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

陈 娟[1] 方滨兴[1),2)] 殷丽华[2)] 苏 申[1)]

[1)](哈尔滨工业大学计算机网络与信息安全技术研究中心 哈尔滨 150001)

[2)](中国科学院计算技术研究所 北京 100190)

摘 要 无线传感器网络广泛应用于目标监测,攻击者能够通过逆向、逐跳追踪数据包的方式定位数据源节点,因此,需要对数据源节点的位置隐私进行保护.已有的源位置隐私保护协议产生的幻像源节点集中在真实的源节点附近,不能够较好地保护真实源节点的位置隐私.为此,文中提出基于源节点有限洪泛的源位置隐私保护协议PUSBRF.考虑到具有更强视觉能力的攻击者,文中进一步提出 EPUSBRF 协议.实验表明,与已有的源位置隐私保护协议相比,文中提出的两种协议显著提高了源位置隐私的安全性,平均安全时间提高将近一倍.

关键词 无线传感器网络;物联网;源位置;隐私保护;安全

中图法分类号 TP393 **DOI 号**: 10.3724/SP.J.1016.2010.01736

A Source-Location Privacy Preservation Protocol in Wireless Sensor Networks Using Source-Based Restricted Flooding

CHEN Juan[1)] FANG Bin-Xing[1),2)] YIN Li-Hua[2)] SU Shen[1)]

[1)](*Research Center of Computer Network and Information Security Technology*, *Harbin Institute of Technology*, *Harbin* 150001)

[2)](*Institute of Computing Technology*, *Chinese Academy of Sciences*, *Beijing* 100190)

Abstract Wireless sensor networks are widely deployed to monitor valuable objects. Attackers can find out the source node by hop-by-hop backtracking strategy. So, we need provide source anonymity for sensor networks. This paper examines that the phantom source nodes generated by the existing source location privacy preservation protocols are near the real source. So they can not protect the real source node well. As such, this paper proposes a protocol called PUSBRF (Source Location Privacy Preservation Protocol in Wireless Sensor Network Using Source-Based Restricted Flooding). And based on PUSBRF, it proposes another protocol called EPUSBRF (Enhancement Source Location Privacy Preservation Protocol in Wireless Sensor Network Using Source-Based Restricted Flooding) under the consideration of an attacker with enhancement visual ability. Simulation results show that compared to the existing protocols, the new protocols provide strong source location privacy preservation and the average safety period is increased by nearly one order of magnitude.

Keywords wireless sensor networks; Internet of Things; source-location; privacy preservation; security

收稿日期:2010-04-26;最终修改稿收到日期:2010-08-02.本课题得到国家"九七三"重点基础研究发展规划项目基金(2005CB321806,2007CB311100)、国家"八六三"高技术研究发展计划项目基金(2007AA01Z446)资助.**陈 娟**,女,1982 年生,博士研究生,主要研究方向为无线网络安全、隐私保护.E-mail:janechen123456@gmail.com.**方滨兴**,男,1960 年生,教授,博士生导师,中国工程院院士,主要研究领域为计算机体系结构、信息安全和计算机网络等.**殷丽华**,女,1973 年生,博士后,主要研究方向为信息安全、安全性评估等.**苏 申**,男,1985 年生,硕士研究生,主要研究方向为无线网络安全、隐私保护.

1 引　言

无线传感器网络作为物联网的重要组成部分,广泛应用于社会生活和战争环境.与有线网络相比,依赖于无线通信的传感器网络更容易受到各种安全威胁,例如节点受害、路由毁坏以及错误数据注入等[1-3].在基于事件驱动的无线传感器网络中,距离监测目标最近的节点作为数据源节点,它将搜集到的信息以数据包的方式逐跳地发送给基站[4].然而,共享的无线传输媒介使得敌方很容易定位数据包的发送者.因此,敌方虽然不能获取加密后数据包的内容,却能够逆向、逐跳追踪到真实的数据源节点(简称源节点),进而捕获数据包.无线传感器网络的一类很重要的应用就是监测有价值的人员或物体.例如,传感器节点布置于野外监测珍贵的动物或者散布于战场中得到军队的实时信息.在对这些物体或人员的监测过程中,要在获取有效信息的前提下保护目标的安全.文献[5]首次提出传感器网络源位置隐私保护问题,文献[6] 基于此提出熊猫-猎人博弈模型,在该模型中,大量传感器节点布置于野外环境中监测熊猫的生活习性.一旦监测到熊猫的行为,距离熊猫位置最近的传感器节点会将观测的结果发送给基站.位于基站处的猎人能够通过逆向、逐跳追踪数据包定位数据源节点并将熊猫捕获.在该模型中,源位置隐私保护技术就是在保证数据包能够发送给基站的前提下,尽力阻止猎人定位源节点的位置.

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.然而,由于传感器节点的通信能力、计算能力和存储能力均受限,因此,安全和性能的兼顾成为一个必然的要求.已有研究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[5-8]和抵御局部流量攻击者的源位置隐私保护协议[9-11].前者,攻击者只能对覆盖区域较小的传感器网络进行全局流量分析,不适用于监测区域广阔的传感器网络.对于后者,将数据包的路由过程分为两个阶段:第 1 个阶段,数据包从源节点经过 h 跳路由到达一个幻像源节点;第 2 个阶段,数据包从幻像源节点通过洪泛或最短路径路由到达基站.第 1 阶段的路由过程是为了产生远离真实源节点且地理位置多样性的幻像源节点,使得敌方难以追踪到真实的源节点.第 2 阶段是为了将数据包路由至基站.已有的研究工作[5-6,8]主要以邻节点距离基站的最小跳数进行下一跳节点的选择.然而,本文理论证明,在第 1 阶段的路由过程中,该选择策略所产生的幻像源节点集中于某些区域.为此,本文提出一种基于源节点有限洪泛的源位置隐私保护协议(PUSBRF).该协议不仅保证前 h 跳的每一跳均朝着远离真实源节点的方向进行,同时保证幻像源节点具有地理位置的多样性,理论分析和实验表明,该协议有效提高了源位置隐私的安全性.此外,考虑具有更强视觉能力的攻击者[7],本文引入可视区的概念即距离真实源节点 r 跳内的节点集合,进一步提出一种基于源节点有限洪泛的增强性源位置隐私保护协议(EPUSBRF).该协议在源节点有限洪泛过程中标记出可视区的节点,同时,通过避开可视区的广播策略,使得数据包在最短路径路由过程能够完全逃离可视区.该协议在不增加计算开销的前提下,避免失效路径[7]的产生,显著提高了源位置隐私的安全性.

本文的主要贡献如下:

(1)当前抵御局部流量攻击的源位置隐私保护协议,以邻节点距离基站的最小跳数进行下一跳节点的选择,在 h 跳有向路由后,产生的幻像源节点集中于某些区域[6,8].因此,产生的幻像路径也集中于某些区域.本文对此进行理论分析和证明.基于此问题,本文提出 PUSBRF 协议,该协议不仅保证幻像源节点尽可能地远离真实源节点,同时保证幻像源节点具有地理位置多样性.理论分析表明,与经典的源位置隐私保护路由协议 phantom single-path 相比,该协议产生的随机有向路径数至少增加了 33.33%.实验表明,与已有的源位置隐私保护路由协议相比,该协议显著提高了源位置隐私的安全性,平均安全时间提高了将近一倍.

(2)考虑具有更强视觉能力的攻击者,本文进一步提出 EPUSBRF 协议.该协议在源节点有限洪泛过程中标记出可视区的节点,同时,采用避开可视区的基站广播策略.理论分析表明在不增加计算开销的前提下,该协议首次避免了失效路径的产生.实验表明,该协议在 PUSBRF 协议的基础上,更进一步提高了源位置隐私的安全性.

