DOI:10.19322/j.cnki.issn.1006-4710.2018.04.018

基于改进证据理论的物联网安全态势评估

冯英伟[1]，王庆福[2]，吕　国[1]，肖瑞雪[1]

(1.河北建筑工程学院 现代教育技术中心，河北 张家口 075000；2.辽宁行政学院 信息技术系，辽宁 沈阳 110161)

摘要：传统证据理论的物联网安全态势评估模型通过专家经验获取物联网态势BPA值，缺乏科学客观性，导致物联网安全评估结果不理想，本文提出基于改进证据理论的物联网安全态势评估模型。首先采用D-S合成规则从mass函数、信任测度与似然测度三方面构建物联网安全态势评估模型，获取的评估结果稍有偏差；然后将采集态势指标输入到GA-BP神经物联网操作层训练学习输出最佳态势BPA，最后基于最佳态势BPA的D-S证据融合流程获取准确的物联网安全态势评估结果。实验结果表明，本文模型能够准确挖掘云计算服务器故障的变化特点，获得了理想的云计算服务器故障诊断结果。

关键词：证据理论；mass函数；证据融合；物联网安全态势；评估模型

中图分类号：TP393.08　　**文献标志码**：A　　**文章编号**：1006-4710(2018)04-0495-07

Security situation assessmenton IOT based on improved evidence theory

FENG Yingwei[1], WANG Qingfu[2], LÜ Guo[1], XIAO Ruixue[1]

(1. Modern Education Technical Center, Hebei University of Architecture, Zhangjiakou 075000, China;
2. Department of Information Technology, Liaoning Academy of Governance, Shenyang 110161, China)

Abstract: The assessment model of security situation on the Internet of Things, based on the traditional evidence theory, obtains the situation BPA value of the Internet of Things through the specialist experience. The results from the security assessment of the Internet of Things proved to be unsatisfactory due to lack of the scientific objectivity. This paper puts forward the assessment model of security situation on the Internet of Things based on the improvement of the evidence theory. First, the D-S synthesis rule is used to construct the assessment model of security situation on the Internet of Things from the three aspects including the mass function, the trust measurement and the likelihood measurement, with the evaluation results slightly deviant. Then, the index for acquisition situation will be inputted to the operation layer of GA-BP neural network to output the best situation of BPA by training and studying. Finally, the accurate results from the assessment on the security situation on the Internet of Things are to be obtained based on the fusion process of D-S evidence in view of the best situation of BPA. The experimental results show that this model can detect the change characteristics of the faults of the cloud computing server, and acquire an ideal result from the fault diagnosis of the cloud computing server.

Key words: evidence theory; mass function; evidence fusion; security situation of the Internet of Things; evaluation model

物联网时代的到来不仅方便了人类的日常生活，更为社会生产力的发展提供了有效手段。由于物联网结构的组成错综复杂涉及范围广泛，一旦遭到攻击，就会爆发连锁性的破坏，物联网安全受到了前所未有的考验[1-3]。如何进行有效的物联网安全态势评估成为研究的重点。物联网设备因为信息汇总与模糊信息逻辑能力的匮乏，保持着独立的状态，干扰管理员判断，致使物联网安全态势不易鉴定，为

收稿日期：2018-04-18

基金项目：河北省科技计划资助项目(16210341)；河北建筑工程学院校级科研基金资助项目(2016XJJQN13)；河北省教育厅青年基金资助项目(QN2017322)；高等教育学会高等教育科学研究课题资助项目(GJXHZ2017-09)

