无线传感器网络源位置隐私保护路由协议

李道全,张玉霞,魏艳婷
(青岛理工大学 信息与控制工程学院,山东 青岛 266033)

摘　要:为了解决无线传感器网络源节点位置隐私保护问题,基于伪正态分布的无线传感器网络幻象路由的源位置隐私保护策略被提出,但该路由协议没有考虑更强攻击者的可视区问题和具有方向攻击性的攻击者,文中在该协议的基础上进行改进。增加了可视区问题,通过随机跳阶段达到过渡节点,将路径路由至可视区外;使用伪随机生成器生成一组高斯分布的随机实数来获得相应的随机跳阶段的随机跳数和伪正态分布路由阶段的跳数,增加了幻影节点的位置分布多样性与动态性;概率路由阶段通过设置的可视区节点标志避免失效路径的产生,并通过概率转发路由机制降低了重合路径产生的可能性。实验结果表明,改进协议避免了失效路径的产生,增加了安全时间,能明显提高源节点位置隐私保护的安全程度。

关键词:无线传感器网络;源节点位置隐私;路由协议;可视区;正态分布
中图分类号:TP393　　**文献标识码**:A　　**文章编号**:1673-629X(2019)07-0088-05
doi:10.3969/j.issn.1673-629X.2019.07.018

A Source-location Privacy Protection Routing Protocol for Wireless Sensor Networks

LI Dao-quan, ZHANG Yu-xia, WEI Yan-ting
(School of Information and Control Engineering, Qingdao University of Technology, Qingdao 266033, China)

Abstract: In order to solve the problem of source node location privacy protection in wireless sensor networks, a pseudo-normal distribution-based source location privacy protection strategy for phantom routing in wireless sensor networks is proposed. However, this routing protocol does not consider the visual area problem of stronger attackers and directional attackers. The improvement is carried out based on this protocol. The visual area problem increased, the transition node is reached through the random hopping phase, and the path is routed outside the visible area. A pseudo-random generator is used to generate a set of Gaussian distributed random real numbers to obtain the random hopping number of the corresponding random jump phase and pseudo-normal distribution route, increasing the diversity and dynamics of the location distribution of the phantom nodes. The probabilistic routing phase avoids the occurrence of failure paths by setting node flags in the visual area, and reduces the possibility of overlapping paths by probabilistic forwarding routing mechanism. Experiment shows that the improved protocol avoids the generation of the failure path, increases the security time, and can significantly improve the security level of the source node location privacy protection.

Key words: wireless sensor networks; source-location privacy; routing protocol; visual area; normal distribution

0　引　言

无线传感器网络(WSN)作为社交物联网的一部分[1],可以感测对象的状态或监视网络中的事件,却也面临一系列安全威胁,如信息窃听、数据捏造、节点破坏和路由中断等,这使得隐私保护变得至关重要[2]。隐私安全问题已成为其进一步发展的主要瓶颈,主要分为两种类型,面向数据的隐私威胁和面向上下文的隐私威胁[3]。面向数据的隐私威胁是指攻击者试图获取数据包内容并获取信息的情况,这些信息可以通过传统安全技术,如数据包加密等进行良好的保护[4-6]。文中主要研究面向上下文隐私威胁的源位置隐私问题。

收稿日期:2018-08-24　　**修回日期**:2018-12-25　　**网络出版时间**:2019-03-21
基金项目:山东省自然科学基金(ZR2016FB21)
作者简介:李道全(1967-),男,博士,教授,硕导,CCF 会员(13935M),研究方向为无线网络、电子商务等;张玉霞(1991-),女,硕士,研究方向为无线网络。
网络出版地址:http://kns.cnki.net/kcms/detail/61.1450.TP.20190321.0904.020.html

广大学者对源位置隐私(SLP)问题进行了大量研究。例如,Qztuk 等[7]在 2004 年对 WSN 中源位置隐私问题进行建模,提出了“熊猫-猎人”模型。在此基础上单径幻影路由算法被提出[8]。基于 k-匿名技术的解决方案[9],利用源节点周围的 k 个幻影节点来迷惑对手。随机有向路由协议[10]中将距离基站跳数大于节点距离基站跳数的邻居节点划分到子节点集,小于节点距离基站跳数的邻居节点划分到父节点集。基于源节点有限洪泛的源位置隐私保护协议(PUSBRF)和增强性源位置隐私保护协议(EPUSBRF)[11],在可视区的基础上,避免了失效路径的产生。基于伪正态分布的无线传感器网络幻象路由的源位置隐私保护策略(PNDBPR)[12],源节点通过伪正态分布来决定源节点的跳数,从而决定幻影源节点的分布。基于可变夹角的动态路由方案[13],改变了以往固定夹角产生候选集的状态,根据剩余延迟计算出每个节点的最优夹角,以此确定节点的候选节点集,在可接受的延迟内提高网络安全周期。

