doi:10.11835/j.issn.1000-582X.2018.03.012

无线传感器网络中源位置隐私保护方法

汪卫星[1,2],李培真[3]

(1.钦州学院 电子信息工程学院,广西 钦州 535011;2.南京大学 软件学院,南京 210093;
3.重庆邮电大学 软件学院,重庆 400065)

摘要:随着物联网的迅猛发展,位置隐私被认为是传感器网络中一个重要的安全问题。传统的加密方法不能有效地防止攻击者通过逆向追踪的方式来找到监测物体的位置。针对这些问题并考虑到攻击者具有较强的可视能力,本文提出了一种基于区域和兄弟节点选择的位置隐私保护策略(PRABNS, phantom routing based on area and brother neighbor selecting)。该策略能够使幻影节点均匀分布在源节点周围,并通过对部分区域的选择来使相邻数据包间隔一定的角度,选择兄弟节点来增加源节点到基站路径的多样性。仿真结果表明,该策略能提供更好地隐私保护性,在不增加太多能耗的前提下延长了安全时间。

关键词:物联网;位置隐私;无线传感器网络

中图分类号:TP212.9　　**文献标志码**:A　　**文章编号**:1000-582X(2018)03-100-09

A privacy protection method of source location in wireless sensor networks

WANG Weixing[1,2], *LI Peizhen*[3]

(1. School of Electronics and Information Engineering, Qinzhou University, Qinzhou 535011, Guangxi, P.R.China; 2. Software Institue, Nanjing University, Nanjing 210093, P.R.China; 3. College of Software Engineering, Chongqing University of Posts and Telecommunications, Chongqing 400065, P.R.China)

Abstract: With the rapid development of the Internet of Things, the location privacy is considered as an important security issue in sensor networks. Traditional encryption methods cannot effectively prevent attackers finding the position of monitoring object by reverse tracing. To solve these problems and considering attackers have enhanced visibility, we propose a location privacy protection strategy called PRABNS (phantom routing based on area and brother neighbor selecting). The strategy can make the phantom nodes evenly distributed around the source node, and the adjacent data packet have a certain angle space through the selection of partial region, and thus it can increase the diversity for the path of source node to the base station by selecting sibling nodes. The simulation results show that the strategy can provide better privacy preservation, and extend the secure time without increasing too much energy consumption.

Keywords: Internet of Things; location privacy; wireless sensor networks

收稿日期:2017-12-15

作者简介:汪卫星(1974—),男,教授,博士,主要从事云制造、网络安全和大数据方面的研究,(E-mail)wwx_ylq@126.com。

随着物联网的兴起，无线传感网络（WSNs，wireless sensor networks）作为物联网的重要组成部分，被广泛应用于国防军事、工农业生产、智慧城市和环境监测等领域[1-5]。WSNs 一般由大量低成本的微型传感器节点自组织构成，具有有限的存储能力、计算能力和能量供给[6-7]。WSNs 通常部署在无人值守的开放区域，常用于监测珍贵资源或散布于战场中获取士兵的实时信息，距离监测目标最近的节点成为源节点，将采集到的数据通过多跳的方式发送到基站[8]。其无线传输特性使攻击者更容易监听、获取和篡改网络中的敏感信息。因此，即使攻击者不能获取加密后数据包的内容，也能够逆向、逐跳追踪到真实的数据源节点。数据信息的安全性可以通过内容加密和匿名来保证，而节点的通信模式和地理位置等背景信息仍然会暴露给攻击者。由于传感器网络中源节点位置隐私的暴露不可避免地威胁所监测目标的安全性，因此，数据源节点的位置隐私保护是一项亟待解决的问题。这些安全隐私问题已成为制约 WSNs 部署应用的关键问题。根据攻击者能力的不同，将源位置隐私保护协议主要分为两类：抵御全局流量攻击者的源位置隐私保护协议和抵御局部流量攻击者的源位置隐私保护协议。对于前者，攻击者只能监测小范围网络的情况，并不适用于大规模的传感器网络。现有的研究工作主要通过最短路径将数据包从幻影节点转发到基站，路由路径较为单一，容易造成路径上的重合。因此，文中针对第二种攻击者提出基于区域与多节点选择的幻影路由协议（PRAMS，phantom routing based on area and multi-node selection）。该协议能使选择的幻影节点保持一定的角度和距离，够好地均匀分布在源节点周围，同时通过多节点选择使路由路径多样化，大大降低重合路径产生的可能性。考虑到具有更强视觉能力的攻击者，该协议通过屏蔽可视区节点的路由选择，减少了不必要的泛洪，并在检测目标离开后对节点状态进行恢复。仿真结果表明该协议能提供更好的安全性能，并且消耗较少的能量。

