第 35 卷 第 5 期 计 算 机 工 程 2009 年 3 月
Vol.35 No.5 Computer Engineering March 2009
·博士论文· 文章编号：1000—3428(2009)05—0004—03 文献标识码：A 中图分类号：TN915.08

移动 Ad Hoc 网络中 DoS 攻击的建模与仿真

马 涛，单 洪
(解放军电子工程学院网络工程系，合肥 230037)

摘 要：研究一种具有随机开关特性的移动 Ad Hoc 网络拒绝服务(DoS)攻击模型。为在仿真场景中反映实际移动 Ad Hoc 网络的流量特性，讨论自相似流量的 Qualnet 生成方法。对 3 种不同网络流量模型下的数据注入 DoS 攻击进行仿真与攻击分析，仿真结果表明，具有开关特性的 DoS 攻击能破坏网络节点、降低网络性能，并可有效地节省能量、避免检测。

关键词：移动 Ad Hoc 网络；DoS 攻击；自相似流量

Modeling and Simulation of DoS Attacks in Mobile Ad Hoc Network

MA Tao, SHAN Hong
(Network Engineering Department, PLA Electronic Engineering Institute, Hefei 230037)

【Abstract】 This paper studies the Denial of Service(DoS) attacks modeling with an on-off characteristic in mobile Ad Hoc network. In order to reflect the realistic mobile Ad Hoc network traffic in the scenarios, building method of self-similar traffic in Qualnet is discussed. DoS attacks by injected with data are simulated and analyzed under three different network traffic models. Simulation results show DoS attacks with the on-off characteristic can destroy the network nodes, reduce the network performance, and can also save the energy and undetected.

【Key words】 mobile Ad Hoc network; DoS attacks; self-similar traffic

1 概述

移动 Ad Hoc 网络的广泛应用已经涉及到远程传感、监视和通信领域[1]。无线移动 Ad Hoc 网络允许产生自组织骨干网，通过动态的路由协议，允许节点适应周围环境的改变，当一个链路被破坏和一个路由失败时，路由协议会尝试发现另一个路径，在无基础设施和无需人为干涉的情况下能够通信。但移动 Ad Hoc 网络的优点也就是其脆弱点[2]，因为缺乏基础构造、数据无线传输、网络拓扑结构随节点移动而动态变化，使其很容易中途被截获和攻击。对移动 Ad Hoc 网络的攻击已有大量研究，但大都集中在路由层协议攻击，而且仿真评估都基于传统的 CBR 或 Poisson 流量模型。研究已经证明[3]，传统的 CBR 或 Poisson 流量模型并不能反映具有自相似特性的实际突发网络流量。因此，攻击效果评估应该建立在能反映真实的网络流量特征的模型上。

2 移动 Ad Hoc 网络中的拒绝服务攻击分析

针对移动 Ad Hoc 网络攻击的主要目标为网络的物理层、链路层和路由层。现有攻击方式研究主要以路由层攻击为主[1, 3]，例如黑洞攻击、虫洞攻击和路由欺骗等。其实，对物理层和链路层的拒绝服务攻击往往会对路由层产生很大的影响，例如物理层的干扰和链路层的数据注入，都会造成链路的中断和延时的增加，导致路由层必须重新建立连接。物理层和链路层的拒绝服务攻击通常都采用连续的攻击方式，通过连续的数据注入以获得对目标节点的信道占用和数据碰撞。如果多个节点被攻击，会造成整个网络的性能下降。

然而，这样的攻击模型也有不足之处。它容易暴露攻击和攻击者，而且是以消耗电池能量来实现攻击。持续的开状态攻击将在一个稳定的频率下耗尽电池能量，限制了攻击持续时间。为克服上述缺点，攻击者通常采用随机开关攻击的方式，但是并没有对随机开关的时间进行建模分析，本文对具体的攻击建模进行分析。

设 Ad Hoc 网络中的一个无线节点 n，$t_{s,n}^{A}$ 是当攻击 A 作用到节点 n 上连续时间内的离散时间。此外，用连续随机变量 $T_{s,n}^{A}$ 描述 $t_{s,n}^{A}$。

定义一个攻击周期为一个开攻击时间紧跟一个关攻击时间。开攻击时间的长度通过随机变量 $A_n^{\text{on}} \geq 0$ 表示，关攻击时间的长度通过随机变量 $A_n^{\text{off}} \geq 0$ 表示，则攻击周期的长度通过随机变量 L 定义为：$L = A_n^{\text{on}} + A_n^{\text{off}}$。

攻击 A 对节点 n 攻击一段时间表示为 $t_{\varepsilon,n}^{A}$，随机变量为 $T_{\varepsilon,n}^{A}$，则 $T_{\varepsilon,n}^{A} = T_{s,n}^{A} + (K \times L)$，其中，$K$ 是一个离散随机变量，$K \geq 0$，代表攻击周期数。

