同济大学
TONGJI UNIVERSITY

毕业设计（论文）
外文科技文献译文

译文题目：	基于复杂网络理论的城市轨道交通脆弱性分析：上海地铁的案例研究
外文题目：	Vulnerability analysis of urban rail transit based on complex network theory: a case study of Shanghai Metro
学　　院：	交通运输工程学院
专　　业：	交通运输
学　　号：	2052105
姓　　名：	宋禧
指导教师：	滕靖
校外指导教师：	伍敏
日　　期：	2024 年 06 月 01 日

基于复杂网络理论的城市轨道交通脆弱性分析：上海地铁的案例研究

Yingying Xing · Jian Lu · Shengdi Chen ·Sunanda Dissanayake

摘要

随着客流和建设规模的增加，大都市的地铁系统已经进入了网络运营的新时代，成为缓解和减少交通拥堵的最有效方式。然而，随机故障和蓄意攻击的频繁发生对地铁安全和可靠性构成了严重威胁。因此，从网络的角度定量评估地铁网络对不同故障或攻击的脆弱性是必要的。基于复杂网络理论，本研究以上海地铁网络（SMN）为例，研究了加权地铁网络在应对随机故障和蓄意攻击方面的脆弱性。特别是与拓扑网络相比，通过分析加权网络的脆弱性来研究交通和空间约束如何影响交通系统的脆弱性，因为复杂网络的拓扑特征通常与边的权重和空间约束有关。模拟结果表明，SMN 对随机故障具有鲁棒性，但对蓄意攻击则脆弱。加权属性的脆弱性分析表明，所有有针对性的攻击都能在影响很少节点的情况下破坏网络的通信或运输属性，并且在五种攻击或故障策略中，从最高节点介数攻击策略能最有效对 SMN 造成破坏。其中客流提供了证据，表明拓扑网络不能传达所有现实世界网络的信息，网络中的交通流量应被视为发掘和发展防御策略的关键特性之一。本文的研究结果为现实世界中的复杂加权网络提供了更为丰富的视角，并为地铁运营部门的风险分析和政策决策提供了可能性。

关键词：地铁安全、脆弱性分析、复杂网络、客流、鲁棒性

1 引言

由于交通量增加和城市建设用地需求增长，许多大都市不断增加地铁线路建设投资以缓解严重的交通拥堵。随着越来越多的新线路投入使用，许多地铁系统如纽约市地铁、上海地铁和东京地铁已经转变为具有高站点密度和复杂的站间耦合关系的复杂地铁网络，引领网络运营的新时代(Angeloudis and Fisk 2006; Xu and Sui 2007; Yang et al. 2015)。然而，历史表明，由于相对封闭的结构和地铁系统内的大客流，地铁系统在紧急情况下面临危险环境。近年来，针对地铁系统的蓄意攻击，如有针对性的破坏和报复性干扰频繁发生；此类事件可能导致整个系统功能丧失，造成重大人员伤亡和社会经济损失。例如，2010 年发生在俄罗斯 Lubyanka 地铁站和 Park Kultury 地铁站的恐怖袭击造成至少 40 人死亡。此外，随机故障的频繁发生表明，不合理的规划和不足的安全预防措施会损害地铁系统的整体可靠性(Albert and Baraba´si 2002; Newman et al. 2001; Wang 2013; Zhou et al. 2014)。显然，规模和复杂性的增加使地铁系统更加依赖于系统的脆弱性分析和相应应对策略的制定，以增强地铁网络的鲁棒性。然而，交通规划者更关注传统特征，如地理、需求、成本等；似乎没有人直接从网络设计入手，这随着交通系统的增长变得越来越重要。同样，交通政策制定者和运营商更多地考虑车站的本地属性（如客流、连接车站的数量），而不是其在整个地铁网络中的位置和作用。因此，有必要从整体的角度对地铁网络的脆弱性进行全面分析。

在过去的几年中，图论和复杂网络理论已被用于研究大规模交通基础设施（铁路、公路

和航空），并成为从系统视角识别运输网络中脆弱组件（例如，边或节点）的强大工具(Ouyang et al. 2014; Taylor et al. 2007; Berdica and Mattsson 2007; Guimera´ and Amaral 2004; Wang et al. 2011)。通过检查世界上十四个主要城市的公共交通网络，Berche 等（2009）识别了特别容易受到攻击的公共交通网络结构和其他特别具有弹性的网络结构。Derrible 和 Kennedy（2010）分析了 33 个地铁系统的复杂性和鲁棒性，并为增强地铁网络的鲁棒性提供了建议。Laporte 等（2010）提出了一个整数线性规划模型，用于在区间故障和竞争模式存在的情况下设计公共交通网络。Zhang 等（2011）通过图论和复杂网络理论研究了地铁网络的连通性、鲁棒性和可靠性。根据分析和讨论，研究发现地铁网络对随机攻击具有鲁棒性，但对蓄意攻击则脆弱。Han 等（2012）从干扰、暴露和脆弱性三个方面分析了城市公共交通事故。他们将脆弱性视为系统的固有缺陷，并建立了理论安全保障机制。Yuan 等（2012）回顾了地铁事故的统计数据，并提出了地铁网络系统的物理、结构和社会脆弱性的概念。尽管如此，这些研究都通过图论简化了地铁网络，只考虑了网络拓扑。因此，它们缺乏对地铁系统动态属性的考虑。

也有学者采用其他方法对地铁网络的脆弱性进行了分析。Cats 和 Jenelius（2012）提出了公共交通网络脆弱性的动态和随机概念，并开发了一个更精细的模型，通过考虑供需互动来评估公共交通网络的脆弱性。De-Los-Santos 等（2012）从用户的角度进行了铁路交通网络的鲁棒性度量。基于前辈的工作，Perea 和 Puerto（2013）讨论并扩展了一个针对故意攻击的鲁棒铁路网络设计的博弈论框架。Rodríquez-Núñez 和 García-Palomares（2014）提出了一种分析公共交通网络关键性和脆弱性的方法。基于 7/7 伦敦爆炸案和其他地铁事件的经验，Bruyelle 等（2014）识别了地铁教练的关键系统，并提出了增强地铁系统鲁棒性的改进措施。以北京地铁系统为例，Yang 等（2015）评估了地铁网络在面对随机故障和蓄意攻击时的鲁棒性。研究结果揭示了北京地铁系统具有典型的无标度网络特征，在面对随机故障时具有相对高的稳定性和鲁棒性，但当枢纽受到蓄意攻击时，容错性相对较低。Cats 等（2015）提出了一种考虑暴露程度的方法，用于识别和评估公共交通网络中的区间关键性。Chopra 等（2016）提出了一个全面的、多方面的框架，分析了网络拓扑、空间组织和客流的信息，以了解伦敦地铁系统的弹性。这些研究提供了有关影响地铁系统可靠性和脆弱性的网络属性的有用见解，并将客流和地理空间纳入网络模型将进一步增强网络模型，提供更丰富的视角来分析城市轨道交通网络的脆弱性。模拟不同站点在不同攻击策略下的故障情况（单节点-多节点-网络），可以帮助识别网络中的关键节点，这对铁路交通规划者和管理者有很大参考价值。

因此，本文进行了系统的城市轨道交通脆弱性分析，为城市轨道交通网络的规划和运营提供理论支持。本文以交通和地理空间的加权地铁网络为研究对象，探讨交通和空间约束如何影响交通系统的脆弱性。讨论了包括蓄意攻击和随机故障在内的不同攻击策略，以确定破坏整个地铁网络的最有效模式。特别地，本文讨论和比较了可用于识别加权网络中最关键节点的拓扑、动态和依赖损伤的方法。整个网络的功能取决于对这些关键节点的保护。此外，分析对比了加权网络与拓扑网络的脆弱性。根据研究发现，提出了几项措施来加强地铁网络的结构鲁棒性，这可能有助于发展针对针对性攻击的适应性反应。根据研究结果，提出了几项措施来加强地铁网络的结构鲁棒性，这可能有助于开发应对针对性攻击的自适应反应。

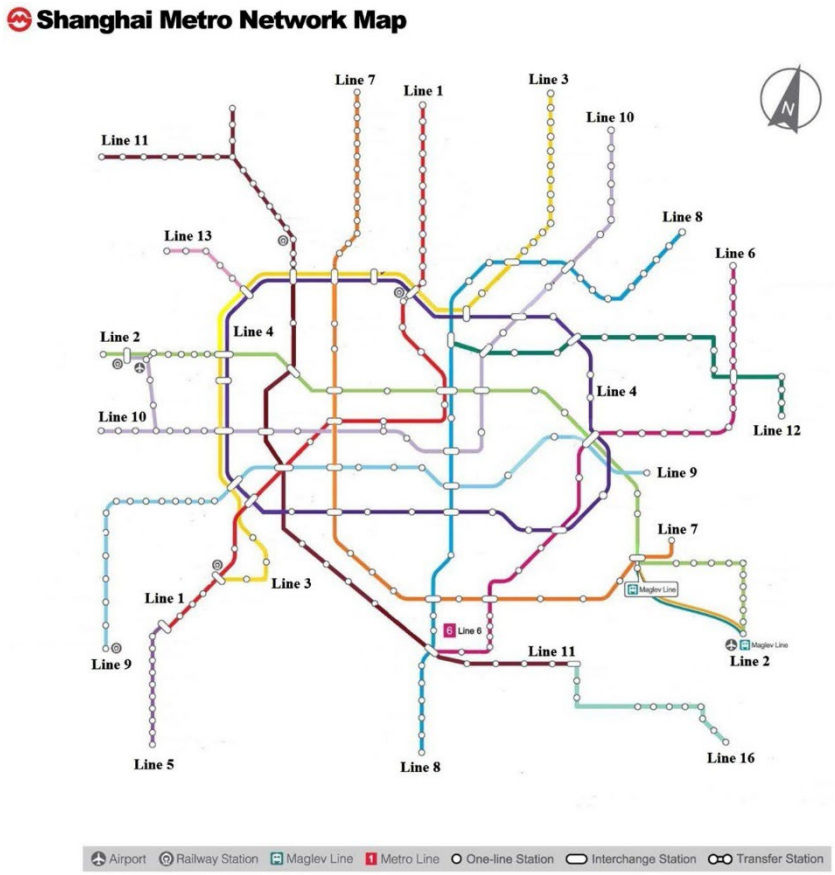

图 1 上海地铁线网示意图（来源：上海申通地铁公司网站）

2 背景

2.1 上海地铁系统

上海是中国最大的城市之一，拥有超过 2000 万人口。随着人口的快速增长，上海的城市交通拥堵问题变得日益严重，迫切需要解决。为了提高公共交通的容量和可达性，上海建设了一个超过 500 公里的巨大地铁网络，交通拥堵得到了缓解。截至 2014 年 12 月，上海地铁网络（SMN）是世界上路线长度最长的快速交通系统（Riedel 2014），拥有 14 条线路、286 个站点、39 个换乘站点，总里程超过 540 公里（图 1）。2014 年，上海地铁以 28 亿次的年客运量排名世界第二，仅次于北京。2014 年平均每天有 102.86 百万人乘坐上海地铁。2014 年 12 月 31 日上海地铁刷新了最高单日客运量，为 1028.6 万人次，同时超过 800 万人在工作日乘坐上海地铁。

SMN 由 286 个代表车站的节点和 317 条连接相邻站点的边组成。正如先前文献（Zhang 等 2011）所观察到的，上海地铁网络的拓扑结构显示出无标度和小世界特性。上海申通地铁公司提供了相关数据：每个站点的小时进出站客流以及相邻站点之间的客流数据。在本研究中，分析了典型工作日早上 7:00 至 9:00 的高峰时段客流，这是一周中可观察到的最大客流量。

2.2 网络脆弱性的基本概念

交通系统脆弱性还没有能够被学术界普遍接受的定义（Mattsson 和 Jenelius 2015）。但 Berdica（2002）提出的定义经常被其他文献引用：“道路运输系统的脆弱性是指系统对可能导致道路网络服务能力大幅降低的事件的敏感性。” 这个定义也适用于其他交通方式。Luathep 等（2011）认为，脆弱性分析主要在于当网络出现随机故障或遭到蓄意攻击时，识别网络中导致最大影响的关键组件。 Berdica 和 Mattsson（2007）提出，交通网络的脆弱性可以被视为一个整体框架，通过它可以进行不同的交通研究，以确定交通系统在面对不同类型和强度的干扰时的表现。Berche 等（2009）指出，脆弱性对于评估某个站点以及整个网络的容错性至关重要。Yang 等（2015）定义了攻击脆弱性，即地铁网络在故意攻击下的存活性。在本研究中，网络脆弱性的概念被用来描述地铁网络在面临各种威胁和危险时缺乏服务能力的情况。威胁和危险是地铁网络潜在损害的来源。危险指的是意外事件（如自然灾害和系统故障），而威胁与故意事件（例如，恐怖袭击）有关。

2.3 不同故障的定义

地铁网络系统通常会遇到各种紧急情况和面临复杂的外部环境，如自然灾害、系统故障和恐怖袭击，总体可以分为两种类型的事件，即随机故障和故意攻击（Kyriakidis 等 2012；Wang 等 2014；Wang 2013）。地铁事故通常是由于一些不同的事件引起的，从自然灾害到蓄意攻击（Kyriakidis 等 2014；Wang 和 Fang 2014）。由于这些突发事件的不确定性，定量地确定每种故障或攻击的相应破坏力是极其困难的。因此，本文将故意攻击定义为由人工力量操纵的蓄意或有针对性的破坏，而随机故障被指定为由于一个或几个节点随机概率的故障而导致的网络功能障碍（Ghedini 和 Ribeiro 2011；Zhang 等 2012）。根据定义，这两种事件的主要区别在于，随机故障的概率在所有站点之间是相等的，而故意攻击通常发生在具有高节点度或高介数中心性的枢纽站点。这两种事件总结在表 1 中。

表 1 地铁系统常见故障和攻击行为汇总

网络故障	事故原因	案例
随机故障	技术故障	钢轨裂纹/其他严重钢轨缺陷、车轮破损、制动功能丧失、信号故障、电源故障、车门故障
	乘客和地铁工作人员	拥堵、自杀、坠轨、扶梯坠落、楼梯坠落、被列车撞伤、醉酒造成无意识破坏、车站/列车抽烟、乘客携带危险或易燃物品、被车门夹住、司机误操作、超过速度限制、危险信号通过 (SPAD)
	管理行为	车站全封闭、车站出入口封闭、线路临时维护
	外部环境	恶劣天气、轨道上的物体、超出间隙限制的物体
蓄意攻击	蓄意或针对性破坏	恐怖主义、破坏公物、乘客携带危险或易燃物品、侵入、放火、枪击、群体斗殴

3 研究方法

3.1 构建加权 SMN 模型

为了分析城市轨道交通系统的各种特性，需要定义一个适当的网络拓扑来描述 SMN 网络的结构。地铁系统通过使用各种网络表示法，可以被简化为网络，如 Space L、Space P、Space B 和 Space C 网络拓扑（Sienkiewicz 和 Hołyst 2005；von Ferber 等 2007；Xu 等 2007a，b；Berche 等 2010）。关于地铁系统的每种网络拓扑方法都提供了其独特的拓扑见解。例如，SpaceL 主要用于研究地铁系统的拓扑属性和脆弱性，而 Space P 广泛用于探索换乘特性，如地铁线路对换乘时间的影响（von Ferber 等 2007）。