1　相关工作

传统的 WSNs 安全保护方案主要涉及传感器网络的密码与密钥管理、安全数据融合、安全定位、安全路由等方面，这些方案不能为源位置隐私提供安全保障。文献[9]首次提出了幻影路由协议，该协议采用泛洪的方式会大大增加通信开销和能量消耗，并且完全随机行走的幻影路由协议产生的幻象节点不能很好地远离数据源节点。文献[10]基于熊猫猎人模型提出了一种基于区域或跳数的定向随机步协议。该协议主要思想是网络中的每个节点根据邻居节点距离基站的跳数，将跳数大于自己的放到集合$\{S_{\max}\}$，小于自己的放到$\{S_{\min}\}$，每次源节点发送数据包时，随机选择 s_0 或者 s_1 中节点作为前 h 跳的转发节点。这种方法能够使数据包的发送每次都远离基站或者靠近基站。然而，该策略产生的幻像源节点集中于某些区域，不具备很好的分散性。文献[11]提出了基于位置角度的幻影路由协议（PRLA，a source location privacy protocol in WSN based on locational angle），首次提出了可视区的概念，一旦攻击者和源节点的距离小于目测距离就认为源位置暴露。PRLA 协议根据邻居节点的偏移夹角的大小确定转发概率，并根据转发概率选择下一跳转发节点，从而尽可能地避开攻击者可视区，减少失效路径，但不能完全避免损耗路径的产生。文献[12]提出了基于源节点的增强型有限洪泛源位置隐私保护协议（EPUSBRF，a source-location privacy preservation protocol in wireless sensor networks using source-based restricted flooding），在源节点 h 跳有限洪泛阶段实现了对可视区内节点的标记，源节点 h 跳有限泛洪结束后，基站进行避开可视区的全网广播，在最短路径路由阶段，数据包总是沿着避开可视区的最短路径转发至基站。然而，一旦检测目标移动到了新的位置，该协议将进行多次全网泛洪，从而大大增加了网络能耗，同时数据包从幻影节点都是沿最短路径传输到基站，由于每个节点到基站的距离固定，增加了攻击者快速追踪源节点的可能性。文献[13]提出了一种基于幻影单径路由的源位置隐私保护策略（PSRMPN，strategy of source-location privacy preservation in WSNs based on phantom single-path routing），该策略增加了 h 跳有限泛洪阶段的跳数范围，增加了幻影节点的数量。但该策略最大跳数值较为固定，并通过增加最小跳数值来延长幻影节点到源节点的距离，能够降低幻影节点数量并提高了网络能耗与延时，并且与文献[12]一样，PSRMPN 通过最短路径将数据包从幻影节点发送到基站。文献[14]提出用周期采集和源模拟的方法来保护源位置隐私，但该方法会产生巨大的能量开销，实时性较低。

2 系统模型

2.1 网络模型

研究的网络模型与熊猫-猎人博弈模型相似。一个大规模同构的无线传感器网络部署在一大片监测区域中,传感器节点随机均匀分布在监测目标区域内。一旦发现监测物体,距离物体最近的节点会将监测结果以数据包的形式周期性地发送给基站,直到攻击者发现目标或者监测目标离开监测区域。笔者对整个网络做了如下假设:

1)网络是连通的,即网络中任意2个节点都可以通过多跳传输进行通信;

2)网络中只有一个基站,在同一时间只有一个被监测目标,目标具有移动性,每隔一定时间后会离开监测区域,最近的节点监测目标息后自动成为数据源节点,并且将信息以数据包的形式发送到基站;

3)网络中的每个节点都有一个唯一的标识ID,并且每个节点都知道自己的位置信息,记为($N_i.x$,$N_i.y$)。

2.2 攻击者模型

攻击者的目标是通过逆向追踪路由路径,直到找到数据源节点。假定攻击者具有下面几个特点:

1)攻击者具有足够大的存储空间和强大的计算能力。攻击者能够快速检测出发送节点并移动至节点位置;

2)攻击者在基站附近进行数据包监听,并且通过监听到的数据包确定下一跳节点的位置;攻击者只有局部流量分析的能力,其监听范围与传感器的通信范围相当;

3)数据内容是安全的,攻击者无法获取数据包中的加密信息。

3 解决方案

研究提出的PRABNS路由协议主要分为3个阶段:有限洪泛阶段、有向路由阶段和多节点选择转发路由阶段。以上3个步骤中,有限泛洪减阶段少了不必要的泛洪,节约了节点能量,降低了源节点被发现的概率;有向路由和多节点路由选择增加了攻击者逆向追踪的难度并延长了安全时间,有效保护了节点的位置隐私。表1说明了使用参数含义。

表1 文中的参数对照表

Table 1 Parameter comparison table

i, j	感知节点
h_w	局部泛洪的跳数
h_x	有向路由的跳数
r	传感器节点通信半径
s	源节点
b	基站
$h_{i,j}$	节点i与j之间的最小跳数
P_i	幻象节点
H	源节点到基站的最小跳数
i.neighbor	邻节点集合
i.parent	父节点集合
i.brother	兄弟节点集合
$i.s\_child$	基于源节点的子节点集合

3.1　网络初始化

在网络初始化阶段，每个节点都要获取邻居节点的位置信息以及自身到基站的最小跳数信息。在该阶段结束后，每个节点 i 存储有源节点有限洪泛跳数值 h_w、可视区半径 r、自身和邻居节点到基站的最小跳数值和邻居节点的位置坐标。在节点部署前，每个节点 i 预载入源节点有限洪泛跳数值 h_w 和可视区半径 r。之后，基站向全网广播泛洪信息 Sink_Msg，其中包括消息类型、节点 ID、节点位置坐标和距离基站的跳数信息 h_b，其初始值为 0。当节点接收到此消息后将 h_b 加 1，如果节点首次收到该消息或跳数信息比自身存储的信息更小时，更新跳数信息 h_i，$b=h_b$ 和邻节点信息，然后继续转发该消息，否则只记录邻节点信息并将消息抛弃。每个节点根据距离基站的最小跳数值将邻节点分为 3 个集合：i.parent、i.brother、i.child。全局泛洪算法如表 2 所示。

表 2　全局泛洪算法

Table 2　Global flooding algorithm

Algorithm 1 全局泛洪算法
1：　**case** 全局泛洪：
2：　　**if**（节点 i 第一次收到消息）**then**
3：　　记录消息中包含的信息并进行广播；
4：　　**else** 记录消息中包含的信息，然后丢弃。
5：　　网络中的每个节点可以将其邻节点划分为 2 个集合。

3.2　有限洪泛

源节点 h_w 跳有限洪泛是 h_x 跳有向路由的基础，本协议中 $h_w=h_{max}$，h_{max} 为幻影节点到源节点的最大跳数。在源节点有限洪泛结束之后，距离源节点 h_w 跳内的每个节点 i 得到自身及邻节点距离源节点的最小跳数值和角度。如图 1 所示，角度是源节点到幻影节点和源节点到基站间直线的夹角。通过与源节点跳数的比较得到集合 $i.s\_child$，$i.s_child$中的节点距离源节点的最小跳数值大于节点 i 距离源节点的最小跳数。

