信息设备电磁辐射信息泄漏的可检测距离估计方法研究

徐艳云, 张 萌, 黄伟庆

中国科学院信息工程研究所 北京中国 100093

摘要 信息设备在工作过程中会产生电磁辐射，通过截获电磁辐射信号可重建信息设备中正在处理的有用信息，这给信息安全带来了巨大风险。本文从信息设备电磁辐射的可检测距离来估计信息设备电磁信息泄漏风险，结合理论和实验分析，从辐射泄漏源、电磁环境信道以及接收设备三个方面，分析了信息设备电磁辐射泄漏可检测距离的影响因素，提出了一种信息设备电磁辐射信息泄漏的可检测距离估计方法。并以传真机为实例，利用本文所提方法估计了使用现场环境下传真机的电磁辐射可检测距离。本方法充分考虑各信息设备电磁泄漏特征和环境的差异，适用于不同信息设备、不同使用现场环境下，对可检测距离的合理估计，从而避免对信息设备的过防护和欠防护。

关键词 电磁安全; 信息泄漏; 电磁辐射; 泄漏发射; 可检测距离
中图法分类号 TP 319 DOI 号 10.19363/J.cnki.cn10-1380/tn.2020.01.05

Study on detectable distance for electromagnetic information leakage of information equipment

XU Yanyun, ZHANG Meng, HUANG Weiqing

Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China

Abstract Information equipment is accompanied with electromagnetic radiation as it works. The radiation brings electromagnetic interference and risks of information leakage. In this paper, based on the theoretical and experimental analysis, the influences of electromagnetic radiating source, environment channel and capability of available receiving devices are discussed. The estimation method of detectable distance for electromagnetic compromising emanation of information equipment is proposed. As an example, the detectable distance of facsimile is estimated using this method. Considering electromagnetic leakage feature and environment, the method is suitable for different information equipments and environment to estimate the detectable distance properly. The over protection and owe protection of information equipment can be avoided.

Key words electromagnetic security; information leakage; electromagnetic radiation; compromising emanation; detectable distance

1 引言

电子信息设备在工作过程中会产生电磁发射，一方面对周围电子设备形成电磁干扰，另一方面形成有用信息的泄漏。虽然国际国内电磁干扰标准限制了电子信息设备的电磁辐射，但信息设备在工作过程中，仍然会产生电磁发射，造成处理信息的电磁泄漏。随着信息化的飞速发展，更多的从信息安全角度关注电磁信息泄漏。信息安全管理系统(Information Security Management System, ISMS)标准也已由国际标准化组织和国际电工委员会联合公布[1]。国际电信联盟的电信标准化部门也制定了电信的 ISMS 标准[2]。在这些信息安全管理系统标准中，由于电子设备电磁发射造成的信息泄漏被认为是物理安全问题，并推荐了评估和防护方法，来应对由电磁发射引起信息泄漏的安全风险，并常用

通讯作者： 徐艳云，博士，高级工程师, Email: xuyanyun@iie.ac.cn。
本课题得到国家自然科学基金资助项目(No. 61601460)资助。
收稿日期: 2018-03-06; 修改日期: 2018-06-23; 定稿日期: 2019-12-09

TEMPEST 和泄漏发射安全(Emanations security, EMSEC)表示此类信息泄漏和防护[3]。

20 世纪 50 年代初, 美国军方发现计算机系统杂散的电磁辐射会导致一部分重要的信息泄漏, 由此发展了信息技术设备的 TEMPEST 技术的研究, 其主要针对电子信息设备信息泄漏的研究。60 年代, 英国开始组织信息电磁泄漏防护与侦收技术研究, 随后德国、加拿大等国相继投入研究。由于涉及军事机密甚至国家安全, 信息电磁泄漏问题自提出之日起就成为美国政府严格保密的军事机密, 研究成果和技术细节不允许公开讨论。直到 90 年代, 美国等国逐渐解密了一批 TEMPEST 文件, 泄漏电磁发射的研究才公之于世[4-7], 经过国内外研究学者的不懈努力, 近年来在电磁泄漏领域不断出现新的挑战, 如泄漏发射限值和距离估计、电力线、传真机、密码芯片、恶意硬件, 以及对现代处理系统电磁泄漏、电磁泄漏防护、电磁测试等[6-20]问题。

20 世纪 80 年代以来, 我国开始关注 TEMPEST 技术, 在泄漏发射及其防护机理、泄漏电磁发射信息接收和重构、微机系统电磁泄漏防护技术等方面取得了一定的成果[21-29], 近几年在电磁泄漏重建和防护、数字系统的电磁泄漏、基于电磁泄漏的隐蔽传输、电磁指纹识别、电力线传导泄漏、传真机电磁泄漏、电磁攻击以及物理空间安全等[30-39]方面取得重大突破。

通过接收和分析信息设备电磁泄漏信号, 可重建信息设备中正在处理的信息, 因此为了对信息设备电磁泄漏进行科学有效的防护, 信息设备在一定距离处的信息泄漏风险评估十分重要。电磁辐射泄漏可检测距离的研究有助于信息泄漏的正常防护, 避免过防护和欠防护。本文讨论电子信息设备电磁辐射造成的信息泄漏风险, 重点关注辐射发射信息泄漏的可检测距离的估计。有学者对此进行了研究[9], 但其结果基于 GB9254(CISPR22)电场强度标准发射限值, 过高的估计了实际可接收的最大距离, 没有考虑到辐射源信号特征对其在电磁空间信道中传播的影响。

在本文, 我们提出了一种具有普适性的信息设备电磁泄漏可检测距离估计的一般方法。其基本思想是在对泄漏发射源激励信号特征和其等效天线参数分析的基础上, 估计其辐射效能及其在空间传播和衰减规律, 然后利用天线和接收机对辐射信号进行接收, 实测泄漏源辐射电场强度, 再通过评估接收设备(天线和接收机)性能, 估计电磁泄漏可检测距离。该方法充分考虑泄漏源信号特征、信道衰减和接收性能, 采用理论和实测相结合的评估方法, 大大提高了信息设备电磁信息泄漏风险评估的准确性和合理性。

本文的主要贡献如下:

(1) 提出了一种信息设备电磁泄漏可检测距离风险评估方法, 该方法将信源、信道和信宿的各因素考虑进去, 提高了风险评估的准确性。

(2) 该估计方法具有普适性, 适用于不同泄漏源、电磁环境和接收设备, 充分考虑各因素的变化, 给出不同的可检测距离。

(3) 该估计方法理论和实测分析相结合, 通过分析泄漏源信号特征、实测泄漏源强度、分析接收设备性能等重要步骤, 估计不同环境下的电磁辐射可检测距离。

本文第二节介绍信息设备电磁辐射发射导致的信息窃收风险。第三节从辐射源、电磁空间信道以及接收设备性能三个方面, 分析信息设备辐射电磁泄漏可检测距离的影响因素, 提出信息设备辐射电磁泄漏可检测距离估计的一般方法。给出了现有条件下, 传真机电磁辐射泄漏可检测距离的估计实例, 讨论了接收带宽对距离估计结果的影响。第四节分析了信号处理增益和信道衰减等参数对可检测距离估计的影响, 对距离估计公式进行修正。第五节为结束语。

2 信息设备电磁辐射信息泄漏风险

2.1 信息设备电磁泄漏框架

信息设备工作过程中产生的电磁辐射会产生信息的泄漏, 其辐射模型如图 1 所示:

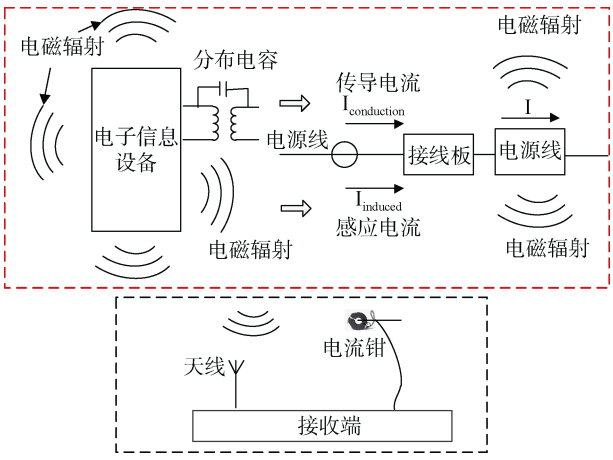


图 1 电磁泄漏框架图

Figure 1 Electromagnetic emanation frame

根据麦克斯韦定律, 信息设备工作过程中的电缆、电路、视频显示器和接地系统等会像天线一样产生电磁辐射, 我们称之为自然天线或等效天线,

由此产生的电场强度记为 E_1。

其次, 电源线、电话线或其他通信线可作为传导介质, 传输信息设备中的电信号导致传导泄漏, 泄漏电流记为 $I_{conduction}$, 同时, 电源线、电话线或其他通信线可感应信息设备辐射的信号, 依据法拉第电磁感应定律[40], 感应电动势可表示为:

$$\varepsilon_{Bin} = -\frac{d\Phi}{dt} = -\frac{d}{dt}\int_S B \cdot \mathrm{d}S \tag{1}$$

其中 Φ 表示磁通量, B表示磁场, $\mathrm{d}S$ 表示面元, 由此产生感应电流记为 I_{Bin} 。除此之外, 线上还含有电场耦合的电流记为 I_{Ein}, 因此得到线上总的感应电流为:

$$I_{induced} = I_{Bin} + I_{Ein} \tag{2}$$

由此, 可得电源线、电话线或其他通信线上传输的总电流为: $I = I_{conduction} + I_{induced}$

同样依据麦克斯韦定律, 变化的电场产生磁场, 变化的磁场产生电场, 由于不断变化的电流 I, 电源线、电话线或其他通信线周围同样存在着自身辐射电磁波, 该电场强度记为 E_2。

利用合适的传感设备和专用接收设备, 即可对电磁波或线上电流进行截获, 重建出信息设备中正在处理的有用信息, 给信息安全带来巨大挑战和威胁。

2.2 信息设备电磁泄漏风险检测

信息设备电磁辐射泄漏风险检测实验场景图如图 2 所示, 被测试信息设备位于图的右侧, 利用天线感应空间电磁信号, 经宽带接收机下变频输出至示波器采集, 实现对电磁泄漏信号获取。

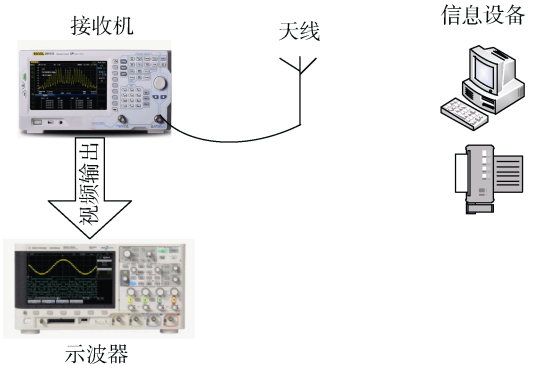


图 2 实验场景图

Figure 2 Measurement setup

2.2.1 计算机电磁信息泄漏

计算机显示的视频图像如图 3 所示。

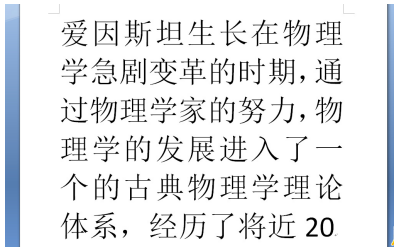
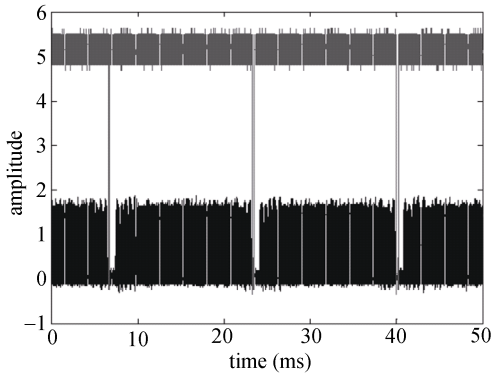


图 3 计算机显示视频图像

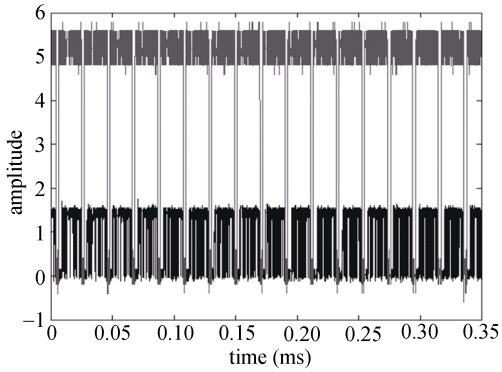
Figure 3 Video image in computer

其时域信号如图 4 所示, 图 4(a)为可看到场同步的视频信号, 图 4(b)为可看到行同步的视频信号, 该信号具有模拟、串行、高频、明文等特点, 存在较大的信息泄漏风险。利用图 2 对计算机电磁泄漏信号进行采集, 得到图 5 所示信号, 对其进行预处理和频谱分析, 得泄漏频谱如图 6 所示。可看到明显的计算机视频信息的频谱特点, 并包含行频和场频等重要参数信息。



(a) 场同步及视频时域信号

(a) Field sync and video time signal



(b) 行同步及视频时域信号

(b) Horizonal sync and video time signal

图 4 时域信号

Figure 4 Time domain signal

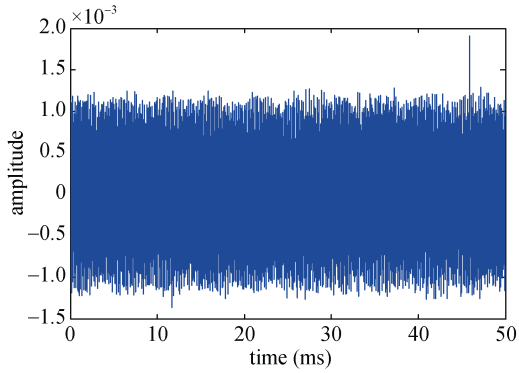


图 5 计算机电磁泄漏信号

Figure 5 Computer electromagnetic emanation signal

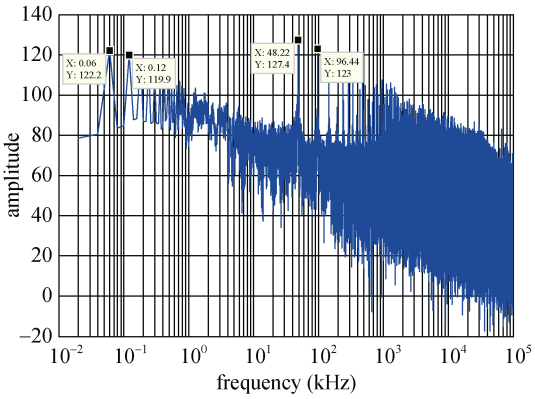


图 6 泄漏频谱

Figure 6 Emanation spectrum

对该电磁泄漏信号进行信息重建得到图 7 所示计算机电磁泄漏视频图像。

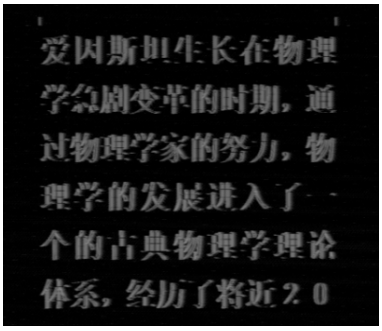


图 7 计算机视频还原图像

Figure 7 Computer video reconstruction image

2.2.2 传真机电磁信息泄漏

传真机在工作过程中同样存在电磁辐射产生信息泄漏。传真机的风险测试模拟系统图如图 8 所示, 被测传真机为发送传真端标记为 1, 标记为 2 的传真机作为接收端, 两个传真机通过电话交换机相连组成一个小型的传真通信系统。

