

移动自组网中非完全信息节点风险评估

付 才¹⁾ 洪 亮²⁾ 彭 冰¹⁾ 韩兰胜¹⁾ 徐兰芳¹⁾

¹⁾(华中科技大学计算机科学与技术学院 武汉 430074)

²⁾(西北工业大学自动化学院 西安 710072)

摘 要 移动自组网是一种无中心、自组织以及多跳的无线网络,能否有效可靠地对通信节点进行风险评估是保障节点高质量通信的重要因素.当前基于可信度或是信誉的评估方法对评估样本都有特殊的要求,对评估对象提出种种假设,无法辨别间接样本的恶意推荐问题,在实际移动自组网中各个节点尤其是恶意节点对外暴露的信息往往偏少,样本数量有限,无法明确判断其状态,大部分是非完全信息,从而导致评估结果缺乏客观性与可靠性.文中提出采用灰色系统理论描述通信节点非完全信息状态,根据灰类白化以及灰色聚类思想进行节点风险评估.方案针对自组网络通信需求对节点行为进行多关键属性划分,采用味集群方法收集原始样本,避免恶意推荐;将难以用数值精确刻画的关键属性以白化权函数量化,引入灰聚类的概念和计算方法,将实体的通信风险水平定义为实体关键属性值序列针对各评估灰类的聚类评估值,从而得到该实体通信风险水平的相对参考值.分析与实际计算表明该方法是一种适合移动自组网中非完全信息节点风险评估的有效方法.

关键词 移动自组网;风险评估;灰色理论;非完全信息

中图法分类号 TP393

DOI号: 10.3724/SP.J.1016.2009.00805

Incomplete Information Nodes Risk Assessment in Mobile Ad Hoc Networks

FU Cai¹⁾ HONG Liang²⁾ PENG Bing¹⁾ HAN Lan-Sheng¹⁾ XU Lan-Fang¹⁾

¹⁾(College of Computer Science & Technology, Huazhong University of Science & Technology, Wuhan 430074)

²⁾(College of Automation, Northwestern Polytechnical University, Xi'an 710072)

Abstract Mobile Ad hoc Networks are distributed self-organized and multi-hop networks, the efficient networks nodes risk assessment is the key factor for high quality communication. Most assessment methods based on reliability or reputation have particular requirement, suppose some conditions to the samples, and can't identify the vicious recommendation. However, in true Ad hoc networks, the exposed information of some nodes is little, which is more serious to some vicious nodes, the samples are so little that the clear state can't be identified and most are incomplete information, which result in that the assessment is not objective and credible. According to these problems, a Ad hoc networks risk assessment method based on grey theory is proposed. In this scheme, the communication nodes incomplete information state is described as grey league, the whitening function and grey clustering idea are used to do the assessment. The key attributes of nodes are marked off, original data is collected using taste concourse method to avoid vicious recommendation, the evaluated nodes are regarded as clustering entities, and the risk grade point value of their key attributes are given by clustering set assessment value, the analysis and computing shows this scheme is a efficient incomplete information nodes risk assessment method in mobile Ad hoc networks.

Keywords Ad hoc networks; risk assessment; grey theory; incomplete information

收稿日期:2008-12-08;最终修改稿收到日期:2009-01-19. 本课题得到湖北省自然科学基金(2008CDB352)、国家自然科学基金(60703048, 60803158)资助. 付 才,男,1976年生,博士,讲师,主要研究方向为无线网络安全、路由协议安全与软件脆弱性. E-mail: stand_fucai@126.com. 洪 亮,男,1979年生,博士,讲师,主要研究方向为 Ad hoc 网络技术、路由安全及密码学. 彭 冰,男,1972年生,博士,讲师,主要研究方向为无线网络安全、密码学. 韩兰胜,男,1972年生,博士,副教授,主要研究方向为计算机病毒、网络安全和密码学. 徐兰芳,女,1953年生,副教授,主要研究方向为密码学与访问控制.

1 引言

移动自组网中节点的风险评估研究已经成为无线网络中的一个研究热点. 移动自组网中的决策制定与运行机制通常是分散的, 许多网络算法都是依赖所有节点的共同参与. 另外由于没有固定的网络基础设施、网络拓扑结构频繁动态变化、无线信道完全开放、网络缺乏自稳定性等原因, 移动自组网环境下的路由协议相对于有线网环境更易遭受各种攻击, 比如路由报文的篡改、假冒节点进行路由欺骗、黑洞攻击、拒绝服务以及虫洞攻击 (wormhole attack) 等等, 因此对节点进行风险评估非常重要, 以区分出恶意节点并采取相应措施, 维护整个移动自组网的通信质量.

目前, 关于网络中通信实体评估的研究比较多, 提出了相应的支撑理论与方法, 主要是从可信度或是信誉的角度进行, 可信度与信誉的高低反映出与该节点通信的风险大小, 主要方法如下:

(1) Guha 等人^[1]提出了基于权重的信任传递方法, 对不同推荐路径的推荐信任值进行加权平均. 这种方法中的推荐权重参数一般由推荐方的信誉、时间等因素决定, 主观性非常强, 在移动自组网环境中难以确定.

(2) 基于概率的信任模型, Beth 等人^[2]首先将信任分为直接信任和推荐信任, 利用概率统计的方法计算信任值, 并提出了信任的合成方法. Wang 等人^[3]用贝叶斯网络来解决信誉问题, 通过计算二元评分 (正或负) 的条件概率值来评估信誉.

(3) 基于证据理论的信任模型, 基于概率的不确定性推理方法不能处理“无知 (ignorance)”, 而证据理论对无知的处理则非常深刻地反映了信任不确定性的本质特征. 如 Yu 等人提出用证据理论解决信任合成问题^[4].

(4) 基于主观逻辑的信任模型, Jøsang 等人提出了描述和度量信任关系的主观逻辑^[5], 用观点 (opinion) 来表示主观信任 (subjective belief). A 对 x 真实性的信任表示为 (b, d, u, a) , 其中 b 、 d 和 u 分别表示信任、不信任 and 不确定, 并且 $b + d + u = 1$. 信任 (不信任) 随着相应的依据的出现而增加. 参数称为相关因子 (relative atomicity), 代表在缺少证据情况下的基本评价概率 (base rate probability), 用于计算一个观点的概率期望值 $b + au$, 这意味着 a 决定 $b + au$ 的不确定程度. 这种方法和贝叶斯方法是

等价的.

(5) 唐文等运用模糊集合理论对信任评估问题进行了数学建模^[6], 并给出了主体信任的一般评价机制和信任关系的推导规则. 但该模型没有提供推荐信任的评估方法以及信任评价尺度的具体含义.

另外, Abdul-Rahman 等人从信任的概念出发, 提出了一个分布式信任模型^[7], 采用一系列离散值对信任关系进行度量. 模型给出了信任度的传递协议和计算公式, 但没有给出具体的信任综合计算公式和直接信任的获取方法; Theodorakopoulos 等人^[8]提出的模型中, 把信任评估问题看作是带权重的有向图 $G(V, E)$ (信任图) 上的最短路径问题, 分别利用基于路径的半环和基于距离的半环传递与合成信任. 目前, P2P 网络环境下的信任机制取得了较多的研究成果^[9-10].

针对移动自组网的自私节点问题, 当前也有学者提出了不同解决方法, 其中比较典型的见文献^[11-13]. 文献^[11]首先引入 Watchdog 部件来监督邻居转发行为, 当 Watchdog 发现邻居丢包的数量超过一个预定门限, 则判定该邻居是不良节点. Watchdog 比较简单, 因此功能非常有限. 文献^[12]提出了一个 CONFIDANT 模型, 该模型由监视器、信任管理、声誉系统和路径管理组成. 其中监视器负责对邻居的监督并获得观察资料; 信任管理用于建立信任关系来处理接收和发送告警信息; 声誉系统综合观察信息和告警信息对邻居节点进行声誉评价; 路径管理用于路由过程中避开和孤立自私节点. 文献^[13]则提出一个基于联合声誉机制的 CORE 模型. 联合声誉机制包括直接声誉、间接声誉和功能声誉. 这些机制联合起来计算节点的总声誉值, 以便决定是否继续合作. 以上这些模型均只提出监控框架模型, 没有给出具体的评价方式.

