Beijing Forest Studio

北京理工大学信息系统及安全对抗实验中心

网络安全态势感知综述

硕士研究生　杨若晗

2020年04月19日

内容提要

- 背景简介
- 基本概念
- 算法原理及优劣分析
- 应用总结
- 参考文献

背景简介

- 预期收获
  - 1. 了解网络安全态势感知概念
  - 2. 了解网络安全态势感知经典模型及算法
  - 3. 了解网络安全态势感知的应用及发展方向

背景简介

- 网络安全的重要性
  - **“没有网络安全就没有国家安全”——习近平**
  - 网络安全是一个关系国家安全和主权、社会的稳定、民族文化的继承和发扬的重要问题。其重要性，正随着全球信息化步伐的加快而变到愈发重要。

- 网络安全发展的四个阶段

序号	时间区间	阶段	主旨思想
1	1960 年以前	设计保证	建立一个绝对安全的系统,保证攻击不会发生
2	1970 ~1980 年代	入侵检测	构建一个安全辅助系统,攻击发生时能检测到,并采取措施
3	1990 年代	主动防御	不只是被动防御,进行主动评价,在攻击发生之前制定防御策略
4	2000 年以后	态势感知	感知时间和空间环境中的元素,把握网络整体安全状况及预测未来变化趋势

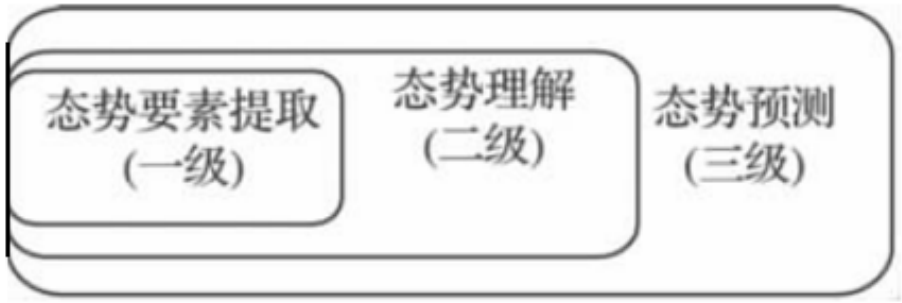
背景简介

- 网络安全态势感知的背景
  - 随着网络的飞速发展，安全问题日益突出，虽然已经采取了各种网络安全防护措施，但是单一的安全防护措施没有综合考虑各种防护措施之间的关联性，无法满足从宏观角度评估网络安全性的需求，网络安全态势感知的研究就是在这种背景下产生的。它在融合各种网络安全要素的基础上从宏观的角度实时评估网络的安全态势，并在一定条件下对网络安全态势的发展趋势进行预测。
  - 2016年4月19日，习近平总书记在网络安全和信息化工作座谈会上提出要“全天候全方位感知网络安全态势”。

基本概念

基本概念

- 态势感知
  - 起源：态势感知（Situation Awareness）这一概念源于航天飞行的人因（Human Factors）研究，此后在军事战场、核反应控制、空中交通监管（Air Traffic Control, ATC）以及医疗应急调度等领域被广泛地研究。
  - 首次提出：1988 年，Endsley 首次明确提出态势感知的定义，态势感知是指“在一定的时空范围内，认知、理解环境因素，并且对未来的发展趋势进行预测“，并给出了概念模型。



基本概念

- 网络安全态势感知
  - 首次提出：1999年， Tim Bass 首次提出了网络态势感知（Cyberspace Situation Awareness）这个概念，并且提出了基于多传感器数据融合的网络态势感知功能模型。
  - 概念：大规模网络环境中，对能够引起网络安全状况发生变化的安全要素进行获取、分析、可视化，并预测发展趋势，为决策和后续处置提供依据。

