文章编号:1671 - 6833(2007)02 - 0077 - 04

# 基于移动 Ad Hoc 网络的分布式拒绝服务攻击检测算法

张迎宾, 史浩山, 卢选民

(西北工业大学 电子信息学院,陕西 西安 710072)

**摘 要**:提出了一种适用于移动 Ad Hoc 网络的分布式拒绝服务攻击(DDoS)检测算法,对基于序列分析的 Kolmogorov 复杂度估值算法做了改进.新算法对网络中的流进行相关分析,并计算序列特征集的复杂度,通过对复杂度分析来检测分布式拒绝服务攻击.仿真实验结果表明,本算法的误检率、检测时间等性能要好于传统的复杂度估计算法.

**关键词**:分布式拒绝服务攻击;自组网络;Kolmogorov 复杂度

**中图分类号**:TN918.91 **文献标识码**:A

## 0 引言

移动 Ad Hoc 网络是一种新型的无线通信网络,节点不依赖于任何固定的基础设施和管理中心,节点的无线通信范围是有限的,在此范围内的节点可以直接通信,对在无线通信范围外的节点,则需要中间节点充当路由器对数据包进行转发.Ad Hoc 网络具备自组织性,网络拓扑结构为高度动态,具有资源有限,通信多跳,网络安全脆弱等特点,主要用于军事战术通信、应急通信、协同移动通信、无线接入系统和传感器网络.移动 Ad Hoc 网络通常比固定网络更容易受到物理安全攻击,也更易于遭受被动窃听、主动入侵、拒绝服务、剥夺"睡眠"、伪造等各种网络攻击[1-4].

Ad Hoc 网络的拓扑和成员经常改变,节点间的信任关系也是经常变化的,网络中不存在值得信任的第三方,使得分布式拒绝服务攻击更容易实施,自组网的安全机制必须能够适应网络拓扑结构的动态变化.节点在敌方环境(如战场)漫游时,缺乏相应的物理保护,具有不可忽视的危险性,其被敌人俘获的机率相对较高.因此不仅要考虑网络外部的恶意攻击,还需要考虑由网络内部被俘获节点发起的攻击.如当某些节点被检测到成为受控节点时,就应该解除对它们的信任,因此在节点间建立信任关系成为 Ad Hoc 网络安全问题的核心.

## 1 移动 Ad Hoc 网络中的 DDoS

移动 Ad Hoc 网络中,由于网络规模、节点能力和带宽的限制,攻击节点往往难以在短时间内发送过多的请求,因而多采用分布式拒绝服务攻击(DDoS)的方式[5].在这些攻击中,为提高攻击的成功率,攻击节点需要入侵或胁持大量的傀儡节点,攻击者远程控制傀儡节点操纵整个攻击过程.例如,攻击节点可以对网络进行探测扫描以寻找可入侵的节点,入侵有安全漏洞的节点并获取系统控制权;或者在被胁迫或被入侵节点中安装攻击程序,利用被胁迫节点继续进行扫描和攻击,这样发起攻击的节点可以采用欺骗技术,以逃避追查.

移动 Ad Hoc 网络的安全弱点可以从 Kolmogorov 复杂度的角度进行分析,尽管一个攻击节点完成拒绝服务攻击的任务非常容易,而系统在一个信息系统中测量和跟踪 Kolmogorov 复杂度量度却非常困难.本文作者提出一种简单有效的、计算量较小的算法,对来自不同节点的码流序列的复杂度进行了估值和分析,计算 Kolmogorov 复杂度差分.该算法抵御 DDoS 的性能与对序列外在复杂度估值的准确性有关.

## 2 检测算法

笔者提出的 DDoS 攻击检测算法利用了 Kol-

**收稿日期**:2007 - 01 - 04;**修订日期**:2007 - 03 - 23

**基金项目**:教育部博士点基金项目(20050699037);西北工业大学"英才计划"基金项目(521020101 - 04XD0108)

**作者简介**:张迎宾(1972 - ),男,河南开封人,西北工业大学博士研究生,主要从事移动通信以及自组网络方面的研究.

mogorov 复杂度的基本理论,对于两个随机序列,有

$$K(XY) \leqslant K(X) + K(Y) + c \qquad (1)$$

这里,$K(X)$ 和 $K(Y)$ 表示相应序列的复杂度,是一个常数;$K(XY)$ 是串连序列的联合复杂度;$C$ 为经验值,是一个常数.

在 DDoS 检测的过程中,不等式(1)被用来区分多节点协同的拒绝服务攻击和流量过载的差异. 假定一个攻击节点使用大量相似的包来(类型、目标地址、执行模式)执行攻击,这些包来源于不同的节点但是目的节点相同,在流量模式上就会具备很多的相似性. 基于 Kolmogorov 复杂度的检测算法可以方便地识别这样的模式,对被怀疑的数据流进一步进行复杂度检测,来判定是一次攻击而非传输过载.

