

基于 Multi-Agent 的入侵检测动态协同机制研究

张 然, 刘 洋, 尹毅锋, 甘 勇

(郑州轻工业学院 计算机与通信工程学院, 河南 郑州 450002)

摘 要: 对一种基于 Multi-agent 的动态协同入侵检测模型进行了定义, 对检测代理之间的协作机制及其安全性以及检测代理之间的通信机制及其安全性进行了分析和讨论, 并在此基础上给出了该模型的协同检测算法. 检测代理的分层组织结构便于对协同检测进行管理和控制; 协调代理进行协同检测前通过加锁操作来保证代理之间协作的安全性; 检测代理通信时通过身份验证来保证代理之间通信的安全性. 该模型的协同机制和安全措施提高了入侵检测的准确性.

关键词: 入侵检测; Multi-agent; 协同; 协调域

中图分类号: TN402

文献标识码: A

文章编号: 1000-7180(2013)08-0057-06

Research on Dynamic Collaborative Mechanism of Intrusion Detection Based on Multi-Agent

ZHANG Ran, LIU Yang, YIN Yi-feng, GAN Yong

(School of Computer and Communication Engineering, Zhengzhou University of Light Industry, Zhengzhou 450002, China)

Abstract: In this paper, a dynamic collaborative intrusion detection model based on multi-agent is defined, the collaboration mechanism between the detection agents and its security, communication mechanism between the detection agents and its security are analyzed and discussed. On the basis, the collaborative detection algorithm of this model is given. The hierarchical organizational structure of the detection agents facilitates the management and control of the collaborative detection; the coordination agents ensure the security of collaboration between agents by the locking operation before collaborative detection; the coordination agents ensure the security of communication between agents through authentication during communication. The collaborative mechanisms and security measures of this model improve the accuracy of the intrusion detection.

Key words: intrusion detection; multi-agent; coordination; coordination domain

1 引言

目前, 入侵检测系统 (IDS)^[1] 的检测机制存在以下问题: 中心管理控制平台作用单一, 只能起到管理检测引擎的作用; 检测引擎单兵作战, 独立进行入侵行为的检测. 可见, 即使 IDS 检测到了入侵行为, IDS 本身也不能对入侵行为之间的相关性做出清楚的描述; 对一些复杂的攻击行为, IDS 不能做出准确判断; 对一些危害极大的拒绝服务攻击, IDS 仅仅简单地向攻击源发送 RST 包, 这只能进一步加剧网络的负载. 因此, 下一代的 IDS 需要协同, 协同的目的

是让入侵检测充分考虑攻击行为的特征和网络安全的整体性与动态性, 以提高入侵检测能力和网络系统的安全防护能力^[2-3].

下面对一种具有动态协同功能的基于多 Agent 的入侵检测模型进行定义, 对该模型的协同检测机制进行分析和讨论, 并提出相应的安全解决方案.

2 基于 Multi-agent 的入侵检测模型

2.1 代理的层次结构

按照功能, 基于 Multi-agent 的层次式入侵检测模型 (MAHID) 中的 agent 可分为四类^[4], 即: 基础

收稿日期: 2013-01-20; 修回日期: 2013-03-08

基金项目: 国家自然科学基金项目 (61272038)

检测 agent(包括应用检测 agent、服务检测 agent、子网检测 agent),局部协调检测 agent(简称局部协调 agent 或 LCA,包括主机上的协调 agent 和子网协调 agent),全局协调检测 agent(简称全局协调 a-

gent 或 GCA)和界面 agent. 这里把前三类代理统称为入侵检测代理(IDA). 系统中各类 agent 的层次结构如图 1 所示.

