文章编号:1671-4598(2015)01-0057-03　　中图分类号:F127　　文献标识码:A

基于双向联想记忆网络的航空雷达在线入侵诊断方法研究

吴　华[1]，王海顺[2]
(1. 安阳师范学院 网络与教育技术中心，河南 安阳　455000；
2. 安阳师范学院 继续教育学院，河南 安阳　455000)

摘要：针对传统的航空雷达网络面临的入侵威胁，以及雷达网络存在的入侵诊断检测效率较低，数据匹配速度较慢等问题，提出了一种基于双向联想记忆网络的航空雷达在线入侵诊断方法，构建航空雷达在线入侵诊断模型，对航空雷达网络中的外部数据进行预处理，并获取数据特征以及数据特征的可辨识属性矩阵和决策辨识函数，计算测试参数集的所有特征向量，从而使入侵检测算子的匹配量减少，以此提升数据匹配效率，实现对外部入侵数据的过滤检测，从而对雷达数据网络进行在线监控，有效抵御外部异常数据的入侵，保证了航空雷达网络的安全性；仿真结果表明文章方法有效提高了航空雷达网络的在线数据检测匹配速度，诊断准确率达到93.3%，且对航空雷达的入侵诊断检测效率、误报率、漏报率等方面都有明显改善。

关键词：BAM网络；航空雷达；在线入侵诊断

Aviation Radar Online Invasive Diagnosis Method Based on BAM Network

Wu Hua[1], Wang Haishun[2]
(1. Network and educational technology center Anyang Normal University, Anyang　455000, China;
2. School of Continuing Education Anyang Normal University, Anyang　455000, China)

Abstract: In view of the traditional aviation radar network invasion threat, and intrusion diagnostic test of radar network low efficiency, data matching speed is slow, this paper proposes an aviation radar online invasive diagnosis method based on BAM network, build invasion diagnosis model of aviation radar online, preprocessing the external data in aviation radar network, and obtain data features and characteristics of discernibility matrix and decision attribute recognition function, all the characteristic vector calculation test parameter set, so that reduce the amount of matching the intrusion detection operator, to enhance the efficiency of data matching, external intrusion data filtering detection, thus for on-line monitoring of the radar data network, effectively resist the invasion of external abnormal data, make sure the safety of aviation radar network. The simulation results show that the method effectively improves the matching speed aviation radar network data online detection, diagnosis accuracy rate reached 93.3%, and the invasion of the aviation radar detection diagnosis efficiency, the rate of false alarm, non-response rates etc have been improved significantly.

Keywords: BAM network; aviation radar; online intrusion diagnosis

0　引言

航空雷达等航空电子装备的组成结构复杂，各功能模块间的交互信息多，其网络化是现代航空空运技术的发展趋势，航空雷达的网络化涉及雷达中心网与计算机网络，航空雷达的网络化要求网络通信必须快速、准确、保密性高，雷达网网络的中心节点间通过战术数据链相连接，整个网络数据信息动态更新，保证了作战信息的实时性，但航空雷达网络面临的外部数据入侵威胁会对整个网络造成巨大损失[1-2]。随着互联网的快速发展，其受到攻击的机会越来越大，因此，采用一种高效的在线入侵诊断方法非常重要[3]。将基于双向联想记忆网络(bidirectional associative memory：BAM)的网络的应用技术、计算方法与入侵诊断技术相结合，构建一个远程航空雷达网络在线入侵诊断模型，对航空雷达网络进行实时在线入侵检测诊断，可以为航空雷达网络建立一个抵御外部网络入侵的闸门[4-6]。使用BAM网络来提取外部入侵数据的模式特征进行匹配，提取网络外部行为特征，对于雷达网络入侵异常行为的检测也就是对网络数据进行分类和识别。

