一种改进的移动自组网络入侵检测系统研究

高永梅[1,2],吴吉义[1,3],平玲娣[1]
(1.浙江大学 计算机科学与技术学院,浙江 杭州 310027;
2.杭州职业技术学院,浙江 杭州 310018;
3.杭州师范大学 电子商务与信息安全重点实验室,浙江 杭州 310036)

摘 要:移动自组网络(MANETS)的安全问题是其走向实用化的重要前提,如何确保自组网络路由协议的安全成为Ad hoc网络研究的一项关键技术。在对Sergio Marti等人提出的Watchdog和Pathrater算法进行详细分析的基础上,针对Watchdog算法存在的问题,提出了功能扩展的SuperWatchdog入侵检测系统。该系统特点是能够发现那些通过提供虚假报告以便分割网络的恶意节点,以保护网络。仿真结果表明,改进系统大大降低了开销,但不会明显地增加吞吐量。

关键词:移动自组网络;入侵检测系统;SuperWatchdog
中图分类号:TP393.03 **文献标识码**:A **文章编号**:1673-629X(2009)08-0140-04

Research on Improved Intrusion Detection System in Mobile Ad hoc Network

GAO Yong-mei[1,2], WU Ji-yi[1,3], PING Ling-di[1]
(1. School of Computer Science and Technology, Zhejiang University, Hangzhou 310027, China;
2. Hangzhou Vocational and Technical College, Hangzhou 310018, China;
3. Key Laboratory of E-commerce and Info. Security, Hangzhou Normal University, Hangzhou 310036, China)

Abstract: Owing to many new characteristics such as central-less control and multi-hop communication, the security situation is more rigorous than that in the traditional Ad hoc network. Especially, when the number of nodes increase, the difficulty of building network, network availability and network security will be influenced badly. After the particular analysis of Sergio Marti's Watchdog and Pathrater arithmetic, intrusion detection system called SuperWatchdog, as the improved solution, was introduced to overcome the weakness of Watchdog. The main feature of the proposed system is its ability to discover malicious nodes which can partition the network by falsely reporting other nodes as misbehaving and then proceeds to protect the network. Simulation results show that our system decrease the overhead greatly, though it does not increase the throughput obviously.

Key words: mobile Ad hoc network; intrusion detection system; SuperWatchdog

0 引 言

移动Ad hoc网络[1]的安全主要以路由安全为核心,到目前为止已经有AODV[2]、DSR[3]、OLSR等成熟的路由协议,但是这些路由协议并没有考虑到Ad hoc网络路由安全问题。路由发现和维护过程中如果不对每个控制消息进行安全认证,将会给网络带来灾难性的后果,对路由信息的恶意篡改、删除、伪造等攻击使得路由协议不能正常工作;针对有限资源的攻击会造成网络带宽、电池资源的浪费;错误的路由更新导致活动路由的断裂。移动Ad hoc网络的安全路由协议必须对上述攻击具有很好的鲁棒性。

恶意节点能够中断网络通信达到破坏网络的目的。为了对网络中的非法节点进行区分并且隔离,斯坦福大学Sergio Marti等人提出了Watchdog[4]和Pathrater算法,这种方法的优点是实现和部署简单,但是由于没有考虑到一些制约,比如有的节点由于资源限制可能不能运行IDS系统,而且由于每个节点只有本地的一些数据,因此对影响整个网络的入侵检测会比较迟钝甚至不能检测出来。笔者首先对Sergio Marti等人的Watchdog和Pathrater算法进行了分析,然后针对算法存在的问题,对Watchdog进行了功能扩展,

收稿日期:2008-12-31;**修回日期**:2009-03-22
基金项目:浙江省教育科研计划项目(20071371);浙江省自然科学基金资助项目(Y1080831)
作者简介:高永梅(1975-),女,硕士,讲师,研究方向为计算机网络、入侵检测系统;吴吉义,博士,高工,CCF高级会员,研究方向为对等计算、网络安全;平玲娣,教授,博士生导师,研究方向为NGN、网络安全。

其功能也是检测来自恶意节点的攻击并将检测信息报告给响应系统,即 Pathrater 或 Routeguard。

1　背景及相关工作

在这一部分将介绍 Sergio Marti 等人提出的检测和减少路由错误的工具 Watchdog 和 Pathrater,同时描述这些工具的限制。尽管这些工具是在(Dynamic Source Routing,DSR)上实现的,其中的一些概念可以泛化到其它的源路由协议中。

