第33卷 第14期 计 算 机 工 程 2007年7月
Vol.33 No.14 Computer Engineering July 2007
·安全技术· 文章编号：1000—3428(2007)14—0160—03 文献标识码：A 中图分类号：TP393

基于移动 agent 的网络攻击效果评估数据采集

王会梅，王永杰，鲜 明
(国防科技大学电子科学与工程学院，长沙 410073)

摘 要：计算机网络攻击效果评估技术是信息系统安全评估中一个重要而具有挑战性的课题。该文提出了一种基于移动 agent 的计算机网络攻击效果评估数据采集模型，由研究网络信息系统的性能入手，给出攻击效果评估指标集，研究了移动 agent 技术，给出了基于移动 agent 的计算机网络攻击效果评估数据采集系统的实现思路和相应模型的校验方法。

关键词：移动 agent；攻击效果；评估指标；数据采集

Data Collection Technique of Computer Network Attack Effect Evaluation Based on Mobile Agent

WANG Huimei, WANG Yongjie, XIAN Ming
(School of Electronic Science and Engineering, National University of Defense Technology, Changsha 410073)

【Abstract】Attack effect evaluation technology for computer networks is an important and challenging subject of security evaluation in information systems. This paper proposes a data collection model of computer network attack effect evaluation based on mobile agent and proper network security index set from the study of the performance of networked information system. Mobile agent technology is studied. The implementation idea of the data collection of attack effect evaluation system based on mobile agent and the corresponding model verification method are also presented.

【Key words】 mobile agent; attack effect; evaluation index; data collection

计算机在各个领域的广泛应用和网络技术的迅猛发展极大地丰富了网络信息资源，其潜在的军事应用价值也逐渐为各国所重视，以美国为首的世界各国均在备战信息战，信息系统的安全性成为一个亟待解决的问题。网络攻击效果评估技术作为信息系统安全综合评估技术的一个组成部分，具有重要的意义：

(1)目前广泛投入使用的各种网络信息系统急须建立一套有效的网络攻击评估准则和检测方法，用以提升系统的网络生存能力，提高系统应对复杂网络环境下各种突发网络攻击的能力；

(2)在反击恶意攻击时，网络攻击效果评估技术可以为网络反击样式和反击强度提供合适的应对策略。网络攻击效果评估的数据采集系统是整个评估过程的基础，为其提供数据支持，直接关系到网络攻击效果评估模型和评估结果的准确性。

网络攻击效果评估的数据采集是当前研究的一个难点。目前关于网络数据采集领域的研究大都集中在网络监控和流量分析，并借鉴了入侵检测系统(IDS)探测引擎的实现思路。文献[1]依照一个基于 Web 的网络管理模型，针对计算机网络性能管理功能域中的性能监视功能进行了分析，并利用 Java 开发了一个基于 Web 的网络性能监视工具；文献[2]从流量工程的角度提出了网络性能评价的原理、体系和方法，给出了基于流量工程的性能监测和控制的实现方案，实现了端到端的网络性能测量和分析；文献[3]研究了网络监控中的包分析和流量信息收集，并提出了相应的实现结构。文献[4]从计算机网络安全评估的角度出发，实现了一种由被动监听、主动探测和信息预处理 3 部分构成的网络实时信息采集技术，但该方法还停留在定性研究方面。

1 攻击效果评估指标的选取

选取合理的评估指标体系是进行网络信息系统攻击效果评估的前提条件，对计算机网络信息系统攻击效果评估系统具有重要意义。

计算机网络信息系统的性能状况主要通过系统的可靠性、可用性、保密性、完整性、可控性、正确性和不可抵赖性等方面衡量。

(1)可靠性指网络信息系统能够在规定的条件下和时间内完成规定功能的特性。网络信息系统的可靠性测度主要有 3 种：抗毁性，生存性和有效性；

(2)可用性指网络信息系统可被授权实体访问并按需求使用的特性，是系统面向用户的安全性能；

(3)保密性指网络信息不被泄漏给非授权用户、实体或过程，或供其利用的特性；

(4)完整性指网络信息未经授权不能进行更改的特性，即网络信息在存储或传输过程中保持不被偶然或蓄意删除、修改、伪造、乱序、重放、插入等破坏和丢失的特性；

(5)可控性指对网络信息的传播及其内容具有控制能力的特性；

(6)正确性指网络信息系统所输入、处理、存储的数据应具有合理、真实和正确的特性；

(7)不可抵赖性指在网络信息系统的信息交互过程中，确

基金项目：国家自然科学基金资助项目(60372039)
作者简介：王会梅(1981－)，女，硕士研究生，主研方向：信息网络安全；王永杰，博士研究生；鲜 明，博士研究生、副教授
收稿日期：2006-08-24 **E-mail：**freshcdwhm@163.com

