软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2015,26(3):617−639 [doi: 10.13328/j.cnki.jos.004715]

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel: +86-10-62562563

无线传感器网络位置隐私保护技术*

彭 辉[1,2], 陈 红[1,2], 张晓莹[1,2], 范永健[3], 李翠平[1,2], 李德英[1,2]

[1](数据工程与知识工程国家教育部重点实验室(中国人民大学),北京 100872)

[2](中国人民大学 信息学院,北京 100872)

[3](河北工程大学 信息与电气工程学院,河北 邯郸 056038)

通讯作者: 陈红, E-mail: chong@ruc.edu.cn

摘 要: 对传感器网络位置隐私保护技术的研究现状与进展进行了综述,首先介绍网络模型、攻击模型和性能评价模型.接着,按照路径伪装、陷阱诱导、网络匿名和通信控制这 4 种策略对现有的研究成果进行了分类,阐述了代表性协议的核心技术.对各协议性能和优缺点的分析比较表明:4 种策略都会在一定程度上影响网络的通信和能耗性能:路径伪装策略主要针对逐跳回溯攻击,网络匿名策略主要针对 ID 分析攻击,陷阱诱导和通信控制策略可以抵御多种类型的攻击.最后,对未来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;路径伪装;陷阱诱导;网络匿名;通信控制

中图法分类号: TP393

中文引用格式: 彭辉,陈红,张晓莹,范永健,李翠平,李德英.无线传感器网络位置隐私保护技术.软件学报,2015,26(3):617−639. http://www.jos.org.cn/1000-9825/4715.htm

英文引用格式: Peng H, Chen H, Zhang XY, Fan YJ, Li CP, Li DY. Location privacy preservation in wireless sensor networks. Ruan Jian Xue Bao/Journal of Software, 2015,26(3):617−639 (in Chinese). http://www.jos.org.cn/1000-9825/4715.htm

Location Privacy Preservation in Wireless Sensor Networks

PENG Hui[1,2], CHEN Hong[1,2], ZHANG Xiao-Ying[1,2], FAN Yong-Jian[3], LI Cui-Ping[1,2], LI De-Ying[1,2]

[1](Key Laboratory of Data Engineering and Knowledge Engineering of the Ministry of Education (Renmin University of China), Beijing 100872, China)

[2](School of Information, Renmin University of China, Beijing 100872, China)

[3](School of Information and Electrical Engineering, Hebei University of Engineering, Handan 056038, China)

Abstract: This paper provides a state-of-the-art survey of location privacy-preserving techniques in WSNs. First, the network model, the attack model and the performance evaluation model are reviewed. Then, existing work is classified into four types, including path camouflage, entrapment attracting, network anonymity and communication control. Further, the key mechanisms of typical location privacy-preserving protocols are elaborated. Performance analysis and comparison show that all these four strategies affect communication and energy efficiency in some degree. In addition, the path camouflage strategy mainly aims at hop-by-hop trace attack, the network anonymity strategy aims at ID analysis attack, while the entrapment attraction and communication control strategies are capable of resisting multiple types of attacks. Finally, suggestions for future research are provided.

Key words: wireless sensor networks; location privacy preservation; path camouflage; entrapment attraction; network anonymity; communication control

作为物联网的重要组成部分,无线传感器网络(以下简称传感器网络)[1]广泛应用于国防军事、环境监测、

* 基金项目: 国家自然科学基金(61070056, 61033010, 61272137, 61202114); 国家重点基础研究发展计划(973)(2012CB316205); 国家高技术研究发展计划(863)(2014AA015204); 高等学校学科创新引智计划(B12028); 河北省自然科学基金(F2013402031)

收稿时间: 2014-04-02; 修改时间: 2014-08-12; 定稿时间: 2014-08-28; jos 在线出版时间: 2014-12-12

CNKI 网络优先出版: 2014-12-12 13:55, http://www.cnki.net/kcms/detail/11.2560.TP.20141212.1355.003.html

灾害预警、交通管理、医疗卫生、工业制造、紧急救援等诸多领域,帮助人们在任何时间、任何地点和任何环境条件下获得大量精确可靠的信息.在实际应用过程中,传感器网络所采用的无线多跳通信方式容易受到攻击者的攻击,引发严重的位置隐私泄露问题.例如:在动物监测领域,攻击者可以通过监听无线链路发现珍稀动物的位置并进行捕捉;在智能交通领域,攻击者可以通过移动轨迹数据推断用户的生活规律、行为习惯等隐私信息;在军事领域,位置隐私信息的泄漏和篡改会导致战术决策的失误,甚至直接威胁友军的安全.传感器网络中暴露出来的位置隐私泄漏问题,严重影响了传感器网络的应用发展,研究位置隐私保护技术对于传感器网络的大规模应用具有重要意义.

传感器网络位置隐私保护技术的目标是:在满足数据查询、事件监测等应用要求的前提下,针对攻击者通过监测分析通信模式,企图获取数据源或基站等重要目标位置信息的攻击方式,采取路径伪装、虚假通信等技术手段隐藏真实通信模式,有效防止网络敏感位置信息的泄露;同时,尽量控制网络能量消耗,降低通信时延,提高查询精度和可靠性.文献[2]中提出了经典的熊猫-猎人位置隐私保护模型.科学家在熊猫的活动区域部署大量传感器节点,用以研究熊猫的生活习性.当某个传感器节点感知到熊猫的位置时,立即作为源节点周期性地将观察到的熊猫生活习性数据以多跳形式发送到基站;同时,网络中存在一个具备移动能力和局部无线通信监听能力的猎人,猎人采用逐跳回溯追踪数据包的方式来确定源节点的位置,从而确定熊猫的位置并进行盗猎活动.在该模型中,位置隐私保护技术的目标就是在保证熊猫监测数据传输的同时,防止猎人确定数据源节点的位置.

传感器网络所具有的资源受限、自组织、多跳通信等特点,给位置隐私保护技术研究带来了巨大挑战:

(1) 传感器节点往往由电池供电,能量非常有限,过多的能量消耗会缩短网络的生存周期,因此,高通信量和高计算量的位置隐私保护方法不适用于传感器网络;

(2) 受节点体积和成本的影响,传感器节点的存储空间和计算能力都受到限制,无法进行大量的数据存储,也无法进行复杂的运算操作;

(3) 传感器网络常常部署在无人值守的环境中,难以进行安全管理,攻击者既可以采取窃听、逐跳回溯追踪等普通攻击方式,也可以采取节点俘获、克隆、虚假消息注入、数据篡改等复杂攻击方式来获得敏感位置信息;

(4) 隐私保护的安全需求比较复杂,主要体现在网络多样化和攻击多样化两个方面:传感器网络需要根据用户特定的应用需求进行个性化的设计和部署,不同的网络环境对应不同的攻击模型和隐私泄露渠道;同时,攻击者的攻击视角和攻击手段各不相同,攻击者既可能只具有局部监听能力,也可能具有全局监听能力,可以采用的攻击手段包括单纯监听、逐跳回溯追踪、时间关联分析、流量分析、ID 分析、节点俘获、数据篡改等等.

