移动 Ad Hoc 社交网络中的安全连通性分析

陆佃杰^{①②}, 张桂娟^{①②}, 郑向伟^{①②}, 刘弘^{①②}, 胡斌^{①②③*}^① 山东师范大学信息科学与工程学院, 济南 250014^② 山东省分布式计算机软件新技术重点实验室, 济南 250014^③ 兰州大学信息科学与工程学院, 兰州 730000

* 通信作者. E-mail: bh@lzu.edu.cn

收稿日期: 2014-09-07; 接受日期: 2014-11-22; 网络出版日期: 2014-12-16

国家自然科学基金 (批准号: 61402270, 61373149, 61202225, 61272094)、教育部博士点基金 (批准号: 20133704120009)、山东省高等学校科技计划项目 (批准号: J13LN13) 和“泰山学者”计划资助项目

摘要 移动 Ad Hoc 社交网络 (MASNs) 的安全性是近年来的研究热点问题. 在 MASNs 中, 安全通信需要将链接建立在相互信任的基础上, 因此具有很大的挑战性. 本文主要对 MASNs 安全连通性的相关特征进行分析. 首先, 通过将节点间的信任关系的分布描述成一种更新随机过程. 在此基础上, 可以通过四个步骤构造安全图: 构造几何图、构造信任图、构造安全图、安全图的增广. 然后, 利用连续渗流理论证明了安全 MASNs 中渗流现象的存在. 最后, 分析了安全连通性中的关键密度特征这一核心问题. 通过聚类系数法获取了关键密度 λ_s^c 的更为严格的下界. 仿真结果表明, 节点密度以及信任关系都会对 MASNs 的安全连通性产生极大影响. 该结论能够为 MASNs 的安全连通性研究提供基础性的指导.

关键词 移动 Ad Hoc 社交网络 连通性 安全性 连续渗流 关键密度

1 引言

近年来, 随着移动互联网的快速发展以及移动设备的广泛使用, 移动社交网络的发展迅速. 其便携性和即时性的特点突破了传统的基于 WEB 的社交网络在空间和时间上的局限性, 极大地方便了人们的工作和生活需求, 提高了社会工作效率. 但是在有些情况下, 移动社交网络还是会受限于用户所处的场景而无法正常工作, 例如, 道路拥堵、比赛现场或者紧急灾害等. 移动 Ad Hoc 社交网络^[1] (mobile Ad Hoc social networks, MASNs) 是将 Ad Hoc 模式与移动社交网络相结合, 社交网络用户可以通过自组织、多跳的方式与具有相同兴趣的其他网络用户进行通信, 这样可以突破移动设备信号覆盖范围有限的约束, 真正让移动社交网络做到“随时随地”.

MASNs 可以在没有基础设施的情况下运行, 这使其应用领域得到广泛地拓展^[2]. 然而, 由于缺乏安全防护意识和措施, 再加上无线传输媒介的广播性, MASNs 中的用户经常受到假冒用户的欺诈, 甚至遭受恶意攻击. 当前, 研究者们主要从微观的角度采用一些具体的方案来加强网络的安全性, 包括分析历史追踪数据^[3]、建立信誉评价体系^[4]、随机密钥预分配 (random key predistribution, RKP)^[5,6] 等技术. 但是很少有人从宏观的角度去深入研究安全需求对 MASNs 网络性能到底产生了多大影响,

引用格式: 陆佃杰, 张桂娟, 郑向伟, 等. 移动 Ad Hoc 社交网络中的安全连通性分析. 中国科学: 信息科学, 2015, 45: 97–110, doi: 10.1360/N112014-00255

图 1 MASNs 安全通信示例

Figure 1 An exemplary secure communication in MASN. (Here solid lines represent physical connection and dashed lines represent trustful connection, respectively.)

而此类研究对保障 MASN 的安全具有指导意义. 网络连通性是衡量网络性能的重要指标, 也是网络用户进行信息分发与共享的基本前提. 本文以安全连通性为切入点, 研究如何建立一种安全连通分析体系, 从而为增强 MASN 用户通信的安全性提供基础性指导.

渗流理论是研究无线网络连通性的有利工具 [7]. 通过将无线网络建模为服从泊松 (Poisson) 点过程的随机几何图, 网络连通性可以被映射为渗流过程中的点渗流或者边渗流: 当节点密度很低时, 网络将被分割成小块; 增加节点的密度, 则会出现一些小的连通簇, 簇中节点之间可以通过单跳或者多跳方式进行通信; 随着密度的不断增加, 网络中就会出现一个极大连通簇; 如果簇中任何一个节点几乎肯定能够连接网络中的其他节点, 该网络就被认为发生了渗流. 但是, 当前关于网络渗流的结论无法直接应用到 MASN 中去. 首先, MASN 中的用户对安全性要求较高. 在 MASN 中, 每个节点都需要具有转发数据包的路由功能, 以便构建一个连通的网络. 然而, 如果节点没有跟其他节点建立信任关系, 该节点发送的数据包就未必能够被其邻居节点正确地处理. 因此, 研究 MASN 中的安全连通性 (图 1 所示) 需要考虑两个约束: (1) 几何距离约束; 当节点在几何距离上是不连通的, 就不可能利用传统的路由机制为任意一对节点提供多跳通信; (2) 信任关系约束; 当节点在信任关系上是不连通的, 就无法建立合作关系, 也就无法完成信息转发的任务. 其次, 已有的研究都是针对同构网络的. 而 MASN 属于异构网络, 其不同用户终端的传输范围是有差异的. 因此对 MASN 安全渗流的研究需要综合考虑用户间的信任关系以及终端传输范围的影响.

针对以上分析, 本文专注于研究移动 Ad Hoc 社交网络的安全连通性. 首先, 通过将节点间的信任关系分布建模成一个更新随机过程, 从四个阶段构建 MASN 的安全图, 即几何图构建、信任图构建、安全图构建以及安全图增广. 其次, 利用连续渗流理论证明了 MASN 的安全图渗流现象的存在性: 当节点密度大于临界密度时, 网络发生渗流; 而当节点密度低于临界密度时, 网络不渗流. 最后, 研究了泊松随机几何图中节点临界密度 λ_c^s 的特征. 利用聚类系数方法, 获取了 λ_c^s 更严格的下界. 本文的相关结论还可以应用于移动 Ad Hoc 社交网络的整体规划中, 从总体上提升网络的性能. 比如, 在信息分发的过程中, 依据网络安全连通程度合理地选择转发节点, 从而实现信息分发时延的最小化; 在网络拓扑控制过程中根据节点安全连通状况动态调整节点部署, 从而达到网络覆盖的最大化.

