Ad Hoc 网络中的入侵检测

曾英佩　郭山清　谢　立

（南京大学软件新技术国家重点实验室　南京 210093）（南京大学计算机科学与技术系　南京 210093）

摘　要　随着 Ad Hoc 网络研究的深入，安全问题已引起广泛的关注。Ad Hoc 网络由于其传输媒介开放、网络拓扑变化快、带宽资源有限、节点间仅靠合作而缺乏集中监控点等特性，容易遭受攻击。然而有线网络中的大部分入侵检测技术在 Ad Hoc 网络中并不适用，目前已有新的体系及算法提出，以适应新的环境。本文分析比较了已有的入侵检测技术，并指出了一些待解决的问题，作为未来研究工作的基础。

关键词　入侵检测，Ad Hoc 网络，安全路由

Intrusion Detection in Wireless Ad Hoc Network

ZENG Ying-Pei　GUO Shan-Qing　XIE Li

(State Key Laboratory for Novel Software Technology, Nanjing University, Nanjing 210093)

(Department of Computer Science and Technology, Nanjing University, Nanjing 210093)

Abstract　Security of the Ad Hoc network is becoming more concerned as the research of this field carry on. Ad Hoc network is generally more vulnerable to threats due to its features of open medium, dynamic network topology, limited bandwidth and resources, cooperation algorithms, and lack of centralized monitoring point. But most techniques developed in the wired network are not applicable in Ad Hoc network, new models and algorithms have been proposed in this new environment. In this paper we analyze and compare the existing intrusion detection techniques and also address the research trends in this area.

Keywords　Intrusion detection, Ad Hoc Network, Secure routing

1　引言

Ad Hoc 网络是一种无组织的对等网络，使用无线通信技术。网络中没有固定的基础设施（如接入点），各节点自主连接，组成网络。相邻的节点间一般可以直接通信，共享同样的物理频段；而非相邻的节点间采用多跳（Multi-hops）的方式进行通信，即通过中间节点进行转发。这种无组织的连接方式具有极大的灵活性，很适合应用在战场、灾难救援现场等地方，因为此时网络通信不能依赖于任何基础设施，也没有节点进行集中控制。由于其重要应用前景，特别是随着蓝牙、IEEE 802.11 等新技术引进以来，Ad Hoc 网络在研究领域引起了广泛的关注[12]。

网络安全一直是网络普及以来网络技术中的一个重要话题，而在 Ad Hoc 网络中，安全的需要变得更加迫切，主要原因如下[1,9,14]：

(1)节点更容易被入侵。一方面，Ad Hoc 网络节点能自主移动不受限制，这使得容易在经过的区域中被入侵，且物理上的保护也更加困难；另一方面，恶意节点容易伪装，可能先进行非法入侵，然后通过断开操作（Disconnect Operation），脱离网络后更换标示，重新加入伪装成正常节点；

(2)使用无线连接，天生容易被窃听和干扰，入侵者无需取得对物理链路的访问就可以监听数据；

(3)节点的资源和带宽有限，资源容易被非法操作耗尽；

(4)Ad Hoc 网络缺乏明显的边界。节点间的连接都是自组织的，区域内的任何节点间均可通信，没有明显边界，因此没有防火墙之类安全设施，这使得节点直接暴露在攻击者面前。

已经有了一些针对 Ad Hoc 网络的安全路由进行的工作[3,7,16,17]，但是它们只是防范措施，在有线网络中已经证明安全的网络应该是具有逐步防御的（Defense-in-Depth）多层设施，入侵检测是在入侵发生后的一层上。从获取数据手段上入侵检测可分为基于网络（Network-based）和基于主机（Host-based）两种[9,11]，从使用的检测技术上又可分为基于误用的检测（Misuse-based）和基于异常的检测（Anomaly-based）。基于误用的检测，如 STAT，通过检测是否匹配预定义的一些指示入侵的特性来进行，因此具有较低的误报率，但不能检测出未定义其特性的未来可能出现的入侵；基于异常的检测如 IDES 则是建立用户在正常行为下的使用模式，如果发现现行情况异于此模式，则认为发生了入侵，这种方法误报率比较高，但是能够检测出一些未来新的入侵。入侵检测是保障网络安全的一个重要手段，显然在 Ad Hoc 网络中也是必需的。

