基于移动代理的新型IDS维护更新机制设计

罗光春，杨俊辉，卢显良

(电子科技大学信息中心 成都 610054)

【摘要】提出了一种基于移动代理的新型分布式入侵检测系统。该系统是针对广域网环境专门设计的，数据的处理通过各节点所设置的代理来进行分布式计算，不仅能实现全网络范围内的入侵检测功能，具有良好的可移植性；而且对网络系统和主机的资源占用较低，减少了出现网络瓶颈的可能。还建立了移动代理的新型分布式入侵检测系统的体系结构和理论分析模型，并讨论了该系统的维护更新机制。

关 键 词 移动代理; 分布式入侵检测系统; 性能; 数据转移

中图分类号 TP309 文献标识码 A

A Novel Distributed IDS Based by Mobile Agent

LUO Guang-chun，YANG Jun-hui，LU Xian-liang

(Information Centre, UEST of China ChengDu 610054)

Abstract This paper presents a new Mobile Agent Distributed IDS (MADIDS) system basing on the mobile agents. This system is specifically designed for WAN, In MADIDS, the agents that are set at each node process the data transfer by distributed computation architecture. It has the ability of intrusion detection within the entire network and has good portability. The consumption of the network and servers' resources is not high, which means the possibility of network bottleneck is decreased. In this paper, we construct the infrastructure and theoretical model of MADIDS, and the deficiencies of MADIDS and future research work are also indicated.

Key words mobile agent; distributed intrusion detection system ; performance; data transfer

现代入侵检测技术系统的发展趋势是宽带高速实时的检测技术、大规模分布式的检测技术、数据挖掘技术、更先进的检测算法和入侵响应技术。移动代理使得分布式协同入侵检测更为灵活，尽管基于移动代理技术的(Intrusion Detection System，IDS)产品目前还没有，但相关的研究和实验室样品已出现较多[1]。移动代理作为一种新兴技术，在大规模、分布式、跨平台的应用中拥有独特优势。对比于静态代理，移动代理技术在入侵检测系统中的应用1996年就有人提出[2]。移动代理具有移动性、自我藏匿性、受损后的自我恢复性等特点，非常适合用于入侵检测，目前最为典型的实例是文献[3]介绍的移动代理的新型分布式入侵检测系统 (Mobile Agent Distributed Intrusion Detection System，MADIDS)，该系统将移动代理用于对入侵行为的检测。本文的研究重点是将移动代理技术运用于入侵检测系统的大规模配置，以及维护系统的完整性和一致性方面[4]。

1 MADIDS体系结构

移动代理的新型分布式入侵检测系统(Mobile Agent Distributed Intrusion Detection System，MADIDS)使用分层体系结构，将部署在整个广域网(Wide Area Network，WAN)上的入侵检测系统划分为若干个域[5~7]。在该体系结构中每个域由域服务器管理，所有域服务器由主服务器管理，其体系结构如图1所示。图中的1~*j*为域的编号；*n*1~*nj*表示每个域的主机个数。在MADIDS中，Agent担负着数据传输、通信、管理协作等任

收稿日期：2004 – 07 – 12

作者简介：罗光春(1974 –)，博士，副教授，主要从事计算机网络信息技术、信息系统安全方面的研究.

