一种基于邻近距离的分布式入侵防御系统模型

张 焕 曹万华 冯 力 张 剑
(武汉数字工程研究所 武汉 430074)

摘 要 分析了现有入侵防御系统的体系结构及存在的主要问题;根据入侵防御系统的特点,提出了一种基于邻近距离的分布式入侵防御系统(Intrusion Prevention System,IPS)模型。模型定义了系统中的消息类型,采用基于消息的协作方式可增强系统部署的灵活性,通过计算节点间的邻近距离优化通信范围,并给出相应的消息转发策略,以减少系统的消息量。实验表明,模型可以显著减少分布式入侵防御系统的网络负载。

关键词 分布式,入侵防御系统,网络负载,协作
中图法分类号 TP393.08 **文献标识码** A

Distributed IPS Model Based on Near Neighbor Distance

ZHANG Huan CAO Wan-hua FENG Li ZHANG Jian
(Wuhan Digital Engineering Institute, Wuhan 430074, China)

Abstract The characteristics and problems of Intrusion Prevention System (IPS) architecture were analyzed and a distributed IPS model based on near neighbor distance was proposed in this paper. In the model, message types transmitted between cooperation nodes were defined, and a message-based cooperation method was adopted to enhance the flexibility for system deployment. In order to reduce the redundant message, the distance between nodes was calculated and the communication region was optimized in the model. The experimental results show that the model decreases the IPS network load evidently.

Keywords Distributed, Intrusion prevention system(IPS), Network load, Cooperation

1 引言

随着网络应用领域的不断扩展,网络安全问题日益突出,传统的入侵检测系统(IDS)已经不能满足人们对网络安全的需求。入侵防御系统(IPS)集入侵检测、入侵追踪、入侵响应于一体,旨在构造一套智能化、集成化的网络安全防护体系。特别是在大规模无人值守的网络环境中,分布式 IPS 对维护网络安全态势更有着举足轻重的作用。可以借鉴对入侵检测系统体系结构的分类方法[1],将 IPS 进行如图 1 所示的分类。

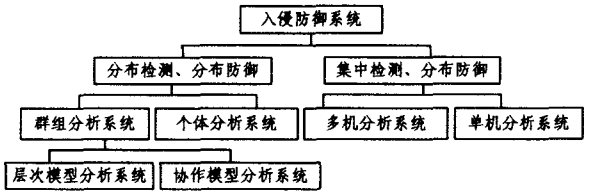

图 1 入侵防御系统分类

在"大规模网络"这一前提下,一般认为 IPS 的入侵防御部分必须是分布式的,否则将存在网络保护的"盲区"[2]。集中检测、分布防御模式采用集中的审计数据(系统日志、数据包)作为数据源,只能从单一视角和有限数据进行检测。分布检测方式中,个体分析系统容易产生单点失效问题,并且随着网络规模的扩大,系统负荷过重也将成为系统运行的瓶颈[1-4]。存在多个分析器的群组分析系统才算是真正意义的分布式系统,其中层次模型分析系统逻辑结构清晰,节点方便管理,但存在处理效率低、延时长等缺陷,并且由于逻辑结构的存在,使得系统部署的灵活性差。协作模型分析系统(全分布系统)具有自主性强、容错性好、部署灵活等特点,但由于节点间逻辑关系不明确,存在节点间协作关系复杂及消息量庞大等问题[3-6]。

本文提出了一种基于邻近距离的分布式 IPS 模型,旨在改善协作模型分析系统的网络负载问题。

2 基于邻近距离的分布式 IPS 模型构成

针对大规模网络中网络设备、安全检测/响应设备以及终端节点类型多样,信息安全相关数据异构的情况,基于邻近距离的 IPS 模型主要由多个异构的 IPS 节点和相关信息节点构

到稿日期:2008-10-27 返修日期:2009-01-07 本文受国防科工委"十一五"预研计划(No. C0820061362-06, No. A1420080183),国家"863"国家信息安全计划(No. 2007AA01Z464),船舶工业国防科技预研基金项目(No. 08J3.7.8)资助。

