

一种新型 WSN 抗毁性评价方法及其仿真实现

林力伟 许力 叶秀彩 (福建师范大学 网络安全与密码技术重点实验室 福建 福州 350007)

摘要: 从特定的以数据为中心的无线传感器网络拓扑结构出发, 首先给出了无线传感器网络连通性的一个新测度—连通系数, 在此基础上给出了抗毁性测度的新定义, 针对面临的两种攻击, 给出了无线传感器网络抗毁性的两个新测度 - 容错度和抗攻击度, 并对基于小世界模型的无线传感器网络抗毁性进行了抗毁性分析, 仿真表明提出的评估模型更能客观, 准确地评估以数据收集为中心的无线传感器网络的抗毁性。

关键词: 无线传感器网络; 小世界网络; 连通性; 抗毁性

A Novel Method and Its Simulation to Evaluate the Invulnerability of Wireless Sensor Networks

LIN Li-Wei, XU Li, YE Xiu-Cai

(Key Lab of Network Security and Cryptology, Fujian Normal University, Fuzhou 350007, China)

Abstract: In this paper, a new measure of wireless sensor network connectivity is proposed based on the characteristics of the data collecting network. A new definition of invulnerability is proposed, and two measures of invulnerability are proposed for the two different damages. At last, this paper studies the invulnerability of the wireless sensor networks based on the small-world model. The simulation indicates that it is a new and effective method to research the invulnerability for the wireless sensor networks.

Keywords: wireless sensor networks; small-word network; connectivity; invulnerability

1 引言

无线传感器网络(WSN)是由一组具有感知能力、计算能力和通讯能力的传感器以 Ad Hoc 方式构成的无线网络, 其目的是协作地感知、采集和处理网络覆盖的地理区域中感知对象的信息, 并发布给观察者^[1]。WSN 在很多领域尤其在无人监测或环境恶劣情况下对事件监测和事件跟踪中有广阔的应用前景^[2]。然而 WSN 节点数量庞大, 但易失效, 极易出现网络中部分节点的失效导致原本连通的网络拓扑分割, 大大降低网络的覆盖度, 甚至使网络失败。

网络抗毁性可以描述网络在电力耗尽、硬件故障或者遭遇入侵等形成的节点失败情况下的可靠程度^[3]。一般认为, 网络抗毁性是指网络拓扑结构的可靠性^[4,5]。文献^[6]中定义了一种综合性网络拓扑抗毁性度量, 以

抗毁连通度 G 表示网络中所有节点团之间可能通信路径的平均值, 并对网络拓扑的抗毁性进行了评估。文献^[7]提出了基于度(degree) 和介数(betweenness) 的关键节点和链路评估模型, 讨论了不同评估模式下网络抗毁能力的差异。文献^[8]介绍了以网络最大连通分支覆盖率为评价标准的评估方法, 文献^[5]给出了复杂性网络环境下抗毁性测度的新定义和网络抗毁性的特点。然而, 对于 WSN 其目的是采集数据发送给观察者, 更强调其节点的协作性及数据收集的目的性。从网络中节点对其链路抗毁性的评估不能准确反映数据收集的 WSN 的抗毁性的特点与需求。

为了更准确、客观地度量网络结构的抗毁性本文提出了基于覆盖率与连通性测度的抗毁性评估模型。主要针对以数据为中心的 WSN 多对一的特点, 综合考

基金项目:福建省自然科学基金(2008J0014)

收稿时间:2009-07-12;收到修改稿时间:2009-08-14

虑了影响该类网络拓扑抗毁能力的相关因素。并以此评估模型评估基于小世界模型的无线传感器网络, 仿真表明该方法的有效性和可行性。

2 一种抗毁性评估模型

本节首先给出了 WSN 网络模型及其相关基本概念; 然后结合网络模型指出网络中部分节点失败形成的连通分支对网络拓扑的影响, 给出了一个新的连通性测度。同时结合网络覆盖率并在此基础上给出了抗毁性测度的新定义。最后, 针对网络中节点面临的两种攻击, 给出了 WSN 抗毁性的两个新测度 - 容错度和抗攻击度。

