基于社团结构的网络协同防御

王　刚，陆世伟，冯　云，伍维甲
（空军工程大学信息与导航学院，西安，710077）

摘要　以公共互联网安全需求为背景，研究基于社团结构的网络协同防御问题。首先，根据网络逻辑结构及节点功能，将目标网络划分为多个网络社团，按照分布式协同控制模式设计了协同防御架构基础通信模型，在此基础上，融合信息蜜罐和蜜网、协同防御策略库、基于节点信任值管理的防火墙等功能模块，提出了基于社团结构的网络协同防御架构。其次，借鉴网络生态系统运维理念，设计了网络协同防御机制，通过态势感知协同、态势分析协同、行动决策协同和调节反馈协同等集体行动，提升网络的病毒检测能力、快速响应能力和应急恢复能力。最后，以潜伏型病毒防御为例，给出了网络协同防御流程，仿真分析了协同防御性能。相比无协同防御网络，基于社团结构的网络协同防御能以较小的通信损失，抑制潜伏型病毒传播和维护网络安全。

关键词　协同防御；社团结构；信息蜜罐与蜜网；节点信任通信；潜伏型病毒
DOI　10.3969/j.issn.1009-3516.2021.02.011
中图分类号　TP393；E824　　**文献标志码**　A　　**文章编号**　1009-3516(2021)02-0068-09

A Cooperative Network Defense Based on Community Structure

WANG Gang, LU Shiwei, FENG Yun, WU Weijia
(Information and Navigation College, Air Force Engineering University, Xi'an 710077, China)

Abstract　Taking public Internet security requirements as a background, the study of network cooperative defense is based on community structure. First, according to the logical structure and node function of the network, the target network is divided into several network communities, and a basic communication model of cooperative defense architecture is designed according to the distributed cooperative control mode. On this basis, a cooperative network defense architecture based on community structure is proposed by integrating information honeypot and honeynet, cooperative defense strategy library, and firewall based on the node trust value management. A cooperative mechanism is designed by using the experience of concept of network ecosystem operation for reference. Through the collective activities as situation awareness, the situation analysis, the action decision and the regulation feedback, the network defense abilities, such as virus detection, rapid response and emergency recovery, can be improved respectively. Finally, taking the latent virus defense as an example, the cooperative network defense flow is given as well as numerical performance simulations. Compared with the non-cooperative defense network, the network cooperative defense based on community structure can inhibit the spread of latent virus and enhance network security with less communication loss.

收稿日期：2020-08-17
基金项目：国家自然科学基金(61573017,61703420)
作者简介：王　刚(1976—)，男，湖北武汉人，教授，研究方向：网络空间安全理论与技术。E-mail：wglxl@nudt.edu.cn

引用格式：*王刚，陆世伟，冯云，等. 基于社团结构的网络协同防御[J]. 空军工程大学学报(自然科学版)，2021，22(2)：68-76. WANG Gang, LU Shiwei, FENG Yun, et al. A Cooperative Network Defense Based on Community Structure[J]. Journal of Air Force Engineering University (Natural Science Edition), 2021, 22(2): 68-76.*

Key words　cooperative defense; community structure; information honey-pot and honey-net; node trust communication; latent virus

公共互联网作为一种普遍使用网络，要求保障关键服务安全可控，保护用户合法权益。然而，网络信息窃取和关键节点破坏等非法蓄意攻击对公共互联网安全造成极大威胁，包括分布式拒绝服务攻击、病毒攻击、先进持续性威胁等。传统防御系统主要采用静态防御的方法来加固系统防护，从而保护网络的安全，相关技术包括防火墙技术、加解密技术、数据鉴别及访问控制技术等。对于网络系统的正常访问、用户合法身份的鉴别和权限管理、数据信息安全，这类技术起到了一定的防护作用。然而，对于隐藏特征的网络病毒，如“震网”病毒、Regin 病毒和“狼人杀”病毒，与传统蠕虫病毒相比，它们的技术手段和行动更为隐蔽高效。“潜伏”是这类网络病毒所共有的典型特性，因而通常将其称为潜伏型病毒。在感染目标网络节点时，潜伏型病毒为实现特定战术目标，将其攻击感染的表征暂时隐藏起来；根据行动需求和前期设定的触发机制，攻击方会选择特定时机或采用特定手段激活启动该病毒。由于潜伏特性，静态防御通常难以检测该病毒潜伏特征，也就无法彻底清除病毒，因而传统防御模式在处理此类外部攻击时存在先天的局限性。

目前，国内外网络安全机构和专家已将此类问题的解决途径转移到主动防御、动态防御和集体防御上来，如邬江兴院士提出的拟态防御架构，可用于应对未知漏洞后门病毒等不确定威胁[1]；沈昌祥院士倡导运用可信计算方法，设计自主可控的网络安全信息技术体系[2-3]；国外 Rathore 等人结合智能城市 IoT 网络的区块链技术，提出一种基于软件定义网络(SDN)的去中心化安全架构，检测物联网网络中的攻击，并能够缓解现有架构固有的“单点故障”问题[4]。总体上看，这些网络安全防御是通过预先设计网络防御机制，实现攻击的诱导与转移，降低外部攻击对网络造成的损失，其实现技术包括节点信任通信[5-6]、动态目标防御[7-8]和信息蜜罐与蜜网[9-10]等，这些研究从不同层面为网络安全防御实践应用提供了先进防御理念和技术支撑。然而，由于不同团队前沿研发技术相对独立，有些忽略了网络防御要素间的兼容性和协同能力，造成网络监控要素分布分散和功能独立，使得网络防御依旧面临系列问题[11]，如持续监控难以实现，被动封锁效果有限，防御分散响应缓慢，攻防管控各自为战。客观上，需要结合网络自身的复杂异构性创新理念，如引入网络生态和分布式集体防御[12-13]，建立新的网络安全协同防御架构，通过定义网络要素间动态联动关系和生态机制，预测和防御包括不确定攻击在内的多类型网络攻击，将攻击后果最小化并快速恢复网络至安全状态。