保参与者身份的真实同一性。

计算机网络攻击的效果就是目标网络系统这些性能改变的综合体现，但不能直接将这些属性作为计算机网络攻击效果的评估指标。为了度量这些属性的值，必须将其进一步分解为易于度量的子属性的集合，该过程可以持续进行，直至各子属性都能被直接度量。

基于上述的分析，主机遭到攻击所造成的损失是通过主机的通信链路、通信连接、数据、软件系统和硬件系统 4 个方面来体现的，由此提出计算机网络攻击效果评估指标体系，如图 1 所示。

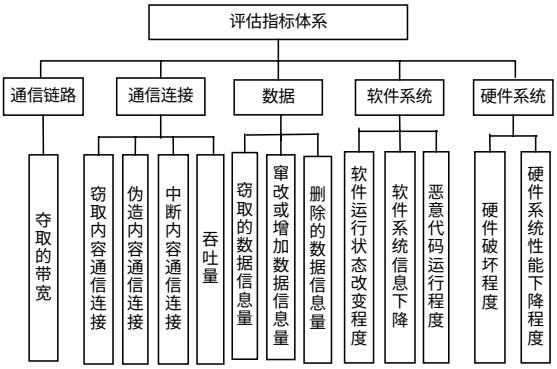

图 1　计算机网络攻击效果评估指标体系

2　移动agent[5,6]

移动agent的概念是 20 世纪 90 年代初由General Magic公司在推出商业系统Telescript时提出的，它是一个能在异构网络中自主地从一台主机迁移到另一台主机，并可与其他agent或资源交互的程序，其实质是agent技术与分布式计算技术的结合[5]。

移动 agent 系统由移动 agent 和移动 agent 服务设施(或称移动 agent 服务器)2 部分组成。移动 agent 服务设施 agent 传输协议(agent transfer protocol)实现 agent 在主机间的转移，并为其分配执行环境和服务接口。agent 在服务设施中执行，通过 agent 通信语言(agent communication language，ACL)相互通信并访问服务设施提供的服务。

移动 agent 的结构模型如图 2 所示。

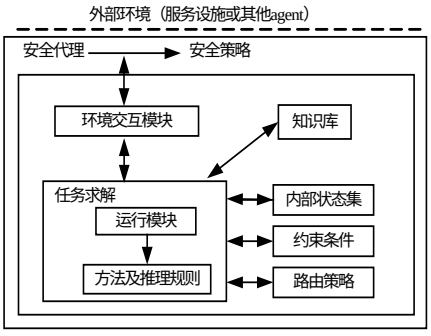

图 2　移动 agent 的结构模型

移动 agent 的主要优点及其应用：

(1)降低网络负载：这一特征概括了基于移动 agent 的分布式计算的特点，即将计算移往数据。这样做可以减少网上原始数据的流量。

(2)克服网络延迟：由中央处理器将移动 agent 派遣到系统局部，直接执行控制器的指令，从而消除网络延迟所带来的隐患。

(3)包装不同协议：可以移动到远程主机上，通过专用协议建立私有数据交换通道。

(4)异步和自主执行功能：可以将任务嵌入到移动 agent 之中，再被派遣到网络上。之后，移动 agent 便可以独立创建它的进程，异步、自主地完成所肩负地任务；移动设备则可以在这之后再连接上网络，收回 agent，取得服务结果。

(5)动态适应环境：移动 agent 具有感知运行环境和对其变化做出自主反应的能力。

(6)自然的异构性：开放分布式计算各平台之间，往往从硬件到软件都是异质的。移动 agent 仅仅依赖于它们的执行环境，因而为进行无缝地系统集成提供了极为有利的条件。

(7)健壮性和容错性：由于移动 agent 具有对不利的情况和事件动态做出反应的能力，因此减小了建立健壮和容错的分布式系统的难度。一台主机被关闭前可以给正在运行的移动 agent 发出警告，使它们快速移动到网络上其他主机中继续运行。

鉴于以上优点，移动 agent 在电子商务、分布式信息检索、网络攻击仿真评估、信息发布、个人助手、安全中介、电信网络业务、工作流应用及并行处理等应用中具有很大的潜力，特别适用于解决传统方法中代价过高或无法解决的问题，如果需要人性化的进程，agent 具有观察能力、主动适应能力，而不是通过一些预先严格确定的接口函数与外界进行交互，能根据目标主动规范化自己的行为，使用户界面达到“人性化”；如需要集成旧系统，可通过给旧系统上包装一层 agent 外壳，其他系统可以调用旧系统的功能。