本文第 2 节简要回顾无线传感器网络源位置隐私保护的相关工作,并分析当前已有研究工作的不足;第 3 节给出问题定义,包括本文协议基于的网络模型、攻击模型;第 4 节给出本文提出的 PUSBRF 协议的细节描述;第 5 节介绍 EPUSBRF 协议;第 6

节理论分析 PUSBRF 协议和 EPUSBRF 协议的通信开销和安全性能;第 7 节是实验对比和分析;最后是总结.

2 相关工作

目前,无线传感器网络安全问题的研究工作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、安全路由等许多方面,但是,对隐私保护尤其是位置隐私保护的研究较少[12].虽然在其它的研究领域,诸如数据挖掘[13-17]、无线社会网络[18-20]等领域,开展了一些相关的研究工作,但是这些研究工作由于没有考虑无线传感器网络数据传输的特点,因此不能很好地应用于无线传感器网络.

已有的研究工作根据攻击者的能力主要分为两类:抵御全局流量攻击者的源位置隐私保护协议[9-11]和抵御局部流量攻击者的源位置隐私保护协议[5-8].为了抵御具有全局流量监测能力的攻击者,文献[9]提出 ConstRate 策略:无论是否接收到真实的数据包,全网所有节点均以恒定的速率发送数据包.该方案非常有效地抵御了全局流量分析攻击,却引入了较多的伪数据包且导致真实数据包的传输时延较大.文献[10]在此基础上提出基于代理的过滤策略,某些作为代理的传感器节点能够过滤掉伪数据包,从而减少网络流量.之后,文献[11]提出 FitProbRate 策略,该策略通过控制节点发送数据包的速率,在增强源位置隐私安全性的同时降低了包传输延迟.然而,文献[9-11]具有一定的局限性,不能被广泛应用.首先,所有节点均发送大量的伪数据包,不仅会大大消耗节点的能量,也会增加包冲突的概率,降低数据包的传输效率.其次,用于监测野外环境和战地的传感器网络大多覆盖面积广泛,例如四川卧龙保护区的面积就有将近 200 万平方千米.显然,攻击者很难对如此巨大的传感器网络进行全局流量监控.因此,本文考虑在大规模传感器网络环境下,具有局部流量监测能力的攻击者.

对于具有局部流量监测能力的攻击者,Ozturk 等人[5]首次提出了一种源位置隐私保护协议即幻像路由协议.该协议分为两个阶段:第 1 阶段,每个数据包从源节点随机路由 h 跳后到达一个幻像源节点;第 2 阶段,数据包从幻像源节点通过洪泛或最短路径路由到达基站.为了使得真实的源节点难以被敌方追踪到,幻像源节点应当尽可能远离真实的源节点.然而,理论分析表明:经过纯粹随机 h 跳后,幻像源节点距离真实源节点不超过 $h/5$ 跳的概率是 $p=1-e^{-h/25}$,不难发现,当 h 足够大时,p 值趋近 1.为了保证幻像源节点距离真实的源节点足够远,文献[6,8]提出有向随机路由协议.在该协议中,每个节点 u 根据其邻节点距离基站的跳数大小,将其邻节点分为两个集合:父节点集和子节点集.前者中的节点距离基站的最小跳数值小于 u 距离基站的最小跳数值.后者中的节点距离基站的最小跳数值大于 u 距离基站的最小跳数值.当源节点 s 产生并发送一个数据包时,s 从父节点集或子节点集中选定一个集合,若选择了父节点集,则该数据包的 h 跳转发均从当前节点的父节点集中选择下一跳的转发节点.这就保证了前 h 跳的每一跳均朝着远离或者靠近基站的方向进行.然而,文献[5-6,8]中的策略产生的幻像源节点集中于某些区域,不具很好的分散性,因此,不能产生地理位置多样性的幻像路由.

引理 1. 节点 u 距离基站的最小跳数与其邻节点距离基站的最小跳数之差的绝对值小于或等于 1.

证明. 根据文献[5-8]的基站广播策略,对于 $\forall v\in u.neighbor$,有 $Hop_{v,u}=1$.其中,$u.neighbor$ 为节点 u 的邻节点集合即 u 通信半径内的节点集合,$Hop_{v,u}$ 为节点 v 与节点 u 间的最小跳数.当 $Hop_{u,b}=Hop_{v,b}$ 时,显然 $Hop_{v,b}-Hop_{u,b}\leq 1$,其中,$Hop_{u,b}$ 表示节点 u 与基站 b 间的最小跳数,$Hop_{v,b}$ 表示节点 v 与基站 b 间的最小跳数.若 $Hop_{u,b}>Hop_{v,b}$,必然存在一条从 u 到 b 的路径 $R_{u,b}=(u,v,\cdots,b)$.该路径包括两部分:从节点 u 经过 1 跳到达节点 v,再从节点 v 经过最短路径路由到达基站.因此 $|R_{u,b}|=1+Hop_{v,b}$.其中,$|R_{u,b}|$ 表示从 u 到 b 的路径所经过的跳数.然而,$|R_{u,b}|\geq Hop_{u,b}$.所以,$1+Hop_{v,b}\geq Hop_{u,b}$,即 $Hop_{u,b}-Hop_{v,b}\leq 1$.同理可证当 $Hop_{u,b}<Hop_{v,b}$ 时,有 $Hop_{v,b}-Hop_{u,b}\leq 1$.因此,$|Hop_{v,b}-Hop_{u,b}|\leq 1$.

定理 1. 以邻节点距离基站的最小跳数进行前 h 跳有向路由,产生的幻像源节点集中于某些区域.

证明. 基于邻节点距离基站的最小跳数进行下一跳节点的选择,若源节点从其父节点集中选择下一跳的转发节点,则之后 h 跳中的每一跳,数据包均从当前节点的父节点集中选择转发节点直至数据包到达幻像源节点 p.因此,根据引理 1,有 $Hop_{p,b}=H-h$,其中,H 为源节点距离基站的最小跳数,$Hop_{p,b}$ 表示幻像源节点 p 与基站 b 间的最小跳数.在节点均匀分布的传感器网络中,假定基站的第 i

个圆为以基站为圆心,$i\times R(i=1,2,3,\cdots)$为半径的圆,其中,$R$ 为节点的通信半径.距离基站最小跳数为 $k(k=2,3,\cdots)$的节点位于基站的第 k 个圆与第 $k-1$ 个圆组成的环之间,距离基站一跳的节点为基站通信半径内的节点.因此,p 位于基站第 $H-h$ 与第 $H-h-1$ 个圆组成的环之间.根据文献[6]的协议描述,有 $Hop_{p,s}\leq h$,如图 1 所示,p 位于$\overset{\frown}{E_1E_5E_2}$的区域,其中,$Hop_{p,s}$表示幻像源节点 p 与真实源节点 s 间的最小跳数.同理可证,若真实源节点 s 从其子节点集中选择下一跳的转发节点,则幻像源节点 p 位于$\overset{\frown}{E_3E_6E_4}$的区域.如图 1 所示,由于 $\theta=\arccos((h-1)/h)$,因此,幻像源节点 p 分布在 4θ 的区域范围内.