算法原理及优劣分析

算法原理——态势要素提取（一级）

- 态势要素提取（一级）
  - 提取单一要素

    通过提取某种角度的态势要素来评估网络的安全态势。如：网络的脆弱性信息、警报信息、利用 honeynet 采的数据信息等。

    ？数据源单一且不能应对多源攻击

  - 提取多源要素

    从态势要素集合中挑选出所需要素集合的过程。即通过对态势要素集合中属性的约简降低态势要素集合维度，删除重复多余的属性，选择出关键的态势要素。
    - PCA（主成分分析法）
    - SVD（奇异值分解法）
    - RS（粗糙集）： PRAMAI

算法原理——态势要素提取（一级）

– 提取多源要素

• PRAMAI

T	对原始态势要素集合中属性进行高效约简
I	原始态势数据

P	For {
	1. 求态势要素信息系统的核属性B
	2. 求态势要素信息系统的次优约简属性P
	3. 求态势要素信息系统的最优约简V
	}

O	最优约简属性集合

算法原理——态势要素提取（一级）

- 提取多源要素
  - PRAMAI
  - 算法基本步骤
    - 描述：在经典粗糙集基础上引入并行约简思想，在保证分类不受影响的情况下，将单个决策信息表扩展到多个，利用条件熵计算属性重要度，根据约简规则删除冗余属性，从而实现网络安全态势要素的高效提取。
    - 概念解释：
      - » 态势要素信息决策系统T：T=(U，R，V，f)
        - U：表示态势要素的样本集合
        - R：表示态势要素属性集合，R=C∪D。（C为特征属性集合；D为决策属性集）
        - V：表示属性的值域
        - f：　U*R→V表示信息函数，它指定U中每一个对象x的属性值
      - » 核属性：对于态势要素信息的决策系统T，包含态势要素特征属性集合C相对于决策属性D的全部必要特征属性组成的集合称为C相对于D的核，表示为$CORE_D(C)$

算法原理——态势要素提取（一级）

- 提取多源要素
  - PRAMAI
  - 算法基本步骤
    - 概念解释：
      - » 属性重要度矩阵：态势要素信息的决策系统T=(U， C ∪ D)，P(T)表示T的所有子表，F ⊆ P(T)，特征属性子集A⊆C，A关于F的相对于D的属性重要度矩阵为：

$$M(A,D,F)=\begin{bmatrix}\sigma_{11} & \sigma_{12} & \cdots & \sigma_{1m}\\ \sigma_{21} & \sigma_{22} & \cdots & \sigma_{2m}\\ \vdots & \vdots & & \vdots\\ \sigma_{n1} & \sigma_{n2} & \cdots & \sigma_{nm}\end{bmatrix} \qquad M'(A,D,F)=\begin{bmatrix}\sigma'_{11} & \sigma'_{12} & \cdots & \sigma'_{1m}\\ \sigma'_{21} & \sigma'_{22} & \cdots & \sigma'_{2m}\\ \vdots & \vdots & & \vdots\\ \sigma'_{n1} & \sigma'_{n2} & \cdots & \sigma'_{nm}\end{bmatrix}$$

其中：$\sigma_{ij}=\sigma(a_j,U_i)=G_i(A;D)-G_i(A-\{a_j\};D),\quad a_j\in B,\ (U_i,C,D)\in F$

$\sigma'_{ij}=\sigma'(a_j,U_i)=G_i(A\cup\{a_j\};D)-G_i(A;D),\quad a_j\in B,\ (U_i,C,D)\in F$

F中子决策表的个数为n，T中属性的个数为m。

算法原理——态势要素提取（一级）

- 提取多源要素
  - PRAMAI
  - 算法基本步骤
    - 步骤一：根据态势要素特征属性集合C建立属性重要度矩阵M(C，D，F)计算并行约简的核属性B；
    - 步骤二：计算矩阵M’(B，D，F)，并将M’(B，D，F)中不为0元素个数最多的列对应的特征属性加入到核属性B中形成属性集合P，重复以上步骤，直到M’(B，D，F)中的元素均为0，此时集合P为次优约简结果；
    - 步骤三：依次删除次优约简集合P中的每个属性并计算删除属性后的条件熵，如果仍等于G(D| P)，则删除该属性，重复此步骤直到遍历次优约简集合P中的每一个属性，此时得到的属性集合即为最优约简集合，即所求的必要的特征属性集合。

