无线入侵检测系统三维定位方法研究

郭培源 何多多 吴 筱
(北京工商大学计算机与信息工程学院 北京 100048)

摘 要 立足无线入侵检测系统这一应用背景,针对系统无法预知目标主机网卡发射功率信息这一问题,尝试在Shadowing模型基础上进行变换,利用接收信号强度差来进行最小二乘定位计算,从而消除对发射功率参数的依赖。通过对无线入侵检测系统定位模块的设计、实现与测试,验证了此方法的可行性,实现了室内环境Room-level级三维定位。试验数据显示,在综合考虑系统定位精度与成本的情况下,保证空间中一点能够被8个检测节点覆盖到时,系统的精度和成本综合最优。

关键词 三维定位,无线入侵检测系统,接收信号强度指示,遮蔽模型,最小二乘
中图法分类号 TP393 **文献标识码** A

Three-dimensional Positioning Method for Wireless Intrusion Detection System

GUO Pei-yuan HE Duo-duo WU Xiao
(School of Computer and Information Engineering, Beijing Technology and Business University, Beijing 100048, China)

Abstract This paper was based on the application background of wireless intrusion detection system, which wants to locate target host, but can not predict transmitted power of target's wireless network card. By using received signal strength indication difference for the least square calculation, which is based on the transformation of Shadowing model, the method can eliminate the dependence of transmitted power parameter. By means of the design, realization and test of the positioning module for wireless intrusion detection system, the feasibility of the method was verified. Finally, an indoor three-dimensional positioning module with Room-level precision was achieved in WIDS. Experiment data shows that precision and cost of the system are integrally optimal as a space point can be covered by 8 detection nodes.

Keywords Three-dimensional positioning, Wireless intrusion detection system, RSSI, Shadowing model, Least square

1 引言

无线局域网(WLAN)因其便捷、通用、易部署等特点,被广泛应用于各个领域。但是,WLAN在给我们带来极大便利的同时,也暴露出诸多安全问题。由于传播介质的开放性以及IEEE802.11标准自身安全漏洞等因素,使得WLAN极易受到各式各样入侵行为的威胁,严重制约了自身发展[1]。

无线入侵检测系统(Wireless Intrusion Detection System)是以检测无线入侵和网络非法攻击为目的的信息安全平台。通过捕获区域内的IEEE802.11帧并对其进行分析,WIDS能够有效地监视网络传输,对可疑传输实施跟踪和预警[2]。WIDS的研究目前主要集中在入侵检测算法、系统设计与部署等方面,而在利用WIDS监视WLAN网络传输时,获取可疑节点的空间物理位置也显得尤为重要,它可以帮助网络管理人员及时到达现场实施管制和入侵取证,快速排除威胁[3]。

如今,定位功能已成为评定WIDS的重要指标之一,一些WIDS集成了相关模块来对目标主机实施定位,但其定位方法仍然存在诸多不足。有的采用手持终端动态搜寻方式寻找目标主机位置,这种方式在结构复杂的楼宇内部将耗费大量人力与时间,管理人员将不能及时到达现场;有的采用静态锚节点平面定位方式,通过定位算法计算目标主机物理位置,这是广泛采用的一种方式,但其局限于平面定位。此外,由于WIDS的定位对象可以是满足IEEE802.11标准的一切无线终端,因此要求系统的定位精度不受定位对象特性的影响,尤其是不受定位对象无线网卡发射功率的影响。针对上述问题,付雄等人提出了二维平面上3个探测器定位一个目标,并且定位误差不受网卡发射功率影响的方法[4],有效地克服了目标主机有意或随意地调整无线网卡发射功率而试图误导系统计算出错误物理位置的情形。但是,该方法依然存在很多局限性,例如限定探测器数量、局限于二维平面等等。对此,本文将WIDS中的定位方法拓展到三维空间,采用不限定检测节点数量,不依赖定位对象网卡发射功率参数的定位算法实施定位计算,有效地提高了WIDS定位功能对楼宇室内环境的适应性,为WIDS场景中的入侵主机定位提供了一种新思路。

2 定位技术选择

目前常见的无线定位技术主要包括GPS卫星定位、基于

到稿日期:2013-01-06 返修日期:2013-03-25
郭培源(1958—),男,教授,硕士生导师,主要研究方向为智能控制、嵌入式系统、光电检测技术;何多多(1988—),男,硕士生,主要研究方向为信息安全、嵌入式系统,E-mail:heduoduo321@163.com;吴 筱(1987—),男,硕士生,主要研究方向为嵌入式系统、密码学。

