采用可交互信任值机制的病毒传播抑制策略

王刚，冯云，伍维甲，马润年
（空军工程大学信息与导航学院，710077，西安）

摘要：为了更加精准地抑制病毒传播，提出了采用可交互信任值机制的病毒传播抑制策略。改进了信任值模型，提出了可交互信任值机制，主要改进措施包括：①为便于数据处理和交互，采用离散信任值；②结合病毒传播免疫机理和直接信任模型，借鉴TCP拥塞控制算法，设计了直接信任值更新算法，实现了对感染信息的初步处理和信任值的恢复；③结合间接信任模型，借鉴RIP路由协议，设计了信任值交互算法，通过节点间共享信任值，实现对感染信息的进一步利用。提出了采用可交互信任值机制的病毒传播抑制策略：节点以信任值为依据判定自身所处安全环境，自主决定中断链路的范围；根据网络新增感染节点数量，自适应地调整信任阈值及不可信链路中断比例参数，实现了链路中断范围随网络安全动态调节。仿真结果表明：在所提参数条件下，通过信任值交互，漏检率下降6%以上，最低信任值处正确率提高了1倍，较高信任值处正确率基本不变，使得正确率关于信任值的曲线由上凸变为下凹，综合作用使得信任值较低处的不可信链路密度更高；在病毒防御过程中，所提策略中断链路比例的最高值仅为随机链路中断策略平均值的63%，不计感染节点清零后的部分，所提策略中断链路的总数为随机链路中断策略的21%。

关键词：病毒传播；抑制策略；信任值交互；动态调节
中图分类号：TP393 **文献标志码**：A
DOI：10.7652/xjtuxb202107005 **文章编号**：0253-987X(2021)07-0041-11

OSID码

Suppression Strategy Against Network Virus Propagation Based on Interactable Trust Value Mechanism

WANG Gang, FENG Yun, WU Weijia, MA Runnian
(Information and Navigation Institute, Air Force Engineering University, Xi'an 710077, China)

Abstract: To suppress virus propagation more accurately, a suppression strategy against virus propagation based on interactable trust value mechanism is proposed, and an interactable trust value mechanism is introduced to improve trust value model. The main improvement measures include: 1) To facilitate data processing and interaction, discrete trust value is adopted; 2) Combined with the immune mechanism of virus propagation and the direct trust model, the direct trust value update algorithm is designed via referencing to TCP congestion control algorithm, so the preliminary processing of infection information and the trust restoration are realized; 3) Following the indirect trust model and RIP routing protocol, a trust value interaction algorithm is designed to further utilize the infection information by sharing the trust value between nodes. Based on interactable trust value mechanism, a virus propagation suppression strategy is put forward, where the node determines its own safe environment based on the trust value and

收稿日期：2021-01-04。 作者简介：王刚(1976—)，男，教授。 基金项目：国家自然科学基金资助项目(61902426，61703420)。
网络出版时间：2021-03-09 网络出版地址：http://kns.cnki.net/kcms/detail/61.1069.T.20210308.1751.004.html

independently decides the range of interrupt link. According to the number of newly infected nodes in the network, the threshold of trust and the ratio of untrusted link interruptions are adjusted adaptively. The range of link interruptions is dynamically adjusted according to network security. Simulation results show that under the condition of parameters here, the interaction of trust values enables to lower miss rate by more than 60%, and heighten accuracy by 1 times at minimum trust value, but the accuracy remains unchanged at maximum trust value, which makes the trust value curve from convex to concave. It is found that unreliable link density is higher at low trust values, and in the process of virus defense, the maximum interrupted link ratio of the proposed strategy is only 63% of the average value of the random link interrupt strategy. The total number of the interrupted links of the proposed scheme is 21% of the random links interrupt strategy without considering the part after completely eliminating the infected nodes.

Keywords: virus propagation; suppression strategy; trust value interaction; dynamic adjustment

病毒往往能够在网络中传播,对用户构成潜在威胁。通过病毒源码解析的传统病毒防御方法在时间上和成本上处于不利地位[1-3],难以应对日益复杂的网络环境和变化多样的病毒攻击。对于可有效管控自身网络的企业、政府以及军队局域网,动态改变网络结构(如链路中断或节点隔离)能够抑制病毒在网络传播[4-7],但是网络结构变化会影响网络的业务承载,需要在安全和业务承载之间保持均衡,在达成网络安全的前提下,减少调整的不确定性和随机性,使得网络结构调整对网络业务的影响最小化。网络结构调整的难点主要表现在 2 个方面:一是调整的度难以把握,关于这一点,病毒传播研究[8-12]从理论上给出了网络中感染节点持续存在的阈值和可能的规模,理论上能够避免网络结构的过调整或欠调整;二是网络及节点状态信息不明确,在网络结构的调整过程中,难以做到针对感染目标的精准调整。对此,虽然无法在病毒被完全解析之前完全掌控网络感染情况,但是可借鉴信任模型[13-17]划定一个连接感染节点链路相对集中的范围,进而实施针对性调整。

信任模型主要根据目标对象的历史行为或者相关信息甄别不可信实体,大体上分为直接型和间接型两类。直接信任模型[13-15]利用网络实体间的历史行为实施信任度更新和可信实体的识别,然而现实网络实体所能接触的信息是有限的,单一实体很难直接甄别一些未对自身造成危害的恶意实体。间接信任模型[16-21]中的网络实体从其他实体处获取相关信息,从而获取对特定实体的信任程度,并通过用户间信息共享,实现了比直接信任模型更高效的恶意实体识别。总之,直接信任模型侧重实体间历史行为信息的收集和处理,间接信任模型强调实体间信任度的共享。在网络安全领域,可借鉴信任模型,探索病毒传播抑制问题,为抑制病毒传播提供信任值参考,从而形成科学可行的病毒传播抑制策略。

在网络病毒传播研究过程中,通常按照节点免疫能力和感染情况将节点分为不同状态,常见状态有易感状态 S、感染状态 I 和免疫状态 R[7,10-11]。一般而言,感染节点具备感染易感节点的能力,网络结构调整的出发点是减少两类节点间的连接,延缓携带病毒信息的传输,进而控制网络中感染节点的规模。在病毒传播过程中,节点间的感染行为一定程度上也标示了感染节点的位置。直接信任模型提供了根据历史感染行为信息调整信任度的思路,能够对有感染行为的节点进行标记。对于易感节点而言,由于在被感染前缺乏感染行为的历史信息,无法采用直接信任方式辨识周围节点状况,需要借鉴间接信任模式,从相邻节点处获取相关信息。

本文首先结合直接信任和间接信任理念,构建了信任值模型:考虑攻击溯源的复杂性,修改信任值下调机制;考虑计算复杂度和交互数据量,采用离散值表示信任值。其次,融合病毒传播免疫机理和信任共享理念,借鉴慢启动算法和路由交换算法,设计了直接信任值更新算法和信任值交互算法。再次,提出了采用可交互信任值机制的病毒传播抑制策略,以信任值为依据调整网络,根据感染情况反馈动态调整信任阈值和策略参数。最后,通过仿真实验:分析了信任值交互对正确率和漏检率的影响;以链路中断为例,验证了所提策略的有效性;对比随机链路中断策略,分析了所提策略在安全-网络结构方面的优越性。