1　航空雷达网络异常数据诊断现存问题

1.1　航空雷达网络入侵诊断

由于雷达网络入侵异常行为的检测常出现滞后性，雷达网络入侵异常行为的在线实时检测越来越受到重视。因此航空雷达网络的在线入侵诊断设计目标为：自动诊断并通过应用软件对入侵数据进行自动防御处理，返回诊断结果；入侵检测信息及诊断结果可以通过电子邮件的形式在网络中进行传送；可通过浏览器网页进行在线诊断检测，现场操作人员可通过网页向目标提出诊断请求并提供诊断信息，诊断结果可通过浏览器进行查询。

1.2　基于BAM网络的入侵数据预处理

雷达网络在线入侵数据预处理就是对网络数据进行简单的分类，将数据分为正常数据已异常数据，对正常数据特征进行轮廓提取，并获取数据特征以及数据特征的可辨识属性矩阵和决策辨识函数，计算测试参数集的所有特征向量，为入侵诊断提供特征匹配样本，其过程如图1所示。

收稿日期:2014-05-16；　**修回日期**:2014-06-25。

作者简介:吴　华(1970-)，男，湖北天门人，副教授，主要从事计算机网络应用技术方向的研究。

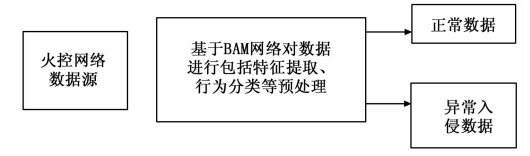

图 1 基于 BAM 网络的入侵数据预处理流程

1.3 雷达网络入侵数据特征判断

雷达网络的在线入侵诊断目的是快速区分出正常数据和异常数据，航空雷达网络所接收到的数据信息用数据集合可表示为 $x^i=(x_1^i,\ldots,x_n^i)\in[0.0,1.0]^n$，所有数据的集合可用 $S\subseteq[0.0,1.0]^n$ 来表示。模型网络中数据变量的现在值与过去值用特征变量来表示，而特征变量的值可以检测也可以进行规定，以适应定义的范围 $[0.0,1.0]$。正常的数据向量集合表示为 $S_{\text{self}}\subseteq S$，而非正常的异常入侵数据向量集合表示为 $S_{\text{nonself}}=S-S_{\text{self}}$。则雷达网络在线入侵数据特征化函数为：

$$\chi_{\text{self}}:[0.0,1.0]^n\rightarrow\{0,1\}$$

$$\chi_{\text{self}}\overrightarrow{(x)}=\begin{cases}1,\text{如果}\ \vec{x}\in\text{正常数据特征向量集合}\ S_{\text{self}}\\0,\text{如果}\ \vec{x}\in\text{异常数据特征向量集合}\ S_{\text{nonself}}\end{cases}\tag{1}$$

模型网络中正常与异常数据信息的特征函数在 $[0.0,0.1]:\mu_{\text{self}}:[0.0,0.1]^n\rightarrow[0.0,0.1]$ 这个区间中取值，其中“1”表示正常数据，“0”用于描述异常数据，“1”与“0”之间的值用于描述异常嫌疑的数据，判断一个数据是否为正常接收的数据或者异常入侵的数据，可以用一个阀值来进行判断，如下：

$$\mu_{\text{self},t}\binom{r}{t}=\begin{cases}1,\text{如果}\ \mu_{\text{self}}\binom{r}{t}>t\\0,\text{如果}\ \mu_{\text{self}}\binom{r}{t}\leqslant t\end{cases}\tag{2}$$

其中：t 就是特征数据判断阀值。

2 航空雷达网络在线入侵诊断方法

2.1 雷达网络在线入侵诊断模型建立

BAM 网络属于人工神经网络的一种，它的网络结构是一种双层双向联想反馈网络，其输入层 X 与输出层 Y 分别有 n，m 个节点，BAM 网络中 X 层的 n 个节点与 Y 层的 m 个节点互连。假设输入层 X 到输出层 Y 的权值矩阵为 $\boldsymbol{W}$，而 Y 到 X 的权值矩阵则为 W^T，即：