作者简介：冯英伟，男，硕士，副教授，主要研究方向为云计算与物联网技术。E-mail：fyw0529@163.com

物联网安全态势的评估增加了难度。因此,亟需一个行之有效的物联网安全态势评估方法[5]。

针对物联网安全态势评估问题,有学者提出了一种基于语义本体和用户定义规则的情况推理的网络安全态势感知模型,该文技术为解决物联网安全领域中的语义异构问题提供了统一、形式化的描述[6]。该方法提出了反映物联网安全状况的四个关键子域:上下文、攻击、漏洞和网络流。但该方法过于笼统,没有针对性的解决明确问题,导致应用性不强。有学者以威胁情报为切入点,提出威胁情报共享方法,实现安全威胁情报共享系统的设计,通过共享重要的第三方情报数据对电网安全的安全态势进行评估及时发现异常行为。该方法应用过程较为简单,但是得到的物联网安全态势评估效果却不够理想,物联网的异常行为检测不彻底,无法得以广泛应用[7]。有学者从网络系统的结构出发,阐述了电子产品编码系统、物理信息融合系统和无线传感器网络系统的运行特点和安全状况,提出了安全挑战和安全防御方法,结合物联网技术的应用与发展,提出了物联网的体系结构,并集成了不同的通用子系统。该方法虽然可以很好的对物联网安全态势进行评估,但是方法过于复杂,应用难度较大[8-9]。D-S 证据理论[10]的基本概率赋值(Basic Probability Assignment,BPA)可对不确定信息实施准确描述以及操作,在智能推理方面具有较高的应用价值。传统 D-S 证据理论的物联网安全态势评估模型采用公式或者专家的经验获取 BPA 值,个人意识较强缺乏科学客观性,致使获取的物联网安全评估结果不理想[11]。

为解决当前物联网安全态势评估存在的问题,提出基于改进 D-S 证据理论的物联网安全态势评估模型,采用 GA-BP 神经物联网训练物联网安全参数指标,输出态势优秀的 BPA,最终获取准确的物联网安全态势评估结果。

1 改进 D-S 证据理论的物联网安全态势评估模型

1.1 基于 D-S 证据理论的物联网安全态势评估模型

1.1.1 D-S 证据理论

设 Θ 表示辨识框架,2^{Θ} 为 Θ 的幂集,如果函数 $m:2^{\Theta}\rightarrow[0,1]$,同时满足 $m(\phi)=0$,$\sum_{A\subseteq\Theta}m(A)=1$,那么 m 就称为 Θ 的基本可信度分配函数,$m(A)$ 为证据对 A 的基本可信度(BPA)。

m_1 和 m_2 为两个证据的基本可信度分配函数,那么 D-S 合成规则为:

$$m(C)=\frac{1}{N}\sum_{A_i\cap B_j=C}m_1(A_i)m_2(B_j) \tag{1}$$

式中,$N=\sum_{A_i\cap B_j=\varnothing}m_1(A_i)m_2(B_j)$。

1.1.2 D-S 证据理论的物联网安全态势评估模型

基于 D-S 证据理论的物联网安全态势评估模型见图 1,其从物联网攻击态势、物联网防御态势、整体安全态势 3 种类型的物联网安全态势进行评估。

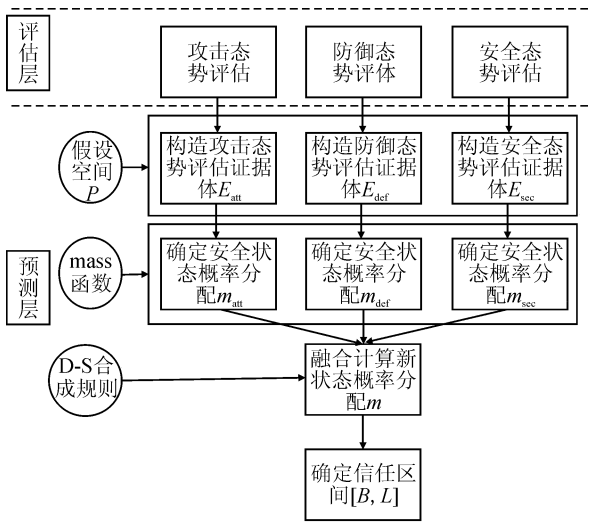

图 1 D-S 证据理论的物联网安全态势评估模型

Fig. 1 Network security situation assessment model of D-S evidence theory

操作步骤如下。

1) $\{A_1,A_2,A_3\}$ 描述辨识框架 Θ 的全部物联网安全态势评估状态,以将来某时段为前提,某段时期中物联网安全、危险和不确定状态分别是 A_1,A_2,A_3。

2) 用 E_{att}、E_{def} 和 E_{sec} 表示辨识框架 Θ 的攻击、防御和整体安全态势评估的 3 类证据体,该种描述基于以往和现在的物联网攻击、防御和整体安全态势的评估结果进行分析。

