基于信息熵的多 Agent DDoS 攻击检测*)

唐 鹏 张自力

(西南大学智能软件与软件工程重点实验室 重庆 400715)

摘 要 分布式拒绝服务攻击(DDoS)在短时间内产生大量的数据包,可以迅速耗尽网络或者主机的资源,对 Internet 的稳定性造成了巨大威胁。文中通过分析 DDoS 攻击的原理及攻击者的行为方式,划分攻击阶段,提取攻击特征,据此建立多 Agent DDoS 检测模型并分配各 Agent 的任务。模型由熵检测算法捕捉网络数据包的异常,再由 DDoS 的 Ontology 推断出攻击的具体情况。根据在 DARPA 2000 入侵检测数据集上的实验结果,模型对 DDoS 攻击的准备阶段和实施阶段有较高的识别率。

关键词 多智能代理,信息熵,本体,分布式拒绝服务

Multi-Agent DDoS Attack Detection Based on Information Entropy

TANG Peng ZHANG Zi-Li

(Key Laboratory of Intelligent Software and Soft Engineering, Southwest University, Chongqing 400715)

Abstract Distributed Denial of Service (DDoS) attacks generate enormous packets, and can easily exhaust the resource of a network or a host within a short period of time. It imposes a very serious threat to the stability of the Internet. This paper analyses the attacking rules and attacker's behaviors of DDoS, and then proposes a DDoS attack detection model based on multi-agent. The model uses the entropy detection algorithm to detect abnormal packets, and deduces details of the attack using specific DDoS Ontology. The experiment is based on DARPA 2000 Intrusion Detection Scenario Specific Data Set. The results indicate that this method can effectively detect DDoS attacks.

Keywords Multi-agent, Information entropy, Ontology, DDoS

1 引言

随着计算机网络技术的高速发展,各种网络攻击技术层出不穷,网络安全问题日益重要。其中分布式拒绝服务(Distributed Denial of Service, DDoS)攻击隐蔽性好,攻击强度大,危害广泛,难以防御。在 DDoS 攻击中,攻击者并不需要利用系统安全漏洞,只通过向受害主机产生大量的恶意数据包,就能让受害主机不能提供正常的服务[1]。有很多知名的 Web 站点,如 Yahoo, eBay 和 Amazon 等,尽管它们都有良好的安全防御措施,但由于它们和 Internet 相连接,都曾经遭到过 DDoS 攻击[2]。可以看出,DDoS 成为 Internet 稳定性的巨大威胁[3]。

为应对 DDoS 攻击,Cabrera 用一个通讯管理信息库(Management Information Base, MIB)和一个流量检测 MIB,分别用于检测攻击的准备和攻击的发生[4]。Lee 和 Shieh 根据访问 IP 的历史记录来检测入侵和过滤包[5]。Gavrilis 和 Dermatas 使用 RBF 神经网络(Radial-Basis-Function neural network)识别 DDoS 攻击[6]。Igor Kotenko 基于 Teamwork 模型和形式语法对 DDoS 攻击建立了模型并进行了模拟[7]。上述研究分别从各个角度分析了 DDoS 的特点、检测方法等,但存在如系统开销大,易产生单点失效等问题。

Agent 是能在特殊环境里持续自治工作的软件实体。它能够以灵活、智能的方式与环境进行交互,从经验中进行学习,能与其它 Agent 或者进程进行通讯。移动 Agent 还可以在网络的不同主机间移动[8]。因此,Agent 具有减小网络负载,缩短网络延迟,动态自适应,异步自治执行等优点,将 Agent 用于 DDoS 检测可以在一定程度上克服系统开销大和单点失效等问题[9]。Tao 等用 Agent 监控网络数据包源 IP 的变化检测 DDoS 攻击[10]。Ping 等通过标记数据包,再用 Agent 追踪攻击者源地址并过滤数据包[11]。Arabnia 等利用 Agent 建立了一个容易与现有网络防御系统结合的 DDoS 防御系统[12]。但在这些研究中,也存在如要求有特殊网络条件,计算量与检测率不平衡等问题。