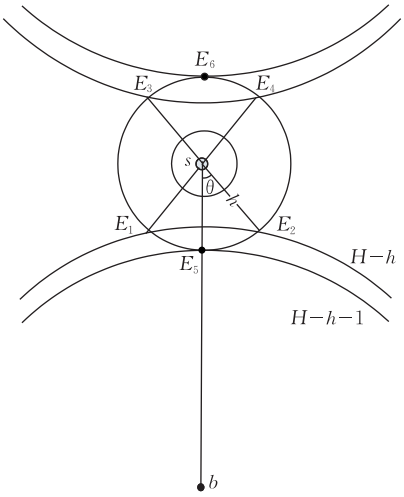

图 1　幻像源节点的分布

文献[7]首次考虑具有更强视觉模型的攻击者,提出可视区的概念,并认为攻击者一旦追踪到可视区内的节点即视为源节点暴露.基于可视区的概念,Wang 等人[7]发现,数据包在最短路径路由阶段经过可视区将大大增加源节点被发现的概率.因此,Wang[7]定义最短路径阶段经过可视区的路径为失效路径.为了进一步保护源节点位置隐私,Wang[7]提出一种基于角度的源位置隐私保护协议,该协议降低了数据包在最短路径路由阶段进入可视区的概率,却具有以下问题:首先,该协议不能避免失效路径的产生.其次,角度的计算引入了额外的计算开销.最后,为了降低失效路径产生的概率,该协议基于角度选择下一跳的节点,使得幻像源节点以较高的概率集中于某些区域.本文的协议能够有效解决上述不足,不但能够等概率的产生地理位置多样性的幻像源节点,而且能够完全避免失效路径的产生,有效地增强了源位置隐私的安全性.

3　问题定义

3.1　系统模型

(1)网络模型

本文的网络模型与熊猫-猎人博弈模型[6]相似.在熊猫-猎人博弈模型中,传感器网络用于监测熊猫的活动和位置.熊猫一旦被发现,距离熊猫最近的节点会将观测结果以数据包的形式周期性地发送给基站.试图非法捕获熊猫的猎人无法解密并获得数据包的真实内容.本文的目标就是使得攻击者通过逆向、逐跳追踪数据包,依然难以定位熊猫的位置.为此,本文对整个网络做了如下假定:

① 传感器节点在全网均匀分布,全网的任意两个节点可以通过多跳方式进行通信.

② 全网仅有一个基站.当监测到目标,距离目标最近的节点即源节点周期性地产生数据包并发送给基站.

(2)攻击模型

受到巨大利益的驱使,攻击者试图配备优质的追踪设备用于目标定位,本文假定攻击者具有如下特征:

① 硬件优良.攻击者具有足够大的存储空间和强大的计算能力.攻击者能够通过无线射频定位技术检测出消息的发送者并迅速移动至发送方的位置.

② 被动流量监测.攻击者不能解密数据包并篡改数据包的内容,也不能够毁坏传感器节点.攻击者仅仅能够监听某个区域内的网络流量,本文假定攻击者的监听半径为传感器节点的通信半径[6].

初始状态,攻击者位于基站处,观察基站与其邻节点间的通信.一旦发现某个节点向基站发送数据包,攻击者迅速移至数据包的发送节点.根据已有的追踪策略,存在两类攻击者:有耐心的攻击者和谨慎的攻击者.前者,攻击者监听数据包并朝着数据包的发送方移动,在其移动过程中,若攻击者监听到有其它节点发送数据包,攻击者忽略该信息.后者,攻击者能够记录他所经历的每一跳,当攻击者在一段时间内监听不到新的数据包的时候,回跳.否则,攻击者等待.文献[6]中的实验表明,与谨慎的攻击者相比,有耐心的攻击者能够提供更强的追踪性能.因此,本文研究有耐心的攻击者.

(3)安全假设

基站具有一对非对称密钥,每个传感器节点都

与基站共享非对称密钥中的公钥. 节点密钥在节点部署前载入节点. 本文假定基站是安全的,不能被攻击者俘获.

4 基于源节点有限洪泛的源位置隐私保护协议

4.1 基本协议描述

本文将传感器网络中的节点分为两类:普通节点和基站节点. 本文提出的 PUSBRF 协议分为 3 个阶段:源节点 h 跳有限洪泛阶段、h 跳有向路由阶段和最短路径路由阶段.

以本文模型,距离熊猫最近的节点为数据源节点,当数据源节点 s 监测到熊猫的活动时,s 向其 h 跳范围内的节点广播消息 SM,通过 SM 消息的广播,每个节点得到或更新该节点及其邻节点距离源节点的最小跳数值. 在 h 跳有限洪泛过程结束之后,源节点每隔 T 个时间单位产生并向基站发送一个数据包. 在 h 跳有向路由阶段中,当前节点基于其邻节点距离源节点的最小跳数值,选取距离源节点跳数较大的邻节点作为下一跳的转发节点. 这一阶段的路由过程保证数据包的每一跳均是朝着远离源节点的方向进行,同时保证经过 h 跳路由后,产生的幻像源节点均匀分布在源节点的各个方向上. 在最短路径路由阶段中,当前节点选取距离基站跳数最小的邻节点作为下一跳的转发节点,直至数据包到达基站. 其中,h 和 T 是预先设定的协议参数.

表 1 本文使用的主要记号

u,v	节点的 ID 号
h	源节点有限洪泛的跳数
(K_{pub},K_{pri})	加密/解密消息的公钥/私钥对
$E_{K_{pub}}(m)$	使用公钥 K_{pub} 加密消息 m
T_u	节点 u 的邻节点列表
s	真实的源节点
b	基站
$Hop_{u,v}$	节点 u 与节点 v 间的最小跳数
$Hop_{\widehat{uv}}$	以真实的源节点 s 为圆心,s 与 u 的距离为半径的圆周上,数据包从 u 沿着该圆到达节点 v 所经过的最小跳数
p_i	幻像源节点
$u.neighbor$	节点 u 的邻节点集合
$u.set\_source$	$\{v\mid v\in u.neighbor\cap Hop_{v,s}>Hop_{u,s}\}$
r	攻击者的视觉区半径/可视区的半径
$u.set\_parent$	$\{v\mid v\in u.neighbor\cap Hop_{v,b}<Hop_{u,b}\}$
H	真实源节点与基站间的最小跳数
R	节点的传输半径
$SP_{u,v}$	节点 u 与节点 v 间的最短路径

4.2 网络安全初始化

在安全的初始启动阶段,作为源位置隐私保护协议的基础,网络初始化过程实现了源位置隐私保护协议的基本安全信息,其中包括完成密钥的建立、实现邻居节点的发现以及发现每个普通节点到基站的最小跳数信息. 在网络安全初始化阶段完成之后,基站存储一对非对称密钥(K_{pub},K_{pri});每个普通节点 u 存储与基站共享的公钥 K_{pub}、源节点有限洪泛的跳数值 h 以及一个邻节点列表 T_u. 表 T_u 具有节点 u 的邻节点 ID 信息以及各邻节点距离基站的最小跳数信息.

在节点部署前,基站载入一对非对称密钥(K_{pub},K_{pri}),每个节点 u 预载入与基站共享的公钥 K_{pub} 以及源节点有限洪泛的跳数值 h. 普通节点使用公钥加密需要发送的数据,用以抵御外部攻击. 在传感器网络部署之后,基站设定计时器并向全网范围内广播 Beacon 消息 $BM=\{BRO\_BASE, ID, hop\_b\}$,其中包括消息类型 BRO_BASE、发送该消息的节点号 ID、hop_bs 表示消息的跳数计数,初始为 0. 对于首次接收到的 BM,u 将其 hop_bs 字段加 1,更新 $Hop_{u,b}=hop\_bs$ 并向邻居广播该消息,然后 u 进入等待状态. 对于接收到的任何一个 BM,节点 u 将节点号 ID 及 hop_bs 加入自己的邻节点列表 T_u 中,重复上述过程直到计时器超时. 这里,计时器时长可以设为网络初始化阶段时长. 由于传感器网络静态部署,对每个节点 u,T_u 是稳定的.

4.3 源节点 h 跳有限洪泛

源节点 h 跳有限洪泛是 h 跳有向路由的基础. 在 h 跳有向路由中,当前节点基于其邻节点距离源节点的最小跳数进行下一跳节点的选择,因此,每个节点需要获得自身及其邻节点距离源节点的最小跳数值. 在源节点 h 跳有限洪泛结束之后,距离源节点 h 跳内的每个节点 u 得到其距离源节点的最小跳数值 $Hop_{u,s}$ 且 T_u 中增加邻节点距离源节点的最小跳数字段并记录该最小跳数值.