2.1 网络模型与基本概念

假设网络中只有一个汇聚节点。网络中节点均知道汇聚节点的位置。节点和汇聚节点一旦布置好就是静止的。

用图 $G=(V, E)$ 表示 WSN 网络拓扑, 其中, V 是节点集, E 表示节点间的无线连接, $|V|$ 表示集合 V 节点数目。本文认为节点间链路对称, 图中的边都是无向边。如果一个子图 $G'=(V', E')$, $V' \subseteq V$, 且 V' 中任意两个节点间都有一条路, 则称 G' 为 G 的连通子图。如果图 $G=(V, E)$ 由 ω 个连通子图构成, 记为 $G_1=(V_1, E_1)$, $G_2=(V_2, E_2)$, \dots , $G_\omega=(V_\omega, E_\omega)$, 则 $G_1, G_2, \dots, G_\omega$ 称为图 G 的 ω 个连通分支, 如图 1(a) 所示, 若 $V' \in \{V_1, V_2, \dots, V_\omega\}$ 且 V' 中任意一个节点到汇聚节点都至少有一条路, 则称 $G'=(V', E')$ 为图 G 的有效连通分支, 记

$$CR = \frac{\sum |V_i|}{|V|} \quad (1)$$

表示网络的有效覆盖率, 其中 V_i 为图的有效连通分支中的节点集。本文认为分割后的 WSN 中只有有效连通分支是可用的, 因为 WSN 最终目的是把数据传递给 sink 节点, 如图 1(a) 所示网络分成 4 个连通分支 G_1, G_2, G_3, G_4 , 如果这些连通分支中所有节点都没有路到 sink 节点, 则连通分支是无效的。如图 1(b) 所示, 当 sink 节点附近的节点能量耗尽时, 虽然保持全连通, 但是网络中的节点无法将数据传递给 sink 节点, 也是无效的。因此用有效连通分支的覆盖率来度量网络中部分节点失败后网络拓扑的可用性。

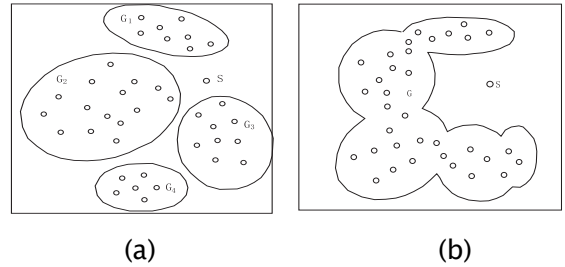


图 1 网络中节点分布示意图

2.2 网络连通性测度

网络的抗毁性从连通性的角度描述了网络拓扑结构的可靠性。以往所指的连通判据都是指网络中任意两个节点都存在通路, 这样的连通性约束对 WSN 是不适用的。对于以传送数据为目的的 WSN 来说, 网络中的节点相互连通并不意味着网络有着较好的连通性, 还与 sink 节点的连通有关, 即与是否为有效的连通有关, 如图 1(b) 所示, 虽然全网保持全连通, 但是网络中的节点无法将数据传递给 sink 节点。如图 1(a) 所示, 虽然网络分割成 4 个连通分支, 但是只要能能够将数据传递给 sink 节点还是能够完成收集数据的任务。因此要用网络中任意节点到 sink 节点的连通性才能更准确度量这类网络的抗毁性。本文将从实际出发, 给出一个适用于以数据为中心的无线传感器网络的网络连通性测度。

定义 1. 称

$$C = \frac{1}{\omega \sum_{i=1}^{\omega} \frac{|V_i|}{|V|} \delta_{is} l_i} \quad (2)$$

为网络的连通系数, 其中 ω 为网络连通分支数, $|V_i|$ 为第 i 个连通分支中节点数目, $|V|$ 为网络节点总数目, l_i 为第 i 个连通分支中的平均最短距离, 即第 i 个连通分支中的所有节点与 sink 节点之间最短路径的平均值。

$$\delta_{is} = \begin{cases} 1 & V_i \text{ 中的任一节点到 sink 节点都有一条通路} \\ 0 & V_i \text{ 中的节点到 sink 节点没有通路} \end{cases} \quad (3)$$