3) 当 $i=1,2,3$ 时,用 $m_{\text{att}}(A_i)$、$m_{\text{def}}(A_i)$ 和 $m_{\text{sec}}(A_i)$ 描述 BPA,此时的 BPA 是各种现在 3 类证据体的安全状态。

4) 用结合证据体得出不同安全状态时的新 BPA 值 m,此前,要将 3 类证据体通过 D-S 合成规则进行合成。

采用上述方法获取包括攻击态势、防御态势、整体安全态势的各类物联网态势评估结果,但获取的评估结果与实际的物联网安全状况稍有偏差,需研究改进。

1.2　改进 D-S 证据理论的物联网安全态势评估模型

基于 D-S 证据理论物联网安全态势评估结果不理想，与实际物联网安全态势有偏差，主要因为 D-S 证据理论评估过程中采用的 BPA 获取方式缺乏说服力与科学性。基于 D-S 证据理论的物联网安全态势评估模型采用单纯的公式计算或者凭借专家的经验之谈进行判断，由于物联网具有繁琐的物联网结构组成、错综的物联网环境的特性，所以各因素间互相干扰，变化多端，此做法很难对物联网安全态势各方面干扰力做出准确判断。基于改进 D-S 证据理论的物联网安全态势评估模型采用遗传算法改善 BP 神经物联网获取准确、可靠的 BPA 值，排除 BPA 赋值时存在的主观意识性。文章分析的态势状态包括物联网正常态势、物联网异常态势和物联网的未知态势分别用 N 、A 、θ 进行描述，图 2 为改进 D-S 证据理论的物联网安全态势评估模型。

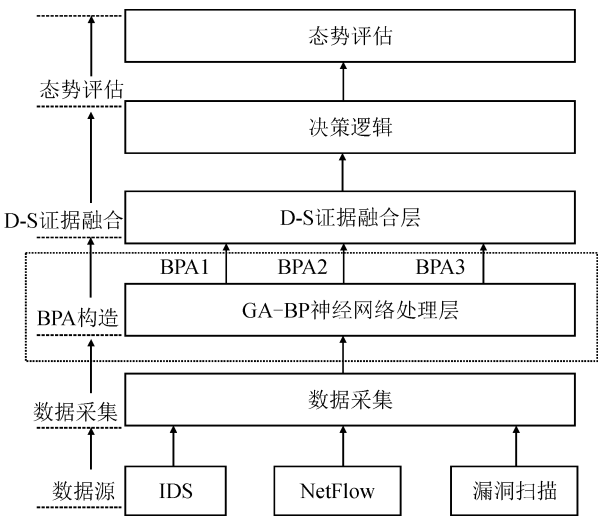

图 2　改进证据理论的物联网安全态势评估模型

Fig. 2　Network security situation assessment model based on improved evidence theory

此模型的操作流程包括数据采集、BPA 构造、D-S 证据融合和态势评估，详细内容如下。

1）从态势信息中采集数据并提炼态势指标后进行统一操作，此态势信息由物联网设备给予。

2）通过遗传算法改进的 BP 神经物联网算法（GA-BP），在 GA-BP 神经物联网操作层训练学习样本集，样本集内是多维度态势指标，最终获取态势 BPA。

3）对新 D-S 证据实施融合过程中，应用 BP 神经物联网获取的态势 BPA 和 Dempster 合成表达式进行循环处理，同时实施态势评估时需要基于决策逻辑分析。

上述基于改进 D-S 证据理论的物联网安全态势评估过程中，对于 BPA 的构造采用遗传算法对 BP 神经物联网实施物联网参数优化操作，提高收敛速度的基础上增加 BPA 评估的准确度。分析 D-S 证据融合时，通常将证据融合过程当成在不同时间点情况下的证据态势 BPA 融合过程。对物联网安全态势进行评估时，将融合过程当成不同时间点情况下的 D-S 证据融合过程，依据时间点的态势 BPA 构成不同的 D-S 证据。不同态势情况同不同的证据命题相关联。详细的融合过程是：面向第 $n-1$ 条证据，向 T_{n-1} 时情况下 BP 神经物联网设置态势 BPA，如果获取第 n 条证据，则融合第 n 条以及第 $n-1$ 条证据获取新证据，通过 Dempste 合成表达式对新证据实施融合，得到最佳态势 BPA，同时基于设置的决策逻辑，基于最佳态势 BPA 的 D-S 证据融合流程，对物联网安全态势实施有效评估，具体的流程用图 3 描述。

