Journal of System Simulation

Volume 27 | Issue 12 Article 14

7-30-2020

Protocol Algorithm Design of Location Privacy Preserving for Sink Node Based on Security Area

Peiyu Li
Network Information Center of Henan University of Science and Technology, Luoyang 471003, China;

Zhixue Zhang
Network Information Center of Henan University of Science and Technology, Luoyang 471003, China;

Protocol Algorithm Design of Location Privacy Preserving for Sink Node Based on Security Area

Abstract

Abstract: In view of problems appear in location privacy protection for sink node of wireless sensor networks, *a location privacy preserving routing algorithm for sink node based on security area* was proposed. This protocol protected location privacy of sink node through methods such as *sending real package or fake package probabilistic from safe area to unsafe area and forming a circular sink area around the sink node*. Performance evaluation was compared between this proposed dynamic routing algorithm and existing one. Network simulation results show that the routing algorithm has advantages such as low energy consumption, small network delay, and high data transmission rate, and it can also make a good balance between location privacy protection of sink node and network energy consumption.

Keywords

location privacy protection, fake package, secure area, circular sink area

Recommended Citation

Li Peiyu, Zhang Zhixue. Protocol Algorithm Design of Location Privacy Preserving for Sink Node Based on Security Area[J]. Journal of System Simulation, 2015, 27(12): 2973-2980.

第 27 卷第 12 期 系统仿真学报© Vol. 27 No. 12
2015 年 12 月 Journal of System Simulation Dec., 2015

基于安全区域的汇聚节点位置隐私保护协议算法设计

李沛谕，张治学
（河南科技大学网络信息中心，河南 洛阳 471003）

摘要：针对无线传感器网络汇聚节点位置隐私安全问题，提出了一种*基于安全区域的动态路由算法*，通过*在非安全区域内向安全区域概率性发送数据包与虚假数据包以及在汇聚节点周围形成环形汇聚区域*等方法保护汇聚节点的位置信息。对提出的动态路由算法与现有的汇聚节点隐私保护算法进行性能比较，网络仿真实验结果显示本路由算法具有能耗小，网络时延小，数据传送成功率高等优点，可以实现汇聚节点位置隐私安全和网络能耗之间的较好均衡。

关键词：位置隐私保护；虚假包；安全区域；环形汇聚区域
中图分类号：TP393 文献标识码：A 文章编号：1004-731X (2015) 12-2973-08

Protocol Algorithm Design of Location Privacy Preserving for Sink Node Based on Security Area

Li Peiyu, Zhang Zhixue

(Network Information Center of Henan University of Science and Technology, Luoyang 471003, China)

Abstract: In view of problems appear in location privacy protection for sink node of wireless sensor networks, *a location privacy preserving routing algorithm for sink node based on security area* was proposed. This protocol protected location privacy of sink node through methods such as *sending real package or fake package probabilistic from safe area to unsafe area and forming a circular sink area around the sink node*. Performance evaluation was compared between this proposed dynamic routing algorithm and existing one. Network simulation results show that the routing algorithm has advantages such as low energy consumption, small network delay, and high data transmission rate, and it can also make a good balance between location privacy protection of sink node and network energy consumption.

Keywords: location privacy protection; fake package; secure area; circular sink area

引言

无线传感器网络中汇聚节点承担了从各个传感器节点中收集信息的重要责任，是数据的存储、处理和分析中心，所有传感器节点所采集到的信息都首先传输到汇聚节点进行初步的分析处理。一旦汇聚节点的位置信息被恶意节点获取攻击并破坏，将导致整个网络的瘫痪。而汇聚节点位置隐私保护比源节点位置隐私保护更具挑战性的原因也是由于汇聚节点的特殊性质导致的，攻击者可根据汇聚节点的特性较容易的推测找到汇聚节点的位置。因此，保护汇聚节点的位置隐私十分重要。

在无线传感器网络中使用传统的单一路径或多路径路由并不能保证汇聚节点的位置隐私安全，例如幻影路由[1-2]可以较好的保护源节点的位置隐私却忽略了汇聚节点的位置隐私保护。而广播路由协议[3-5]可以实现对汇聚节点位置隐私的保护，但

