基于形式化逻辑矩阵的结构化P2P蠕虫对抗模型

唐浩坤[1] 刘宴兵[2] 黄 俊[2] 张 衡[3]
(电子科技大学计算机科学与工程学院 成都 610054)[1] (重庆邮电大学通信与信息工程学院 重庆 400065)[2]
(西南大学计算机与信息科学学院 重庆 400715)[3]

摘 要 良性蠕虫对抗恶性蠕虫是结构化P2P环境下应对蠕虫攻击的有效手段之一,但是已有模型对对抗环境下蠕虫传播过程的描述过于复杂。针对这个问题,提出一种简单的结构化P2P蠕虫对抗模型。该模型利用逻辑矩阵对结构化P2P网络中恶性蠕虫与良性蠕虫的对抗传播过程进行形式化描述,借助模型可以快速地推导出对抗环境下影响恶性P2P蠕虫传播效率的关键因素。此外考虑到P2P节点搅动特征对蠕虫传播的重大影响,将节点变化率引入到模型中,以提高模型的准确性。实验表明,借助形式化逻辑矩阵能有效地降低对抗环境下蠕虫传播模型的复杂度,快速地发现制约蠕虫传播的关键因素,为后续的蠕虫防御提供指导。

关键词 结构化P2P网络,逻辑矩阵,蠕虫对抗,节点搅动
中图法分类号 TP309 **文献标识码** A

Structured P2P Worm-anti-worm Model Based on Formalized Logic Matrix

TANG Hao-kun[1] LIU Yan-bing[2] HUANG Jun[2] ZHANG Heng[3]
(School of Computer Science & Engineering, University of Electronic Science and Technology of China, Chengdu 610054, China)[1]
(School of Communication and Information Engineering, Chongqing University of Posts and Telecommunications, Chongqing 400065, China)[2]
(School of Computer and Information Science, Southwest University, Chongqing 400715, China)[3]

Abstract P2P anti-worms is one of the effective countermeasure to malignant worms in structured P2P networks, but the existing models are too complex in describing the propagation processes of worms under attack-defense environment. To address this problem, a simple structured P2P worm-anti-worm model was presented. This model performs the form description to the antagonistic propagation of P2P anti-worms and malignant worms in structured P2P networks by the support of logic matrix, and a number of key parameters that affect the propagation speed of malignant worm under attack-defense environment can be deduced rapidly by the model, besides, considering the significant influence of P2P churn feature on worm propagation, the change rate of nodes is added to the model to improve its accuracy. The experimental results show that formalized logic matrix can reduce the complexity of worm propagation model under attack-defense environment, rapidly identify the key factors that restrict the spread of worms, and supply the reference for the following research work on defending worms.

Keywords Structured P2P network, Logic matrix, Worm-anti-worm, P2P churn

1 引言

近年来,代表着互联网产业未来发展方向的P2P网络[1]在资源共享、即时通信、企业协同以及在线视频等多个领域得到广泛应用,占据着当前网络流量的主流。P2P网络在给人们带来方便共享、快速路由的同时,也为蠕虫进行隐匿扫描和快速传播大开方便之门,尤其是为借助层叠网拓扑结构进行传播的P2P蠕虫提供了良好的扩散平台。

P2P蠕虫的概念最早是在2005年的国际网络安全会议上被提出的,它被定义为一个利用P2P网络作为生存环境、借助P2P网络的特性进行传播的新型蠕虫[2]。相比于采用随机扫描策略的传统蠕虫,P2P蠕虫因不会扫描无效IP地址而被更加迅速地传播;因不会产生较高的链接失败率而更难被检测;因传播流量可融入到正常流量中而更具隐蔽性。其实它早在被正式定义前,就已经被开发并释放到网络中,并已给人们带来了极大的经济损失[3]。例如2003年的Slapper蠕虫就是一种典型的P2P蠕虫,其复杂性和多变性在文献[4]中有详细的论证,在此不再赘言。为了控制P2P蠕虫在网络中的传播,人们提出一种利用良性蠕虫对抗恶性蠕虫的抑制策略,构建了在此策略下的P2P蠕虫传播模型,评估了影响P2P蠕虫传播速度的关键因素。

鉴于目前还没有一种简单实用的工具,专门针对这种对

到稿日期:2012-07-26 返修日期:2013-03-05 本文受"新一代宽带无线移动通信网"国家科技重大专项课题(2011ZX03002-004-03),重庆市高等教育成果转化项目(Kjzh10206),公安部信息网络安全重点实验室项目(C11609)资助。
唐浩坤(1977—),男,博士生,主要研究方向为网络安全、P2P网络应用,E-mail:tanghk@cqupt.edu.cn;刘宴兵(1971—),男,教授,博士生导师,主要研究方向为网络安全、网格计算。

抗环境下结构化 P2P 蠕虫的传播过程进行描述。本文在充分考虑 P2P 节点搅动特征的前提下，创新性地利用形式化逻辑矩阵来解决这一问题，建立了基于离散时间的结构化 P2P 蠕虫对抗模型，并将对抗模型中的传播过程映射成一系列的逻辑矩阵操作，最后通过数值模拟证明了利用形式化逻辑矩阵描述结构化 P2P 蠕虫对抗模型的有效性，推导出对抗环境下影响恶性蠕虫传播效率的关键因素，评估了良性蠕虫对抗恶性蠕虫的效果。