本文结合公共互联网安全特点，首先根据网络逻辑结构及节点功能，将目标网络划分为多个网络社团，按照分布式协同控制模式设计了协同防御架构基础通信模型，在此基础上融合了多类型功能模块，提出了基于社团结构的网络协同防御架构。其次，借鉴网络生态系统运维理念，设计了基于网络协同架构的协同机制，通过集体行动提升网络的病毒检测能力、快速响应能力和应急恢复能力。最后，以潜伏型病毒为例，给出基于社团结构的协同防御流程和仿真验证。

1　协同防御架构

关于网络病毒传播模型的研究表明，降低网络节点平均度是抑制病毒传播的主要方法[14-17]。定义网络图 $G=(V,E)$ 为某一具体网络，$V=(v_i)_N$ 为节点集，N 为网络节点总数，E 为网络边的集合。网络在遭遇病毒入侵时，通过隔离节点策略可抑制病毒的大规模传播。设隔离节点 v_i 的度为 k_i，隔离 v_i 前后网络平均度分别为 $\langle k\rangle_f$ 和 $\langle k\rangle_l$，则 $\langle k\rangle_l$ 可表示为：

$$\langle k\rangle_l=\frac{\langle k\rangle_f\times N-k_i}{N}=\langle k\rangle_f-\frac{k_i}{N}\qquad(1)$$

显然，节点隔离策略能降低网络平均度，抑制网络病毒的传播。研究表明，少量的节点隔离不足以完全抑制病毒传播，过多的节点隔离又会导致网络通信能力的损失，节点隔离策略需要在维护网络安全的同时，保证网络基本通信能力。现实中，网络病毒的感染过程通常是由一个节点或一个区域向周边节点扩散开来，最终蔓延至整个网络。根据式(1)知，降低病毒所在网络的节点数 N，同样能够降低节点平均度，从而起到抑制病毒传播的作用。按照这一思路，将整个网络分为若干个子网络(社团)，在检测到病毒入侵时，及时封锁病毒所在社团，缩小病毒传播范围，就能通过隔离较少的节点来维护网络的安全。在封锁社团后，来自病毒感染社团的信息需要经过特定的验证机制，在确保安全的条件下转发至其它社团节点。

网络协同防御模型能更好地完成网络安全防御任务[5,18]。在大规模网络主动协同防御模型中，全

局网络可划分为若干个自治系统(autonomous system,AS),单个 AS 采用基于代理的协同控制框架来完成协同防御任务,整体上通过分布式集体协作共同抵御病毒传播[18]。对于划分 AS 后的网络,如果遭遇病毒入侵,只需要隔离病毒感染社团和少量节点,即可抑制病毒传播。

一般网络都具有社团属性,可采用社团识别算法,如 Newman 快速凝聚算法、Girvan-Newman 分裂算法等[19-21],将整体网络划分为多个自治社团(network community,NC)。设划分后的社团数为 n,对应集合为 $NC=\{NC_1,NC_2,\cdots,NC_n\}$。在此基础上,可按分布式协同控制模式[11-12]设计对应的基础通信模型,见图 1。其中,单个社团由用户主机、协同控制中心和社团内的各种安全系统组成[18]。

社团内部安全系统主要包括入侵检测系统(intrusion detection system,IDS)、信息蜜罐与蜜网系统、带有节点信任值管理模块(node trust-value management module,NTVMM)的防火墙系统[6]、入侵防护系统(intrusion prevention system,IPS)、协同防御策略库,对应的协同防御系统架构见图 2。

