(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 104348829 A
(43)申请公布日 2015.02.11

(21)申请号 201410505350.3

(22)申请日 2014.09.26

(71)申请人 智慧城市信息技术有限公司
地址 201209 上海市浦东新区金海路 3288 号 4 幢二楼

(72)发明人 萧海东 陈宁

(74)专利代理机构 北京同达信恒知识产权代理有限公司 11291
代理人 宋珊珊

(51)Int.Cl.
H04L 29/06(2006.01)

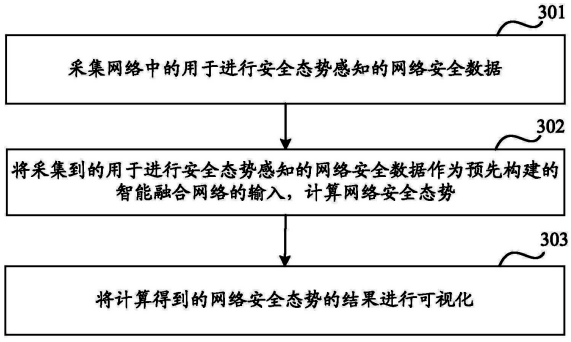
权利要求书3页 说明书14页 附图5页

(54)发明名称

一种网络安全态势感知系统及方法

(57)摘要

本发明提供一种网络安全态势感知系统及方法。所述系统包括：采集模块，用于采集网络中的用于进行安全态势感知的网络安全数据；感知模块，用于将采集到的用于进行安全态势感知的网络安全数据作为预先构建的智能融合模型的输入，计算网络安全态势；可视化模块，用于将计算得到的网络安全态势的结果进行可视化。通过本发明的网络安全态势感知系统能够克服网络安全态势感知系统数据处理异构信息来源困难、输出结果单一、感知过程智能程度不高的问题。



CN 104348829 A

1. 一种网络安全态势感知系统，其特征在于，所述系统包括：

采集模块，用于采集网络中的用于进行安全态势感知的网络安全数据；

感知模块，用于将采集到的用于进行安全态势感知的网络安全数据作为预先构建的智能融合模型的输入，计算网络安全态势；

可视化模块，用于将计算得到的网络安全态势的结果进行可视化。

2. 根据权利要求 1 所述的系统，其特征在于，

所述智能融合模型为 F 层，上一层的每个节点在下一层拥有 N 个子节点，其中 $F \geq 2$，且 $N \geq 2$；

所述智能融合模型中包含有历史网络安全数据的时序记忆模式，所述时序记忆模式至少表征了历史网络安全数据的特征点的时序关系。

3. 根据权利要求 2 所述的系统，其特征在于，所述系统还包括：

训练数据采集模块，用于采集用于训练智能融合模型的网络安全数据；

特征提取模块，用于针对采集的用于训练智能融合模型的网络安全数据，提取该数据的时空关联特征；

样本数据确定模块，用于对采集到的用于训练智能融合模型的网络安全数据以及提取的时空关联特征进行预设定的攻击以获得特征集和攻击反馈数据集，这两个集合作为智能融合模型的样本数据；

训练模块，用于根据获取的样本数据，训练智能融合模型，生成智能融合模型的时序记忆模式。

4. 根据权利要求 3 所述的系统，其特征在于，所述训练模块，包括：

输入单元，用于将特征集和攻击反馈数据集作为智能融合算法的样本数据，输入给智能融合模型；

学习单元，用于智能融合模型根据输入的样本数据进行学习，并形成与各层的节点对应的时序记忆模式。

5. 根据权利要求 1 所述的系统，其特征在于，所述感知模块，包括：

输入模式提取单元，用于提取网络安全数据的时间序列作为一组输入模式，输入给智能融合模型；

处理单元，用于通过预先构建的智能融合模型，计算输入模式与智能融合模型的时序记忆模式的匹配概率，并将匹配概率大于预设阈值的时序记忆模式作为最终匹配的时序记忆模式，形成态势特征结果集，用于进行可视化。

6. 根据权利要求 5 所述的系统，其特征在于，所述可视化模块，用于将态势特征结果集中的时序记忆模式，与预先存储的时空数据片段进行特征匹配，输出匹配结果，将匹配结果作为可视化片段。

7. 根据权利要求 6 所述的系统，其特征在于，所述系统还包括：

记录模块，用于所述可视化模块将态势特征结果集中的时序记忆模式，与预先存储的时空数据片段进行特征匹配之后，记录每个可视化片段的特征点的空间，时间和主方向供可视化使用；

第一划分模块，用于以主方向为起点，以特征点为中心，将可视化空间划分为 p 个扇形区域，其中，$p>1$；

第二划分模块，用于以特征点所在时空位置为基点划分时域推演区间为前后两个区间来明确历史态势和未来态势关系，将时空空间划分为 2p 个区间；

时空编码建立模块，用于按时间先后顺序和预设的空间顺序对每个区间设好索引，建立起该特征点的特征和其他特征点的特征的时空编码关系，其中，所述时空编码关系是依据时间轴建立的安全特征变化数据集；

校验模块，用于根据时空编码关系生成分别与可视化片段和时空片段对应的时空检验矩阵 M_V 和 M_C，然后将 M_V 和 M_C 进行异或运算，得到异或矩阵 D_{VC}，并分析异或矩阵 D_{VC} 中的非零元素所在的行和列，从而剔除掉错误的匹配；

输出模块，用于用直方图相似选优算法做出相似性判断，输出匹配结果。

8. 一种网络安全态势感知方法，其特征在于，所述方法包括：

采集网络中的用于进行安全态势感知的网络安全数据；

将采集到的用于进行安全态势感知的网络安全数据作为预先构建的智能融合模型的输入，计算网络安全态势；

将计算得到的网络安全态势的结果进行可视化。

9. 根据权利要求 8 所述的方法，其特征在于，

所述智能融合模型为 F 层，上一层的每个节点在下一层拥有 N 个子节点，其中 $F \geq 2$，且 $N \geq 2$；

所述智能融合模型中包含有历史网络安全数据的时序记忆模式，所述时序记忆模式至少表征了历史网络安全数据的特征点的时序关系。

10. 根据权利要求 9 所述的方法，其特征在于，所述智能融合模型根据以下方法构建：

采集用于训练智能融合模型的网络安全数据；

针对采集的用于训练智能融合模型的网络安全数据，提取该数据的时空关联特征；

对采集到的用于训练智能融合模型的网络安全数据以及提取的时空关联特征进行预设定的攻击以获得特征集和攻击反馈数据集，这两个集合作为智能融合模型的样本数据；

根据获取的样本数据，训练智能融合模型，生成智能融合模型的时序记忆模式。

11. 根据权利要求 10 所述的方法，其特征在于，所述根据获取的样本数据，训练智能融合模型，生成智能融合模型的时序记忆模式，包括：

将特征集和攻击反馈数据集作为智能融合算法的样本数据，输入给智能融合模型；

智能融合模型根据输入的样本数据进行学习，并形成与各层的节点对应的时序记忆模式。

12. 根据权利要求 8 所述的方法，其特征在于，所述将采集到的网络安全数据作为预先构建的智能融合模型的输入，计算网络安全态势，包括：

提取网络安全数据的时间序列作为一组输入模式，输入给智能融合模型；

通过预先构建的智能融合模型，计算输入模式与智能融合模型的时序记忆模式的匹配概率，并将匹配概率大于预设阈值的时序记忆模式作为最终匹配的时序记忆模式，形成态势特征结果集，用于进行可视化。

13. 根据权利要求 12 所述的方法，其特征在于，所述将计算得到的网络安全态势的结果进行可视化，包括：

将态势特征结果集中的时序记忆模式，与预先存储的时空数据片段进行特征匹配，输

出匹配结果，将匹配结果作为可视化片段。

14. 根据权利要求 13 所述的方法，其特征在于，所述将态势特征结果集中的时序记忆模式，与预先存储的时空数据片段进行特征匹配之后，所述方法还包括：

记录每个可视化片段的特征点的空间，时间和主方向供可视化使用；

以主方向为起点，以特征点为中心，将可视化空间划分为 p 个扇形区域，其中，$p>1$；

以特征点所在时空位置为基点划分时域推演区间为前后两个区间来明确历史态势和未来态势关系，将时空空间划分为 2p 个区间；

按时间先后顺序和预设的空间顺序对每个区间设好索引，建立起该特征点的特征和其他特征点的特征的时空编码关系，其中，所述时空编码关系是依据时间轴建立的安全特征变化数据集；

