



基于垂线的WSN基站位置隐私保护算法

于吉喆,白乐强,曹科研

(沈阳建筑大学 信息与控制工程学院,沈阳 110168)

摘要:针对无线传感器网络基站位置隐私保护问题,提出一种基于垂线的基站位置隐私保护算法。根据源节点的位置与坐标轴上一点随机确定一条直线,过基站做直线的垂线,源节点关于该垂线对称的点为第1个预期幻影源节点,使第1个幻影源节点分布具有地理位置多样性。以第1个预期幻影源节点为垂足建立垂线,在该垂线上确定第2个预期幻影源节点,为第2个幻影源节点提供选择方向,2个幻影源节点不仅能够为数据包传输提供多样性,而且分别沿着直线和垂线传输假包,诱导攻击者向远离基站的方向追踪,增大攻击者捕获基站的难度。仿真结果表明,该算法能够有效地诱导攻击者偏离真实路径,提高安全周期。

关键词:无线传感器网络;基站位置隐私;垂线;幻影源节点;假包

开放科学(资源服务)标志码(OSID):



中文引用格式:于吉喆,白乐强,曹科研.基于垂线的WSN基站位置隐私保护算法[J].计算机工程,2021,47(8):170-176,182.

英文引用格式:YU J Z, BAI L Q, CAO K Y. Perpendicular-based algorithm for the protection of sink location privacy in WSN[J]. Computer Engineering, 2021, 47(8): 170-176, 182.

Perpendicular-Based Algorithm for the Protection of Sink Location Privacy in WSN

YU Jizhe, BAI Leqiang, CAO Keyan

(Information & Control Engineering Faculty, Shenyang Jianzhu University, Shenyang 110168, China)

[Abstract] For the protection of sink location privacy in Wireless Sensor Network (WSN), a perpendicular-based algorithm is proposed. A straight line is randomly established, which passes the location of the source node and a random point on the coordinate axis. Then a perpendicular of the straight line is made through the sink, and the symmetrical point of the source node about the perpendicular is the first expected phantom source node, which provides geographic distribution diversity for the first phantom source node. A perpendicular is established with the first expected phantom source node as the foot of a perpendicular. The second expected phantom source node is determined on this perpendicular, which provides direction for the selection of the second phantom source node. The two expected phantom source nodes provide directions for selecting two phantom source nodes. The two phantom source nodes provide diversity for the packet transmission path, and transmit fake packets along the straight line and the perpendicular respectively. So they mislead an adversary from the sink, increasing the difficulty for the attackers to capture the sink. The simulation results show that the algorithm can effectively mislead an adversary from the real path and improve the safe time.

[Key words] Wireless Sensor Network (WSN); sink location privacy; perpendicular; phantom source node; fake packet

DOI: 10.19678/j.issn.1000-3428.0059065

0 概述

物联网(Internet of Things, IoT)通过连接大量的物体进行接收和交换数据,在智能家居、工业制造、智慧城市等多个领域得到了广泛的应用^[1]。无线传感器网络(Wireless Sensor Network, WSN)由大量资源受限和供电受限的自组织传感器节点组成,是物

联网中数据监控和信息采集的基础组件。然而,近年来大量的研究表明,WSN中基站位置隐私的安全问题尚未得到有效的解决。基站作为整个网络中唯一接收数据信息的节点,如果位置暴露,将严重威胁整个网络的安全。因此,基站位置隐私保护成为近年来的研究热点。

在WSN中,针对基站位置隐私中的攻击者能力

基金项目:国家自然科学基金(61602323);中国博士后基金(2016M591455);辽宁省教育厅科学研究项目(lnqn201913)。

作者简介:于吉喆(1996—),男,硕士研究生,主研方向为隐私保护算法、无线传感器网络;白乐强,教授、博士;曹科研,副教授、博士。

收稿日期:2020-07-27 **修回日期:**2020-09-02 **E-mail:** yujizhe2019@outlook.com

不同,可将攻击者分为具有全局攻击能力和局部攻击能力的攻击者^[2]。在针对具有全局攻击能力的攻击者研究中,文献[3]最早考虑了WSN基站位置隐私的问题,并针对此问题提出了MPR路由、RW路由、FP和建立多个热点区域4种策略^[4],欺骗攻击者远离真实基站的位置,然而以上4种策略产生了额外的通信开销,缩减了WSN的生命周期。文献[5]提出一种基于分组调整发送速率的策略SRA,该策略通过控制数据包的传输速率,平衡了整个网络的通信流量,达到隐藏真实基站位置的目的。文献[6]提出SRCRR策略保护基站位置隐私,该策略网络中的数据包沿着直线路径传输,并存储在网络中的中间节点,基站则在给定的网络区域内以近似圆形的运动轨迹从本地节点收集存储的数据包,从而防止攻击者预测其位置,虽然该策略提高了数据包的收集效率,保护基站的位置隐私,但是数据包传输和基站移动过程产生了额外的能量消耗,缩短了网络寿命。文献[7]通过注入假包的策略统一分配通信流量,使攻击者难以发现基站的位置,但该策略消耗较高的能量,不利于延长网络的生命周期。