本文第 2 节分析相关工作；第 3 节给出逻辑矩阵的形式化定义；第 4 节在第 3 节的基础上构建基于逻辑矩阵的结构化 P2P 蠕虫对抗模型；第 5 节对上述模型进行数值模拟；最后是结束语。

2 相关工作

近年来，国内外学者针对 P2P 蠕虫的传播模型与防御策略等问题开展了大量的研究工作。例如 Chen 等人在文献[5]中将威胁 P2P 网络的蠕虫分为 3 类，即被动蠕虫、沉默蠕虫和主动蠕虫，并对这 3 类蠕虫的传播进行了仿真分析，但没有构建相应的蠕虫传播模型；Xie 等人在文献[6]中给出了 P2P 蠕虫的定义，并对其传播模型、攻防机制都做了总结，但对每种模型与防御机制的描述都过于简单，仅是一篇关于 P2P 蠕虫研究工作的综述；夏春和等人在文献[7]中构建了 P2P 蠕虫在 3 种典型的结构化对等网中的传播模型；罗兴睿等人在文献[8]中提出了基于纯 P2P 原理的蠕虫传播模型，但没有给出相应的蠕虫防治策略；Fan 等人分别在文献[9-12]中提出利用逻辑矩阵乘法求闭包的方式对 P2P 系统中基于拓扑扫描策略的网络蠕虫传播过程进行建模，但忽略了 P2P 节点的搅动特点对蠕虫传播过程的影响，没有专门针对结构化 P2P 蠕虫的传播进行建模，也没有考虑在对抗环境下的蠕虫传播过程；Shin 等人在文献[13]中提出了一种利用声誉机制来抑制被动蠕虫在 P2P 网络中传播的思路，但缺乏相应的传播模型来评估这种抑制效果；冯朝胜等在文献[14]中利用流行病学的 KM 思想对沉默型蠕虫在 P2P 网络中的传播与免疫过程进行了建模；Yang 等人在文献[15]中提出了基于动态隔离的主动蠕虫模型；Yu 等人在文献[16]中分析了基于 P2P 系统的主动蠕虫传播模型；Jafarabadi 等人在文献[17]中结合节点搅动的特点，提出了基于 SIR 的主动蠕虫传播模型。但这些工作都或多或少地忽略了蠕虫传播过程中的某些动态特征，所建立的模型对蠕虫传播过程的描述存在不够准确、形式复杂的问题；Gao 等人在文献[18]中针对不同结构的 P2P 网络拓扑，提出利用良性蠕虫对抗恶性蠕虫的防治策略和防治模型，但所建模型过于复杂，且忽略了恶性蠕虫在完成目标列表地址的扫描后，利用剩余攻击能力对网络中其余地址进行随机探测攻击的情况；邓昳轶在文献[19]中提出了基于 RAWBDP 的主动式非结构化 P2P 蠕虫对抗传播模型，并对该模型进行了详尽的仿真设计和分析，但其分析模型不够全面，且对良性蠕虫终止的条件设定得过于草率。为此本文提出一种简单实用的建模工具，针对 P2P 蠕虫在对抗环境下的传播过程进行形式化的描述和分析。

3 逻辑矩阵的形式化

为了能用逻辑矩阵这种简单工具来描述结构化 P2P 蠕虫对抗模型，本节中将对矩阵的定义进行扩展。若矩阵中每一个元素(包括常量元素与变量元素)都是逻辑类型，那么这个矩阵就是逻辑矩阵。

3.1 逻辑向量

在逻辑矩阵中，每一个元素都是逻辑类型的变量或常量，而逻辑变量的取值只能是两个逻辑常量的其中之一：True(用'T'表示)或 False(用'F'表示)。如果逻辑矩阵只有一行或一列，则这样的逻辑矩阵可以定义为逻辑行向量或逻辑列向量。

3.2 逻辑矩阵的操作

1)逻辑矩阵的绝对值

首先定义逻辑变量元素的绝对值：当逻辑变量 q 的取值为'T'时，其绝对值(用$|q|$表示)为 1，当其取值为'F'时，其绝对值为 0；其次定义逻辑矩阵的绝对值：逻辑矩阵的绝对值被定义为矩阵中取值为'T'的元素个数。根据这个定义，求逻辑矩阵 Q 的绝对值可用以下公式完成：$|Q|=\sum|q|\{q\in Q\}$。

2)逻辑矩阵逆置

逻辑矩阵 Q 逆置后的结果用 Q^{-1} 表示，Q^{-1} 与 Q 具有相同的维度，Q^{-1} 的每一个元素的逻辑值是由 Q 中每个对应位置上的逻辑值进行逻辑非运算后得到的。根据此定义，逆置矩阵 Q^{-1} 中每个位置上元素的逻辑值可由以下公式求得：$q_{inv}=q^{-1}$ $(q_{inv}\in Q^{-1},q\in Q)$，这里逻辑变量 q 上的 -1 代表对变量 q 进行逻辑非操作。逻辑向量的逆置操作可以参照逻辑矩阵的逆置操作进行。

