基于规范的移动 Ad Hoc 网络分布式入侵检测

王 芳[1] 易 平[2] 吴 越[2] 王之旸[2]
(江苏科技大学计算机科学与工程学院 镇江 212003)[1]
(上海交通大学信息安全工程学院 网络信息安全教育部工程研究中心 上海 200030)[2]

摘 要 移动 ad hoc 网络是移动节点自组织形成的网络,由于其动态拓扑、无线传输的特点,容易遭受各种网络攻击。传统的网络安全措施,如防火墙、加密、认证等技术,在移动 ad hoc 网络中难以应用,因此提出一种基于有限状态机分布式合作的入侵检测算法。首先,将整个网络分为子区域,每一区域随机选出簇头担任监视节点,负责本区域的入侵检测。其次,按照 DSR 路由协议构筑节点正常行为和入侵行为的有限状态机,监视节点收集其邻居节点的行为信息,利用有限状态机分析节点的行为,发现入侵者。本算法不需要事先进行数据训练并能够实时检测入侵行为。最后,通过模拟实验证实了算法的有效性。

关键词 移动 ad hoc 网络,路由协议,网络安全,入侵检测,有限状态机
中图法分类号 TP393 **文献标识码** A

Specification-based Distributed Detection for Mobile Ad Hoc Networks

WANG Fang[1] YI Ping[2] WU Yue[2] WANG Zhi-yang[2]
(School of Computer Science and Engineering, Jiangsu University of Science and Technology, Zhenjiang 212003, China)[1]
(Network Information Security Research Center of the Ministry of Education, School of Information Security Engineering, Shanghai Jiaotong University, Shanghai 200030, China)[2]

Abstract Mobile ad hoc networks are highly vulnerable to attacks due to the open medium, dynamically changing network topology, cooperative algorithms, lack of centralized monitoring and management point. The traditional way of protecting networks with firewalls and encryption software is no longer sufficient and effective for those features. We proposed a distributed intrusion detection approach based on finish state machine(FSM). A cluster-based detection scheme was presented, where periodically a node is elected as the monitor node for a cluster. These monitor nodes can not only make local intrusion detection decisions, but also cooperatively take part in global intrusion detection. And then we constructed the finite state machine(FSM) by the way of manually abstracting the correct behaviours of the node according to the routing protocol of Dynamic Source Routing(DSR). The monitor nodes can verify every node's behaviour by the FSM, and validly detect real-time attacks without signatures of intrusion or trained data. Compared with the architecture where each node is its own IDS agent, our approach is much more efficient while maintaining the same level of effectiveness. Finally, we evaluated the intrusion detection method through simulation experiments.

Keywords Mobile ad hoc networks, Routing protocol, Network security, Intrusion detection, Finite state machine

1 引言

移动 ad hoc 网络作为一种新型的移动多跳无线网络,与传统的无线网络有许多不同的特点。它不依赖于任何固定的基础设施和管理中心,而是通过移动节点间的相互协作和自我组织来保持网络的连接,同时实现数据的传递。移动 ad hoc 网络独特的结构产生了一些特点[1]:(1)动态的拓扑:节点可在网络中任意移动,随时加入和退出网络,形成随时变化的网络拓扑结构。(2)有限的资源:节点间无线通信带宽有限,移动节点的能源也有限。(3)多跳的通信:无线节点天线发射功率有限,节点发送报文到接收区域外的节点时,需要其它节点来中转信息,报文需要多跳转发才能到达目标节点。

移动 ad hoc 网络最初用于军事领域,如战场上坦克之间和海洋中舰艇之间的网络组织,但是由于其建网方式灵活、配置快捷方便、构造成本较低等优势,它逐渐运用于商业和民用环境之中,如会议数据交换、紧急援救、偏远地区等一些需要临时组网的应用中。

与固定有线网络相比,移动 ad hoc 网络面临更多的安全威胁。为了保障移动 ad hoc 网络的安全,至今已经提出了许多安全解决方案[2]。但这些安全方案主要集中于密钥的分配与认证[3,4]、路由安全算法两个方面[5,6]。密钥的设置与认证和路由安全算法,这两种可以称为入侵阻止技术,所谓入侵阻