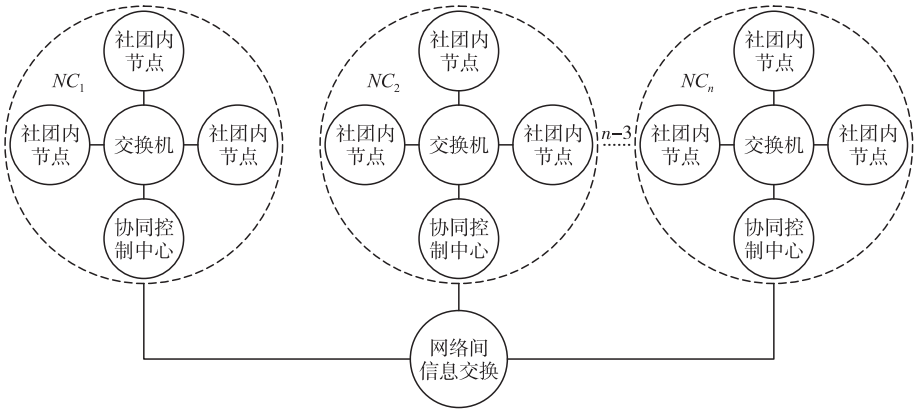

图 1 协同防御中网络社团基础通信模型

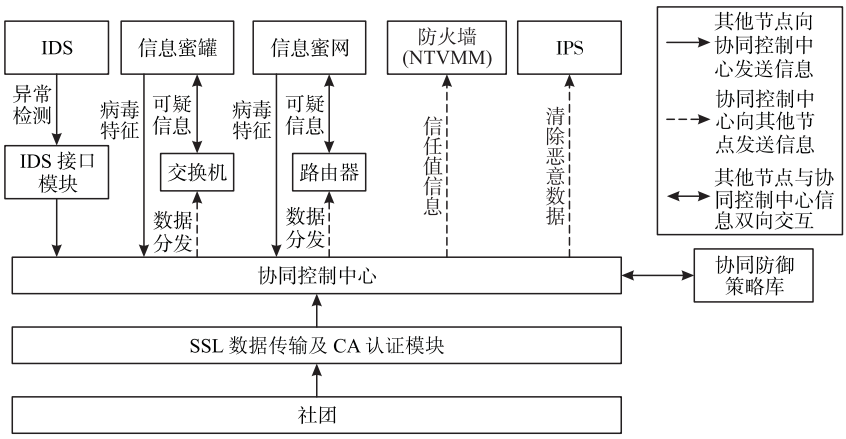

图 2 协同防御系统架构

协同防御架构建立在大规模网络的主动协同防御模型[18]和基于覆盖网的协同式安全防护与分析系统模型[22]基础上,进一步融合了协同防御策略库、带有 NTVMM 的防火墙、信息蜜罐与蜜网模块。除了适用于防御 DDOS 攻击与蠕虫病毒攻击[18],还能提升对潜伏型病毒等新型攻击的防御能力,且具备更强的协同防御功能。

2 协同防御机制

在实际应用中,需要科学的防御机制来确保各模块间的协同协作,保证在低损失情况下网络的整体安全。借鉴网络生态系统态势感知-持续监控-协同防御-快速恢复-溯源反制(situation awareness, monitoring, cooperative defense, recovery, countermeasure,SMCRC)机制[11],设计协同防御架构的协同防御机制。考虑网络攻击形式的多样化,以下以潜伏型病毒防御为例[17]。

潜伏型病毒通常利用其潜伏特性,绕过安全防御单元检测,入侵内部网络,并在激活后迅速感染网络。对于潜伏型病毒入侵,协同防御系统主要功能包括:检测病毒的潜伏特征与感染特征、抑制潜伏型病毒在网络中的传播、清除网络中潜伏型病毒等。根据防御系统对病毒入侵事件的响应顺序,可将协同防御机制划分为态势感知协同、态势分析协同、行动决策协同以及调节反馈协同 4 个部分,构成一个

网络协同防御环，自适应选取最优防御策略来应对潜伏型病毒入侵，如图 3 所示。

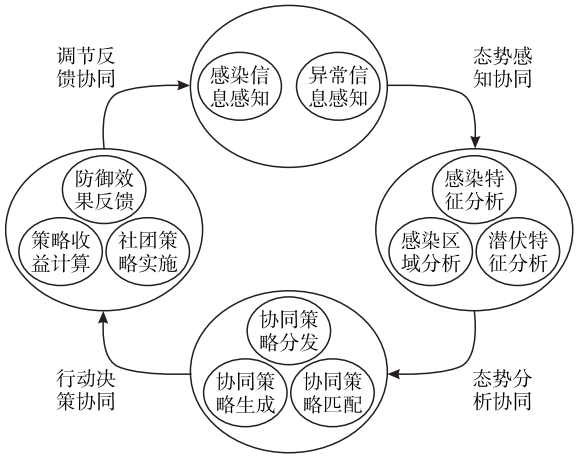

图 3　网络协同防御环路和防御机制

2.1　态势感知协同

态势感知协同防御需要对目标网络状态实施不间断监控，传统防御中 IDS、防火墙等防御单元很难做成集成模块，协作能力较差，对异常信息的监测能力较差，通常会导致直接隔离异常信息或是错将包含潜伏病毒的异常信息放入内网，都可能对节点或网络造成较大的损失[11]。

态势感知协同机制主要依赖于 IDS、信息蜜罐与蜜网和协同控制中心。IDS 可直接检测出已知特征的病毒类型，并发出警报通知协同控制中心。对于潜伏型病毒，IDS 通常只能感知到信息的异常，而无法直接判断信息是否携带病毒。这种情况下，协同防御中的 IDS 会记录异常信息并通知协同控制中心，控制中心命令交换机和路由器控制异常信息传输速率，并将部分异常信息送至信息蜜罐或蜜网中进行监测。如果在信息蜜罐或蜜网中，异常信息表现出感染特性，安全分析设备会立即检测出感染特征，并通知控制中心将检测出的感染特征添加至各 IDS 和防火墙的病毒特征库。特殊地，如果异常信息在蜜罐中的感染过程是有时滞的，可认为该信息中携带潜伏型病毒，蜜罐或蜜网中安全系统会进一步分析异常信息代码，提取病毒潜伏特征，并通知控制中心转发潜伏特征。此外，在网络的关键交换机和路由器中会部署流量分析器和探测器，可用来跟踪异常数据流并完成持续监控。

2.2　态势分析协同

态势感知协同会对每个时间段内的网络状态进行监控，如果网络中节点状态发生改变，需要态势分析协同机制来判断网络是否受到攻击、攻击强度、攻击区域以及网络能否自恢复至安全状态等。态势分析协同主要依赖于协同控制中心，通过收集 IDS 报警信息、信息蜜罐与蜜网检测信息、关键交换机和路由器检测信息，对网络整体态势进行分析，分析内容包括病毒的潜伏能力与感染能力、网络受感染区域分布、网络中可能潜伏病毒的区域、病毒传播趋势、网络对病毒的免疫能力等，态势分析结果有助于对病毒传播模型[14-16]中的参数值进行估计，计算病毒传播的基本再生数，进而选取当前最适合的协同防御策略。

