基于移动代理和动态拓扑结构的入侵检测系统模型

邓一贵[1,2] 王 康[2] 涂光友[1,2] 邱全杰[2]

(重庆大学计算机学院 重庆 400044)[1] (重庆大学网络技术与管理中心 重庆 400044)[2]

摘 要 分布式网络攻击的破坏性越来越大。网络在运行中拓扑结构又是在动态变化的。如何在拓扑结构变化的网络中去发现和阻止网络攻击,本文提出了一个基于移动代理技术的模型。模型由拓扑发现代理、拓扑计算代理、检测代理、追踪代理、阻击代理组成。拓扑发现代理和拓扑计算代理完成网络拓扑结构跟踪,检测代理、追踪代理、阻击代理完成对分布式网络攻击的探测、追踪、阻止。该模型具有适合大规模网络、占用网络带宽少、能自动跟踪网络拓扑变化、系统的入侵检测和响应与拓扑变化无关等特点。

关键词 入侵检测,入侵阻击,移动代理,动态拓扑

Intrusion Detection System Model Based on Mobile Agent and Dynamic Topology

DENG Yi-Gui[1,2] WANG Kang[2] TU Guang-You[1,2] QIU Quan-Jie[2]

(College of Computer Science, Chongqing University, Chongqing 400044)[1] (Network Center, Chongqing University, Chongqing 400044)[2]

Abstract Destroying computer network of distributed attack becoming severer and severer. Topology is dynamic during operation of computer network. How to discover and hold back attacks in this case? A model based on mobile agent technology is presented in this paper. The model is consisted of topology discovering agents, topology computing agents, attack detecting agents, attack tracing agents, and attack stopping agents. Topology is generated from topology discovering agents and topology computing agents. Detecting, tracing and stopping attacks is respectively done by attack detecting agents, attack tracing agents, and attack stopping agents. The system based on the model can adapt to large-scale network, generates less traffic, automatically trace change of topology. It can detect and response to attacks independent of changing of topology.

Keywords Intrusion detection, Intrusion holding back, Mobile agent, Dynamic topology

1 引言

随着 Internet 的迅速发展,越来越多的系统遭到入侵攻击的威胁。当今攻击者的知识日趋成熟,攻击手段的日趋复杂多样,传统的安全方法,已经无法满足网络安全需要,网络的安全防卫必须采用一种纵深的、多样的手段,随着 Internet 的发展,网络规模和技术的膨胀将导致各种数据量剧增,黑客采用联合攻击的方式增多,这种问题会更加突出。入侵检测系统已成为必不可少的重要手段。网络入侵检测现已成为目前众多网络安全手段中的核心技术,它能弥补其他安全技术的不足。

移动 Agent 技术是人工智能技术、分布式技术和网络技术的产物,它的优势逐渐在各个领域中的不断体现,人们对于 Mobile agent 技术的优点与入侵检测技术的结合体现极大的兴趣,有相当的研究表明该技术能够对其检测的实时性、准确性有相当大的提高同时对于扩大网络的检测范围有很明显的作用。

网络在运行中拓扑结构因设备运行状态的变化而在动态变化,如何在变化的拓扑结构中去发现和阻止网络攻击? 本文采用移动 Agent 技术来跟踪网络在运行中拓扑结构的动态变化以及网络入侵检测和入侵阻击。本文第 2 节提出了一个基于移动代理技术的入侵检测系统的设计思想及其体系结构。第 3 节介绍了入侵检测系统各代理算法及实验。最后对所提出的入侵检测系统的特点进行了总结并提出了以后进一步研究内容。