复杂度的差分定义为单个数据流累积的复杂度与序列联合形成一个单一数据流后的总复杂度的差值. 定时对节点数据流进行采样,对样本求复杂度的差分. 定义数据流 $x_1, x_2, \cdots, x_n$ 的复杂度分别为 $K(x_1), K(x_2), \cdots, K(x_n)$,则复杂度的差分计算如下:

$$D = \sum_{i=1}^{n} K(x_i) - K(x_1 x_2 \cdots x_n) \qquad (2)$$

其中 $K(x_1 x_2 \cdots x_n)$ 是数据包连接在一起后的复杂度. 如果数据包 $x_1, x_2, \cdots\cdots, x_n$ 是完全随机的,$K(x_1 x_2 \cdots x_n)$ 将等于单个复杂度之和,复杂度的差分将为零. 然而,如果数据包是高度相关的,一些模式出现在其连接后的包中,则连接包可以由一个小的程序表示,因此其复杂度 $K(x_1 x_2 \cdots x_n)$ 将小于累积复杂度. 如果一个数据流的复杂度差分大于一个预设的门限,数据流被标示为受怀疑,所采集到的样本被提交给运行于节点上的一个本地检测器.

本地节点检测进程收到来自不同的受怀疑数据流的所有样本,使用相同的复杂度差分计算对所有样本进行关联. 如果只有一个受怀疑的数据流,无须进行关联操作. 如果复杂度差分仍然超过门限,所有受怀疑的数据流(包括单一数据流的情况)被提交给运行于本地网络域的区域主节点之上的区域检测进程. 区域检测进程依次对来自于本地检测进程的数据流进行关联操作,采用本地检测所采用的相同方法,来决定攻击是本地的还是分布式的,区域节点进行层级协作来检测网络中的 DDoS 攻击.

## 3 复杂度估计

$K(x)$ 估值与评估序列结构的算法有关. 作者采用的是一种基于序列自相关功率谱密度的方法,强调的是获得序列 $K(x)$ 信息的能力.

序列的复杂度量度与序列的无环自相关特性有关,给定一个 $n$ 比特二进制序列 $S, S = \{s(i)\}$, $0 \leqslant i < n$. 对于任意 $i$ 值,$s(i) \ni \{\pm 1\}$,定义无环自相关 $R, R = \{r(i)\}, 0 \leqslant i < n$,这里有

$$r(i) = \sum_{j=0}^{n-i-1} s(j)s(i+j) \qquad (3)$$

从 $R$ 计算序列的非负功率譜密度 $\Phi_i$,乘以 $R$ 的傅立叶变换乘以其共轭:

$$\Phi_i = \int_{-\infty}^{\infty} R(\tau) e^{-j\omega\tau} d\tau \qquad (4)$$

于是二进制序列的 Kolmogorov 复杂度 $K$ 可以由 $\Phi_i$ 计算:

$$K = \frac{1}{\| \Phi_i \|} \sum_i \Phi_i \log \Phi_i \qquad (5)$$

该序列存在一个自相关,其功率谱旁瓣幅度很低,对局部时间模糊有较好的抵御能力,这样一个自相关函数的傅立叶变换近似带宽受限的白噪声.

序列自相关的功率譜密度和序列的复杂度是有关联的,它具备衡量 $K(x)$ 增加或减少趋势的能力.

## 4 仿真结果与分析

为了评价提出的方案,在 ns-2 网络模拟器下实施笔者的检测算法. 节点运动遵循 CMU Monarch 扩展的随机点运动模型. 表 1 中为详细的仿真参数. DDoS 攻击的实质上是在某一时间间隔内持续的过载. 仿真实验的目标是判定两种不同方法的有效性,即在存在背景流量情况下,区分和识别攻击流的复杂度. 笔者将提出的算法同用于 DDoS 探测的基于简单熵的算法[6]进行了比较,发现笔者的算法大大优于简单熵方法.

**表 1 仿真参数**

**Tab. 1 Simulation parameter**

| | |
|---|---|
| 移动节点数量 | 100 个 |
| Ad Hoc 网络面积 | 1 000 m × 1 000 m |
| 仿真时间 | 300 s |
| 节点暂停时间 | 1 s |
| 节点最高速度 | 10 m/s |

仿真实验在两种情况下进行,一种是只有攻击源打开,只有攻击节点发送数据;另一种是除了攻击节点发送数据包,其它节点也正常开启,发送正常数据包作为背景数据.