到稿日期:2009-11-30 返修日期:2010-02-01 本文受国家自然科学基金重点项目(60932003),国家高技术研究发展计划项目(863 计划)(2007AA01Z452),上海市自然科学基金资助项目(09ZR1414900),国家大学生创新活动计划项目(091024812)资助。

王 芳(1971-),女,硕士,讲师,主要研究方向为网络安全,E-mail:yiping01@163.com;易 平(1969-),男,副教授,主要研究方向为无线网络、信息安全;吴 越(1968-),男,副教授,主要研究方向为无线网络、信息安全;王之旸(1989-),男,主要研究方向为信息网络。

止就是利用加密、认证、防火墙等技术来防止系统遭受外界的攻击。这些措施用于移动 ad hoc 网络之中，能够发挥一定的安全防范作用。但是，由于移动 ad hoc 网络中节点可任意移动，当网络处于敌对的环境时，节点可能被截获而泄露密钥，敌方节点可持密钥冒充合法节点加入网络进行攻击。此时，因为攻击者拥有合法的密钥，加密和认证技术都已经失效，只有通过入侵检测才能发现并清除入侵者。此外，网络安全的发展史告诉我们，任何入侵阻止方案都不可能完全阻挡外界的攻击，总有这样或那样的漏洞，因此，入侵检测就应该成为入侵阻止方案后的第二道防火墙。

作者前期研究提出移动 ad hoc 网络泛洪攻击方式[7]，本文是前期研究的继续，指出了移动 ad hoc 网络按需路由协议的弱点和针对路由协议的一些攻击方式，提出一种可检测多种攻击的方法——基于有限状态机分布式合作的入侵检测系统。整个入侵检测系统由两部分组成，其一是分布式合作的入侵检测架构。移动 ad hoc 网络具有自组织无管理中心的特点，因此必须采用分布式入侵检测的方法，即入侵检测点分布于整个网络。但为了节省网络资源，又不能使所有节点都为入侵检测执行节点，我们提出一种基于簇头的分布式合作的入侵检测，即在每一个区域内选出一个簇头节点作为入侵响应的监视节点，负责整个区域节点行为的监视，同时各个监视节点又相互合作检测整个网络节点，所有监视节点形成了对整个网络的入侵检测。其二是基于有限状态机的入侵检测算法，我们将按需路由协议的规范形成有限状态机，节点的行为使用有限状态机进行分析，如果不符合有限状态机的行为则认为是攻击行为。该检测算法不需要事先知道入侵行为的特征，也不需要事先进行数据训练，就可直接进行检测。

2 相关工作

现阶段在移动 ad hoc 网络安全方面的研究主要分为 3 个方面：密钥的分配与认证、路由安全算法、入侵检测算法。以下首先概述前两个方面的研究内容，然后主要介绍入侵检测方面的研究进展。

密钥的管理与认证研究在移动 ad hoc 网络无中心自组织的情况下，实现密钥的分配、管理、相互认证。主要采用两种方式，基于门限密钥的管理方案[8]和基于 PGP 的自组织的认证方案[9]。在路由安全算法方面，通过对路由协议中的报文提供完整性校验、身份认证等安全措施，防止恶意篡改的发生。其中较具代表性的算法有 SRP[10]，Ariadne[11]，ARAN[12]，SEAD[13]。SRP[10]假定所有通信双方存在共享密钥，任何路由信息都要通过双方认证，防止非法更改路由信息。Ariadne[11]通过单向 HASH 函数和报文鉴别码实现端到端的路由信息认证。在 ARAN[12]算法中，事先给每个节点分配一份公开密钥证书，每个路由报文都要经过节点签名才能转发，接收节点首先校验报文签名才能处理，通过这些措施来防止攻击者加入网络。SEAD[13]利用单向 HASH 链中的元素来认证路由更新报文中的序列号和跳数，防止恶意节点修改路由协议报文。