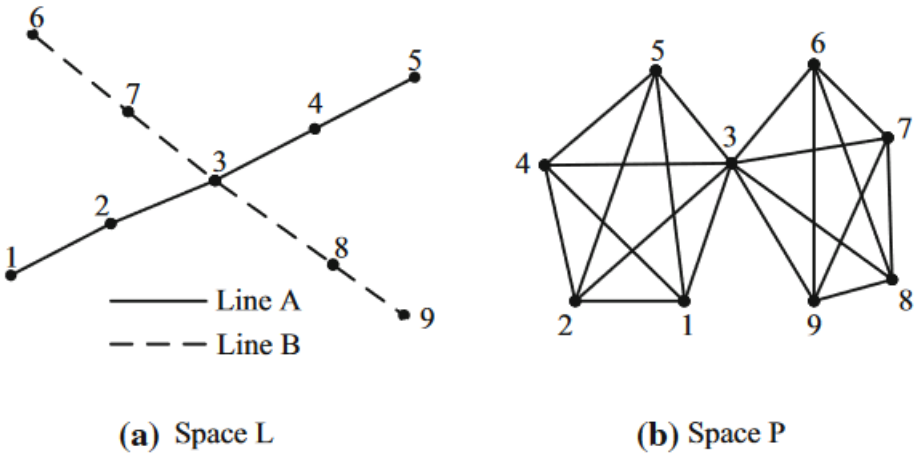

图 2 Space L(a)和 Space P(b)的说明

如图 2 所示，Space L 网络拓扑由代表站点的节点和连接物理相邻站点的边组成，换句话说，如果至少有一条线路为两个连续站点提供服务，则两个节点之间存在一条边。不允许有多重链接（Berche 等 2009）。在这个拓扑网络中，节点的节点度k是它与其他节点共享的边的数量，而距离l是从某个节点到另一个节点跨越边的数量最少。Space L 拓扑是对地铁系统的直观地理表示，允许我们以最简单的方式模拟区间故障并分析其后果（Chopra 等 2016）。在 Space P 中，虽然节点与 Space L 中的节点相同，但这里两个节点之间的边意味着至少有一条地铁线路直接连接它们。因此，这个拓扑中的节点度k是使用单线可达的节点总数，距离可以解释为“最少线路变化数-1”，以便让乘客成功地从一个站点到达另一个站点。这一主要特征使我们能够讨论地铁网络的换乘属性。因此，本文研究选择了 Space L 拓扑方法对 SMN 的网络进行拓扑建模。

到目前为止，大多数研究都集中在未加权网络上，即具有二元性质的网络，其中节点之间的边要么存在，要么不存在。然而，随着复杂的拓扑结构，许多现实网络在连接的能力和强度上显示出很大的特异性。因此，引入了加权网络来描述现实网络的特征和属性。一个加权图$G^w = (V, E, W)$，其中每条边绑定一个数值来衡量连接的强度，由一组节点$V = \{v_i \mid i = 1, 2, \dots, N\}$、一组边$E = \{e_{ij} = (v_i, v_j) | i, j = 1,2, \dots, N, i \neq j\}$和一组权重$W = \{w_{ij} | i, j = 1,2, \dots, N, i \neq j\}$组成，这些权重是附加到边的实数。在矩阵表示中，通常可以用邻接权重矩

阵A^w表示，邻接元素a_{ij}定义为：

$$a_{ij} = \begin{cases} w_{ij}, & (v_i, v_j) \in E \\ 0 \ or \ \infty, & (v_i, v_j) \notin E \end{cases}, \tag{1}$$

其中w_{ij}是连接节点v_i和节点v_j的边的权重，$a_{ij} = 0$ 或∞取决于边的权重是否不同。不同的权重的含义：权重越高，路径长度越大，两个节点之间的连接越疏远，例如邮递员问题中的距离。相反，权重越高，路径长度越小，两个节点之间的连接越紧密，例如科学合作网络中的合作频率的权重。因此，对于相似的权重，如果节点i和j通过节点k连接，则距离$d_{ij} = w_{ik} + w_{kj}$。对于其他的权重，如距离与边的权重成反比，即$d_{ik}^s = \frac{1}{w_{ik}}$，节点$i$和$j$之间的距离可以通过方程$d_{ij}^s = \frac{w_{ik} \times w_{kj}}{w_{ik} + w_{kj}}$计算。基于复杂网络理论，SMN 的站点可以由网络的节点表示，直接连接两个站点的线路可以虚拟化为网络的边。SMN 的许多不同变量可以被视为网络的权重，包括客流、站点间距、出行时间等。此外，假设典型的出行是双向的，因此一对节点（站点）i和j之间的边的权重w_{ij}被定义为两个方向的客流之和，且$w_{ij} = w_{ji}$。

3.1.1 节点度和强度

加权复杂网络最显著的特征是节点之间权重w_{ij}的特异性，它描绘了系统中组件之间的相互作用。对于一个未加权网络中的给定节点i，其节点度$k_i = \sum_{j=1}^{N} a_{ij}\, w_{ij}$是它链接到的节点数量。随后，在加权网络中，通过引入强度s_i，获得了一个更有意义的网络属性度量值，定义s_i为

$$s_i = \sum_{j=1}^{N} a_{ij}\, w_{ij}. \tag{2}$$

从方程(2)中，s_i结合了节点度k_i和边权重w_{ij}，是加权网络中节点i的中心性或连通性的自然度量。对于 SMN，节点强度只考虑了每个站点需要处理的总客流量。

3.1.2 加权最短路径

最短路径在网络内的运输和通信中起着重要作用。图 G 的所有最短路径长度可以表示为一个矩阵 D，其中元素l_{ij}定义为从节点v_i到节点v_j经过的最短路径。特征路径长度，也称为平均路径长度，是所有可能的网络节点对的最短路径长度的平均数（Nawrath 2006），可以表示为

$$L = \frac{1}{N(N-1)} \sum_{i,j \in V (i \neq j)} l_{ij}\,. \tag{3}$$

在一般的加权网络中，两个节点v_i和v_j之间的路径长度可以引入为权重w_{ij}的函数，这取决于边的权重是不同的还是相似的。在本研究中，具有最小数量边的最短路径不是最优的。定义加权最短路径长度d_{ij}为从节点v_i到节点v_j的所有可能路径中边长的最小值之和，其中边长指的是站点间距。很明显，站点间距是一个不同的权重。然后，平均最短路径长度可以定义为

$$\mathrm{L} = \frac{1}{N(N-1)} \sum_{i,j \in V (i \neq j)} d_{ij}. \tag{4}$$

3.1.3 节点介数

两个不相邻节点之间的连接依赖于连接它们的路径。因此，可以通过计算经过它们的最短路径的数量占比来获得给定节点的相关度量，并由此给出节点介数的定义。与节点度一样，介数是衡量节点中心性的一个标准度量，量化了节点在网络中的影响和重要性。更准确地说，节点i的介数b_i定义为（Boccaletti 等 2006）：

$$b_i = \sum_{j,k \in V, j \neq k} \frac{n_{jk}(i)}{n_{jk}} \tag{5}$$

其中n_{jk}是j到k的最短路径总数，$n_{jk}(i)$是通过节点i的这些最短路径的数量。在加权网络中，不等的边长度使得网络中连接两个节点的某些特定路径比其他路径更有利（Dall’Asta 等 2006）。因此，很自然可以通过用它们的加权版本替换节点对之间的最短路径来推广介数中心性的概念。类似于方程(5)，节点i的加权介数b_i^w可以定义为：

$$b_i^w = \sum_{j,k \in V, j \neq k} \frac{n_{jk}^w(i)}{n_{jk}^w} \tag{6}$$

其中n_{jk}^w是j到k的加权最短路径总数，$n_{jk}^w(i)$是通过节点i的这些路径的数量。

在所有边的权重$w_{ij} = 1$的特殊情况下，加权最短路径长度d_{ij}简化为从节点v_i到节点v_j所需的最少边数。对于地铁系统，节点介数代表了站点在网络中的地位和影响，中心站点比边缘站点包含更多的最短路径。

3.2 攻击策略和随机故障

攻击策略描述了对手攻击网络的方式，而随机故障被指定为由于意外事件导致的网络功能障碍。在随机故障的情况下，每个节点或边以相等的概率发生故障。相反，在蓄意攻击中，对手优先攻击他认为将最大化对网络完整性和功能破坏效果的目标。一个复杂的网络通常会遇到两种类型的事件，节点攻击和边攻击。考虑到地铁系统的特点，采用了节点攻击策略，即通过从网络中移除一个节点及其相关的边来攻击网络。对于地铁系统，节点移除意味着站点完全故障，短期内无法恢复功能。此外，假设对手的目的是尽快最大化破坏效果并摧毁网络。为此，对手首先需要评估一个节点的重要性，以识别地铁网络中最重要的节点。因此，生成攻击策略的节点重要性排名至关重要。一般来说，不同的对手从不同的方面对节点重要性进行排序，导致不同的破坏效果。

基于对最重要节点的中心性排名的不同定义，引入了五种不同的攻击策略，以研究地铁网络在蓄意攻击或随机故障下的脆弱性。此外，每次攻击后重新计算网络的节点中心性度量，已被证明是最有效的策略（Petter 等 2002；Dall’Asta 等 2006），因为每次节点删除都会引起其他节点中心性属性的变化。更准确地说，蓄意攻击策略和随机故障被设计如下。（1）根据节点排名进行蓄意攻击，包括度、强度、拓扑介数和加权介数。也就是说，从初始状态开始，最重要的节点及其相关的边将被删除，所有加权网络的属性可以在删除后重新计算，攻击将继续进行。（2）随机故障。节点将被随机删除，每次攻击后都可以重新计算加权网络的属性。节点将根据这五种不同的攻击或故障策略逐个从网络中移除。

3.3 网络整体性能评估模型

在研究评估模型时，另一个需要考虑的关键问题是如何在各种攻击下衡量网络的全局性能。网络脆弱性可以通过许多方式来表征，例如通过观察在节点不断被攻击的情况下最大连通子图的相对大小的变化（Crucitti 等 2003；Berche 等 2009；Ghedini 和 Ribeiro 2011）。最大联通子图的大小快速下降表明网络脆弱形高。网络性能也可以通过网络效率来评估，通过计算任意两个节点之间的最短距离，表征网络的通信功能（Zhang 等 2011；Yang 等 2015）。因此，可以将两个指标结合起来，以评估 SMN 在不同事件下的性能。

3.3.1 最大连通子图的相对大小

如果图中的任何两个节点都是连接的，那么图 G 被称为连通图。当节点受到攻击并从网络中删除时，整个连通图将分裂成多个子图和断开的部分（图 3）。最大连通子图是具有最多连接节点的子图。在未加权网络中，最大连通簇 LCC 是通过最大连通子图的相对大小来定义的，可以描述如下：

$$LCC = \frac{N}{N_0} \tag{7}$$

其中 N 是攻击后最大连通子图上的节点数，N_0是初始网络中最大连通图的节点数。为了评估加权网络的可靠性和鲁棒性，将强度s与最大连通簇结合起来，在加权情况下定义LCC^w为：

$$LCC^w = \frac{S}{S_0} \tag{8}$$

其中 S 是攻击后最大连通子图上节点强度的总和，S_0是初始网络中最大连通图上节点强度的总和。这个指标衡量了网络在局部范围内的结构完整性，因为它指的是在网络的最大连通部分中仍然能够处理的相对流量或客流。

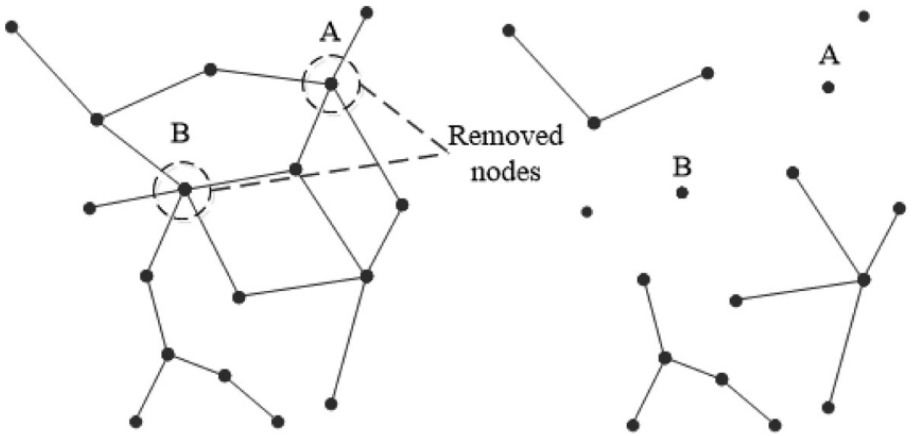

图 3 节点移除前后的连通图结构

3.3.2 网络效率

平均路径长度是网络效率的自然度量，对网络中的运输和通信有重大影响。然而，当网络受到攻击并且节点断开连接时，两个未连接节点的最短路径长度将在邻接矩阵中变为无限大，无法计算。为了解决这个问题，本文定义了一个计算“网络效率”的替代方法，这在许

多情况下都很有用：

$$E = \frac{1}{N(N-1)} \sum \frac{1}{d_{ij}}. \quad (9)$$

变量 E 是地铁网络交通容量的指标，避免了平均路径长度的发散。它有助于探索 SMN 对不同事故的全局反应。具有高网络效率的地铁系统意味着在正常运营条件下出行是快速方便的。在加权网络中，自然通过用它们的加权版本替换最短路径来推广网络效率的概念。SMN 的空间属性体现在物理空间距离上，以公里为单位，表征每个连接边。

4 研究结果

4.1 站点脆弱性

在复杂的交通系统中，并非所有站点都是等效的。传统研究通常将节点的度中心性视为评估节点重要性的唯一度量。但是，介数也是衡量节点全局功能的重要指标，并已被用作节点重要性评估的全局几何因素。然而，很少有研究关注通过攻击节点而非度或介数来衡量节点重要性。

表 2 和表 3 显示了当一个站点从网络中移除时，整个网络功能损失的百分比。如表 2 和表 3 所示，SMN 中具有最大强度和介数的站点是人民广场，它连接到其他站点的边有六条，在早高峰时承担近 700,000 名乘客。然而，其最大连通簇（LCC^w）和全局网络效率（GNE）的损伤值分别为 5.00%和 3.71%，都低于上海火车站、曹杨路和镇坪路。对 SMN 中造成LCC^w最大下降的站点是上海火车站，其下降比例为 6.58%，这意味着 6.58%的客流依赖于上海火车站，这是他们连接到其他站点的唯一选择。

表 2 强度排名前十的车站

排名	节点名	LCC^w下降比例(%)	GNE 下降比例(%)	节点度
1	人民广场	5.00	3.71	6
2	徐家汇	3.67	2.71	6
3	世纪大道	3.75	6.90	8
4	南京东路	2.96	2.22	4
5	静安寺	2.90	2.18	4
6	上海火车站	6.58	7.60	4
7	常熟路	2.82	1.76	4
8	中山公园	2.68	2.61	4
9	江苏路	2.55	1.60	4
10	陕西南路	2.52	1.56	4

表 4 显示了对LCC^w和网络效率影响最大的前十个站点。LCC^w的下降比例反映了网络被分割的程度。一般来说，移除一个节点不会对网络的完整性产生太大影响。但是，从表 4 可以看出，由于站点的关闭，网络分裂成更小的子网络和断开的部分，这将对 SMN 的常规运营产生重大影响。其中造成影响最大的是上海火车站，大约会影响 6.58%的客流。同时，我

们发现连接放射状地铁线路和核心区域的站点通常会对网络造成巨大影响，如上海火车站、宜山路和曹杨路，如图 4 所示。如果这些站点因蓄意攻击而暂时关闭，远离中心区域的放射状线路上的站点将失去与网络中其他站点的联系。而对于核心区域的站点，即使删除了枢纽站点，也可能不会导致网络断开或分割，对网络的完整性影响相对较小，例如徐家汇。这种现象也可以通过地铁网络路线来解释。以曹杨路为例，它是连接 11 号线和市中心的纽带。如果曹杨路受到攻击，曹杨路以北的站点将没有其他路线可以进入市中心，这将导致曹杨路区域发生交通拥堵。但是，如果徐家汇受到攻击，尽管许多乘客会受到影响，剩余的网络可以提供足够的替代路线选择，因此大量的乘客仍然可以通过其他替代路线到达目的地。