3)逻辑矩阵相加

两个逻辑矩阵 A 和 B 只有取相同的维度时，才能进行相加操作，相加后的逻辑矩阵 C 与 A、B 具有相同的维度，而且在每个位置上的逻辑元素取值就是矩阵 A、B 对对应位置的逻辑元素进行逻辑或运算后的结果。因此根据这个定义，假设有两个 m 行 n 列的逻辑矩阵 A 和 B 进行相加运算，其结果逻辑矩阵 C 的元素取值可由以下公式得到：$C_{m\times n}=A_{m\times n}+B_{m\times n}$，其中

$$c_{ij}=a_{ij}+b_{ij}=a_{ij}\ \mathrm{OR}\ b_{ij}$$

$$(c_{ij}\in C,a_{ij}\in A,b_{ij}\in B|i\in[1,m],j\in[1,n])$$

逻辑向量的相加操作可以参照逻辑矩阵的相加操作进行。

4)逻辑矩阵按位相乘

当两个逻辑矩阵 A 和 B 具有相同的维度时，它们可以进行按位相乘。按位相乘后的逻辑矩阵 C 与 A、B 具有相同的维度，而且在每个位置上的逻辑元素取值就是矩阵 A 和矩阵 B 对对应位置的逻辑元素进行逻辑与运算后的结果。根据这个定义，假设有两个 m 行 n 列的逻辑矩阵 A 和 B 进行按位相乘运算，其结果逻辑矩阵 C 的元素取值可由以下公式得到：$C_{m\times n}=A_{m\times n}\cdot B_{m\times n}$，其中

$$c_{ij}=a_{ij}\cdot b_{ij}=a_{ij}\ \mathrm{AND}\ b_{ij}$$

$$(c_{ij}\in C,a_{ij}\in A,b_{ij}\in B|i\in[1,m],j\in[1,n])$$

逻辑向量的按位相乘操作可以参照逻辑矩阵的按位相乘

操作进行。

5)逻辑矩阵相乘

两个逻辑矩阵之间也可以按照普通矩阵的方式相乘。假设逻辑矩阵 A 与逻辑矩阵 B 要进行相乘操作，前提条件是逻辑矩阵 A 的列数要等于逻辑矩阵 B 的行数，相乘后的逻辑矩阵 C 与矩阵 A 具有相同的行数，与矩阵 B 具有相同的列数，矩阵 C 第 i 行第 j 列的元素逻辑值等于矩阵 A 第 i 行的逻辑行向量与矩阵 B 第 j 列的逻辑列向量进行按位相乘后的各个逻辑值再进行逻辑或运算的结果。根据这个定义，假设一个维度为 $m\times s$ 的逻辑矩阵 A 与一个维度为 $s\times n$ 的逻辑矩阵 B 相乘(A 的列数$=B$ 的行数)，能得到一个维度为 $m\times n$ 的逻辑矩阵 C，并且 C 的元素取值可由下面的公式表示：$C_{m\times n}=A_{m\times s}B_{s\times n}$，其中

$$c_{ij}=\sum_{k=1}^{s}a_{ik}\cdot b_{kj}$$

($a_{ik}\in A, b_{kj}\in B, c_{ij}\in C | i\in[1,m], k\in[1,s], j\in[1,n]$)

式中，$a_{ik}\cdot b_{kj}$ 代表对这两个逻辑变量 a_{ik} 与 b_{kj} 进行逻辑与操作，$\sum$ 代表将所有执行完逻辑与操作的结果再进行逻辑或操作。

3.3 拓扑逻辑矩阵和状态逻辑向量

1)拓扑逻辑矩阵

假设结构化 P2P 覆盖网中有 n 个节点，可以用一个 $n\times n$ 的逻辑矩阵 T 来表示。矩阵 T 中任意元素 $t_{ij}=1(t_{ij}\in T)$ 表示覆盖网中第 i 个节点与第 j 个节点相邻接，可用逻辑常量'T'来表示；如果 $t_{ij}=0(t_{ij}\in T)$ 表示覆盖网中第 i 个节点不与第 j 个节点相邻接，可用逻辑常量'F'来表示。因此包含 n 个节点的结构化 P2P 覆盖网可用 $n\times n$ 的拓扑逻辑矩阵 T 来表示。

2)状态逻辑行向量

在本文提到的对抗模型中存在着恶性蠕虫与良性蠕虫，用状态逻辑行向量 B 来表示各节点是否被恶性蠕虫感染，$b_j='T'(b_j\in B)$ 表示第 j 个节点被恶性蠕虫感染，$b_j='F'(b_j\in B)$ 表示第 j 个节点未被恶性蠕虫感染；同理用状态逻辑行向量 G 来表示各节点是否被良性蠕虫感染，第 i 个节点被良性蠕虫感染用 $g_i='T'(g_i\in G)$ 表示，未被感染用 $g_i='F'(g_i\in G)$ 表示。另外考虑到现实情况下，任意一种蠕虫只能感染那些存在安全漏洞的 P2P 节点，用状态逻辑行向量 V 来表示网络中各节点是否会被蠕虫感染，$v_k='T'(v_k\in V)$ 表示第 k 个节点存在安全漏洞，会被蠕虫感染，反之 $v_k='F'(v_k\in V)$ 则表示第 k 个节点不会被蠕虫感染。