2 入侵检测系统模型的设计思想及体系结构

入侵检测系统模型由拓扑发现代理、拓扑计算代理、入侵检测代理、追踪代理、阻击代理组成。拓扑发现代理和拓扑计算代理完成网络拓扑结构跟踪,检测代理、追踪代理、阻击代理完成对入侵的探测、追踪、阻止。拓扑发现代理向全网只发送链路状态变化事件,这样既适合大规模的网络又尽量减少了入侵检测系统占用网络带宽。考虑到绝大部分时间拓扑状态是相对稳定的事实,拓扑计算代理也只更新本地节点到其他节点发生了变化的最短路径表项,如此既跟踪拓扑状态的变化又减少了对最短路径表写入的内容和次数,提高了拓扑计算代理的处理效率和最短路径表的相对稳定性。拓扑发现代理、入侵检测代理和追踪代理只向本地节点当前可到达的节点发送相关消息或事件,减少了系统对网络带宽的占用并使得系统的入侵检测和响应与拓扑变化无关。基于以上的设计思想,入侵检测系统模型设计如图 1 所示。

3 入侵检测系统各代理算法设计及实验

根据所提出的入侵检测系统体系结构及其设计思想,各代理的具体算法如下。

阻击代理:

```
BEGIN
    IF 本节点是网络节点 THEN
       从断口列表中取出一个端口;
    REPEAT
       IF 端口连接的是主机节点 THEN
          IF 端口未指派阻击代理 THEN
             指派阻击代理
          END IF
          IF 端口未收到阻击代理发回的阻击成功的消息 THEN
             REPEAT
                封闭端口一定时间;
                开启端口;
                询问阻击代理阻击结果
```

邓一贵 博士研究生,主要研究方向:计算机网络信息安全;**王 康** 教授,硕士生导师,主要研究方向:INTERNET 网络技术,信息网络安全技术;**涂光友** 博士研究生,主要研究方向:计算机网络信息安全;**邱全杰** 硕士,主要研究方向:INTERNET 网络技术,计算机网络信息安全。

```
            UNTIL 阻击代理阻击成功
          END IF
        ELSE [//端口连接是网络节点]
          从该端口转发相关被入侵节点子集信息
        END IF
        移到下一端口
        UNTIL 所有端口都收到相关阻击代理阻击成功消息 OR 超时
        向上一级代理发阻击成功消息或超时消息
    ELSE [//本节点是主机节点]
      关闭入侵所利用的 TCP 或 UDP 端口;
      杀死入侵进程;
      检查与入侵有关的系统漏洞和当前系统所打的补丁情况;
      向上一级代理发阻击成功消息
    END IF
END
追踪代理:
BEGIN
    WHILE 被入侵节点集合不为空
        从集合中取一个被入侵节点;
        根据被入侵节点从当前最优路由表中找出去往该节点的下一跳地址;
        IF 下一跳地址为新出现的地址 THEN
          新建一个子集合;
          将被入侵节点地址加入到该子集合
        ELSE
          将被入侵节点地址加入到该子集合
        END IF
        从被入侵节点集合减去刚才取出的被入侵节点
    END WHILE
    REPEAT
      从下一跳地址集合中取出一个地址;
      向该地址发送所对应的被入侵节点子集合信息;
      从下一跳地址集合中减去该地址
    UNTIL 下一跳地址集合为空
END
入侵检测代理:
BEGIN
    监视当前系统事件;
    IF 有异常 THEN
      将异常信息与入侵特征库中特征进行匹配;
      IF 匹配成功 THEN
        生成追踪代理;
        将被入侵节点及入侵信息通知追踪代理
      END IF
    END IF
    监视当前网络事件;
    IF 有其他节点的入侵检测代理的入侵通知 THEN
      生成追踪代理;
      将网络通知中的被入侵节点集合通知追踪代理
    END IF
    IF 检测到经本节点攻击其他节点 THEN
      向被攻击节点的入侵检测代理发送通知
    END IF
END
拓扑发现代理:
BEGIN
    检测本地邻接节点连接状态是否变化:
    IF 连接状态有变化 THEN
      向本地拓扑计算代理发送状态变化事件;
      向全网可达的拓扑计算代理发送连接状态变化事件
    END IF
END
拓扑计算代理:
BEGIN
    IF 有本地链路事件到来或者其他节点发来链路状态变化事件
      THEN
      调整本地的全网链路状态图;
      根据 Dijkstra 算法计算本地节点到其他节点的最短路径;
      IF 到其他节点的最短路径发生变化 THEN
      更新最短路径表中相应的表项
      END IF
    END IF
END
```

