基于社会计算的IM恶意代码防御机制

刘 昕[1,3],贾春福[2,3],石乐义[1],辛兆君[1]
(1. 中国石油大学(华东)计算机与通信工程学院,山东青岛 266580;
2. 南开大学信息技术科学学院,天津 300071;3. 南京大学计算机软件新技术国家重点实验室,江苏南京 210093)

摘 要: 即时通信(IM,Instant Messaging)网络已成为恶意代码传播的主要途径之一,本文提出了一种基于社会计算的IM恶意代码防御机制:利用用户与好友之间的社会信任关系,通过社会计算集成网络中多种反病毒软件的检测结果及用户的安全经验形成群体智慧,从而构成一个分布式协作防御机制.该机制利用即时通信网络平台,并依据好友间的交互行为计算动态信任,在IM客户端部署方案,用户之间实时相互协作抵御通过IM传播的恶意代码.实验结果表明,在大多数用户接受好友警告的情况下,即时通信网络中所有节点最终都被免疫,提高了整个社会网络防御IM恶意代码的能力.

关键词: 社会网络;即时通信网络;IM蠕虫;社会计算;社会信任;群体智慧
中图分类号: TP393.08 **文献标识码:** A **文章编号:** 0372-2112 (2013) 06-1130-10
电子学报URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2013.06.014

A Collaborative Defending Scheme Based on Social Computing Against IM Malicious Codes

LIU Xin[1,3], JIA Chun-fu[2,3], SHI Le-yi[1], XIN Zhao-jun[1]
(1. *College of Computer & Communication Engineering, China University of Petroleum, Qingdao, Shandong* 266580, *China*;
2. *Department of Computer and Information Security, Nankai University, Tianjin* 300071, *China*;
3. *State Key Lab for Novel Software Technology, Nanjing University, Nanjing, Jiangsu* 210093, *China*)

Abstract: IM(Instant Messaging) is used widely, which is an avenue for the propagation of IM malicious codes. To restrain IM malicious codes, we proposed a collaborative defending scheme based on social computing. Users can obtain experience after they browse through web pages and run malicious codes. Based on the trust between a user and his friends, through social computing, the experience and the checking results about IM malicious codes from different antivirus softwares on hosts are collected to result in collective intelligence. The platform used in the scheme is the social network formed by IM tool. Dynamic trusts on friends are calculated according to massages from friends. The scheme is a distributed system which is implemented in clients. Users collaborate with their friends to slow down the propagation of IM malicious codes. The experiments show all nodes in the social network are immune at last in the case when most users accept the warning, and the defending capacity of the whole social network is enhanced.

Key words: social network; IM network; IM worm; social computing; social trust; collective intelligence

1 引言

即时通信(Instant Messaging,IM)是指,使用在线识别用户和实时交换信息技术,依靠互联网平台和移动通讯平台,以多种信息格式(如,文字、图片、声音和视频等)进行沟通为目的,通过多平台、多终端的通讯技术实现同平台、跨平台的低成本高效率的综合性通讯方式.IM软件不仅是个人通信的重要方式,也是企业内部沟通及与客户交流的重要工具[1].

常见的IM软件如腾讯QQ、微软MSN Messenger、雅虎Yahoo! Messenger和移动飞信等都具有庞大的用户群,如QQ具有7亿注册用户,同时在线用户已超过1.5亿[2].中国互联网络信息中心发布的第31次中国互联网络发展状况统计报告显示,截至2012年12月底,我

收稿日期:2012-02-18;修回日期:2013-02-03
基金项目:国家自然科学基金资助项目(No.60973141,No.61272423);国家重点基础研究发展计划项目(No.2013CB834204);高等学校博士学科点专项科研基金资助项目(No.20100031110030);中央高校基本科研业务费专项资金资助(No.13CX02027A)

国即时通信用户规模达 4.68 亿,网民的即时通信使用率为 82.9%,而且该比例仍在不断增大[3].

即时通信用户之间通过其社会关系构成即时通信网络,是一种复杂社会网络.用户之间平均路径长度较小,即该网络具有小世界现象;网络中节点的度数遵循幂律分布,具有无标度特性[4,5].即时通信工具实时性、便捷性和易用性的特点,便于用户之间通信,同时也为恶意代码传播提供了一个理想的平台.通过即时通信软件传播的恶意代码包括即时通信蠕虫(简称 IM 蠕虫)、通过即时通信软件传播的病毒和恶意消息等.这些恶意代码利用即时通信工具绕过防火墙到达目的主机,IM 恶意代码的传播是不可避免的[6].

2001 年 8 月发现的第一例 IM 蠕虫 Hello worm[7]通过 MSN 传播.2002 年 8 月出现的"爱情森林"[8],是已知的第一个利用 QQ 自动发送恶意消息的病毒.即时通信工具的普及和迅速发展使其也成为病毒传播的主要渠道之一,已有多起 IM 恶意代码大规模爆发.IM 恶意代码的一个目标是将计算机变成僵尸机,形成僵尸网络,实施 DDoS 或者其他形式的攻击.快速传播的 IM 恶意代码与多种病毒结合,能够增强那些原本传播性不强、危害较大的病毒的感染性,影响着整个互联网的安全.

防御越来越多通过即时通信工具传播的恶意代码,单台主机的能力略显单薄.网络中多种反病毒软件存在多样性,不同反病毒软件能检测出不同恶意代码.有些用户访问恶意网页或者被恶意代码攻击之后,能够获得与这些恶意网页和恶意代码相关的安全经验.若将散布在网络中各种反病毒软件的功能和大规模 IM 网络用户获得的安全经验利用起来,对于整个网络防御 IM 恶意代码将会非常有效.

社会计算研究利用计算系统帮助人们进行沟通与协作,通过社会计算集中个体智慧形成群体智慧是目前网络研究的热点.随着社会网络的广泛应用,通过社会计算用户可以充分、及时地获得其可信任好友所掌握的各种可用资源,融合形成群体智慧应对网络恶意代码,加强用户主机对 IM 恶意代码的防御.

