

# 电力物联网下无线传感器网络位置隐私保护方法研究

华 晔，张 涛，王玉斐，黄秀丽

(中国电力科学研究院，江苏 南京 211106)

**摘 要：**本文中，我们首先对无线传感器网络的概念及其在电力物联网中的应用进行了简单的介绍，指出了无线传感器网络中存在的隐私问题；其次针对位置隐私保护进行了概述，并给出了攻击者模型；接下来，分别介绍了几种源节点位置隐私保护和汇聚节点位置隐私保护技术，并对它们的性能进行了分析和比较；最后，我们对电力物联网中的无线传感器网络位置隐私保护技术所需考虑的问题提出了见解和建议。

**关键词：**电力物联网；无线传感器网络；关键节点；位置隐私；保护

## 0 引言

无线传感器网络(Wireless Sensor Network, WSN)是将大量微型化的传感器分布在需要监测的区域内，每个传感器为一个节点，这些节点之间通过电磁波信号进行通信，组成一个多跳、自组织的网络系统<sup>[1]</sup>。无线传感器网络各个节点之间相互协作地感知网络覆盖区域内的被监测对象，采集和处理相关的数据并传输给观测者。无线传感器网络具有规模大、自组织、多跳路由、动态性、资源受限、以数据为中心、应用相关等特点，目前已广泛应用于军事、环境监测、医疗、工业控制等领域<sup>[2]</sup>。

在电力物联网中，无线传感器网络也已被应用于多个方面，如：远程抄表、变电站自动化、配电网继电保护、配电线路故障定位、输电线路在线监测等<sup>[3]</sup>。其中，输电线路在线监测是无线传感器网络在电力物联网中的典型应用。输电线路在线监测，主要用于监视特高压输电线路的运行状况、诊断输电线路设备状态。系统通过各种传感器，可以探测输电线路及其所处环境的状态数据，如：温度、湿度、风向、风速、污秽、覆冰状况、应力状况、视频图像等，并在多信息集成与融合条件下进行线路故障检测和管理。将无线传感器网络节点部署在输电线路路上，传感器网络网关部署在杆塔上，可对大跨距输电线路进行状态监测，进行灾害预警，为线路数字化和全网可视化奠定基础。

随着无线传感器网络应用领域的增多，网络中的隐私问题也越发明显。隐私威胁直接影响到无线传感器网络的部署与应用，目前已被人们广泛关注。隐私保护已在一些领域被广泛研究，如：数据库、有线网络、无线网络和数据挖掘等。但在无线传感器网络中，环境的不可控、节点资源受限和拓扑限制是对隐私保护的挑战，相关研究还处于起步阶段，有诸多问题尚待解决。无线传感器网络的隐私保护主要涉及三个方面：数据隐私保护、位置隐私保护和身份隐私保护。其中，位置隐私保护的主要任务是保护网络中的关键节点，防止攻击者获知它们的物理位置，并发起攻击。在输电线路在线监测中，对无线传感器网络的关键节点进行位置隐私保护是十分必要的，它是整个监测系统有效工作，保证线路正常、安全运行的前提。

## 1 无线传感器网络中的位置隐私保护

在无线传感器网络中，必须对关键节点的位置隐私进行保护，防止攻击者针对这些节点发动攻击。网络中的关键节点在网络中具有重要的地位，比普通节点承担了更多的责任。一旦关键节点的位置被攻击者知道，攻击者就可对其发起攻击，从而对网络造成极大的破坏。无线传感器网络中的位置隐私保护对象主要是源节点和汇聚节点<sup>[4]</sup>。

### 1.1 源节点的位置隐私保护

源节点收集被监控对象的信息，并在网络中传播所采集的数据，将其发送至汇聚节点，它通常是离被监控对象最近的节点，其位置的暴露会直接导致被监控物体的暴露。源节点采集的数据要发往汇聚节点，必然会形成一条或多条由源节点到汇聚节点的路径，外部攻击者能够通过反向追踪数据包找到源节点的位置。完全避免攻击者窃听数据，追踪源节点的位置是不可能的，目前源节点的位置隐私保护研究