算法原理——态势要素提取（一级）

- 提取多源要素
  - PRAMAI
  - 算法执行结果
    - 数据集：NSL—KDD数据集，包含41个条件属性和1个标签属性。标签属性为：Probe、DoS、U2R、R2L、Normal。
    - 结果分析：约简后的数据集合在分类性能上更优越，并且对于攻击类型的检测上耗时少、准确率高，这说明该算法可以有效去除冗余属性，提高分类性能。

评价指标	类别	全部属性	约简后属性
召回率	Normal	0.599	0.588
	Probe	0.780	0.816
	DoS	0.981	0.991
	U2R	0.900	0.900
	R2L	0.898	0.905
	Weighted Avg.	0.850	0.858
误警率	Normal	0.027	0.021
	Probe	0.006	0.004
	DoS	0.172	0.169
	U2R	0.000	0.000
	R2L	0.014	0.014
	Weighted Avg.	0.069	0.067
分类建模时间/s		35.57	29.66

算法原理——态势理解（二级）

- 态势理解（二级）
  - 基于数学模型

？前提是确定的数据源，
无法处理不确定性信息

综合考虑影响态势的各项态势因素，构造评定函数，建立态势因素集合R到态势空间θ的映射关系进行 态势评估。$\theta = f(r_1, r_2, \ldots, r_n)$，$r_i \in R(1 \le i \le n)$ 为态势因素。

常用方法：权重分析法、集成分析法

？先验知识的获取
存在一定的困难

  - 基于概率统计

充分利用先验知识的统计特性，结合信息的不确定性，建立态势评估的模型，然后通过模型评估网络的安全态势。

常用方法：贝叶斯网络、隐马尔可夫模型（HMM）

算法原理——态势理解（二级）

- 态势理解（二级）
  - 基于知识推理

？当证据出现冲突时，准确性会受到影响

首先模糊量化多源多属性信息的不确定性，然后利用规则进行逻辑推理，实现网络安全态势的评估。

常用方法：基于图模型的推理（模糊认知图等）、基于证据理论的推理（D-S 证据推理等）

？在模式抽取阶段，面对较为复杂的特征比较棘手；原理难以描述，难以从整体角度考虑识别问题

  - 基于模式识别

通过机器学习建立态势模型，经过模式匹配及映射，完成对态势的划分。其目标是不过分依赖专家和经验，自动获取知识，建立科学、客观的评估模型。

常用方法：灰关联法、粗集理论、聚类分析法

算法原理——态势理解（二级）

- 基于模式识别
  - 基于攻击模式识别的网络安全态势评估方法

T	根据网络中的报警数据对当前整个网络的安全态势进行评估
I	网络中的报警数据

P	For {
	1.对网络中的报警数据进行因果分析
	2.以攻击阶段为要素进行态势评估
	}

O	当前整个网络的安全态势

算法原理——态势理解（二级）

- 基于知识推理
  - 基于攻击模式识别的网络安全态势评估方法
  - 算法基本步骤
    - 描述：先对网络中的多源数据进行信息融合，对融合后的结果进行因果分析，识别出攻击意图与当前的攻击阶段，并将攻击阶段作为态势要素进行节点评估。
    - 概念解释：
      - » 攻击发生概率：指将多个网络检测设备的报警数据进行信息融合，得到的某种攻击已经发生的可能性，以m(h)表示。
      - » 攻击阶段支持概率：指已发生攻击在整个攻击意图中所处的某个阶段状态的可能性，以s(h)表示。
      - » 攻击阶段转移概率：指攻击从目前所处的阶段转移到攻击意图中的下一个阶段的可能性，以ns(h)表示。
      - » 攻击威胁：指攻击所处的阶段状态所带来的影响，是专家对攻击破坏性的评估打分，以f(h)表示。