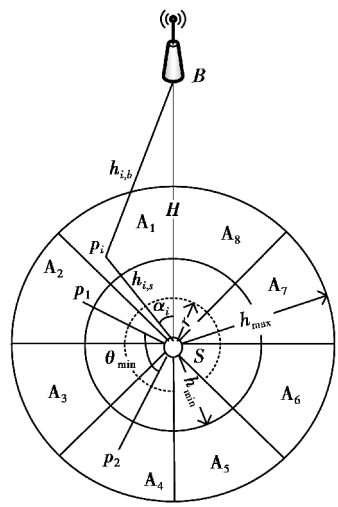

图 1　区域划分

Fig.1　Region division

α_i 将由公式(1)计算得到

$$\alpha_i=\arccos\frac{H^2+h_{i,s}^2-h_{i,b}^2}{2\times H\times h_{i,s}^2}。\tag{1}$$

当监测到目标在附近区域时，数据源节点向其 h_w 跳范围内的节点广播消息 Source_Msg，其过程与全网泛洪过程类似。其中包括消息类型、节点号 ID、角度 α_i，h_s 表示消息的跳数计数，初始为 0。在消息到达每个转发节点时加 1，计数到 h_w，则节点不再广播该消息。当节点 i 接收到广播消息时，记录下消息中 α_i 的值，并根据公式(1)计算出自身的角度 α_i 的值，然后转发给邻节点。若接收到的消息中 $h_s\leqslant r$，则根据消息中的 ID 号在集合 i.parent 中查找该节点信息。如果在 i.parent 中找到该节点，则对该节点进行标记。所有在 i.parent 中标记的节点在多节点选择转发阶段都不能被选择为下一跳转发节点，因此可视区内的节点就被可视区外的节点屏蔽了。若被监测物体离开源节点的监控范围，源节点发送跳数为 $r+1$ 的广播消息，节点接收到消息后在 i.parent 中取消对消息发送节点的标记。

3.3 有向路由

在有限泛洪结束后，将源节点周围的区域分成 n 份，n 为偶数，每份的角度为 $\theta=2\pi/n$，分别定义这些区域为 $A_1,A_2,A_3,\cdots,A_n,A_1$ 与 A_n 相邻。源节点在发送数据包时选择一个区域 A_i，并根据当前所选区域决定下一个发送区域的选择范围，其选择区域的个数为

$$m=\begin{cases}\dfrac{n}{2}, & \dfrac{n}{2}\text{ is an old number},\\ \dfrac{n}{2}+1, & \dfrac{n}{2}\text{ is an even number}。\end{cases}\tag{2}$$

当前区域与选择区域的间隔数 $k=\dfrac{n-m+1}{2}$，最小间隔角度为 $\Delta\beta=(k+1)\times\theta$，发送区域的选择范围是 $\{A_{i+k},A_{i+k+1},A_{i+k+2},\cdots,A_{i+k+m-1}\}$。若源节点第一次发送数据包，则从 n 个区域中随机选择一个作为发送区域。源节点发送的数据包中包含有转发跳数 h_x 和角度范围 $[(i-1)\theta,i\theta]$，h_x 服从 $[h_{\min},h_{\max}]$ 随机分布。若节点 i 接收到一个数据包，则 i 从 $i.s\_child$ 中随机选取一个节点，且该节点的角度 α 在数据包的角度范围中，然后将数据包转发给该节点。重复此过程，直到数据包被转发 h 次。如图 1 所示，源节点周围区域被分成了 8 份，最小间隔角度为 $\pi/2$，A_2 为当前区域，则下一个数据包发送区域的选择范围是 $\{A_4,A_5,\cdots,A_8\}$。由公式(3)可以得到，当 n 趋于无穷大时，最小间隔角度 $\Delta\theta_{\min}=\dfrac{\pi}{2}$。

$$\lim_{n\to\infty}\left(\frac{\frac{n}{2}+\alpha}{2}\right)\cdot\frac{2\pi}{n}=\frac{\pi}{2},\alpha\in\{0,1\}。\tag{3}$$