2　相关研究

很多研究者对 IM 网络和 IM 恶意代码传播进行建模.Wu 等人提出 IM 网络双层无标度网络模型,认为聚类系数和组群数会影响信息在 IM 网络中的传播[9].姚文斌等针对复杂网络的聚集特性和 IM 网络的幂率特性,建立基于超节点的 IM 蠕虫病毒传播模型,分析了 IM 虚拟网络拓扑模型结构,提出了基于 IM 蠕虫病毒群体概率分布的传播模型,并对该传播模型进行分析[10].IM 蠕虫具有如下特点:(1)IM 蠕虫为拓扑蠕虫;(2)由于软件客户端具有相同漏洞,IM 蠕虫能够攻破整个即时通信网络;(3)IM 蠕虫采用目标攻击方式,会使网络在极短时间内崩溃,且难以检测.冯朝胜等在对 IM 蠕虫和即时通信网络特点研究的基础上提出 IM 蠕虫的离散时间数学传播模型[11].

IM 恶意代码出现之后,各安全厂商都设计了针对即时通讯工具的实时监控功能,如趋势科技 PC-cillin 2005.即时通信软件本身也增强了安全性,如腾讯 QQ2009SP5 增强盗号木马病毒查杀功能,并增加 QQ 登录保护功能与传输文件安全判定功能;MSN2009 安全版对聊天内容加密,屏蔽恶意、骚扰消息和链接,自动扫描接收到的文件.

许多研究者对 IM 恶意代码的检测和遏制进行了研究.Smith 等提出切断联系人数量多的用户与服务器之间的连接,可以有效加大网络直径,减缓恶意代码传播,为尽量多的用户争取时间获取补丁[4].基于这样一种前提:一台被恶意代码感染的主机会尽可能多地连接不同的机器,而未被感染的主机通常重复访问最近曾经访问过的主机,Williamson 提出一种限制快速传播恶意代码的通用扼杀机制[12].随后 Williamson 和 Parry 将这种机制应用到遏制 IM 恶意代码的传播中[13].通过区分正常用户和 IM 恶意代码在通信速率上的差异,对异常通信进行限制,从而抑制 IM 恶意代码传播.Mannan 和 Oorschot 对这种方法进行了改进[14],将扼杀机制只应用于文件传输和包含链接的文本信息,并应用验证码区分这些消息是否由用户生成,从而限制自动发送文件和恶意链接.赵彬彬等将检测蠕虫的地点从 IM 服务器转移到普通网络的网关[15],通过统计可疑消息增长情况检测蠕虫,用动态队列减少存储量,并利用用户验证模块对可疑消息进行确认.张静等采用基于行为分析的检测方法[16],根据蠕虫发送信息的速度比正常用户发送信息速度快的特点检测 IM 蠕虫.

云安全技术起源于 2003 年提出的反垃圾邮件网格思想[17],融合并行处理、网格计算和恶意代码行为判断,通过网状的大量客户端对网络中软件行为的异常监测,获取互联网中恶意代码信息,并传送到服务器端进行分析和处理,然后将解决方案分发到客户端.针对同一安全软件,云安全成功应用群体智慧,将散布在互联网上的安全信息集成起来,但服务器收集信息和分发解决方案都需要一定时间,存在相对滞后性,且难以利用多种反病毒软件的多样性.

在社会计算和社会信任研究领域,Wu 认为,如果互联网在某种程度上加入社会信任关系,会提供更强大的防御措施应对垃圾邮件和其他攻击[18].张琳等在信任的综合评判中,融入中间推荐节点的直接交互经验,结合时间衰减和路径衰减更新信任,提高信任计算的准确程度[19].陈超等针对主观信任的动态性,结合模

糊理论中的近似度,提出了一种能够有效防止恶意推荐的信任更新机制[20].

以上研究者都未应用社会计算形成群体智慧,应对 IM 恶意代码的威胁.文献[21]提出了一种基于社会信任的分布式恶意网页协作防御机制,应用群体智慧应对恶意网页的威胁.该机制利用社会网络中好友间的动态信任集成好友的安全浏览经验形成网页综合评价,构建网状防御体系,能够有效减少恶意网页的访问量.该机制未针对 IM 恶意代码采取防御措施.

本文提出一种针对 IM 恶意代码的分布式协作防御机制,通过社会计算融合其信任的即时通信好友掌握的安全经验和网络中各种反病毒软件的功能,充分发挥用户和反病毒软件各自的优势,及时避免用户访问恶意链接指向的网页和接收恶意文件,减缓 IM 恶意代码传播,同时防御反病毒软件检测到的其它恶意代码.

3 IM 恶意代码传播方式

恶意代码利用 IM 工具中好友列表进行传播,已成为病毒传播的重要途径,主要原因是:即时通信用户规模庞大且持续快速增长;即时通信的实时性使得 IM 恶意代码传播速度比通过其他途径传播(如 E-mail 病毒)更快[22];用户之间的社会信任关系使得恶意代码传播成功率提高;IM 集成可用来查找新目标列表,适合病毒的集群传播[23];即时通信软件的社区化功能能够扩大恶意代码传播范围,加快传播速度.

IM 恶意代码传播的方式通常有两种:发送恶意链接和文件传输.

(1)发送恶意链接

恶意代码感染一台主机后,获取好友列表,向列表中的联系人发送包含网页链接的信息,该链接指向一个恶意网页.接收用户点击该链接后,包含在网页中的恶意代码将被自动下载到本地并运行,或者在浏览器中打开欺诈性网页,如钓鱼网站等.被感染的好友主机继续通过其好友列表向更多用户发送恶意链接.