在针对具有局部攻击能力的攻击者研究中,文献[8]提出了基站位置隐私路由的新策略LPR,该策略针对局部攻击者的攻击特征,提出针对基站位置隐私的数据包逐跳追踪攻击者,为延长攻击者捕获基站的时间,网络中收到数据包的节点以一定的概率从远邻集随机选择一个节点作为下一跳,使数据包传输路径具有多样性,从而提升基站的安全周期。但是,数据包传输的方向总是朝向基站,不能有效地保护基站位置隐私。文献[9]在传统的单径路由的基础上通过注入假包和假基站的机制迷惑数据包逐跳追踪攻击者,使其偏离真实路径,从而延长攻击者捕获基站的时间。但是,真实路径为最短路径,产生的交叉节点距离基站较近,其传输的假包路径不能有效地隐藏基站的位置。文献[10]提出基于环的路由策略RBR,数据包通过最短路径传输至最近的路由环,然后通过路由线传输到其他的路由环,使攻击者难以定位到基站的准确位置。由于逐跳追踪攻击者在某种程度上能通过数据包的传输方向推断基站的位置,因此WANG等综合了LPR^[8]和YAO^[9]算法策略,提出了针对方向攻击者的基站位置隐私保护策略MRF^[11],该策略通过注入假包,诱导攻击者偏离真实路径。但是,随着源节点数量的增多,交叉节点和随机路径产生的假包路径也随之增多,由于假包路径距离基站较近,基站的位置容易暴露,因此不能有效地提高基站的安全周期。

在针对同时具有全局攻击能力和局部攻击能力的攻击者研究中,文献[12]提出MimiBS策略,该策略将WSN中的节点分为普通传感器节点、聚集节点

和基站节点,其中聚集节点形成热点区域,将攻击者诱导至该区域上,从而保护基站的位置。该策略的优点是安全性能根据TTL参数调整,缺点是会相应地增加延迟。上述策略虽然获得了较高的安全周期,但相应地增加了通信开销和能量消耗。为减少WSN的能量消耗,文献[13]建立了路径受限移动基站的网络流图模型,提高了网络能量利用率和数据收集的效率。

在当前抵御局部攻击者的基站位置隐私保护协议的研究中,真实数据包的传输方向总是朝向基站,中间节点的位置距离基站较近,其产生的假包路径不能有效地使攻击者偏离真实路径和隐藏基站的位置。为此,本文提出基于垂线的无线传感器网络基站位置隐私保护算法(ABP)。通过建立直线和垂线确定幻影源节点,不仅使其位置远离基站,而且保证其位置在网络中分布均匀,使其产生的真实路径不总是朝向基站传输,同时幻影源节点向目的节点传输假包,使数据包的传输路径具有多样性,增加攻击者捕获基站的难度,以达到保护基站的目的。

1 系统模型

1.1 网络模型

本文的网络模型与文献[14]提出的熊猫-猎人位置隐私保护模型相似。网络模型满足以下条件^[8,15]:

- 1)网络中均匀分布大量的传感器节点,每个传感器节点的计算能力和电池供电非常有限,传感器节点的通信半径为 r 。
- 2)网络中仅有1个基站节点,位于网络中心。基站负责网络初始化和收集网络中所有节点的数据信息。
- 3)无线传感器网络中传输的所有数据包都经过加密^[16],攻击者不具有内容隐私的攻击能力。

1.2 攻击模型

攻击者作为熊猫活动区域内具备局部无线监听能力的猎人,唯一的目的是捕获熊猫。本文对无线传感器网络的攻击模型作如下假设^[17]:

- 1)攻击者配备了先进的无线电设备,具有强大的计算和存储能力。
- 2)攻击者与传感器节点的通信半径相同。攻击者通过计算信号强度和方向估计发送节点的位置,并快速移动到发送节点的位置。
- 3)攻击者不具有窃取或篡改数据包内容、更改路由路径和破坏传感器节点的能力。

1.3 预期幻影源节点模型

以基站 B 为原点建立坐标系 XOY 。设随机选择的源节点 S 的坐标为 (x_s, y_s) 。当 $|x_s| > |y_s|$ 和 $|x_s| < |y_s|$ 时,源节点位于第1象限下,预期幻影源节点 P'_1 和 P'_2 的位置如图1和图2所示。

