网络安全态势感知中D-S证据理论冲突证据的修正研究

寇 广[1,2] 汤光明[1] 徐梓椋[1]

(中国人民解放军信息工程大学 郑州 450001)[1] (信息保障技术重点实验室 北京 100072)[2]

摘 要 D-S证据理论是不确定推理的一种重要方法,在许多方面都得到了广泛的应用。针对D-S证据理论在网络安全态势感知的数据融合过程中的应用,就多源数据的证据组合结果与直觉相悖的问题进行深入研究,提出了一种新的解决方案。该方案通过支持度的思想对冲突证据源进行修正以达到解决证据冲突的目的。最后,以网络安全态势感知环境为背景进行数值算例,证明了所提方法的可行性。

关键词 D-S证据理论,数据融合,态势感知,证据冲突

中图法分类号 TP393 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2015.7.044

Research on Revising Conflict Evidence of D-S Evidence Theory in Network Security Situation Awareness

KOU Guang[1,2] TANG Guang-ming[1] XU Zi-liang[1]

(PLA Information Engineering University, Zhengzhou 450001, China)[1]

(Science and Technology on Information Assurance Laboratory, Beijing 100072, China)[2]

Abstract D-S evidence theory is a kind of important uncertainty reasoning methods, has been widely used in many ways. The paper mainly studied application of D-S evidence in the data integration process of network security awareness. And researching contradictions between combination results of multi-source evidence and intuition, it put forward a new solution. The scheme revises the origin of conflict evidence through using the support ideas in order to solve the conflict of evidence. Finally, through a numerical example in the network security situational awareness environment, it proved the feasibility of this method.

Keywords D-S evidence theory, Data fusion, Situation awareness, Evidence conflict

1 引言

随着时代的发展,人们已经越来越离不开网络;与此同时,各种网络安全问题也引起了人们的广泛关注。如何及时有效地感知到网络安全的态势,已经引起了相关科研人员的足够重视。为了能够及时地发现各种针对网络空间安全的威胁,需要精确、高效地感知整个网络空间的实时态势并且预测未来的态势走向。为此,需要综合考虑来自IDS、Netflow、Firewall等多方面的反馈信息,综合处理多源数据得到态势判定,为决策者提供及时、有效的决策依据。数据融合技术能够对多源信息进行快速有效的处理,能够对网络环境中具有相似或是不同特征模式的多源信息进行互补集成,从而获得对当前网络状态的准确判断。将数据融合技术充分应用至态势感知并针对网络空间各类数据进行融合处理得到态势要素,是态势感知研究的一项重要内容[1]。

Tim Bass首次提出将JDL模型直接运用到网络态势感知领域,这为以后数据融合技术在网络态势感知领域的应用奠定了基础,是该技术在此领域应用的一个起点。Jason Shifflet运用数据融合技术构造了一个网络入侵检测模型,实现了网络空间的态势感知。国内也有一些科研机构尝试把数据融合技术应用到网络安全领域,提出了应用数据融合技术的网络安全分析评估系统、入侵检测系统等。目前,状态估计、不确定性推理、二维与三维的系统可观测性最佳估计等技术都在数据融合中得到了运用,其中以D-S证据理论的应用最为广泛。

2 D-S证据理论及其缺陷

D-S证据理论又称信任函数理论,是经典概率理论的扩展。该理论最早由Dempster于1967年提出,当时Dempster提出了不确定性推理模型的一般框架,成功地把命题不确定问题转化为了集合的不确定问题。之后在20世纪70年代中期,其学生Shafer对理论进行了扩充整理,从而形成了D-S证据理论。D-S证据理论为不确定信息的表达和合成提供了很好的方法。证据理论既可以处理随机性导致的不确定性问题,也可以处理模糊性导致的不确定性问题,能将不知道和不确定区分开来;并且证据理论不需要先验概率和条件概率的密度为先决条件。D-S证据论中的相关概念如下[2,3]所示。

首先需要定义一个识别框架。设U表示目标问题X的

到稿日期:2014-07-03 返修日期:2014-10-22 本文受信息保障技术重点实验室开放基金(KJ-14-106),无线传感器网络异常检测及异常数据重构关键技术研究(61303074)资助。