收稿日期：2014-07-04 修回日期：2015-04-23；
基金项目：河南省科技攻关项目(112102210186)；
河南省科技厅重点攻关项目(132102210246)；
作者简介：李沛谕(1988-)，女，河南南阳，硕士，助教，研究方向为网络性能改善、网络与信息安全与数据分析；张治学(1963-)，男，四川达州，实验师，研究方向为网络性能改善与数据挖掘。

如果在路由选路的过程中每次转发都发送广播包的话，网络能耗较大，不利于大型传感器网络的部署。位置隐私路由协议(LPR)[6-7]避免了洪泛路由，但是由于在源节点开始发包的全部路由过程中时都概率性产生垃圾包，容易导致网络通信拥塞，网络能耗也较大。在一些虚假汇聚节点路由协议[8-9]中，传感器节点只向假汇聚节点发包，所有假汇聚节点在一跳范围内发送广播包，此协议的网络能耗同样较大。而另一些伪汇聚节点协议[10]是在不同的网络分区中各设立一个簇头节点，所有的簇头节点都扮演汇聚节点的功能，并且都能收到整个网络的全部数据，但只有一个簇头节点是真正的汇聚节点，这类协议虽隐藏了汇聚节点的位置隐私却更大概率的暴露了数据隐私的安全，攻击者破获任意一个簇头节点都将获取全网信息。这就需要协议设计者在位置隐私与数据隐私上做到较好的平衡。位置 k-匿名[11-12]算法中每个节点同时要向 k 个邻居发包，网络能耗较大，且算法复杂度较高，对普通传感器节点的计算分析能力以及能量要求较高。因此，位置隐私保护路由协议同样应该在网络能耗和网络安全之间做到较好的平衡。

1 模型构建

1.1 网络模型

网络模型有以下网络环境及假设：

(1) 整个无线传感器网络由 m 个环形区域构成，sink 位于区域中心。网络可用多跳通信形成的连通图 G(V, E)来表示，其中的顶点 v(v∈V)表示无线传感器网络中的节点，边 e(e∈E)表示节点间的通信链路[13]。

(2) 在网络最初的配置阶段，默认网络是安全的，在此阶段传感器节点向周围的邻居节点发送 HELLO 消息，与其交换位置信息，此时汇聚节点收集网络拓扑结构。

在基于安全区域的汇聚节点位置隐私保护的网络模型中有 4 个关键区域：

(1) 源节点 Circle-source 区域：本区域半径 R_{sa} 表示源节点开始使用保护汇聚节点路由算法时距离汇聚节点的最远距离，这个距离一般是源节点通信半径 R_{source} 的 2 或 3 倍，半径大小可根据网络规模设定。

(2) 汇聚节点 Circle-sink 区域：表示汇聚节点的非安全区域，即在此区域内汇聚节点位置隐私被捕获的概率较高，此区域半径为 R_{sink}，这里设定 R_{sink}=2 / 3R_{sa}。

(3) 非安全区域(Area-ns，non-secure area)：Circle-source 和 Circle-sink 两个区域的重合区域为网络节点数据发送的非安全区域。

(4) 安全区域(Area-s，secure area)：在 Circle-source 范围内除非安全区域之外的属于安全区域。

Circle-source 区域半径 R_{sa} 一般选择是源节点通信半径的 2 或 3 倍，是为了在网络能耗和安全性之间得到较好的均衡。R_{sa} 过大会导致路由算法过早进入产生虚假包的高能耗阶段，消耗过多的网络能量；而 R_{sa} 过小会导致汇聚节点被追踪到的可能性增大，网络安全性能达不到要求。因此在本协议算法中选取 R_{sa}=3R_{source}。

Circle-sink 区域为汇聚节点的最小安全区域，半径为 R_{sink}=2 / 3R_{sa}，这样使源节点在距离汇聚节点安全区域还有一段距离时，就开始进入汇聚节点保护算法运行阶段。以此保证汇聚节点位置隐私安全。网络模型如下图 1 所示。

