

基于证据理论物联网安全态势感知方法研究

李剑¹, 董廷鲁¹, 李劫²

(1. 北京邮电大学人工智能学院, 北京 100876; 2. 北京邮电大学计算机学院(国家示范性软件学院), 北京 100876)

摘要: 社会物联网技术迅速发展, 安全问题日益严重, 对简便易用的物联网安全态势感知方法进行了研究。针对当前物联网安全态势感知系统缺乏通用性、过分依赖专家知识的缺点, 提出了一种基于改进D-S证据理论的物联网安全态势感知方法。利用模糊高斯隶属函数计算漏洞信息隶属度矩阵, 归一化后作为证据分布矩阵; 利用改进Topsis方法衡量证据可信度, 聚合两两证据间的局部可信度, 根据态势评估场景改进期望正负解向量, 充分抑制冲突性证据可信度, 提高相互支持证据间可信度, 利用加权平均方法进行漏洞信息融合得到态势评估结果; 基于时间因子折扣和高危漏洞比例折扣证据理论融合形成态势感知结果, 利用时间因子聚合多个态势评估数据, 根据时间尺度对不同时时刻的态势评估证据进行折扣, 越接近当前时刻的证据折扣度越小, 反之越大。同时, 综合考虑不同时刻物联网漏洞信息, 利用高危漏洞比例信息进行自适应动态加权, 把不同时刻的高危信息折扣入识别框架, 系统的危险变化信息集中体现在证据融合过程中。经过实验表明, 在不同数量证据体融合和4种常见冲突证据融合中, 改进Topsis方法对可信命题的融合概率更高; 在态势评估方面, 准确评估当前系统危险程度; 在态势感知方面, 折扣理论可以充分预测高风险和紧急风险概率, 比传统D-S证据理论更加有效。根据所提理论设计了一种物联网安全态势感知方法流程用于指导工程实践, 未来在漏洞信息利用方面, 可以考虑漏洞间的关联关系, 提炼漏洞间更丰富的态势信息, 使态势评估的结果更加准确合理, 也可以借鉴博弈论的思想在攻击者、防御者动态博弈过程中进行态势感知。

关键词: D-S证据理论; 态势感知; 物联网安全; 时间演化; 通用漏洞评分系统

中图分类号: TP393

文献标志码: A

DOI: 10.11959/j.issn.2096-109x.2022022

Research on IoT security situation awareness method based on evidence theory

LI Jian¹, DONG Tinglu¹, LI Jie²

1. School of Artificial Intelligence, Beijing University of Posts and Telecommunications, Beijing 100876, China

2. School of Computer Science(National Pilot Software Engineering School), Beijing University of Posts and Telecommunications, Beijing 100876, China

Abstract: The security problem of IoT became more and more serious with its rapid development. Considering that

收稿日期: 2021-11-22; 修回日期: 2022-01-08

通信作者: 董廷鲁, tinglu@bupt.edu.cn

基金项目: 国家自然科学基金(61472048)

Foundation Item: The National Natural Science Foundation of China (61472048)

引用格式: 李剑, 董廷鲁, 李劫. 基于证据理论物联网安全态势感知方法研究[J]. 网络与信息安全学报, 2022, 8(2): 39-47.

Citation Format: LI J, DONG T L, LI J. Research on IoT security situation awareness method based on evidence theory[J]. Chinese Journal of Network and Information Security, 2022, 8(2): 39-47.

the current IoT security situation awareness system lacks generality and excessively relies on expert knowledge, a IoT security situation awareness method based on improved D-S evidence theory was proposed in this paper. Fuzzy Gaussian membership function was used to calculate the vulnerability information membership matrix, which was normalized as evidence distribution matrix. The improved Topsis method was used to measure the evidence credibility. In order to fully restrain the credibility of conflicting evidence and improve the credibility of mutually supporting evidence, local credibility between two evidence was aggregated and the expected positive and negative solution vectors were improved according to the situation assessment scenario. And the weighted average method was used for vulnerability information fusion, to obtain the result of situational assessment. The result of situational awareness was fused with the time discount and high-risk vulnerability information discount evidence theory. At the same time, the IoT vulnerability information at different moments was considered comprehensively, the evidence was adaptively and dynamically weighted with the ratio information of high-risk vulnerability. The experimental results show that in the fusion of different numbers of evidence bodies and four common conflicting evidence, the improved Topsis method has higher fusion probability on credible proposition. In the aspect of situation assessment, the risk degree of current system is accurately assessed. And in the aspect of situational awareness, this discount evidence theory can predict the probability of high risk and critical risk, which is more effective than the traditional D-S evidence theory. According to this theory, a IoT security situational awareness method process was proposed, which would be used to guide engineering practice. In the future, the relationship between vulnerabilities can be considered and richer information between vulnerabilities can be extracted for vulnerability exploiting, so that the result of situation assessment is more accurate and reasonable. On the other hand, for situational awareness, game theory can be adopted in the process of dynamic game between the attacker and defender.