2 相关工作

随着移动 Ad Hoc 社交网络研究的日益广泛, 针对 Ad Hoc 社交平台建设以及社交关系发现等问

题已经有了很多研究^[8,9], 而对连通性问题的研究还处于初级阶段. 网络连通是 MASN_s 进行信息分发与共享以及其他应用的基本前提. 前人已经从发送功率、传输时延、链路稳定性等几个方面对无线 Ad Hoc 网络的连通性进行了广泛的研究^[10~16]. 其中, 在发送功率方面, Gupta 和 Kumar^[10] 研究了在保证网络近似连通的情况下每个节点发送所需的临界功率. Li 等^[11] 利用定向天线研究了近似连通情况下的关键传输功率问题. 在传输时延方面, Dousse 等^[12] 研究了无线传感器网络中非协调功率节省机制的消息传输时延问题. 他们证明了传输时延与传输距离、节点密度以及节点激活和睡眠的时段等网络参数有关系. 在文献^[13] 中, 作者研究了网络拓扑随着失败的节点不断增加到最终引发关键相变的累积时延问题. 在链路稳定性方面, Kong 和 Yeh^[14] 研究了节点间距离变化导致的链路中断对连通性造成的影响. Zhao 等^[15] 针对大规模无线 Ad Hoc 网络中不稳定的链接, 对节点密度和传输延时的基本关系给出了一个更加精确地描述. 文献^[16] 主要分析了不稳定链路环境下网络连通的最小节点度的特性. 另外, 还有一些学者对其他新兴网络的连通性进行了研究. 比如, 在文献^[17] 中, 作者采用在大规模混合网络中建立基站的方法来提高次临界状态下 Ad Hoc 网络的连通性. 文献^[18] 利用迭代分解的方法获取了网络定向连通性的分析模型, 并将该模型应用于车载自组网 (vehicular ad hoc network, VANET) 连通性的分析. 我们也在认知无线 Ad Hoc 网络的连通性研究领域做了一系列的工作^[19,20], 包括量化动态频谱特征对认知无线网络连通性的影响、获取保证认知网络连通性的关键条件等. 然而, 以上关于连通性的研究并没有考虑到网络安全性的需求. 由于移动 Ad Hoc 社交网络用户的利益及隐私对安全性要求较高, 因此安全连通性的研究对 MASN_s 的应用和发展有至关重要的作用.

目前关于安全连通性的研究才刚刚起步, 研究者们逐渐将安全连通视为 Ad Hoc 网络应用的一个先决条件^[21,22]. Zhang 等^[23,24] 提出了一个通用的模型来分析网络的安全连通性并对安全网络的吞吐量和延迟进行量化. 但他们并没有对网络安全连通关键密度 λ_c^s 的值给出计算. 在之前对 Ad Hoc 网络连通性的研究中, 渗流理论是最为常用的工具. 如何表征渗流发生的临界密度是渗流理论的一个核心问题. 文献^[25] 表明, 二维随机几何图中的关键密度满足 $\lambda^c \approx 1.44$. 文献^[26] 将连通性映射为网格上的边渗流, 从而获得 λ^c 的数值范围为 $1.435 < \lambda^c < 1.437$. Kong 等^[27] 采用聚类系数的方法进行了更为严谨的关键密度计算. 但是, 这些网络渗流临界密度的研究主要是针对具有相同节点传输范围的同构网络, 而对于用户终端各异的 MASN_s 来说, 需要研究能计算不同节点传输范围的新方法.

本文主要针对以上问题, 重点分析异构 MASN_s 的安全连通性特征. 为实现这一目标, 我们首先将安全 MASN_s 映射为一种随机几何图并对其进行了扩展. 然后利用连续渗流理论证明了安全 MASN_s 中渗流现象的存在性, 并利用聚类系数的方法推导出异构 MASN_s λ_c^s 的更严格下界. 在下面的章节中, 我们将介绍随机几何图和渗流理论的初步知识.

3 网络模型

3.1 随机几何图

在不考虑连通安全性的情况下, 无线网络中两个节点间的几何距离只要不大于它们的传输距离, 节点间即可进行数据传输. 让 $\|\cdot\|$ 表示欧式范数. 本文将 MASN_s 建模为一个随机几何图^[28], 并将其表示为 $G(\mathcal{X}_n, r_n)$, 其中 $\mathcal{X}_n = X_n, n \in \mathbb{N}$ 表示节点集, r_n 表示节点的传输范围. X_i 表示 $\mathbb{R}^2$ 中节点 i 的随机位置, $X_1, X_2, \dots, X_n$ 属于区域 $\mathcal{D} = [0, \sqrt{n/\lambda}]^2$ 中独立且均匀分布的节点.

在该模型中, 假设节点的传输半径 r_n 是相同的. 对于由任意两个节点组成的节点对 (x_i, x_j) 来说,

图 2 从图 1 中分解出来的图模型

Figure 2 Graph models decoupled from the original MASN in Figure 1. (a) Physical graph; (b) trust graph

如果 $\|x_i - x_j\| \leq r_n, r_n > 0$, 则该节点对之间存在无向链接.

将 $D = |D|$ 看作区域 D 的面积. 只有当节点 i 位于以 x_j 为圆心 r_j 为半径的圆内时, 节点 i 和 j 之间才会有链接. 忽略边界影响, 这样一条链接存在的概率为 $\pi r^2 / D = \lambda \pi r^2 / n$. 在这种情况下, 当 $n \rightarrow \infty, D \rightarrow \infty$ 并且 $n/D = \lambda$ 固定时, $G(\mathcal{X}_n, r_n)$ 可以被看作是一个同构的泊松点过程.

本文假设每个点 X_i 都有一个独立可变的传输半径 r_i 而不是固定的传输半径. r_i 在 $(0, r)$ 的范围内变化, 比如, $P(r_i < r) = 1$. 特殊情况下, 我们可以取单位长度 $r = 1$, 则根据伸缩定律^[29] 可以将相关结论拓展到任意半径 r . 为了简便起见, 我们假设 r_i 共同服从一个概率密度为 $h(r)$ 的分布 $\mathcal{H}(r)$.

3.2 安全图

定义 1 (几何链接 GLink) 当且仅当节点 X_i 和 X_j 之间的几何距离小于通信范围 r_n , 即, $\|X_i - X_j\| < r_n$ 时, 它们之间即存在几何链接. 如果一个 GLink 存在于 X_i 和 X_j 之间, 它们互相称作几何邻居. 用 $\mathcal{L}_{gl}$ 表示几何链接集合.

定义 2 (几何图 GGraph) 由顶点集 $\mathcal{X}_n$ 和几何链接集 $\mathcal{L}_{gl}$ 可以构成几何图 (如图 2(a) 所示), 可以表示为 $G(\mathcal{X}_n, \mathcal{H}(r), \mathcal{L}_{gl})$.