表 3 介数排名前十的车站

排名	节点名	LCC^w下降比例(%)	GNE 下降比例(%)	节点度
1	人民广场	5.00	3.71	6
2	徐家汇	3.67	2.71	6
3	世纪大道	3.75	6.90	8
4	上海火车站	6.58	7.60	4
5	南京东路	2.96	2.22	4
6	曹杨路	6.05	8.56	4
7	镇坪路	5.38	8.29	4
8	海伦路	1.39	3.03	4
9	东方体育中心	4.25	7.81	5
10	常熟路	2.82	1.76	4

表 4 对网络影响排名前十的车站

排名	节点名	LCC^w 下降比例(%)	节点度	节点名	GNE 下降比例(%)	节点度
1	上海火车站	6.58	4	四平路	9.64	4
2	宜山路	6.50	5	曹杨路	8.56	4
3	曹杨路	6.05	4	镇坪路	8.29	4
4	镇坪路	5.38	4	东方体育中心	7.81	5
5	人民广场	5.00	6	上海火车站	7.60	4
6	桂林路	4.74	2	枫桥路	7.29	2
7	上海南站	4.50	3	宜山路	7.07	5
8	中山北路	4.42	2	世纪大道	6.90	8
9	东方体育中心	4.25	5	岚皋路	6.88	2
10	枫桥路	4.20	2	虹口足球场	6.76	4

其次，在网络效率方面也观察到了类似的情况，值得注意的是一些连接度高的站点，如世纪大道、徐家汇，却具有相对较小的损伤值。相比之下，一些损伤值大的站点，如桂林路和中山北路，连接度相对较小。这些结果揭示了换乘站点可能并不比普通站点影响更大。这

与传统观点不同，传统观点重视换乘站点而忽视普通站点。经过详细研究后，我们发现这些普通站点更有可能导致网络分裂，值得投入更多关注。上述分析为识别站点的重要性提供了新的视角，并表明站点的重要性可以通过删除节点对网络的影响来衡量，而不仅仅是度中心性或介数中心性。

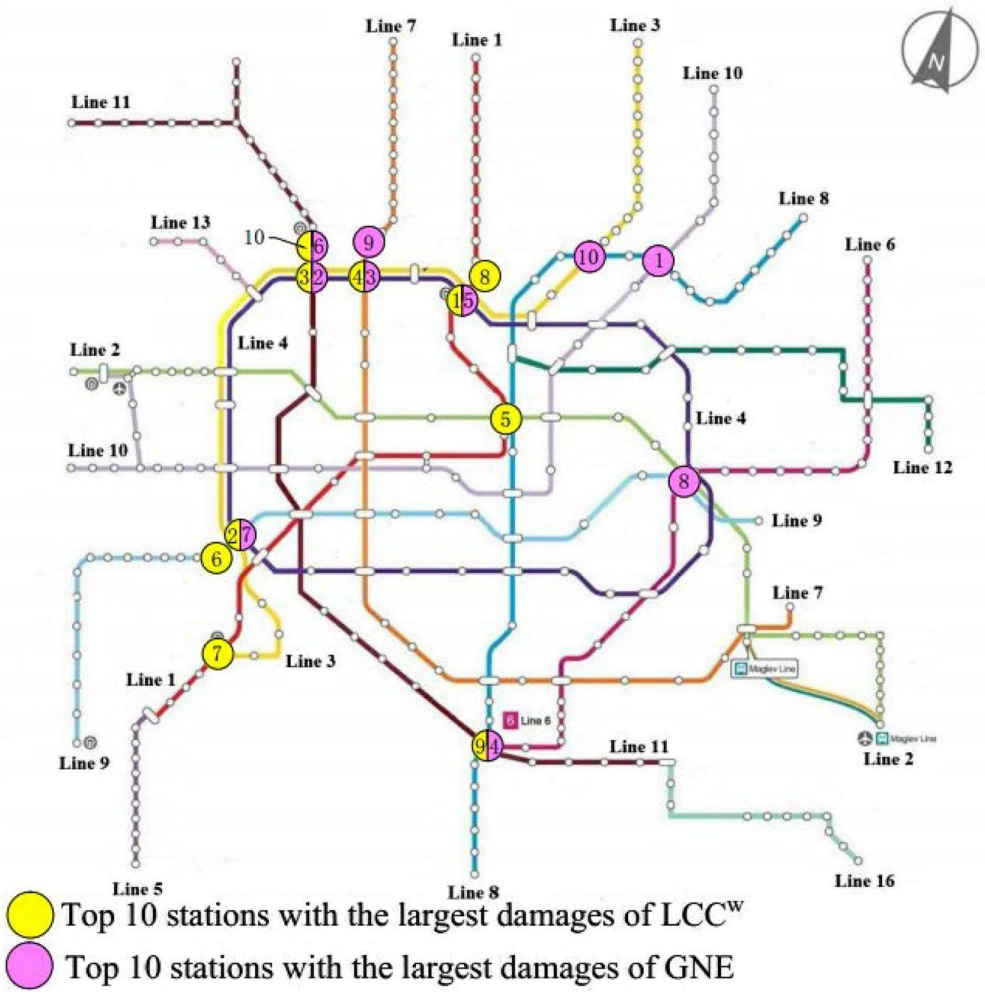

图 4 上海地铁影响最严重的车站位置

4.2 多站点故障的脆弱性

事故通常会影响多个站点。首先，一个站点的故障可能会影响它所连接的区间，并同时导致多个站点故障。其次，恐怖分子经常同时攻击几个地铁站。例如，2005 年 7 月 7 日伦敦爆炸案，四名伊斯兰极端恐怖分子在伦敦地铁列车上分别引爆了三枚炸弹，随后在塔维斯托克广场的一辆双层巴士上引爆了第四枚。2010 年 3 月 29 日，两名女性在莫斯科地铁（卢比扬卡和文化公园）的早高峰期间进行了类似的自杀式爆炸。第三，自然灾害的影响也往往会蔓延到多个站点。根据城市轨道交通突发事故的特点，本节讨论了多站点故障对 SMN 性能的影响。如表 5 所示，多站点故障比单站点故障能造成更大的损害。特别是，通过最大加权介数识别的五个站点，即人民广场、徐家汇、世纪大道、上海火车站和南京东路，能够影响约 37.63%的客流，并导致近 43.13%的全局网络效率损失。其次，通过LCC^W和 GNE 损伤最大的站点识别的五个站点也对 SMN 的性能产生了巨大影响，表明这两种方法也可以帮助识别

网络中的关键节点。此外，通过最大加权介数攻击造成的影响明显大于通过最大介数攻击造成的影响，这意味着引入地理空间因素会引起介数中心性的大幅波动，使枢纽变得更为中心。如 4.1 节所讨论的，通过节点删除识别的站点在单站点受到攻击时可能对 SMN 造成最大的破坏。但是，当多个站点同时受到攻击时，最大加权介数是识别 SMN 中关键站点的最有效方法。研究结果表明，交通管理者不仅要考虑站点的本地属性（如客流、连接站点的数量），还要考虑其在地铁网络中的位置和作用，以及权重动态（客流）和空间约束（地理空间）之间的相互作用。

表 5 多个车站故障对 SMN 性能的影响

车站序列	LCC^w下降比例(%)	GNE 下降比例(%)
强度最大的五个车站	18.05	22.27
节点度最大的五个车站	22.01	27.55
加权介数最大的五个车站	37.63	43.13
介数最大的五个车站	22.96	27.80
LCC^w损失最大的五个车站	29.57	27.68
GNE 损失最大的五个车站	23.30	36.87

4.3 上海地铁网络对不同攻击的脆弱性

本节研究了 SMN 的脆弱性。如前一节（见 3.3 节）所讨论的，通过一些拓扑网络参数，包括加权最大连通簇和网络效率，来评估在五种不同的攻击策略下的网络的性能变化。图 5 表示了在四种蓄意攻击策略以及随机故障下加权最大连通簇的变化，加权最大连通簇是使用公式（5）计算的。如预期的那样，所有蓄意攻击策略都会导致 SMN 迅速崩溃，而随机故障在五种不同的攻击策略中造成的破坏最小。除了初始阶段外，通过最大加权介数和拓扑介数攻击造成的破坏是完全相同的，表明它们的节点移除顺序相似。有趣的是，通过删除具有最

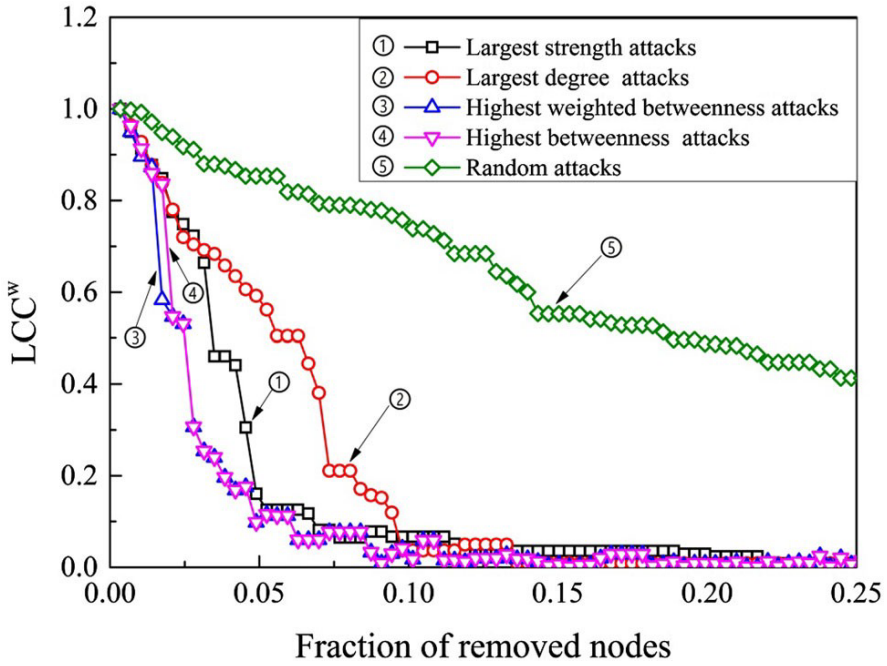

图 5 不同蓄意攻击和随机故障下LCC^w的变化

大介数的节点而不是具有最强强度度和度的节点，LCC^w的下降速度更快。这意味着通过删除被识别为全局（即介数）属性中心的节点而不是局部属性（即度、强度）的节点，能够更有效地破坏 SMN。因此，为了保持网络的结构完整性，不仅需要保护枢纽节点，还需要保护结构要点，如桥梁和瓶颈结构节点。图 4 还表明，SMN 在面对蓄意攻击时非常脆弱，而对随机故障则具有鲁棒性。网络效率是衡量网络全局连通性的更好指标。

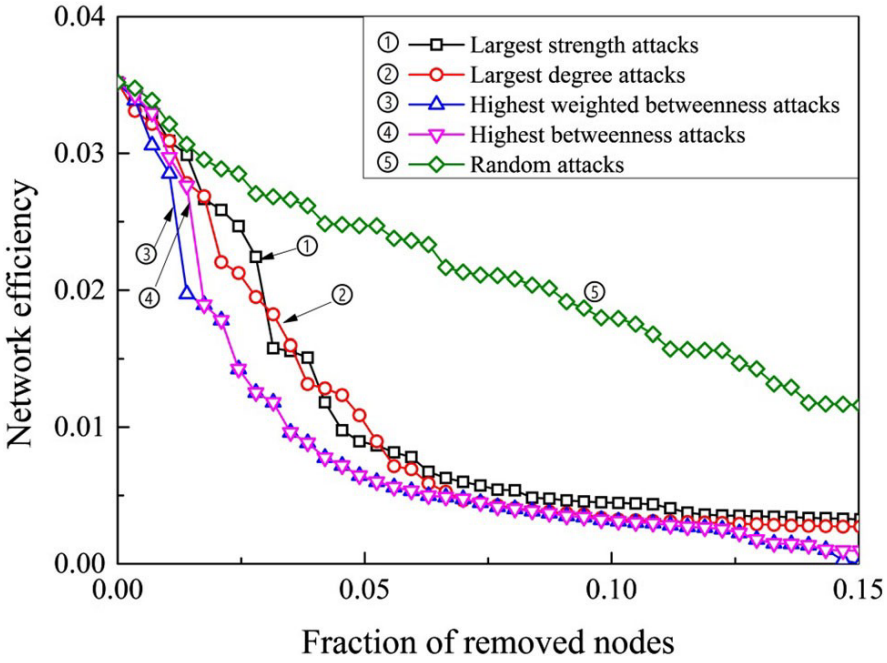

图 6 不同蓄意攻击和随机故障下网络效率的变化

图 6 显示了地铁网络在四种蓄意攻击策略以及随机故障下网络效率的变化。随着被移除节点比例的增加，网络效率在不同攻击规则下都会下降。最大介数攻击对网络造成的破坏最大，最大加权介数和拓扑介数攻击对网络造成的性能下降相同，除了初始状态外，这可能意味着站点间距对网络的影响小于由客流引起的影响。此外，通过最大强度和最大度攻击造成的破坏略小于由最高介数攻击造成的破坏。网络效率在随机故障下能够保持稳定。因此，可以知道，具有大介数和强度的节点比具有小介数和强度的节点对网络的连通性更为重要。图 5 还表明，最大介数攻击将产生比其他三种蓄意攻击策略更多的孤立节点。因此，根据图 5 和图 6，我们可以说明最大介数攻击策略是破坏 SMN 最有效的模式，因此必须给予高介数的节点更多的保护。这个结果与以前的研究（Dall’Asta 等 2006；Zhang 等 2011）一致。当然，强度大的节点对网络也非常重要，因为由最大强度攻击造成的破坏仅仅略低于由最大介数攻击造成的破坏。

4.4 加权网络和拓扑网络脆弱性的比较

目前，此领域的大多数相关研究都是从拓扑的角度进行的，这意味着它们将每个车站视为图论中的一个简单节点。在以往的文献中，很少考虑车站的客流量和出行时间成本。因此，量化加权网络和拓扑网络脆弱性之间的差异是有研究价值的。由于不同网络的全局网络效率存在，因此采用最大连通子图的相对大小来评估加权网络和拓扑网络的脆弱性。图 7 显示了所有攻击策略下的LCC^w和 LCC 的变化。在这个图中，WS 代表加权网络上的最大节点强度

攻击，WD 代表加权网络上的最大节点度度攻击，WB 表示加权网络上的最大介数（加权）攻击，WR 表示加权网络上的随机故障。同样，TS、TD、TB 和 TR 分别代表拓扑网络上的最大节点强度攻击、拓扑网络上的最大节点度攻击、拓扑网络上的最大介数（加权）攻击和拓扑网络上的随机故障。