4 基于逻辑矩阵的结构化 P2P 蠕虫对抗模型

4.1 传播过程与模型假设

本文提到的蠕虫模型是基于离散时间构建的，在对抗环境下，两种不同性质的蠕虫在结构化 P2P 网络中的传播过程如下：在蠕虫爆发初期的每轮感染中，恶性蠕虫会根据覆盖网的拓扑结构向所有存在安全漏洞且没被感染的邻居节点发起攻击，攻击成功后新感染的恶性蠕虫节点又会在下一轮攻击中执行同样的操作；当经过一定轮数的感染后，良性蠕虫加入，在每轮传播中，每个感染良性蠕虫的节点会帮助所有存在安全漏洞的邻居节点(包括已被恶性蠕虫感染的节点)修复漏洞，打上补丁，使其不再被恶性蠕虫重新感染。也就是说，良性蠕虫会逐步感染并清除结构化 P2P 网络中节点存在的安全漏洞，使恶性蠕虫逐步丧失攻击目标。

为简化结构化 P2P 蠕虫对抗模型，以便利用逻辑矩阵对其进行描述，做如下假设。

(1)在蠕虫爆发的初期，网络中只有恶性蠕虫在传播。这时如果一个节点存在安全漏洞且还未被感染，在任意一轮感染中只要它有一个邻居节点已被恶性蠕虫感染，则本轮中，在此节点未下线的情况下，它就必被恶性蠕虫感染，并在下一轮中继续感染其它存在漏洞的邻居节点。

(2)在蠕虫爆发的后期，当恶性蠕虫的感染覆盖率 ρ 达到一定阈值 Thr 时，良性蠕虫被激活，这时网络中同时存在恶性蠕虫与良性蠕虫。如果一个未感染节点存在安全漏洞，且在本轮感染中它的所有已被感染的邻居节点上的蠕虫都属于同一性质(都是被恶性蠕虫感染或都是被良性蠕虫感染)，则本轮中，在此节点未下线的情况下，它会被此种性质的蠕虫感染；如果其已被感染的邻居节点上的蠕虫分属于不同性质(一部分被恶性蠕虫感染，另一部分被良性蠕虫感染)，则本轮中，此节点未下线的情况下，它会被良性蠕虫感染。

(3)蠕虫节点从发现目标节点到展开漏洞攻击，直至注入蠕虫复本的工作在一个时间单元，即一轮感染中完成。

(4)无论一个在线节点是否已被恶性蠕虫感染，其只要存在安全漏洞，都会被良性蠕虫感染。被良性蠕虫感染的在线节点由于清除了安全漏洞，不会再被恶性蠕虫感染，也不会在下一轮中继续感染其它存在安全漏洞的在线邻居节点，反之不成立。

(5)结构化 P2P 网络中的在线节点是否存在安全漏洞是由逻辑行向量 V 表示的，且良性蠕虫与恶性蠕虫都是利用同一种漏洞对结构化 P2P 网络中的在线节点进行攻击，但由于 P2P 节点的搅动特征，在每轮中它们所面对的表示节点健康状态的逻辑行向量 V 是不同的。

(6)假设在一段时间内，结构化 P2P 网络的节点总数保持不变。

(7)假定结构化 P2P 覆盖网中有 n 个节点，最初被恶性拓扑蠕虫感染的节点有 I_0 个，被良性拓扑蠕虫感染的节点有 R_0 个。

4.2 对抗模型形式化

根据上面的假设，在蠕虫爆发的初期，结构化 P2P 覆盖网中共有 n 个节点，其中每个节点是否被恶性蠕虫感染的初始状态可用长度为 n 的状态逻辑行向量 B_0 来表示，由于感染初期有 I_0 个节点被恶性蠕虫感染，因此有 $|B_0|=I_0$；每个节点是否会被蠕虫感染的健康状态可用状态逻辑行向量 V 来表示；在恶性蠕虫进行了第 t 轮感染后，网络中存在的恶性蠕虫节点状态可用长度为 n 的状态逻辑行向量 B_t 来表示，其绝对值为 $|B_t|=I_t$。同理，在良性蠕虫出现的初期，每个节点是否能被良性蠕虫感染的初始状态可以用长度为 n 的状态逻辑行向量 G_0 来表示，由于感染初期有 R_0 个节点被良性蠕虫感染，因此有 $|G_0|=R_0$；在恶性蠕虫进行了第 s 轮感染后，网络中存在的良性蠕虫节点状态可以用长度为 n 的状态逻辑行向

