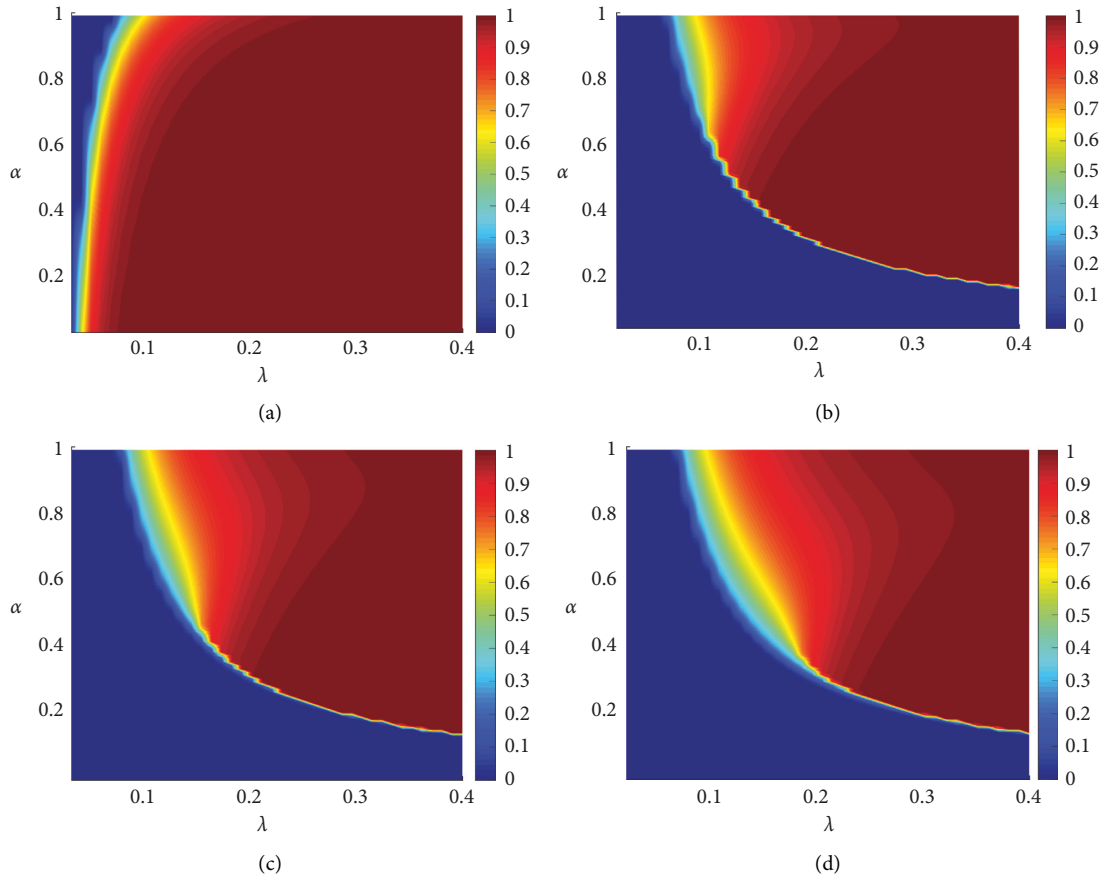


Figure 8: Final adoption size varied with T. (a) to (d) illustrate the result of $T=1$, $T=2$, $T=3$, and $T=4$, respectively.

