

无线传感器网络节点位置隐私保护研究

黄仁季¹, 叶清¹, 吴倩²

(1. 海军工程大学信息安全系, 湖北 武汉 430033;

2. 海军试验基地试验舰中心, 辽宁 葫芦岛 125000)

摘要: 为更加深入地研究解决位置隐私保护问题, 分析了无线传感器节点位置隐私保护的特点和模型, 按照对源节点与对基站以及各自的技术手段分类总结了现有位置隐私保护方案, 从方案针对的攻击类型、安全性、效率性能及能耗等方面比较优缺点, 并对未来的研究方向进行了展望。

关键词: 无线传感器网络; 位置隐私保护; 幻象路由; 假数据分组注入

中图分类号: TP391

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2017.00212

Research of location privacy protection in wireless sensor network

HUANG Ren-ji¹, YE Qing¹, WU Qian²

(1. Department of Information Security, Naval University of Engineering, Wuhan 430033, China;

2. Navy test base experimental ship center, Huludao 125000, China)

Abstract: For deeply studying and solving the problems of location privacy protection in WSN, characteristics and models of location privacy protection were analyzed, schemes of location privacy protection were categorized by source, base station and the classification of their technologies. The merits and demerits in different attack types, security, efficiency and energy consumption were compared and the future research orientation was previewed.

Key words: wireless sensor network, location privacy protection, phantom routing, fake data packet injection

1 引言

无线传感器网络 (WSN, wireless sensor networks) 是物联网的重要组成^[1], 它是由大量传感器节点以自组织方式组成的无线网络。网络主要由源节点、汇聚节点、中央处理单元等部分组成, 以温度、湿度、声音、位置、光照、压力、磁场等多种传感器作为感知节点, 对区域内的环境信息进行监测^[1], 具有大规模、自组织、低能耗、动态性等特点。它在环境监测、灾害预警、医疗卫生、工业制造等领域具有广泛的应用。在

军事方面, 它能够实现以较低的成本对敌情进行侦测获取, 在敌区或人员不便到达的区域布置传感器节点, 既获取情报又最大限度地降低了人力物力成本, 避免不必要的减员。

无线传感器网络自身的开放和自组网的特点^[1]决定了其固有的安全缺陷, 易受到各种攻击。位置隐私窃取是常见攻击方式之一^[2], 攻击者可以在不获取传感器网络中具体传输数据的情况下分析传感器节点、基站的位置信息甚至整个网络的拓扑结构与节点分布。而一旦位置隐私信息泄露, 攻击者可以进一步破坏或捕获相应节点从而破坏

收稿日期: 2017-08-28; 修回日期: 2017-09-24。通信作者: 黄仁季, wuhan_wuyingjituan@163.com

基金项目: 总装预研基金资助项目 (No.9140A06040313JB11084); 信息保障技术重点实验室开放基金资助项目 (No.KJ-14-104)

Foundation Items: GAD Advance Research Fund Project (No.9140A06040313JB11084), Key Laboratory of Information Assurance Technology Open Fund Project (No.KJ-14-104)

整个网络；可以获取监测对象的位置进而对其进行破坏，或者分析其生活规律，挖掘更多隐私信息。因此，深入开展对无线传感器网络中的位置隐私保护问题的研究，能够更好地保证无线传感器网络的安全，有益于推动无线传感器网络技术的发展。

2 无线传感器网络攻击模型

根据无线传感器网络特点，在无线传感器网络位置隐私保护中做出以下假设。

1) 传感器节点足够多且在网络中平均散布，即在各个区域节点密度相等。两个节点相邻表示它们之间能实现直接通信，非相邻节点间的通信可以通过中间节点转发，以多跳方式完成。

2) 网络中有且仅有一个基站且有多个汇聚节点。源节点可以直接搜集信息、采集数据，而数据分组从源节点发出经汇聚节点最终到达基站。基站通常具有较强的通信与计算存储能力。

3) 除基站外其余节点完全相同，即具有相同的有限功耗、初始能量、计算能力、存储能力、通信能力，且节点间可相互替代。

4) 基站与各个节点位置完全随机且在网络中位置可以变动，网络拓扑结构可以变化，新的节点可以随时加入，失效节点可以剔除，同一时刻可能存在多个源节点同时传输信息。

在无线传感器网络位置保护中，根据攻击者的攻击方式可以分为普通攻击模型与复杂攻击模型^[3]。普通攻击模型中攻击者只采用窃听、逐跳回溯^[4,5]、流量分析等被动攻击手段^[6]。这种方式在不对网络施加额外影响的情况下分析网络中节点与基站的位置隐私，不易被发觉。而复杂攻击模型指攻击者除具有被动攻击能力外还具有节点