量 G_s 来表示，其绝对值为 $|G_s|=R_s$。

(1)在只有恶性蠕虫存在的感染初期($\rho<Thr$)：第 t 轮被恶性蠕虫感染的在线节点状态 B_t 只与第 $t-1$ 轮被恶性蠕虫感染的在线节点状态 B_{t-1}、描述网络间在线节点链接状态的逻辑矩阵 T 以及表示网络在线节点健康情况的状态逻辑行向量 V 有关。根据上面的描述很容易推导出它们之间的关系，如式(1)所示：

$$B_t=B_{t-1}+B_{t-1}\cdot T\cdot V \tag{1}$$

(2)在两种蠕虫同时存在的感染中后期($\rho\geq Thr$)：同理可得在第 t 轮，被良性蠕虫感染的在线节点状态可用下面公式表示：

$$G_{t-t_0}=G_{t-t_0-1}+G_{t-t_0-1}\cdot T\cdot V \tag{2}$$

(3)此外良性蠕虫出现后，在两种蠕虫同时传播的每轮感染中，都可能有一些已感染恶性蠕虫的在线节点被良性蠕虫感染，从而改变状态逻辑行向量 B 中元素的逻辑值。此时第 t 轮被恶性蠕虫感染的在线节点状态 B_t 不仅与上述提到的节点状态 B_{t-1}、拓扑逻辑矩阵 T 以及状态逻辑行向量 V 有关，而且与第 t 轮被良性蠕虫感染的在线节点状态 G_t 有关。根据上面的描述很容易推导出它们之间的关系，如式(3)所示：

$$B_t=(B_{t-1}+B_{t-1}\cdot T\cdot V)\cdot G_{t-t_0}^{-1} \tag{3}$$

另外考虑到结构化 P2P 覆盖网的搅动特性，其中的 P2P 节点随时可能上下线，在每轮感染结束后，利用节点变化率 Or 调整拓扑时变对拓扑逻辑矩阵 T、恶性蠕虫感染行向量 B、良性蠕虫感染行向量 G 的影响，以便更真实地反映结构化 P2P 覆盖网的动态特征。

至此完成了基于逻辑矩阵的结构化 P2P 蠕虫对抗模型的构建。

5 基于 P2P 蠕虫对抗模型的数值模拟

为了找到对抗环境下影响恶性 P2P 蠕虫传播效率的关键因素，本文采用 Matlab 仿真工具对上述模型进行数值模拟，并以此验证对抗模型的有效性。运行平台为 Windows XP ServicePack3，CPU 3.10GHz，4GB 内存。假设结构化 P2P 网络的节点规模为 5000，每次实验时，从网络拓扑图中随机选择部分节点，分别将其初始化为 P2P 网络中的易感染节点、恶意蠕虫传播节点以及良性蠕虫驻留节点，通过实验来模拟各类蠕虫传播和对抗的过程。整个实验由节点的状态信息驱动，不模拟节点间的信息传递，模型基于离散时间构建，当前网络节点的状态只受前一轮节点状态、蠕虫扩散情况以及节点变化率的影响，在保持模型中其它参数不变的情况下，将同一参数不同取值所对应的传播曲线放在同一张图中作比较，以观察当达到良性蠕虫释放条件时，感染覆盖率 ρ 的大小，以此评估各参数对恶性蠕虫传播的重要性。

结构化 P2P 网络中每个节点具有相同的度数。将拓扑逻辑矩阵 T 中每个逻辑行向量的绝对值都取成 θ，在保证对角线元素逻辑值为'F'的前提下，每行中逻辑值为'T'的元素位置可任意选择，以此模拟结构化 P2P 网络的拓扑结构。另外为模拟 P2P 节点的搅动特点，在每轮感染结束后，都会利用 Matlab 中的 randperm 函数对模型中的节点变化率 Or、拓扑逻辑矩阵 T、逻辑行向量 B,G,V 上的节点逻辑值做调整。实验参数及含义如表 1 所列。

表 1 模型参数

参数	含义
N	结构化 P2P 网络的节点规模
θ	网络中节点的度数
f	具有免疫能力的节点比例
B_0	初始恶性蠕虫在总体规模中所占的比例
G_0	初始良性蠕虫在总体规模中所占的比例
Or	节点的变化率
B	被恶性蠕虫感染的节点的状态逻辑行向量
G	被良性蠕虫感染的节点的状态逻辑行向量
T	表示节点链接状态的逻辑矩阵
V	表示节点健康状态的逻辑行向量
χ	良性蠕虫释放时的感染覆盖率
ρ	感染上恶性蠕虫的节点比例，简称感染覆盖率，$\rho=\|B_T\|/n$

5.1 节点的度数对恶性蠕虫传播的影响

显然，结构化 P2P 网络中，节点的度数对蠕虫的传播会产生影响。在模型中，将 θ 的取值分别设为 3,6,12,30，在初始化在线节点链接状态的拓扑逻辑矩阵 T 时，利用 randperm 函数从矩阵 T 的每行中随机地选择前 θ 个位置上的节点，将其逻辑值设置为'T'(用 1 表示)，其它的节点的逻辑值设置为'F'(用 0 表示)。假设蠕虫按照此矩阵 T 所描述的网络拓扑进行传播，当恶性蠕虫的感染覆盖率超过 70%时，良性蠕虫被激活，开始工作。从图 1 可以看到，节点的度数越高，达到感染覆盖率峰值的时间越早，且能达到的峰值数也就越大，因此参数对恶性蠕虫传播速度的影响更为显著。