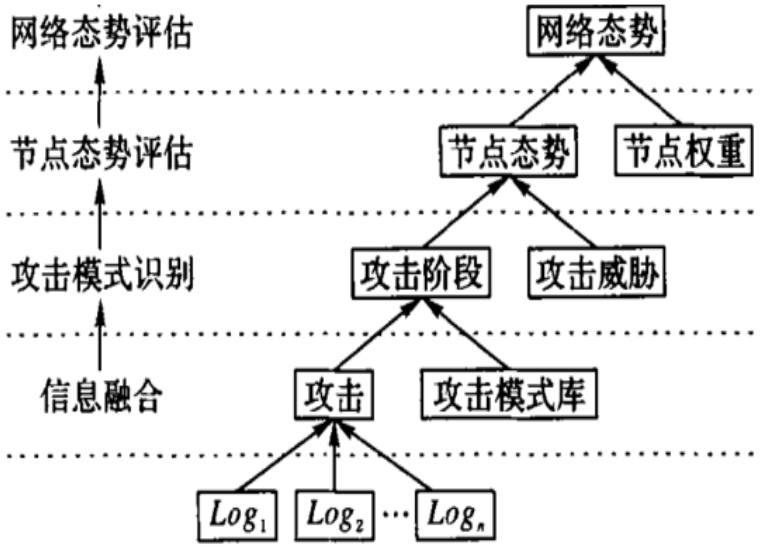
算法原理——态势理解（二级）

- 基于知识推理
  - 基于攻击模式识别的网络安全态势评估方法
  - 算法基本步骤
    - 概念解释：
      - » 报警信息Log：包括入侵检测系统、防火墙、系统日志等传感器检测到的报警日志。

        Log=（$id, time, type, content, id_s, id_d$）
      - » 融合后的安全事件Alert=（$id, time$, Sip, Dip, $Sport, Dport, AttackType$）
      - » 网络攻击模式AttackPattern $= (s_i, s_j)$
      - » 主机信息$hostInf = (HostIp, Services, SoftV, Vuls, Weight)$

算法原理——态势理解（二级）

- 基于知识推理
  - 基于攻击模式识别的网络安全态势评估方法
  - 算法基本步骤
    - 步骤一：信息融合。对网络中的多源报警数据进行信息融合，以减弱数据的冗余与误报，得到更加准确的攻击发生概率m(h)；
    - 步骤二：攻击阶段识别。对已经发生的攻击进行关联分析，得到攻击阶段支持概率s（h）；
    - 步骤三：节点态势评估。根据攻击阶段与其相对应的攻击威胁，计算节点的安全态势；
    - 步骤四：网络整体态势评估。将节点态势依据其权重进行融合，得到网络的安全态势。



算法原理——态势理解（二级）

- 基于知识推理
  - 基于攻击模式识别的网络安全态势评估方法
  - 算法具体步骤解析
    - 信息融合
      - » 预处理：对数据进行清洗，通过设置过滤规则，将不符合规范的数据过滤掉。如字段缺省、参数错误、超出设定范围；
      - » 格式统一化：对多源异构数据进行格式统一化，转化为通用的可扩展标记语言公共数据模型；
      - » 聚类：将在属性上重复或相似的多条报警聚合成同一条报警；
      - » 融合：统计传感器得到的报警信息Log，与该传感器对相应攻击的检测率w_h，然后将各传感器的报警信息经过D-s（Dempster—Shafer）证据理论合成，得到更加精确的攻击发生概率m（h）。

算法原理——态势理解（二级）

- 基于知识推理
  - 基于攻击模式识别的网络安全态势评估方法
  - 算法具体步骤解析
    - 攻击阶段识别：将每收到的一个报警信息与攻击模式库进行匹配，并将匹配的记录放到实时攻击场景中，并计算该报警与其在实时攻击场景中前提报警之间的攻击关联度，通过阈值判断是否对其剪枝。对通过阈值的安全事件，计算其攻击阶段支持概率s（h）。

攻击关联度：
$$cor(a,b) = \left[\sum_{k=1}^{n} \alpha_k Feature_k(a,b)\right] / \left[\sum_{k=1}^{n} \alpha_k\right]$$