Watchdog 方法检测有异常行为的节点,图 1 阐明了 Watchdog 如何工作的原理。当 B 经过 C,从 S 向 D 传输一个数据报时,A 可以监听 B 的传输过程并验证 B 是否已经成功将数据报传给 C。实线代表数据报从 B 传输到 C 的目标方向,而虚线表示 A 处于 B 的可传输范围并能够监听传输过程。假设经过中间节点 A、B、C,存在一条从节点 S 到节点 D 的路径。节点 A 不能联接到节点 C,但是它可以监听到节点 B 的流量。因此,当节点 A 要通过 B 传递一个数据报给 C,一般情况下 A 能知道 B 是否传输了该数据报。如果考虑到代价因素,没有在每条链路上进行单独加密,A 也能知道 B 是否篡改了有效载荷或者报头。

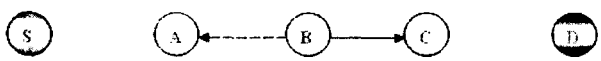

图 1　Watchdog 的工作原理

通过维护一个最近发送数据报的缓冲器来实现 Watchdog,将监听到的数据报和缓冲器中的数据报比较,看它们是否匹配。如果匹配,Watchdog 将数据报从缓冲器中移除,因为它已经被传输了。如果某数据报在缓冲器中超过了某一时限,Watchdog 自动递增负责传递该数据报的节点的失败统计数。当该统计数达到某一极限值,可以判定该节点为异常节点,并发送信息通知源节点。

Watchdog 技术有优点也有缺点。基于 Watchdog 的 DSR 的优点是能同时在链路级和 Forwarding 级检测异常行为,而 Watchdog 技术的缺点是不能完全检测模糊冲突、接收者冲突、有限传输能力、虚假异常、勾结和部分丢失等情况的异常节点。

模糊冲突问题可以防止 A 监听 B 的传输。如图 2 所示,当 A 监听 B 传递数据报时,A 会出现报冲突。这种情况下,A 并不能确定冲突是由 B 传递数据报引起的,因为 B 可能传递了也可能从未传递过数据报,而是由于 A 的其它邻居节点造成的。由于这种不确定性,A 不能马上确定 B 的异常行为,而需要继续监听 B 一段时间。如果 A 重复检测 B 传递数据报过程失败,那么就可以确定 B 的异常行为。

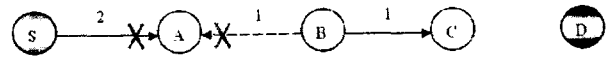

图 2　节点 A 无法监听

在"接收者冲突"问题中,节点 A 仅仅知道 B 是否传递数据报给 C,但是它不知道 C 是否收到数据报,如图 3 所示。如果 B 第一次传递数据报给处于冲突状态的节点 C,A 仅仅知道 B 传递了数据报,并假设 C 成功接收了该数据报。因此,B 不需要重传数据报,蒙蔽 A。通过一直等待 C 处于传递状态时向其传递数据报,B 同样可以故意的造成已传输的数据报在 C 处发生冲突。第一种情况,节点可能是自私的,不想重传来消耗资源。另一种情况,B 行为的唯一的原因就是处于恶意。B 浪费电量和 CPU 时间,因此这不是自私。一个过载的节点也不会有这样的行为,因为它严重浪费可贵的 CPU 时间和带宽。因此,第二种情况应该很少出现。

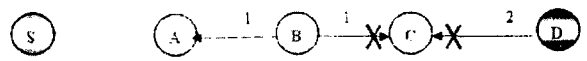

图 3　C 没有接收到数据报

当节点错误地报告其它节点异常时会出现另一个问题,一个恶意的节点可能会通过报告它后面通路上的节点异常分隔网络。例如,节点 A 报告节点 B 没有传递数据报,而实际上 B 传递了。这将导致 S 节点把 B 节点标记为异常节点,A 是罪魁祸首。然而这种行为可以被检测到。因为 A 正在传递消息给 B,作为 S 的验证,然后一些从 D 节点到 S 节点的确认信息将通过 A 节点到达 S 节点,那么 S 将会疑惑:为什么会收到 D 节点的数据保,本来应该在传递过程中被 B 节点丢弃的。另外,如果 A 丢弃确认信息,那么节点 B 将检测到这个异常并报告给节点 D。

