文章编号:1006-9348(2020)10-0249-04

# 多元异构网络安全日志数据融合方法仿真

王 萍
(扬州大学广陵学院,江苏 扬州 225000)

摘要:网络结构日趋复杂,关键性应用的不断普及和深入,网络安全已成为不可忽视的问题。针对网络安全日志数据的分析,提出多元异构网络安全日志数据融合方法。方法首先对采集的异构网络安全日志数据进行预处理,采用Kalman滤波对日志数据形成时产生的噪声影响进行去除,然后通过传感器对网络状态进行观测,并创建网络状态的观测模型,对观测值进行加权处理,建立含有最佳加权系数的加权矩阵;最终将加权矩阵与模糊集理论相结合,实现对网络安全日志数据的加权融合。仿真结果显示,提出的网络安全日志数据融合方法,能够彻底地消除无效数据和错误数据,对有效数据的融合效果较好,具有较高的可信度和准确性。

关键词:多元异构网络;网络安全日志;数据融合
中图分类号:TN911.73 文献标识码:B

# Multi-Heterogeneous Network Security Log Data Fusion Method Simulation

WANG Ping
(Guangling College, Yangzhou University, Yangzhou Jiangsu 225000, China)

**ABSTRACT:** The network structure is becoming more and more complex. With the popularization and deepening of key applications, the network security becomes a problem that can't be ignored. For the analysis of network security log data, this article puts forward a method to fuse security log data in multi-heterogeneous network fusion. Firstly, this method preprocessed the collected security log data in heterogeneous network, and used Kalman filtering method to remove the noise formed by the log data. And then, our method observed the network state through the sensor and created an observation model of network state. Moreover, the observation values were weighted to establish the weighting matrix with the best weighting coefficient. Finally, the weighting matrix was combined with the fuzzy set theory. Thus, the weighted fusion of network security log data was achieved. Simulation results show that the proposed method of network security log data fusion can completely eliminate invalid data and erroneous data. Meanwhile, this method has better fusion effect on valid data and has higher credibility and accuracy.

**KEYWORDS:** Multi-heterogeneous network; Network security log; Data fusion

## 1 引言

计算机网络的应用越来越广泛,现今已与人类生活密不可分。随着网络的不断发展,网络的安全面临着较为严峻的考验,特别是面对多元异构网络情况下,数据中会夹杂着一些具有攻击性的病毒。这些对网络有严重威胁的木马病毒,具有规模较大、类型较多和变化较快的特性,加大了网络安全防护工作的难度[1]。为了解决网络安全的防护问题,各种防御、监控等系统被研发出来。但是这些防护系统在运行的过程中会产生大量的安全日志数据,并且日志数据类型和内容都各不相同,若只想单独通过对日志的读取来分析网络安全信息,无法了解具体的安全问题[2]。由此看来,如何在海量数据的影响下实现对网络安全的高效监控与管理,同时结合多元异构网络在进行安全防护时产生的大量多样化日志,对网络潜在的安全隐患进行综合分析,是将来网络安全的发展方向。数据融合技术可以依据融合算法将海量多样化数据融合在一起,实现多元异构网络安全日志数据的分析,是解决当前网络问题的关键[3]。

基金项目:智慧校园上网数据分析及服务平台(2018-R66972)
收稿日期:2019-02-26 修回日期:2019-04-19

## 2 相关工作

数据融合源由美国国防部于 1973 年研发的针对声呐信息的处理系统，通过多个传感器获取信息，主要的问题在于选取合适的融合算法，经常使用的融合算法主要可分为随机和智能两类。随机融合算法包括 Kalman 滤波法、多贝叶斯估计法等；智能融合算法包含模糊逻辑理论、神经网络等。

1) Kalman 滤波数据融合法，对各个网络日志数据进行预处理，并采用卡尔曼滤波对其进行估计，然后将数据传送到簇头节点进行加权数据融合[4]。

2) 多贝叶斯估计数据融合法，运用离散 Kalman 滤波对网络数据线性化，然后创建网络安全日志数据数学模型，根据模型参数的先验情况下，采用多贝叶斯估计方法对线性化网络安全日志数据进行加权融合[5]。