从图 7 中可以观察到，与仅考虑拓扑属性相比，蓄意攻击策略引起的加权网络功能下降速度更快、更明显。这表明，仅考虑最大连通子图的相对大小的纯拓扑度量并不能传达现实世界网络的所有信息。换句话说，即使网络的物理结构仍然保持全局良好连接，地铁网络的功能也可能因客流而暂时受到影响。这意味着在遭受蓄意破坏时，加权网络比拓扑网络更脆弱。所有蓄意攻击策略都能够非常有效地破坏网络，移除非常少的节点就能够对网络完全破坏。如图 6 所示，无论是对于拓扑网络还是加权网络，最大介数攻击都实现了最大破坏，这导致了最大连通子图的大小快速下降。然而，不幸的是，使用基于更容易获得和计算的局部量（即节点度、强度）的攻击策略，网络也会遭到较大破坏。图 5 还表明，随机故障对加权网络造成的破坏略大于对拓扑网络的破坏。这可能是因为一些枢纽车站在拓扑和交通中占据主导地位，如人民广场和徐家汇。所有发生故障的节点可能具有较小的节点度和强度（像大多数节点一样），这些故障是可以承受的，它们对加权网络的结构完整性和功能的影响较小。另一方面，加权网络容易受到针对枢纽车站的蓄意攻击。尽管存在一些高度连接的节点（枢纽），使网络容易受到攻击，但分散的网络结构和负载高冗余，以及枢纽车站在网络中均匀分布，可以提高网络对突发事件的鲁棒性。这个结论可以通过我们对加权网络和拓扑网络的对比分析来说明。

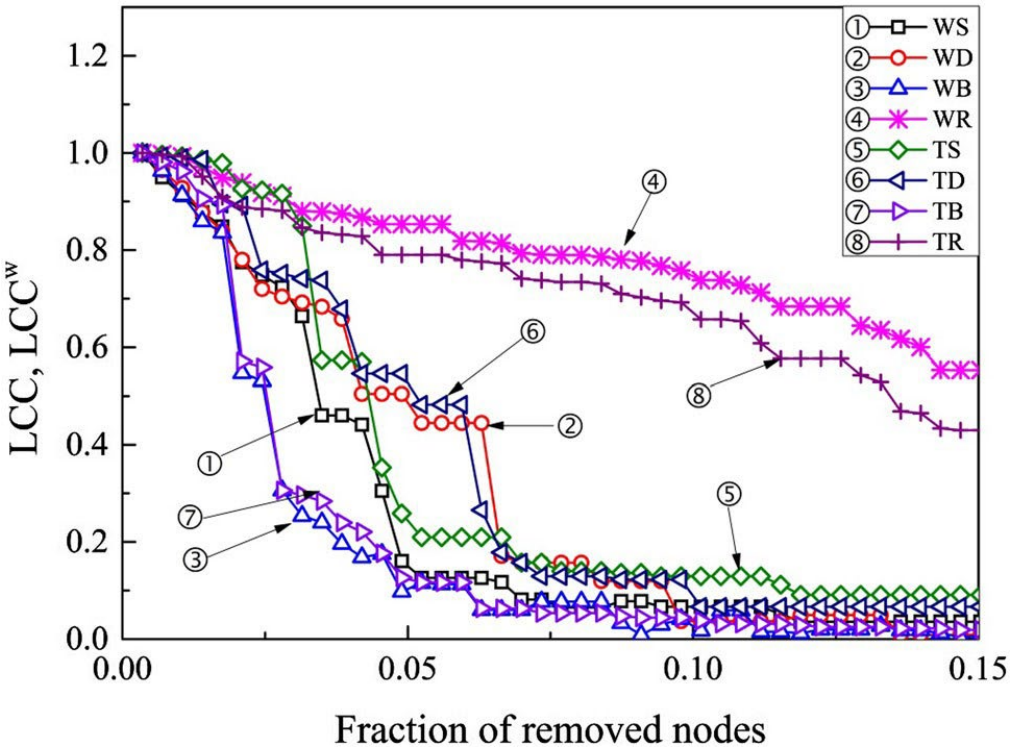

图 7 不同蓄意攻击和随机故障对加权网络和拓扑网络的影响

5 讨论

5.1 提高地铁网络抗故障的鲁棒性

众所周知，在现代社会，交通网络对城市有着重要的意义，因此我们应该更加关注地铁网络的鲁棒性。换句话说，地铁系统的拓扑结构规划对于其运营具有重要的战略意义（Yang 等 2015）。本研究调查了 SMN 的拓扑特征和对随机故障和蓄意攻击的敏感性。通过相对大小的最大连通子图和全局网络性能来衡量随机故障和蓄意攻击下的网络脆弱性。第 4.1 节的定量结果表明，SMN 对随机故障具有鲁棒性，但对蓄意攻击则表现为脆弱性。此外，最大介数攻击策略是破坏 SMN 最有效的策略。自然，如何提高地铁网络的鲁棒性成了重要的问题。一般的解决方案似乎是保护地铁系统中的关键站点并建设更多的换乘站点。然而，换乘站点的位置和数量值得进一步讨论。上海地铁系统的骨干网络已经建设得很好，进入了网络运营的新时代。其网络结构不会发生重大变化，这些地铁网络的鲁棒性只能通过增加新链接和优化网络结构来提高。

根据 Motter 和 Lai（2003）的研究，发现网络的异质性使网络特别容易受到攻击影响，因为通过攻击单个关键节点就可能会引起大规模的级联失效。相反，如果网络中的枢纽节点和负载分布非常均匀，则对攻击具有高鲁棒性。这一发现可以通过我们对加权和拓扑网络的对比分析来说明。有趣的是，我们观察到所有蓄意攻击策略都能非常有效地破坏网络（无论是加权还是拓扑），并且 SMN 的加权网络比其拓扑网络更脆弱。这意味着当前 SMN 的拓扑网络是异质的，而客流等权重的引入加剧了网络的异质性。因此，传统的交通规划者不仅应考虑人口统计、地理、需求、成本等因素，还应考虑网络的布局和结构。东京地铁的布局为上海地铁提供了良好的经验。它有 13 条线路（所有类型），215 个站点；其中 58 个站点是换乘站，换乘站的比例为 26.98%，显著高于平均水平。所有线路在多个点相交，从而使得换乘站在整个系统中均匀分布，每条线路上的负载大致相等。这些均匀分布的换乘站和线路确保了地铁网络能够在受到攻击时为乘客提供足够多的替代路线。此外，均匀分布的换乘站和线路确保了局部中断不会严重破坏地铁系统的全局结构。因此，如果地铁网络结构和客流分布均匀，可以提高网络对故障的鲁棒性。

从对网络的破坏程度数据排名可以识别出关键的车站。如图 6 所示，前 10 名中有一半以上的站点位于或紧邻环形线（4 号线），表明环形线在 SMN 中起着重要作用。它作为市中心和郊区的联系纽带，提供了多条替代路线。环形线在上海地铁网络中起着关键作用，因为它能够很快捷有效地与其他线路建立新的换乘站，而这可以进一步增加网络的连通性和鲁棒性。在这方面，交通规划者和管理者可以考虑建设另一个环形线或（半）环形线，连接周边地区，减轻 4 号线上关键站点的负载压力。

本文的研究结果对地铁运营和管理也具有很高的参考价值。对于单个车站而言，地铁网络的性能损失是识别关键车站最有效和最直接的方法。当多个车站同时遭受攻击时，最大加权介数攻击对 SMN 造成的破坏最大。因此，在预算有限的情况下，决策者应参考不同情况下关键车站的排名，这能够帮助他们决定分配财务和其他有限资源的优先级。例如，地铁运营公司和相关政府机构可以会根据可用资源的数量，优先保护最脆弱的前五个车站。

根据我们的研究结果和前人的研究（张等人，2011 年），最大介数攻击策略是破坏整个 SMN 最有效的策略。这一结果对大规模复杂地铁网络的保护有双重意义。一方面，高效的蓄意攻击策略只需要收集地铁网络初始状态的信息，因此很容易可以对地铁网络进行蓄意攻击。另一方面，识别需要保护的关键节点同时也是相对容易的，但在某种程度上这与攻击序列无关。因此，具有高介数的车站节点必须得到更多的保护。

5.2 概述和未来展望

地铁网络对各种蓄意攻击策略和随机故障的脆弱性是一个极其复杂的问题，需要通过结合相关科学理论进行全面研究。本文旨在通过引入复杂网络理论来研究 SMN 结构与其脆弱性之间的关系。本文研究了几种交通因素，如客流、站点间距，考虑了加权网络对不同蓄意攻击策略的脆弱性，并通过与拓扑网络的比较分析说明加权复杂网络比预期更脆弱。虽然本文只以 SMN 为例，但这项调查和实践可以应用于其他大型地铁系统的网络设计和安全管理。值得注意的是，用于节点移除场景分析的不同指标产生的网络中最重要的节点排名顺序，很难说哪个更重要。因此，在应用过程中应根据实际情况选取不同的指标。目前的研究结果可以为未来的研究提供一个系统和详细的案例，可以将地铁网络纳入更复杂的网络，如公交运输网络。此外，站点的容量和故障、攻击后的动态客流重新分配应考虑并进一步研究，从而更准确地评估地铁网络的脆弱性。

6 结论

总结来说，本文通过使用复杂网络理论，研究了具有交通和地理空间的加权地铁网络的脆弱性，旨在找到合理措施来提高地铁系统的鲁棒性。以地铁网络研究的经典网络上海地铁网络为案例，研究了地铁系统在面对四种蓄意攻击策略以及随机故障下的反应机理，以及交通和空间约束如何影响系统的鲁棒性。

1. 本文对加权网络对各种蓄意攻击策略和随机故障的脆弱性研究表明，SMN 对随机故障具有鲁棒性，但对蓄意攻击则表现为脆弱性，最大介数攻击策略在四种攻击策略中对 SMN 造成的破坏最大。此外，当考虑交通因素时，与拓扑地铁网络相比，加权地铁网络变得更加脆弱，加权地铁网络的结构完整性也更容易被破坏。
2. 本文提出了一种新的节点重要性评估指标，可以应用于识别地铁网络中的枢纽节点和关节点。
3. 对于单个站点，地铁网络的性能下降程度是识别关键站点最有效和直接的方法。当多个站点同时受到攻击时，最大加权介数攻击对 SMN 造成的破坏最大。因此，在预算有限的情况下，地铁管理者应参考不同指标下关键站点的排名，便于决定财务和其他有限资源分配的优先级。
4. 环形线在地铁网络中起着关键作用，因为基于环行线能够快速高效与其他线路建立换乘站，而这能够进一步增强网络的连通性和鲁棒性。在这方面，交通规划者和管理者可以考虑建设另一个环形线或（半）环形线来连接当前线路，提高网络效率。

虽然本文可以为评估地铁系统的脆弱性提供参考，但由于客流量的限制，地铁网络脆弱

性的分析仅基于 SMN 进行分析，同时暴露出一些。在进一步研究中，我们将把当前工作与地铁系统的动态脆弱性分析、相应的客流量、突发事件发生的频率和网络中断机制的研究相结合，从而提出改进风险评估模型和地铁系统安全管理策略。

参考文献

Albert R, Baraba´si A-L (2002) Statistical mechanics of complex networks. Rev Mod Phys 74:47–97

Angeloudis P, Fisk D (2006) Large subway systems as complex networks. Physica A 367:553–558

Berche B, von Ferber C, Holovatch T, Holovatch Y (2009) Resilience of public transport networks against attacks. Eur Phys J B Condens Matter Complex Syst 71(1):125–137

Berche B, von Ferber C, Holovatch T, Holovatch Y (2010) Public transport networks under random failure and directed attack. Dyn Socio-Econ Syst 2(2):42–54

Berdica K (2002) An introduction to road vulnerability: what has been done, is done and should be done.Transp Policy 9:117–127

Berdica K, Mattsson LG (2007) Vulnerability: A Model-Based Case Study of the Road Network in Stockholm. In: Murray AT, Grubesic TH (eds) Critical Infrastructure. Advances in Spatial Science. Springer, Berlin, Heidelberg, pp 81–106

Boccaletti S, Latora V, Moreno Y, Chavez M, Hwang DU (2006) Complex networks: structure and dynamics. Phys Rep 424(4–5):175–308

Bruyelle JL, O'Neill C, El-Koursi EM, Hamelin F, Sartori N, Khoudour L (2014) Improving the resilience of metro vehicle and passengers for an effective emergency response to terrorist attacks. Saf Sci 62:37–45

Cats O, Jenelius E (2012) Vulnerability analysis of public transport networks: a dynamic approach and case study for Stockholm. In: The international symposium on transportation network reliability

Cats O, Yap M, Oort NV (2015) Exposing the role of exposure: identifying and evaluating critical links in public transport networks. In: The international symposium on transportation network reliability

Chopra SS, Dillon T, Bilec MM, Khanna V (2016) A network-based framework for assessing infrastructure resilience: a case study of the London metro system. J R Soc Interface 13(118):20160113

Crucitti P, Latora V, Marchiori M, Rapisarda A (2003) Efficiency of scale-free networks: error and attack tolerance. Physica A 320:622–642

Dall'Asta L, Barrat A, Vespignani L (2006) Vulnerability of weighted networks. J Stat Mech: Theory Exp 25(04):04006

De-Los-Santos A, Laporte G, Mesa JA, Perea F (2012) Evaluating passenger robustness in a rail transit network. Transport Res Part C Emerg Technol 20(1):34–46

Derrible S, Kennedy C (2010) The complexity and robustness of metro networks. Physica A

389(17):3678–3691

Ghedini CG, Ribeiro CH (2011) Rethinking failure and attack tolerance assessment in complex networks.Physica A 390:4684–4691

Guimera´ R, Amaral LAN (2004) Modeling the world-wide airport network. Eur Phys J B Condens Matter Complex Syst 38(2):381–385

Han Y, Cheng H, Zhao X, Xue X (2012) Theoretic structure of urban mass transit operation safety based on vulnerability. Urban Mass Transit 15:15–19

Kyriakidis M, Hirsch R, Majumdar A (2012) Metro railway safety: an analysis of accident precursors. Saf Sci 50:1535–1548

Kyriakidis M, Hirsch R, Majumdar A (2014) A global safety analysis and best practice for metro railways. Soc Sci Electron Publ 166(6):362–374

Laporte G, Mesa JA, Perea F (2010) A game theoretic framework for the robust railway transit network design problem. Transport Res Part B Methodol 44(4):447–459

Luathep P, Sumalee A, Ho HW, Kurauchi F (2011) Large-scale road network vulnerability analysis: a sensitivity analysis based approach. Transportation 38(5):799–817

Mattsson LG, Jenelius E (2015) Vulnerability and resilience of transport systems—a discussion of recent research. Transport Res Part A Policy Pract 81:16–34

Motter AE, Lai Y-C (2003) Cascade-based attacks on complex networks. Phys Rev E: Stat Nonlinear Soft Matter Phys 66(6):114–129

Nawrath C (2006) Unraveling the complex network of cuticular structure and function. Curr Opin Plant Biol 9(3):281–287

Newman ME, Strogatz SH, Watts DJ (2001) Random graphs with arbitrary degree distributions and their applications. Phys Rev E 64:026118

Ouyang M, Zhao L, Hong L, Pan Z (2014) Comparisons of complex network based models and real train flow model to analyze Chinese railway vulnerability. Reliab Eng Syst Saf 123(3):38–46

Perea F, Puerto J (2013) Revisiting a game theoretic framework for the robust railway network design against intentional attacks. Eur J Oper Res 226(2):286–292

Petter H, Beom Jun K, No YC, Seung Kee H (2002) Attack vulnerability of complex networks. Phys Rev E 65(5):056109

Riedel HU (2014) Chinese metro boom shows no sign of abating. Int Railw J 54(11):46–48

Rodríguez-Núñez E, García-Palomares JC (2014) Measuring the vulnerability of public transport networks. J Transp Geogr 35:50–63

Sienkiewicz J, Hołyst JA (2005) Statistical analysis of 22 public transport networks in Poland. Phys Rev E Stat Nonlin Soft Matter Phys 72(4 Pt 2):046127