当监测到目标在附近区域时,数据源节点设定计时器并向其 h 跳范围内的节点广播消息 $SM=\{BRO\_SOURCE, ID, hop\_s\}$,其中包括消息类型 BRO_SOURCE、发送该消息的节点号 ID、hop_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,则节点不再广播该消息. 该阶段与网络安全初始化过程中的基站全网广播行为类似,区别在于两方面:(1) 消息仅在距离源节点 h 跳

内的节点中广播;(2)hop_s 用于计算当前节点距离源节点的最小跳数而非距离基站最小跳数.

4.4 h 跳有向路由

在 h 跳有向路由阶段,本文提出基于邻节点距离源节点的最小跳数进行下一跳节点的选择.如图 1 所示,该选择策略产生的幻像源节点 p 能够均匀散布在以 s 为圆心,h 为半径的圆周上,而不是聚集在某段弧上.

定义 1.　当前节点 u 从其邻节点中选择一个节点 v 作为其下一跳的转发节点,使得节点 v 满足 $Hop_{v,A}-Hop_{u,A}=1$,则定义为数据包的这一跳朝着远离节点 A 的方向进行.其中,A 为传感器网络中的一个节点,$A\neq u$ 且 $A\neq v$.

h 跳有向路由主要有两个目的:产生的幻像源节点足够远,产生幻像源节点具有地理位置的多样性.前者要求前 h 跳路由中的每一跳均是朝着远离数据源节点的方向进行;后者要求产生的幻像源节点分散于距离真实源节点 h 跳处的各方向.

当数据源节点 h 跳有限洪泛过程结束后,数据源节点每隔 T 个时间单位,产生并发送一个数据包 $Packet=\{E_{K_{pub}}(m),\ hop\_rand,\ Next\_hop\_id\}$,其中包括用公钥 K_{pub} 加密后的消息 $E_{K_{pub}}(m)$、数据包被转发的跳数计数 hop_rand 以及下一跳节点的 ID 号.hop_rand 初始为 0,数据包到达每个转发节点时加 1,计数到 h,则数据包完成随机 h 跳转发过程.$u.set\_source\subset u.neighbor$ 且 $u.set\_source$ 中的节点距离源节点的最小跳数值大于节点 u 距离源节点的最小跳数.若节点 u 接收到一个 $Packet$,则 u 从 $u.set\_source$ 中随机选取一个节点进行数据包转发.重复此过程,直至数据包被转发 h 次.每一次均从 $u.set\_source$ 中选择下一跳的转发节点,保证了前 h 跳的每一跳均是朝着远离源节点的方向进行.每一次从 $u.set\_source$ 中随机选择转发节点,保证经过随机 h 跳后,产生更多幻像路径.因此,真实的数据源节点得到更为有效的保护.

4.5 最短路径路由

最短路径路由是为了在较短的时间内将数据包从幻像源节点发送给基站.$u.set\_parent\subset u.neighbor$ 且 $u.set\_parent$ 中的节点距离基站的最小跳数值小于节点 u 距离基站的最小跳数.若数据包已完成随机 h 跳路由过程,接收到该数据包的节点 u 从 $u.set\_parent$ 中随机选取一个节点进行数据包转发.重复此过程,直至数据包到达基站.

5 基于源节点有限洪泛的增强性源位置隐私保护协议

基于 PUSBRF 协议,本文考虑具有更强视觉能力的攻击者,提出 EPUSBRF 协议.攻击者能够观察到距离其 r 跳内的节点,因此,攻击者一旦追踪到距离源节点 r 跳内的节点即视为源节点暴露.如图 2 所示,$\overset{\frown}{p_1p_3p_2}$ 间的幻像源节点到基站的最短路径经过可视区,为失效路径.不难发现,失效路径使得攻击者在最短路径路由阶段就能捕获真实的源节点.

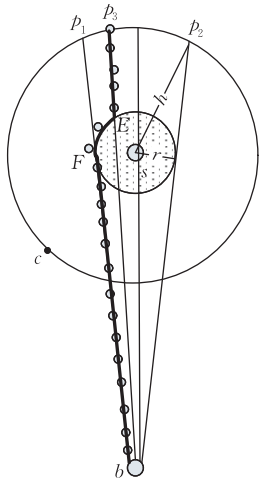

图 2　避开可视区的最短路径路由

文献[7]证明,在节点均匀分布的大规模传感器网络中,产生失效路径的概率为

$$(\arcsin(r/H)+\arcsin(r/h))/\pi \qquad (1)$$

式(1)表明可视区范围越大,源节点距离基站越近,随机路由的跳数越小,产生的失效路径越多.

为了进一步增强对源节点位置隐私的保护,避免产生失效路径,本文提出 EPUSBRF 协议.该协议与 PUSBRF 协议主要有 3 点不同:首先,在网络安全初始化阶段,仅实现节点的静态部署与网络参数的预载入,不进行基站全网广播.其中,每个节点不仅预载入 K_{pub} 和 h,也载入可视区半径 r.其次,在源节点 h 跳有限洪泛的同时标记出可视区内的节点;最后,在源节点有限洪泛之后进行避开可视区的基站全网广播.EPUSBRF 协议在不增加计算开销的前提下,完全避免了失效路径的产生,有效地提高了源位置隐私的安全性.

在 EPUSBRF 协议中,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.EPUSBRF 协议为每个节点 u 增加了可视区标记字段 $u.visual$,若 $Hop_{u,s}\leq r$,则表示节点 u 为可视区内的节点,更

新 $u.visual=1$.

源节点 h 跳有限洪泛结束后,基站进行避开可视区的全网广播.该广播策略与 PUSBRF 协议中的基站全网广播过程类似,不同在于,只有可视区外的节点参与广播过程.具体执行如下:若节点 u 为可视区内的节点,则丢弃接收到的任何 BM 消息.若节点 u 为可视区外的节点,则对于首次接收到 BM,u 将其 hop_bs 字段加 1,更新 $Hop_{u,b}=hop\_bs$ 并向邻居广播该消息,然后 u 进入等待状态.对于接收到的任何一个 BM,节点 u 将发送该消息的节点号 ID 及 hop_bs 加入自己的邻节点列表 T_u 中,重复上述过程直至计时器超时.

在避开可视区的基站广播过程结束后,数据源节点产生一个包含监测信息的数据包并根据 PUSBRF 的数据包路由策略,将该数据包路由至基站.

由于可视区内的节点不参与基站广播,因此对于任意可视区外的节点 u,有 $\forall v\in u.set\_parent$,$v.visual=0$ 且 $Hop_{u,s}>Hop_{v,s}$.因此,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到达基站.如图 2 所示,数据包在到达幻像源节点 p_3 后,经过路径 $SP_{p_3,E}$、$SP_{\overset{\frown}{EF}}$ 以及 $SP_{F,b}$ 到达基站.如图所示,其中,$SP_{p_3,E}$ 表示节点 p_3 与 E 间的最短路径,$SP_{\overset{\frown}{EF}}$ 表示从节点 E 沿着劣弧 EF 到达 F 的路径,$SP_{F,b}$ 表示节点 F 与 b 间的最短路径.