务，如图1所示。本文中，广域网连接以粗虚线表示，局域网连接以粗实线表示。

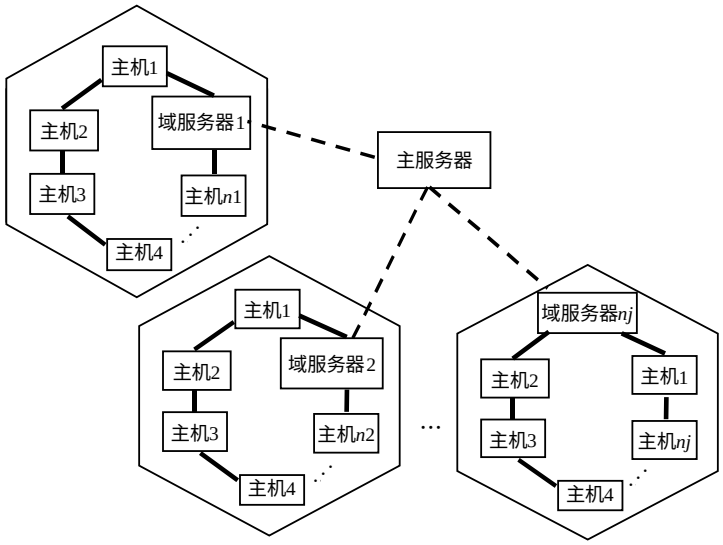

图1 MADIDS 体系结构图

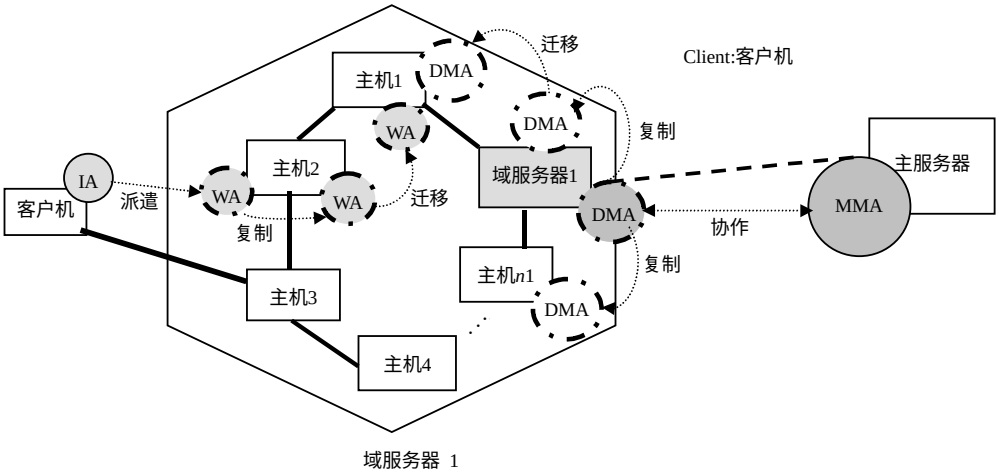

图2 MADIDS中的分工协作图

在移动代理的新型分布式入侵检测系统(MADIDS)中，Agent担负着数据传输、通信、管理协作等任务，如图2所示。各入侵检测部件的功能分别是：

1) 事件产生器(Event Generators，EG)分为基于主机的事件产生器(Host Based Event Generators，HEG)和基于网络的事件产生器(Network Based Event Generators，NEG)两种。NEG 并不需要在每台主机上部署，在一个域的所有主机中只需部署两台即可，一台作为主 NEG，用于获取网络上的入侵数据，一台作为备份 NEG，用于系统功能的备份、修复和抗毁。

2) 事件分析器(Event Analyzers，EA)从逻辑上分为基本事件分析器(Basic Event Analyzers，BEA)和扩展事件分析器(Extend Event Analyzers，EEA)两种。EEA 在每个域中不配置于每台主机(Host)上，而是配置于域服务器中。

3) 控制台(Console，CS)通过接受事件分析器的分析结果，来判定是否存在入侵行为。

4) 响应单元(Response Units，RU)对入侵行为进行相应响应和处理。

5) 事件数据库(Event Databases，ED)分为存放于主服务器的事件数据库(Event Databases Saved in Main Server，EDMS)、存放于域服务器的事件数据库 EDDS(Event Databases Saved in Domain Server)和存放于主机的事件数据库(Event Databases Saved in Host，EDH)3 个层次，分别存放于主服务器、域服务器和所有主机上。

