一种基于网状关联分析的网络蠕虫预警新方法

卿斯汉，文伟平，蒋建春，马恒太，刘雪飞

（1. 中国科学院 软件研究所，北京 100080；
2. 中国科学院 信息安全技术工程研究中心，北京 100080；3. 中国科学院 研究生院，北京 100080）

摘 要：通过对网络蠕虫行为模式的分析，提出一种基于网状关联分析的网络蠕虫预警的新方法，并设计了预警算法，建立了网络蠕虫预警模型和基于预警算法的原型系统，最后给出相关实验数据和分析结果。与现有的网络蠕虫检测方法相比较，新方法更加有效，而且能够预警未知的网络蠕虫。

关键词：网络蠕虫；行为模式；预警；网状关联分析

中图分类号：TP393 **文献标识码**：A **文章编号**：1000-436X(2004)07-0062-09

A new approach to forecasting Internet worms based on netlike association analysis

QING Si-han , WEN Wei-ping, JIANG Jian-chun, MA Heng-tai, LIU Xue-fei

(1. Institute of Software, Chinese Academy of Sciences, Beijing 100080, China;
2. Engineering Research Center for Information Security Technology, Chinese Academy of Sciences, Beijing 100080, China; 3. Graduate School of Chinese Academy of Sciences, Beijing 100080, China)

Abstract: This paper presents a new approach to forecasting the Internet worm infection based on netlike association analysis after analyzing the behavior pattern of Internet worms, and explores their forecast mechanism we design two forecasting algorithms. An Internet worm forecasting model is established and a prototype based on forecasting algorithms is given. At last, we present the related experimental data and analysis results by using our approach. Comparing with the existing methods, our approach becomes more efficient, and has the characteristic of detecting the unknown Internet worms.

Key words: Internet worm; behavior pattern; forecast and warning; netlike association analysis

1 引言

随着互联网应用的深入，网络蠕虫对计算机系统安全和网络安全的威胁日益增加。特别是在网络环境下，多样化的传播途径和复杂的应用环境使网络蠕虫的发生频率增高、潜伏性变强、覆盖面更广，造成的损失也更大。与传统的主机病毒相比，网络蠕虫具有更强的繁殖

收稿日期：2004-02-10
基金项目：国家自然科学基金资助项目（60083007）；国家“973”重点基础研究发展规划基金资助项目（G1999035810）

能力和破坏能力。

互联网具有开放性的特点，缺乏明确的全局管理机构和中心控制能力[1]，没有完善的机制保证互联网络节点不受网络蠕虫的攻击，因此传统的基于单机的病毒预防技术、基于单机联动的局域网病毒防范技术、病毒防火墙技术[2]等都不能很好地适应开放式网络对网络蠕虫的预警要求。例如，传统的单机病毒检测技术依赖于一定的检测规则，不适应网络蠕虫的检测。因为网络中恶意代码种类繁多，形态千变万化，其入侵、感染、发作机制也千差万别，且具有不可预见性。

著名的 GrIDS [3]（基于图形的入侵检测系统）建立节点间的行为图（activity graph），通过它与预定义的行为模式图进行匹配，检测网络蠕虫是否存在，是当前防御分布式网络蠕虫入侵最有效的工具。但是，我们通过分析认为，GrIDS 在检测网络蠕虫方面仍存在以下缺陷：

GrIDS 的探测点对网络中传输的包信息不进行基于上下文的相关性分析，仅对 TCP 连接的建立和关闭、数据传输中的敏感信息（例如登录用户名等）进行采集。没有充分利用更多的、有效的数据，只作简单的基于事件的关联分析； GrIDS 没有对 TCP 连接中的目标地址和目标服务作有效的分析，而上述分析是判断未知网络蠕虫入侵网络的重要依据，因此 GrIDS 不能检测未知网络蠕虫； GrIDS 检测到网络蠕虫后，由于没有建立任何响应机制，不能提供与内部探测点和外部防火墙的互动，因此不能形成有效的预警和防范机制。

本文提出了一种基于网状关联分析预警网络蠕虫的新方法，克服了以上缺陷。它采用分布式体系结构，充分利用网络环境中各探测点提供的信息和数据，采用数据挖掘和异常检测的方法，通过对各探测点之间的数据作关联分析，实现大规模网络环境下网络蠕虫的有效预警。