另外一个问题是,具有控制传输功率能力的异常节点能够绕过 Watchdog。一个节点可以限制它的功率,使它的信号足够强能够被前一个节点监听但又太弱不能被真实接收者收到。这将要求异常节点知道到达每个邻居节点的功率。仅仅恶意节点才会有这种方式的表现,因为自私的节点这样做只是徒劳反而会浪费能量,过载的节点也不会缓解交通挤塞。

多节点的勾结可能发动一场更复杂的攻击。例如,图 1 中的 B 和 C 勾结可能促成一场危害。这种情况下,B 传递数据报给 C,当 C 丢弃报时 B 并不报告给 A。由于这种限制,那么有必要不允许两个连续不信任的节点在路由路径中,在文中,仅仅处理单个节点的情况。更困难的节点勾结问题将在后续研究中考虑。

最后,一个节点可能绕过 Watchdog,通过以低于 Watchdog 设置的最低异常门限值率丢包。尽管

Watchdog 不会检测到这个异常节点，但是可以强制让这个节点传递到达门限带宽。在这种方式，Watchdog 强制执行这个最小带宽。

Watchdog 机制一定程度上可以用来检测重放攻击，但是要求在每个节点维持大量的状态信息，用来监视邻居节点确保它们没有重传它们已经传递的数据报。同样，如果在接收节点处发生了冲突，节点必须正确重传数据报，那样 Watchdog 节点的表现看起来就像一次重放攻击，因此，用 Watchdog 机制来检测重放攻击既非有效也非有用的。

为了使 Watchdog 恰当的工作，必须知道数据报在哪儿应该是两跳。在我们的实现中，Watchdog 有这些信息，因为 DSR 是一个源路由协议。如果 Watchdog 没有这些信息(例如，实现在单跳路由协议之上)，恶意或者破坏的节点可能广播包给不存在的节点，而 Watchdog 无法知晓。由于这种限制，Watchdog 最好工作在源路由协议之上。

2 Watchdog 功能扩展系统

针对 Watchdog 算法存在的一些问题，提出了一种名为 SuperWatchdog 的入侵检测和响应系统。SuperWatchdog 是对 Watchdog 的扩展，其功能也是检测来自恶意节点的攻击并将检测信息报告给响应系统，即 Pathrater 或 Routeguard。

无论是在 Watchdog 还是在 Routeguard 中，每个节点都根据网络中的其他节点提供的信息来更新节点等级(ratings of nodes)。

当一个节点向其他节点提供虚假报告时，不管是出于恶意还是一个意外，都可能会导致非常严重的问题。恶意节点声称路径中与其相邻的节点行为异常，以达到分割的网络的目的。例如，在图 4，节点 S 是通信的源节点，节点 D 是通信的目标节点。节点 A 可能会报告说，节点 B 不转发数据报，但实际上它是可以转发的。这将导致 S 认为 B 行为失常，而真正的罪魁祸首却是 A。

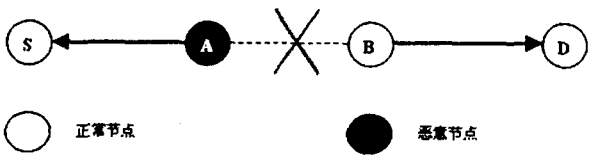

图 4 恶意节点 A 虚假报告 B 的行为异常

Watchdog 的提出者们认为，这种行为可以按如下方式检测："既然 A 把信息传递到 B(通过 S 来核实)，那么从 D 到 S 的任何行为，必将经过 A 到 S，假定在前面的路径中 B 丢失了数据报，当 S 接收到来自 D 的响应时就会非常迷惑了。此外，如果 A 拦截并隐藏发送给 S 的应答信息，那么 B 就会检测的这种异常行为并报告给 D。"

作者们理所当然地认为 Watchdog 能够检测到这类问题。然而，如果恶意节点 A 的目的是分割网络，那么 Watchdog 将会束手无策。进一步思考，当 S 和 A 标记 B 的行为失常，D 和 B 标记 A 行为失常时，就可以发现问题产生了。如果节点 B 检测到 A 的异常行为并报告给 D，那么 D 和 B 就会把 A 视为恶意的。与此同时，S 和 A 把 B 视为恶意的，因为 A 向 S 报告说 B 是恶意的。因此，在某种意义上，其后果是该网络被分为两个部分：S，A 和 B，D。图 4 表明这样一种情况，A 告诉 S，B 的行为异常，那么 S 和 A 标记 B 为恶意的。B 也告诉 D，A 的行为异常，那么 D 和 B 标记 A 是恶意的。因此 A 和 B 间的联系被切断，不能再使用了。