定义 3 (信任关系 TR) 当两个节点之间相互信任时, 则称它们相互拥有信任关系 (也称朋友关系). 在 MASN 中, 信任关系可以看做两个节点共享一个密码, 或者互相知道授权码.

定义 4 (信任链接 TLink) 当且仅当两个节点之间拥有 TR, 则两个节点之间可以建立信任链接.

定义 5 (信任图 TGraph) 可以用 $G(\mathcal{X}_n, \mathcal{H}(r), \mathcal{L}_{tl})$ 来表示信任图 TGraph. 该图包含节点集 $\mathcal{X}_n$ 和信任链接集 $\mathcal{L}_{tl}$. 图 2(b) 是从图 1 中分离出来的信任图的示例. 该信任图的特征可以表示 MASN 中用户之间存在的社交关系.

定义 6 (安全链接 SLink) 当且仅当 X_i 和 X_j 是几何邻居并且相互信任时, 它们之间可以建立安全链接. 我们将安全链接表示为 $\mathcal{L}_{sl}$. 因此, 节点间是否能够建立安全链接是受节点间的几何距离以及信任关系共同决定的.

定义 7 (安全图 SGraph) 安全图可以看做是由节点集 $\mathcal{X}_n$ 和安全链接集合 $\mathcal{L}_{sl}$ 构成的随机几何图, 可以表示为 $G(\mathcal{X}_n, \mathcal{H}(r), \mathcal{L}_{sl})$.

3.3 渗流理论

下面, 我们介绍关于渗流的术语来进一步了解一个随机几何图连续渗流过程是如何与网络的安全连通性相关联的.

定义 8 (极大连通图 $C_{\max}$) $C_{\max}$ 是图 $G(\mathcal{X}_n, r_n)$ 中最大的连通子图. 在极大连通图中, 大部分的节点都能建立安全的链接.

定义 9 (渗流概率 $\text{Prob}_\infty(\lambda_n)$) $\text{Prob}_\infty(\lambda_n)$ 是指极大连通图 $G(\mathcal{X}_n, r_n)$ 中有无穷多个节点的概率, 比如, $\text{Prob}_\infty(\lambda) = \text{Prob}(|C_{\max}| = +\infty)$.

定义 10 (关键密度 λ^c) 在 MASNs 中, 关键密度就是能够使网络发生安全渗流的节点的密度, 比如, $\lambda^c = \inf\{\lambda > 0 : \text{Prob}_\infty(\lambda) > 0\}$.

渗流理论的主要结论就是存在一个关键密度, 当满足 $\lambda > \lambda^c$ 时, 网络发生渗流现象, 相反地, 则没有渗流.

4 安全图的属性

本章主要研究信任关系 TR 的分布以及如何构造一个安全图 $G(\mathcal{X}_n, \mathcal{H}(r), \mathcal{L}_{sl})$. 其次, 我们还证明了图 $G(\mathcal{X}_n, \mathcal{H}(r), \mathcal{L}_{sl})$ 的渗流现象的存在性.

4.1 信任关系的分布

我们假设整个系统的运行时间是按照时长为 T_s 的时隙进行的. 不失一般性, 我们设为 $T_s = 1$. 本文将 TR 的分布建模为一个独立同分布的更新随机过程 (renewal process, RP), 记为 $\mathcal{S}(t)$. $\mathcal{S}(t)$ 可以在两个状态间进行转换: 授权状态, 代表 TR 已经被建立起来了; 非授权状态, 代表 TR 已经被取消. 利用 $\mathcal{S}(t)$ 的马尔科夫 (Markov) 属性, 可以将独立同分布的授权阶段 $\mathcal{Z}_1(t)$ 和未授权阶段 $\mathcal{Z}_0(t)$ 描述为 $\mathcal{S}(t)$ 的离散时间马尔科夫 on/off (授权/未授权) 过程.

我们将授权状态转换到未授权状态的概率表示为 p_{10} , 并将未授权状态转换到授权状态的概率表示为 p_{01} , 而在下一个时隙保持授权或者未授权状态的概率可以分别表示为 p_{11} 和 p_{00} . 其中, $p_{01} = 1/E[\mathcal{Z}_0(t)]$ 并且 $p_{10} = 1/E[\mathcal{Z}_1(t)]$. 则 $\mathcal{S}(t)$ 的稳态分布可以表示为

$$\eta_0 \triangleq \Pr\{\mathcal{S}(t) = 0\} = \lim_{t \rightarrow \infty} \frac{E[\mathcal{Z}_0(t)]}{E[\mathcal{Z}_0(t)] + E[\mathcal{Z}_1(t)]}, \quad (1)$$

$$\eta_1 \triangleq \Pr\{\mathcal{S}(t) = 1\} = \lim_{t \rightarrow \infty} \frac{E[\mathcal{Z}_1(t)]}{E[\mathcal{Z}_0(t)] + E[\mathcal{Z}_1(t)]}. \quad (2)$$

4.2 安全图的构建

按照第 3.2 小节中对安全图的定义, 可将安全图的构建分成几何图构建、信任图构建、安全图建立和安全图的增广等四个阶段.

几何图的构建阶段发生在当节点发现一个新的几何邻居节点出现在其一跳范围内. 通常节点都会周期性地向其邻居节点广播信标信息. 因此, 发现几何邻居最简单的方法就是解码其接收到的信标信息中的 ID 以及相关标识信息. 信任图可以根据式 (2) 中获取的信任概率进行构建. 依据该公式, 在稳态情况下, 两个节点拥有 TR 的概率为 η_1 . 然后, 可以通过判断任意两个节点是否同时拥有几何链路和信任链路来完成安全图的构建.

由于信任关系的限制, 节点只能与相邻节点集的一个子集建立直接的安全链接. 而在 MASNs 的实际应用中, 社交用户可能通过第三方与其他用户建立间接的信任关系. 因此, 最终的安全图还需要利用第三方节点对前面建立的安全图进行增广. 本文将这种情况为两种: 在第一种情况下, 一个节点与另外两个节点拥有 GLink 和 TLink, 但这两个节点彼此之间没有信任关系. 如图 3(a) 所示, 例如, 节点 n_d 和 n_e 都与节点 n_c 有 GLink 和 TLink. n_d 和 n_e 之间有 GLink 但没有 TLink. 幸运的是, 这个

图 3 安全图的增广

Figure 3 The secure graph augmentation: (a) Secure graph; (b) enhanced secure graph

SLink 可以通过节点 n_c 的帮助而建立. 还有另外一种情况, 一个节点与其他两个节点有 TLink, 却只与其中的一个节点有 GLink, 比如图 3(a) 中的节点 n_e , n_f 和 n_g . n_e 与节点 n_f 和 n_g 有 TLink, 但与节点 n_f 只有 GLink. 此时, 节点 n_f 与 n_g 之间的 SLink 可以通过节点 n_e 的帮助获取.