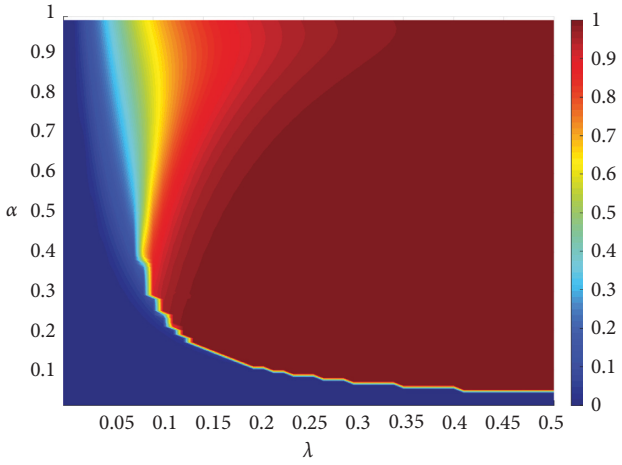


Figure 9: Final adoption size varied with ϵ in BA network. ϵ value is 0.0035, 0.004, 0.0045, and 0.005, respectively.

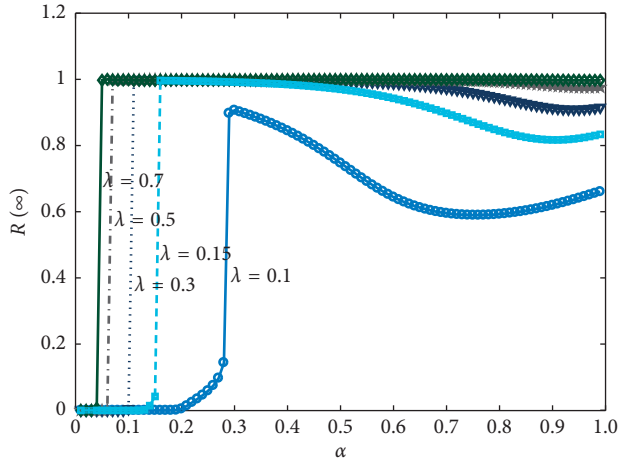


Figure 10: Final adoption size varied with α in SIOT.

5.4. DIOT. For the model introduced above, it assumes that a node can participate in only one type of spreading in each time slice, either local or global propagation. In reality, different propagations may act on nodes at the same time, so we also carry out research on this scenario.

In SIOT hybrid contagion, the spreading rate for local and global propagation is $\lambda_L = \alpha\lambda$ and $\lambda_G = (1-\alpha)\lambda$, respectively, while $\lambda_L + \lambda_G = \lambda$; the parameter α is used to adjust contagion attendance for different propagations. Compared with SIOT hybrid contagion, the spreading rate of DIOT does not have such constraints. λ_L and λ_G are isolated; this also means that a node can receive messages from local or global nodes in same time slice. The information transmission flow can be seen in Figure 12. Besides this trivial difference, other transmission parameters and contagion process are the same with SIOT hybrid

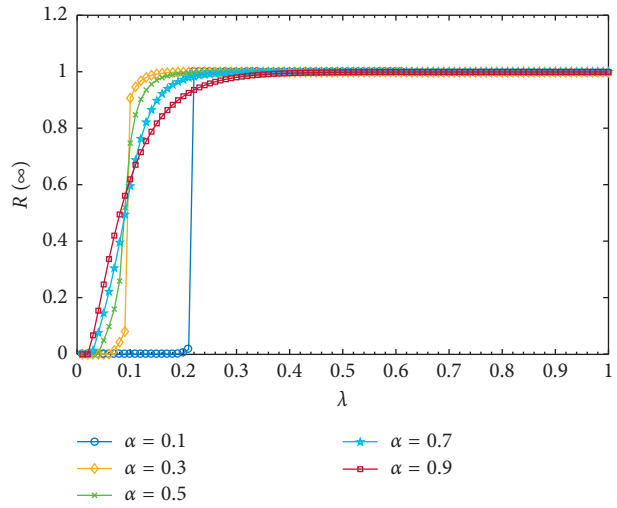


Figure 11: Final adoption size varied with λ in SIOT.