Keywords: D-S evidence theory, situation awareness, IoT security, time evolution, CVSS

0 引言

随着智能化时代到来,物联网系统快速发展,各种基于物联网技术的应用日渐成熟。物联网是传统互联网在“物”上的延伸,“万物互联”是物联网美好愿景。物联网在快速构建人与物交互场景的同时,产生了很多安全问题。在复杂网络环境下,物联网系统拥有数量庞大的设备固件程序,稍有不慎,就会被黑客利用,给社会带来巨大的损失^[1]。日益严峻的物联网安全问题使人们不得不重视对物联网安全态势感知工作的研究。态势感知工作主要包括态势要素提取、设备扫描工作、安全性分析工作、态势评估和态势感知^[2]。一般地,需要对物联网系统进行全面统一的安全数据整合工作,形成统一监测、集中分析、集中呈现的态势感知系统^[3]。传统的信息安全风险研究工作只是一种静态的评估防护工作^[4],态势感知系统利用时间演化,以期在动态的过程中进行安全防护工作。

在传统信息安全风险评估领域,采用定性

和定量结合方法进行综合评价的方案占据主流地位^[5-6]。定性分析方法主要有德尔菲法,凭借专家群体的知识和经验给出综合评价,缺点是主观性太强;定量分析方法主要包括故障树分析法和贝叶斯网络分析法,强调特定场景下客观规律的重要性,但是不适合于复杂场景;定性和定量结合分析方法主要有层次分析法和模糊层次分析法,主观性和客观性有机结合,扩展性较好,但是判断矩阵仍然是根据专家意见确定的。除此之外,D-S 证据理论也被广泛应用于信息安全风险评估,用来融合多个风险证据^[7]。一般地,D-S 证据理论和层次分析法或者模糊层次分析法进行联合使用,层次分析法建立关于特定场景下信息安全风险评估的评价指标集合,在确定层级因素权重时使用 D-S 证据进行多特征融合,使参数的权重分布更加客观合理。不过在传统 D-S 证据理论下证据冲突时融合结果与常理不一致,很多专家学者基于此问题对 D-S 证据理论进行改进,使之适应更加复杂的证据合成场景。

态势感知方法主要利用证据网络模型^[8]、马

尔可夫模型^[9]、神经网络模型^[10-11]、贝叶斯网络模型^[12]，但是这些模型结构复杂，训练难度高，在真实场景下容易出现参数爆炸的情况。

针对上述问题，本文着重研究 D-S 证据理论在物联网安全态势感知模型中的应用。

1) 在态势评估方面，本文利用改进 Topsis 方法衡量证据可信度，降低了冲突证据的可信度，保持了相互支持证据的可信度，经过实验证明，在不同数量证据体和常见冲突证据方面，融合之后对正确命题基本概率分配更高。

2) 在态势感知方面，本文提出了一种基于时间折扣和高风险漏洞比例折扣 D-S 证据理论，通过融合多个时刻的态势评估数据得到了良好的态势感知结果。

1 D-S 证据理论

1.1 传统 D-S 证据理论

在传统 D-S 证据理论中，定义标准变量的识别框架 $\theta = \{\theta_1, \theta_2, \dots, \theta_n\}$ ，属于幂集 2^θ 的元素 A 是关于变量 θ 取值的命题，或称焦元。关于命题 A 的函数被定义成概率分配函数 BPA，一般称为 mass 函数，简称 m 函数。

$$m(\emptyset) = 0, \sum_{A \subseteq \theta} m(A) = 1 \quad (1)$$

信任函数，被定义为命题子集的概率分配和，表示对命题为真的信任程度。

$$\text{Bel}(A) = \sum_{B \subseteq A} m(B), \forall A \subseteq \theta \quad (2)$$

似然函数，被定义为与命题交集为空的集合概率分配和，表示对命题为非假的信任程度。

$$\begin{aligned} \text{Pl}(A) &= 1 - \text{Bel}(\neg A) = \\ 1 - \sum_{B \subseteq \neg A} m(B) &= \sum_{B \cap A = \emptyset} m(B), \forall A \subseteq \theta \end{aligned} \quad (3)$$

信任函数定义了命题为真的信任下界，似然函数定义了命题为非假的信任上界，通过区间的方式描述不确定性。因为 $\{\neg A, A\} \subseteq \theta$ ， $\text{Pl}(A) \geq \text{Bel}(A)$ 。实际上， $[\text{Bel}(A), \text{Pl}(A)]$ 表示命题 A 的不确定区间， $[0, \text{Bel}(A)]$ 表示对命题 A 支持的证据区间， $[0, \text{Pl}(A)]$ 表示对命题 A 的拟信证据区间， $[\text{Pl}(A), 1]$ 表示对命题 A 的拒绝证据区间。

当有 n 个证据 $m_1, m_2, m_3, \dots, m_n$ 需要融合时，合成规则为

$$\begin{aligned} m(A) &= (m_1 \oplus m_2 \oplus \dots \oplus m_n).A = \\ \frac{1}{1-K} \sum_{\bigcap_{i=1}^n A_i = A} \prod_{i=1}^n m_i(A_i) \end{aligned} \quad (4)$$

其中， K 被称为冲突因子，算符 $\oplus$ 被称为融合算子。

$$\begin{aligned} K &= \sum_{\bigcap_{i=1}^n A_i = \emptyset} m_1(A_1)m_2(A_2)\dots m_n(A_n) = \\ \sum_{\bigcap_{i=1}^n A_i = \emptyset} \prod_{i=1}^n m_i(A_i) &= 1 - \sum_{\bigcap_{i=1}^n A_i \neq \emptyset} \prod_{i=1}^n m_i(A_i) \end{aligned} \quad (5)$$