Taylor MAP, D'Este GM (2007) Transport network vulnerability: a method for diagnosis of critical locations in transport infrastructure systems. Critical infrastructure. Springer, Berlin, pp 9–30

von Ferber C, Holovatch T, Holovatch Y, Palchykov V (2007) Network harness: metropolis public transport. Physica A 380(7):585–591

Wang J (2013) Robustness of complex networks with the local protection strategy against cascading failures. Saf Sci 53:219–225

Wang J, Fang W (2014) A structured method for the traffic dispatcher error behavior analysis in metro accident investigation. Saf Sci 70:339–347

Wang J, Mo H, Wang F, Jin F (2011) Exploring the network structure and nodal centrality of China's air transport network: a complex network approach. J Transp Geogr 19(4):712–721

Wang H, Huang J, Xu X, Xiao Y (2014) Damage attack on complex networks. Physica A 408:134–148 Xu Z, Sui DZ (2007) Small-world characteristics on transportation networks: a perspective from network autocorrelation. J Geogr Syst 9(2):189–205

Xu X, Hu J, Liu F (2007a) Scaling and correlations in three bus-transport networks of China. Physica A 374(1):441–448

Xu X, Hu J, Liu F (2007b) Empirical analysis of the ship-transport network of China. Chaos 17(2):471–516

Yang Y, Liu Y, Zhou M, Li F, Sun C (2015) Robustness assessment of urban rail transit based on complex network theory: a case study of the Beijing subway. Saf Sci 79:149–162

Yuan J, Li Q, Jia R, Wang Z (2012) Analysis of operation vulnerabilities of urban metro network system.China Saf Sci J 22:92–98

Zhang J, Xu X, Hong L, Wang S, Fei Q (2011) Networked analysis of the Shanghai subway network, in China. Physica A 390(23):4562–4570

Zhang J, Xu X, Hong L, Wang S, Fei Q (2012) Attack vulnerability of self-organizing networks. Saf Sci 50:443–447

Zhou Z, Irizarry J, Li Q (2014) Using network theory to explore the complexity of subway construction accident network (SCAN) for promoting safety management. Saf Sci 64:127–136

Public Transp (2017) 9:501–525
DOI 10.1007/s12469-017-0170-2

CASE STUDY AND APPLICATION

Vulnerability analysis of urban rail transit based on complex network theory: a case study of Shanghai Metro

Yingying Xing[1] · Jian Lu[2] · Shengdi Chen[3] · Sunanda Dissanayake[4]

Accepted: 12 August 2017 / Published online: 11 September 2017

Abstract With increasing passenger flows and construction scale, metro systems in metropolises have entered a new era of networking operation and become the most effective way to alleviate and decrease traffic congestion. However, frequent occurrence of random failures and malicious attacks pose a serious threat to metro security and reliability. Thus, it is necessary to quantitatively evaluate the vulnerability of the metro network to different failures or attacks from a networking perspective. Based on the complex network theory, this study took the Shanghai Metro Network (SMN) as an example to investigate vulnerability of a weighted metro network in responding to random failures as well as malicious attacks. In particular, compared to topological networks, the vulnerability of weighted networks was analyzed to investigate how traffic and spatial constraints influence the transport system's vulnerability, since topological features of complex networks are

✉ Jian Lu
jianjohnlu@tongji.edu.cn

Yingying Xing
yingying199004@163.com

Shengdi Chen
sdchen@shmtu.edu.cn

Sunanda Dissanayake
sunanda@ksu.edu

[1] School of Naval Architecture, Ocean and Civil Engineering, Shanghai Jiao Tong University, 800 Dongchuan Road, Shanghai, People's Republic of China

[2] College of Transportation Engineering, Tongji University, 4800 Cao'an Road, Shanghai, People's Republic of China

[3] College of Transport and Communication, Shanghai Maritime University, 1550 Haigang Ave, Shanghai, People's Republic of China

[4] Department of Civil Engineering, Kansas State University, 2118 Fiedler Hall, Manhattan, Kansas 66506, USA

often associated with the weights of the edges and spatial constraints. Simulation results show that the SMN is robust against random failures but fragile for malicious attacks. The vulnerability analysis of weighted properties shows that all targeted attacks are capable to shatter the network's communication or transport properties at a very low level of removed nodes and the highest betweenness attack strategy is the most effective mode to cause destructive effects on SMN among five attack or failure strategies. The inclusion of passenger flows provides evidence for the view that topological networks cannot convey all the information of a real-world network and traffic flow in the network should be considered as one of the key features in the finding and development of defensive strategies. Our results provide a richer view on complex weighted networks in real-world and possibilities of risk analysis and policy decisions for the metro operation department.

Keywords Metro safety · Vulnerability analysis · Complex network · Passenger flow · Robustness

1 Introduction

Due to the increasing traffic volume and growing demands for land because of urban construction and development, many metropolises have continually increased investments in construction of metro lines to relieve serious traffic congestion. With more and more new lines being added into service, many metro systems such as New York City Subway, Shanghai Metro, and Tokyo Metro have transformed into complex metro networks that possess high station densities and intricate inter-station coupling relationships leading to a new era of networking operations (Angeloudis and Fisk 2006; Xu and Sui 2007; Yang et al. 2015). However, recent history has shown that metro systems entail dangerous environments in case of emergencies due to the comparatively enclosed structure and large passenger flows in metro systems. Malicious attacks such as targeted destructions and retaliatory disruptions to the metro system have occurred frequently in recent years; such incidents could result in the functionality loss of the entire system and cause considerable casualties and socio-economic loss. For example, the terrorist attacks that happened in the Lubyanka metro station and Park Kultury metro station of Russia in 2010 killed at least 40 people. In addition, the frequent occurrence of random failures shows that unreasonable planning as well as inadequate safety precautions would impair the overall reliability of a metro system (Albert and Barabási 2002; Newman et al. 2001; Wang 2013; Zhou et al. 2014). It is apparent that increasing size and complexities are making metro systems more dependent on systematic vulnerability analysis and formulation of corresponding coping strategies to increase the robustness of metro networks. However, transit planners pay more attention on traditional characteristics, such as geography, demand, cost and others; none seems to address the network design in a direct way, which becomes increasingly important as transit systems grow. Similarly, transit policymakers and operators considered more about station local properties (such as passenger flows,

the number of connected stations) rather than its position and role in the whole metro network. Therefore, it is necessary to conduct a comprehensive analysis of the vulnerability of metro networks from a holistic perspective.

During the past few years, graph and complex network theories have been used to study large-scale transportation infrastructures (railways, highways and airlines) and have become a powerful tool to identify the vulnerable (weak) components (e.g., links or nodes) in a transport network from a systematic view (Ouyang et al. 2014; Taylor et al. 2007; Berdica and Mattsson 2007; Guimerá and Amaral 2004; Wang et al. 2011). By examining public transportation networks of fourteen major cities in the world, Berche et al. (2009) identified public transport network structures which are especially vulnerable and others, which are particularly resilient against attacks. Derrible and Kennedy (2010) analyzed the complexity and robustness of 33 metro systems and provided insights/recommendations for increasing the robustness of metro networks. Laporte et al. (2010) presented an integer linear programming model to design public transit networks in the presence of a link failure and a competing mode. Zhang et al. (2011) investigated the connectivity, robustness and reliability of the subway network by graph theory and complex network theory. According to the analysis and discussion, the study found that the subway network is robust against random attacks but fragile for malicious attacks. Han et al. (2012) analyzed urban mass transit accidents from three aspects, including interference, exposure and vulnerability. They regarded vulnerability as inherent defects of the system and established a theoretical safety insurance mechanism. Yuan et al. (2012) reviewed the statistics of metro accidents and proposed the concepts of physical, structural and social vulnerabilities of metro network systems. Nevertheless, these studies simplified the metro networks with graph theory and considered only the network topology. Thus, they were lacking consideration on dynamic properties of metro systems.

Other approaches to vulnerability analysis of metro networks were also employed. Cats and Jenelius (2012) proposed a dynamic and stochastic notion of public transport network vulnerability and developed a more refined model to assess public transport network vulnerability by considering supply and demand interactions. De-Los-Santos et al. (2012) provided rail transit network robustness measures from the user's point of view. Based on the work of predecessors, Perea and Puerto (2013) discussed and extended a game-theoretic framework for the robust railway network design against intentional attacks. Rodríguez-Núñez and García-Palomares (2014) presented a methodology for analyzing the criticality and vulnerability of a public transport network. Based on the experience of the 7/7 London bombings and other subway incidents, Bruyelle et al. (2014) identified critical systems of metro coach and proposed enhancements to the robustness of subway systems. Taking the Beijing Subway system as an example, Yang et al. (2015) assessed the robustness of a subway network in face of random failures as well as malicious attacks. The research results revealed that the Beijing Subway system exhibits typical characteristics of a scale-free network, with relatively high survivability and robustness when faced with random failures, whereas error tolerance is relatively low when the hubs undergo malicious attacks. Cats et al. (2015) presented and applied a method to explicitly account for exposure in identifying and evaluating

link criticality in public transport networks. Chopra et al. (2016) presented a comprehensive, multi-pronged framework that analyzed information on network topology, spatial organization and passenger flow to understand the resilience of the London metro system. Although these studies provide useful insights on network properties that effect reliability and vulnerability of metro systems, an incorporation of passenger flow and geographical space would further enhance network models and provide a richer view on vulnerability analysis of urban rail transit networks. Simulating different station failure situations (single node-multiple nodes-network) under different attack strategies could help to identify critical nodes in the network, which was particularly useful for the rail transit planners and managers.

Therefore, this paper conducts a systematic vulnerability analysis of urban rail transit to provide theoretical support to the planning and operation of urban rail transit networks. The paper focuses on a weighted metro network with traffic and geographical space to explore how traffic and spatial constraints influence the transport system's vulnerability. Different attack strategies including malicious attacks and random failures are discussed to identify the most effective mode to destroy the whole metro network. In particular, the topological, dynamic and damage-depending measures that can be used to identify the most crucial nodes in a weighted network are discussed and compared. The functionality of the whole network depends on the protection of these crucial nodes. Moreover, the vulnerability of weighted networks was analyzed compared to topological networks. According to the findings in this study, several measures are proposed to strengthen the structural robustness of a metro network, which may help in the development of adaptive reactions aimed at dealing with targeted attacks.

2 Background

2.1 Shanghai Metro System

Shanghai is one of the largest cities in China, with more than 20 million people. With a rapidly increasing population, urban traffic congestion in Shanghai becomes even worse which needs to be solved immediately. In order to enhance capacity and accessibility of public transportation, a massive network by a considerable amount over 500 km is constructed and the traffic congestion of ground transportation has been reduced. Until December, 2014, the Shanghai Metro Network (SMN) was the world's largest rapid transit system by route length (Riedel 2014), with 14 lines, 286 stations, 39 transfer stations and a mileage totaling more than 540 km (Fig. 1). It also ranks second in the world by annual ridership after Beijing, with 2.8 billion rides delivered in 2014. The newest daily ridership record was set at 10.286 million on December 31, 2014, while over 8 million people use the system on an average weekday.

The SMN consists of 286 nodes denoting stations and 317 edges accounting for a link connecting two stations which are adjacent to each other. As already observed in previous literatures (Zhang et al. 2011), the topology of the network exhibits both scale-free and small-world properties. Datasets that are provided by the Shanghai

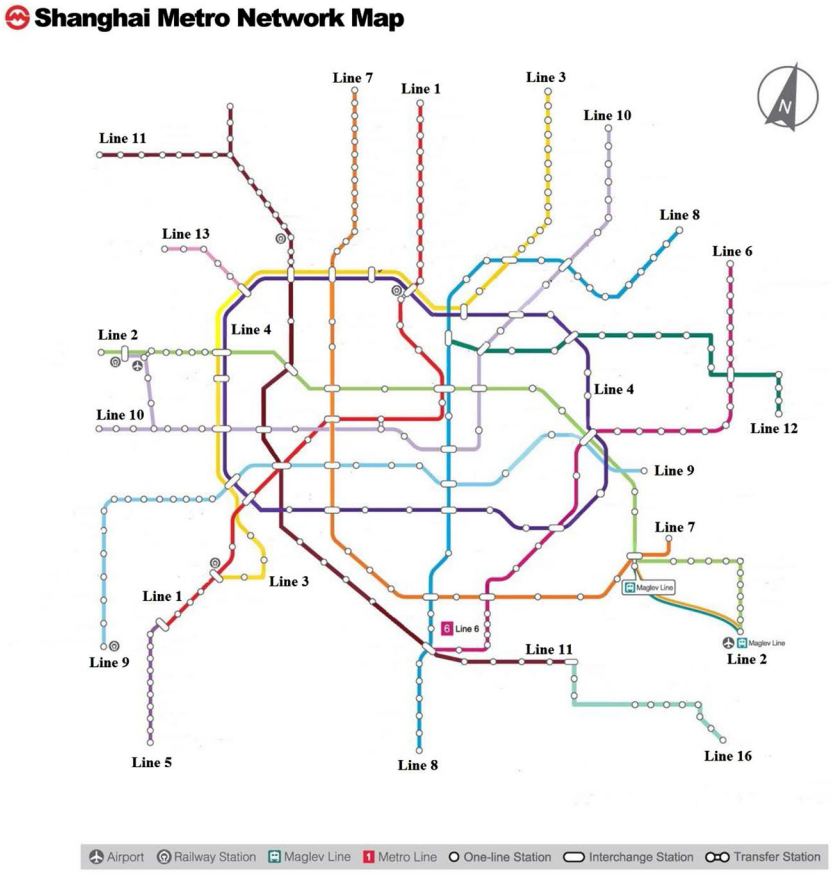

Fig. 1 Schematic map of Shanghai Metro Network (Source: The website of Shanghai Shentong Metro Company)

Shentong Metro Company, list the hourly in and out passenger flows for each station and passenger flows between adjacent stations. In this study, passenger flows during morning peak hours from 7:00 to 9:00 in a typical weekday are analyzed, during which time the highest volume on a weekday could be observed.

2.2 Fundamental concepts of network vulnerability

There is no commonly accepted definition of transport system vulnerability (Mattsson and Jenelius 2015). The definition suggested by Berdica (2002) is often cited by other literatures: "vulnerability in the road transportation system is a susceptibility to incidents that can result in considerable reductions in road network serviceability." This definition can also apply to other modes of transport. Luathep et al. (2011) deem that vulnerability analysis principally focuses on identifying the critical components of the network that result in the most adverse effect on network

performance when they are subjected to random failures or malicious attacks. Berdica and Mattsson (2007) propose that vulnerability in transport networks can be seen as overall framework through which different transport studies could be conducted to determine how well a transport system would perform when exposed to different kinds and intensities of disturbances. Berche et al. (2009) note that vulnerability is essential to assess the fault tolerance of a local station as well as a global network. The notion of attack vulnerability is defined as the survivability of a metro network under intentional attacks by Yang et al. (2015). In this study, the concept of network vulnerability is used to describe a lack of serviceability of a metro network when subjected to various threats and hazards. Threats and hazards are the sources of potential damage for a metro network. Hazards refer to accidental events (such as natural disasters and system failures), while threats are related to intentional events (for example, terrorist attacks).

2.3 The definition of various failures

A metro network system generally encounters various emergencies and complex external environments, such as natural disasters, system failures and terrorist attacks, and can be categorized into two types of incidents, i.e., random failures and intentional attacks (Kyriakidis et al. 2012; Wang et al. 2014; Wang 2013). A metro accident is most often due to several different precursors, varying from a natural error to a malicious attack (Kyriakidis et al. 2014; Wang and Fang 2014). Due to the uncertainties of these precursors, it is extremely difficult to quantitatively specify the corresponding destructive power for each failure or attack. As a consequence, an intentional attack in this paper is defined as a malicious or targeted destruction manipulated by artificial forces, while a random failure is specified as the disfunction of a network caused by failure on one or several nodes with a random probability (Ghedini and Ribeiro 2011; Zhang et al. 2012). According to the definition, the main difference between these two incidents is that the probability of a random failure is equal among all stations while an intentional attack generally happens to hub stations with high degree or betweenness centrality. Different precursors of these two incidents are summarized in Table 1.