(2)文件传输

利用即时通信软件的文件传输功能,恶意文件通常伪装成正常文件或流行文件,向被感染主机好友列表中的联系人发送文件传输请求.由于对该用户的信任,好友通常会接收并运行来自该用户的文件,则恶意代码即可感染本地主机.即时通信工具的文件传输功能融合 P2P 技术,用户和好友之间直接发送和接收文件,不需要从服务器下载,使得恶意文件迅速传播且成功率很高.

4 分布式协作防御机制

即时通信网络是一种复杂社会网络,基于该网络平台部署分布式协作防御体系,需要在社会信任的基础上传播防御信息,通过社会计算实现用户之间相互协作,并在用户本地使用恶意文件列表和网页评价表分别应对文件传输和发送恶意链接恶意代码的两种传播方式.

4.1 信任值的指定、计算和反馈

将社会信任应用于防御系统,实现用户之间信息交换和实时相互协作,需要对其进行量化管理.

在 IM 客户端,对用户好友列表中联系人进行信任程度的统一指定,计算用户间接好友的信任值,并根据好友和用户的交互及时动态更新每个好友的信任值,避免那些长期伪装为良好节点突然发送恶意代码的联系人带来的威胁.

4.1.1 信任值的指定

用户为好友列表中每个好友指定初始信任值,是[0,1]上的一个百分数,表示用户对好友的信任程度.

用户指定信任值之前,系统根据用户即时通信软件中对好友关系的设定(比如朋友、同事、同学、客户、陌生人等),评定一个建议信任值.若用户未对其好友信任值指定,系统默认建议值为其初始信任值.

4.1.2 间接信任值计算

用户信任其好友,好友信任自己的好友,则用户能够信任其间接好友,即信任可以传递.那么用户的可信任间接好友所掌握的信息和经验也可以为用户所用.用户对其间接好友的信任值,通过其好友对该间接好友的信任值计算得到.

Golbeck 提出的信任计算模型算法简单[24],非常适合在分布式系统中应用,直接引用其间接信任计算方法.两个用户之间间接信任值的计算如式(1)所示.

$$T_{is}=\frac{\sum\limits_{j\in N(i)}\begin{bmatrix}(T_{js}\times T_{ij}), & \text{if} \quad T_{ij}\geqslant T_{js}\\ (T_{ij}^2), & \text{if} \quad T_{ij}<T_{js}\end{bmatrix}}{\sum\limits_{j\in N(i)}T_{ij}} \tag{1}$$

其中 T_{ij}代表用户 i 对用户 j 的信任值,$N(i)$代表 i 的所有好友集合,包括直接好友与间接好友.

4.1.3 信任度阈值

用户对某好友的信任值低到一定程度,表示该用户不再信任该好友,不会采纳好友的建议.设置信任度阈值,对于用户信任值小于信任度阈值的好友发送的警告信息不存入本地网页评价表和恶意文件列表.

以用户为节点,好友关系为边,信任值为权重(为了简化,在此假设好友之间的信任是相互的且相互信任值相同),构成以用户节点为中心的网络拓扑图.图 1 是以用户节点 S 为中心,与其好友节点构成的社会网络,图 2 为将信任值小于信任度阈值的信任关系忽略(在此阈值设置为 50%),简化之后用户 S 的社会网络

拓扑图.由图 2 可以看出,可信任用户之间形成信任链.由一个用户节点出发,信任链中节点数目通常不超过 3 个.如果多个用户之间的信任值比较高,社会网络中会出现较长的信任链,如用户 nn_1 和 nn_2 之间的信任链:$nn_1 \rightarrow n_1 \rightarrow S \rightarrow n_4 \rightarrow nn_2$.长的信任链意味着可以利用更多用户的资源.

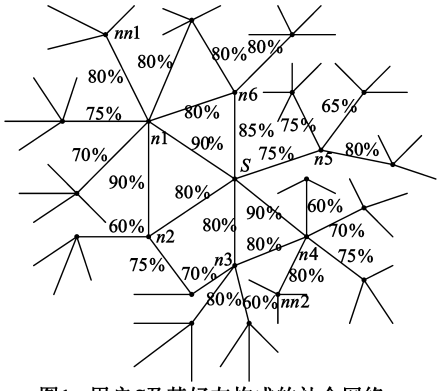


图1　用户S及其好友构成的社会网络

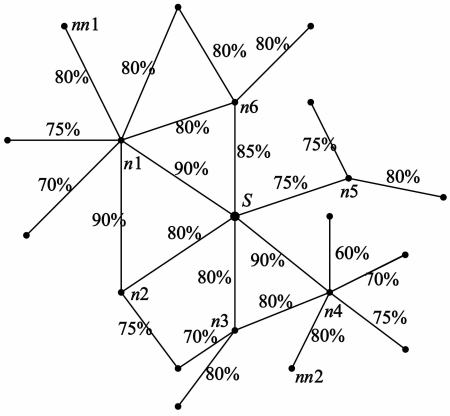


图2　用信任度阈值简化之后的社会网络

4.1.4　动态计算信任值

用户对好友的信任程度是动态的,随着用户之间的交互而改变.良好的信誉需要慢慢积累,而某个用户的恶意行为会立即降低好友对其信任程度.用户向好友传送补丁或者发送关于恶意链接和恶意文件的警告信息,则会相应提高用户信任值.第三方专业机构定期更新恶意网址名单,反病毒公司公布新出现恶意代码的解决方案,这些措施触发防御系统的反馈评价机制,将用户本地网页评价表和恶意文件列表中的信息与公布的信息比较,判断好友提供的相关警告信息是否正确,动态计算其实时信任值.

用户发送给好友的安全警告信息内容和方式不同,其重要程度也不相同.设用户主机中正确警告信息集合为 M,错误警告信息集合为 E,w_k 和 v_k 分别为 M 和 E 中第 k 条信息的权重(即其重要程度),其中 $0 < w_k < 1, 0 < v_k < 1$.用户 i 对直接好友 j 的动态信任值 $T_{ij}^{'}$ 可以自式(2)计算得到.

$$T_{ij}^{'} = T_{ij} + \sum_{m_j^k \in M} w_k - \sum_{e_j^k \in E} v_k \tag{2}$$

其中 T_{ij} 为计算之前用户 i 对用户 j 的信任值,即代表信任的历史信息,m_j^k 为节点 j 发送给用户 i 的正确警告信息,在 M 中为第 k 条信息,e_j^k 为节点 j 发送给用户 i 的错误警告信息,在 E 中为第 k 条信息.