重点是如何延长攻击者追踪到源节点的时间，为网络提供更好的安全性能。

### 1.2 汇聚节点的位置隐私保护

与源节点一样，汇聚节点也是无线传感器网络中的关键节点。汇聚节点是无线传感器网络与外部网络连接的网关，源节点采集的数据通过汇聚节点发送给观测者，同时，汇聚节点还负责向整个网络发布检测任务。如果汇聚节点的位置被攻击者得到，进而被破坏，则会导致整个网络的瘫痪。由于数据包通常按照一定的路由路径由源节点发往汇聚节点，网络中的通信流量模式会呈现出不对等性，越接近汇聚节点的节点，流量就越大，汇聚节点的流量在全网中最高，攻击者很容易通过流量分析方法获得汇聚节点的位置。

### 1.3 攻击者模型

无线传感器网络位置隐私保护问题中的攻击者分为两类：内部攻击者和外部攻击者。内部攻击者掌握了数据包的交换格式和语义，可以破解在网络中传输的数据包的内容。外部攻击者无需破解数据包的内容，只需通过监听网络中的通信，即可根据有无数据流，数据流的大小和信号来源等获取位置隐私。内部攻击的难度较大，而外部攻击相对来说较为容易。目前，针对无线传感器网络位置隐私的攻击者最常见的就是外部攻击者，又分为逐跳追踪数据包传输的攻击者（局部攻击者）和流量分析的攻击者（全局攻击者）。本文主要考虑针对外部攻击者进行位置隐私保护的情况。

#### 2.3.1 逐跳追踪源节点位置的攻击者

攻击者通过无线信号定位装置监控一定范围内的数据包传输行为，监听的范围通常为一跳传输范围，其通过与数据包传输方向相反的方向追踪源节点的位置。攻击者首先处于汇聚节点附近，监听局部区域内的无线信号，当检测到一个新的信号后推测出该信号发送节点的位置，之后移动到这个节点处继续监听，直到以逐跳的方式追踪到源节点位置。图 1 描述了攻击者反向追踪源节点位置的过程：攻击者首先位于汇聚节点处，当其探测到数据包 m1 后，利用无线信号定位装置推断出 m1 是由 B 节点发来的，则移至 B 节点处继续监听，接着其又探测到数据包 m2，并推断出是由 A 节点发来的，又移往 A 节点处继续监听。只要源节点发送的数据包足够多，攻击者总能监听到数据包，进行反向追踪，不断接近源节点。

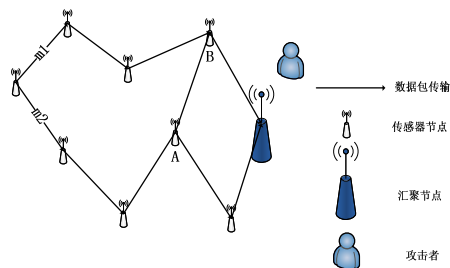


图 1 攻击者反向追踪源节点位置

#### 2.3.2 逐跳追踪汇聚节点位置的攻击者

攻击者以这种方法追踪汇聚节点位置的时候，根据数据包发送的时间顺序判断传输路径上的节点，逐跳移动到汇聚节点。图 2 是对追踪过程的描述：首先，攻击者位于节点 A，监听一跳范围内的信号传输，当监听到 A 向外发送了一个数据包，随后节点 B 也发送了一次数据包后，攻击者可推断出链路 A->B 必然在本次数据传输路径上，节点 B 的位置暴露，攻击者移至节点 B 处继续监听，直到追踪到汇聚节点。

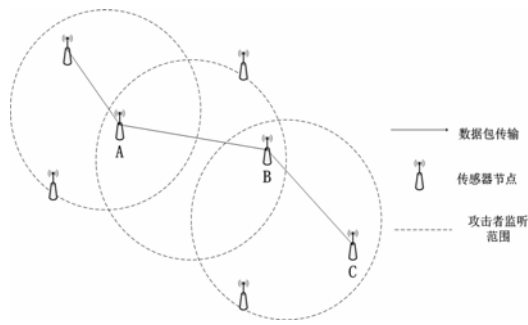


图2 逐跳追踪汇聚节点的方式

### 2.3.3 流量分析攻击者

流量分析攻击者可以对整个网络的无线通信进行监控，攻击能力很高。攻击者在网络中布设大量的廉价监控设备来进行全局监控，通过观察分析网络中通信流量的模式，可定位出源节点或汇聚节点的位置。