信息熵是 Shannon 于 1948 年提出,用于解决对信息的量化度量问题。信息的随机性越大,熵也就越大。而 DDoS 攻击会使得网络数据包里某些域的不确定性发生变化,因此可以通过信息熵快速检测。Laura Feinstein 等分别使用了信息熵和 Chi-Square 的方法研究了 DDoS 的攻击和响应[13]。Keunsoo Lee 等将数据包通过信息熵分簇,通过计算它们之间的欧几里德距离检测 DDoS 攻击[14]。这些研究中,对 DDoS 的特征发掘还欠缺,也没有提出适合 DDoS 攻击状况的检测方式。针对目前方法的不足,本文提出了一种将多 Agent 技术与信息熵算法结合检测 DDoS 攻击的系统。此系统中,Agent 被指派到适合的位置,收集相应数据包中地址、端口、标志位等信息,通过计算它们的信息熵,得到网络状况随机性的描述。在此基础上,Agent 根据 DDoS 攻击特征的 Ontology 推导出攻击的状况。通过在 DARPA 2000 DDoS 入侵数据集[15]上的实验,验证了此系统有较高的检测率。

*)本项目得到重庆市自然科学基金资助。唐 鹏 硕士研究生,研究方向为人工智能,网络安全;张自力 教授,研究生导师,目前从事人工智能、基于代理的计算、混合智能系统等方面的研究。

本文第 2 节对 DDoS 攻击进行分析；第 3 节在分析的基础上提出多 Agent 系统模型；第 4 节用 DARPA 2000 DDoS 入侵数据集进行实验及分析；最后对全文进行总结，并对未来工作进行展望。

2 DDoS 攻击分析

DDoS 攻击采用分布式结构，攻击者通过控制大量的本地或异地计算机，一致对攻击目标发送大量恶意数据包以实施攻击。与传统拒绝服务攻击(DoS)相比，DDoS 更容易使受害者网络发生拥塞，让受害主机不能提供正常服务，同时也更难发现攻击者的位置。

2.1 DDoS 的攻击方式

一般情况下，发起 DDoS 攻击要经过以下 3 个步骤[1]：1) 用扫描工具，寻找网络中可用主机。对这些主机用端口扫描工具，查询主机上运行的网络服务。2) 根据上一步得到的结果，分析主机可能存在的漏洞，入侵主机，并在上面安装 DDoS 工具。3) 远程控制在上一步中安装的 DDoS 工具，对目标发起攻击。目前用于 DDoS 攻击的工具主要有 Trinity、MSTREAM、TFN2K、Trin00 等。以 Trin00 为例，它由主控程序 master 和守护程序 daemon 组成。如图 1 所示，攻击者通过控制若干 master，向更多的安装了 daemon 的主机发出攻击命令，daemon 所在的主机就会同时向受害节点发送恶意数据包，耗尽受害者网络或者主机的资源[7]。

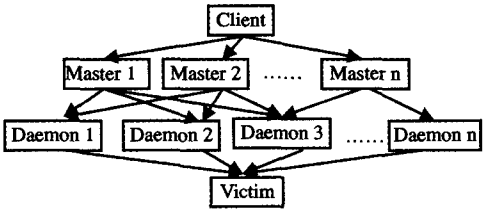

图 1 DDoS 攻击示意图

从 DDoS 攻击的三个步骤中，可以看出每个步骤都有各自的特点，最好区分开来进行检测。一般情况下，在第一步的扫描阶段，目标网络上会出现大量的同类数据包，它们的源地址仅有一个或少数几个，但目的地址和目的端口分布却很广泛，如随机变化或者递增。与此相反，在第三步的攻击实施阶段，目标网络上会出现非常多的源地址分布广泛，目标地址却很集中的数据包。

2.2 DDoS 攻击的 Ontology

Ontology 由分层的概念组成。它们描述了在不同层次上实现 DDoS 攻击的细节[7]。对于 DDoS 的 Ontology，可以分为宏观和微观两层来描述 DDoS 的细节。宏观层中的每个概念，由以下两种关系相连接：1) “Part of” 代表部分与整体关系。2) “Kind of” 代表分类的关系。它描述每一种 DDoS 攻击工具，主要使用了哪些攻击方法。图 2 展示了几种 DDoS 攻击工具(Trinity V3，MSTREAM，SHAFT，TFN2K，Trin00)的部分宏观层 Ontology。在微观层中的两种连接关系是：1) “Seq of” 表示整体和若干子序列的关系。2) “Example of” 表示示例关系。它描述各种攻击方法在数据包级的具体实现。图 3 给出了三种攻击方法(Ack flood，SMURF，LAND)的具体实现。Ontology 形式化地描述了 DDoS 攻击的实现方式，此后就可根据它来决定 Agent 的组织结构、Agent 的交互机制和角色分配等[7]。