传感器网络位置隐私保护技术由 Ozturk 等人[2]于 2004 年提出,近年来逐渐受到学术界的广泛关注.本文对现有的传感器网络隐私保护研究成果进行了系统总结,按照算法的基本策略,将现有成果划分为路径伪装、陷阱诱导、通信控制、网络匿名 4 类,对代表协议的核心技术进行了较详细的阐述,对比了各协议能够抵御的具体攻击类型,分析了各协议的优缺点,展望了未来需要深入研究的方向.

本文第 1 节相关研究方向.第 2 节介绍研究模型,包括网络模型、攻击模型和性能评价模型.第 3 节分别对基于路径伪装、陷阱诱导、网络匿名、通信控制策略的位置隐私保护技术进行讨论.第 4 节从保护对象、针对的攻击手段、隐私保护强度、通信性能、能耗控制性能等角度全面对比代表协议的性能.第 5 节指出未来的研究方向.

1 相关研究方向

传感器网络位置隐私保护技术既要隐藏真实的通信模式,防止攻击者通过对通信模式的监听分析,获得数据源或基站等重要目标的位置信息,同时又要对性能进行优化,减少通信时延、数据丢失率和能量消耗.目前,与传感器网络位置隐私保护技术具有一定相关性的研究方向主要包括传感器网络数据隐私保护技术[3]、基于位置服务中的位置隐私保护技术和新型网络中的位置隐私保护技术.

1.1 无线传感器网络数据隐私保护技术

传感器网络隐私保护技术主要分为数据隐私保护技术和位置隐私保护技术.数据隐私保护技术以保护节点感知数据为目标,针对攻击者通过链路层窃听或俘获控制传感器节点,企图窃取或篡改隐私信息的攻击方式,主要采用扰动[4,5]、重组[6]、匿名[7]和加密[8−12]等隐私保护技术,保证在不泄露隐私信息的情况下实现数据聚集和数据查询等任务.隐私保护数据聚集技术主要针对聚集节点可能被俘获的情况,研究在聚集节点不能获知感知数据的前提下实现数据聚集,并对聚集结果进行完整性验证;数据查询隐私保护技术主要面向 Top-*k* 查询[13]、范围查询[14−17]和类型查询[18]中的数据隐私保护问题,针对两层传感器网络中高资源节点可能被俘获的情况,研究在高资源节点不能获知感知数据和查询信息的前提下实现查询操作,并对查询结果进行完整性验证.传感器网络数据隐私保护技术在保护目标、攻击模型、网络模型和保护方法等方面与位置隐私保护技术存在明显区别.

1.2 基于位置服务中的位置隐私保护技术

随着无线通信技术和智能移动终端的广泛应用,基于位置的服务 LBS(location based service)[19,20]得到飞速发展与普及.基于位置的服务是指:移动终端利用各种定位技术获得当前位置信息,再通过无线网络得到某项服务.早期的 LBS 系统主要用于在紧急情况下快速定位求助者的位置以实施救援.当前,LBS 已经广泛应用在军事、交通、物流、医疗、民生等领域中.

用户在接受服务的同时并不希望向外界泄露自身的位置信息,这就对 LBS 位置隐私保护技术提出了要求.在 LBS 中,位置信息既包括当前的具体位置,也包括对象的移动轨迹、行为习惯等.最常用的 LBS 位置隐私解决方案是空间伪装[21],即:用户将位置伪装成为一个区域之后再发送给服务提供商,服务提供商则根据用户所提供的区域信息为用户提供服务.在这种方式下,服务提供商无法准确得知用户的位置.实际上,位置隐私保护强度和服务质量是一对矛盾关系,需要用户根据具体情况进行选择.现有的 LBS 位置隐私保护技术研究主要从两个方向展开:一是依赖可信任第三方机构的隐私保护方法,另一个是基于网络 *k*-匿名的方法.一些复杂攻击手段的出现,例如推测攻击[22]、共谋攻击[23],也为 LBS 位置隐私保护技术研究提出了新的挑战.LBS 位置隐私保护技术为传感器网络位置隐私保护技术研究提供了参考,但由于应用场景、网络模型、攻击模型等方面差异明显,并不能直接应用于传感器网络中.

1.3 新型网络下的位置隐私保护技术

硬件技术的快速发展和人们日益增长的应用需求推动了新型传感网的发展,车载传感网、参与式感知网络、多基站室内定位网络等新型网络已经成为学术界的研究热点.在新型网络的实际应用中,位置隐私保护仍然是一个关系到未来发展前景的重要研究课题.当前,对新型网络位置隐私保护技术的研究主要有两类:一类是面向 LBS 中的位置隐私保护[24],另一类是面向本文中提到的传感器网络中的位置隐私保护.针对传感器网络中各类型攻击,通常采用虚假源/基站[25,26]、网络匿名[27]、通信静默[28]、数据中转[29]等机制保护源节点和基站的敏感位置信息.由于新型网络在应用目标、通信模式、网络架构等方面与传感器网络存在差异,新型网络中的位置隐私保护技术与传感器网络既有联系又有区别,传感器网络位置隐私保护技术研究可以为新型网络提供一定的支持.

2 研究模型

2.1 网络模型

传感器网络位置隐私保护技术一般针对单层传感器网络,网络中不存在高资源节点,所有节点初始能量、通信能力、存储能力、计算能力都是相似的.而攻击者在硬件设备上具有明显的优势,因此能量更充足,通信能力、存储能力、计算能力也更强;同时,局部攻击者具备一定的移动能力.

2.2 攻击模型

基于已有研究成果中对攻击者的定义,我们从攻击模式、攻击视角和攻击手段这 3 个角度来对攻击模型进行界定.攻击模式分为普通攻击模式和复杂攻击模式两类,攻击视角分为局部视角和全局视角两类,攻击手段依据攻击者所使用的具体技术分为监听、逐跳回溯追踪、流量分析、ID 分析、时间关联分析、节点俘获和数据篡改 7 类.

2.2.1 攻击模式

根据攻击者是否对网络正常性能施加影响,将攻击模式分为普通攻击模式和复杂攻击模式:

- 在普通攻击模式中,攻击者不对网络的性能产生影响,攻击者采用诚信但好奇模型[30],作为外部节点存在,采取监听、逐跳回溯追踪、流量分析等非主动攻击手段获取源节点和基站节点的位置信息;
- 在复杂攻击模式中,攻击者主动对网络的正常性能施加干扰,通常使用节点俘获、克隆等主动攻击手段进入网络内部,作为内部节点截获源节点和基站节点位置信息;同时,可以对感知数据进行篡改、丢弃,甚至直接进行路由风暴攻击和耗尽攻击,导致网络瘫痪.

现有的成果主要关注普通攻击模式,对复杂攻击模式的研究较少.