寇 广(1983-),男,博士生,讲师,主要研究方向为网络安全态势感知、数据融合,E-mail:kg5188@163.com;汤光明(1963-),女,博士,教授,主要研究方向为信息隐藏、安全评估;徐梓椋(1990-),男,硕士生,主要研究方向为可信计算。

所有可能取值的一个论域集合，且 U 既可以是有限集也可以是无限集，但其中的所有元素之间必须是互不相容的，则称 U 是 X 的识别框架。

证据理论中给出了基本信任程度的表达方法：U 为一个识别框架，当函数 $m:2^U\to[0,1]$ 满足条件：

(1) $m(\varnothing)=0$；

(2) $\sum_{A\subset U} m(A)=1$。

则称 $m(A)$ 为 A 的基本概率分配，表示对命题 A 的基本信任程度。

其次，定义两个用于衡量证据之间的支持程度和拒绝程度的函数，即信任函数和似真度函数。

定义 1 设 U 为一个识别框架，$m:2^U\to[0,1]$ 是 U 上的基本概率分配，则

$BEL:2^U\to[0,1]$

$BEL[A]=\sum_{B\subset A} m(B)$，$\forall A\subset U$

称该函数是 U 上的信任函数，即 A 的信任函数为 A 中每个子集的基本信任度值之和，它表示对 A 的总信任，从而可得

$BEL(\varnothing)=0, BEL(U)=1$

定义 2 $PL(A)=1-BEL(\overline{A})=\sum_{B\cap A\neq\varnothing} m(B)$ 为似真度函数，表示不否定 A 的信任度，是所有与 A 相交的集合的基本概率赋值之和。

BEL 函数表示命题成立的最小不确定函数，称为下限函数；PL 函数表示命题非假的信任程度成立的不确定性度量，称为不否定函数。如果 $A=B$，那么 B 的 BEL 值为 A 的概率；如果 B 为一般命题，那么 B 的 BEL 值为所有组成 B 的原始命题的基本概率分配的和。

最后是证据理论的合成规则，证据理论中的组合规则提供了组合两个证据的规则。

定义 3 设 m_1 和 m_2 是 2^U 上的两个互相独立的基本概率分配，则组合这两个证据的基本概率分配可定义为：

$$m(A)=\begin{cases}\dfrac{\sum_{A_i\cap B_j=A} m_1(A_i)m_2(B_j)}{1-\sum_{A_i\cap B_j=\varnothing} m_1(A_i)m_2(B_j)}, & \forall A\subset U, A\neq\varnothing\\ 0, & A=\varnothing\end{cases}$$

其中，$\sum_{A_i\cap B_j=\varnothing} m_1(A_i)m_2(B_j)$ 为归一化因子，令 $K=\sum_{A_i\cap B_j=\varnothing} m_1(A_i)m_2(B_j)$。

定义 4 对于多个证据组合的情况，令 $m_1, m_2, \cdots, m_i$ 分别表示 n 个信息的基本概率分配，且独立，则多证据组合的基本概率分配可定义为：

$$m(A)=\begin{cases}\dfrac{\sum_{\cap A_i=A}\prod_{i=1}^{n} m_i(A_i)}{1-\sum_{\cap A_i=\varnothing}\prod_{i=1}^{n} m_i(A_i)}, & \forall A\subset U, A\neq\varnothing\\ 0, & A=\varnothing\end{cases}$$

此时归一化因子 $K=\sum_{\cap A_i=\varnothing}\prod_{i=1}^{n} m_i(A_i)$。

然而，由于网络安全态势感知中各类型探测器是相互独立探测的，其间没有沟通和协作，探测到的多源数据往往存在冗余甚至是证据冲突。例如，当 IDS 的部分探测器探测到存在入侵信息时，日志信息可能提示是安全的。而如果不处理好数据冲突的问题，那么在证据组合时，会对交集为空的两个焦元的基本可信度分配造成不当处理，最终造成组合结果与直觉相悖的现象。

许多学者针对上述冲突证据合成问题进行了研究，提出了一些解决方法，主要分为两类：第一种是修改 D-S 合成规则。持这种观点的学者认为最终造成组合结果与直觉相悖的现象是由于在修改 D-S 合成规则时对交集为空的两个焦元的处理不当，解决方法是研究如何将冲突重新分配。第二种是修改证据源模型。此方法认为不必对 D-S 合成规则本身进行修改，而是在使用 D-S 合成规则前选择适当的方法首先对冲突证据进行预处理[4,5]。