根据时空编码关系生成分别与可视化片段和时空片段对应的时空检验矩阵 M_V 和 M_C，然后将 M_V 和 M_C 进行异或运算，得到异或矩阵 D_{VC}，并分析异或矩阵 D_{VC} 中的非零元素所在的行和列，从而剔除掉错误的匹配；

用直方图相似选优算法做出相似性判断，输出匹配结果。

一种网络安全态势感知系统及方法

技术领域

[0001] 本发明涉及网络信息安全领域，尤其涉及一种网络安全态势感知系统及方法。

背景技术

[0002] 随着供应链的发展，信息流在其中的作用越来越明显。现代供应链的目标是提高整体效率、降低成本、满足客户需求，信息化成为现代供应链运营的核心驱动力。供应链信息平台上核心网络的 IP 化，移动通信、固定通信和互联网的融合逐渐成为新的发展趋势。供应链信息流在网络传输过程中，经常会遭到黑客的拦截、窃取、篡改、盗用、监听等恶意破坏，给商户带来重大损失。以各种非法手段企图入侵计算机网络的黑客，其恶意攻击构成信息系统中信息安全的威胁，已经成为供应链信息流安全的隐患。

[0003] 自从Tim Bass提出应用多传感器安全态势分析以来，关于安全态势的研究就一直是信息管理领域的热点，最初的安全态势感知是建立网络空间态势的框架，通过推理识别入侵者身份、速度、威胁性和入侵目标，进而评估网络空间的安全状态。欧美发达国家相关研究机构在这方面做着积极探索，如美国劳伦斯伯克利国家实验室的 The Spinning Cube of Potential Doom 系统；卡内基梅隆大学的 SILK 系统；美国国家高级安全系统研究中心 (NCASSR :National Center for Advanced Secure Systems Research) 的 SIFT 项目；Bruce D’Ambrosio 提出基于问卷调查方式的计算机攻击态势评估软件系统 SSARE；在这样的背景下，已有一些学者取得了一些进展，如Stephen G.Batsell等集成现有网络安全系统，开发了一个网络安全框架用来识别和抵御攻击，该框架由入侵检测、攻击源定位和攻击抵御二部分组成，采用可视化方式反映网络整体的安全状祝，这种方法对于同一企业内部网络中来挖掘态势感知信息比较有效，但针对于复杂的供应链信息网络环境有局限性，原因来自供应链上下游企业的信息共享在网络应用高层，同时供应商之间存在合作博弈利益关系，对商务交易或电子数据交换 (EDI) 信息环境安全保障需求有高度的利益一致性，却由于信息安全底层数据无法共享难以实现。

[0004] 由于供应链信息环境的不对称性，以及供应链环境特有的“牛鞭效应”，信息共享、传递、甚至决策过程中，使得安全信息感知处理困难，现有网络安全态势感知系统存在以下不足：

[0005] 1) 针对供应链所面临的信息安全风险的研究大多采用与企业运营风险几乎相同的方法，从时间、空间和成本三个维度对信息安全的危害程度建立测量指标体系，在提取特征时没有把信息和其他运营要素区别对待；

[0006] 2) 在发生应急事件时生成的汇聚指标不鲁棒，而且没有考虑到网络信息空间数据本身的结构、传输速率、分布性存在互补特性，因此使整体辅助决策系统的性能和效率降低。这一问题将在未来的供应链云环境和物联网应用环境下变得更严重。

[0007] 3) 在实际网络环境中部署困难。而随网络信息技术的不断发展，企业面临海量信息处理的情况已普遍存在。很难将统一的网络安全构架部署到网络环境异构的复杂的实际应用信息环境中去。

发明内容

[0008] 本发明的目的是提供一种网络安全态势感知系统及方法，以克服相关技术中网络安全态势感知系统数据处理异构信息来源困难、输出结果单一、感知过程智能程度不高的问题。

[0009] 本发明提供一种网络安全态势感知系统，包括：

[0010] 采集模块，用于采集网络中的用于进行安全态势感知的网络安全数据；

[0011] 感知模块，用于将采集到的用于进行安全态势感知的网络安全数据作为预先构建的智能融合模型的输入，计算网络安全态势；

[0012] 可视化模块，用于将计算得到的网络安全态势的结果进行可视化。

[0013] 其中，所述智能融合模型为 F 层，上一层的每个节点在下一层拥有 N 个子节点，其中 $F \geq 2$，且 $N \geq 2$；

[0014] 所述智能融合模型中包含有历史网络安全数据的时序记忆模式，所述时序记忆模式至少表征了历史网络安全数据的特征点的时序关系。

[0015] 其中，所述系统还包括：

[0016] 训练数据采集模块，用于采集用于训练智能融合模型的网络安全数据；

[0017] 特征提取模块，用于针对采集的用于训练智能融合模型的网络安全数据，提取该数据的时空关联特征；

[0018] 样本数据确定模块，用于对采集到的用于训练智能融合模型的网络安全数据以及提取的时空关联特征进行预设定的攻击以获得特征集和攻击反馈数据集，这两个集合作为智能融合模型的样本数据；

[0019] 训练模块，用于根据获取的样本数据，训练智能融合模型，生成智能融合模型的时序记忆模式。

[0020] 其中，所述训练模块，包括：

[0021] 输入单元，用于将特征集和攻击反馈数据集作为智能融合算法的样本数据，输入给智能融合模型；

[0022] 学习单元，用于智能融合模型根据输入的样本数据进行学习，并形成与各层的节点对应的时序记忆模式。

[0023] 其中，所述感知模块，包括：

[0024] 输入模式提取单元，用于提取网络安全数据的时间序列作为一组输入模式，输入给智能融合模型；

[0025] 处理单元，用于通过预先构建的智能融合模型，计算输入模式与智能融合模型的时序记忆模式的匹配概率，并将匹配概率大于预设阈值的时序记忆模式作为最终匹配的时序记忆模式，形成态势特征结果集，用于进行可视化。

[0026] 其中，所述可视化模块，用于将态势特征结果集中的时序记忆模式，与预先存储的时空数据片段进行特征匹配，输出匹配结果，将匹配结果作为可视化片段。

[0027] 其中，所述系统还包括：

[0028] 记录模块，用于所述可视化模块将态势特征结果集中的时序记忆模式，与预先存储的时空数据片段进行特征匹配之后，记录每个可视化片段的特征点的空间，时间和主方

向供可视化使用；

[0029] 第一划分模块，用于以主方向为起点，以特征点为中心，将可视化空间划分为 p 个扇形区域，其中，p>1；

[0030] 第二划分模块，用于以特征点所在时空位置为基点划分时域推演区间为前后两个区间来明确历史态势和未来态势关系，将时空空间划分为 2p 个区间；

[0031] 时空编码建立模块，用于按时间先后顺序和预设的空间顺序对每个区间设好索引，建立起该特征点的特征和其他特征点的特征的时空编码关系，其中，所述时空编码关系是依据时间轴建立的安全特征变化数据集；

[0032] 校验模块，用于根据时空编码关系生成分别与可视化片段和时空片段对应的时空检验矩阵 M_V 和 M_C，然后将 M_V 和 M_C 进行异或运算，得到异或矩阵 D_{VC}，并分析异或矩阵 D_{VC} 中的非零元素所在的行和列，从而剔除掉错误的匹配；

[0033] 输出模块，用于用直方图相似选优算法做出相似性判断，输出匹配结果。

[0034] 本发明还提供一种网络安全态势感知方法，所述方法包括：

[0035] 采集网络中的用于进行安全态势感知的网络安全数据；

[0036] 将采集到的用于进行安全态势感知的网络安全数据作为预先构建的智能融合模型的输入，计算网络安全态势；

[0037] 将计算得到的网络安全态势的结果进行可视化。

[0038] 其中，所述智能融合模型为 F 层，上一层的每个节点在下一层拥有 N 个子节点，其中 $F \geq 2$，且 $N \geq 2$；

[0039] 所述智能融合模型中包含有历史网络安全数据的时序记忆模式，所述时序记忆模式至少表征了历史网络安全数据的特征点的时序关系。

[0040] 其中，所述智能融合模型根据以下方法构建：

[0041] 采集用于训练智能融合模型的网络安全数据；

[0042] 针对采集的用于训练智能融合模型的网络安全数据，提取该数据的时空关联特征；

[0043] 对采集到的用于训练智能融合模型的网络安全数据以及提取的时空关联特征进行预设定的攻击以获得特征集和攻击反馈数据集，这两个集合作为智能融合模型的样本数据；