本文主要对现有的基于 Ad Hoc 网络的入侵检测做一概述，为进一步的研究打下基础。文章第 2 节介绍入侵检测在 Ad Hoc 网络中遇到的问题，第 3 节介绍 Ad Hoc 网络中的入侵检测。最后指出未来研究的方向。

2　入侵检测在 Ad Hoc 网络中遇到的问题

传统的入侵检测技术并不能在 Ad Hoc 网络中直接使用，这是由其与有线网络不同的一些特性决定的[1,6,9,22]：

曾英佩　硕士，主要研究方向为计算机网络安全；**郭山清**　博士，主要研究方向为网络安全，机器学习；**谢　立**　博士生导师，主要研究方向为分布式计算和并行处理，信息安全等。

(1)节点间大部分算法都是合作的形式,恶意节点容易渗透进入网络从而攻击。因为 Ad Hoc 网络中没有固定的基础设施,大部分操作如路由均需通过节点相互间合作来进行,恶意节点可随意加入网络而发起攻击,节点认证也没有受信任节点进行集中控制。

(2)没有集中网络流量的地方,无法集中进行监控。在 Ad Hoc 中如节点间自主进行连接通信,不存在交换机、路由器等固定的集中流量的地方,这使得传统的基于网络的入侵检测变得不可行,而只能以一种分布式的形式进行监控,即将检测功能分散到节点中去。

(3)正常节点和恶意节点之间行为区别不够明显。比如由于网络拓扑结构变化快,某节点可能会广播一个错误信息,这可能是恶意行为也可能该节点对网络的情况变化比较迟钝而已。

(4)移动设备只有有限的资源和带宽。比如设备一般使用电池供电,而且无线网络的带宽一般都小于有线网络,因此设计通信协议时还必须考虑到节点间的通信带宽,计算开销都比较昂贵。

这些客观条件使得必须在已有的入侵检测技术上建立新的入侵检测系统框架,比如因前面提到的特性(2)的制约,在 Ad Hoc 中我们必须采用分布式的方式进行入侵检测。在审计数据源获取上,一方面节点也可以监控本地的运行情况如系统调用、网络使用情况;另一方面,从物理的角度上看,节点如果在另一个节点的传输范围(Transmission Range)内,也可以接收该节点发出的信号。因此,一个节点可以直接获得的监控数据有本地节点的所有情况和本地监听到的邻居节点的网络情况。一般即采用这两方面数据作为审计数据源。

目前的研究主要集中在两个方面:入侵检测体系结构和入侵检测算法。入侵检测体系结构方面,因为审计数据源反映的只是网络局部的情况,能够检测本地入侵,但是要在这种局部数据上检测整个网络的攻击行为是不全面的,因此在检测一些攻击的时候,需要各个检测部分合作进行,而不同的合作方式形成了不同的体系结构。入侵检测算法方面,主要是因为 Ad Hoc 网络是一个全新的环境,缺乏入侵数据、路由协议和 MAC 层协议等均与传统网络中不同,已有的算法可能不能直接使用,或者必须加以修改。下面我们将就这两方面对当前研究现状进行分析。

3 Ad Hoc 网络中入侵检测的体系结构

由于 Ad Hoc 网络移动性强,网络拓扑和通信均不稳定,使得怎样部署 IDS 系统以及它们之间是否有数据交换、如何交换数据、相互协作等成为比较关键的问题。已提出的体系结构中,按照各个节点 IDS 间的关系,可以大致分为 3 种不同类型的体系结构。

3.1 各自独立的 IDS 体系

体系结构如下:每个节点都安装有 IDS 系统,它们各自独立进行入侵检测,之间并不互相交流、合作,因此各节点检测所采取的方法也可以不一样,检测结果也只是通知本地的管理员而不会告知其他的节点。典型工作如:Sergio Marti 提出的 Watchdog[10],每个节点都运行有一个监控的 Watchdog 和选路的 Pathrater,Watchdog 维护了一个缓冲区,放自己发送的数据包。如果检测到邻居发送的数据包中有与之匹配的,则认为邻居行为良好;如果超过计时没有监听到包与之匹配,则认为它的下一跳即那个邻居的行为异常(丢弃或篡改数据包),这将会导致在 Pathrater 中该邻居节点的等级(Rating)降低,Pathrater 在选择路由时会避开这些节点。虽然这种体系结构里一个节点可以向另外一个节点通报某个节点为异常节点,但最后核实过程必须还是由自己完成,且对于异常情况没有节点间协同的检测。

