面向P2P网络的DDoS攻击抑制方法

刘 丹[1]，李毅超[1]，余三超[2]，陈沁源[2]

(1. 电子科技大学电子科学技术研究院 成都 610054; 2. 电子科技大学计算机科学与工程学院 成都 610054)

【摘要】提出了一种分布式的基于对P2P网络中各节点进行分级的DDoS攻击抑制方法。采集了多个能分别反映当前节点本身或周围节点网络状况的评级因子，并通过不确定性推理确定当前节点分级值。分级值决定转发率。使用线性分类作为丢包策略对需发送数据包进行分组、丢弃，以降低误报率。仿真实验表明该方法能够有效抑制P2P网络上的DDoS攻击，提高整个网络抗攻击弹性。

关 键 词 分布式拒绝服务攻击; 网络安全; 覆盖网; 分类器;
中图分类号 TN393.08 **文献标识码** A doi:10.3969/j.issn.1001-0548.2010.06.016

Method to Inhibit DDoS Attack for P2P Overlay Network

LIU Dan[1], LI Yi-chao[1], YU San-chao[2], and CHEN Qin-yuan[2]

(1. Research Institute of Electronic Science and Technology, University of Electronic Science and Technology of China Chengdu 610054;
2. School of Computer Science and Engineering, University of Electronic Science and Technology of China Chengdu 610054)

Abstract A novel distributed method based on peer level model is presented to inhibit DDoS attack. The level model collects four factors including the behaviors of the current peer and its network status to evaluate level value by uncertain inference. Forwarding rate is decided by level value. The data on each peer are sorted by linear classifier and then discarded according to level value. Simulation experiment indicates this method could inhibit DDoS attack and enhance resilience of P2P overlay network.

Key words distributed denial of service; network security; overlay network; pattern classification;

传统DDoS攻击大多从运输层发起，随着覆盖网的快速发展，P2P网络开始吸引众多DDoS攻击者。面对攻击，P2P网络显得更加脆弱。

1) P2P网络具备多个发生DDoS攻击的条件。据统计，P2P已经占据网络60-80%的流量[1]，影响范围广、用户多。P2P的开放性允许用户不经检验地分发任何内容，不可避免地带来蠕虫、病毒的传播，形成规模庞大的僵尸网络，以发起DDoS攻击[2]。另外，P2P网络的查询和请求机制存在漏洞[3-4]，少量攻击源通过发起海量无用查询请求就能迅速消耗目标机资源实现拒绝服务攻击。2) P2P网络防御方法滞后。目前主流的DDoS防御方法主要基于协议分析或数据挖掘。文献[5]提出对TCP连接状态进行研究，以主动识别SYN FLOOD攻击。该类方法工作在传输层，不适合分析应用层P2P协议；文献[6]将K-means聚类算法应用于数据挖掘实现了DMDoSD；文献[7]实现了一个过滤器，能够监控并分析数据流，在发现攻击时中断连接。但P2P的匿名性以及攻击者采用对应用层报文加密等手段使该类方法无法进行有效防御。而传统的集中式DDoS防御[4-6]，直接检测并切断攻击连接，不可避免地带来大量误报、漏报及实时性等问题[8]。文献[9]提出一种新架构SOS抵御DDoS攻击，所有数据通过建立在P2P之上名为Chord overlay network的覆盖网进行认证和路由，可疑数据一律被丢弃。但该方案极大地改动了原P2P网络，降低了其灵活性，且需要在网络部署大量新设备以及在通信过程中进行繁琐的认证。3) P2P网络的穿透性。P2P网络能穿透防火墙和安全代理，从内部打开缺口，使DDoS攻击更易成功。4) P2P网络的动态性。P2P网络高度的动态性，允许各节点随时加入或退出覆盖网，使攻击者在初次攻击无效或遭瓦解后，易于快速组织下一轮攻击。

本文针对P2P网络DDoS攻击防御现状，提出了一种新的、基于分级模型的DDoS攻击抑制方法PLIM(peer level inhibit model)。该方法具有以下优点：1) 根据P2P网络分布性，提出了工作在应用层

收稿日期：2009 – 05 – 11; 修回日期：2010 – 03 – 24
基金项目：中央高校基本科研业务费专项资金(ZYGX2009J090)
作者简介：刘 丹(1969 –)，男，副教授，主要从事网络攻防、信息安全方面的研究.