2.2.2 攻击视角

攻击者按照可以监听的网络范围分为两类:全局视角攻击者和局部视角攻击者.全局攻击者具有良好的设备条件,一般使用一组由多个网络侦听器、网络抓包工具和配套服务器组成的无线监听设备,实现对整个网络通信状况的监听;局部攻击者不具备全局攻击者的设备条件,通常只依靠自身携带的侦听设备对自身周围一定半径范围内局部网络的通信状况进行监听.全局攻击者倾向于使用窃听和流量分析、ID 分析、时间关联分析结合的攻击方式,局部攻击者倾向于使用窃听和逐跳回溯追踪结合的攻击方式.

2.2.3 攻击手段

攻击者常用的攻击手段包括以下 7 类,其中,监听、逐跳回溯追踪、流量分析、ID 分析和时间关联分析属于非主动攻击手段,节点俘获和数据篡改属于主动攻击手段:

(1) 监听:攻击者对节点间的通信进行监听,分析无线信号的特点.这是实现逐跳回溯追踪、流量分析、时间关联分析等攻击的基础.在监听的同时,攻击者也会尝试通过窃取和截获的方式得到消息包中的数据内容,通常把这种攻击手段称为数据窃听;

(2) 逐跳回溯攻击:通过逐跳地反向追踪数据包的来源来确定源节点或基站节点的位置,是局部攻击者最常用的攻击方式.如图 1 所示,攻击者通常使用配备多个天线的无线电测向仪(radio direction finder)[31,32],通过三角定位法确定信号发送节点的位置,图中 A1 和 A2 为天线.当确定信号发送节点位置后,攻击者立刻移动到该节点,并继续对无线信号进行监听.重复以上过程,局部攻击者就可以通过逐跳回溯追踪的方式找到源节点或基站节点的位置;

(3) 流量分析:流量分析包括网络热点分析和数据包分析两种方式.在监测型传感器网络中,敏感事物所在范围内的传感器节点的通信量会比其他节点高一些,因此,攻击者可以在对全网或局部区域网络监听的前提下,通过网络通信热点分析来确定源节点或基站节点的位置;攻击者也可以通过分析节点接收和发送数据包的大小、时间间隔等属性来确定数据流的起始节点和目的节点;

(4) ID 分析:攻击者通过获得先验消息或窃听数据包信息的方式来获得节点的 ID 信息,并通过监听分析得出节点 ID 与网络拓扑之间的对应关系;

(5) 时间关联分析:攻击者通过观察节点与其邻居节点之间消息发送操作的时序相关性来推断消息数据的传输路径;

(6) 节点俘获:攻击者通过俘获网络中的单个或多个节点,参与到网络通信中,既可以获得加密密文、通信协议、拓扑结构等敏感消息,也可以对网络节点进行克隆.文献[33]中给出了俘获和克隆网络中部分节点来控制通信,进而推测出网络拓扑结构和节点位置信息的攻击方法;

(7) 数据篡改:攻击者对消息包中的数据进行恶意修改、删除或虚假消息注入,影响网络的正常性能.

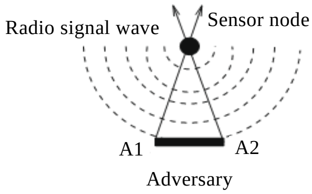


Fig.1 Radio detection model of adversary[32]
图 1 攻击者无线信号探测模型[32]

针对主动攻击,部分文献给出了攻击手段.例如:文献[34]中,攻击者可以在固定节点引发路由阻塞,并通过监听该节点的消息交互获得敏感信息;文献[33]认为,在俘获或克隆节点后,通过对比该节点在网络中和不在网络中两种情况下汇聚结果的差别来分析网络的拓扑和位置信息,当同时俘获或克隆多个节点时,该攻击的效果较好.由于以上攻击手段使用较少,所以不作为本文的重点讨论内容.

2.3 协议分类标准

已有的位置隐私保护研究成果可以从不同角度进行分类:按照保护对象不同,位置隐私保护协议可以分为源位置保护协议和基站位置保护协议;按照所能抵御的攻击模式不同,位置隐私保护协议可以分为普通攻击保护协议和复杂攻击保护协议;按照所针对的攻击视角不同,位置隐私保护协议可以分为局部攻击保护协议和全局攻击保护协议.

在本文中,我们按照协议中所使用的位置隐私保护策略,将现有研究成果分为路径伪装、陷阱诱导、通信控制和网络匿名 4 大类.按照所使用的具体技术,进一步将路径伪装策略划分为随机游走机制和多路径机制两类,将陷阱诱导策略划分为环路陷阱机制和虚假源/基站机制两类,将通信控制策略划分为静默机制、跨层机制、网络编码、定向通信和数据中转机制这 5 类.

2.4 性能评价模型

评价位置隐私保护技术的性能指标主要有 4 类:抵御的攻击手段、位置隐私保护强度、网络通信质量和能耗控制.

(1) 抵御的攻击手段:位置隐私保护技术往往需要同时面对局部攻击者和全局攻击者的多种攻击方式,位置隐私保护协议抵御的攻击手段类型反映了协议的适用性;

(2) 位置隐私保护强度:用来衡量位置隐私保护算法的安全强度.目前还没有统一的评价标准,已有研究成果往往选用自己提出的安全标准对位置隐私保护强度进行评价.较为常用的两个评价指标是安全周期和逃脱概率:安全周期是指敏感事物被攻击者捕获前,源节点可以执行的通信周期的个数,也可以认为是能够发出的消息数据包的个数;逃脱概率是指在一定的时限内,敏感事物不被攻击者捕获的概率;

(3) 网络通信质量:采用位置隐私保护协议后,网络的通信时延、通信速率、端到端投递率等方面的性能;

(4) 能耗控制:能耗控制是位置隐私保护技术中的重要研究内容,位置隐私保护技术必须在提供高强度位置隐私保护的同时对网络整体能耗进行控制,尽量减小对网络生命周期的影响.网络能耗通常使用通信能耗与节点计算能耗之和来衡量.

3 无线传感器网络位置隐私保护技术

本节中,按照路径伪装、陷阱诱导、网络匿名和通信控制这 4 种策略,将现有的无线传感器网络位置隐私保护研究工作进行了分类,每一种策略下又按照协议采用的具体技术划分为了多个小类.对各个协议的核心原理和特点进行了描述,并简要分析了协议的性能.

3.1 基于路径伪装策略的位置隐私保护技术

路径伪装策略是指在传感器节点通信时,源节点不选择最短路径传输数据,而是故意选择某一条或某多条伪装路径作为通信链路,以达到迷惑攻击者、延长位置隐私保护安全周期的目的.路径伪装策略的主要实现方法为随机游走机制和多路径机制.