TOA/TDOA/AOA 的定位和基于接收信号强度指示(RSSI)的定位技术。GPS 定位需要接收卫星信号,适用于开阔的户外环境定位。基于电波传输时间的定位技术(TOA/TDOA)是通过测量电波从发射点传播到多个接收点的传播时间或时间差来确定目标点的位置信息,需要设备间的时间同步。然而,这种设备间同步在低功率高密度的 WLAN 中实现起来比较困难,加之无线设备间距离往往较短,电波传输时延几乎可以忽略不计,无法保证 TOA/TDOA 定位法的精度。此外,复杂的室内环境通常会使无线信号产生严重的多径传播效应,到达接收点的信号在幅值相位以及入射角等方面将产生叠加效果,这些都会降低基于电波入射角(AOA)定位方法的精度。

基于接收信号强度指示(Received Signal Strength Indication)的定位因其成本低、易实现等特点,被广泛应用于室内环境定位。RSSI 定位技术与 TOA/TDOA/AOA 定位相比,它不需要添加额外硬件设备来进行时间和角度的同步与测量,能充分利用现有覆盖广泛的 WLAN 设施,便捷高效地将高质量定位的应用范围延伸到密集城区和室内。因此,本文将在 WIDS 中采用基于 RSSI 的三维定位方法来获取入侵行为主机的物理位置[5]。

3 三维定位算法

3.1 无线信号传播模型

目前被广泛使用的无线信号传播模型主要包括 Free space propagation 模型、Two-ray ground reflection 模型和 Shadowing 模型 3 种[6]。其中,前两种模型假定了一个理想的传播环境,在发送者和接收者之间只有一条无障碍的直线路径,这也是根据球体面积和能量守恒定律所得来的结果。在现实中,由于无线信号多径传播的褪色效应,前两种模型不再具有实用价值。Shadowing 模型是一个更具综合性而被广泛应用的模型[7]。

Shadowing 模型由两部分组成,第一部分是 Pass loss 模型,该模型以一个已知距离 d_0 及此距离上的路径损耗 $PL(d_0)$为参考,预测出距离为 d 处的路径损耗 $PL(d)$,模型如下:

$$PL(d)=PL(d_0)+10\beta\lg\left(\frac{d}{d_0}\right) \tag{1}$$

式中,β是 Pass loss 系数,它是测量得来的经验值,障碍物越多,β的相对数值越大,随着距离的增加能量损耗越大,接收到的能量下降越快。Pass loss 系数 β参考值如表 1 所列。

表 1 Pass loss 系数 β参考值

环境		β
室外	自由空间	2
	有障碍物的城市空间	2.7~5
室内	直线传输	1.6~1.8
	有障碍物传输	4~6

接收信号强度与路径损耗之间的关系如式(2)所示:

$$P_r(d)=P_t-PL(d) \tag{2}$$

式中,P_t 是发射功率,$P_r(d)$是距离为 d 处的接收信号强度。利用式(2)可将式(1)转化为:

$$P_r(d)=P_r(d_0)+10\beta\lg\left(\frac{d_0}{d}\right) \tag{3}$$

Shadowing 模型的第二部分 X_{dB} 反映了当距离一定时,接收到的能量的变化。X_{dB} 满足均值为 0、均方差为 σ_{dB} 的正态分布。完整的 Shadowing 模型可以表示为:

$$P_r(d)=P_r(d_0)+10\beta\lg\left(\frac{d_0}{d}\right)+X_{dB} \tag{4}$$

在 WIDS 的应用场景中,由于无法预知目标主机无线网卡发射功率 P_t,而在距离被定位主机 d_0 处的 RSSI 值 $P_r(d_0)$与网卡发射功率相关,因此无法直接使用式(4)推算距离。考虑使用接收信号强度差来进行计算,设 $P_r(d_m)$和 $P_r(d_n)$分别是距离被定位主机 d_m 和 d_n 距离处的 RSSI 值,根据式(4)建立两个 Shadowing 模型方程,两式相减消去 d_0 与 $P_r(d_0)$得:

$$P_r(d_m)-P_r(d_n)=10\beta\lg\left(\frac{d_n}{d_m}\right) \tag{5}$$

3.2 空间定位方程组

设 $S_1,S_2,S_3,S_4,\cdots,S_k$ 是能够捕获到目标主机 RSSI 值的 k 个入侵检测节点(不共面),它们的空间坐标已知,S_0 为目标主机,如图 1 所示。