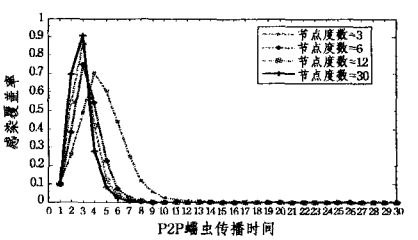

图 1 节点度数对恶性蠕虫传播的影响

5.2 恶性蠕虫初始感染率对恶性蠕虫传播的影响

该实验比较在结构化 P2P 网络中，恶性蠕虫的初始感染率对恶性蠕虫传播速度的影响。在模型中，将 B_0 的初始值分别取为 1%,10%,30%和 60%，利用 randperm 函数从在线节点的状态逻辑行向量 B 中随机地选择前 B_0 比例个位置上的节点，将其逻辑值设置为'T'(代表此节点初始时已被恶性蠕虫感染，其状态值用 1 表示)，其它的节点的逻辑值设置为'F'(代表此节点初始时未被恶性蠕虫感染，其状态值用 0 表示)。假设恶性蠕虫按逻辑行向量 B 所表示的初始感染比例进行传播，当恶性蠕虫的感染覆盖率超过 70%时，良性蠕虫被激活，开始工作。从图 2 中可以看到，恶性蠕虫的初始感染率越高，达到感染覆盖率峰值的时间就越早，但这个参数对感染覆盖率所能达到的峰值影响不大。

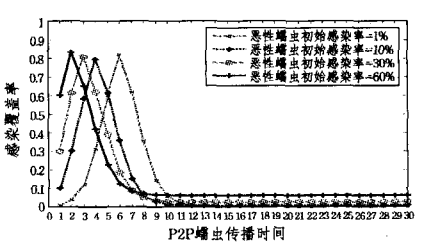

图 2 恶性蠕虫初始感染率对恶性蠕虫传播的影响

5.3 良性蠕虫初始感染率对恶性蠕虫传播的影响

该实验比较在结构化 P2P 网络中，良性蠕虫的初始感染率对恶性蠕虫传播速度的影响。操作如上所述，分别修改逻辑行向量 G 中受良性蠕虫感染的节点初始感染率 G_0 为 1%，10%，30%和 60%，并在恶性蠕虫的感染覆盖率超过 40%时，激活良性蠕虫开始工作。从图 3 中可以看到，良性蠕虫的初始感染率越低，达到感染覆盖率峰值的时间就越晚，且能达到的峰值数也就越大；但当良性蠕虫的初始感染比例超过 10%以后，其对感染覆盖率的影响就不明显了，只是良性蠕虫初始感染率越低，对恶性蠕虫传播的抑制速度越慢。

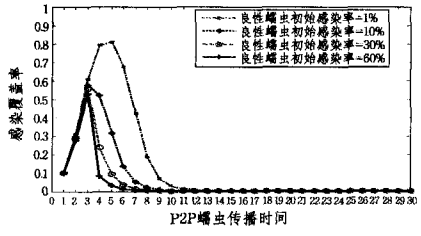

图 3 良性蠕虫初始感染率对恶性蠕虫传播的影响

5.4 良性蠕虫的释放时间对恶性蠕虫传播的影响

另外，良性蠕虫的释放时间也会对恶性蠕虫的传播产生影响。本实验检验此参数对蠕虫传播的重要程度。在模型中，将良性蠕虫释放时的感染覆盖率 χ 的取值分别设为 20%，50%，75%和 90%，在每轮感染后，通过比较 $\rho=|B_T|/n$ 和 χ 的大小，决定是否激活良性蠕虫开始工作。从图 4 可以看到，当 $\rho\geq\chi$ 时，良性蠕虫被激活，χ 取值越小，良性蠕虫的释放时间越早，最终感染覆盖率的峰值就越小，对恶性蠕虫传播速度的抑制效果也就越好。此参数对恶性蠕虫传播效率的影响很大。

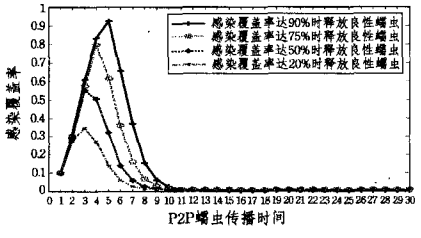

图 4 良性蠕虫释放时间对恶性蠕虫传播的影响

5.5 节点的初始健康状态对恶性蠕虫传播的影响

这个实验主要测试在结构化 P2P 网络中，节点的初始健康状态对恶性蠕虫传播速度的影响。参数调整的方法与 5.2 节和 5.3 节的类似，分别设置具有免疫能力的节点比例 f 为 1%，10%，35%和 60%，通过 randperm 函数从逻辑行向量 V 中随机选取前 f 比例个位置的节点，将其逻辑值设置为'F'(表示其存在漏洞，可被蠕虫感染)，其它的节点的逻辑值设置为'T'(表示其具有免疫力，不被蠕虫感染)，并在恶性蠕虫的感染覆盖率超过 70%时，激活良性蠕虫开始工作。从图 5 可以看到，初始时存在安全漏洞的节点比例越高，达到感染覆盖率峰值的时间越早，且能达到的峰值数也就越大，当良性蠕虫被激活时，它对恶性蠕虫传播速度的抑制效果也就越好；但这个参数对感染覆盖率所能达到的峰值影响不大。