图 1 由一个拓扑结构分布的移动节点集合构成. 对于 100 个节点,存在 1 个攻击节点 $A$ 的情

况，该节点在仿真过程中可以随机控制 10 个其它节点 $A_1$，…，$A_{10}$进行协同攻击. 节点 $A_i$ 连续生成由随机产生的数据包构成的数据流，其目的地为节点 $D$. 由于该数据流产生的负载足够高，在节点 $C_i$ 处注册为受怀疑流，即一个数据流其复杂度差分超过门限值，由这个流所引发的负载在整个实验中保持恒定. 节点 $A_2$ 受节点 $A$ 控制生成攻击流. 由攻击流引发的负载变化以决定算法的性能.

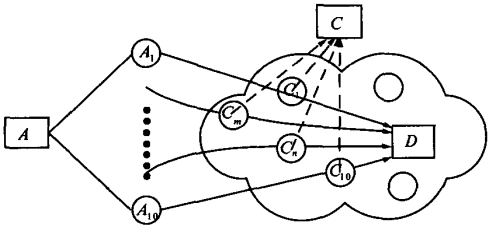


**图 1　DDoS 攻击检测的拓扑示意图**

**Fig. 1　Topology of DDoS attack detection**

仿真时间共计 300S，攻击节点控制 10 个其它节点参与进行协同攻击，共计发出大约165 000 个攻击包. 仿真实验需要在节点的不同特征序列长度下，两种不同算法在不同的参与攻击的节点数量下，对下列参数进行评估：成功检测出 DDoS 攻击概率、虚警概率，成功检测出 DDoS 攻击所需的时间. 本文的算法需要对数据序列的整个内容进行评估，我们从仿真实验中获得良好的结果

### 4.1　DDoS 攻击检测成功率

图 2 显示了基于简单熵的复杂度方法和笔者提出的基于功率谱密度的复杂度方法在检测 DDoS 攻击的成功率上的性能比较. 图中所使用的符号含义如下：Algorithm1 表示基于简单熵方法的复杂度计算方法；Algorithm2 表示基于功率谱模式的复杂度计算方法；$L$ 表示序列特征长度. 由图 2 可看出，基于简单熵的方法不能在复杂模式下很好的检测出一个 DDoS 攻击，对 DDoS 攻击的检全率最高只有 70% ~80%. 当背景数据源和攻击源同时在网络中发送时，运行于节点 $C_i$ 上的检测算法对于途经的数据流进行复杂度计算. 由于来自同一个节点源的攻击序列的相似性必定导致基于简单熵方法的结果相似性很高，无论在序列特征长度大或小的情况下，基于简单熵的复杂度方法的性能是达不到理想的结果的，对一个特征序列长度为 20 的攻击流的检全率只能达到 40% 左右. 而本文提出的基于功率谱密度的复杂度方法很好地解决了这一问题，尽管来自不同攻击节点的攻击源可能具备共同的或相似的序列特征，但基于功率谱密度的方法成功地解决了对攻击流的识别问题，即使在复杂的情况下，检测的成功率也达到了 80% 以上.

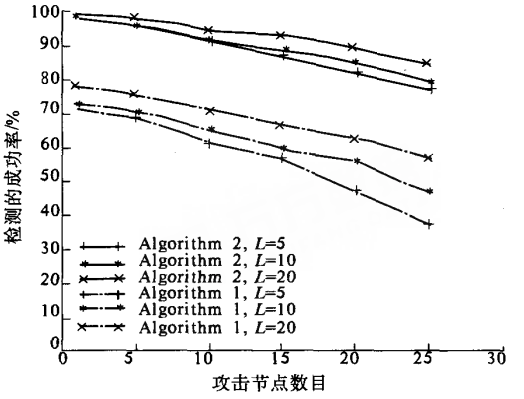


**图 2　检测 DDoS 的成功率**

**Fig. 2　Success ratio of DDoS detection**

### 4.2　错误检测的概率

图 3 给出了在不同情况下，两种不同复杂度计算方法对 DDoS 攻击检测的错误概率. 从图 3 可以看出，由于基于简单熵的复杂度方法的结果具有相似性，导致在很多情况下无法区分来自不同攻击源和数据源的攻击序列特性，大大降低了检测的准确度. 基于功率谱密度的复杂度计算方法在真正的组合流中分离虚假攻击的精确度更高，因为它可以识别攻击流和数据流的不同序列特征模式.