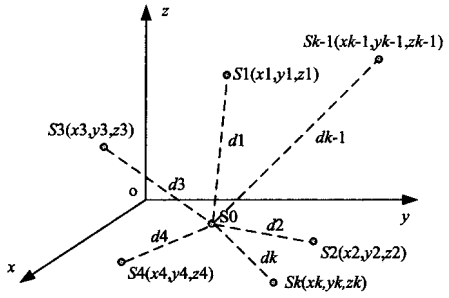

图 1 空间定位坐标系

若 $S_1,S_2,S_3,S_4,\cdots,S_k$ 各检测节点捕捉到的 RSSI 值分别为 $P_1,P_2,P_3,P_4,\cdots,P_k$,由式(5)可得方程组式(6):

$$\begin{cases} P_2-P_1=5\beta\lg\left(\dfrac{(x_1-x)^2+(y_1-y)^2+(z_1-z)^2}{(x_2-x)^2+(y_2-y)^2+(z_2-z)^2}\right) \\ P_3-P_2=5\beta\lg\left(\dfrac{(x_2-x)^2+(y_2-y)^2+(z_2-z)^2}{(x_3-x)^2+(y_3-y)^2+(z_3-z)^2}\right) \\ P_4-P_3=5\beta\lg\left(\dfrac{(x_3-x)^2+(y_3-y)^2+(z_3-z)^2}{(x_4-x)^2+(y_4-y)^2+(z_4-z)^2}\right) \\ \quad\vdots \\ P_k-P_{k-1}=5\beta\lg \\ \quad\left(\dfrac{(x_{k-1}-x)^2+(y_{k-1}-y)^2+(z_{k-1}-z)^2}{(x_k-x)^2+(y_k-y)^2+(z_k-z)^2}\right) \end{cases} \tag{6}$$

令 $H_i=10^{\frac{P_{i+1}-P_i}{5\beta}}$ (i=1,2,3…$k-1$),则式(6)可简化为式(7):

$$\begin{cases} H_1[(x_2-x)^2+(y_2-y)^2+(z_2-z)^2]= \\ \quad(x_1-x)^2+(y_1-y)^2+(z_1-z)^2 \\ H_2[(x_3-x)^2+(y_3-y)^2+(z_3-z)^2]= \\ \quad(x_2-x)^2+(y_2-y)^2+(z_2-z)^2 \\ H_3[(x_4-x)^2+(y_4-y)^2+(z_4-z)^2]= \\ \quad(x_3-x)^2+(y_3-y)^2+(z_3-z)^2 \\ \quad\vdots \\ H_{k-1}[(x_k-x)^2+(y_k-y)^2+(z_k-z)^2]= \\ \quad(x_{k-1}-x)^2+(y_{k-1}-y)^2+(z_{k-1}-z)^2 \end{cases} \tag{7}$$

在式(7)中,当 H_i 不等于 1 时,式(7)中第 i 个方程可整

理为球面方程形式：

$$(x-X_i)^2+(y-Y_i)^2+(z-Z_i)^2=R_i^2 \tag{8}$$

其球心坐标为：

$$[X_i,Y_i,Z_i]=\left[\frac{x_i-H_ix_{i+1}}{1-H_i},\frac{y_i-H_iy_{i+1}}{1-H_i},\frac{z_i-H_iz_{i+1}}{1-H_i}\right] \tag{9}$$

半径为：

$$R_i=\sqrt{\frac{H_i[(x_i-x_{i+1})^2+(y_i-y_{i+1})^2+(z_i-z_{i+1})^2]}{(1-H_i)^2}} \tag{10}$$