阶段支持概率：
$$s(h) = \prod_{i=1}^{n} m(T_i) \cdot \prod_{i=1}^{n} cor(T_i, T_{i+1})$$

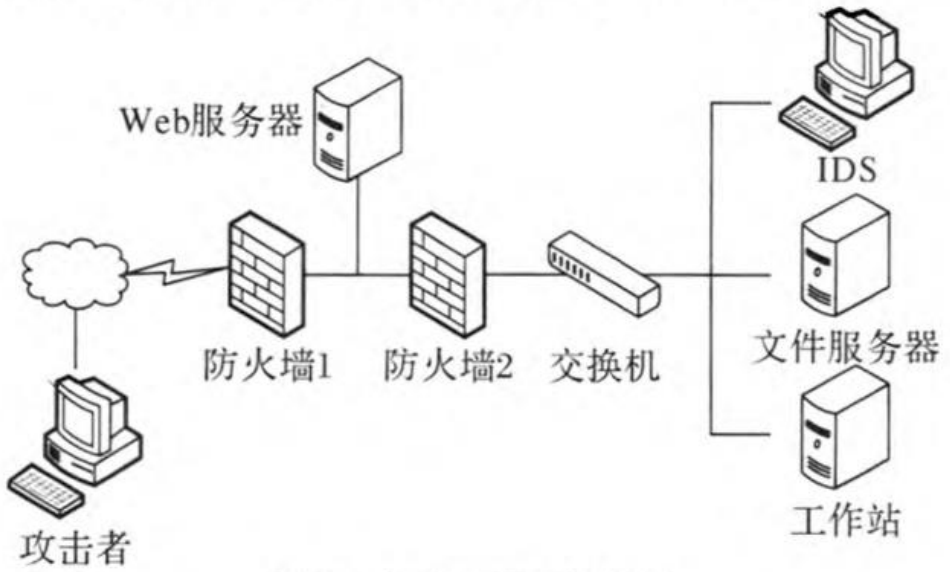
算法原理——态势理解（二级）

- 基于知识推理
  - 基于攻击模式识别的网络安全态势评估方法
  - 算法具体步骤解析
    - 网络安全态势评估量化
      - » 对接点态势进行评估：将攻击阶段支持概率s(h)结合该攻击阶段所对应的攻击威胁t(h)，得到该攻击阶段对节点态势的影响e=s(h)·t(h);若该接点在同一阶段受n个攻击，则 $SA = \sum_{i=1}^{n} e_i$
      - » 整个网络的安全态势NSA：

$$NSA = \sum_{i=1}^{n} SA_i \cdot w_i$$

算法原理——态势理解（二级）

- 基于知识推理
  - 基于攻击模式识别的网络安全态势评估方法
  - 算法执行结果
    - 实验环境



    - 实验过程：攻击者对该网络实施一次特洛伊木马攻击。设置web服务器、文件服务器、工作站的权重分别为0.2、0.3、0.5

算法原理——态势理解（二级）

- 基于知识推理
  - 基于攻击模式识别的网络安全态势评估方法
  - 算法执行结果
    - 结果分析
      - » 计算结果基本随着攻击阶段的深入逐渐增加，更具合理性
      - » 对权重越大的主机进行攻击，其对整体网络的影响就越大

攻击阶段	攻击发生概率	Web 服务器	文件服务器	工作站	*NSA*
A1_state1	0.907	0.036	0	0	0.0072
A1_state2	0.923	0.335	0	0	0.0670
A1_state3	0.874	0	0.366	0	0.1098
A1_state4	0.890	0	0.456	0	0.1368
A1_state5	0.848	0	0	0.442	0.2210