传统 D-S 证据理论在融合算子上满足交换律和结合律。交换律为 $m_1 \oplus m_2 = m_2 \oplus m_1$ ，结合律为 $m_1 \oplus (m_2 \oplus m_3) = (m_1 \oplus m_2) \oplus m_3$ 。

传统 D-S 证据理论在合成规则上，采用乘积项的方式进行融合，然后归一化得到最终的融合结果，当证据对命题的基本概率分配为 0 时，经过证据融合后的结果仍然是 0，即使其他证据都以大概率确认该命题。除了“0 置信冲突”，传统 D-S 证据理论还有“1 置信冲突”“完全冲突”“高冲突”等特殊情况，在这 4 种悖论情况下，传统的证据合成规则不再适用^[13]。

对传统的 D-S 证据理论改进主要体现在两个方向，改进合成规则或者改进证据分布^[13]。改进证据的合成规则，认为引起 4 种悖论问题的根源在于证据合成规则不完善，改进的方案中大多在原有乘积项的基础上进行加权和改进。改进证据分布，认为合成规则普遍适用，证据分布不合理才是产生 4 种悖论的问题所在，对证据间的冲突性充分衡量，并把证据间的冲突性转移。

1.2 基于改进 Topsis 方法证据可信度量

Topsis 方法一般用在多目标的综合评价场景中^[14]，基于评价目标在评价指标中与期望正负解的距离确定最优目标方案。一般地，期望正解是每一个评价指标中最大值组成的向量，期望负解是每一个评价指标中最小值组成的向量，在评估之前往往需要对初始数据进行标准化正向化处理。

假设有 n 个评价目标、 m 个评价指标， z_{ij} 表

示评价目标 i 在评价指标 j 下的得分, 由于不同的评价指标有不同的量纲, 因此避免“大数吃小数”的情况, 需要进行标准化处理, 如下。

$$\widetilde{z}_{ij} = \frac{z_{ij}}{\sqrt{\sum_{i=1}^n z_{ij}^2}}, i=1, 2, \dots, n, j=1, 2, \dots, m \quad (6)$$

定义期望正解为各评价指标中最大值组成的向量如下。

$$\mathbf{Z}^+ = [z_1^+, z_2^+, \dots, z_m^+] = [\max(\widetilde{z}_{11}, \widetilde{z}_{21}, \dots, \widetilde{z}_{n1}), \dots, \max(\widetilde{z}_{1m}, \widetilde{z}_{2m}, \dots, \widetilde{z}_{nm})] \quad (7)$$

定义期望负解为各评价指标中最小值组成的向量如下。

$$\mathbf{Z}^- = [z_1^-, z_2^-, \dots, z_m^-] = [\min(\widetilde{z}_{11}, \widetilde{z}_{21}, \dots, \widetilde{z}_{n1}), \dots, \min(\widetilde{z}_{1m}, \widetilde{z}_{2m}, \dots, \widetilde{z}_{nm})] \quad (8)$$

定义评价目标 i 到期望正解的距离为

$$D_i^+ = \sqrt{\sum_{j=1}^m (\widetilde{z}_{ij} - z_j^+)^2} \quad (9)$$

定义评价目标 i 到期望负解的距离为

$$D_i^- = \sqrt{\sum_{j=1}^m (\widetilde{z}_{ij} - z_j^-)^2} \quad (10)$$

定义评价目标 i 未归一化得分为

$$S_i^+ = \frac{D_i^-}{D_i^+ + D_i^-} \quad (11)$$

Topsis 方法通过计算评价目标与正解的相对贴近程度衡量目标间优劣, 如果与正解的距离越近, 说明评价目标在评价指标上的分布与正解越相似, 评价目标在评价指标上的数值与最大值接近程度越高, 甚至等于最大值。

在本场景下, 需要充分评估证据间可信度, 降低冲突证据的可信度, 提高相互支持证据的可信度。经过分析发现, 冲突证据命题间的差距较大, 分布不均衡, 往往某个单一命题上的基本概率分配接近于 1, 而其他命题的基本概率分配为 0, 因此在评估证据的冲突性时, 证据与最大值向量距离越近, 判定为冲突证据的可能性越高, 可信度评分越低, 本文采用式(12)衡量证据间的可信度。

$$S_i^- = \frac{D_i^+}{D_i^+ + D_i^-} \quad (12)$$

本场景下, 先计算两两证据间的可信支持度, 然后求和确定证据整体间的支持度, 并把归一化后的求和结果作为证据的最终可信度衡量依据。

证据体可信支持度矩阵为

$$\mathbf{S}^- = \begin{bmatrix} s_{11}^- & s_{12}^- & \dots & s_{1n}^- \\ s_{21}^- & s_{22}^- & \dots & s_{2n}^- \\ \vdots & \vdots & \ddots & \vdots \\ s_{n1}^- & s_{n2}^- & \dots & s_{nn}^- \end{bmatrix} \quad (13)$$

$$s_{ij}^- = \begin{cases} 0, & i = j \\ 1, & i \neq j, m_i = m_j \\ \frac{D_i^{j+}}{D_i^{j+} + D_i^{j-}}, & i \neq j, m_i \neq m_j \end{cases} \quad (14)$$