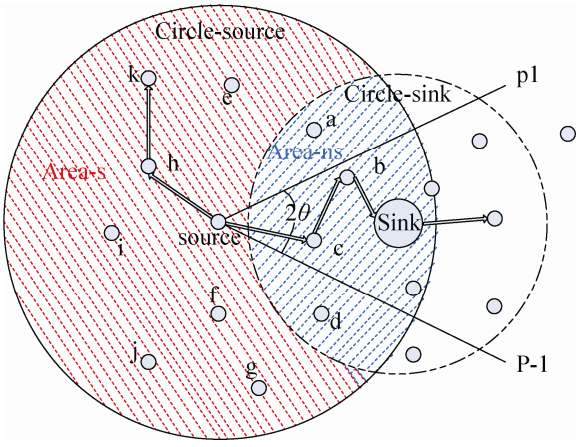

图 1 网络拓扑图

1.2 攻击模型

假设本网络结构中对汇聚节点的位置隐私攻击主要有以下 2 种：

(1) 攻击者通过统计分析全局数据接收率以及转发率得到汇聚节点的位置。这种攻击模式对攻击节点的性能要求比较高，攻击者既需要较高能量同时也需要有较强的计算能力。并且网络需要同时布置多个监控点，攻击成本也较大，因此，全局攻击模式的存在并不广泛。

(2) 攻击者根据包发送的时间顺序来判断传感器节点的传输路径，逐跳移动，最终获得汇聚节点位置信息。这种攻击模式是无线传感器网络中应该抵御的主要攻击类型

2 汇聚节点位置隐私保护算法

2.1 算法描述

为了更全面的保护传感器节点的位置隐私安全，本文对源节点位置隐私保护协议(FS-DRP)[14]进行补充和改进，增加了汇聚节点的位置隐私保护算法，提出了一种基于安全区域的汇聚节点位置隐私保护动态路由协议(Dynamic Routing Protocol based on Secure Area，SA-DRP)，通过在非安全区域内向安全区域概率性发送数据包与虚假数据包以及在汇聚节点周围形成环形汇聚区域等方法保护汇聚节点的位置信息。

由于 FS-DRP 路由协议的网络能耗较低，因此，当源节点处在安全区域范围内时，选择使用 FS-DRP 路由协议发送包，只有当源节点位距离汇聚节点在一定的非安全范围之内时，才使用 SA-DRP 路由协议概率性发送虚假包，实现能耗与安全的良好平衡。

SA-DRP 汇聚节点位置隐私保护动态路由协议基本步骤具体如下：

1) 在普通节点端：

Step 1 判断当前节点是发送本节点所采集的数据，还是转发其他节点产生数据。若是发送本节点所采集的数据，执行 Step 2，否则算法执行 Step 3。

Step 2 检测当前节点与汇聚节点的距离是否在 Circle-source 区域的半径 R_{sa} 之内，如果不在则仍使用 FS-DRP 路由协议传递包，本算法结束。如果在 R_{sa} 之内则源节点执行 SA-DRP 路由协议，算法转向 Step 4。

Step 3 当前节点判断被转发包是否是虚假包。若是虚假包则算法执行 Step 6。若不是虚假包，则先判断生存时间 T_r 是否≥5，如果，$T_r \geq 5$，则 T_r-1，执行 Step 2；如果 $T_r < 5$，则选择通信半径内最远中继节点，以定向随机步发送数据至汇聚节点方向的邻居节点，并且以概率 P_f 产生虚假包向邻居节点发送。并对产生的虚假包设定适当的生存时间 T_f，来表示虚假包在被丢弃之前所走跳数。算法转向 Step 7。

Step 4 判断节点的通信半径内能不能达到安全区域，若真实包在发送的过程中距离汇聚节点较近，距离安全区域较远，导致节点通信半径内不能达到安全区域，那么此中继节点将直接发送包到汇聚节点，本算法结束。若能到达安全区域，则顺序执行 Step 5。

Step 5 节点选择以概率 P_s 发送真实包到安全区域，也就是以概率 P_{ns} 即 $1-P_s$ 发送到非安全区域。对真实包设置适当的生存时间 T_r，来表示真实包到达汇聚节点前所走的跳数。在发送真实包的同时，源节点以概率 P_f 产生虚假包向邻居节点发送。算法转向 Step7。

Step 6 检测虚假包生存时间是否为 0，若不为零，则将生存时间 T_f 域值减 1，当 T_f 为 0 时，当前传感器节点选择丢弃虚假消息。算法转向 Step 7。

Step 7 发送或转发包，算法结束。

2) 在汇聚节点端：

Step 1 如果是汇聚节点接收到包，同样也会以概率 P_f 产生虚假信息包，并向邻居发送。并且对产生的虚假包加上适当的生存时间 T_f。

2.2 算法参数分析

本算法中提到的以概率 P_s 向安全区域发送包，以概率 P_f 产生虚假包，配置虚假包的生存时间 T_f，这 3 个都是 SA-DRP 路由协议的自定义变量参数，因此需要根据实际情况计算分析出合适的取值。