1 可交互信任值机制

对于政府、企业等,其内部网络操作系统、软件

等基本一致，某类病毒只要能感染其中一台计算机，就可利用已经被感染的用户终端进行自我复制，并在网络中传播。一旦病毒对用户造成危害，用户能察觉到病毒的存在，并单方面地认为自身处于一个相对危险的网络环境中。这种情况下，为了保护自身，用户可以考虑降低对周围节点的信任等级，若后续相应节点未表现出感染行为则逐步恢复。通过感染行为调整自身信任值属于后发地被动信任调节，而通过信任共享，未被感染的节点能够根据相邻节点的信任信息先发地主动调整自身信任值。本文在直接信任模型和间接信任模型基础上，设计可交互信任值机制，实现更加高效地信任管理，协助节点判断安全环境，进而更加精准地抑制病毒传播。可交互信任值机制由 3 部分组成：一是信任值模型，以信任值为核心的可信链路判定以及信任值演化规则；二是信任值更新算法及交互算法，病毒传播过程中对历史感染行为和共享信任信息的处理算法；三是信任值评估标准，用于评估信任值的标记效果。

1.1　信任值模型

对病毒防御，黑白名单机制就是一种较为简单的信任模型，在反垃圾邮件、骚扰拦截以及病毒防御等领域得到了广泛的应用。对于政府、企业的内部网络，多数情况下，网络中的其他用户是可信的，而在病毒入侵时，又需要尽可能地将感染节点添加进黑名单，在其恢复后将其从黑名单中移除。考虑这种需求，仅依赖手动管理黑白名单是不现实的，需要建立一种使节点能够自主调控周围节点可信程度的信任管理机制。信任值机制[15,22-23]是一种采用信任值量化节点间信任程度的信任管理机制，这种机制能够根据网络中感染信息更新信任值，实现节点可信名单的动态调节。但是，这些信任值机制多是对感染信息的直接利用，属于直接信任模型。本文借鉴这些信任值机制，结合间接信任模型，主要从 3 个方面改进信任值机制，构建信任值模型：①在病毒被彻底解析之前，节点被感染后难以迅速准确溯源，应下调其所有相邻节点的信任值；②考虑计算复杂度和交互数据量，信任值采用离散值替代连续值；③充分利用节点间的信息交互，通过信任值交互改善信任值标记效果。

信任值模型如图 1 所示。信任值是节点对其自身周围节点的信任度量。首先，需要考虑信任值的存储问题。考虑网络病毒的传播对象为网络中断设备，一般不对集线器、交换机和路由器等中继设备造成危害，因此可将计算机网络抽象为有向图 $\boldsymbol{G}=\{\boldsymbol{V},\boldsymbol{E}\}$，其中：$\boldsymbol{V}=\{v_i \mid i=1,2,\cdots,N\}$，$v_i$ 表示图中节点 i，对应网络用户 i；$\boldsymbol{E}=\{(v_i,v_j) \mid i,j=1,2,\cdots,N$ 且 $i\neq j\}$，(v_i,v_j) 为有序节点对，是 v_i 到 v_j 的有向边，表示节点 i 和节点 j 之间存在逻辑连接。定义 $T_{i,j}(t)$ 为 t 时刻网络中用户 v_i 对 v_j 的信任值。若用户之间不存在逻辑连接，则信任值为 0，否则信任值初始状态下为 -1，表示最高信任等级。$T_{\min}$ 为最低信任值，对应的信任值矩阵可表示为

$$\boldsymbol{T}(t)=[T_{i,j}(t)],(v_j,v_i)\in\boldsymbol{E} \tag{1}$$

网络中每一个用户仅需存储和管理信任值矩阵中属于自身的部分（对于节点 v_i 而言，即为信任值矩阵的第 i 列的非 0 元素），由所有节点共同完成信任值矩阵的存储和维护。

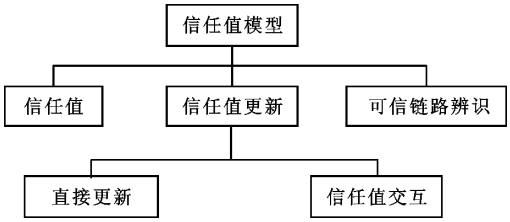


图 1　信任值模型

Fig. 1　Trust value model

信任值更新是网络运维的常态化行为，有直接更新和信任值交互两种方式。直接更新是指节点根据自身被感染情况更新信任值，若被感染则下调自身对周围所有节点的信任值，反之则逐步恢复信任值。信任值交互是指节点从相邻节点处获取其信任值，并据此修改自身信任值。具体的信任值更新和对应算法见 1.2 小节。

可信链路辨识指节点通过信任值对自身周围链路进行判定。引入信任阈值 T_{thro}。若 $T_{i,j}(t)\geqslant T_{\text{thro}}$，则表示节点 v_i 认定节点 v_j 为正常节点，相应链路为可信链路；反之，则节点 v_i 认定节点 v_j 为感染节点，相应链路为不可信链路。

1.2　信任值更新算法

信任值更新算法包括直接信任值更新算法和信任值交互算法。直接信任值更新算法利用历史感染行为对信任值进行更新。当 v_i 被感染后，将下调其所有相邻节点的信任值至最低；若该节点没有感染，则自动恢复其相邻节点信任值。

抑制病毒传播过程中，信任值的作用在于为节点提供判断周围安全环境的依据，以便节点实施恰当程度的防御。不同网络病毒的传播和感染能力各不相同，需要根据病毒实际感染能力采取不同的调整方案。因此，信任值恢复机制需要满足如下条件：

①恢复至信任状态的速度动态可调，病毒感染能力越强，则被标记为不可信链路、处于不可信状态的时间需要越长，使得被感染节点和防御方有时间进行免疫和防御；②网络环境较好时，能够相对快速地恢复至最高信任值处，以恢复网络正常运行。

综合考虑，借鉴 TCP 拥塞控制机制中的慢启动算法设计信任值的恢复算法。设置可动态调整的阈值 T_{thro}，若节点信任值小于该阈值则被认定为感染节点，否则被认定为正常节点。通过网络安全态势反馈调整信任阈值，实现恢复至信任状态的速度动态可调。信任值恢复分段控制：当信任值低于阈值时，信任值恢复较慢；当信任值高于阈值时，信任值恢复较快。在不影响不可信状态持续时间的前提下，实现在较好的网络安全环境下信任值快速恢复。由此，设计算法 1 为直接信任值更新算法。

算法 1 直接信任值更新算法

输入：上一时刻信任值矩阵 $\boldsymbol{T}(t-1)$，单位时间内被感染的节点集合 $\boldsymbol{N}_{\text{I}}$，阈值 T_{thro}，邻接矩阵 $\boldsymbol{A}$，最低信任值 $T_{\min}$。