SuperWatchdog 实际上是对 Watchdog 的扩展，目的是检测到提供虚假报告的节点。一般来说，这些节点本身就是恶意的，它们可能会对网络性能造成更严重的损害。本系统仍然使用 Routeguard 作为响应系统。在该系统中，提出以下假设：使用了一些加密机制，密钥长度足够长，仅仅知道公用密钥去计算或猜测私有密钥是不可能的，另一方面，不为移动设备提供昂贵的计算。根据这一假设，恶意节点不能篡改数据报。

通过维护一张表来实现入侵检测功能，这张表存储了＜source，destination，sum，path＞等内容。无论是当前节点、源节点、目标节点还是中间节点，当第一次发送、转送或接收包时，都要向表中插入一条记录。每个字段的值为：

Source：源地址

Destination：目标地址

Sum：当前节点分别作为源节点、中间节点或目标节点，通过路由路径 path 发送、转送、接收包的数量。

Path：＜source，destination＞之间通信的路径。Path 节点地址的列表或者是简化的路径 ID。

当路由路径中的一个中间节点向源节点报告，它的下一个节点是恶意的，源节点不会立即降低恶意节点的等级。相反，它会选择路由表中的另一条路径向目标节点发送信息，信息中包含＜source，destination，sum，malicious_node_address＞，其中 source，destination，sum 如上所述。malicious_node_address 是被报告的恶意节点的地址。然后源节点从路由表中搜查一条不含恶意节点的路径，如果找不到这样的路径，源节点将发出一个"路由发现"以寻找一条新路径，找到路径后，源节点将使用新的路径发送信息。

一旦收到信息，目标节点会搜索自己的表，看看是否有与之比配的记录。如果表中没有匹配的记录，这

就表示该节点是恶意的,目标节点返回消息给源节点,证实该恶意节点的确是恶意的。如果有与之匹配的记录,那么目标节点则把传递信息中的 sum 字段与在表中找的 sum 字段进行比较。如果这两个 sum 相等,这意味着该恶意节点转发了源节点发送的所有的数据报,因此它不是恶意的。相反,如果这两个 sum 不相等,节点提供虚假报告可能是恶意的,那么 Routeguard 将利用这一信息来更新相应节点的等级。

与 Watchdog 相比,这个解决方案具有相同的优势,与此同时,SuperWatchdog 解决了一个很大的弱点:虚假的行为异常报告。如果节点虚假地报告其他节点行为失常,它可以检测到。如前所述,虚假地报告可能会导致网络分割,甚至会降低网络性能。

然而,这个解决方案也有缺陷,如果真正的恶意节点位于从源节点到目标节点的所有路径中,那么源节点向目标节点求证报告的正确性是不可能的。对于这种情况,没有也不能采取任何行动,因为不知道是谁在撒谎,而且也无法检测。Routeguard 也没有降低报告节点和被报告节点的等级。

3　仿真实验与性能评价

本节主要是评估 SuperWatchdog 的性能。SuperWatchdog 系统的仿真模型已经在网络模拟器(NS-2)[5,6]实现。仿真实验是在一个散落着 50 个无线移动节点的 300m×300m 平面空间的网络中进行的。

这些节点采用 10 个固定比特率进行通信,节点与节点之间以每秒 4 包的数据传输速率相连接。所有的节点在 0 米/秒到 3 米/秒的速度随机移动,模拟时间为 100 秒。在所有的实验中,行为失常的节点往往是那些愿意转发包(他们没有改变包的内容)却因为超载、自私、恶意、破坏等导致转发失败。在仿真模拟中,行为异常的节点能破坏网络的性能,尤其是那些把其他正常节点虚假地报告为行为异常的节点。特别关注了这些恶意行为是如何影响网络性能的,在被模拟网络中的 50 个节点中,行为异常的节点的百分比是变化的。变化范围是以 10% 的递增量从 0% 到 40%。首先,以 30% 的节点行为异常(这些节点提供虚假报告)运行该仿真系统,然后以 80% 的行为异常节点提供虚假报告重复实验。