一个攻击周期模型如图 1 所示。

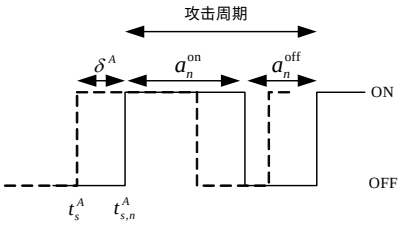

图 1 攻击周期模型

其中，$T_{s,n}^{A}$ 为攻击 A 对节点 n 的开始时间的概率分布；A_n^{on} 为开周期的长度的概率分布；A_n^{off} 为关周期的长度的概率分布；K 为攻击周期的数目的概率分布；概率 p 为一些节点 n 是一

基金项目：国家部委基金资助项目
作者简介：马 涛(1979－)，男，博士研究生，主研方向：无线网络，信息安全；单 洪，教授、博士
收稿日期：2008-07-13 **E-mail：**bbmtao@sohu.com

个攻击者的概率；Δ^A 为攻击抖动的概率分布。

上述的各种随机变量可采用不同的概率分布，例如均匀分布、指数(exponential)分布和 Pareto 分布等。

3 自相似流量

自相似过程是基于连续时间变量的直接尺度变换，由于网络流量的分析已经被严格地限制为离散时间的二阶或近似二阶自相似过程，因此本文给出离散时间序列的自相似定义。

假定离散时间随机过程 $X=\{x_t, t=0,1,\cdots\}$，是一个广义平稳随机过程，其均值为 u，方差为 σ^2，自相关函数为 $r(k)$，$k\geq 0$。$r(k)$满足：当 $k\to\infty$ 时 $r(k)\sim k^{-\beta}L_1(k)$，其中，$0<\beta<1$，$L_1$ 是慢变函数，即对所有 $x>0$，$\lim_{t\to\infty} L_1(tx)/L_1(t)=1$。

对 m=0, 1,…，令 $X^{(m)}=\{x_t^m, t=0,1,\cdots\}$ 表示由 X 得到的 m 重聚集时间序列，它可以表达为

$$x_t^m=\frac{1}{m}\sum_{i=tm-m+1}^{tm} x_i$$

对每个 m，x_t^m 为一个协方差平稳的随机过程。$X^{(m)}$也是均值为 u 的、自相关函数为 $r^{(m)}(k)$的广义平稳随机过程。

如果对所有 m=0, 1,…，有

$$Var(X^{(m)})=\sigma^2 m^{-\beta},\quad r^{(m)}(k)=r(k),\quad k\geq 0$$

则 X 被称为有自相似系数 $H=1-\beta/2$ 的严格二阶自相似(exactly second order self-similar)过程。

如果对所有足够大的 k，有

$$Var(X^{(m)})=\sigma^2 m^{-\beta},\quad r^{(m)}(k)\sim r(k),\quad m\to\infty$$

则 X 被称作有自相似系数 $H=1-\beta/2$ 的近似二阶自相似(asymptotically second order self-similar)过程。

在仿真环境下，自相似流量可以通过多个 on/off 源叠加生成，on/off 的停留时间服从重尾分布[4]。

4 DoS 攻击仿真分析

DoS 攻击具有开关特性，在开状态时，攻击节点连续向目标节点发送大量数据数据包，在关状态时停止发送。采用 Qualnet 网络仿真工具来实现攻击场景的建模与仿真。Qualnet 是 GloMoSim 的商业版，运行于 Parsec 并行可扩展离散事件仿真环境，非常适合对大型无线移动网络进行仿真[5-6]。

(1)攻击参数

具体参数设置如下：

1)单个攻击节点开始时间 $T_{s,n}^A$ 是确定的，等于 5 s，在有多个攻击节点时，满足[1 s, 10 s]之间的均匀分布；

2) A_n^{on} 开周期是一个确定值，A_n^{off} 关周期的长度满足 Pareto 分布，攻击周期的值应连续且比一次交互的时间要短；

3)攻击周期数目 K 的选择包含在仿真时间内；

4)攻击概率 p 的取值为 1；

5)攻击抖动 Δ^A 是一个 uniform 随机变量 $U[a, b]$，1 个攻击者，Δ^A=0；10 个攻击者 Δ^A 服从 U[0, 10]；15 个攻击者 Δ^A 服从 U[0, 15]。

(2)自相似流量的生成

Qualnet 提供以下 3 种方式的流量生成模型。

1)CBR：连续比特率流量模型。按一个确定的速率产生数据，分组的长度为一常数值。

2)Exponential：按指数 on/off 分布产生数据。在 on 状态，分组以一定的速率发送；在 off 状态，分组停止发送。on 和 off 这 2 种状态的时间都符合指数分布。