上述这些评估机制, 从评估的支撑基础理论来讲, 大致可以分为两类, 一类是基于概率论的评估方法, 如基于权重的评估方法, 基于贝叶斯评估方法, 另外基于主观逻辑、基于证据理论等信任模型也需要概率论的理论支撑. 另外一类是基于模糊集合理论的信任评估模型. 目前, 概率论与模糊理论是两种重要的不确定信息研究理论, 通过概率与数理统计, 解决样本量大、数据多但缺乏明显规律的问题, 即“大样本不确定性”问题; 用模糊数学处理人的经验与认知先验信息的不确定问题, 即“认知不确定性问题”. 概率与数理统计强调统计数据与历史关系, 研究历史的统计规律. 模糊理论强调先验信息, 依赖人

的经验,研究经验认知的表达规律.但在移动自组网中,由于节点的动态性、临时性,尤其是恶意节点的保护性,使得能够体现统计规律的事件数量并不是很多,运用概率论的方法在小样本情况下,其评估效果与客观性会受到一定影响.而模糊理论依赖人的经验,通过经验认知获得表达规律,评估一般假设节点的行为特性符合人的一般经验,在移动自组网中,有一定的应用局限性,对于新出现的事件或是恶意节点,过多依赖人的先验认知同样会导致一定评估上的影响,另外目前基于模糊理论的信任评估方法缺乏具体的实施准则.针对样本多的情况,我们在文献[14]中提出采用数据挖掘中的关联规则方法,用于评估不可信节点;针对少样本,我们在文献[15]中对电子商务中商家信誉进行评估时引入灰色系统理论,但电子商务基于集中式交易平台,味集群方式样本选择等操作较容易实现,同时将信任定义为评估属性集对最优属性集的灰关联度,由于最优属性集在有些情况下并没有上界,尤其是在移动自组网中,其实用性受到影响,另外在面对移动自组网中的多属性、量化单位不确定、极性不确定问题的时候,需要研究新的灰聚类手段,灰色理论在自组织网络中应用面临着新的挑战.

从前面分析可知,移动自组网中针对节点进行风险评估需要解决3个方面的核心问题:

(1)需要解决样本获取的问题,移动自组网中,被评估节点可能会存在事件样本偏少,或是样本不全的问题,评估方案既要能够对大样本处理,也能够对少样本进行有效处理,并能够判断有效样本,从而达到样本少而精的目的;

(2)要解决恶意推荐即间接样本的问题,对一个节点进行评估,采用间接样本是必须的,能够提高评估的客观性与可靠性,但是带来了恶意推荐的问题,尤其是存在恶意节点串通的情况下,因此,必须采取方法避免恶意推荐;

(3)样本的聚集与应用问题,大数量样本可以通过统计规律获取评估结果,少样本非完全信息必须采取一定的手段,使得能够得出较为客观的评估结果.

针对上述核心问题,本文引入灰色系统理论对移动自组网中的节点信息进行处理,重点解决移动自组网中非完全信息少样本双极性多属性的节点风险评估问题.灰色系统理论(简称灰理论 Grey Theory)是针对既无经验,数据又少的不确定性问题进行分析的支撑理论^[16].在本方案中,针对移动

自组网中节点的通信需求,对节点行为进行多关键属性划分,采用味集群方法收集原始样本,避免恶意推荐;将难以用数值精确刻画的关键属性以白化权函数量化,引入灰聚类的概念和计算方法,将实体的风险程度定义为实体的关键属性值序列对各灰类的评估值,从而得到该实体风险程度的相对参考值.

本文第2节对灰色系统理论做一个基础描述,并证明灰数白化函数存在定理;第3节描述恶意节点评估方案,证明方案中各节点样本聚类权满足灰色关联度3个必要条件;第4节针对实验数据进行实例计算;第5节对本文的非完全信息节点风险评估机制特点进行总结.

2 基本概念

定义 1. 评估节点集、味集群.

设移动自组网节点 t_0 在对通信节点进行评估的时候,收到有 n 个节点发出的评估结果报文,则由 t_0, t_1, \dots, t_n 构成的集合 $T = \{t_i | i = 0, 1, 2, \dots, n\}$ 为评估节点集,评估节点集根据时间或是路由簇又分为各个分集合 T_i , 则 $T = T_1 \cup T_2 \cup \dots \cup T_u \cup \dots \cup T_v \cup \dots \cup T_q$, 其中 $T_u, T_v \subseteq T$, 且若 $T_u, T_v \subseteq T$, 则 $T_u \cap T_v = \emptyset, 1 \leq u, v \leq q$. 设 $T_u = \{t_{u0}, t_{u1}, t_{u2}, \dots, t_{up}, \dots, t_{us}\}$, 设被评估节点 $d_i (d_i \in D, 1 \leq i \leq m)$ 的关键属性集为 $A = \{a_h | h = 1, 2, \dots, e\}$, 若 $\forall t_{up} \in Cu$, 且 $1 \leq p \leq s$, t_{up} 对 d_i 的 A 中的所有关键属性的评分与 t_{u0} 对 d_i 的 A 中的所有关键属性的评分的偏离在可允许范围内,称 T_u 为味集群, t_{u0} 为味集群 T_u 的核心. 每一个味集群有且仅有一个核心,称由味集群 T_1, T_2, \dots, T_q 的核心组成的集合 T_0 为核心集, $T_0 = \{t_{u0} | u = 1, 2, \dots, q\}$.

定义 2. 灰数、灰类集.

灰数是指信息不完全的数.比如“该节点的丢包率在 35% 左右”,35% 左右便是灰数,可记为 $\otimes(35\%)$ (读作“灰 35%”),还比如“该节点可能还要工作 6h”,6h 也是一个灰数,因为无法精确知道节点的未来工作时间.这是由于对被评估节点缺乏了解,对其确实的丢包状况缺乏信息.类似的,对于某些无法精确定义边界信息不完全的类称之为灰类,由所有相关灰类组成的集合为灰类集,如对一个节点的评价可以分为“无恶意”、“怀疑恶意”、“恶意”,由于这 3 个类别无法精确量化,可以用 3 个灰类构成的灰类集 G 表示, $G = \{g_k | k = 1, 2, \dots, r\}$, 其中, g_k 表示第 k 灰类.

定义 3. 形态灰数与白化函数.

令 \wp 为数字命题, $\wp(\theta)$ 为 \wp 的命题信息域, \otimes 为 \wp 的灰数, \tilde{D} 为 \otimes 的数值覆盖, 若 \tilde{D} 是 \wp 表现的默认空间, 或者默认与承认的混合空间, 并且具有形态内涵, 则称 \otimes 为形态灰数, 并且“大于等于 c 的数”为上类形态灰数, “在 c 左右的数”为中类形态灰数, “小于等于 c 的数”为末类形态灰数.

灰数的白化是将不确定值的灰数, 按照白化函数取一个确定的值, 或者说, 对属于某一个区间的灰数, 按照某种“偏好”的程度, 在该区间取白化值.

令 \otimes 为形态灰数, $\tilde{\otimes}$ 为 \otimes 的白化值, f 为 $\tilde{\otimes}$ 的确认率, 则称以白化数 $\tilde{\otimes}$ 为横坐标, f 为纵坐标的平面为形态灰数认知平面 P_{ken} , 在 P_{ken} 上, 形态灰数 \otimes 的白化值 $\tilde{\otimes}$ 与确认率 f 的最少信息图像, 称之为形态灰数的白化函数, 若 $f \in [0, 1]$, 则称白化函数是典型的, 一般情况下, 均为典型白化函数.

下面采用灰色系统相关理论证明针对灰类的白化函数存在定理.