在大多数传感器网络中，尽管网络总体趋势让是更多的包发向更靠近汇聚节点的位置，但网络数据发向节点各个方向的概率是比较相近的。在 SA-DRP 算法中，通过控制概率来控制发包情况。N_{ns} 是非安全区域内传感器结点个数，N_s 是安全区域内传感器结点个数，令两区域的结点个数比值为 ω=N_{ns} / N_s，由此可得，非安全区域内的某一节点得到数据的接收率是 $R_{ns} = P_{ns} / N_{ns}$，安全区域内的某一节点得到数据的接收率是 $R_s = P_s / N_s$，那么这两个区域的概率比值是 $R_0 = R_{ns} / R_s = (1 - P_s) / P_s\omega$。本模型中有 3 个自定义参数 P_s, T_f 和 P_f，如此以来可以建立 R_s 与 R_{ns} 之间的与参数 P_s, T_f 和 P_f 相关的函数：

$$R_s = F(P_s, T_f, P_f)R_{ns} \tag{1}$$

为了达到较高的扰乱性，本文期望非安全区域和安全区域内的某一节点得到数据的概率相同 $R_s = R_{ns}$，因此可以通过计算分析得到合适的参数 P_s, T_f 和 P_f 来满足方程：

$$F(P_s, T_f, P_f) = 1 \tag{2}$$

如果在发送真实包的同时，加入虚假包，R_{ns}' 表示发向非安全区域的真实包与虚假包的总体占通信区域内包总数的比率，R_s' 表示发向安全区域的真实包与虚假包的总体占通信区域内包总数的比率，R_{nsf} 表示发向非安全区域的虚假包占总包个数的比率，R_{sf} 表示发向安全区域的虚假包占总包个数的比率。所以有以下关系：

$$R_{ns}' = R_{ns} + R_{nsf} \tag{3}$$

$$R_s' = R_s + R_{sf} \tag{4}$$

当源节点向安全区域节点 h 发送数据，此时 $T_f = t$，那么在 $T_f = t + 1$ 时刻，另外一个节点 k 就会接收到来自安全区域的同样数量的包，如此推算到整个生存周期可以得到：

$$N_s R_{sf}(t) = N_{ns} R_{sf}(t + 1) \tag{5}$$

结合 N_s 和 N_{ns} 的关系，由 $\omega = N_{ns} / N_s$ 可得：

$$R_{sf}(t) = \omega R_{sf}(t + 1) \tag{6}$$

因此，由公式(5)和(6)可以得出在包的整个生存时间内累加发向安全区域的虚假包占总包个数的比率是：

$$R_{sf} = R_{sf}(T_f)\sum_{t=1}^{T_f}\omega^{t-1} \tag{7}$$

源节点每发送一个真实包都会以概率 P_f 产生一个虚假包，那么在生存时间 T_f 跳内安全区域虚假包传送率即 $R_{sf}(T_f)$ 可以通过以下方法的来：源节点向邻居节点发送的真实包是 $(N_{ns}R_{ns} + N_sR_s)$，在生存时间 T_f 跳内安全区域传送的虚假包是 $N_sR_{sf}(T_f)$，因此可得：

$$(N_{ns}R_{ns} + N_sR_s)P_f = N_sR_{sf}(T_f) \tag{8}$$

由 ω=N_{ns} / N_s 可得：

$$R_{sf}(T_f) = \omega(1 + \frac{P_s}{1 - P_s})P_f R_{ns} \tag{9}$$

因此，由公式(8)和(9)可以得出在包的整个生存时间内累加发向安全区域的虚假包占总包个数的比率是：

$$R_{sf} = \omega(1 + \frac{P_s}{1 - P_s})P_f R_{ns}\sum_{t=1}^{T_f}\omega^{t-1} \tag{10}$$

本算法的最终目的是通过 $R_s' = R_{ns}'$ 来确定函数 $R_s' = F(P_s, T_f, P_f)R_{ns}'$ 中 3 个参数的值的，因此由公式(2)可得：

$$\frac{\omega P_s}{1 - P_s} + \omega(1 + \frac{P_s}{1 - P_s})P_f\sum_{t=1}^{T_f}\omega^{t-1} = 1 \tag{11}$$