3)Pareto：按 Pareto on/off 分布产生数据。除了 on 和 off 这 2 种状态的时间都符合 Pareto 分布之外，其他与指数 on/off 分布相同，Pareto 分布是一种重尾分布，多个 Pareto on/off 分布的叠加可产生自相似流量。

本文的自相似流量模型通过大约 20 个通信源节点产生，这些源节点集中将更多的数据流量汇到模拟目标来促使突发流量生成，因此，可产生自相似流量。具体各个流量模型的参数配置如表 1 所示。

表 1 流量模型的具体参数配置

	流量模型	分布函数	参数值
CBR 参数	Packet size	Constant	512 Byte
	Holding time	Constant	600 s
Exponential 参数	Start time	Exponential	5 s
	Holding time	Constant	600 s
	Date size	Exponential	1 000 Byte
	Data interval	Exponential	500 ms
	Gen probability	[0, 1]	1
Pareto 参数	Start time	Pareto	[1 s, 10 s]
	Holding time	Constant	600 s
	Date size	Pareto	[1 000, 2 000] Byte
	Data interval	Pareto	[100 ms, 10 s]
	Alpha	[1, 2]	1.5
	Gen probability	[0, 1]	1

(3)场景及节点模型参数设置

在 Qualnet 下的建立场景，主要场景及节点模型参数设置如表 2 所示。

表 2 场景及节点模型协议参数设置

参数	值	参数	值
仿真区域	1 500 m×1000 m	节点设置	36
数据传输速率	2 Mb/s	发射距离	376 m
信号衰减模型	TWO-RAY	PHY 协议	PHY-ABSTRACT
MAC 协议	IEEE802.11 DCF	路由协议	AODV
业务类型	不同的流量模型	仿真时间	10 min

(4)攻击效果评估指标

为了能对比攻击效果，本文选用 2 种性能指标：1)数据分组传递率(*PDR*)是成功传递到目的端的分组数与发送端成功发射的数据分组数之比。*PDR* 越小，攻击效果越好，反之则越差。2)平均端到端时延(*AED*)是从源节点成功到达目的节点的所有数据分组的端到端时延的平均值。*AED* 越大，攻击效果越好，反之则越差。

(5)仿真结果分析

1)场景 1：传统的攻击仿真场景，移动 Ad Hoc 网络流量和攻击流量均由 CBR 流量模型生成。图 2 和图 3 分别给出了攻击仿真后攻击节点数与数据分组传递率和平均端到端时延的关系。

从图 2 可以看出，数据分组传递率随着攻击节点数的增加而下降。发送数据包时间间隔增大时，数据分组转发率明显下降，说明攻击流量增加，增加了数据包的碰撞率。图 3 显示被攻击节点的平均端到端时延随着攻击节点数的增加而增加。当发送数据包时间间隔增大时，平均端到端的时延也有所增加。

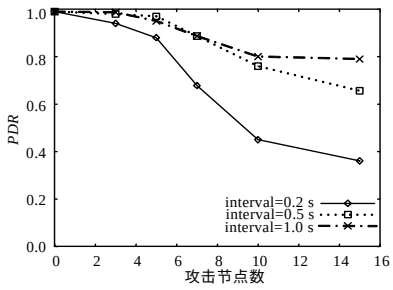

图 2 CBR 流量下 *PDR* 与攻击节点数关系

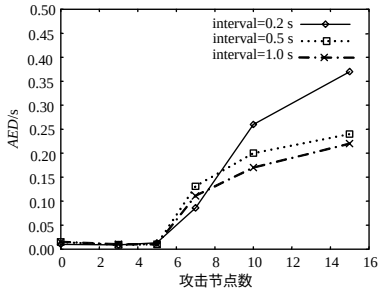

图 3　CBR 流量下 *AED* 与攻击节点数关系

2)场景 2：移动 Ad Hoc 网络流量由满足 Perato 分布的 on/off 模型叠加生成，攻击流量具有开关特性。从图 4 可以看出数据分组传递率随着干扰节点数的增加而下降。当攻击节点在 on 状态发送的数据包数增加时，数据分组传递率有所下降。图 5 显示被干扰节点的平均端到端的时延随着干扰节点数的增加而增加，当 on 状态发送的数据包数增加时，平均端到端的时延也有所增加。