[0044] 根据获取的样本数据，训练智能融合模型，生成智能融合模型的时序记忆模式。

[0045] 其中，所述根据获取的样本数据，训练智能融合模型，生成智能融合模型的时序记忆模式，包括：

[0046] 将特征集和攻击反馈数据集作为智能融合算法的样本数据，输入给智能融合模型；

[0047] 智能融合模型根据输入的样本数据进行学习，并形成与各层的节点对应的时序记忆模式。

[0048] 其中，所述将采集到的网络安全数据作为预先构建的智能融合模型的输入，计算网络安全态势，包括：

[0049] 提取网络安全数据的时间序列作为一组输入模式，输入给智能融合模型；

[0050] 通过预先构建的智能融合模型，计算输入模式与智能融合模型的时序记忆模式的

匹配概率，并将匹配概率大于预设阈值的时序记忆模式作为最终匹配的时序记忆模式，形成态势特征结果集，用于进行可视化。

[0051] 其中，所述将计算得到的网络安全态势的结果进行可视化，包括：

[0052] 将态势特征结果集中的时序记忆模式，与预先存储的时空数据片段进行特征匹配，输出匹配结果，将匹配结果作为可视化片段。

[0053] 其中，所述将态势特征结果集中的时序记忆模式，与预先存储的时空数据片段进行特征匹配之后，所述方法还包括：

[0054] 记录每个可视化片段的特征点的空间，时间和主方向供可视化使用；

[0055] 以主方向为起点，以特征点为中心，将可视化空间划分为 p 个扇形区域，其中，$p>1$；

[0056] 以特征点所在时空位置为基点划分时域推演区间为前后两个区间来明确历史态势和未来态势关系，将时空空间划分为 2p 个区间；

[0057] 按时间先后顺序和预设的空间顺序对每个区间设好索引，建立起该特征点的特征和其他特征点的特征的时空编码关系，其中，所述时空编码关系是依据时间轴建立的安全特征变化数据集；

[0058] 根据时空编码关系生成分别与可视化片段和时空片段对应的时空检验矩阵 M_V 和 M_C，然后将 M_V 和 M_C 进行异或运算，得到异或矩阵 D_{VC}，并分析异或矩阵 D_{VC} 中的非零元素所在的行和列，从而剔除掉错误的匹配；

[0059] 用直方图相似选优算法做出相似性判断，输出匹配结果。

[0060] 本发明至少具有以下有益效果：通过本发明实施例提供的网络安全态势感知系统，实现智能数据聚融，在不完整的数据呈现中，记忆模式能够被学习并识别出来。通过组合模式学习的记忆与当前的输入，HTM 网络能够预测下一步可能发生什么，可以更准确、全面地进行网络安全态势感知。针对泛在网络中信息流安全多特征存在互补的特性，可以进行多角度的学习；从多个层次、多个角度对网络的安全态势进行分析，采用定量分析和定性描述相结合的方法，保证评估结果系统而全面。此外，本发明在安全态势评估的基础上，采用可视化片段与态势特征匹配方法，对感知数据进行进一步优化处理，完成匹配特征可视化精炼和匹配态势演化过程精炼。这对于动态预测网络系统安全态势变化趋势非常有帮助，使得态势数据集直观迅速的展示，有助于提高网络系统安全响应效率。

[0061] 应当理解的是，以上的一般描述和后文的细节描述仅是示例性和解释性的，并不能限制本发明。

附图说明

[0062] 图 1 为本发明实施例中网络安全态势感知系统的示意图；

[0063] 图 2 为本发明实施例中网络安全态势感知系统的另一示意图；

[0064] 图 3 为本发明实施例中网络安全态势感知方法的示例性流程图；

[0065] 图 4 为本发明实施例中智能融合网络的示意图；

[0066] 图 5 为本发明实施例中空间矩阵的示意图；

[0067] 图 6 为本发明实施例中欧几里得高斯函数分布示意图；

[0068] 图 7 为本发明实施例中匹配特征可视化精炼的示意图；

[0069] 图 8 为本发明实施例中划分空间域的示意图；

[0070] 图 9 为本发明实施例中网络安全态势感知框架的示意图。

具体实施方式

[0071] 以下结合说明书附图对本发明的优选实施例进行说明，应当理解，此处所描述的优选实施例仅用于说明和解释本发明，并不用于限定本发明，并且在不冲突的情况下，本发明中的实施例及实施例中的特征可以相互组合。

[0072] 本发明基于HTM(Hierarchical Temporal Memory，层级时序记忆)，提出了一种网络安全态势感知系统和方法。HTM 是一项对大脑新皮层进行建模的技术。大脑新皮层占了大约 75％的人脑的容量，负责所有高层次的理解，包括视觉、听觉、语言、触觉等。因为 HTM 是从生物学中得到的，所以它适合那些对于人类非常容易而对计算机非常困难的工作，例如物体的识别、做出预测、理解语言、在复杂的数据中发现模式等。根据 HTM 理论构建的 HTM 网络是一个记忆系统，随着时间变化，它通过给它的感知数据来学习它的世界，并从数据中抽象出高层的概念。抽象允许 HTM 网络来进行一般化，并对于传统计算机编程处理的严格规则提供灵活性和效率。例如，在不完整或是模糊不清的数据呈现中，模式能够被学习并识别出来。通过组合模式学习的记忆与当前的输入，HTM 网络能够预测下一步可能发生什么。

[0073] HTM 网络的设计确定了分层结构的大小与架构，然后为分层结构提供感知数据来训练它。感知数据来自供应链业务中的历史数据。重要的是在分层中，有许多数据用来训练，而且数据是具有时间这一基本元素。在供应链信息流安全分析中，为了进行有效的学习，都需要在时间的流逝中观察一组模式。

[0074] 一方面，本发明基于 HTM 网络的原理，提出一种网络安全态势感知系统，如图 1 所示，为本发明提出的网络安全态势感知系统，包括：

[0075] 采集模块 101，用于采集网络中的用于进行安全态势感知的网络安全数据；

[0076] 感知模块 102，用于将采集到的用于进行安全态势感知的网络安全数据作为预先构建的智能融合模型的输入，计算网络安全态势；

[0077] 可视化模块 103，用于将计算得到的网络安全态势的结果进行可视化。

[0078] 其中，在一个实施例中，智能融合模型为 F 层，上一层的每个节点在下一层拥有 N 个子节点，其中 $F \geq 2$，且 $N \geq 2$；

[0079] 智能融合模型中包含有历史网络安全数据的时序记忆模式，时序记忆模式至少表征了历史网络安全数据的特征点的时序关系。

[0080] 其中，在一个实施例中，如图 2 所示，系统还包括：

[0081] 训练数据采集模块 104，用于采集用于训练智能融合模型的网络安全数据；

[0082] 特征提取模块 105，用于针对采集的用于训练智能融合模型的网络安全数据，提取该数据的时空关联特征；

[0083] 样本数据确定模块 106，用于对采集到的用于训练智能融合模型的网络安全数据以及提取的时空关联特征进行预设定的攻击以获得特征集和攻击反馈数据集，这两个集合作为智能融合模型的样本数据；

[0084] 训练模块 107，用于根据获取的样本数据，训练智能融合模型，生成智能融合模型的时序记忆模式。

[0085] 其中，在一个实施例中，如图 2 所示，训练模块 107，包括：

[0086] 输入单元 108，用于将特征集和攻击反馈数据集作为智能融合算法的样本数据，输入给智能融合模型；

[0087] 学习单元 109，用于智能融合模型根据输入的样本数据进行学习，并形成与各层的节点对应的时序记忆模式。

[0088] 其中，在一个实施例中，如图 2 所示，感知模块 102，包括：

[0089] 输入模式提取单元 110，用于提取网络安全数据的时间序列作为一组输入模式，输入给智能融合模型；

[0090] 处理单元 111，用于通过预先构建的智能融合模型，计算输入模式与智能融合模型的时序记忆模式的匹配概率，并将匹配概率大于预设阈值的时序记忆模式作为最终匹配的时序记忆模式，形成态势特征结果集，用于进行可视化。

[0091] 其中，在一个实施例中，可视化模块 103，用于将态势特征结果集中的时序记忆模式，与预先存储的时空数据片段进行特征匹配，输出匹配结果，将匹配结果作为可视化片段。

[0092] 其中，在一个实施例中，如图 2 所示，系统还包括：

[0093] 记录模块 112，用于可视化模块将态势特征结果集中的时序记忆模式，与预先存储的时空数据片段进行特征匹配之后，记录每个可视化片段的特征点的空间，时间和主方向供可视化使用；