6 理论分析

6.1 通信开销分析

通信开销即为节点转发数据包的次数[6].PUSBRF 协议与 EPUSBRF 协议的通信开销包括 4 个部分:基站全网广播开销、源节点有限洪泛的开销、数据包有向 h 跳路由开销、数据包最短路径路由至基站的开销.其中,文献[5-8]中均有基站的广播过程且开销相同,因此,本文不做分析.对于熊猫-猎人博弈模型,熊猫在短期内其位置是不变的[5],只有熊猫的移动才会导致源节点的变更.变更后的源节点仅进行一次有限 h 跳洪泛且 $h\ll n$,因此,其开销可以忽略不计.因此,本文分析的通信开销仅包括数据包有向 h 跳的开销和数据包最短路径路由至基站的开销.

6.1.1 PUSBRF 协议的通信开销分析

如图 3 所示,C 为以 s 为圆心,h 为半径的圆周.根据 PUSBRF 协议,数据包从真实的源节点路由至幻像源节点 $p_4\in C$ 后,再从 p_4 经过最短路径路由到达基站.因此,PUSBRF 协议的通信开销为 $Hop_{s,p_4}+Hop_{p_4,b}$.在节点均匀分布的大规模传感器网络中,本文用两节点间的跳数值表示路径长度.在由 s,p_4,b 组成的三角形中,$Hop_{s,p_4}=h$,$Hop_{p_4,b}=\sqrt{h^2+H^2-2hH\cos\alpha}$,因此,PUSBRF 协议的通信开销为

$$h+\sqrt{h^2+H^2-2hH\cos\alpha} \tag{2}$$

其中,$\alpha\in(0,2\pi]$.当 $\alpha=\pi$ 时,通信开销达到最大值 $H+2h$,即数据包经过 h 跳有向路由后到达 p_5,从 p_5 经过最短路径路由到达基站;当 $\alpha=2\pi$ 时,通信开销达到最小值 H,即数据包经过 h 跳有向路由后到达 p_6,从 p_6 经过最短路径路由到达基站;考虑一般情况,p_3 为圆周 C 上任意一个点,p_3 到基站的平均最小跳数为

$$\int_0^{\pi}\sqrt{h^2+H^2-2hH\cos\alpha}/\pi\mathrm{d}\alpha.$$

因此,对于 PUSBRF 协议,通信开销的平均值为

$$h+\int_0^{\pi}\sqrt{h^2+H^2-2hH\cos\alpha}/\pi\mathrm{d}\alpha.$$

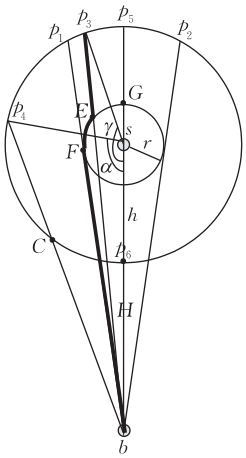

图 3 从幻像源节点路由至基站的路径

6.1.2 EPUSBRF 协议的通信开销分析

对于 EPUSBRF 协议,如图 3 所示,根据幻像源节点位置的不同,通信开销的计算分为两种情况:

(1)若幻像源节点位于 $\overset{\frown}{p_1Cp_6}$ 上,如节点 p_4,此时,EPUSBRF 协议的通信开销与 PUSBRF 协议的通信开销相同:

$$Hop_{s,p_4}+Hop_{p_4,b}=h+\sqrt{h^2+H^2-2hH\cos\alpha}.$$

(2)若幻像源节点位于劣弧 p_1p_5 上,如节点 p_3.根据第 5 节的协议描述,数据包到达节点 p_3 后,首先沿着 p_3 到 bs 的最短路径路由至可视区附近即 E 处.根据避开可视区的基站广播策略以及 EPUSBRF 协

议中的最短路径路由策略,数据包将沿着劣弧 EF 路由至 F 处,最后从 F 经过最短路径路由至基站.因此,EPUSBRF 协议的通信开销为

$$Hop_{s,p_3}+Hop_{p_3,E}+Hop_{\widehat{EF}}+Hop_{F,b},$$

其中,$Hop_{s,p_3}=h$,$Hop_{F,b}=\sqrt{H^2-r^2}$.若设 $\angle 1=\angle bp_3s$,$\angle 2=\angle sbp_3$,$\angle 3=\angle sEb$,$\angle 4=\angle Esp_3$.在 $\triangle p_3sb$ 中,有 $Hop_{p_3,b}=\sqrt{h^2+H^2-2hH\cos\gamma}$ 且由正弦定理可得 $\angle 1=\arcsin(H\sin\gamma/Hop_{p_3,b})$,$\angle 2=\arcsin(h\sin\gamma/Hop_{p_3,b})$.在 $\triangle Esb$ 中,由正弦定理可得 $\angle 3=\arcsin(H\sin\angle 2/r)$.在 $\triangle p_3Es$ 中,有 $\angle 4=\angle 3-\angle 1$,则由余弦定理可得

$$Hop_{p_3,E}=\sqrt{h^2+r^2-2hr\cos\angle 4}.$$

因此,$Hop_{\widehat{EF}}=(\gamma-\arccos(r/H)-\angle 4)r$.

综合(1)、(2),考虑一般情况,p_4 为 $\overset{\frown}{p_1Cp_6}$ 上任意一个点,p_3 为劣弧 p_1p_5 上任意一个点,有 $\alpha\in[0,\arccos(r/H)+\arccos(r/h))$ 且 $\gamma\in[\arccos(r/H)+\arccos(r/h),\pi]$.当 $\gamma=\pi$ 时,通信开销达到最大值为 $2h+(\pi-1-\arccos(r/H))r+\sqrt{H^2-r^2}$,即数据包经过 h 跳有向路由后到达幻像源节点 p_5,再从 p_5 经过避开可视区的最短路径路由到达基站;当 $\alpha=0$ 时,通信开销为最小值 H.此时,数据包经过 h 跳有向路由后到达 p_6,从 p_6 经过最短路径路由到达基站.EPUSBRF 协议的通信开销平均值为

$$h+\sqrt{H^2-r^2}(\arcsin(r/H)+\arcsin(r/h))/\pi+\int_0^{\arccos(r/H)+\arccos(r/h)}(\sqrt{h^2+H^2-2hH\cos\alpha})/\pi\mathrm{d}\alpha+\int_{\arccos(r/H)+\arccos(r/h)}^{\pi}(\sqrt{h^2+r^2-2hr\cos\angle 4}+(\alpha-\arccos(r/H)-\angle 4)r)/\pi\mathrm{d}\alpha\ .$$

6.1.3　PUSBRF 协议与 EPUSBRF 协议的通信开销对比

根据前两小节的通信开销分析,当幻像源节点位于 $\overset{\frown}{p_1Cp_2}$ 时,PUSBRF 协议与 EPUSBRF 协议的通信开销相同;当幻像源节点 p_3 位于 $\overset{\frown}{p_1p_5p_2}$ 时,EPUSBRF 协议与 PUSBRF 协议相比,通信开销增加.若设通信开销的增加量为 f,如图 3 所示,考虑一般情况:当幻像源节点 p_3 位于 $\overset{\frown}{p_1Cp_6}$ 上某处时,$f=0$;当幻像源节点 p_3 位于劣弧 p_1p_5 上某处时,$f=Hop_{\widehat{EF}}+Hop_{F,b}-Hop_{E,b}$.

若设 $\beta_1=\angle Esb$,$\beta_2=\angle Fsb=\arccos(r/H)$,则 $Hop_{\widehat{EF}}=(\beta_1-\beta_2)r$.在 $\triangle Esb$ 中,由余弦定理可得 $Hop_{E,b}=\sqrt{H^2+r^2-2Hr\cos\beta_1}$.因此,当 p_3 位于劣弧 p_1p_5 上某处时,

$f=(\beta_1-\beta_2)r+\sqrt{H^2-r^2}-\sqrt{H^2+r^2-2Hr\cos\beta_1}$,且

$$f'=\partial f/\partial\beta_1=(r/\sqrt{H^2+r^2-2Hr\cos\beta_1})\cdot(\sqrt{H^2+r^2-2Hr\cos\beta_1}-H\sin\beta_1).$$

由于 $\beta_1\in[\beta_2,\pi]$,因此 $f'\geq 0$,即当且仅当 p_3 位于 p_5 时,得到通信开销增加量的最大值:$f_{\max}=(\pi-1-\beta_2)r+\sqrt{H^2-r^2}-H$.