6) 系统管理平台(System General Manager，SGM)在主服务器上，负责 MADIDS 系统的整体管理、维护、升级等工作。

各入侵检测部件的部署情况如图 3 所示。

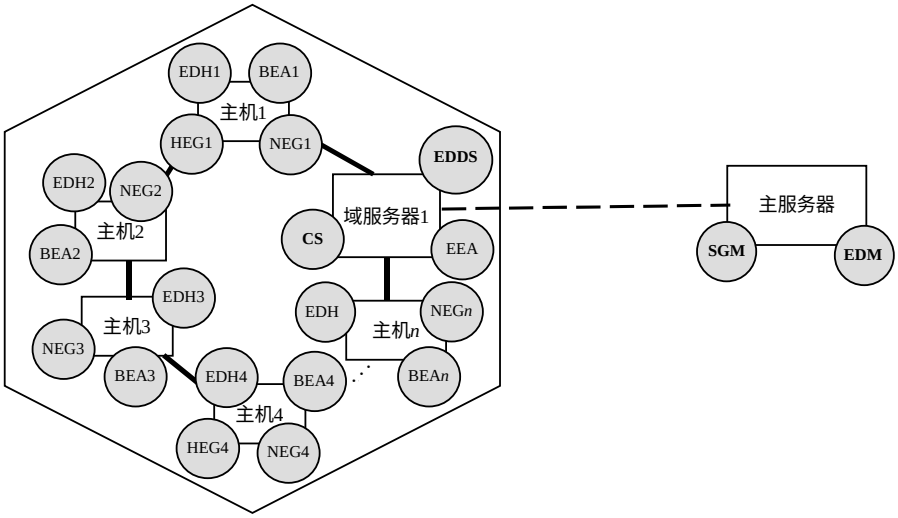

图3　MADIDS中各入侵检测部件的部署情况

2　MADIDS的维护更新机制

如前所述，事件数据库 ED 分为存放于主服务器的事件数据库、存放于域服务器的事件数据库和存放于主机的事件数据库 3 个层次。在以上层次结构的基础上，MADIDS 中有系统整体规则生成流程和系统整体规则更新流程两个系统更新流程。限于篇幅，本文仅介绍整体规则生成流程，如图 4 所示。