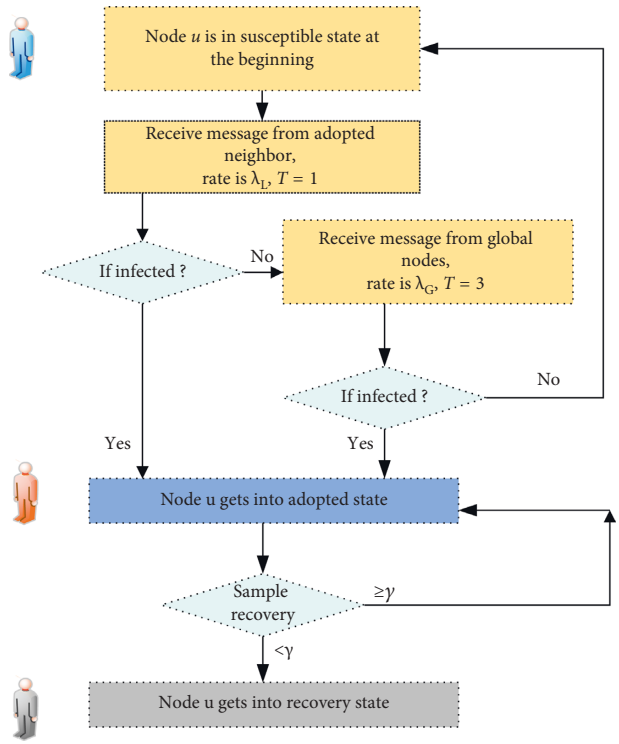


Figure 12: The flow chart of node state transferring; in each spread phase, a node will act in both local and global propagation.

transmission. For illustration convenience, we set $\lambda_L = \lambda$ and introduced global transmission rate scale parameter ζ to change transmission rate of λ_G, that is, $\lambda_G = \lambda/\zeta$; the value of ζ is from 1 to 100. As illustrated in Figure 13, we can find that nodes spread in the DIOT mode can reach outbreak threshold at lower λ than in the SIOT mode. When λ is larger than 0.12, it may reach the outbreak threshold, but if the value of λ is smaller than 0.005, it can never outbreak. The final adoption size $R(\infty)$ changes with ζ; as shown in Figure 14, we can find the multiple factor ζ can play a major role when its value is small, and as it increases, the global transmission rate will be too small to affect the adoption result. We can find from Figure 15 that changing the global spreading rate can vary the approach speed to full outbreak, but the critical point is the same, which means the discontinuous growth is controlled by local propagation.

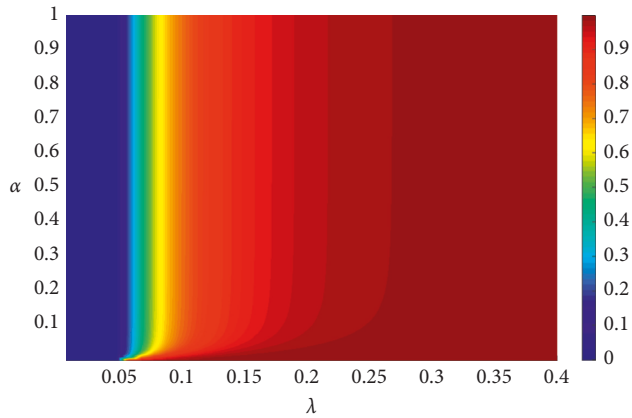


Figure 13: DIOT propagation. The final behavior adoption size $R(\infty)$ versus the global transmission rate scale and local transmission rate; other parameters are $N = 10{,}000$, $\epsilon = 0.004$, $T = 3$, and $\gamma = 0.5$, respectively. The lines are the theoretical predictions.