输出：当前时刻信任值矩阵 $\boldsymbol{T}(t)$。

```
for i←1:N do
  for j in A[i,:]do
    if i in N_I then
      T_{i,j}(t)←T_min
    else if T_{i,j}(t−1)<T_thro
      then T_{i,j}(t)←T_{i,j}(t−1)+1
    else
      T_{i,j}(t)←⌈T_{i,j}(t−1)/2⌉
    end
  end
end
return T(t)
```

设网络节点的平均度为 k，若信任值集中维护，直接信任值更新算法更新一次需要遍历网络中所有链路。此时，直接信任值更新算法的时间复杂度约为 $O(Nk)$。信任值存储在网络所有节点上，网络节点仅需处理自身对其相邻节点的信任值，不需要管理和维护整个信任值矩阵。因此，在分布存储信任值情况下，直接信任值更新算法的时间复杂度为 $O(k)$。

网络节点按照信任值交互算法处理接受到的信任值信息。在信任值交互过程中，节点 v_i 发送自身信任值信息的格式为

$$\boldsymbol{T}_i=[I_i,I_1^{\text{A}},T_1^{\text{A}},I_2^{\text{A}},T_2^{\text{A}},\cdots,I_m^{\text{A}},T_m^{\text{A}}] \tag{2}$$

式中：I_i 表示节点 v_i 的编号（相应节点的辨识信息，可视为网络用户 IP 地址）；$(I_k^{\text{A}},T_k^{\text{A}})$ 表示节点 v_i 的一个相邻节点的编号和相应信任值，$k=1,2,\cdots,m$，m 为节点 v_i 相邻节点的数量。参考 RIP 协议中路由交互算法，设计算法 2 为信任值交互算法。

算法 2 信任值交互算法

输入：当前信任值矩阵 $\boldsymbol{T}(t)$，节点编号 v^{D}，接收到的信任值信息 $\boldsymbol{T}_i^{\text{A}}=[i^{\text{A}},I_1^{\text{A}},T_1^{\text{A}},I_2^{\text{A}},T_2^{\text{A}},\cdots,I_m^{\text{A}},T_m^{\text{A}}]$，

输出：交互后的信任值矩阵 $\boldsymbol{T}(t)$

```
T_v^D←T(t)[v^D,:]   获取当前节点的信任值
A_i←[I_1^A,I_2^A,⋯,I_m^A]   获取收到的信任值信息中的相邻节点编号
T_i^A←[T_1^A,T_2^A,⋯,T_m^A]   获取收到的信任值信息中的信任值
if all(T_i^A)=T_min   若节点 v_i 的所有信任值均为最低值，将其信任值降至最低
   then T_v^D[v^D]←T_min
end
for j←1:m do
  if T_v^D[A_i[j]]=0 then
    continue
  else
    T_v^D[A_i[j]]←⌊(T_v^D[A_i[j]]+T_i^A[i])/2⌋
  end
end
T(t)[v^D,:]←T_v^D
return T(t)
```

信任值交互算法的时间复杂度取决于接收到的相邻节点信任值信息量。对于节点平均度为 k 的网络，网络节点收到的相邻节点信任值信息包含 k 个节点信任值信息。因此，信任值交互算法的时间复杂度约为 $O(k)$，单个节点需要处理所有相邻节点发送的节点信任值信息，时间复杂度约为 $O(k^2)$。信任值在存储和交互过程中需要占用存储空间和带宽，平均信任值存储所需空间约为 $k(l_i+l_t)$ bit，其中 l_i 为节点 v_i 标识信息的长度，l_t 为信任值本身的长度。从网络节点层面分析，一个节点将自身信任值信息发送至所有相邻节点，发送的信息量约为 $k^2(l_i+l_t)$ bit，网络节点发送信息量之和为 $Nk^2(l_i+l_t)$ bit。通常，节点 v_i 发送给其相邻节点 v_j 的信任值信息包含 3 类：①v_j 自身信任值信息；②共同相邻节点的信任值信息；③其他新节点信任值信息。对于信任值接受方，只有第 2 类信息是有必要的，为减少信任值共享过程中带宽占用，考虑仅发送第 2 类

信任值信息。设某个节点的平均聚类系数为 c_{lu}，则该节点的相邻节点之间彼此链接概率为 c_{lu}，信息交互过程中所有节点需要发送的信息总量为 $Nk^2c_{\mathrm{lu}}\cdot(l_i+l_t)$ bit。在这种情况下，每个节点需要初步掌握相邻节点链接情况，可以在第一次信任值交互后进行反馈，信息接收方在反馈中告知信息发送方哪些信息是必要的，并在自身链接发生变化时再次进行反馈。

1.3　信任值评估标准

信任值用于网络中链路可信程度的标记，节点需要根据信任值判断自身所处的安全环境。因此，信任值标记效果很大程度上决定着最终防御效果。为此，参考文献[24-25]定义正确率 A 和漏检率 M

$$A=\frac{I_{\mathrm{I}}}{N_{\mathrm{I}}};\quad M=\frac{I_{\mathrm{A}}-I_{\mathrm{I}}}{I_{\mathrm{A}}} \tag{3}$$

式中：N_{I} 表示起点被标记为感染节点的链路数量；I_{I} 表示起点为感染节点且被标记的链路数量；I_{A} 为网络中实际起点为感染节点的链路数量；A 为正确率，表示不可信链路标记正确的比例；M 为漏检率，表示不可信链路中未被标记的比例。

对任一时刻 t，设未发生信任值交互时，网络中起点被标记为感染节点的链路数量为 $N_{\mathrm{I}}^0(t)$，起点为感染节点且被标记的链路数量为 $I_{\mathrm{I}}^0(t)$，网络中实际起点为感染节点的链路数量为 $I_{\mathrm{A}}(t)$，则 t 时刻的正确率 $A^0(t)$ 和漏检率 $M^0(t)$ 为

$$A^0(t)=\frac{I_{\mathrm{I}}^0(t)}{N_{\mathrm{I}}^0(t)};\quad M^0(t)=\frac{I_{\mathrm{A}}(t)-I_{\mathrm{I}}^0(t)}{I_{\mathrm{A}}(t)} \tag{4}$$