捕获^[7]、数据篡改、数据伪造、拒绝服务攻击等主动攻击能力，可以对网络和数据造成直接破坏^[3]。

无线传感器网络攻击模型如图1所示，根据攻击者的攻击能力可以分为局部流量攻击与全局流量攻击^[3]。全局流量攻击者具有良好的硬件条件，在整个无线网络区域内布置有大量窃听节点与多种分析工具，可以对整个网络的流量、通信状况进行监听，具有强大的攻击能力；局部流量攻击者通常仅为一个或有限个窃听节点，只能对其通信范围内的节点进行窃听与分析，具有有限的攻击能力，通常采取逐跳回溯的攻击方式。局部流量攻击又可分为有耐心的攻击者与谨慎的攻击者，有耐心的攻击者在逐跳回溯过程中会忽略其他消息，仅对当前回溯的数据分组进行监听直到找到源节点，而谨慎的攻击者则在回溯过程中记录每一跳，当在一段时间内不再收到当前回溯数据分组信息时则停止回溯并返回上一跳。有耐心的攻击者具有更强的追踪性能但同时需要消耗更多的追踪时间。

3 无线传感器网络位置保护方案

无线传感器网络位置隐私保护可以分为对源节点的保护和对基站的保护，对源节点保护的主要目的是保护数据采集端，防止暴露监控的目标或监控点；而对基站的保护也可称为对汇聚节点的位置隐私保护，主要是为保护整个无线传感器网络的安全，防止攻击者破坏关键节点以瘫痪整个网络。

3.1 无线传感器网络源节点位置保护方案

无线传感器网络中源节点的位置保护主要有幻象路由、动态ID、环形路由以及假消息注入等技术手段。

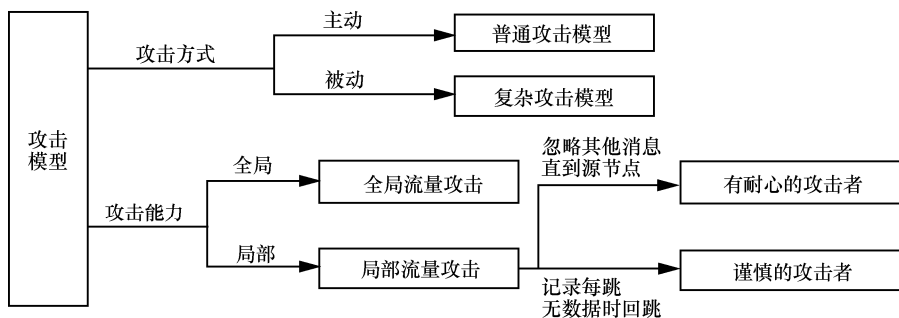


图1 攻击模型

3.1.1 基于幻象路由的源节点位置保护方案

幻象路由^[8]是最常见的源节点位置保护方案。在这一方案中, 数据分组先到达一个随机的节点称为幻影节点, 转发节点随机决定下一跳节点; 第二步数据分组从幻影节点转发回基站, 使幻影节点被伪装成源节点。

幻象路由最早在 Ozturk^[9,10]等的 PR(phantom routing) 方案和 PSPR(phantom single-path routing) 方案中提出。该方案源节点将相邻节点分为方向相反的两个集合, 从中选一个转发数据分组, 转发一定跳数后采用泛洪的方式将数据分组发送回基站。

原始的幻象路由存在幻影节点分布规律性等安全问题, 因此, 2012 年陈涓^[11]提出基于有限泛洪的源节点位置隐私保护方案(PUSBRF, source location privacy preservation protocol in wireless sensor network using source-based restricted flooding) 改进了幻象路由的安全性。该方案主要由 h 跳有限泛洪、 h 跳有向路由以及最短路由 3 个部分所构成。距离源节点 h 跳内的所有节点通过第一阶段获得源节点的最小跳数; 在第二阶段, 每个节点转发数据分组时都是向着距离源节点跳数最小的远离源节点方向的相邻节点, 最终在距离源节点 h 跳的圆周上分布幻影节点; 最后利用最短路径将数据由幻影节点传至基站。

在提升了安全性之后, 为改进能量控制与优化, 2014 年, Zhou^[12]提出基于蚁群算法的高效节点位置保护方案(EELP, energy efficient location privacy preservation protocol), 该方案将节点作为人工蚂蚁, 通过模拟蚂蚁寻找最短路径的思路实现。节点间的信息以被称为信息素的形式存储在路由表中, 当节点接收数据分组时, 根据信息素, 节点间距离以及能量情况计算接收者并更新信息。在不断传输的过程中, 路由中的信息素含量随着其挥发和积累而调整, 从而指引最优全局传输路径。

2016 年, 贾宗璞等^[13]提出基于随机角度和圆周路由的位置隐私保护策略(BRACRS, based on random angle and circumferential routing), 进一步提升了幻象路由的安全性^[14]。该方案分为网络初始化、基于角度幻象路由、圆周路由与最短路径路由。在幻象路由阶段通过角度、距离等因子产

生幻影节点并将数据传递至幻影节点; 在圆周路由阶段, 定义了伪幻影节点与标节点, 距离源节点最远的幻影节点被称为伪幻影节点, 而与伪幻影节点在同一圆上的随机节点则称为标节点; 数据分组先从幻影节点传递至标节点, 再进行最短路径路由到达基站。