从持第一类观点的学者的角度来讲，产生结果与直觉相悖的不合理现象的主要原因是证据理论中的合成规则为了满足基本概率赋值为 1 的要求，在处理归一化因子 K 时，将两个证据公共焦元的基本可信度分配函数变为原来的 $K-1$ 倍，而冲突分配并非所有焦元共同造成的，也并非基本信任分配大的公共焦元产生冲突的可能性大。实际上，冲突可以说是矛盾双方在某些方面非常近似，或者说是由某方面或某时刻的干扰所致[6,7]。

从持第二类观点的学者的角度来讲，在使用 D-S 合成规则前如何对冲突证据进行处理，是解决结果与直觉相悖的现象的核心所在。证据的冲突信息是不容忽视的，对冲突信息的直接遗弃必然造成信息的损失甚至是误判，而采取合理的特征提取方法对冲突信息提取特征，之后将其加入组合规则，分析、挖掘冲突信息中的有用信息会使组合结果更有效、更合理[8-10]。

3 针对证据源的改进

对于 D-S 证据理论中的冲突证据问题，前人已经提出了解决方法。其中，Yager 等人针对修改 D-S 合成规则，提出的统一信度函数组合方法；Murphy，Haenni 等人针对冲突证据源修正提出了一种证据源平均的方法。陈炜军、景占荣等人在文献[11]中提出了一种同时对规则和证据源进行修正，并考虑证据交叉融合的证据理论修正模型。下面将就冲突证据源修正的方法提出一些新看法。

虽然在证据的获取上所有证据的获取是相互独立的，但是这些证据都是由相同问题引发的，本质上存在着内在的关联。解决好合成规则上的证据冲突问题的关键就是处理好各个证据之间的关联性问题，从而消除某些偏差很大的数据对整个融合过程的影响。

为了更好地处理证据间的关联性问题，参考文献[12]中提到的距离函数的概念来度量系统中各个证据间的支持程度。

先假定识别框架 U 下的两个证据 E_1 和 E_2，其相应的基本概率分配函数分别为 m_1 和 m_2，焦元分别为 A_i 和 B_j，则可以计算得到证据 E_1 和 E_2 的相似系数为：

$$d_{12}=\prod_{A_i\cap B_j=A\neq U}\frac{2\cdot m_1(A_i)m_2(B_j)}{m_1^2(A_i)+m_2^2(B_j)}$$

假设系统收集了 n 个证据，则可以计算出在条件 $A_i\cap B_j=A\neq U$ 下的证据 E_i 和 E_j 间的相似系数，并可以用相似矩阵的形式表达如下：

$$S=\begin{bmatrix}1 & d_{12} & \cdots & d_{1n}\\ d_{21} & 1 & \cdots & d_{2n}\\ \vdots & \vdots & \vdots & \vdots\\ d_{n1} & d_{n2} & \cdots & 1\end{bmatrix}$$

将每行相加可得到条件 $A_i \cap B_j = A \neq U$ 下的各证据对的支持度为：

$$Sup(m_i)=\sum_{j=1}^{n} d_{ij}, i,j=1,2,3,\cdots,n$$

$Sup(m_i)$表示证据 m_i 被其他证据所支持的程度。假设一个证据与其他证据都比较相似，则它们之间的相互支持度就会比较高；相反，如果一个证据和其他证据的相似度较低，则认为它们相互支持的程度也较低。当两个证据完全相似时，支持度将达到 1。

将证据的支持度归一化可得到证据 E_i 的可信度：

$$Crd(m_i)=\frac{Sup(m_i)}{\sum_{i=1}^{n} Sup(m_i)}, i,j=1,2,\cdots,n$$

比较得出受支持最多的证据 $\max(E_i)$，支持度为 $\max(Crd(m_i))$。定义其为引导者，利用引导者来处理冲突数据，而不是像文献[12]直接用支持度取代证据源。