如图 3 所示,考虑最坏情况,假定当 p_3 位于劣弧 p_1p_5 上任意位置时,$f=f_{\max}$,而当 p_3 位于 $\overset{\frown}{p_1Cp_6}$ 时,$f=0$.因此,EPUSBRF 协议与 PUSBRF 协议相比,通信开销增加量的平均值为

$$f_{\mathrm{avg}}=\Big(\int_{\arccos(r/H)+\arccos(r/h)}^{\pi}f_{\max}\mathrm{d}\alpha+\int_0^{\arccos(r/H)+\arccos(r/h)}0\mathrm{d}\alpha\Big)\Big/\pi=(f_{\max}/\pi)[\pi-\arccos(r/H)-\arccos(r/h)],$$

其中,$r/h\in(0,1)$,$r/H\in(0,1]$.r 表示攻击者的视觉能力,H 与基站位置以及真实源节点的位置相关,因此,r 与 H 为相对固定的值.f_{avg} 随着 h 的减小而增加,当 $h\gg r$ 时,f_{avg} 达到最大值.表 2 显示,当 $h=r$,$H=100$ 时,随着 r/H 的变化,f_{avg} 的取值有变化.

表 2　通信开销增加量的平均值

r/H	f_{avg}
1/2	28
1/5	8
1/10	3
1/15	2
1/20	1

目前已有的 Mica 系列的传感器节点,单个节点间的最大通信距离约 60m.当 $r=6$ 时,表明攻击者的可视区半径大约为 360m,已经具有相当强的视觉能力.因此,本文假定 $r\leq 6$.当 $r/H=1/2$ 时,表明真实的源节点距离基站非常近,如当 $r=3$ 时,基站距离真实的源节点仅有 6 跳.在大规模无线传感器网络中,一般情况,$r/H\leq 1/5$,而此时 $f_{\mathrm{avg}}=8$.由表 2 可以看出,EPUSBRF 协议与 PUSBRF 协议相比,通信开销的增加量是可接受的,不会严重影响网络的生存性.

6.2　计算开销分析

当不考虑可视区时,PUSBRF 协议与文献[5-6,8]中的协议均未引入额外的计算开销.当考虑可视区时,PRLA[7] 为了减少数据包进入可视区的概率,在源节点洪泛时,距离源节点 h 跳内的每个节点需要

计算一个角度值,并依据此角度值计算每个节点被选择的概率.假定传感器网络中的节点密度为 ρ,节点的通信半径为 R,则距离源节点 h 跳内的节点共有 $\pi h^2R^2\rho$ 个,因此,需要进行 $\pi h^2R^2\rho$ 次角度计算.此外,每个节点还需计算每个邻节点被选择的概率,$\pi h^2R^2\rho$ 个节点共需计算 $\pi R^2h^2\rho(R^2\rho-1)$ 次.本文提出的 EPUSBRF 协议不但可以完全避开可视区内的节点,并且没有引入额外的计算开销.

6.3 安全性能分析

定义 2. 数据包从真实源节点经过有向随机 h 跳后到达幻像源节点的路径定义为随机有向路径.

当攻击者通过逆向追踪数据包到达某个幻像源节点时,源位置隐私保护协议产生的随机有向路径数越多,攻击者追踪到真实源节点的难度越大.在节点均匀分布的大规模传感器网络中,本文提出两种源位置隐私保护协议,幻像源节点均匀分布在以 s 为圆心,h 半径的圆周上.与 phantom single-path[6] 相比,PUSBRF 协议与 EPUSBRF 协议所产生的随机有向路径增加了 $\Phi=1-4\theta/2\pi=1-2\arccos((h-1)/h)/\pi$.表 3 为在 h 取值不同的情况下,Φ 值变化,其中 $h\geq2$.从表中可以看出,当 $h=2$ 时,本文提出的两种源位置隐私保护协议与 phantom single-path 相比,所产生的随机有向路径数至少增加了 33.33%.随着 h 的增加,Φ 值也在不断增大,当 $h=60$ 时,Φ 增加到 88.36%.若 h 值由 2 增加到 60,则本文提出的两种源位置隐私保护协议产生的随机有向路径平均增加了

$$1-\frac{\frac{2}{\pi}\sum_{h=2}^{60}\arccos\left(1-\frac{1}{h}\right)}{60}=79.83\%.$$

随着 h 值的增加,平均增加的随机有向路径数会更多.表 3 说明,与文献[5-6,8]的协议相比,PUSBRF 协议与 EPUSBRF 协议能够明显增加随机有向路径的数量,从而有效地提高源节点位置隐私的安全性.

表 3 随机有向路径增加百分比

	PUSBRF/EPUSBRF(Φ) /%
$h=2$	33.33
$h=20$	79.78
$h=30$	83.52
$h=40$	85.73
$h=50$	87.15
$h=60$	88.36

定理 2. 采用避开可视区的基站全网广播策略,能够产生避开可视区的父节点集,从而数据包在最短路径路由过程中能够完全避免失效路径的产生.

证明. 根据避开可视区的基站全网广播策略,可视区内的节点不参与该广播过程,因此对于任意非可视区内的节点 u,有 $u.set\_parent\neq\varnothing$,$\forall v\in u.set\_parent$ 且 v 是非可视区内的节点.在最短路径路由阶段,由于 $h>r$,因此,当前转发节点 u 位于可视区外.当前节点每一次均从 $u.set\_parent$ 中任意选择一个节点作为下一跳的转发节点,因此,最短路径路由的过程并不经过可视区内.又由于 $Hop_{u,b}>Hop_{v,b}$,因此数据包的转发总是朝着靠近基站的方向进行.

上述分析表明,在考虑可视区的情况下,EPUSBRF 协议在显著增加随机有向路径数量的同时避免了失效路径的产生,增强了源位置隐私的安全性.

6.4 通信开销 vs 安全性能

协议 PUSBRF 与 EPUSBRF 的通信开销及安全时间均随着 h 的增大而增大,其中,$r<h\leq H$.当 h 取值较大时,两协议的通信开销较大.此时,由于源节点有限洪泛的区域较大,因此,产生的随机有向路径数较多,攻击者从幻像源节点追踪至源节点需要花费较多时间.当 h 取值较小时,考虑极限情况:当 $h=r+1$ 时,两协议的通信开销均达到最小值.然而,源节点有限洪泛的区域较小,产生的随机有向路径数较少,攻击者在到达幻像源节点后,只需经过一跳即可追踪至目标,安全性能较差.由 6.1.3 小节的分析可知,r 与 H 为相对固定的值.因此,本文对不同取值范围的 r/H 进行讨论,进一步分析本文提出的两个协议如何在通信开销和安全性之间进行权衡.

当 $r/H>1/5$ 时,由 6.1.3 小节的分析可知,这种情况较少且基站与源节点的距离较近,又因为 $h\leq H$,因此,PUSBRF 的通信开销较小.即使 EPUSBRF 与 PUBSRF 相比,通信开销增加较多,EPUSBRF 的通信开销也是不高的.此外,由于基站与源节点的距离较近,攻击者很容易从基站追踪至源节点,此时,安全性能的要求远远高于通信开销.因此,为了更有效地保护源位置隐私,h 应取较大的值.若安全性能要求较高,H 较小,h 可取值 H.

