本文节选自《这就是搜索引擎：核心技术详解》第八章

如上所述，目前搜索引擎作弊手段五花八门，层出不穷，作为应对方的搜索引擎，也相应调整技术思路，不断有针对性地提出反作弊的技术方案，所以如果整理反作弊技术方案，会发现技术方法很多，理清思路不易。

尽管如此，如果对大多数反作弊技术深入分析，会发现在整体技术思路上还是有规律可循。从基本的思路角度，可以将反作弊手段大致划分为以下三种："信任传播模型"、"不信任传播模型"和"异常发现模型"。其中前两种技术模型可以进一步抽象归纳为"链接分析"一章提到的"子集传播模型"，为了简化说明，此处不再敷述，而是直接将这两个子模型列出。将具体**算法**和这几个模型建立起关系，有助于对反作弊算法的宏观思路和相互联系树立起清晰的概念。

8.5.1信任传播模型

图8-6展示了"信任传播模型"的示意图。所谓"信任传播模型"，基本思路如下：在海量的网页数据中，通过一定技术手段或者人工半人工手段，从中筛选出部分完全值得信任的页面，也即肯定不会作弊的页面（可以理解为白名单），算法以这些白名单内的页面作为出发点，赋予白名单内的页面节点较高的信任度分值，其它页面是否作弊，要根据其和白名单内节点的链接关系来确定。白名单内节点通过链接关系将信任度分值向外扩散传播，如果某个节点最后得到的信任度分值高于一定阈值，则认为没有问题，而低于这一阈值的网页则会被认为是作弊网页。

