自适应虚警处理框架研究与实现 *

段祥雯
(国防科技大学 计算机学院, 长沙 410073)

摘 要: 在分析虚警来源及现有处理技术的基础上,提出了一个具有自适应能力的入侵检测系统虚警处理框架。该框架可以自动适应环境的变化和攻击技术发展带来的变化,从不同角度减少虚警,提高警报数据质量。

关键词: 网络安全; 入侵检测; 虚假警报; 自适应
中图分类号: TP309 **文献标志码**: A **文章编号**: 1001-3695(2009)06-2141-04
doi:10.3969/j.issn.1001-3695.2009.06.043

Research and realization on adaptive framework for false alarms reduction

DUAN Xiang-wen
(*School of Computer Science, National University of Defense Technology, Changsha* 410073, *China*)

Abstract: On research of the causal of false alarms and existing techniques in false alarm reduction, this paper proposed an adaptive framework. This framework is able to auto-adapt to the variation of environment and the movement of attack techniques, improves alerts data qualities and reduces false alarms from multi point of view.

Key words: network security; intrusion detection; false alarm; adaptive

IDS(intrusion detection system,入侵检测系统)对于保障网络安全有着重要作用,然而虚假警报问题却严重影响到其使用。来自 IDS 底层的大量虚假警报,往往使得管理员疲于应付,大量精力耗费于虚假警报,难以从中辨别真实攻击,对所发生事件无法作出准确判断,并快速、及时地响应;甚至有管理员因此忽略所有警报。减少虚假警报,提高警报有效性,已成为 IDS 使用过程中亟需解决的问题。

1 虚警处理技术分析

目前已提出的虚假警报处理技术大体可分为两类:第一类手动配置 IDS 以过滤虚假警报的方法,第二类自动分析并减少虚警的方法。第一类方法主要通过调整 IDS 检测策略,包括 IDS 的放置位置、IDS 检测规则、检测特征、警报严重级别等来实现。可采用专家分析的途径,根据用户关注目标制定相应检测策略,也可使用特殊的分析技术,如 Julisch[1] 提出的根原因分析方法,利用数据挖掘探寻虚警产生的根原因,再以此为依据配置 IDS。第一类通常可将 IDS 警报真实率提高至 60% 以上[2],但也存在明显的缺点:a)在配置 IDS 前需清楚地了解网络拓扑及站点知识;b)规模大且拥有多个 IDS 的网络中,配置工作量大且繁琐,很可能会因此导致配置失误。

第二类属于自动实现的方法,主要包括多种检测技术相结合的方法、脆弱性评估方法、警报验证方法、自动分类并过滤的方法和警报关联方法。

多种检测技术相结合[3] 的方法,如将主机型与网络型检测结合、滥用与异常检测方法结合,特征分析、协议分析、统计分析多种分析技术结合,可以提高检测性能,从检测层减少虚假警报。很多系统已采用这种方法,如 EMERALD、DIDS、MCAfee Intrushield,取得了比较明显的效果。但是,由于检测技术本身仍不够完善,目前仍需其他各类方法的辅助。

脆弱性评估方法[4] 使用脆弱性评估工具分析网络薄弱点并自动配置 IDS,有助于从检测层减少无效警报,但局限于已知攻击漏洞和评估工具本身,会出现对未知攻击漏报的情况。

警报验证方法采用警报验证技术来确定警报的真实性,典型的应用如 Cisco 的威胁响应技术[5]。该类方法又可分为消极验证和积极验证两种[6]。消极验证方法预先收集网络拓扑、操作系统、开放端口等信息,以此判断目标是否存在漏洞,从而确定警报是否有效。消极验证方法无须干扰网络设备的正常运行,不会运行额外的测试从而延迟响应,但是存储为先验知识的网络状态与当前实际状态之间往往会产生偏差,从而导致判断失误。积极验证方法通过检查目标主机上的信息来寻找攻击成功的证据,通常需要与目标机建立连接并对其进行扫描,准确性高,但需消耗网络带宽以及被扫描主机的系统资源,在警报数量大时,未验证的警报往往需要排队等待,验证时间受到网络性能及验证方法的制约,易导致判断及响应延迟,使攻击者有机可乘。