$$\boldsymbol{W}:R^n(X)\rightarrow R^m(Y)\tag{3}$$

$$\boldsymbol{W}^T:R^m(Y)\rightarrow R^n(X)\tag{4}$$

基于 BAM 网络航空雷达在线入侵诊断算法引入双层双向联想过程，将动态数据运行到稳态，当输入数据样本 X_{t-1} 作用于 X 层时，将此样本通过 W 矩阵加权到 Y 层，经 Y 层的网络节点转移函数 f_x 进行非线性变换后转化为 Y_{t-1}，Y_{t-1} 作为 Y 层输入再通过 $\boldsymbol{W}^T$ 矩阵加权传回 X 层，经 X 层节点转移函数 f_x 进行非线性变换得到 X_t 后再次进行输入，从而获取在线接收数据是否为入侵数据的结果。其数据样本诊断过程如图 2 所示。

其中：$X(t)=f_x\{f_y[X(t-1)\boldsymbol{W}]\boldsymbol{W}^T\}$；$Y(t)=f_y\{f_x[Y(t-1)\boldsymbol{W}^T]\boldsymbol{W}\}$；若诊断模型有 P 对输入数据样本，则应用外积和法来设计权值矩阵 $\boldsymbol{W}$，如式（5）、式（6）所示

$$\boldsymbol{W}=\sum_{i=1}^{P}X_i^TY_i\tag{5}$$

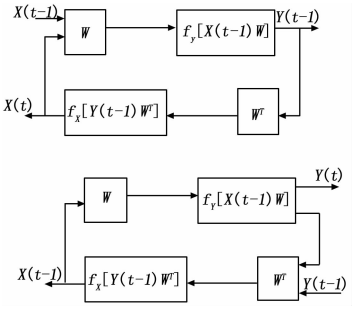

图 2 基于 BAM 网络的数据样本诊断过程

$$\boldsymbol{W}^T=\sum_{i=1}^{P}(X_i^TY_i)^T=\sum_{i=1}^{P}Y_i^TX_i\tag{6}$$

2.2 雷达网络异常行为在线检测算法

雷达网络在线入侵诊断的效率取决于权值矩阵 $\boldsymbol{W}$，如果测试向量维数较多，$\boldsymbol{W}$ 矩阵抑制作用较差，BAM 网络异常数据特征匹配识别需要时间过多，模型无法快速作出诊断识别，因此，要对传统的权值矩阵和测试向量最小化进行优化改进。对于 P 对两两正交的记忆模式 $A_p,p=1,2,\cdots,P,a\in\{-1,1\}^n$，且权值矩阵 $\boldsymbol{W}$ 是按照式（5）与式（6）构造得到，则向 BAM 网络输入 P 个记忆模式中的任何一个 A_p 时，只需一次便能正确计算出相应模式的 B_p。即若

$$A_iA_j^T=\begin{cases}0,i=j\\1,i\neq j\end{cases}$$

$$\boldsymbol{W}=\sum_{i=1}^{P}\boldsymbol{W}_i=\sum_{i=1}^{P}A_i{}^TB_iA_i\boldsymbol{W}=A_iA_i{}^TB_i+\sum_{i\neq j}A_iA_j{}^TB_j=B_i\tag{7}$$

利用层次分析法建立模型网络的层次入侵诊断树图模型，采用上行法简化入侵诊断模型，以实现最小割集。通过在线入侵诊断模型对最小割集进行优化，生成两两正交且维数较少的学习样本空间，以便建立最优化的异常数据特征匹配映射对，并生成权值矩阵 $\boldsymbol{W}$。实时采集外部入侵数据的测试向量，对于航空雷达网络接收到的疑似异常数据向量（$\boldsymbol{X}_t=a_1X_1+a_2X_2+\ldots+a_pX_p,a_i\in(0,1),i=1,2,\cdots,P$）进行入侵诊断，经过入侵诊断模型算法的自学习、自适应能力快速得到异常数据特征匹配向量 $\boldsymbol{Y}_t=\boldsymbol{X}_t\boldsymbol{W}=a_1Y_1+a_2Y_2+\ldots+a_pY_p$。利用 BAM 网络的离散特性来完成特征匹配、搜索，从而优化雷达网络的异常行为诊断。