在入侵检测算法方面，Yongguang Zhang 和 Weeke Lee 提出了一个基于 agent 的分布式协作入侵检测方案[14]。在该方案中 IDS agent 运行于网络中每一个节点上，执行本地数据收集和入侵检测，一旦发现有异常行为则触发整个网络的入侵检测和响应。该方案的优点是提出了使用异常检测技术的分布式合作的入侵检测和响应的框架，其不足之处是没有描述具体实现算法和进行实验评估。Yongguang Zhang 在后续文献[15]中对上述方案进行了详细的论述，建立了一个 IDS 模型并用网络模拟器进行了模拟实验。Oleg Kachirski 和 Ratan Guha 提出了基于移动 agent 的入侵检测方案[16]。他们认为 Yongguan Zhang 的方案中每个节点都有 agent，过于占用网络资源，为了节省资源，其算法只是在某些节点上驻留有监视网络的 agent，并且 agent 的数量可按要求进行增减。R. S. Puttini 等人设计了一种分布式的入侵检测架构[17]，该架构使用基于特征的入侵检测技术。Yi-an Huang 和 Wenke Lee 提出合作检测的系统[18]，该系统通过一些简单的规则来识别入侵者。B. Sun，K. Wu 和 U. W. Pooch 设计了一种入侵检测 agent[19]，该 agent 利用马尔可夫链来进行入侵行为识别。P. Albers 提出一种利用简单网络管理协议（SNMP）所使用的管理信息库（MIB）作为入侵检测源数据的架构[20]。S. Bhargava 和 D. P. Agrawal 提出一种入侵检测和响应的模型[21]。Weichao Wang 提出一种鉴别 AODV 协议中序列号伪造的方法[22]。Subhadrabandhu，D. 提出一种误用检测架构，它包含两种近似算法，并证明其算法取得了最好的优化效果[23]。

3 背景知识

3.1 DSR 概述

DSR（Dynamic Source Routing）路由协议[24]是较为经典的移动 ad hoc 网络路由协议，它是一种按需路由协议。若源节点 S 需要给目标节点 D 发送数据报文，但它的路由缓存中并没有从源 S 到达目标 D 的路由，此时节点 S 应先将数据存入它的数据缓存区，再以广播方式向周围节点发送路由查询报文（ROUTE REQUEST），每个路由查询报文通过序列号和源节点来惟一标识。周围节点收到路由查询报文后，如果它以前收到并处理过同样的报文，则直接抛弃不处理。如果没有收到过该报文，节点则把自己的地址添加到路由发现报文的地址列表中，并向周围广播转发。若路由查询报文到达目标节点或中间节点具有到目标节点的路由，该节点把路由发现记录的地址信息再加上自己的地址信息结合生成路由回答报文（ROUTE REPLY）单播发送回源节点 S。源节点收到路由回答报文时，存储该路由信息，用于数据报文的发送。

路由维护负责监测网络中正在使用路由的通断情况，并随时通知源节点有关该路由出现的错误情况。当网络中的某一节点按照报文中的路由信息进行报文转发，出现无法将报文继续转发到下一节点的情况，并且经过多次重发无效后，它就产生一个路由出错报文（ROUTE RRER）来通知源节点目前使用的路由已经失效，路由出错报文指出了出错的链路，即产生路由出错报文的节点地址和不能到达的下一跳的节点地址。源节点和其它的节点一旦收到路由出错报文，就会检查自己路由缓存中的路由并且删除出错的路由，同时，源节点会立刻查询自己的路由缓存以寻找一条替代路由使用，若找不到替代路由，则重新激发路由请求报文寻找目的节点。

3.2 DSR 的弱点和攻击方式

DSR 路由协议中没有考虑到安全因素，容易遭受各种安全攻击。在 DSR 路由协议中，一些关键的数据字段，如源节点地址、目标地址、地址列表，是非常重要的，对其任何非法修改都将导致路由的不正常。一个入侵者可采用下列攻击方