自动分类并过滤方法利用机器学习[7]、统计分析[8] 等技术,结合历史知识、环境知识或专家经验,可以实现对来自底层的警报进行自动分类并过滤。但是统计分析方法的有效性依赖于所建立的数学模型,往往不易于分析与理解,不能及时适应网络环境和用户习惯的改变,无法识别某些非大规模的网络攻击;而机器学习的效果取决于所采用的训练数据及规则挖掘方法,在网络环境变化时往往需要重新学习。

警报关联方法[9,10] 利用警报之间往往并非独立的特性,采用种种手段发现警报之间的关联关系,以发现完整的入侵事

收稿日期: 2009-01-15; **修回日期**: 2009-03-26 **基金项目**: 国家"863"高技术研究发展计划资助项目(2003AA142010)
作者简介:段祥雯(1973-),女,湖南郴州人,工程师,硕士,主要研究方向为信息安全、计算机应用(annywen_001@163.com).

件,重构完整的攻击场景。这种方法能提高警报的准确性,提升警报的抽象级别。但是当 IDS 产生大量虚警时,某些警报关联方法同样会出现分析效率下降,被误导,甚至分析错误。

2　自适应的 IDS 虚警处理框架

2.1　设计目标

在深入分析虚警成因和现有技术的基础上[11],本文提出了一个自适应的虚警处理框架,以达到如下目标:a)能够处理来自多种不同类型 IDS 产生的警报信息;b)自动适应环境的变化和攻击技术发展带来的变化;c)准确、自动地完成警报信息中的虚假警报过滤;d)自动分析过滤效果,并根据效果自动进行调整;e)自动分析并生成综合的、抽象级别较高的警报;f)过滤过程易于专家分析和检查。

2.2　设计思路

Julisch 指出,IDS 产生的大量警报中,90% 的警报是由少数几个根原因引起的。在引起误报的根本原因未排除的情况下,相似的警报通常会持续不断地产生,而且累计数量巨大。因此,通过分析数目众多的相似警报可以找出导致虚警产生的根原因。文献[1]提出基于启发式的数据挖掘算法,通过面向属性的概念聚类,对警报库中的警报信息进行挖掘,再利用得到的根原因分析结果设置相应的 IDS 过滤规则,将虚警数量减少了 87%。这种方法虽大大减少了虚警数量,但准确度不高,容易导致漏报。经过虚警成因分析,笔者认为:由网络故障、配置错误等原因引起的网络流量,是可以通过根原因分析来减少的,即通过排除故障,修改错误来减少触发虚警的外部因素,从而减少虚警。因此,笔者将采用根原因分析方法,判断网络故障并将其作为调整网络设备配置的依据。

机器学习技术较早地应用于知识发现,可以用于学习和掌握虚假警报和真实警报的分类规律,实现警报的自动分类和过滤,但性能往往受制于所选择的学习方法和训练数据。在以往提出的机器学习方法中,训练数据往往是通过专家分析,对警报数据手工分类形成,不仅工作量大而且容易引入错误数据。警报验证中的积极验证方法通过与目标机建立连接并对其进行扫描,得到的数据通常具有高准确性,但是存在消耗网络资源,形成等待延迟等缺点,应用在实时处理中可能会影响处理效率。因此,本文将警报验证中的积极验证方法,用于训练数据的形成阶段与分类结果的验证阶段,以准确标记虚警与真实警报,自动形成高质量的训练数据,此外,在验证阶段通过检查自动分类的效果而形成反馈。

警报关联技术,可以从低层次的警报中产生高抽象级别及更加有效的警报,对于处理来自多个 IDS 的警报非常重要。在处理过程中,也起到去除来自底层的虚假警报的作用。但是,当来自底层的虚警量巨大时,警报关联过程将耗费大量资源和处理时间,甚至产生误导。因此,在进行关联分析前提高警报质量非常必要。本文尝试将其与自动分类技术结合,对于自动分类过程中可能出现的错误(漏报和虚警),在警报关联过程中采用漏报假设和推理技术进行分析,分析结果将作为虚警自动处理部分的反馈,以增加分类器的自适应能力。

