基于信任关联的免疫软件人群体检测模型

周 芳[1] 郑雪峰[1] 于 真[2]

(北京科技大学计算机与通信工程学院 北京 100083)[1] (北京物资学院信息学院 北京 101149)[2]

摘 要 免疫软件人具有自适应性、智能性和协作性,能够对动态的分布式网络进行实时监控。大部分分布式入侵检测系统的实现都会产生大量的报警信息,误报率也较高,影响了入侵检测的效果。针对此问题,将免疫软件人群体检测应用于分布式入侵检测,提出了一种基于信任关联的免疫软件人群体检测方法。实验表明,使用该信任机制可以提高软件人群体入侵报警的检测准确率。

关键词 入侵检测,免疫软件人,关联规则,信任

中图法分类号 TP393.08 **文献标识码** A

Groups of Immune-softman Intrusion Detection Model Based on Trust correlation

ZHOU Fang[1] ZHENG Xue-feng[1] YU Zhen[2]

(School of Computer and Communication Engineering, University of Science and Technology Beijing, Beijing 100083, China)[1]

(School of Information, Beijing Wuzi University, Beijing 101149, China)[2]

Abstract The immune-softman is provided with adaptability, intelligence and collaboration, so it is used to monitor distributed dynamic network environment in real time. Most of Distributed Intrusion Detection System will produce large amounts of alarm information and the false-alarm rate is also high, which affects the effectiveness of intrusion detection. To address this issue, groups of immune-softman intrusion detection model based on trust correlation was proposed. Through the trust correlation algorithms the credibility of the Immune-softman producing alarm can be measured. Simulations show that the groups of immune-softman intrusion detection model based on trust correlation can improve the accuracy of intrusion detection alerts.

Keywords Intrusion detection, Immune soft-man, Correlation rule, Trust

1 引言

分布式入侵检测系统(Distributed Intrusion Detection System, DIDS)的实现要求各个入侵检测系统之间能够实现高效的信息共享和协作检测,其关键技术是检测信息的协同处理与入侵攻击的全局信息的提取。由于分布式计算机网络的复杂性,DIDS的实现会产生大量的虚警率和误警率,使得系统管理人员难以及时做出正确反应[1-3]。因此,怎样提高DIDS的报警准确率是目前分布式入侵检测乃至整个网络安全领域的热点之一。

涂序彦教授等人提出的软件人技术赋予了普通的Agent人工生命的活性和功能,其可以通过以往积累的知识学习和修正自己的行为来适应动态的网络环境,具有良好的应答性和自主性[4-6]。马占飞在软件人的基础上结合网络安全提出了"免疫软件人"的概念,"免疫软件人"具有软件人的所有特点,是软件人技术在网络安全领域的具体实现[7,8]。基于免疫软件人自身的智能性、自治性和移动性等特点使得其对分布式入侵的复杂问题的分解、处理和求解表现出较高的智能性和鲁棒性[9-11]。

分布式的网络环境要求免疫软件人必然是以群体的方式进行检测。由多个免疫软件人个体相互联系、相互通信,可以组成类似于自然人群组织的"免疫软件人群体"。免疫人群中每个个体都可以独立地进行入侵检测任务,并向附近的免疫软件人传播自己的检测信息。对于某次入侵的检测,不同的软件人可能给出不同的结果,尤其是不能排除某些软件人已经被敌方控制而导致发布的信息是不正确的。所以,一个免疫软件人最终是否发出入侵报警信息就不只是自己独立测试的结果,还综合了该软件人收到的其他软件人的判断信息。对其他软件人发出信息的采纳程度可以根据软件人的以往经验和信誉来判定。因此,文献[12,13]将信任模型引入入侵检测领域,文献[14-16]分别将模糊规则、地址关联等应用于分布式入侵检测并取得了较好的效果。本文基于免疫软件人群体检测,提出一种计算免疫软件人信誉度的方法,使得软件人的报警信息既考虑到自身检测结果也结合其他软件人的检测结果,从而有效地减少了虚警率和误警率。

2 免疫软件人群体检测模型

本文提出的基于免疫软件人的分布式入侵检测模型,采

本文受北京市自然基金项目(4102041)资助。

周 芳(1972—),女,博士生,讲师,主要研究方向为计算机网络技术和信息安全,E-mail:ustbzhou@126.com;郑雪峰(1951—),男,硕士,教授,主要研究方向为计算机网络技术和信息安全;于 真(1983—),女,博士,讲师,主要研究方向为网络信息安全。