2016 年, Sathishkumar 和 patel^[15]将幻象路由应用在具体场景中, 在物联网的背景下提出增强的基于随机路由的源节点位置保护算法。该方案首先在节点网络中初始化若干随机路径, 当数据分组转发时, 如果节点不在初始化的路径之中则随机转发至任意相邻节点, 如果在初始路径中则沿路径转发, 转发时不转发到已经过的节点。当某一节点在转发时无法找到尚未经过的相邻节点时, 则将数据分组发回上一跳从而保证数据分组最终可以到达基站。

幻象路由采用随机游走的方法, 产生随机的幻影节点以保护真实源节点, 目前已有较多研究^[16,17], 安全性有了很大提升。为提高效率, 产生了环形路由技术, 在数据传输过程中经过一段环形回路, 使攻击者在回溯过程中陷入环路循环中难以找到源节点, 大量消耗回溯时间。

3.1.2 基于环形路由的源节点位置保护方案

基于环形路由的方案是指在源节点发送的数据分组路由过程中构造一个环路, 通过让数据分组在环路中循环的方式迷惑、打乱攻击者, 达到破坏攻击者位置追踪的目的。

2014 年, 徐智富^[18]提出基于布朗运动的隐私保护方案。这一方案采用了环形路由技术, 在网络中组建多个链路以保障到汇聚节点的路径分布均匀, 汇聚节点通过泛洪得到环路到汇聚节点最短距离。源节点发出的数据分组首先进入链路环中, 在环路中随机运动后发送至汇聚节点或进入下一个环路, 经过反复循环后最终到达汇聚节点。

2016 年, 张江南等^[19]提出基于假分组策略的单个虚拟圆环陷阱路由方案(SVCRM, single virtual circle rooting method based on fake package)。数据分组从源节点发出逐跳传递到虚拟圆环, 在圆环中数据分组沿一特定方向在圆环中环绕, 最后数据分组随机地离开圆环以最短路由的方式到达汇聚节点。当存在较多靠近汇聚节点的

源节点时易造成虚拟圆环过早失效,为此进一步提出基于假分组策略的多个虚拟圆环陷阱路由方案(MVCRM, multiple virtual circle rooting method based on fake package)。

3.1.3 基于假消息注入的源节点位置保护方案

假消息注入是另一项常用技术,指在网络中注入虚假消息使攻击者将其与真实消息混淆,不能分清真实消息来源,它通常可以与其他技术结合,提供更高的安全性。

2008年,Shao^[20]基于假消息注入技术提出FitProbRate方案。该方案分为假分组注入、真消息嵌入与采样均值调整3个阶段。在假分组注入阶段节点按服从指数分布的时间间隔发送虚假数据分组;当源节点获取到真实数据时进入真消息嵌入阶段,利用A-D Test^[21]找出服从指数分布的最小传输时间间隔来发送消息;真实消息发送后则重新计算数据分组发送时间间隔。邓美清等^[22]对FitProbRate方案作出改进,提出基于能量的位置隐私保护方案EBS(energy-based scheme)。在FitProbRate方案基础上引入能量影响因子、参数基准以及能量影响比重从而平衡了能耗。

假消息注入技术还可以应用在伪造数据源上,2013年肖戊辰^[23]提出支持被动RFID(radio frequency identification)的通用假数据源策略GFS(general fake source)。该方案通过产生伪造数据分组的方式伪造数据源,首先在网络中选择一个源节点并令其产生伪造的数据分组,模拟发现目标并转发,通过令牌传递的形式改变产生伪造数据分组的节点以模拟目标的移动过程,从而实现了真实数据源行为模仿。

2014年,胡小燕^[24]进一步提出伪区域隐私保护策略。首先在整个网络中建立虚假源区域^[25],除源节点外其余节点均向各区域中心节点发送虚假数据分组;数据分组到汇聚节点的过程通过各区域中心节点与之通信完成,使源节点与汇聚节点之间直接通信数据量得以减少。当源节点位置发生变化时,区域中心节点随之改变来克服区域差别。

为高效区分真假数据分组,2016年,牛晓光^[26]等将假分组注入技术与环策略结合起来,提出基于匿名量化动态混淆的源节点位置隐私保护方案

(ADRing, anonymity-quantified dynamic mix-ring-based source location anonymity protocol)。首先以基站为圆心,以到基站的跳数为半径将网络中的节点划分为多个圆环,从而随机选取一个环作为混淆环并由它接受和过滤网络中的数据,真实的数据分组在混淆环上进行混淆并转发至基站,虚假数据分组在混淆环上直接丢弃。此过程中采用匿名度评价机制对混淆环的效果进行评估,混淆环可以动态调整变化。

假数据分组技术方便易行,应用广泛成熟,与其他技术也结合得最多^[27]。另一方面,动态ID的技术可以从节点匿名的角度实现位置隐私的保护。

3.1.4 基于动态ID的源节点位置保护方案

除了从路由的角度考虑位置隐私的保护,还需要从节点自身信息的角度考虑。各节点自身的ID之间存在的关联性就是可能被攻击者进行位置分析的信息之一。

针对ID分析攻击,往往可以采用匿名通信的方式应对,即在通信中隐藏节点ID等实际身份信息,防止由于对节点间身份信息的关联分析而泄露隐私。常芬等^[28]对此问题进行了研究,提出了实施匿名的具体方案及其安全性能。