当 H_i 等于 1 时，式(7)中第 i 个方程可直接整理为线性方程：

$$2x(x_i-x_{i+1})+2y(y_i-y_{i+1})+2z(z_i-z_{i+1})=D_i^2-D_{i+1}^2 \tag{11}$$

式中，$D_i^2=x_i^2+y_i^2+z_i^2$。

将式(7)中的方程按上述方式整理为式(8)或式(11)的形式。整理后若方程组中形如式(8)的方程数大于 1，则可通过球面方程间做差消去 2 次项的方式将其线性化；若方程组中形如式(8)的方程数等于 1，则可直接忽略此球面方程。最终得到形如式(12)的线性方程组：

$$GX=D \tag{12}$$

求解式(12)的最小二乘解，即求：

$$\min_X \| GX-D \|_2 \tag{13}$$

其结果为：

$$\hat{X}_{LS}=(G^TG)^{-1}G^TD \tag{14}$$

在传统三维空间定位中，锚节点数大于等于 4 时就可实现定位[8]。但在 WIDS 的应用场景中，由于无法预知目标主机网卡发射的功率信息，因此利用接收信号强度差来组建定位方程组，k 个接收信号强度值只能组建 $k-1$ 个与接收信号强度差相关的线性无关方程。所以，在本文的应用场景中，至少需要 5 个 RSSI 值即 5 个检测节点，才能实现定位。

4 WIDS 系统结构与定位模块设计

在分布式 WIDS 中，入侵检测引擎分布于各个入侵检测节点中，使用 SVM 与特征识别相结合的方式来检测各种潜在的攻击行为。检测节点采用嵌入式 ARM 体系架构，通过使大功率无线网卡工作在 Monitor 模式，来捕获一定区域内的 IEEE802.11 帧，供入侵检测引擎分析甄别[9]。由于无线网卡驱动的支持，捕捉到的 802.11 帧会被添加 Radiotap 头部，Radiotap 中包含了 Header revision、Channel frequncy、SSI Signal、SSI Noise 等附加信息，其中，SSI Signal 便是该 802.11 帧发射主机的 RSSI 值[10]。

入侵检测引擎对 IEEE802.11 帧的分析结果以及该帧的 RSSI 值将通过 syslog 系统保存为本地日志或发送给 WIDS 管理中心。管理中心与各入侵检测节点通过 SSL 安全通信隧道进行通信，节点数据经日志管理子系统处理后，存入 MySQL 数据库。WIDS 管理中心的作用在于对各检测节点实施统一的设备管理与健康状况维护，对 syslog 数据进行集中分析与挖掘，利用多个节点所捕捉的 RSSI 值定位目标主机物理位置，制定黑名单、特定行为警报等防御策略，并通过 XML 编码器编码后发送给特定检测节点，供节点执行实施等。此外，WIDS 管理中心采用 B/S 架构，用户通过浏览器便可访问管理中心的控制页面，系统结构如图 2 所示。

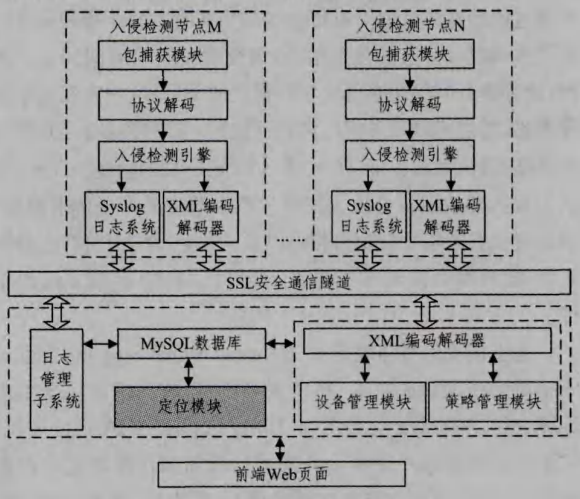

图 2 WIDS 系统结构图

定位模块是一个相对独立的软件模块，它是 WIDS 管理中心的重要组成部分。在实现定位前，管理中心要对建筑物的楼层信息进行登记，注册现有入侵检测节点的物理位置，建立空间坐标系。当管理中心要定位某目标主机时，定位模块首先从数据库读入“(目标主机 MAC 地址，RSSI 值，检测节点 ID，时间戳)”格式数据，然后进行定位计算。根据定位计算结果，定位模块需判断目标点坐标所在楼层，结合事先导入的建筑物各层平面结构图与层高信息，将定位点显示在对应楼层的平面图上，图 3 描述了定位模块进行单次定位计算的流程。此外，当目标主机的空间位置发生变化时，还可通过多次定位，根据时间戳绘制出它的运动轨迹。

