非打扰式无线传感器网络测试仪的设计与实现

李天林[1,3] 皇甫伟[2,3] 杨 煦[3,4] 张志强[3,4] 孙利民[2] 李方敏[1]

(武汉理工大学信息工程学院 武汉 430070)[1] (信息安全国家重点实验室 北京 100190)[2]

(中国科学院软件研究所 北京 100190)[3] (北京大学软件与微电子学院 北京 102600)[4]

摘 要 无线传感器网络的测试工具对于传感器网络的深入研究和应用具有重要意义。提出了一种非打扰式的无线传感器网络测试方法,并介绍了基于该方法的无线传感器网络测试仪的设计思路和详细实现。该测试仪采用可编程逻辑阵列(FPGA)高速采集传感器节点的内部互连信息,并将采集的信息通过额外网络传输到测试服务器进行集中处理,还原节点状态信息和获取整个无线网络的通信情况,避免了对传感器网络节点运行和无线通信的影响。实验测试表明,该测试仪可以很好地获取节点状态,并在数据采集的过程中不干扰节点的正常工作。

关键词 无线传感器网络,无线传感器网络测试仪,无线传感器网络测试平台

Design and Implementation of Non-intrusive Wireless Sensor Network Tester

LI Tian-lin[1,3] HUANGFU Wei[2,3] YANG Xu[3,4] ZHANG Zhi-qiang[3,4] SUN Li-min[2] LI Fang-min[1]

(School of Information Engineering, Wuhan University of Technology, Wuhan 430070, China)[1]

(State Key Laboratory of Information Security, Beijing 100190, China)[2]

(Institute of Software, Chinese Academy of Sciences, Beijing 100190, China)[3]

(Department of Software and Microelectronics, Peking University, Beijing 102600, China)[4]

Abstract Wireless sensor network test tool is great significant for the wireless sensor network's in-depth research and applications. A testing method of non-intrusive wireless sensor network was proposed, and the design and implementation of a wireless sensor network tester based on this method were introduced. This tester uses the FPGA to speedily collect the signal of the node inner communication without intrusive to work of the node, and then send the signal to the center servicer. With processing these signals, the center servicer can revert the communication of the node or all wireless sensor network. The experiment proved that this tester can be very good at collection of the nodes communication data without interference to the work of nodes.

Keywords Wireless sensor networks, Wireless sensor network tester, Wireless sensor network testbed

1 引言

无线传感器网络(wireless sensor network, WSN)由部署在监测区域的大量廉价微型传感器节点组成,通过无线通信方式形成多跳的自组织网络系统,协作地感知、采集和处理网络覆盖区域中感知对象的信息[1]。无线传感器网络在工业控制、精准农业、军事国防、环境监视、医疗救护等领域都有巨大的应用前景,未来可能涉及到人类日常生活和社会生产活动的诸多领域,被认为是将对21世纪产生重大影响的技术之一,已受到国内外学术界的普遍重视。

目前对无线传感器网络的研究手段主要分为两种:一是理论分析和计算机仿真实验,二是实际部署的验证实验。通常而言,无线传感器网络应用场景复杂恶劣,无线通信存在高度动态性且难以预测。而仿真实验通常假设较为理想的模型条件,因而与实际场景有较大区别,降低了仿真性能分析的可信度[2]。

无线传感器网络测试平台是开展实际部署验证的通用平台设施,现有的典型方案包括Crossbow公司提出的MoteWorks[3]、哈佛大学提出的MoteLab[4]、美国加州大学(UCLA)提出的SCALE[5]以及美国俄亥俄州立大学提出的Kansei[6]方案。

Crossbow公司提出的MoteWorks方案经由传感器网络自身的无线通信链路收集测试数据,正常业务数据和测试数据均通过节点的微处理器(MCU)发送到节点的射频模块,然后在无线传感器网络链路上传输。基于MoteWorks平台,用户能够远程监视传感器网络的运行情况,通过文本或图形方