Gurjar与Patil^[29]提出基于簇的源节点匿名方案。将传感器节点划分为不同区域,每个区域由一个簇头节点控制,簇头节点通过改变动态ID的方式取消节点ID与位置之间的关联。每次源节点捕获事件发送数据分组时使用的不是自己真实的ID,而是由簇头节点随机分配更新的ID,数据分组先发送至簇头节点再由它转发至基站。簇头节点及时对区域内节点ID进行更新,每次更新为一段随机数字区间内的连续数字。

3.2 无线传感器网络汇聚节点与基站位置隐私保护方案

汇聚节点与基站的位置保护主要采用伪造节点、注入虚假数据分组、平衡流量等方式。

3.2.1 基于虚假数据分组注入的基站位置保护方案

注入虚假数据分组^[30]是改变网络流量分布的最简单有效的手段,因此这一技术在基站的位置保护方案十分常见,大部分保护方案都融入了假分组注入的思想。

2014年,Priyadarshini^[31]引入假数据分组注

入技术, 提出减少流量信息的基站位置保护方案。该方案根据区域中节点密度以及节点剩余能量来决定假数据分组的产生, 当区域节点密度较小时, 以小概率产生假数据分组; 如区域节点密度较大且转发节点能量充足, 以大概率产生假数据分组; 当区域节点密度较大但节点能量不足时则不产生假数据分组。

Rios 等^[32]则将假数据分组注入与路由规则相结合, 提出一种汇聚节点位置保护方案 HISP-NC (homogenous injection for sink privacy with node compromise protection)。该方案分为数据转发与路由表伪装两个部分, 在数据转发时所有节点都同时转发真实数据与一个假数据分组, 并采用随机游走的方式在节点间传递, 而真实数据分组以更高的概率向会聚节点方向转发, 假数据分组以更高概率向远离方向转发; 在路由表伪装部分, 它通过对原始路由表进行优化, 改变了原来路由表第一项为最近距离节点的规则, 攻击者无法通过截获路由表而分析出会聚节点的位置。

3.2.2 基于伪造节点的基站位置保护方案

伪造节点是采用诱导欺骗的思想, 将流量或其他可能标识基站身份的信息引向一个伪基站节点以误导攻击者, 从而达到保护真正基站的目的。伪造节点通常通过与产生假数据分组结合来实现^[33], 也有部分方案为不影响网络整个性能而通过其他方式伪造节点。

2015 年, Bangash 等^[34]对假数据分组注入的方式进行了优化, 提出基于虚拟基站的基站位置保护方案。该方案将无线传感器网络中的节点分为 SN (source node)、AN (aggregator node) 和 BS (base station) 三类, SN 即普通源节点, BS 即基站, AN 则具有更大的通信半径且每个 SN 都至少与一个 AN 相邻, 数据分组通过 AN 转发至 BS。AN 在转发数据分组时同时沿相反方向向相邻 AN 或 BS 发送真实与虚假的数据分组, 从而使 AN 周围模拟了 BS 的流量。在转发真实与虚假数据分组时还通过延迟时间这一参数进行控制使位置保护的安全性能可以随需要调节。

2016 年, Bangash 等^[35]基于 SDN (software defined networking) 的思想, 提出了 LPSDN (location privacy via software defined networking)

方案^[35]。该方法主要思想是采用一种叫作 SDFN (software defined forwarding node) 的节点, 来替代基站节点分担数据流量。具体方法是所有源节点发送的数据分组首先到达 SDFN 节点, 由 SDFN 对数据进行分析筛选, 对于内容相同的数据则丢弃多余数据, 仅将一份数据分组转发至基站节点处, 保证了网络流畅, 分担了基站的流量使流量密度集中于 SDFN 从而保护基站的位置。

2017 年, 王舰等^[36]将假数据分组注入与随机游走结合进行改进以抵御方向性攻击, 进一步提升汇聚节点位置的安全性。该方法将最短路径、假消息注入、伪造节点等技术结合起来, 达到抵御多种攻击方式的目的。首先数据分组沿最短路径到达第一个交叉节点, 产生发向伪造基站的虚假数据分组; 而真实数据分组则以随机路径到达下一个交叉节点, 产生发向其他普通节点的虚假数据分组; 最终当真实数据分组结束随机路由后, 由交叉节点转发至基站。

3.2.3 基于路由控制的基站位置保护方案

基于路由控制的方案是通过改变数据分组传递的路由规律以增加不确定性来防止位置信息泄露的技术方案。

2012 年, 李福龙^[37]提出简单的基于动态调整节点分组发送速率的基站位置隐私保护策略 SRA (send rate dynamically)。它基于增加不确定性的考量, 使网络中所有节点都具有相同的特征和属性, 使整体不确定度达到最大, 让攻击者无从分析哪一个节点为基站。网络中各节点具有相同的数据分组发送速率并由基站统一调控, 同时基站保持与普通节点相同的分组发送速率, 使基站与普通节点之间在流量上不存在区别。最后, 根据节点数量与网络实际情况, 基站可以动态地调整各个节点分组发送速率, 平衡网络效率与基站负荷。