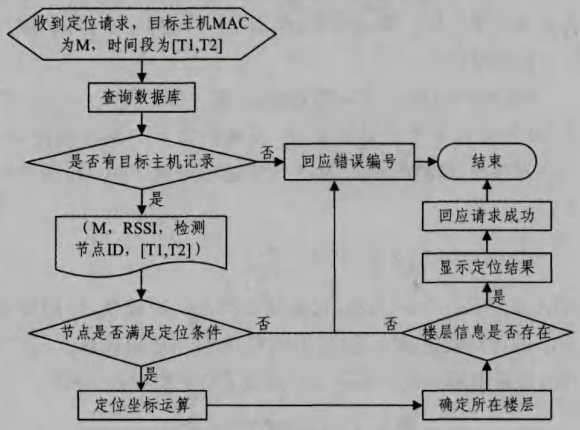

图 3 定位模块单次定位流程

5 测试与结果分析

选择实验室所在建筑为测试场所。首先有如下准备工作要做：①测量建筑物内的 Pass loss 系数：使用内置无线网卡的笔记本电脑作为测量工具(安装 inSSIDer 工具)，以 1 米步长为单位远离某无线 AP，每步停留 20 秒，记录 20 秒内 RSSI 值的平均值。再根据 Pass loss 模型，计算 β 值。这期间要充分考虑墙壁、楼板等障碍物的影响，最终计算出测试场所的平均 $\beta=4.23$。②导入建筑物各层平面结构图(JPG/GIF/PNG/

BMP 格式)，设置各层 x-y 平面坐标系与空间层高。③注册各入侵检测节点的位置信息。

首先使用 5 个节点进行测试，由于节点数目有限，并且实验室位于建筑物 6 层(建筑内各层层高约为 3.5 米)，为了适增加当 5 个节点的有效定位区域，即 5 个节点探测范围的公共重叠区域(节点探测半径 40 米)，采用较为密集的布置方式将节点随机分布在 5 层至 7 层中。节点坐标如表 2 所列，其中，1 个坐标单位代表 0.1 米实际距离。

表 2　入侵检测节点位置信息

节点 ID	所在楼层	X 坐标	Y 坐标	Z 坐标
001	5	85	142	152
002	5	110	32	153
003	6	64	190	187
004	6	69	217	187
005	7	15	69	220

准备一台装有 BackTrack5 操作系统的笔记本和一张发射功率可调的无线网卡，尝试对一台使用 WEP 加密的合法 AP 进行密钥破解攻击。BackTrack5 预装了很多网络安全审计工具，其中，Aircrack-ng 套件可以轻易实现 WEP/WPA/WPA2 密钥破解(WPA/WPA2 需借助攻击字典)[11]。

在破解过程中，当入侵主机向 AP 发送大量相同 ARP 包，试图获取多个不同的 IVs 时(Arp-request Reinjection)，入侵检测引擎发现网络中的 Arp-request 探寻量超过正常指标上限，并将发包主机添加到 Suspect List 中。在对嫌疑主机流量进行进一步跟踪分析后，引擎确认了该嫌疑主机的流量行为符合无线破解攻击特征，并生成相应日志数据。随后，检测节点将引擎分析所得的高风险日志数据上报到管理中心(见图 4)，提醒管理员进行核实和处理。

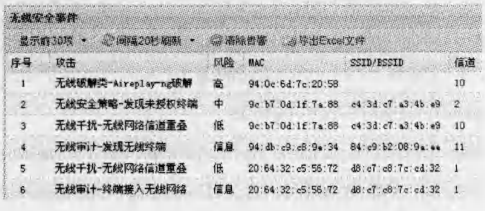

图 4　无线破解事件被上报到管理中心日志页面

当捕捉到入侵行为主机的 802.11 帧满足定位条件时(至少 5 个节点捕捉到该主机帧数据)，WIDS 会自动定位到该主机所在楼层，显示其物理位置。定位模块每隔 $T=100$ms 对入侵主机进行一次定位，生成一个定位点。图 5 显示了检测节点数为 5 时，入侵主机在该楼层(6 层)的运动轨迹(Heat-map 由 Javascript 动态绘制)，颜色越深代表定位点密度越高，也说明入侵主机在该位置滞留的时间越长。

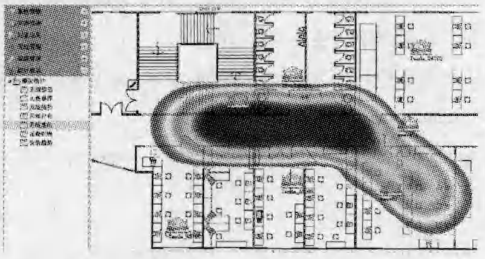

图 5　入侵主机楼层内运动轨迹 Heat map(节点数:5)

