基于计算机技术实现信息安全体系架构设计

李 静[1]
LI Jing

摘 要 针对现有电力系统安全体系架构防护性能弱、网络延迟高等问题，基于计算机技术构建安全体系架构。基于一个新型物理层防火墙硬件原型，其仅允许接收器在与传入主信号同时检测到有效水印的情况下进行访问，并且可以与几乎任何网络波形一起使用，将任何未经验证的消息标记为不受信任，如果消息未请求未经授权的权限，则按正常方式处理。同时提出一种在电力系统线监测算法模型，对调试系统中的安全防护软件进行针对性的调整，增加系统防护能力。实验结果表明，防护系统风险更小，安全性更强。

关键词 计算机技术；网络信息安全；物理层防火墙；无线光纤技术；可变形零件模型

doi：10.3969/j.issn.1672-9528.2024.03.045

0 引言

在电力发展过程中，信息网络的安全至关重要，特别是对于监控信息的保护，而传统电力网络安全的防护技术薄弱，在实际应用中容易产生防护漏洞，导致重要信息泄露，或者网站信息被篡改等事故的发生[1]。由于计算机网络体系结构的复杂性，黑客以各种形式对网络进行攻击。因此，为加强监控网络信息的安全性，需要设计出新型信息安全体系架构[2-3]。

国内外网络安全部门针对安全漏洞进行研究，文献 [4] 通过设计软件定义网络架构完成漏洞修复。但这种方法无法提前预防，只能做后续处理。国内相关研究人员对其预防措施进行研究，其中文献 [5] 设计 Emulab 网络模拟系统对网络防护薄弱点进行加强，但这种方法容易造成网络延迟，信息传输速度变慢。

1 总体方案设计

针对上述研究的网络安全防护技术存在的问题，本研究通过对传统防护网络进行改装，并在此基础上增强网络安全防护能力，建立了新型网络信息安全体系架构。如图 1 所示，本研究构建的网络信息安全体系架构由三个方面组成，分别为应用安全、网址访问和系统运营安全。应用安全由无源光纤网络进行防护，通过检测垃圾邮件和识别恶意网页的形式确定安全程度，采用的技术方式为无线光纤技术，由分光器和无源光纤负责应用软件的安全；运营安全包括组成芯片、账号信息和代码加密，芯片检测内容为型号分析、参数对比和功能验证，账号组成主要分为账号密码安全和信息保密协议，代码加密主要功能为恶意代码分析和在线 AES 加密设置。而对于网络监控信息汇总的安全问题，由网络安全技术分步解决，对其软件参数进行安全管控，通过特征提取分析其运行状态，对监控信息和传输方式进行专项防护，最大程度避免信息干扰，安全验证和效果评估负责验证处理结果并记录[6-7]。

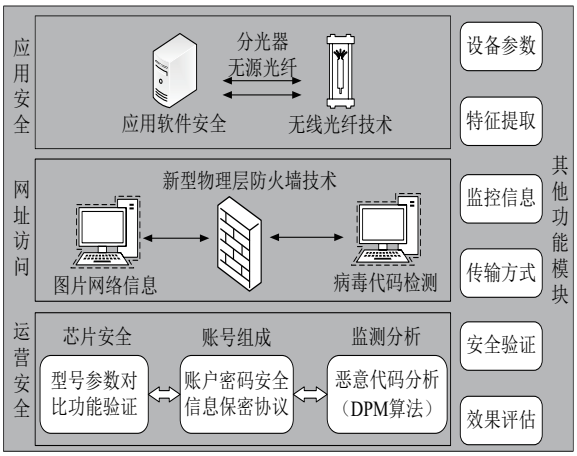

图 1 网络安全架构改装方案

2 关键技术

2.1 新型物理层防火墙设计

为实现网络信息安全，本研究构建了一个新型物理层防火墙硬件原型，其仅允许接收器在与传入主信号同时检测到有效水印的情况下进行访问，并且可以与几乎任何网络波形一起使用。此外，使用不重复的任意相位扩频信号消除了许多常见的重放攻击。该物理层防火墙硬件原型采用 802.11g 主信号，并以高阶相移键控信号（high-order phase shift keying signaling，HOPS）波形为基础。给定只需要在接收器处提供其存在的参考基线信号，水印本身可能完全由前导码