对于冲突证据的查找，选择支持度最低的 n 个证据 $\min(E_i), \min_1(E_i), \cdots, \min_{n-1}(E_i)$ 为冲突证据。而对于最低支持度证据的个数 n 的确定，通过以下方法来评定：凡是满足以下条件的证据均为最低支持度证据。

$$\overline{Crd(m_l)}-Crd(m_j)>\max Crd(m_i)-\overline{Crd(m_l)}$$

其中，$\overline{Crd(m_l)}$为支持度的均值。

我们认为在合成规则中大部分证据的关联性都是可信的，只有少部分的证据存在冲突偏差。所以只针对找到的冲突证据进行修正。冲突证据与引导者间出现的偏差，导致我们对冲突证据的关联性产生怀疑，冲突证据的支持度越低，引导者受到的支持度越高，则我们对冲突证据的信任也就越低。所以，定义修正系数为冲突证据与引导者之间的相差度。以最小支持度证据 $\min(E_i)$ 为例。

$$k=1-\frac{2\cdot\min(Crd(m_i))\max(Crd(m_j))}{\max^2(Crd(m_j))+\min^2(Crd(m_i))}$$

利用修正系数对冲突证据置信程度进行修正，来降低冲突证据的基本分配概率：

$$\begin{cases} m_i'(A)=m_i(A)+k\cdot[m_j(A)-m_i(A)] \\ m_i'(\overline{A})=m_i(\overline{A})-k\cdot[m_j(A)-m_i(A)] \end{cases}, A\subset U$$

而对于其它没有经过修正的证据，为了避免引导者对全局的影响，直接按比例用修正值对其进行归一化处理。最后，利用证据理论的合成规则对修正后的冲突证据以及其余原始数据进行合成。

4 网络安全态势感知中的数值算例[13,14]

下面先给出一个在网络安全态势感知中的简单数值算例。设在网络环境中可能存在安全威胁，计算机网络态势感知中的 5 种探测器提供威胁的类型信息（A 类攻击，B 类攻击，C 类攻击）。假设在某时刻探测器给出的基本概率赋值为：

$$\begin{cases} m_1: m_1(A)=0.6, m_1(B)=0.23, m_1(C)=0.17 \\ m_2: m_2(A)=0.5, m_2(B)=0.4, m_2(C)=0.1 \\ m_3: m_3(A)=0.7, m_3(B)=0.29, m_3(C)=0.01 \\ m_4: m_4(A)=0.6, m_4(B)=0.29, m_4(C)=0.11 \\ m_5: m_5(A)=0.6, m_5(B)=0.3, m_5(C)=0.1 \end{cases}$$

分别用原始的证据合成规则、文献[15]的方法、文献[16]的方法以及本文的两种方法进行处理，得到的结果如表 1 所列。

表 1 数值算例结果分析(一)

证据组合	规则	m(A)	m(B)	m(C)	s	识别结果
$m_1\oplus m_2\oplus m_3$	Dempster	0.88664	0.11265	0.00071	—	A
	文献[15]	0.60016	0.30613	0.09371	—	A
	文献[16]	0.88664	0.11265	0.00071	—	A
	本文方法	0.88664	0.11265	0.00071	0	A
$m_1\oplus m_2\oplus m_3\oplus m_4$	Dempster	0.94021	0.05785	0.00014	—	A
	文献[15]	0.60013	0.30175	0.09812	—	A
	文献[16]	0.94021	0.05785	0.00014	—	A
	本文方法	0.94021	0.05785	0.00014	0	A
$m_1\oplus m_2\oplus m_3\oplus m_4\oplus m_5$	Dempster	0.97019	0.02979	0.00002	—	A
	文献[15]	0.60010	0.30136	0.09854	—	A
	文献[16]	0.97019	0.02979	0.00057	—	A
	本文方法	0.97019	0.02979	0.00002	0	A

通过该算例可以发现，在证据冲突较小甚至不存在的情况下，原始的证据合成规则、文献[15]的方法、文献[16]的方法以及本文的方法都可以得出最佳结果，而且本文方法相对于文献[15]的方法更具收敛性，当数据变多时，数据结果向 A 聚焦；本文方法虽然与文献[16]方法结果相近，但通过计算就可以明显看出本文方法计算过程更方便快速。然而在网络安全态势感知中存在各种网络环境问题的不确定性因素影响，所以需要对存在证据冲突的情况再做数值算例分析。其它探测器数据不变，假设 m_2 探测到的数据由于受网络环境的影响存在较大误差，$m_2: m_2(A)=0.01, m_2(B)=0.4, m_2(C)=0.59$。此时，再分别采用原始的证据合成规则、文献[15,16]的方法以及本文的方法进行处理，得到的结果如表 2 所列。