取免疫软件人群体结构，通过众多免疫软件人的相互协作来完成入侵检测任务。免疫软件人群体的组织形式可以是分散、集中和递阶，但是在免疫软件人相互协作进行入侵检测工作的时候，如在入侵检测信息的传播时，软件人相互之间是一种对等的关系，即任何软件人都可以独立地进行入侵检测并向“附近”的软件人传播这个入侵信息。“附近”的这个软件人可能和发出入侵检测信息的软件人处于同一组中，也可能处于不同组。模型构成如图 1 所示。

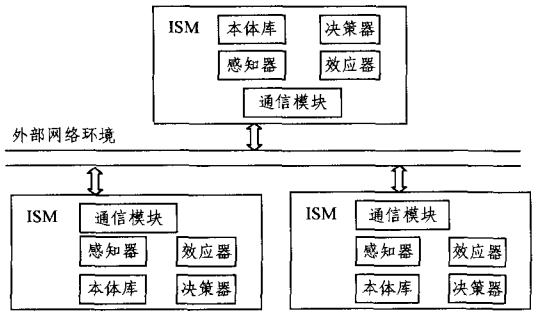

图 1　ISM 群体结构图

这样软件人在判断是否入侵发生时就有两种凭据：一个是软件人自身检测到的入侵信息；另一个是其他软件人传来的入侵检测信息。软件人是否发出入侵警报应该是这两种信息综合的结果。这样，系统在判断系统是否遭到入侵就有两方面的凭据。一方面，针对一次入侵报警信息，衡量的是这次入侵报警信息的有效程度，需要关联所有发出这次入侵报警的免疫软件人的看法；另一方面，针对某个发起入侵报警的免疫软件人，衡量的是该软件人的可信程度，需要关联自身的主观信任（也称直接信任）和其他软件人的推荐信任。

3　免疫软件人群体检测的算法

3.1　免疫软件人的定义

马占飞提出的“免疫软件人”（ISM）是一种具有免疫特性的 SM，它能接受环境（抗原）刺激，自主地产生免疫应答或通过与其他 ISM 共同协作进行免疫应答，实现其目标（消除抗原）的计算系统[7]。ISM 的结构定义为：

$ISM=(Id,St,Sa,Rs,Re,Co,Gb)$

式中：Id 表示 ISM 的标识，用于唯一确定 ISM；St 表示 ISM 所处的状态（包括未成熟状态、成熟状态、记忆状态、死亡）；Sa 表示 ISM 的本质属性；Rs 表示 ISM 的应答策略；Re 表示 ISM 的决策机制，主要用于建立认知模型，从而充实和完善基因数据库；Co 表示 ISM 的通信接口，实现与外界环境或其他 ISM 的通信；Gb 表示 ISM 的基因数据库，用于存储 ISM 的基因[8]。

由于免疫软件人群体进行检测工作，模型中多个免疫软件人既能独立进行检测工作，又相互通信、协同工作，最后入侵检测系统的报警信息的产生是一个软件人集体的决策。由于免疫软件人工作在开放的网络环境中，自身也可能成为攻击的目标甚至被攻击方控制而发出虚假的检测信息；另外由于软件人有自我学习、自我进化的功能，经过一段时间后，免疫软件人的检测能力不同。因此作者将信誉度引入免疫软件人的属性中，免疫软件人的报警经历决定了该软件人的检测信誉。

在上述免疫软件人的定义中加入一个表示该软件人自身信誉度的属性 Cr，网络中的每个软件人都用 Cr 表示本地经验值和推荐信息值。本地经验值表示对自身接收到的报警信息（来自于其他若干软件人）的评价；另外一个是推荐经验值，表示其他软件人（曾接收过该软件人发起的报警）对该软件人发起的报警信息的看法，体现了该软件人发起报警的准确度。加入该属性后免疫软件人的结构定义为：

