隐藏 Sink 位置的无线传感器网络寿命界①

戈 军[1], 周莲英[2]

[1](宿迁学院 计算机科学系, 宿迁 223800)
[2](江苏大学 计算机科学与通信工程学院, 镇江 212013)

摘 要: 攻击无线传感器网络(WSNs)的基站(sink)可能使整个网络无效. 因此, 某些情况下隐藏 sink 物理位置显得非常必要. 鉴于以往研究都是假定了一个弱对手模型. 通过线性规划(LP)框架, 提出了两种 sink 隐藏方法: 假 sink(FS)方法和平衡流量(BF)方法. 通过仿真实验, 分析并比较了两种方法对网络寿命的影响. 研究结果表明: (1)保护 sink 不可观测对网络寿命的影响相当大; (2)在大型网络中, BF 的网络寿命优于 FS.

关键词: 无线传感器网络; 线性规划; 能效; 网络寿命; 位置隐私; sink 位置

Lifetime Bounds of Wireless Sensor Networks Concealing Sink Location

GE Jun[1], ZHOU Lian-Ying[2]

[1](Department of Computer Science, Suqian College, Suqian 223800, China)
[2](College of Computer Science and Communication Engineering, Jiangsu University, Zhenjiang 212013, China)

Abstract: An attack to the base station (sink) in wireless sensor networks (WSNs) may make the entire network to be invalid, Therefore, it is very necessary to conceal the physical location of the sink in certain circumstances. In view of previous studies has all assumed a weak adversary model. Through a Linear Programming (LP) framework we present two different sink hiding methods: fake sinks (FS) method and balanced flows (BF) method. By simulation we analyzed and compared two methods with respect to their impact on network lifetime. Our results show: (1) The impact of preserving sink unobservability on network lifetime is considerable; (2) Network lifetime with BF is better than with FS in large networks.

Key words: wireless sensor networks; linear programming; energy efficiency; network lifetime; location privacy; sink location

WSN 是一种针对特定应用的网络, 与 WSN 节点 ID 信息关联不大; 相反, WSN 的节点位置信息往往起到标识作用, WSN 位置隐私具有特殊而关键地位. 传统意义上以 IP 地址为中心的隐私保护机制往往无法适应 WSN 的需要; 从而使得位置隐私保护成为 WSN 的迫切需求.

但单独密码方案还不足以防范位置隐私攻击. 传统技术(如加密)应结合混淆攻击者的虚拟流量方法. 就 WSN 而言, 这一问题可分为两大类: 源位置隐私和 sink 位置隐私.

为了使对手难以跳到跳逆向追踪到信源的位置, 文献[1]提出了定向贪心游走算法, 其具有较大的安全期; 针对基于位置的服务(LBS)中的多个节点在一个互不信任的分布式环境下合作计算时, 任何节点可能从其他节点处获取隐私信息及敏感数据, 文献[2]提出了一种新自适应隐私保护策略架构及执行模型; 针对已有源位置隐私保护协议所产生的幻像源节点集中在实际的源节点附近, 从而无法较好保护真实源节点的位置隐私, 文献[3]提出基于源节点有限洪泛的源位置隐私保护协(PUSBRF); 针对移动用户不断发出查询请求, 文献[4]提出了 MPA(移动模式攻击), 使得传统孤立查询的隐私保护算法均无效, 提出了熵匿名度度

① 基金项目:国家高技术研究发展计划(863)(2007AA04ZIB2);江苏宿迁市科技创新专项资助(S200109)
收稿时间:2012-03-30;收到修改稿时间:2012-05-04

量, 并以此为基础提出了移动环境下的模糊化算法 Mclique.

评估任何隐私增强技术的有效性, 首先, 需要对攻击者的能力有一个了解. 现实的威胁模型涉及到全局、被动及外部窃听者. 以前只研究过源位置隐私问题[5,6], 尚未真正研究过 sink 位置隐私保护问题. 基于 Sink 位置隐私保护, 本文给出了两种线性规划(LP) 框架下的 WSNs 寿命界方法. 为未来隐藏基站(sink)的协议设计提供了一定基础.