式：

入侵者假冒另外一个节点的地址发出路由查询报文。

入侵者转发报文时，对报文中的地址列表进行插入、删除或修改。

入侵者假冒目标节点编造路由回答报文，发回源节点。

全部或部分抛弃路由查询报文、路由回答报文和数据报文。

编造路由出错报文，谎称正常的路由已经中断。

上述攻击将会导致下列后果：

黑洞：节点不转发任何报文。

环路：路由首尾相连形成一个环路，进入环路的报文一直在绕圈子，永远不能达到目标节点。

网络分割：物理上相连的整个网络，逻辑上被分割为互相不相连的几个子网，导致许多节点之间不能通信。

拒绝服务：节点因为资源被大量占用，不能接收和转发报文。

4 入侵检测算法

4.1 监视节点选举算法

在移动 ad hoc 网络中，节点的资源是有限的，将每个节点都作为入侵检测节点，是非常耗费网络节点资源的。为了节省节点资源，我们提出基于簇头的监视模式，即整个网络划分为一个个区域，每个区域选出一个簇头作为监视节点负责整个区域的入侵检测。该簇头收集整个区域内的节点的行为信息，并按路由规范进行分析，确定入侵行为。

选举算法由两部分组成，选举阶段和维持阶段。在选举阶段，随机而竞争性地选出监视节点。起始时，整个网络没有一个监视节点，在一段时间内如果没有任何监视节点的信息，任一节点可以广播一份告示报文宣称自己是监视节点，任何收到此告示报文的节点就成为被监视节点，不能再发告示报文。告示报文只能在一跳范围内传播，不能被转发。因为通信是双向的，某个节点能收到告示报文，那么它所发出的报文也能被监视节点收到，所以监视节点能够监视告示报文传播范围内的节点行为。当区域内选举出一个监视节点后，就进入了维持阶段，监视节点周期性地广播告示报文，以维持其监视节点的地位。监视节点服务时间到了后，就重新启动一个新的选举过程，为了保证公平和随机性，上一届的监视节点将不能参加下一届监视节点的选举，除非整个区域只有它一个节点存在。图 1 示出 3 个监视节点及其监视区域的分布。

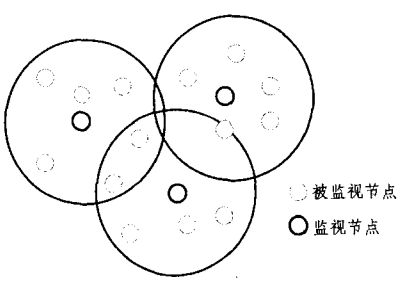

图 1 监视节点及监视区域

监视节点的选举是公平而又随机的。所谓公平性，即每个节点都能够有公平的机会选为监视节点，同时每个节点有相同的服务时间。公平性意味着选举的随机性。每个监视节点相同的服务时间要求周期性地重新选举新的监视节点。随机地选举和周期性地更换监视节点，保证了检测的安全性。如果某个节点是入侵者，又被选举为监视节点，那么在其作为监视节点的期间可以攻击网络而不被发现，因为它是这个区域内的唯一入侵检测点。但它的监视服务时间结束后，又会选出新的监视节点，此时就会发现入侵者。

移动 ad hoc 网络中节点可任意移动，监视节点和被监视节点都可能移动而离开原来的区域，如果一个节点在一段时间内收不到告示报文，它就可以启动一个选举过程，发出告示报文，宣称自己是监视节点。如果两个监视节点靠近且相互收到了告示报文，就比较它们的 ID，ID 较小的节点继续保持为监视节点，另外一个节点就转变为被监视节点。

4.2 有限状态机

监视节点使用有限状态机来分析监视区域内被监视节点的行为是否符合路由规范。它对所监视的每个节点建立有限状态机进行分析。在 DSR 路由协议中，节点可能收到并处理 4 种类型的报文：路由查询报文、路由回答报文、路由出错报文和数据报文。我们首先对路由查询报文按 DSR 路由规范形成有限状态机，如图 2 所示。