张 焕(1982-),男,硕士研究生,主要研究方向为网络信息安全,E-mail:zhanghuan0222@163.com;曹万华(1966-),男,研究员,博士生导师,主要研究方向为指控系统、软件工程;冯 力(1974-),男,博士,主要研究方向为信息安全;张 剑(1979-),男,博士,主要研究方向为无线传感器、网络信息安全。

成。各节点之间的通信关系如图 2 所示。

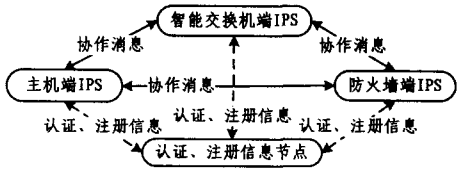

图 2　异构 IPS 节点及信息节点间通信关系图

信息类节点：为主机端 IPS、智能交换机端 IPS 以及防火墙端 IPS 提供认证、注册、路由等服务的信息服务节点。系统中可能部署着一个或多个此类节点。该类节点不具有入侵检测、防御等功能，只在各 IPS 节点加入、退出系统时提供相关信息服务。此类节点只是间歇性地与 IPS 节点进行通信。在全局网络环境中部署适当冗余的信息服务节点，就可以避免系统因此而产生的单点失效问题。

IPS 终端类节点：包括主机端 IPS、智能交换机端 IPS 以及防火墙端 IPS 3 类节点，如图 2 所示。一个典型的 IPS 终端类节点由图 3 所示的 4 个模块组成。

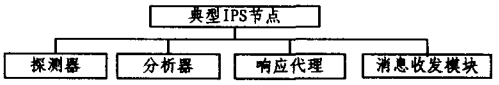

图 3　典型 IPS 节点组成模块图

探测器、分析器与传统 IPS 的功能并非不同，只是其分析数据源更加多样化，包括本地数据源和协查数据源；响应代理是系统主要的异构部件，需要根据 IPS 节点配置的安全响应设备量身定制；主机端 IPS 的响应代理可能响应的是软件防火墙、操作系统配置文件等；防火墙 IPS 的响应代理响应的是防火墙的访问控制列表等；消息收发模块负责节点间各类消息的收发，是分布式 IPS 系统协作、部署的核心模块。

协作消息：协作消息是终端类 IPS 节点间数据交互的载体，包含报警事件、响应请求、转发参数等相关信息。IPS 终端节点之间主要传递报警、响应、协查 3 种类型的协作消息，采用入侵检测信息交换协议（IDXP）[7] 进行通信。消息机制的建立增加了系统部署的灵活性，新设备的增加不需要更改系统设计，开发与该设备适合的 IPS 节点就能使设备很好地融合入整个系统。

2.1　邻近距离的提出

传统分布式 IPS 节点通信模型中，随着分布式 IPS 节点的不断增多，节点之间的消息量会急剧增长。然而增加的每条消息并非都有助于提升系统性能，其中存在大量的冗余消息。因此，通过有效途径裁减冗余消息，是解决分布式 IPS 系统网络负载问题的关键所在。本文借鉴分布式系统中“分而治之”的思想[8]，假设分布式入侵防御系统中每个节点只关注自己周围的网络状态，只与自己“邻近”的节点通信、协作，以每个节点的局部安全确保网络的全局安全。

2.2　邻近距离的定义

定义　“邻近距离”描述网络环境中任意两个节点 M,N 之间的邻接关系，该关系可以用邻接向量 $V=(\alpha,\beta,\gamma,\eta,\cdots)$ 的相似性来度量，其中 α,β 等元素为实际考虑到的影响邻接关系的因子。本模型中考虑节点 IP 地址、节点类型、通信频率、通信时间和路由转发数 5 个影响因子，则邻接向量可以表示为：

$$V=(IP,nodType,conRate,conTime,ttlNum)$$

其中，IP 地址因子与路由转发数因子反映了两节点网络位置和消息转发路径的邻接性；节点类型因子主要反映主机 IPS 节点、防火墙 IPS 节点等不同类型节点之间的邻接关系，该影响因素可以增加网络中智能交换机、防火墙等关键防御设备的信息量，提高防御效果；通信频率因子和通信时间因子通过两节点单位时间通信量的多少和时间来评估节点间的逻辑距离。