3.1.1 随机游走机制

随机游走机制最早应用在传感器网络路由协议设计中,用来解决网络能耗不均衡问题.在单播随机游走机制中,每个邻居节点被选择为转发节点的概率是 $1/N$(N 为邻居节点数).洪泛可以被认为是随机游走的特殊形式,即,每个邻居节点被选择为转发节点的概率都是 100%.单纯随机游走并不能满足源位置隐私保护的需求,原因有两个:一是可能形成路由环路,二是过高的能耗和时延.在单纯随机游走过程中,当前节点的任意邻居节点都有可能成为下一跳目的节点,包括已经转发过该消息的节点,当数据包再次传输到已经转发过该消息的节点时,传输路径会形成路由环路.路由环路不能够很好地实现位置隐私保护效果,因为当局部攻击者监听范围足够大时,可以直接跳过环路到达上游节点.文献[35]中的仿真结果证明,攻击者只需要追踪单纯随机游走路径跳数的 1/5 就可以找到源节点.同时,由于路径的随机性,单纯随机游走常常会导致明显的冗余能耗和冗余时延问题,并且网络规模越大,平均冗余能耗就越多,平均冗余时延也越长.

因此,基于随机游走机制的位置隐私保护协议基本都对单纯随机游走进行了改进,增加了新的技术,延长了安全周期,提升网络的通信质量和能耗控制.

Ozturk 等人[2,35]提出了 PR(phantom routing)协议和 PSPR(phantom single-path routing)协议,首次将随机游走方法引入到了位置隐私保护中.PR 协议分两个阶段实施:

- 第 1 阶段中,节点将自身邻居节点划分成两个方位相反的集合,源节点准备发送信息时,首先在一个集合中随机选择一个邻居节点作为转发节点,转发节点从远离上一跳节点的集合中选择一个节点继续转发数据包.当数据包传输达到指定跳数,或数据包无法继续转发时,第 1 阶段结束,并将此时数据包所在的节点指定为幻影源节点;
- 第 2 阶段中,幻影源节点通过洪泛将数据包发送到基站节点.PSPR 算法将集合划分方法由相对方位改为了相对跳数,并且在第 2 阶段中,幻影源节点使用单播方法将数据包传送到基站节点.

Shaikh 等人[36]提出的 IRL(identity, route, location)协议采用了与 PR 类似的方法,节点根据与基站的相对地理位置将邻居节点分为 4 个集合,并为每个邻居节点计算信任度.当源节点生成消息时,通过集合和信任度来共同决定转发节点.

Xi 等人[37]提出了 GROW(greedy random walk)协议,要求源节点和基站同时进行随机游走,两段随机游走的目的节点是网内的同一个代理节点.当源节点和基站节点发出的消息都通过随机游走到达代理节点时,两段随机游走的路径组合起来就得到了从源节点到基站节点的随机游走路径.为防止路由环路出现,GROW 协议在数据包中添加了布隆过滤器.GROW 协议的另一个特点是贪婪性,随机游走路径的生成以覆盖尽量多的节点为目标,协议中的两段随机游走都设定了最小跳数,在达到最小跳数之前,中间不选择代理节点作为下一跳目的节点.GROW 协议在保护强度和能耗控制性能上优于 PR 算法.

Wang 等人[38]首先定义了攻击者侦听范围这一概念,认为只要源节点在攻击者的侦听范围内就会被攻击者识别出来,并以此为依据提出了基于位置角度的随机游走协议 PRLA.图 2 给出了攻击者在追踪过程中发现源节点的示例.图中虚线区域为幻影源节点可能存在的范围,r 为攻击者的监听半径.从图中可以看到:攻击者在对幻影源节点 $P1$ 进行追踪的过程中会发现源节点的位置.PRLA 的实现步骤是:首先,网内节点维护其邻居节点的地理位置信息,当基站节点以洪泛方式发出查询时,在消息中携带基站节点位置信息,所有节点在接收到查询消息后计算邻居节点的相对角度,用相对角度来计算每个邻居节点的转发概率,依据概率从邻居节点中随机选择一个节点作为下一跳目的节点.中间节点在接到消息后,首先根据源节点位置将自身邻居节点划分为两个集合:离源节点位置更近的集合和离源节点位置更远的集合.在离源位置更远的集合中,根据相对角度计算每个节点的转发概率,根据概率随机选择转发节点,并转发消息,直到无法继续转发或满足 h 跳要求为止.选择当前节点作为

幻影节点,将数据包通过最短路径传送给基站节点,该幻影节点可以防止源节点在追踪过程中被攻击者发现的问题.实验结果表明 PRLA 的平均安全周期比 PSPR 长 50%.

陈娟等人[39]同样基于攻击者侦听范围提出了基于源节点有限洪泛的源位置隐私保护协议 PUSBRF.该协议不仅可以保证前 h 跳均朝着远离真实源节点的方向游走,而且可以保证幻影源节点具有地理位置的多样性.另外,考虑到具有更强侦听能力的攻击者,文中提出了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,并且使用避开可视区的广播策略,使得数据包在最短路径路由过程中能够完全逃离可视区.该协议可以在不增加计算开销的前提下避免失效路径的产生,显著提高了源位置隐私的安全性.

Li 等人[40,41]提出一个基于复合环的源位置隐私保护协议 NMR(network mixing ring),在该协议中,多个节点围绕基站组成一个复合环,环上的节点称为环节点.环节点又分为中继环节点和普通环节点,中继节点上会生成中继虚假消息,虚假消息在混合环上传播.环内节点使用邻居共享密钥来对数据包进行加密解密操作和传输操作,因此在攻击者看来,环内节点之间一直在传输不同的消息.图 3 给出了一个混合环的示意图.协议执行步骤是:源节点产生数据包后,首先在网内随机找到一个既不在混合环内又距离源节点 h 跳远的节点作为媒介节点,源节点通过随机游走将数据包发送到媒介节点,媒介节点再将该消息发送到混合环上.消息到达混合环后,将隐藏在虚假信息中传输到基站节点.文献[41]中还给出了位置隐私保护强度度量的 3 个参数,分别是源节点位置泄露指数、源节点空间泄露指数和归一化源节点空间泄露指数,做出了建立隐私保护强度评价标准的初步尝试.

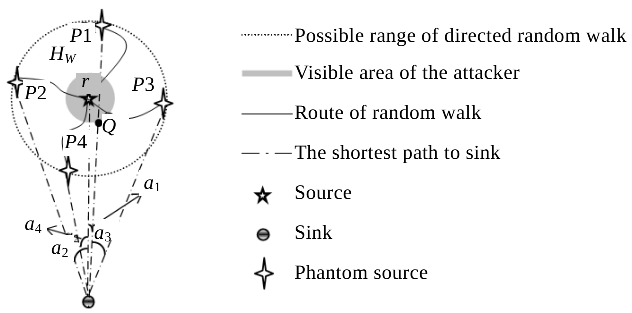


Fig.2 Trace process of adversary[38]

图 2 攻击者的追踪过程[38]

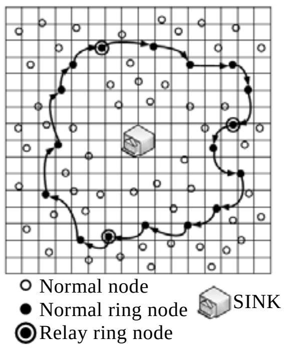


Fig.3 Mixing ring of NMR algorithm[40]

图 3 NMR 协议混合环结构[40]

Kang 等人[42]提出了 LPSS(location privacy support scheme)协议,LPSS 协议中引入了梯度的概念,节点以到基站的跳数为梯度指数,节点距离基站的跳数越多,梯度指数就越大.网内节点以一定概率选择向同梯度或是低梯度的邻居节点发送数据包,选择概率的设定可以平衡位置隐私保护强度和通信时延.向同梯度节点发送数据,则位置隐私保护能力更强,但数据包端到端时延也越长;向低梯度节点发送数据则端到端时延更短,但位置隐私保护强度也随之降低.当一个节点发送真实数据包时,它同时生成具有 h 跳生命期的虚假数据包,并向任意一个远离基站节点的大梯度方向传输.虚假数据包和梯度机制的结合可以对局部攻击者造成迷惑,同时保护源节点和基站位置隐私.