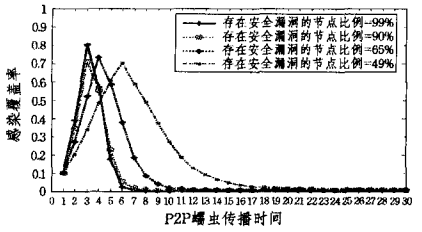

图 5 节点初始健康状态对恶性蠕虫传播的影响

5.6 P2P 节点离线率对恶性蠕虫传播的影响

P2P 节点的搅动特征会对蠕虫传播产生影响，本实验主要测试该参数对恶性蠕虫传播效率的影响。在模型中，将节点的变化率 Or 分别取值为 1‰，3‰，5‰和 1%，在每轮感染结束后，借助 randperm 函数随机地从逻辑矩阵 T、逻辑行向量 B,G,V 中选择前 Or 比例个位置上的节点，对其逻辑值做调整，以此模拟 P2P 节点可以随时上下线的搅动情况，并当恶性蠕虫的感染覆盖率超过 70%时，激活良性蠕虫开始工作。从图 6 中可以看到，P2P 节点的离线率越高，最终达到感染覆盖率峰值的时间就越晚，且能达到的峰值数也就越小。

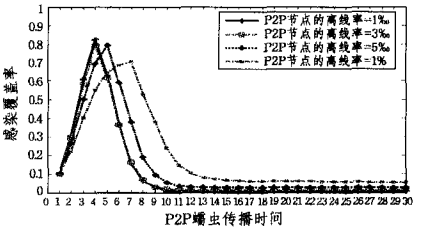

图 6 P2P 节点的离线率对恶性蠕虫传播的影响

综上所述，通过本次数值模拟实验可以证明形式化逻辑矩阵这种简单工具可以有效地描述蠕虫在对抗环境下的传播过程；快速发现抑制恶性蠕虫传播的关键因素。即在结构化 P2P 覆盖网中可以通过加强网络主机的安全性能，提高网络中各节点的健康状态，提升对蠕虫入侵的检测能力，并在发现蠕虫攻击后人为加快 P2P 节点的离线率，及早释放尽可能多的良性蠕虫与之对抗等来有效地防御主动蠕虫的入侵。

结束语 本文利用形式化逻辑矩阵来描述结构化 P2P 蠕虫在对抗环境下的传播模型。通过模型推导出影响蠕虫传播效率的关键因素，最后通过模拟实验证明了此模型的有效性与实用性。下一步将研究如何建立基于形式化逻辑矩阵的非结构化 P2P 蠕虫对抗模型以及如何描述 P2P 蠕虫分片传播的过程。

参 考 文 献

[1] Lui S M, Kwok S H. Interoperability of Peer-To-Peer File Sharing Protocols[J]. ACM SIGCOM Exchanges, 2002, 3(3): 25-33

[2] Zhou L D, Zhang L T, Frank M, et al. A first look at peer-to-peer worms threats and defenses[C]//Proceedings of IPTPS05. Peer-to-Peer Systems IV Lecture Notes in Computer Science, 2005, 3640: 24-35

[3] Yu W. Analyze the worm-based attack in large scale P2P networks[C]//Proceedings of The 8th IEEE International Symposium on High Assurance Systems Engineering. Tampa, Florida: IEEE Press, 2004: 308-309

[4] Arce I, Levy E. An analysis of the Slapper worm[EB]. IEEE Se-

curity & Privacy, 2003: 82-87

[5] Chen G, Gray R S. Simulating non-scanning worms on peer-to-peer networks[C]// Proceedings of the 1st International Conference on Scalable Information Systems. Hong Kong, China, 2006

[6] Xie C, Yin Z Y. The Research of Worms in P2P Networks[C]// Proceedings of Computational Intelligence and Natural Computing International Conference. 2009: 389-392

[7] 夏春和,石昀平,李肖坚. 结构化对等网中的 P2P 蠕虫传播模型研究[J]. 计算机学报,2006,29(6):952-959

[8] 罗兴睿,姚羽,高福祥. 基于纯 P2P 原理的蠕虫传播模型的研究[J]. 通信学报,2006,27(11):53-58

[9] Fan X, Xiang Y. Modeling the Propagation of Peer-to-Peer Worms under Quarantine[C]// Proceedings of Network Operations and Management Symposium (NOMS). Osaka, Japan: IEEE Press, 2010: 942-945

[10] Fan X, Xiang Y. Modeling the Propagation Process of Topology-Aware Worms: An Innovative Logic Matrix Formulation[C]// Proceedings of Network and Parallel Computing 2009 Sixth IFIP International Conference. Gold Coast, QLD: IEEE Press, 2009: 182-189

[11] Fan X, Xiang Y. Propagation Modeling of Peer-to-Peer Worms [C]// Proceedings of 24th IEEE International Conference on Advanced Information Networking and Applications. 2010: 1128-1135

[12] Fan X, Guo W W, Looi M. Modeling and Simulating the Propagation of Unstructured Peer-to-Peer Worms[C]// Proceedings of Computational Intelligence and Security 2011 Seventh International Conference. Hainan, China: IEEE Press, 2011: 573-577