以上算法产生的幻影节点都分布在源节点的某些固定方向的范围内,如 PNDBPR 协议,幻影节点分布的区域更加广泛,但是还是分布在源节点周围的圆环上,也没有考虑可视区和失效路径问题。对于具有方向性的攻击者可以快速找到源节点的范围,文中针对更强攻击者和可视区问题对 PNDBPR 进行了分析和改进。

1　系统模型

1.1　网络模型

(1)传感器节点均匀分布,节点之间通过多跳的方式进行通信。节点具有相同的通信半径。

(2)全网只有一个基站,且基站位置信息是公开的;任意时刻只有一个节点成为源节点,当检测目标移动时距离最近的节点成为新的源节点。

(3)传输的所有数据包都是加密的。攻击者无法对数据包的内容进行破解。

1.2　攻击模型

(1)设备优良。攻击者配备了先进的设备,如天线和频谱分析仪。这些设备允许攻击者轻松检测接收到的数据包的信号强度,确定数据包的发送者,并决定是否采取行动。假设攻击者不会错过其监测范围内的任何数据包。

(2)攻击者只监视网络流量并定位源节点。它不会更改数据包的内容,更改路由信息以及破坏任何节点等,因为这些都不会有助于加快定位源节点位置,相反,它们可能存在使安装在网络中的入侵防御机制检测到对手的风险。

(3)攻击者初始位于基站附近,监听传送到基站的数据流量信息,根据监听到的流量信息逐跳回溯到源。攻击者监听半径与传感器节点通信半径相同。

2　改进路由协议

文中在基于伪正态分布幻象路由源位置隐私保护协议的基础上,考虑到更强攻击对手,增加了可视区和失效路径的问题。可视区即为距离源节点 r 跳内的区域,其中 r 称为可视区半径。幻影节点到基站路由阶段经过可视区的路径为失效路径。文中所用参数如表 1 所示。

表 1　参数列表

参数	说明
Sink_Hop	节点到基站的最小跳数
Trans_Hop	节点到过渡节点的最小跳数
$d_{\min}$	过渡节点到幻影节点的最小跳数
d_{ps}	过渡节点到幻影节点的随机跳数
p	幻影节点
Tr	过渡节点
H	源节点到基站的最小跳数
r	可视区半径
h	过渡节点到源的跳数
Select	源节点洪泛阶段节点标志
Vi_select	可视区节点标志
Flag	概率路由阶段节点标志

2.1 网络初始化

网络初始化阶段主要是为了确定网络中节点位置和节点到基站的最小跳数。每个节点都有自己的标识标签,即节点 ID,并将每个节点设置一个 Flag 标志,初始为 False。基站节点在全网范围内广播消息 BM = {ID,Coord,Sink_Hop},Coord 为节点位置坐标,Sink_Hop 为节点到基站的最小跳数,初始设置为 0,若节点首次接收到消息 BM 则将 Sink_Hop 加 1,并记录发送者的 ID, Coord , Sink_Hop ,更新消息 BM 并广播给邻居节点。邻居节点重复此过程,直到所有节点都接收到消息。初始化后,每个节点都能将 Sink_Hop 小于本节点 Sink_Hop 的邻居节点放到 u. parent 中。

2.2 幻影节点产生

幻影节点的产生分为两步,首先通过随机跳阶段到达过渡节点,然后伪正态分布路由阶段到达幻影节点。通过随机数发生器产生随机数 x ($d_{ps} > \rho d_{min}$),使 $X \sim N(0,\sigma)$,即 x 服从正态分布。设置伪正态分布路由阶段的跳数 $d_{ps} = d_{min}(|x|+1)$,当时,令 $d_{ps} = \rho d_{min}$, ρ 为大于零的常数。据正态分布的分布函数知, $d_{min} \leqslant d_{ps} \leqslant \rho d_{min}$ 的概率为 $p = 2\varphi(\frac{\rho-1}{\sigma}) - 1$,其中 $\varphi(x)$ 为标准正态分布的分布函数。当 $\rho = 2$ 时, $d_{min} \leqslant d_{ps} \leqslant 2d_{min}$ 的概率为 0.682 7,当 $\rho = 3$ 时, $d_{min} \leqslant d_{ps} \leqslant 3d_{min}$ 的概率为 0.954 5。设置随机跳阶段的跳数 $h = r + \rho d_{min}$ 。通过合理设置以上参数,可以控制幻影节点的位置和区域大小。