动态信任值不可能无限增长,为其设置一个上限.计算方式如式(3)所示.

$$T_{ij}^{'} = \begin{cases} T_{ij}, & \text{if} \quad T_{ij} \geqslant 90\% \ \& \ T_{ij}^{'} < T_{ij} \\ 90\%, & \text{if} \quad T_{ij}^{'} \geqslant 90\% \ \& \ T_{ij} < 90\% \\ T_{ij}^{'}, & \text{if} \quad T_{ij}^{'} < 90\% \end{cases} \tag{3}$$

另外,若一用户向好友发送恶意文件或者恶意链接,好友系统立即将该用户的信任值降为 0.该用户清除恶意代码变为健康节点之后,好友可重新设置其信任值.

4.2　部署协作防御机制

基于即时通信网络平台,将基本防御功能部署在 IM 客户端,通过社会计算传播用户的网页浏览经验和多种反病毒软件的检测信息,分布式实现用户之间的协作防御,减缓和抑制恶意代码集中爆发.

根据 IM 恶意代码的两种传播方式,分布式协作防御机制应对方法如下.

4.2.1　文件传输

若一用户向好友发送文件传输请求,从接收方和发送方分别采取相应措施抑制恶意文件传播.

(1)从接收方抑制恶意文件的传输

不同反病毒公司的病毒库之间存在差别,检测各种恶意代码的能力不同,对于新出现的恶意代码尤其明显.各即时通信用户安装多种反病毒软件,且都具有对本地接收到文件进行扫描的功能.在用户本地设置一个文件,用于存放本地和好友主机反病毒软件检测到的恶意文件信息,称为恶意文件列表,如表 1 所示.恶意文件列表存储用户 id、信任值以及反病毒软件对可疑文件或者恶意文件的扫描信息.扫描信息包括扫描该文件使用的反病毒软件和扫描结果.

在用户确认接收文件之前,首先检查恶意文件列表,显示相应文件的检测信息,提示用户是否接收;若该文件不存在于恶意文件列表,则不提示.用户接收好友发送的文件后,本地反病毒软件自动对文件检测.若本地反病毒软件检测出恶意代码,则会阻止恶意代码从该节点继续传播.同时,协作防御系统将检测信息存入本地恶意文件列表,并立即向好友发送警告(即检测

信息),避免好友接收或运行接收到的恶意文件.接收到警告的用户将该信息存入本地恶意文件列表,并继续将该信息及其来源发送给其好友.间接接收到警告的用户根据对警告来源用户的信任值决定是否采纳和存入本地恶意文件列表.

表 1 恶意文件列表

用户 id	信任值	FILENAME1	FILENAME2	FILENAME3	FILENAME4
id1	100%				
id2	90%	360,可能是蠕虫变种			
id3	70%			诺顿,恶性病毒	
id4	70%				
id5	90%		NOD32, 可能是潜在不受欢迎程序的变种		
id6	80%				卡巴斯基,木马

经过第三方认证之后,可以将用户检测到的新出现恶意代码加入恶意代码库,增强反病毒软件的能力.

(2)从发送方抑制恶意文件的传输

为实现快速传播,IM 恶意代码通常隐蔽自身,不立即对宿主机进行严重破坏.主机被感染之后,若反病毒软件没有检测到恶意代码,则用户对本地系统已被感染不知情,此时主机不可信.

用户好友分为各种类型:同学、朋友、亲人、同事和客户等,通常情况下,用户会向某个或几个好友发送特定文件,不会向所有联系人发送相同的文件.而 IM 恶意代码感染一台主机之后,会自动向所有或者部分联系人发送恶意文件.对用户发送的文件数设置阈值可以限制恶意代码自动传播.用户发送文件时,对其发送的同一个文件进行计数.若该数值超过发送阈值,则弹出对话框提示用户确认是否继续发送.若用户未发送该文件,即可禁止文件传送.

Mannan 等采用验证码方式对抗恶意代码自动发送:每次用户向好友发送文件请求时,都需要输入验证码[14].在本文机制中,正常通信时用户通常不会对多个用户同时发送同一个文件,不需要用户确认,避免每次发送文件时输入验证码,在减缓恶意代码传播同时不额外增加用户过多操作.

4.2.2 恶意链接

若一用户向好友发送包含恶意链接的信息,从接收方和发送方分别采取相应措施抑制恶意代码传播.

(1)从接收方减少恶意网页访问量

当 IM 用户点击好友发送消息中的链接,则访问相应网页.此时,直接采用文献[21]中恶意网页协防机制的网页评价表,以应对通过恶意链接传播的恶意代码.

在用户点击好友发送的链接,打开该链接指向的网页之前,系统首先查找网页评价表,根据评价表中该网页的综合评价值提示用户,避免用户登录恶意网页,实现对恶意网页的协作防御.若用户继续访问该网页,则可以通过浏览器插件对该网页进行评价,其评价信息存入网页评价表,利用即时通信工具定期或及时与好友交换网页评价信息.本地根据好友信任值和好友对网页的评价值计算每个网页的综合评价值.

(2)从发送方抑制恶意链接传播

采用与从发送方抑制恶意文件的传输相同的方法,设置相同的发送阈值.

网页评价表中的好友信任值与恶意文件列表中的好友信任值保持一致,都是经用户指定和系统计算得到的动态信任值.

本文直接将文献[21]的网页评价表应用于防御通过恶意链接传播的恶意代码,融入本文机制;反之,通过 IM 传播的恶意链接能够丰富网页评价表,两个机制组合形成一个整体,共同防御恶意网页和通过 IM 传播的恶意代码,增强用户主机和整个网络的防御能力.