2.3　邻近距离的计算

通过以上分析可知，计算两节点之间的邻近距离可以转化为比较节点间两组邻接向量 V_1,V_2 的相似性问题。评估向量相似性，常用的方法有马氏距离法[9] 和格贴近度法[9] 等。这里根据邻接向量的具体情况对马氏距离法进行改进，建立邻近距离的计算方法。

马氏距离如式(1)所示：

$$M^2(X,Y)=\frac{(x_1-y_1)^2}{\sigma_1^2}+\frac{(x_2-y_2)^2}{\sigma_2^2}+\cdots+\frac{(x_n-y_n)^2}{\sigma_n^2} \tag{1}$$

其中，X,Y 表示两组特征向量，x_n,y_n 表示其中第 n 个分量，σ_n^2 为两组特征向量中第 n 个分量的方差。马氏距离法对相似性的测定是基于距离的，计算所得距离值越小，说明两组向量越接近。

马氏距离法中的两组特征向量采用的是两实体各自的特征信息，然而邻接向量中通信频率和路由转发跳数因子反映的是两节点之间的共有特征，并且 IP 因子的方差项在本模型中并不适用。另外，该方法没有考虑到各分量的影响大小，在实际应用中并不合理。因此引入临界值 φ 和权重因子 k 对马氏距离公式进行改进，得到邻近距离的计算方法，如式(2)所示。

$$M^2(V_1,V_2)=k_{ip}(IP_1-IP_2)^2+k_{nt}\frac{(|nt_1-nt_2|-1)^2}{\sigma_{nt}^2}+k_{cr}\frac{(cr-\varphi_{cr})^2}{\sigma_{cr}^2}+k_{ct}(ct-\varphi_{ct})^2+k_{tn}(tn)^2,$$
$$k_{ip}\geqslant 0,k_{nt}\geqslant 0,k_{cr}\geqslant 0,k_{ct}\geqslant 0,k_{tn}\geqslant 0 \tag{2}$$

其中，IP 为 ipv4 中 ip 字符串对应的整型值，IP 值越相似，距离越小；节点类型分为主机型节点和安全设备型节点，量化为离散型数值 1 和 0，其方差可以根据网络中各节点出现的概率和部署数量计算得到，节点类型不同，邻近距离小；通信频率临界值 φ_{cr} 和方差由经验值得到，且需满足 $cr\leqslant\varphi_{cr}$，频率越接近，临界值距离越小；通信时间 ct 为当前系统时间，φ_{ct} 为上次通信时间，间隔越短，距离越小；节点间路由转发数可以通过网络探测得到，转发跳数越少，距离越小。其中各项影响因素的权值需要根据网络规模和节点性能需求调整设定。

2.4　消息转发表

消息转发表的结构如表 1 所列。

表 1　消息转发表结构

名称	内容
IP_address	节点 IP 地址
Nod_type	节点类型
Con_rate	通信频率
ttlNum	路由转发数
Node_distance	邻近距离
Last_rec_time	最后一次接收时间
Last_sed_time	最后一次发送时间
Node_state	节点状态