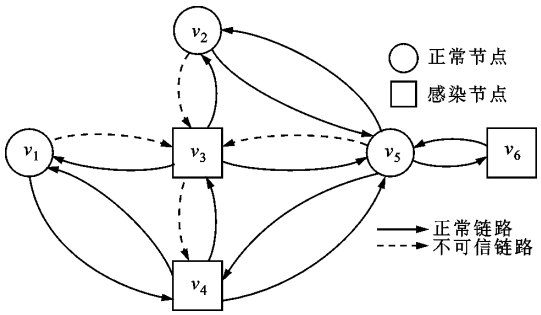
信任值交互后，由于信任值交互本身并不改变节点状态，因此实际起点为感染节点的链路数量不发生任何变化，仍为 $I_{\mathrm{A}}(t)$。通过信任值交互，未被感染的节点在两种情况下会降低自身周围链路信任值：①相邻节点所有信任值均为最低，判定该节点被感染，将来自该节点的链路信任值降至最低，这部分被标记的链路正确率为 1，设其数量为 $I_{\mathrm{N}}^0(t)$；②根据相邻节点的信任值，下调部分共有相邻节点的信任值，这一部分被标记链路的正确率取决于其相邻节点标记的正确率，设这部分节点数量为 $I_{\mathrm{N}}^1(t)$。因此，信任值交互后，t 时刻的正确率 $A^1(t)$ 和漏检率 $M^1(t)$ 为

$$\left.\begin{aligned}A^1(t)&=\frac{I_{\mathrm{I}}^0(t)+I_{\mathrm{N}}^0(t)+A^0(t)I_{\mathrm{N}}^1(t)}{N_{\mathrm{I}}^0(t)+I_{\mathrm{N}}^0(t)+I_{\mathrm{N}}^1(t)}\\M^1(t)&=\frac{I_{\mathrm{A}}(t)-[I_{\mathrm{I}}^0(t)+I_{\mathrm{N}}^0(t)+A^0(t)I_{\mathrm{N}}^1(t)]}{I_{\mathrm{A}}(t)}\end{aligned}\right\} \tag{5}$$

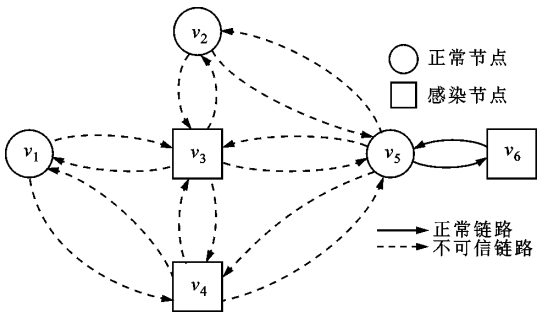
当 $I_{\mathrm{N}}^0(t)\geqslant 0$ 且 $I_{\mathrm{N}}^1(t)\geqslant 0$，$0\leqslant A^0(t)\leqslant 1$ 时，有

$$\left.\begin{aligned}A^1(t)&=\frac{I_{\mathrm{I}}^0(t)+I_{\mathrm{N}}^0(t)+A^0(t)I_{\mathrm{N}}^1(t)}{N_{\mathrm{I}}^0(t)+I_{\mathrm{N}}^0(t)+I_{\mathrm{N}}^1(t)}=\\&\frac{[N_{\mathrm{I}}^0(t)+I_{\mathrm{N}}^0(t)+I_{\mathrm{N}}^1(t)]A^0(t)}{N_{\mathrm{I}}^0(t)+I_{\mathrm{N}}^0(t)+I_{\mathrm{N}}^1(t)}+\\&\frac{[1-A^0(t)]I_{\mathrm{N}}^0(t)}{N_{\mathrm{I}}^0(t)+I_{\mathrm{N}}^0(t)+I_{\mathrm{N}}^1(t)}\geqslant A^0(t)\\M^1(t)&=\frac{I_{\mathrm{A}}(t)-[I_{\mathrm{I}}^0(t)+I_{\mathrm{N}}^0(t)+A^0(t)I_{\mathrm{N}}^1(t)]}{I_{\mathrm{A}}(t)}=\\&M^0(t)-\frac{I_{\mathrm{N}}^0(t)+A^0(t)I_{\mathrm{N}}^1(t)}{I_{\mathrm{A}}(t)}\leqslant M^0(t)\end{aligned}\right\} \tag{6}$$

图 2 是信任值交互前后网络中链路标记情况，在包含 6 个节点的小型网络中，节点 v_4 和 v_6 为感染节点，在通信过程中 v_3 被 v_4 感染，同样转化为感染节点。



(a)交互前



(b)交互后

图 2　信任值交互前后网络中链路标记情况

Fig. 2　Link marking before and after trust value interaction

从图 2a 可以看出，按照直接信任值更新算法，v_3 将所有相邻节点到其自身的链路信任值下调，相应链路被标记为不可信链路。从图 2b 可以看出，通过信任值交互，v_3 的所有相邻节点根据其提供的信任值信息判定 v_3 为感染节点，将相应链路信任值下调，标记为不可信链路。节点 v_2、v_4 和 v_5 根据节点 v_3 的信任值信息判定其与节点共同的 v_3 相邻节点为感染节点，将相应链路信任值下调，标记为不可信链路。按照式(3)：图 2a 中正确率为 0.25，漏检率约为 0.85；图 2b 中正确率为 0.5，漏漏检率约为

0.14。对比分析图 2a 和 2b 可知，通过信任值交互，网络将更多的链路标记为不可信链路。这些不可信链路中包含两大部分：一部分($I_N^0(t)$)是被感染节点的相邻节点之间的链路，由被感染节点的相邻节点根据被感染节点的信任值信息直接判定，判定的正确性由信息源头判定的准确性决定，这部分新增不可信链路的正确率为 0.33；另一部分($I_N^1(t)$)则是被感染节点的相邻节点根据被感染节点的信任值信息对被感染节点进行的判定，这种判定在节点公布正确信任值的前提下是准确的，这部分新增链路的正确率为 1。综合分析可知，通过信任值交互，网络中更多链接感染节点的链路被标记，I_1 增大，而链接感染节点的链路总数 I_A 不变。因此，漏检率下降。正确率部分，$I_N^0(t)$(新增不可信链路的正确率)与信息源头节点标记不可信链路的正确率相当，而$I_N^1(t)$(标记的不可信链路)则绝对准确，二者共同作用下表现出正确率的提升。

结合式(3)～(6)及图 2 分析可得，信任值能够有效提升信任值标记的正确率并降低漏检率，提升信任值标记效果。具体表现为以下两个方面：①直接信任值更新仅能通过相邻节点对自身感染行为评估周围信任值，通过信任值交互，则能使未被感染的节点从被感染的节点处获取感染信息；②节点信任值一方面反映了自身对周围节点的信任程度，同时也反映了自身状态，当节点被感染后下调其所有信任值至最低，相邻节点一旦接受到类似状态的信任值信息，即可精准判断该节点被感染。相对应地，这种信任值交互虽然能够提升标记效果，但需要网络中绝大部分节点客观上可信，不存在恶意发送虚假信任值信息的行为。

2 病毒传播抑制策略

在病毒传播过程中，可交互信任值机制给定了所有链路信任值，用于标记节点之间的信任程度。节点可根据信任值评估自身周围安全环境，为精确有效抑制病毒传播提供依据。本节给出采用可交互信任值机制的病毒传播抑制策略，流程如图 3 所示。

管理员根据当前网络中的感染状况对感染参数进行粗略估计，根据预估的参数值，计算采取相应病毒传播抑制策略的阈值。设置信任值相关参数。用户向管理员反馈感染状况(新增感染节点数量)，管理员根据反馈信息估计当前网络安全等级并进行针对性调整，网络安全等级具体表现为信任阈值 T_{thro} 和策略参数，可按照如下规则调整：①安全等级提

