可回卷的自动入侵响应系统[1]

张剑，龚俭

（东南大学计算机科学与工程系，江苏省计算机网络技术重点实验室 南京 210096）

摘要：本文描述了入侵响应回卷的形式化方法及其实现，然后建立了一个可回卷的自动入侵响应系统模型。该系统在检测到误报或入侵停止的情况下，采取响应回卷动作，从而消除了响应带来的负面影响，即响应代价。试验证明，通过计算入侵检测代价，响应回卷技术能较好地降低响应代价，从而以较低的代价换取相同的安全目标。

关键词：入侵检测系统；自动响应系统；响应回卷；中止检测算法

中国法分类号：TP393　　**文献标识码**：A　　**文章编号**：030613

Rollbackable Automated Intrusion Response System

ZHANG Jian, GONG Jian

（Dept. of Computer Science and Technology, Southeast University, Nanjing, Jiangsu 210096, China）

Abstract: Traditional intrusion detection systems only carry out response when intrusion is detected, while don't respond to "nonexistence" of intrusion. That has two shortcomings. First, when the previous intrusion events that had been responded are proved to be false alarms, the response system cannot correct its response. Secondly, when the intrusion behavior terminates, the response system cannot withdraw the corresponding response so as to eliminate the negative effect. In this paper, a Rollbackable Automated Intrusion Response System (RAIRS) is established to cope with the above two problems. RAIRS can not only automatically direct response, but also detect false alarms and termination of intrusion, and then triggers the rollback of corresponding response to eliminate its negative effect. By calculating the cost of intrusion detection system, the experiment proves that the response rollback technique can decrease the response cost so that it can achieve the same security goal with lower cost.

Key words: intrusion detection system; automated response system; response rollback; termination detection algorithm

一．引言

入侵检测系统（intrusion detection system，简称 IDS）的目的是监视计算机网络和系统，以发现违背安全政策的行为。IDS 的主要功能包括检测和分析用户在网络中的活动，识别已知的攻击行为，统计分析异常行为、检查系统配置和漏洞和入侵响应等。入侵响应是对入侵事件所采取的措施，目的是为了抑止、评估和恢复入侵损失，甚至追踪和封堵入侵源，没有响应就不可能实现 IDS 的安全目标。

根据响应方式的不同可将响应系统分为三类：告警型、人工响应型和自动响应型。告警型响应系统仅能产生入侵事件报告和警报，而完全由安全管理员做出响应，这种响应方式不但时延较长，而且当警报多时，安全管理员就无法一一做出响应了；人工响应系统除了具有告警型响应的功能外，还能够为安全管理员提供响应帮助，例如列举出针对目前事件的响应方式供安全管理员选择，这种响应方式仍然具有告警响应系统的缺点；自动响应系统可以根据当前的安全状态自动做出响应决策，无需安全管理员的干预，它具有反应灵敏、能适应复杂环境的特点，但目前其判断的准确度仍然不够理想。

为了改进自动响应功能，Curtis[1]提出一种入侵响应的分类方法，他认为应该根据入侵时间、入侵事件类型、攻击者类型、事件可信度、攻击意义和环境制约这些条件来选择响应

[1]本文受国家自然科学基金项目 90104031 资助。

方式。其中入侵时间是指响应相对于入侵的时间，可分为入侵前、入侵进行中和入侵后；攻击意义是指攻击目标的关键度;环境制约是指响应要考虑到法律、伦理和系统资源等的限制。在其响应分类的基础上，Curtis 进一步提出了一个自动入侵响应的系统框架。Christopher[2]提出将意图识别技术应用到入侵响应中，根据当前攻击者的行为推断其下一步动作或意图，从而做出具有预见性的响应。DARPA 的“自动入侵追踪和响应”项目[3][4]研究将入侵检测系统和防火墙、路由器和主机等结合在一起建立企业内部局域网范围内的自动防御系统技术。其核心是建立一个入侵检测和隔离协议（Intrusion detection and isolation protocol，IDIP），系统的各组件通过该协议协同检测入侵、交换入侵行为信息和动态地配置防火墙、路由器和主机以自动做出响应。上述的自动响应技术都是针对“存在”入侵事件而做出响应，而无法对“不存在”入侵事件的情形而做出响应。这样会导致：