2.3　处理框架的设计

处理框架整体结构(图 1)由下至上可分为三个部分:

a)探测器部分。主要由各种类型的 IDS 探测器构成,包括 NIDS(网络型入侵检测系统)、HIDS(主机型入侵检测系统),其他类型 IDS(如混合型入侵检测系统)的探测器,负责监控网络,主机或其他数据源,发现可疑事件即触发警报。

b)虚警自动处理部分。主要由警报缓存器、自适应过滤器及警报传输模块构成。警报缓存器负责将探测器触发的警报以队列方式暂存在内存中以待处理;自适应过滤器负责实现虚警的自动划分,标记虚假警报及可疑警报;警报传输模块负责将被标记为可疑的警报按约定的格式进行编码,并传送至警报关联部件。

c)警报关联部件。包括警报收集模块、警报格式统一化模块、警报规约模块和警报关联模块。负责对收集到的警报数据进行解码、格式统一化、规约和关联处理,生成更高级别的抽象警报信息,提供给其他高层处理系统(如决策、响应系统或 SIM 管理平台);另一方面,分析并统计漏报及虚警的数量,作为反馈信息提供给自适应过滤器。

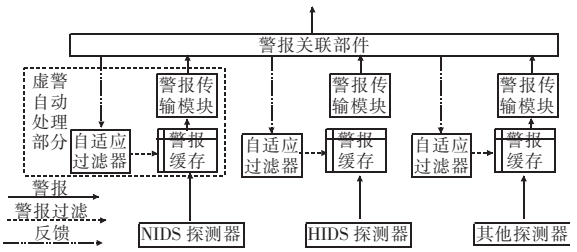

图 1　自适应虚警处理框架体系结构图

3　自适应虚警处理框架功能实现

3.1　自适应过滤器的实现

自适应过滤器由自动分类器、警报过滤模块、警报验证模块、机器学习模块和警报库组成。警报库存储经过标记的警报;机器学习模块将警报库中已分类(标记)的警报作为训练数据,进行学习并建立分类模型;自动分类器根据建立的分类模型实现虚警的自动划分,标记虚假警报及可疑警报;警报验证模块根据警报验证结果对缓存中的警报进行标记,在学习阶段负责形成训练数据,在验证阶段负责验证警报的真实性;警报过滤模块过滤标记为虚警的警报,上传可疑警报。其结构和构建过程如图 2 所示。

自适应过滤器共有五个工作状态,即开始、结束、学习、工作和检验。其转换过程如图 3 所示,详细描述如下:

a)初始时,系统启动,进入学习状态。学习状态下,分类模型处于训练之中,自动分类器未工作。

b)分类模型训练完毕,进入工作状态,自动分类器开始进行警报的自动分类工作。

c)当到达规定的时间(上次学习结束时间 + 规定时间间隔),或来自警报关联部件统计的反馈信息超出设定的阈值时,进入检验状态。警报验证模块启动,在自动分类器工作的同时进行警报验证。

d)当自动分类器与警报验证模块的分类结果相差大,以致低于设定的检验阈值时,自适应过滤器重新进入学习状态;

否则,视为达到检验标准,自适应过滤器返回工作状态。

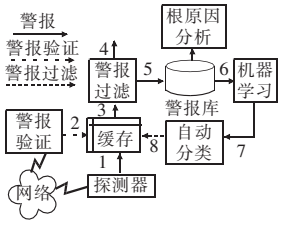

图 2　自适应过滤器的结构及分类器构建流程图

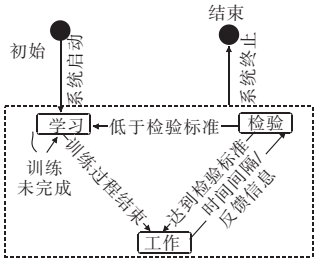

图 3　自适应过滤器工作状态图

学习、工作、检验状态下自适应过滤器各部分工作情况并不相同。学习状态下,分类模型处于构建之中,自动分类器未工作,警报验证模块、机器学习模块启动。详细描述如下:

(a)探测器触发的警报信息送警报缓存器,根据警报到达时间及严重等级将警报放至警报队列。

(b)警报验证模块从队列中取待验证警报进行验证;验证完毕,对警报进行标记。

(c)已标记的警报送警报过滤模块。

(d)警报过滤模块将未标记为虚警的警报送至上层模块。

(e)将已标记的警报(虚警及真实警报)送警报库,以形成训练数据(包含附加信息)。

(f)训练数据送机器学习模块,训练分类模型。

(g)分类模型训练完毕后,形成自动分类器。

(h)自动分类器开始分类工作。

工作状态下,自动分类器工作,而警报验证模块、机器学习模块则暂时停止。警报处理过程如下:

(a)探测器触发的警报信息送警报缓存器。

(b)动分类器对缓存器中的警报进行自动分类并标记。

(c)已标记的警报送警报过滤模块。

(d)警报过滤模块将未标记为虚警的警报送至上层模块。

(e)对已标记的警报送至警报库,形成历史信息。

检验状态下,自动分类器工作的同时,警报验证模块启动。检验过程如下:

(a)探测器将触发的警报信息送警报缓存器。

(b)自动分类器对缓存器中的警报进行自动分类并标记。

(c)警报验证模块启动,验证并标记缓存器中的警报。

(d)自动分类器、警报验证模块都已标记的警报送至警报过滤模块。

(e)警报过滤模块将未标记为虚警的警报送至上层模块。

(f)对已标记的警报送至警报库,比较警报验证模块与自动分类器的警报标记,根据比较结果,生成统计信息。

(g)将统计信息与设定的检验阈值比较,若低于检验阈值,转学习状态;否则返回工作状态。

自适应过滤器部分重点使用了两种技术,即警报验证与机器学习。警报验证模块启动时,通过代理进程对各个目标主机进行实时调查,判断可能得逞的攻击;根据返回的验证结果对警报进行标记。为了提高警报验证的效率,减少警报验证时间,减轻对网络造成的压力,在验证子模块中采用了警报压缩技术:设置缓存窗口,根据缓存窗口对警报进行规约,如合并短时间间隔内的重复警报,合并短时间间隔内扫描类及拒绝服务攻击类警报,再对合并后生成的压缩警报进行验证。

3.2　根原因分析模块的实现

当达到约束条件时(规定的时间间隔),根原因分析模块将启动,对警报库中存放的警报信息进行分析,得到触发警报的根原因并输出分析结果。其实现过程如下:

a)根据警报属性及属性取值范围设置概化值,如源主机和目标主机端口值可概化为特权(1 ~1 025)、非特权(1 025 以上),源主机和目标主机 IP 地址值可概化为 Internet、DMZ、Firewall、WWW\FTP、ANY-IP,报警时间值可概化为工作日、周末、上半月、下半月等,如图 4 所示。

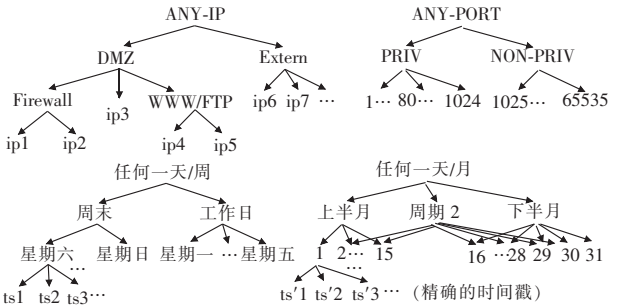

图 4　地址、端口与时间属性值概化样例

b)将相似警报聚类。采用启发式算法,对警报库中的每一条警报实现属性值概化,将概化属性值相同的警报合并,并统计数量。

c)将聚类时统计的警报数量与预定值比较,对于警报数量大于预定值的聚类,将其概化警报作为其根原因输出。

聚类算法描述如下:

a)将警报库中的警报记录存储在表 T 中,为每一条警报增加一个 count 属性(用于计数),其初始化值为 1。

b)当表 T 中存在警报 a,$a[\text{count}] < \min\_size$(count 属性值小于预定聚类阈值)时,根据启发式(针对每个属性计算属性值最大重复次数,再从中选取重复次数最少的属性)选取警报属性 A_i。

c)将表 T 中所有警报的属性 A_i 值进行概化,当存在两个警报 a,a'所有属性值完全相同,则增加计数值:令 $a[\text{count}] = a[\text{count}] + a'[\text{count}]$,并且从表 T 中删除警报 a'。

d)重复步骤 b)c)。

e)输出所有计数值大于预定聚类阈值($a[\text{count}] \geqslant \min\_size$)的概化警报。

根原因分析模块输出的结果,可供网络管理员分析和参考,作为判断网络故障、调整网络设备配置的依据,减少由故障和错误引发的网络流量或虚警。

3.3　警报关联部件的实现

一次完整的攻击通常是分阶段完成的,而且每个阶段往往都拥有多个相关步骤。攻击触发的警报信息之间也往往不是独立的,而是存在多种复杂的关系,如重复关系、并发关系、因果关系、时序关系。通过对警报信息进行多角度的分析与处理(分簇、融合、关联等),即可发现警报之间的复杂关系,从而发现完整的入侵事件,重构完整的攻击场景。对于某些孤立的、未关联的警报,则可视为虚警,不予上报。

警报关联部件的结构与工作流程如图 5 所示。

图 5　警报关联部分的结构及工作流程

1)警报信息收集模块　收集来自各警报传输模块的警报信息,解码后送警报格式统一化模块处理。

2)警报格式统一化模块　按照统一的 CVE 命名方式、分类方式、警报格式对各类 IDS 警报进行转换,对空属性值进行填充,使其适于后续模块处理;处理后的信息送事件规约模块。

3)事件规约模块　对警报信息进行分析,合并短时间间隔内的重复警报,如来自同一探测器的重复警报和不同探测器对同一事件的警报;合并短时间间隔内来自同源或针对同目标同类攻击产生的警报;规约后的事件流送事件关联模块。

4)事件关联模块　负责关联和重构攻击线程、攻击会话、多步骤攻击等,以及其他协同、时序、并发攻击。生成的抽象报警信息及推测信息送高层模块处理,同时,分析、统计漏报及虚警,作为反馈传送给虚警自动处理部分。

4　实验分析

实验采用计算机硬件环境如下:Intel Pentium 4 CPU 3.00 GHz 处理器,IntelD915G 主板。软件环境如下:WindowsXP Professional Service Pack2, SQL2000, Clementine 8.0, Snort2.4.3, WinPcap3.1。采用的实验数据集为 DARPA1999 与 DARPA2000 DataSets,这是 MIT Lincon 实验室 IST 小组,为评估 IDS 的检测率及虚警率,在 DARPA 建立的网络测试平台上模拟数百个用户和上千台主机产生的正常网络流量和多种攻击流量,并采集生成的可重放数据集。其中,DARPA2000 则是新一代 IDS 实时评价工具,用于实现可重构的实时 IDS 测试,评价 IDS 检测复杂、多步骤攻击的能力。