发送传真的样张如图 9 所示的英文字符。传真机中光电变换后的电信号如图 10 所示, 可见其模拟、串行、明文等特点。

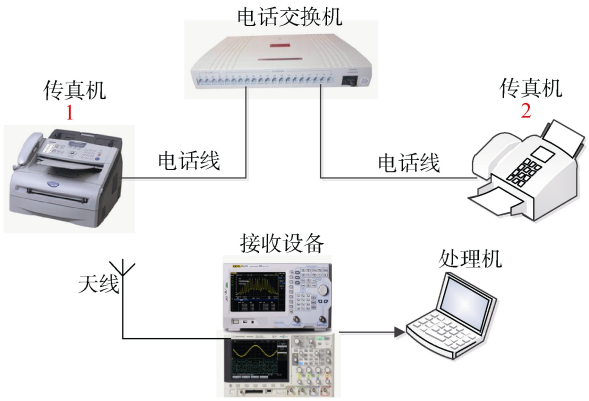


图 8 模拟传真系统

Figure 8 Analog fax system

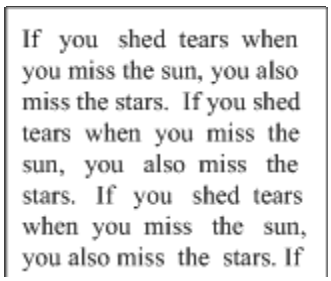


图 9 发送传真样张

Figure 9 Faxing paper information

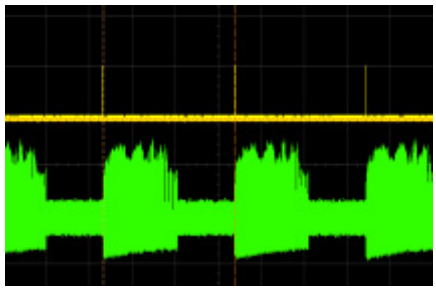


图 10 传真时域信号

Figure 10 Faxing signal in time domain

在传真机传真工作过程中, 利用图 2 对其电磁泄漏信号进行采集, 并进行信号处理和信息还原, 得到重建传真信息如图 11 所示。

由以上分析可见, 信息设备在工作过程中处理的有用信息可通过电磁辐射的途径产生信息泄漏, 给信息安全带来极大的风险隐患。为了更好的估计信息设备电磁信息泄漏风险, 确定信息设备工作的

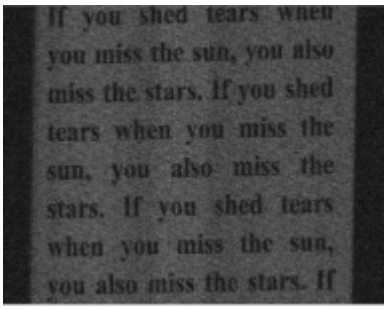


图 11 传真信息还原图像

Figure 11 Reconstruction image of faxing information

安全距离, 本文提出信息设备电磁泄漏最大可检测距离估计的一般方法, 从而可对信息设备实施有效防护, 降低电磁信息泄漏风险。

文中后续描述中用到的主要符号和变量, 总结如下表:

表 1 文中用到的主要符号和变量

Table 1 The main symbols and variables

符号	含义	符号	含义
I_0	幅值	λ	波长
T	周期	η	真空波阻抗
t_r	升降沿	φ	场点在 xy 平面的垂点与 x 轴的夹角
T_w	脉宽	θ	场点与 z 轴的夹角
ω	角频率	f	频率
μ_0	真空磁导率	β	波数
SNR	接收机要求的输入信噪比(输入信号电压与噪声电压的比值)	P_n	接收机噪声功率
Z_r	接收机输入阻抗	P_{dn}	接收机噪声功率密度
Z	天线输出阻抗	B	接收机带宽
V_n	接收机输入噪声电压	Z_{ref}	半波偶极子天线输出阻抗
V_i	接收机输入信号电压	V_o	天线开路电压
G	相对增益	d_r	参考距离
E_{d_r}	参考点泄漏电场强度值	d	场点到信息设备的距离
E_{Bw}	带宽为 Bw 时接收机可接收到的最小电场强度	E_d	距离 d 处信息设备电磁辐射电场强度
x	电磁波衰减指数	d_m	最大可检测距离

3 电磁泄漏可检测距离的估计方法

由通信系统模型表征信息设备的电磁辐射泄漏, 如图 12 所示。辐射源为信息设备电磁辐射泄漏源即信源, 电磁环境为电磁辐射传播介质即信道, 接收设备为接收和检测电磁辐射泄漏的专用设备即信宿。对电磁泄漏可检测距离的估计, 与信源辐射电场强度、信道衰减特性以及信宿接收性能有着密切关系。本节将针对其各方面的影响研究信息设备电磁泄漏可检测距离的估计方法。

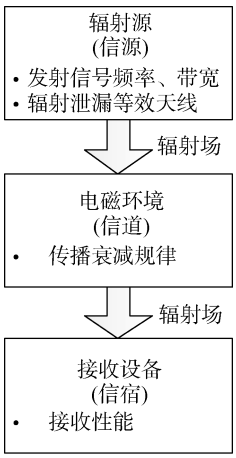


图 12 信息设备电磁辐射通信模型

Figure 12 Electromagnetic radiation model of information equipment

3.1 信息设备辐射泄漏电场强度

信息设备辐射泄漏可检测距离与辐射泄漏电场强度密切相关, 而辐射电场强度与泄漏源的激励信号和等效天线特性密切相关。因此, 本节首先分析信息设备激励信号基本特征, 然后根据信息设备中普遍存在的潜在等效天线基本参数, 如电流、频率、极化、长度等特点, 对辐射泄漏发射源建模, 进而可估计辐射电场强度、辐射信号频率范围、及其在电磁信道中的传播衰减规律。

3.1.1 信息设备激励信号

信息设备中常见的激励信号是参数各异的梯形波。图 13 所示为周期梯形波, 设其为 $f(t)$, 幅值、周期、升降沿及脉宽分别由 I_0, T, t_r, T_w 表示。

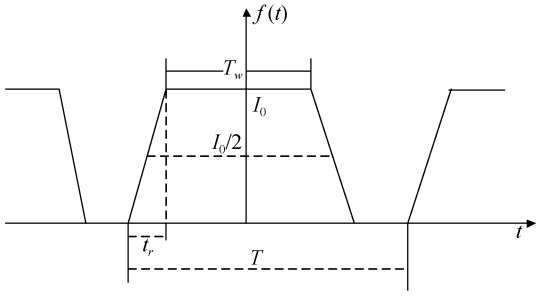


图 13 激励信号

Figure 13 Drive signal

该激励信号可表示为傅里叶级数的形式:

$$f(t)=\sum_{n=-\infty}^{\infty}F_n e^{j\omega_n t} \tag{3}$$

其中,

$$F_n=\frac{1}{T}\int_{-T/2}^{T/2}f(t)e^{-j\omega_n t}\mathrm{d}t=\frac{I_0T_w}{T}H(\omega_nT_w)H(\omega_nt_r) \quad (4)$$