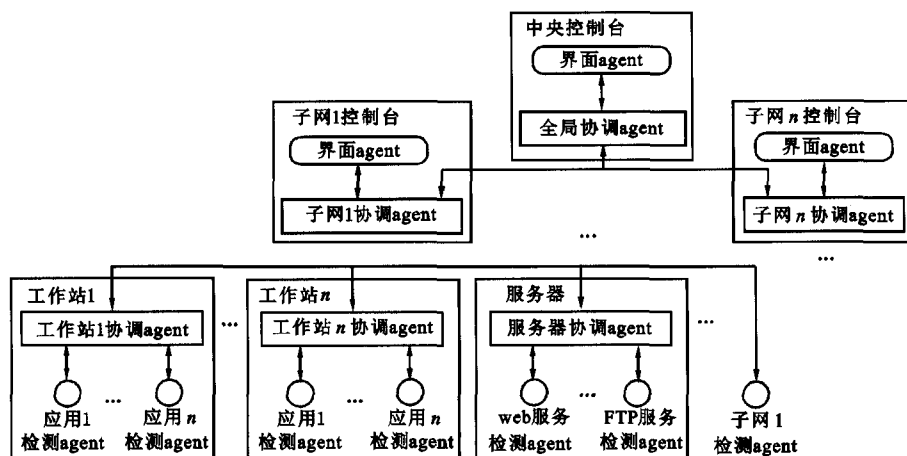


图 1 Agents 的层次结构

2.2 模型描述

定义 1 基于 Multi-agent 的入侵检测模型(MAHID)是一个七元组^[5]:

MAHID :: = <IDO, BA, DP, RP, CA, CP, MA>. 其中:

IDO: 为被检测对象的集合, 记为: IDO = {ido₁, ido₂, ..., ido_n}, 其中 n 为系统中被检测对象的个数. 被检测对象由系统安全管理员定义, 系统也可根据当前受监视系统的安全需求动态地加入或删除被检测对象.

BA: 为基础检测代理的集合, 记为: BA = {ba₁, ba₂, ..., ba_n}, 其中 n 为基础检测代理的个数. 被检测对象与基础检测代理是一一对应关系.

DP: 为检测策略的集合, 记为: DP = {dp₁, dp₂, ..., dp_l}, 其中 l 为检测策略的个数. 每个被检测对象对应一个或多个检测策略.

RP: 为响应策略的集合, 记为: RP = {rp₁, rp₂, ..., rp_t}, t 为响应策略的个数. 一种威胁对应一种或多种响应策略, 一种响应策略也可对应一种或多种威胁. 检测代理发现可疑活动时按照相应的响应策略进行动态响应.

CA: 为协调代理的集合, 记为: CA = {ca₁, ca₂, ..., ca_p}, p 为协调代理的个数. 协调代理包括局部协调代理和全局协调代理, 分别记为: LCA 和 GCA, 显然 CA = LCA ∪ GCA. 局部协调代理包括主机协调代理和子网协调代理.

这里把一个协调代理能够协调的下层入侵检测代理的集合, 称为协调域, 并用 CD 来表示. 因此, 每

个协调代理都有自己的协调域, 且对于每个协调代理的协调域 CD, 有 CD ⊂ (BA ∪ LCA). 协调域中的检测代理可以分布在不同的主机或子网上, 并能够通过其上层的协调代理相互协作共同完成一项较为复杂的检测任务. 每个入侵检测代理(除了全局协调代理)都对一个直系的上层协调代理, 而一个协调代理可以在自己的协调域内协调一个或多个入侵检测代理对可疑行为进行协同检测, 但不能对其协调域外的代理进行协调. 显然, 协调代理在进行一次协同检测时, 它所调用的入侵检测代理的集合是协调域的子集. 因此, 协调域的提出与划分有助于系统对协同检测过程进行管理和控制, 提高协同检测的安全性和效率.

CP: 为协调策略的集合, 记为: CP = {cp₁, cp₂, ..., cp_q}, q 为协调策略的个数. 每个协调代理在不同情况下可能对应一个或多个协调策略. 当有多个协调策略时, 协调代理能够根据具体情况从中挑选最优的协调策略对下层入侵检测代理进行协调.

MA: 为动态生成的入侵检测代理的管理应用, 记为: MA = {ma₁, ma₂, ..., ma_m}, m 为管理应用的个数. 入侵检测代理与其管理应用是一一对应的关系. 入侵检测代理的管理应用可以对入侵检测代理进行启动、停止、配置、修改等操作.

定义 2 基础检测代理(ba)可以定义为一个六元组:

ba = <a_id, ido, a_type, a_location, a_key, time, state>

其中: a_id 是基础入侵检测代理的唯一标识, 每

增加一个基础检测代理,系统都会按照它在代理层次图中的位置自动为其分配一个 id,每个基础检测代理的 id 用其在代理层次图中的树状索引来表示;ido 是被检测对象的 id 号,可以是重要的网络设备、应用或服务; a_type 是基础检测代理的类型,基础入侵检测代理包括:应用检测代理、服务检测代理、子网检测代理; a_location 是基础检测代理的位置,如位于哪个子网的入口处,或哪个子网的哪台主机上; a_key 为检测代理的密钥; time 是基础检测代理的创建时间; state 是基础检测代理的当前状态,包括正常运行、停止、异常终止三种状态。