对于异常信息，协同控制中心根据收集到的相关信息对该类信息可疑度进行判定；借鉴异常信息检测方法[23-25]，选择既往攻击信息为训练集，训练异常信息分类模型，即可实时判定该类信息类型或是否包含潜伏型病毒，进而选取合适的免疫或隔离策略[26-28]来防御潜伏型病毒。

2.3　行动决策协同

态势分析协同可深入分析网络受感染程度等安全态势信息，社团中的协同管理中心会根据安全态势分析结果，查询协同防御策略库，生成当前最优防御策略，分发给社团中的节点，节点采取相应的防御措施共同应对网络威胁。如果已获取病毒的攻击特征或潜伏特征，控制中心会将这些特征广播给社团内的用户主机、交换机以及社团间的路由器节点，这些节点对接收或传输的数据包进行检查和过滤，拒绝包含病毒特征数据的接收或限制其传输速度。

若社团中部分节点的安全设备检测出异常信息，但未能发现病毒特征，协同控制中心会通知社团中其它节点进行协同检测与分析。通过收集网络中异常信息存在的区域与规模，并根据目前网络的通信需求，对比策略库中策略适用条件，选择防御策略。以下列举了几种参考策略：①若网络各社团均被感染，此时网络需要尽快恢复到安全状态，而对通信能力要求不高，协同控制中心可选择基于最大节点度的隔离策略[29]，尽快降低网络平均度，从而迅速抑制病毒传播；②若网络各社团均被感染，而网络正在进行重要通信，需要在维护网络安全的同时保证网络的通信损失较少，可采用基于节点信任关系的恶意信息拦截策略[6]，通过选择最合适的信任阈值，在控制病毒传播的同时，保证网络的业务承载能力。被隔离社团发出的信息及其它社团发往被隔离社团的信息可由路由器转送至信息蜜网中进行存储与检测，从而提高病毒特征的检测率，并降低策略造成的信息损失。

协同防御策略由社团中协同控制中心共同制定，为了便于模型的架构扩展与实现，需要统一协同策略的生成格式和字段：

＜Community＞—＜Target＞—＜Type＞—＜Event＞—＜Level＞—＜Objects＞—＜Operation＞

其中,Community 表示策略所适用社团编号;Target 表示策略所适用目标,如 IP 地址,端口;Type 表示策略种类,包括检测、抑制、清除或免疫病毒等;Event 指当前针对的网络安全事件,如潜伏型病毒入侵、感染型病毒入侵、混合型病毒入侵或 DDOS 攻击等;等级表示网络当前所处的安全级别;Objects 表示操作的对象,如 IDS、交换机、信息蜜罐和信息蜜网等;Operation 表示操作对象所要执行的操作,包括扫描、分析、隔离或转发信息至蜜罐等。

协同控制中心通过安全协议(如 SSL 协议等)与社团内其他用户和安全模块建立安全通信连接,在协同策略生成后,协同控制中心将策略安全分发至社团中目标节点。

2.4 调节反馈协同

协同策略分发后,网络节点会根据策略内容实时调节自身行为。用户主机的行为调节包括改变 IDS 检测级别及需要检测内容、防火墙过滤规则、NTVMM 模块阈值(阈值会决定异常信息的接收比例)、IPS 的清除对象;交换机和路由器行为调节包括信息分发规则、控制异常信息流速、端口开放情况;信息蜜罐和蜜网会调整对特殊事件记录及监视频率、提升安全分析软件对日志的审查和分析频率、以及允许转存信息的数量。控制中心可以协同计算策略库中策略的期望收益,分配最高收益的策略,社团根据接收到的指令调整各自行为。调整后的网络状态经过感知与分析,就可以判断网络安全状态经过调整是否得到提升。调节反馈协同的具体流程见图 4。

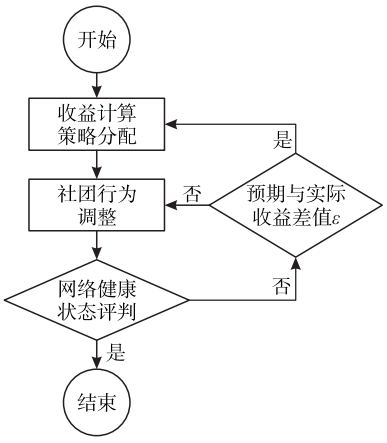

图 4 调节反馈协同流程

首先,由协同控制器根据具体情况生成初始策略并分发至各社团,同时计算预期收益。社团根据协同控制中心产生的策略调整自身行为。调整行为后,网络整体安全状态会发生改变,此时节点将调节后的状态反馈给协同控制中心,包括节点安全状态的变化和通信损失情况等。根据收集到的反馈信息,协同控制中心计算网络实际收益,通过对比实际收益与期望收益,实时调整协同防御策略,确保网络获得最佳收益。网络收益计算方法可根据策略对网络整体的通信能力及网络受感染情况的影响来设计[30]。以潜伏型病毒为例,根据网络病毒传播 SEIQRS 模型[17],可以计算出病毒传播的基本再生数为:

$$Rv=\frac{\beta\langle k\rangle\delta\gamma}{\omega(\delta+\psi)(\gamma+\theta+b)} \tag{2}$$