定理 1. 令 K 为灰类集, $K = \{1, 2, \dots, n\}$. f_k 为 k 灰类白化函数, 且 f_1 为上类白化函数, f_n 为末

类白化函数, 其余 $f_i (i \neq 1, i \neq n)$ 为中类白化函数, 则白化函数有如下算式, 即

(1) 上类白化函数:

$$f_1 = f_1(c_1, \infty) \\ \Rightarrow f_1(\xi_{ij}) = \begin{cases} (1/c_1)\xi_{ij}, & \xi_{ij} \in [0, c_1] \\ 1, & \xi_{ij} \in [c_1, \infty] \end{cases}.$$

(2) 中间灰类白化函数:

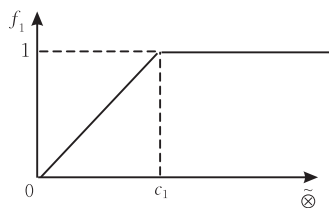
$$f_i = f_i(-, c_i, +), i \in K, i \neq 1, i \neq n \\ \Rightarrow f_i(\xi_{ij}) = \begin{cases} (1/c_i)\xi_{ij}, & \xi_{ij} \in [0, c_i] \\ -(1/c_i)\xi_{ij} + 2, & \xi_{ij} \in [c_i, 2c_i] \end{cases}.$$

(3) 末类白化函数:

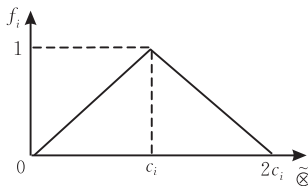
$$f_n = f_n(0, c_n) \\ \Rightarrow f_n(\xi_{ij}) = \begin{cases} 1, & \xi_{ij} \in [0, c_n] \\ -(1/c_n)\xi_{ij} + 2, & \xi_{ij} \in [c_n, 2c_n] \end{cases}.$$

证明.

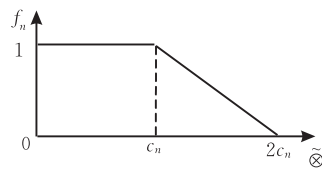
(1) 按照定义 3, 白化函数是指形态灰数认知平面 P_{ken} 上形态灰数 \otimes 的白化值 $\tilde{\otimes}$ 与确认率 f 的最少信息图像, 根据文献[16]中灰色系统理论最少信息原理 8, 直线相对曲线为最少信息, 图 1(a)即为上类形态灰数的白化函数.



(a) 上类形态灰数白化函数



(b) 中类形态灰数白化函数



(c) 末类形态灰数白化函数

图 1

根据该图, 当 $\tilde{\otimes} \leq c_1$, 直线斜率 $k = 1/c_1$, 所以 $f_1(\tilde{\otimes}) = (1/c_1)\tilde{\otimes}$; 当 $\tilde{\otimes} > c_1$, $k = 0$, $f_1(\tilde{\otimes}) = 1$, 所以,

$$f_1 = f_1(c_1, \infty) \\ \Rightarrow f_1(\xi_{ij}) = \begin{cases} (1/c_1)\xi_{ij}, & \xi_{ij} \in [0, c_1] \\ 1, & \xi_{ij} \in [c_1, \infty] \end{cases};$$

(2) 基于最少信息原理 8, “对称”相对于“非对称”, “直线”相对于“曲线”为最少信息, 依据定义 3 可知, 图 1(b)所示函数为中灰类的白化函数.

根据该图, 当 $\tilde{\otimes} \leq c_i$, 直线斜率 $k = 1/c_i$, 所以 $f_i(\tilde{\otimes}) = (1/c_i)\tilde{\otimes}$; 当 $\tilde{\otimes} > c_i$, $k = -(1/c_i)$, $f_i(\tilde{\otimes}) = -(1/c_i)\tilde{\otimes} + 2$, 所以,

$$f_i = f_i(-, c_i, +), i \in K, i \neq 1, i \neq n$$

$$\Rightarrow f_i(\xi_{ij}) = \begin{cases} (1/c_i)\xi_{ij}, & \xi_{ij} \in [0, c_i] \\ -(1/c_i)\xi_{ij} + 2, & \xi_{ij} \in [c_i, 2c_i] \end{cases};$$

(3) 同理可以证明末类函数的白化函数 f_n .

定义 4. 聚类集、灰色聚类.

记 d_1, d_2, \dots, d_m 为被评估节点, 即聚类对象, 组成集合 $D = \{d_i | 1 \leq i \leq m\}$ 为聚类集, a_1, a_2, \dots, a_h 为被评估节点的关键属性, 即聚类指标, g_1, g_2, \dots, g_r 为灰类, $\xi_{ij}(u)$ 表示第 u 个味集群 c_u 对节点 d_i 的第 a_j 个关键属性指标的评分, 则第 u 个味集群 c_u 对所有聚类对象 d_1, d_2, \dots, d_m 的所有指标 a_1, a_2, \dots, a_h 的样本矩阵为

$$D_u = \begin{Bmatrix} \xi_{11}, \xi_{12}, \dots, \xi_{1e} \\ \xi_{21}, \xi_{22}, \dots, \xi_{2e} \\ \dots \\ \xi_{m1}, \xi_{m2}, \dots, \xi_{me} \end{Bmatrix}.$$

若 $\sigma_{ik} = \sum_{j=1}^e f_{jk}(\xi_{ij}) \eta_{jk}$, $\eta_{jk} = c_{jk} / \sum_{j=1}^e c_{jk}$, 其中 c_{jk} 为 f_{jk} 的阈值, f_{jk} 为白化函数, σ_{ik} 为灰色聚类权, σ_i 为 σ_{ik} 的向量, $\sigma_i = (\sigma_{i1}, \sigma_{i2}, \dots, \sigma_{ir}) = (\sum_{j=1}^e f_{j1}(\xi_{ij}) \eta_{j1}, \sum_{j=1}^e f_{j2}(\xi_{ij}) \eta_{j2}, \dots, \sum_{j=1}^e f_{jr}(\xi_{ij}) \eta_{jr})$, 其中, r 表示灰类的基, 即灰类的总个数. e 表示关键属性的个数, 则称 ξ_{ij} 到 σ_i 的映射为灰色聚类.

令 $\sigma_i = (\sigma_{i1}, \sigma_{i2}, \dots, \sigma_{ir})$, 若有 σ_{ik}^* 满足 $\sigma_{ik}^* = \max_k \sigma_{ik} = \max\{\sigma_{i1}, \sigma_{i2}, \dots, \sigma_{ir}\}$, 则称聚类对象 i 属于灰类 g_{k^*} . 该分析过程称为灰色聚类分析.

3 移动自组网节点风险评估方案

3.1 非完全信息节点风险评估框架

根据前面灰色理论聚类分析过程以及节点风险评估需求, 首先对被评估节点进行关键属性定义, 得到关键属性集合 $A = \{a_h | h = 1, 2, \dots, e\}$, 各个评估节点 $T = \{t_i | i = 0, 1, 2, \dots, n\}$ 对这些关键属性进行监测后, 将样本数据发给 t_0 , 通过选择, 得到味集群, 对每个味集群样本进行量化单位统一化处理以及指标多极性处理后, 进行灰聚类计算, 最后通过味集群决策得出结论, 味集群内部的样本由于都在有效偏差范围之内, 可直接对样本进行算数平均后进行灰聚类计算. 非完全信息可信节点评估方案框架如图 2 所示.

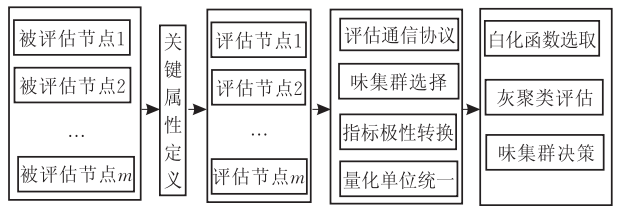


图 2 恶意节点评估框架

该方案由被评估节点关键属性定义、评估通信协议、味集群/核心集选择、指标极性转换、量化单位统一化处理、白化函数选取、灰聚类评估计算以及味集群决策等过程构成.

3.2 非完全信息节点风险评估流程

本方案的基本思想是评估发起节点将收到的评估样本进行味集群划分与选取, 对味集群数据进行灰色聚类分析, 最后通过味集群决策得出最终结论. 步骤如下:

(1) t_0 发起评估请求广播, 将关心的节点属性集

$A = \{a_h | h = 1, 2, \dots, e\}$ 告诉各个节点, 通信细节由评估通信协议决定, 可引入的密码机制, 保证通信的完整性与可靠性.

(2) 各个评估节点将样本进行安全验证后发给 t_0 , 由 t_0 进行味集群选择, 得到味集群 T_1, T_2, \dots, T_q .