当 $r/H\leq1/5$ 时,由 6.1.3 小节的分析可知,EPUSBRF 与 PUSBRF 的通信开销相当,两协议的安全性能均随着 h 的增大而增大.然而,若 h 取较大的值,两协议的通信开销均较大.表 3 显示,当 $2<h\leq20$ 时,随机有向路径数增加较明显,如 $h=20$

时,随机有向路径数增加至 79.78%. 而当 $h>20$ 时,随机有向路径数增加较缓慢. 当 h 由 20 增加至 40 时,随机有向路径数仅增加了约 6%. 因此,为了平衡安全性能与通信开销,$h=20$ 较为合适. 此外,若整个网络的安全需求较高,可进一步增大 h 的取值,增强协议的源位置隐私保护能力.

7　实验结果对比及分析

本文在 VS2005 的环境下用 C++构建了一个基于事件的模拟器,该模拟器包括 5 个模块:拓扑生成模块、图模块、事件发生队列模块、应用模块和逆向追踪模块. 拓扑生成模块生成传感器节点的位置拓扑信息并交给图模块;图模块记录图中节点属性等信息并与事件发生对列模块交换事件信息并相应修改图节点属性;事件发生队列模块维护一个事件发生队列,顺序地处理排队发生的事件;应用模块包含协议的实现函数,这些函数以事件响应的形式被事件发生队列模块调用;逆向追踪模块从事件发生队列模块和图模块读取信息,并相应修改攻击者的位置以实现攻击者的逆向、逐跳追踪. 本文在该模拟器中,对比 phantom single-path、PRLA 与本文提出的源位置隐私保护路由协议的性能. 为了便于实验对比,本文采用与文献[6-7] 相同的仿真环境配置. 本文中的 10,000 个传感器节点均匀分布于 $6000\times6000m^2$ 的网络区域,其中,每个节点的通信半径为 110m. 因此,每个节点的平均邻节点数为 8.64,少于 1%的节点松散地连接于少于或等于3 个邻节点. 为了实现节点的"随机且均匀"分布,本文将被监测区域划分为网格,节点初始布置在网格的中心位置上,之后,为每一个节点的位置加上一个随机扰动 ε,ε 服从正态分布,$\varepsilon\sim N(\mu,\sigma^2)$. 该拓扑生成方法既保证了每个网格内有一个传感器节点,又保证了每个网格内的传感器节点位置各不相同. 基站位置固定,源节点随机选择. 攻击者的监听半径为传感器节点的传输半径,可视区半径 r 设为 6,因此,当攻击者距离源节点 r 跳范围内时,能够捕获目标. 图 4 与图 6 为源节点距离基站的跳数 H 为 60,对于不同的 h,进行 50 次的追踪实验获得的平均结果. 图 5 与图 7 为 h 为 15,对于不同的 H 值,进行 50 次的追踪实验获得的平均结果.

7.1　通信开销对比与分析

图 4 显示,4 种协议的平均传输时延均随着 h 的增加而增加. 这是因为,随着 h 的增加,数据包在有向 h 跳路由阶段需要转发更多次才能到达幻像源节点,然而该阶段并不为数据包路由至基站做出贡献,因此增加了通信开销(此处指数据包个数). 图 4 还表明,phantom single-path、PRLA 与 PUSBRF 协议的通信开销相当,EPUSBRF 协议的通信开销略高. 这是因为 EPUSBRF 协议在最短路径路由阶段避开可视区的转发行为增加了额外的通信开销. 与通信开销最小的 phantom single-path 协议相比,EPUSBRF 的通信开销平均增长了 8.26%;当 $h=30$ 时,通信开销增长量达到 14.27%. 与 PUSBRF 协议相比,EPUSBRF 协议的通信开销平均增加了 3.91%,平均增加约 3 次数据包的转发. 6.1.3 小节的分析表明,当 $r/H=1/10$ 时,$f_{avg}=3$. 因此,实验结果与理论分析是相符的且两者均说明 EPUSBRF 协议的通信开销增长是可接受的.

图 5 显示,随着 H 的增加,4 种协议的平均传输时延也随之增加. 这是因为,随着基站距离源节点距离的增加,数据需要经过更多跳才能到达基站. 图 5 还表明,当 h 取值相同时,4 种协议的通信开销相当. 与通信开销最小的 phantom single-path 协议相比,EPUSBRF 的通信开销平均增长了 6.50%;平均增加约 4 次数据包的转发. 与 PUSBRF 协议相比,EPUSBRF 协议的通信开销平均增加了 4.98%,平均增加约 3 次数据包的转发,这说明 EPUSBRF 协议的通信开销增长是可接受的.

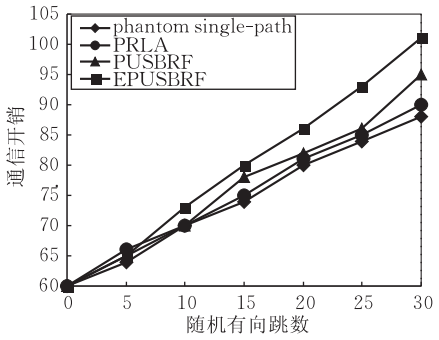

图 4　通信开销 vs 随机有向跳数

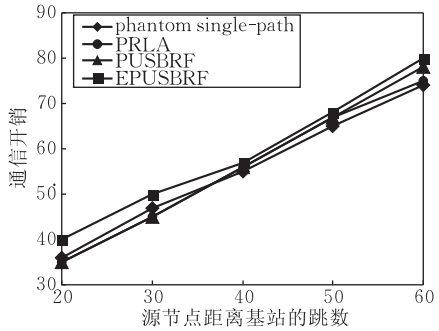

图 5　通信开销 vs 源节点距离基站的跳数

7.2 安全性能对比与分析

图 6 显示，随着 h 的增加，4 种协议的安全时间(此处指数据包个数)均有所增加. 这是因为随着 h 的增加，四种协议产生的幻像源节点距离真实源节点更远，产生的有向随机路径也更多. 与安全性能较差的 phantom single-path 相比，EPUSBRF 的平均安全时间增加了 147.68%，与 PRLA 相比，EPUSBRF 的平均安全时间也增加了 91.58%. 此外，与 PUSBRF 相比，EPUSBRF 的平均安全时间也增加了 15.58%. 图 7 表明，随着 H 的增加，4 种协议的安全时间均有所增加. 这是因为当源节点距离基站较远时，位于基站的攻击者需要逆向追踪更多跳才能到达真实的源节点. 与安全性能较差的 phantom single-path 相比，EPUSBRF 的平均安全时间增加了 145.44%，与 PRLA 相比，EPUSBRF 的平均安全时间也增加了 114.94%. 此外，与 PUSBRF 相比，EPUSBRF 的平均安全时间增加了 7.71%. 图 6 与图 7 同时显示，PRLA 的安全时间略高于 phantom single-path 且 PUSBRF 协议的安全时间明显高于 PRLA. 与 PRLA 相比，PUSBRF 的平均安全时间增加将近一倍. 这是因为 PRLA 基于角度计算进行邻节点的选择，降低了失效路径的产生概率，从一定程度上提升了协议的安全性能. 然而，PRLA 产生的幻像源节点以较高的概率分布于某些区域. 同时，PRLA 基于邻节点的角度值进行下一跳节点的选择，不能保证数据包的每一跳均是朝着远离源节点的方向进行，最终导致一部分幻像源节点位于真实的源节点附近. 图 6、图 7 还表明，与 PUSBRF 协议相比，EPUSBRF 协议更进一步提高了安全时间. 我们分析主要有两方面原因：首先，EPUSBRF 能够产生远离源节点且地理位置多样性的幻像源节点，因此，能够产生足够多的随机有向路径；其次，通过避开可视区的基站广播，EPUSBRF 在最短路径路由阶段能够完全避免产生失效路径，显著增强了源位置隐私的安全性能.