3 雷达网络在线入侵诊断工作流程

由下文分析，雷达网络在线入侵诊断工作分两阶段进行，第一阶段为基于 BAM 网络的建模与自学习阶段，建模过程中要根据入侵检测信息及特定用户需求建立模型，引入上行法或下行法建立最小割集。在 BAM 网络的自学习阶段，要根据上行法或下行法建立的最小割集建立映射，获取特征样本，进行自训练。建模与自学习阶段具体流程如图 3 所示。

第一阶段基于 BAM 网络的建模与自学习完成后，要进行第二阶段的在线入侵诊断，具体流程如图 4 所示。

4 实验与分析

实验采用某型航空雷达历史数据特征记录，具体如下表 1 所示，采用本文算法进行在线诊断。其中随意提取 10 组数据，

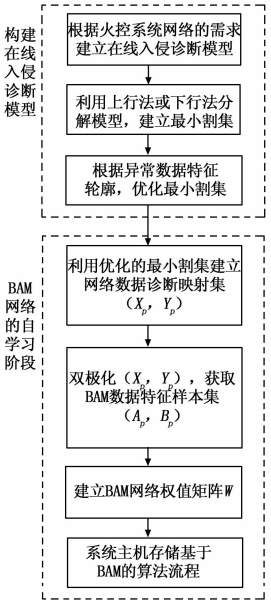

图 3　基于 BAM 网络的建模与自学习流程

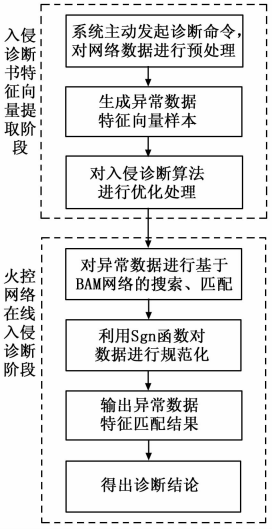

图 4　数据预处理与在线入侵诊断流程

数据编号分别为 $V_1 \sim V_{10}$。每个数据有 9 个特征决定。表示为 V_i（a_1，a_2，a_3；b_1，b_2，b_3；c_1，c_2，c_3，）。

表 1　某大型航空雷达历史数据

V	a_1	a_2	a_3	b_1	b_1	b_1	c_1	c_1	c_1
V_1	0	1	1	1	0	1	1	1	1
V_2	1	0	1	0	0	1	0	1	1
V_3	1	1	0	1	1	1	1	1	1
V_4	1	1	0	1	1	1	1	0	1
V_5	1	1	1	0	1	1	0	1	1
V_6	1	1	1	1	0	1	1	1	1
V_7	1	1	1	0	1	0	1	1	1
V_8	1	0	0	1	1	1	1	0	1
V_9	1	0	1	1	1	1	0	1	1
V_{10}	0	1	1	1	0	1	1	1	1

用本文诊断方法对表 1 中的测试样本数据进行在线诊断，诊断结果如表 2 所示。分析数据可知，本文方法诊断准确率达到 93.3%。

表 2　某大型航空雷达数据诊断结果

V	a_1	a_2	a_3	b_1	b_1	b_1	c_1	c_1	c_1
V_1	0	1	1	1	0	1	0	1	1
V_2	0	0	1	0	0	1	0	1	1
V_3	0	1	0	1	1	1	1	1	1
V_4	1	1	0	1	1	1	1	0	1
V_5	1	1	1	0	1	1	0	1	1
V_6	1	1	1	1	0	1	1	1	1
V_7	1	1	1	0	1	0	1	1	1
V_8	1	0	0	1	1	1	1	0	1
V_9	1	0	1	1	1	1	1	1	1
V_{10}	0	1	1	1	0	1	1	0	1

为了进一步验证本文方法的有效性，下面对本文算法的入侵诊断的错误率及与传统系统的性能进行比较。通过由协议标识、标志位、序列号、应答号、源 IP 地址、源端口号等组成的 6 组诊断数据样本对基于 BAM 网络的入侵诊断能力进行仿真实验，测试的一组数据包含 100 个数据包，分别对正常数据与异常入侵数据进行诊断识别，并得出错误率。仿真结果如表 3 所示。