从选择区域选择下一跳数据包的发送区域能保证相邻数据包发送间隔角度最小为 $\pi/2$。这使得相邻数据包产生的幻影节点相隔一定的距离，增加了攻击者逆向追踪的难度并延长了安全时间。局部泛洪算法、有向路由算法、兄弟路由选择算法见表 3～表 5。

表 3 局部泛洪算法

Table 3 Limited flooding algorithm

Algorithm 2 局部泛洪算法
case 局部泛洪：
if ($h_s<=h_w$)
if (节点 i 第一次收到消息) **then**
记录邻节点信息；
$h_s=h_s+1$；
计算角度 α_i；
广播修改后的消息；
else 记录邻节点信息并丢弃该消息；
if ($h_s<=r$) **then**
搜索集合 i.parent 中的邻节点信息；
if (找到邻节点) **then**
在路由列表中标记邻节点；
else 停止泛洪；
随机游走区域中的每个节点可以得到一个集合 i.child。

表 4　有向路由算法

Table 4　Brother selecting routing algorithm

Algorithm 3 有向路由算法
case 有向路由:
从可选区域中选择发送区域;
随机数 $h_s \subseteq [\mathrm{hop}_{\min}, \cdots, \mathrm{hop}_{\max}]$;
if ($h_{i,s} < h_x$) **then**
if (i.child$\neq\varnothing$) **then**
从角度范围内的 i.child 中选择一个邻节点作为下一个节点并发送消息;
else 通过兄弟选择路由算法将消息发送到接收器。

表 5　兄弟路由选择算法

Table 5　Brother selecting routing algorithm

Algorithm 4 兄弟路由选择算法
case 兄弟路由:
从集合 i.parent 和 i.brother 中选择一个节点 i;
if (node $i \in i$,brother) **then**
if ($h_1 \neq 0$) **then**
if (equal==1) **then**
检查向量是否满足公式(4);
if (向量不能满足公式(4)) **then**
选择另一个节点;
else 设置等于 1 并向节点 i 发送消息;
else 发送消息到节点 i;
else 从集合 i.parent 和 i.brother 中选择另一个节点。

3.4　多节点选择转发

在有向路由转发完成后进入多节点选择转发路由阶段。接收到数据包的节点 i 从 i.parent 和 i.brother 2 个集合的节点中随机选择一个作为下一跳转发节点。转发的数据包中包含等距离节点标记字段 equal 和跳数限制值 h_1。每当下一跳节点是从 i.brother 集合中选择的则将 equal 置为 1,h_1的值减 1,当 h_1为 0 后就只从 i.parent 中选择节点,使数据包快速到达基站。数据包过多地通过等距离节点进行转发而增加了网络时延和能量开销。本协议通过从 i.brother 集合中选择节点扩大了节点转发路径的范围,减小了重合路径产生的可能性,同时延长了安全时间。如图 2 所示,节点间的震荡就是节点在选择等距离节点时选择了数据包的发送节点及周围节点。为了能防止在选择 i.brother 中节点是产生节点间震荡,本协议通过公式(4)决定数据包的发送方向,