2　网络蠕虫预警机制的原理性探索

网络蠕虫是一种智能化、自动化的攻击载体，它会扫描和探测网络上存在服务漏洞的节点主机，一旦渗透成功，会自我复制许多副本，通过局域网、国际互联网或者电子邮件从一个节点传播到另外一个节点。其攻击行为模式如图 1 所示。

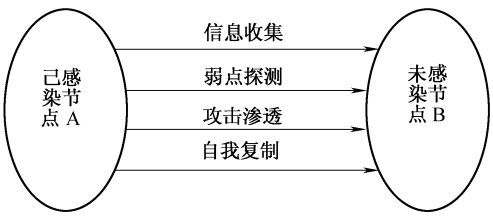

图 1　蠕虫攻击行为模式图

由图 1 可见，网络蠕虫的攻击行为可以分为 4 个阶段：信息收集、弱点探测、攻击渗透和自我复制。信息收集主要完成对目标网络和主机的信息汇集，包括目标网络拓扑结构和网络中节点主机的操作系统类型；弱点探测主要完成对具体目标主机服务漏洞的检测；攻击渗透利用已发现的服务漏洞实施攻击；自我复制完成对目标节点的感染。网络蠕虫在整个攻击过程中，要向目标网络和目的节点发送大量的服务请求。为了加深对网络蠕虫传播共性的认识，我们分析了 2001 年至 2003 年国际权威应急响应网站 CERT 上发布的知名网络蠕虫信息（参看表 1），从这些历史数据分析得到，网络蠕虫传播具有以下特征：

(1) 传出数据的相似性。网络蠕虫在传播的各个阶段，感染节点传出的数据具有相似性。数据包都包含了相应的请求、攻击代码或蠕虫的主体程序，内容相对稳定，因此其传输数据的大小基本不变。例如 Code Red 利用 IIS 漏洞进入被感染节点的主机后，产生 100 个线程，前面 99 个线程都利用随机产生的 IP 地址，探测其它节点主机是否存在 IIS 的 Indexing Service 缓冲区溢出漏洞。在一定时间内，每个线程对目的主机的请求内容都是相似的。

(2) 大量的无效 IP 地址和无效服务请求：网络蠕虫为了在网络中迅速传播和扩散，攻击目标的选择具有盲目性。信息的收集和探测都会导致大量无效 IP 地址的产生，由于攻击目标 IP 地址的无效性，因此相应的服务请求也得不到应答。

(3) 节点间的传播行为具有相似性：网络蠕虫感染一个节点主机后，这个节点成为新的蠕虫载体，并开始扫描、探测、攻击新的目标节点，这个传播行为和最初发生的传播行为具有相似性。

从上面对网络蠕虫攻击行为模式的分析可以看出，如果网络中的某一节点主机在短时间内对外进行大量的 TCP 连接请求，这些连接请求的目标端口相同、数据包大小一定、数据包内容相似，且目标 IP 地址和目标服务都得不到应答，则可判断该节点可能被某种蠕虫侵入。在一定时间范围内，如果网络中另外一个节点也发生了与上述节点类似的行为，则可判断某种网络蠕虫已经侵入该网络并正在扩散。这时，控制中心应当立即预警，并采取有效措施阻止网络蠕虫的大规模探测、渗透和自我复制。这就是通过网状关联分析预警网络蠕虫的基本思想。

表 1 具有相同攻击行为模式的网络蠕虫

蠕虫	信息收集	探测（端口）	攻击渗透	自我复制（端口）	发布文档
Nimda	有	80，139，600	IIS，Code Red II 和 Sadmind 后门	有（80，139，600），E-mail 和网络共享	CA-2001-06
Code Red I	有	80	IIS 4.0/5.0 Index Service	有（80）	CA-2001-13
Code Red II	有	80	IIS 4.0/5.0 Index Service	有（80）	CA-2001-13, IN-2001-09
Adore	有	23，53，111，515	Bind,LPRng,Rpc.statd,wu-ftpd	有（23，53，111，515）	CA-2001-02, IN-2001-01
Sadmind/IIS	有	80，111	IIS, Solstice, Sadmind	有（80，111）80：Windows 平台 111：Unix 平台	CA-2001-11, MS00-078
Lion	有	53	BIND	有（53）	CA-2001-02
Ramen	有	21,111，515	wu-ftp,rpc.statd,LPRng	有（21,111，515）tar 压缩包：ramen.tgz	IN-2001-01
Cheese	有	10008	Lion 后门	有（10008）	IN-2001-05
Digispid.B	有	1433	Microsoft SQL Server	有（1433）	IN-2002-04
Slapper	有	80，443	OpenSSL 和 Apache	有（80）	CA-2002-27
MSSQLWorm	有	1433	Microsoft SQL Server	有（1433）	CA-2003-04