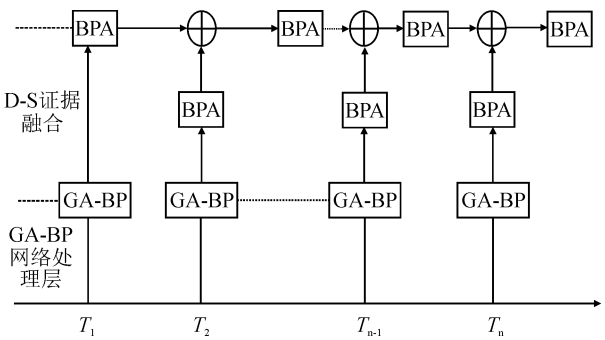

图 3　最佳态势 BPA 的 D-S 证据融合流程

Fig. 3　D-S evidence fusion process in the best situation BPA

图 3 中差异时间点的态势 BPA 实施 Dempster 合成过程用 ⊕ 描述，基于遗传算法优化的 BP 神经物联网算法用 GA-BP 描述。

上述过程经过 BPA 构造、D-S 证据融合进行物联网安全态势评估，有效解决了传统 D-S 证据理论 BPA 赋值缺乏客观科学性的问题，提高了物联网安全态势评估的准确度。

2　实验结果与分析

为验证本文方法在物联网安全态势评估方面精确高、评估效果好，实验采用本文方法对某时段的某物联网安全态势进行评估实验，将本文方法获取的评估结果与真实的评估结果进行对比，使本文方法更具有说服力。真实评估结果的获取条件为：某高校的物联网 2013 年 2 月 13 日 13：00—14：00 时间段的物联网；间隔 5 分钟实施一次物联网评估；从攻击态势、防御态势、整体安全态势三方面进行评估。

获取的真实评估结果用图 4 描述。采用本文方法进行实验的具体环境为:定义低、中、高三个评估值区间(0,1]、(1,2]、(2,3],将待评估的时间段分割成 10 个小时间段,采用本文方法对相同时间段相同地点的物联网安全态势进行评估。获取的物联网安全态势评估结果用表 1 描述,其中,A_1 表示物联网处于安全状态的概率,A_2 表示物联网处于危险状态的概率。

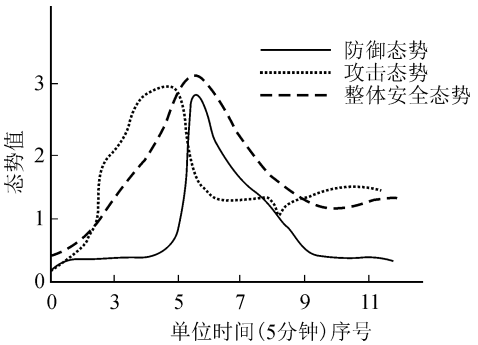

图 4 真实物联网安全态势评估结果

Fig. 4 Real network security situation assessment results

表 1 本文方法在 13:00～14:00 时间段的物联网安全态势评估结果

Tab. 1 Network security situation assessment results by this method from 13:00 to 14:00 time period

时间段	处于各类安全状态的概率(A_1,A_2)
13:10—3:15	(0.902,0.147)
13:15—3:20	(0.650,0.300)
13:20—3:25	(0.568,0.481)
13:25—3:30	(0.283,0.586)
13:30—3:35	(0.089,0.771)
13:35—3:40	(0.293,0.662)
13:40—3:45	(0.504,0.312)
13:45—3:50	(0.902,0.147)
13:50—3:55	(0.834,0.230)
13:55—4:00	(0.652,0.300)

结合图 4 与表 1 进行实验结果分析可知,本文方法在分析上一时间段内的各类物联网安全状态评估结果的基础上,获取一下时间段的物联网态势评估实验结果,实验详细分析三个时间段内两种安全态势评估结果。