从上述定义可知, 连通分支越少, 各分支的平均最短路径越小, 网络的连通性越好, 连通系数 C 就越大。当全网连通时 $\omega=1$, 此时 C 取得极大值。以此连通性系数度量网络中部分节点失败后网络拓扑的连通性。

2.3 网络抗毁性测度

定义 2. 在一定的连通性与可用性的约束下, 将网络能承受的最大节点的移除比例称为网络的抗毁度。

要测度一个无线传感器网络的抗毁性, 要解决两个问题: 确定连通性约束和可用性约束; 确定打击策略, 即节点的移除方式。

无线传感器网络通常面临两种打击: 1) 随机性打击, 就是网络节点以某种概率被随机破坏; 2) 选择性打击就是网络节点按一定的策略被破坏。一般网络自身原因引起的损伤属于随机性打击, 网络中每个节点发生故障的概率是相同的。而蓄意的破坏属于选择性打击, 网络中不同节点遭受攻击的概率不同, 网络中作用大的或脆弱的节点被入侵的概率要大。下面针对传感器网路面临的两种不同打击, 给出传感器网络抗毁性的两个新测度。

定义 3. 在无线传感器网路模型 $G=(V,E)$ 中, 在满足网络的有效覆盖率 $CR \geq CR^*$ 的条件下, 随机移除网络中的 $f(n)$ 个节点。若 $f(n)=f^*$ 时, 网络连通系数达到阈值 $C=K_C$, 称 $\frac{f^*}{n}$ 为网络的节点容错度。

定义 4. 在无线传感器网路模型 $G=(V,E)$ 中, 在满足网络的有效覆盖率 $CR \geq CR^*$ 的条件下, 选择性移除网络中的 $f(n)$ 个节点。若 $f(n)=f^*$ 时, 网络连通系数达到阈值 $C=K_C$, 称 $\frac{f^*}{n}$ 为网络的节点抗攻击度。

3 基于小世界模型的无线传感器网络抗毁性分析

3.1 构造具有小世界特性的无线传感器网络

假设无线传感器网络由 n 个节点组成, 随机分布在边长为 a 的正方形 A 中。本文对整个网络做如下的假设:

网络中只有一个汇聚节点, 处于网络站中任意位置。每个节点都知道其位置。节点和汇聚节点布置完后不发生移动。

网络中的所有节点同构, 具有相同的性能和传输半径。

节点信号传输满足对称性。

簇头对从簇成员收集到的数据可以进行数据融合。

假设每个簇里簇成员同时发送数据给簇头的概率为 p 。

网络生成后, 先利用算法 SMCA 对其进行分簇^[9], 然后长程联接^[10]。通过这两个步骤, 使无线传感器网络同时具有小世界的大的集聚系数和小的最短路径两个良好性质。

3.2 打击方式与分析

我们假设随机性打击均匀分布在网络中的所有节点上。选择性打击由攻击者按照一定的策略对网络中影响较大的节点进行有针对性的打击。在本文中, 我们按照 3 种策略进行打击: 1) 打击网络中的簇头节点; 2) 打击靠近 sink 节点的传感器节点, 但不包括长程联接的节点; 3) 打击靠近 sink 节点的传感器节点, 且包括长程联接的节点。

按照分簇算法 SMCA, 如果簇头节点失败, 该簇要重新选取剩余能量最大的节点为新的簇头节点。若簇头节点还未选取出, 节点数据就只能通过离 sink 节点较近的节点进行转发, 这样不仅会消耗更多的能量, 还会增大网络的平均最短路径, 因此打击簇头节点对网络性能具有较大的影响。

在 WSN 中, 靠近 sink 节点的传感器节点, 需要转发其他节点数据, 这些节点如果失败, 远处的节点数据无法传给 sink 节点将导致网络瓦解。因此, 关键是要均衡网络节点能量消耗, 构造具有小世界特性的 WSN 可以均衡整个网络的能量, 延长网络的生存周期。而网络之所以具有小世界特性其中一个重要的原因就是因为它添加了长程联接(加线)。