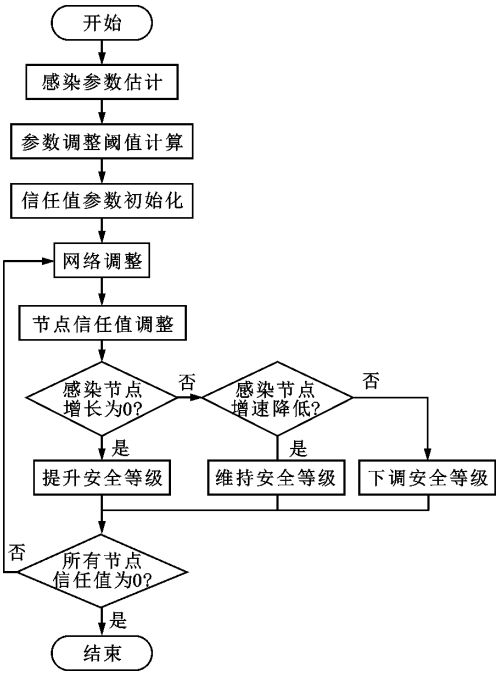
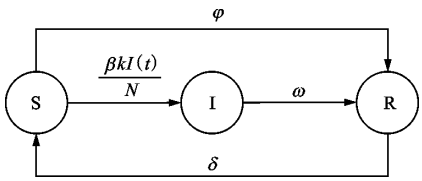


图 3 网络病毒传播抑制流程

Fig. 3 Virus propagation suppression process

升，网络中不再出现感染节点，可以初步认定网络达到安全状态，T_{thro} 下降；②安全等级下降，根据反馈信息，网络中感染节点保持增长或数量维持不变，当前参数下不足以完全消除病毒，T_{thro} 上调，当 T_{thro} 上调至最大仍然不足以消除病毒时，可考虑调整策略参数，加大调整程度；③维持安全等级，尽管仍然有新增感染节点出现，但总体上感染节点规模开始下降，可保持参数不变。

以链路中断为例，参考文献[7,26]所构建的 SIRS 病毒传播模型描述网络中病毒传播情况，构建节点状态转化关系，如图 4 所示。



S、I、R—易感状态、感染状态和免疫状态；β—接触感染概率；ω、δ、φ—相应状态之间的转化概率。

图 4 SIRS 模型节点状态转移图

Fig. 4 Node state transition diagram of SIRS model

图 4 对应的微分方程为

$$\left.\begin{aligned}\frac{\mathrm{d}S(t)}{\mathrm{d}t}&=-\varphi S(t)-\frac{\beta k S(t)I(t)}{N}+\delta R(t)\\ \frac{\mathrm{d}I(t)}{\mathrm{d}t}&=\frac{\beta k S(t)I(t)}{N}-\omega I(t)\\ \frac{\mathrm{d}R(t)}{\mathrm{d}t}&=\varphi S(t)+\omega I(t)-\delta R(t)\end{aligned}\right\}\quad(7)$$

式中 $S(t)$、$I(t)$、$R(t)$分别为 t 时刻 S、I、R 状态的节点数。

根据文献[7,26]中的稳定性分析可知，网络能够依靠自身免疫能力消除病毒的前提是平均度需满足

$$k < \frac{(\varphi+\delta)\omega}{\beta\delta} \tag{8}$$

当 $k>\frac{(\varphi+\delta)\omega}{\beta\delta}$时，需要中断部分链路降低平均度。设策略参数(链路中断比例)为 p，则 p 需满足

$$p \geqslant 1-\frac{(\varphi+\delta)\omega}{\beta\delta k} \tag{9}$$

在抑制病毒传播过程中，仅需断开被标记为不可信的链路。结合图 3 及本节分析，可根据网络感染情况反馈，按照一定的规则调整信任阈值以及策略参数，即

$$\left.\begin{aligned} &T_{\text{thro}} = \\ &\begin{cases} \lfloor T_{\text{thro}}/2 \rfloor, & I_{\text{new}}^{\text{now}} > I_{\text{new}}^{\text{before}} \\ T_{\text{thro}}, & I_{\text{new}}^{\text{now}} < I_{\text{new}}^{\text{before}} \\ \lfloor (T_{\text{thro}}+T_{\min})/2 \rfloor, & I_{\text{new}}^{\text{now}} = 0 \end{cases} \\ &p = \\ &\begin{cases} \min(p+0.001,1), & T_{\text{thro}} = -1 \,\&\, I_{\text{new}}^{\text{now}} > I_{\text{new}}^{\text{before}} \\ p, & \text{其他} \end{cases} \end{aligned}\right\} \tag{10}$$

式中：$I_{\text{new}}^{\text{now}}$表示当前时段的平均新增感染节点数量；$I_{\text{new}}^{\text{before}}$表示上一时段平均新增感染节点数量。为了避免病毒传播过程中由于节点被感染的随机性引发对网络安全环境的误判，可视实际情况设定单位时间段，根据单位时间段内新增感染节点数量，判断网络安全环境的变化。

3　仿真分析

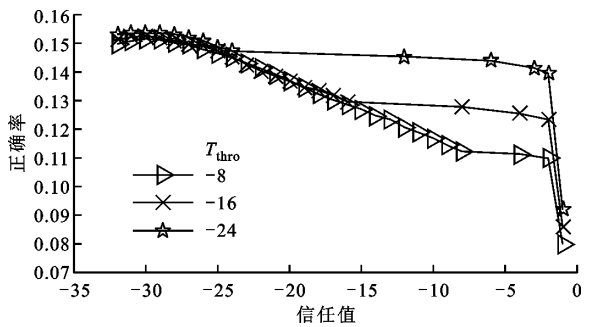
仿真过程中，SIRS 模型部分参数设置[7]如下：$T_{\min}=-32$，$k=16$，$N=2\,000$，$\delta=0.1$，$\omega=0.08$，$\varphi=0.2$，时间单位为 h，初始值设定为$(S(0),I(0),R(0))=(1\,800,200,0)$。当 $\beta<0.015$ 时，$R_0<1$，网络在无病毒平衡点处稳定；当 $\beta>0.015$ 时，$R_0>1$，网络在有病毒平衡点处稳定。若采用 IP 地址作为节点标识，网络节点存储信任值信息平均占用空间约为 608 bit，在内网环境下，如果系统管理员为每一个用户设定编号，则仅需 288 bit 存储空间。