的对P2P中各节点进行分级的分布式防御方法，不会成为网络通信瓶颈和单点故障，自适应性高；2) 在研究P2P网络中DDoS攻击发起、传播和响应各阶段特征的基础上，从节点本身和周围环境两方面提出了计算节点分级的4个评级因子，不同级别节点对应不同数据转发率。该模型不分析数据包内容，对加密和匿名攻击包检测效果良好；不回溯数据包源头，仅从最近一跳邻居获取所需信息，实现简单；3) 提出了基于线性分类方法的自适应丢包策略。该策略对用户透明，能根据节点分级动态调整丢包率，误报率低，能有效防御基于P2P网络的DDoS攻击。

1 实 现

1.1 分级防御方法原理

PLIM是一个基于P2P网络的、节点间相互协作的、动态评价当前节点在P2P网络中分级的可量化方法，各节点能依据分级实施不同的转发率，以实现攻击抑制。

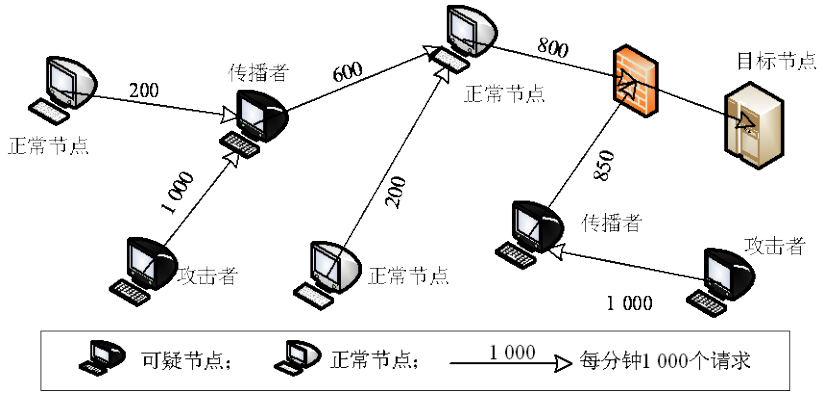

图1 部署PLIM的网络

从宏观看，通过部署PLIM到网络各节点，作为防御策略核心的分级模型能评估当前节点级值(level value)$\boldsymbol{V}$，$\boldsymbol{V}$为n维行向量。如图1所示，正常节点$\boldsymbol{V}$值较小，全速工作；可疑节点因$\boldsymbol{V}$值较大，启用线性分类规则筛选出可疑数据进行丢弃，达到降低发起及传播攻击的节点在P2P网络中的作用，提高网络弹性的目的。

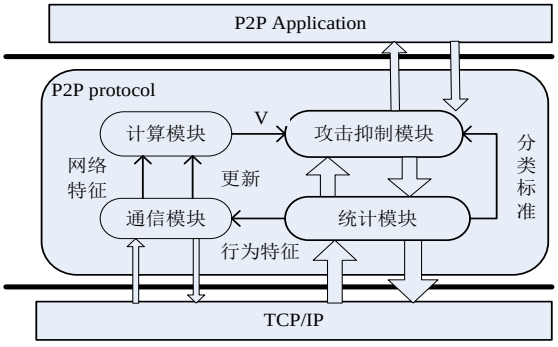

图2 协议栈

具体到各节点上，分级模型在应用层P2P协议上实现。如图2所示，计算模块周期性地根据各评级因子计算出当前节点分级值，攻击抑制模块依据分级值进行攻击抑制，而统计模块负责收集各模块所需要的输入参数，各节点评级因子的交换由专门的通信模块实现。

1.2 分级评定的数学模型

分析评级因子到节点V的映射，以真实反映其网络特征，其数学模型需具备以下特性：1) 能够评估当前节点的恶意性；2) 能够评估周围网络状况；3) 能够动态评定节点级别，根据攻击强度自适应地抑制攻击；4) 收敛于(0,1)，不会恶化周围节点分级。

首先，分析通过当前节点c的流量。设$R_{ic}(t)$表示t时间内某输入节点i流入c的数据流量，$S_{cj}(t)$代表t时间内节点c流向某输出节点j的数据流量。那么t时间内流量恒等式为：

$$\sum_{i=1}^{n} R_{ic}(t) - A_c(t) + I_c(t) = \sum_{j=1}^{m} S_{cj}(t) \tag{1}$$