图 1 为文中改进路由协议的过程,其中 S 为源节点, B 为基站, Tr 为过渡节点, p 为幻影节点,图中所示阴影部分为幻影节点分布区域。

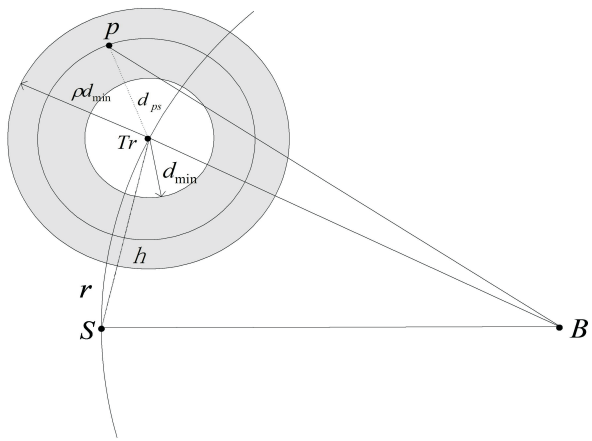


图 1 改进路由协议过程

2.2.1 随机跳阶段

当网络中的某一个节点称为源节点时,源节点与基站相同进行有限洪泛,将到基站跳数与源节点到基站跳数相同的节点放到节点 u. equal 中,并为每个节点设置一个选择标志 Select ,初始为 0,同时设置可视区内节点的选择标志 Vi_select 为 0。

源到过渡节点的路由过程:源节点从其同跳集 u. equal中的邻居节点中随机选择一个节点为转发节点,并将 Select 标志赋值为 1;转发节点与源节点相同,依次从 u. equal 集中的邻居节点中随机选择转发节点,并判断 Select 标志是否为 0,是则选择本节点为下一跳节点,并将 Select 标志赋值为 1;否则重新选择,设置跳数 h ,每经过一跳令 $h = h - 1$,直到 h 为 0,此时到达的节点称为过渡节点。若没有找到满足上述条件的节点或者满足条件的节点选择完毕,可以选择邻居节点中到基站的跳数与源节点到基站跳数相差为 1 的节点,继续选择,直到 h 为 0。

2.2.2 伪正态分布路由阶段

过渡节点与基站广播消息相同,通过有限洪泛广播消息 SM = {ID,Coord,Trans_Hop} , ID 和 Coord 与之前相同, Trans_Hop 表示节点到过渡节点的最小跳数,初始为 0,每达到一个转发节点加 1,直到 ρd_{min} ,每个节点将 Trans_Hop 值大于本节点 Trans_Hop 的邻居节点加入到 u. setTrans 中。

伪正态分布路由阶段,设置跳数 d_{ps} ,每次从 u. setTrans中随机选择一个节点作为下一跳节点且令 $d_{ps} = d_{ps} - 1$,直到 d_{ps} 为 0,此时到达的节点称为幻影节点。伪正态分布路由阶段保证了每一跳都是向着远离过渡节点的方向进行。

2.3 概率转发路由阶段

概率转发路由阶段,以最小跳数传输到基站,从父节点集中选择下一跳节点,并在选择下一跳节点时首先检查节点 Vi_select 标志,避开可视区节点,然后再检查节点 Flag 标志,当 Flag 为 False 时可以作为转发节点,并转换为 True ,否则,重新选择转发节点且将 Flag 标志转换 Flag 标志为 False 。