[0094] 第一划分模块 113，用于以主方向为起点，以特征点为中心，将可视化空间划分为 p 个扇形区域，其中，$p>1$；

[0095] 第二划分模块 114，用于以特征点所在时空位置为基点划分时域推演区间为前后两个区间来明确历史态势和未来态势关系，将时空空间划分为 2p 个区间；

[0096] 时空编码建立模块 115，用于按时间先后顺序和预设的空间顺序对每个区间设好索引，建立起该特征点的特征和其他特征点的特征的时空编码关系，其中，时空编码关系是依据时间轴建立的安全特征变化数据集；

[0097] 校验模块 116，用于根据时空编码关系生成分别与可视化片段和时空片段对应的时空检验矩阵 M_V 和 M_C，然后将 M_V 和 M_C 进行异或运算，得到异或矩阵 D_{VC}，并分析异或矩阵 D_{VC} 中的非零元素所在的行和列，从而剔除掉错误的匹配；

[0098] 输出模块 117，用于用直方图相似选优算法做出相似性判断，输出匹配结果。

[0099] 关于上述实施例中的网络安全态势感知系统中的各装置，其中各个模块执行操作的具体方式将在有关该方法的实施例中进行详细描述，下面对基于上述网络安全态势感知系统进行网络安全态势感知的方法进行详细说明。

[0100] 实施例一

[0101] 另一方面，本发明基于上述的网络安全态势感知系统，提出一种网络安全态势感知方法，如图 3 所示，包括：

[0102] 301：采集网络中的用于进行安全态势感知的网络安全数据。

[0103] 302：将采集到的用于进行安全态势感知的网络安全数据作为预先构建的智能融合模型的输入，计算网络安全态势。

[0104] 其中，历史网络安全数据指用于训练智能融合模型的样本数据和后期通过智能融

合模型进行网络安全态势感知的网络安全数据。

[0105] 其中，在一个实施例中，智能融合模型中包含有历史网络安全数据的时序记忆模式，时序记忆模式至少表征了历史网络安全数据的特征点的时序关系。

[0106] 303：将计算得到的网络安全态势的结果进行可视化。

[0107] 通过本发明实施例提供的网络安全态势感知方法实现网络安全态势感知，需要基于 HTM 网络构建智能融合模型，并对该智能融合模型进行训练，然后基于该智能融合模型进行安全态势感知。该智能融合模型在进行网络安全态势感知的过程中可以不断的学习和自我完善。

[0108] 下面对本发明实施例提供的网络安全态势感知方法进行展开说明：

[0109] 一、构建智能融合模型包括：

[0110] 步骤 A1：获取样本数据。

[0111] 步骤 A2：根据获取的样本数据，训练智能融合模型，生成智能融合模型的时序记忆模式。

[0112] 下面对上述两个步骤进行详细说明：

[0113] 1) 对于步骤 A1：

[0114] 步骤 A1 具体包括以下步骤 B1-B3：

[0115] 步骤 B1：采集用于训练智能融合模型的网络安全数据。

[0116] 其中，在一个实施例中，网络安全数据包括：应用层、网络传输层以及物理层面的数据；其中应用层的网络安全数据将包括云计算登陆认证种类及安全等级，供应链信息应用集成安全信息，web service 安全，解析服务安全数据等，此外，信息利用环节，企业中间件涉及的安全数据也纳入到这一部分；对于涉及泛在网络环境的网络安全数据可以通过网关和安管设备如防火墙、IDS 等获得，网络环境包括移动通信网、计算机网络、无线网络等；物理层的安全数据主要涉及到物联网的传感节点，可从传感器网关获得。

[0117] 步骤 B2：针对采集的用于训练智能融合模型的网络安全数据，提取该数据的时空关联特征。

[0118] 其中，时空关联特征用于得到多层面的局部时空对象的特征表述。

[0119] 步骤 B3：对采集到的用于训练智能融合模型的网络安全数据以及提取的时空关联特征进行预设定的攻击以获得特征集和攻击反馈数据集，这两个集合作为 HTM 网络的样本数据。

[0120] 可以通过摒弃权重弱化的特征达到特征筛选的目的，具体的：采集的网络安全数据中，若 IDS 虚警高的话可以减少 IDS 权重，防火墙策略可靠的话可以提高防火墙数据的权重。

[0121] 其中，在一个实施例中，步骤 B3 可具体执行为：对采集到的网络安全数据以及提取的时空关联特征进行预设定的攻击，获取鲁棒性高的时空关联特征，其中，对于每一种攻击，由对应于该攻击的鲁棒性高的时空关联特征形成对应于该攻击的特征集；并根据进行预设定的攻击后的结果，获取与该攻击对应的安全攻击反馈数据集。

[0122] 其中，在特征筛选的过程中可以摒弃权重弱化的特征达到特征筛选的目的，具体的如：采集的网络安全数据中若 IDS 虚警高的话可以减少 IDS 权重，防火墙策略可靠的话可以提高防火墙数据的权重。

[0123] 至此，样本数据的获取过程已经阐述清楚，下面介绍一下 HTM 网络的训练学习过程。

[0124] 2) 对于步骤 A2

[0125] 智能融合模型的设计确定了分层结构的大小与架构，然后为分层结构提供感知数据来训练它。感知数据来自业务中的历史网络安全数据（在智能融合模型的初始形成阶段，该感知数据即为前述采集到的网络安全数据）。重要的是在分层中，有许多数据用来训练，而且数据是具有时间这一基本元素。在供应链信息流安全分析中，为了进行有效的学习，都需要在时间的流逝中观察一组模式。由此，步骤 A2 可具体执行为：

[0126] 步骤 C1：将特征集和攻击反馈数据集作为 HTM 算法的样本数据，输入给智能融合模型。

[0127] 其中，在一个实施例中，智能融合模型为 F 层，除最低层外其他层的各节点拥有 N 个子节点，其中，F 和 N 均大于等于 2。

[0128] 其中，需要说明的是，除底层外其他各层的节点的子节点的数目可以相同也可以不相同，可以视实际需要进行设定，本发明对此不做限定。

[0129] 步骤 C2：智能融合模型根据输入的样本数据进行学习，并形成与各层的节点对应的时序记忆模式。

[0130] 在智能融合模型中，当由高层到低层，节点数量指数级扩展时，可以有效实现大规模信息流的态势汇聚。如图 4 所示，可以构建 3 层 HTM 网络作为智能融合模型，每一层中每一个网格表示一个节点，每一个节点为一个特征描述区域。上层的一个节点对应下层的 4 个节点。该 HTM 网络中，每个节点的输入都是一组模式构成的时间序列，每一层都用于进行安全数据聚融，第 3 层的节点（即最高层的节点）用来实现最终的态势汇聚。具体的，在该 HTM 网络中，最低层（即第 1 层）用于接收样本数据（特征集和安全攻击反馈数据集），进行安全信息流处理。该样本数据还可以由第三方设备提供，如由安管设备提供安全特征值序列，可以通过多维向量引入安全特征值序列。对于每一层：第 1 层的各节点对输入的样本数据进行学习，形成并记忆样本数据之间的时序特征模式，然后将时序特征模式数据作为第二层的输入。第 2 层的各节点对时序特征模式进行分析，形成并记忆时序特征模式中稳定的特征，从而形成中间层模式（可以理解为第 2 层的实现特征模式），并将中间层模式作为第 3 层的输入。第 3 层为融合输出层，它基于大量已得到训练的中间层模式，将空间及时间变化特征一致的中间层模式归为一类，并可以统一输出网络安全态势感知结果，如对当前网络安全态势的评估结果和预测结果。

[0131] 例如，样本数据中包括入侵检测数据、防火墙数据和系统安全漏洞数据；除去量纲，保留影响因子，对该样本数据归一化处理后的结果为：入侵检测安全为 3，防火墙安全为 1，系统安全漏洞为 1，空间矩阵化为 [311]，该矩阵图示如图 5 所示。根据该空间矩阵获得 3*3 大小的特征矩阵作为信息流输入特征数据作为第 1 层的输入，对于图 4 中标识为 a 的节点，它的输入为一个“拐角形”特征的描述，如果该空间矩阵向右移动一帧，也就是在下一个时刻，该节点的输入对应的是一个变化后的“拐角形”；