3) 模糊逻辑理论数据融合法，首先对各种网络完全日志数据进行分析，然后采用贴进度算法对网络安全日志数据进行初步融合，并消除无效数据和融合错误，最后采用模糊逻辑理论对第一步融合的数据进行二次融合，最终得到融合结果[6,7]。

4) 神经网络数据融合法，按照相应的神经网络对不同的网络安全日志数据进行处理，然后对神经网络处理结果进行统一化处理，最后根据 D－S 证据对经过处理的网络安全日志数据进行融合[8]。

以上方法虽然能够将数据融合，为网络安全防护工作作出贡献，但在数据融合过程中，均有较大误差出现，导致融合效果较差。所提方法综和上述方法的优势，提出针对多元异构网络安全日志数据的融合方法。所提方法不仅可以弥补上述方法的不足之处，还能够给予网络安全防护工作最大的支持。

## 3 针对多元异构网络安全日志数据的融合

### 3.1 网络安全日志数据预处理

在多元异构网络环境中，安全日志数据的数量巨大，参与融合数据的数量也比较大。并且还会受到网络环境的影响，在融合时会出现较大的误差，影响数据融合的效果[9,10]。为了减少数据形成时所受的环境干扰，需要对网络日志数据进行预处理。所提方法采用 Grubbs 统计算法对数据进行预处理，该算法的优势是可以同时消除多个异常数据，且计算过程简洁。

假设一组网络安全日志数据 $x_1, x_2, \cdots, x_n$ 服从正态分布，令

$$x_0 = \frac{1}{n}\sum_{i=1}^{n} x_i, v_i = x_i - x_0, \delta = \sqrt{\frac{1}{n}\sum_{i=1}^{n} v_i^2} \quad (1)$$

式中：$n$ 表示为安全日志数量，$v_i$ 表示正态分布参数，$\delta$ 表示方差。

按照顺序统计原理，Grubbs 计算统计分布

$$g_i = \frac{x_i - x_0}{\delta} \quad (2)$$

在特定的显著水平（$\alpha = 0.05$）之后，采用查表法找出临界值 $g_0(n,\alpha)$，即 $p[g_i \geqslant g_0(n,\alpha)] = a$ 为极小概率事件。如果检测值中统计量为 $g_i \leqslant g_0(n,\alpha)$，该数据为有效数据；反之，该数据为无效数据，需要对其进行消除。

在对数据进行预处理后，消除了大量的无效数据，但是在数据形成时，不可避免地会受到周围环境噪声的干扰，为了能够有效地去除噪声影响，所提方法采用 Kalman 滤波对网络安全日志数据进行滤噪处理。

Klaman 滤波算法具有较好的包容误差的能力，是一种以最小均方误差为标准的估计算法，主要为创建滤除噪声过程的状态空间模型，运用当前时刻和上一时刻的网络系统状态估计值和观测值，依据过程噪声和观测噪声对网络系统状态的估计值进行更新。具体过程如下。

网络状态方程为

$$X(k) = AX(k-1) + W(k) \quad (3)$$

式中：$X(k)$、$X(k-1)$ 分别表示 $k$、$k-1$ 时刻网络状态值，$A$ 表示状态变换矩阵，$W(k)$ 表示过程噪声，$W(k) \sim N(0,Q)$。