5 系统实现

在即时通信软件中添加一个插件,其功能包括:用户通过该插件指定好友列表中联系人的信任值;计算好友动态信任值和间接好友的信任值;将信任值存入本地恶意文件列表和网页评价表;显示好友发送的警告信息;判断是否将该信息存入本地恶意文件列表和网页评价表.浏览器插件提供用户评价网页接口,计算、显示网页综合评价值,提示用户将要浏览的网页是否安全.用户与好友在动态信任的基础上通过 IM 软件传送警告信息、交换网页评价表.

初始恶意文件列表存放本地反病毒软件恶意文件检测信息,随着用户与好友交互,添加好友传送的恶意文件信息.反病毒软件病毒库更新后,及时在恶意文件列表中删除病毒库中已有恶意文件信息.

当用户好友发送一个文件传输请求给用户,用户系统在恶意文件列表中查询与该文件相关的信息.若没有相关信息,接收该文件;若有相关信息,显示该信息,提示用户是否接收.

用户接收来自好友发送的文件之后,本地反病毒软件自动检测该文件并提示用户.若接收的文件安全,用户可以放心使用;若不安全,警告用户,防御系统自动将该检测结果存入恶意文件列表,并发送该信息至其好友列表中的联系人.好友根据对该用户的信任值决定是否将该信息存储到本地恶意文件列表.

系统对本地发送的同一个链接或同一个文件进行

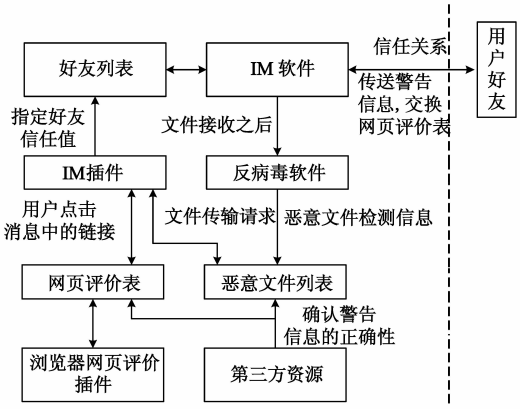


图3　防御系统结构图

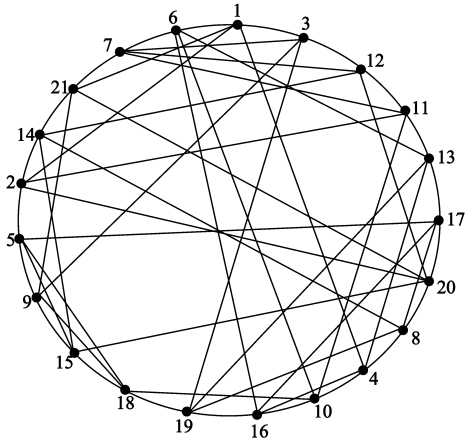


图4　21个节点的社会网络拓扑结构

计数,若超过设置的发送阈值,询问用户是否继续发送.若用户没有人工发送该链接或文件,即可发现存在恶意代码并中止发送.

恶意文件列表和网页评价表随着时间会不断增大.为了保持恶意文件列表和网页评价表是轻量级的,采取以下措施:(1)新的恶意代码在网络中流传一段时间之后,相应的补丁会发布,病毒库会更新,此时可以将本地恶意文件列表中相应信息删除.(2)一个恶意网页存活的时间并不长,超过其存活时间之后,可以将指向该网页的链接从网页评价表中删除.(3)设置信任度阈值,若好友动态信任值达不到信任度阈值,恶意文件列表和网页评价表都不会存放相关信息.

为了保护恶意文件列表和网页评价表,对这两个文件进行加壳,只允许插件程序访问这些文件,防止恶意代码利用、篡改或删除这些文件.

6　实验分析

根据恶意代码传播的方式,实验分为两个部分,分别针对恶意文件和恶意链接.

6.1　恶意文件传播方式

实验环境:VC6.0,Windows XP Service Pack 3 操作系统.组建一个由 21 个用户和 1 台服务器构成的 IM 网络,其拓扑结构如图 4 所示(图中忽略了服务器,由于 IM 节点之间传输信息不经过服务器).每个用户拥有多个好友.用户分别安装以下反病毒软件:诺顿、金山毒霸、360、NOD32、McAfee、卡巴斯基、瑞星.客户端之间以及客户端与服务器之间均采用 TCP 方式通信.恶意代码获取用户好友列表,然后向所有好友发送其自身,称这个过程为一步.一个用户节点有 3 种状态:未被感染(恶意代码未到达)、已被感染(该节点恶意代码能够向其好友传播)、免疫(本地反病毒软件检测出恶意代码或收到好友警告信息而不接收文件,此时该主机不会被感染).

该实验基于以下前提:

(1)每个用户只安装 1 种反病毒软件.

(2)每个反病毒软件都能检测出已知恶意代码,只有部分反病毒软件可以检测出新出现的恶意代码.

(3)一个恶意文件在用户主机被检测到,不能够通过该用户继续在网络中传播,且该用户向其所有好友发送对该文件的检测信息.

(4)IM 恶意代码不破坏即时通信软件的通信功能,用户主机被感染之后,仍然能够与好友继续通信.一个已经被感染的用户节点收到好友发送的警告信息,能够变为免疫节点并继续传播该警告信息.

一个恶意代码从网络中 1 个节点开始传播,实验记录每步感染该恶意文件的所有节点数(即那些能够向好友发送恶意文件的节点)和收到警告信息免疫的用户节点.