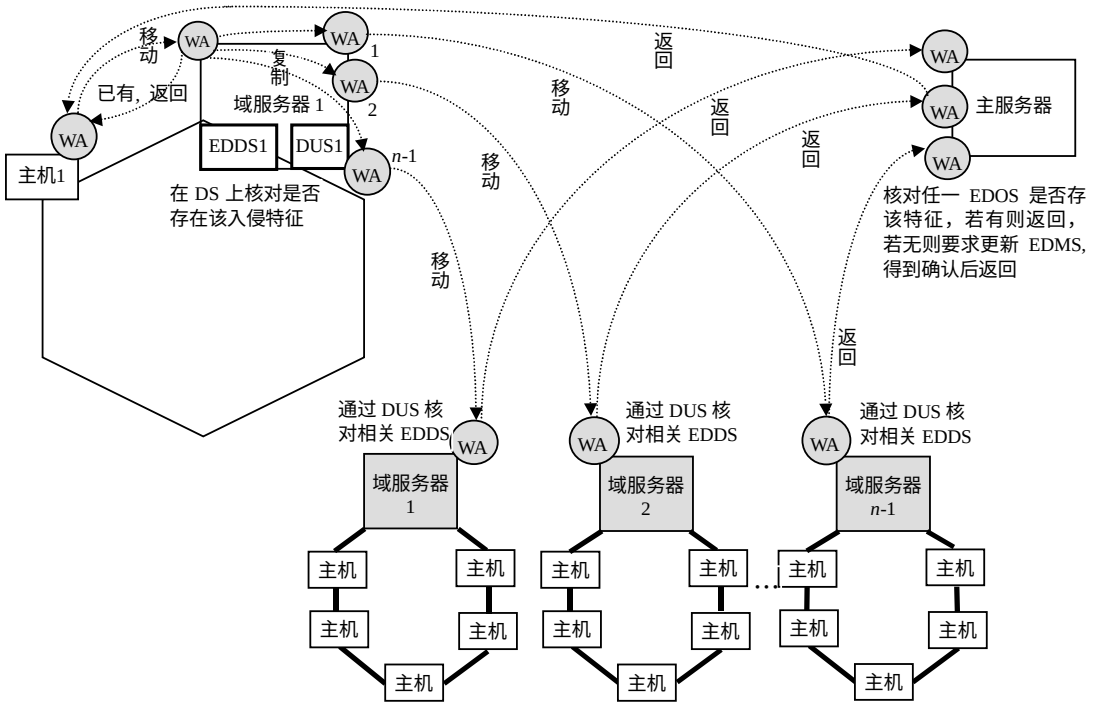

图 4　MADIDS 的分层更新机制

3 实验环境、结果与性能分析

为验证 MADIDS 的性能，可针对其规则更新进行实验。由于条件限制，实验环境仅在电子科技大学校园网内选取三处位置进行，如图 5 所示。数据库平台为 mysql4.0，实验中管理的 IDS 为 snort。移动 Agent 平台采用 Windows NT4+Aglet1.3+JDK1.0 来搭建，通过 Aglet Workbench 及相应软件包实现。实验中首先配准所有主机的时钟，在每个节点上都由一个读系统时间的程序进行计时，并与 MADIDS 的运行配合进行。从主服务器（Main Server，MS）上的 EDMS 更新开始计时，直到最后一个主机上的 EDH 得到更新为止，作为一次完整的实验过程，对规则更新进行 500 次实验。由于已对所有节点的时钟进行了配准，系统一次规则更新的周期时间，可由最后一个完成移动 Agent 返回动作的主机上的时间标记减去主服务器上的初始时间标记得到。从实验情况来看，每次实验都能完成 MADIDS 的设计目标，一个新规则在两个域的 8 个节点得到全面配置，最短耗时 0.8 s，最长耗时 3.3 s。

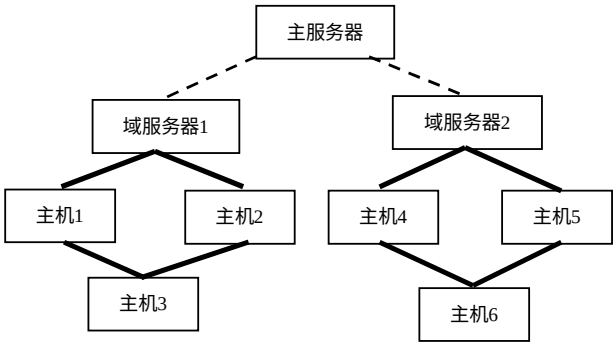

图 5 MADIDS 实验环境示意图

由实验与分析可知，这种“分层核对”机制具有如下优点：(1) 有效减少MADIDS中对新的入侵行为特征标记内容的管理和复制的通信量，特别是在广域网上的通信量；(2) 主服务器不需维护每一个主机的新入侵特征，仅仅需要维护域服务器即可，大大降低了维护的整体开销。

限于篇幅，规则生成机制外的其他内容不再赘述。

4 总 结

本文提出了一种基于移动Agent的新型入侵检测系统 — MADIDS。MADIDS使用分层体系结构，整个系统由若干域组成，域内通过局域网连接，域间通过广域网连接。每个域由域服务器管理，所有域服务器由主服务器管理，这种体系结构保证了很好的伸缩性和扩展性，MADIDS在系统管理中使用了“分层生成”机制，这种机制降低了维护系统整体性和一致性的负荷，网络通信量较小，非常适合在广域网中使用。

参 考 文 献

[1] Mell P, McLarnon K. Mobile agent attack resistant distributed hierarchical intrusion detection system[C].In Proceedings of RAID'99, CERIAS, Purdue University, 1999.

[2] White G B, Fisch E A, Pooch U W. Cooperating security managers: a peer-based intrusion detection system[J]. IEEE Network, 1996, 10(1): 20-23.

[3] Slagell, M. The design and implementation of MAIDS [D]. Des Moines: Iowa State University, 2001

[4] 张云勇. 移动Agent及其应用[M]. 北京: 清华大学出版社, 2002

[5]Baumann J, Hohl F, Rothermel K, et al. Mole-concepts of a mobile agent system[R]. Stuttgart: University of Struttgart, 1997

[6] Karnik N M, Tripathi A R, Design issues in mobile agent programming systems[J]. IEEE Concurrency Magazine, 1998,6(3): 52-61

[7] Johansen D. Mobile agent applicability[C]. In Proceedings of the Second International Workshop on Mobile Agents(MA '98), Stuttgart, 1998.

编 辑 熊思亮