[0132] 如：

[0133] $$[3\ \ 1\ \ 1]\rightarrow\begin{bmatrix}1&0&0\\1&0&0\\1&1&1\end{bmatrix}\rightarrow\left\{\begin{bmatrix}0&1&0&0\\0&1&0&0\\0&1&1&1\\0&0&0&0\end{bmatrix}\begin{bmatrix}0&0&0&0\\1&0&0&0\\1&0&0&0\\1&1&1&0\end{bmatrix}\right\}$$

[0134] 根据矩阵变换可以看出，在时序流逝的过程中，[3 1 1] 矩阵的拐角的特征模式不变，那么这些输入对于一个节点来说，就是一组模式构成的时间序列。对于样本数据，在第 1 层中各个节点进行学习，学习后的结果输入给下一层对应的节点，由下一层的节点对学习的结果进行汇聚。在图 4 所示的智能融合模型中，数据的输入在最底层，节点在每个网格里表示，顶层节点用例实现最终的态势汇聚。中间分层节点数可以指数级扩展，从而可以有效实现大规模信息流的态势汇聚。在图 4 中，输入的特征矩阵为 3*3 大小，每 4 个下层特征描述区域与上层一个节点对应，如第 2 层中的 c 节点对应第 1 层中的 4 个子节点。第 1 层中标记为 a 和 b 的节点分别对应信息流输入特征数据中标记分别为 A 和 B 的特征区域；第二层的 c 和 d 节点分别与信息流输入特征数据中的 C 和 D 区域对应。其中第 2 层的特征融合部分每个顶点下层的 4 个区域空间矩阵化特征向量的中心，完成模式的融合。

[0135] 综上，各层对应的模式是对该层的输入数据进行聚融的结果，该模式表征了对多个输入进行学习后，抽象出的鲁棒性高的特征。不同节点对其输入进行观察和学习后得到各自的模式。在同一层中，节点再把这些模式进行分组，那些属于同一事物的变体的模式属于同一组。对于第一层，变体的来源之一就是安全特征与预设的信息安全观测标准的相对偏离，另外一个就是随机噪声。当第一层的节点能够将对应于同一个源变体的模式分在一组，那么这个组就是这个变体的恒定体。就被认为是同一个安全特征的汇聚。一旦形成分组，节点就可以产生输出。其他层具有同样的道理，当节点能够对输入的模式进行分组形成恒定体，便可认为训练结束，可以产生输出。

[0136] 需要说明的是，当初步训练完智能融合模型后，在应用过程中智能融合模型还可以根据安全态势感知的结果不断的自适应学习和校正。

[0137] 至此，智能融合模型的构建已经完成，下面介绍一下网络安全态势感知阶段。

[0138] 二、网络安全态势感知

[0139] 网络安全态势感知包括将采集到的网络安全数据作为预先构建的智能融合模型的输入，对网络安全态势进行识别；

[0140] 对网络安全态势进行识别后，可以根据识别结果，对网络安全态势进行预测。下面对这两方面进行介绍：

[0141] 1) 网络安全态势识别

[0142] 其中，网络安全态势识别可执行为：

[0143] 步骤 D1：提取网络安全数据的时间序列作为一组输入模式，输入给智能融合模型。

[0144] 步骤 D2 :通过预先构建的智能融合模型,计算输入模式与智能融合模型的时序记忆模式的匹配概率,并将匹配概率大于预设阈值的时序记忆模式作为最终匹配的时序记忆模式,形成态势特征结果集,用于进行可视化。

[0145] 其中,比如来一个输入模式,如果它与哪个量化中心相似,其在对应的位就为 1,其它位为 0。比如输入模式与第 3 个量化中心最相似,则输出的结果为 [0,0,1,0,...0]。其中,1 表示与输入相似的量化中心的位置。但实际上,这个输出的向量不是非 0 即 1 的表示,而是在量化中心的空间上的一个概率分布,该概率分布说明输入模式与对应的量化中心的匹配程度,概率越大表明匹配程度越高,否则匹配程度越低。例如,依然以 3 层智能融合模型为例进行说明,步骤如下 :

[0146] 步骤 F1 :提取网络安全数据的时间序列作为一组输入模式,输入给预先构建的智能融合模型。

[0147] 步骤 F2 :智能融合模型的第 1 层计算输入模式与该层经学习训练后记忆的时序记忆模式之间的匹配概率。

[0148] 其中,步骤 F2 可执行为先计算输入模式与该层经学习训练后记忆的时序记忆模式之间的欧几里得距离,两者之间的欧几里得距离用 D_i 来表示,该计算公式如公式 (1) 所示 :

[0149] $$D_i = \sqrt{(x_1^2 - c_1^2) + (x_2^2 - c_2^2) + ... + (x_n^2 - c_n^2)} \quad (1)$$

[0150] 其中,x_1、x_2…x_n 分别表示输入模式,c_1、c_2…c_n,分别表示时序记忆模式,D_i 越大,说明输入模式距离记忆的模式越远,即输入模式与该记忆的模式的匹配程度就越小,一个输入模式与记忆的模式 i 的匹配概率正比于符合规则知识表达公式的值。因此,可假设一个输入模式属于记忆的时序记忆模式的概率符合欧几里得的高斯函数分布,如图 6 所示,其中,标记分别为 1、2、3 的曲线的标准偏差 σ 的平方依次分别为 0.2、1.0、5.0,上述三条曲线的期望值 μ 均为 0,标记为 4 的曲线的标准偏差 σ 的平方为 0.5,期望值 μ 为 -2。根据高斯函数可以计算出两者之间的匹配概率,其中,该高斯函数概率公式如公式 (2) 所示 :

[0151] $$F_{D_i} = \int_{-\infty}^{+\infty} \frac{1}{\sigma\sqrt{2\pi}} e^{\frac{(x-\mu)^2}{2\sigma^2}} \quad (2)$$

[0152] 其中,在公式 (2) 中,F_{D_i} 表示概率分布,σ 表示标准偏差,μ 表示期望值 ;e 表示自然常数 ;π 表示圆周率。

[0153] 步骤 F3 :第 1 层中各节点将计算得到的匹配概率,作为输入给智能融合模型的第 2 层中对应的节点。

[0154] 步骤 F4 :第 2 层重复执行步骤 A2,将产生的匹配概率作为输入给第 3 层。

[0155] 步骤 F5 :第 3 层重复执行步骤 A2,并将匹配概率大于预设阈值的时序记忆模式作为最终匹配的时序记忆模式,形成态势特征结果集。

[0156] 2) 网络安全态势预测

[0157] 智能融合模型的每一层在得出输入模式与记忆的时序记忆模式的匹配概率的同时,都在预测,因此成功训练智能融合模型后,智能融合模型便可以根据学习的结果自动进行预测。网络安全态势预测可执行为 :通过预先构建的智能融合模型,根据当前的网络安全

态势识别结果，预测预设时间段内网络安全态势的走向。

[0158] 三、网络安全态势可视化

[0159] 网络安全态势可视化主要包括两部分：一是匹配特征可视化精炼、二是匹配态势演化过程精炼，下面对这两部分进行说明：

[0160] 1) 匹配特征可视化精炼

[0161] 这个过程处理的主要目的是通过特征匹配来发现适合当前态势可视化表现的可视化片段。可执行为：将态势特征结果集中的时序记忆模式，与预先存储的时空数据片段进行特征匹配，得到用于进行可视化的可视化片段；然后，根据预先存储的时空数据片段对得到的可视化片段进行分类并建立索引，设计快速映射算法以便于将要展示的态势数据可视化出来。

[0162] 2) 匹配态势演化过程精炼：

[0163] 演化过程是个动态的概念，通过匹配特征可视化精炼可以迅速匹配映射某个确定点的态势可视化结果，但不能展示整个演化过程，所以还需要分析历史态势和推演空间来完成演化过程的精炼处理。

[0164] 匹配态势演化过程精炼具体可执行为：

[0165] 步骤 G1：记录每个可视化片段的特征点的空间，时间和主方向供可视化使用。

[0166] 步骤 G2：以主方向为起点，以特征点为中心，将特征向量空间划分为 p 个扇形区域 (p>1)。

[0167] 其中，在一个实施例中，将特征向量空间划分为 p 个等角度扇形区域。

[0168] 步骤 G3：以可视化片段的特征点所在时空位置为基点，划分时域推演区间为前后两个区间来明确历史态势和未来态势关系，将时空空间划分为 2p 个区间。

[0169] 步骤 G4：按时间先后顺序和预设的空间顺序对每个区间设好索引，建立起该特征点的特征和其他特征点的特征的时空编码关系，其中，时空编码关系是依据时间轴建立的安全特征变化数据集。