定义 3 协调代理(ca)定义为一个六元组:

$ca = \langle ca_id, ca_location, ida_set, ca_key, time, state \rangle$

其中, ca_id 是协调代理的唯一标识,用协调代理在代理层次图中的树状索引来表示; ca_location 是协调代理的位置; ida_set 为 ca 的协调域,即受 ca 所管的下层入侵检测代理的集合; ca_key 为协调代理的密钥; time 是协调代理被激活的时间; state 是协调代理在某一时间的状态。

一个基础检测代理是能够完成基本检测功能的单元;一个协调代理是能够完成复杂检测任务的高级单元,由系统根据具体需求动态激活。入侵检测代理库 DB_{ida} 用来存放系统中所有入侵检测代理的定义,即上面描述的定义。 DB_{ida} 定义为: $DB_{ida} = \{ida_1,$

$ida_2, \dots, ida_n\}$ 。为了便于上下层检测代理进行联系,每个受监视主机都有一个存储入侵检测代理信息的数据库。这个数据库中存储了在代理层次图中上下层直接相邻主机上的所有入侵检测代理的具体信息。每个入侵检测代理可以通过唯一的标识 ID 被查询。

2.3 分级的安全策略管理

MAHID 系统采用集中与分布相结合的管理机制。系统中入侵检测代理之间的关系具有等级结构的特点,因此,从管理层次上看该系统也具有分级的等级树的特点。

各个入侵检测代理可以独立地配置本地的局部安全策略,但局部安全策略必须服从全局安全策略。初始时或全局策略发生变化时,由总控制台管理中心分发安全策略表,并由其下层代理一级一级地向下分发。上一级代理负责监控其下一级代理局部策略的变化;若与全局策略无冲突,则默认其变化;否则,强制更改局部策略表。总控制台管理中心定时查询各个入侵检测代理的工作状况,对出现的问题进行及时地处理。

3 入侵检测代理的功能结构

在这个模型中,主要包括两类入侵检测 agent (IDA),即基础检测 agent (DA) 和协调 agent (CA)^[4],其内部功能结构如图 2 所示。

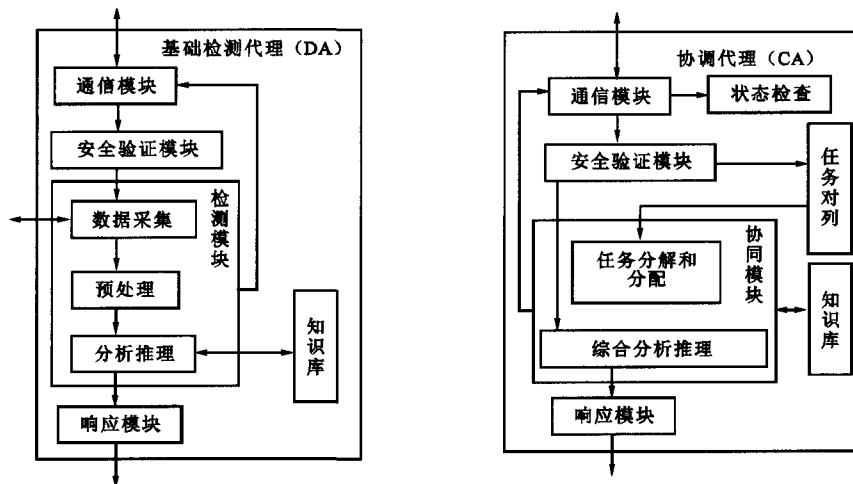


图2 基础检测 agent 和协调 agent 的内部功能结构

基础检测 agent 能够完成针对被检测对象的最基本的检测功能,主要由以下几部分组成:

- (1)通信模块:用于实现 agent 之间的通信。
- (2)安全验证模块:用于实现通信的安全性,验证通信对方身份的合法性。
- (3)检测模块:包括采集、预处理、分析推理三个

子模块,实时运行。采集子模块可从周围环境收集相应的信息,然后交由预处理子模块进行数据集成、数据清理、数据简化、分类等处理,接着由分析推理子模块对结果做出判断。如果检测到可疑行为但不能做出进一步判断,就还要通过通信模块向协调 agent 提交。