式中，$A_c(t)$表示t时间内c处理的数据流量，即当前节点可提供服务或丢弃，不需要转发；$I_c(t)$表示时间t内节点c自身所发生的流量，即请求包。

下面分别介绍4个评级因子。

1) 当前节点发生的总流量。当前节点自身发生数据包的总流量是其可疑程度的直观反映，当自身发生的流量大于指定的阈值时，可认为该节点是攻击发起者。

定义节点r发生流量与阈值比为$\boldsymbol{I_r}$；时间为t；当前节点正常请求数据上限值为Q_I，则由文献[10]中统计方法得到的恶意节点的临界流量为$I_r = \min\left\{0, \dfrac{Q_I - I_r(t)}{Q_I}\right\}$。

2) 当前节点的转发总流量。DDoS攻击最危险

的特性是其分布性，攻击者可能是成千上万个傀儡机。在发起攻击的节点，攻击强度并不大，但通过多次汇集后的强度就足以使目标瘫痪，所以当某节点转发的流量超过转发阈值时，便产生了DDoS攻击。通过式(1)可以计算出t时间内转发流量$F_c(t)=\sum_{i=1}^{n}R_{ic}(t)-A_c(t)=\sum_{i=1}^{m}S_{ci}(t)-I_c(t)$，则节点$r$转发流量与转发阈值比为$F_r=\min\left\{0,\frac{Q_F-F_r(t)}{Q_F}\right\}$，其中$Q_F$为正常节点转发数据上限值。

3) 各输入节点分级值的合成。上述两个评级因子都是从节点本身特征分析DDoS攻击是否发生，而周围节点分级可以反映该节点所处的网络环境特征。从传播阶段看，当周围节点均为恶意节点时，该节点所转发的数据也被认定为可疑。因此各输入节点$\boldsymbol{V}$值的合成值可以作为评级因子。而作为证据的$\boldsymbol{V}$值具不确定性，可能存在误差或被伪造。如果只将输入节点$\boldsymbol{V}$值简单合成，则会产生积累误差或被恶意欺骗，因此PLIM采用专家系统MYCIN使用的不确定性推理算法。将各输入节点$\boldsymbol{V}$值视为证据，$\boldsymbol{V}$值交换视为推理规则，各输入节点$\boldsymbol{V}$值推导当前节点$\boldsymbol{V}$值评级因子视为多个知识推导同一个结论。

定义证据为$\boldsymbol{E}$；结论为H；证据信任度为$\mathrm{CF}(E_q)$，置为某输入节点q的$\boldsymbol{V}$值；规则信任度为$\mathrm{CF}(H,E_q)$，置为1；结论信任度即节点评级因子为$\mathrm{CF}(H)$，则$\mathrm{CF}_1(H)=\mathrm{CF}(H,E_1)\times\max\{0,\mathrm{CF}(E_1)\}$，同理可得则$\mathrm{CF}_2(H)$，合成信任度为$\mathrm{CF}_{1,2}(H)=\mathrm{CF}_1(H)+\mathrm{CF}_2(H)-\mathrm{CF}_1(H)\times\mathrm{CF}_2(H)$。当存在$N$个证据时，令推理函数：

$$f(\boldsymbol{x})=\sum_{i=1}^{n}\mathrm{CF}_i(H)-\sum_{1\leqslant i<j\leqslant n}\mathrm{CF}_i(H)\mathrm{CF}_j(H)+\sum_{1\leqslant i<j<k\leqslant n}\mathrm{CF}_i(H)\mathrm{CF}_j(H)\mathrm{CF}_k(H)-\cdots+(-1)^{n-1}\prod_{i=1}^{n}\mathrm{CF}_i(H)\tag{2}$$

式中，$\boldsymbol{x}=(x_1,x_2,\cdots,x_n)$。由上式可推得输入节点评级因子为$f_c(\boldsymbol{V})$，$\boldsymbol{V}$代表节点$c$的各输入节点的分级值。