1. 广西博联信息通信技术有限责任公司 广西南宁 530000

芯片组成，并且检测足以提供认证。关于 802.11g/HOPS 的同信道频域描述如图 2 所示。

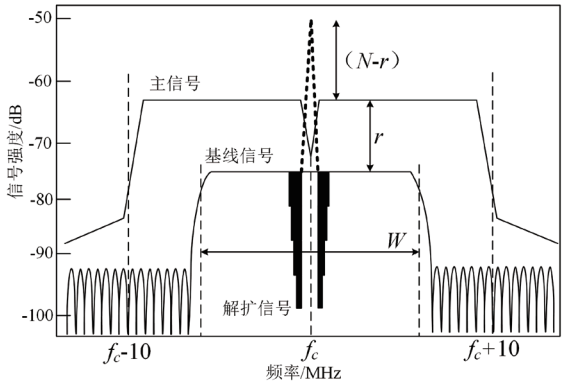

图 2 802.11g/HOPS 的同信道频域

图 2 中衬底具有带宽 W、扩频增益 N 和信号功率谱密度（power spectral density，PSD）退避 r。增加 W 和 N 将以改善的认证性能换取主信号降级，而降低这些值将减少降级认证的任何误码率降级。退避 r 可以基于期望的信干噪比（signal-to-interference plus noise ratio，SINR）工作点进行动态调整。由于 802.11g 占用的带宽为 16.6 MHz，尽管信道带宽为 20 MHz，但低截获概率 / 低检测概率水印被限制为 W≤16.6 MHz。主信号的同信道干扰使得窃听者在不首先知道传输的数据的情况下重构水印更加困难，进而增强了网络信息安全性 [8]。

物理层防火墙硬件原型的每个HOPS衬底扩展芯 $X=(a+jb)$ 取自单位圆上的任意点，因此 N 也是水印序列 $\{X_n\}$ 的长度，该水印在传输之前与主信号样本时间对齐，如图 3 所示。

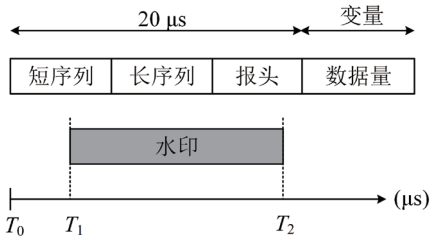

图 3 802.11g/HOPS 的信道时域

在图 3 中，为了保证 $T_1 > T_0$，802.11g/HOPS 的网络数据序列长度会因变量而导致不同。主要信号样本长度由物理层传输，并且与二进制相移键控调制的前报头相比，潜在的更高速率调制数据有效载荷对同信道干扰的弹性更小，因此在接收机处可能不优选更长的水印。对于基于剩余数系统算法的伪随机数发生器方法来说，这相对简单，并且涉及选择适当的剩余值输入 key[9]。所选择的 key 对应输入到伪随机数发生器的剩余向量，给出从允许的相位字的任意分布均匀获得的 N 长度码片相位序列 $\{\theta_n\}$，$\theta_i \in \{\theta_n\}$ 的每一个都映射到水印的相关扩展码片 $X_i \in \{X_n\}$。有关发送器与接收器物理层的框图分别如图 4、图 5 所示。