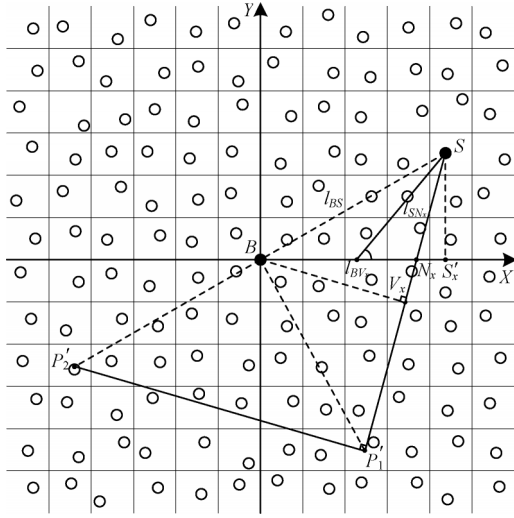
图1 $|x_s| > |y_s|$ 时的预期幻影源节点数学模型

Fig.1 Expected phantom source node mathematical model

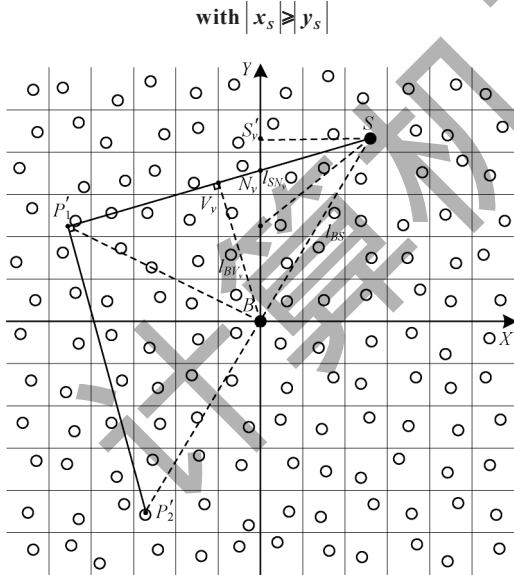
图2 $|x_s| < |y_s|$ 时的预期幻影源节点数学模型

Fig.2 Expected phantom source node mathematical model

with $|x_s| < |y_s|$

当 $|x_s| > |y_s|$ 时,源节点 S 位于第1象限,源节点 S 向 X 轴投影,确定一点 S'_x ,基站 B 和 S'_x 形成一条线段,源节点 S 在该线段的中点与 S'_x 形成的线段上随机选择一点 N_x ,连接 S 和 N_x 形成直线 l_{SN_x} ,直线与 X 轴夹角为 α ,过基站 B 做直线 l_{SN_x} 的投影 V_x , B 和 V_x 形成线段 l_{BV_x} , S 关于线段 l_{BV_x} 对称的点为预期幻影源节点 P'_1 ,预期幻影源节点 P'_1 的坐标为:

$$\left(\frac{(\tan^2 \alpha - 1)x_s - 2\tan \alpha y_s}{\tan \alpha \sqrt{1 + \tan^2 \alpha}}, \frac{(1 - \tan^2 \alpha)y_s - 2\tan \alpha x_s}{\tan \alpha \sqrt{1 + \tan^2 \alpha}} \right) \quad (1)$$

过预期幻影源节点 P'_1 做直线 l_{SN_x} 的垂线,垂线与 S 和基站 B 形成的直线 l_{BS} 交于一点 P'_2 ,可得预期幻影

源节点 P'_2 的坐标为:

$$\left(\frac{x_s y_s - \tan \alpha x_s^2}{y_s - \tan \alpha x_s}, \frac{y_s^2 - \tan \alpha x_s y_s}{y_s - \tan \alpha x_s} \right) \quad (2)$$

同理可求源节点 S 位于第2、3、4象限下对应的预期幻影源节点 P'_1 和 P'_2 的坐标。

当 $|x_s| < |y_s|$ 时,源节点 S 位于第1象限,源节点 S 向 Y 轴投影,确定一点 S'_y ,基站 B 和 S'_y 形成一条线段,源节点 S 在该线段的中点与 S'_y 形成的线段上随机选择一点 N_y ,连接 S 和 N_y 形成直线 l_{SN_y} ,直线与 Y 轴夹角为 β ,过基站 B 做直线 l_{SN_y} 的投影 V_y , B 和 V_y 形成线段 l_{BV_y} , S 关于线段 l_{BV_y} 对称的点为预期幻影源节点 P'_1 ,预期幻影源节点 P'_1 的坐标为:

$$\left(\frac{(\tan^2 \beta - 1)x_s - 2\tan \beta y_s}{\tan \beta \sqrt{1 + \tan^2 \beta}}, \frac{(1 - \tan^2 \beta)y_s - 2\tan \beta x_s}{\tan \beta \sqrt{1 + \tan^2 \beta}} \right) \quad (3)$$

过预期幻影源节点 P'_1 做直线 l_{SN_y} 的垂线,垂线与 S 和基站 B 形成的直线 l_{BS} 交于一点 P'_2 ,可得预期幻影源节点 P'_2 的坐标为:

$$\left(\frac{x_s y_s - \tan \beta x_s^2}{y_s - \tan \beta x_s}, \frac{y_s^2 - \tan \beta x_s y_s}{y_s - \tan \beta x_s} \right) \quad (4)$$

同理,可求源节点 S 位于第2、3、4象限下对应的预期幻影源节点 P'_1 和 P'_2 的坐标。

2 ABP 算法设计

2.1 ABP 算法描述

ABP 算法分为网络初始化阶段、基于直线的幻影路由阶段、幻影源节点 P_1 注入假包和基于垂线的幻影路由阶段、幻影源节点 P_2 注入假包和最短路径路由阶段。基站 B 进行网络初始化,每个节点得到相关信息,源节点 S 计算预期幻影源节点 P'_1 和 P'_2 的坐标,为实际确定幻影源节点 P_1 和 P_2 提供方向, S 沿着直线传输真包至 P_1 ,然后 P_1 沿着垂线传输真包至 P_2 ,最后 P_2 将真包沿着最短路径传输至 B ;同时收到真包的幻影源节点 P_1 和 P_2 分别沿着直线和垂线传输假包。