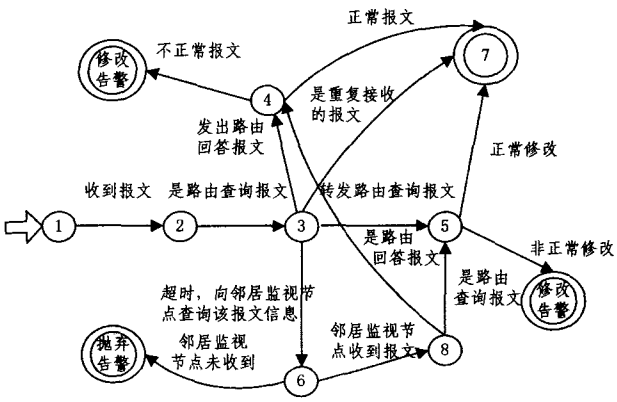

图 2 节点收到路由查询报文后处理过程的有限状态机

设起始状态是 1，节点收到报文后转向状态 2。如果收到的报文是路由查询报文，进入状态 3。如果该节点产生了路由回答报文，则进入状态 4，接下来对路由回答报文按 DSR 路由规范进行检查，如果是正常的，则达到状态 7，有限状态机正常结束。如果报文有些字段被非法修改了，则发出非法修改告警。在状态 3 时，如果收到的是以前收到过的路由查询报文，则直接抛弃报文进入终止状态 7。如果转发路由查询报文，则进入状态 5，接下来对转发的路由查询报文按 DSR 路由规范进行检查，如果修改了一些不能变化的字段，则发出非法修改告警，否则进入终止状态 7。如果在状态 3 超过一定时间没有动作，这时有可能是节点移动离开了监视区域，监视节点不能收到节点所转发的路由报文，所以向周围监视节点发出是否收到该节点的转发报文的询问，如果邻居监视节点收到，则状态转向 8，若是路由查询报文，则将报文信息发到监视节点，转到状态 5 进行比较，若是路由回答报文，则将报文信息发到监视节点，转到状态 4 进行比较。如果邻居节点未收到报文，说明该节点不参与路由转发，则发出抛弃报文告警。

在 DSR 路由协议中，对于路由回答报文、路由出错、数据报文 3 种报文的处理过程是同样的，可以采用相同的有限状态机进行分析处理。如图 3 所示，起始状态是 1，节点收到报文后转向状态 2。如果收到的报文是路由回答、路由出错、数据报文 3 种报文之一，则进入状态 3，以下可能分别转入 3 个

状态，如果本节点已经是报文目标节点，则进入终止状态。如果转发报文，则进入状态4，在DSR路由协议中对这3种报文只能原样转发，不能进行修改，接下来只对照一下转发前后的报文，如果有不同则发出非法修改告警，如果相同则进入终止状态。在状态3时，如果超时没有收到转发报文，则向邻居监视节点查询该报文信息，进入状态5，如果邻居监视节点收到其发出的报文，则将信息发来，进入状态4，如果邻居没有收到，则发出抛弃报文告警。