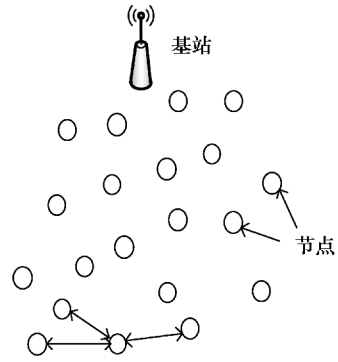

图 2　数据包在节点间震荡

Fig.2　Packet Shock Between Nodes

$$\boldsymbol{a} \cdot \boldsymbol{b} > 0。 \tag{4}$$

假设接收数据包的节点为节点 i,发送数据包的节点为节点 j,在 i.brother 中数据包的转发节点为节点

$\boldsymbol{k}$。$\boldsymbol{a}=(N_i.x-N_j.x, N_i.y-N_j.y)$为节点 j 的坐标与节点 i 的坐标形成的向量，$\boldsymbol{b}=(N_k.x-N_i.x, N_k.y-N_i.y)$为节点 k 的坐标与节点 i 的坐标形成的向量。若 equal 的值为1，则从 i.brother 中选择节点后计算向量是否满足公式(4)，如果不满足则重新选择下一跳转发节点。

4 实验验证

研究提出的策略将在 OMNeT++上进行仿真并和 EPUSBRF 和 PSRMPN 策略进行比较。为了方便比较各策略的性能，设计了以下仿真场景。

假设有 10 000 个节点均匀分布在 6 000 m×6 000 m 的区域中。每个节点的通信半径是 100 m。平均每个节点的邻节点数是 8.64。少量节点的邻节点个数为 3。攻击者的监听半径与节点通信半径相当。可视区的半径时 600 m。限制跳数 h_l 为 10，有限泛洪跳数 h_w 属于集合{10，20，30，40，50}。有向路由跳数 h_x 服从[h_w-3，h_w+3]均匀分布。对每一个参数均进行 50 次仿真。

4.1 安全时间

安全时间被用来评估策略的隐私保护性能，被定义为攻击者找到源节点时源节点发送的数据包个数。图 3 和图 4 展示了在源节点距离基站为 60 跳时，不同有向行走跳数所带来的安全时间。结果表明安全时间随着有向行走跳数的增加而增加，这是因为幻影节点到基站的距离越来越长，传输路径变得更为复杂，攻击者需要更多时间来找到源节点位置。同时，也产生了数量更多的幻影节点，能减少重合路径产生的可能性。如图 3 所示，PRABNS 的安全时间平均比其他 2 个策略增加了 34.7%和 21.7%。这是因为 PRABNS 能使幻影节点更为均匀地分布在源节点周围，使相邻产生的幻影节点保持一定的距离，通过对兄弟节点的选择使路径更为多样。如图 4 所示，这些策略的安全时间随 H 的升高而升高，这是因为路由路径随着 H 的升高变长了，攻击者需要更多的时间进行追踪。PRABNS 比其他 2 个策略在安全时间上平均提升了 58.6%和 36.8%。因此该策略能提供更好的安全性。