网络状态观测方程

$$Z(k) = HX(k) + V(k) \quad (4)$$

式中：$Z(k)$ 表示 $k$ 时刻的检测值，$H$ 表示检测矩阵，$V(k)$ 表示观测噪声，$V(k) \sim N(0,R)$。

这两种噪声之间没有联系，相互独立。

在多元异构网络环境中，将这两种噪声 $W(k)$、$V(k)$ 视为高斯白噪声，依据式(3) 对网络状态进行初步检测，采用 $k-1$ 时刻的网络状态 $X(k-1|k-1)$ 对 $k$ 时刻的检测值 $X(k|k-1)$ 进行计算，计算公式为

$$X(k|k-1) = AX(k-1|k-1) + \delta U(k) \quad (5)$$

其中：$U(k)$ 表示为网络当前状态的控制量，该值也可为 0。

对于 $X(k|k-1)$ 协方差的表达式为

$$P(k|k-1) = AP(k|k)A^T + U(k) \quad (6)$$

式中，$P(k|k-1)$ 和 $X(k|k-1)$ 分别表示 $P(k-1|k-1)$ 和 $X(k-1|k-1)$ 对应的协方差，$A^T$ 表示 $A$ 的转换安置矩阵。

通过式(4) 和式(5) 可以计算出 $k$ 时刻的网络状态最佳估计值 $X(k|k)$

$$X(k|k) = X(k|k-1) + Kg(k)[Z(k) - HK(k|k-1)] \quad (7)$$

式中：$Kg(k)$ 表示 Klaman 增益，表达式为

$$Kg(k) = P(k|k-1)H^T[HP(k|k-1)H^T + R]^{-1} \quad (8)$$

为了使 Kalman 算法可以循环迭代，还需要对 $k$ 时刻 $K(k|k)$ 的协方差进行更新，更新公式为

$$P(k|k) = [I - Kg(k)H]P(k|k-1) \quad (9)$$

式中，$I$ 表示单位阵。当网络进入到下一时刻时，$P(k|k)$ 就是式(6) 中的 $P(k-1|k-1)$，这样 Kalman 滤波就可以实现无限循环迭代。

在多元异构网络中，存在干扰较多的情况下，数据在进

行预处理后，采用 Kalman 滤波对其进行滤噪处理，可有效地消除噪声干扰。

### 3.2 网络状态观测模型及最佳加权系数的确定

假设运用 $N$ 个相同类型的传感器对网络环境的状态进行观测，$x_{ik}$ 为第 $i$ 个传感器在 $k$ 时刻生成的数据，观测方程表达式为

$$x_{ik} = x_k + \varepsilon_i \tag{10}$$

式中，$x_k$ 表示真实值，$\varepsilon_i$ 表示观测过程中存在的误差，包含传感器自带的误差和检测系统的误差等，为了使观测模型更加简洁，假设 $\varepsilon_i$ 具有平稳的统计特性 $\varepsilon_i \sim N(0,\sigma_i^2)$，在 $i \neq j$ 时 $\varepsilon_i$ 和 $\varepsilon_j$ 之间没有联系，相互独立，$\sigma_i^2$ 表示第 $i$ 个观测误差的方差。

将观测值的加权平均视为对真实值的估计

$$\hat{x}_k = \sum_{i=1}^{n} \omega_i x_{ik} \tag{11}$$

式中，$\hat{x}_k$ 表示 $k$ 时刻真实值的估计值，$\omega_i$ 表示第 $i$ 个观测数据的加权系数。对上式的等号左右求期望得出

$$E[\hat{x}_k] = E\left[\sum_{i=1}^{n} \omega_i x_{ik}\right] = \left(\sum_{i=1}^{n} \omega_i\right) x_k \tag{12}$$