其中, $H(\omega_nT_w)=\sin(\omega_nT_w/2)/\omega_nT_w/2$, $\omega_n=2n\pi/T$, 推导可得到其傅里叶变换为:

$$F(\omega)=\frac{1}{2\pi}\sum_{n=-\infty}^{\infty}F_n\int_{-\infty}^{\infty}e^{j(\omega_n-\omega)t}\mathrm{d}t$$

$$=\sum_{n=-\infty}^{\infty}F_n\delta(\omega-\omega_n) \quad (5)$$

可见周期梯形波信号的谱分布只有窄带谱, 分布在 $\omega=\omega_n$ 的频率点上。

对于非周期梯形波信号, 其傅里叶变换可表示为:

$$f(t)=\int_{-\infty}^{\infty}F(\omega)e^{j\omega t}\mathrm{d}\omega \quad (6)$$

其中,

$$F(\omega)=\lim_{T\to\infty}\frac{T}{2\pi}\int_{-\infty}^{\infty}F_n\delta(\omega'-\omega)\mathrm{d}\omega'$$

$$=\frac{I_0T_w}{2\pi}H(\omega T_w)H(\omega t_r) \quad (7)$$

3.1.2 信息设备等效发射天线模型

(1) 信息设备 PCB 电路模型

信息设备的电路一般由数字 PCB 实现, 数字电路驱动电流大, 辐射强度大, 高速时钟脉冲和数字信号使辐射频带加宽, 造成潜在的信息泄漏风险。

当 PCB 的某一轨迹为单根电路, 轨迹长度远小于激励信号波长和轨迹至场点距离时, 可认为轨迹上电流均匀分布, 为电偶极子模型。

当 PCB 的某一轨迹为小回路, 回路的线度远小于激励信号波长和轨迹至场点距离时, 则构建为磁偶极子模型。

对于周期梯形波的电流激励, 远场区电偶极子和磁偶极子模型的辐射电场强度可表示为:

$$E_\theta(r,t)=\sum_{n=1}^{\infty}E_\theta(f_n)\sin(\omega_nt-\beta_nr) \quad (8)$$

$$E_\varphi(r,t)=\sum_{n=1}^{\infty}E_\varphi(f_n)\cos(\omega_nt-\beta_nr) \quad (9)$$

其中

$$E_\theta(f_n)=-\frac{2K_eI_0lT_wf_n}{Tr}H(\omega_nT_w)H(\omega_nt_r)\sin\theta \quad (10)$$

$$E_\varphi(f_n)=\frac{2K_mI_0ST_wf_n^2}{Tr}H(\omega_nT_w)H(\omega_nt_r)\sin\theta \quad (11)$$

$\beta_n=2\pi/\lambda_n$, λ_n 为波长, r 为源到场点的距离, l 为轨迹长度。

对于非周期波的电流激励, 设 η 为真空波阻抗, S 为回路的等效面积, 辐射场为频率为 ω 的辐射(表示信号带宽内某一频点的宽带辐射), 其远场区电偶极子和磁偶极子模型的辐射电场强度可表示为:

$$E_\theta(r,t)=\int_0^{\infty}E_\theta(f)\sin(\omega t-\beta r)\mathrm{d}\omega \quad (12)$$

$$E_\varphi(r,t)=\int_0^{\infty}E_\varphi(f)\cos(\omega t-\beta r)\mathrm{d}\omega \quad (13)$$

其中 $\beta=2\pi/\lambda$,

$$E_\theta(f)=-\frac{K_eI_0lT_wf}{Tr}H(\omega T_w)H(\omega t_r)\sin\theta \quad (14)$$

$$E_\varphi(f)=\frac{2K_mI_0ST_wf^2}{Tr}H(\omega T_w)H(\omega t_r)\sin\theta \quad (15)$$

其中 $K_e=\eta/2c$, $K_m=\pi\eta/c^2$。

从以上分析可见, 周期电流激励为窄带幅频关系, 非周期电流激励为宽带幅频关系[22]。由电偶极子和磁偶极子的辐射电场强度可分别画出图 14(a)和图 14(b)的辐射特性, 其中 dB/dec 表示分贝/每十倍频, 可以看出, 电偶极子的辐射在频率低端呈上升趋势, 而在频率高端呈衰减趋势, 磁偶极子的辐射在频率高端几乎无衰减, 在频率中低端具有增加趋势。

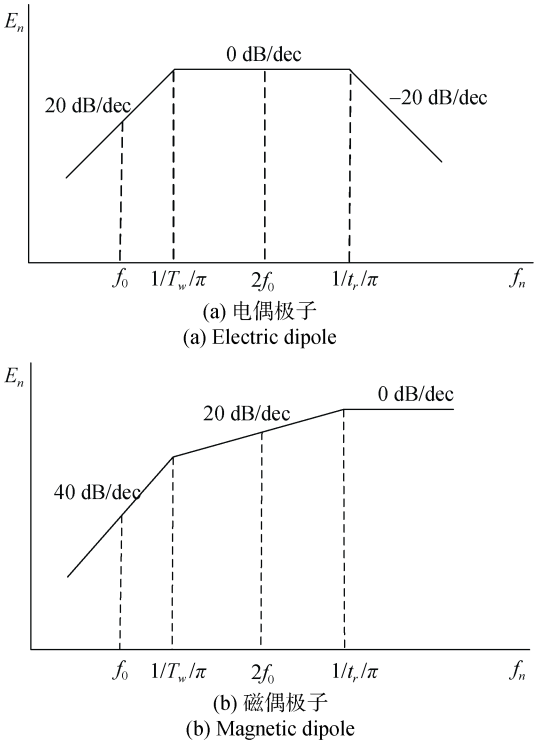


图 14 辐射特性

Figure 14 Radiation characteristic

(2) 信息设备传输线模型

当信息设备中存在线缆产生电磁信息泄漏, 而其线度 l 比激励信号波长和源至场点距离 r 大的多时, 可建立传输线双线模型如图 15 所示[22]。

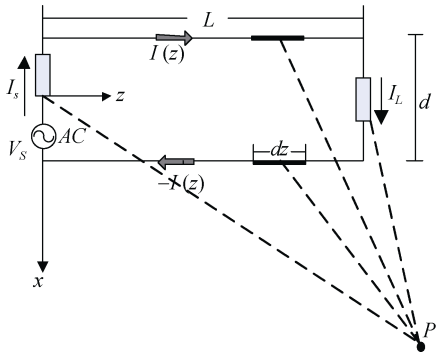


图 15 传输线模型

Figure 15 Transmission line model

当已知线缆的参数, 依据传输线理论, 可以认为沿线电流分布 $I(z)$是已知的。设两线间的距离 d 远小于线缆到场点 P 的距离 D, 场点与双线平面成夹角 α, 场点 P 可获取的最大辐射电场可表示为:

$$E_z=\begin{cases}\dfrac{\omega\mu_0 Il}{4\pi D}e^{-j\beta D}\left(1+\dfrac{1}{j\beta D}+\dfrac{1}{(j\beta D)^2}\right)\cos\alpha, & f<100\text{MHz}\\ \dfrac{\omega\mu_0 le^{-j\beta D}}{4\pi D}\dfrac{\sin(\beta l/2)}{\beta l/2}\left(I^{+}+I^{-}\right)\cos\alpha, & f\geqslant 100\text{MHz}\end{cases} \tag{16}$$

式中, 对于信号频率 f < 100MHz, 设 V_S 为激励源电压, 线缆激励源阻抗为 Z_S, 负载阻抗为 Z_L, 则可认为:

$$I(z)=I=V_S/(Z_S+Z_L) \tag{17}$$

对于 f>100MHz, I^{+}和 I^{-}可由传输线理论确定:

$$I^{+}+I^{-}=\frac{V_S}{Z_C+Z_S}e^{-j\beta l/2}\left[\frac{1-\rho_L e^{-j\beta l}}{1-\rho_L\rho_S e^{-2j\beta l}}\right] \tag{18}$$