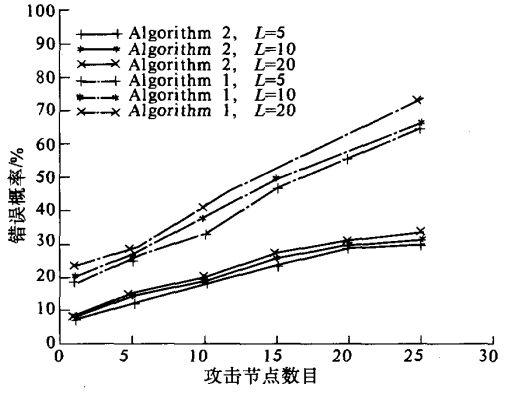


**图 3　错误检测 DDoS 的概率**

**Fig. 3　False ratio of DDoS detection**

### 4.3　响应时间

DDoS 检测要求系统能够实时响应各目标的状态变化，要求算法时延和通信时延达到最小，对于移动 Ad Hoc 网络，节点间通信时延占据了系统响应时间的大部分，因此，减少通信时延是我们的首要目标. 增大节点发射功率可以减小网络直径，减小链路跳数通常意味着减少通信时延，移动 Ad Hoc 网络的

传输时延必然受到网络直径 $D$ 的影响.放宽对网络直径的限制可以确保减小网络时延,增加覆盖密度可以减少链路的最大跳数,减小网络直径.

如图4所示,本文作者所提出的算法在检测攻击所需的时间上并不占优势,与传统的简单熵统计算法比较,本文作者所提出的算法的检测时间增加了20%甚至更多.

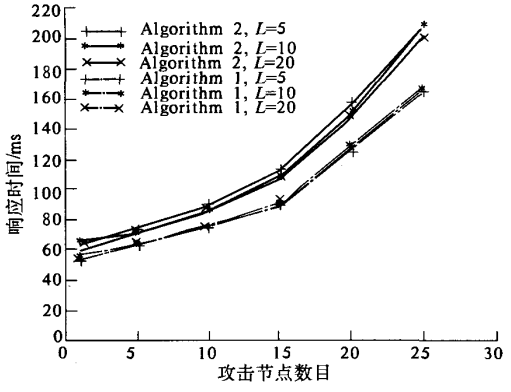


**图4 DDoS检测所需时间**

**Fig.4 Time required for DDoS detection**

## 5 结论

作者提出了移动 Ad Hoc 网络中一种分布式拒绝服务攻击检测算法,对 Kolmogrov 复杂度的估值、表示方式进行了深入的研究,并在 DDoS 攻击探测问题上作为一个模型应用.显然,Kolmogrov 复杂度估值是鉴别攻击流之间关联关系的关键所在.仿真表明,基于序列功率谱密度的估值是衡量 Kolmogrov 复杂度的有效的量度.今后需要进一步深入的研究工作是对更多的智能 DDoS 探测算法进行比较以确定其性能,并拓展为一种利用 Kolmogrov 复杂度理论来检测移动 Ad Hoc 网络中 DDOS 攻击,并跟踪和识别攻击源的有效方法.

## 参考文献:

[1] LAKSHMINARAYANAN K, ADKINS D, PERRIG A, et al. Taming IP packet flooding attacks[J]. Computer Communication Review, 2004, 34 (1):45 - 50.

[2] YAAR A, PERRIG A, SONG D. SIFF: a stateless Internet flow filter to mitigate DDoS flooding attacks [C]//IEEE Symposium on Security and Privacy. New York:IEEE, 2004: 130 - 143.

[3] YU W, LIU K J R. Defense against injecting traffic attacks in cooperative ad hoc networks [C]//IEEE Globecom. New York:IEEE,2005: 1737 - 1741.

[4] GU Q J, LIU P, ZHU S C, et al. Defending against packet injection attacks in unreliable ad hoc networks [C]//IEEE Globecom. New York:IEEE,2005: 1837 - 1841.

[5] REN W, YEUNG D Y, JIN H, et al. Pulsing RoQ DDoS attack and defense scheme in mobile Ad Hoc networks[J]. International Journal of Network Security, 2007,4(2):227 - 234.

[6] KULKARNI A B, BUSH S F, EVANS S C. Detecting distributed denial - of - service attacks using kolmogorov complexity metrics[R]. GE CRD: Technical Report 2001CRD176, Fairfield:GE,2001.

## A Detecting Algorithm for Distributed DoS Attacks in Wireless Ad Hoc Networks

ZHANG Ying - bin, SHI Hao - shan, LU Xuan - min

(College of Electronic and Information, Northwestern Ploytechnical University, Xi'an 710072, China)

**Abstract**: This paper presents an algorithm to detect distributed denial of service (DDoS) attacks in wireless ad hoc networks that is based on improvements to Kolmogorov complexity algorithm of sequence analysis. The proposed algorithm correlates traffic flows in the network and computes the complexity of sequence attribute set, and then detects any possible distributed denial - of - service attacks through complexity analysis. Simulation results show that the algorithm presented in this paper performs better than common Kolmogorov complexity measuring approaches in detection of DDoS attacks. It can reduce the false detecting ratio and responding time, and can increase the success ration of detection obviously.

**Key words**: distributed DoS; ad hoc network; kolmogorov complexity