机器学习方法在本文中用于分类模型的构建,而分类模型的好坏直接关系到虚警处理框架的工作效果,因此对其进行了重点研究。根据设计需求,本实验选用了三种机器学习方法,分别是 Neural Networks(神经网络)、C5.0、Classification 和 Regression(C&R)Trees。由于分类模型的构建过程与采用的学习算法及训练数据密切相关,笔者先后使用了两组训练数据进行实验。实验将 DARPA1999 数据集的 1、2 周数据用于训练,4、5 周数据用于测试;DARPA2000 则用于测试环境约略发生变化后的分类性能;其中 DARPA1999 第 4、5 周数据、DARPA2000 数据都包含训练数据中未出现的攻击类型。实验分为两组:第一组实验的训练数据集采用 snort 警报信息原有属性,例如,攻击源 ip_src、攻击目标 ip_dst、源主机端口 layer4_sport、目标主机端口 layer4_dport、协议类型 ip_proto、严重等级 sig_priority、攻击名称 sig_name、攻击类别 sig_class_name 等。第二组实验的训练数据集在采用 snort 警报信息原有属性的基础上附加了其他信息,如源主机系统信息 srcsys、srcnote,目标主机系统信息 dstsys、dstnote;针对各类攻击统计得到的探测器报警置信度 P0,支持度 Surp 信息;根据时间窗口(如 2 s)统计所得的警报信息,如同源攻击数 samesrc2、同目标攻击数 samedst2、同源且同目标攻击数 samesrcdst2、同名攻击数 samesig2、同名且同类别攻击数 samesigcls2。两组数据中都添加了攻击分类标记 is_attack,is_attack=0 表示警报为虚警,is_attack=1 则表示警报真实。实验中选用 is_attack 属性作为训练目标(输出),而其他属性作为训练输入。实验结果如表 1~3 所示。

表 1　两组实验中三种模型分类正确率　%

模型	DPRAP1999week1,2		DPRAP1999week3,4		DPRAP2000	
	1	2	1	2	1	2
C5	97.25	99.83	87.97	98.24	52.24	94.55
Neural Net	99.92	99.95	98.42	98.71	55.96	95.9
C&RTree	94.08	93.35	94.39	93.42	53.87	59.46

表 2　两组实验中三种模型对实验数据的分类结果

模型		DPRAP1999 week1,2				DPRAP1999 week3,4				DPRAP2000			
		1		2		1		2		1		2	
		0	1	0	1	0	1	0	1	0	1	0	1
C5	0	161939	5151	1166857	233	20043	2 748	22424	367	1066	124	1182	8
	1	69	22639	90	22618	14	30	35	9	901	55	109	847
Neural Net	0	167022	68	167059	31	22 460	331	22 525	266	1187	3	1179	11
	1	83	22625	64	22644	29	15	28	16	942	14	77	879
C& RTree	0	164566	2524	164579	2511	21547	1244	21321	1470	1136	54	1140	50
	1	8706	14002	10105	12603	38	6	32	12	936	20	820	136

表 3　两组实验中得到的三种模型训练时间及检验时间

模型	训练时间 (hh:mm:ss)		DPRAP1999 week1,2(CPU)		DPRAP1999 week3,4(CPU)		DPRAP2000 (CPU)	
	1	2	1	2	1	2	1	2
C5	0:00:35	0:10:42	11.02	12.18	1.34	1.42	0.15	0.14
Neural Net	1:04:50	0:06:41	11.81	7.13	1.37	0.81	0.14	0.08
C&RTree	0:00:24	0:04:58	6.01	6.97	0.75	0.75	0.11	0.10

由上面的实验数据可见第二组训练模型分类效率几乎均高于第一组,尤其在用 DPRAP2000 数据检验时效果相差明显;神经网络方法与 C5 算法建立的学习模型分类准确率高,其中神经网络方法建立模型的分类效果最好且较为稳定;三种模型的建立时间长短不一,与训练模型的配置有关,但神经网络模型训练的最长时间远超出其他两类模型的训练时间。模型检验时间都在秒级,其中 C&RTree 模型与神经网络模型检验时间略短。根据实验结果分析和设计需求,选择 C5.0 模型建立 IDS 虚警自适应处理框架的自适应过滤器。

5　结束语

本文针对严重影响 IDS 实用性的虚假警报问题,从提高报警信息质量的角度,提出了一个具有自适应能力的虚警处理框架。该框架具有下列特点:a)将警报验证技术与机器学习方法相结合,构建分类模型,使得分类器能够自动、准确地区分和过滤虚假警报;b)在警报关联部分采用虚警及漏报分析功能,将分析结果用做分类器的反馈信息,与警报验证技术结合,使系统具备自适应特性,自动判断并启动学习过程,以适应环境变化及攻击方法的发展;c)将过滤过程应用于警报关联过程之前,使得警报关联部分可以集中关注可疑警报,关联效率得到明显提高。

参考文献:

[1] JULISCH K. Clustering intrusion detection alarms to support root cause analysis[J]. ACM Trans on Information and System Security, 2003, 6(4): 443-471.