## 2 无线传感器网络位置隐私保护技术

目前已有的位置隐私保护策略主要分为三类：随机路由策略、垃圾包策略和伪装策略。在随即包策略中，每次发送数据包时，不是从源节点向汇聚节点的方向传输，而是以一定的概率向远离汇聚节点的方向传输，并且随机生成每个数据包的传输路径。由于这个过程增加了传输路径的长度，攻击者必须等待较长的时间才可监听到无线信号继续追踪，网络的安全时间得以延长；垃圾包策略的主要思想是在网络中加入垃圾包，通过混淆攻击者，使其不能正确区分数据包和垃圾包，从而将其引入错误的位置，延长追踪时间；伪装策略通过在网络中安置能够模拟被保护节点行为的假节点，从而将攻击者引向远离真实目标节点的错误位置。在本章节中，我们对典型的源节点和汇聚节点的位置隐私保护方法分别进行了研究。

### 2.1 源节点位置隐私保护方法

#### 2.1.1 洪泛法

洪泛法包括基线洪泛和概率洪泛两种。基线洪泛在每个传感器节点收到自己邻居节点发来的数据包后，将数据包向它其他所有的邻居节点广播。基线洪泛需要所有传感器节点参与数据包的传播，攻击者无法通过传输路径追踪到源节点。但是，基线洪泛法对隐私保护的效力严格依赖于源节点到汇聚节点的路径上的节点数量。太短的路径会导致攻击者在探测到第一个到达汇聚节点的数据包后即可推测出这个包的路由路径是源节点到汇聚节点间最短的路径，然后，攻击者在这条路径上追踪上一个节点，直到发现源节点。基线洪泛需要额外消耗大量的能量，大大降低了无线传感器网络的生命周期。

概率洪泛可用来解决基线洪泛带来的不足。在概率洪泛中，不需所有节点参与数据包的传输，节点通过一个预设定的概率来转发/广播其收到的数据包。这个方法在保证攻击者不能轻易追踪到源节点的同时降低了网络能量消耗。不过，随机性的存在也使得汇聚节点能否接收到数据不能得到保证。

#### 2.1.2 随机路由

幻影路由协议在数据包的传输时引入随机转发过程。数据包由源节点传输至汇聚节点的过程分为两步：第一步是进行随机转发，可以是完全随机的转发，也可是指定跳数或传输角度的有指导的随机转发。通过这一步，为数据包寻找一个假源节点；第二步，使用洪泛方式或最短路径方式，将数据包发往汇聚节点。在第一步中，完全随机转发只会使得数据包在源节点四周徘徊，并不能真正远离源节点；使用定向随机转发机制可将路径尽可能地拉直，使假节点远离真实源节点。其中，定向随机转发包含基于区域的定向随机转发和基于跳数的定向随即转发。在第二步中，使用洪泛将消耗较多的能量，而且攻击者更容易捕捉到数据包，更快地追踪到源节点；而使用最短路径方法可以克服这些问题，为网络带来更长的生命周期和安全时间。

双向贪婪随机转发也是一种随机路由机制<sup>[5]</sup>。它的主要思想是：先由汇聚节点发起一个一定跳数的

随机步，处于这个随机步路径上的传感器成为感受器；随后，源节点将数据包随机发送，当数据包到达某一个感受器时，它将沿着汇聚节点之前建立的路径传输至汇聚节点。

### 2.1.3 环路陷阱路由协议

垃圾包策略可以迷惑攻击者，保护源节点的位置隐私。环路陷阱路由协议是一种典型的垃圾包策略，通过网络中预设的垃圾包环路达到迷惑攻击者，妨碍其追踪的目的。网络预布置阶段，节点以一定的概率建立起一些环路，数据包在传输时，源节点沿最短路径向汇聚节点发送数据，当路径上的某个点也是某个环路上的点时，则激活所有经过这个节点的环路，并在环路上以同样的速率方发送垃圾包。由于外部攻击者不可破解数据包，因而无法根据包的内容分辨真实数据包和垃圾包，其会以一定的概率被吸引至预先设置的环路上，然后在环路上持续追踪，直至再次回到数据传输路径上。这样，延长了攻击者从汇聚节点追踪到源节点的时间。但是发送垃圾包会额外消耗较多的能量，并且通过持续追踪，攻击者依然能够回到真实的数据传输路径上来，而静态预设环路无法阻止能力较强的攻击者。

### 2.1.4 假源节点策略

通过选择一个或多个传感器节点，使其模拟源节点的行为，从而迷惑攻击者，达到保护源节点位置隐私的目的。假源节点的数目越多，则隐私保护的效果越好，但是过多的假源节点会给无线传感器网络造成较多的额外能量消耗。并且，如何模拟源节点的行为而不被攻击者察觉，是一个尚待解决的问题。