(4)响应模块:用于对检测到的攻击行为进行响应决策。

(5)知识库:用来存放攻击特征或系统正常行为特征,供检测机制进行匹配。

与检测 agent 不同的是,协调 agent 进行判断的依据来自相关的下层检测 agent 提交的数据。它不仅能够把检测任务分配给下层检测 agent,而且能够对下层代理发送来的数据进行综合分析和推理。除了通信模块和安全验证模块外,协调 agent 还包括以下几部分:

(1)协同检测模块:包括任务分解分配和综合分析推理两个子模块。任务分解分配子模块负责对任务进行分析分解,然后把子任务分配给合适的下层检测 agent 去处理。综合分析推理子模块负责对与某任务相关的下层 agent 提交上来的数据进行综合分析,如果检测到攻击,则在本地产生响应;否则,还要向其上层的协调 agent 提交。处理完毕后,如果没有新的任务,则转为对自身状态和行为的检测。

(2)任务队列:用于存放下层检测代理提交上来的任务,这些任务按照优先级顺序排列,等待任务分解分配子模块来处理。

(3)高级知识库:具有较高级的知识,这些知识可以为协同检测提供相关任务的检测 agent 的信息。

(4)状态检查:分为“忙”和“休眠”两种状态。如果协调 agent 正在和别的检测 agent 通信,则值为 1,否则为 0。

(5)超时检查:用来控制一项任务执行的时限,防止某任务长时间独占协调 agent。

4 检测代理的协作

4.1 协作原则

检测 agent 之间要有效协作,必须遵循一定的原则。MAHID 模型中各种 agent 之间的协作主要遵循以下原则:

协作原则 1 检测 agent 自身能解决的检测任务由自身来解决,当发现入侵行为时在本地主机上产生报警、报告或通知本地管理员。检测 agent 对于自己解决不了的检测任务,交由其上层的局部协调 agent 进行处理。

协作原则 2 局部协调 agent 分析其下层检测 agent 提交的检测任务,需要时协同下层各相关检测 agent 进行处理,当发现入侵行为时在本地主机上产生报警、报告或通知本地管理员。协调 agent 对

于自身不能解决的检测任务(如跨时间和空间的分布式入侵),则提交给其上层协调 agent。

协作原则 3 全局协调 agent 分析从不同子网提交上来的检测任务,协同整个受监视网络内的检测 agent 对其进行处理。当发现可疑活动时,在控制台上发出警报、命令或直接通知系统管理员。

4.2 协作的安全性

在该协同检测模型中,入侵检测 agent 通过协调 agent 实现相互之间的协作,而 agent 之间的协作是通过交换信息实现的。

入侵检测 agent 通过协调 agent 进行协同操作,主要有两种协同情况:一种情况是检测 agent 面对无法完成的检测任务时,请求本地协调 agent 帮助进行协同操作;另一种情况是本地协调 agent 面对检测 agent 提交上来的检测任务,命令下级其他检测 agent 进行协同操作。

安全约定 1 一个入侵检测 agent 与协调 agent 通信前,必须对协调 agent 执行加锁操作。加锁期间其他入侵检测 agent 不能与协调 agent 交互;超出规定时限或完成任务解锁后,协调 agent 才能与其他入侵检测 agent 交互。

为了避免并发请求冲突,保证数据的一致性和充分利用资源,系统对通信中的协调 agent 执行加“锁”操作,并规定占用时限。一个入侵检测 agent 与协调 agent 通信前,首先检查协调 agent 是否被锁定,如果没有,则对协调 agent 执行加锁操作,然后进行身份验证、提交任务等操作。在加锁期间,其他入侵检测 agent 不能对协调 agent 进行访问。二者的一次通信过程(包括验证身份、提交任务)完毕,该检测 agent 对协调 agent 进行解锁。解锁后其他入侵检测 agent 才能继续与协调 agent 进行通信。为了避免某个检测 agent 长时间占用主机上的协调 agent 造成拒绝服务攻击,系统对加锁时间有一定限制,每次执行完一次对话后检查计时值,超出时限仍没有完成通信任务的,协调 agent 自行解锁。此外,为了保证数据的一致性,系统还要返回到加锁前的状态。

5 检测代理的通信

该系统的安全通信问题主要包括四部分:不同层次的各检测 agent 之间、检测 agent 与控制台之间、检测 agent 与数据库之间、控制台与数据库之间。其中检测 agent 之间的通信是关键,因为检测 agent 之间安全、有效的协同是检测分布式协同攻击

的保证。

入侵检测系统要实现有效的协同检测,需要解决 agent 之间的两个通信问题:

(1) 系统中的一个检测 agent 怎样能够安全地联系到其上层的检测 agent,其中包括 agent 的定位和 agent 的认证。

(2) 系统如何保证检测 agent 之间通信的安全有效。

关于 agent 的定位问题,可以通过查询入侵检测代理库得到入侵检测代理的位置信息。查询到 agent 的位置信息后,还要确认将要通信的对方身份是否真实,这可以通过 agent 的认证来解决。

5.1 代理之间的认证

安全约定 2 入侵检测 agent 向协调 agent 请求帮助时,先提交证明其合法性的密钥,协调 agent 对其密钥进行验证,验证通过后二者方可建立通信联系。

为了确保 agent 之间通信的安全性,入侵检测 agent 请求协调 agent 帮助时,要先向协调 agent 发送一个证明其请求合法性的密钥,假设为 key。由于这个密钥可由检测 agent 的直系上层代理利用自己的私有信息和公共信息推导出,假设导出的密钥为 key',所以如果 key=key',则可验证检测 agent 的真实性。身份验证通过后,入侵检测 agent 才能向协调 agent 提交数据。

同样,协调 agent 向入侵检测 agent 发布命令时,入侵检测 agent 也要验证协调 agent 的合法性,如果协调 agent 发送来的密钥 key'与检测 agent 的密钥 key 一致,检测 agent 才会按照其命令执行操作,否则不予理会。

身份验证时请求信息的具体格式如下:

```
{
    aid;           //检测 agent 的 ID
    key            //证明其合法性的密钥
}
```

身份验证通过后,入侵检测 agent 之间才能进行信息交换。Agent 之间为了有效地协作,交换的信息应具有统一的数据格式,其通用格式定义如下:

```
{
    sender;        //发送 agent 的 id
    receiver;      //接收 agent 的 id
    time;          //信息发送的时间
    information;    //向对方发送的信息,可以是检测到的可疑情况,或请求对方完成的任务;
}
```

对于 information,它的内容视具体情况而不

同,可能包括以下三项:

(suspi_info, task_statu, data_needed)

suspi_info 表示已检测到的可疑情况;task_statu 表示任务状态,包括“无法判断”、“不能肯定”和“可以肯定”三种,“无法判断”是指发现情况可疑但不能判断,“不能肯定”是指怀疑是某种攻击但还缺少其他证据来进一步确认,“可以肯定”表示可以肯定发生了某种攻击;data_needed 表示确定某种攻击还需要的数据。

5.2 通信内容的安全

在该体系结构中,由于各检测 agent 之间要进行协作,所以各 agent 之间的通信是非常重要的。如果入侵者攻破 IDA 获得很大的系统权限,或 agent 间的通信内容被截获或篡改,那么恶意用户就能够很容易地修改 agent 的状态或破坏 agent。因此,对 agent 之间的通信内容必须加以保护。

这里采用加密和数字签名的二合一方法 RIM (RSA+IDEA+MD5)^[6]来保护 agent 之间通信内容的安全。在加密技术方面,目前大多采用 RSA 算法。它的安全性很高,但计算量太大,不适合于大数据量的加密。MAHID 对需要大量传输的日志信息采用计算量相对较小的对称加密算法 IDEA (International Data Encryption Algorithm),而对 IDEA 算法的密钥则采用 RSA 进行加密。对于数字签名,采用单向散列算法 MD5 (Message Digest 5) 产生信息摘录,并用 RSA 对摘录加密(用私有密钥),从而得到签名。这样的链式加密方法既有 RSA 体系的保密性,又有 IDEA 算法的快捷性。

检测 Agent 与控制台之间、检测 Agent 与数据库之间、控制台与数据库之间的通信可采用类似的方法来解决。

6 协同检测算法

协同检测需要多个代理进行合作,假设一个人侵检测代理的上层协调代理在本协调域内能够找到解决方案,则系统中代理之间的交互过程可以用如图 3 所示的顺序图来表示。

每个基础检测代理 BA 针对各自的检测对象进行入侵检测,当遇到不能解决的检测任务时,则激活其直系上层的协调代理 CA,并向该 CA 提交任务。协同检测的具体过程描述如下。

(1) 身份验证和任务的提交

BA 在提交任务前,首先检查 CA 的状态,若 CA 空闲,则锁定 CA,否则等待。锁定期间其他 BA 不能与该 CA 通信。锁定 CA 后,BA 向 CA 提交密