[0170] 其中，对每个区间设好索引用于表征每个区间的时空关系。

[0171] 其中，时空编码用于描述特征点之间的时空关系。

[0172] 步骤 G5：根据时空编码关系生成分别与可视化片段和时空片段对应的时空检验矩阵 M_V 和 M_C，然后将 M_V 和 M_C 进行异或运算，得到异或矩阵 D_{VC}，并分析异或矩阵 D_{VC} 中的非零元素所在的行和列，从而剔除掉错误的匹配。

[0173] 步骤 G6：用直方图相似选优算法做出相似性判断，输出匹配结果。

[0174] 如图 7 所示，为匹配特征可视化精炼的示意图：根据这种可视化映射，生成分别与可视化片段 V 和态势特征结果集对应的时空检验矩阵 M_V 和 M_C。其中，以可视化片段索引为行，时空片段索引为列，构建二维可视化时空校验矩阵。该时空校验矩阵中元素的个数为对应匹配特征的个数，例如可视化片段 V 的时空校验矩阵 M_V 中元素的个数为，属于 V 的与时空片段匹配的特征的个数。其中，时空检验矩阵的任一元素 Mi_j 表示可视化片段中的元素 x_j 相对于可视化片段中的元素 xi 的时空关系编码，即以 xi 为中心将空间划分为 2_p 个区间，x_j 的编码由其所在区间的索引来确定。

[0175] 下面是一个可视化片段与态势特征结果集进行匹配运算的例子：每个特征点将空间域划分为 4 个区间如图 8 所示。对应的时空校验矩阵 M_V 和 M_C 分别计算出来，其中，

[0176] $$M_v=\begin{bmatrix}2&0&1&3\\3&2&1&2\\2&1&3&2\\1&2&2&0\end{bmatrix}$$

[0177] $$M_c=\begin{bmatrix}2&3&1&3\\1&2&2&1\\2&2&3&2\\1&1&2&0\end{bmatrix}$$

[0178] 然后将 M_V 和 M_C 进行异或运算，得到异或矩阵 D_{VC}，

[0179] $$D_{vc}=XOR(M_V,M_c)=\begin{bmatrix}0&1&1&0\\1&0&1&1\\0&1&0&0\\0&1&0&0\end{bmatrix}$$

[0180] 通过分析 D_{VC} 中非零元素所在的行和列，可以剔除错误的匹配元素，该错误的匹配元素如最大值元素，如在三个匹配原素 [1 0 1 1]、[0 1 1 0]、[0 1 0 0] 中，剔除最大值 [1 0 1 1]，保留 [0 1 1 0]，[0 1 0 0]。

[0181] 在态势推演时，上述匹配运算将连续进行，即加入了时间轴。同时时空匹配空间也划分为 8 个区间。当匹配运算很多时，剔除错误匹配会复杂些，所以需要找出几个特征点作为参考，再进行矩阵的检测，剔除就会加速。

[0182] 综上，通过本发明实施例提供的网络安全态势感知方法，实现智能数据聚融，在不完整的数据呈现中，记忆模式能够被学习并识别出来。通过组合模式学习的记忆与当前的输入，HTM 网络能够预测下一步可能发生什么，可以更准确、全面地进行网络安全态势感知。针对泛在网络中信息流安全多特征存在互补的特性，可以进行多角度的学习；从多个层次、多个角度对网络的安全态势进行分析，采用定量分析和定性描述相结合的方法，保证评估结果系统而全面。此外，本发明在安全态势评估的基础上，采用可视化片段与态势特征匹配方法，对感知数据进行进一步优化处理，完成匹配特征可视化精炼和匹配态势演化过程精炼。这对于动态预测网络系统安全态势变化趋势非常有帮助，使得态势数据集直观迅速的展示，有助于提高网络系统安全响应效率。

[0183] 实施例二

[0184] 基于上述网络安全态势感知系统和方法，如图 9 所示为本发明实施例中网络安全态势感知框架示意图，该框架构建在对供应链应用情景中多层次异构安全数据的基础上，从感知的层次上由低向高划分为指标提取、特征评估、态势汇聚三个部分。下面结合该框架对本发明中网络安全态势感知方法进行说明：

[0185] 1) 首先对网络安全数据利用现有技术进行采集，得到应用层、网络传输层以及物理层面的数据，作为后面处理的对象。

[0186] 其中应用层安全数据可以包括云计算登陆认证种类及安全等级，供应链信息应用集成安全信息，web service 安全，解析服务安全数据等信息利用环节，企业中间件涉及的安全数据也纳入到这一部分；对于涉及泛在网络环境的网络安全数据可以通过网关和安管

设备如防火墙、IDS 等获得，网络环境包括移动通信网、计算机网络、无线网络等；物理层的安全数据主要涉及到物联网的传感节点，可从传感器网关获得。

[0187] 2) 对每个层面的网络安全数据信息，提取时空关联特征，得到多层面的局部时空对象的特征表述。

[0188] 3) 然后对这些特征信息进行评估筛选，摒弃权重弱化的特征，保留抗数据污染强的鲁棒特征。在特征评估筛选过程中，对特征样本进行预设定的攻击，得到特征集和安全攻击反馈数据集，一并作为后面智能融合模型的样本数据；

[0189] 4) 通过基于 HTM 的鲁棒态势汇聚方法，确定智能融合模型的分层结构，将样本数据转化为分层结构感知数据，并训练它。结合多层面信息安全特征表达的互补优势，利用基于半监督学习的 HTM 鲁棒态势汇聚器，完成样本数据在空间阶段和时间阶段的学习，同时得到 HTM 量化中心数据描述集，存储到安全态势知识库并构建推理索引。

[0190] 5) 对于态势感知结果，根据指定时间节点或一段时间段进行基于时空检验矩阵运算，对错误的虚警匹配删除，精练后的结果将可视化展现；

[0191] 6) 同时态势感知的时空检验矩阵参数可作为学习训练各级信息处理层的负反馈输入，一方面保证态势感知体系在受到突发事件重创时能自行修复，恢复态势数据的上行通畅，增加系统整体鲁棒性，另一方面，给智能融合模型提供更多的学习数据，使 HTM 量化中心数据集更加贴近实际。

[0192] 综上，该框架有以下特点：

[0193] 1) 对于数据信息的处理可以在线也可以离线，虽然在特征提取时会涉及到一些计算量较大的操作，但兼容离线方式，使得系统响应并不受学习影响。

[0194] 2) 数据在感知层次上逐级提炼，在保留信息安全特征同时并不形成数据的爆炸，极适应不断增长的大规模数据集的需求。

[0195] 3) 在数据信息、特征信息、态势信息、特征筛选、可视化处理等方面，都强调数据的时空关系，有助于形成安全态势推演，理解供应链信息风险演化。

[0196] 本领域内的技术人员应明白，本发明的实施例可提供为方法、系统、或计算机程序产品。因此，本发明可采用完全硬件实施例、完全软件实施例、或结合软件和硬件方面的实施例的形式。而且，本发明可采用在一个或多个其中包含有计算机可用程序代码的计算机可用存储介质（包括但不限于磁盘存储器、CD-ROM、光学存储器等）上实施的计算机程序产品的形式。

[0197] 本发明是参照根据本发明实施例的方法、设备（系统）、和计算机程序产品的流程图和/或方框图来描述的。应理解可由计算机程序指令实现流程图和/或方框图中的每一流程和/或方框、以及流程图和/或方框图中的流程和/或方框的结合。可提供这些计算机程序指令到通用计算机、专用计算机、嵌入式处理机或其他可编程数据处理设备的处理器以产生一个机器，使得通过计算机或其他可编程数据处理设备的处理器执行的指令产生用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的装置。

[0198] 这些计算机程序指令也可存储在能引导计算机或其他可编程数据处理设备以特定方式工作的计算机可读存储器中，使得存储在该计算机可读存储器中的指令产生包括指令装置的制造品，该指令装置实现在流程图一个流程或多个流程和/或方框图一个方框或

多个方框中指定的功能。

[0199] 这些计算机程序指令也可装载到计算机或其他可编程数据处理设备上，使得在计算机或其他可编程设备上执行一系列操作步骤以产生计算机实现的处理，从而在计算机或其他可编程设备上执行的指令提供用于实现在流程图一个流程或多个流程和 / 或方框图一个方框或多个方框中指定的功能的步骤。

[0200] 尽管已描述了本发明的优选实施例，但本领域内的技术人员一旦得知了基本创造性概念，则可对这些实施例作出另外的变更和修改。所以，所附权利要求意欲解释为包括优选实施例以及落入本发明范围的所有变更和修改。