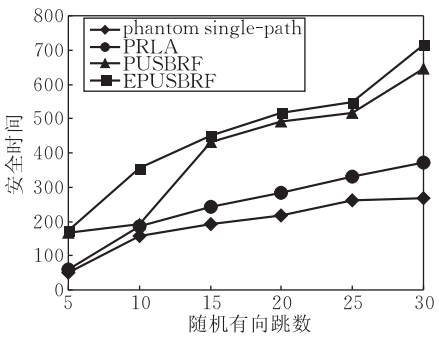

图 6 安全时间 vs 随机有向跳数

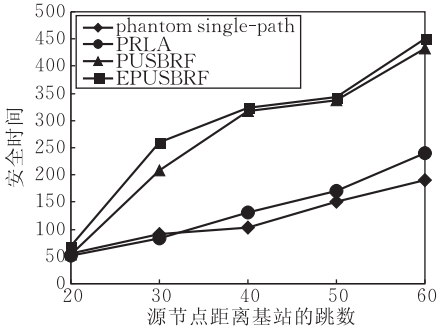

图 7 安全时间 vs 源节点距离基站的跳数

8 结束语

广泛应用于目标监测的无线传感器网络，源节点位置的暴露会直接威胁到目标的安全性. 本文分析并总结了当前抵御局部流量攻击的源位置隐私保护协议存在的问题，针对这些问题，本文提出 PUSBRF 协议，理论分析表明，该协议能够产生远离真实源节点且地理位置多样性的幻像源节点，与 phantom single-path 协议相比，该协议产生的随机有向路径数至少增加了 33.33%. 基于该协议并考虑具有更强视觉能力的攻击者，本文提出 EPUSBRF 协议. 理论分析表明该协议在不增加计算开销的前提下，首次避免了失效路径的产生. 实验表明，与已有的源位置隐私保护协议相比，本文提出的两种协议明显提高了源位置隐私的安全性.

参 考 文 献

[1] Shao M, Zhu S, Zhang W, Cao G. pDCS: Security and privacy support for data-centric sensor networks//Proceedings of the 26th IEEE International Conference on Computer Communications (INFOCOM). Alaska, USA, 2007: 1298-1306

[2] Joseph M, Choudhury R R. Hiding stars with fireworks location privacy through camouflage//Proceedings of the ACM Special Interest Group on Mobility of Systems, Users, Data and Computing (SIGMOBILE). Beijing, China, 2009: 345-356

[3] Hoh B, Gruteser M, Xiong H, Alrabady A. Enhancing security and privacy in traffic-monitoring systems. IEEE Pervasive Computing, 2006, 5(4): 38-46

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

[5] Ozturk C, Zhang Y, Trappe W. Source-location privacy in energy constrained sensor networks routing//Proceedings of the ACM Workshop on Security of Ad Hoc and Sensor Net-

works (SASN). Washington DC, USA, 2004: 88-93

[6] Kamat P, Zhang Y, Trappe W, Ozturk C. Enhancing source-location privacy in sensor network routing//Proceedings of the 25th International Conference on Distributed Computing Systems (ICDCS). Ohio, USA, 2005: 599-608

[7] Wang W P, Chen L, Wang J X. A source-location privacy protocol in WSN based on locational angle//Proceedings of the IEEE International Conference on Communications (ICC). Beijing, China, 2008: 1630-1634

[8] Kang L. Protecting location privacy in large-scale wireless sensor networks//Proceedings of the IEEE International Conference on Communications (ICC). Dresden, Germany, 2009

[9] Mehta K, Liu D, Wright M. Location privacy in sensor networks against a global eavesdropper//Proceedings of the IEEE International Conference on Network Protocols (ICNP). Beijing, China, 2007: 314-323

[10] Yang Y, Shao M, Zhu S, Urgaonkar B, Cao G. Towards event source unobservability with minimum network traffic in sensor networks//Proceedings of the ACM Conference on Wireless Network Security (WiSec). Alexandria, Virginia, USA, 2008: 77-88

[11] Shao M, Yang Y, Zhu S, Cao S. Towards statistically strong source anonymity for sensor networks//Proceedings of the 27th Conference on Computer Communications (INFOCOM). Phoenix, AZ, USA, 2008: 51-55

[12] Jian Y, Chen S G. Protecting receiver-location privacy in wireless sensor networks//Proceedings of the 26th Conference on Computer Communications (INFOCOM). Alaska, USA, 2007: 1955-1963

[13] Zhou Shui-Geng, Li Feng, Tao Yu-Fei, Xiao Xiao-Kui. Privacy preservation in database applications: A survey. Chinese Journal of Computers, 2009, 32(5): 847-861(in Chinese)
(周水庚, 李丰, 陶宇飞, 肖小奎. 面向数据库应用的隐私保护研究综述. 计算机学报, 2009, 32(5): 847-861)

[14] Xiao X, Tao Y. Dynamic anonymization: Accurate statistical analysis with privacy preservation//Proceedings of the ACM SIGMOD Conference on Management of Data (SIGMOD). Vancouver, BC, Canada, 2008: 107-120

[15] Kantarcioglu M, Clifton C. Privacy-preserving distributed mining of association rules on horizontally partitioned data. IEEE Transactions on Knowledge and Data Engineering, 2004, 16(9): 1026-1037

[16] Jiang W, Clifton C. A secure distributed framework for achieving k-anonymity. The International Journal on Very Large Data Bases, 2006, 15(4): 316-333

[17] Wang K, Fung B C M, Yu P S. Handicapping attacker's confidence: An alternative to k-anonymization. Knowledge and Information Systems, International Journal of Knowledge and Information Systems (KAIS), 2006, 11(3): 345-368

[18] Xu T, Cai Y. Exploring historical location data for anonymity preservation in location-based services//Proceedings of the 27th Conference on Computer Communications (INFOCOM). Phoenix, AZ, USA, 2008: 547-555

[19] Xu T, Cai Y. Feeling-based location privacy protection for location-based services//Proceedings of the 16th ACM Conference on Computer and Communications Security (CCS). Chicago, Illinois, USA, 2009: 348-357

[20] Julien F, Hossein M M, Hubaux J P. On non-cooperative location privacy a game-theoretic analysis//Proceedings of the 16th ACM Conference on Computer and Communications Security (CCS). Chicago, Illinois, USA, 2009: 9-13

CHEN Juan, born in 1982, Ph. D. candidate. Her research interests include wireless network security and privacy preservation.

FANG Bin-Xing, born in 1960, professor, Ph. D. supervisor, member of Chinese Academy of Engineering. His current research interests include computer architecture, information security and computer network.

YIN Li-Hua, born in 1973, postdoctor. Her current research interests include information security and security properties evaluation.

SU Shen, born in 1985, master candidate. His current research interests include wireless network security and privacy preservation in wireless sensor networks.

Background

This research is partly supported by the National Basic Research Program (973 Program) of China under grant (Nos. 2005CB321806, 2007CB311100), the National High Technology Research and Development Program (863 Program) of China under grant No. 2007AA01Z446.

For sensor networks deployed to monitor and report real events, source location privacy is an attractive and critical security property, which unfortunately is also very difficult and expensive to achieve. Attackers can find out the source node and finally catch the object by hop-by-hop backtracking strategy.

In this paper, the authors propose a source location privacy preservation protocols called PUSBRF, which can generate phantom source nodes with geographical diversity. Theoretical analysis shows that compared to the typical phantom single-path protocol, the number of the random directed paths generated by PUSBRF has increased by at least 33.33%. Based on PUSBRF, the authors propose another source location privacy preservation protocol called EPUSBRF under the consideration of an attacker with enhancement visual ability. Theoretical analysis shows that the protocol, for the first time, generates no waste path without increasing any computational overhead. Simulation results show that compared to the existing protocols, the protocols provide strong source location privacy preservation.