2013 年, 陈娟^[38,39]针对具体的 PAS 和 TP-PAS 攻击, 提出基于子孙的基站位置保护方案 CB。在该方案中每个节点只存储一个子节点集并且只转发来自子节点集的数据分组, 且节点实时更新消息密钥, 保证攻击者不能推断节点间消息转发关系。同时还提出了基于无父节点的基站位置保护方案 PF^[38,39]。此方案中每个节点不存储父节点

信息, 而用 u 个洋葱包替代, 一个洋葱包表示节点到基站的一条路径并由它将消息路由至基站。

除假数据分组注入, 还可以通过网络全局路由的控制实现位置隐藏, 2015 年, 周黎鸣^[40]提出基于混淆区的基站位置保护方案 MR-PAIA (proxy and interference area sink location privacy protection scheme)。该方案初始化若干随机路径并在源节点周围构建虚拟环即代理区, 隐藏数据传播路径, 在基站周围建立混淆区, 保护基站流量信息。当数据分组由源节点随机传输至代理区时, 代理节点顺时针传递数据分组, 经过若干跳后离开并到达下一节点; 到达初始随机路径时沿路径到末节点; 到达混淆区后采用广播的方式传递至基站。

对基站的位置隐私保护主要思路还是通过对全局流量信息的控制, 实现对基站的伪装, 因此注入假数据分组技术使用较多。

4 无线传感器网络节点位置隐私保护方案对比

4.1 无线传感器网络源节点位置隐私保护方案优缺点比较

幻象路由技术可以提高幻影节点的随机性, 使有效路径增加, 阻止失效路径的产生。它可以有效针对逐跳回溯等局部攻击手段, 实现上较为

简单, 不需要很强的计算能力, 对网络性能影响不大, 不影响信息传输效率。但幻象路由仅能够抵御具有局部监听能力的攻击者, 且选择幻影节点时要求具有位置多样性与随机性。采用幻象路由的方案中, Sathishkumar&patel 的方案较易实现, 简单方便且数据分组都可以到达基站, BRACRS、EELP 等方案具有更长的安全时间, 产生更多的有效路径, EELP 均衡了全局能耗控制, 提高安全性的同时 Sathishkumar&patel、BRACRS 方案牺牲了小部分网络性能, 增加了传输延时。构造环路的方案中, Base-brown 方案较为简单, 安全时间较长但有一定的失败风险, ADRing 与 MVCRM 方案都与假数据分组注入相结合, 融合了各自的优点, 增加了抵御全局攻击的能力, 可以有效防止逐跳回溯与流量分析等攻击, 但采用假分组注入引入了多余数据分组, 可能增加通信开销与网络负担, 需要在安全性与效率上进行平衡。伪造数据源方案的安全性与构造的伪数据源数量直接相关, 因此它可以调整安全级别, 平衡安全性与网络能耗。Gurjar&Patil 的方案考虑了 ID 分析攻击, 可以与其他方案结合提高安全性能。各方案优缺点详细比较如表 1 所示。

4.2 无线传感器网络基站位置隐私保护方案的优缺点比较

基站与汇聚节点的位置隐私保护主要改变基

表 1 源节点位置隐私保护方案优缺点比较

方案	主要技术	优点	缺点
PR&PSPR ^[9,10]	幻象路由、随机游走	抵御局部流量攻击者	幻象路由节点集中在特定区域、不能抵抗全局流量攻击
PUSBRF&EPUSBRF ^[11]	幻象路由、有限泛洪	幻影节点位置随机、避开失效路径、能耗较低	重复泛洪增加通信开销
Sathishkumar&patel ^[15]	随机游走、初始化随机路径	方案简单有效、数据总能够到达基站	可能产生的路径较长, 加大数据分组时延
EELP ^[12]	蚁群算法	可以进行全局能耗控制	需要一定的计算开销
BRACRS ^[13]	幻象路由、圆周路由	基于随机角度选择幻影节点、利用标节点在能量受限下增加安全时间	增加了通信开销
Base-brown ^[18]	链路环	安全周期长、传递时间短、流量分布平均	成环有一定概率, 可能失败
ADRing ^[26]	混淆环、假分组注入	平衡网络能耗、抵御全局流量分析攻击	增加了消息传输时间、混淆环上能耗较高
SVCRM&MVCRM ^[19]	虚拟环、假分组注入	增加了平均安全时间	源节点位置固定
Gurjar&Patil ^[29]	动态 ID	抵抗 ID 分析攻击	抵抗攻击方式单一、需要动态更新 ID
GFS ^[23]	伪造数据源、假分组注入	支持被动 RFID	能耗增大
文献[24]	虚假数据源区域、假分组注入	充分利用非热区能量、提高数据分组有效到达效率	安全性能与能耗成正比