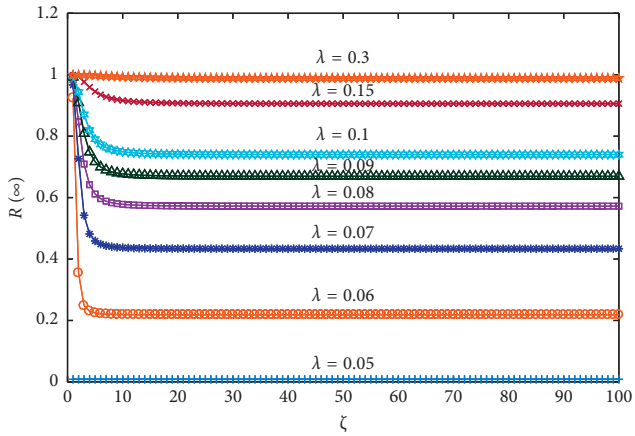


Figure 14: Final adoption size $R(\infty)$ varied with ζ in DIOT.

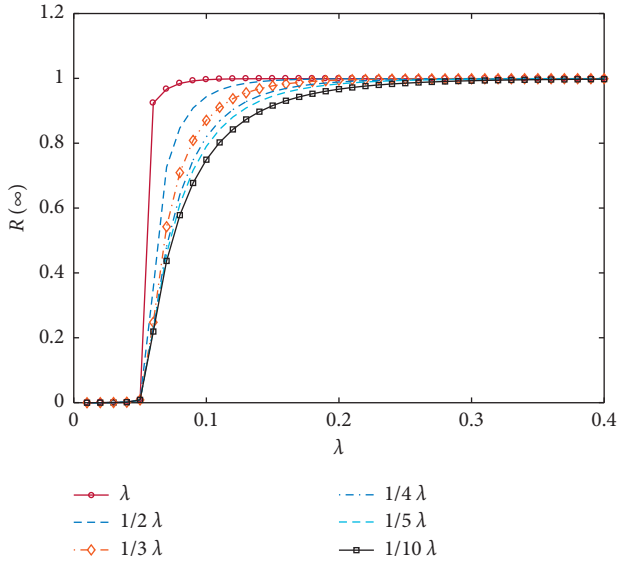


Figure 15: Final adoption size $R(\infty)$ varied with λ in DIOT.

6. Conclusion

In this paper, we studied the effects of hybrid propagation with different spreading rates and memory reinforcements on botnet contagions. We first proposed an information contagion model to describe the botnet spreading dynamics on complex networks. We then developed a generalized heterogeneous edge-based compartmental theory to describe the proposed model.

Through extensive numerical simulations on the ER network and BA network, we found that the growth pattern of the final behavior size $R(\infty)$ versus the hybrid ratio α exhibits discontinuous pattern when fixed transmission rate λ is large. But when λ is small, $R(\infty)$ shows the phenomenon of fluctuation, and at critical point, it reaches peak value first, followed with small amplitude declining and gradually rising. In addition, we also fixed the hybrid ratio α to analyze the final adoption size $R(\infty)$ changing with transmission rate λ, and the growth pattern of $R(\infty)$ changing from continuous to discontinuous is observed.

For comparing the effect of different hybrid methods, SIOT and DIOT are proposed, and the simulation result is presented; obviously, DIOT can spread faster especially when global transmission rate is high. We finally studied the effect of other parameters and found that memory threshold T, recovery rate γ, and global propagation range controller ϵ can affect $R(\infty)$ growing pattern, respectively; when T is small, it grows much faster because more seeds can be generated and global spreading can contribute more. With increasing γ , it gets slower to reach the burst value. Also, global range controller ϵ can change the pattern; when ϵ gets larger, it reaches critical value much faster. By introducing hybrid propagation mechanism and spreading scope controller, with memory character, the method can support modeling different spreading scenarios flexibly, but it simplifies the life states of bot, and the immune characteristics of nodes are not taken into account, so our future work will focus on these points.

Our proposed theory agrees well with the numerical simulations on ER and BA networks. The model proposed in this paper can provide theoretical reference for hybrid propagation modeling of botnet in complex networks and also provide guidance for medical industry to deal with botnet threats.