收到好友的警告信息,一部分用户会接受好友的警告,而另一部分用户会继续打开恶意文件,使其主机被感染.设分别有 0%,30%,50%,80%,100%用户接受好友的警告,每个用户有 5 个好友,只有 1 种反病毒软件能够检测出该恶意代码的情况下,网络中节点变化状况如图 5 所示.(*a*)图表示被感染节点数目;(*b*)图表示免疫节点数目.若用户都不接受好友的提醒,即表示没有应用该防御系统的情况,此时网络中只有能够检测到该恶意代码的主机未被感染,其余节点均被感染且未被免疫;随着接收好友警告的用户比例增加,被感染的节点数目明显减少,且网络中所有节点最终都被免疫.

恶意代码可能同时从多个节点开始传播.设恶意代码从 1、2、3 和 5 个用户节点开始传播,网络防御情况如图 6 所示.(*a*)图表示每步未感染节点数目;(*b*)图表示已被感染节点数目;(*c*)图表示免疫节点数目.初始感染节点数目不影响后期被感染节点总数,但初始感

染节点个数较多时,网络到达最终状态步数减少,因为检测到恶意代码的用户节点数增加.

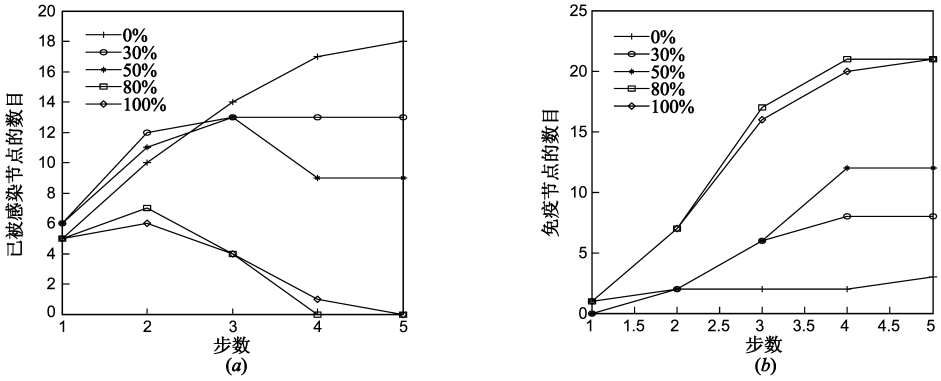


图5 接受警告的用户数目变化对防御机制的影响

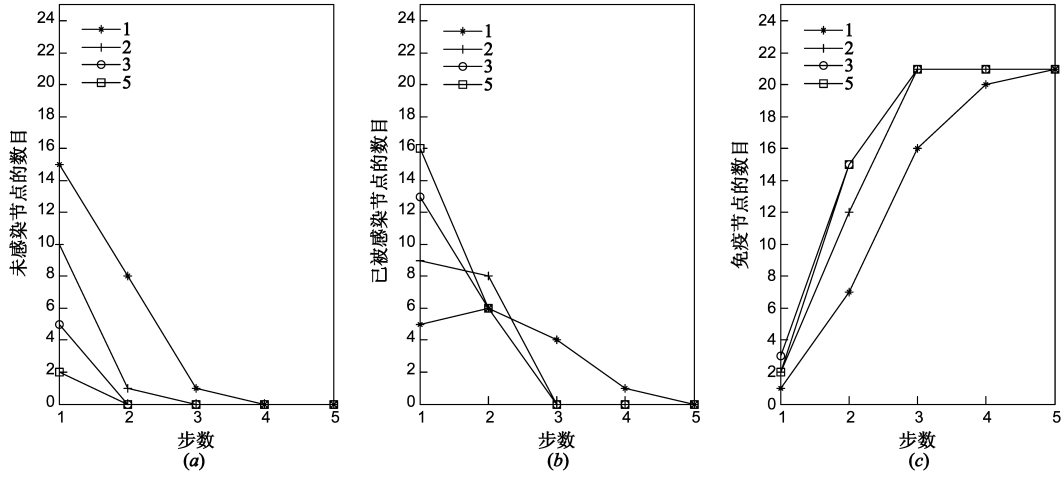


图6 初始感染节点个数对防御机制的影响

设能够检测到恶意代码的反病毒软件个数为 1、2、4 和 7 个时,防御情况如图 7 所示.随着能够检测到恶意软件的反病毒软件数目增加,被感染节点数目明显减少,但对于免疫节点数目影响不大.

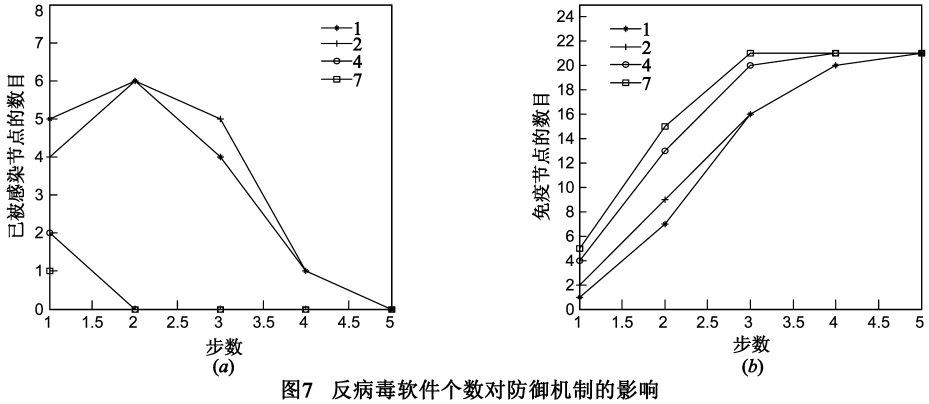


图7 反病毒软件个数对防御机制的影响

改变用户的好友数目对防御效果的影响如图 8 所示.每个用户 1 个好友,24 步之后所有节点全被免疫,而每个用户有 10 个好友,3 步之后所有节点全被免疫.

设置文件发送阈值分别为 2、4、6 和 8,网络中节点防御状况如图 9 所示.随着发送阈值增大,网络中被感染节点数目显著增多,免疫节点增长速度较快.