3　基于移动 agent 的网络攻击效果数据采集模型

鉴于移动agent的优点，设计了基于移动agent的数据采集模型框架[8]。为了对攻击效果性能指标进行数据采集，搭建了一个网络攻击效果评估数据采集系统的实验平台(如图 3 所示)，通过对目标靶网发动模拟攻击，测试网络安全性能指标参数的变化，得到具体的评估性能指标。

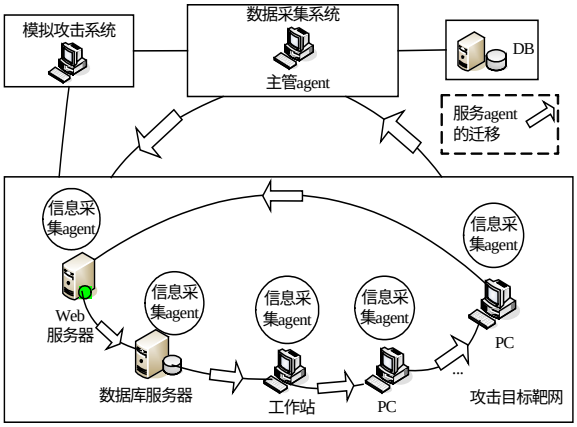

图 3　网络攻击效果评估数据采集系统实验平台

根据分担的功能不同，agent 分为如下 3 种：

(1)主管 agent。它一方面与模拟攻击系统进行交互，确定攻击的方法，并且根据不同的攻击派遣相应的信息采集 agent 到目标节点上进行信息采集；另一方面对服务 agent 返回的信息进行收集，加工整理，最终把结果存进数据库中。另外，移动 agent 还负责任务的规划和统筹管理。该 agent 驻留在信息采集系统中。

(2)服务 agent。它可以运行在信息采集系统中或被管节点上，可以与主管 agent 和信息采集 agent 进行交互。为了共同完成求解任务，服务 agent 之间可以进行相互合作，共享

各自的资源、能力和知识，构成同一个任务组，并由主管 agent 负责协调。需要注意的是，当服务 agent 运行在目标靶网上并且其中一个被管节点瘫痪时，服务 agent 可向主管 agent 汇报超时，主管 agent 再采取相应的措施。

(3)信息采集 agent。它被派遣到攻击目标靶网的节点上运行，负责信息的采集。根据所采信息的不同，有不同的功能的信息采集 agent。同时它要为服务 agent 提供所需数据。当所要采集的指标变化或更新时，节点上的信息采集 agent 被新的 agent 替代。因而提高了管理的灵活性和可扩展性。

下面以网络系统的可用性为例，介绍几类信息采集 agent。

经研究发现，在网络的可用性方面，对网络性能影响较大的指标主要有以下几项：(1)吞吐量：单位时间内节点之间成功传送的无差错的数据量；(2)信道利用率：在特定时间段内所使用的网络容量与带宽之比；(3)延迟：报文从进入到离开网络/节点/链路网络的时间间隔；(4)延迟抖动频率：指单位时间内平均延迟变化的次数。(5)CPU 和内存的利用率。根据这些指标，确定有 4 类信息需要采集：

(1)网络资源吞吐量信息采集 agent。可通过使用简单的网络管理协议 SNMP，采集操作就是 SNMP 的 GET 操作，采集对象是 SNMP MIB-II 接口的变量。进一步分析处理可得端口收发总字节数、端口接收包总数、端口发送包总数。前面采集到的原始数据是端口某一时刻的数据，需要在此基础上比较前后 2 个时刻的差别，计算出该时间段的数据流量。