4) 各输出节点丢包率反馈值的合成。目标节点tar的丢包率能反映其是否因受到攻击无法处理请求，或是因降级而丢弃数据包，两种情况都说明DDoS攻击正在发生。当丢包率处于稳定且较低的数值时，说明网络状况良好。当目标节点处理率低下，甚至无法正常反馈丢包率时(网络堵塞)，上一跳节点的$\boldsymbol{V}$值会立即调整，并适时启动攻击抑制。定义目标节点在时间t内的丢包率$L_{\mathrm{tar}}(t)$；反馈值传递时延T(单位：0.01 s)；D为丢包率反馈值，则$D=\max\{L_{tar}(t)+T,1\}$。通过式(2)计算出当前节点c各输出节点反馈值合成度为$f_c(\boldsymbol{D})$。将所有评级因子合成，得到$\boldsymbol{V}$值的计算公式$V_c=\alpha\cdot I_r+\beta\cdot F_r+\gamma\cdot f_c(V)+\varphi\cdot f_c(\boldsymbol{D})$，其中$\alpha$、$\beta$、$\gamma$和$\varphi$分别代表各评级因子的权重，$\alpha+\beta+\gamma+\varphi=1$。容易证明，$\boldsymbol{V}$收敛于(0,1)。

1.3　线性分类的丢包策略

据统计数据分析[11]，DDoS攻击发生时，流量会发生明显异常。为降低误报率，PLIM对判定为恶意的节点不是直接断开连接，而是通过线性分类算法区分可疑数据和正常数据，再根据由$\boldsymbol{V}$决定的转发率丢弃可疑数据。

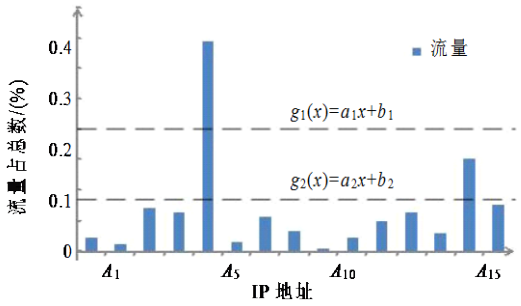

图3　节点流量分布

图3将时间T内发送的数据总量看作样本空间，各输出节点IP看作样本空间的一个有限划分，将样本划分向量化，以各IP流量占总量百分比作为纵向量，构建二维向量空间。依据线性划分的思想，找到一组线性函数$g(x)=ax+b$,将整个二维空间划分成以转发率为标准的多个组。

通常DDoS攻击都持续数十分钟，因此PLIM根据该节点在周期T的$\boldsymbol{V}$及需丢弃的IP所对应的流量比预测下一时间周期的攻击行为。在周期$T+1$按预测值对数据包进行转发。$\boldsymbol{V}$与转发率的组合关系是优化问题，经过大量的数据训练，取误报率最小的一组作为$\boldsymbol{V}$与转发率的对应组合。

表1　节点分级值与转发率对应表

分级	$\boldsymbol{V}$	转发率/(%)
1级	0～0.30	100
2级	0.30～0.60	90
3级	0.60～0.85	40
4级	0.85～1.00	0

攻击抑制模块具有以下特性：1) 实时性，线性分类算法计算速度快，能满足网络高速处理海量数据的要求。2) 准确性，准确对数据包进行分类，便

于后期处理，误报率低。3) 自适应性，选定被丢弃的IP后，能根据其攻击强度动态更改其在丢弃总量中的配额，以动态调整抑制强度。

2 实 验

为验证PLIM的有效性和误报率，进行了防御DDoS攻击的仿真实验。实验中使用的数据包括作为背景数据的正常P2P网络流量和DDoS攻击数据两组。使用P2PSim构造类似Chord[12]拓扑结构的仿真网络，共有节点512个，其中攻击节点32个，目标节点1个；每个节点拥有平均4个、最多9个邻居；请求包平均大小128字节，链路带宽5 M/s，目标节点链路带宽10 M/s。设节点交换评级因子及预测周期均为90 s。$\boldsymbol{V}$值计算参数 $\alpha=\beta=\gamma=\varphi=0.25$，$Q_I=120$，$Q_F=300$。普通节点每分钟随机发出0～10个查询数据请求。攻击节点从每分钟发送50个查询请求开始，每10分钟递增30个直到每分钟发送300个查询。