## 2.2 汇聚节点位置隐私保护方法

### 2.2.1 重加密策略

数据重加密技术类似于传统无线网络中的匿名技术，数据包在路由路径上传输时被逐跳进行重加密。重加密技术通过改变数据包的外表达达到保护汇聚节点位置隐私的目的<sup>[6]</sup>。

### 2.2.2 多父节点路由

在多父节点策略中，每个传感器节点随机选择它的一个父节点作为下一跳，向汇聚节点传输数据。使用多父节点策略可以平衡父节点和子节点之间的流量，从而使攻击者无法轻易判断哪个节点更靠近汇聚节点，也就无法通过监听数据的传输追踪到汇聚节点。

### 2.2.3 伪造汇聚节点

无线传感器网络的流量模式具有不对等性，高流量区域总是出现在汇聚节点周围，使得攻击者可以通过流量分析确定汇聚节点的位置。使用伪造汇聚节点协议，在网络中设置多个假汇聚节点，采集到数据后先进行一次数据融合，然后发送给假汇聚节点，假汇聚节点对数据进行第二次融合，最后将两次融合后的数据发送至汇聚节点。多个假汇聚节点分担了指向真实汇聚节点的流量，网络中出现多个高流量的区域，从而攻击者无法判断出真实汇聚节点的位置。协议对汇聚节点位置隐私保护的有效性取决于假汇聚节点的数量，假汇聚节点数量较少时，攻击者依然可以以较大的概率追踪到汇聚节点，同时，攻击者对假汇聚节点的攻击会使得假汇聚节点处的数据丢失。

### 2.2.4 随机路由

协议根据一个节点的邻居节点距离汇聚节点的跳数将它们划分至两个表格中：远邻居节点表和近邻居节点表。传感器节点在传输数据的时候，以一定的概率 $Pr$ 随机从两个表格中选择下一跳节点，或以 $(1-Pr)$ 的概率随机发送数据，这样大大降低了攻击者成功进行分析的可能性<sup>[7]</sup>。但是方法也带来了额外的能耗，且不能保证汇聚节点成功接收数据包。

### 2.2.5 位置保护路由协议

位置保护路由协议的思想是：将传感器节点的邻居节点划分为远邻居集合和近邻居集合，节点收到数据包后以一定的概率随机选择一个远邻居节点作为下一跳。因此，攻击者无法判断数据包的下一跳是否趋向于汇聚节点。同时，在位置保护路由中加入了假包策略，节点向下一跳发送数据包的同时，以一定的概率  $P_{fake}$  发送一个垃圾包给它的远邻居节点，攻击者可能被垃圾包引到错位的方向。为了不使网络额外消耗过多的能量，策略为假包设置了一个最大传输跳数  $TTL$  (Time To Live)，当假包的传输跳数等于最大跳数时，则丢弃该假包。结合垃圾包策略的位置保护路由协议能够有效防御攻击者追踪数据包

定位汇聚节点。

2.2.6 有差分的分支路由协议

有差分的分支路由协议通过使用多种去除流量相关性的协议来保护汇聚节点的位置隐私。当节点收到数据包时，它以  $Pr$  的概率将包发送给它的父节点，而以  $(1-Pr)$  概率进行随机转发。 $Pr$  通常大于 50%，以确保网络的额外消耗不会过大。同时，转发节点根据自己当前流量的大小以不同的概率产生假包，并在网络中有选择性地转发，在汇聚节点之外形成了高流量的区域，平衡了网络中的流量。这种方法既可以使逐跳追踪数据包的攻击者无法判断汇聚节点的位置，又能以网络中的多个高流量区域迷惑流量分析攻击者。但是这种方法的缺点是会导致网络较多的额外能量消耗，缩短网络生命周期。

2.2.7 随机选择发送时间

攻击者可以通过一个传感器节点发送数据时，它的邻居节点接收到数据的短时间间隔计算出父节点和子节点的关系。可通过一种方法，将时间段  $T$  分成  $m$  个部分，此时一个传感器节点有 1 个父节点和  $(m-1)$  个子节点。节点为其子节点分配时间段，每个传感器节点将在它的时间段中选择一个随机时间发送数据 [8]。

3 无线传感器位置隐私保护技术分析比较

上一章节，我们分别对典型的源节点位置隐私保护和汇聚节点位置隐私保护技术进行了研究。本章节中，将对这些技术的性能进行评价和比较。我们选择了以下四种指标来评价各种位置隐私保护方法的性能：隐私保护的程度、精确度、延时情况、额外能量消耗情况。其中，精确度包含了以下两个方面：