(2)信道利用率信息采集 agent。对于信道利用率需要采集一段时间内的网络流量。根据采集到的数据，在每个采样时间段内进行统计计算可得到信道利用率，计算公式为

$$U_i = [B_T(i)/T_i]/B \tag{1}$$

其中，$B_T(i)$ 为第i个采样时刻在T_i时间段内传送的数据总量；B为网络带宽。

(3)网络延迟和延迟抖动频率信息采集 agent。采集网络包，并把每个包的时间戳和序列号在传输端和接收端记录下来，进一步计算得到希望值。网络延迟 R 被作为数据包发送和到达之间的间隔计算。计算公式为

$$T_i = T_R(i) - T_T(i) \tag{2}$$

其中，T_i是第i个包的延迟；$T_R(i)$是第i个包的收到时间戳；$T_T(i)$是第i个包的发送时间戳。再计算归一化延迟抖动频率 ω，网络受到攻击后其延迟抖动频率一般会增大，从而影响网络服务的QoS。延迟抖动时间通过 2 个连续的包之间的时间间隔来计算，假设第i时刻收到第n个数据包，则i时刻的延迟抖动频率 $f(i)$为

$$f(i) = 1/\{[T_R(n) - T_T(n)] - [T_R(n-1) - T_T(n-1)]\} \tag{3}$$

其中，$T_R(n)$是第 i 个包的收到时间戳；$T_T(n)$是第 i 个包的发送时间戳；$T_R(n-1)$是第 i-1 个包的收到时间戳；$T_T(n-1)$是第 i-1 个包的发送时间戳。

(4)攻击目标子节点主机的 CPU 利用率、内存利用率信息采集 agent。可直接调用任务管理器得到所需数据。并记录一段时间内的值，进行统计分析得到。

根据系统的工作流程图(图 4)，工作方式简要叙述如下：

(1)主管 agent 将信息采集 agent 指派到管理节点执行各自的任务。信息采集 agent 驻留在节点上，根据主管 agent 给其设定的参数进行相应的数据采集，并按照其自身的功能作必要的计算分析，将结果返回给主管 agent。

(2)主管 agent 派遣服务 agent 实现多种应用。服务 agent 顺序访问主管 agent 所安排的一系列节点，在一个节点获得统计数据并进行必要的计算分析后访问下一个节点。访问完各指定节点后，返回给主管 agent。如果某个节点由于瘫痪连接不通时，服务 agent 应该以超时报告主管 agent，以作相应的处理。

(3)主管 agent 根据服务 agent 返回的数据进行分析整理，存入数据库中并提交数据采集报告。

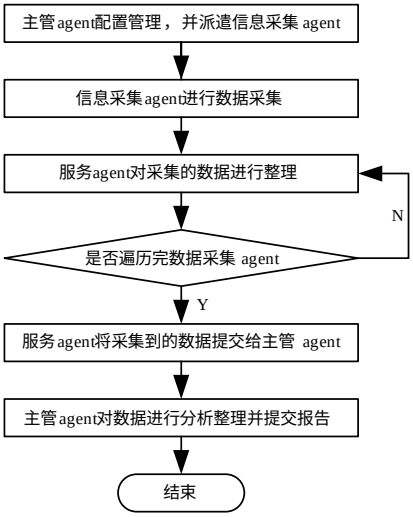

图 4　系统的工作流程

4　结论

计算机网络攻击效果评估技术在我国网络信息系统建设、国家信息安全基础设施实施和网络攻防对抗实践等诸多领域具有广泛的应用价值，而数据采集又为效果评估提供数据支持，因此，研究具有重要的意义。鉴于移动 agent 的优点，本文提出了一种基于移动 agent 的计算机网络攻击效果评估数据采集模型，并详细阐述了攻击效果评估指标的选取。在此基础上，给出了基于移动 agent 的攻击效果评估数据采集系统的实现思路和相应的模型校验方法。关于模型的进一步深化和完善以及模型的实现正在研究之中。

参考文献

1 萧　幪, 丁志强. 基于 WEB 的网络性能监视工具[J]. 计算机工程与应用, 2001, 37(2): 61-64.

2 何　飞, 李　建, 有　悦. 基于流量工程的网络性能监测和控制系统[J]. 计算机工程与应用, 2001, 37(16): 50-53.

3 高　翔, 苏广文, 胡正国. 入侵检测系统中的网络监测[J]. 微电子学与计算机, 2002, 19(2): 37-39.

4 张义荣, 赵志超, 鲜　明, 等. 网络安全评估中的实时信息采集技术研究[J]. 计算机应用研究，2004, 21(增刊): 222-223.

5 张云勇, 刘锦德. 移动 agent 技术[M]. 北京: 清华大学出版社, 2003-09.

6 Picco G P. Mobile Agents: An Introduction[J]. Journal of Microprocessors and Microsystems, 2001, 25(2): 65-74.

7 Sinkovic V, Lovrek I. Generic Model of a Mobile Agent Network Suitable for Performance Evaluation[C]//Proceedings of the 4th International Conference on Knowledge-based Intelligent Engineering Systems and Allied Technologies. 2000: 675-678.