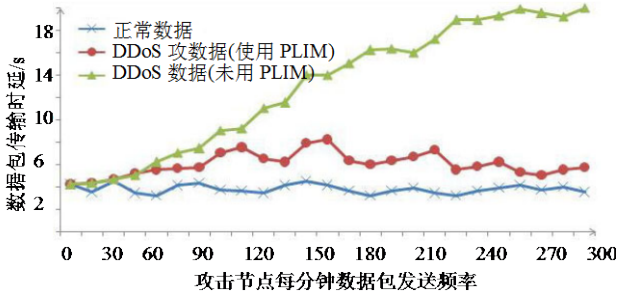

图4 数据包传输时延

图4中，在攻击强度逐渐增大的情况下，使用了PLIM的P2P网络传输时延一直控制在稳定范围，说明PLIM能够根据攻击强度自适应地调整转发率，抑制DDoS攻击。

表2 节点分级值分布

分级值($\boldsymbol{V}$)	节点数
0～0.30	466
0.30～0.60	6
0.60～0.85	29
0.85～1.00	7

表2列出了仿真网络中节点分级值的分布情况，仿真攻击节点只有32个，但是实际计算$\boldsymbol{V}$>0.6的节点有36个，原因是某些节点周围全是攻击节点，其$\boldsymbol{V}$必然会增大。另外，有6个$\boldsymbol{V}$>0.3的节点因为处于攻击请求汇集的路径上，所以也遭到了降级。

图5描述了正常数据包的丢包率即误报率。虽然表2数据说明一些正常节点被误标记为可疑，但是由于使用了线性分类策略对数据进行分类丢弃，所以PMLIS的误报率仍然较低。

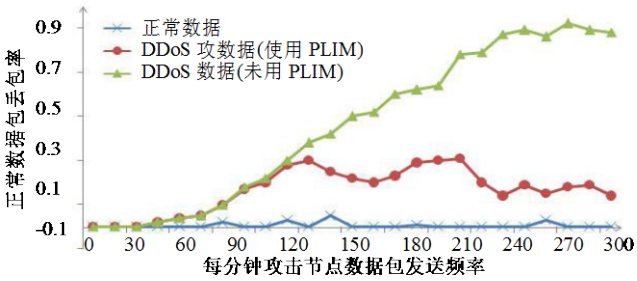

图5 误报率

3 结论和未来的工作

本文分析了P2P覆盖网更容易遭到DDoS攻击的原因，针对现有的主流防御工具难以被运用到应用层防护的现状，提出了在应用层防御的思路。为解决传统DDoS防御方法存在的单点故障，实时性差和误报率高等问题，根据P2P网络天然的分布性，提出了以分级模型为核心的分布式防御体系PLIM。讨论了分级值计算和线性分类丢包策略的细节，以有效判断节点可疑程度，并在发起和传播环节抑制DDoS攻击。仿真实验验证了PLIM能够迅速有效、自适应地抑制DDoS攻击。

在后续的工作中，该方法将结合开源项目eMule[13]，发布测试版，以调整各项参数，并进一步给出一种智能配置参数的方法。

参 考 文 献

[1] CNNIC. 第23次中国互联网络发展状况统计报告[EB/OL]. [2009-01-13]. http://www.cnnic.net.cn/uploadfiles/pdf/2009/1/13/92458.pdf.

[2] 夏春和, 石昀平, 李肖坚. 结构化对等网中的P2P蠕虫传播模型研究[J]. 计算机学报, 2006, 29(6): 952-959.
XIA Chun-he, SHI Yun-ping, LI Xiao-jian. Research on epidemic models of P2P worm in structured Peer-to-Peer networks[J]. Chinese Journal of Computers, 2006, 29(6): 952-959.

[3] MOORE D, SHANNON C, BROWN D, et al. Inferring internet denial of service activity[J]. ACM Transactions on Computer Systems, 2006, 24(2): 115-139.

[4] 任超, 李战怀, 张英. 异构P2P网络的分布式查询协议[J]. 电子科技大学学报, 2009, 38(1): 108-112.
REN Chao, LI Zhan-huai, ZHANG Ying. Distributed query protocol on heterogeneous P2P overlay networks[J]. Journal of University of Electronic Science and Technology of China, 2009, 38(1): 108-112.

[5] XIAO Bin, CHEN Wei, HE Yan-xiang, et al. An active detecting method against SYN flooding attack[C]//11th International Conference on Parallel and Distributed Systems Workshops. Fukuoka，Japan: IEEE, 2005: 709-715.