其中 Z_C 为线缆特征阻抗, ρ_L, ρ_S 为负载和激励源的反射系数。

对于信息设备中存在的多线电缆泄漏, 一般公用一根导线作为地线或者回流线, 因此 n 根导线组成的电缆可以看作(n–1)对传输线, 整个电缆的辐射结果则为(n–1)对传输线各自辐射结果的叠加。

3.1.3 参考场点电场强度估计

基于以上分析, 在对信息设备激励信号和等效发射天线评估的基础上, 提出参考场点电场强度的总体估计方案, 如图 16 所示, 用于估计信息泄漏源在参考点处的辐射电场强度。

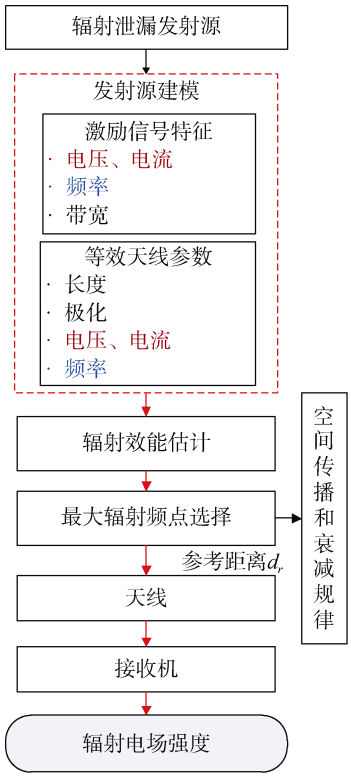


图 16 参考场点泄漏电场强度估计方案

Figure 16 Electric field intensity estimation scheme at reference point

参考点电场强度估计步骤如下:

(1) 泄漏源分析与建模: 分析信息设备激励信号特征, 包括电压、电流、频率、带宽等。分析电磁辐射等效发射天线模型及其参数, 包括天线长度、极化状态以及可辐射的电压、电流和频率。

(2) 辐射效能估计: 依据步骤 1 的分析结果估计信息设备电磁泄漏辐射效能。

(3) 频率范围和传播规律估计: 确定可能产生最大辐射泄漏的频率范围, 进而确定远近场点, 从而得出发射信号在空间中传播和衰减规律。

(4) 电场强度实测: 在开阔场、屏蔽暗室或者使用现场等环境下, 基于以上分析, 利用天线和接收机等传感和接收设备, 在参考距离 d_r 处, 对辐射电场值进行实际测试, 从而实现不同环境下参考点处辐射泄漏电场强度的估计。

3.2 接收性能

实际接收设备的接收性能影响电磁泄漏可检测距离的估计, 本节对接收性能, 包括天线和接收机性能进行分析和估计。

3.2.1 天线性能

首先分析天线馈电点的感应电压, 任一天线开路等效电路示意图如图 17 所示。

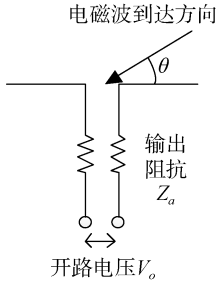


图 17 开路天线等效电路

Figure 17 Equivalent circuit of open loop antenna

天线的输出阻抗为 $Z_a(\Omega)$, 电磁波到达天线的方向角为 $\theta(°)$, 设天线有效长度为 l_a (m), 电磁波电场强度为 E(V/m)则天线的开路电压(V)可表示为[9]:

$$V_o = E \cdot l_a \cdot \sin\theta \tag{17}$$

当天线正对电磁波传播方向时, $\theta = \pi/2$, 开路电压达到最大值, 上式可表示为:

$$V_o = E \cdot l_a \tag{18}$$

则其有效功率 P 可表示为:

$$P = \frac{V_o^2}{4 \cdot Z_a} \tag{19}$$

将半波偶极子天线作为参考天线, 其有效长度可表示为 $l_a = \frac{c}{\pi f}$, 设电磁波频率为 f, 传播速度为光速 c=3×10^{8}m/s, 由式(18)可得参考天线的开路电压 V_{ro} 为:

$$V_{ro} = \frac{E \cdot \mathrm{c}}{\pi \cdot f} \tag{20}$$

由式(19)和(20), 可得参考天线的有效功率 P_r 为:

$$P_r = \frac{E^2 \cdot \mathrm{c}^2}{4 \cdot \pi^2 \cdot f^2 \cdot Z_{ra}} \tag{21}$$

其中 Z_{ra}= 73.13 Ω 参考天线的输入阻抗, 为输出阻抗的实部。

设任一天线相对参考天线的相对增益为 G(dBd), 则:

$$P = P_r \cdot G \tag{22}$$

由式(19)(21)(22)可得任一天线的开路电压 V_o 与天线馈电点的电场强度 E(V/m)的关系为:

$$E = \frac{\pi \cdot V_o \cdot f}{\mathrm{c}} \sqrt{\frac{Z_{ra}}{G \cdot Z_a}} \tag{23}$$

由上式可见, 除了与天线的增益和阻抗特性有关之外, 接收机所需的电场强度将取决于接收频率 f。

3.2.2 接收机性能

接收机的性能主要由其噪声功率 P_n 和要求的输入信噪比 SNR(即输入信号电压与噪声信号电压之比)决定。

当已知接收机的噪声功率密度 P_{dn}, 单位为 dBm/Hz, 则其噪声功率 P_n(W)可表示为:

$$P_n = 10^{\frac{(P_{dn}+10\lg(B))}{10}-3} \tag{24}$$

其中, B 为接收机带宽。

设接收机的输入阻抗为 Z_r, 单位为 Ω, 接收机的输入噪声电压可表示为:

$$V_n = \sqrt{P_n \cdot Z_r} \tag{25}$$

则接收机可接收的输入信号电压表示为:

$$V_i = V_n \cdot SNR \tag{26}$$

上式即为接收机能够接收到的最小电压值, 以此来表征接收机的接收能力。

3.2.3 接收性能

当天线与接收机相连, 其等效电路如下图所示。

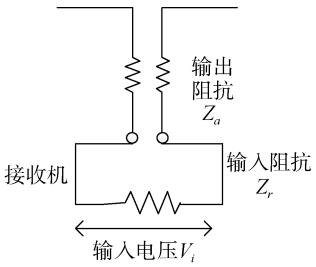


图 18 天线与接收机连接等效电路

Figure 18 Equivalent circuit as antenna connected to receiver

天线的输出阻抗为 Z_a, 接收机的输入阻抗为 Z_r, 当天线输出阻抗与接收机输入阻抗匹配时, 天线的开路电压 V_o 是接收机输入信号电压 V_i 的 2 倍, 即 V_o =2V_i, 则由式(26), 得接收机可接收到的最小电场强度 E(V/m)为:

$$E = \frac{2 \cdot \pi \cdot \sqrt{10^{\frac{(P_{dn}+10\lg(B))}{10}-3} \cdot Z_r} \cdot SNR \cdot f}{\mathrm{c}} \sqrt{\frac{Z_{ra}}{G \cdot Z_a}} \tag{27}$$

3.3 最大可检测距离估计方法

依据对辐射泄漏源电场强度的分析, 可由图 16 所示方案, 获得信息设备在参考距离为 d_r 处的辐射电场强度, 即参考点泄漏电场强度值, 表示为 E_{d_r} (dBμV/m)。