3 Methodology

3.1 Construction of the weighted SMN model

To analyze various properties of urban rail transit systems one should define a proper network topology to describe the structure of the SMN network. Metro systems have been simplified as graphs by using various network representations in previous literature, such as space L, space P, space B, and space C network topologies (Sienkiewicz and Hołyst 2005; von Ferber et al. 2007; Xu et al. 2007a, b; Berche et al. 2010). Each network topology supplies its unique topological insights with respect to metro systems. For instance, space L is mainly applied to investigate topological properties and vulnerabilities of metro systems while space P is widely

Table 1 Summary of common behaviors of failures and attacks for a metro system

Network failure	Precursors categories	Examples
Random failure	Technical failures	Cracked rail/other serious rail defect, broken wheels, loss of brake function, Signal failures, power failure, train doors failure
	Human performance—passenger and metro workers	Congestion, suicide, fall onto track, falls on escalators, fall on stairs, people hit by train, unconscious destruction due to drunkenness, smoke in station/train, passenger carrying dangerous or flammable goods, caught in train doors, wrong operation by driver, exceeding speed limits, signals passed at danger (SPADs)
	Management actions	Station totally closed, Station access closed, Temporary line maintenance
	External environment	Severe weathers, object on track, object exceeding clearance limit
Intentional attack	Malicious or targeted destruction	Terrorism, act of vandalism, passenger carrying dangerous or flammable goods, trespass, set fires, gun shooting, group fighting

used to explore transfer properties like the role of the metro line on transfer times (von Ferber et al. 2007).

As shown in Fig. 2, space L network topology consists of nodes representing stations and edges connecting physically adjacent stations, in other words, an edge between two nodes exists if there is at least one line that provides service to two consecutive stations. No multiple links are allowed (Berche et al. 2009). The node degree k in this topology is just the number of edges that a node shares with others while the distance l is the minimum number of links traversed from one node to another. Space L topology is an intuitive geographical representation of the metro system, and allows us to simulate link failures and analyze their consequences in the

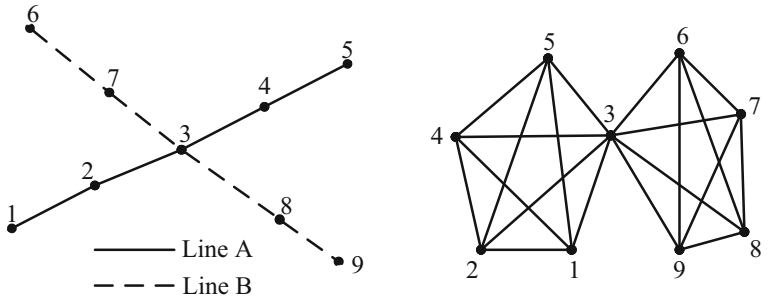

Fig. 2 Explanation of the space L (**a**) and the space P (**b**)

most simplistic manner (Chopra et al. 2016). In the space P, although nodes are the same as in the space L, here an edge between two nodes means that there is at least a direct metro line connecting them. Consequently, the node degree k in this topology is the total number of nodes reachable using a single line and the distance can be interpreted as "the minimum number of line changes +1" to be made by a trip maker in order to successfully get from one station to another. This main characteristic allows us to specifically discuss transfer properties of the metro network. Consequently, the Space L representation of the SMN was chosen for our analysis.

Up to now, most studies have focused on unweighted networks, i.e. networks that have a binary nature, where the edges between nodes are either present or not. Nevertheless, along with a complex topological structure, many real networks display a large heterogeneity in the capacity and the intensity of the connections. Therefore, the weighted network was introduced to describe the characteristics and properties of real networks. A weighted graph $G^w = (V, E, W)$, where each edge carries a numerical value measuring the strength of the connection, consists of a set $V = \{v_i | i = 1, 2, \ldots, N\}$ of nodes, a set $E = \{e_{ij} = (v_i, v_j) | i, j = 1, 2, \ldots, N, i \neq j\}$ of edges and a set of weights $W = \{w_{ij} | i, j = 1, 2, \ldots, N, i \neq j\}$ that are real numbers attached to the edges. In matricial representation, G^w could usually be represented by the so-called adjacency weights matrix A^w with adjacency element a_{ij} being defined as

$$a_{ij} = \begin{cases} w_{ij}, & (v_i, v_j) \in E \\ 0 \ or \ \infty, & (v_i, v_j) \notin E \end{cases}, \tag{1}$$

where w_{ij} is the weight of the edge connecting node v_i to node v_j, and $a_{ij} = 0$ or ∞ depends on whether the weight of the edge is dissimilar or similar. The dissimilar weight means that the higher the weight is, the larger the path length and the more aloof the connection between two nodes, for example, the distance in a postman problem. Conversely, the higher the weight is, the smaller the path length and the more intimate the connection between two nodes, the more similar the weight of, for instance, cooperation frequencies in scientific collaboration networks. Therefore, for similar weights, if nodes i and j are connected by node k, the distance $d_{ij} = w_{ik} + \mathrm{w_{kj}}$. For dissimilar weights, the distance is inversely proportional to the edge weight, thus $d^s_{ik} = \frac{1}{w_{ik}}$ and the distance between nodes i and j could be calculated by the equation $d^s_{ij} = \frac{w_{ik} \times w_{kj}}{w_{ik} + w_{kj}}$. Subsequently, based on complex network theory, the stations of the SMN can be represented by the nodes of the network and the lines directly connecting two stations can be virtualized into the edges of the network. Many different quantities of the SMN could be considered as weight of the network, including passenger flow, station spacing, travel time and so on. Moreover, it is assumed that typical travel is bi-directional, and hence the weight w_{ij} of one edge between a pair of nodes (stations) i and j is defined to be the sum of passenger flows in both directions and $w_{ij} = w_{ji}$.

3.1.1 Node degree and strength

The most prominent feature of weighted complex networks is heterogeneity of weights w_{ij} between pairs of nodes, which depicts the interactions between the components in the system. For a given node i in an unweighted network, its degree, $k_i = \sum_j^N a_{ij}$, is the number of nodes it is linked to. Subsequently, in a weighted network, a more meaningful measure of the network properties in terms of the actual weights is obtained by introducing strength s_i, defined as

$$s_i = \sum\nolimits_{j=1}^{N} a_{ij} w_{ij}. \tag{2}$$

From Eq. 2, the quantity s_i combines node degree k_i with edge weight w_{ij}, and is a natural measure of the centrality or connectivity of a node i in the weighted network. For the SMN, the node strength simply accounts for the total passenger flows handled by each station.

3.1.2 Weighted shortest paths

Shortest paths play an important role in the transport and communication within a network. All the shortest path lengths of a graph G can be expressed as a matrix D in which the element l_{ij} is defined as the minimum number of links traversed to get from node v_i to node v_j. Characteristic path length, also known as average path length, is defined as the average number of steps along the shortest paths for all possible pairs of network nodes (Nawrath 2006) and can be expressed by

$$\mathrm{L} = \frac{1}{N(N-1)} \sum\nolimits_{i,j \in V(i \neq j)} l_{ij}. \tag{3}$$

In a generic weighted network, the path length between two nodes v_i and v_j can be introduced as the function of weight w_{ij}, depending on whether the weight of the edge be dissimilar or similar. In this study, the shortest path with the minimum number of edges is not an optimal one. It then defines the weighted shortest path length d_{ij} as the minimum value of the sum of edge lengths throughout all the possible paths from node v_i to node v_j, where the edge length refers to station spacing. It is obvious that the station spacing is a dissimilar weight. Subsequently, the average shortest path length can be defined as

$$\mathrm{L} = \frac{1}{N(N-1)} \sum\nolimits_{i,j \in V(i \neq j)} d_{ij}. \tag{4}$$

3.1.3 Node betweenness

The communication of two non-adjacent nodes depends on the paths connecting them. Consequently, a measure to investigate relevance of a given node can be obtained by counting the fraction of shortest paths between pairs of nodes passing

through it, and defining the so-called node betweenness. Together with the degree, the betweenness is one of the standard measures of node centrality and quantifies the influence and importance of a node in the network. More precisely, the betweenness b_i of a node i is defined as (Boccaletti et al. 2006):

$$b_i = \sum\nolimits_{j.k \in V, j \neq k} \frac{n_{jk}(i)}{n_{jk}}, \tag{5}$$

where n_{jk} is the total number of shortest paths from j to k, and $n_{jk}(i)$ is the number of these shortest paths that pass through the node i.

In weighted networks, unequal link capacities make some specific paths more favorable than others in connecting two nodes of the network (Dall'Asta et al. 2006). Thus, it seems natural to generalize the notion of betweenness centrality through replacing shortest paths between pairs of nodes with their weighted versions. Similar to Eq. (5), the weighted betweenness b_i of a node i can be defined as:

$$b_i^w = \sum\nolimits_{j.k \in V, j \neq k} \frac{n_{jk}^w(i)}{n_{jk}^w}, \tag{6}$$

where n_{jk}^w is the total number of weighted shortest paths from j to k, and $n_{jk}^w(i)$ is the number of them that pass through the node i. In the particular case of $w_{ij} = 1$ for all edges, the weighted shortest path length d_{ij} reduces to the minimum number of edges necessary to go from node v_i to node v_j. For metro systems, node betweenness represents status and influence of a station within the network, and central stations are part of more shortest paths than peripheral stations.

3.2 Attack strategies and random failure

An attacking strategy describes the way that an adversary attacks a network, while a random failure is specified as the disfunction of a network caused by accidental incidents. In case of a random failure each node or edge fails with an equal probability. On the contrary, in a malicious attack, an adversary preferentially attacks the target that he believes will maximize the destructive effect on network integrity and functionality. A complex network generally encounters two types of incidents, node attack and edge attack. Considering characteristics of metro systems, a node attack strategy is adopted, that is, attacking a network by removing a node as well as its incident edges from the network. For metro systems, a node removal means that the station is broken down completely and cannot restore function in the short term. Therefore, passengers in the station and travelling on its incident edges cannot reach their destination. Moreover, it is assumed that the purpose of adversaries is to maximize the destructive effect and destroy the network as soon as possible. For this purpose, adversaries first need to evaluate the importance of a node for identifying the most important nodes in the metro network. As a consequence, the ranking mechanism of node importance is crucial for generating an attacking strategy. In general, different adversaries sort the node importance from different aspects, and resulting in different destructive effects.

Based on the different definitions for the centrality ranking of the most important nodes, five different deletion strategies are introduced to investigate the vulnerability of the metro network when subjected to malicious attacks or random failures. Moreover, node centrality measures will be recalculated after each attack. This has been shown to be the most effective strategy (Petter et al. 2002; Dall'Asta et al. 2006), as each node deletion will give rise to a change in the centrality properties of the other nodes. More precisely, the malicious attack strategies and random failures are designed as follows. (1) The malicious attacks according to nodes rank in terms of degree, strength, topological betweenness, and weighted betweenness. That is, from the initial state, the most important node and its incident edges will be deleted and all the properties of weighted networks can be recalculated after a deletion, and the attacks continue. (2) Random failures. The nodes are deleted randomly and the properties of weighted networks can be recalculated after each attack. The nodes will be removed from the network one by one, subjected to these five different attack or failure strategies.

3.3 Assessment model for overall performance of a network

When investigating the assessment model, another key issue to consider is how the global performance of a network under various attacks is measured. Network vulnerability can be characterized in many ways, such as by observing the change of relative size of maximal connected subgraph while nodes are continuously attacked one by one (Crucitti et al. 2003; Berche et al. 2009; Ghedini and Ribeiro 2011). A fast decrease of the largest component size indicates that a network is highly vulnerable. The network performance can also be evaluated by the network efficiency, which is performed by computing possible shortest distance between any two nodes and represents the communication functionality of the network (Zhang et al. 2011; Yang et al. 2015). Therefore, these two indexes were combined to explore how the performance of the SMN responded to different accidents.

3.3.1 Relative size of the largest connected sub-graph

If any two nodes in a graph are connected, the graph G is called a connected graph. When nodes are under attack and deleted from the network, the entire connected graph will disintegrate into multiple subgraphs and disconnected parts (Fig. 3). The largest connected subgraph is the one that has most connected nodes. In the unweighted networks, the largest connected cluster LCC is defined by the relative size of the maximal connected subgraph and can be described as follows

$$LCC = N/N_0, \tag{7}$$

where N is the number of nodes on the largest connected subgraph after attacks, and N_0 is the number of nodes on the largest connected graph of the initial network. In order to assess the reliability and robustness of the weighted networks, the strength s is integrated with the largest connected cluster for the weighted case and LCC^w is defined by the equation

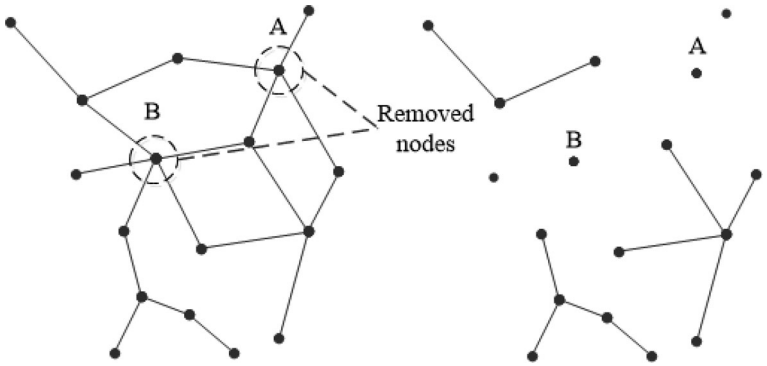

Fig. 3 Structures of the connected graph before and after node removal

$$LCC^{w} = S/S_0, \tag{8}$$

where S is the sum of the strength of nodes on the largest connected subgraph after attacks, and S_0 is the sum of the strength of nodes on the largest connected graph of the initial network. This quantity measures the structural integrity of the network in reference to strength in local scope, as it refers to the relative traffic or passenger flow that is still handled in the maximal connected component of the network.

3.3.2 Network efficiency

The characteristic path length is a natural measure of the efficiency of a network, and has large implications for the transport and communication in a network. However, when a network is attacked and nodes become disconnected, the shortest path length will be infinite for two unconnected nodes stored in an adjacent matrix and cannot be computed. To overcome this problem, an alternative approach, the so-called "network efficiency" that is useful in many cases is defined as follows:

$$E = \frac{1}{N(N-1)} \sum \frac{1}{d_{ij}}. \tag{9}$$

This quantity E is an indicator of the traffic capacity of a metro network, and avoids the divergence of the characteristic path length. It helps to explore how the topological properties of the SMN responded to different accidents in global scope. Metro systems with high network efficiency mean that travel should be fast and convenient under normal operating conditions. In weighted networks, it seems natural to generalize the notion of network efficiency through replacing the shortest paths with their weighted versions. The spatial attributes of the SMN are embodied in the physical spatial distance, measured in kilometers, characterizing each connection.

4 Results

4.1 Station vulnerability

In a complex transportation system, not all stations are equivalent. Conventional researchers usually regarded the degree centrality of a node as the only measurement for evaluating the significance of the node. In addition, betweenness is also an effective measurement of the global function of a node and has been used as a global geometric factor for node importance evaluation. However, there are few studies on node importance that is measured by damage rather than degree or betweenness.