$ISM=(Id,St,Sa,Rs,Re,Co,Gb,Cr)$。

3.2　基于信任的免疫软件人群体检测算法

模型中免疫软件人传播自身检测消息的方式如图 2 所示。软件人群体检测算法描述如下：

1）系统初始化。免疫软件人群同步，免疫基因传播到系统的每个免疫软件人。

2）系统开始工作后，免疫软件人实时地独立运行检测模块，根据系统传播的知识和自己积累的知识得到自己的一个基本的检测结果，并向附近的软件人传播此检测结果。

3）软件人收到其他软件人的检测结果，根据软件人群的信任算法，得到一个综合评估值，并根据该评价值的大小决定是否发出报警信息。

4）系统根据软件人群发出入侵报警的情况是否超出采纳阈值（可以事先设置），得出系统现在是否遭到入侵和入侵发生的程度。

5）最后，每个软件人根据实际入侵是否发生作为依据，更新自身 Cr 属性，即该软件人的本地经验值和发起此次发起报警软件人的推荐信息。系统工作转 2）。

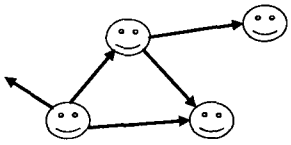

图 2　软件人入侵检测消息传播方式

上面 2）中的免疫软件人群信誉度算法具体描述如下：

a）首先采用式（1）来计算单个免疫人检测信息的有效性：

$$S_{ij}=W_iC_i+(1-W_i)\sum_{j=1}^{n}T_{ij} \tag{1}$$

式中，S_{ij} 表示软件人 i 的该次报警信息的有效值。其中 $W_i\in[0,1]$，表示软件人 i 自身的报警所占的权重，C_i 表示软件人 i 自身发起的报警的可信度，T_{ij} 表示在软件人 i 看来软件人 j 发起报警的可信任程度。

b）T_{ij} 的计算方法如式（2）所示：

$$T_{ij}=\lambda\times D_{ij}+(1-\lambda)\times r_{ij} \tag{2}$$

式中，λ 表示软件人对于自身经验和间接经验的侧重程度，$\lambda\in[0,1]$，$j\neq i$，通过计算 T_{ij} 来衡量报警节点的可信任程度；D_{ij} 表示软件人 i 对报警软件人 j 的直接信任值；r_{ij} 表示的是来自于其他软件人的间接信任值。

c）D_{ij} 计算方法如下：

$$D_{ij}=\frac{G_{ij}}{G_{ij}+B_{ij}} \tag{3}$$

式中，G_{ij} 表示软件人 j 发起报警成功的次数，B_{ij} 表示发起报警失败的次数。

其中，r_{ij} 计算方法如下：

$$r_{ij}=\frac{1}{\sum\limits_{r\in I(j)}R_r}\sum_{r\in I(j)}D_{rj}\times R_r \tag{4}$$

式中，$r_{ij}\in[0,1]$，$I(j)$ 为曾经从软件人 j 收到入侵报警的软

件人集合，$i \notin I(j)$，$j \notin I(j)$。D_η 表示推荐软件人集合中的软件人 r 对发起报警软件人 j 的直接信任值，来源于节点 r 的直接经验。R_r 表示软件人 r 所提供的推荐的可信程度，称为推荐可信度，在网络中有唯一值，$R_r \in [0,1]$。

4 实验结果

本文在 Linux 操作系统下构造了一个 P2P 覆盖 IDS 网络仿真系统，使用 Java 语言实现。网络中按照一定的概率发起对目标系统的入侵行为和正常行为，检测到入侵行为的免疫软件人可以向其他邻居发起入侵报警消息，消息以类似 Gnutella 的方式进行广播，通过 TTL 控制消息的规模。免疫软件人可以分为 A 类和 B 类，其中 A 类软件人易发起入侵报警，占系统所有软件人的 30%，B 类软件人能较准确地发起入侵报警，占系统所有软件人的 70%。实验结果图 3 所示。

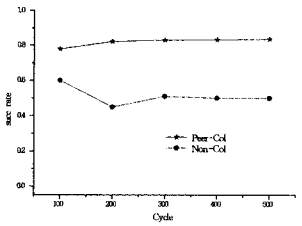

图 3 A 类 30%，B 类 70%的检测准确率

加入信任度评估后，免疫软件人的检测准确率得到了提高，入侵检测准确率如图 3 所示，基本能保持在 80%以上。即使网络中存在大量的易发报警软件人，即当 A 类软件人的比例增大(见图 4)时，算法的检测准确率虽略有下降，但仍高于无信任度关联下的检测准确率，这是由于易发报警软件人的信任值较低，若仍按照同样的采纳阈值来处理，则容易造成漏警，因此应该根据网络的实际情况进行平衡处理，来设定合适的采纳阈值。

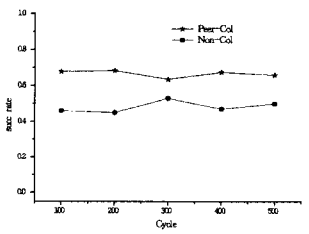

图 4 A 类 70%，B 类 30%的检测准确率

5 免疫软件人群体检测的特点

免疫软件人的自治性、移动性、智能性等特性解决了传统 IDS 中存在的检测服务器负载重、容易单点失效等问题，尤其是对于分布式的入侵检测任务，免疫软件人群检测方式具有其他方式不可比拟的优势：