(3) 对每个味集群 T_j 得到的样本矩阵进行指标极性转换; 为应对移动自组网中的多属性指标极性不统一问题, 引入成本余值法进行极性转换^[17]. 由于风险评估中各个节点的需求并不完全确定, 导致指标的极性可能不一致. 比如: 有些评估关心丢包率, 丢包率是越小越好, 而有些节点关心转发速度, 速度越快越好, 丢包率与转发速度属于极性不同, 而在一般的灰聚类评估中, 由于白化函数的非一般性, 无法对双极性样本值处理. 成本余值法处理过程如下:

设某属性 $a_i = \xi_i$, 且 $0 \leq a_i \leq \max(a_i)$, 该属性对评估方来讲越小越好, 为极小值极性, 令 $a_i^* = \max(a_i) - \xi_i$, 则 a_i^* 对评估方来讲, 变化为越大越好, 为极大值极性. 通过本方法, 可将所有属性极性得到统一.

(4) 属性量化单位统一处理, 由于移动自组网节点属性的多样性, 其量化的指标数值与单位差距较大, 需要统一处理为无单位属性值. 为此, 可采用样本初值化方法. 处理过程如下:

设有节点 d_1 属性样本 $D_1 = \{\xi_{11}, \xi_{12}, \xi_{13}\}$ 与 d_2 属性样本 $D_2 = \{\xi_{21}, \xi_{22}, \xi_{23}\}$, 任取节点 d_1 , 令其样本为 $D_1^* = \{\xi_{11}/\xi_{11}, \xi_{12}/\xi_{12}, \xi_{13}/\xi_{13}\} = \{1, 1, 1\}$, 则 $D_2^* = \{\xi_{21}/\xi_{11}, \xi_{22}/\xi_{12}, \xi_{23}/\xi_{13}\}$, 通过该方法, 可消去所有单位, 同时数值表示更加规范. 样本初值化后, 对应的白化函数也按照选取的节点进行初值化. 比如: 原样本第一个属性 a_1 上灰类阈值 c_{11} 现在变换为 $c_{11}^* = c_{11}/\xi_{11}$.

(5) 结合移动自组网的通信需求, 定义各个属性的白化函数, 然后 t_0 针对每个味集群 T_j 得到的样本矩阵进行灰色聚类评估, 得到被评估节点 $d_i (d_i \in D, 1 \leq i \leq m)$ 的灰类 g_{ji}^* .

定理 2. 经过上述初值化处理后, 样本的聚类权在白化函数灰定义域满足样本与相应灰类阈值样本关于灰关联度的规范性、整体性以及接近性 3 个必要条件.

证明. 对于上灰类, 当样本值 $\xi > c_1$, $f_1(\xi) \equiv 1$, 因此, 上灰类灰定义域为 $(0, c_1]$, 同理, 中灰类灰定义域为 $(0, 2c_1)$, 下灰类灰定义域为 $[c_n, 2c_n)$.

针对上灰类, 设初值化后样本值

$$D_1^* = \left\{ \begin{array}{c} \xi_{11}^*, \xi_{12}^*, \dots, \xi_{1e}^* \\ \xi_{21}^*, \xi_{22}^*, \dots, \xi_{2e}^* \\ \dots \\ \xi_{m1}^*, \xi_{m2}^*, \dots, \xi_{me}^* \end{array} \right\},$$

上灰类阈值样本为 $c_1^* = \{c_{11}^*, c_{21}^*, \dots, c_{e1}^*\}$,

① 根据上灰类白化函数定义, 对于灰定义域的所有样本, 有 $\xi_{ij}^* \leq c_{j1}^*, 1 \leq i \leq m$, 所以, $f_{j1}(\xi_{ij}^*) \leq 1$, 又因为 $\sum_{j=1}^e \eta_{j1} = \sum_{j=1}^e (c_{j1} / \sum_{j=1}^e c_{j1}) = 1$, 所以,

$\sum_{j=1}^e f_{j1}(\xi_{ij}^*) \eta_{j1} \leq 1$ 且 $\sum_{j=1}^e f_{j1}(\xi_{ij}^*) \eta_{j1} > 0$, 显然, 当

$\xi_{ij}^* = c_{j1}^*$ 时, $\sum_{j=1}^e f_{j1}(\xi_{ij}^*) \eta_{j1} = 1$, 所以, $0 < \sigma_{i1} =$

$\sum_{j=1}^e f_{j1}(\xi_{ij}^*) \eta_{j1} \leq 1$, 满足灰关联度的规范性。

② 根据聚类权的定义,

$$\begin{aligned} \sigma_{i1} &= \sum_{j=1}^e f_{j1}(\xi_{ij}^*) \eta_{j1} = \sum_{j=1}^e f_{j1}(\xi_{ij}^*) (c_{j1} / \sum_{j=1}^e c_{j1}) \\ &= \sum_{j=1}^e (f_{j1}(\xi_{ij}^*) c_{j1}) / \sum_{j=1}^e c_{j1}, \end{aligned}$$

对于上灰类, $f_{j1}(\xi_{ij}^*) = \xi_{ij}^* / c_{j1}$, 代入上式, 得到

$$\begin{aligned} \sigma_{i1} &= \sum_{j=1}^e (f_{j1}(\xi_{ij}^*) c_{j1}) / \sum_{j=1}^e c_{j1} = \sum_{j=1}^e ((\xi_{ij}^* / c_{j1}) c_{j1}) / \sum_{j=1}^e c_{j1} \\ &= \sum_{j=1}^e \xi_{ij}^* / \sum_{j=1}^e c_{j1}, \quad 1 \leq i \leq m, \end{aligned}$$

对于样本矩阵来讲,

$$\sum_{j=1}^e \xi_{ij}^* \neq \sum_{j=1}^e \xi_{i'j}^*,$$

其中, $1 \leq i, i' \leq m, i \neq i'$, 所以有 $\sigma_{i1} \neq \sigma_{i'1}$, 满足灰关联度的整体性。

③ 考虑单属性 $a_h, 1 \leq h \leq e$, 设有两个该属性样本 ξ_{ph}, ξ_{qh} , 且 $0 < \xi_{ph}, \xi_{qh} \leq c_{h1}, 1 \leq p, q \leq m, p \neq q$, 令 $|\xi_{ph} - c_{h1}| < |\xi_{qh} - c_{h1}|$, 根据上灰类的白化函数图, 易知 $\xi_{ph} > \xi_{qh}$, 所以, $f_{h1}(\xi_{ph}) \eta_{h1} > f_{h1}(\xi_{qh}) \eta_{h1}$, 若所有属性满足该条件, 则有 $\sigma_{p1} > \sigma_{q1}$, 满足灰关联度的接近性。

针对中灰类与下灰类可以同理证明。

当前, 大部分各领域文献只是灰聚类评估应用, 没有指出灰聚类的评估内涵, 定理 2 说明了灰色聚类权反映了样本属性跟相应白化函数阈值的综合接近程度, 由此通过比较各个样本的聚类权, 即可判断该样本所属的灰类。需要指出的是, 由于灰聚类评估是一个多样本的比较, 因此, 样本个数 $m \geq 2$, 结合灰类阈值构成的理想样本, 总的样本个数 $m \geq 3$, 因此, 灰关联度的偶对对称性没有存在的基础, 因此定理

中没有说明。

(6) 味集群决策, 其算法如下:

输入: 味集群 T_1, T_2, \dots, T_q 对被评估节点集 $\{d_1, d_2, \dots, d_m\}$ 灰聚类评估矩阵

$$G^* = \left\{ \begin{array}{c} g_{11}^*, g_{12}^*, \dots, g_{1m}^* \\ g_{21}^*, g_{22}^*, \dots, g_{2m}^* \\ \dots \\ g_{q1}^*, g_{q2}^*, \dots, g_{qm}^* \end{array} \right\};$$

输出: 味集群 T_1, T_2, \dots, T_q 对 $\{d_1, d_2, \dots, d_m\}$ 决策结果

$$G^o = \{g_1^o, g_2^o, \dots, g_m^o\}.$$

步骤:

对 $\{d_1, d_2, \dots, d_m\}$ 中的每个节点 d_i :