注：在表 1 中，CA（CERT advisory）和 IN (CERT incident note)是由 CERT[4]发布的警告信息。

3 基于网状关联分析的网络蠕虫预警

网络蠕虫对新的目标节点主机进行扫描、自我复制和传播，在网络上传播的路径以网状的方式呈现。如图 2 所示，网络蠕虫从节点 A 传播至节点 B、节点 C、节点 D、节点 E 和节点 F，由于节点 F 受到网络蠕虫感染，所以网络蠕虫再由节点 F 传播至节点 G 与节点 H。长期来看，网络蠕虫传播扩散的路径会产生一个较大的网状图形，如图 3 所示。

网络数据的传输行为，可以通过数据流的源节点与目标节点的关联分析，描绘成网状图。以下，我们通过探测点或控制中心分析数据传输行为，对数据流信息作关联分析。对异常网

络的数据传输行为，进行较长时间的观察。在本节的以下部分，我们给出若干定义和预警算法。首先，我们定义网络蠕虫传播的数据传输行为，其中，节点 A 和节点 B 是控制中心和所有探测点中的任意两个节点。

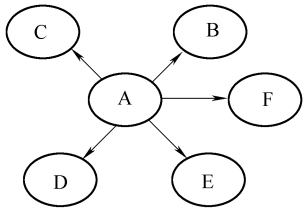

图 2　网络蠕虫传播路径图

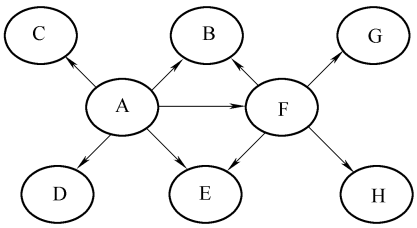

图 3　网络蠕虫扩散图

定义 1　数据传输行为　在 TCP 协议中，四元组（srcHost,srcPort,dstHost,dstPort）惟一确定一个 TCP 连接（srcHost 为源主机 IP，srcPort 为源端口，dstHost 为目的主机 IP，dstPort 为目的端口）[5]。在本文中，为了对数据流进行更细致的分析，对此定义进行扩充，定义如下七元组（timestamp，srcHost，srcPort，dstHost，dstPort，dataSize，data）为惟一确定的 TCP 连接。其含义是，在时间 timestamp 源节点主机（srcHost，srcPort）向目的节点主机（dstHost，dstPort）发出 TCP 连接请求，dataSize 为此次连接请求交换数据的大小，data 为数据的前 m 个字节，其中，m 为可配置参数。

定义 2　数据传输行为集合　所有源节点主机（srcHost，srcPort）向目的节点主机（dstHost，dstPort）发出的 TCP 连接请求的集合 C，C_i 表示 C 中第 i 个 TCP 连接（$1 \le i \le n$，n 为集合 C 中所含 TCP 连接的个数）。

定义 3　传出信息属性　对于任意一个 TCP 连接 C_i（C_i　C），定义 ATTR_FIRST（timestamp，srcHost，dstPort，dataSize，noHost，noService）为此连接的第一传出信息属性，记为 ATTR_FIRST（C_i），其中 noHost 是 dstHost 有效性判断谓词，noService 是请求服务有效性谓词。当 dstHost 没有应答时，noHost 之值为 0；反之为 1。当目的端口的服务请求没有应答时，noService 之值为 0，反之为 1。定义 ATTR_SECOND（dstPort，dataSize，data，noHost，noService）为此连接的第二传出信息属性，记为 ATTR_SECOND（C_i）。第一传出信息属性主要用于判断一个节点是否存在异常数据传出行为。当存在异常数据传出行为的节点时，第二传出信息属性主要用于这些节点间的相似度计算。