[0201] 显然，本领域的技术人员可以对本发明进行各种改动和变型而不脱离本发明的精神和范围。这样，倘若本发明的这些修改和变型属于本发明权利要求及其等同技术的范围之内，则本发明也意图包含这些改动和变型在内。

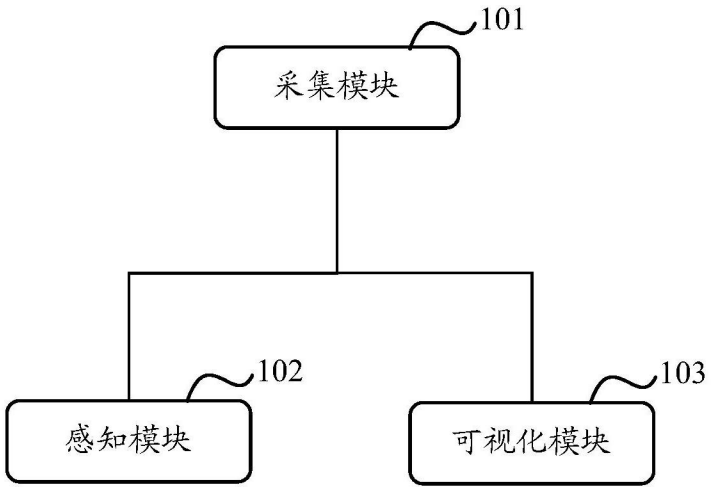


图 1

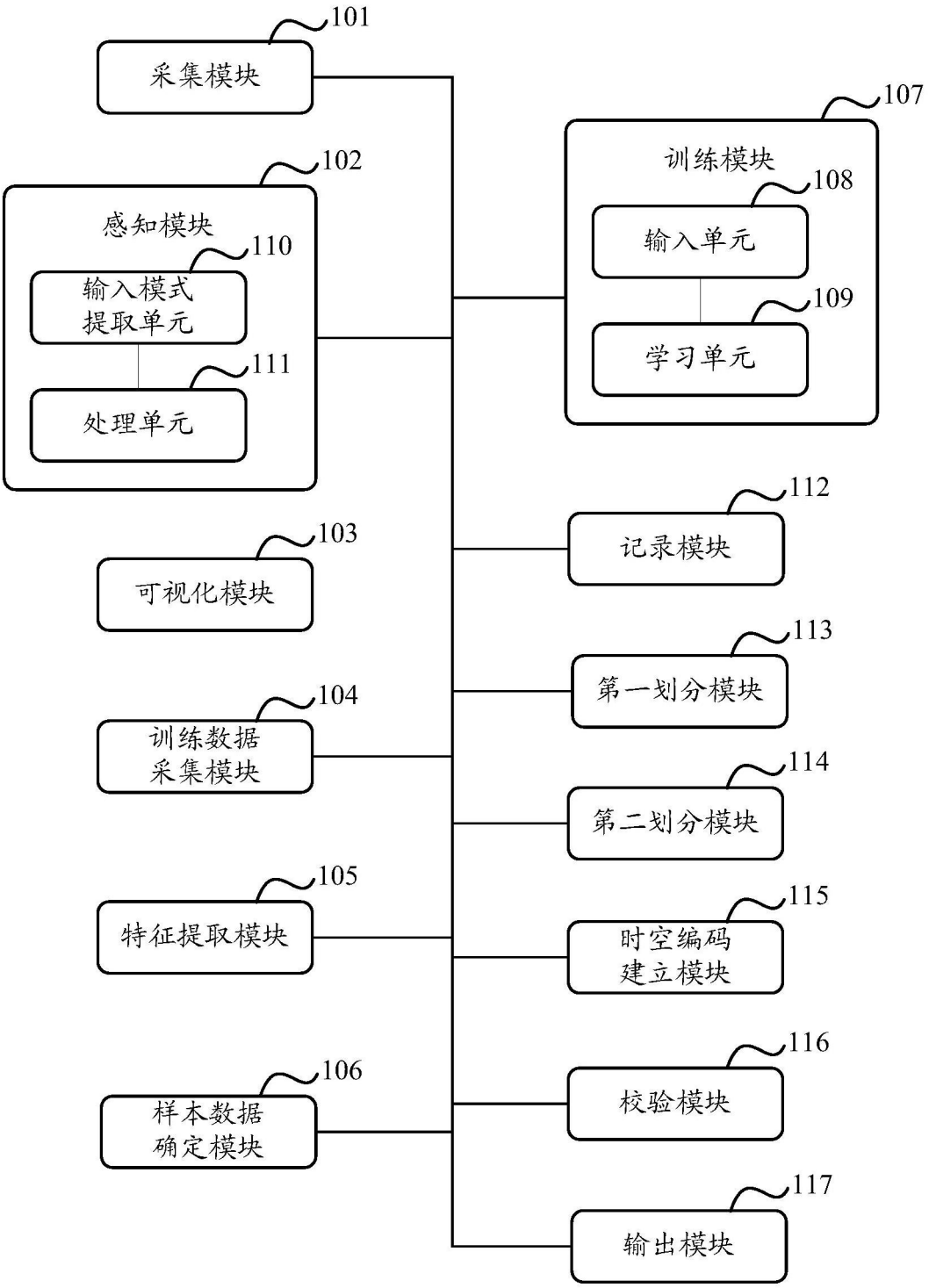

101
采集模块
102
感知模块
110
输入模式
提取单元
111
处理单元
103
可视化模块
104
训练数据
采集模块
105
特征提取模块
106
样本数据
确定模块
107
训练模块
108
输入单元
109
学习单元
112
记录模块
113
第一划分模块
114
第二划分模块
115
时空编码
建立模块
116
校验模块
117
输出模块

图 2

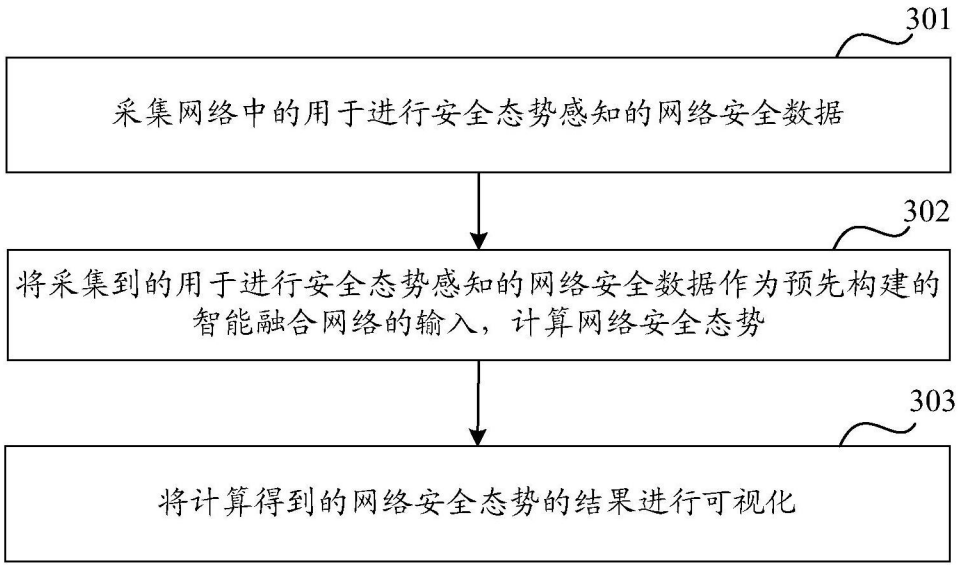

301
采集网络中的用于进行安全态势感知的网络安全数据
302
将采集到的用于进行安全态势感知的网络安全数据作为预先构建的智能融合网络的输入，计算网络安全态势
303
将计算得到的网络安全态势的结果进行可视化