1) 在 13:10～13:15 时间段内:本文方法评估的物联网安全状态概率值是 0.902,物联网危险状态概率值是 0.147;真实的物联网安全态势评估结果显示 1.56 是物联网攻击态势值,0.31 是防御态势值,1.01 是整体的物联网安全态势值,说明物联网安全状况良好,本文方法获取的评估结果与真实评估结果相似程度高。

2) 在 13:30～13:35 时间段内:本文方法评估的物联网安全状态概率值是 0.089,物联网危险状态概率值是 0.771;真实的物联网安全态势评估结果显示 1.48 是物联网攻击态势值,2.18 是防御态势值,2.56 是整体的物联网安全态势值,说明物联网安全状况不乐观。本文方法获取的评估结果与真实评估结果基本相似。

3) 在 13:55～14:00 时间段内:本文方法评估的物联网安全状态概率值是 0.652,物联网危险状态概率值是 0.300;真实的物联网安全态势评估结果显示 1.5 是物联网攻击态势值,0.45 是防御态势值,1.55 是整体的物联网安全态势值,说明物联网安全状况乐观。本文方法获取的评估结果与真实评估结果基本吻合。实验结果表明,本文方法获取的物联网安全态势评估结果准确度高。

实验为验证本文方法对于物联网安全态势的评估的有效性和可行性,从 BPA 值对比、态势识别率两方面展开实验分析。实验数据内容为:Kddcup 99 实验数据,实验物联网的态势指标参数。实验具体设置是:100M 局域网,192.168.1.0/24 内网 IP 网段,采用 222.89.32.71C 类网址与 Internet 进行连接;将 Snort2.1.0、NIP2100D 分别安放在 web 服务器、ftp 服务器与 samba 服务器中,物联网安全态势的研究参数的获取是通过存储不同的 IDS 时间到数据中心的方式实现的,实验的源数据则是通过记录路由器 NetFlow 流量信息与 Nessus 漏洞信息的方式获取的。实验采用的测试集是从源数据中提取的训练集,主要包括样本的输入与输出信息,表 2 对部分训练集进行了详细的描述。

表 2 样本的输入与输出

Tab. 2 Input and output of samples

样本编号	样本输入			样本输出		
	X_1	X_2	X_3	N	A	θ
1	240	340 0	9	0.19	0.69	0.09
2	250	350 0	11	0.14	0.74	0.09
3	290	330 0	9	0.29	0.54	0.04
4	170	280 0	8	0.54	0.39	0.04
5	140	260 0	6	0.64	0.29	0.04
6	310	290 0	14	0.24	0.69	0.04
7	190	300 0	5	0.44	0.49	0.04
8	210	330 0	7	0.44	0.49	0.04
9	280	361 0	15	0.09	0.79	0.09
10	320	320 0	14	0.19	0.74	0.04

分析表 2 能够看出，态势指标参数 X_1、X_2、X_3 是样本输入，输出的样本是待评估的态势 N、A、θ，根据这些信息获取本文方法进行物联网安全态势评估时的训练误差变化图，用图 5 描述。

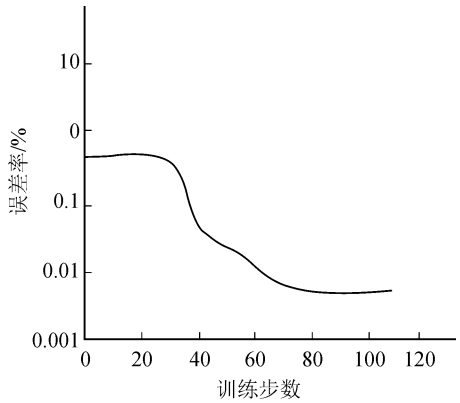

图 5 本文方法物联网安全态势评估误差变化图

Fig. 5 Proposed method network security situation assessment error change diagram

分析图 5 能够看出，训练开始的初期，本文方法的评估误差率仅为 0.07%，随着样本数量的增加，本文方法的评估误差率呈明显下降的趋势，由 0.07%降低到 0.01%左右且趋于稳定，说明本文方法对物联网安全态势的评估误差率较小，性能好。