到稿日期:2009-05-14 返修日期:2009-07-01 本文受国家重点基础研究发展规划(973)项目(编号:2006CB303007),国家高科技研究发展计划(863)项目(编号:2008AA01Z120),国家自然科学基金课题(编号:60773212)资助。

李天林(1983—),男,硕士生,主要研究方向为嵌入式系统体系结构、无线传感器网络,E-mail:litianlin@163.com;**皇甫伟**(1975—),男,博士,副研究员,主要研究方向为自组织网络技术和网络测量技术;**杨 煦**(1982—),男,硕士生,主要研究方向为嵌入式软件;**张志强**(1983—),男,硕士生,主要研究方向为软件工程和测试技术;**孙利民**(1966—),男,博士,研究员,博士生导师,主要研究方向为无线传感器网络;**李方敏**(1968—),男,博士,教授,博士生导师,主要研究方向为无线传感器网络和嵌入式系统。

式显示测试结果。MotoWorks 的测试目标是固定设定的，包括网络的拓扑结构、节点的剩余能量、链路质量、传输速率等。以 MoteWorks 为代表的方案无需额外的硬件和传输网络，但测试数据由于占用了传感器网络链路带宽和节点处理器资源，必然对无线传感器网络的自身运行状态有一定的影响。

在哈佛大学开发的 MoteLab 方案中，网络中的每个传感器节点都被连接在额外的测试模块上，而测试模块通过额外的传输通道与中心服务器相连。在 MoteLab 方案中，正常业务数据通过传感器网络自身链路传输，而测试数据通过额外的网络传送到中心服务器，因而不占用无线传感器网络通信资源，极大地降低了测试行为对传感器网络自身状态的影响。然而，MoteLab 仍然需要节点运行特定的测试软件模块，需要占用一定的节点计算资源，仍然对传感器网络运行有一定的干扰。

在上述现有的方案中，其共同特点是节点主动参与测试，测试行为对网络有一定的干扰，从而降低测试结果的准确性。为了更为准确地获得传感器网络运行状态的数据，本文提出一种新的免打扰测试方案，即以旁路侦听的方式捕获节点上微控制器和射频芯片之间的互连信号，进而解析得到节点收发的数据包情况，实现对网络结构和节点正常工作无打扰地测试。

本文介绍非打扰测试系统结构、非打扰式无线传感器网络测试平台的核心部件（无线传感器网络测试仪，简称测试仪）的软硬件设计和实现，以及相关的测试实验结果。

2 系统结构设计

整个无线传感器网络测试平台包括测试仪硬件平台和相关的 PC 机数据分析软件。测试仪将获取的数据转化为特定格式，将预处理的数据发送到中心服务器。测试平台可以用以太网作为传输网络，TCP/IP 协议作为数据传输协议，也可以用其它的网络和协议进行数据传输。本文将主要介绍以太网 TCP/IP 的通信方式。然后根据 PC 机数据分析软件采集的数据即可得到节点通信的所有信息。如图 1 所示，无线传感器网络节点 1，节点 2，…，节点 N 构成了一个无线传感器网络。PC 机作为中心服务器，每个测试仪收集一个节点的信息并通过网络传送给 PC 机。

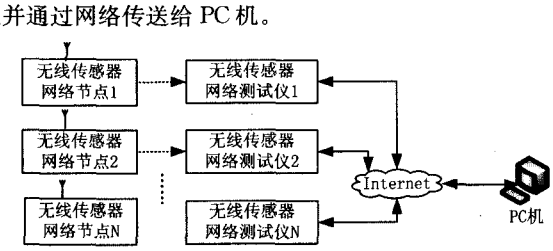

图 1 测试系统结构

测试仪是无线传感器网络测试平台的硬件核心部分。测试仪在对节点自身工作无打扰的前提下，利用硬件采集信号的方法，收集节点内部数字通信信息，并将采集到的信号和数据进行传感器网络性能分析。如图 2 所示，通过采集节点板上 CPU 与射频芯片之间的数据通信信息，从而实现了无打扰、数据真实全面的特性。同时，该方法无需占用传感器网络的无线数据通信链路，也不占用节点 CPU 的资源。