为使 $\hat{x}_k$ 为 $x_k$ 的无偏差估计，则 $E[\hat{x}_k] = x_k$，由此可得到

$$\sum_{i=1}^{n} \omega_i = 1 \tag{13}$$

上述为加权系数的满足条件，可以令所有观测值的加权系数总和为 1。

假设 $x_{1k}, x_{2k}, \cdots x_{nk}$ 之间没有任何联系，创建加权估计均方误差的公式为

$$\xi = E[(\hat{x}_k - x_k)^2] = \sum_{i=1}^{n} \omega_i^2 \sigma_i^2 \tag{14}$$

由该式可以得出，对最佳加权系数进行求解，就是对含有约束条件下多元函数进行求解，运用拉格朗日乘子法，计算出传感器的最佳加权系数，计算公式为

$$\omega_i^* = 1/\sigma_i^2 \sum_{j=2}^{n} \frac{1}{\sigma_j^2} \tag{15}$$

式中：$\omega_i^*$ 表示第 $i$ 个传感器的最佳加权系数。

### 3.3 最佳加权融合方法

所提的数据融合方法将加权矩阵和模糊推理结合在一起，结合优先级概念防止拥塞，减少数据传输延迟，提升多元异构网络安全日志数据融合的准确性和方差。该方法使用于分簇型多元异构网络，用于分簇间数据和分簇头数据的融合。

假设 $i$ 节点在 $t$ 时刻检测到 $j$ 类的感知值为 $d_{ij}(t)$，$i \in [1,N]$，$j \in [1,M]$，从节点 $i$ 采集到的所有相同类数据可表示为

$$d_{ij}(t) = \begin{pmatrix} d_{11}(t) & d_{12}(t) & \cdots & d_{1M}(t) \\ d_{21}(t) & d_{22}(t) & \cdots & d_{1M}(t) \\ \vdots & \vdots & & \vdots \\ d_{N1}(t) & d_{N2}(t) & \cdots & d_{NM}(t) \end{pmatrix} \tag{16}$$

考虑到多元异构网络环境下，影响网络安全日志数据的主要因素为网络类型、对网络造成威胁的具体行为以及安全日志产生的环境，将这些因素视为模糊逻辑中的输入变量，由此可得出可信度。在分簇过程前，可信度较低的节点数据将被排除，不能参与分簇过程。输入变量，即置信因子的计算公式为

$$\tilde{A} = \int_{x \in X} (x)/x = \int_{x \in X} \left[\int_{u \in J_x} 1/u\right]/x, J_x \subseteq [0,1] \tag{17}$$

式中，$u$ 表示主隶属度值，$J_x$ 为主隶属度值的范围，区间Ⅱ型模糊集的二级隶属度值为 1，$(\tilde{A}) = U_{x \in X}(\underline{\mu}_{\tilde{A}}(x), \overline{\mu}_{\tilde{A}}(x))$，如果置信因数没超过 0.5，那就说明数据不可信，需要排除，不能参与分簇。

节点生成的任意数取值范围在 0 ~ 1，若不超过阈值 $T$，就将该节点视为簇头节点。由于在分簇之前排除了部分无用节点，因此需要对 $P$ 的参数进行优化，$i$ 的计算公式为

$$T(i) = \begin{cases} \dfrac{lp}{1 - lp\{rmod[1/lp]\}}, i \in G \\ 0, \text{其他} \end{cases} \tag{18}$$

式中，$p$ 表示节点中能参与成簇头的百分比，$r$ 表示当前的循环次数，$l = \sqrt{(N-n)/N}$ 为对簇头百分数的优化参数，$n$ 表示排除节点的数量，$G$ 为最新 $rmod[1/(lp)]$ 次循环中不是簇头的节点集合。节点在选成簇头之后，需要通知别的节点自身是新簇头，其它节点由自身到簇头之间距离的大小选择性加入分类簇。

假设每次循环都有 $K$ 个簇，分簇过程实现后，进入到相对稳定的数据传输状态。每个异构网络安全日志，通过生成的模糊逻辑控制器为数据 $d_{ij}(t)$ 产生一个置信因子 $CF_i$，$i \in [1,N_k]$，$N_k$ 为第 $k$ 个簇的簇内节点数，$k \in [1,K]$。数据融合方程表示为

$$\begin{cases} fd_1 = d_{11}(t)\alpha_1 + d_{21}(t)\alpha_2 + \cdots + d_{N_k1}(t)\alpha_{N_k} \\ fd_2 = d_{12}(t)\alpha_1 + d_{22}(t)\alpha_2 + \cdots + d_{N_k2}(t)\alpha_{N_k} \\ \vdots \\ fd_M = d_{1M}(t)\alpha_1 + d_{2M}(t)\alpha_2 + \cdots + d_{N_kM}(t)\alpha_{N_k} \end{cases} \tag{19}$$