Lightfoot 等人[43]提出了 STaR(sink toroidal region routing)协议,在提供高强度位置隐私保护的同时控制了网络的能耗.STaR 算法的思想是:幻影节点应当位于一个合适的区域内,离源节点既不太近也不太远.因此,STaR 算法将网络划分成多个网格,然后在基站节点周围设置一个圆环形的 STaR 区域,基站节点位于该区域的中心位置.当源节点准备发送数据包时,它首先在 STaR 区域中随机选择一个幻影坐标,将数据包发往该幻影源坐标所在的网格,并指定网格中的头节点为幻影节点.当幻影坐标所在的网格中不存在节点时,选取传输路径上最后一个节点所在网格的头节点作为幻影节点.幻影节点通过最短路径单播方式将数据包传送到基站节点.在数据传输过程中,节点采用动态 ID 机制,全网周期性更换 ID,以防止 ID 隐私泄露.与 STaR 的思路类似,Li 等人[36]也基

于幻影节点位置的选择机制提出了 RRIN 协议,以在局部攻击和全局攻击下保护源节点的位置信息.在 RRIN 协议中,源节点首先将消息传输到网络中随机选择的代理节点上,由于单纯的随机代理节点机制并不能在全局攻击下保护源节点的位置隐私,RRIN 又给出了基于角度和象限的多代理节点选择算法.RRIN 协议的缺点是需要网络中的节点维护代理节点和基站的地理位置信息,在一定程度上约束了算法的适用范围.

文献[45]针对逐跳回溯追踪攻击提出了基于机会路由机制的位置隐私保护协议.在基础协议中,中间节点在转发消息前,首先通过握手机制优先选择离基站近的节点作为下一跳转发节点,转发节点的选择随着数据传输周期而动态变化,以达到节省能量的目的.由于基础协议在抵御逐跳回溯追踪攻击时无法提供足够的安全强度,文中又给出了 3 种改进机制,分别是无握手机制、随机延迟转发机制和随机握手转发机制.实验结果证明,随机延迟转发机制能够在隐私保护强度和网络性能之间达到较好的均衡.

SPENA[46]协议的设计目标是解决网络监听和节点俘获情况下的位置隐私保护问题.攻击者通过监听可以获得网络流量信息,通过俘获节点可以获得报文中的敏感数据,从而推测敏感位置信息.在 SPENA 协议中,节点内嵌两个哈希函数、一个映射函数和一个重构函数.第 1 个哈希函数用来生成单向哈希链以标记数据源节点,第 2 个哈希函数与映射函数结合来确定路由链路上的中间重构节点.中间重构节点使用重构函数对数据包进行重构,并使用节点-基站共享密钥加密,最后,通过多跳链路将重构后的数据包转发到基站.攻击者无法在重构后的数据包和重构前的数据包之间建立联系,因此无法有效地对网络流量进行监听.SPENA 协议可以分别抵御网络中的逐跳回溯攻击和节点俘获攻击以及两者的联合攻击.

Lopez 等人[47]为传感器网络位置隐私保护协议的实用性制定了 3 个条件:一是转发节点与基站的距离不能大于源节点与基站的距离;二是中间节点在进行数据流转发时必须均匀地选择各个邻居节点;三是虚假数据流和真实数据流不能相交.基于以上 3 个条件,文中分两种情况给出了基于随机游走机制的位置隐私保护协议.当攻击者仅仅进行流量监听攻击时,网络同时传输一组真实数据包和一组虚假游走数据包,转发节点的选择以短投递时延和流量均匀分布为原则;当攻击者具有节点俘获能力时,节点自动依据设定的扰动参数将转发路由表的顺序扰乱,通过设置扰动参数,可以在位置隐私保护强度和通信性能之间进行调整.

Zhou 等人[48]基于蚁群算法给出了高效节能的源节点位置隐私保护算法.在 EELP 协议中,节点被看做人工蚂蚁,节点路由表中记录与邻居节点间链路的信息素数量,当节点需要转发数据时,它以信息素、节点距离和剩余能耗为参数选取下一跳目的节点.经过一定的数据转发周期后,网络会进行挥发和沉积操作,以帮助节点调整信息素数量,进而调整数据传输路径,达到节省全局能量的目的.为提高数据传输路径的随机性,达到位置隐私保护的目的,文中给出了 LRP-EELP 协议为单个链路的信息素数量设置阈值,减少单个链路重复选择的概率,以及 LPU-EELP 协议来增加未被选节点的转发概率.蚁群算法的引入,可以在实现位置隐私保护的同时较好的控制网络的整体能耗.

文献[49]给出了基于随机数据采集的移动基站位置隐私保护协议 LPMS(location privacy for mobile sinks).在 LPMS 中,节点将感知数据的拷贝随机传输并存储到其他节点,基站节点在网络中随机移动,并收集它周围邻居节点上存储的数据.LPMS 对流量分析、逐跳回溯追踪、时间关联分析、移动轨迹预测等多种攻击方式具有良好的防御效果.图 4 给出了 LPMS 协议实现的示意图.

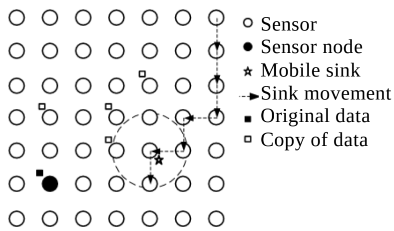


Fig.4 Data collection of LPMS[49] protocol

图 4 LPMS[49]协议消息采集机制

图 4 中,原始数据的拷贝分散存储在网络中的多个节点上,只要基站节点通信范围覆盖到任何一个存储有数据拷贝的节点,就可以完成数据的传输.LPMS 协议的缺点是基站移动的随机性容易导致较长的数据采集时间延迟,当网络中数据量较多时,简单的随机存储机制会引发过多的能耗,并引发节点缓存溢出,明显降低数据采集的成功率.

文献[50]给出了一种全新的针对随机游走机制的攻击模型,全局攻击者通过整合网络边界节点的通信状况,可以推测出使用随机路由机制的源节点位置.该攻击模型的提出,给基于随机游走机制的传感器网络位置隐私保护研究提出了新的挑战.