Data Availability

We conducted our experiment with the numerical simulation method, without using any open dataset.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

Acknowledgments

This study was financially supported in part by a program of National Natural Science Foundation of China (NSFC)

(grant nos. 61272447 and 61802271) and in part by the Fundamental Research Funds for the Central Universities (grant nos. SCU2018D018 and SCU2018D022). This support is gratefully acknowledged.

References

[1] M. Antonakakis, T. April, M. Bailey et al., "Understanding the mirai botnet," in *Proceedings of the 26th USENIX Security Symposium*, pp. 1093–1110, USENIX Security 17, Vancouver, BC, Canada, August 2017.

[2] C. Kolias, G. Kambourakis, A. Stavrou, and J. Voas, "Ddos in the IoT: mirai and other botnets," *Computer*, vol. 50, no. 7, pp. 80–84, 2017.

[3] D. Chen, N. Zhang, R. Lu, N. Cheng, K. Zhang, and Z. Qin, "Channel precoding based message authentication in wireless networks: challenges and solutions," *IEEE Network*, vol. 33, no. 1, pp. 99–105, 2019.

[4] D. Chen, N. Zhang, Z. Qin et al., "S2M: a lightweight acoustic fingerprints-based wireless device authentication protocol," *IEEE Internet of Things Journal*, vol. 4, no. 1, pp. 88–100, 2016.

[5] Q. Wang, D. Chen, N. Zhang, Z. Qin, and Z. Qin, "LACS: a lightweight label-based access control scheme in IoT-based 5G caching context," *IEEE Access*, vol. 5, pp. 4018–4027, 2017.

[6] K. Zhang, X. Liang, J. Ni, K. Yang, and X. S. Shen, "Exploiting social network to enhance human-to-human infection analysis without privacy leakage," *IEEE Transactions on Dependable and Secure Computing*, vol. 15, no. 4, pp. 607–620, 2016.

[7] C. Zhang, S. Zhou, J. C. Miller, I. J. Cox, and B. M. Chain, "Optimizing hybrid spreading in metapopulations," *Scientific Reports*, vol. 5, no. 1, p. 9924, 2015.

[8] R. M. Anderson, "Discussion: the Kermack-McKendrick epidemic threshold theorem," *Bulletin of Mathematical Biology*, vol. 53, no. 1-2, pp. 3–32, 1991.

[9] M. Newman, *Networks: An Introduction*, Oxford University Press, Oxford, UK, 2010.

[10] M. Feily, A. Shahrestani, and S. Ramadass, "A survey of botnet and botnet detection," in *Proceedings of the 2009 Third International Conference on Emerging Security Information, Systems and Technologies*, pp. 268–273, IEEE, Athens, Greece, June 2009.

[11] A. Laha, N. Zhang, H. Wu, D. Chen, and T. Han, "Online proactive caching in mobile edge computing using bidirectional deep recurrent neural network," *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 5520–5530, 2019.

[12] E. Bertino and N. Islam, "Botnets and internet of things security," *Computer*, vol. 50, no. 2, pp. 76–79, 2017.

[13] D. Chen, N. Zhang, N. Cheng, K. Zhang, Z. Qin, and X. S. Shen, "Physical layer based message authentication with secure channel codes," *IEEE Transactions on Dependable and Secure Computing*, p. 1, 2018.

[14] Q. Wang, D. Chen, N. Zhang, Z. Ding, and Z. Qin, "PCP: a privacy-preserving content-based publish-subscribe scheme with differential privacy in fog computing," *IEEE Access*, vol. 5, pp. 17962–17974, 2017.

[15] D. Acarali, M. Rajarajan, N. Komninos, and B. B. Zarpelão, "Modelling the spread of botnet malware in IoT-based wireless sensor networks," *Security and Communication Networks*, vol. 2019, Article ID 3745619, 13 pages, 2019.

[16] M. Ajelli, R. Lo Cigno, and A. Montresor, "Modeling botnets and epidemic malware," in *Proceedings of the 2010 IEEE International Conference on Communications*, pp. 1–5, IEEE, Cape Town, South Africa, May 2010.