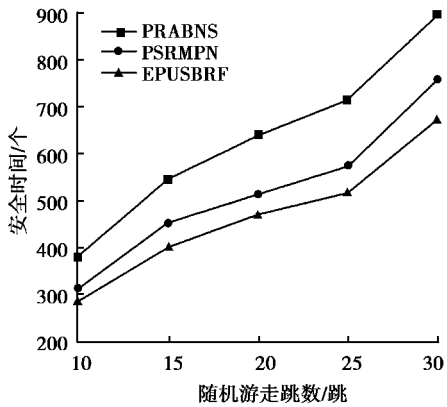

图 3 不同随机游走跳数的安全时间

Fig.3 The safe time of different random walk hops

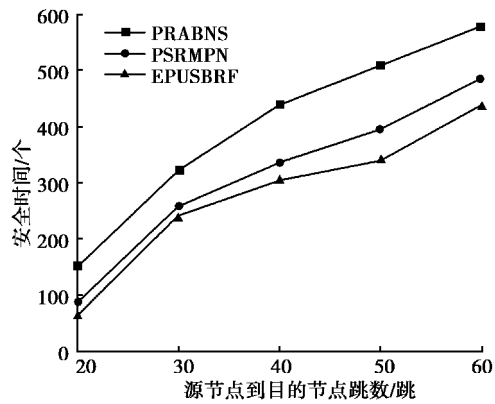

图 4 不同源节点到目的节点跳数的安全时间

Fig.4 The safe time of jumping from different source nodes to destination nodes

4.2 能量消耗

能耗被定义为数据包从源节点到基站被转发的跳数。图 5 和图 6 展示了不同 H 和 h_w 下的能耗情况。能耗随着 H 和 h_w 的增加而增加，这是因为路由路径随着这 2 个参数的增加变得更长。PRABNS 在 $H=60$、$h_w=25$ 时，能耗增加了 9.6%和 13%，因为兄弟节点的选择增加了部分能耗开销，但以此得到了更长的安全时间。

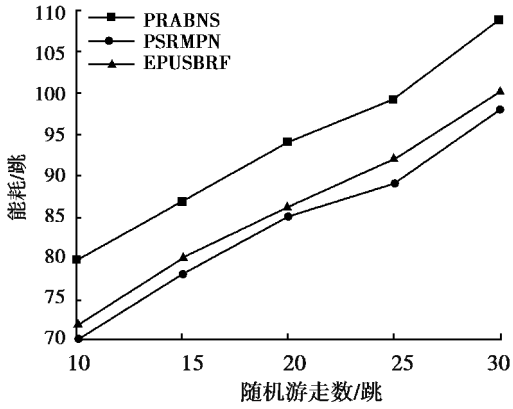

图 5　不同随机游走跳数的能量消耗

Fig.5　Energy consumption of different random walk hops

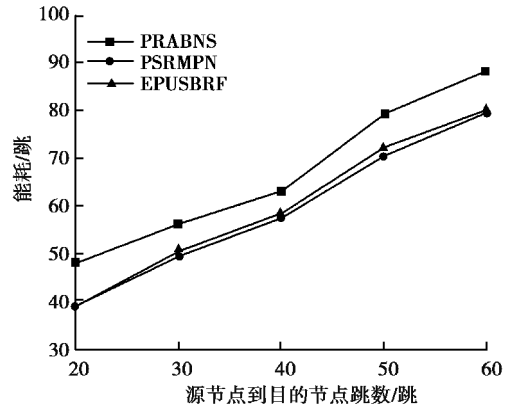

图 6　不同源节点到目的节点跳数的能量消耗

Fig.6　Energy consumption of hops from different source nodes to destination nodes

4.3　全局泛洪能耗

在全局泛洪阶段广播消息的总数和不同位置源节点的数量之比被定义为全局洪泛的能耗。如图 7 所示,EPUSBRF 的全局泛洪能耗比 PRABNS 策略要高出许多,这是因为在 EPUSBRF 中每有一个新的源节点发送消息时都会进行一次全局洪泛,而在 PRABNS 中只进行一次。因此在 EPUSBRF 中的全局泛洪能耗是一直不变的,在 PRABNS 中随着源节点的增多该能耗逐渐趋向于 0。这表明了 PRABNS 节省了巨大的能量开销。