3.1　实验环境

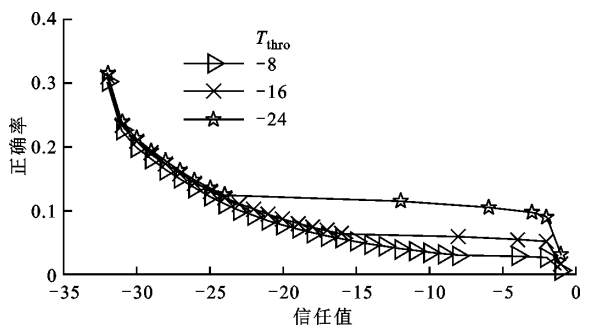
病毒传播需要依赖网络中的信息流，病毒传播网络实际上是人的社交网络在计算机网络中的映射，因此本文在能够反映社交网络的小世界网络中进行仿真实验。具体步骤如下：①采用 python 的 networkx 复杂网络工具，生成节点数为2 000、平均度为 16 的小世界网络，其重连概率为 0.3；②在随机生成的小世界网络中，按照图 4 所示状态转化关系模拟网络中病毒的传播情况，记录病毒传播过程中的感染情况及节点数量变化；③采用 matlab 求解式(7)微分方程，将其结果用与步骤②中模拟的病毒传播情况对比；④为生成的小世界网络中的每一个节点建立信任值管理表(本文采用信任值矩阵来存储信任关系)，根据步骤②中记录的信息，实时更新信任矩阵中的信任值。

3.2　正确率及漏检率

本小节实验在 $\beta=0.02$ 时进行。无信任值交互和有信任值交互时不同信任值处的正确率如图 5 所示。可以看出：无论有无信任值交互，信任值越低处正确率越高，原因是信任值恢复过程中，部分被标记的染节点的免疫，正确率也就随之降低；可交互信任值机制在较低信任值处正确率较高，可达到无信任值交互时的 2 倍，在信任值较高处低于无信任值交互时的正确率；正确率随信任值的曲线由上凸变为下凹，表明通过信任值交互，不可信链路在信任值较低处更加集中。



(a)无信任值交互

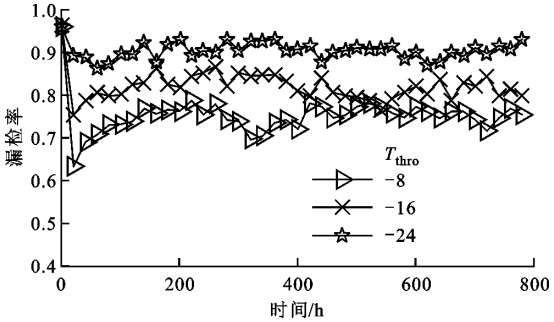


(b)有信任值交互

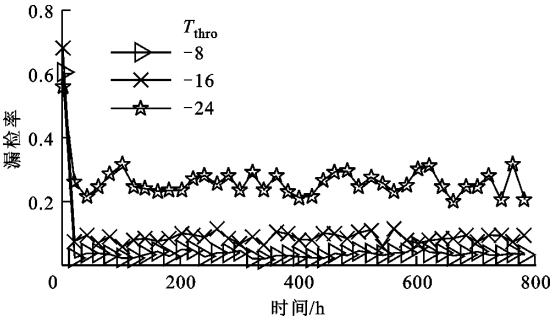
图 5　不同信任值处的正确率

Fig. 5　Accuracy at different trust values

漏检率如图 6 所示。可以看出，信任阈值为 −8、−16 和 −24 时，可交互信任值机制的漏检率分别下降了约 0.72、0.7 和 0.6。这表明通过信任值交互标记了更多的不可信链路，不可信链路在信任值较低处的占比更大。



(a)无信任值交互



(b)有信任值交互

图 6 漏检率统计结果

Fig. 6 Statistical results of miss rate

不可信状态下的链路比例如表 1 所示。

表 1 不可信状态下的链路比例

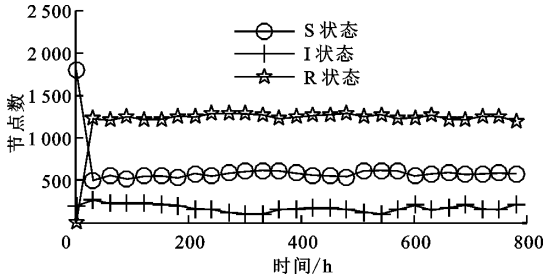
Table 1 Link ratio in untrusted state

T_{thro}	不可信状态下的链路比例	
	信任值机制	可交互信任值机制
−8	0.164 6	0.615 9
−16	0.116 3	0.558 4
−24	0.061 3	0.386 5

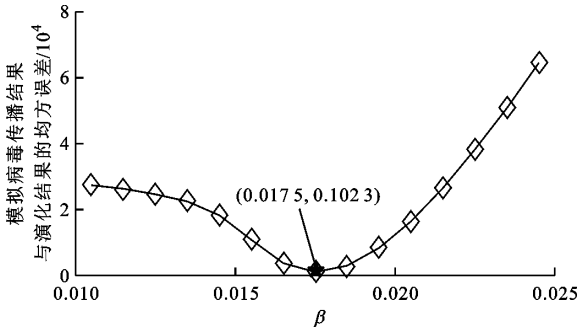
结合表 1、图 5 和图 6 分析可知，通过信任值交互，更多链路被标记为不可信链路，不可信范围扩大，信任值交互加大了不可信范围内真实不可信链路的密度，能为抑制病毒传播提供更有益的参考。

3.3 有效性

以链路中断为例，验证采用可交互信任值机制的病毒传播抑制策略的有效性，结果如图 7 所示。可以看出，当 $\beta=0.175$ 时，模拟病毒传播结果与模型演化结果的均方误差最小。



(a)$\beta=0.02$ 时的模拟病毒传播情况



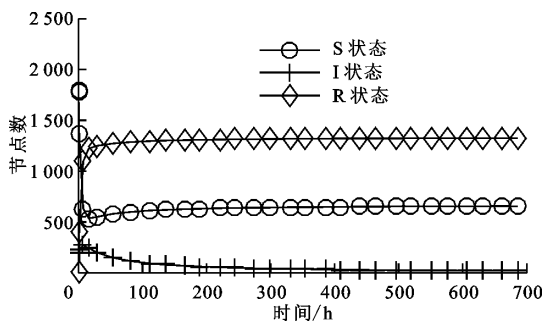
(b)均方误差曲线

图 7 模拟病毒传播情况及其和模型演化结果的均方误差

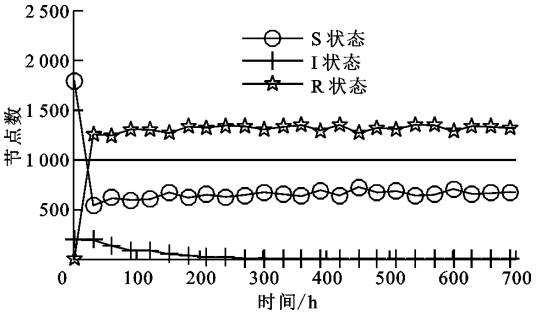
Fig. 7 Simulation of virus transmission and mean square error between simulation and model evolution results

根据文献[7,24]，当 $\beta=0.175$ 时，网络稳定在有病毒平衡点 P_1(569.5,162.1,1 268.4)处，与模拟病毒传播情况基本一致。由式(8)(9)可知，当 $k\leqslant 13.714$ 时，能达到无病毒状态。设置初始参数为 $T_{thro}=-24$，$p=22.8\%$，新增感染节点统计的时间段设置为 20 个单位时间。模型演化结果和模拟病毒传播情况如图 8 所示，策略执行过程中的参数变化情况如图 9 所示。