1)移动性。免疫软件人在系统内部自由移动，直接在主机上对数据进行分析处理，不用将采集的有关数据专门送到某个地方进行检测任务，从而大大降低了网络负载。

2)自治性。免疫软件人具有智能，当与系统其它部分通信连接中断时，它可以根据自身的知识储备继续检测工作。

3)平台无关性。软件人平台允许免疫软件人在异构的环境中移动，这就允许各个不同责任区域的 IDS 之间通过免疫软件人迁移实现数据共享。

4)动态适应性。免疫软件人可以通过系统内部的共享机制获得免疫知识，也可以根据自身具体的网络环境而学习到独特的免疫知识并可以与其它成员共享，体现出动态适应性。

5)协作性。软件人能够根据周围环境自主学习，当入侵检测以一种群体的方式进行时，可以综合多个免疫软件人的意见得到一个综合评估值来判断系统是否入侵和入侵程度如何。避免单个软件人由于知识所限或者是被敌方控制而导致的误报，提高报警的准确性。

结束语 免疫软件人具有较强的自适应性、智能性和协作性，能够将入侵检测的分析工作分散到不同的软件人个体，进行深度分析的同时又能相互协作，共同抵御攻击。通过软件人之间的动态信任评估，实现免疫软件人的协作报警，降低了误警率和虚警率，有效地提高了分布式 IDS 的有效性。ISM 技术对于解决分布式 IDS 遇到的网络流量大、检测效率不高等问题提出了一种解决的思路，ISM 群的协商合作机制便于更好地发挥软件人的集体智慧，ISM 应用于分布式 IDS 将有着广泛的研究前景。

参 考 文 献

[1] 胡华平，张怡，陈海涛，等. 面向大规模网络的入侵检测与预警系统研究[J]. 国防科技大学学报，2003，25(1)：21

[2] 鲍旭华，戴英侠，冯萍慧，等. 基于入侵意图的复合攻击检测和预测算法[J]. 软件学报，2005，16(12)：2132

[3] 张有东，曾庆凯，王建东. 网络协同取证计算研究[J]. 计算机学报，2010，33(3)：504

[4] 曾广平，涂序彦. 软件人[C]//中国人工智能学会第 10 届全国学术年会论文集. 北京：北京邮电大学出版社，2003：677-682.

[5] 曾广平，涂序彦，王洪泊. “软件人”研究及应用[M]. 北京：科学出版社，2007

[6] 王洪泊，班晓娟，曾广平. 网络环境下虚拟机器人—"SoftMan"系统平台总体设计[J]. 计算机科学，2005，32(8)：152-155

[7] 马占飞，郑雪峰，曾广平，等. “软件人”群在入侵检测系统中的协调控制[J]. 控制与决策，2008，23(8)：944-948

[8] 马占飞，郑雪峰. “免疫软件人”概念及其协商控制模型[J]. 控制与决策，2010，25(5)：740-743

[9] 王洪泊，马忠贵，曾广平，等. 网络虚拟机器人——“软件人”安全策略与授权模型[J]. 计算机科学，2009，36(2)：275-277

[10] 马忠贵，周贤伟，曾广平，等. “软件人”社会的递阶协调模型研究[J]. 计算机科学，2007，34(12)：189-192

[11] 马忠贵，叶斌，曾广平，等. 基于Π演算的软件人群体形式化建模[J]. 北京理工大学学报，2006，26(2)：130-134

[12] 闫巧. 入侵检测系统的可信问题[J]. 计算机研究与发展，2003，40(8)：10233

[13] 穆成坡，黄厚宽，田盛丰. 入侵检测系统报警信息聚合与关联技术研究综述[J]. 计算机研究与发展，2006，43(1)：1

[14] 穆成坡，黄厚宽，田盛丰，等. 基于模糊综合评判的入侵检测报警信息处理[J]. 计算机研究与发展，2005，42(10)：6

[15] 段海新，于雪丽，王兰佳. 基于地址关联图的分布式 IDS 报警关联算法[J]. 大连理工大学学报，2005，45(z1)：126

[16] 吴吉义，平玲娣，范容，等. 基于自适应信任报警关联的 P2P 覆盖 IDS[J]. 解放军理工大学学报：自然科学版，2008，9(5)：455