Tables 2 and 3 show the percentage of functionality loss of the entire network when a station is removed from the network. As shown in Tables 2 and 3, the station with the largest strength and betweenness in the SMN is People's Square, which has six edges connecting to other stations and undertakes nearly 0.7 million passengers on morning rush hours. However, its damage value of the largest connected cluster (LCC^w) and global network efficiency (GNE) is 5.00 and 3.71%, which are both lower than Shanghai Railway Station, Caoyang Road and Zhenping Road. The station resulting in the largest damage of LCC^w in the SMN is Shanghai Railway Station, whose damage is 6.58%, implying that 6.58 percent of passenger flows rely on Shanghai Railway Station, which is their unique choice to connect to other stations.

The top ten stations with the largest damage of LCC^w and network efficiency are shown in Table 4. The damage of LCC^w depicts the level that the network is divided. Generally speaking, the removal of one node will not have a great influence on the integrity of the network. But, it can be seen from Table 4 that the network disintegrates into smaller sub-networks, disconnected parts because of the closure of station, which would have a major effect on regular operations of SMN. Of these, the most serious one is Shanghai Railway Station, which would affect about 6.58%

Table 2 Top 10 stations with the largest strength

Rank	Node name	Damage of LCC^w (%)	Damage of GNE (%)	Degree
1	People's Square	5.00	3.71	6
2	Xujiahui	3.67	2.71	6
3	Century Avenue	3.75	6.90	8
4	East Nanjing Road	2.96	2.22	4
5	Jing'an Temple	2.90	2.18	4
6	Shanghai Railway Station	6.58	7.60	4
7	Changshu Road	2.82	1.76	4
8	Zhongshan Park	2.68	2.61	4
9	Jiangsu Road	2.55	1.60	4
10	South Shaanxi Road	2.52	1.56	4

Table 3 Top 10 stations with the largest betweenness (weighted)

Rank	Node name	Damage of LCC^w (%)	Damage of GNE (%)	Degree
1	People's Square	5.00	3.71	6
2	Xujiahui	3.67	2.71	6
3	Century Avenue	3.75	6.90	8
4	Shanghai Railway Station	6.58	7.60	4
5	East Nanjing Road	2.96	2.22	4
6	Caoyang Road	6.05	8.56	4
7	Zhenping Road	5.38	8.29	4
8	Hailun Road	1.39	3.03	4
9	Oriental Sports Center	4.25	7.81	5
10	Changshu Road	2.82	1.76	4

of passenger flows. Meanwhile, it was found that stations connected radial metro lines and core areas usually result in serious damage of subgraph, such as Shanghai Railway Station, Yishan Road and Caoyang Road, as shown in Fig. 4. If such sorts of stations are temporarily off-line due to malicious attacks, the stations of radial lines away from central areas would lose contact with other stations in the network. Whereas for stations in the core areas, even the deletion of hub stations may not

Table 4 Top 10 stations with the largest damages

Rank	Node name	Damage of LCC^w (%)	Degree	Node name	Damage of GNE (%)	Degree
1	Shanghai Railway Station	6.58	4	Siping Road	9.64	4
2	Yishan Road	6.50	5	Caoyang Road	8.56	4
3	Caoyang Road	6.05	4	Zhenping Road	8.29	4
4	Zhenping Road	5.38	4	Oriental Sports Center	7.81	5
5	People's Square	5.00	6	Shanghai Railway Station	7.60	4
6	Guilin Road	4.74	2	Fengqiao Road	7.29	2
7	Shanghai South Railway Station	4.50	3	Yishan Road	7.07	5
8	North Zhongshan Road	4.42	2	Century Avenue	6.90	8
9	Oriental Sports Center	4.25	5	Langao Road	6.88	2
10	Fengqiao Road	4.20	2	Hongkou Football Stadium	6.76	4

cause disconnection and division of network and have a relatively small impact on the integrity of the network, such as Xujiahui. This phenomenon can also be explained by the metro network route. Taking Caoyang Road as an example, it serves as a link connecting Line 11 and downtown. If Caoyang Road was attacked, the stations located north of Caoyang Road had no other route to enter the inner city, which would lead to traffic congestion in Caoyang Road. Similarly, if Xujiahui was attacked, although many passengers would be affected, the remaining network could supply enough alternative route choices for passengers, so a large amount of passengers can still arrive at their destinations through other alternative routes.

Similar patterns were also observed in network efficiency and secondly, it is interesting to find that some stations that are highly connected, such as Century Avenue, Xujiahui, have relatively small damage values. In contrast, some stations with large damages, such as Guilin Road and North Zhongshan Road, have quite small degrees. These results reveal that transfer sites may not have much more influence than regular stations. It is different from conventional views that value transfer sites and undervalue regular stations. After a comprehensive investigation,

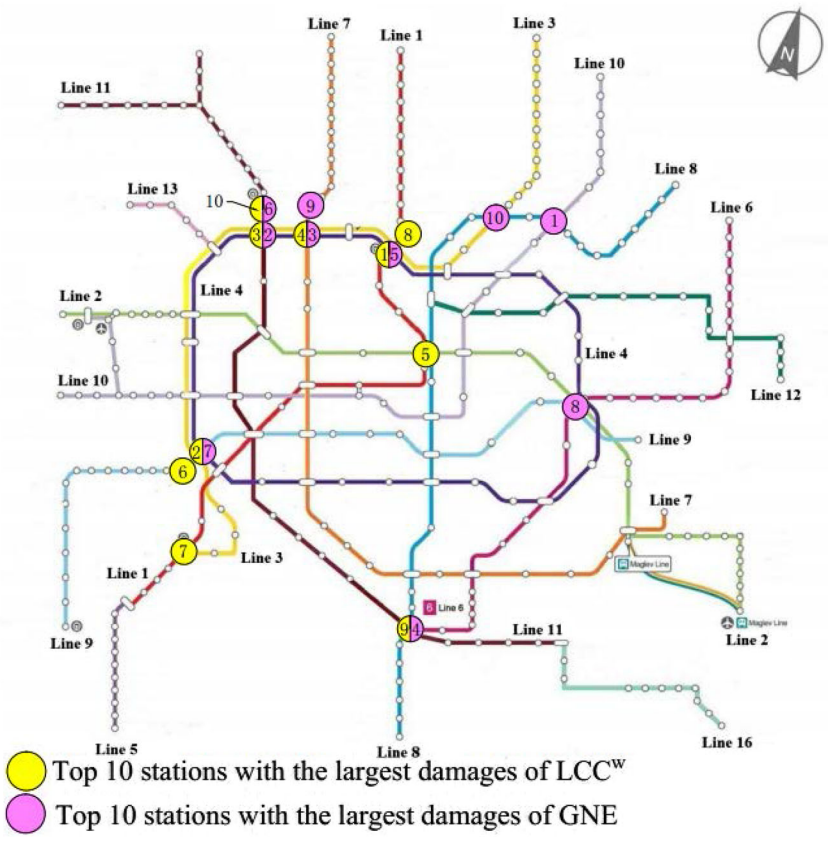

Fig. 4 Locations of stations with the largest damages of Shanghai metro

it was found that these kinds of regular stations can result in division of networks and deserve more attention. The above analysis provides a new perspective to examine the essentiality of a station and clearly shows that the essentiality of a station can be characterized by its damage, not just degree centrality or betweenness centrality.

4.2 Vulnerability of multiple stations failure

Accidents often affect more than one station. Firstly, the failure of a station may affect a continuous section and cause multiple stations failure at the same time. Secondly, terrorists often attack several metro stations simultaneously. For example, the July 7, 2005 London bombings, four Islamist extremists separately detonated three bombs in quick succession aboard London Underground trains across the city, and later, a fourth on a double-decker bus in Tavistock Square. On March 29, 2010, similar suicide bombings were carried out by two women during the morning rush hour, at two stations of the Moscow Metro (Lubyanka and Park Kultury). Thirdly, the impact of natural disasters also tends to spread to multiple stations. According to the characteristics of urban rail transit operation accidents, this section discusses the impact of multiple stations failure on the performance of SMN.

As seen in Table 5, multiple stations failure causes much more damage than a single station failure. In particular, the failure of five stations identified by the highest weighted betweenness i.e., People's Square, Xujiahui, Century Avenue, Shanghai Railway Station and East Nanjing Road, has affected about 37.63% of passenger flows and caused nearly 43.13% loss of global network efficiency. Secondly, multiple stations identified by the largest damages of LCC^w and GNE also have a great influence on the performance of SMN, indicating that these two approaches can also help identify the key node in the network. Besides, the damage caused by the highest weighted betweenness attack was significantly larger than that caused by the highest betweenness attack, which implies that the introduction of geographical space induces large betweenness centrality fluctuations and makes the hubs become more central.

As discussed in Sect. 4.1, stations identified by the functional loss could cause the largest damage on the SMN when a single station is attacked. But when multiple

Table 5 The influence of multiple stations failure on SMN performance

Index stations	Damage of LCC^w (%)	Damage of GNE (%)
Top 5 stations with the largest strength	18.05	22.27
Top 5 stations with the largest degree	22.01	27.55
Top 5 stations with the highest weighted betweenness	37.63	43.13
Top 5 stations with the highest betweenness	22.96	27.80
Top 5 stations with the largest damages of LCC^w	29.57	27.68
Top 5 stations with the largest damages of GNE	23.30	36.87

stations are under attack at the same time, the highest weighted betweenness is the most effective way to identify the crucial stations in the SMN. The presented results suggest that the transit managers cannot only think about the station local properties (such as passenger flows, the number of connected stations), but also its position and role in the metro network and the interplay between weight dynamics (passenger flow) and spatial constraints (geographical space).

4.3 Vulnerability of Shanghai Metro Network to different attacks

The vulnerability of the SMN is investigated in this section. As discussed in the previous section (see Sect. 3.3), several topological parameters including the weighted largest connected cluster, and network efficiency were applied to assess the changes of the characteristics for subjection to five different deletion strategies. Figure 5 portrays the changes in the weighted largest connected cluster subjected to four malicious attack strategies as well as random failures and the weighted largest connected cluster is calculated by using formula (5). As expected, all intentional attack strategies result in a rapid breakdown of the SMN with a very small threshold value of the fraction of removed stations, while the random failures result in the minimum damage among five different station failure modes. In addition to the initial phase, the damage caused by the highest weighted betweenness and topological betweenness attack is precisely the same, showing that they share the similar order of node removal. It is interesting to find that the LCC^w decreases faster upon removal of nodes with the highest betweenness instead of nodes with the largest strength and degree. This implies that it is more effective to destroy the SMN by deleting nodes which are identified as central according to global (i.e. betweenness) properties rather than local properties (i.e. degree, strength). Therefore, it is necessary to protect not only the hubs but also strategic points such as bridges and bottleneck structures in order to maintain the structural integrity

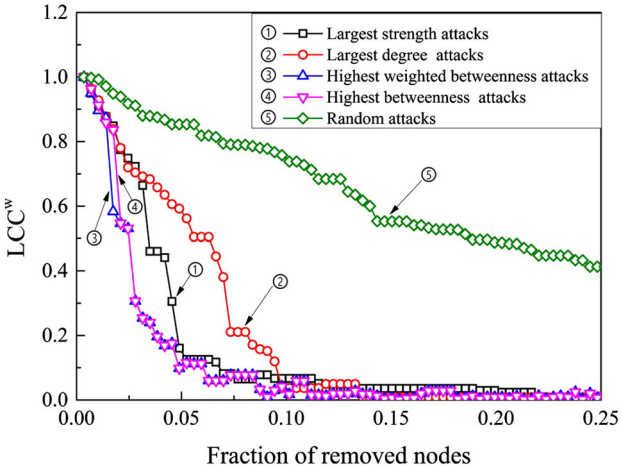

Fig. 5 The changes of LCC^w with different malicious attack strategies and random failures

of a network. Figure 4 also shows that the SMN is very fragile when subjected to malicious attacks, and it is robust against random failures.

The network efficiency is a better metric to measure the global connectivity of the network. Figure 6 shows the changes of the network efficiency for a metro network subject to four malicious attack strategies as well as random failures. With the increase of the fraction of the removed nodes, the network efficiency decreases when subjected to different attack rules. The highest betweenness attacks cause the maximum damage to the network and the highest weighted betweenness and topological betweenness attack also cause the same functionality loss to the network except the initial state, which probably implies that station spacing has less effect on the network than the one caused by passenger flows. Furthermore, the damage caused by the largest strength and largest degree attacks are slightly smaller than that caused by the highest betweenness attacks. The network efficiency can be preserved by random failures. So it can be known that the nodes with large betweenness and strength are more important than the nodes with small betweenness and strength to the connectivity of the network. Figure 5 also shows that the highest betweenness attacks will generate more isolated nodes than the other three malicious attack strategies. Therefore, according to Figs. 5 and 6, we can declare that the highest betweenness attack strategy is the most effective mode to destroy the SMN, so the nodes with high betweenness must be given more protection. This result is consistent with previous studies (Dall'Asta et al. 2006; Zhang et al. 2011). Certainly, the nodes with large strength are very important to the network, as the damage caused by the largest strength attacks is slightly lower than the damage caused by the highest betweenness attack.

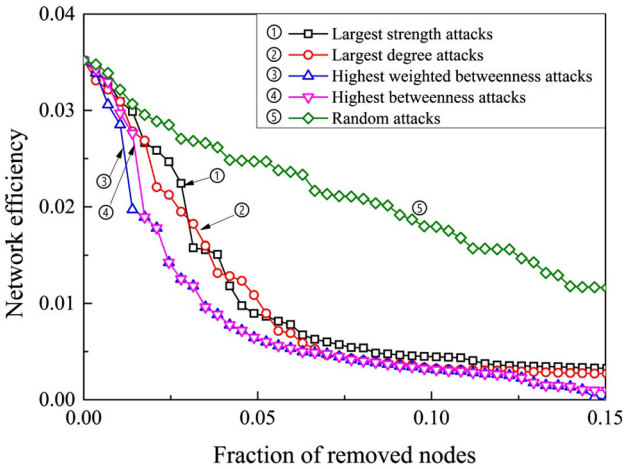

Fig. 6 The changes of the network efficiencies under malicious attacks and random failures

4.4 Comparison of weighted and topological networks vulnerability

Currently, most relevant studies in this field were conducted in the view of topology, which meant they considered each station as a simple node in graph theory. The traffic of a station and cost of travel time were rarely considered in previous literatures. It is therefore interesting to quantify the difference between weighted and topological networks vulnerability. As the global network efficiency varies with different networks, the relative size of the largest connected component is adopted to evaluate the vulnerability of weighted and topological networks. Figure 7 shows the behavior of LCC^w and LCC of all cases. Within this figure, WS represents the largest strength attack on the weighted network, WD the largest degree attack on the weighted network, WB denotes the highest betweenness (weighted) attack on the weighted network and WR denotes random failure on the weighted network. Similarly, TS, TD, TB and TR represent the largest strength attack on the topological network, the largest degree attack on the topological network, the highest betweenness (weighted) attack on the topological network and random failure on the topological network, respectively.