对 d_i 所有聚类灰类 $G_i^* = \{g_{1i}^*, g_{2i}^*, \dots, g_{qi}^*\}$ 进行计算, 针对每个灰类 g_k :

if ($g_{ki}^* = g_k$) then $C_i(g_k)++$;

然后, $C_i = \max(C_i(g_k))$; 得到 C_i 对应的 g_k ,

if ($\text{Count}(g_k) > 1$) then: 将 σ_{ik} 进行累加, 取最大的 σ_{ik} 对应的灰类 g_k 作为最终结果。

g_k 为节点 d_i 的决策结果 g_i^o 。

4 实例计算

4.1 关键属性定义

根据移动自组网节点安全通信需求, 一个低风险节点应该提供安全可靠并且高效的数据通信服务。当前, 在解决移动自组网安全通信风险方面已经取得了一定成果, 这些成果可以归结为两类: 一类是采用常规的“硬安全”措施, 比如各种分布式数字签名、群签名、通信加密等; 另外一类是“软安全”, 如节点风险评估。“硬安全”措施解决的实际是节点合法性的问题, 即降低了身份风险, 但在移动自组网中, 降低身份风险并不能满足安全通信的需求, 一方面, 有些新的“友好”节点需要加入移动自组网, 但无法通过身份验证; 另一方面, 有些节点骗取了身份信任, 但实际行为表现为一个自私或是不可靠节点, 因此, 还必须对行为风险进行评估与处理, 这也是移动自组网节点风险评估需解决的焦点问题。在确定一个节点的行为风险之前, 需要定义关键属性, 即确定评估指标。这些关键属性必须体现移动自组网节点行为特征, 以客观有效地进行行为风险的评估与处理。

关键属性定义首先要符合移动自组网的结构特点。该网络基于开放的无线网络环境, 具有完全分布式、自组织以及动态拓扑特点, 网络中的节点可以自由移动, 整个网络的工作性能依赖于节点之间的相

互协作程度,一般网络的节点评估,多数只观察通信会话或是路由转发的成功与否,再结合间接信息进行处理.但是对于移动自组网节点风险评估,除了网络通信特性(如:丢包率)外还应该考虑该节点的自身物理属性,包括移动特性、无线信号特性以及空间特性等,各个特性分析如下:

网络通信特性是指节点对于网络报文收发的特性,是反应节点风险水平的核心因素.网络通信特性包括传输速度、丢包率等,传输速度体现了节点的工作性能,传输速度太低不利于网络通信,若将其作为路由节点风险程度提高;丢包率则是评价节点工作可靠性的关键指标,丢包率除了跟自身工作的稳定性以外,还跟一些特定的移动自组网攻击相关,如黑洞攻击、虫洞攻击等,是评估不可缺少的部分.

在节点的物理属性方面,移动特性主要关心节点运动速度,运动速度越快,丢包率会提高,也会导致路由频繁变化程度越高,不利于稳定的通信;无线信号特性则包括两个方面的因素,一个是信号强弱水平,信号越强,则工作越可靠,另外一个信号是信号稳定程度,即信号变化率,信号变化太快,既可能是节点移动过快,也可能是节点自身的不稳定以及环境的干扰导致,甚至节点本身是一个攻击节点,因此,信号稳定程度也反应了通信的风险级别;空间特性则主要是节点之间的距离,节点越近,则传输可靠性越高,距离也是通信风险需要考虑的因素.

关键属性定义还需要满足可监测以及客观性的特点.可监测是指该属性指标在移动自组网中需具备测量的手段,如转发速度与丢包率可通过文献[11]所述的 Watchdog 方法,将网络接口设置为监听方式,即可完成数据的监测,该方法同样适用于无线信号的检测;客观性是指指标测量是客观的,应避免恶意伪造指标数值,如被评估节点的电池能量指标,虽然电池能量的多少可影响通信的风险,但需要节点自身进行检测并报告给评估节点,较容易伪造.根据可监测的要求,移动特性与空间特性的测量需要专门的设备,如测距雷达、GPS 定位设备等,这在资源短缺的移动自组网环境中难以满足,但是可以根据信号强度与距离的转换关系,将移动的速度反映到无线信号的变化中,而将距离的远近反应到信号的强度中,同样可以对其进行评估与处理.

综上所述,可将移动自组网风险评估的关键属性集定义为 $A = \{\text{丢包率 } a_1, \text{传输速度 } a_2, \text{信号强度 } a_3, \text{信号变化率 } a_4\}$,其中,传输速度与信号强度反映节点的可用性,而丢包率与信号变化率则反映通

信可靠性.整个定义过程如图 3 所示.

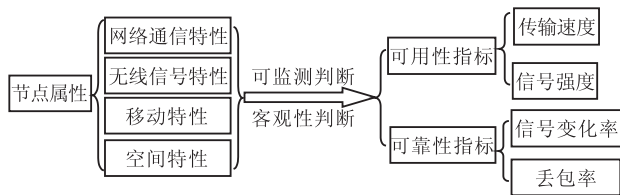


图 3 评估指标定义示意图

需要指出的是,这些属性一方面单位不同,属性极值不同,如丢包率是无量纲数据,值越小越好,但传输速度单位是千字节每秒,值越大越好,另外一方面,各个节点表现特性无法完全确定,如节点 A 丢包率低,但传输速度慢,节点 B 丢包率高,但信号强度可观,同时由于节点动态性,采集的样本不可能很多,因此无法直接通过数值统计或是概率的方法进行评估,而引入灰色聚类分析则可以较为有效地进行聚类判断.

4.2 灰类集定义

根据评估目的,定义灰类集 $G = \{g_1, g_2, g_3\}$,其中 g_1 表示与该节点通信风险很低, g_2 表示风险一般, g_3 表示风险较高.

4.3 白化函数定义

针对每个评估指标,可以根据通信的需求以及网络指标要求,定义其白化函数.不妨设采用 802.11b 无线设备组建移动自组网,其理想传输速度与距离如表 1 所示,在实际应用中,通常有一半的“原始速度”被分组负载、校验和、帧位、错误恢复数据和和其它“无用”的信息占用,即使不考虑传播范围和障碍物对性能的削弱影响,实际吞吐率也仅能达到最高传输速率的一半甚至更低,约为 0.5Mbps~5.5Mbps,在实际工作环境中,802.11b 室外有效工作范围为 300m,超过 550m 认为数据传输不可靠.根据这个原则,同时结合表 1 可知,对于传输速率,小于 0.5Mbps(63KB/s)为不可靠,大于 5.5Mbps(688KB/s)为可靠性高,而 2Mbps(250KB/s)左右为一般可靠;根据一般网络评估指标,丢包率小于 10%可认为可靠程度高,而 30%左右为正常丢包率,大于 70%则认为可靠性低;对于信号强度,802.11b 网络设备的发射功率根据国家无线电管理规定,不能超过 20dBm,即 100mW,因此可设网络设备发射功率为 100mW,根据自由空间模型^[18-19],可计算出在不同距离对应的信号功率.自由空间模型中,传输距离与功率衰减关系为

$$FSPL(\text{dB}) = 10 \log_{10} \left(\left(\frac{4\pi}{c} df \right)^2 \right)$$

$$=20\log_{10}(d)+20\log_{10}(f)+20\log_{10}\left(\frac{4\pi}{c}\right)$$
$$=20\log_{10}(d)+20\log_{10}(f)-147.56,$$

其中, $FSPL(\text{dB})$ 表示衰减的功率以 dBm 为单位, d 表示距离, c 表示光速, f 表示频率, 802.11b 使用 2.4GHz 频率. dBm 与 mW 的换算关系为

$$\text{mW}=10^{\text{dBm}/10} \text{ 或 } \text{dBm}=10\times\log_{10}\text{mW}.$$

表 1 802.11b 理想速度表

序号	距离/m	速度/Mbps
1	160	11.0
2	270	5.5
3	400	2.0
4	550	1.0

根据上述公式以及工作距离, 可知在 160m, 300m 以及 550m 处的衰减强度分别为 84.74dB、90.21dBm 以及 95.47dBm, 而网卡发射功率为 20dBm 左右, 因此, 当检测到的信号强度大于 $-64.74\text{dBm}(3.36\times10^{-7}\text{mW})$ 的时候, 可认为该节点信号较可靠, 在 $-70.21\text{dBm}(0.953\times10^{-7}\text{mW})$ 左右的时候该节点为一般可靠, 在 $-75.47\text{dBm}(0.284\times10^{-7}\text{mW})$ 的时候, 则认为该节点信号不可靠. 对于信号变化率, 可结合移动速率进行判断, 不妨以一般文档传输作为判断, 假定移动自组网中需要传输的文件最大为 10MB, 在平均 2Mbps(250KB/s) 的速度下需要 40s, 以影响最大的直线远离方式运动, 则节点如果在该时间内运动了 550m, 可认为该文档无法完成传输, 此时, 信号变化率为 $95.47/40=2.39\text{dBm/s}$, 即信号变化率大于 2.39dBm/s 的时候, 可认为该节点通信风险高, 同理, 信号变化率小于 2.12dBm/s 的时候为低风险, 2.26dBm/s 左右为一般风险, 又设节点运动最大速度为 20m/s , 则信号变化最大值为 3.47dBm/s .