3.1.2 多路径机制

路径伪装策略的另一个方法是多路径机制.在局部攻击者进行逐跳回溯追踪时,需要追踪在同一路径上传输的一系列数据包才能准确定位源节点的位置,完成追踪所需要的数据包的数量由攻击者的监听范围和攻击者与源节点的距离共同决定.通常情况下,攻击者距离源节点较远,且攻击者的监听范围有限,因此,攻击者需要对较多数量的数据包进行追踪才能到达源节点.多路径机制中,源节点在传输每一个数据包时,在多条可用的备选传输路径中随机选择一个,这样,多个数据包就经不同路径传输到基站,增大了局部攻击者的监听难度.

文献[32]针对局部攻击者的逐跳回溯追踪给出了 RP(random parallel routing)和 WRS(weighted random stride)算法,针对全局攻击者的流量分析攻击给出了 WRSE(weighted random stride extended)算法.RP 算法基于简单的并行多路径机制,路径设置时互不相交,并且覆盖尽量大的网络区域,每条路径的选择概率与路径长度成正比.RP 算法在数据传输过程中仍然存在泄漏源节点相对方位的风险,为此,WRS 算法提出了类似 PRLA 算法的解决方案,节点将源节点与基站节点的相对方位作为考虑对象,以避免相对方位信息的泄漏.WRSE 算法在多路径机制的基础上引入了虚假消息机制和间隙式数据发送方法,虚假消息机制可以误导全局攻击者的流量分析攻击,间隙数据发送方法可以使时间关联攻击失效.

3.2 基于陷阱诱导策略的位置隐私保护技术

陷阱诱导策略是指在攻击者进行无线监听时,通过在网络中故意设置路由环路、虚假数据源或虚假基站节点,将攻击者吸引到陷阱中,使攻击者在路由环路中不停地重复监听-移动过程,或因认为成功找到真实源节点而在虚假源节点或虚假基站附近长时间停留.陷阱诱导策略的两个具体实现方法是虚假源/基站机制和环路陷阱机制.

3.2.1 虚假数据源/基站机制

基于虚假数据源的源位置隐私保护协议——SLFSR(short-lived fake source routing)协议最早由 Kamat 等人[35]提出.在 SLFSR 协议中,当节点接收到真实数据包时,有一定概率生成虚假数据包,并发送给邻居节点.为节省网络能量,邻居节点直接丢弃虚假数据包.通过调整生成概率,可以平衡网络能耗和位置隐私保护强度.与基于随机游走的 PR 协议相比,SLFSR 协议的能耗更大;同时,一跳式的虚假数据包转发机制并不能很好地延长源位置隐私保护的安全周期.

文献[35]还提出 PFSR(persistent fake source routing)协议来提供更加有效的源位置隐私保护.PFSR 协议对 SLFSR 协议的改进是使用了主动式虚假数据发送机制,不只是接收到数据包后才决定是否发送虚假消息,而是自主地向网络中发送虚假数据消息.文献[35]中还指出,虚假源节点在网络中的位置对保护效果有明显的影响.

Mehta 等人[51]提出了 PeCo(periodic collection)协议来应对全局流量分析攻击.PeCo 不但可以实现源位置隐私保护,还可以实现基站位置隐私保护.在 PeCo 协议中,节点与每个邻居之间共享独立的密钥,当节点接收到数据包后,将解密后的数据包加入到一个先进先出队列中,每个节点都启动一个传输定时器,当定时器期满时,选择队列中的第 1 个数据包,加密后发送给下一跳节点.如果队列中没有消息,则发送虚假数据包.虚假数据包在到达下一跳节点时即被丢弃.为保证网络投递率,节点必须要有足够大的存储空间来保存数据包队列.为实现基站位置隐私保护,网络中构建了一个虚拟主干网结构,主干网的设置要求是需要将基站覆盖在通信范围内.节点向基站传输数据时,不是直接将数据传输到基站节点,而是将数据转发到主干网上,主干网上的节点将接收到信息在主干网内进行洪泛,这样就可以保证基站节点在不泄露位置隐私的同时接收到消息.

Shao 等人[52]提出了 3 种方法来优化虚假数据流的发送操作:第 1 种方法使用时隙式数据传输机制,节点在每个时隙到来时发送加密的真实数据或虚假数据,攻击者难以区分真实数据包和虚假数据包,但是网络中的虚假数据流量较大,能量浪费严重,且通信时延较长;第 2 种方法和第 3 种方法分别基于指数分布模型和统计模型来控制虚假数据的传输,相比于时隙式传输方案,这两种方法对全局流量分析攻击的针对性更强,抵御效果更好,同时减少了虚假数据发送量,节省了网络能耗.

TARP(timing analysis resilient protocol)[53]主要针对流量分析攻击.协议采用统一化通信模式,要求所有节点以相同速率发送相同数量的由多个数据包组成的大小相同的数据组合.数据组合中的每个数据包有对应的目的节点,当接收到数据组合时,节点将指向它的数据包保存在缓存中.当发送计时器清零时,将需要发送的消息封装成一个或多个新的数据组合广播出去,大小不足一个数据组合的,用虚假信息填充.节点采用邻居共享密钥加密数据组合,因此,攻击者无法区分数据组合中的数据包.M-TARP(multipath-TARP)和 A-TARP(adaptive-TARP)对 TARP 协议进行了改进.M-TARP 协议使用多播代替单播,增加了保护强度.A-TARP 协议采用自动适配计时器代替固定计时器,节点根据通信量动态调整数据发送速率,以保证网络通信质量.文献[54]中指出,A-TARP 协议对网络热点分析攻击的防御能力较差.

Chen 等人[55]提出了一系列位置隐私保护协议 FRW(forward random walk),DBT(dynamic bidirectional tree)和 ZBT(zigzag bidirectional tree):

- 在 FRW 协议中,数据的转发基于简单的邻居节点集合划分和前向随机游走机制,不能满足位置隐私保护的需求;
- 在 DBT 协议中,首先在源节点和基站之间建立一条定向随机游走路径,路径上的节点按照跳数距离划分为临近源节点的集合和临近基站的集合:临近源节点集合中的节点上建立虚假数据源分支,临近基站集合中的节点上建立虚假基站分支.图 5 给出了 DBT 的实例,网络中共生成了 3 条虚假数据源分支和 3 条虚假基站分支;
- ZBT 协议中,基站在相反的方位授权两个代理基站节点,源节点授权一个 i 跳节点作为代理源节点.真实数据包按以下路径传输:从真实源节点到代理源节点,再到距离最远的代理基站节点,最后到达真实基站节点.在传输过程中,中间节点按照 DBT 协议中的方法来生成虚假分支,并发送虚假数据包.图 6 给出了 ZBT 的一个实例,A 为代理源节点,B 为代理基站节点,网络中存在 4 个虚假源分支和 3 个虚假基站分支.