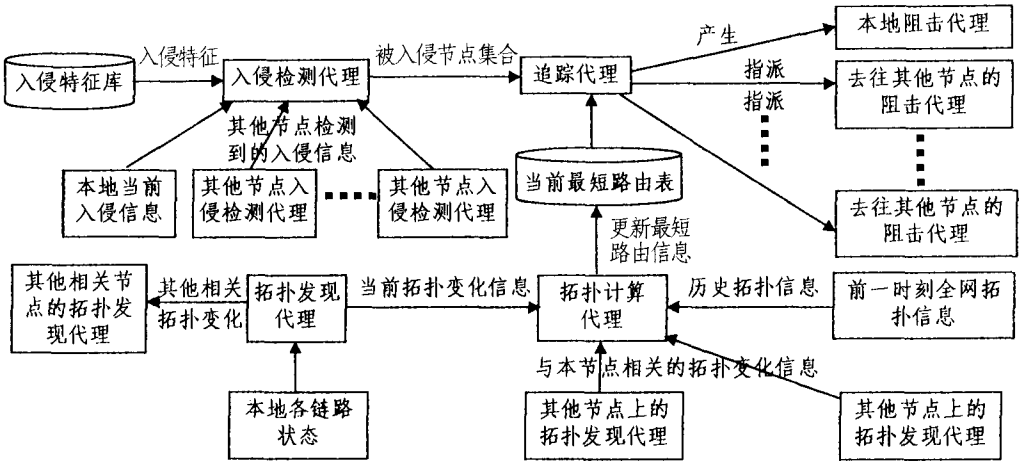

图 1　入侵检测系统模型的体系结构

基于移动代理和动态拓扑结构的入侵检测模型系统在 IBM Aglets 平台上进行编程实验，并对模型的能否跨网段、适用的网络规模、占用网络带宽情况、自动跟踪网络拓扑变化情况、系统的入侵检测和响应与拓扑变化是否相关等目标进行了测试，测试的结果较好地体现了模型的设计目的和思想。

测试环境选用 4 台 Window2000 professional PC 机(PⅢ 450，128M 内存，20G 硬盘)和一台 Linux 服务器(P4 1.3G，256M 内存，40G 硬盘)；网络环境为具有 40 多个子网的校园网。测试软件工具采用 Snot，根据检测规则发送指明规则文件、源地址、目的地址以及数据包产生频率入侵数据包。Snot 的使用简单，只需要指明规则文件、源地址、目的地址以及数据包产生频率。例如：snot -r snort. rules -s 192. 168. 0. 1 -d 192. 168. 1. 1/24 -l 0. 1 在当前运行的主机上发送源地址为 192. 168. 0. 1，目标网段为 192. 168. 1. 1/24，数据包符合 snort. rules 格式的数据包，发送频率为每 0. 1 秒发送一个包，即 10pk/s。

总结　移动 Agent 技术对入侵检测和入侵阻击具有实时性、准确性，对于扩大入侵检测的范围和网络拓扑跟踪以及灵活进行入侵阻击有很明显的作用。实验表明，本文所提出的入侵检测系统模型具有适合大规模网络、占用网络带宽少、能自动跟踪网络拓扑变化、系统的入侵检测和响应与拓扑变化无关等特点。

本文的重点是研究入侵检测和入侵阻击的系统模型，未涉及入侵检测代理和入侵阻击的具体内容。以后将进一步研究入侵检测和入侵阻击的相关技术及其在实际网络如何同移动 Agent 技术相结合，并研究其有效性和可靠性。

参 考 文 献

1　翁莉萍. 基于轻量级 Agent 的入侵检测模型. 计算机工程，2002，5

2　IBM Aglet Workbench，http://www. trl. ibm. co. jp/aglets

3　蒋建春，马恒太，等. 网络安全入侵检测：研究综述，软件学报，2000，11(11)：1460～1466