图 5 显示了模拟结果,使用与 Watchdog 相同的指标来评价我们的扩展系统:吞吐量和开销(Throughput and Overhead)。吞吐量是发送的数据报与目标实际接收到的数据报的百分比。系统开销是仿真中相关路由传输(routing - related transmissions)与数据传输的比率。在图 5 和图 6 中,从 0% 至 40% 逐渐改变一般违规节点的百分比,提供虚假报告的行为失常节点的百分比固定在 30%。

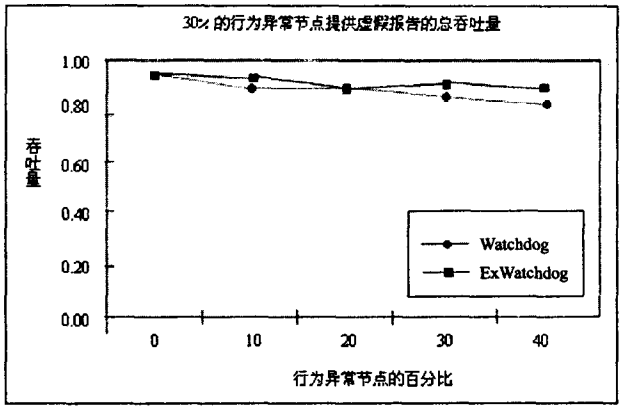

图 5　随异常节点的百分比而变化的整个网络的吞吐量

图 5 显示了整个网络的吞吐量,如果网络中不包含行为异常节点,这两条曲线吞吐量达到 95% 左右。在这种情况下,由于没有行为异常的节点,我们看不到 SuperWatchdog 的好处,这恰恰是 SuperWatchdog 的目标所在。然而,异常行为节点超过 20% 后,结果就发生了变化。在最坏的情况下时,40% 的节点行为异常,Watchdog 的平均吞吐量降低了 18%,而 SuperWatchdog 的平均吞吐量只降低了 7%。与 Watchdog 相比,SuperWatchdog 增加了 11% 的吞吐量,性能改善并不太多。

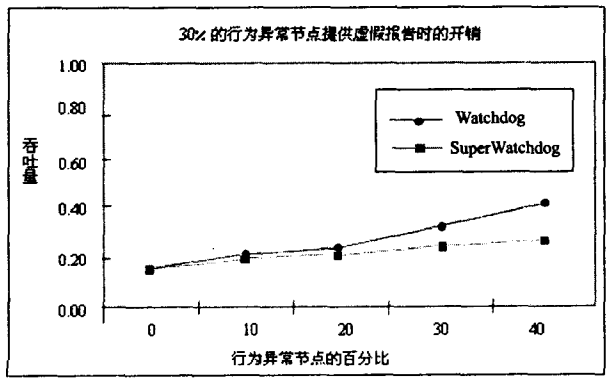

图 6　随异常节点的百分比而变化的网络开销

在 Watchdog 中,当一个恶意节点向源节点提供虚假报告,下一节点是恶意的,即使检测不到虚假报告,源节点也将选择另一个路径发送数据报。某些恶意节点的意图是分割网络,不是破坏数据报,因此,它不会影响目标节点接收数据报的数量。

4　结束语

移动 Ad hoc 网络的安全性问题是一个很复杂的问题,已经出现了很多安全设施[7],诸如安全路由、加密、入侵检测[6-10]等。在文中,提出了入侵检测系统

(下转第 147 页)

用户可以由导航栏快捷地选择自己想要进入的学习阶段。所有这些部件,都是为了方便用户更好地学习密钥加密算法。

2) 实验管理方便。本实验平台首页有注册及登录页面,当用户登录后能显示用户之前的登录信息。这些信息用在教学过程中,指导老师就可以方便地查询各学生登录和使用本平台软件的基本情况,有利于老师了解同学们的实验细节,利于管理。

3) 原理分析直观。在分步执行的过程中,实验平台所包括的各个算法可以实时、直观地进行原理的分析。如:在算法的演示过程中,用户可以直观并清楚地知道"数"的流向及具体算法的执行过程。相比书本上的"枯燥"内容来说,此平台演示就相当于请了个老师,一步一步地演示出算法的基本原理和过程,直观地展现给用户,有效降低了学习的难度。