    - 改进方向：该算法依赖于已知的攻击模式，需加强对新型攻击场景还原的研究，进一步增强模型的通用性。

算法原理——态势预测（三级）

- 态势预测（三级）
  - 基于传统方法的预测

    时间序列预测：根据态势的时间序列的历史变化，对未来做出延展预测。但该方法缺乏对事物发展因果关系的联系，预测的精准性效果欠佳。

    因果关系预测：由若干变量的观测值来确定变量之间的依赖关系。

    经典方法：PSO-SVM

  ？利用简单的统计数据预测非线性过程随时间变化的趋势存在较多误差；对专家先验知识过于依赖

  ？模型参数、复杂性设计上还存在依赖于人工经验的问题

  - 基于神经网络的预测

    通过建立机器的自动感知和自学习机制，使其拟合专家的思维能力和分析判断能力，达到更加灵活地对复杂网络安全事件进行预测的目的。

    经典方法：BP、RBF（**PSO-RBF**）

算法原理——态势预测（三级）

– 基于神经网络的预测

- PSO-RBF

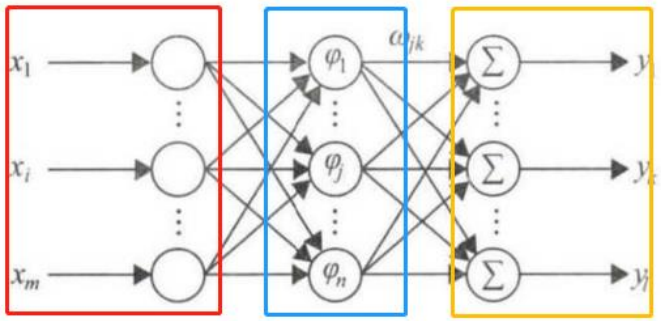
T	根据获取的历史和当前的态势值进行态势预测
I	网络安全态势值

P	For {
	通过权重因子的调节自动寻优，将搜寻到的全局最优值解码成RBF的网络参数；通过优化的RBF网络进行网络安全态势预测
	}

O	网络安全态势预测值

算法原理——态势预测（三级）

- 基于神经网络的预测
  - PSO-RBF
  - 算法基本步骤
    - 描述：首先，PSO的惯性权重因子按一条开口向左的抛物线递减，在保证全局寻优的同时增强了局部搜索能力；其次，通过权重因子的调节自动寻优，并将搜寻到的全局最优值解码成RBF的网络参数；最后，通过优化的RBF网络进行网络安全态势预测。
    - 概念解释：
      - » RBF（径向基神经网络）：是一种三层向前型神经网络，包含一个输入层、一个具有径向基函数神经元的隐含层、一个具有线性神经元的输出层。
        - 隐含层： 由若干径向基函数构成，作用是将输入空间中线性不可分的数据经激活函数进行非线性变换后映射到线性可分的空间，从而为输出层进一步分类做准备。