为使本文方法的有效性和可行性更具有说服力，采用本文方法、K-均值聚类方法、BP 神经物联网方法对实验数据集进行物联网安全态势评估，获取 BPA 评估结果，表 3 对三种方法的性能对比结果进行描述，图 6 对三种方法获取的 BPA 结果进行了描述。

表 3 不同方法的性能对比

Tab. 3 Comparison of performance by different methods

方法	迭代次数/次	均方误差/%
本文方法	104	0.001
K-均值聚类方法	164	0.001 9
BP 神经物联网方法	250	0.004 6

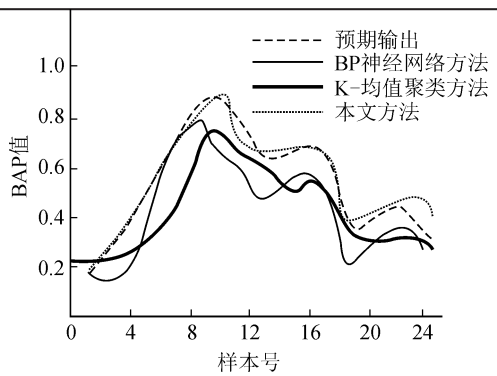

图 6 三种方法的 BPA 值评估结果

Fig. 6 BPA value evaluation results by three methods

分析表 3 可以看出，在完成等量的物联网评估的情况下，本文方法使用的迭代次数最少，均方误差最小，说明本文方法在收敛速度与均方误差方面具有明显的优势，性能较好。

分析图 6 可以看出，三种方法的 BPA 值评估结果曲线走势大致相同，具体看来，采用 K-均值聚类方法与 BP 神经物联网方法获取的 BPA 值位于曲线图的下方，明显低于预期输出结果；本文方法获取的 BPA 值位于曲线图的上方，最高达 0.89，超过其余两种方法，且与预期输出曲线走势基本吻合。实验结果表明，本文方法的物联网安全态势评估精度高、评估效果好。

在实验态势指标参数的基础上，在时间 $T(T_1 \sim T_{10})$ 内，采用本文方法分别输出态势状态 N、A、θ 的 BPA 值，获取的结果用表 4 描述。

表 4 时间态势 BPA

Tab. 4 Time situation BPA

编号	N	A	θ
T_1	0.145 4	0.523 3	0.308
T_2	0.028 7	0.828 3	0.120 9
T_3	0.062 7	0.755 1	0.16
T_4	0.019 9	0.819 9	0.15
T_5	0.013 3	0.83	0.134 4
T_6	0.070 2	0.831	0.082 5
T_7	0.034 5	0.831	0.148 7
T_8	0.030 6	0.807 1	0.15
T_9	0.062 2	0.840 9	0.084 5
T_{10}	0.073 4	0.801	0.102 4

基于 D-S 证据融合与物联网安全态势评估过程，实验采用 Dempster 公式融合本文方法输出的物联网安全态势 BPA，本次融合依照时间顺序合理实施，获取的关于时间点的融合态势 BPA 用表 5 描述。

表 5 关于时间点的融合态势 BPA

Tab. 5 Fusion situation of time points BPA

T	N	A	θ
m_1	0.145 4	0.523 3	0.308 1
$m_1 \oplus m_2$	0.033 1	0.766	0.176 6
$m_1 \oplus m_2 \oplus m_3$	0.070 1	0.81	0.101 6
$m_1 \oplus m_2 \oplus m_3 \oplus m_4$	0.015 4	0.876 8	0.097 4
$m_1 \oplus m_2 \oplus m_3 \oplus m_4 \oplus m_5 \cdots$	0.003	0.946 7	0.040 9

分析表 5 能够看出,在融合的过程中,随着时间的推进,本文方法获取的未知态势值由 0.308 1 持续降低至 0.040 9,同时异常态势值由 0.523 3 持续升高至 0.946 7。实验引入决策逻辑最大 Bel 方法对实验结果进行状态判断,根据表 5 提供的数值显示此物联网处于异常状态。经过数次的融合使得采用本文方法获取的数据呈现峰值,并且具有容易区分的优点,便于对物联网安全态势进行评估。实验结果表明,本文方法能够准确评估物联网安全态势,获取结果的不确定因素几乎为 0,具有较高的物联网安全态势评估性能。