（1）汇聚节点获得数据的精确度，（2）数据成功传送至汇聚节点的可能性；延时情况包括了中间节点传输数据时的计算和通信时间；额外能量消耗情况指的是隐私保护方法采用的技术给无线传感器网络带来额外的能耗情况。表 1 从以上 4 个方面对本文提到的无线传感器网络位置隐私保护方法的性能进行了分析。

表 1 各种位置隐私保护技术的性能分析

位置隐私保护方法	隐私保护程度	精确度	时延情况	额外能耗情况
洪泛法（保护源节点）	对于基线洪泛：可以很轻易地找到汇聚节点和源节点之间的最短路径。 对于概率洪泛：依赖于预先设置的概率。	对于基线洪泛：保证数据达到基站。 对于概率洪泛：不保证数据到达基站。	对于概率洪泛而言：不保证数据在最短路径上进行传输。	额外能量消耗主要在于在全网上进行洪泛。
随机路由（保护源节点）	使得攻击者不容易发现真正的源节点。	对于幻影路由：数据百分之百可以到达基站。 对于贪婪随机步：数据的到达依赖于两条路径的交叉点。	对于幻影路由：依赖于随机步的跳数。 对于贪婪随机步：依赖于游走的随机性。	额外能量消耗主要在于随机步。
环路陷阱路由协议（保护源节点）	可将攻击者引到错误的路径上，延长其追踪到源节点的时间。	对数据的到达和精确度没有影响。	延迟真实数据的到达，以使得它的传输速率与假包的传输速率一致。	额外能量消耗主要在于注入和传输假包。
假源节点策略（保护源节点）	将攻击者的注意力从真实源节点处转移。	对数据的到达和精确度没有影响。	没有额外的延迟。	额外能量消耗主要在于由假源节点产生虚假的数据。
逐跳重加密（保护	对数据进行重加密，	对数据的到达和精确度没有影响。	中间节点对数据进行加密和解	没有额外的能量消耗。

汇聚节点)	改变数据包的外表 对汇聚节点位置隐私进行保护。	密需要花费时间。		
多父节点路由(保护汇聚节点)	使用多条路由路径发送数据。	对数据的到达和精确度没有影响。	没有额外的延迟。	没有额外的能量消耗。
伪造汇聚节点(保护汇聚节点)	使用多个假汇聚节点分担真实汇聚节点的流量,使得攻击者无法判断真实汇聚节点的位置。	攻击者对假汇聚节点的攻击会造成部分数据的丢失。	没有额外的延迟。	假汇聚节点处的数据融合会带来能量消耗。
随机路由(保护汇聚节点)	依赖于选择父节点作为下一跳的概率。	对数据到达没有保证,依赖于所选的概率。	依赖于所选择的下一跳。	额外能量消耗主要在于随机步。
位置保护路由(保护汇聚节点)	攻击者无法判断下一跳是否接近汇聚节点,并有可能被垃圾包引向错误的方向。	对数据的到达和精确度没有影响。	依赖于所选择的下一跳。	额外的能量消耗主要在于随机选择下一跳节点以及传输垃圾包。
有差分的分支路由(保护汇聚节点)	使用随机转发和垃圾包策略,能够同时防御逐跳追踪的攻击者和流量分析攻击者。	对数据的到达和精确度没有影响。	依赖于所选择的下一跳。	额外的能量消耗主要在于随机选择下一跳节点以及传输垃圾包。
随机选择发送时间(保护汇聚节点)	使得父节点和子节点的关系模糊不清。	对数据的到达和精确度没有影响。	在每个时间片段上随机选择传输时间。	时间段控制的同步需要消耗较少的能量。

4 电力物联网下无线传感器网络位置隐私保护

无线传感器网络在电力物联网中的一个典型的应用就是输电线路在线监测。在输电线路在线监测系统中,无线传感器网络的源节点负责采集与线路有关的各种数据,并将这些数据通过多跳网络发送至汇聚节点。如果源节点的位置被攻击者知道,攻击者就有可能对节点进行攻击,节点的失效将会导致网络不能及时、准确地获取监测线路的状态,系统无法对线路的故障做出应急处理。汇聚节点是连接无线传感器网络和外部网络的网关,负责对源节点发来的数据进行分析 and 融合,并发送给管理者。对汇聚节点进行破坏或孤立会造成整个网络的故障,从而导致在线监测系统失去对线路的有效监测。因此,对输电线路在线监测系统中无线传感器网络的源节点和汇聚节点进行位置隐私保护十分重要。