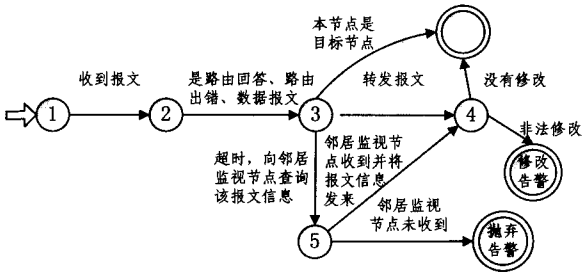

图3 节点收到路由回答报文、路由出错、数据报文时处理过程的有限状态机

图2和图3都是处理一个节点接收报文后的处理流程。图4显示的是节点发送报文后的有限状态机处理流程。当监视节点监视某个节点A发出报文时，状态由1到2，下面可能是下列3种情况之一：其一，以A节点为源节点的报文，即A节点发出了这个报文，状态由2到终止状态。其二，A节点是中间节点，它只是转发报文，进入状态3，因为节点A接收报文时，不在监视节点的区域内，转发时节点移动进入监视节点的范围内，所以只看到节点A发出了报文，此时监视节点等待邻居监视节点查询，如果有邻居监视节点查询，则将报文信息发到邻居监视节点，有限状态机进入终止状态。如果没有邻居监视节点查询，说明没有节点发送过此报文，是节点A编造了此报文，有限状态机发出编造告警。第3种情况是，节点A不在报文地址列表中，就是说节点A与报文没有任何关系，但它又发出该报文，即节点A假冒其它节点发送了这份报文，有限状态机发出假冒告警。

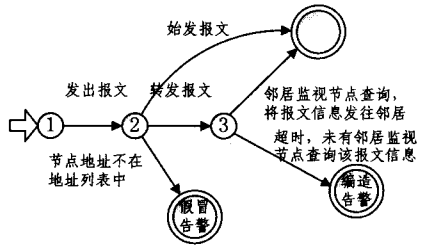

图4 节点发送报文后处理过程的有限状态机

5 模拟实验

5.1 实验设置

实验平台为Pentium4 1.8GHz，512MB RAM，使用的操作系统是Red Hat Linux 7.12，仿真平台是NS-2。仿真中，节点总数设置为50个，节点运动范围为1500m×300m，运动速度为0～20m/s，网络中节点的运动采用随机运动模型，即每个节点在该区域内从一点向另一点运动，运动速度在[0，20m/s]内均匀分布，到达目标点后，停留一段时间，然后选择一个新的目标点，同时再选择一个新的速度，向新的目标点运动，依次类推，直至仿真结束。MAC层使用802.11，传输半径为250m，链路带宽为2Mbps，模拟时间为900秒。

5.2 实验结果

我们将选举算法和有限状态机在NS-2中进行了编码实现。为了检验入侵检测效果，按3.2节的分析，我们设计了4种对DSR路由协议的攻击方式。攻击方式1是非法修改攻击，即入侵者转发报文时，非法插入、删除和修改报文中的信息。攻击方式2是抛弃攻击，即入侵者只收报文，不转发任何报文。攻击方式3是假冒攻击，即入侵者假冒其它节点发送各种报文，如路由查询报文、数据报文等。攻击方式4是编造攻击，入侵者编造一些由它转发的报文，但实际上源节点并未发出此报文。

表1列出了有限状态机对4种攻击方式的入侵检测率和误报率。从表1可以看出，对假冒攻击的检测率最高，主要原因是监视节点只需将发出报文的节点地址与报文中的地址列表对照一下，如果没有就是假冒攻击，最为简单。抛弃攻击检测率最低，主要原因是监视节点不能直接做出判断，要到邻居节点去查询才能得出结果。编造攻击也是需要邻居监视节点查询才能判断，检测率也较低。但是总的来说，检测率均在80%以上，说明我们的算法还是十分有效的。

表1 4种攻击方式的入侵检测率

攻击方式	检测率	误报率
修改攻击	91.3%	2.9%
抛弃攻击	83.7%	5.7%
假冒攻击	97.4%	1.3%
编造攻击	88.5%	7.2%

结束语 本文提出了基于簇头的分布式合作的入侵检测架构，即整个网络分成一个个区域，每个区域内的监视节点既负责本地入侵检测又合作检测整个网络节点，通过随机选举簇头作为监视节点，并周期性地重新选举簇头，既节省网络资源又保证了入侵检测系统的安全性。在入侵检测架构的基础上，设计了基于规范的入侵检测算法，即通过DSR路由协议规范形成节点处理过程的有限状态机，对节点的每个报文的处理过程按有限状态机进行分析，实时地发现入侵行为。最后通过模拟实验检测了我们方法的有效性。

参考文献

[1] Corson S, Macker J. Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations[S]. RFC 2501. January 1999