其中, 在基于证据体 m_i 和 m_j 评估时, D_i^{j-} 表示证据体 m_i 与期望负解的距离; D_i^{j+} 表示证据体 m_i 与期望正解的距离; s_{ij}^- 表示证据体 m_j 对证据体 m_i 的支持程度。

定义 m_i 证据体获得的支持度为 $\text{Sup}(m_i)$ 。

$$\text{Sup}(m_i) = \sum_{j=1}^n s_{ij}^- \quad (15)$$

归一化之后得到证据间的可信度量为

$$\text{Be}(m_i) = \frac{\text{Sup}(m_i)}{\sum_{j=1}^n \text{Sup}(m_j)}, \sum_{i=1}^n \text{Be}(m_i) = 1 \quad (16)$$

不同数量证据体经过融合后的结果如表 1 所示粗体数据表示融合后对正确命题的基本概率分配。文献[15]提出的方法用 Jousselme 公式衡量证据间的距离确定证据间可信度计算公式, 利用可信度对证据分布进行加权得到加权平均证据, 然后进行迭代融合, 根据表 1 结果可知, 本文方法对正确命题的指认与文献[15]一致, 符合预期, 且本文方法对正确命题的融合结果高于文献[15]方法。

4 种常见证据冲突融合结果如表 2 所示, 粗体数据表示融合后对正确命题的基本概率分配。针对前面提到的 4 种悖论情况, 比较符合常理的正确命题为 {AACA}, 可以看出两种方法指认结果与常理相符, 本文方法对正确命题指认概率高于文献[15]方法, 指认效果明显。

1.3 基于动态折扣率的 D-S 证据理论

在改进证据分布的研究方法中,有一种折扣理论,引入折扣度对原始证据分布进行折扣,通常冲突性高的证据折扣度大,通过折扣的方式把证据间的冲突性分配给不确定度。

$$W = \{w_1, w_2, \dots, w_n\}, \sum_{i=1}^n w_i = 1 \quad (17)$$

$$m'_i(A) = \begin{cases} w_i m_i(A), & A \neq \theta \\ w_i m_i(\theta) + 1 - w_i, & A = \theta \end{cases} \quad (18)$$

W 为一个标准化的证据折扣集合,可以根据专家意见得出,也可以基于证据分布矩阵客观性地计算得到。上述折扣理论是一种静态折扣理论,没有考虑证据在时间上的演化,融合的结果仍然是静态性的。

表 1 不同数量证据体融合结果

Table 1 Fusion result of different numbers of evidence

方法	命题	m_1, m_2	m_1, m_2, m_3	m_1, m_2, m_3, m_4	m_1, m_2, m_3, m_4, m_5
文献[15]	A	0.154 3	0.581 6	0.806 0	0.890 9
	B	0.746 9	0.243 9	0.048 2	0.008 6
	C	0.098 8	0.174 5	0.145 8	0.100 5
本文方法	A	0.040 8	0.631 5	0.878 5	0.934 0
	B	0.943 4	0.259 9	0.028 7	0.003 8
	C	0.015 8	0.108 6	0.092 8	0.062 2

表 2 4 种常见证据冲突融合结果

Table 2 Fusion result of four conflicted evidence

冲突类型	方法	命题				
		A	B	C	D	E
完全冲突	文献[15]	0.816 6	0.116 4	0.067 0	—	—
	本文方法	0.980 0	0.019 0	0.001 0	—	—
0 置信冲突	文献[15]	0.431 8	0.295 5	0.272 7	—	—
	本文方法	0.614 9	0.188 3	0.196 8	—	—
1 置信冲突	文献[15]	0.138 8	0.131 8	0.729 4	—	—
	本文方法	0.016 8	0.010 1	0.973 1	—	—
高冲突	文献[15]	0.532 4	0.152 1	0.146 2	0.045 1	0.124 1
	本文方法	0.974 4	0.008 4	0.008 4	0.000 4	0.008 4

本文着重研究物联网安全态势演化过程,利用多个时刻的静态态势评估数据进行动态的态势感知。经过分析发现,多个时刻的证据在时间演

化过程中有不同的作用,距离当前时刻越久的证据对感知结果的支持度越低,折扣性越强;距离当前时刻越近的证据对感知结果的支持度越高,折扣性越弱^[7]。假设目前有 k 个时刻的证据, $m_1, m_2, m_3, \dots, m_k$, 融合后的感知结果为 $R_k(m_1, m_2, m_3, \dots, m_k)$, 证据间融合的过程如下。

$$\begin{aligned} R_2(m_1, m_2) &= M(m_1^{w(t_2-t_1)}, m_2) \\ R_3(m_1, m_2, m_3) &= M(R_2(m_1, m_2)^{w(t_3-t_2)}, m_3) \\ &\dots \\ R_k(m_1, \dots, m_k) &= \\ &M(R_{k-1}(m_1, m_2, \dots, m_{k-1})^{w(t_k-t_{k-1})}, m_k) \end{aligned} \quad (19)$$