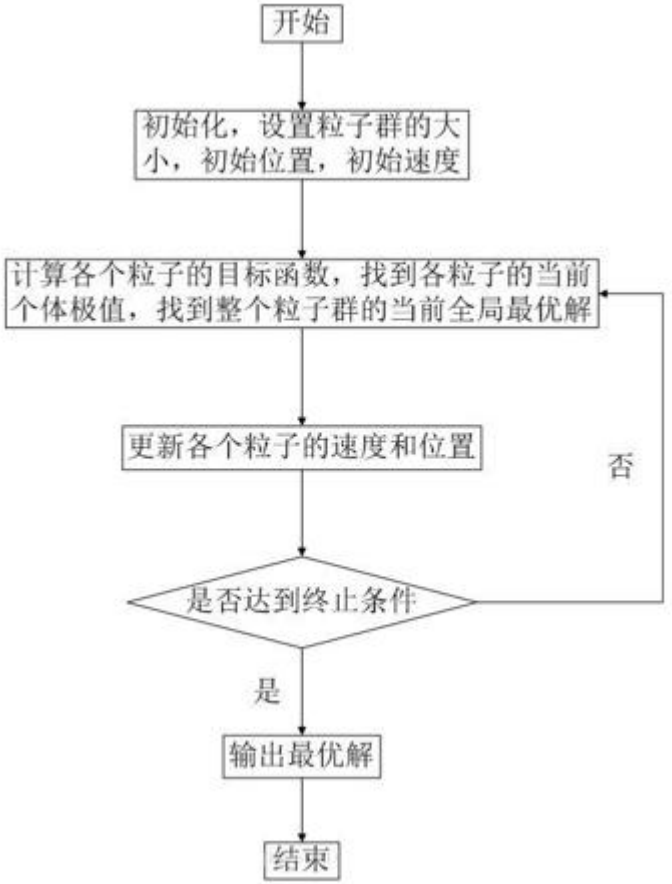


算法原理——态势预测（三级）

- 基于神经网络的预测
  - PSO-RBF
  - 算法基本步骤
    - 概念解释：
      - » PSO（粒子群优化算法）：本质是一种随机搜索算法，能以较大概率收敛于全局最优解。假设在一个D维的搜索空间中，有N个粒子组成一个群落：
        - 第i个粒子的位置表示为：$X_i = (x_{i1}, x_{i2}, \dots, x_{iD}), i = 1,2, \dots, N$
        - 第i个粒子的飞行速度：$V_i = (v_{i1}, v_{i2}, \dots, v_{iD}), i = 1,2, \dots, N$
        - 个体极值：$P_{best} = (p_{i1}, p_{i2}, \dots, p_{iD}), i = 1,2, \dots, N$
        - 全局极值：$g_{best} = (p_{g1}, p_{g2}, \dots, p_{iD}), i = 1,2, \dots, N$
        - **在搜索过程中粒子更新自己速度和位置的公式：**

          $v_{id} = \theta \times v_{id} + c_1 r_1 (p_{id} - x_{id}) + c_2 r_2 (p_{gd} - x_{id})$

          $x_{id} = x_{id} + v_{id}$
        - 改进的惯性权重因子：$\theta = f_{min} + (f_{max} - f_{min}) \sqrt{\frac{t_{max} - t}{t_{max}}}$

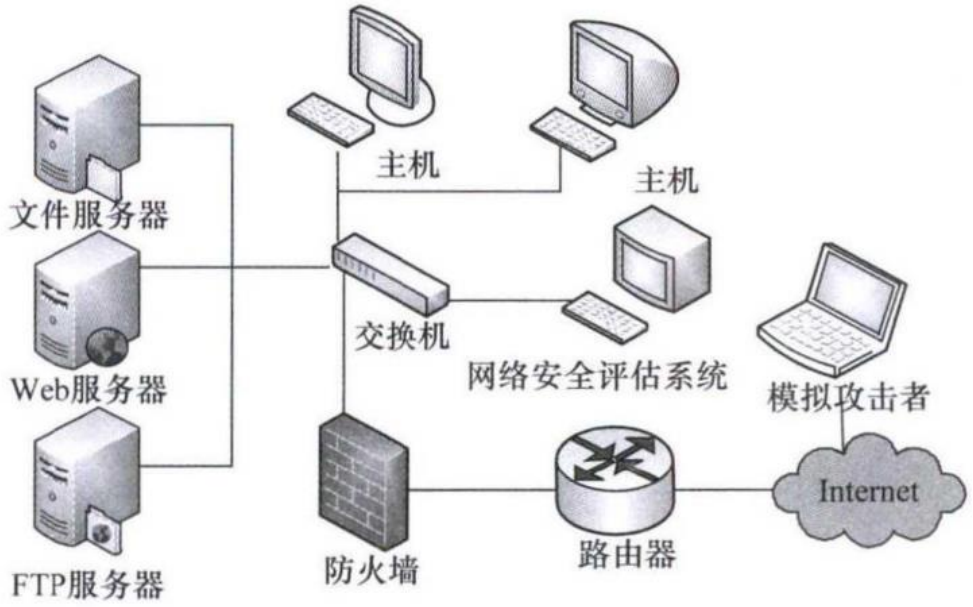


算法原理——态势预测（三级）

- 基于神经网络的预测
  - PSO-RBF
  - 算法基本步骤
    - 步骤一：对网络安全态势预测训练样本做归一化处理，对RBF网络参数进行编码，并初始化粒子群；
    - 步骤二：训练网络并计算适应度值，利用权重系数按横向抛物线递减的方法迭代寻优；
    - 步骤三：更新粒子群，并计算更新后的适应度值；
    - 步骤四：更新P_{best}和g_{best}；
    - 步骤五：判断是否达到迭代次数，如果达到，则进行下一步；如果没有达到，则转到步骤三；
    - 步骤六：获取最终的g_{best}值，并解码成RBF网络的权值；
    - 步骤七：测试样本归一化处理，用构建好的网络对测试样本进行分析，并输出结果；
    - 步骤八：输出数据反归一化处理结果，得到预测值。