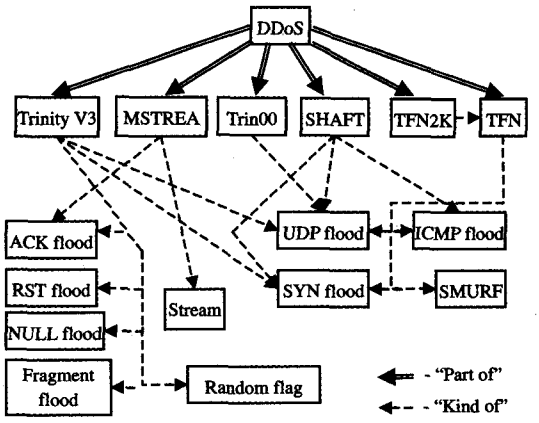

图 2 DDoS 的部分宏观层 Ontology

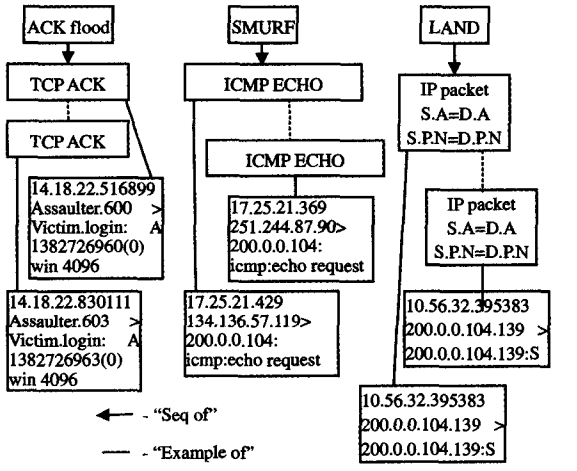

图 3 部分微观层的 Ontology

3 系统模型

从 DDoS 的攻击方式可以看出，若采用集中式的方法检测，不能够充分利用 DDoS 攻击的特点。并且发生 DDoS 攻击时，网络会发生拥塞，普通检测方式容易发生单点失效的问题。因此，本文试图通过 Agent 技术，分布式对网络各个节点进行检测。

3.1 使用 Agent 的优势

当发生 DDoS 攻击时，网络的可用性受到威胁，Agent 能充分发挥其自主性的优势。而对于熵检测算法，使用 Agent 作为检测主体有更多的优势。

1) 提高结果的准确性。一般在网络主干节点做检测时，由于数据流复杂，噪声多，使得数据包的统计规律不明显。若是在网络终端节点处做检测，又不能了解到全局性的状况，尤其是在扫描阶段，必须做全局检测。因此，本文将 Agent 分布式地放置在某些主要节点，全局检测和局部检测协同工作。

2) 提高检测效率。在分配了 Agent 的位置以后，Agent 的任务可以据此简化。位于网络主干节点的 Agent 只检测 ICMP、TCP SYN 等扫描相关的包，以发现扫描的发生。位于主机的 Agent 只检测数据包的源地址和源端口，用以发现攻击的发生。这样能降低 Agent 所在主机的负担，并提高 Agent 检测的速度。

3)更有效地处理检测出的结果。通过 Agent 的 Ontology，可以有效地推断攻击发生的状态，分析攻击者的意图。

3.2 熵检测算法

由于DDoS攻击的特殊性，攻击数据包与正常数据包很相似，常规检测方法如规则匹配、样本学习等很难发现异常。而熵检测方法对于DDoS攻击时，网络统计参数的变化却能够敏感地觉察到。基于DDoS攻击的规律，可以通过捕获网络适当位置的数据包，然后计算它们的源地址、源端口或目的地址、目的端口的熵，以此来检测出现的异常。

设信源有 n 个独立的随机变量，每一个被选中的概率为 P_i，则信息熵 H 可定义如下[16]：

$$H=-\sum_{i=1}^{n} p_i \log_2 p_i \quad (1)$$

根据式(1)，Laura Feinstein 等设计了一个滑动窗口计算熵的算法[13]。即对每一次获取的长度为 $W(W=10000)$ 的数据包，利用公式1计算出它的熵值，再向下滑动一个窗口重新计算。因此若一共截获了 m 个数据包，算法的时间复杂度为 $O(m\times n)$。