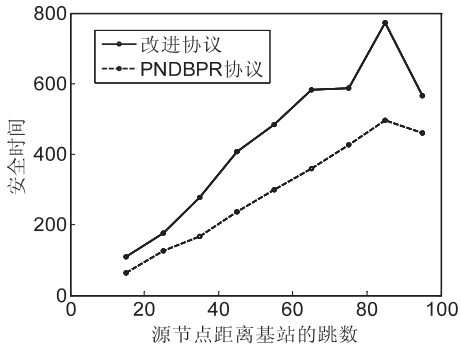
概率转发路由尽可能快地将数据包传输到基站并最小化路径重叠。

3　实验结果与分析

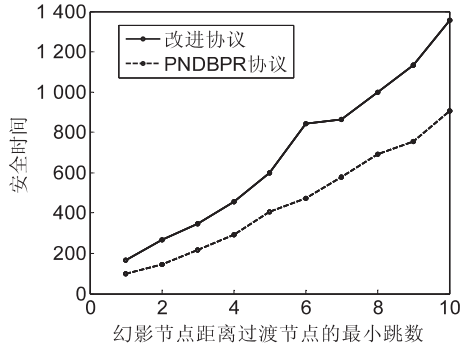
文中采用 MATLAB 7.0 对 PNDBPR 算法和文中算法进行仿真分析。在 1 000 m × 1 000 m 的环境中均匀部署 10 000 个传感器节点,节点通信半径为 15 m,正态分布参数 $\sigma = 1$。

3.1　安全周期

安全时间定义为源节点被攻击者捕获前发送的数据包的数量[14]。首先设置 $\rho = 2$, $d_{min} = 2$, $r = 1$,分别选取不同位置的 10 个源节点,每次发送 1 500 个数据包,求出安全时间。重复反追踪实验 100 次,获得平均安全周期如图 2(a)所示。再设置 $H = 30$, $\rho = 2$, $r = 1$,分别选择不同 d_{min},每次发送 1 500 个数据包,求出安全时间,如图 2(b)所示。



(a)不同源距离基站的跳数对应的安全时间



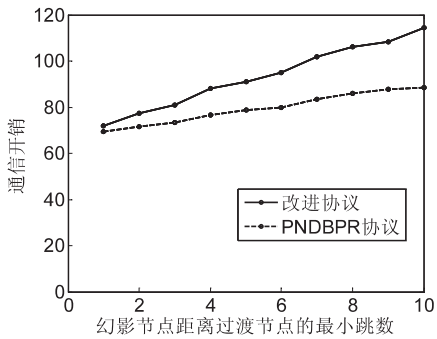
(b)不同 d_{min} 对应的安全时间

图 2　安全时间

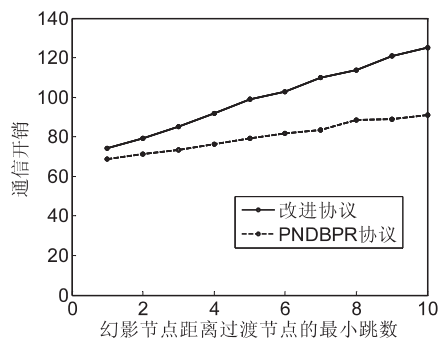
由图 2 可以看出,文中改进路由协议比改进之前安全性有所提高。由图 2(a)知,文中路由协议的平均安全周期平均增加了 54.55%,而且随着 H 的增加,安全时间也在增加,这是因为源节点距离基站越远,对手逆追踪找到源节点所需要的跳数越多,时间也就越长。由图 2(a)知,随着幻影节点到过渡节点最小跳数 d_{min} 的增加,安全时间也在增加,这是因为 d_{min} 越大,幻影节点分布的区域越大,从而产生的幻影节点越多,从而产生更多的路由路径,使对手更难捕捉到源节点。

3.2　通信开销

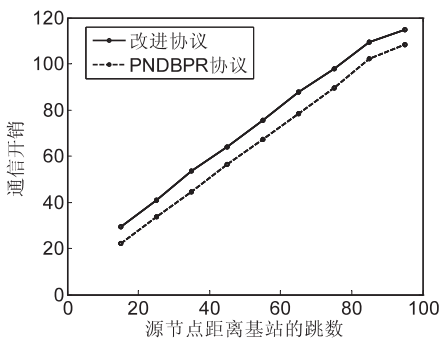
定义通信开销为源节点发送一个数据包到达基站节点所需要的跳数。首先,设置 $H = 60$,分别令 $\rho = 2$ 和 $\rho = 3$,得到不同 d_{min} 对应的通信开销,如图 3(a)和(b)所示。再设置 $d_{min} = 2$,分别令 $\rho = 2$ 和 $\rho = 3$,得到不同源节点位置对应的通信开销,如图 3(c)和(d)所示。