为验证本文方法对于物联网安全态势的评估的有效性,根据态势指标标准,以渗透攻击的方式对局域网展开模拟实验,最终实现对模拟物联网安全态势的识别与评估。定义该次实验时间是一小时,在这一时间段内获取的物联网态势数据的基础上进行实验,同时采用本文方法与 D-S 证据理论方法进行对比分析,两者获取的物联网安全态势识别制成曲线图,用图 7 描述。

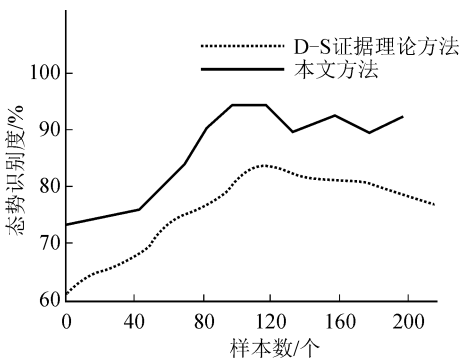

图 7 2 种方法的态势识别率对比

Fig. 7 Situation recognition rate by two methods

分析图 7 能够看出,采用本文方法获取的物联网安全态势识别率总体位于 D-S 证据理论方法获取态势识别率的上方;本文方法获取的最低物联网安全态势识别率在 70% 以上,最高识别率达到 95%,且后期稳定在 90% 左右;D-S 证据理论方法获取的最低物联网安全态势识别率为 62%,最高识别率仅为 83%,持续时间较短后期呈下降趋势。实验结果表明,本文方法比未改进的 D-S 证据理论方法具有更强的物联网安全态势评估性能,评估精度高、识别效果好。

3 结 语

提出了改进 D-S 证据理论物联网安全态势评估模型,在解决 D-S 证据理论 BPA 赋值存在主观片面性问题的基础上,科学地融合物联网安全态势信息,准确获取物联网安全态势评估结果,具有精确度高、误差小的优势。为互联网环境有效评估提供了科学的手段,一定程度上促进了物联网环境的良好运转。

参考文献:

[1] 武传坤. 物联网安全关键技术与挑战[J]. 密码学报, 2015,2(1):40-53.
WU Chuankun. An overview on the security techniques and challenges of the Internet of Things[J]. Journal of Cryptologic Research, 2015, 2(1): 40-53.

[2] 李俊霖, 周华, 夏金虎,等. 物联网安全协议攻击者模型形式化构建研究[J]. 云南大学学报(自然科学版), 2013, 35(增刊 2):147-151.
LI Junlin, ZHOU Hua, XIA Jinhu, et al. Research of formal establish security protocol attacker model in communicating sequential processes[J]. Journal of Yunnan University(Natural Sciences Edition), 2013, 35(S2): 147-151

[3] 赵健,王瑞,李正民,等. 物联网系统安全威胁和风险评估[J]. 北京邮电大学学报, 2017, 40(增刊 1):135-139.
ZHAO Jian, WANG Rui, LI Zhengmin, et al. Security threats and risk assessment of IOT system[J]. Journal of Beijing University of Posts and Telecommunications, 2017, 40(S1):135-139.

[4] 姚琛. 参数联合优化的物联网安全分析与研究[J]. 内蒙古师范大学学报(自然科学汉文版), 2016,45(5): 664-666.
YAO Chen. Analysis and research on the security of the Internet of Things[J]. Journal of Inner Mongolia Normal University(Natural Science Edition) , 2016,45(5): 664-666.

[5] 雷璟. 物联网安全测评和风险评估技术研究[J]. 电讯技术,2013,53(3):323-328.
LEI Jing. Research on security evaluation and risk assessment for Internet of Things[J]. Telecommunication Engineering, 2013, 53(3): 323-328.

[6] 李若瑜,周亦鹏,方德英,等. 物联网信息安全风险评估研究[J]. 物联网技术, 2018,8(3):32-34.
LI Ruoyu, ZHOU Yipeng, FANG Deying, et al. Research on information security risk assessment of Internet of Things [J]. Internet of Things Technologies, 2018, 8(3): 32-34.