定义 4　传出信息属性一致　对于任意两个 TCP 连接 C_i 和 C_j(C_i,C_j　C)，如果 ATTR_FIRST(C_i)＝ATTR_FIRST(C_j)，则称这两个连接的传出信息属性一致。以节点主机(srcHost)为源节点的 m 个 TCP 连接 C_i ，C_{i+1} ，C_{i+m-1}，若　k　[1,m-1], ATTR_FIRST(C_i)＝ATTR_FIRST(C_{i+k})，则称节点主机 srcHost 存在传出信息属性一致的 m 个连接。

定义 5　节点异常数据传出行为　如果节点 A 在特定的时间范围 t 内，存在传出信息属性一致的 N 个连接（N 为判定节点异常数据传出行为的阈值），则认为节点 A 发生了异常数据传出行为。记与节点 A 异常数据传出行为相关的 TCP 连接集合为$[C_A]=\{C_{A\,1},C_{A\,2},\cdots,C_{A\,i},\cdots,C_{A\,N}\}$。$N$ 为$[C_A]$中元素的个数，记作$|[C_A]|=N$，其中 C_A 为该集合的特征连接。

定义 6　节点间异常数据传出行为间的相似性　如果节点 A 和节点 B 发生了异常数据传出行为，且与节点 A 和节点 B 的异常传出行为相关的 TCP 连接集合$[C_A]$和$[C_B]$中的第二传出信息属性 ATTR_SECOND(C_A)与 ATTR_SECOND(C_B)的相似度大于设定阈值时，则认为节点

A 和节点 B 发生的异常传出行为是相似的。

当节点 A 和节点 B 发生的异常数据传出行为相似时，则可判断节点 A 和节点 B 已被同类型网络蠕虫感染。

根据第 2 节对网络蠕虫预警原理的分析，结合本节给出的定义，我们给出如下的网络蠕虫预警算法。预警算法有 2 个：探测点的节点异常传出行为分析算法、控制中心数据关联分析算法，分别描述如下：

N：判断节点异常数据传出行为的阈值

T：时间阈值

S：相似度阈值

A,B：控制中心和所有探测点中的两个节点

ABNORMAL：存储送往控制中心的，与异常数据传出行为相关的 TCP 连接集合的缓冲池

WN：蠕虫网络

Sim(ATTR_SECOND(C_A), ATTR_SECOND(C_B))：传出信息属性相似度计算函数

探测点分析节点异常传出行为的算法如下：

```
/* 判断节点的异常传出行为,A 为预警网络中具有唯一标识的节点*/
Begin
    Create Profile A ATTR_FIRST(C_A)=( IP_A, dstPort_A,dataSize_A,0,0)
    for each Connection C_i: < timestamp,srcHost,srcPort,dstHost , .>
        create ATTR_FIRST (C_i)=(srcHost, dstPort,dataSize,noHost,noService)
          if  ATTR_FIRST (C_i)  ATTR_FIRST(C_A)＝ATTR_FIRST(C_A)
          Then
                save C_i  to [C_A]
          End if
          If  |[C_A]| ≥N and  (timestamp_AN－timestamp_A N-N+1)<T
            Then
                Send [C_A] to ABNORMAL
                Empty [C_A]
                go to Begin
            End if
        End for
End begin
```

控制中心对异常传出行为进行关联分析的算法如下：

```
begin
        Receive：[C_A]  ABNORMAL
        Receive：[C_B]  ABNORMAL
          If  Sim(ATTR_SECOND (C_A), ATTR_SECOND(C_B)) > S
            Then
                A,B  WN
                Send (warning ,Response) to all sensors
```

End if

End begin

上述算法首先由探测点获得 Connection C，提取与节点 A 相关的 TCP 连接，并建立第一传出信息属性集合 ATTR_FIRST。当节点 A 在一定的时间 T 内，存在 N 次传出信息属性一致的连接请求，则可判断节点 A 有异常数据传出行为。同样可以判断，节点 B 是否存在异常数据传出行为。当异常传出行为集合 ABNORMAL 的元素有两个或两个以上时，便可对其属性进行相似度计算：Sim(ATTR_SECOND(C_A)，ATTR_SECOND(C_B)) (本文不对相似度算法详细描述，请参考文献[6])。若相似度大于我们规定的阈值 S，则判断节点 A 和节点 B 已经加入某种类型的蠕虫网络 WN，并向所有的探测点发送预警响应指令。

