电网技术 2011, 35(4) 176-182 DOI: ISSN: 1000-3673 CN: 11-2410/TM

自动化

基于支持向量机和粒子群算法的信息网络安全态势复合预测模型

高昆仑1，刘建明2，徐茹枝3，王宇飞3，李怡康3

1．中国电力科学研究院 信息与通信研究所，北京市 海淀区 100192；2．国网信息通信有限公司，北京市 宣武区 100761；3．华北电力大学 控制与计算机工程学院，北京市 昌平区 102206

摘要：

提出一种基于支持向量机和粒子群算法的网络态势复合预测模型。模型使用滑动窗口方法将各原始离散时间监测点的安全态势值构造成部分线性相关的连续时间序列，以其作为安全态势数据样本集对支持向量机加以训练，生成预测模型。在支持向量机训练过程中，利用粒子群算法搜寻支持向量机的最优训练参数，以降低支持向量机参数选择的盲目性，提高预测精度。最后通过基于大量电力企业信息网络现场安全监测数据的实验，验证了复合预测模型的有效性。

关键词： 信息网络安全态势 回归预测 支持向量机 粒子群算法 时间序列

A Hybrid Security Situation Prediction Model for Information Network Based on Support Vector Machine and Particle Swarm Optimization

GAO Kunlun1, Liu Jianming2, XU Ruzhi3, WANG Yufei3, LI Yikang3

1. Information & Communication Department of China Electric Power Research Institute, Hardian District, Beijing 100192, China;2. State Grid Information & Telecommunication Company Limited, Xuanwu District, Beijing 100761, China;3. School of Control and Computer Engineering, North China Electric Power University, Changping District, Beijing 102206, China

Abstract:

A security situation prediction model for information network based on support vector machine (SVM) and particle swarm optimization (PSO) is proposed. By use of sliding window, in the proposed model a continuous time series that is partially linearly dependent is constructed by security situation values sampled from original discrete time monitoring points, and taking the time series as the sample set of security situation data the SVM is trained to generate a prediction model. During the training of SVM, the PSO algorithm is used to search for the optimal training parameters of SVM to reduce the blindness in the selection of SVM parameters and improve precision of prediction. Through the experiments based on on-site installation and monitoring data of a lot of power enterprise information networks, the effectiveness of the proposed security situation prediction model is verified.

Keywords: security situation of information network regression prediction support vector machine particle swarm optimization time series

收稿日期 2010-10-25 **修回日期** 2011-01-10 **网络版发布日期** 2011-04-12

DOI:

基金项目:

国家电网公司科技项目(B11-09-109)

通讯作者: 高昆仑

作者简介:

作者Email: gkl@epri.sgcc.com.cn

参考文献：

[1] 王慧强，赖积保，朱亮，等．网络态势感知系统研究综述[J]．计算机科学，2006，10(2)：5-10． Wang Huiqiang，Lai Jibao，Zhu Liang，et al．Survey of network situation awareness system[J]．Computer Science，2006，10(2)：5-10(in Chinese)． [2] 陈秀镇，郑庆华，管晓宏．层次化网络安全威胁态势量化评估方法[J]．软件学报，2006，17(4)：885-897． Chen Xiuzhen，Zheng Qinghua，Guan Xiaohong．Quantitative hierarchical threat evaluation model for network security[J]．Journal of Software，2006，17(4)：885-897(in Chinese)． [3] 李雄伟，周希元，杨义先．基于层次分析法的网络攻击效果评估[J]．计算