节点在启动、运行过程中动态构造和维护消息转发表。其初始化构造过程主要有以下几个步骤：

1)向信息节点注册，并从信息节点获取已注册的节点IPList及节点类型信息；

2)根据节点IP探测路由转发跳数ttlNum；

3)计算节点间邻近距离，并根据邻近距离排序转发表；

4)根据系统设定的距离阈值 φ_{s1} 和 φ_{s2} 将转发表分为“转发段”和“备选段”，并舍弃剩余节点。

系统运行过程中，新节点的增加，通信频率、通信时间、节点状态的改变，需要对消息转发表进行动态调整，一般有以下事件出现时，需要对转发表进行维护。

1)时间戳到期；

2)数据包信息中出现新的IP地址；

3)从信息节点更新数据；

4)节点状态改变。

2.5 消息分发策略

IPS节点之间存在报警、响应、协查3种消息。其中响应消息和协查消息的目的明确、转发环节少；报警消息转发环节多，可能造成消息循环或大量冗余[10]。本文依据3种消息的特点给出相应的分发策略及转发参数，如表2所列。

表2 转发参数表

名称	内容
ID_num	参数表ID
Max_node_num	最大节点数
Node_num	转发节点数
Max_send_num	最大转发次数
Send_num	转发次数
Node_List	节点IP列表

协查消息：IPS节点在对某些入侵行为(例如分布式拒绝服务攻击)的检测分析过程中，需要其它节点的数据支持，协查消息的发布者只需要将消息发送到指定节点，等待消息回执即可。

报警消息：当IPS节点检测到入侵信息后，将报警消息发布给所有邻近节点，并选取距攻击源IP最近节点作为转发节点，并附加转发请求及转发参数表(转发节点和参数的选取可以根据实际情况调整设定)。

响应消息：响应消息的交互过程主要发生在网络防御设备IPS节点与其它IPS节点之间，响应消息的发布基本可以视为点对点的通信。

节点发布消息的过程如下：

1)如果是协查消息或者响应消息，直接发送；如果是报警消息，转2)。

2)初始化转发参数表，Node_num=0，Send_num=0，并将本节点IP及邻近节点IP加入Node_List。

3)从邻近节点中选取距攻击源IP最近的节点作为转发节点，将转发参数表附在报警信息后发送给转发节点。

4)将报警信息发送给其余邻近节点。

节点接收消息的过程如下：

1)如果是响应消息或协查消息，不需转发，节点根据消息内容进行相关处理。如果是报警消息，转2)。

2)查看报警信息附带的转发参数表，若Node_List中无本节点IP，转3，若有本节点IP，转4)。

3)处理该消息并修改转发表参数。将节点IP加入Node_List，Node_num++，Send_num++，转5)。

4)修改转发参数表Send_num++；

5)判断转发参数关系，如果Node_num>Max_node_num或者Send_num>Max_send_num，停止转发，丢弃该消息，否则转6)；

6)从邻近节点表中随机选取一节点，转发该消息及转发参数表。

3 实验分析

以IP地址为192.168.0.1～192.168.0.253的局域网环境为例。为便于消息量的统计，各节点间只进行报警信息的消息传递。为便于定性分析消息增长趋势，只考虑节点IP对邻近距离的影响(省略式(2)中其余各项计算结果会影响分布式IPS系统性能，但不会影响该模型的合理性)。从而该网络环境下邻近距离的计算公式变为：

$$M^2(V_1,V_2)=k_{ip}(IP_1-IP_2)^2 \tag{3}$$

将式(3)中的权重系数 k_{ip} 取4，由此可以计算出每个节点的邻近距离表。以节点192.168.0.2为例，计算结果如表3所列。

表3 节点192.168.0.2邻近距离表

节点IP	邻近距离
192.168.0.1	4
192.168.0.3	4
192.168.0.4	16
192.168.0.5	36
192.168.0.6	64
192.168.0.7	100
192.168.0.8	144
……	……

实验中设定最大转发次数等于 A，最大转发节点数等于 B，邻近距离阈值为 φ_{s1}，则邻近节点数 n_c 与 φ_{s1}，节点数 n_t 的关系可表示为式(4)：

$$n_c=\left\lfloor\frac{\sqrt{\varphi_{s1}}}{2}+1\right\rfloor, n_c\in N, n_c<n_t \tag{4}$$