（1）当 IDS 发现某个事件是误报时，无法撤销对该事件的响应。

（2）当 IDS 察觉采取响应后入侵已经停止时，不能自动解除响应，而该响应会产生一定的负面影响，例如造成用户不能访问服务，因为该服务已作为响应的一部分被挂起。

本文提出一种响应回卷（Response Rollback）方法和基于这种响应回卷方法的的自动入侵响应系统(Rollbackable Automatic Response System，RARS)，响应回卷可自动判别响应命令的可回卷性，然后将可回卷的响应命令转化为响应回卷命令，响应回卷命令进一步被编译为某种响应执行脚本，该脚本可自动执行响应回卷动作。RARS 据此可检测到入侵事件的“不存在”，然后完成响应回卷功能，从而有效地弥补传统响应系统的缺陷。

本文的第二节讨论响应回卷形式化描述和误报及入侵中止的检测问题，第三节讨论建立可回卷的自动入侵响应系统，第四节给出相应的试验结果，最后是总结。

二．响应回卷

响应回卷的基本思想是撤销多余的甚至有负面影响的入侵响应。最常见的情形是当入侵检测系统发现误报和入侵行为已经停止时，应该撤销对这些入侵行为的响应，否则可能会增加 IDS 的负荷或负面影响。响应回卷的实现涉及两个关键技术：

（1）响应和响应回卷的形式化定义。由于响应回卷是建立在已有响应的基础上的，因此如果不能完整和正确地描述响应，就不能有效地实现响应回卷；另外在自动入侵响应系统中，要求自动地将响应转化为响应回卷，这就需要一种形式化方法来支持该功能。

（2）误报和入侵中止的自动检测。如果不能发现误报和入侵停止，那么响应回卷就无从实施。这一点对以往的 IDS 来说是无能为力的。

本节以下内容将围绕这两个关键技术展开讨论。

2.1 响应回卷的形式化定义

定义 1 响应主体是可唯一标识的对象，它是一个具有如下形式的 ***RS***：

$$RS := \langle Domain\rangle[!\langle Sub\text{-}domain1\rangle[!\langle Sub\text{-}domain2\rangle\ldots]]$$

其中 *domain* 和 *Sub-domain* 是响应主体的定位符，$Domain \supset Sub\text{-}domain1 \supset Sub\text{-}domain2 \supset \ldots$，“!”是域间的分割符。

例如路由器 192.168.2.1 中的访问控制列表 *AL* 可表示为：192.168.2.1!*AL*

定义 2 元操作是对响应主体施加的最基本和独立的动作类型。元操作可分为两类，一类存在某种元操作与其效果相反，且会改变响应主体的状态，这种元操作称为可逆元操作，该动作效果相反的元操作称为该可逆元操作的逆元操作，记可逆元操作为 o_r，其逆元操作集合为$\neg\ o_r$；另一种不存在动作效果相反的元操作或不会改变响应主体的状态，称为不可逆元操作，记可逆元操作为 o_n，其逆元操作为$\neg\ o_n = \phi$。ϕ表示空操作。

例如 *add*、*delete* 等操作称为可逆元操作，而 *send*、*kill* 则是不可逆元操作。*Run* 的逆元操作集合为{*hangup*，*kill*}。而 *kill* 虽然是 *run* 的逆元操作，但它没有逆元操作。

下表是常用元操作的意义和相应的逆元操作：

表 1 常用元操作意义及逆元操作

	意义	逆元操作集	实例
Add	向响应主体添加操作数	{remove}	阻塞攻击源地址（路由器响应）
Create	创建响应主体	{delete}	创建系统备份
Run	运行程序	{hangup,kill}	运行其他入侵检测工具
Send	向响应主体发送信息	ϕ	向安全管理员发出警报
Enable	使响应主体参数生效	{disable}	额外日志生效
Lock	封锁响应主体	{unlock}	锁住用户帐户，使其不可用
Shutdown	关闭响应主体	{startup}	关闭主机
Kill	中止程序运行	ϕ	中断用户会话