各个指标选定单位分别为: 丢包率采取百分比、无量纲单位; 传输速度采用 KB/s ; 信号强度采用 10^{-7}mW ; 信号变化率采用 dBm/s . 则针对各个指标的白化函数为

(1) 第 1 灰类(上灰类):

$$f_{11}(0,c_{11})=f_{11}(0,0.1),$$
$$f_{21}(c_{21},\infty)=f_{21}(688,\infty),$$
$$f_{31}(c_{31},\infty)=f_{31}(3.36,\infty),$$
$$f_{41}(0,c_{41})=f_{41}(0,2.12).$$

(2) 第 2 灰类(中灰类):

$$f_{12}(-,c_{12},+)=f_{12}(-,0.3,+),$$
$$f_{22}(-,c_{22},+)=f_{22}(-,250,+),$$

$$f_{32}(-,c_{32},+)=f_{32}(-,0.953,+),$$
$$f_{42}(-,c_{42},+)=f_{42}(-,2.26,+).$$

(3) 第 3 灰类(下灰类):

$$f_{13}(c_{13},\infty)=f_{13}(0.7,\infty),$$
$$f_{23}(0,c_{23})=f_{23}(0,63),$$
$$f_{33}(0,c_{33})=f_{33}(0,0.284),$$
$$f_{43}(0,c_{43})=f_{43}(2.39,\infty).$$

上述白化函数自变量针对不同属性有不同的单位, 在聚类分析前需要做统一化处理. 需要指出的是, 这些指标的制定是针对特定的传输要求提出的一个简化指标阈值, 实际中可针对具体的移动自组网采用相应的指标参数.

4.4 灰色聚类评估与味集群决策

设经过选择后有 3 个味集群, 针对 4 个被评估节点的样本矩阵分别为

$$D_1=\left\{\begin{matrix}0.23, 270, 1.10, 2.21\\0.81, 060, 0.30, 2.51\\0.12, 299, 1.46, 3.32\\0.35, 298, 3.41, 2.14\end{matrix}\right\},$$
$$D_2=\left\{\begin{matrix}0.31, 230, 1.01, 2.29\\0.75, 060, 0.26, 2.50\\0.07, 670, 4.12, 1.19\\0.12, 598, 3.34, 1.18\end{matrix}\right\},$$
$$D_3=\left\{\begin{matrix}0.13, 657, 5.12, 1.09\\0.89, 030, 0.16, 2.30\\0.31, 272, 1.17, 2.25\\0.28, 240, 0.89, 2.29\end{matrix}\right\}.$$

先对样本 D_1 进行灰聚类分析.

(1) 极性统一

考虑到样本属性中丢包率与其它属性极性相反, 先进行极性统一操作. 采用成本余值法将丢包率与信号强度变化率的极小值极性变换为极大值极性.

$$\xi_{i1}^*=1-\xi_{i1}, \left\{\begin{matrix}\xi_{11}^*=1-\xi_{11}=1-0.23=0.77,\\ \xi_{21}^*=1-\xi_{21}=1-0.81=0.19,\\ \xi_{31}^*=1-\xi_{31}=1-0.12=0.88,\\ \xi_{41}^*=1-\xi_{41}=1-0.35=0.65;\end{matrix}\right.$$
$$\xi_{i4}^*=3.47-\xi_{i4}, \left\{\begin{matrix}\xi_{14}^*=3.47-\xi_{14}=1.26,\\ \xi_{24}^*=3.47-\xi_{24}=0.96,\\ \xi_{34}^*=3.47-\xi_{34}=0.15,\\ \xi_{44}^*=3.47-\xi_{44}=1.33;\end{matrix}\right.$$

极性统一后的样本矩阵为

$$D_1^o = \begin{Bmatrix} 0.77, 270, 1.10, 1.26 \\ 0.19, 060, 0.30, 0.96 \\ 0.88, 299, 1.46, 0.15 \\ 0.65, 298, 3.41, 1.33 \end{Bmatrix}.$$

极性统一后,针对丢包率与信号变化率的上、中及下灰类白化函数变换为

$$\begin{cases} f_{11}(c_{11}, \infty) = f_{11}(0.9, \infty), \\ f_{12}(-, c_{12}, +) = f_{12}(-, 0.7, +), \\ f_{13}(0, c_{13}) = f_{13}(0, 0.3). \\ f_{41}(c_{41}, \infty) = f_{41}(1.35, \infty), \\ f_{42}(-, c_{42}, +) = f_{42}(-, 1.21, +), \\ f_{43}(0, c_{43}) = f_{43}(0, 1.08). \end{cases}$$

(2) 样本矩阵初值化

为统一白化函数,将样本矩阵按列(即按项目)初值化:

$$D_1^* = \begin{Bmatrix} \xi_{11}/\xi_{11}, \xi_{12}/\xi_{12}, \xi_{13}/\xi_{13}, \xi_{14}/\xi_{14}, \\ \xi_{21}/\xi_{11}, \xi_{22}/\xi_{12}, \xi_{23}/\xi_{13}, \xi_{24}/\xi_{14}, \\ \xi_{31}/\xi_{11}, \xi_{32}/\xi_{12}, \xi_{33}/\xi_{13}, \xi_{34}/\xi_{14}, \\ \xi_{41}/\xi_{11}, \xi_{42}/\xi_{12}, \xi_{43}/\xi_{13}, \xi_{44}/\xi_{14} \end{Bmatrix} = \begin{Bmatrix} 1.000, 1.000, 1.000, 1.000 \\ 0.247, 0.222, 0.273, 0.762 \\ 1.143, 1.107, 1.327, 0.119 \\ 0.844, 1.104, 3.100, 1.556 \end{Bmatrix}.$$

(3) 白化函数统一

根据上述的样本初值化矩阵,白化函数统一为第 1 灰类(上灰类):

$$\begin{cases} f_{11}^*(c_{11}, \infty) = f_{11}^*(1.169, \infty), \\ f_{21}^*(c_{21}, \infty) = f_{21}^*(2.548, \infty), \\ f_{31}^*(c_{31}, \infty) = f_{31}^*(3.055, \infty), \\ f_{41}^*(c_{41}, \infty) = f_{41}^*(1.071, \infty); \end{cases}$$

第 2 灰类(中灰类):

$$\begin{cases} f_{12}^*(-, c_{12}, +) = f_{12}^*(-, 0.909, +), \\ f_{22}^*(-, c_{22}, +) = f_{22}^*(-, 0.926, +), \\ f_{32}^*(-, c_{32}, +) = f_{32}^*(-, 0.866, +), \\ f_{42}^*(-, c_{42}, +) = f_{42}^*(-, 0.960, +); \end{cases}$$

第 3 灰类(下灰类):

$$\begin{cases} f_{13}^*(0, c_{13}) = f_{13}^*(0, 0.390), \\ f_{23}^*(0, c_{23}) = f_{23}^*(0, 0.233), \\ f_{33}^*(0, c_{33}) = f_{33}^*(0, 0.258), \\ f_{43}^*(0, c_{43}) = f_{43}^*(0, 0.857); \end{cases}$$

(4) 计算灰色聚类权

根据灰色聚类分析计算过程,灰色聚类权系数如表 2.