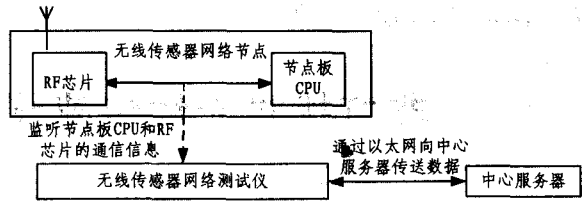

图 2 非打扰式无线传感器网络测试方式

测试仪包含以下几个功能模块：

(1)数据采集模块。负责采集来自节点板的数据通信信息，包括 GPIO 数据采集、AD 采样电路、SPI、I2C 等常用芯片间通信协议的解析电路等。

(2)数据处理模块。其功能是将数据打包成固定格式的数据帧并存放到存储模块中。

(3)数据存储模块。该系统中使用的存储模块是先进先出队列(FIFO)，数据按照采集的时间先后顺序存放。

(4)数据传输模块。负责从 FIFO 区域取出数据并通过以太网或者其他方式发送到 PC 机，包括串口、USB、以太网等可以跟 PC 机通信的设备。

(5)供电模块。

(6)显示输出电路。用于实时显示一些相关信息。

3 无线传感器网络测试仪软硬件实现

本文提出的测试仪采用硬件和软件相结合的设计方式。利用硬件来实现数据采集处理和存储，利用软件来实现数据传输和系统控制。一般节点的数据通信速度在几十 kB/s，短时间内记录节点所有的数据信息并打包处理，一般的处理器难以胜任。所以本文的测试仪选用 FPGA(现场可编程逻辑门阵列)来完成数据的采集和处理，选用 ARM 处理器来实现嵌入式 TCP/IP 协议，充分结合了 FPGA 并行处理的优点和 ARM 程序控制的灵活性。

3.1 硬件设计

本设计选用 Altare Cyclone II 系列中的 EP2C8。此款芯片是在第一代 Cyclone 系列的基础上，基于 90nm，1.2V SRAM 工艺设计，包含 8256 个逻辑单元、36 个 M4K RAM 块共 165888bits、18 个嵌入式乘法器、两个锁相环、182 个用户 IO[7] 等资源。

ARM 处理器选用的是 Atmel 的 AT91SAM7X256。此款芯片的特点是：集成 RISC 架构的 ARM7TDMI ARM Thumb 内核，最高工作频率 55MHz；片内集成 256kB Flash 和 64kB SRAM，集成以太网 MAC 控制器，完全满足一般嵌入式操作系统和嵌入式 TCP/IP 协议的需求；集成了 3 个 USART 串口、SPI 控制器、USB 控制器等[8]。

FPGA 和 ARM 的通信采用 SPI 加 IO 的方式，AT91SAM7X256 芯片上集成的 SPI 控制器的最大通信波特率可达到 ARM 芯片系统时钟的速度，对于我们系统的应用是完全可以满足要求的。利用 AT91SAM7X256 芯片上集成的以太网 MAC 控制器外加一款 10/100M 自适应的以太网物理层控制芯片 DM9161，就构成了一个以太网通信系统。

供电模块支持外接直流 5V，USB，PoE 等供电方式，可以通过开关灵活选择。PoE 供电是本系统的一大特点。PoE 全称为 Power Over Ethernet，是指通过 10BASE-T，100BASE-TX，1000BASE-T 以太网网络供电，其可靠供电的距离最长