4.3 安全 MASN 的渗流现象

虽然渗流现象的存在性已经分别在单信道场景^[2,7]和多信道场景^[19,20]中被研究和证明过, 但是在安全场景中还没有被证明过. 因此在研究渗流发生条件之前, 我们先证明渗流现象在安全 MASN 中的存在性.

定理 1 用 $\lambda_s^c(\eta_1)$ 表示安全 MASN 模型 $G(\mathcal{X}_n, \mathcal{H}(r), \mathcal{L}_{sl})$ 的关键密度. 当 $\lambda < \lambda_s^c(\eta_1)$ 时, $G(\mathcal{X}_n, \mathcal{H}(r), \mathcal{L}_{sl})$ 在所有 $t > 0$ 的情况下都不会渗流; 当 $\lambda > \lambda_s^c(\eta_1)$ 时, 对于所有的 $t > 0$, 网络都处于渗流状态.

证明 一方面, 考虑 $\lambda > \lambda_s^c(\eta_1)$ 的场景. 让 E 代表 $G(\mathcal{X}_n, \mathcal{H}(r), \mathcal{L}_{sl})$ 发生渗流的事件, 则 E 属于长尾事件^[30]. 根据 Kolmogorov 的 0-1 定理^[30], E 事件发生的概率 $\Pr(E)$ 取值为 0 或 1. 由于 $\Pr(E)$ 与节点密度 λ 成非递减关系, 当 λ 较小时 $\Pr(E) = 0$, 网络处于非渗流状态. 而当 λ 增大到一定程度时 $\Pr(E) = 1$, 网络处于渗流状态, 即满足条件 $\lambda > \lambda_s^c(\eta_1)$ 时, 渗流现象发生. 其中, $\lambda_s^c(\eta_1)$ 为状态转换时的临界密度. 为了证明当 $\lambda > \lambda_s^c(\eta_1)$ 时, 网络在所有 $t > 0$ 情况下都处于渗流状态, 我们构造安全模型 $G(\mathcal{X}_n, \mathcal{H}(r), \mathcal{L}'_{sl})$ 并且选择 $\sigma > 0$ 以便 $\lambda > \lambda_s^c(\eta'_1) > \lambda_s^c(\eta_1)$, 其中 $\eta'_1 = (1 - \sigma)\eta_1$. 选择 $\tau > 0$ 以便对于任何安全链接 (i, j) , 存在 $\Pr\{\mathcal{S}_{ij}(\tau) = 1 | \mathcal{S}_{ij}(0) = 1\} > 1 - \sigma$, 其中 $\mathcal{S}_{ij}(\tau) \triangleq \min_{t \in [0, \tau]} \mathcal{S}_{ij}(t)$. 从而, $\Pr\{\mathcal{S}_{ij}(\tau) = 1\} > (1 - \sigma)\eta_1 = \eta'_1$. 再加上条件 $\lambda > \lambda_s^c(\eta'_1)$, 可以认为对于任何 $t \in [0, \tau]$, $G(\mathcal{X}_n, \mathcal{H}(r), \mathcal{L}_{sl})$ 都是渗流的. 将所有的 m 为整数的间隔 $[m\tau, (m+1)\tau]$ 重复该过程. 用 E_m 表示 $G(\mathcal{X}_n, \mathcal{H}(r), \mathcal{L}_{sl})$ 对于 $t \in [m\tau, (m+1)\tau]$ 发生渗流的事件, E_m^c 表示未发生渗流的事件. 我们可以知道 $\Pr\{\bigcap_m E_m\} = 1 - \Pr\{\bigcup_m E_m^c\} \geq 1 - \sum_m \Pr\{E_m^c\} = 1$.

另一方面, 考虑 $\lambda < \lambda_s^c(\eta_1)$ 的场景. 正如我们在 3.2 小节提到的, 安全图 $G(\mathcal{X}_n, \mathcal{H}(r), \mathcal{L}_{sl})$ 可以被看做是网络 $G(\mathcal{X}_n, r_n)$ 的子图, 即 $G(\mathcal{X}_n, \mathcal{H}(r), \mathcal{L}_{sl}) \subset G(\mathcal{X}_n, r_n)$. 当节点的密度满足条件 $\lambda < \lambda_s^c(\eta_1)$ 时, 网络 $G(\mathcal{X}_n, r_n)$ 不会发生渗流. 因此, 由耦合定理^[29]可知, 安全图 $G(\mathcal{X}_n, \mathcal{H}(r), \mathcal{L}_{sl})$ 也不会发生渗流. 为了证明当 $\lambda > \lambda_s^c(\eta_1)$ 时, 网络在所有 $t > 0$ 情况下都处于非渗流状态, 我们也构造一个新安全 MASN 模型 $G(\mathcal{X}_n, \mathcal{H}(r), \mathcal{L}'_{sl})$ 并且选择 $\sigma > 0$ 使得 $\lambda < \lambda_s^c(\eta'_1) \leq \lambda_s^c(\eta_1)$, 其中 $\eta'_1 = \sigma(1 - \eta_1) + \eta_1$. 然后, 选择 $\tau > 0$ 以便对于任何安全链接 (i, j) , 存在 $\Pr\{\mathcal{S}_{ij}(\tau) = 0 | \mathcal{S}_{ij}(0) = 0\} > 1 - \sigma$, 其中 $\mathcal{S}_{ij}(\tau) \triangleq \max_{t \in [0, \tau]} \mathcal{S}_{ij}(t)$. 从而, $\Pr\{\mathcal{S}_{ij}(\tau) = 1\} = 1 - \Pr\{\mathcal{S}_{ij}(\tau) = 0\} < 1 - (1 - \eta_1)(1 - \sigma) = \eta'_1$. 又因为 $\lambda > \lambda_s^c(\eta'_1)$, 则对于任何 $t \in [0, \tau]$, $G(\mathcal{X}_n, \mathcal{H}(r), \mathcal{L}_{sl})$ 都不渗流. 将所有的 m 为整数的间隔 $[m\tau, (m+1)\tau]$ 重复该过程. 我们可以

知道 $\Pr\{\bigcap_m E_m^c\} = 1 - \Pr\{\bigcup_m E_m\} \geq 1 - \sum_m \Pr\{E_m\} = 1$. 因此定理 1 可以得证.

在后面的章节中, 我们将使用聚类系数方法获取更加精确的安全连通关键密度 λ_s^c 的下限值.