将上述公式改写成矩阵形式，并提取置信因子，表达式为

$$S_{fd} = \frac{1}{CF_1 + CF_2 + \cdots + CF_{N_k}}(CF_1, CF_2, \cdots, CF_{N_k}) \begin{pmatrix} d_{11}(t) & d_{11}(t) & \cdots & d_{1M}(t) \\ d_{21}(t) & d_{22}(t) & \cdots & d_{2M}(t) \\ \vdots & \vdots & & \vdots \\ d_{N_k1}(t) & d_{N_k2}(t) & \cdots & d_{N_kM}(t) \end{pmatrix} = \{fd_1, fd_2, \cdots, fd_M\} \tag{20}$$

式中，$S_{fd} = \{fd_1, fd_2, \cdots, fd_M\}$ 表示簇内节点数据融合后的形式，$\alpha_i = CF_i / \sum_{i=1}^{N_k} CF_i$。

在多元异构网络中，按照安全日志数据的类型拆分成等

成的列队，实现对数据融合的缓存，根据采用优先程度将各个列队从 0 标记到 $P_{max}$。在正常情况下，直接进行数据融合处理。但在特殊情况下，节点在采集日志数据之前，需要对数据进行优先程度分级，簇头节点依据数据使用优先级，对优先级较高的数据先行融合，与此同时，利用聚合因子防止网络拥塞现象的产生。

簇头节点采集到源自分簇间 $N_k$ 个节点的数据信息有 $M \times N_k$ 个，其中 $M$ 表示为数据的类型。将加急的数据放入优先程度较高的列队中，先进行融合并传输到网络环境中。每个列队中最多包含 $M \times N/(1+P_{\max})$ 个信息，聚合因子表示为

$$\beta_i = \frac{M \times N_k \times TD_i}{P_{\max}\left(\sum_{i=0} TD_i \times (1+P_{\max})\right)} \tag{21}$$

其中，$i$ 表示数据的优先级，$TD_i$ 表示优先程度为 $i$ 的数据每跳延迟。依据列队调整 $\beta_i$ 值，以保证数据得到快速处理。

## 4 仿真证明

为了验证所提方法的性能，以仿真环境为 Matlab2018Rb，计算机配置为 Intel(R) i7 CPU@3.5GHz，8GB 内存，windows7 旗舰版操作系统的仿真平台，采用卡尔曼滤波数据融合法和神经网络数据融合法，与所提方法进行对比实验。

实验选用某网络的安全日志数据集，该数据来源于某公司 2000 台主机和 50 台服务器在遭受到网络攻击时产生的安全日志，希望在这些数据中获取到异常行为。实验参数具体如表 1：

表 1 实验参数具体

| 数据名 | 数据类型 | 数据大小 | 包含主机数量/台 |
|---|---|---|---|
| 网络流量数据 | 网络流量 | 50GB | >1000 |
| IPS 日志数据 | 防火墙 | >50GB | >1000 |