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。

3.2 对等合作的 IDS 体系

由于每个节点都只有一部分监测数据,而某些入侵的数据、场景可能分散在很多地方,如两个分散的恶意节点可能通过不同路径对目标进行攻击。而且,Ad Hoc 网络中节点容易被俘获,通过多个节点共同合作,可以更容易隔离被入侵,防止节点处于"孤岛"的境地。

对等合作的体系结构如下:每个节点独立地对入侵进行检测,在检测某些入侵需要其他节点的信息或帮助时可以进行合作,各个节点间不存在层次关系。

Yongguang Zhang 在文[9,14]中提出了一个如图 1 所示的 IDS 结构。

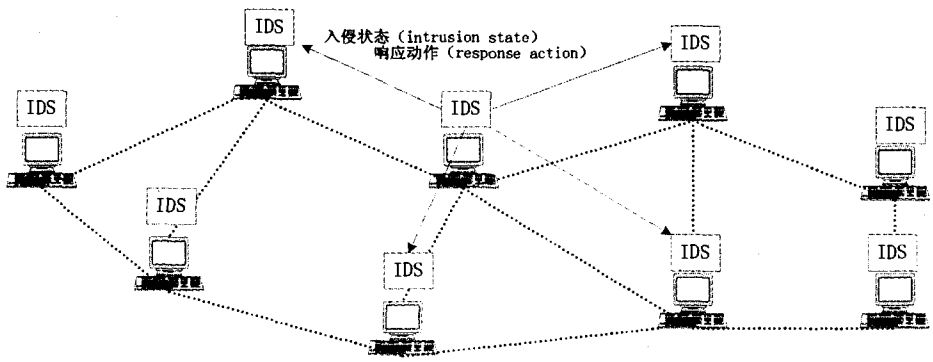

图 1 对等合作的 IDS 结构

其中每个节点都安装有 IDS,都必须在本地负责检测入侵信号和参与节点间的合作调查。本地 IDS 要检测的包括用户、系统行为和本地辐射范围内的通信。为了能进行 IDS 间的合作,从而构成一个统一的 IDS 系统,本地的 IDS 代理(IDS Agent)结构如图 2 所示。

本地检测引擎(Local Detection Engine)被用来检测本地的异常。如果检测到一个特定的入侵或者有很充分的证据(如触发了有很高准确性的规则)证明确实正遭遇入侵,则可调用两个响应模块进行响应(Intrusion Response)。否则,如果证据较弱或者不足,而且允许进行更广的调查,则该 IDS 可

以调用合作检测引擎(Cooperative Detection Engine)给邻居广播入侵信息。然后每个节点都可以广播发送入侵信息和自己判断的几率。这样形成一个简单的投票,每个节点如果发现收到的大多数都显示入侵,就可判定存在入侵,可以发起响应。在投票决定的时候,还可以将与攻击场景发生处附近的节点的优先级设置得相对高一点,以真实反映对某次入侵的感知能力。

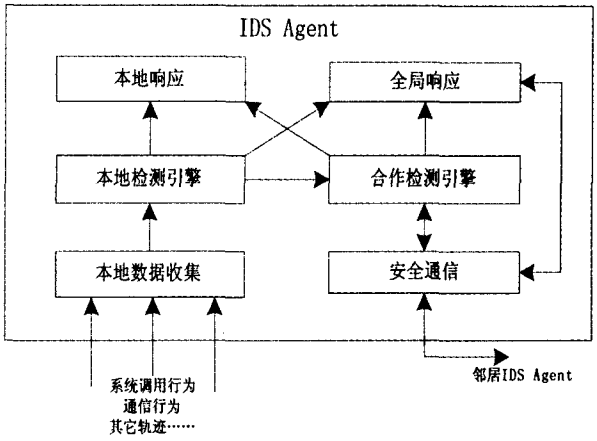

图 2 IDS代理的结构

Patrick Albers 等人采用了与 Yongguang Zhang 类似的框架[6],但较特别的是他们提出了使用移动 Agent 作为各个节点的 IDS 间交换数据、警报等的媒介。由于 Agent 具有代码移动的特点,可以根据发出者不同的需要来取得相应的信息。而且,他们提出使用标准 IDMEF 和 IDXP 来进行信息交换,使用 SNMP 代理来取得审计数据,通用性得到了提高,不过提出的框架还没有得到实现。