由公式(11)可以得出合适的自定义参数 P_s, T_f 和 P_f。协议可以针对不同的网络规模，以及实际需求，计算出最适合的网络参数，以达到最好的网络性能。

2.3 算法性能分析

在本网络模型中使用 SA-DRP 动态路由协议保护汇聚节点的位置隐私，网络的安全性和能耗强度主要是由安全区域和非安全区域中接收和发送真实包和虚假包之间的比率决定的，选取非安全区域内的节点所构成的路由路径是快速的节能的，但安全性却是较低的；相反，选取安全区域内的节点所构成的路由路径是耗能或冗余的，但却具有较高的安全性。当包在安全区域传递的比率越高时，网络耗能就越大，安全性越高，反之，当包在非安全区域传递的比率越高时，网络耗能就越小，安全性越高，实际应用中可以根据需求修改算法参数取值，在能耗与安全之间做到较好的平衡。

2.3.1 安全性分析

为了让包到达汇聚节点的时间较短，经历的跳数较少，算法中可以设置 $P_s \leqslant 50\%$。由于 $\omega = N_{ns} / N_s$，因此，ω 与网络安全性成反比，ω 的值越大，那么包传递到非安全区域的概率就越高，网络安全性就越小；相反，ω 的值越小，安全性越大。SA-DRP 汇聚节点位置隐私保护动态路由算法主要是通过以下几点来提高汇聚节点的位置隐私安全性。

首先，当源节点检测到自己与汇聚节点的距离在 Circle-source 区域的半径 R_{sa} 之内时，源节点以概率 P_f 产生虚假包，并把真实的包和虚假的包同时以概率 P_s 发送到里汇聚节点较远的安全区域(Area-s)，以概率 P_{ns} 发送到里汇聚节点较近的非安全区域(Area-ns)，这样的安全区域最终会形成一个安全环形区域，如图 2 所示。因此，当攻击节点追踪到当前节源节点时，无法判断真实的包被发送到哪个区域，以此可以防御攻击者通过分析包的发送时间顺序，来逐跳追踪获得汇聚节点位置信息。

其次，在 SA-DRP 路由协议中，当汇聚节点收到真实的包后，同时以概率 P_f 向邻居发送虚假包，以此来增大数据转发率，减小数据转发率与接收率之间的差距，避免攻击者通过全局流量分析得到汇聚节点的位置信息。

最后，为达到更高的安全性，算法使用环形汇聚区域模糊 Sink 节点的位置。环形汇聚区域是指：以 sink 节点为圆心，以 Circle-source 区域直径 $2R_{sa}$ 与 Circle-sink 区域半径 R_{sink} 的差值为半径，即 $R = 2R_{sa} - R_{sink}$ 为半径形成的区域。可以在安全区域环中周期性选定几个节点，例如下图 2 中的节点 a-i，网络设定把源节点产生的虚假包更多的传递给这几个固定节点，伪造这几个节点具有大量数据流向的假象，制造出多个类似于汇聚节点的混淆节点即网络热点(Hot Spot)，来保护汇聚节点的位置安全，网络热点可周期性更替。如下图中安全环型区域中的节点 b 与 k 等节点，他们被伪造成具有大量数据流向的混淆节点，这样不容易让攻击者通过全局数据流量判断出真实的汇聚节点。