根据灰色聚类权公式:

$$\sigma_{ik} = \sum_{j=1}^e f_{jk}(\xi_{ij}) \eta_{jk}, \text{ 对节点 } 1(i=1) \text{ 的灰类 } 1(k=1), \text{ 有}$$

$$\begin{aligned} \sigma_{i1} &= \sum_{j=1}^e f_{jk}(\xi_{ij}) \eta_{jk} \\ &= f_{11}(\xi_{11}) \eta_{11} + f_{21}(\xi_{12}) \eta_{21} + \\ &\quad f_{31}(\xi_{13}) \eta_{31} + f_{41}(\xi_{14}) \eta_{41} \\ &= f_{11}(1) \cdot 0.149 + f_{21}(1) \cdot 0.325 + \\ &\quad f_{31}(1) \cdot 0.389 + f_{41}(1) \cdot 0.137 \\ &= 0.510. \end{aligned}$$

类似的,可得到 $\sigma_{12} = 0.908, \sigma_{13} = 0.411$.

同理,得到其它各个灰色聚类权后,形成表 3.

(5) 灰色聚类分析

对于节点 1,灰聚类序列 σ_1 :

灰类 1 灰类 2 灰类 3

$$\sigma_1 = \begin{pmatrix} \sigma_{11}, & \sigma_{12}, & \sigma_{13} \\ 0.510 & 0.908 & 0.411 \end{pmatrix}$$

$$\begin{aligned} \sigma_{1k^*} &= \max(\sigma_{11}, \sigma_{12}, \sigma_{13}) \\ &= \max(0.510 \quad 0.908 \quad 0.411) \\ &= 0.908 = \sigma_{12} \end{aligned}$$

$$k^* = 2.$$

表明节点 1 属于灰类 2,即“一般风险节点”;同理,可知节点 2 属于灰类 3,属于“高风险节点”;节点 3 属于灰类 2,属于“一般风险节点”;节点 4 属于“低风险节点”,得到评估结果集 $G_1^* = \{g_2, g_3, g_2, g_1\}$.

表 2 灰色聚类权系数表

	k=1				k=2				k=3			
	j=1	j=2	j=3	j=4	j=1	j=2	j=3	j=4	j=1	j=2	j=3	j=4
c_{jk}	1.169	2.548	3.055	1.071	0.909	0.926	0.866	0.960	0.390	0.233	0.258	0.857
$\sum_{j=1}^m c_{jk}$	7.843				3.661				1.738			
$\eta_{jk} = c_{jk} / \sum_{j=1}^m c_{jk}$	0.149	0.325	0.389	0.137	0.248	0.253	0.237	0.262	0.224	0.134	0.149	0.493

表 3 灰色聚类权表

	<i>i</i> =1			<i>i</i> =2			<i>i</i> =3			<i>i</i> =4		
	<i>k</i> =1	<i>k</i> =2	<i>k</i> =3	<i>k</i> =1	<i>k</i> =2	<i>k</i> =3	<i>k</i> =1	<i>k</i> =2	<i>k</i> =3	<i>k</i> =1	<i>k</i> =2	<i>k</i> =3
$\sigma_{ik}=\sum_{j=1}^cf_{jk}(\xi_{ij})\eta_{jk}$	0.510	0.907	0.411	0.192	0.411	0.992	0.471	0.531	0.068	0.772	0.671	0

灰色聚类是一种多因子评估,既有白化结果,又有灰类的区别.从以上计算过程及结果可知,该评估方法具备几个特点:①计算结果具有较好的离散性与区分度,各个灰类之间可明确区分,分辨率高,若以灰类聚类权差值与较大聚类权比值作为区分度,则各个节点灰类聚类权的最小区分度分别为 19.4%、53.4%、11.3%以及 13.1%,为移动自组网安全通信与风险决策提供有意义的基础.②计算结果具有较好的指标贴进度,白化函数的意义在结果中得到合理的体现,如节点 3 与节点 4 的各类指标在数值上若简单求和,结果完全相同,但是经过灰色聚类分析后,节点 3 虽然丢包率较低,但由于其信号变化过快,为通信带来不稳定的影响,经过灰色聚类分析后,依然划分为一般风险节点,而节点 4 信号较强,为通信提供了很好的保障,虽然其它各个指标性能一般,但仍然划分为低风险节点.③计算过程避免了计算综合指数等中间环节,从指标白化函数结合原始样本直接确定节点综合风险所属的灰类,意义十分明确,很适合软件作自动化处理.这 3 个特点综合体现了灰色聚类风险评估的有效性,该方法是一个既能反映节点风险的灰性,又具有直观、简洁语义的定量描述机制,为进一步进行大规模风险分析提供了较好的基础.

(6) 味集群决策

根据灰色聚类分析过程,由样本矩阵 D_2, D_3 , 同理可得到各个评估结果集: $G_2^* = \{g_2, g_3, g_1, g_1\}$, $G_3^* = \{g_1, g_3, g_2, g_2\}$, 形成味集群评估决策矩阵:

$$G^* = \begin{Bmatrix} g_2, g_3, g_2, g_1 \\ g_2, g_3, g_1, g_1 \\ g_1, g_3, g_2, g_2 \end{Bmatrix}.$$

根据决策算法,对于节点 1, $C(g_2)=2$, 为最大值, 对应灰类 g_2 ; 节点 2, $C(g_3)=3$, 为最大值, 对应灰类 g_3 ; 节点 3, $C(g_2)=2$, 为最大值, 对应灰类 g_2 ; 节点 4, $C(g_1)=2$, 为最大值, 对应灰类 g_1 . 所以最后决策结果为 $G^* = \{g_2, g_3, g_2, g_1\}$.

4.5 灰色聚类算法复杂性分析

针对灰色聚类风险评估方法,设有节点 n , 评估属性个数为 k , 极小属性个数为 k_1 , 则极大属性个数 $k_2=k-k_1$, 味集群个数为 q 个, 灰类的个数为 r . 整

个评估计算过程可分为 5 个阶段:(1) 极性统一阶段. 该阶段需要将极小属性极性转换为极大属性极性, 时间复杂度为 $O(k_1 \times n)$, $k_1 \leq k$. (2) 样本初值化阶段. 该阶段先将第 1 节点指标值全部置 1, 然后计算剩下的 $n-1$ 个节点的初值化值, 时间复杂度为 $O(k \times (n-1))$. (3) 灰色聚类权计算阶段. 该阶段分为两个子步骤, 聚类权系数计算子步骤中, 对每个灰类的白化函数阈值, 先是一个循环求和, 然后再通过一个循环求得各个属性的系数, 两个循环是串行的, 总时间复杂度为 $O(r \times k)$, 灰色聚类权计算子步骤中, 针对每个节点的每个灰类, 计算聚类权, 而聚类权计算时间复杂度为 $O(k)$, 因此, 该子步骤时间复杂度为 $O(n \times r \times k)$, 本阶段总的计算时间复杂度为 $O(r \times k) + O(n \times r \times k) = O(n \times r \times k)$. (4) 灰色聚类分析阶段. 该阶段对每个节点的灰类进行判断, 挑选一个最大的权值, 显然其时间复杂度为 $O(n \times r)$. (5) 味集群决策阶段. 该阶段对每个节点的每个灰类个数进行统计, 在统计时需要判断每个味集群对应该节点的灰类值, 最后挑选一个最大统计值对应的灰类作为决策结果, 因此, 其时间复杂度为 $O(n \times r \times q)$. 所以, 整个灰聚类风险评估方法的时间复杂度为

$$\begin{aligned} &O(k_1 \times n) + O(k \times (n-1)) + O(n \times r \times k) + \\ &O(n \times r) + O(n \times r \times q) \\ &= O(n \times r \times k) + O(n \times r \times q) \\ &= O(n \times r \times \max(k, q)). \end{aligned}$$

事实上, 移动自组网中的味集群一般由节点认为可信的其它节点组成, 数量非常有限, 可视为常量. 而灰类的个数为了决策方便, 一般只会设置有限的几个, 如本文中设计的 3 个, 因此, 总的时间复杂度等同于 $O(n \times k)$, 用类似的方法可分析出该评估方法的空间复杂度为 $O(n \times k)$. 需要指出的是, 评估系统中属性个数一般是确定的常量, 因此, 灰色聚类风险评估方法的计算复杂性完全可以接受, 是一种高效的评估方法.