由图 8 可知，所提策略能有效抑制网络中病毒传播。由图 9a 和图 8b 可知，信任阈值的变化符合网络中感染节点数量的变化：当网络中感染节点数量上升时，上调信任阈值，扩大链路中断可执行范围；当感染节点清零后，信任阈值及时恢复，使网络恢复正常状态。由图 9b 可知，当信任阈值调整至最



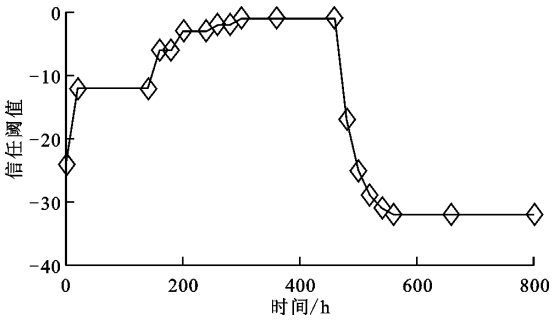
(a)模型演化结果



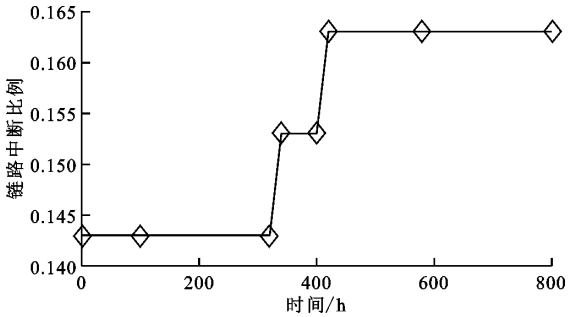
(b)模拟病毒传播情况

图 8　$p=22.8\%$时的模型演化结果和模拟病毒传播情况

Fig. 8　Model evolution and simulation results of virus transmission when $p=22.8\%$



(a)信任阈值



(b)不可信链路中断比例

图 9　所提策略执行过程中的参数变化曲线

Fig. 9　Parameter change curves during implementation of the proposed strategy

高仍然无法彻底消除病毒时，网络能够进一步地通过调整策略参数(不可信链路中断比例)消除病毒。

本小节分析表明，采用可交互信任值机制的病毒传播抑制策略在执行过程中能够利用网络中的感染信息(新增感染节点数量)对网络安全环境进行评估，进而针对性地调整相关参数，实现彻底抑制病毒传播。

3.4　安全性与对网络结构的影响

采取同 3.3 小节相同的参数配置，在随机链路中断策略下，模拟病毒传播情况如图 10 所示。

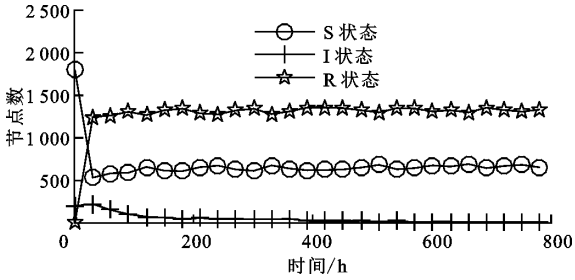


图 10　随机链路中断策略下的模拟病毒传播情况

Fig. 10　Simulation for virus propagation under random link interrupt strategy

与图 8b 对比分析感染节点数量变化趋势可知，采用可交互信任值机制的病毒传播抑制策略能够确保网络安全，并且能通过信任阈值和链路中断比例的调整加速网络消除感染节点的速度。

可交互信任值机制的主要目的在于为病毒传播抑制策略的实施提供依据，以便实施更加精准的隔离。链路是网络中通信业务的载体，链路中断在提升网络安全性的同时会影响网络通信能力，因此应对比随机链路中断策略和采用可交互信任值机制的链路中断策略在实施过程中断开链路的数量，图 11 为二者执行过程中的链路中断比例。可以看出，本文策略最高链路中断比例仅为随机链路中断策略中断链路比例均值的 63%，不计感染节点清零后的阶段，病毒防御过程中，本文策略中断链路数量仅为随机链路中断策略的 21%。因此，采用可交互信任值机制的随机链路中断策略较随机链路中断策略对网络结构的改变更小。

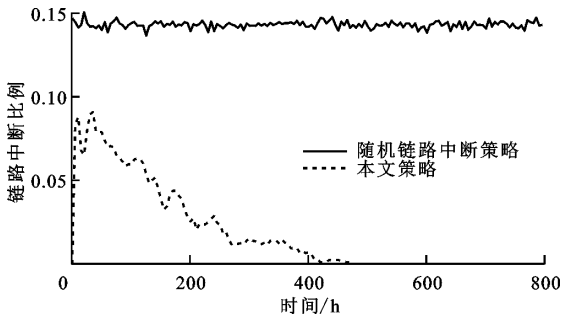


图 11　不同策略执行过程中的链路中断比例

Fig. 11　Comparison of the proportion of link interruptions during execution of different strategies

对比图 8b、图 9 和图 11 可知，本文策略在执行过程中的链路中断比例和网络中感染节点的数量以及信任阈值变化趋势在一定程度上吻合。随着感染节点的减少，信任阈值和链路中断比例逐渐提高，但链路中断比例却不断下降，这是因为随着感染节点

和感染行为的减少，总体上连接感染节点的链路和被标记为不可信任的链路也随之减少，并且随着网络彻底消除病毒，信任阈值下调，网络也逐渐恢复至正常状态。这表明可交互信任值机制能为病毒传播策略的执行提供有效参考，并且可根据网络中的具体安全环境调整参数，降低链路中断过程中的随机性，在提升安全性的同时降低对网络结构的影响。

4 结 论

根据网络病毒传播和免疫特点，提出了可交互信任值机制，设计了新的病毒传播抑制策略，并以随机链路中断为例，开展了仿真验证。本文所提可交互信任值机制通过网络中感染信息的收集处理和共享，为网络中节点判断安全环境提供了有力依据，实现了更加有效的防御。本文主要结论如下。

(1)相比传统的信任值机制，可交互信任值机制通过信任值共享，提高了网络中链路标记的效果，具体表现为信任值较低处正确率提高、整体漏检率下降，使得信任值较低处的不可信链路密度更大。

(2)在病毒防御过程中，仅对低于信任值阈值的链路采取隔离中断等措施能够有效抑制病毒传播。这表明在病毒传播过程中，感染节点并非完全均匀分布，不同节点所处安全环境有所差异，具体表现为不同节点周围感染节点数量不同。

(3)采用可交互信任值机制的病毒防御过程中，通过动态调整信任阈值及不可信链路隔离比例等参数可实现防御范围的动态调整。

在后续工作中，将针对节点发布信息的可信度等因素，考虑引入相邻节点可信因子对可交互信任值机制进行进一步优化。

参考文献：

[1] SHENG Zhao, HAN Huishan, KUI Shixue. Research on computer network virus defense technology in cloud technology environment [J]. International Journal of Security and Its Applications, 2016, 10(3): 449-460.