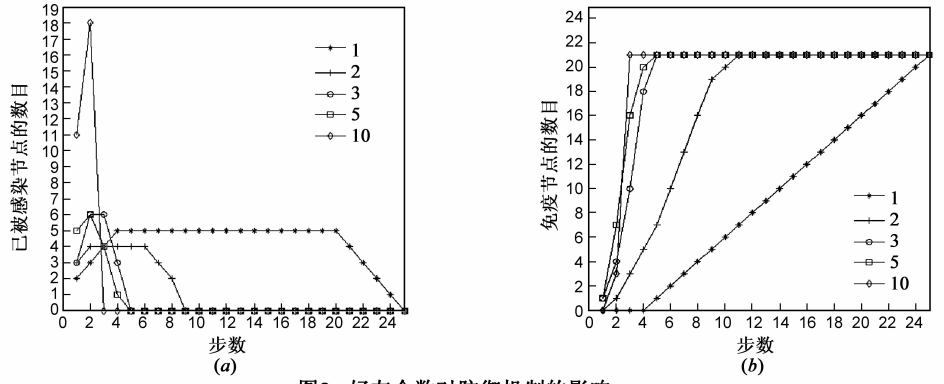


图8　好友个数对防御机制的影响

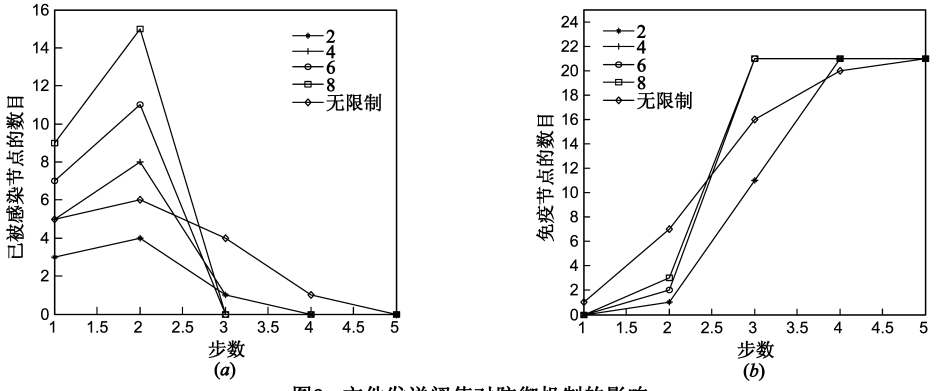


图9　文件发送阈值对防御机制的影响

6.2　恶意链接

通过恶意链接传播的恶意代码,采用了文献[21]的恶意网页防护机制.文献[21]的实验结果表明,在社会信任的基础上应用群体智慧,能够有效地降低恶意网页的访问量,显著提高网络防御恶意网页的能力.

6.3　与其他方法比较

Mannan 和 Oorschot 采用的方法部署在服务器上[14],设置延迟队列抑制 IM 恶意代码的爆发,该机制增大了服务器的负载,使得即时通信工具不再具有实时的特性,降低了即时通信工具的功能.

赵彬彬等将检测 IM 蠕虫的地点部署到普通网络的网关[15],相比文献[14]的方法,减小了服务器负载,但是增大了网关负载,降低了网络传输速度.

张静等采用基于行为分析的检测方法[16],根据 IM 蠕虫与用户发送文件的速度不同检测蠕虫,未提出限制蠕虫传播的措施.

本文提出的机制分布式部署在客户端,不影响即时通信用户正常实时通信,且可以有效抑制 IM 恶意代码的传播.

7　结论及未来工作

为了抑制 IM 恶意代码的传播,本文提出了一个分布式协作防御机制.以即时通信网络为平台,根据用户与好友之间的交互动态计算好友信任值,应用社会计算将多种反病毒软件的检测结果以及多个用户的网页浏览经验融合形成群体智慧,及时、迅速、动态抵御 IM 恶意代码.该机制在即时通信系统客户端部署方案,针对 IM 恶意代码两种传播方式,采取不同应对措施,用户通过即时通信工具互相协作.实验结果表明,该机制能够增强整个即时通信网络中所有用户节点的防御能力,从而有效抑制 IM 恶意代码.

在以后的研究工作中,我们将社会计算应用到基于双邻居列表的 P2P 网络中[25],解决 P2P 蠕虫围堵机制中漏洞信息的安全性问题,更有效地抑制利用 P2P 网络传播的蠕虫,增强整个信息网络的安全性.

参考文献

[1] iResearch. iResearch China Instant Messaging Research Report [EB/OL]. http://www. 2chinable. com /china-internet-market-free-reptort-download/cat_ view/45-china-social-media-market-free-reports,2010.

[2] hugo.腾点:腾讯 2011 年同时在线用户达 1.5,注册用户达 7 亿[EB/OL]. http://www. tendow. com/? p = 2653, 2011.11.17.

[3] 中国互联网络信息中心.中国互联网络发展状况统计报

告[EB/OL]. http://www.cnnic.cn/research/bgxz/tjbg/201201/P020120118512855484817.pdf,2013.

[4] Smith R D. Instant Messaging as a Scale-Free Network [EB/OL]. http://arxiv.org/abs/cond-mat/0206378,2002.

[5] P Holme, B J Kim. Growing scale-free networks with tunable clustering[J]. Physical Review E,2002,65(2):026107.

[6] Ryan Naraine. Researchers Say Automated IM Worm Is Inevitable[EB/OL]. http://www.eweek.com/c/a/Security/Researchers-Say-Automated-IM-Worm-Is-Inevitable/,2005.

[7] McAfee. W32/Hello.worm[EB/OL]. http://www.mcafee.com/threat-intelligence/malware/default.aspx? id = 99077, 2003.

[8] Rising. 爱情森林病毒[EB/OL]. http://it.rising.com.cn/newSite/Channels/Anti_Virus/Antivirus_Base/TopicDatabasePackage/27-155400316.htm,2002.