5 小 结

移动自组网通信中节点风险评估是保障通信质

量的一个重要因素。本文结合灰色系统理论与移动自组网特点,提出了非完全信息节点风险评估方案,并证明了灰数白化函数存在以及灰聚类评估的原理。方案特点如下:

(1)采用灰类描述非完全信息节点的风险状态,引入灰数白化函数与灰色聚类对节点进行灰类判断,可针对移动自组网中样本少,信息不完全的节点进行评估,避免了传统基于概率方法需要大量样本的问题。

(2)采用味集群方法采集原始监测样本,避免使用主观评价的量化值,减少了一般信任评估方法中的恶意推荐。在灰聚类评估完成后,结合味集群进行决策,提高了评估的可靠性。

(3)引入成本余值法、样本初值化等方法解决移动自组网中多属性、双极性以及量化单位不确定的问题,提高了移动自组网基于灰色理论风险评估的客观性与适应性。

分析与实例计算表明,基于灰聚类的非完全信息节点风险评估方法能够有效地判断节点的风险状态,符合实际移动自组网风险评估需求,是一种适合计算机自动处理的风险评估方式。在后续工作中,我们将进一步研究移动自组网中味集群最佳偏离范围确定、灰数白化函数的准确定位以及灰聚类的动态性等内容。

参 考 文 献

- [1] Guha R, Kumar R, Raghavan P. Propagation of trust and distrust//Proceedings of the 13th International World Wide Web Conference Proceedings (WWW2004). New York, USA: Association for Computing Machinery, New York, United States, 2004: 17-22
- [2] Beth T, Borchering M, Klein B. Valuation of trust in open networks//Proceedings of the European Symposium on Research in Security (ESORICS). Brighton: Springer-Verlag, 1999: 59-63
- [3] Wang Y, Vassileva J. Bayesian network trust model in peer-to-peer networks//Proceedings of the 2nd International Workshop: AP2PC 2003—Agents and Peer-to-Peer Computing. Melbourne, Australia: Springer Verlag, Heidelberg, D-69121, Germany, 2003: 23-24
- [4] Yu B, Munindar P. An evidential of distributed reputation management//Proceedings of the 1st International Joint Conference on: Autonomous Agents and Multiagent Systems (AAMAS02). Bologna, Italy: ACM Press, 2002: 294-301
- [5] Jøsang A. Trust-based decision making for electronic transactions//Yngström L, Svensson T eds. Proceedings of the 4th Nordic Workshop on Secure Computer Systems. Kista: Stockholm University Press, 1999: 1-21
- [6] Tang Wen, Chen Zhong. Research of subjective trust management model based on the fuzzy set theory. Journal of Software, 2003, 14(8): 1401-1408(in Chinese)
(唐文, 陈钟. 基于模糊集合理论的主观信任管理模型研究. 软件学报, 2003, 14(8): 1401-1408)
- [7] Abdul-Rahman A, Hailes S. A distributed trust model//Proceedings of the 1997 New Security Paradigms Workshop. Cumbria, UK: ACM Press, 1998: 48-60
- [8] Theodorakopoulos G, Baras J S. Trust evaluation in Ad Hoc networks//Proceedings of the 2004 ACM Workshop on Wireless Security. Philadelphia, USA: ACM Press, 2004: 1-10
- [9] Buchegger S, Boudec J L. A robust reputation system for P2P and mobile Ad-hoc networks//Proceedings of the 2nd Workshop on the Economics of Peer-to-Peer Systems. Harvard University, Boston, Cambridge MA, 2004: 1-10
- [10] Xiong L, Liu L. PeerTrust: Supporting reputation-based trust in peer-to-peer communities. IEEE Transactions on Data and Knowledge Engineering, Special Issue on Peer-to-Peer Based Data Management, 2004, 16(7): 843-857
- [11] Marti S, Giulì T J, Lai K, Baker M. Mitigating routing misbehavior in mobile Ad hoc networks//Proceedings of the 6th ACM International Conference on Mobile Computing and Networking. NY USA, ACM, 2000: 255-265
- [12] Buchegger S, Boudec J L. Performance analysis of the CONFIDANT protocol: Cooperation of nodes fairness in dynamic ad hoc networks//Proceedings of the IEEE/ACM Symposium on Mobile Ad Hoc Networking and Computing. Lausanne, 2002: 226-236
- [13] Pietro Michiardi, Refik Molva. CORE: A collaborative reputation mechanism to enforce node cooperation in mobile Ad hoc networks//Proceedings of the 6th IFIP Conference on Security Communications and Multimedia (CMS 2002). Portoroz, Slovenia, 2002: 107-121
- [14] Fu Cai, Hong Fan, Hong Liang, Peng Bing, Cui Yong-Quan. Mobile Ad Hoc secure routing protocol based on trust preserving. Chinese Journal of Computers, 2007, 30(10): 1853-1863(in Chinese)
(付才, 洪帆, 洪亮, 彭冰, 崔永泉. 基于信任保留的移动 Ad Hoc 网络安全路由协议 TPSRP. 计算机学报, 2007, 30(10): 1853-1864)
- [15] Xu Lan-Fang, Hu Huai-Fei, Sang Zi-Xia, Xu Feng-Ming, Zou De-Qing. A prestige reporting mechanism based on gray system theory. Journal of Software, 2007, 18(7): 1730-1737(in Chinese)
(徐兰芳, 胡怀飞, 桑子夏, 徐凤鸣, 邹德清. 基于灰色系统理论的信誉报告机制. 软件学报, 2007, 18(7): 1730-1737)
- [16] Deng Ju-Long. Grey Theory Base. Wuhan: Huazhong University of Technology & Science Press, 2002(in Chinese)
(邓聚龙. 灰理论基础. 武汉: 华中科技大学出版社, 2002)

[17] Deng Ju-Long. Grey Prediction and Decision. Wuhan: Huazhong University of Technology & Science Press, 2002 (in Chinese)
(邓聚龙. 灰预测与灰决策. 武汉: 华中科技大学出版社, 2002)

[18] Liu Ming, Gong Hai-Gang, Mao Ying-Chi, Chen Li-Jun, Xie Li. A distributed energy-efficient data gathering and aggregation protocol for wireless sensor networks. Journal of

Software, 2005, 16(12): 2106-2116(in Chinese)
(刘明, 龚海刚, 毛莺池, 陈力军, 谢立. 高效节能的传感器网络数据收集和聚合协议. 软件学报, 2005, 16(12): 2106-2116)

[19] Heinzelman W R. An application-specific protocol architecture for wireless microsensor networks. IEEE Transactions on Wireless Communications, 2002, 1(4): 660-670



FU Cai, born in 1976, Ph. D. , lecturer. His main research interests include wireless networking security, routing algorithms and software vulnerability.

HONG Liang, born in 1979, Ph. D. , lecturer. His main research interests include networking, routing algorithms and security in Ad hoc networks.

Background

Now, in mobile Ad hoc networks, the problems on uncertainty and less data little sample exist commonly, the ones in myriad sample can be solved by probability and statistics ways, the ones in kenning uncertainty can be dealt with by fuzzy mathematics. However, In true Ad hoc networks, the exposed information of some nodes is little, which is more serious to some vicious nodes, the samples are so little that the clear state can't be identified and most are incomplete information, which result in that the assessment is not objective and credible. This paper proposes a Ad hoc networks risk assessment method based on grey theory. The authors focus on the following three aspects;

(1) The less data little sample, incomplete information

PENG Bing, born in 1972, Ph. D. , lecturer. His main research interests include wireless networking security and cryptology.

HAN Lan-Sheng, born in 1972, Ph. D. , Ph. D. supervisor. His main research interests include access control and cryptology.

XU Lan-Fang, born in 1956, professor, Ph. D. supervisor. Her main research interests include information security and security model.

and devoid experience are dealt with grey system theory, which suit the mobile Ad hoc networks proved by the samples computing and theory analysis.

(2) Original data is collected through using taste course method, which can reduce the vicious recommendation.

(3) The special data initializing method is used to unify the data sample to make the grey clustering more efficient.

This work is supported by the Natural Science Foundation of Hubei Province under grant No.2008CDB352 and the National Natural Science Foundation of China under grant Nos.60703048 and 60803158.