4　网络蠕虫预警系统的结构模型

网络蠕虫检测的目的在于发现网络中的节点主机是否感染网络蠕虫，而网络蠕虫预警的主要功能是在网络蠕虫尤其是未知的网络蠕虫大规模探测、渗透和自我复制之前，及时发现痕迹进行预警，并采取相应的有效措施。本系统采用分布式协同预警体系结构模型，该模型的基本策略是将大规模网络划分为若干子网，在每个子网中设立探测点，同时建立一个控制中心，在各个子网的探测点和控制中心之间建立预警通道。一旦局部发现疫情，通过预警通报机制能够迅速将该警报信息通知控制中心及其它探测点，从而形成全网络的协同预防机制。其结构模型如图 4 所示。

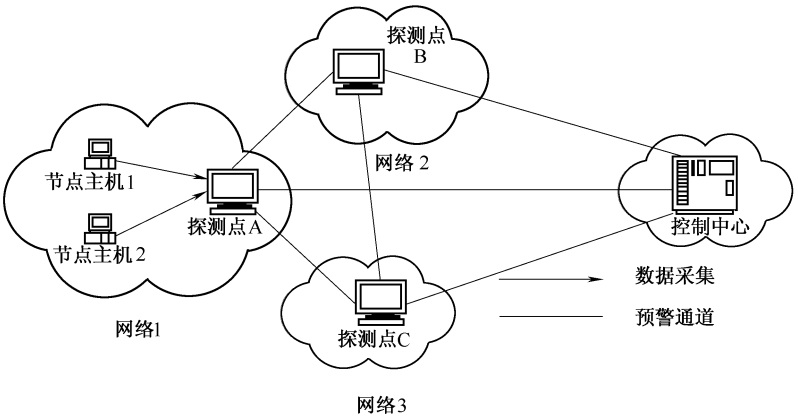

图 4　网络蠕虫预警模型

在网络蠕虫预警模型中，探测点能够完成数据采集、节点异常检测和预警响应功能。控制中心完成数据关联分析、抽取蠕虫特征样本、向探测点发送预警响应指令和分发最新蠕虫特征样本的功能。所以要求探测点和控制中心之间能够很好地协同工作，具体来说主要有以下两个方面：

数据分析协同。探测点对自己采集到的数据进行模式匹配分析，发现一些已知的蠕虫攻击行为；同时，采用异常检测技术判断本网段各节点的异常数据传输行为，并把相关异常数据上报给控制中心。控制中心根据各探测点上报的异常数据进行网状关联分析。

预警响应协同。控制中心如果发觉节点存在异常，立即把预警响应指令发送给异常的探测点；同时，挖掘未知蠕虫，抽取蠕虫特征样本，并向各探测点分发最新蠕虫的攻击特征码。探测点接收控制中心的预警响应指令和最新蠕虫的攻击特征码，及时更新本地的蠕虫攻击特征样本库，并把响应结果返回控制中心。

5　测试结果

我们以 Code Red 和 Nimda 网络蠕虫为例，设计了一个测试环境验证上述技术的有效性。

采用我们自行研制的安胜网络入侵检测系统（类似于 Snort-1.9[7]入侵检测系统），修改了默认的攻击检测和报警机制，屏蔽了探测点对 Code Red 和 Nimda 网络蠕虫的检测，使 Code Red 和 Nimda 相对于当前测试环境是一种未知的网络蠕虫。探测点能够提取各种数据信息，并把这些数据记录到中央数据库中，并且在 Windows 平台上开发了数据分析器，行使控制中心的数据分析功能。测试环境拓扑如图 5 所示。