[2] RANUM M J. False positives: a user's guide to making sense of IDS alarms[EB/OL]. (2003-07-05). http://www.icsalabs.com/html/communities/ids/whitepaper/FalsePositives.pdf.

[3] 唐正军,李建华. 入侵检测技术[M]. 北京:清华大学出版社, 2004.

(下转第 2147 页)

$M/(n\times b)$,至此,可以计算:

$$t_{p2p}=M/(n\times b'')+(\lceil\log_2(N+1)\rceil-1)\times M/(n\times b)+(n-1)\times M/(n\times b) \quad (4)$$

在 P2P-PKI 模型中,所有节点的带宽资源都是能够利用的,在节点内部进行 P2P 共享分块时,也可以利用 CA 中心的带宽,继续下载分块,因此 t_{p2p} 的计算是保守的。

根据式(4)简化可得

$$t_{p2p}=M/(n\times b)(b/b''+\lceil\log_2(N+1)\rceil+n-2) \quad (5)$$

依据式(3)和(5)得到

$$t_{CS}/t_{p2p}=N\times n\times b/(b'\times(b/b''+\lceil\log_2(N+1)\rceil+n-2)) \quad (6)$$

若 CA 节点为一普通节点,有 $b'=b$,$b''=b/n$,则

$$t_{CS}/t_{p2p}=N\times n/(2n+\lceil\log_2(N+1)\rceil-2) \quad (7)$$

对于一个基于 P2P 的地形漫游共享系统,节点个数较多,证书数据较大[14],分成的数据块数 n 也较多,则有 $t_{CS}/t_{p2p}\approx N/2$,即提高的效率依据每个节点个数 N 成倍增长。

3　仿真测试与结果分析

利用 OPNET 建立仿真环境,设 N 分别为 100、150、200、250、300 和 350。M 设置为 56 KB,n 取 20,f 取 0.01 次/s,证书管理中心和下载终端均为普通节点,$b_{ca}=b$,设为 10 MBps。仿真运行 10 次,取平均值。图 2 为传统 C/S 和基于 P2P 模式下,安全认证中心的负载与 CA 带宽消耗变化的对比结果,图 3 为两种模式下,所有证书下载或更新完毕所需时间的对比。

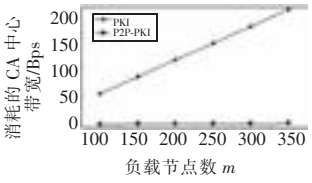

图 2　负载和 CA 带宽消耗对比测试结果

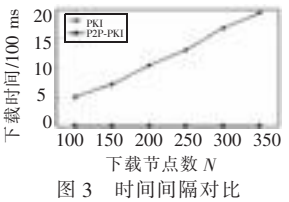

图 3　时间间隔对比测试结果

仿真节点规模和数据分组 n 不是特别大,式(7)中忽略 $\lceil\log_2(N+1)\rceil-2$ 导致存在一定的误差,这时的 $t_{CS}/t_{p2p}\approx N/2\times0.86$,当节点规模扩大时,$M$ 和 n 也扩大,忽略 $\lceil\log_2(N+1)\rceil-2$ 导致的误差也越小;仿真结果和理论计算可以看出,新方法效率提高明显。

结果表明,在 P2P-PKI 安全认证模式下,CA 的负载更小,证书下载或更新完毕所需时间更短,综合性能更优,更加适合基于P2P的海量地形漫游服务;实际系统中,由于节点的动态性和节点查找、分块拼合以及完整性和合法性验证开销,与理论值和仿真结果可能存在一定的偏差,但这种偏差和新系统性能相比是很小的。

4　结束语

利用 P2P 进行海量地形数据传输成为了地形漫游新的研究热点,由此带来的新安全性问题研究文献还相对较少。本文提出的基于 P2P-PKI 的安全传输模型,能较好地解决通过 P2P 进行海量地形下载漫游的安全性问题。

参考文献:

[1] 何建邦,闾国年,吴平生,等. 地理信息共享的原理与方法[M]. 北京:科学出版社,2003.