由式(4)可知，在 $n_t>n_c$ 及 $n_t\leqslant n_c$ 两种情况下，该网络中 n_t 个节点各发送一个报警消息，产生的总消息量 Tm 为

$$Tm=\begin{cases} n_t\left\lfloor\frac{\sqrt{\varphi_{s1}}}{2}+1\right\rfloor(1+A), n_t\geqslant\frac{\sqrt{\varphi_{s1}}}{2}+1 \\ n_t(n_t-1)(1+A), n_t<\frac{\sqrt{\varphi_{s1}}}{2}+1 \end{cases} \tag{5}$$

由式(5)可得，邻近阈值与总消息量关系如图4所示，网络节点数与消息总量的关系如图5所示。

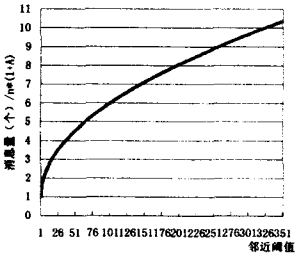

图4 邻近阈值与总消息量关系图

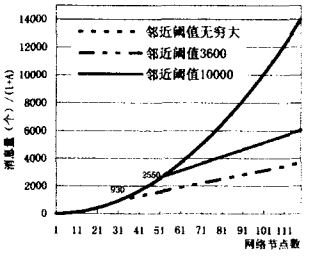

图5 节点数与消息量关系图

由图5及式(4)、式(5)可知，当 $n_t\leqslant n_c$ 时，系统消息量呈抛物线增长。但是当 $n_t>n_c$ 后，Tm 的增长趋势由抛物线转变为线性。由此可见，随着网络规模的扩大，该方法能够将消

息量的复杂度由 $O(n^2)$ 转变为 $O(n)$，有效降低了入侵防御系统的网络负载。

结束语 本文提出了一种分布式 IPS 模型。模型从分布式 IPS 系统应用特点出发，提取出影响节点间协作关系的邻近距离因子，并通过邻近距离的计算优化节点通信范围，裁减冗余消息，以减少系统网络负载。模型中消息机制的引入，缓解了节点间协作的耦合性，扩展了系统部署的灵活性。网络负载小和系统部署灵活这两个特点使模型为中大规模网络环境中安全防御系统的部署提供了一套很好的解决方案。在下一步的工作中，还需要对网络环境与邻近计算公式权值之间的关系做进一步的分析和探索，以提高模型在实际应用中的性能。

参 考 文 献

[1] 连一峰，戴英侠，胡艳，等. 分布式入侵检测模型研究[J]. 计算机研究与发展，2003，40(8)：1196-1202

[2] Abraham A，Jain R，Thomas J. Distributed soft computing intrusion detection systems[J]. Journal of Network and Computer Applications，2007，30(1)：81-98

[3] 马恒太. 基于 Agent 的分布式入侵检测系统模型[J]. 软件学报，2000，11(10)：1312-1319

[4] 李旺. 分布式网络入侵检测系统 NetNumen 的设计与实现[J]. 软件学报，2002，13(8)：1723-1728

[5] Patrick D，Allen D. Increasing Flexibility in Network Visibility and Intrusion Response[J]. Military Communications Conference，2006，8 (23-25)：1-6

[6] 吴骏，王崇骏，陈世福. 基于多 Agent 的动态层次化分布式入侵检测系统[J]. 计算机科学，2007，34(2)：71-75

[7] Feinstein B. The Intrusion Detection Exchange Protocol(IDXP)[S]. RFC4767. 2007

[8] Kannadiga Z P. A distributed intrusion detection system using mobile agents[J]. Software Engineering，2005，25(23)：238-245

[9] 孙即祥. 现代模式识别[M]. 长沙：国防科技大学出版社，2002：15-17

[10] Lupu E，Sloman M. Conflicts in Policy-based Distributed Systems Management[J]. IEEE Transaction on Software Engineering，1999，25 (6)：335-349

(上接第 38 页)

如表 1 所列，将本文方案与文献[8]中提出的方案作了比较，签名和验证过程中模幂运算太多的一些方案没有在表中列出进行比较。表中 EXP 表示模幂运算，INV 表示求逆运算，n 表示群成员个数，m 表示撤销成员的个数。