在目标主机周围，逐步增加检测节点数量，位置依然随机分布，并保证目标主机在每个节点的探测范围之内。图 6 给出了目标主机无线网卡发射功率分别为 28mW、32mW、64mW 时检测节点数对定位误差的影响。

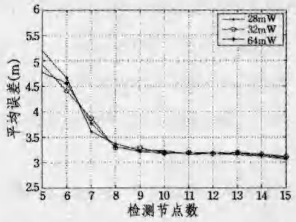

图 6　检测节点数对定位误差的影响

从图 6 可以看出，目标主机网卡发射功率对系统定位误差无太大影响，3 种发射功率下曲线基本一致。平均定位误差随着检测节点数的增加呈下降趋势：当节点数只有 5 时，平均定位误差约为 4.9 米；当节点数增加至 8 时，平均定位误差约为 3.3 米；当节点数继续增加时，尽管平均定位误差仍在减小，但趋势已不明显，并且过多的检测节点将使系统成本大大增加。综合考虑精度与成本因素可以看出，保证空间中一点能够被 8 个检测节点覆盖到时，系统的精度和成本综合最优。

图 7 为检测节点数为 8 时，入侵主机的运动轨迹热图。对比图 5 可以看出，在相同的运动轨迹下，节点数为 8 时的定位点分布明显较集中，误差较大的定位点数量减少，轨迹热图更加细致明确，轨迹精度较高。

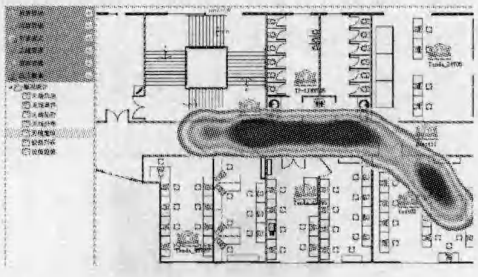

图 7　入侵主机楼层内运动轨迹 Heat map(节点数:8)

结束语　本文研究了 RSSI 三维定位在无线入侵检测系统这一特殊场景中的应用。事实上，由于室内环境的复杂性以及 Shadowing 模型对参数 β 的依赖，使得系统可能存在定位精度不高的问题[12]。在 z 轴方向，系统对定位误差十分敏感，较大的 z 轴误差将使系统在楼层判断上出现偏差，这些都是需要改进的地方。但是，在 WIDS 的应用场景中，本方法完全能够满足 Room-level 定位需求，适用于一些楼层空间较高的室内环境定位场景。

参 考 文 献

[1] Park J S, Dicoi D. WLAN Security: Current and Future [J]. IEEE Internet Computing, 2003, 7(5): 60-65

[2] Boob S, Jadhav P. Wireless Intrusion Detection System [J]. Interational Journal of Computer Applications, 2010, 5(8): 9-13

[3] Chen Ying-ying, Trappe W, Martin R P. Attack Detection in Wireless Localization[C]// INFOCOM 2007: 26th IEEE International Conference on Computer Communications. Piscataway: IEEE, 2007: 1964-1972

[4] 付雄,彭冰. 基于 Shadowing 模型的无线入侵主机物理定位研究[J]. 微电子学与计算机,2010,27(12):4-9

[5] Li Bing-hao, Dempster A, Rizos C, et al. Hybrid Method for Localization Using Wlan[C]// Spatial Sciences Conference. Melbourne: Spatial Sciences Institute, 2005: 12-16

[6] Dricot J-M, De Doncker P. High-accuracy physical layer model for wireless network simulations in NS-2[C]// Wireless Ad-Hoc Networks, 2004 International Workshop. Oulu: CWC Oulu, 2004: 249-253

[7] Xu Jiu-qiang, Liu Wei, Lang Feng-gao, et al. Distance measurement model based on RSSI in WSN[J]. Wireless Sensor Network, 2010, 2(8): 606-616

[8] 彭建盛,李兴秦,志强. 三维立体空间定位算法的研究与实现[J]. 传感器与微系统,2012,31(7):33-35

[9] Lim Yu-xi, Schmoyer T, Levine J, et al. Wireless Intrusion Detection and Response[C]// Information Assurance Workshop, 2003. IEEE Systems, Man and Cybernetics Society. New York: IEEE, 2003: 68-75