为 100m。通过这种方式，可以有效地解决一些网络终端设备的供电问题[9,10]。

采用一片 64Mbits 的 SDRAM 芯片 HY57V641620E 缓存数据，在程序中利用 FPGA 控制 SDRAM 构成一个 FIFO（先进先出队列）的形式。10MHz 并行 AD 采样电路采用 TI 公司的 TLV5510，用于收集节点功耗等模拟信息。4 个八段数码管、蜂鸣器、LED 等声光显示电路用于提示用户系统运行的情况。

利用 FPGA 内部布线的灵活性，来自节点板的采样信号线、串口、AD、LED 显示等外设都是与 FPGA 相连的，然后通过 FPGA 连接在 ARM 上。这种连接方式使得 ARM 和 FPGA 都可以方便地控制这些外设或者采集信号，并且可以简化 PCB 布线。系统的硬件连接结构如图 3 所示。

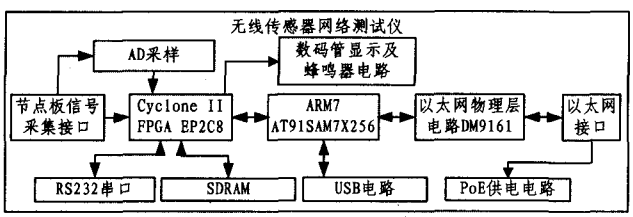

图 3　硬件结构图

3.2　FPGA 程序设计

在测试仪中，FPGA 的作用是采集处理数据，存储数据到 FIFO 中以及响应 ARM 发送的指令，读取 FIFO 中的数据送给 ARM 或者读取计时时间送给 ARM。

FPGA 程序设计采用 Verilog HDL。FPGA 程序包括数据采集模块、时钟模块、FIFO 模块、数据处理存储模块和 ARM 通信及 FIFO 读模块。图 4 是 FPGA 程序的模块结构图。

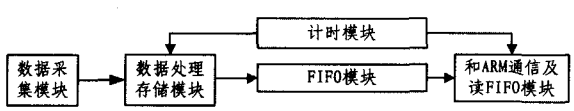

图 4　FPGA 程序模块结构图

FPGA 程序对一些常用的芯片间通信协议解析提供支持，如 SPI 等。解析这些常用的通信协议可以减少存储的数据量。

以下是 SPI 通信数据采集的 Verilog 代码。

```
module SPI_datCollection(SCK,MISO,MOSI,CS,RI,datout);
input SCK;//SPI 通信时钟
input MISO;//SPI 通信的主入从出线
input MOSI;//SPI 通信的从入主出线
input CS;//SPI 通信片选信号
output RI;//收到一个字节后标志信号
output[15:0] datout;//数据输出寄存器
reg[7:0] rMISO,rMOSI;//接收寄存器
reg[2:0] bitcnt;//计数收到的比特数
always @ ( posedge SCK or posedge CS)begin
if( CS ) bitcnt<=3'b0;
else begin
//在每个 SCK 上升沿同时采集 MOSI,MISO 信号
    rMOSI<={rMOSI[6:0],MOSI};
    rMISO<={rMISO[6:0],MISO};
    bitcnt<=bitcnt + 1'b1;
end
//每收到 8bits 产生一个通知信号
assign RI = (bitcnt == 0);
//将收到的数据组成一个 16 位数据送给处理模块
assign datout = { rMISO,rMOSI };
endmodule
```

在 SPI 数据采集模块中，采集数据的时钟来自外边的 SPI 通信时钟，同时均收集主从信号，将数据丢失的可能性降到最低。采集其他通信方式的信号与此类似。

对 GPIO 的采集方式：当 GPIO 管脚有变化时采集一次数据，采集的数据记录的是变化后的 GPIO 管脚的状态，如图 5 所示。AD 数据的采集方法和 GPIO 基本相同，当 AD 数据变化超过设定阈值时采集一次，记录当前值采集的数值，以减小数据量。