[2] 易平，蒋嶷川，钟亦平，等. 移动ad hoc网络安全综述[J]. 电子学报，2005，33(5)

[3] Ramkumar M, Memon N. An Efficient Key Predistribution Scheme for Ad Hoc Network Security[J]. IEEE Journal on Selected Areas of Communication, 2005, 23(3): 611-621

[4] Zhu Sencun, Xu Shouhuai, Setia S, et al. LHAP: A lightweight network access control protocol for ad hoc networks[J]. Ad Hoc Networks, 2006, 4(5): 567-585

[5] 易平，蒋嶷川，钟亦平，等. 移动ad hoc网络路由协议安全研究[J]. 计算机科学，2005，32(6)

[6] Argyroudis P G, O'Mahony D. Secure routing for mobile ad hoc networks[J]. IEEE Communications Surveys & Tutorials, 2005, 7(3): 2-21

[7] Yi Ping, Zhong Yiping, Zhang Shiyong, et al. Flooding Attack and Defence in Ad Hoc Networks[J]Journal of Systems Engineering and Electronics, 2006, 17(2): 410-416

[8] Zhou Lidong, Haas Z J. Securing ad hoc networks[J]. IEEE

Networks Special Issue on Network Security, November/December 1999

[9] Capkun S, Nuttyan L, Hubaux J-P. Self-organized public-key Management for mobile ad hoc networks[J]. IEEE Transactions on mobile computing, 2003, 2(1)

[10] Papadimitratos P, Haas Z. Secure routing for mobile ad hoc networks[C]// Proceedings of the SCS communication Networks and Distributed Systems Modeling and Simulation Conference. San Antonio, TX, January 2002

[11] Hu Y-C, Perrig A, Johnson D B. Ariadne: A secure On-Demand Routing Protocol for Ad hoc Networks[C]// Proceedings of the MobiCom 2002. Atlanta, Georgia, USA, September 2002

[12] Sanzgiri K, Dahill B, Levine B N, et al. A Secure Routing Protocol for Ad Hoc Networks[C]// Proceedings of 2002 IEEE International Conference on Network Protocols(ICNP). November 2002

[13] Hu Y-C, Johnson D B, Perrig A. SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks[C]// Proceedings of the 4th IEEE Workshop on Mobile Computing Systems & Applications(WMCSA 2002). IEEE, Calicoon, NY, June 2002: 3-13

[14] Zhang Yongguang, Lee W. Intrusion Detection in Wireless Ad-Hoc Networks[C]// Proceedings of The Sixth International Conference on Mobile Computing and Networking (MobiCom 2000). Boston, MA, August 2000

[15] Zhang Yongguang, Lee W. Intrusion Detection Techniques for Mobile Wireless Networks[J]. Mobile Networks and Applications, 2003

[16] Kachirski O, Guha R. Intrusion Detection Using Mobile Agents in Wireless Ad Hoc Networks[C]// IEEE Workshop on Knowledge Media Networking(KMN'02)

[17] Puttini R S, Percher J-M, Mé L, et al. A Modular Architecture for Distributed IDS in MANET[C]// Proceedings of the 2003 International Conference on Computational Science and Its Applications(ICCSA 2003). LNCS 2668. San Diego, USA, Springer Verlag, 2003

[18] Huang Yi-an, Lee W. A Cooperative Intrusion Detection System for Ad Hoc Networks[C]// 2003 ACM Workshop on Security of Ad Hoc and Sensor Networks(SASN '03). Fairfax, VA, USA, October 2003

[19] Sun B, Wu K, Pooch U W. Routing Anomaly Detection in Mobile Ad Hoc Networks[C]// Proceedings of 12th International Conference on Computer Communications and Networks (ICCCN 03). Dallas, Texas, October 2003: 25-31

[20] Albers P, Camp O, Percher J-M, et al. Security in Ad Hoc Networks: a General Intrusion Detection Architecture Enhancing Trust Based Approaches[C]// Proceedings of the First International Workshop on Wireless Information Systems(WIS-2002). Apr. 2002