本文根据窗口中间部分数据包不会发生变动的规律，对检测算法做以下调整。设一次获取数据包序列的窗口大小为 W，调整后的信息熵算法如下：

1) 多次获取数据包中某个域(如源地址)的数据，并对其中相同的数据进行计数，设为 $c_1, c_2, \cdots, c_n$，直到 $c_1+c_2+\cdots+c_n=W$，n=序列中不同数据的个数。

2) 根据式(1)计算此序列的熵 H，其中参数 n 为 c 的个数 n，$P_i=\frac{c_i}{W}$。

3) 从上一个序列中去掉第一个包，并加入网络中第 $W+1$ 个包，更新相应的两个计数值 c。

4) 返回步骤2，计算下一个序列的熵值。

由此算法可得到信息熵的序列 H_i。由于每次循环仅更新2个域的数据，不需要进行累加，因此对于 m 个数据包，算法时间复杂度为 $O(n)$。

在DDoS攻击中，第一步和第三步数据包的统计规律比较明显，最适合用信息熵来做检测。

3.3 Agent 结构模型

根据以上分析，本文将模型中的 Agent 分为以下几类：

1) 扫描检测 Agent (SA)。它们位于主干网络上的主机，用于监听流过的数据包。在捕获到某些类型的数据包时，通过熵检测算法，计算它们地址和端口的统计规律，确定是否有扫描发生。

2) 攻击检测 Agent (DA)。它们位于提供服务的主机附近，用于监听到达此主机的数据包。通过熵检测算法，检测这些数据包的源地址和源端口数据的统计规律，根据 DDoS 微观层的 Ontology，确定攻击的具体类型。

3) 信息融合 Agent (IA)。它们首先收集 SA 提供的数据，判断可能的攻击目标；然后移动到此目标对应的 DA 所在的主机上，使得在攻击开始后网络拥挤的状态下，可以接受 DA 的数据进行分析。另外，它也是人机交互界面，并将各个阶段的情况做记录并发出警报。

模型的结构图如图4所示。假设攻击者要对 Server1 发动 DDoS 攻击，他首先要控制大量的能与 Server1 通讯的主机。因此，需要扫描网络中活动的主机，以安装 master 和 daemon 程序。当扫描主机 Host1 到 Host n 时，由于 Hub1 的网络中出现大量某种类型的源地址比较单一而目标地址或端口分布广泛的扫描数据包，SA1 可以很快发现在此网段上出现了扫描活动。之后，它将此信息告知 IA1。IA 收到消息后，对自身进行复制，然后将复制体移动到某些 DA 所在的主机，协同 DA 对后期的攻击进行检测。再假设攻击者扫描到一定数量的主机，利用各种漏洞安装了 master 或者 daemon 程序，并在某一时刻，他控制这些主机对 Server1 发起 DDoS 攻击。当攻击开始后，Hub1 的网络被堵塞。此时 DA1 将从 Server1 的网络上捕获到的数据包，通过 DDoS 的微观层 Ontology 分析，把结果告知移动到本机的 IA。IA 再根据此信息，借助之前得知的扫描信息和 DDoS 宏观层的 Ontology，分析出关于此次攻击的相关情况。

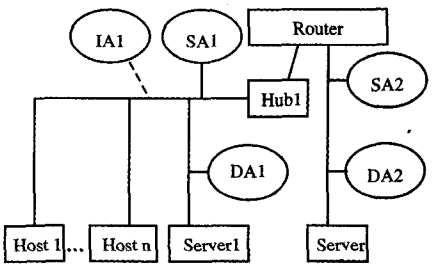

图4 模型结构图

4 实验

4.1 实验设计

本实验基于 DARPA 2000 入侵检测数据集[15]中的 DDoS 攻击数据。此数据集采样于有几十台运行各种操作系统的计算机的网络，这些计算机被路由器和防火墙分割在外部网络、DMZ 区域和内部网络中。此网络上实现了一次完整的对内部服务器的 DDoS 攻击。攻击分为以下5个步骤：