M 表示两个证据间的融合函数, $W(t)$ 表示在时间尺度上的折扣率。传统 D-S 证据理论在多证据融合时具有交换性,考虑到时间的演化过程,有下式成立。

$$M(m_1^{w(t_3-t_2)w(t_2-t_1)}, m_3) = M(m_1^{w(t_3-t_1)}, m_3) \quad (20)$$

因此,可以选择特征函数 $w(t) = e^{-\alpha t}, \alpha \geq 0$, 该函数在时间上是一个递减函数。

本文不仅考虑时间折扣的作用,还考虑前一个时刻漏洞危险程度对将来感知结果的影响,如果某个时刻检测出的高风险和紧急风险漏洞数量较多,说明当时系统整体的安保措施有极大的漏洞,对将来态势感知的影响较大,折扣度较高,把这种高危影响保留到不确定度中,因此,最终的折扣因子是时间折扣与当时高风险漏洞比例折扣的综合结果。在 m_k 融合 $R_{k-1}(m_1, m_2, m_3, \dots, m_{k-1})$ 时,保留原始乘法合成规则基础上,综合考虑命题间的平均证据支持,引入加权平均证据,使证据的融合结果更加全面。

$$\begin{aligned} m(A) &= (m_1 \oplus m_2)A = \\ &\sum_{A_1 \cap A_2 = A} m_1(A_1)m_2(A_2) + K \sum_{i=1}^2 \text{Be}(m_i)m_i(A_i) \end{aligned} \quad (21)$$

其中, $\text{Be}(m_i)$ 为证据可信度, K 是冲突因子。

2 物联网安全态势感知模型

2.1 物联网安全态势感知方法流程

物联网安全态势感知方法流程如图 1 所示。首先根据固件安全性分析结果确定漏洞,利用通用漏洞评分系统获得漏洞评分;其次利用高斯隶

属函数确定隶属矩阵，归一化隶属度矩阵为证据分布矩阵；然后利用改进 Topsis 方法确定新的证据分布，进行静态态势评估；最后利用多个时刻的态势评估结果，基于动态折扣率 D-S 证据理论得到态势感知结果，指导安全人员进行后期防护工作。

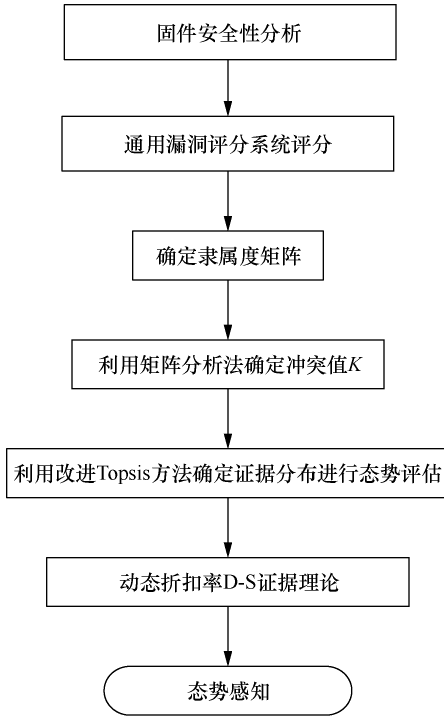


图 1 物联网安全态势感知方法流程

Figure 1 Process of IoT security situational awareness method

2.2 确定隶属度矩阵

在本文设计的物联网安全态势感知模型中，设识别框架（评语集） θ 为{无风险 N，低风险 L，中风险 M，高风险 H，紧急风险 C}，利用高斯隶属函数基于 CVSS 评分得到处于识别框架中每一个风险评语的隶属度，归一化隶属度矩阵并作为 D-S 证据理论的 BPA 分布。高斯隶属度函数

$$y = e^{-\frac{(x-\mu)^2}{2\delta^2}} \quad (22)$$

其中， x 为输入，在本文方案中为漏洞的 CVSS 得分， μ 是函数的中心， δ 表示宽度，利用模糊数学的方法提高 CVSS 在单漏洞评估方面的泛化能力，在多漏洞信息融合上 D-S 证据理论可以得到更加客观的评估结果。参照 CVSS，定义 5 个评语的隶属度中心为 1.0、2.0、5.5、8.0、9.5。

在传统风险评估领域中， δ 设置比较主观，一般地，由专家给出评价值 x ，并同时给出该评价不确定度的衡量范围，缺乏一定的说服力，并且在很多模糊综合评价方法中，对评语集的考虑总是认为评语间互不影响，互不相容，相互独立，并没有考虑到评语间的递进关系。在语义上，这 5 个评语表征了漏洞在危险程度上不断增强，位于较高风险的漏洞默认有较低风险的语义基础和评分基础，在计算高风险漏洞时不能只刻意提高对应风险的隶属度，抑制其他风险的隶属度，而应该综合考虑，体现高风险漏洞对低风险评语的隶属度增强而不是降低，同时保证较低风险的漏洞在较高风险评语处的隶属度仍然较低。为了刻画这种增强关系，本文尝试使用 δ 描述关联性， δ 越大高斯函数曲线越低宽，较高风险漏洞在计算属于较低风险评语的隶属度会增强， δ 越小高斯函数曲线越高窄，较低风险漏洞在计算属于较高风险评语的隶属度会降低，结合 CVSS 漏洞评级划分区间，5 个评语的隶属度函数为

$$y = e^{-\frac{(x-1.0)^2}{2 \times 10^2}} \quad (23)$$

$$y = e^{-\frac{(x-2.0)^2}{2 \times 6^2}} \quad (24)$$

$$y = e^{-\frac{(x-5.5)^2}{2 \times 5^2}} \quad (25)$$

$$y = e^{-\frac{(x-8.0)^2}{2 \times 4^2}} \quad (26)$$

$$y = e^{-\frac{(x-9.5)^2}{2 \times 3^2}} \quad (27)$$

经过物联网固件安全性模块分析之后得到系统中的安全性测试报告，定位系统中的安全性问题，利用 CVSS 计算每一项安全性问题得分，通过隶属度函数计算隶属度矩阵，并将归一化的隶属度矩阵作为 D-S 证据理论的 BPA 分布。

$$\forall v \in V, \sum_{\theta_i \in \theta} m_v(\theta_i) = 1, V = \{v_1, v_2, \dots, v_n\} \quad (28)$$