[9] Yu WU, Yanrong YANG, Huanzheng WU, Gongxiao WANG. Modeling and simulation on information propagation on instant messaging network based on two-layer scale-free networks with tunable clustering[A]. Proceedings of the 2009 IEEE International Conference on Systems, Man, and Cybernetics [C]. San Antonio, TX: IEEE Press, 2009.5184 – 5188.

[10] 姚文斌,杨松涛.复杂网络中即时通信蠕虫病毒传播的研究[J].计算机工程与应用,2009,45(18):129 – 131.
YAO Wen-bin, YANG Song-tao. Study of instant messaging worms spreading on complex network[J]. Computer Engineering and Applications, 2009, 45(18): 129 – 131. (in Chinese)

[11] 冯朝胜,邓婕,秦志光,刘霞,劳伦斯·库珀特.即时通信蠕虫传播建模[J].计算机工程,2010,36(5):143 – 145.
FENG Chao-sheng, DENG Jie, QIN Zhi-guang, LIU Xia, Laurence Cuthbert4. Modeling of instant message worms propagation[J]. Computer Engineering, 2010, 36(5): 143 – 145. (in Chinese)

[12] Williamson M W. Throttling viruses: Restricting propagation to defeat malicious mobile code[A]. Proceedings of Computer Security Applications Conference [C]. Las Vegas, Nevada: IEEE Press, 2002.61 – 68.

[13] Williamson M W, Parry A, Byde A. Virus throttling for instant messaging[A]. Proceedings of Virus Bulletin Conference[C]. Chicago, USA: Virus Bulletin Limited, 2004.1 – 10.

[14] Mannan M, Oorschot P C. On instant messaging worms, analysis and countermeasures[A]. Proceedings of ACM CCS Workshop on Rapid Malcode[C]. Fairfax, Virginia, USA: ACM Press, 2005.2 – 11.

[15] 赵彬彬,张玉清,刘宇.IM 蠕虫检测方案的设计与实现[J].计算机工程,2009,35(21):147 – 150.
ZHAO Bin-bin, ZHANG Yu-qing, LIU Yu. Design and implementation of IM worm detection method[J]. Computer Engineering, 2009, 35(21): 147 – 150. (in Chinese)

[16] 张静,胡华平,刘波.基于行为分析的 IM 蠕虫检测方法[J].通信学报,2007,28(8A):154 – 157.
Zhang Jing, Hu Huaping, Liu Bo. Behavior analysis based IM worm detecting[J]. Journal on Communication, 2007, 28(8A): 154 – 157. (in Chinese)

[17] 百度百科.云安全[EB/OL]. http://baike.baidu.com/view/1725454.htm,2011.

[18] Katharine Gammon. Networking: Four Ways to Reinvent the Internet [OL]. http://www.nature.com/news/2010/100203/full/463602a.html,2010.

[19] 张琳,王汝传,张永平.一种基于模糊集合的可用于网格环境的信任评估模型[J].电子学报,2008,36(5):862 – 868.
ZHANG Lin, WANG Ru-chuan, ZHANG Yong-ping. A trust evaluation model based on fuzzy set for grid environment[J]. Acta Electronica Sinica, 2008, 36(5): 862 – 868. (in Chinese)

[20] 陈超,王汝传,张琳.一种基于开放式网络环境的模糊主观信任模型研究[J].电子学报,2010,38(11):2505 – 2509.
CHEN Chao, WANG Ru-chuan, ZHANG Lin. The research of subjective trust model based on fuzzy theory in open networks[J]. Acta Electronica Sinica, 2010, 38(11): 2505 – 2509. (in Chinese)

[21] 贾春福,刘昕,刘国友,胡志超,王冬.一种基于社会信任的恶意网页协防机制[J].通信学报,2012,33(10):110 – 116.
JIA Chun-fu, LIU Xin, LIU Guo-you, HU Zhi-chao, WANG Dong. A collaborative defending scheme against malicious Web pages based on social trust[J]. Journal on Communications, 2012, 33(10): 110 – 116. (in Chinese)

[22] 卿斯汉,王超,何建波,李大治.即时通信蠕虫研究与发展[J].软件学报,2006,17(10):2118 – 2130.
Qing SH, Wang C, He JB, Li DZ. Research and development of instant messaging worms[J]. Journal of Software, 2006, 17(10): 2118 – 2130. (in Chinese)

[23] iResearch. 2009 China IM Communication Security Study Report[EB/OL]. http://www.2chinable.com/china-internet-market-free-reptort-download/cat_view/45-china-social-media-market-free-reports,2010.

[24] GOLBECK J. Computing and Applying Trust in Web-Based Social Networks[D]. Maryland: University of Maryland, College Park, 2005.

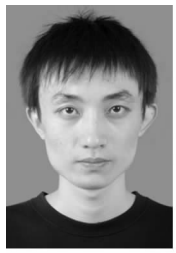
[25] Jia Chunfu, Liu Xin, Liu Guoyou, et al. Worm containment based on double-neighbor lists in P2P overlay networks [A]. Proceedings of 2010 IEEE International Conference on Information Theory and Information Security (ICITIS 2010) [C]. Beijing: IEEE Press, 2010.558 – 562.

作者简介

刘　昕　女,1974 年 10 月出生于山东省潍坊市.2012 年毕业于南开大学计算机与信息安全系,现为中国石油大学(华东)讲师.从事网络安全和社会计算方面的研究工作.
E-mail:liuxin_star@163.com

贾春福　男,1967 年 5 月出生于河北省文安市,现为南开大学教授、博士生导师,主要研究方向为信息安全与可信计算、恶意代码发现与分析.
E-mail:cfjia@nankai.edu.cn

石乐义　男,1975 年 9 月出生于山东临朐,中国石油大学(华东)副教授,硕士生导师,主要研究方向为网络安全,博弈理论和移动计算.
E-mail:shileyi@upc.edu.cn



辛兆君　男,1988 年 5 月出生于山东青岛.研究生.主要研究方向为网络安全.
E-mail:xinzhaojun567@sina.com