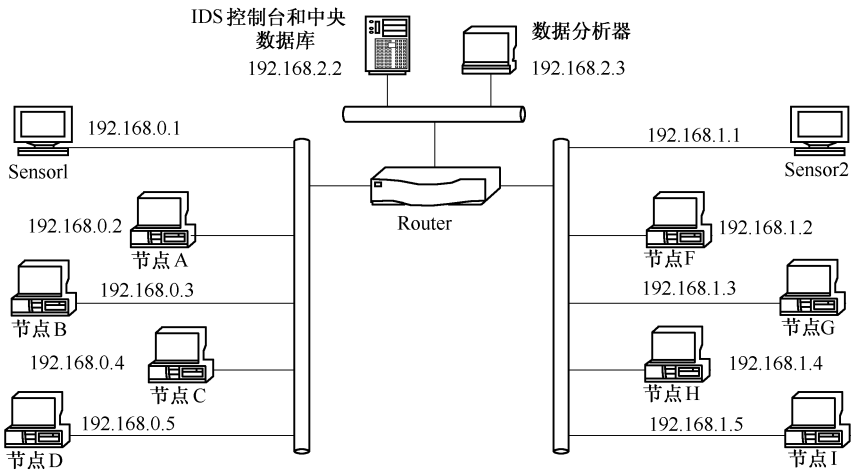

图 5 测试环境拓朴图

在测试环境中，启动安胜入侵检测系统和所有参与测试的节点主机（A，B，C，D，F，G，H，I）。这些测试节点的操作系统均为 Windows 2000 Advance Server，且都为默认设置。为了检验该方法在复杂环境中的抗干扰能力，我们在两个 Sensor 所在的子网启动了发包器，以一定速率发送长度为 64 字节的网络报文。

我们选择节点主机 A（IP 地址：192.168.0.2）释放 Code Red，我们启动数据分析器，对截获的节点 A 传出的数据进行分析，其结果如表 2 所示。

表 2 节点 A 的传出数据属性（IP 地址：192.168.0.2）

timestamp	DstHost	dstPort	dataSize	data(*m*=18)	noHost	noService
15:13:31. 984723	171.64.232.31	80	0x5dc	GET/default.ida?N	0	0
15:13:31. 985175	66.114.64.236	80	0x5dc	GET/default.ida?N	0	0
15:13:31. 985218	65.115.68.15	80	0x5dc	GET/default.ida?N	0	0
15:13:31. 986233	64.67.86.5	80	0x5dc	GET/default.ida?N	0	0
……	……	……	……	……	……	……
15:45:31.312281	192.168.1.2	80	0x5dc	GET/default.ida?N	1	1
……	……	……	……	……		……

由表 2 可以看出，在很短的时间内，就有大量的数据包从节点 A 传出，目标 IP 地址大部分为无效 IP 地址，请求的服务（GET/default.ida?N..）也得不到应答，故可初步判断节点 A 有异常数据传出行为。经过一段时间后，Codered 蠕虫感染了节点主机 C 和 F。为了使我们的分析更具有代表性，我们把节点主机 F 作为新的观察点。

我们调出节点主机 F 的传出数据，如表 3 所示。

表 3　　节点 F 的传出数据属性（IP 地址：192.168.1.2）

timestamp	dstHost	dstPort	dataSize	data(*m*=18)	noHost	noService
16:01:18: 113271	141.149.29.129	80	0x5dc	GET/default.ida?N	0	0
16:01:18: 113750	212.38.12.73	80	0x5dc	GET/default.ida?N	0	0
16:01:18: 115293	160.75.71.14	80	0x5dc	GET/default.ida?N	0	0
16:01:18: 115587	63.222.184.69	80	0x5dc	GET/default.ida?N	0	0
16:01:18: 115811	203.27.20.20	80	0x5dc	GET/default.ida?N	0	0
……	……	……	……	……	……	……

对比表 2 和表 3 中的数据，可以看出，节点 A 和节点 F 的传出信息属性具有相似性，故可以初步判断：节点 A 和节点 F 已经加入 Code Red 蠕虫网络。最后的判断，由控制中心进行相似度计算后作出。

我们对 Nimda 蠕虫进行了相同的测试，在节点 A 释放 Nimda 蠕虫，获取节点 A 的数据传出属性如表 4，一段时间后得到节点 F 的数据如表 5，综合表 4 和表 5 的数据，亦可初步判断：节点 A 和节点 F 加入 Nimda 蠕虫网络，再次证明了上述技术在开放式网络环境下预警网络蠕虫的有效性。

表 4　　节点 A 的传出数据属性（IP 地址：192.168.0.2）

timestamp	dstHost	dstPort	dataSize	data(*m*=19)	noHost	noService
……	……	….	….	….	….	….
18:52:25.563432	192.168.1.2	80	0x21d	GET /msadc/..%e0%80%af../	1	1
……	……	….	….	……		……
18:52:36. 154275	192.168.4.12	80	0x21d	GET /msadc/..%e0%80%af../	0	0
18:52:37. 364324	192.168.4.15	80	0x21d	GET /msadc/..%e0%80%af../	0	0
18:52:38.657234	192.168.4.23	80	0x21d	GET /msadc/..%e0%80%af../	0	0
18:52:39. 983452	192.168.4.34	80	0x21d	GET /msadc/..%e0%80%af../	0	0