1) 从一个远程主机，用 IPsweep 工具扫描 DMZ 中的主机。

2) 探测 Solaris 主机中运行的 sadmind 后台程序。

3) 尝试通过 sadmind 的漏洞侵入主机。

4) 在侵入的主机上安装 DDoS 工具 MSTREAM。

5) 开始 DDoS 攻击。

其中第一步主要发生于 DMZ 中，由 SA 检测在此过程的异常。SA 的检测窗口 $W=20$，监视 DMZ 网络中 ICMP、TCP SYN、TCP FIN 等各种方式的扫描包。第五步主要面向网络内的主机，由 DA 检测此攻击。DA 的检测窗口 $W=10000$，发送到 IA 完成收集 SA 和 DA 检测结果，分析攻击情况的任务。

4.2 实验平台与试验系统的实现

实验采用两台 X86 计算机作为硬件平台。主机 A 为 2.6GHz 的 CPU、512M 内存，Windows 2003 系统，主机 B 为 1.7GHz，512M 内存，Windows Xp 系统。软件平台采用 IBM 的 Aglet 移动 Agent 平台[17]。

按照系统模型，根据 I. Kotenko 对 DDoS 的 Ontology 的描述[7]，在 Aglet 上实现了 SA、DA 和 IA。其中 DA 和 SA 位于主机 A，通过信息熵算法，对 DARPA 2000 DDoS 数据进行统计分析。根据微观层 Ontology 的描述，SA、DA 通过检测数据包的地址、端口、标志位等信息的熵值的变化，从数据包序列得到攻击的类型，然后 SA 和 DA 将此信息发送给位于主机 B 上的 IA。接着 IA 搜索到与此信息匹配的宏观层 Ontology 的叶节点，再从叶节点反向推导出具体状况。

4.3 实验结果及分析

在扫描阶段，SA 对 ICMP 数据包的检测情况如表1。

表 1 SA 对 DMZ 中 ICMP 扫描的熵检测结果

检测项目	正常时的平均值	扫描时的平均值
源地址的熵	1.793	0.074
目的地址的熵	1.793	4.538

数据表明，当 DMZ 的网络上出现扫描行为时，SA 能检测到 ICMP 包源地址和目的地址熵值的变化。其中源地址即扫描端地址比较固定，熵值很小。目标地址覆盖 172.16.112.X 到 172.16.115.X 的大片区域，因此熵值相对较高。由于此次攻击是直接寻找 Solaris 主机 sadmind 开放的端口，因此未进行端口扫描。

表 2 是未对协议类型进行区分的情况下，熵的检测情况。可以看出，区分后的结果优于不加区分的结果。

表 2 DMZ 中扫描的全部数据熵检测结果

检测项目	正常时的平均值	扫描时的平均值
源地址的熵	1.476	0.794
目的地址的熵	1.711	3.787

在攻击阶段，DA 对被攻击主机 131.84.1.31 的检测结果如表 3。可以比较出，在正常状态和受攻击状态，检测到的源端口和源地址熵值差异很大，表明 DA 对于 DDoS 攻击有较强的识别能力。同时，DA 检测到了 ack 和 win 数值的异常，向 IA 告知检测到了 ACK Flood。IA 通过收集这一异常的详细数据，发现产生这一原因的是网络中大量的特殊 UDP 包，其 win 大小为 16384，ack 数值为 0。IA 根据 Ontology 可以推断出，攻击的工具为 MSTREAM。

表 3 DA 对 IP 为 131.84.1.31 的主机的熵检测的结果

检测项目	正常时的平均值	攻击时的平均值
源地址的熵	2.123	12.297
源端口的熵	2.877	12.301
ack 值的熵	7.773	1.279
win 值的熵	2.263	0.446