式中:$\langle k\rangle$为网络平均度;β 为潜伏型病毒的感染系数;γ 为潜伏病毒在网络节点中被激活的概率;ψ 为网络节点具有抗病毒攻击感染能力的概率;δ 为节点抗病毒能力退化的概率;ω 为受病毒攻击感染的节点断开网络连接的概率;θ 表示潜伏的病毒失去激活机会的概率;b 表示节点在病毒潜伏期具备免疫能力的概率。由此,可进一步计算网络相对安全指数[30]:

$$\delta(t)=\begin{cases}1, & \text{if } Rv\leqslant 1\\ 1-\dfrac{I^1}{N}, & \text{if } Rv>1\end{cases} \tag{3}$$

式中:

$I_1=\dfrac{N\omega\varepsilon[\beta\langle k\rangle\delta\gamma-(\psi+\delta)(\gamma+\theta+b)\omega]}{\langle k\rangle\beta\gamma[\delta(\omega\varepsilon+\gamma_\varepsilon+\gamma\omega)+(\gamma+b)\omega\varepsilon]}$,$N$ 为网络节点总数[17]。网络平均信息强度[30]为:

$$\mu(t)=\frac{\sum_{i=1}^{N}\sum_{j=1}^{N}p_{ij}im_{ij}(t)}{N^2}, \tag{4}$$

式中:p_{ij} 为单位时间内网络节点 i 和 j 节点间信息传递概率,可根据节点之间的最短路径和信息传递单位时间计算 $p_{ij}=\dfrac{1}{d_{ij}t_U}$;$im_{ij}$ 为 t 时刻节点和节点 j 传递信息的重要性。根据网络平均信息强度和网络相对安全指数,可计算隔离策略带来的网络收益为:

$$Q(t)=\begin{cases}a_1\Delta\mu(t)+b_1\Delta\delta(t), \text{if } \lambda\leqslant\lambda_{\max}\\ a_2\Delta\mu(t)+b_2\Delta\delta(t), \text{if } \lambda>\lambda_{\max}\end{cases} \tag{5}$$

式中:$\lambda_{\max}$由网络鲁棒性确定,λ 为隔离节点后造成网络信息损失的比例;a_1,b_1 为网络鲁棒性范围内通信和安全所占的比例系数,$a_1+b_1=1$。在网络鲁棒性范围内隔离节点,对网络通信影响较小,而安全提升明显,因而通常 $a_1<b_1$。a_2,b_2 分别为网络鲁棒性范围外通信和安全所占的比例系数,$a_2+b_2=1$,通常 $a_2>b_2$。$\Delta\mu(t)$和 $\Delta\delta(t)$为 t 时刻后网络平均信息强度和网络相对安全指数变化值,计算如下:

$$\begin{cases}\Delta\mu(t)=\mu(t+1)-\mu(t)\\ \Delta\delta(t)=\delta(t+1)-\delta(t)\end{cases} \tag{6}$$

如果网络未到达安全状态,可以计算实际收益与期望收益的差值,若差值大于某个阈值,协同控制中心可根据最新的态势感知与分析结果,调整协同防御策略的生成与分发,以获取更高的网络收益。

3　潜伏型病毒协同防御流程

潜伏型病毒通常先潜伏至网络关键节点，在激活后迅速感染网络其它节点，由于潜伏型病毒的隐蔽性，传统防御架构难以有效查杀，病毒清除过程普遍滞后于病毒感染与传播[27]。网络协同防御可基于大规模网络的主动协同防御模型[18]，用于防御 DDOS 攻击和蠕虫病毒攻击，还可按照协同防御机制抵御潜伏型病毒入侵。以潜伏型病毒为例设计网络协同防御流程，如图 5 所示。

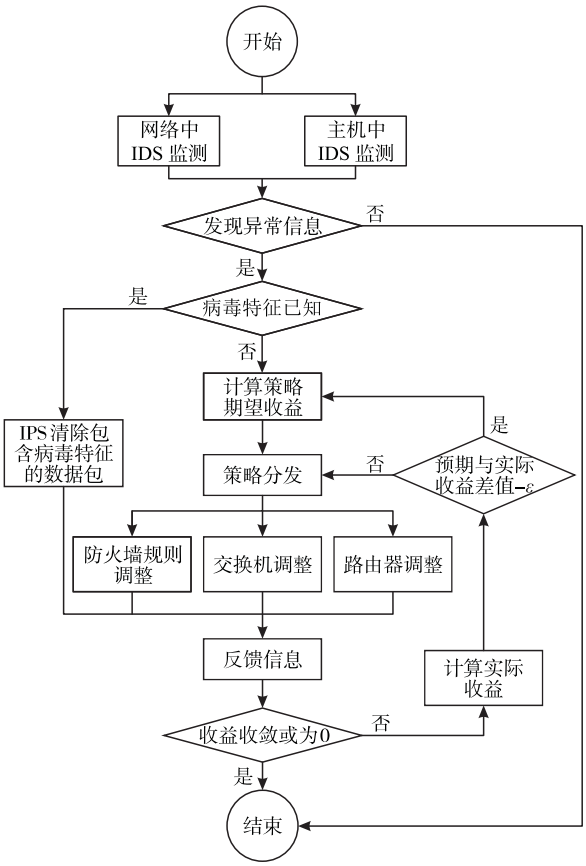

图 5　潜伏型病毒的协同防御流程

在协同防御系统中，信息蜜罐与蜜网、网络链路中的 IDS 系统都能对潜伏型病毒实时进行监控。如果网络中流量异常，IDS 立即通知协同控制中心，控制中心命令交换机或路由器将信息诱导至信息蜜罐或蜜网中，进行长期的观察。由于信息蜜罐或蜜网中会设置一些能满足潜伏型病毒激活条件的环境，如调整系统时间，键盘键入，访问次数触发等，从而提升网络对异常信息中病毒的检测能力。若未能检测到异常信息中的病毒信息，可进一步提取分析信息中部分内容，以便寻找出病毒潜伏的特征。对于数据内容的提取，蜜罐和蜜网需要向协同控制中心提出数据访问请求，在协同防御中心通过后，可对异常信息的内容进行访问与提取，以此来确保蜜罐或蜜网中信息的安全性。一旦检测出病毒潜伏特征，信息蜜罐和蜜网会将特征告知协同控制中心，控制中心通知其它节点启用 IPS 和防火墙，清除和过滤包含潜伏特征的流量数据，从而提升病毒的免疫率。