5 关键密度的下限值

受同构网络使用聚类系数 (clustering coefficient, CC) 方法研究关键密度^[27]的启发, 本文将这些方法拓展到安全 MASN 以便获取网络安全连通的特性. 与前人的安全连通性研究^[23]不同, 本文的方法不仅考虑了邻居节点之间的空间相关性, 还考虑了异构网络中节点的不同传输范围以及节点间信任关系的影响. 该方法能够为具有安全保障的 MASN 渗流现象提供更加精确的关键密度.

定理 2 对于一个安全 MASN $G(\mathcal{W}_\lambda, \mathcal{H}(r), \mathcal{L}_{sl})$ 来说, 存在节点的关键密度 λ_s^c , 高于该密度时网络是渗流的, 低于该密度时, 网络不发生渗流. 而且,

$$\lambda_s^c \geq \frac{1}{\xi(1 - C_{SLC})}, \quad (3)$$

其中 $\xi = 2\pi \int_0^1 \int_0^r \eta_1 x(1 - \mathcal{H}(x)) dx d\mathcal{H}$, η_1 可以通过式 (2) 获取. C_{SLC} 代表安全链接系数, 详细计算过程见第 5.1 小节.

定义 11 (聚类系数 CC) 在网络 $G(\mathcal{X}_n, 1)$ 中给出三个节点 X_i, X_j 和 X_k , 则聚类系数就是指在节点 X_i 和 X_j 分别与 X_k 相邻的前提下, X_i 和 X_j 也相邻的条件概率. 其中, 相邻是指节点在互相的传输范围之内.

聚类系数能够体现同构网络中邻居链接之间的空间相关性. 利用该系数可以获取网络 $G(\mathcal{X}_n, 1)$ 渗流的如下引理^[27]:

引理 1 给定网络 $G(\mathcal{X}_n, 1)$, 其节点度的均值为 μ , 聚类系数为 C_c ; 如果满足条件 $\mu < \frac{1}{1-C_c}$, 则网络 $G(\mathcal{X}_n, 1)$ 不渗流.

然而, 安全 MASN 中邻居链接之间的依赖关系除了考虑空间相关性以外, 还需要考虑邻居间的信任关系以及异构网络中节点传输范围差异的影响. 为了将聚类系数方法的相关结论应用到安全 MASN 中去, 本文在综合考虑以上各种相关性影响因素的基础上, 引入了安全链接系数来研究 MASN 中的安全连通性.

定义 12 (安全链接系数 SLC) 给定 $G(\mathcal{X}_n, \mathcal{H}(r), \mathcal{L}_{sl})$ 以及三个节点 X_i, X_j, X_k , 则安全链接系数 C_{SLC} 是在安全链接 ℓ_{ij} 和 ℓ_{ik} 存在的前提下, 链接 ℓ_{jk} 也存在的条件概率. 其中, 安全链接是指节点间既是几何邻居又具有朋友关系.

5.1 C_{SLC} 的计算

考虑到异构 MASN 节点的不同传输半径, 本文将场景分成了 6 个阶段: $r_a \leq r_b \leq r_c, r_b \leq r_a \leq r_c, r_b \leq r_c \leq r_a, r_a \leq r_c \leq r_b, r_c \leq r_a \leq r_b, r_c \leq r_b \leq r_a$. 其中 r_a, r_b 和 r_c 分别是节点 n_a, n_b 和 n_c 的传输半径. 由于节点 n_b 和 n_c 的对称性, 这里我们只考虑前面三个阶段. 将 u 定义为节点 n_a 和 n_b 之间的欧氏距离, 例如, $u = \sqrt{(x_a - x_b)^2 + (y_a - y_b)^2}$, 其中 x 和 y 是节点的坐标. 我们还定义圆心为 n_i , 半径为 r_i 的圆为 S_i , 其覆盖的区域为 $S_i (i \in a, b, c)$. 下面我们计算安全 MASN 的 C_{SLC} .

图 4 阶段 I: $r_a < r_b < r_c$. 该阶段被分为两种情况: (1) $r_b > r_a + u$; (2) $r_b < r_a + u$

Figure 4 Phase I: $r_a < r_b < r_c$. This phase can be divided into two cases: (1) $r_b > r_a + u$; (2) $r_b < r_a + u$

5.1.1 阶段 I ($r_a \leq r_b \leq r_c$)

图 4 展示的是 $r_a \leq r_b \leq r_c$ 的场景. 通过该图我们可以很容易计算出条件概率为

$$\eta_1 \frac{S_a \cap S_b}{S_a}. \quad (4)$$

如果 $r_b > r_a + u$, 可以得到 $S_a \cap S_b = S_a$, 条件概率为 η_1 .

如果 $r_b < r_a + u$, 圆形区域 $S(n_b, r_a - u)$ (以 n_b 为中心, $r_a - u$ 为半径) 内相邻节点的数量为 $\int_0^{r_a - u} \eta_1 2\pi x dx$. 在 S_a 和 S_b 交叠区域内部, 但不在 $S(n_b, r_a - u)$ 的相邻节点数量为 $\int_{r_a - u}^{r_b} 2\eta_1 \alpha_1 x dx$. 由此可以得到概率

$$q_1(u) = \eta_1 \frac{\pi(r_a - u)^2 + \int_{r_a - u}^{r_b} 2\alpha_1 x dx}{\pi r_a^2}, \quad (5)$$

其中,

$$\alpha_1 = \angle n_a n_b O = \cos^{-1} \frac{x^2 + u^2 - r_a^2}{2xu}. \quad (6)$$

将 r_a, r_b and r_c 的联合分布表示为 $h(r) = h_a(r_a)h_b(r_b)h_c(r_c)$. 则阶段 I 的条件概率 Π_1 可以写为

$$\Pi_1 = \int_0^{1/2} \int_u^{1-u} \int_{r_a+u}^1 \int_{r_b}^1 2u\eta_1 h(r) dr_c dr_b dr_a du + \int_0^1 \int_u^1 \int_{r_a+u}^{r_a+u} \int_{r_b}^1 2uq_1(u)h(r) dr_c dr_b dr_a du. \quad (7)$$

5.1.2 阶段 II ($r_b < r_c < r_a$)

图 5 展示的是 $r_b < r_c < r_a$ 的场景. 条件概率可以写为

$$\eta_1 \frac{S_a \cap S_b}{S_a}. \quad (8)$$

如果 $r_a > r_b + u$, 我们可以得到 $\frac{S_a \cap S_b}{S_a} = \frac{r_b^2}{r_a^2}$, 条件概率为 $\eta_1 \frac{r_b^2}{r_a^2}$.