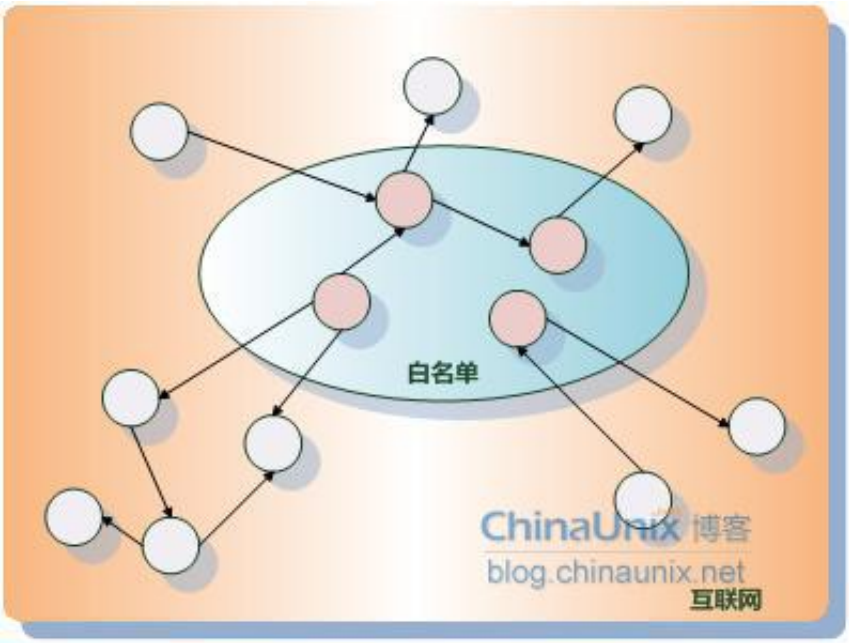

图8-6 信任传播模型

很多算法在整体流程和算法框架上遵循如上描述，其区别点往往体现在以下两方面：

a.如何获得最初的信任页面子集合，不同的方法手段可能有差异。

b.信任度是如何进行传播的，不同的方法可能有细微差异。

8.5.2不信任传播模型

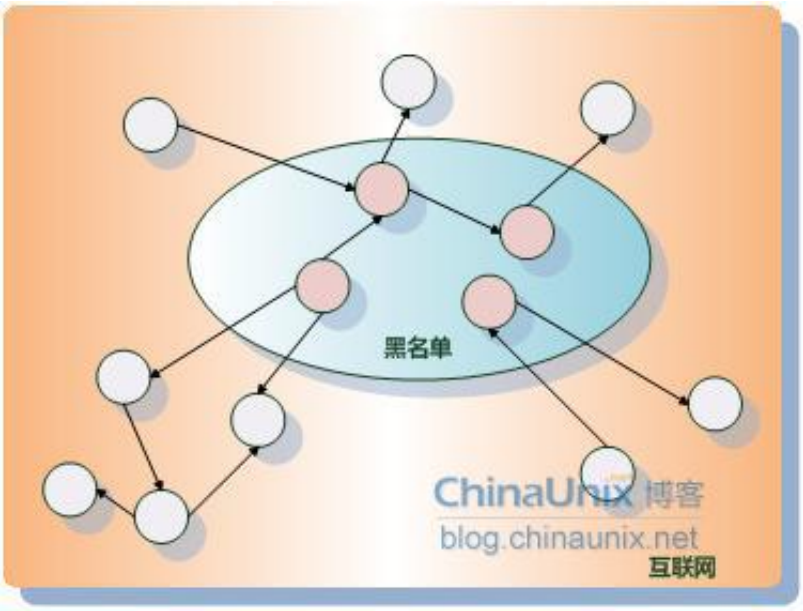

图8-7 不信任传播模型

图8-7展示了“不信任传播模型”的整体框架示意图。从大的技术框架上来讲，其和“信任传播模型”是相似的，最大的区别在于：初始的页面子集合不是值得信任的页面节点，而是确认存在作弊行为的页面集合，即不值得信任的页面集合（可以理解为黑名单）。赋予黑名单内页面节点不信任分值，通过链接关系将这种不信任关系传播出去，如果最后页面节点的不信任分值大于设定的阈值，则会被认为是作弊网页。

同样，很多算法可以归入这一模型框架，只是在具体实施细节方面有差异，整体思路基本一致。

8.5.3异常发现模型

异常发现模型也是高度抽象化的一个算法框架模型，其基本假设认为：作弊网页必然存在有异于正常网页的特征，这种特征有可能是内容方面的，也有可能是链接关系方面的。而制定具体算法的流程往往是先找到一些作弊的网页集合，分析出其异常特征有哪些，然后利用这些异常特征来识别作弊网页。

具体来说，这个框架模型又可细分为两种子模型，这两种子模型在如何判断异常方面有不同的考虑角度。一种考虑角度比较直观，即直接从作弊网页包含的独特特征来构建算法（参见图8-8）；另外一种角度则认为不正常的网页即为作弊网页，也就是说，是通过统计等手段分析正常的网页应该具备哪些特征，如果网页不具备这些正常网页的特征，则被认为是作弊网页（参见图8-9）。图8-8和图8-9体现了这两种不同的思路。