根据式(27), 当接收机带宽设置为 Bw 时, 可计算接收机可接收到的最小电场强度, 由 E_{Bw}(V/m)表

示, 并由下式将其单位转换为 dBμV/m:

$$E'_{Bw} = 20\log_{10}\left(E_{Bw}\right) + 120 \tag{28}$$

设距离 d (m)处, 信息设备电磁辐射电场强度为 E_d (dBμV/m), 若要求接收机能够检测到信息设备在该距离处的电磁辐射泄漏信号, 需满足:

$$E_d \geqslant E'_{Bw} \tag{29}$$

辐射源电磁辐射发射在空间传播和衰减规律, 可近似如下式所示:

$$E_{d_r} - E_d = 10\log_{10}\left(\frac{d}{d_r}\right)^x \tag{30}$$

其中, x 表示电磁波在自由空间中的衰减指数 $x \in \{2,3\}$, 由辐射源电磁辐射信号特征决定。当测试距离为远场时, 电磁场按距离的平方衰减计算, 即 x=2, 当测试距离为近场时, 电磁场将按距离的立方衰减计算, 即 x=3。因此, 由式(29)和式(30)可得, 可检测到信息设备电磁辐射泄漏信号需满足的条件为:

$$E_{d_r} - 10\log_{10}\left(\frac{d}{d_r}\right)^x \geqslant E'_{Bw} \tag{31}$$

通过上式可解得最大可检测距离 d_m 由下式计算:

$$d_m = d_r \cdot 10^{\frac{E_{d_r} - E'_{Bw}}{10 \cdot x}} \tag{32}$$

3.4 传真机电磁泄漏可检测距离估计实例分析

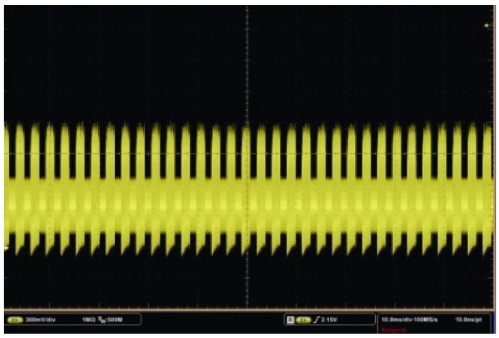
本小节将以传真机电磁泄漏发射为实例, 详细阐述利用本文所述方法估计其电磁泄漏可检测距离的过程。

图 8 给出了传真通信系统图, 标记 1 的传真机为我们要进行测试的发送传真机。

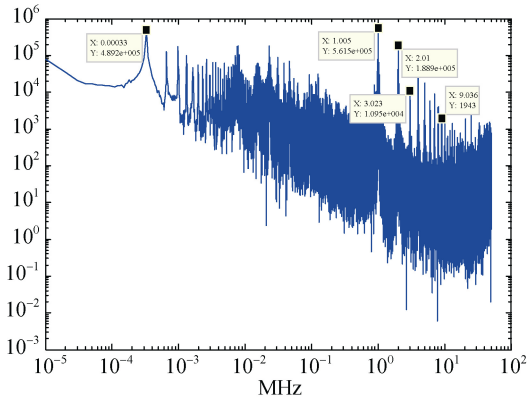
为了便于在普通实验室环境下展开测试, 被测传真机的后盖打开, 在传真机的电磁泄漏点即光电变换处[11,12], 引出其约 50 cm 的单根电路轨迹为辐射等效天线。

传真激励信号如图 19(a)所示, 为梯形波信号, 频谱如图 19(b)所示, 可以得出传真机信号以 330 Hz 为行频率, 以 1.005 MHz 为点频间隔, 频谱特征包括行频及其谐波频率、点频及其谐波频率, 高端频率可到 30 MHz, 一个点频谐波对应的带宽约为 100 kHz。可见, 传真机信号波段为中短波, 波长在 10 m~300 m 范围内, 传真机电磁泄漏信号在空间的衰减按近场规律计算, 即令 x=3。

设置参考距离 d_r = 0.6 m, 在实验室环境下对传真机辐射电磁泄漏信号进行检测。检测天线为有源单极子天线, 接收机设备为高性能的频谱及信号分析仪 R&S FSW。



(a) 时域信号
(a) time domain signal



(b) 频域信号
(b) Spectral signal

图 19 传真信号
Figure 19 Faxing signal

有源单极子天线为宽带、高灵敏度的电场接收天线, 包括一个可调节的单极子元件、一个天线衡网、一个前置放大器, 具体性能参数如下表所示:

表 2 天线性能参数
Table 2 performance parameters of antenna

频率范围	灵敏度	动态范围
Hz	dBμV/m	dB
30-50M	7@1MHz with Bandwidth=1kHz	141

接收机设备 R&S FSW 具体性能参数如下表所示:

表 3 接收机参数
Table 3 Parameters of receiver

噪声功率密度	接收带宽	输入阻抗	信噪比
P_{dn}(dBm/Hz)	B(Hz)	Z_r(Ω)	SNR
–173	1~10×10^6	50	10

接收频率为 1.005 MHz 时, 具有信噪比最高的辐射电场强度, 其接收频谱图如图 20 所示。

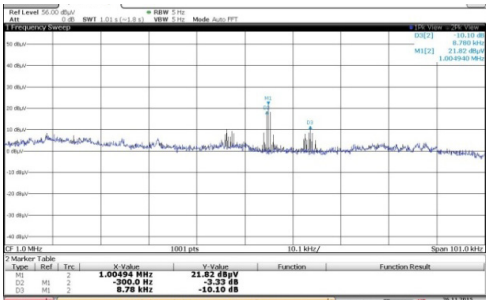


图 20 参考距离处传真机电磁泄漏信号谱图

Figure 20 Spectrum of fax electromagnetic emanation at reference distance

已知该频率处天线因子为 29.3, 从而得到在参考距离处, 传真机电磁辐射泄漏电场强度值为 E_{d_r} =51.12 dBμV/m。

当接收机带宽设置为 5 Hz, 接收中心频率为 1.005 MHz 时, 根据式(27), 计算电场强度 $E_{5\mathrm{Hz}}$= 6.53×10^{-7}V/m, 并利用式(28)转换单位, 得到可接收到的最小电场强度 $E'_{5\mathrm{Hz}}$ =–3.7 dBμV/m。

由信息设备辐射电场强度 E_{dr} 以及接收设备可接收到的最小电场强度 $E'_{5\mathrm{Hz}}$, 参考距离为 0.6 m, x=3, 根据式(32)估计最大可检测距离 d_m=40.32 m。

当接收机带宽设置较小时, 具有较低的噪声电平, 更高的检测信噪比, 更小的可接收电场强度, 将得到更远的可检测距离估计。然而, 带宽的设定并不是越小越好, 只有当接收机带宽设置满足下式条件时, 可检测距离及电磁泄漏风险估计才更有意义。

$$B \geqslant B_{signal} \tag{33}$$

其中 B 为接收机带宽, B_{signal} 为电磁泄漏信号带宽。

随着接收带宽的增加, 会引入较多的噪声, 最大可检测距离将减小, 仅当接收机带宽刚好满足电磁泄漏信息带宽时, 此时的风险估计才更可靠。当接收机带宽小于电磁泄漏信息带宽时, 无法采集完整的时域泄漏信息, 因此无法实现信息还原, 对信息安全不会带来威胁。

依据传真机电磁泄漏信号特征, 信息可重建的最小带宽为一个点频谐波包络, 其带宽为 100 kHz。因此, 当接收机带宽设置为 100 kHz 时, 依据上述方法估计, 得到最大可检测距离为 d_m=1.49 m。