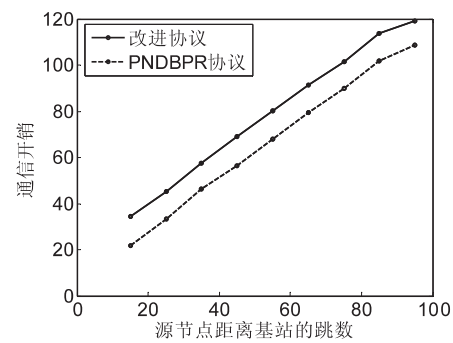
(a) $\rho = 2$



(b) $\rho = 3$



(c) $\rho = 2$



(d) $\rho = 3$

图 3　通信开销

由图 3 可以看出,文中改进路由协议比 PNDBPR 协议通信开销有所增加,这是因为增加可视区之后,为了将幻影节点路由出可视区之外,增加了过渡节点。由图 3(a)和(b)可以看出,随着幻影节点到过渡节点最小跳数 d_{min} 的增加,通信开销也在增加,因为 d_{min} 越大,随机跳阶段路由路径越长,幻影节点分布区域也越大。由图 3(c)和(d)知,源节点到基站的跳数 H 大,即源节点距离基站越远产生的路由路径越长,通信开销就越大。文中改进协议比 PNDBPR 协议通信开销在 $\rho = 2$ 时平均增加了 15.93% 左右,在 $\rho = 3$ 时平均增加了 23.49% 左右,这是因为 ρ 越大产生的幻影节点分布区域越大,路由路径越长,通信开销也越大。

由以上分析知,适当参数 ρ 和幻影节点到过渡节点最小跳数 d_{min},可以调节安全性能和通信开销之间的平衡。当需要较高安全性能时,可以适当牺牲通信开销增加节点的安全性。若网络对安全性要求不高,可以适当减少通信开销以节省网络能量。

4 结束语

对基于伪正态分布的无线传感器网络幻象路由的源位置隐私保护策略进行了改进,考虑了更强攻击者的可视区问题和具有方向攻击性的攻击者,并避免了失效路径的产生,提高了源节点位置的安全性。如何进一步减少通信开销,在安全性能和通信开销之间进行权衡选择将是下一步的研究方向。

参考文献:

[1] 弭宝瞳,梁 循,张树森. 社交物联网研究综述[J]. 计算机学报,2018,41(7):1448-1475.

[2] HAN Guangjie,ZHOU Lina,WANG Hao,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.

[3] 许 建,杨 庚,陈正宇,等. WSN 数据融合中的隐私保护技术研究[J]. 计算机工程,2012,38(15):134-138.

[4] 杨 庚,王安琪,陈正宇,等. 一种低耗能的数据融合隐私保护算法[J]. 计算机学报,2011,34(5):792-800.

[5] 赵小敏,梁学利,蒋双双,等. 安全的 WSN 数据融合隐私保护方案设计[J]. 通信学报,2014,35(11):154-161.

[6] 王军号,黄 娟,杜 朋. 基于分布式梯度算法的 WSN 隐私保护技术研究[J]. 传感技术学报,2017,30(9):1396-1400.

[7] OZTURK C,ZHANG Y,TRAPPE W. Source-location privacy in energy-constrained sensor network routing[C]//Proceedings of the 2nd ACM workshop on security of ad hoc and sensor networks. Washington DC,USA:ACM,2004:88-93.

[8] KAMAT P,ZHANG Y,TRAPPE W,et al. Enhancing source-location privacy in sensor network routing[C]//25th IEEE international conference on distributed computing systems. Columbus,OH,USA:IEEE,2005:599-608.

[9] BAHSI H,LEVI A. Energy efficient privacy preserved data gathering in wireless sensor networks having multiple sinks[C]//International conference on computer science and ITS applications. Jeju,Korea:IEEE,2009:1-8.

[10] KANG L. Protecting location privacy in large-scale wireless sensor networks[C]//Proceedings of the IEEE international conference on communications. Dresden, Germany: IEEE, 2009:1-6.

[11] 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[J]. 计算机学报,2010,33(9):1736-1747.

[12] HUANG Jun,SUN Meisong,ZHU Shitong,et al. A source-location privacy protection strategy via pseudo normal distribution-based phantom routing in WSNs[C]//Proceedings of the 30th annual ACM symposium on applied computing. Salamanca,Spain:ACM,2015:688-694.

[13] 刘 亚,许拥晶,宋 梁. WSNs 中基于可变夹角动态路由的源位置隐私保护方案[J]. 计算机应用研究,2018,35(1):257-260.

[14] 孔祥雪,袁少卿,陈 梦. 基于虚拟环的源位置隐私保护路由协议[J]. 传感器与微系统,2018,37(1):66-69.