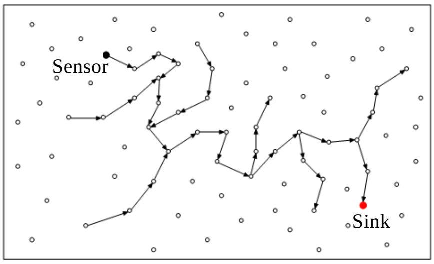


Fig.5 Dummy routing of DBT protocol[55]

图 5 DBT 协议的虚假通信机制[55]

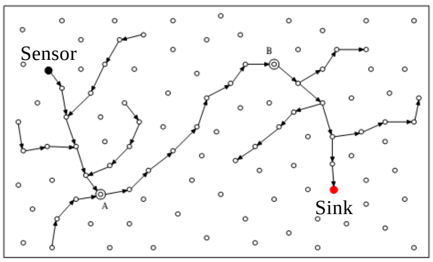


Fig.6 Dummy routing of ZBT protocol[55]

图 6 ZBT 协议的虚假通信机制[55]

DBT 和 ZBT 协议可以同时保护基站位置和源位置的隐私,对于逐跳回溯攻击的防御效果较好,但是由于虚假分支数量多,能量消耗比较大.

Mahmoud 等人[56]设计了一种利用虚假通信在源节点周围区域形成虚拟流量云来隐藏源节点位置的方法.流量云随着真实数据的发送产生,多个局部区域的流量云可以在发生交汇时进行融合,同时,每个节点上的数据包处理机制可以保证数据包随每一跳数据传输发生变化.因此,攻击者无法通过流量分析和时间关联分析来确定源节点的位置.协议中还引入了虚假 ID 机制来保护节点的 ID 隐私.

Xiao 等人[57]基于虚假数据源机制给出了可以应对全局攻击者的 GFS 协议.与之前的研究不同,GFS 能够支持被动式的 RFID(radio frequency identification),网络中的节点配备了 RFID 读取设备.在 GFS 协议中,虚假数据源节点通过传输虚假令牌来模拟敏感事物的位置和移动轨迹,以达到误导攻击者的目的.隐私保护的强度与网络中传输的虚假令牌的数目成正比.

文献[33]首先给出了 3 种关联协作攻击模型,接着,针对通过节点俘获、克隆、局部共谋来推测敏感位置信息的复杂攻击方式,给出了基于加密机制和虚假数据机制的 PPSS 算法,既保证在汇聚节点不泄露隐私的情况下完成聚集操作,又提供了位置隐私保护功能.文中基于 PPA[58]算法提出了 PPSRA 协议,通过在用户和汇聚中心间共享私钥,实现了对网络动态行为的高适应性.同时,针对在节点加入、离开过程中存在的位置隐私泄露问题,提出了使用汇聚中心虚假数据来增加真实数据权重、克服传统差分隐私方法数据污染问题的 DDRI 算法.

文献[59]对虚假数据源机制的位置隐私保护性能进行了仿真研究,评估了虚假数据传输速率、路由碰撞和隐私保护强度三者之间的关系.实验结果证明:虚假数据传输速率并不与位置隐私保护强度呈完全的正相关,在较低的范围内,数据传输速率的提高可以增加隐私保护强度;然而,过高的数据传输率会引发更多的路由碰撞,反而降低位置隐私保护的效果.

文献[60]基于虚假基站机制实现了基站位置隐私保护.网络中存在多个随机选定的与真实基站有一定距离的虚假基站节点,当需要进行数据传输时,真实数据包仍然按照最短路径传输,多个源节点通信路径上的交叉节点自动作为代理节点向虚假基站节点发送虚假消息,每个代理节点可以同时向多个虚假基站发送消息,以增加对攻击者的误导.文献[60]的方法可以延长攻击者发现基站节点的时间,隐私保护的强度与虚假基站节点的虚假链路的数目成正比.

Chai 等人[61]基于虚假基站机制提出了满足 k-匿名条件的基站位置隐私保护协议.虚假基站的定位需要同时考虑通信能耗和隐私保护强度问题,文中将这一对冲突问题转换成了非线性优化问题:首先,基于遗传算法给出了近似定位算法 GAQO;接着,作为对已给出算法的改进,基于人工势场给出了更高效的近似算法 APQO.通过对虚假基站节点的近似最优定位,GAQO 和 APQO 算法可以在满足隐私保护需求的前提下尽量降低网络的通信能耗.

Taha 等人[25]提出了 FPC 协议来保护车载传感网(VANET)中的位置隐私.在车载传感网中,攻击者可以很容易地通过 RSS(received-signal-strength)攻击确定节点的位置,简单地使用功率控制和噪声添加,并不能很好地保护位置隐私.FPC 协议使用虚假数据源机制来实现节点位置隐私保护,协议共包含两个部分:

- 一是同一个通信热点范围内的节点都选择同一个位置作为虚假位置,并通过信号功率调整将自己的位置映射到该虚假位置上.这样,当攻击者对信号强度进行检测时,无法将单个节点从多个节点中区分出来;
- 二是在网络中引入不规则网格划分机制,在每个网格中确定虚假位置以增加攻击者错误判断的概率,提升位置隐私的保护效果.

文献[26]针对多基站传感网进行节点定位时的位置隐私保护问题给出了 SLRS 协议.在多基站节点定位网络中,多个基站通过接收到的节点信号的强度和到达时间来确定移动节点的位置,同时,攻击者通过定向和定时的发送虚假消息来误导基站的判断.因此在 SLRS 协议中,系统将多个基站随机划分为一些集合,通过集合内部多个基站的合作可以确定移动节点的位置,同时,集合外部的基站可以通过发送虚假探测消息来伪装成集合内部基站.攻击者由于无法确定集合的内部成员基站节点,因此也无法进行定向和定时的虚假信号攻击.

3.2.2 环路陷阱机制

环路陷阱机制是指在网络中故意设计路由环路,攻击者在进行逐跳追踪时会被引入到路由环路中,只有当攻击者具有环路检测功能并且经过逐跳追踪回到环路起始节点时,才有可能发现处于环路陷阱中.

CEM[62]算法采用了环路陷阱机制,网络中的每个节点以概率 p 决定是否作为环路初始点来发起陷阱环路,当某节点作为环路发起者时,会在两个随机选择的邻居节点间建立一条不包含发起节点的路由环路作为陷阱环路.当环路上有节点在转发真实数据包时,陷阱环路开始运行,接到基站发送的停止消息后,陷阱环路停止运

行.为解决能耗过高的问题,文中提出了概率转发机制,陷阱环路上的节点以一定的概率在环路上继续发送虚假消息.

iHIDE[63]算法引入了虚拟环和逻辑链路结构.网络中存在多个互不相交的环,每个环上有一个主节点,称为 BUNs 节点,网络中存在一条逻辑链路将各个主节点连接起来,基站节点作为一个端点.当源节点发送数据时,首先将数据包发送到最近的 BUNs 节点上,BUNs 节点将数据包继续转发到逻辑链路上的下一个 BNUs 节点,直到数据包到达基站节点.同时,BUNs 节点将该数据包的备份在虚拟环上传输,以达到诱导攻击者的目的.另外,iHIDE 协议中还引入了伪命名空间机制防止 ID 分析攻击.