2.2 ABP 算法流程

2.2.1 网络初始化阶段

网络安全初始化阶段主要完成如下的任务:获取网络中的节点信息建立节点信息表,以及获取节点的邻居建立邻居表。节点的信息表中存放节点的ID、坐标、到基站的最小跳数 Hop。节点的邻居表中存放邻居节点的ID、坐标、到基站的最小跳数 sender_Hop。网络中任意节点通过定位算法获得自己的坐标^[18]基站 B 生成网络初始化信息包 Sink_Init^[19]在整个网络范围内广播。Sink_Init = {InformationType, sink_coordinate, sender_ID, sender_coordinate, hop},其中:InformationType 代表发送消息的消息类型;sink_coordinate 代表基站的坐标;sender_ID

代表发送节点的ID;sender_coordinate代表发送节点的坐标;hop代表发送节点到基站所经历的跳数,初始值为0。

设节点 Q 为网络中收到Sink_Init信息包的节点,其处理信息包的步骤如下:

步骤1 节点 Q 读取Sink_Init信息包,判断是否首次收到Sink_Init信息包,若首次收到,则在邻居表中存储sender_ID、sender_coordinate、sender_Hop,转步骤2,否则转步骤3。

步骤2 节点 Q 判断自己是否为基站,若是基站,则停止传输数据包,否则存储基站坐标,更新Hop=hop+1,转步骤4。

步骤3 节点 Q 查询sender_ID是否在邻居表中,若在邻居表中,则更新此邻居到基站的最小跳数sender_Hop=hop,否则在邻居表中存储sender_ID、sender_coordinate、sender_Hop。节点 Q 判断hop+1和Hop的大小,若Hop>hop+1,则更新Hop=hop+1,转步骤4,否则停止传输数据包。

步骤4 节点 Q 更新Sink_Init信息包中的sender_ID为节点 Q 的ID, sender_coordinate为节点 Q 的坐标, hop为Hop, 传输数据包。

2.2.2 基于直线的幻影路由阶段

如图3和图4所示, S 沿着直线 l_{SP_1} 向 P_1 传输数据包。设节点 Q 为收到数据包的节点, S 和 Q 处理数据包的步骤如下:

步骤1 S 计算 P_1' ,传输数据包至邻居节点中距离 P_1' 最近的节点。

步骤2 节点 Q 判断自身的通信半径范围内是否存在 P_1' ,若 P_1' 在节点 Q 的通信半径范围内,则停止传输数据包,节点 Q 视为幻影源节点 P_1 ,否则,节点 Q 搜索邻居表,计算每个邻居节点到 P_1' 的距离,传输数据包至邻居节点中距离 P_1' 最近的节点。

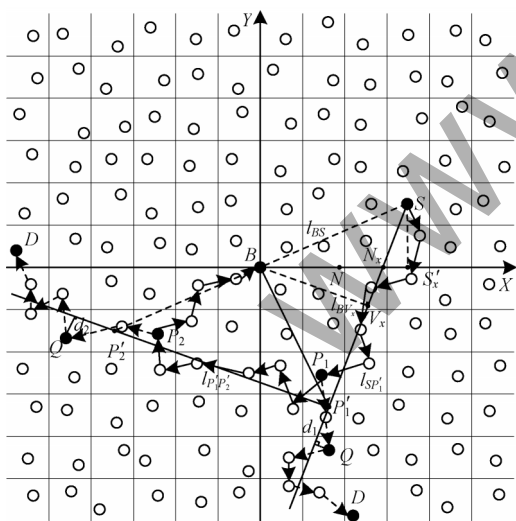


图3 $|x_s| \geq |y_s|$ 时的ABP算法示意图

Fig.3 ABP algorithm schematic with $|x_s| \geq |y_s|$

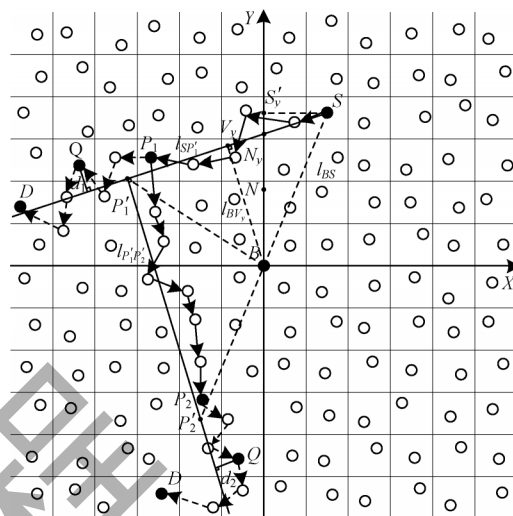


图4 $|x_s| < |y_s|$ 时的ABP算法示意图

Fig.4 ABP algorithm schematic with $|x_s| < |y_s|$

2.2.3 P_1 注入假包和基于垂线的幻影路由阶段

如图3和图4所示, P_1 沿着直线 l_{SP_1} 向目的节点 D 传输假包,同时 P_1 沿着垂线 $l_{P_1'P_2'}$ 向 P_2' 传输真包。设节点 Q 为收到数据包的节点, Q 的坐标为 (x_Q, y_Q) , S 的坐标为 (x_S, y_S) , 直线 l_{SP_1} 与 x 轴的夹角为

γ ($\gamma = \arctan \frac{y_S - y_N}{x_S - x_N}$), P_1 和 Q 处理数据包的步骤如下:

步骤1 P_1 向 P_2' 传输真包,同时传输生命周期TTL=5的假包。

步骤1.1 P_1 计算 P_2' ,传输数据包至邻居节点中距离 P_2' 最近的节点。

步骤1.2 P_1 沿着直线 l_{SP_1} 向邻居节点传输TTL=5的假包,直线方程如式(5)所示:

$$\tan \gamma X - Y - \tan \gamma x_S + y_S = 0 \quad (5)$$

步骤2 节点 Q 判断收到的数据包是否为真包,若为真包,则转步骤2.1,否则,转步骤2.2。

步骤2.1 节点 Q 判断自身的通信半径范围内是否存在 P_2' ,若 P_2' 在节点 Q 的通信半径范围内,则停止传输数据包,节点 Q 视为幻影源节点 P_2 ,否则,节点 Q 搜索邻居表,计算每个邻居节点到 P_2' 的距离,传输数据包至邻居节点中距离 P_2' 最近的节点。

步骤2.2 节点 Q 判断TTL是否为0,若收到TTL=0的假包,丢弃该假包,节点 Q 视为 D ;否则TTL-1,节点 Q 计算自身至直线 l_{SP_1} 的垂直距离 d_1 如式(6)所示,传输假包至邻居节点中 d_1 值最小的节点。

$$d_1 = \left| \frac{\tan \gamma x_Q - y_Q - \tan \gamma x_S + y_S}{\sqrt{\tan^2 \gamma + 1}} \right| \quad (6)$$

2.2.4 幻影源节点 P_2 注入假包和最短路径路由阶段

如图3和图4所示,幻影源节点 P_2 沿着垂线 $l_{P_1P_2}$ 向目的节点 D 传输假包,同时 P_2 沿着最短路径向基站 B 传输真包。设节点 Q 为收到数据包的节点, S 的坐标为 (x_s, y_s) , P_1 的坐标为 (x_1, y_1) , 直线 l_{SP_1} 与 x 轴的夹角为 γ ($\gamma = \arctan \frac{y_s - y_N}{x_s - x_N}$), P_2 和 Q 处理数据包的步骤如下:

步骤1 P_2 向 B 传输真包,同时传输生命周期 $TTL=5$ 的假包。

步骤1.1 P_2 传输真包至邻居节点中距离 B 最近的节点。

步骤1.2 P_2 沿着垂线 $l_{P_1P_2}$ 向邻居节点传输 $TTL=5$ 的假包,垂线方程如式(7)所示:

$$X + \tan \gamma Y - x_1 - \tan \gamma y_1 = 0 \quad (7)$$

步骤2 节点 Q 判断收到的数据包是否为真包,若为真包,则转步骤2.1,否则,转步骤2.2。

步骤2.1 节点 Q 判断自身是否为 B ,若是 B ,则停止传输数据包,否则 Q 传输真包至邻居节点中距离 B 最近的节点。

步骤2.2 Q 判断 TTL 是否为0,若收到 $TTL=0$ 的假包,丢弃该假包,节点 Q 视为 D ,否则 $TTL-1$,节点 Q 计算自身至垂线 $l_{P_1P_2}$ 的垂直距离 d_2 如式(8)所示,传输假包至邻居节点中 d_2 值最小的节点。

$$d_2 = \left| \frac{x_Q + \tan \gamma y_Q - x_1 - \tan \gamma y_1}{\sqrt{\tan^2 \gamma + 1}} \right| \quad (8)$$

3 理论分析

本文对传输时延进行理论分析,传输时延为真包从源节点传输至基站所移动的平均跳数。在节点均匀分布的大规模传感器网络中,数据包移动的跳数可用两点间的距离表示^[20]。本文的传输时延包括基于直线的幻影路由阶段、基于垂线的幻影路由阶段、最短路径路由阶段3个部分。如图5所示,建立坐标系 XOY ,以第1象限内的源节点,其横坐标的绝对值大于纵坐标的绝对值的情况为例分析平均传输时延,其他象限内由源节点传输数据包产生的平均传输时延同理。设基于直线的幻影路由阶段的平均传输时延为 D_{line} ,基于垂线的幻影路由阶段的平均传输时延为 D_{per} ,最短路径路由的传输时延为 $D_{shortest}$,总的平均传输时延为 D_{avg} ;源节点 S 的坐标为 (x_s, y_s) , S 关于直线 l_{BV_x} 为对称轴的对称点 P_1 的坐标为 (x_1, y_1) ,由垂线 $l_{P_1P_2}$ 和直线 l_{BS} 确定的预期幻影源节点 P_2 的坐标为 (x_2, y_2) ,且 P_1 和 P_2 的求解结果如式(1)~式(4)所示。