### 4.1 实验结果分析

实验采用网络基站接收到的数据准确率作为融合方法的评价指标，图 1 是网络基站接收数据的准确率与通信时间之间的关系：

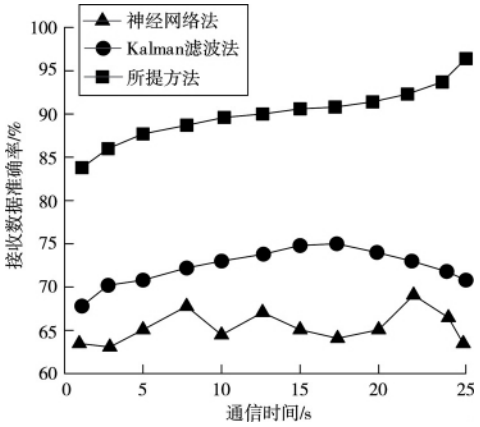


图 1 接收数据准确率

分析图 1 可知：采用神经网络数据融合方法、Kalman 滤波数据融合法和所提方法进行安全日志数据融合时，神经网络数据融合方法是三种方法中准确率最低的，Kalman 滤波数据融合法相对来说较好一些，但这两种方法都没有对数据的有效与否作出判断的步骤，将所有数据进行加权融合，其中包含了无效或错误数据，这些数据具有较高的权值，对最终融合结果有很大影响；所提方法在进行数据融合时不仅对数据的可信度进行分辨，考虑了时间延迟因素，因此所提算法在三种方法中准确率最高。

采用残差平方和(RSS)和方差(P)作为三种方法的评价指标，再次进行对比实验，实验对比结果如表 2 所示：

表 2 融合结果对比

| 融合方法 | 指标 | |
|---|---|---|
| | RSS/cm$^2$ | P/cm$^2$ |
| 神经网络法 | 84.684 | 2.016 |
| Kalman 滤波法 | 98.632 | 4.827 |
| 所提方法 | 35.018 | 0.713 |

通过分析表 1 可知：神经网络数据融合方法与 Kalman 滤波方法相比，具有较低的 RSS，但是其方差也低，而 Kalman 滤波方法与之相反，具有较高的方差，RSS 也是三种方法中最高的；所提方法具有最小的方差和 RSS，说明所提方法进行网络安全日志数据融合，具有较高的可信度和准确性。

## 5 结束语

本文着重分析了多元异构网络的安全隐患，提出安全日志数据的融合方法，根据融合结果可实现网络安全日志数据的分析。该方法将几种常用的数据融合方法的优势作为参考，在融合处理之前对数据的可信度进行分辨，最后对有效数据进行数据融合。仿真证明所提方法具有较高的可信度，融合效果较好，可为网络安全的防护工作提供很大帮助。

参考文献：

[1] 唐菁敏，王超. 基于中继节点机制的分簇数据融合算法[J]. 云南大学学报(自然科学版)，2016，38(5)：703－707.

[2] 吕丹，龙华，赵继东，等. 基于地图地理信息点的数据融合算法的改进[J]. 西北大学学报(自然科学版)，2017，47(5)：687－692.

[3] 杨中杰. 分布式多维空间传输信息准确融合仿真研究[J]. 计算机仿真，2017，34(5)：205－208.

[4] 张靖，陈鸿跃，陈雨，等. 一种基于联邦卡尔曼滤波器的多源信息融合定位算法[J]. 导弹与航天运载技术，2018，360(2)：98－106.

(下转第 346 页)

[7] 刁建新,杜一凡. 智能化建筑结构抗震强度性能准确预测仿真[J]. 计算机仿真,2019,36(3):327-330.
[8] 苏仁权,董伟娜. 基于椭球面屈服模型的钢框架梁柱全焊节点断裂分析[J]. 价值工程,2018,37(1):108-110.
[9] 陈健,袁慎芳,王卉,等. 基于高斯权值-混合建议分布粒子滤波的疲劳裂纹扩展预测[J]. 航空学报,2017,38(11):163-171.
[10] 黄元昌. 橡胶与塑料材料的疲劳裂纹处理方法[J]. 橡塑技术与装备,2017,43(24): 33-38.
[11] 李云强,赵立普,李伟东,等. 考虑进气冷却效应的活塞低周疲劳寿命预测[J]. 西安交通大学学报,2019,53(7):45-51.
[12] 陈家骐,华建兵,段园煜,等. 基于粒子群优化的DGM(1,1)模型在基坑变形安全预测中的研究[J]. 中国安全生产科学技术,2019,15(03):161-166.