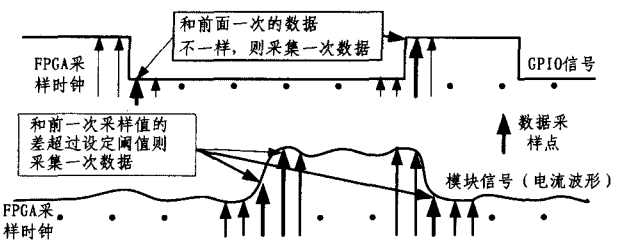

图 5　FPGA 采集 GPIO 和模拟信号数据示意图

单纯用采集的数据恢复通信过程是不全面的，还需加上时间信息。在设计中我们把采集到的节点板通信信息加上 FPGA 时间所形成的固定格式的数据帧称为事件帧。事件帧记录采集数据的类型、时间和数据信息。FPGA 计时模块采用 1MHz 时钟，44bits 计时数据从上电为零开始在整个系统运行过程中一直加计数。

FPGA 采用 1MHz 频率脉冲计时，总共 44bits 来表示时间，可以表示 203.6 天的时间。但是要是每次都把这么长的时间记录在事件帧中，将有很大的数据冗余，所以在系统设计时事件帧中只记录时间低位 14bits，就能表示 16.348ms 的时间。一次无线节点的通信时间也就在毫秒数量级，数据采样的频率也是 1MHz。如果在记录一个事件的时候发生时间高位与上一次记录事件时不同，则先发送一个时间高位变化帧。时间帧的格式基本相同，也是 32bits，只是用高两位表示这是一个时间帧，后面 30bits 表示目前的时间高位值。

数据处理存储模块工作的过程：每次有效时钟到来时就判断是否有新的数据采集到。如果有新的数据采集到，则判断 FPGA 计时时间的高位（14bit～43bit）是否和上次相同；如果不同，则先存入一个时间高位数据帧到存储区，并等到下一个时钟周期处理相关数据。如果有数据采集到，则将数据加上时间低位（0～13bit）及类型值，组成事件帧存入存储区。以下是数据处理存储部分的关键代码。

```
always @ ( posedge clk )
begin
//首先判断是否采集到新数据并且时间高位(14bit～43bit)和上次采集数据时不同
if( ( SPIfull ||( PreIOdat ! = regIOdat )||ADGET…) &&( PreTime[43:14]! =TMR[43:14] ) )begin
wrdat = {2'b11,TMR[43:14]};//写时间高位帧到存储区
wrreq = 1'b1;
PreTime = TMR;//记录下本次采集的时间高位
```

```
end
else if( SPIfull ) begin//如果采集的是 SPI 数据
//写 SPI 数据帧到存储区
wrdat = {2'b00,TMR[13:0],SPIdat};
  //事件帧,2'b00 表示事件类型,TMR[13:0]是时间低位,SPI-
dat 是采集到的数据
wrreq = 1'b1;
  SPIRD =~SPIRD;//设置数据已经处理的标志
end
……//其他通信方式或者数据记录处理
else wrreq = 0;// wrreq 下降沿写入数据到存储区
end
```

与 ARM 通信的一端是一个 SPI 从机。当 ARM 发送指令过来时,就做出相应的回答。

3.3 ARM 程序设计

本测试仪的 ARM 软件系统基于 FreeRTOS 和 LwIP。FreeRTOS[11]和 LwIP[12]都是开源软件,很容易获取,并且易学易用,在嵌入式系统中有广泛的应用。

ARM 程序的主要功能是从 FPGA 中读取数据或时间,并通过以太网或者是其他方式发送到 PC 机。

程序分为两个任务,其中任务 1 是查询 FIFO 中是否有数据,如果有则读取并发送;任务 2 是每间隔 1s～2s 的随机时间后读取 FPGA 的计时时间,并通过 UDP 发送到上位机。