[17] M. J. Farooq and Q. Zhu, "Modeling, analysis, and mitigation of dynamic botnet formation in wireless IoT networks," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 9, pp. 2412–2426, 2019.

[18] B. K. Mishra and D. K. Saini, "SEIRS epidemic model with delay for transmission of malicious objects in computer network," *Applied Mathematics and Computation*, vol. 188, no. 2, pp. 1476–1482, 2007.

[19] A. Singh, A. K. Awasthi, K. Singh, and P. K. Srivastava, "Modeling and analysis of worm propagation in wireless sensor networks," *Wireless Personal Communications*, vol. 98, no. 3, pp. 2535–2551, 2018.

[20] D. Dagon, C. C. Zou, and W. Lee, "Modeling botnet propagation using time zones," in *Proceedings of the NDSS Symposium 2006*, vol. 6, pp. 2–13, San Diego, CA, USA, February 2006.

[21] M. Todd Gardner, C. C. Beard, and M. Deep, "Using seirs epidemic models for IoT botnets attacks," in *Proceedings of the DRCN 2017—Design of Reliable Communication Networks*, pp. 1–8, Munich, Germany, March 2017.

[22] C. Castellano, S. Fortunato, and V. Loreto, "Statistical physics of social dynamics," *Reviews of Modern Physics*, vol. 81, no. 2, pp. 591–646, 2009.

[23] J. C. Flack and R. M. D'Souza, "The digital age and the future of social network science and engineering," *Proceedings of the IEEE*, vol. 102, no. 12, pp. 1873–1877, 2014.

[24] R. Pastor-Satorras, C. Castellano, P. Van Mieghem, and A. Vespignani, "Epidemic processes in complex networks," *Reviews of Modern Physics*, vol. 87, no. 3, pp. 925–979, 2015.

[25] V. Constantin Craciun, A. Mogage, and E. Simion, "Trends in design of ransomware viruses," in *International Conference on Security for Information Technology and Communications*, pp. 259–272, Springer, Berlin, Germany, 2018.

[26] S. Mohurle and M. Patil, "A brief study of wannacry threat: ransomware attack 2017," *International Journal of Advanced Research in Computer Science*, vol. 8, no. 5, 2017.

[27] A. Zimba, L. Simukonda, and M. Chishimba, "Demystifying ransomware attacks: reverse engineering and dynamic malware analysis of wannacry for network and information security," *Zambia ICT Journal*, vol. 1, no. 1, pp. 35–40, 2017.

[28] S. Aral and D. Walker, "Identifying influential and susceptible members of social networks," *Science*, vol. 337, no. 6092, pp. 337–341, 2012.

[29] A. Banerjee, A. G. Chandrasekhar, E. Duflo, and M. O. Jackson, "The diffusion of microfinance," *Science*, vol. 341, no. 6144, article 1236498, 2013.

[30] P. S. Dodds and D. J. Watts, "Universal behavior in a generalized model of contagion," *Physical Review Letters*, vol. 92, no. 21, article 218701, 2004.

[31] D. J. Watts, "A simple model of global cascades on random networks," *Proceedings of the National Academy of Sciences*, vol. 99, no. 9, pp. 5766–5771, 2002.

[32] P. S. Dodds and D. J. Watts, "A generalized model of social and biological contagion," *Journal of Theoretical Biology*, vol. 232, no. 4, pp. 587–604, 2005.

[33] W. Wang, X.-L. Chen, and L.-F. Zhong, "Social contagions with heterogeneous credibility," *Physica A: Statistical Mechanics and Its Applications*, vol. 503, pp. 604–610, 2018.