在合作的体系下,对入侵的响应也必须是合作性的,提出界外(Out of Bound)重新认证并建立新的通信通道[9]。

对等合作的 IDS 体系能够利用各个节点共同检测到的入侵信息,检测能力与各自独立的体系相比有了提高,但是它存在着一些弊端:

(1)要求每个节点都必须安装运行 IDS 系统,这对于一些资源较少的节点太苛刻,而且在安全威胁较小时也不必要;

(2)节点间每次合作都不得不互相传递很多信息,即使能使用组播或广播进行,也浪费了很多宝贵的带宽。而如果不能识别恶意节点让其频频发起合作,将严重影响网络流量。

3.3 分级的 IDS 体系

为了避免每个节点同时都运行 IDS 带来的计算额外计算开销,以及各个子 IDS 间进行合作产生通信开销,提出了分级的 IDS 体系。它的体系结构如下:采取多级的方式,对 IDS 功能进行分布,处于底层的部分可能进行初级的 IDS 检测或者不进行检测,高层的可以综合利用底层获取的信息进行判断,提供更好的准确性并减少开销。典型工作如下:

Oleg Kachirski 等人提出了一个基于 Agent 的多层的 IDS 体系[2],其中有 4 种 Agent 分别专注:主机监控(Host monitoring)、响应(Action)、网络监控(Network monitoring)、决策(Decision-making)。主机监控 Agent 用于监控节点的系统调用和应用程序,响应 Agent 用于对攻击进行响应,这两种 Agent 必须在每个节点都安装并运行。而网络监控 Agent 用于对网络传输数据进行监控,不需要在每个节点安装。决策 Agent 如果用于收集信息对网络级别的安全进行检测,则也不需要在每个节点上都安装。为了节省节点电池等资源,而又不降低安全检测能力,提出用一种簇计算算法选出安装网络监控和决策的节点——簇头节点(Cluster Head),在这些节点上运行这两种 Agent。在分簇时,需要在覆盖全部节点和减少重叠中取得平衡。

Yi-an Huang 等人提出了 MANET 中基于簇的入侵检测(Cluster-based Intrusion Detection)[5],他们首先采用文[18]中的簇生成算法,利用圈计算协议(Clique Computation Protocol)来计算出互相间能直接通信的节点圈,然后再利用簇头计算协议(Clusterhead Computation Protocol)计算出一个簇的簇头节点。在计算簇头时,假定有 S_c 个节点,每个节点随机地选用一个 R_i 值。在每个节点均得到了其他簇内节点的 R 值后,便可以使用 XOR 函数各自计算出簇头为 $f(R_0,R_1,R_2,\cdots,R_{S_c-1})=(\bigoplus_{i=0}^{S_c-1}R_i) \bmod S_c$。使用 XOR 的优点是,在输入是随机的情况下,输出也是随机的。另外,还提供了簇恢复协议(Cluster Recovery Protocol),来在普通节点失去与簇头联系或者簇头与所有簇内节点均失去联系时发起,以加入或重新组建簇。这个体系内,一个簇中同时只有一个节点(即簇头)在进行入侵检测,而所有节点在一般情况下选为簇头的概率是相同的。作者在设计细节时还考虑到了一些恶意节点可能干扰簇头的正常选取,但是没有考虑到各个节点间的资源不同、可信性不同等等。

Bo Sun 等人提出了一个基于区域的入侵检测体系(ZBIDS)[4],它将网络分为多个不同的区域,区域的大小与节点移动性、密集度等有关,采用 Joa-Ng 等人在文[19]提出的算法来划分和维持区域。一个区域与其他区域相连的节点成为网关节点(Gateway node),区域内的节点通过警告洪泛(Alert Flooding)发出警告(Alert),网关节点则获取这些警告从而发布警报(Alarm)。由于在 MANET 中警告可能会很多,为了不被突发的大量警告淹没,网关节点不是警告触发而是周期性地运行。

当然,合理分级的 IDS 体系必须能保证对所有需要检测的节点进行检测,不能出现检测的空白区域。在基于簇的分级体系中,构造出合理的簇,还存在诸多需要考虑的地方,这将在后面讨论。