ARM 初始化后就进入任务 1 和任务 2。任务 1 开始进入尝试建立 TCP/IP 连接状态。如果建立成功,就进入查询 FIFO 状态。如果 FIFO 中有数据,则读出并通过 TCP/IP 发送。这样,在建立成功前的数据就全部存在 FPGA 控制的 FIFO 中,数据就不会丢失。任务 2 的功能是隔一段时间向中心服务器发送 FPGA 的计时时间。发送时间的要求是要尽量小的延迟,所以任务 2 中时间的发送选用 UDP。

4 实验测试

测试实验选用 ZN-05 组建具有无线传感器网络分布式自组织特点的待测网络,ZN 系列节点是中国科学院软件研究所无线自组织网络研究中心自行研发的无线传感器网络节点。该节点兼容 Crossbow 公司的 Telosb 节点。ZN-05 节点的设计结构与特点如下:

通信模块采用 Chipcon 公司的支持 IEEE 802.15.4 协议的无线收发芯片 CC2420,最大通信速率为 250k bps,0dbm 功率通信距离可达 100m。

将 TI 公司的超低功耗微处理器芯片 MSP430F1611 用作 CPU,MSP430F1611 和 CC2420 的通信方式是 SPI 及几个 IO 端口。

提供了丰富的 40 引脚外部接口,可以连接编程板或传感器板。

支持 TinyOS 操作系统,方便软件编程与烧写,体积小(面积 80mm * 35mm,厚度 2mm)。

将 ZN-05 节点和测试仪通过数据采集转接板相连,如图 6 所示,转接板的作用就是适配不同型号的节点。根据 CC2420 的操作特点,本实验中要引出的是 MSP430F1611 和 CC2420 通信的 SPI,INT,SFD,FIFOP,FIFO,CCA,GPIO[14]等引脚的信号。连接转接板和测试仪,然后将测试仪通过交换机和 PC 机相连。给系统上电后,启动为测试仪配套的上位机软件 HCAT,捕捉数据后保存。再通过 HCAT 系列软件中的分析软件分析数据结果。

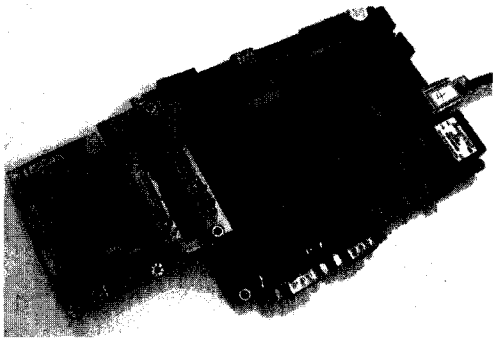

图 6 测试仪连接测试节点实物图

通过分析这些数据,就可以得到节点收发包的情况了。图 7 是节点收包过程逻辑分析仪捕捉波形和测试仪捕捉波形的比较图。根据 CC2420 数据手册说明,在接收模式中,若收到帧起始定界符(the Start of Frame Delimiter,SFD)管脚变高。若收到正确的数据帧,INT 管脚变低,CPU 开始通过 SPI 通信方式读取 CC2420 的 RXFIFO 中的数据。图 7(a)是逻辑分析仪捕捉的,所用的逻辑分析仪是周立功公司的 LA1016 型逻辑分析仪。图 7(b)是通过无线传感器网络测试平台软件中的 HCAT 波形分析软件分析测试仪上传的数据而画出的波形。由图可以看出,测试仪良好、准确地采集了节点通信信息。