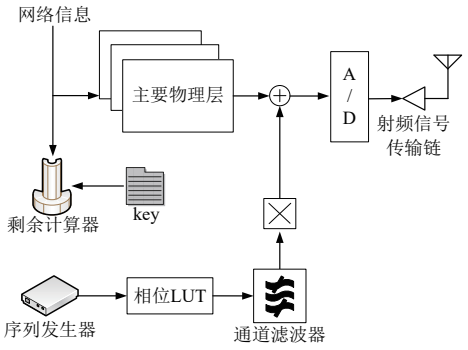

图 4 信号发送器物理层框图

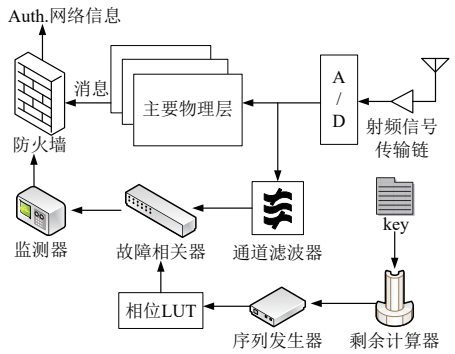

图 5 信号接收器物理层框图

图 3 中的发射器框图遵循中描述的核心技术，不需要修改主信号物理层。然而，由于水印是以码片速率（R）在内部生成的，如果 R 小于基带采样率（f_s），则在与主信号的时间对齐之前插入内插信道滤波器，或者选择在插值之前将水印衰减 α。在图 5 接收器处，如果传入信号样本形成数据帧，如果水印检测与接收帧同时发生，则认证成功（参考图 3）。因此，用衬底信号检测逻辑扩展传统物理层充分实现了水印验证功能。$R < f_s$ 的设计应能对接收信号进行带通滤波，以减少带外噪声 / 同频干扰，并可选择抽取输入样本，以降低接收机复杂度。

构建物理层防火墙硬件原型后，对于防火墙配置，假设理想的网络信息输出信号 $z[n]$ 对于任意相位跳数波形将具有幅值 n，验证输入信号的决定使用充分的统计数据 $Z=|z[n]|$ 和相对于预期主信号加噪声功率设置的检测阈值 τ，其表达式为：

$$Z=\left|\sum_{i=0}^{n} X_{(n)}Y_{(n)}\right| \tag{1}$$

式中：$\{Y_n\}$ 表示网络信息安全体系架构内部生成水印 $\{X_n\}$ 的有效接收水印。已知延迟（1）给出了相对于每个认证决策 δ 的接收信号延迟线的时间戳。也就是说，如果 $\delta[Y]=1$，那么 $\{Y_n\}$ 绝对有效，并且传入的主信号在信号源头是真实的，其中：

$$\delta[Y]=\begin{cases}1 & Z \geq \tau \\ 0 & Z < \tau\end{cases} \tag{2}$$

式中：τ 表示检测阈值，忽略误报的可能性，水印检测可用

于优化 τ，以便在（2）中做出未来的认证决策。相关长度 N 用于除以 Z 以提供基线信号功率估计，而在检测之前 / 之后的实例中 $|z(n)|$ 的值（加上 10 ～ 20 个接收码片以考虑滤波）可用于估计同信道干扰加上噪声功率。

在实际系统中，将任何未经验证的消息标记为不受信任，如果消息未请求未经授权的权限，则按正常方式处理，这种方式可以有效地允许授权用户访问，同时继续所有其他网络操作 [10]。

2.2 可变形零件模型回访运算

假设网络信息安全防护结构反馈数据为待解决问题，通过建立问题函数，将反馈数据标量化：

$$H(t+1)=\tau_H H(t)+\sum_{N_k}(\Delta H_A+\Delta H_I) \tag{3}$$

式中：t 表示网络信息安全防护结构对调试反映时间，$H(t)$ 表示 RVDPM 程序反映时间内建立回访函数，$H(t+1)$ 表示后续反映时间建立的回访算法程序，τ_H 表示算法程序建立过程中的时间常数，ΔH_A 表示网络信息安全防护结构前后系统安全差值，ΔH_I 表示经过算法程序调整后的系统安全差值。

对标量化问题函数分析，通过研究不同系统防护软件的相关参数，完成网络信息的整体把握：

$$H_n(t)=\{s=\alpha s_a(g,t)-\beta s_r(g,t)|V_n\} \tag{4}$$

式中：$H_n(t)$ 表示系统防护软件整体参数汇总，s 表示调试系统防护软件信息，α 表示系统防护软件安全系数，s_a 表示系统防护软件运行状态，(g,t) 表示系统防护软件安全指标，β 表示系统运行中产生的隐患，s_r 表示自身硬件隐患，V_n 表示系统防护软件对安全体系结构的影响范围，n 表示参数序号。将系统中的防护软件存在的隐患用矩阵的方式表示出来，即：

$$N_p=\begin{bmatrix} n_{1,1} & n_{1,2} & \mathrm{L} \\ n_{2,1} & n_{2,2} & \mathrm{L} \\ \mathrm{M} & \mathrm{M} & \mathrm{O} \end{bmatrix} \tag{5}$$

式中：N_p 表示系统防护软件安全隐患矩阵。通过分析不同软件的安全隐患，经过网络信息安全防护结构加固各防护软件安全，得到加固的系统防护软件安全性函数为：

$$s_a(g,t)=(1-E_a)\begin{bmatrix}(1-G_a)\begin{pmatrix}s_a(g,t-1)\\+kpd_a(g,t)\end{pmatrix}\\+g_a(g,t)\end{bmatrix} \tag{6}$$

$$g_a(g,t)=\frac{1}{L_{N(p)}}\sum_{g_{xy}\in U}G_a\begin{bmatrix}s_a(g_{xy},t-1)\\+d_a(g_{xy},t)\end{bmatrix} \tag{7}$$