4　结束语

实现了密钥加密实验平台,给出了实验平台的总体框架,分析了平台实现的主要技术方法。该实验平台最终实现了对各密钥加密算法的基本介绍,能够对算法原理进行较为深入的剖析。通过本实验平台完成了各个算法的实验演示,实际使用过程中取得了较为理想的实验效果。平台通过网页的形式将算法进行分步剖析,使得算法清晰直观,大大减少了学习者的理解难度。下一步工作是进一步丰富和完善算法系统,并考虑和远程控制实验平台、攻击防范实验平台等的进一步融合,以便扩展成为信息安全的综合实验平台。

参考文献:

[1] 胡向东,魏琴芳. 应用密码学[M]. 北京: 电子工业出版社, 2006.

[2] Bao Feng, Lee Cheng - Chi, Hwang Min - Shiang. Cryptanalysis and improvement on batch verifying multiple RSA digital signatures[J]. Applied Mathematics and Computation, 2006,172(2):1195 - 1200.

[3] Ashrafi M Z, Ng S K. Privacy - preserving e - payments using one - time payment details[J]. Computer Standards & Interfaces, 2009,31(2):321 - 328.

[4] 曹建国,王　丹,王　威. 基于RSA公钥密码安全性的研究[J]. 计算机技术与发展, 2007,17(1):172 - 173

[5] 张焕国,王丽娜. 信息安全综合实验教程[M]. 武汉: 武汉大学出版社, 2006.

[6] Castagnos G. An efficient probabilistic public - key cryptosystem over quadratic fields quotients [J]. Finite Fields and Their Applications, 2007,13(3):563 - 576.

[7] Matthew M, Erik J. C#数据安全手册[M].崔　伟, 毛尧飞译.北京: 清华大学出版社, 2003.

[8] 张　宏, 刘晓霞, 张若岩. RSA公钥密码体制中安全大素数的生成[J]. 计算机技术与发展, 2008,18(9):131 - 133.

(上接第 143 页)

SuperWatchdog,该系统是在现有解决方案 Watchdog 的基础上提出的。SuperWatchdog 解决了 Watchdog 的一个致命的问题,即一个恶意节点可以通过虚假报告其他节点行为异常来分割的网络。使用的吞吐量和系统开销作为评价 SuperWatchdog 性能的指标,SuperWatchdog 系统中一些恶意节点虚假报告其他节点行为异常。对于每一个指标,分别对 Watchdog 和 SuperWatchdog 进行了比较检验。仿真结果表明,解决方案虽然没有明显的增加吞吐量,但大大地降低了开销。

参考文献:

[1] IETF Mobile Ad hoc Networks(MANET) Working Group [EB/OL]. 2008 - 08 - 21. www. ietf. org/html. charters/manet - charter. html.

[2] Perkins C, Belding - Royer E. RFC3561:Ad hoc On Demand Distance Vector (AODV) Routing[EB/OL]. 2003. http://www. ietf. org/rfc/rfc3561. txt.

[3] Johnson D B, Maltz D A, Hu Y C, et al. The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks (DSR) [EB/OL]. 2003 - 04. http://www. cs. cmu. edu/dmaltz/internet - drafts/draft - ietf - manet - dsr - 09. txt.

[4] Marti S, Giuli T J, Lai K, et al. Mitigating Routing Misbehavior in Mobile Ad Hoc Networks[C]// in 6th International Conference on Mobile computing and Networking, MOBICOM'00, IEEE CS. U S A:[s. n.],2000:255 - 265.

[5] Zhou L, Haas Z. Securing ad hoc networks[J]. IEEE Network Magazine Special Issue on Network Security, 1999,13(6):1 - 12.

[6] 石　硕,顾学迈,张文彬,等.移动 Ad hoc 网络的 NS2 仿真机制及代码分析[J]. 计算机工程与设计,2008,29(18):4639 - 4643.

[7] 林果园,黄　皓,张永平.入侵检测系统研究进展[J].计算机科学,2008,35(2):69 - 74.

[8] 李　兵.一种基于对等模型的网络入侵检测系统模型[J].计算机技术与发展,2008,18(3):173 - 176.

[9] 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 - 459.

[10] 高永梅,吴吉义,张启飞.基于智能信任关联的对等协同IDS仿真[J].系统仿真学报,2008,21(4):56 - 65.