图 3

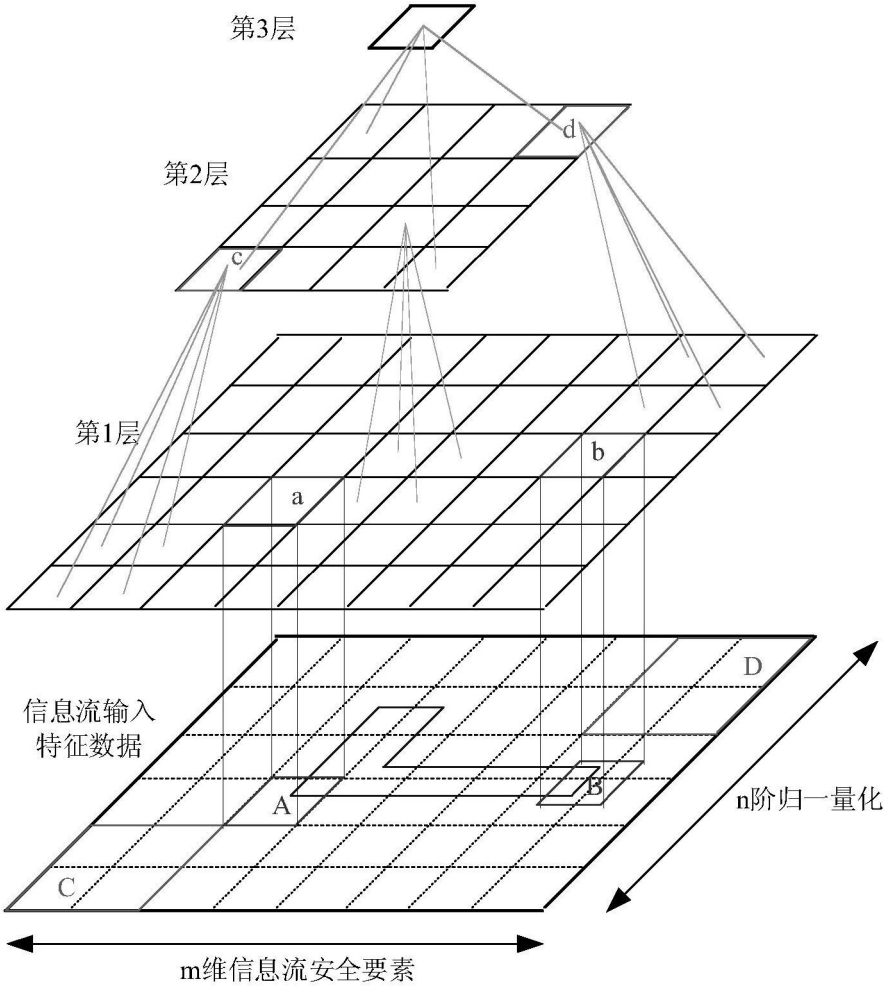

第3层
第2层
第1层
d
c
b
a
信息流输入
特征数据
D
B
A
C
n阶归一量化
m维信息流安全要素

图 4

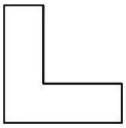


图 5

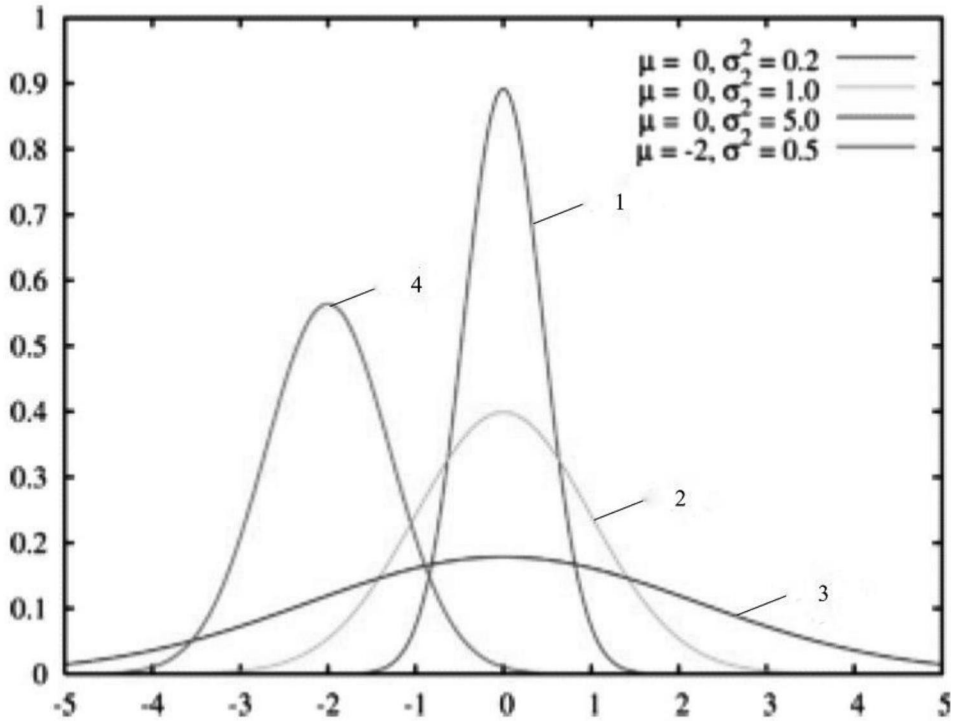

μ = 0, σ² = 0.2
μ = 0, σ² = 1.0
μ = 0, σ² = 5.0
μ = -2, σ² = 0.5
1
2
3
4

图 6

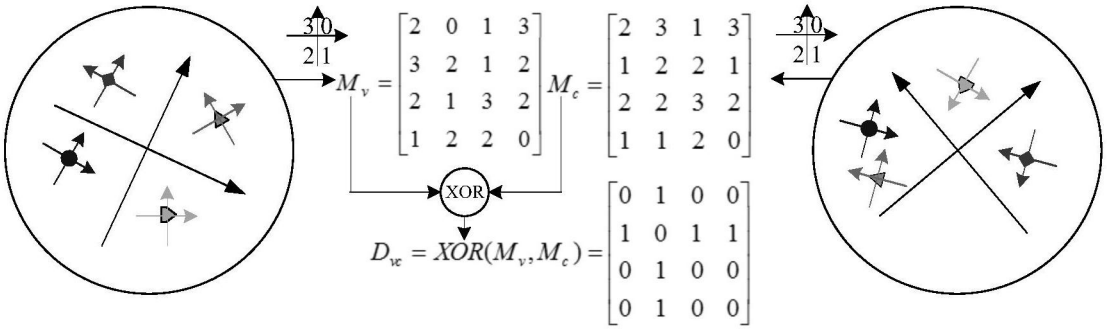

3 0
2 1
$M_v = \begin{bmatrix} 2 & 0 & 1 & 3 \\ 3 & 2 & 1 & 2 \\ 2 & 1 & 3 & 2 \\ 1 & 2 & 2 & 0 \end{bmatrix}$
$M_c = \begin{bmatrix} 2 & 3 & 1 & 3 \\ 1 & 2 & 2 & 1 \\ 2 & 2 & 3 & 2 \\ 1 & 1 & 2 & 0 \end{bmatrix}$
XOR
$D_{vc} = XOR(M_v, M_c) = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}$
3 0
2 1

图 7


3 0
2 1

图 8

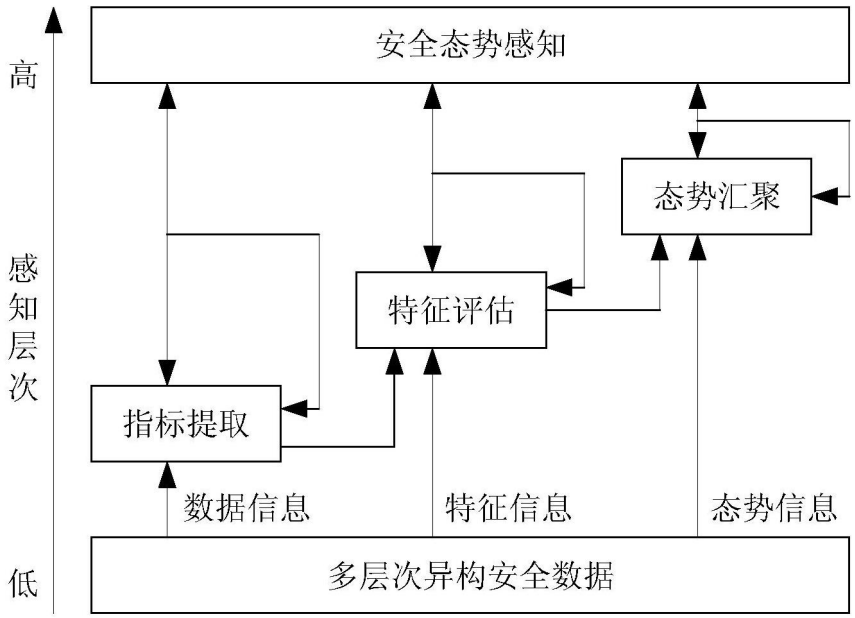


图 9