以上特征提取过程主要针对处于潜伏阶段的病毒，对于感染阶段的病毒，协同防御系统可将其视为蠕虫病毒。此外，在防御感染阶段病毒的同时，网络节点还需要检测病毒是否包含潜伏特性，避免网络恢复安全后的二次感染。如果协同控制中心确定病毒类型潜伏型病毒但未检测出潜伏特征，可命令网络用户开启防火墙的 NTVMM 模块，在可承受的通信损失范围内选择一个合适的阈值，并以部分通信代价来提升网络的安全性。

以上潜伏型病毒防御流程能对已知类型病毒的潜伏和感染特征进行检测，也能利用模块间的协同作用来检测未知类型病毒的潜伏和感染特征，从而有效提升网络对病毒的检测能力。在检测出病毒特征之前，即病毒监测阶段，协同控制中心会生成并分发协同防御策略，来抑制病毒传播规模，确保病毒对网络造成的损失降到最低。

4　仿真验证

仿真部分重点验证所构建协同防御架构及机制在防御潜伏型病毒方面的有效性。节点信任值管理算法(NTVMM)[6]和基于最大性能收益的隔离算法(maximum performance gain isolation algorithm，MPGIA)[29]在网络收益方面要优于最大度隔离算法(maximum degree isolation algorithm，MDIA)[30]，仿真主要将协同防御策略与前两种策略进行对比。

4.1　网络社团划分

生成一个小世界网络，网络节点数 ，边的数量，平均度近似等于 2，平均聚类系数为 0.273。根据 Newman 快速凝聚算法，将网络划分为 6 个社团。图 6 和图 7 分别给出了网络社团划分图及每个社团中节点的数量图。

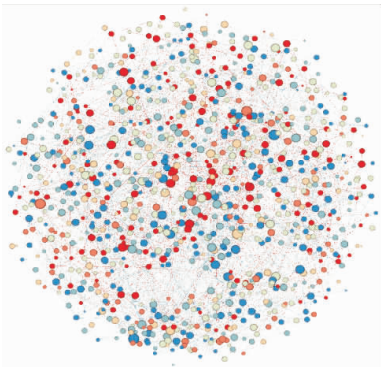

图 6　网络社团划分图

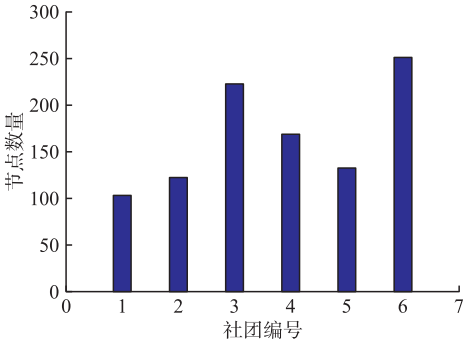

图 7 每个社团中节点的数量

在图 6 中,网络节点尺寸越大,节点的度越大;节点的颜色表示该节点所处的社团,共有 6 种颜色,每种颜色节点的数量对应于图 7 中社团节点的数量。

4.2 仿真参数设置

选取 SEIQRS 病毒传播模型[17],模型中转移参数设置为 $\beta=0.6$、$\theta=0.1$、$\gamma=0.6$、$\omega=0.2$、$\varepsilon=0.2$、$\varphi=0.2$、$\delta=0.2$、$b=0.1$。网络总节点数 $N=1\ 000$,网络平均度 $k=2$,令状态节点数量初始值($S(0)$, $E(0)$, $I(0)$, $Q(0)$, $R(0)$) = (980, 0, 20, 0, 0),计算可得直接潜伏型病毒传播模型的基本再生数分别为 $R_0=2.25$,该参数设置下网络中是有病毒的存在,而且网络利用自身免疫系统无法恢复至安全状态,需要合理的策略来抑制病毒的传播。仿真中,在整个网络中单独采用 MPGIA 和 NTVMM 来恢复网络安全(作为对照组),计算网络恰好达到安全时 2 种防御算法带来的网络性能收益。假设网络中单位时间内两个节点间通信一次,即有 2 条信息传输。仿真中单位时间取为 1 s。由于只在网络鲁棒性范围内计算策略的收益,小世界网络中网络收益函数参数[30]取 $a_1=0.5$、$b_1=0.5$。

在整个网络中用 2 个策略恢复网络安全后,将网络按照 4.1 中方法划分为 6 个社团,并在相同仿真参数环境下模拟协同防御过程(作为实验组)。由于是从数值上对协同防御仿真,对其中的部分模块功能进行量化处理。信息蜜罐和信息蜜网对潜伏病毒的潜伏特征和感染特征进行检测,设置检测周期为 20 s,网络对潜伏节点和感染节点的免疫概率增加 20%。蜜罐和蜜网存储 MPGIA 和 NTVMM 中未能成功发送的信息,并在网络恢复安全后将这些信息转发至目的节点。由于网络中信息对时间的依赖程度是随机的,只有部分信息对时间是敏感的,即延迟发送有很大损失,而其它信息对时间的敏感度较低,在网络安全后发送也不会有太大的损失。因此,根据平均场理论,可认为蜜罐和蜜网会降低网络中一半的信息损失,即协同防御中总的信息损失会在原有损失基础上减少至 50%。协同防御过程中被病毒感染的社团,会采用收益最高的策略来进行隔离与恢复。没有发现病毒的社团可保持正常通信,只需与受感染的社团间中断通信。据此,计算协同防御在恢复网络安全时的累积网络收益。