其中， V 表示发现的漏洞集合， $m_v(\theta_i)$ 表示漏洞 v 在评语 θ_i 上的基本概率分配。

2.3 利用矩阵分析法确定冲突值 K

假设有 n 个证据， $\bar{m}$ 个命题，在传统方法求冲突值 K 时所需要的时间复杂度为 $O(\bar{m}^n)$ ，利用矩阵

分析法求冲突值 K 所需要的时间复杂度为 $O(nm^2)$ ，时间复杂度由原来指数级降为多项式级^[16]。

假设证据体分布为

$$\mathbf{M} = \begin{bmatrix} \mathbf{M}_1 \\ \vdots \\ \mathbf{M}_n \end{bmatrix} = \begin{bmatrix} m_{11} & m_{12} & \cdots & m_{1m} \\ m_{21} & m_{22} & \cdots & m_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ m_{n1} & m_{n2} & \cdots & m_{nm} \end{bmatrix} \quad (29)$$

$\mathbf{M}_1$ 证据体转置为一个列向量和 $\mathbf{M}_2$ 证据体行向量相乘得到一个 mm 矩阵。

$$\Phi = \mathbf{M}_1^T \mathbf{M}_2 = \begin{bmatrix} m_{11} & \cdots & m_{1m} \end{bmatrix}^T \begin{bmatrix} m_{21} & \cdots & m_{2m} \end{bmatrix} = \begin{bmatrix} m_{11}m_{21} & m_{11}m_{22} & \cdots & m_{11}m_{2m} \\ m_{12}m_{21} & m_{12}m_{22} & \cdots & m_{12}m_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ m_{1m}m_{21} & m_{1m}m_{22} & \cdots & m_{1m}m_{2m} \end{bmatrix} \quad (30)$$

对角线元素是两个证据体对于同一个命题的融合乘积项，如果只有两个证据体融合，那么非对角线元素之和是冲突因子 K ，结合 D-S 证据理论结合律，将 Φ 矩阵的对角线元素（排成一个列向量）与 $\mathbf{M}_3$ 证据体行向量相乘得到一个新的矩阵。

$$\Phi = \begin{bmatrix} m_{11}m_{21}m_{31} & \cdots & \cdots & \cdots \\ \cdots & m_{12}m_{22}m_{32} & \cdots & \cdots \\ \vdots & \vdots & \ddots & \vdots \\ \cdots & \cdots & \cdots & m_{1m}m_{2m}m_{3m} \end{bmatrix} \quad (31)$$

新矩阵取出对角线元素依次与剩余的每一个证据体相乘，直到融合 $\mathbf{M}_n$ ，对角线元素是 n 个证据对同一个命题乘积融合结果，将所有结果矩阵的非对角线元素相加可得到冲突因子 K 。

3 案例分析

本文搭建的实验环境如图 2 所示，利用虚拟机和常见物联网设备搭建一个物联网场景进行态势感知工作，本文场景中使用了常见物联网设备，如蓝牙手环、无线路由器、Zigbee 设备等，手环主要是测试蓝牙模块的安全性，无线路由器主要是测试 Wi-Fi 模块安全性，Zigbee 设备主要是测试 Zigbee 协议上的安全性。

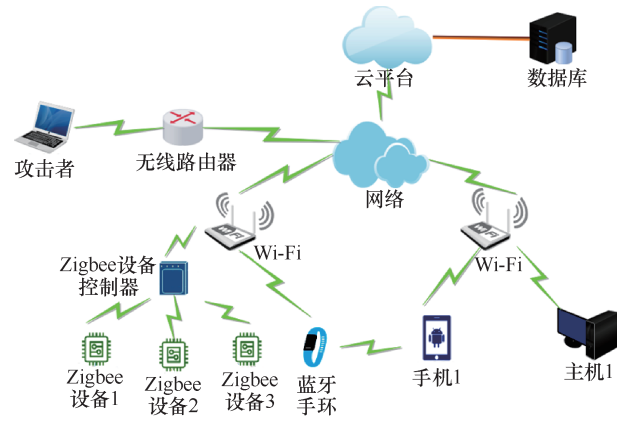


图 2 实验环境

Figure 2 Experimental environment

经过物联网固件安全性分析模块得到各固件的安全性测试报告。选取 T 时刻的安全性情况进行态势评估，漏洞分布情况如表 3 所示。

表 3 漏洞分布情况
Table 3 Vulnerabilities distribution

机器	CVE 编号	漏洞	漏洞等级评估
主机 1	CVE-2021-31939	v1	高危
数据库服务器	CVE-2021-26691	v2	紧急
Web 服务器	CVE-2021-31970	v3	中危
蓝牙手环	CVE-2021-31974	v4	中危
Wi-Fi 模块	CVE-2021-31169	v5	中危
Zigbee 设备	CVE-2021-31205	v6	低危