如果 $r_a < r_b + u$, 圆形区域 $S(n_a, r_b - u)$ (以 n_a 为中心, $r_b - u$ 为半径) 内相邻节点的数量为 $\int_0^{r_b - u} \eta_1 2\pi x dx$. 在 S_b 和 S_a 交叠区域内部但是不在 $S(n_a, r_b - u)$ 的相邻节点数量为 $\int_{r_b - u}^{r_b} 2\eta_1 \alpha_2 x dx$. 由此可以得到概率

$$q_2(u) = \eta_1 \frac{\pi(r_b - u)^2 + \int_{r_b - u}^{r_b} 2\alpha_2 x dx}{\pi r_b^2}, \quad (9)$$

图 5 阶段 II: $r_b < r_a < r_c$. 该阶段被分为两种情况: (1) $r_a > r_b + u$; (2) $r_a < r_b + u$

Figure 5 Phase II: $r_b < r_a < r_c$. This phase can be divided into two cases: (1) $r_a > r_b + u$; (2) $r_a < r_b + u$.

图 6 阶段 III: $r_b < r_c < r_a$. 该阶段被分为两种情况: (1) $r_c > r_b + u$; (2) $r_c < r_b + u$

Figure 6 Phase III: $r_b < r_c < r_a$. This phase can be divided into two cases: (1) $r_c > r_b + u$; (2) $r_c < r_b + u$

其中,

$$\alpha_2 = \angle n_b n_a O' = \cos^{-1} \frac{x^2 + u^2 - r_b^2}{2xu}. \quad (10)$$

将 r_a , r_b and r_c 的联合分布表示为 $h(r) = h_a(r_a)h_b(r_b)h_c(r_c)$.

因此,对于阶段 II 来说,条件概率 Π_2 可以写为

$$\Pi_2 = \int_0^{1/2} \int_u^1 \int_{r_b+u}^1 \int_{r_a}^1 2u\eta_1 \frac{r_b^2}{r_a^2} h(r) dr_b dr_a dr_c du + \int_0^1 \int_u^1 \int_{r_b+u}^1 \int_{r_a}^1 2uq_2(u) h(r) dr_b dr_a dr_b du. \quad (11)$$

5.1.3 阶段 III ($r_b < r_c < r_a$)

图 6 展示的是 $r_b < r_c < r_a$ 的场景. 条件概率可以写为

$$\eta_1 \frac{S_b \cap S_c}{S_c}. \quad (12)$$

如果 $r_c > r_b + u$, 我们可以得到 $\frac{S_b \cap S_c}{S_c} = \frac{r_b^2}{r_c^2}$, 条件概率为 $\eta_1 \frac{r_b^2}{r_c^2}$.

如果 $r_c < r_b + u$, 圆形区域 $\mathcal{S}(n_c, r_b - u)$ (以 n_c 为中心, $r_b - u$ 为半径) 内相邻节点的数量为 $\int_0^{r_b-u} \eta_1 2\pi x dx$. 在 $\mathcal{S}_b$ 和 $\mathcal{S}_c$ 交叠区域内部但是不在 $\mathcal{S}(n_c, r_b - u)$ 的相邻节点数量为 $\int_{r_b-u}^{r_c} 2\eta_1 \alpha_3 x dx$. 由此可以得到概率

$$q_3(u) = \eta_1 \frac{\pi(r_c - u)^2 + \int_{r_b-u}^{r_c} 2\alpha_3 x dx}{\pi r_c^2}, \quad (13)$$

其中

$$\alpha_3 = \angle n_b n_c O'' = \cos^{-1} \frac{x^2 + u^2 - r_c^2}{2xu}. \quad (14)$$

因此, 对于阶段 III 来说, 条件概率 Π_3 可以写为

$$\Pi_3 = \int_0^{1/2} \int_u^1 \int_{r_b+u}^1 \int_{r_c}^1 2u\eta_1 \frac{r_b^2}{r_c^2} h(r) dr_a dr_c dr_b du + \int_0^1 \int_u^1 \int_{r_b+u}^1 \int_{r_c}^1 2uq_3(u) h(r) dr_a dr_c dr_b du. \quad (15)$$

最后, 由于节点 n_b 和 n_c 的对称性, 我们可以得到

$$\mathcal{C}_{\text{SLC}} = 2(\Pi_1 + \Pi_2 + \Pi_3). \quad (16)$$

5.2 定理 2 的证明

定理 2 的证明如下:

证明 在 $G(\mathcal{X}_n, \mathcal{H}(r), \mathcal{L}_{sl})$ 中, 节点度的均值为

$$\mu = \int_0^1 2\pi\lambda \int_0^r \eta_1 x(1 - \mathcal{H}(x)) dx d\mathcal{H}. \quad (17)$$

通过与文献 [27] 引理 1 相似的证明, 我们可以获得与引理 1 相同的结论, 即给定一个平均节点度 μ 以及安全链接系数 $\mathcal{C}_{\text{SLC}}$, 如果

$$\mu < \frac{1}{1 - \mathcal{C}_{\text{SLC}}}, \quad (18)$$

则安全 MASNs $G(\mathcal{X}_n, \mathcal{H}(r), \mathcal{L}_{sl})$ 是不渗流的. 由于篇幅的限制, 本文不再详细论述.

将式 (17) 代入式 (18), 可以将网络不发生渗流的条件转换为

$$\lambda < \frac{1}{\xi(1 - \mathcal{C}_{\text{SLC}})}, \quad (19)$$

其中 $\xi = 2\pi \int_0^1 \int_0^r \eta_1 x(1 - \mathcal{H}(x)) dx d\mathcal{H}$. 因此, $\lambda \geq \frac{1}{\xi(1 - \mathcal{C}_{\text{SLC}})}$ 是网络渗流的必要条件. 又由第 4.3 小节定理 1 中安全 MASNs 渗流的特征知道, MASNs 安全连通的关键密度 λ_s^c 存在且满足 $\lambda_s^c \geq \frac{1}{\xi(1 - \mathcal{C}_{\text{SLC}})}$, 因此定理 2 得证.

6 仿真实验

本章将展示 MASNs 中安全连通性的仿真结果. 仿真实验在 Matlab 7.1 的环境下进行. 我们构建了一个 $10 \text{ m} \times 10 \text{ m}$ 的区域并部署 $120 \sim 200$ 个节点, 即节点密度在 $1.2 \sim 2.0$ 范围内变化. 然后, 区域内的每个节点依据安全图的构建过程与周围邻居建立安全链接. 下面我们将展示安全图拓展的示例, 并在此基础上给出安全 MASNs 渗流现象的示例.