[2] 喻占武, 郑胜, 李忠民. 一种混合式 P2P 下的大规模地形数据传输机制[J]. 测绘学报,2008,37(1):243-250.

[3] 喻占武,李忠民,郑胜. 基于对象存储的新型网络 GIS 体系结构研究[J]. 武汉大学学报:信息科学版,2008,33(3):285-288.

[4] 王来刚,王震. GIS 中基于 RBAC 的空间信息安全研究[J]. 地理空间信息,2006,4(4):22-24.

[5] 贾培宏,马劲松. 基于数字水印的地理空间数据共享安全技术研究[J]. 测绘通报,2007(2):70-72.

[6] 田斌, 孙敬业, 扬军. 一种基于 Web 的数字地理信息系统安全解决方案[J]. 四川测绘,2007,30(2):141-144.

[7] 袁帅,宋晓宇,王永会,等. GIS 海量影像数据管理系统的设计与实现[J]. 沈阳建筑工程学院学报:自然科学版, 2003,19(3):236-239.

[8] ADAMS C, LLOYD S. 公开密钥基础设施——概念、标准和实施[M]. 北京:人民邮电出版社,2001:5-12.

[9] HOUSLY R, FORD W, POLK W, *et al*. RFC2459, Internet X.509 public key infrastructure certificate and CRL profile[S]. 1999.

[10] LEWIS J. Public key infrastructure architecture[R]. [S. l.]: The Burton Group,1997.

[11] BERKOVITS S, CHOKHANI S, FURLONG J. Public key infrastructure study:Final report[R]. MITRE Corporation for NIST, 1994.

[12] 雷　,阳福明,胡惯荣. 一种新的 PKI 证书撤销机制[J]. 华中科技大学学报:自然科学版,2002,30(11):13-15.

[13] 谭良,刘震,余　,等. CRL 分段—过量发布综合模型研究[J]. 电子学报,2005,33(2):227-230.

[14] ARNES A. Public key certificate revocation schemes[D]. Norway: Norwegian University of Science and Technology,2000.

(上接第 2144 页)

[4] RAMESH S, ELANGO K. Reducing false positives using vulnerability assessment[EB/OL]. (2004). http://www.securitydocs.com/library/2563.

[5] Cisco. IDS 降低误报率的最新方法——思科威胁响应技术[J]. 计算机安全,2003,6(9):30-31.

[6] VALEUR F, VIGNA G. A comprehensive approach to intrusion detection alert correlation[J]. IEEE Trans on Dependable and Secure Computing,2004,1(3):146-169.

[7] PIETRASZEK T. Using adaptive alert classification to reduce false positives in intrusion detection[C]//Proc of Recent Advances in Intrusion Detection(LNCS 3224). Berlin: Springer-Verlag,2004:102-124.

[8] WANG J, LEE I. Measuring false-positive by automated real-time correlated hacking behavior analysis[C]//Proc of the 4th International Conference on Information Security Table of Contents (LNCS 2200). London: Springer-Verlag,2001:512-535.

[9] PENG N, XU D. Hypothesizing and reasoning about attacks missed by intrusion detection systems [J]. ACM Trans on Information and System Security,2004,7(4):1-37.

[10] QIN Xin-zhou, LEE W. Statistical causality analysis of INFOSEC alert data[C]//Proc of the 6th International Symposium on Recent Advances in Intrusion Detection (LNCS 2820). Berlin: Springer-Verlag, 2003:73-93.

[11] 段祥雯,张怡. IDS 虚警处理技术研究[J]. 计算机研究与发展,2006,43(2):447-451.