[10] Kowalik K, Bykowski M, Keegan B, et al. Practical issues of power control in IEEE 802. 11 wireless devices[C]// International Conference on Telecommunications, 2008, ICT 2008. Berlin: ICWE, 2008: 1-5

[11] 杨哲. 无线网络安全攻防实战进阶[M]. 北京:电子工业出版社,2011:12-21

[12] Erceg V, Greenstein L J, Tjandra S Y. An empirically based path loss model for wireless channels in suburban environments[J]. IEEE Journal on Selected Areas in Communications, 1999, 17(7): 1205-1211

(上接第 28 页)

以及跨基本块和循环分布向量化方法 3 个版本进行了测试,最后给出各版本的加速比,如图 10 所示。SIMD 代表常规向量化加速比,Across Basic Block 代表本文提出的跨基本块变换策略向量化之后得到的加速比,Across Basic Block and Loop Distribution 代表按照本文提出的跨基本块和循环分布向量化算法所得到的加速比。从图中可以看出,本文所介绍的基于跨基本块变换和循环分布的 SLP 优化算法相对于常规的 SIMD 向量化有明显的性能提升,3 个测试用例 convolve、173. applu 核心函数(buts)和 183. equake 的加速比分别为 1. 92、1. 46 和 1. 66,算法所带来的收益比较明显。

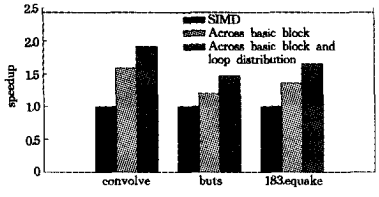

图 10 跨基本块和循环分布优化加速比

结束语 由于 SLP 算法能更好地对数字信号处理领域的应用进行向量化,而该算法不能充分发掘跨越基本块边界语句的并行性,因此本文在对现有的循环变换和跨基本块数据依赖分析的基础上,提出了基于跨基本块变换和循环分布的 SLP 优化技术,以尽可能地发掘不同基本块之间语句的并行性,消减不必要的冗余运算,使跨基本块变换代价达到最优。最后基于 SPEC2000 测试集和数字信号处理领域的程序核心片段对该优化方法进行了测试,结果表明,该方法结合 SLP,可以提升向量化程序的执行效率。

参 考 文 献

[1] Franchetti F, Kral S, Lorenz J, et al. Efficiem utilization of SIMD extensions[J]. Proceedings ofthe IEEE, 2005, 93(2): 409-425

[2] TMS320C6000 CPU and Instruction Set Reference Guide(Rev. F)[M]. TexasInstruments Inc. 2000

[3] SC140 DSP Core Reference Manual[R/OL]. http://cache. freescale. com/files/dsp/doc/ref _ manual/MNSC140CORE. pdf, 2012-05-20

[4] Fridman J, Greenfield Z. The Tiger SHARC DSP Architecture [J]. IEEE Micro, 2000, 20(1): 66-76

[5] Tanaka H, Ota Y, Matsumoto N, et al. A New Compilation Technique for SIMD Code Generation Across Basic Block Boundaries[C]// Design Automation Conference(ASP-DAC), 2010 15th Asia and South Pacifi. Jan. 2010: 101-106

[6] Larsen S, Amarasinghe S. Exploiting superword level parallelism with multimedia instruction sets[C]// Proc of the ACM SIGPLAN Conference on Programming Language Design and Implementation. June 2000: 145-156

[7] Shin J, Hall M, Chame J. Superword-level Parallelism in the Presence of Control Flow[C]// Proc. of the International Symposium on Code Generation and optimization. March 2005: 165-175

[8] Nuzman D, Zaks A. Outer-loop vectorization: revisited for short simd architectures[C]// Proceedings of the 17th international conference on parallel architectures and compilation techniques, PACT '08. New York, NY, USA, ACM, 2008: 2-11

[9] Aho A V, Lam M S, Sethi R, et al. 编译原理[M]. 赵建华,郑滔,戴新宇,译. 北京:机械工业出版社,2009

[10] 陈火旺,刘春林,谭庆平,等. 程序设计语言编译原理(第 3 版)[M]. 北京:国防工业出版社,2001

[11] Allen F E, Cocke J. A program data flow analysis procedure[J]. Communications of ACM, 1976, 19(3)

[12] Open64[EB/OL]. http://open64. sourceforge. net, 2012-09-10