机工程与应用，2005，24(49)：157-159． Li Xiongwei，Zhou Xiyuan，Yang Yixian．Study on the evaluation methods of the attack effect of network based on AHP[J]．Computer Engineering and Applications，2005，24(49)：157-159(in Chinese)． [4] 邓欹，孟洛明．基于贝叶斯学习的告警相关性分析[J]．计算机工程，2007，33(12)：40-42． Deng Xin，Meng Luoming．Analysis of alarm correlation based on bayesian learning[J]．Computer Engineering，2007，33(12)：40-42(in Chinese)． [5] Elattar E E，Goulermas J，Wu Q H．Electric load forecasting based on locally weighted support vector regression[J]．IEEE Translations on Systems，Man，and Cybernetics，Part C：Applications and Reviews，2010，40(4)：438-447． [6] 陈涛，龚正虎，胡宁．基于改进BP算法的网络态势预测模型[C]//2009全国计算机网络与通讯学术会议．中国深圳：中国电子学会通信学分会，2009：93-99． [7] 任伟，蒋兴浩，孙锬锋．基于RBF神经网络的网络安全态势预测方法[J]．计算机工程与应用，2006，31(40)：136-144． Ren Wei，Jiang Xinghao，Sun Tanfeng．RBFNN-based prediction of networks security situation [J]．Computer Engineering and Applications，2006，31(40)：136-144(in Chinese)． [8] 王晋东，沈柳青，王坤，等．网络安全态势预测及其在智能防护中的应用[J]．计算机应用，2010，30(6)：1480-1488． Wang Jindong，Shen Liuqing，Wang Kun，et al．Network security status forecasting and its application in intelligent defense[J]．Journal of Computer Applications，2010，30(6)：1480-1488(in Chinese)． [9] 张翔，胡昌振，刘胜航，等．基于支持向量机的网络攻击态势预测技术研究[J]．计算机工程，2007，11(3)：10-12． Zhang Xiang，Hu Changzhen，Liu Shenghang，et al．Research on network attack situation forecast technique based on support vector machine[J]．Computer Engineering，2007，11(3)：10-12(in Chinese)． [10] 邓万宇，郑庆华，陈琳，等．神经网络极速学习方法研究[J]．计算机学报，2010，2(9)：279-287． Deng Wanyu，Zheng Qinghua，Chen Lin，et al．Research on extreme learning of neural networks[J]．Chinese Journal of Computers，2010，2(9)：279-287(in Chinese)． [11] 韩中合，朱霄珣．基于信息熵的支持向量回归机训练样本长度选择[J]．中国电机工程学报，2010，30(20)：112-116． Han Zhonghe，Zhu Xiaoxun．Selection of training sample length in support vector regression based on information entropy[J]．Proceedings of the CSEE，2010，30(20)：112-116(in Chinese)． [12] 郭创新，朱承治，张琳，等．应用多分类多核学习支持向量机的变压器故障诊断方法[J]．中国电机工程学报，2010，30(13)：128-134． Guo Chuangxin，Zhu Chengzhi，Zhang Lin，et al．A fault diagnosis method for power transformer based on multiclass multiple-kernel learning support vector machine[J]．Proceedings of the CSEE，2010，30(13)：128-134(in Chinese)． [13] 王雷，张瑞青，盛伟，等．基于支持向量机的回归预测和异常数据检测[J]．中国电机工程学报，2009，29(8)：92-96． Wang Lei，Zhang Ruiqing，Sheng Wei，et al．Regression forecast and abnormal data detection based on support vector regression[J]．Proceedings of the CSEE，2009，29(8)：92-96(in Chinese)． [14] 杨耿煌，温渤婴．基于量子行为粒子群优化－人工神经网络的电能质量扰动识别[J]．中国电机工程学报，2008，28(10)：123-129． Yang Genghuang，Wen Boying．Identification of power quality disturbance based on QPSO-ANN[J]．Proceedings of the CSEE，2008，28(10)：123-129(in Chinese)． [15] 姚舜才，潘宏侠．粒子群优化同步电机分数阶鲁棒励磁控制器[J]．中国电机工程学报，2010，30(21)：91-97． Yao Shuncai，Pan Hongxia．Fractional order PID controller for synchronous machine excitation using particle swarm optimization [J]．Proceedings of the CSEE，2010，30(21)：91-97(in Chinese)． [16] 李奇，陈维荣，刘述奎，等．基于自适应聚焦粒子群算法的质子交换膜燃料电池机理建模[J]．中国电机工程学报，2009，29(20)：119-124． Li Qi，Chen Weirong，Liu Shukui，et al．Mechanism modeling of proton exchange membrane fuel cell based on adaptive focusing particle swarm optimization[J]．Proceedings of the CSEE，2009，29(20)：119-124(in Chinese)． [17] 陈勇强，刘开培．一种基于径向基函数动态阈值模型的机组状态监测方法[J]．中国电机工程学报，2007，27(26)：96-101． Chen Yongqiang，Liu Kaipei．A condition monitoring method of generators based on RBF dynamic threshold model[J]．Proceedings of the CSEE，2007，27(26)：96-101(in Chinese)．

本刊中的类似文章

1．郝文斌，李群湛，马庆安，郑永康.基于支持向量机的变压器励磁涌流仿真实现[J]. 电网技术, 2006,30(1): 60-64

2．兰飞 唐玲.基于有向无环图支持向量机的水轮发电机组故障诊断模型[J]. 电网技术, 2010,34(2): 115-119

3．肖军 刘天琪 苏鹏.基于双种群粒子群算法的分时段电力系统无功优化[J]. 电网技术, 2009,33(8): 72-77

4．方群会 刘强 周林 马永强 武剑 .模式分类方法在电能质量扰动信号分类中的应用综述[J]. 电网技术, 2009,33(1): 31-36

5．刘述奎 陈维荣 李奇 郑永康 张雪霞 .基于随机聚焦粒子群算法的电力系统无功优化[J]. 电网技术, 2008,32(26): 8-11

6．罗 楠|朱业玉|杜彩月 .支持向量机方法在电力负荷预测中的应用[J]. 电网技术, 2007,31(Supp2): 215-218

7．栗 然|郭朝云|韦仲康 .京津唐电网电力日峰荷与气象指数的关联性分析[J]. 电网技术, 2008,32(6): 87-92

8．王德意 杨卓 杨国清.基于负荷混沌特性和最小二乘支持向量机的短期负荷预测[J]. 电网技术, 2008,32(7): 66-71

9．娄素华|吴耀武|熊信银.基于适应度空间距离评估选取的多目标粒子群算法在电网无功优化中的应用[J]. 电网技术, 2007,31(19): 41-46

10．杨健维 罗国敏 何正友.基于小波熵权和支持向量机的高压输电线路故障分类方法[J]. 电网技术, 2007,31(23): 22-26

11．牛东晓|刘 达|邢 棉|冯 义|陈广娟.基于自组织映射支持向量机的日前电价预测[J]. 电网技术, 2007,31

(18): 15-18
12. 张庆宝，程浩忠，刘青山，郑季伟，倪东海.基于粗糙集属性约简算法和支持向量机的短期负荷预测[J]. 电网技术, 2006,30(8): 56-59
13. 姜惠兰，刘晓津，关 颖，王梦宾.基于硬C均值聚类算法和支持向量机的电力系统短期负荷预测[J]. 电网技术, 2006,30(8): 81-85
14. 张永明|齐维贵|王军栋|唐海燕|陈 烈.基于支持向量机的时间序列交叉负荷预报方法[J]. 电网技术, 2007,31(Supp2): 207-210
15. 叶圣永 王晓茹 刘志刚 钱清泉 .电力系统暂态稳定概率评估方法[J]. 电网技术, 2009,33(6): 19-23