4.3 协同防御收益的有效性验证

初始状态节点数 ($S(0)$,$E(0)$,$I(0)$,$Q(0)$,$R(0)$) =(980,0,20,0,0),表示在病毒爆发初始时刻,网络协同感知和分析系统检测出被感染病毒节点有 20 个,此时还未检测出有潜伏病毒的节点,且所有节点都不具备抵御病毒感染的能力。假设检测出的潜伏型病毒具有明显的地域特性,集中分布在某个社团内,但不确定病毒所在社团编号。在此条件下,仿真验证有协同防御和无协同防御时 2 种策略带来的网络收益。

图 8 是病毒分别出现在在 1-6 号社团时,网络整体采用 NTVMM 和 MPGIA,以及隔离对应社团后采用 NTVMM 和 MPGIA 得到的网络收益,即不同策略组合的网络性能收益。

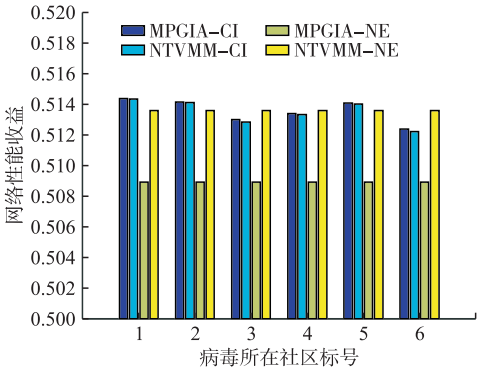

图 8 不同策略组合的网络性能收益

此时,网络中所隔离的社团一定是病毒存在的社团编号。其中,MPGIA-CI 表示社团隔离后在受感染社团中采用 MPGIA 来恢复网络的安全;NTVMM-CI 表示社团隔离后在受感染社团中采用 NTVMM;MPGIA-NE 为不隔离社团,网络整体采用 MPGIA;NTVMM-NE 为不隔离社团,网络整体采用 NTVMM。

由图 8 分析知,社团隔离后采用 MPGIA 和 NTVMM 恢复网络安全所获得的网络收益是近似相等的,且通常优于在整个网络中采用这两种策略获得的收益。由于社团 3 和社团 6 的节点数量较多,隔离社团后会对较多节点通信造成影响。因此,如果病毒存在于这两个社团时,可对网络整体采用收益较高的策略,不需要隔离社团。此外,网络整体采取策略所获得的收益与病毒所在的具体社团无关。在协同防御系统具体运行时,协同控制中心总会根据病毒所在社团,选择最佳防御方案,如病毒在社团 1 时选择 MPGIA-CI 防御方案,病毒在社团 3 时选择 NTVMM-NE 防御方案。为进一步探究协同防御

的有效性，图 9 给出了网络采用协同防御时两种策略的收益和不采用协同防御时两种策略的收益。

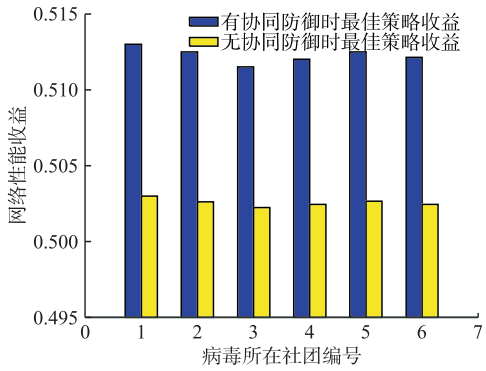

图 9　有无协同防御时最佳收益对比

由图 9 可以看出，协同防御下所采用的最佳策略收益总优于无协同防御时最佳策略收益。协同防御增强了网络对潜伏型病毒的检测能力，降低了防御策略造成的信息损失比例。因此，网络防御的收益得到有效提升。此外，协同防御策略能以更小的通信代价提升网络安全性能。

仿真结果表明，协同防御在防御潜伏型病毒传播方面比无协同防御更具优势，能以较小的通信损失来恢复网络的安全。

5　结语

在大规模网络的主动协同防御模型基础上，融合了信息蜜罐与蜜网、带有节点信任管理功能的防火墙、协同防御策略库等安全模块，构建了新的网络协同防御系统架构。通过设计合理的协同防御机制，打破了网络防御要素间的独立性，使这些防御要素以协同的方式共同抵御外部攻击。相比于无协同防御的系统，该协同防御系能提升网络对潜伏型病毒的防御能力，在一定程度上增强了网络全系统感知、元素认证、防御动态化、行为可监控、快速响应与恢复能力，符合网络空间安全生态系统的要求。此外，协同防御架构模型具有较强的扩展性，针对其它类型的网络攻击，可通过增加安全模块和防御机制，增强协同防御系统的功能。

参考文献

[1] 邬江兴. 网络空间拟态防御导论[M]. 北京：科学出版社，2017.

[2] 沈昌祥. 用主动免疫可信计算构筑新基建网络安全保障体系[J]. 网络传播，2020(6)：38-41.