3.4 三种体系的比较

这三种体系中,从实现上看,各自独立的体系实现最简单,但是没有利用其他节点或全局的网络信息,这限制了它的检测能力。对等合作的体系次之,因为它虽各自独立进行检查但还牵涉到多个 IDS 的协作。分级的体系由于牵涉到不同级节点(比如簇头)的选择和维持,实现最为复杂。从开销上看,各自独立的体系由于节点间没有额外的通信,通信开销较小,但每个节点均需要运行 IDS 系统,有一定的计算开销;对等合作的体系在协作时各个子 IDS 间相当于进行了全连接的方式进行信息交换,通信开销较大,而且同样每个节点均需运行 IDS 系统;分级体系中典型的如基于簇的分级体系,在协作时只是进行了簇头节点间的全连接,与对等合作的体系相比减少了通信开销,而且也不需要每个节点运行 IDS 子系统,因此计算开销也较小。其实对等合作体系相当于分级体系中一级的特例,比如基于簇的分级体系中单个节点为一个簇的情况。目前提出的框架在体系选择上一般倾向于选择这两种体系,因为这样能最大限度地利用审计数据。

4 入侵检测系统的检测算法

节点 IDS 的检测信息一般包括系统调用行为、应用层行

为、网络通信行为，在系统调用和应用层上进行的研究很少，这主要是因为 Ad Hoc 网络中目前还缺乏有代表性的应用。因此，目前大部分都注重于网络通信上的检测。下面将讨论在 Ad Hoc 网络中已提出的几种入侵检测算法。

4.1 基于 RIPPER 分类器的检测算法

Yongguang Zhang 在文[9]中提出了一种基于 RIPPER 分类器的检测方法，属于基于异常的检测。它采用 PCR(路由改变比率)和 PCH(路由总跳数改变比率)等几个属性来表示记录数据。在文[5]中作了改进，特征度量属性的数目被增加到了 141 个。算法大致过程为：给出训练数据集，设为 $\{f_1, f_2, \cdots, f_L\}$ 为所使用的特征属性，采用 $\{f_1, f_2, \cdots, f_{i-1}, f_{i+1}, \cdots, f_L\}$ 组成的特征属性集合来训练分类器 C_i。对于某个纪录 $x=\langle v_1, v_2, \cdots, v_L\rangle$，首先应用每个 C_i 来计算出其他属性的值给出时 v_i 的概率 $p_i\{v_i \mid v_1, v_2, \cdots, v_{i-1}, v_{i+1}, \cdots, v_L\}$，然后计算其平均概率(average probability) $\frac{\sum_i p_i}{L}$，再与门槛值比较。如果低于门槛值，则发出警报，因为正常情况下其发生概率极小。显然，这种情况下门槛值大小决定着误报率的高低。

4.2 基于支撑向量机的检测算法

Hongmei Deng 等在文[21]提出了基于支撑向量机(SVM)的检测算法，也属于基于异常的检测。检测中有两种分类器 1-SVMDM 和 2-SVMDM，两者的区别在于前者工作在无监督的状态，使用的训练数据没有先被标记；后者则使用已标记的数据集进行训练。由于对训练数据进行标记是一项费时且容易出错的工作，而且正常的记录一般远多于异常的记录，因此往往先使用 1-SVMDM 进行异常点检测，得出的超平面可以用来区分正常与异常记录。而在得到足够多的已知类别记录后，也可以使用 2-SVMDM 训练和区分数据。这种方法很大程度上利用了 SVM 的高检测率和容忍噪音(Noise-tolerance)特性。

4.3 基于人工免疫的检测算法

Sarafijanovic 等人在文[15]及其以前的几篇论文中引入了人工免疫系统(Artificial Immune System)，用以检测 DSR 路由协议。他们先将人体免疫系统(HIS)到人工检测系统间进行映射，自我细胞映射到正常节点；抗原映射到一系列观察到的 DSR 路由协议的事件，并编码成二进制串，加以表示事件(如“数据包接收”、“数据包接收后再发送”等)，然后利用 AIS 的抗原和检测器间的匹配来加以检测。