表 2 数值算例结果分析(二)

证据组合	规则	m(A)	m(B)	m(C)	s	识别结果
$m_1\oplus m_2\oplus m_3$	Dempster	0.1317	0.8368	0.0315	—	B
	文献[15]	0.4909	0.2934	0.2157	—	A
	文献[16]	0.6917	0.2960	0.0123	—	A
	本文方法	0.8069	0.1749	0.0182	1	A
$m_1\oplus m_2\oplus m_3\oplus m_4$	Dempster	0.2431	0.7463	0.0106	—	B
	文献[15]	0.5313	0.2907	0.1780	—	A
	文献[16]	0.8264	0.1709	0.0027	—	A
	本文方法	0.9028	0.0946	0.0026	1	A
$m_1\oplus m_2\oplus m_3\oplus m_4\oplus m_5$	Dempster	0.3933	0.6038	0.0029	—	B
	文献[15]	0.5501	0.2922	0.1577	—	A
	文献[16]	0.9058	0.0937	0.0005	—	A
	本文方法	0.9500	0.0497	0.0003	1	A

从分析结果可以看出，当存在较大的冲突证据影响时，原有的 Dempster 证据合成规则就出现了偏差，导致出现错误的结果。而文献[15,16]的方法以及本文的方法都能够降低误差，做出较为正确的判定。但文献[15]的方法缺少收敛性；文献[16]方法虽然与本文方法结果相近，但通过计算可知本文方法计算过程更方便快速。在文献[16]方法中如果存在多条冲突证据，就需要在 1 至 3 步间进行多次循环冲突检测，直到不存在冲突，当存在大量冲突时必然要耗费大量时间；而本文方法不论存在多少冲突量，都只用进行一次冲突检测，大大节约了网络安全态势感知的时间。

综合两次数值算例的分析结果，可以证明，本文对证据合成的改进方法在网络安全态势感知的数据融合中是切实可行的。首先，本文的方法在较大的冲突证据影响时仍然可以保持结果的正确性和较好的收敛性；同时，相对文献[16]的方法具有更低的计算复杂度，更加方便快捷，能为瞬息万变的网络

安全态势感知内容做出更为及时的估计。

结束语 在网络安全态势感知中的数据融合的大背景下，本文针对 D-S 证据合成规则不能正确处理冲突证据的缺陷进行了深入的研究，针对冲突证据源的预处理提出了新的解决方法。最后利用数值算例进行了证明，结果表明本文方法能够有效地解决证据冲突问题，并且具有更好的收敛性和高效性，更加适用于网络安全态势感知环境。当然，我们也考虑过将证据支持度的处理方法运用到合成规则的改进上，但是还不够成熟。在下一步工作中，将着重针对合成规则本身的改进进行研究。

参 考 文 献

[1] Wang Ping, Zhu Xue-mei. Fact Reasoning with Reliable D-S Evidence Theory[C]// Proceedings of the 3rd International Conference on Intelligent Information Technology Application. 2009: 441-444

[2] 赵争业，夏远，钟求喜. 基于 D-S 证据理论的脆弱性态势数据融合方法研究[J]. 计算机应用与软件，2013，30(9)：80-86
Zhao Zheng-ye, Xia Yuan, Zhong Qiu-xi. Research on vulnerability situational data fusion method based on D-S evidence theory [J]. Computer Applications and Software, 2013, 30(9): 80-86

[3] 杨国胜，窦丽华. 数据融合及其应用[M]. 北京：兵器工业出版社，2004
Yang Guo-sheng, Dou Li-hua. Data Fusion and Its Application [M]. Beijing: Weapon Industry Press, 2004

[4] 刘效武. 基于多源融合的网络安全态势量化感知与评估[D]. 哈尔滨：哈尔滨工程大学，2009
Liu Xiao-wu. Network Security Situation Quantification Awareness and Evaluation Based on Multi-source Fusion[D]. Harbin: Harbin Engineering University, 2009

[5] Chen Yi, Huang Qing, Chen Yan-lan. An Improve Information Fusion Algorithm Based on BP Neural Network and D-S Evidence Theory[C]// 2012 Third International Conference on Digital Manufacturing & Automation. 2012: 179-181