4 仿真与性能分析

在 VC++6.0 环境下进行仿真试验。采用前文介绍的网络模型, 仿真中在边长 $a=1500m$ 的正方形区域中随机布置 1000 个节点, 节点传输半径 $r=50m$, $p=0.5$, 有效覆盖率阈值取为 0.5。采用具有小世界特性的无线传感器网络模型^[10], 先用算法 SMCA 对网络进行分簇, 将各个簇内的节点数控制在 40 个以内, 平均跳数控制在 3 跳内, 再按加线 24 条。仿真时我们忽略信号冲突与外来干扰的影响。下面的每个结果都是 100 次随机生成网络拓扑的实验的平均值。

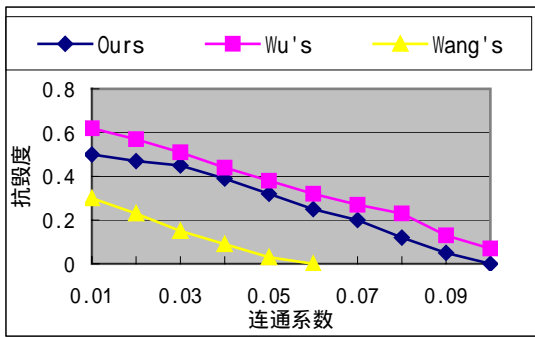


图 2 随机打击情况下抗毁性评价方法的比较

在节点遭受随机打击的情况下将我们的评估方法与文献[5]中吴和文献[8]中王的评估方法进行比较。如图 2 所示，用吴的评估方法网络有较好的抗毁度，而该评估方法采用的连通系数的最短路径是网络中任意两个节点之间的最短路径，在 WSN 中该方法不够客观。王的方法评估网络的抗毁度较差，按该方法超过百分之三十的节点受打击网络就瓦解，该评估方法是以网络最大连通分支的覆盖率来衡量可用性，而事实上只要连通分支中的节点可以将数据传递到 sink 节点仍是可用的，因此用该方法对于 WSN 过于严格，不符合实际。而本文的评估方法是从实际网络拓扑出发考虑，其网络抗毁性介于这两者之间。

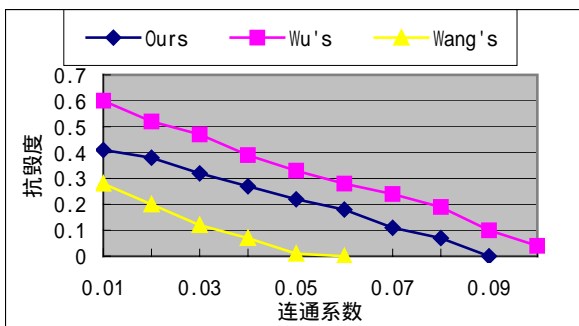


图 3 选择打击簇头节点情况下抗毁性评价方法的比较

接着，我们继续考查节点遭受选择性打击的情况。如图 3 所示，是网络选择打击簇头节点情况下(第 3.2 节中打击策略 1)，分别用这三种评估模型的评估情况。吴的方法与王的方法较随机性打击情况下网络的抗毁度变化不大，而从我们的评估方法可以看出网络的抗毁度明显下降，这是较符合客观实际的，因为打击簇头节点对网络性能具有较大的影响，会使其抗毁度下降。

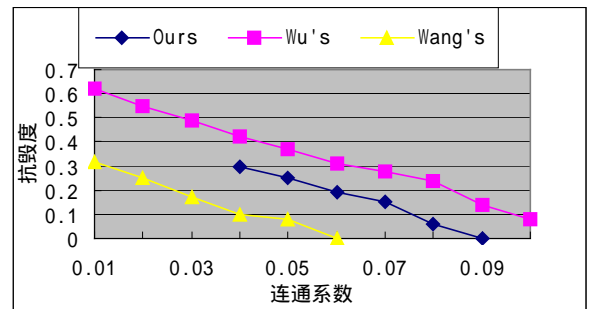


图 4 特定选择打击情况 1 下抗毁性评价方法的比较

图 4 是网络在特定选择打击情况 1(第 3.2 节中打击策略 2)的几种抗毁性评价方法的比较。根据 WSN 网络模型，如果 sink 节点附近的大量节点被打击则会造成远处的节点无法将数据传递至 sink 节点使网络瓦解。如图 4，本文的评估方法当网络中超过百分之三十的靠近 sink 节点的传感器节点被打击则其它节点无法将数据传递至 sink 节点网络瓦解，符合客观实际。但是用吴的方法和王的方法，网络在瓦解时仍有不错的抗毁度，与前面的几种打击比较变化不大。因此可以看出，对于 WSN，我们的评估方法更具客观准确性。