通过对本文提出的位置隐私保护技术进行分析和比较,可以看出:(1)不同的位置隐私保护技术对关键节点都起到了保护其位置隐私的作用,延长了网络的安全时间,但是不同的技术对位置隐私的保护效果有所不同;(2)使用某些技术可能会延长汇聚节点收到数据的时间,甚至汇聚节点不能顺利接受数据;(3)无线传感器网络在位置隐私保护上的主要代价是能量的消耗,多数方法都需要额外的能量消耗。

在输电线路在线监测系统必须考虑:(1)源节点和汇聚节点的位置隐私被有效保护;(2)汇聚节点必须能够顺利地接收到线路的监测数据;(3)汇聚节点必须在规定的时间内接收到线路的监测数据;(4)整个无线传感器网络的额外能量消耗不能过大,以保证网络的生命周期。因此,选择位置隐私保护方法时需要综合考虑,如:对于源节点的位置隐私保护,可选择假源节点机制,对于汇聚节点的位置隐私保护,位置保护路由和有差分的分支路由将是不错的选择。

无线传感器网络位置隐私保护仅仅是处于一个起步的阶段,有很多问题尚待解决,如:如何减少网络中的能量消耗,如何为网络获得更高的安全时间,如何保护动态节点的位置隐私等。结合无线传感器网络在电力物联网中的应用,下一步的研究方向是结合已有的位置隐私保护技术,设计出保证无线传感器网络低能耗、高安全时间、低时延和高到包率的隐私保护方法。

## 5 结束语

随着电力、通信、网络和传感器技术的进步发展,无线传感器网络在电力物联网中的应用将更加广泛。然而,无线传感器网络中的隐私问题也将随着各种应用而越发明显,如果不采取适当的措施保护网络的隐私,网络的安全性和可用性将会大大降低。位置隐私是无线传感器网络中一项重要的隐私,源节点位置隐私的泄露将直接暴露被监测的物体,攻击者对源节点的破坏会使得网络将不能采集此处的数据;汇聚节点是无线传感器网络和外部网络的网关,同时也负责收集和融合源节点发来的数据,并将其传输至管理者处,破坏和孤立汇聚节点会导致网络的瘫痪,因此,必须对源节点和汇聚节点的位置隐私进行保护。现有的位置隐私保护方法能够在一定的程度上保护关键节点的位置隐私,但却不能完全做到使网络满足低能耗、高安全时间、低时延和高到包率。对于电力物联网下无线传感器网络位置隐私保护方法研究而言,下一步的研究方向是结合电力物联网对无线传感器网络位置隐私保护方法的要求,设计出更有效的位置隐私保护方法。

## 参考文献:

- [1] 赵宝康. 无线传感器网络隐私保护关键技术研究[D]. 长沙: 国防科技大学, 2009.
- [2] 刘敏钰, 吴泳, 伍卫国. 无线传感网络WSN研究[J]. 吉林电力, 2010,38(2): 20-23.
- [3] 张强, 孙雨耕, 杨挺, 等. 无线传感器网络在智能电网中的应用[J]. 中国电力, 2010,43(6): 31-36.
- [4] 王生. 无线传感器网络位置隐私保护研究[D]. 长沙: 中南大学, 2009.
- [5] Y. Xi, L. Schwiebert, W.S. Shi, Preserving source location privacy in monitoring-based wireless sensor networks, in: Proceedings of the 20th International Parallel and Distributed Processing Symposium (IPDPS 2006), April 2006.
- [6] Na Li, Nan Zhang, Sajal K. Das, Bhavani Thuraisingham, Privacy preservation in wireless sensor networks:
- [7] A state-of-the-art survey, Ad Hoc Networks 7 (2009) 1501-1514.
- [8] Y. Jian, S.G. Chen, Z. Zhang, L. Zhang, Protecting receiver-location privacy in wireless sensor networks, in: Proceedings of the 26th IEEE International Conference on Computer Communications (INFOCOM2007), May 2007, pp. 1955-1963.
- [9] J. Deng, R. Han, S. Mishra, Decorrelating wireless sensor network traffic to inhibit traffic analysis attacks, Pervasive and Mobile Computing Elsevier 2 (2) (2006) 159-186.

---

## 作者简介:

华 晔 (1985—), 男, 江苏南京人, 工程师, 研究方向为网络信息安全, E-mail: huaye2@epri.sgcc.com.cn.