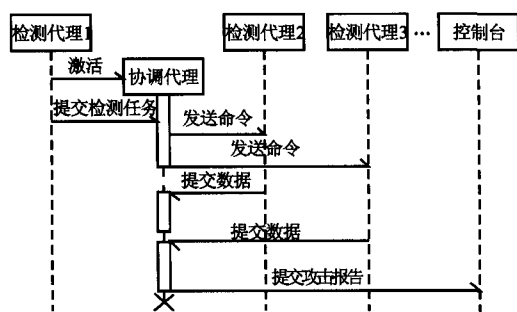


图3 协同检测的顺序图

钥,CA的安全验证模块对其进行身份验证,验证通过后BA才能向CA提交任务信息。任务提交完毕后,BA对该CA解锁,解锁后其他BA才能与该CA通信。

(2)任务的计算与排队

CA接收到任务后,计算该任务的优先级,并按计算出的优先级 p_i 大小将其添加到任务列表中。威胁度 t_i 和可疑度 d_i 的综合指数越高,则优先级越高,优先级越高的任务则排在任务队列的越前面。

任务优先级的计算方法是: $p_i = (t_i + d_i) / 2$ 。

将任务添加到任务队列中的方法是:比较新到任务与队列中的第一个任务的优先级,若新任务的优先级“小于”被比较任务的优先级,则与队列中的下一个任务进行比较,依次类推,直到比较结果为“大于”时,则停止比较,并将新任务放在该任务的前方。

(3)任务的分解与分配

CA的任务分解分配子模块从任务队列中依次将任务取出并处理。当该任务到达队首时,CA的任务分配模块从队列中将任务取出,并在知识库中查找相应的解决方案。如果没有找到解决方案,则说明涉及到了其它协调域的知识,于是上传给更高一级的CA;如果找到解决方案,则CA的任务分配模块根据知识库中的知识选择合适的BA执行任务,并按IDA列表中提供的信息与BA通信。

(4)任务的执行

收到命令的BA执行CA的命令前,先验证CA的身份,验证通过后方可按CA发送来的命令进行相关的数据采集、整理和缩减,最后提交给该CA。

(5)任务的综合分析

CA的协同检测模块接收下级BA提交的信息,并按照知识库中的知识对所有和任务相关的信息进行综合的分析和处理。如果CA可以确定系统发生了入侵,则会产生报警和报告;如果不能确定,则会在缩减无关数据后,把重要的相关数据提交给全

局CA。

任务执行完毕后,检查任务队列是否为空。若队列为空,那么CA的一个生命周期就结束了,接着进入休眠状态,只等待新的任务再次把它激活;如果不为空,则从上面的第3步骤开始,依次处理等待服务的任务。

7 结束语

为了有效地发现和识别攻击,入侵检测系统各部件必须进行有效协同。本文对具有动态协同能力的基于多agent的入侵检测系统进行了研究,提出了安全有效的协同方案,增强了检测复杂攻击的能力,同时也提高了检测攻击的准确性。

参考文献:

- [1] Dorothy E Denning. An intrusion - detection model [J]. IEEE Transactions on Software Engineering, 1987, SE-13(2): 222-232.
- [2] Chenfeng Vincent Zhou, Christopher Leckie, Shanika Karunasekera. A survey of coordinated attacks and collaborative intrusion detection[J]. Computer & Security, 2010(29): 124-140.
- [3] Huwaida Tagelsir Elshoush, Izzeldin Mohamed Osman. Alert correlation in collaborative intelligent intrusion detection systems - A survey[J]. Applied Soft Computing, 2010(11): 4349-4365.
- [4] Ran Zhang, Depei Qian, Heng Chen, et al. Collaborative intrusion detection based on coordination agent [C]//The International Conference on Parallel and Distributed Computing, Applications and Technologies (PDCAT' 2003). America: IEEE Press, 2003: 175-179.
- [5] 张然. 动态自适应的入侵检测与响应模型研究[J]. 北京工业大学学报, 2005(31): 97-102.
- [6] 杨鲲, 刘大有, 郭欣. 一个具有高安全性的移动Agent系统模板结构[J]. 软件学报, 2002, 13(1): 130-135.

作者简介:

张 然 女, (1973-), 博士. 研究方向为网络安全、入侵检测、网络攻防对抗等。

刘 洋 男, (1978-), 博士. 研究方向为信息安全、优化算法等。

尹毅峰 男, (1971-), 博士. 研究方向为信息安全、网络安全协议、多态性密码理论。

甘 勇 男, (1965-), 博士. 研究方向为计算机网络与网络安全。