[7] 边金良. 数据挖掘技术在物联网安全中的应用研究[J]. 物流技术, 2013, 32(7): 439-441.
Bian Jinliang. Study on application of data mining technology in IOT safety[J]. Logistics Technology, 2013, 32(7): 439-441.

[8] 高洪波. 灰色关联算法在物联网安全状态评估中的应用[J]. 制造业自动化, 2012, 34(22): 23-25.
GAO Hongbo. Study of the application for the security state assessment about the Internet of Things based on grey correlation algorithm[J]. Manufacturing Automation, 2012, 34(22): 23-25.

[9] 朱景锋. 基于三角模糊 AHP 的物联网电子政务安全评价模型分析[J]. 制造业自动化,2012,34(7):90-92.
ZHU Jingfeng. Network security of e-government evaluation model analysis based on the triangular fuzzy AHP[J]. Manufacturing Automation, 2012, 34(7): 90-92.

[10] 赵秋月,左万利,田中生,等. 一种基于改进 D-S 证据理论的信任关系强度评估方法研究[J]. 计算机学报, 2014,37(4):873-883.
ZHAO Qiuyue, ZUO Wanli, TIAN Zhongsheng, et al. A method for assessment of trust relationship strength based on the improved D-S evidence theory [J]. Chinese Journal of Computers, 2014, 37(4): 873-883.

[11] 张琳,刘婧文,王汝传,等. 基于改进 D-S 证据理论的信任评估模型[J]. 通信学报, 2013,34(7):167-173.
ZHANG Lin, LIU Jingwen, WANG Ruchuan, et al. [J]. Trust evaluation model based on improved D-S evidence theory[J]. Journal on Communications, 2013, 34(7):167-173.

(责任编辑 王绪迪)

(上接第 459 页)

[4] GEUSEBROEK J M, VAN DEN BOOMGAARD R, SMEULDERS A W M, et al. Color invariance [J]. IEEE Transactions on Pattern Analysis and Machine Intelligence, 2011, 23(12): 1338-1350.

[5] ZHANG Lin, GU Zhongyi, LI Hongyu. SDSP: a novel saliency detection method by combining simple priors [C] // 2013 IEEE International Conference on Image Processing, IEEE, 2013: 171-175.

[6] NAFCHI H Z, SHAHKOLAEI A, HEDJAM R, et al. Mean deviation similarity index: efficient and reliable full-reference image quality evaluator [J]. IEEE Access, 2016, 4: 5579-5590.

[7] PONOMARENKO N, IEREMEIEV O, LUKIN V, et al. Color image database TID2013: peculiarities and preliminary results [C]// European Workshop on Visual Information Processing, IEEE, 2013: 106-111.

[8] PONOMARENKO N, LUKIN V, ZELENSKY A, et al. TID2008-A database for evaluation of full-reference visual quality assessment metrics [J]. Adv Modern Radioelectron, 2009, 10: 30-45.

[9] SHEIKH H R, SABIR M F, BOVIK A C. A statistical evaluatuion of recent full reference image quality assessment algorithms [J]. IEEE Transactions on Image Processing, 2006, 15(11): 3440-3451.

[10] ZHANG Lin, SHEN Ying, LI Hongyu. VSI: a visual saliency-induced index for perceptual image quality assessment [J]. IEEE Transactions on Image Processing, 2014, 23(10): 4270-4281.

[11] ZHANG Lin, ZHANG Lei, MOU Xuanqin, et al. FSIM: A feature similarity index for image quality assessment [J]. IEEE Transactions on Image Processing, 2011, 20(8): 2378-2386.

[12] LIU Anmin, LIN Weisi, NARWARIA M. Image quality assessment based on gradient similarity [J]. IEEE Transactions on Image Processing, 2012, 21(4): 1500-1512.

[13] LARSON E C, CHANDLER D M. Most apparent distortion: full-reference image quality assessment and the role of strategy [J]. Journal of Electronic Imaging, 2010, 19(1): 011006.

[14] CHANG Huawen, YANG Hua, GAN Yong, et al. Sparse feature fidelity for perceptual image quality assessment [J]. IEEE Transactions on Image Processing, 2013, 22(10): 4007-4018.

(责任编辑 王绪迪)