定义 3 操作数 *Ou* 是对响应主体施加的动作内容，操作数为空记为 *null*。

例如在路由器的访问控制列表中增加某条访问控制规则，该规则就是操作数。

定义 4 元响应是具有以下形式的三元组 *UR*：

$$UR=<Op,RS,Ou>$$

其中 *Op* 是元操作，*RS* 是响应主体，*Ou* 是操作数。元响应是最基本的响应动作，逆元响应是与元响应动作效果相反的元响应，记元响应 *UR* 的逆元响应为¬ *UR*，则¬ *UR*＝<¬ *Op,RS,Ou*>，若¬ *Op*＝ ϕ，则¬ *UR*＝ ϕ，称为空响应。

定义 5 响应 ***R*** 是一个元响应序列。其形式为：

$$\boldsymbol{R}=<UR_1,UR_2,\ldots,UR_n>,\ n=0,1,2,\ldots$$

响应回卷是与某响应动作效果相反的响应，记为¬ ***R***，则¬ ***R***＝<¬ UR_n, ¬ UR_{n-1},…, ¬ UR_1>。

响应定义的意义在于：每个具体的响应都可以分解成元响应序列，响应回卷则是从最后一个元响应开始取逆元响应，如果其中某些逆元响应为 ϕ，则不执行这些逆元响应。

2.2 误报的检测

并非所有的误报都可被检测，在下列情况下可以发现误报：

（1）基于非单调逻辑的 IDS 可以自动检测误报。

文献[5]提出建立一种基于非单调逻辑的 IDS，该系统的入侵检测模块不是遵循传统的命题逻辑推理规则，而是基于模糊默认逻辑的推理方式。这种推理方法能在不充分证据的前提下推出有一定可信度的安全结论，不但提高了 IDS 的灵敏度和海量数据的分析处理能力，还能发现误报，从而推翻原来做出的安全结论判断，然后向响应系统提出响应回卷请求。

（2）由入侵意图识别模块发出的入侵警报

入侵意图识别技术能根据当前的入侵状况预测未来的入侵趋势，然后发出预警，从而指示响应系统做出有预见性的响应。但这也可能产生误报，这时候应该撤销原有的响应，而根据当前状态重新做出响应。

（3）人为干预

安全管理员可能通过各种途径发现误报，在这种情况下安全管理员可发起响应回卷。

2.3 入侵停止的自动检测

入侵会话过程是指由多个步骤组成的的复合攻击方式的入侵过程，它通常表现为一个入侵事件序列，该序列中的每个事件都为了实现某个子目标。

入侵会话过程的入侵事件序列很难事先确定，因为该入侵方式可能是未知的，也可能它存在多种入侵事件序列。然而属于同一入侵会话过程的入侵事件之间必然存在某些相似的特征值，这些特征称为本质特征。因此如果能找到本质特征，就能将属于同一入侵会话过程的入侵事件聚合在一起。

设某入侵事件序列 $\boldsymbol{IS}=<E_1,E_2,\ldots,E_n>$，本质特征集 $EC=\{c_1,c_2,\ldots,c_k\}$，$n,k=1,2,\ldots$，***IS*** 是入侵会话过程当且仅当 $E_i.c_u=E_j.c_v$，$u,v=1,2,\ldots k$，$i,j=1,2,\ldots,n$，且 $TI_i=T_{i+1}-T_i\leqslant\tau$，其

中 T_i 代表 i 事件发生的事件，TI_i 代表相邻事件的时间间隔，τ 是相邻事件到达间隔阀值。

最常见的本质特征集是{源地址，目标地址}。但这不是绝对的。例如对于 DDOS 攻击，本质特征就只有目标地址；而对于扫描攻击，本质特征只有源地址。因此在入侵事件聚合时应先识别事件类型。

定义 6 中止检测算法是指发现入侵会话过程已经停止的检测算法。它可描述为：

对入侵事件序列 $IS=<E_1,E_2,\ldots,E_n>$，若 $\neg\exists E'\forall i((E'.c_i=E_n.c_i)\wedge(0<TI_n\le t)),i=1,2,...,k$，则宣称该入侵会话过程已经停止；否则 $E_{n+1}=E'$，$IS=<E_1,E_2,\ldots,E_n,E_{n+1}>$。