1 问题描述

1.1 LP 模型

模型中的每个 WSN 节点生成相同数据量, 并最大化其生成数据(D)的值. 假定所有节点具有相同数据生成率, 这也意味着网络寿命最大化. 当不隐藏 sink 位置(索引$i=1$)时, LP 问题的约束公式化为方程(1)-(3):

第(1)约束: 声明网络的所有流量非负(f_{ij} 表示从节点 i 到节点 j 的流量).

$$f_{ij} \ge 0 \tag{1}$$

第(2)约束: 制定流量平衡. 在 $N-1$ 传感器节点组成的网络和单基站(节点总数为 N), 每个传感器节点(不包括基站, $i \ne 1$), 传出流总量等于传入流和生成数据的总和.

$$\sum_j f_{ij} = \sum_j f_{ji} + D \quad for \quad i \in [2, N] \tag{2}$$

第(3)约束: 能量约束建模. 假定基站无能量约束, 每个节点都有相同有限能源(e_i)和两种消耗量(用于发送和接收的能量). 能量参数[7]: $E_{tx,ij} = \rho + \varepsilon d_{ij}^{\alpha}$ 和 $E_{rx} = \rho$ 分别代表一个比特的传输能量和接收能量($\rho = 50nJ$ 和 $\varepsilon = 100pJ$). 我们选择的路径损耗指数 α 为 4, 且不限制节点传输范围(d_{ij} 是节点 i 和节点 j 间距离).

$$\sum_j E_{tx,ij}\ f_{ij} + E_{rx} \sum_j f_{ji} \le e_i \quad for\ i \in [2, N] \tag{3}$$

方程(4)-(7)公式化假 sink(FS)问题(即, 包括真正基站的每个节点所生成的数据不仅到单 sink, 还要到每个其他节点). 因此, 网络中的每个节点起到一个 sink 作用. 真正 sink 照常处理接收数据, 假 sink 静默丢弃其数据. 我们假定无法监测基站与外界的通信. 方程(5)用于确保源自每个节点的流量到自己. 添加索引用来表示每个流量的最终目的地, 以及方程(6)所述的流量平衡约束. 我们还需要方程(7)平衡每个节点能耗(方程(12) 类似), 因为即使所有流量都均等, 能耗不平衡也可泄露 sink 位置 (请参阅下面的安全分析).

$$f_{ij}^{k} \ge 0 \tag{4}$$

$$f_{ij}^{k} = 0 \ for\ i = k \tag{5}$$

$$\sum_j f_{ij}^{k} = \sum f_{ji}^{k} + D \ for\ \forall i,k \quad i \ne k \tag{6}$$

$$\sum_k \sum_j E_{tx,ij} f_{ij}^{k} + E_{rx} \sum_k \sum_j f_{ji}^{k} \le e_i \ for \forall i,k\, i \ne k \tag{7}$$

方程(8)-(12)代表最后 LP 公式化. 本文的想法是不使用假 sink, 但要引入更加智能的网络虚拟流量. f 流量和 g 流量分别表示网络的真实和虚拟流量. 利用方程(9)的 f 流量公式化流量平衡约束. 方程(10)用于平衡总传出量, 方程(11)用于平衡所有节点的传入流量. 我们将平衡流量(BF)作为隐藏 sink 位置的第二种方法.

$$f_{ij} \ge 0, g_{ij} \ge 0 \tag{8}$$

$$\sum_j f_{ij} = \sum_j f_{ji} + D \ for\ i \in [2, N] \tag{9}$$

$$\sum_j (f_{ij} + g_{ij}) = \sum_j (f_{kj} + g_{kj}) \ for\ \forall i,k \tag{10}$$

$$\sum_j (f_{ji} + g_{ji}) = \sum_j (f_{jk} + g_{jk}) \ for\ \forall i,k \tag{11}$$

$$\sum_j E_{tx,ij} (f_{ij} + g_{ij}) + E_{rx} \sum_j (f_{ji} + g_{ji}) \le e_i \ for \forall i \tag{12}$$

1.2 安全分析

一般而言, WSNs 的 LP 模型用于获取节点间流量, 优化给定约束的线性目标函数. 这些模型没有任何分组调度约束. 因此, 在下面的安全分析中我们只考虑流量分配及相关现象.

本节表明, 如果采用 FS 或 BF 解决方案, 一个对手不能获得 sink 位置的任何有用信息, 即使他观察到所有流量. sink 不可观测有如下定义.

定义 1. 考虑一个拥有节点的 WSN. 设 sink 节点 A_i 的概率为 $P(A_i)$, o 表示对手的观测. 对于所有节点和观测, 系统具有 sink 不可观测的性质, 则有

$\forall i, \forall o, P(A_i) = P(A_i \mid o)$. 接下来, 我们概略地证明两种方法, 表明其都可实现 sink 不可观测.

定理 1. 如果采用 FS 或 BF, sink 不可观测的性质得以保持.

证明: 定义 1 的 $P(A_i) = P(A_i \mid o)$ 意味着, 是 sink 的概率独立于 o $(P(A_i \cap o) = P(o).P(A_i \mid o) = P(o).P(A_i))$. 为了证明该独立性, 我们应考虑不同类型的:

1) 流量上的 o, 在 FS 和 BF 解决方案中, 由于总传入量和每个节点的总传出量都独立于 sink, 通过观测流量获取不到信息. 对比所提出解决方案, 通过观测 sink 可以判断哪个节点拥有最高传入流量和/或节点没有传出流量.