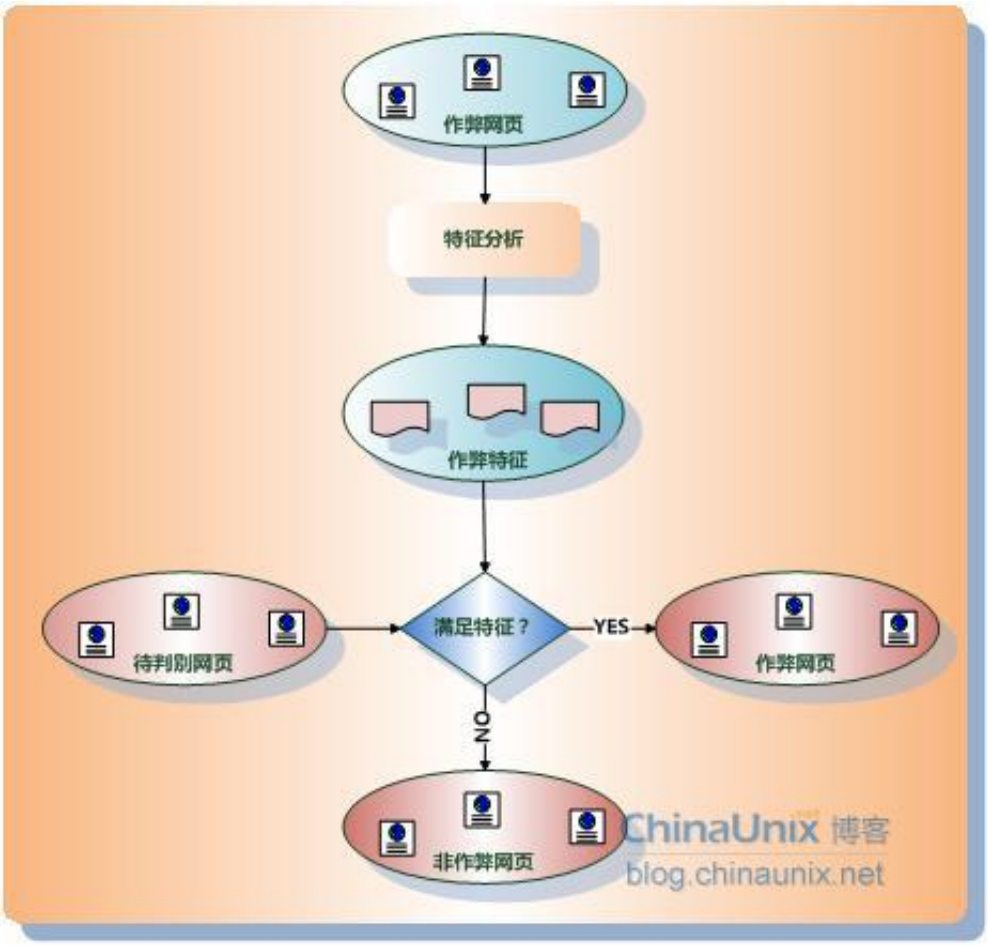

图8-8 异常发现模型一

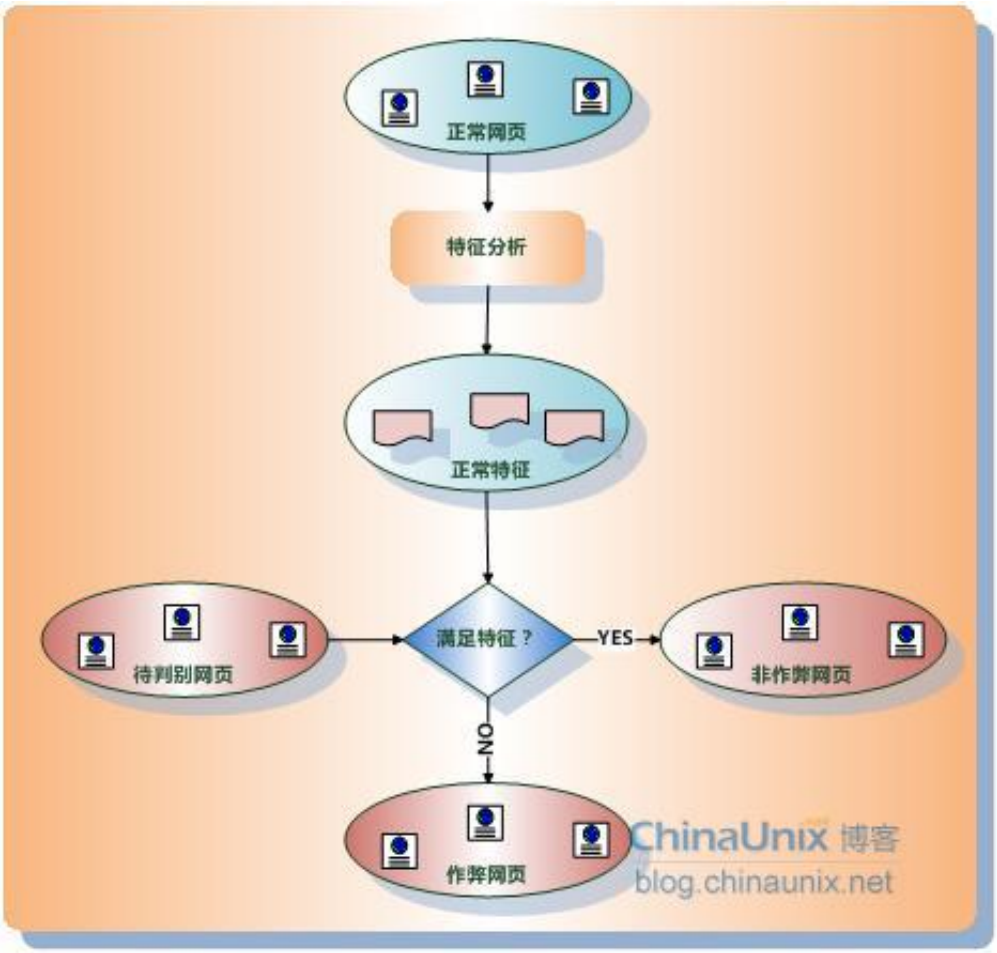

图8-9 异常发现模型二

尽管反作弊算法五花八门，但是不论采取哪种具体算法，其实都包含了一些基本假设，经常被反作弊算法使用的基本假设有：

a. 尽管作弊网页喜欢将链接指向高质量网页，但是很少有高质量网页将链接指向作弊网站的现象；

b. 作弊网页之间倾向于互相指向；

很多算法的基本思路都是从这些基本假设出发来构造的。