Sarafijanovic 还提出几种方法以增强检测能力，减少误报率。集簇(Clustering)是用于将对某个节点的匹配(检测器和抗原间)进行集簇，使得在该节点匹配的抗原和总的抗原超过一定比率时才检测为恶意节点，可以减少误报率。危险信号是仿照人体免疫系统中的危险信号核实检测，只有危险信号的匹配才会被检测时计数，而危险信号只在包丢失的路由上分发，其内容包含发生时间和与包丢失有关的节点，这与集簇一样可以减少误报率。虚胸腺(Virtual thymus)是指一组用来表示当前自我的设施，当前自我是动态的并被不断地进行阴性选择，可以有效反映当前正常状态并不需要提前训练阶段。记忆检测器(Memory detector)是检测器如果在检测中被证明是有用的，将成为记忆检测器，它们与一般的检测器不同，在于有更长的生存时间及在检测时要求更低的集簇，使得能够更快地进行再次应答(Secondary response)。

4.4 基于 STAT 的检测算法

Gwalani 在文[20]中提出的方法 AODVSTAT，它基于 STAT[13]。AODVSTAT 包括 AODV 事实库，(AODV Fact Base)用于存放 AODV 路由协议信息、网络拓扑、邻接信息等；场景数据库(Scenario Base)，用于保存状态转换图(State Transition Diagram)；探测器(Probe)，与网络交互，它在这里被用于监控网络流量及进行响应；分析引擎和规则构造器(Analysis Engine and Rule Builer)，前者利用事实库和场景数据库对攻击进行刻画，后者将前者的分析结果用于配置探测器。它与 STAT 框架上有所不同但整体功能上没有变化，主要在于将 STAT 中的推理引擎(Inference Engine)匹配功能移到了分析引擎，而将攻击响应部分与获取数据部分合并。在这种方法下，场景(Scenario)还是最重要的部分。一般，一个攻击需要有对应的状态转换图才能被检测，比如需要一个单独的转换图用来检测 RREP 丢包攻击。因为场景的产生都靠人工分析，所以比较耗时并且容易出错。

4.5 算法的比较分析

基于 RIPPER 分类器和 SVM 的检测算法属于基于异常的算法，可以检测到复杂的新出现的攻击。在设计时，如何选取适当的特征属性是核心问题，因为不同类的攻击需要不同的属性，比如选取单位时间内连接数目可以辅助检测 DoS 攻击；对于底层协议采用不同的优化方法，也有事半功倍的效果，如文[9]中提出其方法可针对底层不同的网络协议如 DSR 进行优化。基于人工免疫的检测，仿照人体免疫系统进行工作，由于有记忆功能，可以对一些训练时已知的攻击快速地检测，另外从人体免疫原理来看对新攻击也有很高的检测能力。但由于人体免疫系统的一些原理也在探索中，而且没有很好地仿真人体免疫系统的一些防止误判措施，人工免疫系统中容易出现高误报率。运用中还存在一些其他问题都没有解决，比如如何更好地从人体免疫系统映射到人工免疫系统、确定检测为异常时是针对一个节点还是一系列消息等。基于攻击特征的检测属于基于误用的检测算法，对已知攻击的检测率高，并且误报情况少，但生成表示攻击场景或攻击序列是比较费时的工作，并且由于很多的应用将会移植到 Ad Hoc 网络中，因此会出现很多针对这些应用的攻击。因此，基于误用检测的系统需要频繁地更新特征库，这个开销将是比较大的。

4 尚待解决的一些问题

Ad Hoc 网络中的入侵检测研究目前还处于起步阶段，主要集中在路由协议上的检测上[5,8,10,14]。在 Ad Hoc 网络中的入侵检测也没有一些通用的数据集，而且大部分都是仅限于模拟(Simulation)，缺乏实验(Experiment)验证[20]。在 Ad Hoc 网络中还有很多需要进一步研究的问题：

(1)各子 IDS 系统之间的合作问题

在对等合作和分级的体系中，IDS 驻留在不同的节点，需要解决它们之间如何有效进行信息交换。文[9]中提出的各节点通过投票的方法进行合作，无疑是比较初级的合作方式；另外，分级时簇的形成与簇头的选择需要各个节点合作进行。由于已有工作大部分没有深入考虑节点资源不同和移动情况下的问题，因此有待提出合理、健壮的分簇算法以及簇头选择算法。

(2)IDS 子系统的检测算法

基于异常的检测算法中，特征属性如何选取，还没有一个很好的方案。文[5]中选取了 141 个属性，可是对某些攻击的检测不理想。在基于人工免疫的检测中，更好地模拟人体免