表 3　基于 BAM 网络的入侵诊断仿真结果

诊断数据样本	正常数据的检测率/(%)	入侵数据的检测率/(%)	错误率/(%)
1	94.32	94.22	5.68
2	95.26	94.56	4.74
3	95.48	94.57	4.52
4	95.87	95.09	4.23
5	94.56	93.47	5.44
6	94.78	93.89	5.22

通过表 3 的仿真结果可以看出基于 BAM 网络的在线入侵诊断算法对于异常入侵数据具有较好的识别分类能力，为了验证本方法的优越性，对以上样本数据分别用传统诊断检测方法与应用基于 BAM 网络的诊断方法进行仿真对比实验。仿真对比实验结果如表 4 所示。

表 4　传统算法与本算法的比较结果

仿真算法	诊断率	误报率	漏报率
传统算法	0.930 34	0.030 23	0.018 07
基于 BAM	0.982 04	0.010 28	0.010 05

通过表 4 可以看出，应用基于 BAM 网络的在线入侵诊断算法相比于传统诊断算法在数据的诊断率、误报率、漏报率方面均有明显的提高，因此，本方法具有一定的先进性与实用性。

5　结语

根据以上研究建立的基于 BAM 网络的航空雷达网络在线入侵诊断方法，BAM 网络具有的离散的网络结构以及双向联

（下转第 63 页）

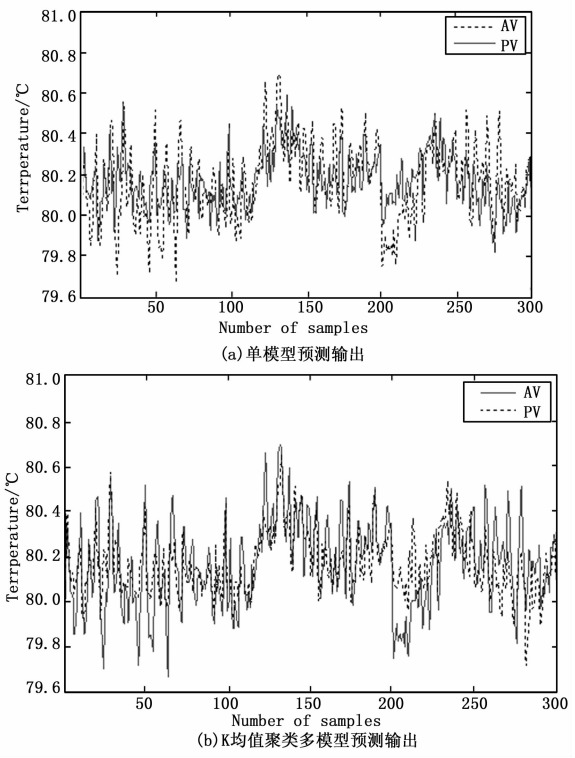

图 4　气液分离器温度预测对比

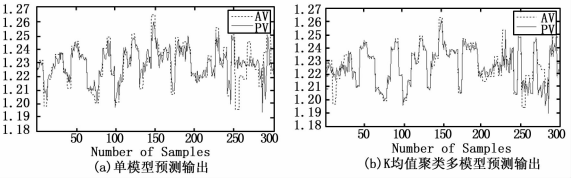

图 5　G 与 H 产率比预测对比

度较单模型与基于 C 均值聚类的多模型建模方法有所提高。相关分析和最小二乘支持向量机多模型建模方法，在 TE 化工过程建模和预测中取得了很好的测试性能。

4　结论

TE 化工过程是一个高度非线性，复杂的化工过程，过程变量繁多，并且工业数据会随着工况的改变成堆聚集的特性。如果采用 MIMO 模型对整体进行建模时需要很大的计算量，并且难以保证模型精度。本文首先采用相关分析法将 TE 过程分为 3 个子系统，对每个子系统分别采用了基于 LSSVM 的单模型建模，基于 C 均值的多模型建模和基于 k 均值的多模型建模进行建模仿真，并且采用泛化均方根误差和最大相对误差对两种模型进行比较，结果表明基于 k 均值的多模型具有更好的泛化能力，提高了整体的预测精度。

参考文献：

[1] 李修亮，苏宏业，褚　健. 基于在线聚类和关联向量机的多模型软测量建模 [J]. 化工自动化及仪表. 2008，35 (3)：34－37.