中止检测算法的基本思想是当在相邻事件到达间隔阀值内没有新的入侵事件到达，则认为当前入侵会话过程已经停止。

三．响应回卷的实现模型

3.1 依赖平台的自动响应执行脚本

不同响应是在响应设备不同的操作系统平台之中执行的，响应设备通常包括路由器、防火墙和主机等。由于响应设备分散在网络中，要做到自动响应，必须将响应命令通过某种方式传递给响应设备，有两种方法可以做到这一点：

（1）设计一种自动响应协议，该协议负责在 IDS 和响应设备之间传递响应命令，响应设备一旦接收到响应命令，即自动运行响应脚本或修改自身相关配置。这种做法的典型例子就是 IDIP，IDIP 不仅能传递响应命令，还可以在 IDS 的各组件中进行协同入侵检测等工作。

（2）利用某种自动交互脚本，该脚本能够自动登录到响应设备中，执行响应程序或配置系统相关参数。这种方法类似于人工响应，人工响应动作对应于脚本中的语句，但自动交互脚本完全由其解释器解释执行。Expect 正是这种自动交互工具，目前对其应用主要用于 IDS 评估中。

两种方法的优劣比较如表 2 所示：

表 2 自动响应实现方式比较

	自动响应协议方式	自动响应脚本方式
通用性	好。通过一种独立于平台的协议在 IDS 和响应设备之间通信，但是响应设备必须支持该协议。	不好。对不同平台的相同响应，必须编写不同的自动交互脚本。响应设备不需要理解该脚本
实用性	不好。就 IDIP 而言，它目前已被实现而处于测试阶段，功能还待完善。而且它要求每种响应设备都要支持 IDIP 协议，从而不能与目前使用的路由器兼容。	较好。自动响应脚本以文件的形式存储于响应系统中，只需由一个解释器解释执行，响应设备不需要做任何修改就与该技术兼容；要增加新的响应方式，只需编写相应的自动响应脚本。
扩展性	取决于协议制订得是否完善。但就响应方式而言，是无法定义完全的，不同的环境有不同的可用响应方式集；就网络规模而言，其扩展性较好。	一般。要增加新的响应方式，只需编写相应的自动响应脚本；但当网络规模扩大时，要维护的响应脚本将大大增加。
对响应回卷的支持	很难支持。即使能支持，协议的复杂度也必然大大增加。	支持。响应脚本只需做轻微的修改便可变为响应回卷脚本。

从表 2 可以看出，交互协议的弱点主要体现在兼容性和复杂性，而本文的重点是研究响应回卷技术，不是制订自动响应协议，因此不采用该技术。自动响应脚本具有简单易于实现的优点，而且与现有响应设备兼容，易于做试验，并且支持响应回卷，因此尽管它有通用性和扩展性的问题，本文还是采用该技术来实现自动响应和响应回卷。

3.2 响应回卷触发时机

响应状态的改变有两种情况，第一是当前的响应状态回退到过去的状态，这种情况可以通过响应回卷来实现；第二是当前的响应状态迁移到从来未出现的新状态。第一种情况引发响应回卷，其原因有：