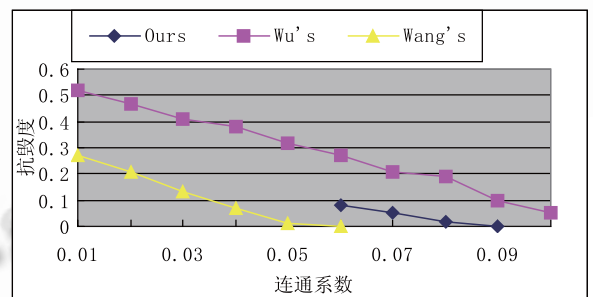


图 5 特定选择打击情况 2 下抗毁性评价方法的比较

图 5 是网络在特定选择打击情况 2(第 3.2 节中打击策略 3)下的几种抗毁性评价方法的比较。从吴和王的评估方法来看，网络的抗毁度只是稍微下降，但是从本文的评估方法来看，网络的抗毁性有显著的变化。这是因为如果 sink 节点附近的部分节点失败，远处的节点可以通过长程联接来传递数据，因此可以提高网络的抗毁性，但是当这些长程联接也被打击后，就会加快 sink 节点与网络中其它节点的分割，使得网络不可用相当于网络瓦解。用我们的评估方法可以更加客观准确的评估以数据为中心的无线传感器网络的抗毁性。

5 结论

本文在以数据为中心的 WSN 模型基础上研究基于小世界模型无线传感器网络的抗毁性。为了更精确、客观地度量网络结构的抗毁性我们提出了一种基于覆盖率与连通性测度的抗毁性评估模型：从特定的实际网络拓扑结构出发，给出了 WSN 连通性的一个新测度—连通系数，在此基础之上给出了抗毁性测度的新定义，针对面临的两种攻击，给出了 WSN 抗毁性的两个新测度 - 容错度和抗攻击度，并对基于小世界模型的无线传感器网络节点遭受打击的模式进行分析，最后，网络仿真平台 VC++6.0 做了实验，仿真表明我们的评估方法可以更加客观准确的评估以数据为中心的 WSN 抗毁度。

参考文献

- 1 Tilak S, Abu-Ghazaleh NB, Heinzelman W. A taxonomy of wireless micro-sensor network models. *Mobile Computing and Communications Review*, 2002, 1(2):1 - 8.
- 2 Akyildiz IF, Su W, Sankarasubramaniam Y, Cayirci E. Wireless sensor networks: A survey. *Computer Networks*, 2002,38(4):393 - 422.
- 3 Page LB, Perry JE. Reliability polynomials and link importance in networks. *IEEE Trans. on Reliability*, 1994, 43(1):51 - 58.
- 4 Wilkov R. Analysis and design of reliable computer networks. *IEEE Trans. on Communication*, 1972,20(3):660 - 678.
- 5 Wu J, Tan YJ. Study on measure of complex network invulnerability. *Journal of Systems Engineering*, 2005, 20(2):128 - 131.
- 6 肖伟峰,钟联炯.一种通信网络抗毁性评价方法. *西安工业学院学报*, 2002,22(4):292 - 296.
- 7 Crucitti P, Latora V, Marchiori M, Andrea Rapisarda. Error and attack to larence of complex networks. *Physica A*, 2004. 340,388 - 394.
- 8 王良民,马建峰,王超.无线传感器网络拓扑的容错度与容侵度. *电子学报*, 2006,34(8):1446 - 1451.
- 9 Ye XC, Xu L, Lin LW. Small world model based Clustering Division Scheme in Wireless Sensor Network. *International Conference on Communication and Mobile Computing*. Jan. 2009:87 - 91
- 10 Ye XC, Xu L, Lin LW. Small World Model based Topology Optimization in Wireless Sensor Network. *The International Symposium on Information Science and Engineering (ET)* 2008,12:1102-1106 <http://www.c-s-a.org.cn>