疫来判别自我，可以缓解误报问题。在应用多层联合检测时还需要上层与下层间进行协调[9]。

(3)IDS系统自身的安全

IDS系统间通信应该保密和节点间进行认证，防止伪造IDS命令或它们之间的通信。而目前Ad Hoc网络的大部分研究中，对IDS的安全只是提及[9]，或者放在下一步工作中[20]。另外，由于Ad Hoc网络的特殊性，网络节点也容易被俘获，因此密钥等设施也可能被敌对者得知。可以引入信任，如Marti在文[10]中提到的使用先验信任(Apriori trust)，不过这种静态给定的信任度显然不能适应Ad Hoc网络的环境，可以采用动态改变信任度的方法。

结束语 Ad Hoc网络中的安全十分重要，已经出现了很多安全设施，诸如安全路由、加密、入侵检测等。其中入侵检测是最近才提出的，但由于其在安全中的重要性，并且由于Ad Hoc网络的特性而与传统有线网络存在很多不同，得到较多的关注。本文对当前Ad Hoc网络的入侵检测研究做了分析比较，指出了一些待解决的问题，在下一步工作中解决。

参考文献

1 Brutch P, Ko C. Challenges in Intrusion Detection for Wireless Ad-hoc Networks. In: 2003 Symposium on Applications and the Internet Workshops (SAINT'03 Workshops), 2003
2 Kachirski O, Guha R. Effective Intrusion Detection Using Multiple Sensors in Wireless Ad Hoc Networks. In: Proc. of the 36th Hawaii Intl. Conf. on System Sciences IEEE (HICSS'03), 2002
3 Hu Y C, Johnson D, Perrig A. SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks. In: Fourth IEEE Workshop on Mobile Computing Systems and Applications (WMCSA '02), 2002. 3～13
4 Sun B, Wu K, Pooch W, et al. Alert Aggregation in Mobile Ad Hoc Networks. In: WiSE'03. San Diego, California, 2003
5 Huang Yi-an, Lee W. A Cooperative Intrusion Detection System for Ad Hoc Networks. In: 2003 ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN '03), 2003
6 Albers P, Camp O, Percher J-M, et al. Security in Ad Hoc Networks: a General Intrusion Detection Architecture Enhancing Trust Based Approaches. In: The 1st Intl. Workshop on Wireless Information Systems, Proc. of the 4th International Conf. on Enterprise Information Systems, 2002
7 Buttyan L, Hubaux J P. Report on a Working Session on Security in Wireless Ad Hoc Networks Mobile Computing and Communications Review, 2002, 6(4)
8 Anjum F, Subhadrabandhu D, Sarkar S. Signature based Intrusion Detection for Wireless Ad-Hoc Networks: A Comparative study of various routing protocols. In: Proc. of Vehicular Technology Conference, Wireless Security Symposium, Orlando, Florida, Oct. 2003
9 Zhang Y, Lee W. Intrusion detection in wireless ad hoc networks. In: Proc. of the sixth annual Intl. conf. on Mobile computing and networking, MOBICOM'2000, ACM Press New York, USA, 2000. 275～283
10 Marti S, Giuli T J, Lai K, et al. Mitigating routing misbehavior in mobile ad hoc networks. In: Proc. of the Sixth Annual Intl. Conf. on Mobile Computing and Networking, 2000. 255～265
11 Lippmann R, Fried D, Graf I, et al. Evaluating intrusion detection systems: The 1998 darpa online intrusion detection evaluation. In: Proceedings of the 2000 DARPA Information Survivability Conference and Exposition, January 2000
12 Chlamtac I, Conti M, Liu J. Mobile Ad Hoc Networking: Imperatives and Challenges. Ad-Hoc Networks Journal, 2003, 1(1)
13 Ilgun K, Kemmerer R A, Porras P A. Statetransition analysis: A rule-based intrusion detection approach. IEEE Transactions on Software Engineering, 1995, 21(3): 181～199
14 Zhang Y G, Lee W, Huang Yi-An. Intrusion detection techniques for mobile wireless networks. Wireless Networks, 2003
15 Sarafijanovic S, Le Boudec J Y. An Artificial Immune System for Misbehavior Detection in Mobile Ad-Hoc Networks with Virtual Thymus, Clustering, Danger Signal and Memory Detectors. In: Proceedings of ICARIS-2004, 3rd International Conference on Artificial Immune Systems, Catania, Italy, September 2004. 342～356
16 Hu Y, Perrig A, Johnson D B. Ariadne: A secure on-demand routing protocol for ad hoc networks. In: Proceedings of the Eighth Annual International Conference on Mobile Computing and Networking (MobiCom 2002), 2002
17 Zapata M G. Secure ad hoc on-demand distance vector (SAODV) routing. IETF Internet Draft, draft-guerrero-manet-saodv-00.txt, August 2001 (Work in Progress)
18 Krishna P, Vaidya N H, Chatterjee M, et al. A cluster-based approach for routing in dynamic networks. ACM SIGCOMM Computer Communication Review, 1997, 27(2): 49～64
19 Joa-Ng M, Lu I. A Peer-to-Peer zone-based two-level link state routing for mobile Ad Hoc Networks. IEEE Journal on Selected Areas in Communications, 1999, 17(8): 1415～1425
20 Vigna G, Gwalani S, Srinivasan K, et al. An Intrusion Detection Tool for AODV-based Ad hoc Wireless Networks. In: Proceedings of the Annual Annual Computer Security Applications Conference (ACSAC) Tucson, AZ December 2004
21 Deng H, Zeng Q-A, Agrawal D P. SVM-based Intrusion Detection System for Wireless Ad Hoc Networks. In: Proceedings of the IEEE Vehicular Technology Conference (VTC'03), 2003
22 Zhou L, Haas Z J. Securing ad hoc networks. IEEE Network Magazine, 1999, 13(6): 24～30