2) 能耗上的 o: 由于所有节点花费相同能量, 能耗和 sink 间没有关联性. 因此, 收集不到 sink 信息.

3) 消息内容上的 o: 由于消息是加密的, 通过检查信息内容, 对手无法获得 sink 的任何有用信息.

因此, 即使对手拥有所有这些观测, 都不能获取任何 sink 位置信息. 因此, 根据定义 1, 实现了 sink 不可观测的性质.

2 仿真

我们只关注 sink 不可观测性, 不可观测程度和所提解决方案的效率之间的权衡有待以后研究. 我们解决了三种网络线性拓扑中的 LP 问题. 线性拓扑才是本文分析重点. 由于没有闭合 LP 问题的解决方案, 我们使用计算机程序包(GAMS[8])求解问题. 需要强调的是, 下面所有分析, 都是利用基准方案的网络寿命归一化寿命值. 注意, 无论使用哪种 LP 模型, WSN 寿命总是网络规模的一个单调递减函数.

仿真 1: 增量为 5, 网络节点数变化区间为 5-100, 节点间距离为 1m, 描述四种情况的归一化寿命值. 图 1 的仿真结果表明: 1)当真 sink 处于线性拓扑边缘, 隐藏 sink 位置对网络寿命的影响更严重. 这是由于基线方案寿命大于中央位置的 sink 寿命. 2)FS 解决方案可以看出: 一方面归一化寿命是网络规模的单调递减函数; 另一方面, 一旦达到网络规模的阈值, 随着网络规模的扩大, BF 解决方案的归一化寿命开始稳步提高. 因此, FS 解决方案不太适合大型网络. 3)与 FS 相比, BF 网络寿命量的提高不太依赖真 sink 位置.

仿真 2: 固定网络节点数量(50 个), 探讨节点间距离对网络寿命的影响, 当采用 BF 或 FS 解决方案(见图 2)时, 我们看到: 一方面, FS 归一化寿命无明显变化. 另一方面, 当节点间距离为 3 米时, BF 归一化寿命达到峰值(即 0.48). 因此, 当节点间距离为 3 米时, 实现了隐藏 sink 的网络寿命最低成本, 其平衡流量开销最小.

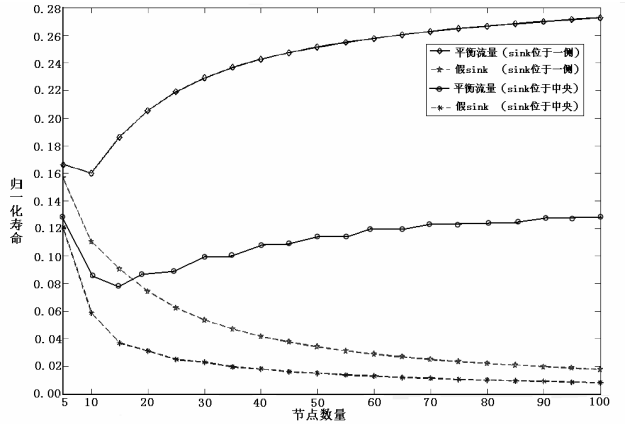

图 1　归一化寿命与节点数量关系曲线图

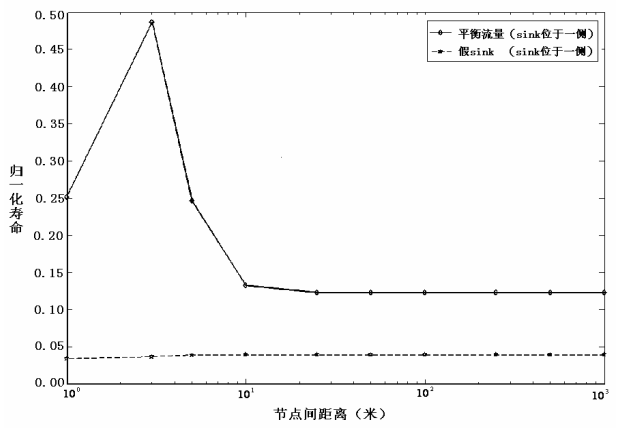

图 2　归一化寿命与节点间距离关系曲线图

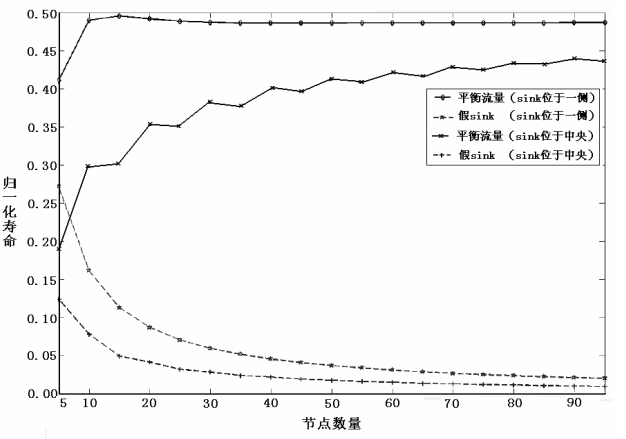

图 3　归一化寿命与节点数量关系曲线图

仿真 3: 当节点距离更改为 3 米(图 3)时, 我们重复仿真 1. 我们可以看到: 当 sink 位于线性拓扑一侧时, 维

持 0.48 左右的归一化寿命后网络规模达到阈值(即 10).