式中：$s_a(g,t)$ 表示加固后的系统安全指标，E_a 表示防护结构作用下的防护能力，G_a 表示传统方法运行手段下系统的防护能力，g_{xy} 表示安全系数，p 表示系统硬件有功功率，d_a 表示防护结构对调试系统的影响程度，g_a 表示防护安全函数，$L_{N(p)}$ 表示防护标准参数。

对经过 RVDPM 算法监测后的输出信息数据进行安全评估，由此计算系统最大运行安全值为：

$$P_1(x_i(k))=max\left\{0,\left(R_m-\sqrt{(xp_i(k)-ox_m)^2-(Qp_i(k)-ox_m)^2}\right)\right\} \tag{8}$$

式中：$x_i(k)$ 表示待评估软件安全参数，x_m 表示网络安全信息自变量，P_1 表示系统最大评估安全值，R_m 表示系统威胁因素裕度，Q 表示网络安全体系架构的隐患因素，下角标 i 表示信息样本序号，$p_i(k)$ 表示安全标准下的系统硬件有功功率，o 表示网络安全受影响程度。

可以看出，式（8）存在最大值，对于存在安全隐患的网络信息以及软件，推算结果与实际偏差较大，通过对比偏差的大小确定调试系统有效性，由此完成回访反馈操作，保证系统网络信息的安全。

3 实验与分析

为了验证本研究所设计的信息安全体系架构的实用性，本研究对于网络安全环境的实验。

本设计实验通过对建立的防护网进行攻击，根据反馈数据进行分析，利用网络安全防护系统统计数据信息，通过矢量化加速器调整运行频率，并通过 AES 算法模型对软件进行加密，计算出网络安全评估风险系数的取值范围为：

$$M=\left[M_1(L(C,V)),F(I_a,V_a)\right] \tag{9}$$

式中：M 表示安全风险计算函数，M_1 表示上一次计算安全风险评估值，L 表示威胁事件出现的可能性，C 表示威胁元素，V 表示安全软件的脆弱性，F 表示风险事件造成的损失，I_a 表示物理层防火墙产生的安全价值，V_a 表示恶意文件攻击的强弱程度。分别采用文献 [4] 方法中的预测预警防火墙模型防火墙预警模型与文献 [5] 方法中的 Emulab 网络模拟系统进行对比验证，将三种信息安全体系架构分别对数据包、账户网址、应用软件和图片文件进行在线监测，通过评判防护网的安全等级保证本研究的可行性，将实验结果汇总数据表，如表 1 所示。

表 1 网络安全测试表

网络信息类别	安全风险信息量范围 /MB		
	本文方法	文献 [4]	文献 [5]
数据包	53	85	105
账户网址	27	49	70
应用软件	34	70	90
图片文件	28	54	67

通过对比三种不同网络安全防护系统对网络安全风险信息量范围，将各系统计算的安全风险信息量范围用柱状图的形式描述，得到对比结果如图 7 所示。从图 7 中

可以看出，本研究防护系统网络安全风险信息量范围在 15 ～ 60 MB；文献 [4] 的防护系统网络安全风险信息量范围在 30 ～ 90 MB；文献 [5] 的防护系统网络安全风险信息量范围在 60 ～ 105 MB。结果表明，本研究防护系统风险更小，安全性更高。

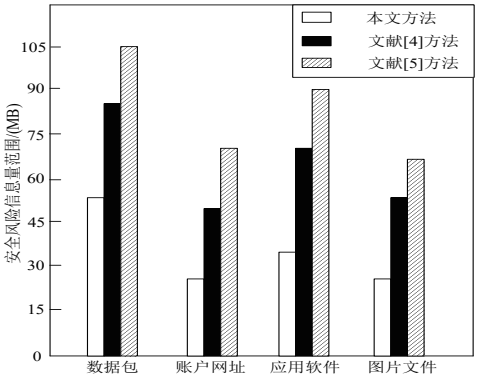

图 7 三种方法性能对比结果

通过对比各研究网络安全系统对威胁性木马文件的防护能力，通过若干次（2 ～ 18）模拟攻击进一步完成对比实验，根据计算机处理结果进行仿真对比，得到网络安全评估系数对比如图 8 所示。