(上接第15页)

可考虑结合容错CORBA平台，或借鉴其失效恢复机制在动态配置平台中提供事务机制。动态配置技术为灵活高效的QoS管理提供了支持，包括容错和负载均衡等。如何将动态配置技术和容错、负载均衡等技术具体结合起来，实现系统的自管理和自适应，也有待研究。

参考文献

1 Shaw M, Garlan D. Software Architecture: Perspectives on an Emerging Discipline. Prentice Hall, 1996
2 Moazami-Goudarzi K. Consistency preserving dynamic reconfiguration of distributed systems: [Ph. D. thesis]. London: Imperial College, March 1999
3 Object Management Group. CORBA Component Model Specification V3.0. Formal/2002-06-65
4 Object Management Group. Common Object Request Broker Architecture: Core Specification. V3.0, formal/02-11-03, November 2002
5 Warren, Sommerville I. A model for dynamic configuration which preserves application integrity. In 3rd International Conference on Configurable Distributed Systems, 1996. 81～88
6 Hofmeister C R. Dynamic Reconfiguration of Distributed Applications: [Ph. D. Thesis]. University of Maryland, 1993
7 Kramer J, Magee J. The evolving philosophers' problem: dynamic change management. IEEE Transactions on Software Engineering, 1990, 16(11): 1293～1306
8 Bidan C, Issarny V, Saridakis T, et al. A dynamic reconfiguration service for CORBA. In: Proc IEEE International Conference on Configurable Distributed Systems, May 1998
9 Chen Xuejun. Extending RMI to Support Dynamic Reconfiguration of Distributed Systems. In: Proceeding of the 22nd International Conference on Distributed Computing Systems (ICDCS 2002)
10 Almeida J P A, van Sinderen W M, Nieuwenhuis L. Transparent Dynamic Reconfiguration for CORBA. In: Proc. of the 3rd International Symposium on Distributed Objects & Applications (DOA 2001), 2001. 17～20
11 Wermelinger W A. Specification of software architecture reconfiguration: [Ph. D. thesis]. Universidade Nova de Lisboa, September 1999
12 Object Management Group. Fault Tolerant CORBA Specification. V1.0, ptc/00-04-04, April 2000
13 Object Management Group. Online Upgrades. Draft Adopted Specification. OMG Document ptc/2002-07-01
14 Tewksbury L A, Moser L E, Melliar-Smith P M. Live upgrades of CORBA applications using object replication. In: Proc. IEEE International Conference on Software Maintenance, 2001. 488～497
15 Kon F. Automatic Configuration of Component-Based Distributed Systems: [PhD Thesis]. Department of Computer Science, University of Illinois at Urbana-Champaign, 2000
16 Minsky N H, Ungureanu V, Wang Wenhui, et al. Building Reconfiguration Primitives into the Law of a System. In: Proc. of the 3rd International Conference on Configurable Distributed Systems, 1996. 89～97
17 homepage of StarCCM on SourceForge website: http://sourceforge.net/projects/starccm/