图 5 是 DA 检测的各个域的熵变化情况，攻击发生在最末尾。可以看出，在发生 MSTREAM 的 DDoS 攻击时，这四个域熵的变化非常明显。

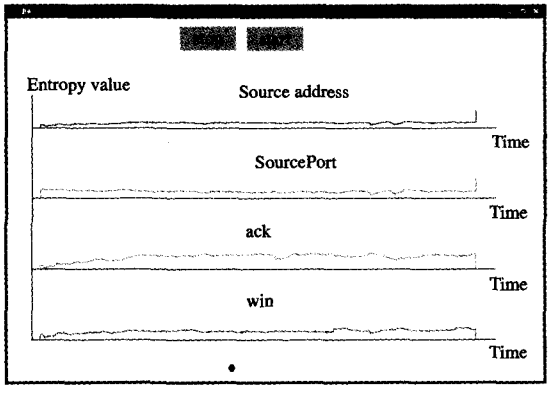

图 5 DA 检测的各个域的熵状况

表 4 是不区分主机的情况下检测到的熵值。对比表 3 可以看出，因为多了其它主机通讯的干扰，检测效果略差于单独对某一主机的检测。

表 4 对全部数据进行熵检测的结果

检测项目	正常时的平均值	攻击时的平均值
源地址的熵	3.590	11.938
源端口的熵	5.153	12.004

结论 本文基于 Agent 技术，利用信息熵算法对 DDoS 攻击进行检测。在结合 Agent 和信息熵检测算法优势的基础上，提出了一个检测系统的模型。并通过 IBM 的 Aglet 平台实现此模型，最后在 DARPA 2000 数据集上，对模型进行了验证。

在引入 Agent 技术后，熵检测算法对 DDoS 攻击有更好的识别效果。由于实验条件的限制，不能对更多类型的 DDoS 攻击进行测试。目前扫描工具和 DDoS 攻击工具种类很多，本文仅对实验中出现的 IPsweep 和 MSTREAM 进行了深入分析，并没有对各种攻击手段建立详细的 Ontology 模型，这方面的工作还有待进一步研究。

参 考 文 献

1 Chang R K C. Defending against flooding-based distributed denial-of-service attacks: a tutorial. IEEE Communication Magazine, 2002,40 (10): 42～51
2 EBay W M, Buy A. com hit by attacks. IDG News Service, 2000
3 David J, et al. Results of the distributed-systems intruder tools workshop. Published at the CERT Coordination Center Software Engineering Institute Carnegie Mellon University Pittsburgh, Nov. 1999
4 Cabrera J B D, et al. Proactive detection of distributed denial of service attacks using MIB traffic variables-A feasibility study. In: The seventh IEEE/IFIP International Symposium on Integrated Network Management Proceeding, May 2001. 609～622
5 Lee F, Shieh S. Defending against spoofed DDoS attacks with path fingerprint. Computers and Security, 2005, 24(7): 571～586
6 Gavrilis D, Dermatas E. Real-time detection of distributed denial-of-service attacks using RBF networks and statistical features. Computer Network, 2005, 48 (2): 235～245
7 Kotenko I. Teamwork of Hackers-Agents: Modeling and simulation of coordinated distributed attacks on computer networks. Multi-Agent Systems and Applications III. In: Proceedings of 3rd International Central and Eastern European Conference on Multi-Agent Systems, 2003, 2691: 464～474
8 Bradshaw M. An introduction to software agents. Software Agents, chapter 1. AAAI Press/The MIT Press, 1997
9 Jansen W, et al. Applying mobile agents to intrusion detection and response: [NIST Interim Report (IR)－6416]. Oct. 1999
10 Peng T, Leckie C, Ramamohanarao K. Detecting distributed denial of service attacks by sharing distributed beliefs. Information Security and Privacy. Wollongong, 2003. 9～11
11 Ping S Y, Moonchuen L. IP traceback marking scheme based packets filtering mechanism. In: IEEE International Workshop on IP Operations and Management Beijing, Oct. 2004
12 Arabnia H R, Joshua R. Mobile network end host remote monitoring agent - Mobile agents based approach for detection and prevention of distributed denial of services attacks. In: ICOMP'05 Proceedings of the 2005 International Conference on Internet Computing, 2005. 164～173
13 Feinstein L, et al. Statistical approaches to DDoS attack detection and response. In: DARPA Information Survivability Conference and Exposition, 2003, 1: 303～ 314
14 Lee K, et al. DDoS attack detection method using cluster analysis. Expert Systems with Applications, Feb. 2007
15 Lincoln Laboratory. 2000 DARPA intrusion detection scenario specific. http://www.ll.mit.edu/IST/ideval/data/2000/ LLS_DDOS_1.0.html, 2000
16 MceLiece R J. 信息论与编码理论. 电子工业出版社, 2004
17 Tokyo Research Laboratory. Aglets. http://www.research.ibm.com/trl/aglets/index.html, Mar. 2002