表 5　　节点 F 的传出数据属性（IP 地址：192.168.1.2）

timestamp	dstHost	dstPort	dataSize	data(*m*=19)	noHost	noService
18:57:10. 565441	192.168.43.8	80	0x21d	GET /msadc/..%e0%80%af../	0	0
18:57:11. 834522	192.168.43.15	80	0x21d	GET /msadc/..%e0%80%af../	0	0
18:57:13. 154656	192.168.43.23	80	0x21d	GET /msadc/..%e0%80%af../	0	0
18:57:14. 496235	192.168.43.34	80	0x21d	GET /msadc/..%e0%80%af../	0	0
18:57:15. 932413	192.168.43.52	80	0x21d	GET /msadc/..%e0%80%af../	0	0
……	……	….	….	….	….	….

6　结论及未来研究方向

传统的基于主机的病毒预防技术和病毒防火墙技术等，都不能很好地检测和预警网络蠕虫。基于图形的入侵检测系统 GrIDS，是当前防御分布式网络蠕虫入侵最有效的工具。但它也具有一系列缺陷，最重要的是不能发现未知蠕虫。

本文通过对网络蠕虫攻击行为模式的分析，对预警网络蠕虫的原理作了进一步的探索，给出了基于网状关联分析预警网络蠕虫的方法，并设计了预警算法，建立了网络蠕虫预警模型。测试结果证明这种方法能够有效地对网络蠕虫进行预警，且具有较强的抗干扰能力。本方法突破传统技术的框架，从网络攻击的角度，充分利用网络中传输的数据进行异常行为分析，实现网络蠕虫预警的目标。同时，这种方法能够有效地预警未知的网络蠕虫。

我们提出的新方法，对网络蠕虫预警机制进行了有益的探索。今后，我们的研究方向是：网络蠕虫的发展趋势是：更加智能化，隐蔽性更强。因此，需要不断研究新一代网络蠕虫的攻击行为模式。 分布式协同预警技术对预警模型中各组件的协同能力提出了更高的要求，需要作进一步的研究。

参考文献：

[1] LINGER R C, MEAD N R, LIPSON H F. Requirements definition for survivable network systems[A]. Requrements Engineering' 98[C]. Colorado, 1998.14-23.

[2] Understanding symantec' s anti-virus strategy for internet gateways[EB/OL]. http://www. symantec.com/avcenter/reference/ wpnavieg.pdf. 1999.

[3] CHEUNG S, HOAGLAND J, LEVITT K, *et al*. The Design of GrIDS: A Graph-Based Intrusion Detection System[R]. Technical Report CSE-99-2, U.C. Davis Computer Science Department, 1999.

[4] Computer emergency response team(CERT)[EB/OL]. http://www.cert.org/advisories/.

[5] STEVENS W R. TCP/IP Illustrated, Volume 1:The Protocols[M].USA: Addison Wesley, 1994.

[6] CARLA T L, BRODLEY C E. Temporal sequence learning and data reduction for anomaly detection[A]. Proc of the 5th Conference on Computer and Communications Security[C]. New York,1999.

[7] ROESCH M. Writing snort rules: how to write snort rules and keep your sanity[EB/OL]. http://www.snort.org.

作者简介：

卿斯汉（1939-），男，湖南隆回人，中国科学院软件研究所研究员，博士生导师，主要研究方向为信息系统安全理论和技术。

文伟平（1976-），男，湖南桃江人，中国科学院软件研究所博士生，主要研究方向为信息安全对抗、恶意代码。

蒋建春（1971-），男，广西桂林人，工程师，中国科学院软件研究所博士生，主要研究方向为信息安全对抗、网格计算。

马恒太（1970-），男，山东临朐人，博士，中国科学院软件研究所工程师，主要研究方向为网络信息安全和分布式计算。

刘雪飞（1975-），女，湖南宁乡人，中国科学院软件研究所博士研究生，主要研究方向为计算机网络、信息安全、数据挖掘。