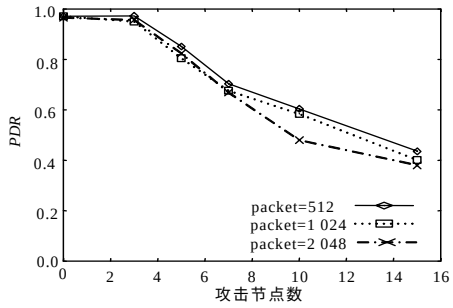

图 4　自相似流量下 PDR 与攻击节点数关系

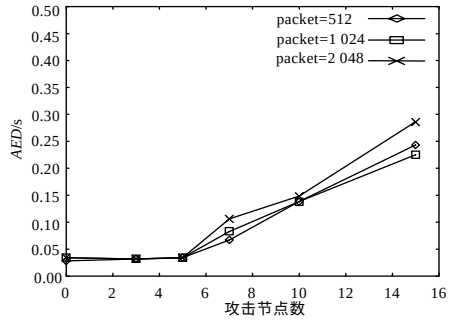

图 5　自相似流量下 *AED* 与攻击节点数关系

3)场景 3 移动 Ad Hoc 网络流量由满足指数分布的 on/off 模型叠加生成。在该场景中，攻击流量的产生方式不变。从图 6 可以看出，数据分组传递率也随着攻击节点数的增加而下降。当 on 状态发送的数据包数增加时，数据分组传递率有所下降。从图 7 可以看出，被干扰节点的平均端到端的时延随着干扰节点数的增加有所增加，但增幅不大。

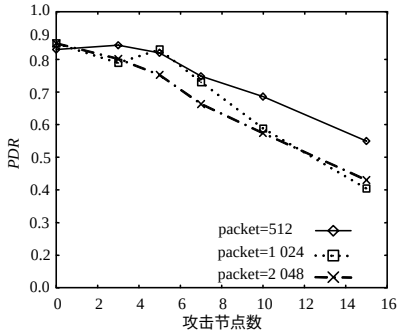

图 6　Exponential 流量下 *PDR* 与攻击节点数关系

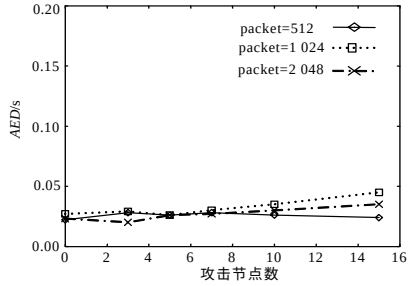

图 7　Exponential 流量下 *AED* 与攻击节点数关系

综上所述，具有开关特性的拒绝服务攻击，在节省能量和保护自己的情况下，同样能够使网络性能下降，取得良好的攻击效果，而且该攻击方式在自相似流量下的攻击效果优于其他流量产生模型的攻击效果，例如图 4 中 *PDR* 最小为 0.38 左右，而图 4 中最小为 0.46 左右，图 5 中平均端到端时延相对的变化幅度也较大。产生的原因可以从网络自相似流量的角度来解释。本文攻击流的关时间长度满足 Perato 分布，整个攻击周期其实就是一个近似自相似流，当注入到网络中后，其结果相当于自相似流量的进一步叠加。文献[7]的研究表明，过多的自相似流量叠加，会增加自相似系数，从而造成网络性能的下降。因此，该攻击方式既可使网络性能下降，又不会暴露自身。

5　结束语

可以看出，具有开关特性的攻击方式在网络拓扑结构不变的情况下具有较好的攻击效果和较低的检测率。为了更适合实际应用，下一步将研究在动态网络拓扑环境下的攻击效能。

参考文献

[1] Zhou Lidong, Haas Z J. Securing Ad Hoc Networks[J]. IEEE Network, 1999, 13(6): 24-30.

[2] Zhang Yongguang, Lee Wenke. Intrusion Detection in Wireless Ad Hoc Networks[C]//Proc. of the ACM MOBICOM'00. Boston, MA, USA: [s. n.], 2000.

[3] Aad I, Hubaux J P, Knightly E W. Denial of Service Resilience in Ad Hoc Networks[C]//Proceedings of MOBICOM'04. Philadelphia, Pennsylvania, USA: [s. n.], 2004.

[4] 王　楠. 无线局域网的网络流量特性与建模研究[D]. 北京: 中国科学院, 2003.

[5] Xu Kaixing, Hong Xiaoyan, Gerla M. Landmark Routing in Large Wireless Battlefield Networks Using UAVs[C]//Proceedings of MILCOM'01. Mclean, VA, USA: [s. n.], 2001.

[6] Baras J S. Modeling and Simulation of Telecommunication Networks for Control and Management[C]//Proc. of the 2003 Winter Simulation Conference. New Orleans, Louisiana, USA: [s. n.], 2003.

[7] AhleHagh H, Michalson W R. Statistical Characteristics of Wireless Network Traffic and Its Impact on Ad Hoc Network Performance[C]//Proceedings of the Advanced Simulation Technologies Conference. Orlando, USA: [s. n.], 2003.

编辑　顾姣健