（1）入侵检测进程检测到误报后

典型的情况是入侵检测进程支持非单调逻辑推理机制，当它采集到的数据推翻其原有的安全结论时，它发出响应回卷命令，要求响应系统回卷以前做出的响应。

（2）入侵意图识别进程取消预警后

当前的安全状态与先前预测的不一致时，应该取消原有的预警，通知响应系统回卷先前的响应。

（3）中止检测模块检测到入侵已停止后

中止检测模块采用中止检测算法探测复合攻击的进展情况，如果在一定的时间阀值内没有发现目标复合攻击的进一步行动，则发出入侵中止信号，指示响应系统做出响应回卷。

（4）人为干预

当安全管理员发现误报或入侵中止后，也可以触发响应回卷。

3.3 RARS 系统模型

RARS 应该能满足以下要求：

（1）能够自动做出响应和响应回卷，也要提供用户界面以触发人为的响应回卷。

（2）能够进行中止检测及对误报事件做出响应回卷。

该系统模型如图 1 所示：

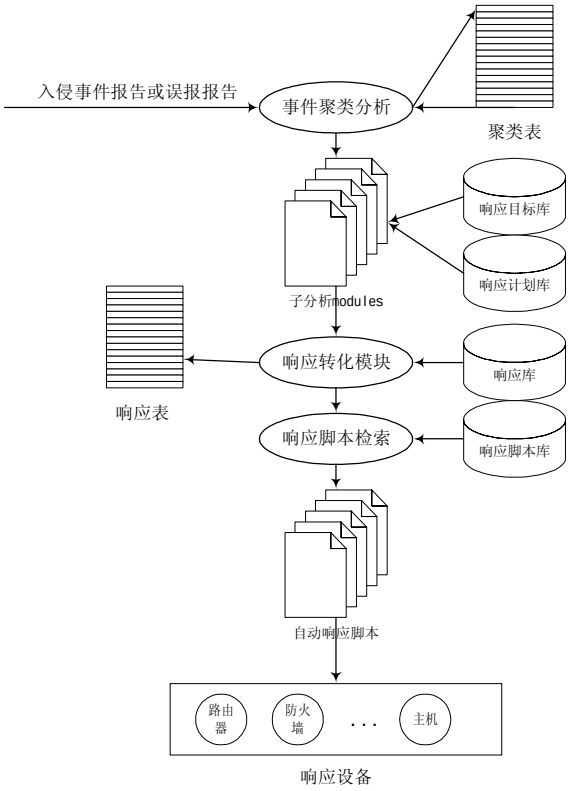

图 1 RARS 系统模型

下面对图 1 每个组件功能做说明

（1）事件聚类分析模块分析入侵事件报告，判断它是否属于已有的入侵会话过程，如果是，则将该事件报告传递给该入侵会话过程的子分析模块；否则新创建一个子分析模块来分析该事件，并将该模块信息记录在聚类表中。如果事件聚类分析模块接收到误报报告，则将响应回卷命令和误报报告传递给相应的子分析模块。

（2）子分析引擎分析接收到的入侵事件报告，首先查询响应计划库以获取可行计划集，然后根据响应目标评估各种计划的优劣，从中挑选最优计划和事件报告传递给响应转化模块。如果接收到响应回卷命令，则将响应回卷命令和误报的入侵事件编号传递给响应转化模块；子分析引擎的另一个功能是中止检测，如果发现当前入侵会话过程已经停止，就回卷该入侵会话过程的全部入侵事件响应。

（3）响应转化模块负责将输入的响应计划转化为响应，即元响应序列，然后将入侵事件编号和相对应的元响应序列记录在响应表中，并输出元响应序列。在转化过程中需要查询响应库和参考事件报告。响应库中存储了对应每种响应的元响应集合。对于响应回卷命令，它根据入侵事件编号查询响应表，以获取元响应序列，然后将其转化为逆响

应的元响应序列，排除空响应，然后输出该序列。

（4）响应脚本检索模块从响应脚本库中取得每个元响应的自动响应脚本，并依次执行。在必要的时候它会动态产生当前元响应的响应回卷脚本。

（5）自动响应脚本操纵响应设备执行响应和响应回卷。

四．试验及其结论

4.1 试验目的和环境

本试验的目的是对 RARS 与不带响应回卷功能的自动入侵响应系统 ARS 从代价角度做一比较评估，并量化之。入侵响应系统中的代价类型包括操作代价 OCost、响应代价 RCost、入侵代价 DCost 和响应回卷代价 RRCost，其中操作代价是指执行响应所需要的 CPU、内存和网络带宽等的资源总量；响应代价是指响应造成的负面影响，例如网络服务、信道资源不可用等；入侵代价是指从入侵成功到响应后的这段时间入侵带来的损失；RRCost 是指执行响应回卷的操作代价。入侵响应的综合代价就是这四类代价的和。设入侵响应系统 R 的期望综合代价为 *CumulativeCost*（*R*），入侵事件类型集合为 E，则