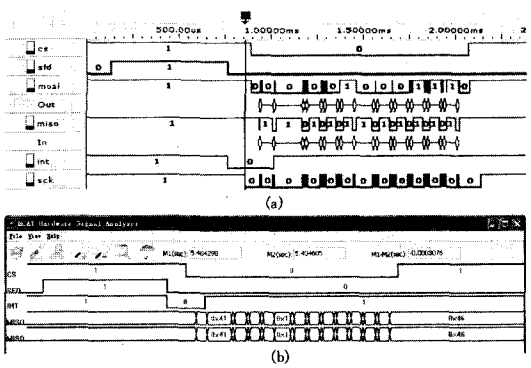

图 7 节点收包过程逻辑分析仪捕捉波形和测试仪捕捉波形比较

结束语 网络性能的测量评估是传感器网络研究领域的共性技术需求之一,经过近年国际国内的研究,已经取得了一定的研究成果。本文提出了一种新型非打扰式无线传感器网络测试方法,并介绍了该方法的测试仪的软硬件设计思路和实现方法。通过测试证明,此测试仪可以客观地反映节点的通信情况。测试仪可以全部截取节点数据通信的过程,得到节点通信的所有信息。通过无线传感器网络测试平台软件,可以分析从测试仪上传的数据,得到无线链路的质量(吞吐率、延迟、丢包率等)、节点功耗等参数。

参 考 文 献

[1] 孙利民,李建中,等.无线传感器网络[M].北京:清华大学出版社,2005

[2] 柯欣,舒坚,等.无线传感器网络测试技术与测试平台研究[J].计算机科学,2007,34(1):120-122

[3] MoteWorks. Wireless Sensor Network Platform[EB/OL]. www.xbow.com,2009

(下转第 62 页)

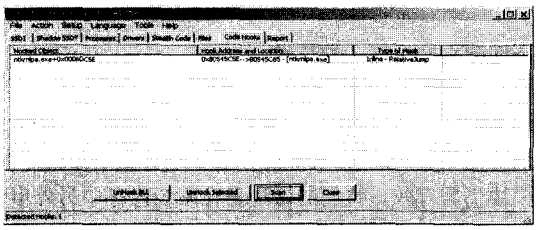

图 5 Rootkit Unhooker 代码钩子检测结果

结束语 网络攻防技术日新月异，隐藏技术也在攻防交替中不断发展和演变。本文在对传统 Rootkits 隐藏技术分类研究的基础上，提出了一个集驱动模块整体移位、内核线程注入、IRP 深度内联 HOOK 3 种技术为一体的 Rootkits 隐藏技术体系，并实现了一个基于该隐藏技术体系的 Rootkits 原型系统。实验结果显示，本 Rootkits 能够很好地躲避专业的 Anti-Rootkits 工具(如 Rootkit Unhooker 和冰刃)的检测，充分表明了这种三位一体的 Rootkits 隐藏体系的有效性。

Rootkits 技术是计算机系统安全的关键技术之一，其本身是中性的。在杀毒软件、防火墙、入侵检测系统等安全软件中，Rootkits 技术同样得到了广泛应用，发挥了强大的作用。随着网络安全的重要性日益显现，Rootkits 技术也必定会有更广阔的应用前景。

参 考 文 献

[1] CERT/CC. Ongoing Network Monitoring Attacks[EB/OL]. http://www.cert.org/advisories/CA-1994-01.html,1997-09-19

[2] Alisa S. Rootkit evolution [EB/OL]. http:// www. viruslist.com/en/analysis? pubid=204792016,2008-08-28

[3] Greg H, James B. Rootkits: Subverting the Windows kernel [M]. Addison Wesley Professional,2005:46-47

[4] Intel. Intel 6 4 and IA-32 Architectures Software Developer's Manual Volume 1: Basic Architecture, chapter 6[EB/OL]. http://download.intel.com/design/processor/manuals/253665.pdf,2006:5-11

[5] Rutkowski J K. Advanced Windows 2 0 0 0 Rootkit Detection [Z]. http://www.securitytechnet.com/resource/rsc-center/presentation/black/vegas03/bh-us-03-rutkowski.pdf. ,2003-07-01

[6] Levine J G. A Methodology for Detecting and Classifying Rootkit Exploits[D]. School of Electrical and Computer Eng. ,Georgia Inst. of Technology,2004