[13] Shin J, Kim T, TAK S. A Reputation Management Scheme Improving the Trustworthiness of P2P Networks[C]// Proceedings of Convergence and Hybrid Information Technology 2008 International Conference. Daejeon, Korea: IEEE Press, 2008: 92-97

[14] 冯朝胜,秦志光,Cuthbert L,等. P2P 网络中沉默型蠕虫传播建模与分析[J]. 计算机研究与发展,2010,47(3):500-507

[15] Yang W, Li Y. P2P worm Propagation modeling and analysis under dynamic quarantine defense[C]// Proceedings of e-Business and Information System Security 2010 2nd International Conference. Wuhan, Huhei: IEEE Press, 2010: 1-4

[16] Yu W, Boyer C, Chellappan S, et al. Peer-to-Peer System-based Active Worm Attacks: Modeling and Analysis[C]// Proceedings of IEEE International Conference on Communications. 2005: 295-300

[17] Jafarabadi A, Azgomi M A. An SIR model for the propagation of topology-aware active worms considering the join and leave of hosts[C]// Proceedings of Information Assurance and Security 7th International Conference. 2011: 204-209

[18] Gao C X, Zhang F Y, Xin Y, et al. Research on Worm's Propagation and Defense Model in Different P2P Networks[J]. Journal of Beijing University of Posts and Telecommunications, 2006, 29(22): 49-53

[19] 邓眹轶. 对等网络蠕虫及其防御技术研究[D]. 成都:电子科技大学,2007

(上接第 125 页)

8000 个指令周期,但根据处理器对浮点数乘除运算的支持程度不同,所消耗的指令周期差别也很大。以试验 1 条件为基础,10 个待测点在理想情况下的 $\bar{E}$ 为 0.686m,其中最大误差为 1.62m,最小误差为 0.05m。可见修改过的算法进一步提高了定位精度。

6 算法复杂度分析

本文的算法复杂度与传统的质心定位算法复杂度相似,但是本文算法通过判断语句与简化的目标节点估计方法,大幅降低了求解的复杂性。若取 3 个满足定位条件的锚节点确定目标节点的估计坐标,利用传统的质心算法平均需要做 66 次加法、88 次减法、92 次乘法、32 次除法、12 次开平方运算、3 次比较判断才能计算出估计节点坐标;本文算法则至多需要 10 次加法、无减法、无次乘法、2 次整除运算、6 次移位运算、无开平方运算、42 次比较判断。对于目前常用的一些低处理能力 MCU,开平方运算以及浮点数除法运算需要占用大量的 MCU 指令周期,甚至于很多低运算能力 MCU 都无法进行开方运算。该方法一方面避免了开方运算以及浮点数除法运算的出现,从而大幅减小了 MCU 的运算量,提高了运算速率,更重要的是为低运算能力的处理器通过距离量直接求解定位估计坐标提供了可能性,实现了降低通信开销的目的。

结束语 本文意在提出一种适用于物联网感知层节点低运算能力微处理器也能直接计算目标节点位置的计算方法。该方法通过多层判断语句的嵌套,分类计算目标节点的估计目标值,来达到快速定位、降低通信开销的目的。试验表明,该方法有效地改善了算法的运算量,从而达到了降低功耗的目的,并且保证引入误差控制在要求范围内,能够满足多数的短距离无线定位的需求。下一步还将分析如何通过 RSSI 值在低运算的处理器下计算通信距离,从而实现低处理能力的处理器直接实现定位应用的功能。

参 考 文 献

[1] 刘锋,章登义. 基于 RSSI 的无线传感器网络质心定位算法[J]. 计算机科学,2012,39(B06):96-98

[2] 夏心江,胡钢,王烨华. 基于同心圆定位算法的改进算法研究[J]. 计算机科学,2012,39(6):68-71

[3] 苟胜难. 基于改进的 RSSI 无线传感器网络节点定位算法研究[J]. 计算机应用研究,2012,29(5):1867-1869

[4] Vivekanandan V, Wong V W S. Concentric anchor beancon location algorithm for wireless sensor networks[J]. IEEE Transactions on Vehicular Technology, 2007, 56(5): 2733-2744

[5] Bahl P, Padmanabhan V N. RAFAR: An In Buiding RF-based User Location and Tracking System[C]// Proc. IEEE Joint Conf. IEEE Computer Communications Societies (INFOCOM). Telaviv, Israel, Mar. 2000: 775-784

[6] Bergamo P, Mazzini G. Location in Sensor Networks with Fading and Mobility[C]// Proc. IEEE Int. Symp. Personsal, Indoor Mobile Radio Communicatons (PIMRC). Lisbon, Portugal, Sep. 2002: 750-754

[7] 李娟,王珂,李莉. 基于锚圆交点加权质心的无线传感器网络定位算法[J]. 吉林大学学报:工学版,2009,39(6):1649-163

[8] 朱剑,赵海,徐久强,等. 无线传感器网络中的定位模型[J]. 软件学报,2011,22(7):1612-1625

[9] 顾晶晶,陈松灿,庄毅. 基于无线传感器网络拓扑结构的物联网定位模型[J]. 计算机学报,2010,9:1548-1556

[10] 王琦. 基于 RSSI 测距的室内定位技术[J]. 电子科技,2012,6:50-54