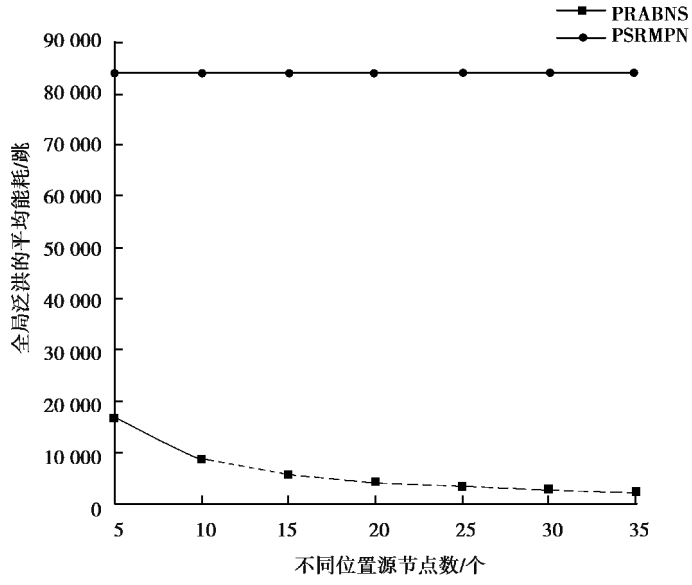

图 7　全局泛洪的平均能量消耗

Fig.7　Average energy consumption of global flooding

5　总　结

笔者研究了在无线传感器网络中的源位置隐私保护方法。考虑到攻击者具有更强的视觉能力,提出了基于区域和兄弟节点选择的幻影路由策略。该策略通过有向路由和多节点选择转发,增加了攻击者对源节点逆向追逐的难度,延长了源节点的安全时间,有效地保护了源节点的位置隐私性;有限泛洪减少了源节点

不必要的泛洪消息，节约了节点的能源，并且降低了源节点被追踪到的概率。总体来说，该策略有效地保护了源节点的额、位置隐私。

参考文献：

[1] Akyildiz I F, Su W, Sankarasubramaniam Y, et al. Wireless sensor networks: a survey[J]. Computer networks, 2002, 38(4): 393-422.

[2] Akkaya K, Younis M. A survey on routing protocols for wireless sensor networks[J]. Ad hoc networks, 2005, 3(3): 325-349.

[3] Potdar V, Sharif A, Chang E. Wireless sensor networks: a survey[C]// International Conference on Advanced Information NETWORKING and Applications Workshops.[S.l]: IEEE, 2009: 636-641.

[4] Frey H, Rührup S, Stojmenovič I. Routing in Wireless Sensor Networks[C]// International Conference on Multimedia Computing and Systems. [S.l]: IEEE Xplore, 2015: 495-500.

[5] Doavi A. Security in wireless sensor networks[J]. Communications of the Acm, 2015, 47(6): 53-57

[6] Dong K N, Hur J. Using a dynamic backbone for efficient data delivery in solar-powered wsns[J]. Journal of Network and Computer Applications, 2012, 35(4): 1277-1284.

[7] Zhi A E, Tan H P, Seah W K G. Design and performance analysis of mac schemes for wireless sensor networks powered by ambient energy harvesting[J]. Ad Hoc Networks, 2011, 9(3): 300-323.

[8] Chen X Q, Makki K, Yen K. Sensor network security: a survey[J]. IEEE Communications Surveys & Tutorials, 2009, 11(2): 52-73.

[9] Ozturk C, Zhang Y, Trappe W. Source-location privacy in energy-constrained sensor network routing[C]// ACM Workshop on Security of Ad Hoc and Sensor Networks. [S.l]: ACM, 2004: 88-93.

[10] Kamat P, Zhang Y, Trappe W, et al. Enhancing source-location privacy in sensor network routing[C]// IEEE International Conference on Distributed Computing Systems, ICDCS 2005.[S.l]: IEEE, 2005: 599-608.

[11] Wang W P, Chen L, Wang J X. A source location privacy protocol in WSN based on locational angle[C]// IEEE International Conference on Communications. Washington: IEEE Computer Society, 2008: 1630-1634.

[12] Chen J, Fang B X, Yin L H, et al. A source-location privacy preservation protocol in wireless sensor networks using source-based restricted flooding[J]. Chinese Journal of Computers, 2010, 33: 1736-1747.

[13] Tao Z L, Liu Y B, Li C X. Strategy of source-location privacy preservation in WSNs based on phantom single-path routing[J]. Journal of Chongqing University of Posts and Telecommunications, 2013, 25(2): 178-183.

[14] Mehta K, Liu D G, Wright M. Location privacy in sensor networks against a global eavesdropper[C]// International Conference on Network Protocols. [S.l]: IEEE Xplore, 2007: 314-323.

（编辑 詹燕平）