[2] 李雅芹，杨慧中. 基于仿射传播聚类和高斯过程的多模型建模方法 [J]. 计算机与应用化学，2010，27 (1)：51－54.

[3] Frey B J，D. Dueck. Clustering by passing messages between data points [J]. Science，2007，315 (5814)：972－976.

[4] 夏梁志，李　华，饶克克，等. 基于 QGA－LSSVM 的醋酸乙烯聚合率软测量建模 [J]. 计算机测量与控制，2012，20 (4)：907－909.

[5] Downs J J，Vogel E F . Aplant wide industrial process control problem [J] . Computers Chem Engng，1993，17 (3) ：245－25.

[6] Ben C. Juricek，Dale E. Seborg，Wallace E. Larimore. Identification of the Tennessee Eastman challenge process with subspace methods [J]. Control Engineering Practice，2001 (9)：1337－1351.

[7] 袁志发，周静芋. 多元统计分析 [M]. 北京. 科学出版社，2004.

[8] 宋　坤. 基于 SVM 多模型建模的软测量研究 [D]. 南京：南京工业大学，2010.

[9] 陈文亮，张　湜，李　晖. 基于 LS-SVM 沼气进化变压吸附过程甲烷浓度建模 [J]. 天然气化工，2013，38 (1)：36－38.

[10] Jain A K，Flynn P J. Image segmentation using clustering [A]. In：Ahuja N，Bowyer K. eds. Advances in Image understanding：A. Festchrift for Azriel Rosenfeld [C]. Piscataway：IEEE press，1996：65－83.

[11] 周世兵，徐振源，唐旭清. 新的 K-均值算法最佳聚类数确定方法 [J]. 计算机工程与应用，2010，46 (16)：27－31.

[12] 李丽娟，潘　磊，张　湜. 基于 AP 聚类算法的跳汰机床层松散度软测量建模 [J]. 化工学报，2012，63 (9)：2675－2680.

[13] Frey B J，Dueck D. Clustering by passing messages between data points [J]. Science，2007，315 (5814)：972－976.

[14] Yang H，Luo F，Xu Y G，et al. New LS-SVM nonlinear predictive controller method based on chaos optimization [J]. Computer Engineering and Applications，2010，46 (5)：229－232.

(上接第 59 页)

想记忆搜索功能，可以有效的提高了航空雷达网络入侵监测诊断效率，且具有较好的适应性与多样性，本文方法诊断准确率达到 93.3%。相比于传统的检测算法，在检测率、误报率、漏报率等方面均有明显改善，并通过仿真实例验证了该方法的有效性与通用性。

参考文献：

[1] 马殿哲，常天庆，陈军伟. 基于 BAM 网络的坦克航空雷达在线故障诊断方法研究 [J]. 计算机测量与控制，2011，19 (12)：3001－3003.

[2] 龙鹏飞，宋　振. 基于 BAM 网络和遗传免疫的入侵检测算法 [J]. 计算机工程与设计，2007，28 (12)：2793－2795.

[3] 文　莹，肖明清，盛　晟，等. 基于概念格的航空雷达故障诊断研究 [J]. 计算机测量与控制，2013，21 (10)：2612－2614.

[4] 戴英侠，连一峰，王　航. 模型安全与入侵检测 [M]. 北京：清华大学出版社，2002.

[5] 刘　赛，许　斌，梁意文. 入侵检测模型中的一种免疫遗传算法 [J]. 计算机工程，2004，30 (8)：63－64.

[6] 徐琰珂，梁晓庚，贾晓洪. 雷达/红外双模导引头信息融合算法研究 [J]. 计算机测量与控制，2013，21 (1)：129－132.