$$CumulativeCost(R) = \sum_{e \in E} l(e)(OCost(e) + RCost(e) + DCost(e))$$

其中 $\lambda(e)$表示该入侵类型在全部入侵事件中所占的比例。

本试验是在 CERNET 的环境中进行，根据该网络环境入侵发生特点和入侵检测模块的性能，即网络入侵事件类型的分布情况和误报率来确定两种自动响应系统的综合代价。

4.2 试验方法

首先需要确定 CERNET 中的主要已知网络入侵事件类型和针对每种类型的响应，然后确定入侵事件类型的数量分布情况和针对 RARS 和 ARS 每种响应的综合代价，最后计算出这两种自动响应系统在该入侵事件类型分布集中的期望综合代价。

各种代价类型的代价量化是一个难点，本试验采用的量化根据来源于 Wenke Lee 和 Wei Fan 等人的工作[5]、CERNET 的实际情况和简化假设。以下是几条量化规则和简化假设，

（1）假设入侵事件的攻击目标是提供 CERNET 公共服务的设备，例如路由器、邮件服务器和域名服务器等。对这些设备的入侵响应一般会造成较大的负面影响。

（2）对操作代价和入侵代价的量化方法主要来自[6]。而响应回卷代价与操作代价相同。

（3）响应代价是随着时间增长而单调递增的量，这一点在表 3 可以看出，因此在此将响应代价简化假设为时间的一阶线性函数。即 $RCost = a \times t$，其中 a 是单位时间的响应代价，t 代表从响应完成开始到当前的时间。

（4）响应代价的量化以货币价值为标准，例如 Yahoo 的收费邮件服务有 n 用户，月费用为 c 元，则如果采用将邮件服务器从网络中隔离开的响应方式，响应后每分钟的响应代价 $RCost \approx (n \times c) \div (30 \times 1440)$ 元/分钟。

4.3 试验过程和结果

本试验采用的入侵检测系统是 Snort，Snort 是一个开放源代码的网络入侵检测系统，它能够检测多种网络入侵类型，我们将其改造成将每条检测到的入侵事件都写入数据库中，每天检测的事件是一张表，其数据规模大约是 200－400 条记录，误报率为 10.23%。以下是 CERNET 的主要已知入侵事件类型、每天数量分布情况和相应的响应计划：

表 3 入侵事件类型分布及响应计划

事件类型	所属类别	破坏代价 *ICost*	所占比例	响应计划
Dos	DOS	30	0.01%	记录、将主机从网络中断开（1）
				记录、封锁攻击源（2）

Buffer Overflow	ROOT	100	10.11%	记录，封锁攻击源，封锁用户帐户（3）
				记录，挂起存在堆栈溢出漏洞的进程（4）
Scan	PROBE	2	59.9%	记录，封锁攻击源（2）
				记录,将攻击目标的 ICMP echo 功能设置为不可用（5）
Decoding	R2L	50	4.49%	记录，封锁攻击源（2）
				记录，使被攻击端口不可用（6）
Web based Attack	R2L	50	10.39%	记录，封锁攻击源（2）
				记录，使被攻击端口不可用（6）
Virues	R2L	50	0.57%	记录，封锁攻击源（2）
				记录，将主机从网络中断开（1）
BackDoor or Trojan horses	R2L	50	12.04%	记录，封锁攻击源（2）
				记录，使被攻击端口不可用（6）