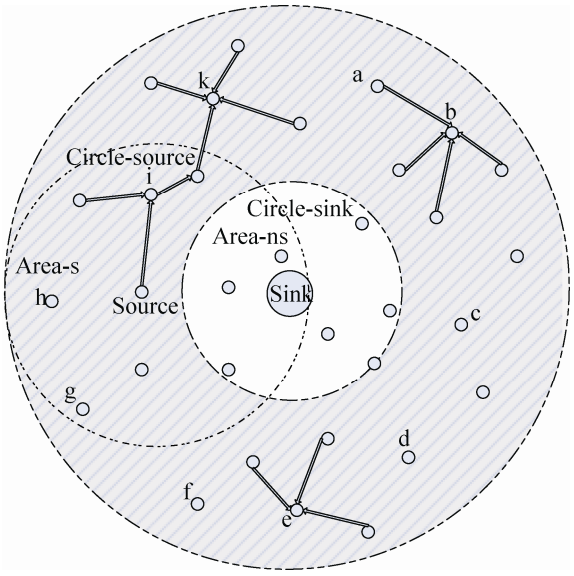

图 2 安全环形区域中的混淆汇聚节点

2.3.2 能耗耗分析

为了让包到达汇聚节点的时间较短，经历的跳数较少，减少网络能耗，算法中可以设置 $P_s \leqslant 50\%$。由于 $\omega = N_{ns} / N_s$，因此 ω 与网络能耗成反比，ω 的值越大，那么包按照离汇聚节点较近的路线传递的比率越高，网络耗能就越小，相反 ω 的值越小，能耗越大。SA-DRP 汇聚节点位置

隐私保护动态路由算法的网络开销是：

$$E = \frac{N_s R_s}{N_{ns} R_{ns}} = \frac{R_s}{\omega R_{ns}} \tag{12}$$

在数据传输的过程中，为了避免包在安全区域和非安全区域的往返多次传递，当节点转发的真实包进入使用 SA-DRP 算法的范围后，设置真实包的生存时间 T_r。如果，$T_r < 5$，那么转发节点将不再向安全区域发送数据，直接按照定向随机步路由协议进行路由选路，但选路过程仍以概率 P_f 产生虚假包。这样既避免路由路径的折叠往返，同时也也降低网络能耗。在本模型中，SA-DRP 算法的网络开销保持在<1 的范围内。

3 仿真实验

仿真场景设置为将 10 000~50 000 个传感器节点随机部署在 200m×200 m 的区域内，Sink 节点位于区域中心，传感器节点的通信半径设置为 30 m，并随机选取其中的 100 个传感器节点定期的向汇聚节点发送包，设定攻击者在距离汇聚节点 10 跳的位置。

仿真实验对位置隐私保护路由协议(LRP)、幻影路由协议(Phantom)和基于安全区域的汇聚节点位置隐私保护路由协议(SA-DRP)在网络能耗、安全时间、网络时延等方面进行了比较。实验仿真参数设置如表 1 所示。

表 1 OMNet++仿真参数设置

参数名称	参数值
E^{ele}	50×10^{-9} J /bit
ξ^{fs}	10 pJ/bit/m^2
E^{mp}	0.001 3 pJ/bit/m^4
网络区域	200 m×200 m
节点通信半径	30 m
节点数	10 000~50 000

本文通过两方面来测试本路由协议的安全性能：(1) 汇聚节点接收数据的安全时间，通过汇聚节被捕获到之前所接收的包数量来衡量；(2) 追踪者的攻击时间，通过追踪者捕获到汇聚节点之前所移动的跳数来衡量。

图 3 从能量消耗方面反映了本文中路由协议的网络性能，其中，网络节点密度为 0.75 个/m^2，虚假包发送概率为 0.3。从图 3 中可以看出，本文所提出的路由协议在能耗方面比位置隐私保护路由(LRP)网络性能优越，但能耗略高于 Phantom 路由。位置隐私保护路由(LRP)在包发送的全部路由过程中都不断地产生虚假包，这样不仅增加了网络能耗，并且会导致网络拥塞，加网络时延。但是，本文所提出的汇聚节点位置隐私保护路由协议(SA-DRP)中，包到达安全区域之前使用低能耗的 FS-DRP 路由协议，到达安全区域后通过发送虚假包，安全区域，虚假汇聚节点等方法很好的保证了汇聚节点的位置隐私，因此，安全性能高于 Phantom 路由，网络能耗低于位置隐私路由。

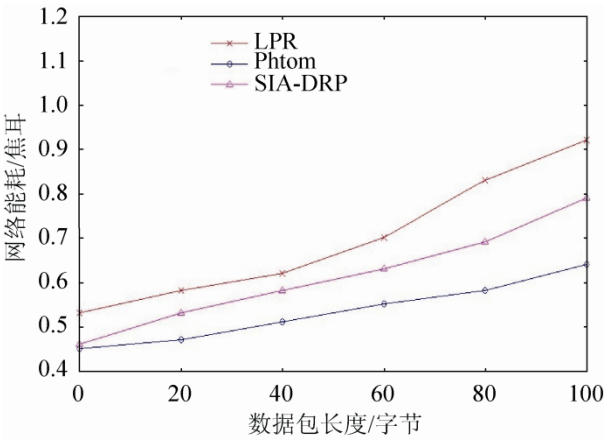

图 3 网络能耗比较

图 4 从网络时延这个方面对 Phantom、LRP 和 SA-DRP 路由协议进行比较。实验中设置包长度为 40 字节，虚假包发送概率为 0.3。在网络时延方面，随着节点密度的增大，网络中节点间的距离就会减小，安全区域和非安全区域内路由路径跳数增多，因此节点密度的的增加会导致网络时延的上升。虽然 SA-DRP 路由路径中使用 FS-DRP