站原有的流量分布特点，使基站与普通节点不可区分。Priyadarshini、SRA、MR-PAIA、MimiBS 与 HISP-NC 都实现了抵御全局流量攻击，其中 SRA 算法需要由基站对全网节点进行实时控制和调整，Priyadarshini 平衡了网络整体能量增加了寿命，MR-PAIA 算法的通信开销与传输时延相对较小。LPSDN 方案采用了伪造基站的思想，但只是通过改变流量分布的方式，没有引入假数据分组，从而没有增加网络负担，而对重复数据的筛选反而降低了网络通信流量，在保护基站安全的同时节省了能量。CB 与 PF 算法都是为应对 PAS 与 TP-PAS 攻击而设计，需要与其他基站位置隐私保护方案配合使用才能抵御其他攻击。MimiBS 的安全性可以根据需要进行调整，整体性能平均没有增加太多负荷。而 HISP-NC 可以防止路由表截获导致的路由表分析攻击。各基站位置隐私保护方案优缺点比较如表 2 所示。

5 结束语

无线传感器网络技术正不停向前发展并在众多关键领域有了愈加广泛的应用，而其位置隐私安全越来越重要，要求也越来越高，许多方面需要进一步研究。

1) 位置隐私保护能力评价体系

目前的无线传感器网络位置隐私保护协议的评价方式大多采用安全时间、通信开销、计算开销、能量消耗等参数指标，但具体指标的量化与评价方法各不相同，没有统一的标准。对协议的

评价流程没有形成统一的规范^[41]。因此，尽管位置隐私保护协议很多，但各种协议的效果与保护强度很难直观地进行比较，保护效果的可信度不够权威。

2) 多种保护策略融合

第 3 节中涉及的方案都主要采用了一种或两种技术结合的设计，如单一采用幻象路由的 patel 方案、BRACRS 方案和 EELP 方案，或者仅与假数据分组注入技术相结合的 ADRing 与 MVCRM 方案；但是缺少一种能够包含多种防护技术基于多层次的综合方案，许多技术之间不能兼容。不同的技术针对不同的攻击手段，多种技术的结合能够提供全面的防护能力。

3) 针对主动攻击的位置隐私保护策略

现有方案主要针对普通模型中的攻击者，如基于幻象路由的方案主要解决逐跳回溯攻击，基于假数据分组注入主要解决流量分析攻击等问题；但是应对主动攻击，如节点捕获等的位置隐私保护协议研究相对较少。因此，加强这方面的研究并将现有隐私保护策略与身份认证、访问控制、密码保护等数据隐私手段和密码学方法相结合的研究具有重要意义。

4) 移动节点的位置隐私保护

现有的方案主要在网络中节点位置相对固定的背景下设计，文中所提到的方案都是假定源节点与基站的位置不发生变化。而在一些应用场合，如对野生动物观测、海战场敌情探测等则需要考虑在移动源节点与会聚节点^[42]下进行位置隐私

表 2 基站位置隐私保护方案优缺点比较

方案	主要技术	优点	缺点
Priyadarshini ^[31]	假分组注入	平衡节点能量，提高网络生存时间	流量、能耗增加，增加网络延迟
SRA ^[37]	数据分组发送速率动态控制	抵御全局流量分析、全局数据发送速率动态调整	所有节点与基站数据发送速率相同使网络缺乏灵活性
CB&PF ^[39]	转发关系控制、洋葱包	有效抵御 PAS 与 TP-PAS 攻击	可能增加通信开销或传输时延
MR-PAIA ^[40]	伪源节点、伪基站	通过代理区与混淆区抵御流量分析攻击	混淆区通信负担较重
文献[36]	伪造基站、假分组注入、随机游走	抵御方向性攻击、抵御数据分组追踪、平衡全局流量	产生假数据分组过多，网络延迟增加较快
LPSDN ^[35]	伪造基站、数据分组筛选	改变流量密度分布，不会增加额外负担，节省能量	SDFN 节点分担了基站流量，自身容易暴露
MimiBS ^[34]	伪基站	安全性能可根据 TTL 参数调整、抵御流量分析攻击	增加延迟
HISP-NC ^[32]	假分组注入、路由表改动	可以抵抗流量分析攻击与路由表分析攻击	增加节点能耗，不能抵抗节点捕获

保护。节点的移动将为保护方案的设计带来新的问题^[43],如移动节点信息的广播与更新、节点移动路径的隐藏等,许多问题有待进一步研究。

参考文献:

- [1] 孙利民, 张远, 刘庆超, 等. 无线传感器网络基础[M]. 北京: 清华大学出版社, 2014: 3-13.
SUN L M, ZHANG Y, LIU Q C, et al. Fundamentals of wireless sensor networks[M]. Beijing: Tsinghua University, 2014: 3-13.
- [2] YNAG X, MA K. Evolution of wireless sensor network security[C]//World Automation Congress. 2016: 1-5.
- [3] 彭辉, 陈红, 张晓莹, 等. 无线传感器网络位置隐私保护技术[J]. 软件学报, 2015, 26(3): 617-639.
PENG H, CHEN H, ZHANG X Y, et al. Location privacy preservation in wireless sensor networks[J]. Journal of Software, 2015, 26(3): 617-639.
- [4] CHENG L, WANG Y, WU H, et al. Non-parametric location estimation in rough wireless environments for wireless sensor network[J]. Sensors and Actuators A: Physical, 2015, 224: 57-64.
- [5] WANG H, SHENG B, LI Q. Privacy-aware routing in sensor networks[J]. Computer Networks, 2009, 53(9): 1512-1529.
- [6] GROAT M, HE W, FORREST S. KIPDA: k -indistinguishable privacy-preserving data aggregation in wireless sensor networks[C]//The IEEE INFOCOM. 2011: 2024-2032.
- [7] BABAR, STANGO A, PRASAD N, et al. Proposed embedded security framework for Internet of Things (IoT)[C]//The Wireless Communication, Vehicular Technology. 2011: 1-5.
- [8] ROY K, KUMAR P. Source location privacy using fake source and phantom routing(FSAPR) technique in wireless sensor networks[J]. Procedia Computer Science, 2015, 57: 936-941.
- [9] OZTURK C, ZHANG Y, TRAPPE W. Source-location privacy in energy-constrained sensor network routing[C]//The 2nd ACM Workshop on Security of Ad Hoc and Sensor Networks. 2004: 88-93.
- [10] KAMAT P, ZHANG Y, TRAPPE W, et al. Enhancing source- location privacy in sensor network routing[C]//The 25th IEEE International Conference on Distributed Computing Systems. 2005: 599-608.
- [11] 陈涓, 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.
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(9): 1736-1747.
- [12] ZHOU L, WEN Q. Energy efficient source location privacy protecting scheme in wireless sensor networks using ant colony optimization[J]. Journal of Distributed Sensor Networks, 2014(1): 1-14.
- [13] 贾宗璞, 魏晓娟, 彭维平. WSNs 中基于随机角度和圆周路由的源位置隐私保护策略研究[J]. 计算机应用研究, 2016, 33(3): 886-890.
JIA Z P, WEI X J, PENG W P. Privacy protection strategy about source location in WSNs based on random angle and circumferential routing[J]. Application Research of Computers, 2016, 33(3): 886-890.
- [14] LI S, XIAO Y, LIN Q. A novel routing strategy to provide source location privacy in wireless sensor networks[J]. Wuhan University Journal of Natural Sciences, 2016, 21(4): 298-306.
- [15] SATHISHKUMAR J, DHIREN R. Enhanced location privacy algorithm for wireless sensor network in Internet of things[C]//2016 International Conference on Internet of Things and Applications (IOTA) Maharashtra Institute of Technology. 2016: 208-212.
- [16] RAJ M, LI N, LIU D, et al. Using data mules to preserve source location privacy in wireless sensor networks[J]. Pervasive and Mobile Computing, 2014, 11: 244-260.
- [17] CHEN H, LOU W. On protecting end-to-end location privacy against local eavesdropper in wireless sensor networks[J]. Pervasive and Mobile Computing, 2015, 16: 36-50.
- [18] 徐智富. 无线传感器网络位置隐私保护机制的研究与实现[D]. 成都: 电子科技大学, 2014.
XU F Z. Research and implementation of location privacy protection solution in wireless sensor network[D]. Chengdu: University of Electronic Science and Technology of China, 2014.
- [19] 张江南, 褚春亮. 无线传感器网络中源节点位置隐私保护方案研究[J]. 传感技术学报, 2016, 9(9): 1405-1409.
ZHANG J N, CHU C L. A Scheme to protect the source location privacy in wireless sensor networks[J]. Chinese Journal of Sensors and Actuators, 2016, 29(9): 1405-1409.
- [20] SHAO M, YANG Y, ZHU S, et al. Towards statistically strong source anonymity for sensor networks[C]//The 27th Conference on Computer Communications. 2008: 51-55.
- [21] ANDERSON W. Anderson-darling tests of goodness-of-fit[M]. International Encyclopedia of Statistical Science. Berlin :Springer, 2011: 52-54.
- [22] 邓美清, 彭代渊. 节能无线传感器网络源位置隐私保护方案设计[C]//2015 年信息、电子与控制技术学术会议(IECT 15)论文集. 2015: 11-15.
DENG M Q, PENG D X. Energy-efficient design on source location privacy preservation in wireless sensor networks[C]//2015 Symposium on Information, Electronics, and Control Technologies. 2015: 1-15.
- [23] XIAO W, ZHANG H, WEN Q, et al. Passive RFID-supported source location privacy preservation against global eavesdroppers in WSN[C]//The 5th IEEE International Conference on Broadband Network & Multimedia Technology. 2013: 289-293.
- [24] 胡小燕. 面向全局攻击的无线传感器网络源节点位置隐私保护研究[D]. 长沙: 中南大学, 2014.
HU X Y. Research on the source-location privacy in wireless sensor networks against a global eavesdropper[D]. Changsha: Central South University, 2014.
- [25] LERON L, JIAN R. R-STaR destination-location privacy schemes in wireless sensor networks[C]//IEEE International Conference on Communications. 2015: 7335-7340.
- [26] 牛晓光, 魏川博, 姚亚兰. 传感网中能量均衡高效的源位置隐私保护协议[J]. 通信学报, 2016, 37(4): 23-33.
NIU X G, WEI C B, YAO Y L. Energy-consumption-balanced efficient source-location privacy preserving protocol in WSN[J]. Journal on Communications, 2016, 37(4): 23-33.
- [27] ZHANG J, JIN Z. Energy-aware location privacy routing for wireless sensor networks[C]//Springer International Publishing. 2016: 26-32.
- [28] 常芬, 崔杰, 王良民. WSN 中基于椭圆曲线的可追踪匿名认证方案[J].