From Fig. 7, it is interesting to observe that the functionality decrease of weighted networks caused by intentional attack strategies is even faster and more pronounced than thought by considering only topological properties. This indicates that the purely topological measure of the relative size of the largest connected subgraph does not convey all the information of a real-world network. In other words, the functionality of a metro network could be temporarily endangered in terms of passenger flows even though the physical structure of the network is still globally well-connected. This implies that weighted networks are more fragile than topological networks when subject to malicious destructions. All intentional attack strategies are very effective in damaging the network, reaching the complete destruction at a very low level of removed nodes. As seen in Fig. 6, the maximum

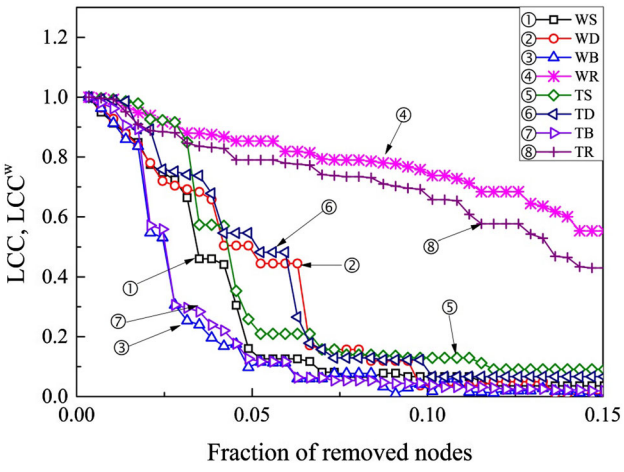

Fig. 7 Effect of malicious attacks and random failures on weighted and topological network

damage is still achieved by the highest betweenness attack which leads to a very fast decrease of the giant component size both for topological and weighted networks. Whereas, the network may unfortunately be damaged by using attack strategies based on local quantities (i.e. degree, strength) which are more easily obtained and calculated. Figure 5 also shows that the random failure causes slightly more damage to the weighted network than the topological network. This is probably due to a few hub stations dominating their topology and traffic, such as People's Square and Xujiahui. Any node that fails probably has small degree and strength (like most nodes), which is expendable and has less effect on the structural integrity and functionality of a weighted network. The flip side is that the weighted networks are vulnerable to intentional attacks on the hub station. Despite the existence of a few highly connected nodes (hubs) which leave the network vulnerable to attacks, a decentralized network structure and high redundancy may help to improve robustness and network efficiency under normal circumstances or in the case of failures.

5 Discussion

5.1 Improving robustness of a metro network against failures

In the modern society, it is known that transit networks have a significant impact on the city, so more attention should be paid on the robustness of a metro network. In other words, the planning of the topological structure is a critical issue of great operational significance for a subway system (Yang et al. 2015). In this study, the topological features and sensitivity of the SMN to random failures and malicious attacks were investigated. The failure tolerance and attack vulnerability were measured by the relative size of a large component and global network performance. Quantitative results in Sect. 4.1 show that the SMN is robust against random failures but fragile for malicious attacks. In addition, the highest betweenness attack protocol is the most effective mode to destroy the SMN. Then, it is natural to ask how to improve the robustness of a metro network. General solutions seem to protect the crucial stations in metro systems and build more interchange stations. However, the positions and the number of interchange stations deserve to be further discussed. The backbone network of the Shanghai Metro System had been well constructed and entered a new era of networking operation. Its network structure will not change significantly and the robustness of these metro networks can be only improved by adding new links and optimizing the network structure.

According to research by Motter and Lai (2003), it is found that the heterogeneity of the networks makes them particularly vulnerable to attacks in that a largescale cascade may be triggered by disabling a single key node. In turn, the hub nodes and load are distributed very evenly in the network, resulting in the high robustness against failures. This finding could be illustrated by our contrastive analysis of weighted and topological network. It is interesting to observe that all intentional attack strategies are very effective in damaging the network (both weighted and topological) and the weighted version of SMN is more vulnerable than its

topological network when subjected to intentional attacks. This implies that the current topological network of SMN is heterogeneous and the introduction of passenger flow exacerbates the heterogeneity of the networks. Thus, traditional transit planners should not only consider such characteristics as demography, geography, demand, cost and others, but also the layout and structure of a network. The layout of Tokyo Metro provides good experience for Shanghai Metro. It has 13 lines (of all types), with 215 stations; 58 of these stations are transfers, hence a ratio of 26.98%, which is significantly high. All lines intersect at multiple points, resulting in that interchange stations distribute evenly throughout the whole system and load on each line is approximately equal. These span-uniform interchange stations enable the metro to offer sufficient alternative routes for passengers when subject to attacks. Furthermore, the well-distributed transfer stations and lines ensure that a local disruption cannot impair the global structure of a metro system severely. Thus, it can improve the network robustness against failures by making the network structure and passenger flow more homogeneous.

The exposure of the stations has been obtained from data on criticality. As seen in Fig. 6, over half of the top 10 stations locate on or next to the circular line (line 4), indicating that the circular line plays an important role in the SMN. It serves as the link between urban and rural areas and provides multiple alternative routes. Circular lines play a key role in the metro network because it is the most effective way to create new transfer stations that will further increase the connectivity and robustness of a network. In this regard, transit planners and managers can consider to build another circle line or (semi)-circle line to connect peripheral regions and relieve heavy stress of crucial stations on line 4.

The results obtained are also of high interest in metro operation and management. For a single station, the functional loss of the metro network is the most effective and direct method to identify crucial stations. While multiple stations are attacked simultaneously, the highest weighted betweenness attack causes the largest damage to the SMN. Therefore, under a constrained budget, the policymakers should consult the ranking of crucial stations in different situations, which will allow them to prioritize the allocation of financial and other constrained resources. For example, metro operators and relevant government agencies may decide to protect the top one to five vulnerable stations, depending on the amount of available resources.

According to our results and previous research (Zhang et al. 2011), the highest betweenness attack protocol is the most effective mode to destroy the whole SMN. This evidence brings both good and bad news concerning the protection of large-scale metro systems. On one hand, the planning of an effective targeted attack only needs to gather information on the initial state of the network. On the other hand, the identification of crucial nodes to protect is an easier task that somehow is weakly dependent on the attack sequence. As a consequence, the stations with high betweenness must be given more protection.

5.2 Generality and future work

The vulnerability of a metro network against various malicious attack strategies and random failures is an extremely complicated issue, and comprehensive studies are

required to be carried out by combining relevant scientific theory. This paper aims to investigate the underlying relationship between the structure of the SMN and its vulnerability by introducing complex network theory. Several traffic characteristics such as passenger flows, station spacing are considered in the study of the vulnerability of weighted networks to different malicious attack strategies, and simulation results show that weighted complex networks are more fragile than expected through comparative analysis with topological networks. Although only taking the SMN as an example, this investigation and the practice are possible to be applied to the network design and safety management of other large-scale metro systems. Note that different metrics used for node removal scenario analysis will have different rank order for the most important nodes in the network, so it is difficult to say which is more crucial. So it should use these different metrics case by case. The current results could supply a systematic and detailed case for future research, which can be incorporated into more complex networks such as bus transport. Besides, the capacity of station and dynamic traffic redistribution after failures and attacks should be considered and further studied in order to assess the vulnerability of a metro network more accurately.

6 Conclusion

To summarize, this paper investigates the vulnerability of a weighted metro network with traffic and geographical space by using complex network theory, aiming to find reasonable measures to improve the robustness of metro systems. The Shanghai metro, a typical resource of metro network research, is taken as an example to examine how a metro system responds to four malicious attack strategies as well as random failures and how traffic and spatial constraints influence the system's robustness.

1. The study of the vulnerability of weighted networks to various malicious attack strategies and random failures shows that the SMN is robust against random failures but fragile for malicious attacks and the highest betweenness attack strategy causes the most damage to SMN among four attack modes. In addition, when the traffic characteristics are taken into account, the weighted metro network becomes more fragile than expected from the comparison with topological quantities and the structural integrity of the weighted network is vanishing before the topological network is fragmented.
2. A new indicator for node importance evaluation is proposed, which could apply to identify hubs, bridges and bottlenecks for a metro network.
3. For a single station, the functional loss of the metro network is the most effective and direct method to identify crucial stations. While multiple stations are attacked simultaneously, the highest weighted betweenness attack causes the largest damage to the SMN. Therefore, under a constrained budget, the policymakers should consult the ranking of crucial stations in different situations, which will allow them to prioritize the allocation of financial and other constrained resources.

4. Circular lines play a key role in the metro network because it is the most effective way to create new transfer stations that will further increase the connectivity and robustness of a network. In this regard, transit planners and managers can consider building another circle line or (semi)-circle line to connect the current lines and improve the network efficiency.

Although this work could make a contribution to the assessment of the vulnerability of the metro system, due to the limitation of the passenger flow, the analysis of metro network vulnerability is only based on the analysis over the SMN and exposes several insufficiencies. In our further research, the dynamic vulnerability analysis of metro systems, a corresponding study of passenger flows, the frequency of threat occurrence and the mechanism of network disruption, would integrate with the current work to provide an improved risk assessment model and safety management strategies for metro systems.

Acknowledgements The authors thank the Shanghai Shentong Metro Company, for providing valuable information about the SMN for academic and research activities. In addition, the authors acknowledge the financial support of Project 71671127 by the National Natural Science Foundation of China.

References

Albert R, Barabási A-L (2002) Statistical mechanics of complex networks. Rev Mod Phys 74:47–97
Angeloudis P, Fisk D (2006) Large subway systems as complex networks. Physica A 367:553–558
Berche B, von Ferber C, Holovatch T, Holovatch Y (2009) Resilience of public transport networks against attacks. Eur Phys J B Condens Matter Complex Syst 71(1):125–137
Berche B, von Ferber C, Holovatch T, Holovatch Y (2010) Public transport networks under random failure and directed attack. Dyn Socio-Econ Syst 2(2):42–54
Berdica K (2002) An introduction to road vulnerability: what has been done, is done and should be done. Transp Policy 9:117–127
Berdica K, Mattsson LG (2007) Vulnerability: A Model-Based Case Study of the Road Network in Stockholm. In: Murray AT, Grubesic TH (eds) Critical Infrastructure. Advances in Spatial Science. Springer, Berlin, Heidelberg, pp 81–106
Boccaletti S, Latora V, Moreno Y, Chavez M, Hwang DU (2006) Complex networks: structure and dynamics. Phys Rep 424(4–5):175–308
Bruyelle JL, O'Neill C, El-Koursi EM, Hamelin F, Sartori N, Khoudour L (2014) Improving the resilience of metro vehicle and passengers for an effective emergency response to terrorist attacks. Saf Sci 62:37–45
Cats O, Jenelius E (2012) Vulnerability analysis of public transport networks: a dynamic approach and case study for Stockholm. In: The international symposium on transportation network reliability
Cats O, Yap M, Oort NV (2015) Exposing the role of exposure: identifying and evaluating critical links in public transport networks. In: The international symposium on transportation network reliability
Chopra SS, Dillon T, Bilec MM, Khanna V (2016) A network-based framework for assessing infrastructure resilience: a case study of the London metro system. J R Soc Interface 13(118):20160113
Crucitti P, Latora V, Marchiori M, Rapisarda A (2003) Efficiency of scale-free networks: error and attack tolerance. Physica A 320:622–642
Dall'Asta L, Barrat A, Vespignani L (2006) Vulnerability of weighted networks. J Stat Mech: Theory Exp 25(04):04006
De-Los-Santos A, Laporte G, Mesa JA, Perea F (2012) Evaluating passenger robustness in a rail transit network. Transport Res Part C Emerg Technol 20(1):34–46
Derrible S, Kennedy C (2010) The complexity and robustness of metro networks. Physica A 389(17):3678–3691

Ghedini CG, Ribeiro CH (2011) Rethinking failure and attack tolerance assessment in complex networks. Physica A 390:4684–4691
Guimerá R, Amaral LAN (2004) Modeling the world-wide airport network. Eur Phys J B Condens Matter Complex Syst 38(2):381–385
Han Y, Cheng H, Zhao X, Xue X (2012) Theoretic structure of urban mass transit operation safety based on vulnerability. Urban Mass Transit 15:15–19
Kyriakidis M, Hirsch R, Majumdar A (2012) Metro railway safety: an analysis of accident precursors. Saf Sci 50:1535–1548
Kyriakidis M, Hirsch R, Majumdar A (2014) A global safety analysis and best practice for metro railways. Soc Sci Electron Publ 166(6):362–374
Laporte G, Mesa JA, Perea F (2010) A game theoretic framework for the robust railway transit network design problem. Transport Res Part B Methodol 44(4):447–459
Luathep P, Sumalee A, Ho HW, Kurauchi F (2011) Large-scale road network vulnerability analysis: a sensitivity analysis based approach. Transportation 38(5):799–817
Mattsson LG, Jenelius E (2015) Vulnerability and resilience of transport systems—a discussion of recent research. Transport Res Part A Policy Pract 81:16–34
Motter AE, Lai Y-C (2003) Cascade-based attacks on complex networks. Phys Rev E: Stat Nonlinear Soft Matter Phys 66(6):114–129
Nawrath C (2006) Unraveling the complex network of cuticular structure and function. Curr Opin Plant Biol 9(3):281–287
Newman ME, Strogatz SH, Watts DJ (2001) Random graphs with arbitrary degree distributions and their applications. Phys Rev E 64:026118
Ouyang M, Zhao L, Hong L, Pan Z (2014) Comparisons of complex network based models and real train flow model to analyze Chinese railway vulnerability. Reliab Eng Syst Saf 123(3):38–46
Perea F, Puerto J (2013) Revisiting a game theoretic framework for the robust railway network design against intentional attacks. Eur J Oper Res 226(2):286–292
Petter H, Beom Jun K, No YC, Seung Kee H (2002) Attack vulnerability of complex networks. Phys Rev E 65(5):056109
Riedel HU (2014) Chinese metro boom shows no sign of abating. Int Railw J 54(11):46–48
Rodríguez-Núñez E, García-Palomares JC (2014) Measuring the vulnerability of public transport networks. J Transp Geogr 35:50–63
Sienkiewicz J, Hołyst JA (2005) Statistical analysis of 22 public transport networks in Poland. Phys Rev E Stat Nonlin Soft Matter Phys 72(4 Pt 2):046127
Taylor MAP, D'Este GM (2007) Transport network vulnerability: a method for diagnosis of critical locations in transport infrastructure systems. Critical infrastructure. Springer, Berlin, pp 9–30
von Ferber C, Holovatch T, Holovatch Y, Palchykov V (2007) Network harness: metropolis public transport. Physica A 380(7):585–591
Wang J (2013) Robustness of complex networks with the local protection strategy against cascading failures. Saf Sci 53:219–225
Wang J, Fang W (2014) A structured method for the traffic dispatcher error behavior analysis in metro accident investigation. Saf Sci 70:339–347
Wang J, Mo H, Wang F, Jin F (2011) Exploring the network structure and nodal centrality of China's air transport network: a complex network approach. J Transp Geogr 19(4):712–721
Wang H, Huang J, Xu X, Xiao Y (2014) Damage attack on complex networks. Physica A 408:134–148
Xu Z, Sui DZ (2007) Small-world characteristics on transportation networks: a perspective from network autocorrelation. J Geogr Syst 9(2):189–205
Xu X, Hu J, Liu F (2007a) Scaling and correlations in three bus-transport networks of China. Physica A 374(1):441–448
Xu X, Hu J, Liu F (2007b) Empirical analysis of the ship-transport network of China. Chaos 17(2):471–516
Yang Y, Liu Y, Zhou M, Li F, Sun C (2015) Robustness assessment of urban rail transit based on complex network theory: a case study of the Beijing subway. Saf Sci 79:149–162
Yuan J, Li Q, Jia R, Wang Z (2012) Analysis of operation vulnerabilities of urban metro network system. China Saf Sci J 22:92–98
Zhang J, Xu X, Hong L, Wang S, Fei Q (2011) Networked analysis of the Shanghai subway network, in China. Physica A 390(23):4562–4570

Zhang J, Xu X, Hong L, Wang S, Fei Q (2012) Attack vulnerability of self-organizing networks. Saf Sci 50:443–447

Zhou Z, Irizarry J, Li Q (2014) Using network theory to explore the complexity of subway construction accident network (SCAN) for promoting safety management. Saf Sci 64:127–136