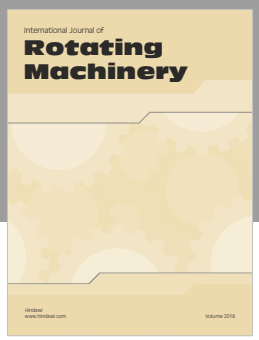
[34] J. C. Miller, "A note on a paper by Erik Volz: sir dynamics in random networks," *Journal of Mathematical Biology*, vol. 62, no. 3, pp. 349–358, 2011.

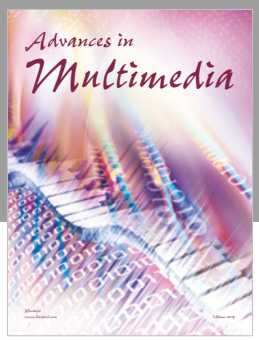
[35] W. Wang, M. Tang, P. Shu, and Z. Wang, "Dynamics of social contagions with heterogeneous adoption thresholds: crossover phenomena in phase transition," *New Journal of Physics*, vol. 18, no. 1, article 013029, 2016.

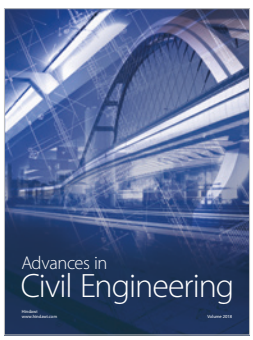
[36] W. Wang, M. Tang, H.-F. Zhang, H. Gao, Y. Do, and Z.-H. Liu, "Epidemic spreading on complex networks with general degree and weight distributions," *Physical Review E*, vol. 90, no. 4, article 042803, 2014.

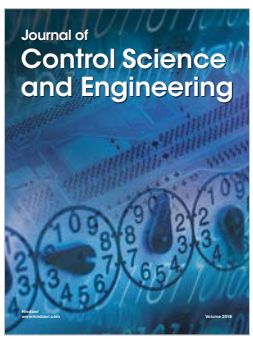
[37] P. Erdos and A. Rényi, "On random graphs I," *Publicationes Mathematicae Debrecen*, vol. 6, pp. 290–297, 1959.

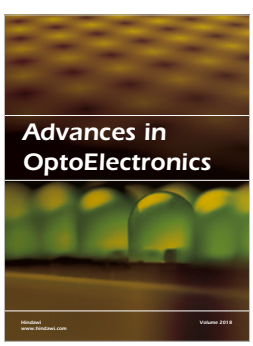
[38] A. Hagberg, D. Schult, P. Swart et al., *Networkx. High productivity software for complex networks*, Webová Strá Nka, 2013, https://networkx.lanl.gov/wiki.

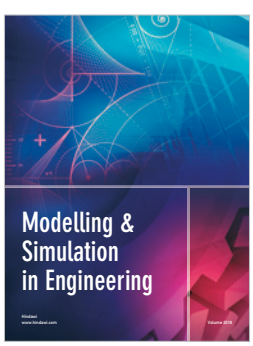


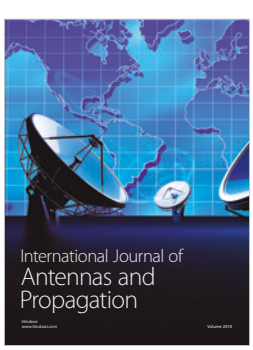


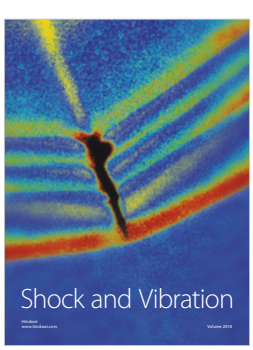


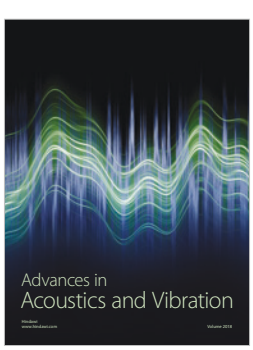












Hindawi

Submit your manuscripts at
www.hindawi.com