表 1 方案的比较

方案	签名	验证	打开
本文方案	2EXP	(3+m)EXP	3EXP+3INV
CHEN 的方案	3EXP	(3+m)EXP	(n/2+3)EXP+3INV

结束语 本文在充分考虑到群签名过程中可能出现的各种问题的前提下，提出了一种多安全策略的群签名方案，方案不仅具有前向安全性，同时首次在群签名方案中能有效地防止群成员的超前签名。方案支持成员的有效撤销。签名的打开算法，将模幂运算和求逆运算量与成员个数线性相关优化成线性无关，效率得到了较大程度的提高。本文所提出的方案，没有时间段周期的限制，解决了一旦时间周期结束，就必须重新初始化系统的弊病。

参 考 文 献

[1] Chaum D，van Heyst E. Group signatures[C]// Advances in Cryptology-EuroCrypt'91，Lecture Notes in Computer Science 547. Berlin：Springer，1991：257-265

[2] Camenish J，Stadler M. Efficient group signatures for large groups[C]// Proceedings of CRYPTO'97，Lecture Notes in Computer Science. Springer-Verlag，1997，1296：410-424

[3] Camenish J，Michels M. A. group signature scheme with improved efficiency[C]// Proceedings of ASIACRYPT'98，Lecture Notes in Computer Science. Springer-Verlag，1998，1541：160-174

[4] Ateniese G，Tsudik G，Tsudik. A coalition-resistant group signature[EB/OL]. http：//www. isi. edu/~gts/pubs. html

[5] Ateniese G，Tsudik G. Some open issues and new directions in group signatures[EB/OL]. http：//www. isi. edu/~gts/pubs. html

[6] Anderson R. Invited lecture[C]// Proceedings of the 4th ACM Conference on Computer and Communications Security. Zurich，Switzerland，1997：1-7

[7] Song D-X. Practical forward secure group signature schemes [C]// Proc. of the 8th ACM Conf on Computer and Communications Security (CCS 2001). New York：ACM Press，2001：225-234

[8] 陈少真，李大兴. 有效取消的向前安全群签名体制[J]. 计算机学报，2006，29 (6)：998-1003

[9] 李如鹏，于佳，李国文，等. 高效撤消成员的前向安全群签名方案[J]. 计算机研究与发展，2007，44 (7)：1219-1226

[10] Michel A，Leonid R. A New Forward-Secure Digital Signature Scheme [C]// ASIACRYPT2000，LNCS 1976. Berlin Heidelberg：Springer-Verlag，2000：116-129

[11] 王晓明，符方伟，张震. 前向安全的多重数字签名方案[J]. 计算机学报，2004，27 (9)：1177-1191

[12] Chaum D，van Heyst E. Group signatures[C]// Advances in Cryptology-EuroCrypt'91，Lecture Notes in Computer Science 547. Berlin：Springer，1991：257-265

[13] Boneh D，Boyen X. Short signatures without random oracles [A]//Christian Cachin，Jan Camenisch，eds. Eurocrypt'04 [C]. Interlaken，Switzerland：Springer-Verlag，2004：56-73

[14] Mitsunari S，Sakai R，Kasahara M. A new trator tracing[J]. IEICE Trans. Fundamentals，2002，E85A (2)：481-484

[15] Vo Duc-Liem，Kim Kwangjo. Yet Another Forward Secure Signature from Bilinear Pairings [C]// ICISC 2005，LNCS 3935. Berlin Heidelberg：Springer-Verlag，2006：441-455

[16] Cheng X，Zhu H，Qiu Y，et al. Efficient Group signatures from Bilinear Pairing[C]// CISC'05LNCS 3822. Springer-Verlag，2005：128-139

[17] Park H，Kim H，Chun K，et al. Untraceability of Group Signature Scheme based on Bilinear Mapping and their Improvement [C]// International Conference on Information Technology(ITNG'07). IEEE，2007：103-109