图 7 增广安全网络示例

Figure 7 An example of secure network augmentation. (a) Geographic network; (b) secure network (without augmentation); (c) enhanced secure network

6.1 安全图增广示例

本节通过仿真来展现安全图增广对 MASNs 安全链接的影响. 我们引入平均节点度 μ , 即网络中节点间链接的平均数, 来衡量安全图增广的程度.

在该仿真实验中, 首先构建几何连通图. 在 $10\text{ m} \times 10\text{ m}$ 的区域内随机部署 200 个节点, 只要两个节点在相互的传输范围之内, 节点间即可建立一条边, 最终得到的几何连通图如图 7(a) 所示. 然后, 在图 7(a) 的基础上引入信任关系的影响来构建安全连通图. 不失一般性, 我们假设所有的节点 TR 存在的概率为 $\eta_1 = 0.2$. 区域内节点之间只有同时存在几何链接和信任链接时才建立一条边, 得到的安全图如图 7(b) 所示. 该图的节点平均度为 $\mu = 1.7$. 最后, 将图 7(b) 中的节点通过第三方的信任关系进行安全链接增广. 图 7(c) 展示的是增广后的安全图. 该图的节点平均度为 $\mu = 5$, 要远远高于图 7(b) 中的平均节点度. 由此可见, 安全图增广能够极大地增强 MASNs 的安全连通性.

6.2 渗流现象示例

本节通过仿真节点密度对极大连通簇的影响来展现安全 MASNs 渗流现象的发生. 为了衡量节点极大连通的程度, 我们引入极大连通比例 ρ_g , 即极大连通簇 $C_{\max}$ 中的节点占整个网络节点的比例:

$$\rho_g = \frac{C_{\max} \text{中节点的数量}}{\text{整个网络中节点的数量}} \quad (20)$$

在该仿真实验中, 我们采用与 6.1 小节中相同的场景和不同的节点数量. 在该区域内部署 120 到 180 个节点, 即节点密度在 $\lambda = 1.2$ 到 $\lambda = 1.8$ 的范围内变化 (如图 8 所示). 图中粗线条表示最大连通簇中的边, 细线条表示其他簇中的边. 从图 8(a) 可以看出, 网络被分割成很多小簇. 其中, 极大连通簇的 $\rho_g = 35.8\%$. 将节点数量从 120 ($\lambda = 1.2$) 增加到 150 ($\lambda = 1.5$), 则得到图 8(b) 所示的网络. 该网络也被分成很多个簇, 其中极大连通簇的连通比例变为 $\rho_g = 30.7\%$. 这说明提高网络的节点密度并没有增大 ρ_g 的值. 在图 8(b) 中, 由于节点数量的增多, 连通比例反而降低. 整体来说图 8(a) 和 (b) 的连通比例变化不大. 然而, 与以上两图不同, 当我们将节点密度增加到 180 ($\lambda = 1.8$), 一个包含了网络中绝大多数节点的极大连通簇形成 ($\rho_g = 88.9\%$). 这说明在 $\lambda = 1.8$ 这个关键点处发生了渗流现象 (如图 8(c) 所示).

图 8 渗流现象示例

Figure 8 An example of percolation phenomenon. (a) $n = 120, \lambda = 1.2, \rho_g = 35.8\%$; (b) $n = 150, \lambda = 1.5, \rho_g = 30.7\%$; (c) $n = 180, \lambda = 1.8, \rho_g = 88.9\%$

7 结论及下一步工作

已有的关于连通性的研究很少考虑到网络的安全需求. MASNs 的安全连通性已经成为一个重要且具有挑战性的问题. 本文利用连续渗流理论证明了安全 MASNs 中渗流现象的存在性, 并利用聚类系数法, 获取了渗流时节点关键密度的下限值. 该结果能够为 MASNs 的安全性研究提供重要的理论指导.

然而, 本文提出的安全连通性分析方法本质上都是理论分析, 缺少在实际移动 Ad Hoc 社交网络场景中的测试. 我们下一步的研究重点是将本文的研究成果应用于移动 Ad Hoc 社交网络的信息分发与共享机制中去, 从总体上提升网络的性能. 比如, 在信息分发的过程中, 依据网络安全连通程度选择最优的转发节点, 从而降低信息分发的时延; 同时, 还可以在信息分发过程中根据节点安全连通状况动态调整节点布署, 从而达到信息的最大化覆盖.

参考文献

- 1 Sarigol E, Riva O, Stuedi P, et al. Enabling social networking in Ad Hoc networks of mobile phones. In: Proceedings of the VLDB Endowment. Berlin: Springer, 2009. 1634–1637
- 2 Gambhir S, Aneja N. Ad-hoc social network: a comprehensive survey. Int J Sci Eng Res, 2013, 4: 156–160
- 3 Dong W, Dave V, Qiu L L, et al. Secure friend discovery in mobile social networks. In: Proceedings of the 30th Annual IEEE International Conference on Computer Communications (INFOCOM'11), Shanghai, 2011. 1647–1655
- 4 Jiang W J, Xu Y S, Guo H, et al. Dynamic trust calculation model and credit management mechanism of online trading. Sci Sin Inform, 2014, 44: 1084–1101 [蒋伟进, 许宇胜, 郭宏, 等. 网络在线交易动态信任计算模型与信誉管理机制. 中国科学: 信息科学, 2014, 44: 1084–1101]
- 5 Yavuz F, Zhao J, Yagan O, et al. On secure and reliable communications in wireless sensor networks: towards k-connectivity under a random pairwise key predistribution scheme. In: Proceedings of the IEEE International Symposium on Information Theory, Piscataway, 2014. 2371–2375
- 6 Yagan O, Makowski A M. Modeling the pairwise key predistribution scheme in the presence of unreliable links. IEEE Trans Inform Theory, 2013, 59: 1740–1760
- 7 Dousse O, Thiran P, Hasler M. Connectivity in ad-hoc and hybrid networks. In: Proceedings of the 21st Annual IEEE International Conference on Computer Communications (INFOCOM'02), Piscataway, 2002. 1079–1088
- 8 Podobnik V, Lovrek I. An agent-based platform for Ad-Hoc social networking. In: Proceedings of the 5th KES International Conference on Agent and Multi-agent Systems: Technologies and Applications. Berlin: Springer, 2011. 74–83