[7] Pietrek M. Peering Inside the PE: A Tour of the Win32 Portable Executable File Format[J]. Microsoft Systems Journal,1994

[8] xrayn. Hide your SSDT hooks[EB/OL]. http://www.rootkit.com/newsread.php? newsid=922,2008-11-08

[9] Doug W. Methods for Detecting Kernel Rootkits [D]. University of Louisville,2007

[10] Barry B. Intel 微处理器[M]. 北京：机械工业出版社，2008：45-47

[11] Russinovich M, Solomon D. 深入解析 Windows 操作系统[M]. 潘爱民，译. 北京：电子工业出版社，2007：87-90

[12] Levine J G, Grizzard J B, Hutto P W, et al. A Methodology to Characterize Kernel Level Rootkit Exploits that Overwrite the System Call Table[C]// Proceedings of IEEE. SoutheastCon, IEEE,2004:25-31

[13] Levine J G, Grizzard J B, Owen H L. A Methodology to Detect and Characterize Kernel Level Rootkit Exploits Involving Redirection of the System Call[C]// Second IEEE International Information Assurance Workshop. 2004

[14] Levine J G, Grizzard J B, Owen H L. Detecting and categorizing kernel-level rootkits to aid future detection[M]. IEEE Security & Privacy,2006

[15] 张帆，史彩成. 驱动开发技术详解[M]. 北京：电子工业出版社，2008：186-187

[16] Molina D, Zimmerman M, Roberts G. Timely Rootkit Detection During Live Response [M]. Springer Boston,2008:139-148

[17] Hoglund G, Butler J. Rootkits: Subverting the Windows kernel [M]. Addison Wesley Professional,2005:290-291

[18] Microsoft Corporation. Windows 2000 驱动程序开发大全(第 1 卷)[M]. 北京：机械工业出版社，2001：27-36

[19] Greg H, James B. Rootkits: Subverting the Windows kernel [M]. Addison Wesley Professional,2005:173-183

[20] 罗云彬. Windows 环境下 32 位汇编语言程序设计(第 2 版)[M]. 北京：电子工业出版社，2007：667-670

(上接第 48 页)

[4] Werner-Allen G, Swieskowski P, Welsh M. MoteLab: A Wireless Sensor Network Testbed[C]// Proceedings of the 4th International Symposium on Information Processing in Sensor Networks. 2005

[5] Cerpa A, Busek N, Estrin D. Scale: A Tool for Simple Connectivity Assessment in Lossy Environments[R]. CENS Technical Report 0021. Los Angeles: Center for Embeded Networked Sensing, University of California, September 2003

[6] Emre E, et al. Kansei: a testbed for sensing at scale[C]// Proceedings of the 5th International Symposium on Information Processing in Sensor Networks. 2006

[7] Altare. Cyclone II Data Sheet CII5V1-3.3[EB/OL]. www.altera.com,2008

[8] Atmel, AT91 ARM Data Sheet[EB/OL]. www.atmel.com, 2007

[9] IEEE 802.3af. Data Terminal Equipment (DTE) Power via Media Dependant Interface(MDI)[M]. IEEE Computer Society, June 2003

[10] Dwelley D. Linear Technology Inc. New Power for Ethernet-The LTC4255 Delivers[J]. Linear Technology Magazine, Augst 2002

[11] 刘滨，王琦，刘丽丽. 嵌入式操作系统 FreeRTOS 的原理及实现[J]. 单片机与嵌入式系统应用，2005(07)

[12] Dunkels A. Design and Implementation of the LwIP TCP/IP Stack[J]. Swedish Institute of Computer Science, February 2001

[13] Labrosse J J. 嵌入式实时操作系统 μC/OS-Ⅱ(第 2 版)[M]. 邵贝贝，译. 北京：北京航空航天大学出版社，2003

[14] Chipcon. CC2420 Data Sheet[EB/OL]. www.ti.com,2004