4 可检测距离影响因素分析

4.1 信号处理增益

本小节讨论当考虑信号处理增益时, 如何修正可检测距离的估计。

通过对原始电磁泄漏信号进行信号处理, 可提高信噪比, 从而有利于还原电磁泄漏信息。针对电磁泄漏信号的周期性特点, 如不断刷新的计算机视频信号, 平均是一种高效实用的增强信噪比的方法[6]。当平均次数为 N 次时, 信号处理增益可表示为下式所示:

$$G_p = \sqrt{N} \tag{34}$$

N由电磁泄漏信号可重复次数决定, 即对N个相位对准、波形相同的电磁泄漏信号做平均处理。

当考虑信号处理增益 G_p 时, 修正接收机可接收的最小电场强度为:

$$E = \frac{2\cdot\pi\cdot\sqrt{10^{\frac{(P_{dn}+10\lg(B))}{10}-3}\cdot Z_r\cdot SNR\cdot f}}{c\cdot G_p}\sqrt{\frac{Z_{ra}}{G\cdot Z_a}} \tag{35}$$

4.2 信道衰减

一般情况下, 要求在最好的接收环境下, 对电磁泄漏信号可检测距离进行估计, 即在辐射源到天线之间一定范围内(第一菲涅尔区)没有障碍物, 自由空间衰减是电磁波传播过程中主要的衰减。

当条件不允许时, 即电磁泄漏信号传播过程中存在障碍物, 信道衰减存在其他因素的影响时, 可对式(30)的电磁泄漏信号传播衰减进行修正。

首先, 参考通信无线信道衰减基本模型, 对式(30)中的 x 因子进行重新定义, x 表示随环境而改变的路径损耗指数, 其变化范围为 2~6, 障碍物越多 x 越大。

其次, 考虑周围环境存在随机变化性, 相同距离处的电磁波衰减也可能不同, 进一步修正式(30)由如下所示:

$$E_{d_r} - E_d = 10\log_{10}\left(\frac{d}{d_r}\right)^x + X_\sigma \tag{36}$$

其中 X_σ 为均值为 0, 标准差为 σ 高斯随机变量。

5 结束语

电磁信息泄漏的可检测距离与电磁泄漏辐射强度、接收机性能、天线性能以及信道衰减密切相关, 本文基于信息设备辐射发射模型、接收性能以及信道衰减估计, 提出了一种信息设备电磁泄漏最大可检测距离的估计方法, 该方法充分考虑各信息设备电磁泄漏特征和环境的差异, 适用于不同信息设备、不同使用环境下对可检测距离进行合理估计, 进而避免对信息设备进行过防护和欠防护。并以传真机为实例, 给出了传真机电磁泄漏可检测距离的估计。最后讨论了信号处理及电磁环境信道衰减对估计的影响。

随着信息设备、接收性能、信号处理等技术和能力的不断提升, 对可检测距离的估计将具有不同的估计结论, 因此信息设备的风险评估需要持续跟踪和研究。

参考文献

[1] Information Technology - Security Techniques - Code of Practice for Information Security Controls Based on ISO/IEC 27002 for Telecommunications Organizations[S]. BSI British Standards, . DOI:10.3403/30299332.

[2] Information Security Management System-Requirements for Telecommunications (ISMS-T), ITU Standard ITU-T X.1051, 2004.

[3] RFC2828: Internet security glossary, Internet Engineering Task Force, BBN Technologies, Cambridge, MA, 2000.

[4] van Eck W. Electromagnetic Radiation from Video Display Units: An Eavesdropping Risk?[J]. *Computers & Security*, 1985, 4(4): 269-286.

[5] Highland H. Tempest over Leaking Computers[J]. *Computers & Security*, 1987, 6(6): 457-458.

[6] Kuhn M G. Security Limits for Compromising Emanations[M]. Cryptographic Hardware and Embedded Systems – CHES 2005. Berlin, Heidelberg: Springer Berlin Heidelberg, 2005: 265-279.

[7] Szilagyi A, Nicolaescu I. Evaluation of the Compromising Radiation by Electromagnetic Compatibility Tests[C]. *2012 9th International Conference on Communications (COMM)*, June 21-23, 2012. Bucharest, Romania. Piscataway, NJ: IEEE, 2012: 143-145.

[8] Tosaka T, Yamanaka Y, Fukunaga K, et al. Evaluation of Information Leakage from PC Displays Using Spectrum Analyzers[J]. IEICE Transactions on Communications, 2007, E90-B(11): 3315-3318.

[9] Sekiguchi H, Seto S. Study on Maximum Receivable Distance for Radiated Emission of Information Technology Equipment Causing Information Leakage[J]. *IEEE Transactions on Electromagnetic Compatibility*, 2013, 55(3): 547-554.

[10] Degauque P, Laly P, Degardin V, et al. Compromising Electromagnetic Field Radiated by In-House PLC Lines[C]. *2010 IEEE Global Telecommunications Conference GLOBECOM 2010*, December 6-10, 2010. Miami, FL, USA. Piscataway, NJ: IEEE, 2010: 1-5.

[11] Tosaka T, Taira K, Yamanaka Y, et al. Feasibility Study for Reconstruction of Information from near Field Observations of the Magnetic Field of Laser Printer[C]. *2006 17th International Zurich Symposium on Electromagnetic Compatibility*, February 27-March 3, 2006. Singapore. Piscataway, NJ: IEEE, 2006: 630-633.

[12] Krystian Grzesiak, Artur Przybysz. Emission security of laser printers[C]. *MCC 2010: Military Communications and Information Systems Conference*, Wrocław, 2010:125-134.

[13] Todri A, Marek-Sadowska M. Reliability Analysis and Optimization of Power-Gated ICs[J]. *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, 2011, 19(3): 457-468.

[14] Kasuya M, MacHida T, Sakiyama K. New Metric for Side-channel Information Leakage: Case Study on EM Radiation from AES Hardware[C]. *2016 URSI Asia-Pacific Radio Science Conference (URSI AP-RASC)*, August 21-25, 2016. Seoul. Piscataway, NJ: IEEE, 2016: 1288-1291.

[15] Kumar A, Scarborough C, Yilmaz A, et al. Efficient Simulation of EM Side-channel Attack Resilience[C]. *2017 IEEE/ACM International Conference on Computer-Aided Design (ICCAD)*, November 13-16, 2017. Irvine, CA. Piscataway, NJ: IEEE, 2017: 123-130.

[16] Soll O, Korak T, Muehlberghuber M, et al. EM-based Detection of Hardware Trojans on FPGAs[C]. *2014 IEEE International Symposium on Hardware-Oriented Security and Trust (HOST)*, May 6-7, 2014. Arlington, VA, USA. Piscataway, NJ: IEEE, 2014: 84-87.

[17] Guri M, Monitz M, Elovici Y. USBee: Air-gap Covert-channel Via Electromagnetic Emission from USB[C]. *2016 14th Annual Conference on Privacy, Security and Trust (PST)*, December 12-14, 2016. Auckland, New Zealand. Piscataway, NJ: IEEE, 2016: 264-268.

[18] Zajic A, Prvulovic M. Experimental Demonstration of Electromagnetic Information Leakage from Modern Processor-Memory Systems[J]. *IEEE Transactions on Electromagnetic Compatibility*, 2014, 56(4): 885-893.

[19] Tajima K, Ishikawa R, Mori T, et al. A Study on Risk Evaluation of Countermeasure Technique for Preventing Electromagnetic Information Leakage from ITE[C]. *2017 International Symposium on Electromagnetic Compatibility - EMC EUROPE*, September 4-7, 2017. Angers. Piscataway, NJ: IEEE, 2017: 1-4.

[20] Sekiguchi H, Seto S. Measurement of Computer Rgb Signals in Conducted Emission on Power Leads[J]. *Progress in Electromagnetics Research C*, 2009, 7(2): 51-64.

[21] Liu D X, Guo W L, Fan C X. Principle Analysis of Computer Information Leakage[J]. *Journal of Xidian University*, 1993, 20(2): 74-79.
(刘德修, 郭万里, 樊昌信. 计算机信息泄漏的机理分析[J]. *西安电子科技大学学报*, 1993, 20(2): 74-79.)