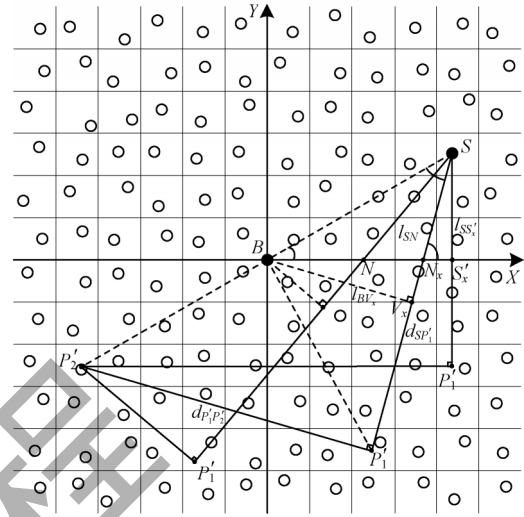


图5 S 向 B 传输数据包路径示意图

Fig.5 Schematic diagram of data packet transmission path from S to B

在基于直线的幻影路由阶段中,源节点 S 向预期幻影源节点 P_1 传输数据包,该阶段的传输时延如式(9)所示:

$$d_{SP_1} = 2 \frac{x_s + \tan \alpha y_s}{1 + \tan^2 \alpha} \sqrt{1 + \tan^2 \alpha} \quad (9)$$

其中: $\alpha \in \left[\arctan \left(\frac{2y_s}{x_s} \right), \frac{\pi}{2} \right]$, 当 $\alpha_{min} = \arctan \left(\frac{2y_s}{x_s} \right)$ 时,传输时延达到最大值 $2 \frac{x_s^2 + 2y_s^2}{\sqrt{x_s^2 + 4y_s^2}}$,即 S 沿着直线 l_{SN}

向 P_1 传输数据包;当 $\alpha_{max} = \frac{\pi}{2}$ 时, S 关于 x 轴对称,传输时延达到最小值为 $2y_s$,即 S 沿着直线 l_{SS_x} 传输数据包;在一般情况下, S 选择线段 l_{NS_x} 上一点 N_x ,沿着直线 l_{SN_x} 传输数据包,其平均传输时延如式(10)所示:

$$\int_{\alpha_{min}}^{\alpha_{max}} \frac{d_{SP_1}}{\alpha_{max} - \alpha_{min}} d\alpha \quad (10)$$

因此,基于直线的幻影路由阶段的平均传输时延 D_{line} 如式(11)所示:

$$D_{line} = 2y_s + \int_{\alpha_{min}}^{\alpha_{max}} \frac{d_{SP_1}}{\alpha_{max} - \alpha_{min}} d\alpha \quad (11)$$

在基于垂线的幻影路由阶段中, P_1 沿着垂线向 P_2 传输数据包,该阶段的传输时延如式(12)所示:

$$d_{P_1P_2} = d_{SP_1} \tan \beta \quad (12)$$

其中: $\beta = \alpha - \gamma$ ($\gamma = \arctan \frac{y_s}{x_s}$), 当 $\alpha_{max} = \frac{\pi}{2}$ 时,传输时延达到最大值 $d_{SP_1} \tan \left(\frac{\pi}{2} - \arctan \frac{y_s}{x_s} \right)$,即 S 沿着直线 l_{SS_x} 传输数据包;当 $\alpha_{min} = \arctan \left(\frac{2y_s}{x_s} \right)$ 时,传输时延到达

最小值 $d_{SP'_1} \tan \left(\arctan \frac{2y_s}{x_s} - \arctan \frac{y_s}{x_s} \right)$, 即 S 沿着直线 l_{SN} 传输数据包。因此, 基于垂线的幻影路由阶段的平均传输时延 D_{per} 如式(13)所示:

$$D_{per} = \int_{\alpha_{min}}^{\alpha_{max}} \frac{d_{SP'_1} \tan \left(\alpha - \arctan \left(\frac{y_s}{x_s} \right) \right)}{\alpha_{max} - \alpha_{min}} d\alpha \quad (13)$$

由图5可知, S 传输多条数据包路径, 都到达同一 P'_2 , 因此, 基于最短路径阶段的平均传输时延 $D_{shortest}$ 如式(14)所示:

$$D_{shortest} = \sqrt{x_2^2 + y_2^2} \quad (14)$$

由上述分析可得, ABP算法的平均传输时延 D_{avg} 如式(15)所示:

$$D_{avg} = D_{line} + D_{per} + D_{shortest} \quad (15)$$

4 仿真结果与分析

本文通过传输时延、安全周期和通信开销3个指标评估ABP算法的性能, 基于Matlab R2017b仿真平台, 对LPR算法^[8]、MRF算法^[11]和ABP算法进行仿真实验。为实现传感器节点均匀分布, 将6 000 m×6 000 m的区域均匀划分成100×100个大小相同的网格, 10 000个传感器节点初始位于各个网格中心。为模拟自然状态下传感器节点的随机分布情况, 给各个传感器节点加一个服从正太分布的随机扰动 $\varepsilon(\varepsilon \sim N(\mu, \sigma^2))$, 使传感器节点随机出现在网格中的任意位置, 基站位于网络的中心位置。源节点周期定义为源节点传输2个数据包的间隔时间^[8]。

4.1 传输时延

传输时延指在某一路由协议下真包从源节点传输至基站所移动的平均跳数。如图6所示, 随着源节点到基站跳数的不断增加, 3种算法的传输时延不断提高, 这是因为随着源节点距离基站跳数的不断增加, 源节点传输路径长度可能不断增大, 源节点到基站的平均路径长度也随之增大。在MRF算法中, 数据包的传输路径分为最短路径和随机路径。该算法主要的传输路径为最短路径, 由于随机路径短, 其传输方向总是朝向基站, 因此传输时延增长量小, 该算法的传输时延最低。在LPR算法中, 节点以一定的概率随机地将数据包向近邻集或远邻集传输, 其传输路径为随机路径, 相比最短路径增加了额外的传输时延, 因此该算法的传输时延略高于MRF算法。在ABP算法中, 首先源节点沿着直线将数据包传输至距离基站较远的地方, 该阶段提高了传输时延的增长量; 为了避免产生额外的传输延迟, 沿着垂线将数据包向基站方向传输; 最后通过最短路径传输至基站, 总体上增加了数据包的转发次数, 增加了传输时延, 因此该算法的传输时延略高于LPR算法