- 9 Smailovic V, Podobnik V. Bfriend: context-aware ad-hoc social networking for mobile users. In: Proceedings of the 35th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), Opatija, 2012. 612–617
- 10 Gupta P, Kumar P R. Critical power for asymptotic connectivity. In: Proceedings of the 37th IEEE Conference on Decision and Control, Piscataway, 1998. 547–566
- 11 Li P, Zhang C, Fang Y G. Asymptotic connectivity in wireless ad hoc networks using directional antennas. *IEEE/ACM Trans Network*, 2009, 17: 1106–1110
- 12 Dousse O, Mannersalo P, Thiran P. Latency of wireless sensor networks with un-coordinated power saving mechanisms. In: Proceedings of the 5th ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc'04), New York, 2004. 109–120
- 13 Xing F, Wang W Y. On the critical phase transition time of wireless multi-hop networks with random failures. In: Proceedings of the 14th Annual International Conference on Mobile Computing and Networking (MobiCom'08), New York, 2008. 175–186
- 14 Kong Z, Yeh E M. Connectivity and latency in large-scale wireless networks with unreliable links. In: Proceedings of the 27th Annual IEEE International Conference on Computer Communications (INFOCOM'08), Phoenix, 2008. 1–9
- 15 Zhao S Z, Fu L Y, Wang X B, et al. Fundamental relationship between node density and delay in wireless ad hoc networks with unreliable links. In: Proceedings of the 17th Annual International Conference on Mobile Computing and Networking (MobiCom'11), New York, 2011. 337–348
- 16 Zhao J. Minimum node degree and k-connectivity in wireless networks with unreliable links. In: Proceedings of the IEEE International Symposium on Information Theory (ISIT), Piscataway, 2014. 246–250
- 17 Yi C, Wang W. On the connectivity analysis over large-scale hybrid wireless networks. In: Proceedings of IEEE INFOCOM'10, San Diego, 2010. 1–9
- 18 Zhang L, Cai L, Pan J P. Connectivity in two-dimensional lattice networks. In: Proceedings of the 32nd IEEE International Conference on Computer Communications (INFOCOM'13), Turin, 2013. 2814–2822
- 19 Lu D J, Huang X X, Li P, et al. Connectivity of large-scale cognitive radio ad hoc networks. In: Proceedings of the 31st Annual IEEE International Conference on Computer Communications (INFOCOM'12), Orlando, 2012. 1260–1268
- 20 Lu D J. Research on spectrum allocation and connectivity in cognitive radio networks. Dissertation for Ph.D. Degree. Beijing: Graduate University of Chinese Academy of Sciences, 2012 [陆佃杰. 认知无线网络中频谱分配与连通性研究. 博士学位论文. 北京: 中国科学院研究生院, 2012]
- 21 Panyim K, Krishnamurthy P, Le A. On secure connectivity with adjusting power to cope with jamming in sensor networks. In: Proceedings of Intelligent Signal Processing and Communications Systems, Naha, 2013. 476–480
- 22 Zhao J, Yagan O, Gligor V. Secure k-connectivity in wireless sensor networks under an on/off channel model. In: Proceedings of International Symposium on Information Theory (ISIT), Istanbul, 2013. 2790–2794
- 23 Zhang C, Song Y, Fang Y G. Modeling secure connectivity of self-organized wireless ad hoc networks. In: Proceedings of the 27th Annual IEEE International Conference on Computer Communications (INFOCOM'08), Phoenix, 2008. 1–9
- 24 Zhang C, Song Y, Fang Y G, et al. On the price of security in large-scale wireless ad hoc networks. *IEEE/ACM Trans Network*, 2011, 19: 319–331
- 25 Quintanilla J, Torquato S, Ziff R M. Efficient measurement of the percolation threshold for fully penetrable discs. *Phys A*, 2000, 33: 399–407
- 26 Balister P, Bollobas B, Walters M. Continuum percolation with steps in the square or the disc. *Random Struct Algor*, 2005, 26: 392–403
- 27 Kong Z, Yeh E M. Analytical lower bounds on the critical density in continuum percolation. In: Proceedings of the Workshop on Spatial Stochastic Models in Wireless Networks, Limassol, 2007. 1–6
- 28 Haenggi M, Andrews J G, Baccelli F, et al. Stochastic geometry and random graphs for the analysis and design of wireless networks. *IEEE J Sel Area Commun*, 2009, 27: 1029–1046
- 29 Meester R, Roy R. Continuum Percolation. New York: Cambridge University Press, 1996. 28–30
- 30 Billingsley P. Probability and Measure. New York: Wiley, 1995. 18–25

Secure connectivity analysis of mobile Ad Hoc social networks

LU DianJie^{1,2}, ZHANG GuiJuan^{1,2}, ZHENG XiangWei^{1,2}, LIU Hong^{1,2} & HU Bin^{1,2,3*}

1 School of Information Science and Engineering, Shandong Normal University, Jinan 250014, China;

2 Shandong Provincial Key Laboratory for Novel Distributed Computer Software Technology, Jinan 250014, China;

3 School of Information Science and Engineering, Lanzhou University, Lanzhou 730000, China

*E-mail: bh@lzu.edu.cn

Abstract The security of mobile ad hoc social networks (MASNs) has received considerable attention in the past several years. In MASNs, achieving secure communication is challenging, because all the links must operate with mutual trust. In this paper, we explore the analytical characterization of secure connectivity in MASNs. First, we formulate the distribution of trust relationships between nodes as a renewal process, enabling us to construct a secure graph with four phases, namely geographic graph construction, trust graph construction, secure graph establishment, and secure graph augmentation. Then, we prove the existence of percolation phenomenon in secure MASNs using continuum percolation theory. Finally, we investigate the characterization of the critical density, which is the central problem of secure connectivity. By employing the clustering coefficient method, we derive a tighter lower bound on the critical density. Simulation results show that both the density and trust relationships of nodes can greatly impact the secure connectivity of MASNs. Our results enable a fundamental understanding of secure connectivity in MASNs.

Keywords mobile Ad Hoc social networks, connectivity, security, continuum percolation, critical density

LU DianJie was born in 1981. He received the Ph.D. degree in computer science from the Institute of Computing Technology, Chinese Academy of Sciences, in 2012. Currently, he is an associate professor at Shandong Normal University. His research interests include cognitive wireless network, wireless sensor network and mobile computing. Dr. Lu is a member of CCF.

ZHANG GuiJuan was born in 1980. She received the Ph.D. degree in computer science from the Institute of Computing Technology, Chinese Academy of Sciences, in 2011. Currently, she is an associate professor at Shandong Normal University. Her research interests include distributed computing, visualization and computer animation.

ZHENG XiangWei was born in 1971. He received the Ph.D. degree in computer science from Shandong Normal University, in 2008. Currently, he is a professor at Shandong Normal University. His research interests include computer networks, computational intelligence and collaborative computing.

LIU Hong was born in 1955. She received the Ph.D. degree in computer science from the Institute of Computing Technology, Chinese Academy of Sciences, in 1998. Currently, she is a professor at Shandong Normal University. Her research interests include pervasive computing, computer-aided design, multi-agent system and cooperative design.