[22] Han Fan. Computer Electromagnetic Compromising Emanation and Protection[M]. *Science Press*, 1993.
(韩放. 计算机电磁泄漏发射与防护[M]. 科学出版社, 1993.)

[23] Shi S, Liu T K, Jiang Y. Based on Red and Black Signal on the Host Computer for Testing and Analysis of Electromagnetic Leakage[J]. *Computer Security*, 2011(1): 44-46.
(石森, 刘泰康, 姜云. 基于红黑信号的计算机主机电磁泄漏的测试与分析[J]. *计算机安全*, 2011(1): 44-46.)

[24] Yang W H, Lü Y H. Analysis of Information Recovery from EM

Leakage of Computers[J]. *Journal of Beijing University of Posts and Telecommunications*, 2011, 34(1): 26-29.
(杨文翰, 吕英华. 计算机电磁辐射信息再现分析[J]. *北京邮电大学学报*, 2011, 34(1): 26-29.)

[25] Sun D G, Shi J, Wei D, et al. A New Method to Recognize Computer through Electromagnetic Radiation Based on Spectral Centroid[C]. *2016 Asia-Pacific International Symposium on Electromagnetic Compatibility (APEMC)*, May 17-21, 2016. Shenzhen, China. Piscataway, NJ: IEEE, 2016: 184-186.

[26] Zhu D L, He P, Zhang J Q. Research of Key Problem of Receiving and Recovery of Signal Based on Wide Band Receiver[C]. *2010 International Conference on Internet Technology and Applications*, August 20-22, 2010. Wuhan, China. Piscataway, NJ: IEEE, 2010: 1-8.

[27] Zhou C L, Zhang H L, Yu Q, et al. The Impact of Electromagnetic Security on Computer Systems and Networks[C]. *2011 IEEE 3rd International Conference on Communication Software and Networks*, May 27-29, 2011. Xi'an, China. Piscataway, NJ: IEEE, 2011: 56-59.

[28] Chen R M, Ren J C, Gong Z H. Research on Soft-TEMPEST Technology for Monitor Electromagnetic Trojans[J]. *Computer Engineering and Applications*, 2012, 48(27): 63-68.
(陈荣茂, 任江春, 龚正虎. 显示器电磁木马的 Soft-TEMPEST 技术研究[J]. *计算机工程与应用*, 2012, 48(27): 63-68.)

[29] Dong N. Research on Electromagentic Leakage Emanations of USB Keyboard[D]. Beijing: Beijing University of Posts and Telecom, 2012.
(董宁. USB 键盘信息电磁泄漏的测试、仿真及防护技术研究[D]. 北京: 北京邮电大学, 2012.)

[30] L. Jinming, Z. Jiemin, L. Taikang, etal. “The reconstitution of LCD compromising emanations based on wavelet denoising”, *2017 12th International Conference on Computer Science and Education (ICCSE)*, 22-25 Aug. 2017, pp.294-297, 2017.

[31] Liu J M, Zhang J M, Liu T K, et al. The Reconstitution of LCD Compromising Emanations Based on Wavelet Denoising[C]. *2017 12th International Conference on Computer Science and Education (ICCSE)*, August 22-25, 2017. Houston, TX, USA. Piscataway, NJ: IEEE, 2017: 294-297.

[32] Zhang J M, Sun H M. The New Approach of Preventing the Electromagnetic Information Leakage[C]. *2014 9th International Conference on Computer Science & Education*, August 22-24, 2014. Vancouver, BC, Canada. Piscataway, NJ: IEEE, 2014:337-340.

[33] Wang S, Qiu Y, Tian J, et al. Research on Digital Video Signal Electromagnetic Information Leakage Based on DVI[C]. *2016 IEEE International Symposium on Electromagnetic Compatibility (EMC)*, July 25-29, 2016. Ottawa, ON, Canada. Piscataway, NJ: IEEE, 2016: 594-599.

[34] Sun D G, Wei D, Zhang N, et al. Network Transmission of Hidden Data Using Smartphones Based on Compromising Emanations[C]. *2016 Asia-Pacific International Symposium on Electromagnetic Compatibility (APEMC)*, May 17-21, 2016. Shenzhen. Piscataway, NJ: IEEE, 2016: 190-193.

[35] Shi J, Sun D G, Yongacoglu A, et al. Computer Recognition Based on the Compromising Emanations Fingerprint[C]. *2016 IEEE Canadian Conference on Electrical and Computer Engineering (CCECE)*, May 15-18, 2016. Vancouver, BC, Canada. Piscataway, NJ: IEEE, 2016: 1-6.

[36] Shi J, Yongacoglu A, Sun D G, et al. Computer LCD Recognition Based on the Compromising Emanations in Cyclic Frequency Domain[C]. *2016 IEEE International Symposium on Electromagnetic Compatibility (EMC)*, July 25-29, 2016. Ottawa, ON, Canada. Piscataway, NJ: IEEE, 2016: 164-169.

[37] Xu Y Y, Huang W Q, Fan W, et al. Modeling and Experimental Research on Electromagnetic Information Leakage from Power Lines[J]. *Scientia Sinica(Informationis)*, 2015, 45(10): 1341-1354.
(徐艳云, 黄伟庆, 范伟, 等. 基于电源线的电磁信息泄漏建模与实验分析[J]. *中国科学:信息科学*, 2015, 45(10): 1341-1354.)

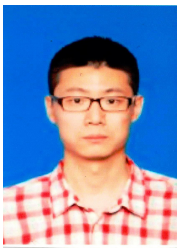
[38] Xu Y Y, Hu J L, Zhang M, et al. Electromagnetic Side Channel Analysis of Laser Facsimile[C]. *2017 IEEE International Conference on Communications (ICC)*, May 21-25, 2017. Paris, France. Piscataway, NJ: IEEE, 2017: 1-6.

[39] Gan H, Zhang H X, Li J, et al. Independent Component Analysis Applied in Electromagnetic Attack[J]. *Chinese Journal of Radio Science*, 2016, 31(2): 401-405.
(甘罕, 张洪欣, 李静, 等. 独立成分分析在电磁攻击中的应用[J]. 电波科学学报, 2016, 31(2): 401-405.)

[40] Zhang M, Huang W Q, Wang S Y, et al. Summary of Physical Space Information Security Technology Development[J]. *Journal of Information Security Research*, 2016, 2(2): 107-116.
(张萌, 黄伟庆, 王思叶, 等. 物理空间信息安全技术发展综述[J]. 信息安全研究, 2016, 2(2): 107-116.)

[41] Xie C F, Rao K J. Electromagnetic Field and Electromagnetic wave (Fourth Edition)[M]. Beijing: Higher Education Press, 2006.
(谢处方, 饶克谨. 电磁场与电磁波[M]. 北京: 高等教育出版社, 2006.)

徐艳云 于 2012 年在中国科学院研究生院电磁场与微波专业获得博士学位。现任中国科学院信息工程研究所高级工程师。研究领域为电磁信息安全、信号处理等。研究兴趣包括: 电磁泄漏发射检测、电磁指纹特征等。Email: xuyanyun@iie.ac.cn



张萌 于 2013 年在北京航空航天大学电子信息工程专业获得硕士学位。现中国科学院信息工程研究所高级工程师。电磁泄漏发射、信号处理、电磁环境监测等。Email: zhangmeng@iie.ac.cn

黄伟庆 于 2002 年在北京邮电大学获得硕士学位。现任中国科学院信息工程研究所正研级高级工程师。研究领域为电磁信息安全、信号处理等。研究兴趣包括: 电磁泄漏发射检测、无线通信安全、电磁信息安全等。Email: huangweiqing@iie.ac.cn