表 3 为每类入侵事件制定了两种响应计划，每种不同的响应计划用唯一的数字来标识。

表 4 是 RARS 和 ARS 针对以上几种入侵类型的综合代价：

表 4 对几种入侵事件类型进行自动响应的综合代价

响应计划	Ocost		RCost		DCost		RRCost		CumulativeCost	
	ARS	RARS	ARS	RARS	ARS	RARS	ARS	RARS	ARS	RARS
（1）	20	20	228t	228t’	$e_1 \times ICost$	$e_1 \times ICost$	0	20	228t＋20＋…	228t’＋40＋…
（2）	20	20	10t	10t’	$e_1 \times ICost$	$e_1 \times ICost$	0	20	10t＋20＋…	10t’＋40＋…
（3）	30	30	11t	11t’	$e_1 \times ICost$	$e_1 \times ICost$	0	30	11t＋30＋…	11t’＋30＋…
（4）	20	20	150t	150t’	$e_1 \times ICost$	$e_1 \times ICost$	0	20	150t＋20＋…	150t’＋40＋…
（5）	20	20	5t	5t’	$e_1 \times ICost$	$e_1 \times ICost$	0	20	5t＋20＋…	5t’＋40＋…
（6）	20	20	150t	150t’	$e_1 \times ICost$	$e_1 \times ICost$	0	20	150t＋20＋…	150t’＋40＋…

其中 *t* 代表从采取响应后直到人工消除响应代价的一段时间，*t’*则代表从采取响应后直到响应回卷完成的一段时间，总的来说 *t*＞＞*t’*。*DCost* 是与入侵事件类型相关的，本文对它的量化方法是该入侵类型的破坏代价 *ICost* 乘以一个折扣参数 $e_1 \in [0,1]$ 。

设对每种入侵类型的响应计划是使用机会均等的，*t*＝1（天）＝24×60＝1440（分钟），*t’*＝10（分钟），ε_1＝0.1。则

$$CumulativeCost(ARS) \approx 50217.46, CumulativeCost(RARS) \approx 392.10$$

从结果可以看出，RARS 的综合代价要比 ARS 的低得多，从而反映了响应回卷对降低代价起了非常明显的效果。

五．总结

本文介绍在入侵响应系统系统中引入响应回卷技术，使对误报和停止的入侵现象的响应能被撤销，从而能降低了响应带来的负面影响。该技术包含几个技术要点，一个是响应回卷的形式化，该形式化使得响应回卷的意义能够被严格地确定下来；第二是执行自动响应的自

动响应脚本技术，该技术使得响应回卷命令能自动产生并自动执行，比起交互协议形式具有简单易于实现和与现有设备兼容的特点；第三是可回卷的自动入侵响应系统 RARS 模型，该结构使得响应回卷技术在响应系统中被支持和实现。

试验从代价角度衡量了 RARS 和 ARS 的性能。在 CERNET 这个具体环境中，通过文献[6]和我们的代价量化方法，试验证明 RARS 能大大降低响应的综合代价。这个结论也能扩充到大多数的环境中。

【参考文献】

1. Curtis A. Carver and Udo W. Pooch[C], *An intrusion response taxonomy and its role in automatic intrusion response*, Proceeding of the 2000 IEEE Workshop on information assurance and security, United states military academy, West Point, NY, 2000, 129-135.
2. Christopher W Geib and Robert P Goldman[C]；*Plan Recognition in Intrusion Detection System*. In DARPA Information Survivability Conference & Exposition II，Hilton Anaheim, California, 2001，46-55.
3. Dan Schnackenberg, Kelly Djahandari and Dan Sterne[C]；*Infrastructure for intrusion detection and response*, In proceedings of the DARPA information survivability conference and exposition(DISCEX) 2000, Hilton Head, S.C,2000, 1507-1516
4. Dan Schnackenberg, et al[C]. *Cooperative intrusion traceback and response architecture(CITRA)*, In proceedings of the DARPA information survivability conference and exposition(DISCEX) 2001, Anaheim Califonia, 2001
5. ZHANG Jian，GONG Jian and DING Yong[C], *Intrusion detection system based on fuzzy default logic*, Proceeding of the 2003 IEEE Workshop on fuzzy system，St. Louis, 2003.
6. Wenke Lee, Wei Fan, et al[J]. *Toward Cost-Sensitive Modeling for intrusion detection and response*, Journal of Computer Security, 2002,10, 1: 318-336

作者简介：

张剑：男，1977 年生，博士研究生，主要研究方向为网络安全监测

Zhang Jian, male, born in 1977, Ph.D, Major in network security monitoring and intrusion detection.

龚俭：男，1957 年生，工学博士，教授，博士生导师，主要研究方向为网络安全、网络管理、网络体系结构

Gong Jian, male, born in 1957, Ph.D director, major in network security , network management and network system architecture