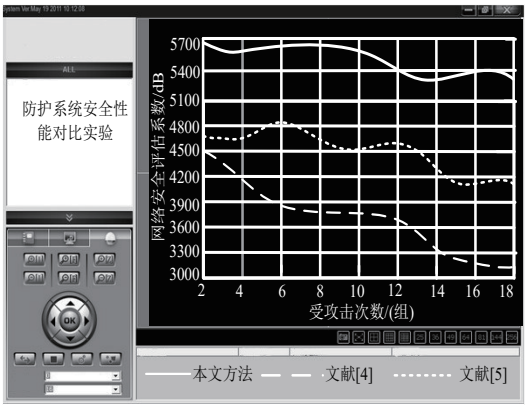

图 8 安全评估系数对比

从图 8 中可以看出，三种系统安全评估系数随受攻击次数增加有所下降，本研究最高评估安全系数最高为 5 691.61 dB，最低系数为 5 308.26 dB，整体呈不规则下降状态；文献 [4] 所设计的信息安全系统最高评估安全系数最高为 4500 dB，最低系数为 3 164.57 dB，安全系数下降速度较快；文献 [5] 所设计的信息安全系统最高评估安全系数最高为 4 652.68 dB，最低系数为 4 198.31 dB，整体下降速度略缓，但以上两种系统整体安全系数均低于本研究的安全体系架构。

综上所述，本研究的安全体系架构对网络威胁具有明显效果，使计算机中的数据包、账户网址、应用软件和图片文件等信息安全风险值范围缩小，计算结果表明，本研究所设计的安全体系架构的安全系数为最高，验证了本设计安全系统的实用性与可靠性。

4 结语

在信息化时代的网络恶意入侵环境下，本研究提出了一种新型电力系统信息安全防护方法，通过检测垃圾邮件和识别恶意网页的形式确定安全程度，采用的技术方式为无线光纤技术，由分光器和无源光纤负责应用软件的安全。运用 RVDPM 算法 24 小时实时监测输入的网络信息，并通过对以太网访问地址状态变化进行记录，对输入的电力系统网络信息进行分析，利用计算机软件程序推算其受影响程度，根据实验结果分析本文研究的可行性。然而，在系统计算性能方面仍存在计算框架较为复杂的问题，未来会进行下一步优化研究。

参考文献：

[1] 尹超 , 安娜 , 黄凡帆 . 一种面向嵌入式操作系统的信息安全防护体系架构设计 [J]. 单片机与嵌入式系统应用 , 2021, 21(4): 12-14.

[2] 杨天开 , 鲁洁 . 新型智慧城市环境下信息安全体系架构浅析 [J]. 中国管理信息化 ,2019,22(19):140-142.

[3] 安高峰 , 朱长明 , 雷晓锋 , 等 . 我国工业控制系统信息安全政策和标准体系架构研究 [J]. 信息安全研究 , 2018, 4(10): 959-964.

[4] 金梦然 . 计算机网络安全中的防火墙技术应用 [J]. 电子技术 , 2021,50(12):270-271.

[5] 杨林 . 数据加密技术在计算机网络安全中的应用 [J]. 无线互联科技 , 2021,18(23):20-21.

[6] 陈华盛 . 信息化时代计算机网络安全防护技术 [J]. 数字技术与应用 , 2021,39(11):237-239.

[7] 王瑞萍 , 鲍喜 , 张海超 , 等 . 人工智能审计流程的设计及平台构建 [J]. 微型电脑应用 ,2022,38(1):62-65.

[8] 曾振环 . 变电站二次安全防护系统设计研究 [J]. 企业技术开发 , 2018,37(9):98-100.

[9]VOLLALA S ,VARADHAN V V,GEETHA K ,et al. Design of RSA preprocess for concurrent cryptographic transformations[J].Microelectronics journal, 2017,63:112-122.

[10] 高阳 , 李天豪 , 王宁 , 等 . 基于物联网架构的智能变电站数据管理系统设计 [J]. 物联网技术 ,2020,10(8):71-73.

【作者简介】

李静（1988—），女，本科，研究方向：电力信息化、企业架构的研发。

（收稿时间：2023-12-28）