[21] Bhargava S, Agrawal D P. Security Enhancements in AODV Protocol for Wireless Ad Hoc Networks[C]// Vehicular Technology Conference. vol. 4, 2001: 2143-2147

[22] Wang Weichao, Lu Yi, Bhargava B K. On Vulnerability and Protection of Ad Hoc On-demand Distance Vector Protocol[C]// Proceedings of 10th IEEE International Conference on Telecommunication(ICT). 2003

[23] Subhadrabandhu D, Sarkar S, Anjum F. A Framework for Misuse Detection in Ad Hoc Networks—Part I[J]. IEEE Journal on Selected Areas in Communications, 2006, 24(2): 274-289

[24] Johnson D B, Maltz D A, Hu Y-C. The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks (DSR), Internet-Draft, draft-ietf-manet-dsr-09. txt, 15 April 2003[OL]. http://www.ietf.org/internet-drafts/draft-ietf-manet-dsr-09.txt

(上接第 104 页)

置为 0，随着它不断提供错误服务，与之进行交易的风险值急剧上升，在第 30 次时，风险值就上升到 1。因此，基于信任的风险计算算法能够较准确地区分节点的善恶，并且对节点能够赏罚分明。

(2)节点请求下载服务时，对发出服务响应的服务节点进行风险评估，选择风险值最低的节点进行文件下载。如果风险评估模型评估后所选中的节点恰好是 Good peers，则风险评估是成功的；反之，如果经风险评估模型评估后所选中的节点恰好是 Worst peers，则风险评估失败。W 和 M 在 3 种不同的取值情况时，基于信任的 P2P 网络节点信息交换的风险评估成功率如图 5 所示。实验结果表明 W 和 M 取值比较大时更有利于提高风险评估的准确性。信任风险的权重 W 设置为大于 0.5 即可，而风险影响 M 设置为接近或等于 1 能更好地保证对节点信息交换的风险评估质量。实验得到的数据表明，在 P2P 网络中对节点的信息交换运用基于信任的风险评估方法能够较成功地评估节点，从而验证了该模型的可行性。

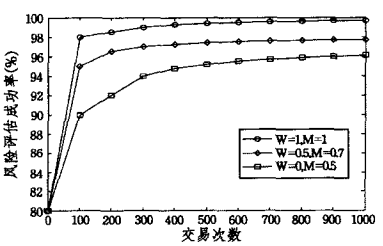

图 5 3 种参数情况下的风险评估成功率

结束语 由于 P2P 网络的开放性和动态性，节点间信息交换所存在的潜在风险是不确定的，对信息交换进行风险评估是解决安全问题的有效途径。本文提出从 P2P 网络的信任模型着手，利用信任和风险之间的内在联系同时结合传统的风险计算函数，得到一个新的风险计算方法。通过实验验证了该方法的有效性和可行性。在下一步工作中，将进一步探讨和改进基于信任的 P2P 网络风险评估模型。

参 考 文 献

[1] Wang Y, Vassileva J. Trust and reputation model in peer-to-peer networks[C]// Proceedings of the Third International Conference on Peer-to-Peer Computing(P2P'03). IEEE, 2003: 150-157

[2] Wang Y, Lin F. Trust and Risk Evaluation of Transactions with Different Amounts in Peer-to-Peer E-commerce Environments [C]// Proceedings of IEEE International Conference on e-Business Engineering(ICEBE'06). IEEE, 2006: 102-109

[3] Asnar Y, Zannone N. Perceived risk assessment[C]// Proceedings of the 4th ACM workshop on Quality of protection(QoP'08). ACM, 2008: 59-63

[4] Josang A, Presti S. Analysing the relationship between risk and trust[C]// Proceedings of Second International Conference on Trust Management (iTrust 2004). Oxford, UK, March 2004: 120-134

[5] Singh A, Lilja D. Improving risk assessment methodology: a statistical design of experiments approach[C]// Proceedings of the 2nd International Conference on Security of Information and Networks(SIN'09). ACM, 2009: 21-29