当前情况下多为中危风险项，同时存在一定程度的高风险项和紧急风险项，经过上述理论融合得到的态势评估结果如表 4 所示，可以看到系统以 64% 的概率处于中风险等级，即该时刻系统风险评估等级为中风险，在高风险等级上的概率接近 12%，符合该时刻的真实情况。

表 4 T 时刻态势评估结果
Table 4 T time situation assessment result

时刻	评语集				
	无风险	低风险	中风险	高风险	紧急风险
T	0.002 5	0.185 1	0.631 6	0.117 0	0.063 8

对于图 2 搭建的物联网环境进行连续监测，对同一固件的不同版本进行测试，收集一段时间内 8 个时刻的态势评估结果进行态势感知任务，收集到的 8 个时刻态势评估结果如表 5 所示，可以看出，有两个时刻系统呈现出高风险等级，其

余时刻是中风险等级。

表 5 T1~T8 时刻态势评估结果
Table 5 T1~T8 time situation assessment result

时刻	评语集				
	无风险	低风险	中风险	高风险	紧急风险
T1	0.100 8	0.406 8	0.270 1	0.220 1	0.002 2
T2	0.012 0	0.214 5	0.589 7	0.123 5	0.060 3
T3	0.009 8	0.198 8	0.657 9	0.100 1	0.033 4
T4	0.010 1	0.098 7	0.246 9	0.532 7	0.111 6
T5	0.237 8	0.453 2	0.290 8	0.007 8	0.010 4
T6	0.079 0	0.076 4	0.473 2	0.256 5	0.114 9
T7	0.035 4	0.149 8	0.105 9	0.467 8	0.241 1
T8	0.000 1	0.203 2	0.593 3	0.176 4	0.027 0

态势感知结果如表 6 所示。从表 6 中可以看出, 在该时间段内系统以接近 49% 的概率处于中风险等级, 受到 T7 时刻的影响, 高风险等级概率处于 20% 左右, 未来需要注意加强安全防护措施。传统 D-S 证据理论融合结果显示中风险等级概率约 99%, 但是基本概率分配几乎接近 1, 忽视对其他风险的感知, 而本文方法在各风险等级上都有合理的基本概率分配, 既与预期相符合, 又能指出高风险和紧急风险的可能性, 更具有指导意义。

表 6 态势感知结果
Table 6 Situation awareness result

方法	评语集					不确定值
	无风险	低风险	中风险	高风险	紧急风险	
传统 D-S 证据理论	0	0.008 0	0.990 9	0.001 1	0	—
本文方法	0.002 9	0.176 7	0.485 4	0.207 4	0.041 7	0.086 0

为了量化描述态势感知结果, 绘制态势感知曲线, 本文方案对 5 个评语量化值分配^[17]{2,4,6,8,10}, 定义态势值为

$$T = \sum_{\theta_i \in \theta} e(\theta_i) m(\theta_i) \quad (32)$$

其中, $e(\theta_i)$ 是 θ_i 评语的分值, $m(\theta_i)$ 是融合后的 θ_i 评语基本概率分配值。

对 T1-T8 时刻绘制物联网安全态势感知趋势曲线, 结果如图 3 所示, 从曲线趋势上来看, 态势呈上升趋势, 意味着将来风险升高, 需要加强防护措施。

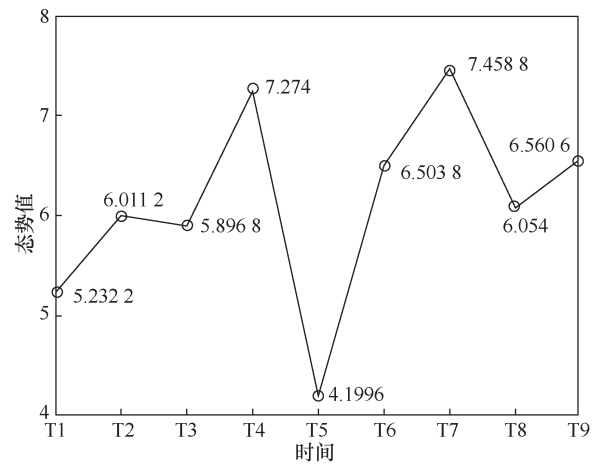


图 3 物联网安全态势感知趋势曲线
Figure 3 IoT security situational awareness trend curve

4 结束语

本文通过深入调研物联网态势感知系统的现状, 提出了基于改进 D-S 证据理论的态势评估和态势感知方法, 经过实验对比, 主要结论如下。

1) 利用改进的 Topsis 方法衡量证据间的可信度, 能准确快速识别冲突证据, 降低冲突证据的可信度, 并保证相互支持证据间的高可信度。在不同数量证据体融合和常见冲突证据融合时对正确命题的基本概率分配高。

2) 提出基于时间折扣和高风险漏洞比例折扣的 D-S 证据理论, 在态势感知过程中, 充分预测了高风险和紧急风险的概率, 并得到了态势感知曲线, 对将来安全防护有良好的指导意义。