3 结论

定位技术是 WSN 必不可少的一项关键技术, 其提供的位置信息为事件监测或目标位置信息获取、路由协议、覆盖质量及其他相关研究起到关键性作用. 然而, 节点的定位信息一旦被非法滥用, 必将导致严重位置隐私问题.

但对于位置隐私问题的以往研究都是假设窃听者不能监控整个网络. 相对于良好协调、严重的攻击, 这个假设是无效的. 本文假定存在全局窃听者, 通过 LP 框架, 提出并形式化 FS 和 BF 这两种 sink 隐藏方法. 我们分析并比较了两种方法对网络寿命的影响. 研究结果表明: 保护 sink 不可观测对网络寿命的影响相当大. 同时也表明: BF 实现的网络寿命数量级高于大型网络的 FS.

参考文献

1 姚剑波.基于定向贪心游走的 WMSN 位置隐私.计算机应用与软件,2011,28(3):137−138,165.

2 刘昭斌,刘文芝,顾君忠.位置感知的自适应隐私保护策略.计算机工程与设计,2011,32(3):839−841,1032.

3 陈娟,方滨兴,殷丽华,等.传感器网络中基于源节点有限洪泛的源位置隐私保护协议.计算机学报,2010,33(9):1736−1747.

4 彭志宇,李善平.移动环境下 LBS 位置隐私保护.电子与信息学报,2011,33(5):1211−1216.

5 任丹丹,杜素果.一种基于攻击树的 VANET 位置隐私安全风险评估的新方法.计算机应用研究,2011,28(2):728−732.

6 Yang Y, Shao M, Zhu S, et a1. Towards event source unobservability with minimum network traffic in sensor networks. Proc. of the ACM Wisec'08, USA: Alexandria and VA,2008.77−88.

7 Cheng Z, Perillo M, Heinzelman W. General network lifetime and cost models for evaluating sensor network deployment strategies. IEEE Trans. on Mobile Computing, 2008,7(4): 484−497.

8 Brook A, Kendrick D, Meeraus A, et a1. GAMS: A User's Guide. The Scientific Press, 1998.

(上接第 211 页)

运行, 从而提高了网络的稳定性和可靠性. 该实现机制在大型企业网和运营商网络中具有广泛应用.

参考文献

1 孟华.互联网路由技术及发展前景展望.中国新技术新产品,2011,19(15):19−20.

2 王勐.核心路由器高可用性研究.信息与电脑,2011,23(9):151−152.

3 Coltun R, Ferguson D, Moy J. OSPF for IPv6. IETF RFC2740, 1999.

4 Moy J, Pillay-Esnault P, Lindem A. Graceful OSPF Restart. IETF RFC3623, 2003.

5 Pillay-Esnault P, Lindem A. OSPFv3 Graceful Restart. IETF RFC5187, 2008.

6 孙作聪,王立松,顾宝根.基于 OSPF 的温和重启的触发机制的研究与实现.计算机工程与技术,2006,27(14):2653− 2656.

7 张丹,商云飞,张显峰.基于 OSPF 协议的 Graceful Restart 技术的研究与实现.仪器仪表用户,2007,14(6):21−22.

(上接第 221 页)

用,2003,23(4):26−28.

3 Ratle A, Sebag M. Genetic Programming and Domain Knowledge: Beyond the Limitations of Grammar-Guided Machine Discovery. Parallel Problem Solving form Nature(PPSN 2000), Berlin: Springer, 2000,211−220.

4 朱彦廷.基于遗传算法的关联规则挖掘.西昌学院学报,2010,24(3):60−62.

5 KoZa, John R, Keane MA, Yu J, Bennett FH, Mydlowee W. Automatic creation of human-competitive programs and controllersby means of genetie programming. Genetlc Prograrnming and Evolvable Maehines, 2000,l(1-2):124−164.

6 徐哲,白焰.遗传编程.自动化仪表,2002,23(10):1−6.

7 徐扬,任庆生,戚飞虎.一个基于遗传编程的机器人足球系统.计算机仿真,2005,22(4):178−182.

8 江海燕.关于 GP 的研究与探索.山东教育学院学报,2007,1:96−100.