和MRF算法的传输时延。

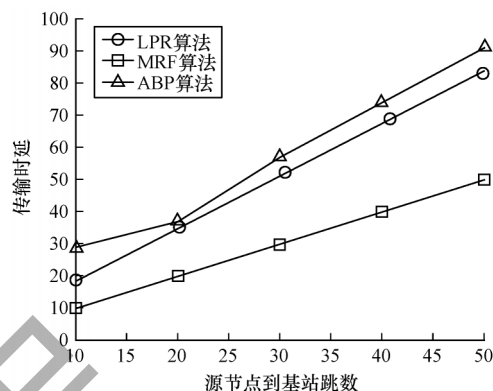


图6 传输时延示意图

Fig.6 Schematic diagram of transmission delay

4.2 安全周期

安全周期指基站被攻击者捕获之前收到数据包个数。如图7所示, 随着源节点数目的增多, 3种算法的安全周期不断下降。LPR算法由于没有假包注入, 且数据包传输方向总是朝向基站, 不能有效地保护基站位置隐私, 因此该算法的安全周期最低。MRF算法由于真实路径主要为最短路径, 攻击者很容易追踪到随机路径上, 该算法通过随机路径上产生的假包路径能够起到迷惑攻击者且保护基站位置隐私的作用, 但是随机路径短, 随着源节点数目的增多, 假包路径距离基站较近, 难以隐藏基站的位置, 因此MRF算法的安全周期明显高于LPR算法。与MRF算法相比, ABP算法进一步提高了安全周期, 主要有2点原因: (1) ABP算法有2个具有位置多样性的幻影源节点, 第1个幻影源节点距离基站较远, 能够保护基站位置隐私, 第2个幻影源节点为数据包向基站传输提供方向, 因此2个幻影源节点为数据包传输提供有向的随机路径; (2) 2个幻影源节点都注入假包, 产生的假包路径距离基站较远且能够有效地诱导攻击者偏离真实路径, 增大攻击者捕获基站的难度, 提高安全周期。

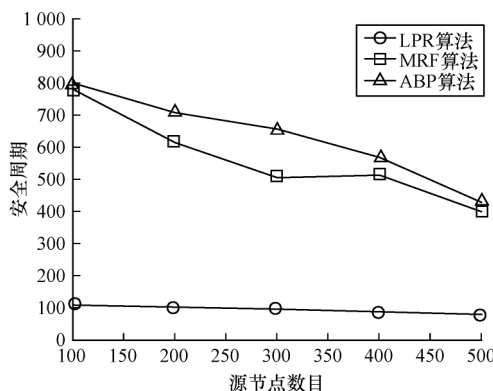


图7 安全周期示意图

Fig.7 Schematic diagram of safety cycle

4.3 通信开销

通信开销指传输数据包的总跳数。如图8所示,随着源节点数量的不断增加,3种算法的通信开销不断增大。在LPR算法中,由于没有假包注入,只有通过增加数据包传输路径长度的方式提高通信开销,因此该算法的通信开销最低。在ABP和MRF算法中都有假包注入,且MRF算法的通信开销略高于ABP算法,这是因为ABP算法的假包仅由幻影源节点 P_1 和 P_2 传输。然而,MRF算法中的假包由交叉节点和随机路由路径上的节点传输,其中交叉节点传输假基站上的假包至假基站,随机路径上的节点传输假包至目的节点,增加了额外的通信开销,因此MRF算法的通信开销略高于ABP算法的通信开销。

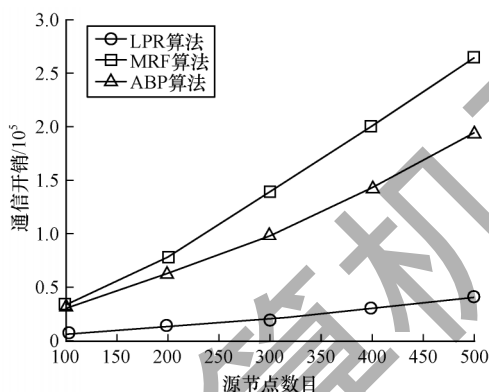


图8 通信开销示意图

Fig.8 Schematic diagram of communication overhead

5 结束语

本文针对无线传感器网络基站位置隐私保护问题,提出一种基于垂线的无线传感器网络基站位置隐私保护算法。通过在直线和垂线上随机确定2个均匀分布的幻影源节点,为真实数据包传输路径提供多样性,2个幻影源节点分别沿着直线和垂线传输假包,诱导攻击者偏离真实路径,隐藏基站的真实位置。理论分析与仿真结果表明,该算法不仅能够使攻击者朝远离基站的方向追踪,而且同时能使数据包传输路径具有多样性,虽然增加了部分传输时延,但总体上提高了安全周期,减少了通信开销,达到了保护基站位置隐私的目的。本文仅针对具有逐跳追踪数据包攻击能力的攻击者,下一步将针对具有全局攻击能力的流量分析攻击者,通过在网络中设置假基站节点,实现网络中聚集节点数据传输流量的均衡,提升基站位置隐私的保护强度。

参考文献

[1] QIU T, QIAO R X, WU D P. EABS: an event-aware backpressure scheduling scheme for emergency internet of things[J]. IEEE Transactions on Mobile Computing, 2017, 17(1): 1-14.