[6] 朱静. 基于 D-S 证据理论的网络安全风险评估模型[D]. 保定：华北电力大学，2008
Zhu Jing. Network Security Risk Assessment Model Based on D-S Evidence Theory[D]. Baoding: North China Electric Power University, 2008

[7] Huang Yan-bo, Lan Yu-bin, Hoffmann W C, et al. Multisensor Data Fusion for High Quality Data Analysis and Processing in Measurement and Instrumentation[J]. Journal of Bionic Engineering, 2007, 4(1): 53-62

[8] Miao Yan-zi, Ma Xiao-ping, Zhang Jian-wei. Research on the Combination Rules of the D-S Evidence Theory and Improvement of Extension to Fuzzy sets[C]// Proceedings of 2010 Chinese Control and Decision Conference. 2010: 2143-2149

[9] Wu Wen-jie, Huang Da-gui, Dong Zheng. Fault Diagnosis of the Aeroengine Based on Neural Network and D-S Evidence Theory [C]// Proceedings of 2011 ICCSIT. 2011

[10] Xing Xiao-qin, Wang Wei-dong, Wang Zhe, et al. Weighted Cooperative Spectrum Sensing Based on D-S Evidence Theory and Double-Threshold Detection[C]// 2013 IEEE 5th International Symposium on Microware, Antenna, Propagation and EMC Technologies for Wireless Communication. 2013: 145-149

[11] 陈炜军，景占荣，袁芳菲，等. D-S 证据理论的不足及其数学修正[J]. 中北大学学报，2010，31(2)：162-168
Chen Wei-jun, Jing Zhan-rong, Yuan Fang-fei, et al. Shortcoming of D-S Evidence Theory and Its Mathematic Modification[J]. Journal of North University of China, 2010, 31(2): 162-168

[12] 王洪发，王先义. D-S 证据理论在多源数据融合中的应用及改进[J]. 现代电子技术，2009，32(15)：7-9
Wang Hong-fa, Wang Xian-yi. Development and Problems of D-S Evidential Reasoning in Multisensor Data Fusion[J]. Modern Electronics Technique, 2009, 32(15): 7-9

[13] Miao Yan-zi, Ma Xiao-ping, Zhang Jian-wei. Research on IDS Data Fusion Model Based on D-S Evidence Theory[C]// Proceedings of 2010 International Conference on Services Science. 2010

[14] Liu Ping, Zhang Ling-xiao, Yang Xin-feng. Data Fusion of Distributed D-S Evidence Theory Based on Predicted Reliability[C]// Proceedings of 2011 International Conference on Computer and Automation Engineering. 2011: 131-135

[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 Yong, Shi Wen-kang, Zhu Zhen-fu. Efficient combination approach of conflict Evidence[J]. Journal of Infrared and Millimeter Waves, 2004, 23(1): 27-32

[16] 关欣，衣晓，孙晓明，等. 有效处理冲突证据的融合方法[J]. 清华大学学报(自然科学版)，2009，12(1)：138-141
Guan Xin, Yi Xiao, Sun Xiao-ming, et al. Fusion Method of Conflict Evidence[J]. Journal of Tsinghua University (Science and Technology), 2009, 12(1): 138-141

(上接第 185 页)

[9] Xia Xue-wen, Li Yuan-xiang, Zeng Hui. Data Encryption Algorithm Based on Two Dimension Toggle Cellular Automata[J]. Computer Science, 2010, 37(3): 46-48

[10] Abdo A A, Lian S G, Ismail I A, et al. A cryptosystem based on elementary cellular auto-mata[J]. Commun Nonlinear Sci Numer Simul, 2013, 18(1): 136-147

[11] Chen R J, Lai J L. Image security system using recursive cellular automata substitution[J]. Patter Recognit, 2007, 40(5): 1621-1631

[12] Seredynski M, Pienkosz K, Bouvry P. Reversible cellular automata based encryption[M]// Network and Parallel Computing. Springer, 2004: 411-418

[13] Chen G, Dong X. From chaos to order: methodologies, perspectives and applications[M]. Singapore: World Scientific, 1998

[14] Kari J. Reversibility and surjectivity problems of cellular automata[J]. Journal of Computer and System Sciences, 1994, 48(1): 149-182

[15] Toffoli T, Margolus N H. Invertible cellular automata: A review [J]. Physica D: Nonlinear Phenomena, 1990, 45(1): 229-253