[6] 高能, 冯登国, 向继. 一种基于数据挖掘的拒绝服务攻击检测技术[J]. 计算机学报, 2006, 29(6): 944-951.
GAO Neng, FENG Deng-guo, XIANG Ji. A data-mining

based DoS detection technique[J]. Chinese Journal of Computers, 2006, 29(6): 944-951.
[7] LEE J W, GUSTAVO De V. Scalable multicast based filtering and tracing framework for defeating distributed DoS attacks[J]. International Journal of Network Management, 2005, 15(1): 43-60.
[8] ENGLE M, KHAN J I. Vulnerabilities of P2P systems and a critical look at their solutions[J/OL]. [2006-11-01]. http://medianet.kent.edu/techreports/TR2006-11-01-p2pvuln-EK.pdf.
[9] KEROMYTIS A D, MISRA V, RUBENSTEIN D. SOS: secure overlay services[C]//ACM SIGCOMM 2002 Conference. Pittsburgh, USA: ACM, 2002: 61-72.
[10] SRIPANIDKULCHAI K. The popularity of Gnutella queries and its implications on scalability[EB/OL]. [2009-01-19]. http://www.cs.cmu.edu/~kunwadee/research/p2p/gnutella.html, 2001.
[11] XIE Yi, YU Shun-zheng, Monitoring the application-layer DDoS attacks for popular websites[J]. IEEE/ACM Transactions on Networking, 2009, 17(1): 15-25.
[12] STOICA I, MORRIS R, KARGER D, et al. Chord: A scalable Peer-To-Peer lookup service for Internet applications[C]//Applications, Technologies, Architectures, and Protocols for Computers Communications. Seattle, WA, USA: ACM, 2001: 149-160.
[13] Merkur. Emule-project[EB/OL]. [2009-01-19]. http://www.emule-project.net/.
[14] NAOUMOV N, ROSS K. Exploiting P2P systems for DDoS attacks[C]//Proceedings of the 1st International Conference on Scalable Information Systems. [S.l.]: [s.n.], 2006.

编 辑 漆 蓉

(上接第72页)

参 考 文 献

[1] SU Y P, XUN L, HUI S Y R. Mutual inductance calculation of movable planar coils on parallel surfaces[J]. IEEE Transactions on Power Electronics, 2009, 24(4): 1115-1123.
[2] LI H L, HU A P, COVIC G A, et al. Optimal coupling condition of IPT system for achieving maximum power transfer[J]. Electronics Letters, 2009, 45(1): 76-77.
[3] WU H H, HU A P, SI P, et al. A push-pull resonant converter with dual coils for Transcutaneous Energy Transfer systems[C]//4th IEEE Conference on Industrial Electronics and Applications. Xi'an: IEEE, 2009: 1051-1056.
[4] BOYS J T, COVIC G A, GREEN A W. Stability and control of inductively coupled power transfer systems[J]. Electric Power Applications, IEE Proceedings-Electric Power Applications, IEE Proceedings, 2000, 147(1): 37-43.
[5] HU A P, HUSSMANN S. A phase controlled variable inductor designed for frequency stabilization of current fed resonant converter power supplies[C]//Proceedings of the 6th International Power Engineering Conference. [S.l.]: [s.n.], 2003: 175-180.
[6] SI P, HU A P, MALPAS S, et al. A frequency control method for regulating wireless power to implantable devices[J]. IEEE Transactions on Biomedical Circuits and Systems, 2008, 2(1): 22-29.
[7] Jr HSU W U, HU A, AKSHYA S, et al. A new contactless power pick-up with continuous variable inductor control using magnetic amplifier[C]//International Conference on Power System Technology. Chongqing: [s.n.], 2006.
[8] CHEN G, SUN Y, DAI X, et al. On piecewise control method of contactless power transmission system[C]// 27th Chinese Control Conference. Piscataway, NJ, United States: Institute of Electrical and Electronics Engineers Computer Society, 2008: 72-75.
[9] WANG C S, COVIC G A, STIELAU O H. General stability criterions for zero phase angle controlled loosely coupled inductive power transfer systems[C]//The 27th Annual Conference of the IEEE Industrial Electronics Society. [S.l.]: IEEE, 2001: 1049-1054.
[10] SUN Y, HU A P, DAI X, et al. Discrete time mapping modeling and bifurcation phenomenon study of a ZVS converter[C]//Power Conference 2004. Singapore: [s.n.], 2004.
[11] GREEN A W. Modelling a push-pull parallel resonant convertor using generalised state-space averaging[J]. IEE Proceedings-B, 1993, 140(6): 350-356.
[12] TANG C S, SUN Y, SU Y G, et al. Determining multiple steady-state ZCS operating points of a switch-mode contactless power transfer system[J]. IEEE Transactions on Power Electronics, 2009, 24(2): 416-425.

编 辑 漆 蓉