- [2] JIANG J F, HAN G J, WANG H, et al. A survey on location privacy protection in wireless sensor networks[J]. Journal of Network and Computer Applications, 2019, 125: 93-114.
- [3] DENG J, HAN R, MISHRA S. Intrusion tolerance and anti-traffic analysis strategies for wireless sensor networks[C]// Proceedings of 2004 International Conference on Dependable Systems and Networks. Florence, Italy: [s. n.], 2004: 508-520.
- [4] DENG J, HAN R, MISHRA S. Decorrelating wireless sensor network traffic to inhibit traffic analysis attacks[J]. Pervasive and Mobile Computing, 2005, 2(2): 159-186.
- [5] CHEN J, LIN Z, LIU Y, et al. Sink location protection protocols based on packet sending rate adjustment[J]. International Journal of Distributed Sensor Networks, 2016, 12(1): 1-10.
- [6] LIU A F, LIU X, TANG Z P, et al. Preserving smart sink-location privacy with delay guaranteed routing scheme for WSN[J]. ACM Transactions on Embedded Computing Systems, 2017, 16(3): 1-25.
- [7] BAROUTIS N, YOUNIS M. Load-conscious maximization of base-station location privacy in wireless sensor networks[J]. Computer Networks, 2017, 124: 126-139.
- [8] YING J, CHEN S, ZHANG Z, et al. A novel scheme for protecting receiver's location privacy in wireless sensor networks[J]. IEEE Transactions on Wireless Communications, 2008, 7(10): 3769-3779.
- [9] YAO L, KANG L, SHANG P F, et al. Protecting the sink location privacy in wireless sensor networks[J]. Personal and Ubiquitous Computing, 2013, 17(5): 883-893.
- [10] LONG J, LIU A F, DONG M X, et al. An energy-efficient and sink-location privacy enhanced scheme for WSN through ring based routing[J]. Journal of Parallel and Distributed Computing, 2015, 81: 47-65.
- [11] WANG J, WANG F Y, CAO Z Z, et al. Sink location privacy protection under direction attack in wireless sensor networks[J]. Wireless Networks, 2017, 23(2): 579-591.
- [12] BANGASH Y A, ZENG L F, FENG D. MimiBS: mimicking base-station to provide location privacy protection in wireless sensor networks[J]. Journal of Computer Science and Technology, 2017, 32(5): 991-1007.
- [13] KUMAR N, DASH D. Flow based efficient data gathering in wireless sensor network using path-constrained mobile sink[J]. Journal of Ambient Intelligence and Humanized Computing, 2020, 11(3): 1163-1175.
- [14] HAN G J, ZHOU L N, WANG H, et al. A source location protection protocol based on dynamic routing in WSNs for the social Internet of Things[J]. Future Generation Computer Systems, 2018, 82: 689-697.
- [15] MUTALEMWA L C, SHIN S. Secure routing protocols for source node privacy protection in multi-hop communication wireless networks[J]. Sensors, 2020, 13(2): 1-30.

(下转第182页)

(上接第 176 页)

- [16] 周倩,秦小麟,丁有伟. 基于攻击感知的能量高效源位置隐私保护算法[J]. 通信学报,2018,39(1):101-116.
ZHOU Q, QIN X L, DING Y W. Preserving source-location privacy efficiently based on attack-perceiving in wireless sensor network[J]. Journal on Communications, 2018, 39(1):101-116. (in Chinese)
- [17] MUTALEMWA L C, SHIN S. Achieving source location privacy protection in monitoring wireless sensor networks through proxy node routing[J]. Sensors, 2019, 19(5):1-19.
- [18] 冯秀芳,吕淑芳. 基于RSSI和分步粒子群算法的无线传感器网络定位算法[J]. 控制与决策,2014,29(11):1966-1972.
FENG X F, LÜ S F. Wireless sensor networks location algorithm based on RSSI and split-step particle swarm optimization algorithm[J]. Control and Decision, 2014, 29(11):1966-1972. (in Chinese)
- [19] 刘敬坡,刘朝晖,丁琳. 基于距离和节点能量的源位置隐私保护方案[J]. 计算机技术与发展,2020,30(2):121-126,120.
LIU J P, LIU Z H, DING L. A source-location privacy protection scheme based on distance and node energy[J]. Computer Technology and Development, 2020, 30(2):121-126, 120. (in Chinese)
- [20] 张鹏,马小南. 基于路由协议的无线传感器网络源位置隐私保护探究[J]. 湘潭大学自然科学学报,2014,36(1):110-114.
ZHANG P, MA X N. Research of the networks source location privacy protection of wireless sensor based on routing Protocols[J]. Natural Science Journal of Xiangtan University, 2014, 36(1):110-114. (in Chinese)

编辑 索书志