算法原理——态势预测（三级）

- 基于神经网络的预测
  - PSO-RBF
  - 算法执行结果
    - 实验环境：



    - 实验过程：
      - » 每隔一段时间从网络安全评估系统里读取网络安全态势值，形成态势数据库；
      - » 通过前n个时间段的态势值预测下一个时间段的态势值。

算法原理——态势预测（三级）

- 基于神经网络的预测
  - PSO-RBF
  - 算法执行结果
    - 结果分析
      - » 通过与BP、RBF方法比较发现本算法在拟合度和准确性上都更优，且收敛速度也较快；
      - » N=5比n=3更优，说明用连续5个时间段的态势值预测下一个时间段的态势值更合适；

预测方式	算法	迭代次数	均方误差
$n=3$	改进 BP 算法	100	0.0023
	RBF 算法	50	0.0018
	本文算法	28	0.0010
$n=5$	改进 BP 算法	86	0.0012
	RBF 算法	48	0.0015
	本文算法	26	0.0008

    - 改进方向：调整RBF网络结构，结合更好的优化算法，使改进后的算法能处理大样本数据，适用于大规模的计算机网络。

应用总结

应用总结

- 应用领域
  - 因特网
    - 利用态势感知强大的全局监控能力，实时掌握网络的运行状态并采取对应的安全措施，保证网络系统的安全。
  - 工业网
    - 利用态势感知对工控系统的整体运行情况进行有效地监测和控制，从而保证工控系统的安全运行。
  - 物联网
    - 利用态势感知的应急响应和预测能力，为物联网的安全问题保驾护航。
    - 车联网

应用总结

- 未来的发展
  - 数据融合。面对海量流式安全数据的集中或分布式存储，快速融合的手段对于态势精准分析则显得尤为重要。
  - 人工智能应用。借助人工智能技术提升网络安全态势感知每个环节的能力是研究领域的大趋势。
  - 可视化与人机交互。准确、实时、全方位展示态势感知的各个阶段；增强人机交互性。
  - “反态势感知”。指利用态势感知系统的弱点或缺陷来进行攻击和破坏，或者直接采用其他技术对态势感知的不同阶段进行破坏和干扰。

参考文献

[1]Theureau J. Use of nuclear-reactor control room simulators in research & development. In:7th IFAC /IFIP /IFORS /IEA Symposium on Analysis, Design and Evaluation of MAN-MACHINE SYSTEMS , Kyoto. 1998. 425 ~ 430

[2] Endsley M R. Design and evaluation for situation awareness enhancement. Paper presented at the Human Factors Society 32nd Annual Meeting. Santa Monica, CA , 1988

[3] Bass T. Multisensor data fusion for next generation distributed intrusion detection systems[A]. Proceedings of the Iris National Symposium on Sensor &Data Fusion[C]. US: Hop

[4]赵冬梅, 李红. 基于并行约简的网络安全态势要素提取方法[J].计算机应用, 2017,37(4):1008-1013.

[5]王坤, 邱辉, 杨豪璞. 基于攻击模式识别的网络安全态势评估方法[J]. 计算机应用, 2016,36(1):194-198，226.

[6]江洋，李成海，魏晓辉，等. 改进PSO优化RBF的网络安全态势预测研究[J].测控技术，2018,37(5):56-60.

道德经

上善若水。水善利万物而不争，处众人之所恶，故几於道。居善地，心善渊与善仁，言善信，正善治，事善能，动善时。夫唯不争，故无尤。