[3] 沈昌祥. 用主动免疫可信计算筑牢“新基建”网络安全防线[J]. 科学中国人，2020(14)：29-31.

[4] RATHORE S, KWON B W, PARK J H. Block SecIoTNet: Blockchain-Based Decentralized Security Architecture for IoT Network[J]. Journal of Network and Computer Applications, 2019, 143：167-177.

[5] 余洋，夏春和，原志超，等. 计算机网络协同防御系统信任启动模型[J]. 浙江大学学报(工学版)，2016，50(9)：1684-1694.

[6] WANG G, LU S, FENG Y, et al. Ma, A Method to Improve the Security of Information Diffusion in Complex Networks—Node Trust-Value Management Mechanism [J]. IEEE Access, 2019, 7: 138175-138191.

[7] 刘江，张红旗，刘艺. 基于不完全信息动态博弈的动态目标防御最优策略选取研究[J]. 电子学报，2018，46(1)：82-89.

[8] HONG J B, YUSUF E S, SEONG K D, et al. Dynamic Security Metrics for Measuring the Effectiveness of Moving Target Defense Techniques[J]. Computers & Security, 2018, 79(11)：33-52.

[9] 贾召鹏，方滨兴，崔翔，等. 基于协同机制的 Web 蜜罐[J]. 计算机学报，2018，41(2)：413-425.

[10] 赵宇韬，李清宝，张贵民，等. 基于虚拟机监控器的类蜜罐实时内存取证[J]. 浙江大学学报(工学版)，2018，52(2)：387-397.

[11] 杨小牛，王巍，许小丰，等. 构建新型网络空间安全生态体系实现从网络大国走向网络强国[J]. 收藏，2018，4(1)：105-116.

[12] Argonne National Laboratory. Enabling Distributed Security in Cyberspace: Building a Healthy and Resilient Cyber Ecosystem with Automated Collective Action[M]. Washington DC: Department of Homeland Security，2001.

[13] 王刚，胡鑫，伍维甲，等. 网络生态系统动态演化[M]. 西安：西安电子科技大学出版社，2019.

[14] LI T, WANG Y, GUAN Z H. Spreading Dynamics of a SIQRS Epidemic Model on Scale-free Networks[J]. Communications in Nonlinear science and Numerical Simulation, 2014, 19(3)：686-692.

[15] HUANG S Y, CHEN F D, CHEN L J. Global dynamics of a network-based SIQRS epidemic model with demographics and vaccination[J]. Communications in Nonlinear Science & Numerical Simulation, 2017, 43：296-310.

[16] KANG H, LIU K, FU X. Dynamics of An Epidemic Model with Quarantine on Scale-Free Networks[J]. Physics Letters A, 2017, 381(47)：3945-3951.

[17] 王刚，陆世伟，胡鑫，等. 潜伏机制下网络病毒传播 SEIQRS 模型及稳定性分析[J]. 哈尔滨工业大学学报，2019，51(5)：137-143.

[18] 楼润瑜，王备战，王伟. 大规模网络的主动协同防御模型研究[J]. 厦门大学学报(自然科学版)，2010，49(2)：198-204.

[19] LI H J, BU Z, LI A, et al. Fast and Accurate Mining the Community Structure: Integrating Center Locating

and Membership Optimization[J]. IEEE Transactions on Knowledge & Data Engineering, 2016, 28(9): 2349-2362.

[20] 韩忠明,刘雯,李梦琪,等. 基于节点向量表达的复杂网络社团划分算法[J]. 软件学报,2019,30(4):185-201.

[21] 汪林玉,谷科,余飞,等. 基于个人意愿的社会网络团体结构与信息检测方案[J]. 电子学报,2019,47(4):886-895.

[22] 韩阜业,陈震,梁勇,等. 基于覆盖网的协同式网络安全防护与分析系统[J]. 信息网络安全,2012,4:7-13.

[23] MEDICO R, LAMBRECHT N, PUES H, et al. Machine Learning Based Error Detection in Transient Susceptibility Tests[J]. IEEE Transactions on Electromagnetic Compatibility, 2019, 61(2):352-360.

[24] CAMACHO J, MACIÁ-FERNÁNDEZ G, FUENTES-GARCíA N, et al. Semi-Supervised Multivariate Statistical Network Monitoring for Learning Security Threats[J]. IEEE Transactions on Information Forensics and Security, 2019, 14(8): 2179-2189.

[25] ZHOU J T, DU J, ZHU H, et al. AnomalyNet: An Anomaly Detection Network for Video Surveillance [J]. IEEE Transactions on Information Forensics and Security, 2019, 14(10): 2537-2550.

[26] 黄春林,刘兴武,邓明华,等. 复杂网络上疾病传播溯源算法综述[J]. 计算机学报,2018,41(6):1376-1399.

[27] 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.

[28] 葛炎,蒋国平,宋玉蓉,等. 加权网络中考虑边权和度的熟人免疫策略[J]. 计算机工程与应用,2019,55(8):80-85.

[29] WANG G, LU S, FENG Y, et. al. Node Isolated Strategy Based on Network Performance Gain Function: Security Defense Trade-Off Strategy Between Information Transmission and Information Security [C]//International Conference on Data Science, Medicine and Bioinformatics. Singapore: Springer, 2019: 272-286.

[30] BAMAAROUF O, OULD BABA A, LAMZABI S, et al. Effects of Maximum Node Degree on Computer Virus Spreading in Scale-Free Networks[J]. International Journal of Modern Physics B, 2017, 31(26): 1750182.

(编辑:徐楠楠)