- 计算机研究与发展, 2017, 54(9): 2011-2020.
- CHANG F, CUI J, WANG L M. A traceable and anonymous authentication scheme based on elliptic curve for wireless sensor network[J]. Journal of Computer Research and Development, 2017, 54(9): 2011-2020.
- [29] GURJAR A, PATIL B. Cluster based anonymization for source location privacy in wireless sensor network[C]// The International Conference on Communication Systems and Network Technologies. 2013: 248-251.
- [30] YAO L, KANG L, SHANG P F, et al. protecting the sink location privacy in wireless sensor networks[J]. Personal and Ubiquitous Computing, 2013, 17(5): 883-893.
- [31] PRIYADARSHINI P, PANDEL M. Concealing of the base station's location for preserving privacy in wireless sensor network by mitigating traffic patterns[C]// IEEE International Conference on Advanced Communication Control and Computing Technologies. 2014: 852-857.
- [32] RIOS R, CUELLAR J, LOPEZ J. Probabilistic receiver-location privacy protection in wireless sensor networks[J]. Information Sciences, 2015, 321: 205 - 223.
- [33] MALVIYA A R, JAGDALE B N. Location privacy of multiple sink using zone partitioning approach in WSN[C]// International Conference on Applied & Theoretical Computing & Communication Technology. 2016: 449-454.
- [34] BANGASH Y, ZENG L, FENG D. MimiBS: mimicking base-station to provide location privacy protection in wireless sensor networks[C]// IEEE International Conference on Networking. 2015: 158-166.
- [35] BANGASH Y, ZENG L, DENG S, et al. Lpsdn: sink-node location privacy in WSNs via SDN approach[C]// IEEE International Conference on Networking. 2016: 1-10.
- [36] WANG J, WANG F, CAO Z, et al. Sink location privacy protection under direction attack in wireless sensor networks[J]. Wireless Network, 2017, 23: 579-591.
- [37] 李福龙. 无线传感器网络基站位置隐私保护协议研究[D]. 哈尔滨: 哈尔滨工业大学, 2012.
- LI F L. Research on base station location protection in wireless sensor networks[D]. Harbin: Harbin Institute of Technology, 2012.
- [38] CHEN J, ZHANG H, DU X, et al. Base station location protection in wireless sensor networks: attacks and defense[C]// IEEE International Conference on Communications (ICC). 2012: 554-559.
- [39] 陈娟. 无线传感器网络中节点位置隐私保护与自愈技术研究[D]. 哈尔滨: 哈尔滨工业大学, 2013.
- CHEN J. Research on node location protection and self-healing techniques in wireless sensor networks[D]. Harbin: Harbin Institute of Technology, 2013.
- [40] 周黎鸣. 无线传感网中节点位置和数据隐私保护研究[D]. 北京: 北京邮电大学, 2015.
- ZHOU L M. Research on privacy protection of nodes' location and data in wireless sensor networks[D]. Beijing: Beijing University of Posts & Telecommunications, 2015.
- [41] JIANG R, LUO J, WANG X. An attack tree based risk assessment for location privacy in wireless sensor networks[C]// The 8th IEEE International Conference on Wireless Communications, Networking and Mobile Computing (WICOM 2012). 2012: 1-4.
- [42] ZHANG J, CHOW C. REAL: A reciprocal protocol for location privacy in wireless sensor networks[C]// IEEE Transactions on Dependable and Secure Computing. 2015: 458-471.
- [43] HAYES T, ALI F. Location aware sensor routing protocol for mobile wireless sensor networks[J]. IET Wireless Sensor Systems, 2016, 6(2): 49-57.

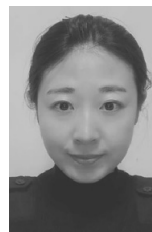
作者简介:



黄仁季(1994-), 男, 山东青岛人, 海军工程大学硕士生, 主要研究方向为无线传感器网络位置隐私保护。



叶清(1978-), 男, 湖北蕲春人, 博士, 海军工程大学副教授, 主要研究方向为无线传感网络安全。



吴倩(1989-), 女, 河北秦皇岛人, 海军试验基地试验舰中心助理工程师, 主要研究方向为信息与网络安全。