路由协议那部分的网络时延是会随着网络节点的密度增加而降低的，但由于之后部分使用虚假包使网络时延增加，因此整体的平均网络时延随着节点密度的增加呈上升趋势。

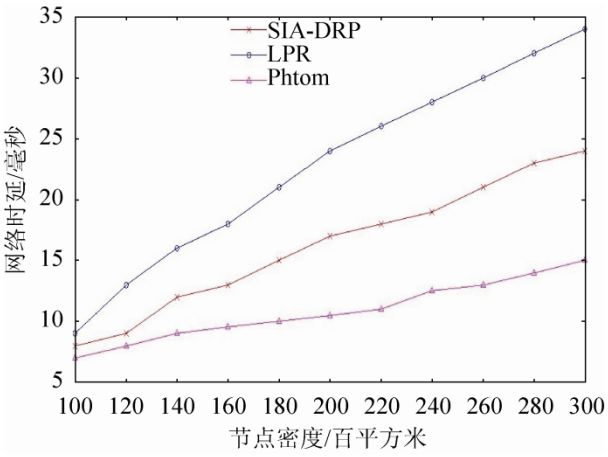

图 4 节点密度对网络时延的影响

总的来说，在安全区域内开始产生虚假包可以保护汇聚节点的位置信息不被披露，并且隐私保护程度与在整个路由过程都使用虚假包所提供的隐私保护程度区别并不大，但能耗却大大降低，因此 SA-DRP 路由协议网络性能更好。

图 5 从虚假包发送概率对网络安全时间的影响这个方面对三种路由协议进行比较，网络安全时间即在被捕获前汇聚节点的收包数量，设置网络节点密度为 0.75 个/m^2，包的长度为 40 个字节。可以看出随着虚假包产生概率的增加，汇聚节点在被捕获前接收的包的数目增多，因此汇聚节点的位置隐私安全时间增长。而 Phantom 路由协议的网络安全时间较低，是由于 Phantom 路由协议没有加入虚假包机制，不能很好地保护汇聚节点的位置信息安全，导致汇聚节点很容易被追踪捕获。LRP 的安全时间低于 SA-DRP 路由协议是由于 LRP 路由协议忽略了对源节点的隐私保护。由于在源节点中同样存在关于汇聚节点位置信息，对汇聚节点的位置安全也是一种威胁。因此 SA-DRP 路由协议在安全性能上有较好的表现。随着虚假包产生概率的增大，网络安全性也会随之提高。在实际应用中，可以通过加大 P_f 来提高安全性；反之减小 P_f 以减小网络能耗，以此实现安全与能耗之间的均衡。