[2] SULTANA N, CHILAMKURTI N, PENG Wei, et al. Survey on SDN based network intrusion detection system using machine learning approaches [J]. Peer-to-Peer Networking and Applications, 2019, 12(2): 493-501.

[3] ALI M Q, AL-SHAER E, SAMAK T. Firewall policy reconnaissance: techniques and analysis [J]. IEEE Transactions on Information Forensics and Security, 2014, 9(2): 296-308.

[4] CAI Jun, WANG Yu, LIU Yan, et al. Enhancing network capacity by weakening community structure in scale-free network [J]. Future Generation Computer Systems, 2018, 87: 765-771.

[5] CAI Jun, LUO Jianzhen, LIU Yan, et al. A network community restructuring mechanism for transport efficiency improvement in scale-free complex networks [J]. Concurrency and Computation: Practice and Experience, 2018, 30(5): e4273.

[6] 田思，李慧嘉，赵岳. 复杂网络中的弱化免疫策略分析 [J]. 计算机应用，2012，32(9)：2620-2623.
TIAN Si, LI Huijia, ZHAO Yue. Analysis of weakened immunization strategy on complex network [J]. Journal of Computer Applications, 2012, 32(9): 2620-2623.

[7] 王刚，冯云，陆世伟，等. 多操作系统异构网络的病毒传播模型和安全性能优化策略 [J]. 电子与信息学报，2020，42(4)：972-980.
WANG Gang, FENG Yun, LU Shiwei, et al. Virus propagation model and security performance optimization strategy of multi-operating system heterogeneous network [J]. Journal of Electronics & Information Technology, 2020, 42(4): 972-980.

[8] 刘烃，郑庆华，管晓宏，等. IPv6 网络中蠕虫传播模型及分析 [J]. 计算机学报，2006(8)：1337-1345.
LIU Ting, ZHENG Qinghua, GUAN Xiaohong, et al. Modeling and analysis of worm propagation in IPv6 networks [J]. Chinese Journal of Computers, 2006(8): 1337-1345.

[9] 苏飞，林昭文，马严，等. IPv6 网络环境下的蠕虫传播模型研究 [J]. 通信学报，2011，32(9)：51-60.
SU Fei, LIN Zhaowen, MA Yan, et al. Research on worm propagation model in IPv6 networks [J]. Journal on Communications, 2011, 32(9): 51-60.

[10] ZHOU Tao, LIU Jianguo, BAI Wenjie, et al. Behaviors of susceptible-infected epidemics on scale-free networks with identical infectivity [J]. Physical Review: E Statistical, Nonlinear, and Soft Matter Physics, 2006, 74: 056109.

[11] ZHU Linhe, GUAN Gui, LI Yimin. Nonlinear dynamical analysis and control strategies of a network-based SIS epidemic model with time delay [J]. Applied Mathematical Modelling, 2019, 70: 512-531.

[12] EL-SAYED A M A, ARAFA A A M, KHALI M, et al. A mathematical model with memory for propagation of computer virus under human intervention [J]. Progress in Fractional Differentiation and Applications, 2016, 2(2): 105-113.

[13] KIM Y A，PHALAK R. A trust prediction framework in rating-based experience sharing social networks without a Web of Trust [J]. Information Sciences，2012，191：128-145.

[14] JØSANG A，ISMAIL R，BOYD C. A survey of trust and reputation systems for online service provision [J]. Decision Support Systems，2007，43(2)：618-644.

[15] WANG Gang，LU Shiwei，FENG Yun，et al. A method to improve the security of information diffusion in complex networks：node trust-value management mechanism [J]. IEEE Access，2019，7：138175-138191.

[16] 滕婕，夏志杰，罗梦莹，等. 基于 Multi-Agent 的网络谣言传播事件中信息主体信任识别研究 [J]. 情报杂志，2020，39(3)：105-114.
TENG Jie，XIA Zhijie，LUO Mengying，et al. Research on trust recognition of information subject in network rumor propagation event based on Multi-Agent [J]. Journal of Intelligence，2020，39(3)：105-114.

[17] TANG Jinchuan，CHEN Gaojie，COON J P. Route selection based on connectivity-delay-trust in public safety networks [J]. IEEE Systems Journal，2019，13(2)：1558-1567.

[18] 夏辉，张三顺，孙运传，等. 车载自组网中基于信任管理的安全组播协议设计 [J]. 计算机学报，2019，42(5)：961-979.
XIA Hui，ZHANG Sanshun，SUN Yunchuan，et al. Design of trust-based secure multicast routing protocol in VANETs [J]. Chinese Journal of Computers，2019，42(5)：961-979.

[19] 李本霞，夏辉，张三顺. 一种基于信任的组播路由协议 [J]. 信息网络安全，2019(1)：59-67.
LI Benxia，XIA Hui，ZHANG Sanshun. A trust-based multicast routing protocol [J]. Netinfo Security，2019(1)：59-67.

[20] 曹洁，曾国荪，姜火文，等. 云环境下服务信任感知的可信动态级调度方法 [J]. 通信学报，2014，35(11)：39-49.
CAO Jie，ZENG Guosun，JIANG Huowen，et al. Trust-aware dynamic level scheduling algorithm in cloud environment [J]. Journal on Communications，2014，35(11)：39-49.

[21] 李美子，黄震华，向阳，等. 社交网络中基于信任评估的推荐控制模型 [J]. 同济大学学报(自然科学版)，2014，42(7)：1117-1122.
LI Meizi，HUANG Zhenhua，XIANG Yang，et al. Trust evaluation-based recommendation control model in social network site [J]. Journal of Tongji University (Natural Science)，2014，42(7)：1117-1122.

[22] ZHANG Guangxue，WANG Tian，WANG Guojun，et al. Detection of hidden data attacks combined fog computing and trust evaluation method in sensor-cloud system [J]. Concurrency and Computation：Practice and Experience，2018：e5109.

[23] LIU Yuxin，DONG Mianxiong，OTA K，et al. ActiveTrust：secure and trustable routing in wireless sensor networks [J]. IEEE Transactions on Information Forensics and Security，2016，11(9)：2013-2027.

[24] SHANG Keke，LI Tongchen，SMALL M，et al. Link prediction for tree-like networks [J]. Chaos，2019，29(6)：061103.

[25] SHANG Keke，SMALL M，YAN Weisheng. Fitness networks for real world systems via modified preferential attachment [J]. Physica：A Statistical Mechanics and Its Applications，2017，474：49-60.

[26] 顾海俊，蒋国平，夏玲玲. 基于状态概率转移的 SIRS 病毒传播模型及其临界值分析 [J]. 计算机科学，2016，43(S1)：64-67.
GU Haijun，JIANG Guoping，XIA Lingling. SIRS epidemic model and its threshold based on state transition probability [J]. Computer Science，2016，43(S1)：64-67.

（编辑　陶晴）