[作者简介]
高田冰(1987-),男(汉族),山东海阳人,硕士,工程师,研究方向:建筑工程。

(上接第158页)

[2] 邹劲柏,谢浩,艾渤,等. 高速移动环境大规模MIMO信道建模与性能分析[J]. 铁道学报,2018,40(4):68-73.
[3] 李倩,王公仆,李清勇,等. 适应高速铁路场景的新型基扩展信道估计模型[J]. 铁道学报,2017,39(9):81-88.
[4] 张嘉驰,陶成,孙溶辰,等. 基于传播图理论的隧道场景无线信道模型构建与验证[J]. 铁道学报,2016,38(10):46-54.
[5] 滕志军,滕利鑫,谢露莹,等. 基于多态蚁群优化算法的认知无线电动态频谱接入策略[J]. 江苏大学学报(自然科学版),2020,41(2): 230-236.
[6] 刘流,陈勇,张建照. 面向CR-NOMA的动态频谱共享模型与分配算法研究[J]. 通信技术,2019,52(11):2677-2682.
[7] 董晓庆. 异构无线网络密集部署场景下高效网络接入及频谱分配[J]. 计算机工程与应用,2019,55(04):101-111.
[8] 蔡畅,王亚芳,苗兵梅,等. 基于改进遗传算法的认知无线传感网动态频谱分配方案[J]. 电信科学,2017,33(08):85-93.

[作者简介]
朱发财(1979-),男(汉族),福建龙海人,硕士,副教授,主要研究方向:移动通信、物联网。
许济金(1979-),男(汉族),福建漳州人,硕士,讲师,主要研究方向:电子信息、物联网。

(上接第190页)

[11] Ulaby F T, Moerr R K, Fung A K. Micorwave Remote Sensing[M]. Vol.1, Massachusetts: Addison-Wesley Publishing Com-Pany,1986.
[12] 张祖荫,林士杰. 微波辐射测量技术及应用[M]. 北京:电子工业出版社, 1995-2.
[13] Stumpf R, Pennock J. Calibration of a General Optical Equation for Remote Sensing of Suspended Sediments in a Moderately Turbid Estuary[J]. J Geo Res, 1989,94(C10):14363-14371.
[14] 肖泽龙. 毫米波对隐匿物品辐射成像研究[D]. 南京理工大学. 2007.

[作者简介]
李 珊(1996-),女(汉族),陕西省渭南市人,硕士研究生,主要研究领域为毫米波。
张光锋(1975-),男(汉族),河北省石家庄市人,副研究员,硕士研究生导师,主要研究领域为亚毫米波、毫米波目标辐射特性与建模。
史 强(1995-),男(汉族),山西省大同市人,硕士研究生,主要研究领域为毫米波。
朱 莉(1979-),女(汉族),江苏省无锡市人,副研究员,硕士研究生导师,主要研究领域为微波毫米波精确探测系统设计、研究及工程化实现。

(上接第252页)

[5] 史春燕,翟羽婷,王磊. 基于贝叶斯网络的体域网多模态健康数据融合方法[J]. 传感技术学报,2017,30(10):1602-1607.
[6] 胡昌林,王蕾. 一种基础模糊理论的自适应数据平滑方法[J]. 现代雷达,2016,38(7): 49-51.
[7] 石爱业,徐立中,杨先一,等. 基于神经网络-证据理论的遥感图像数据融合与湖泊水质状况识别[J]. 中国图象图形学报,2018,10(3):372-377.
[8] 林家泉,张天娇,陈维兴. 桥载监控网络路由中基于分簇的数据融合算法[J]. 计算机工程与设计,2016,37(5):1125-1128.
[9] 冯长中,吴松华,刘秉义. 激光雷达探测信号数据融合算法[J]. 光子学报,2018,47(6): 99-107.
[10] 丁浩晗,冯辉,徐海祥,等. 基于改进加权融合算法的动力定位数据融合[J]. 武汉理工大学学报(交通科学与工程版),2016,40(4): 663-669.

[作者简介]
王 萍(1977-),女(汉族),江苏扬州人,硕士,高级实验师,研究方向:网络管理,网络安全。