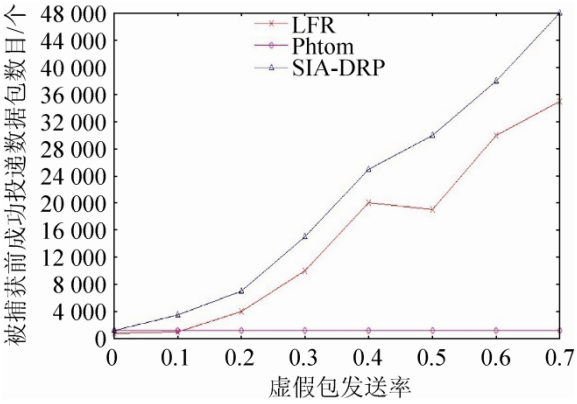

图 5 虚假包的发送概率对网络安全时间的影响

4 结论

针对 Phantom 和 LRP 路由协议在保护汇聚节点位置隐私方面存在的安全性能较低，网络能耗大的缺点，本文提出了一种基于安全区域的汇聚节点位置隐私保护协议(SA-DRP)。本协议首次引入安全区域与非安全区域的设计，以及在非安全区域内向安全区域概率性发送虚假数据包的机制，既保证了无线传感器网络数据传输的安全性，同时在网络能耗上做了很好的平衡。本文首先对汇聚节点位置隐私保护网络模型进行概述。然后，给出 SA-DRP 算法的设计与流程，通过在安全区域和非安全区域概率性发送包以及汇聚节点转发虚假包等方法保护汇聚节点的位置信息，并针对一些主要的攻击模型分析了本路由协议的安全性与网络能耗强度。最后，通过仿真实现了该路由协议，并对本动态路由协议的安全性能、能量消耗、网络时延、网络安全时间等网络性能进行了全面的实验仿真与分析比较。实验结果表明，SA-DRP 算法可以实现源节点位置隐私安全和网络能耗之间的均衡，扰乱攻击者对汇聚节点位置的追踪，路由算法具有能耗小，网络时延小，数据传送成功率高等优点。

参考文献:

[1] Kamat P, Zhang Y, Trappe W, *et al*. Enhancing source-location privacy in sensor network routing [C]// Proceedings-25th IEEE International Conference on Distributed Computing Systems, Columbus, OH, USA. USA: IEEE, 2005: 599-608.

[2] Yao J, Wen G. Preserving source-location privacy in energy-constrained wireless sensor network [C]// Proceedings of the 28th International Conference on Distributed Computing Systems Workshops, Beijing, China. Beijing, China, Institute of Electrical and Electronics Engineers Inc, 2008: 412-416.

[3] Chen R, Yu C, Wu T. A Small-World Routing Protocol and the Effect of Pass-Over for Wireless Sensor Networks [J]. Wireless Personal Communications (S09296212), 2013, 68(4): 1493-1523.

[4] Zungeru A, Seng K, Ang L. Energy Efficiency Performance Improvements for Ant-Based Routing Algorithm in Wireless Sensor Networks [J]. Journal of Sensors (S1687725X), 2013(4):572-575.

[5] Intanagonwiwat C, Govindan R, Estrin D. Directed Diffusion: A Scalable and Robust Communication Paradigm for Sensor Networks [C]// Proc. ACM MobiCom, 2000, Boston, MA, USA. USA: ACM, 2000: 56-67.

[6] Jian Y, 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 (S15361276), 2008, 7(10): 3769-3779.

[7] Jian Y, Chen S, Zhang Z, Zhang L. Protecting Receiver-Location Privacy in Wireless Sensor Networks [C]// IEEE INFOCOM 2007: 26th IEEE International Conference on Computer Communications, Anchorage, Anchorage, AK, USA. USA: IEEE, 2007: 1955-1963.

[8] Kiran M, Liu D, Matthew W. Location privacy in sensor network against a global eavesdropper [C]// 15th IEEE International Conference on Network Protocols, ICNP, China. USA: IEEE, 2007: 314-323.

[9] William C, Abdelzaher T, Nahrstedt K. Using Data Aggregation to Prevent Traffic Analysis in Wireless Sensor Networks [C]// 2nd IEEE International Conference - Distributed Computing in Sensor Systems, DCOSS 2006, San Francisco, CA, USA. USA: IEEE, 2006: 202-217.

[10] Chiu W, Chen B, Yang C. Robust relative location estimation in wireless sensor networks with inexact position problems [J]. IEEE Transactions on Mobile Computing (S15361233), 2012, 11(6): 935-946.

[11] Machanavajjhala A, Kifer D, Gehrke J, Venkitasubramaniam. L- diversity: Privacy beyond k-anonymity [J]. ACM Transactions on Knowledge Discovery from Data (TKDD) (S1556-4681), 2007, 1(3): 24-35.

[12] Marco G, Grunwald D. Anonymous usage of location-based and services through spatial and temporal cloaking [C]// Processing of the International Conference on Mobil e Systems, Applicat MobiSys. San Francisco, California, USA: International Conference on Mobile Systems, 2003: 163-168.

[13] Han JQ, Zhao W, Zheng M. An analytical model on unbalanced energy consumption in large scale wireless sensor network [C]// The 3rd International Conference on Measuring Technology and Mechatronics Automation, Shanghai, China. USA: IEEE, 2011: 375-378.

[14] Li FY, Li PY, Gao FX, *et al*. Location privacy protection for wireless sensor networks based on fan-shaped region [J]. Journal of Northeastern University (S10053026), 2013, 34(1): 21-24, 34.