参考文献:

- [1] 杨毅宇, 周威, 赵尚儒, 等. 物联网安全研究综述: 威胁、检测与防御[J]. 通信学报, 2021, 42(8): 188-205.
YANG Y Y, ZHOU W, ZHAO S R, et al. Survey of IoT security research: threats, detection and defense[J]. Journal on Communications, 2021, 42(8): 188-205.
- [2] 张方哲. 物联网安全态势感知系统的研究与实现[D]. 济南: 山东大学, 2021.
ZHANG F Z. Research and implementation of Internet of things security situation awareness system[D]. Jinan: Shandong University, 2021.
- [3] 龚俭, 臧小东, 苏琪, 等. 网络安全态势感知综述[J]. 软件学报, 2017, 28(4): 1010-1026.
GONG J, ZANG X D, SU Q, et al. Survey of network security situation awareness[J]. Journal of Software, 2017, 28(4): 1010-1026.
- [4] 简玲, 叶天鹏, 林祥, 等. 多源融合的大数据网络安全态势感知

- 平台研究与探索[J]. 信息安全, 2020, (S2).
- JIAN L, YE T P, LIN X, et al. Research and exploration of multi-source fusion on big data network security situation awareness platform[J]. Netinfo Security, 2020, (S2).
- [5] LIVIA M B. An approach for information security risk assessment in cloud environments[J]. Informatica Economica Journal, 2020, 24(4): 29-40.
- [6] ZENONAS T, NIKOLAJ G, ASSEL N, et al. Information security risk assessment in critical infrastructure: a hybrid MCDM approach[J]. Informatica, 2019, 30(1):187-211.
- [7] 黄亭亭. 水电工程洪水灾害链态势推演和应急决策的研究[D]. 武汉: 华中科技大学, 2017.
- HUANG T T. Research on emergency situation evolution and emergency decision making for flood disaster chain of hydropower project construction[D]. WuHan: Huazhong University of Science and Technology, 2017.
- [8] BENAVALI A, RISTIC B, FARINA A, et al. An application of evidential networks to threat assessment[J]. IEEE Transactions on Aerospace and Electronic Systems, 2009, 45(2): 620-639.
- [9] LIAO Y W, ZHAO G S, WANG J, et al. Network security situation assessment model based on extended hidden markov[J]. Mathematical Problems in Engineering, 2020.
- [10] HAN Z, LI X, HUANG K, et al. A software defined network based security assessment framework for cloud IoT[J]. IEEE Internet of Things Journal, 2018, 5(3): 1424-1434.
- [11] 魏青梅, 李宇博, 应雨龙. 结合 Dempster-Shafer 证据理论与循环神经网络的网络安全态势预测[J]. 济南大学学报(自然科学版), 2020, 34(3): 238-246.
- WEI Q M, LI Y B, YING L Y. Network security situation prediction based on Dempster-Shafer evidence theory and recurrent neural network[J]. Journal of University of Jinan(Science and Technology), 2020, 34(3): 238-246.
- [12] PAN Z, WU Y. Building and testing network security situational awareness model based on bayesian method[C]//Third International Conference on Cyberspace Technology(CCT 2015). 2015:1-4.
- [13] 张欢, 陆见光, 唐向红. 面向冲突证据的改进 DS 证据理论方法[J]. 北京航空航天大学学报, 2020, 46(3): 616-623.
- ZHANG H, LU J G, TANG X H. An improved DS evidence theory algorithm for conflict evidence[J]. Journal of Beijing University of Aeronautics and Astronautics, 2020, 46(3): 616-623.
- [14] LO H W, LIOU J J H. Comments on “factors influencing medical tourism adoption in malaysia: a DEMATEL-fuzzy TOPSIS approach” [J]. Computers & Industrial Engineering, 2021,157.
- [15] 邓勇, 施文康, 朱振福. 一种有效处理冲突证据的组合方法[J]. 红外与毫米波学报, 2004, 23(1): 27-32.
- DENG Y, SHI W K, ZHU Z F. Efficient combination approach of conflict evidence[J]. Journal of Infrared and Millimeter Waves, 2004, 23(1): 27-32.
- [16] 奚婷婷, 熊伟丽, 张林, 等. 基于矩阵分析的 DS 合成算法[J]. 计算机工程, 2009, 35(16): 264-266.
- XI T T, XIONG W L, ZHANG L, et al. DS compositive algorithm based on matrix analysis[J]. Computer Engineering, 2009, 35(16): 264-266.
- [17] 秦涛, 鲁冬林, 曾拥华. 基于 D-S 理论的分队级 BDR 能力指标评估模型研究[J]. 中国设备工程, 2021, (9): 153-155.
- QIN T, LU D L, ZENG Y H. Research on unit level BDR capability index evaluation model based on D-S Theory[J]. China Plant Engineering, 2021, (9): 153-155.

[作者简介]



李剑(1976—), 男, 陕西西安人, 北京邮电大学教授、博士生导师, 主要研究方向为智能网络安全和量子密码学。



董廷鲁(1996—), 男, 山东齐河人, 北京邮电大学硕士生, 主要研究方向为大数据与网络信息处理。



李劫(1977—), 男, 北京人, 北京邮电大学讲师, 主要研究方向为知识图谱和强化学习。