3.3 基于匿名策略的位置隐私保护技术

网络匿名机制通常只针对 ID 分析攻击,目标是在实现数据传输的过程中,通过隐藏敏感节点的 ID 信息来实现节点位置的隐私保护,一般不考虑逐跳回溯追踪、流量分析、时间关联分析等攻击方式的影响.

文献[64]提出了基于标签交换机制和分层加密机制的 DCARPS 协议,同时实现基站和源节点的 ID 匿名隐私保护.协议分 6 个阶段执行,分别执行 ID 分配、拓扑感知、拓扑树建立、路由机制创建、标签分层加密和基站命令下发操作.在路由阶段,引入负载均衡策略进行能耗控制.文中进一步对 DCARPS 协议进行了改进,给出了基于概率的 P-DCARPS 算法.在 P-DCARPS 算法中,节点可以拥有多个标签和多条指向基站的通信路径,在数据传输时通过概率方式选择通信路径.

Chen 等人[65]提出了 EAC(efficient anonymous communication)协议来实现源节点和基站的 ID 匿名.在 EAC 协议中,每个节点分配 1 个 ID、两个随机数 a 和 b 以及两个 hash 函数 H1 和 H2.节点使用随机数、hash 函数和节点 ID 以及节点与基站的最短跳数分别生成全局匿名身份 AI、广播匿名身份 BAI、一跳匿名身份信息 OHAI 和匿名确认身份信息 AAI.当源节点准备向基站发送数据时,它以概率 p 选择一个邻居节点,并以它的 OHAI 为目的发送消息.消息由 3 部分组成:第 1 部分是用邻居共享密钥加密的 OHAI 信息;第 2 部分是用基站-源节点共享密钥加密的感知数据信息;第 3 部分是源节点的 AI 信息,用来帮助基站节点确定密钥.中间节点接收到信息后,返回 AAI 给发送节点,用下一跳节点的 OHAI 更新消息的第 1 部分,并将数据包发送给下一跳节点.这种消息转发方式可以保证路由过程中 ID 信息不会被泄露,但是隐私保护的操作过程复杂,节点需要维护和更新的信息也比较多.从文献[66]可以看出:基于哈希函数的ID匿名策略与基于环签名机制[66]的ID匿名策略在面对以监听为主的 ID 分析攻击时效果都比较好;但是在面对通过俘获节点获得 ID 信息的恶意攻击时,基于哈希函数的策略可以通过分配一对一的随机数和哈希函数来保证 ID 隐私,而环签名机制更容易泄露 ID 隐私信息.

MQA(max query aggregation)[67]协议设计的目标是,在最大值汇聚过程中隐藏节点的 ID 信息.网络为层次树型结构,基站为根、传感器节点为叶子.每个节点与基站间有独立的共享密钥.节点感知数据转换为一个 i 位的二进制整型数值,网络通过 i 轮查询来获得结果,每轮只检查 1 位.当节点的第 1 位为 1 时,则下一轮继续上传第 2 位;如果第 1 位为 0 且网络中存在第 1 位不为 0 的节点,当前节点设为非活动节点,下一轮不再上传数据.如果上轮中所有节点的数据都为 0,则下一轮所有活动节点继续上传数据.最后一轮的活动节点中,数值最大的即为最大值节点,它的取值即为最大值.通过 i 轮的数据上传操作,基站可以在不泄露所有节点 ID 的前提下获得网络的最大值,但是数据聚集的时间也被明显的延长了.

为防止攻击者通过获取报文消息内容来确定源节点的 ID 信息,Li 等人[68]针对传统的多项式报文加密技术存在的最大阈值问题,给出了一种基于椭圆曲线加密技术的网络匿名协议.源节点在选择密钥时,从一组不可区分的公钥组中进行选择,加密消息在传输过程中进行逐跳身份认证,因此,当节点中存在俘获节点时,节点的 ID 信息也不会被泄露.由于协议中使用的椭圆曲线加密技术确保了数据的完整性,当基站连续接收到不完整信息时,可以通过对密钥取交集操作来确定被俘获节点的 ID.因此,文中给出的方法可以较好地实现节点的 ID 匿名隐私.

Christin 等人[27]为解决参与式感知网络中的位置隐私问题提出了 TrustMeter 协议.在参与式感知网络中,攻击者可以通过关联节点 ID 和所发送的消息来分析获取节点的隐私位置信息,单纯的加密机制会对节点间的协作感知产生影响.因此在 TrustMeter 协议中,节点采用相遇时才进行消息的交换和传输的机会机制来保证 ID 匿

名;同时,协议基于周期性运行的三元组对等评级(peer-based rating)机制确定每个节点的可信任等级,并识别恶意节点.TrustMeter 可以在保证协作感知效率的前提下抵御恶意节点发起的路由风暴攻击、时延攻击和数据包丢弃攻击.

3.4 基于通信控制策略的位置隐私保护技术

通信控制策略是指从修改网络通信协议的角度出发,通过调整网络常用的通信模式来防止攻击者获得敏感信息,从而为传感器网络提供位置隐私保护功能,主要采用静默、跨层路由、网络编码、定向通信和数据中转这 5 种机制.静默机制是指在检测到攻击者时,在一定区域范围内停止节点间通信,保持无线静默状态直到攻击者离开;跨层路由机制针对攻击者只监听网络层数据传输的特点,提出了使用 MAC 层传输感知数据,绕过攻击者监听的方法;网络编码机制针对时间关联攻击和流量分析中的数据包分析攻击,通过在消息传输过程中对数据进行重新编码来保证位置隐私信息安全;定向通信是指节点在传输数据时使用定向天线,只向指定的方向传输数据,从而降低被攻击者监听的概率;数据中转机制针对局部攻击者逐跳追踪的特性,通过在网络中设置移动中转节点,使得通信链路由连续的变为分段式的,以达到增加攻击者追踪难度的目的.

3.4.1 静默机制

文献[69]提出了 ALBS(anti-localization by silencing)协议,该协议将网络划分成多个网格,假设节点可以检测到攻击者,并且网格边界附近的节点可以发现攻击者的跨格行为.当网格内的某个节点检测到攻击者时,该网格保持静默,直至攻击者离开.检测到攻击者离开的边界节点向攻击者的目的网格发送警告消息,并在本网格内广播激活消息.

文献[70]提出了 CALP(context-aware location privacy)协议.与 ALBS 协议类似,网络中节点也具有检测攻击者的能力.当检测到攻击者时,节点通过 MAC 层向周围节点发送警告消息,消息内容包括攻击者所在位置和根据攻击者监听距离划定的最小安全区域.当最小安全区域内的节点作为通信链路的中间节点时,节点可以选择两种操作:一是保持完全静默,将接收到的数据包缓存,等到攻击者离开后再进行传输;二是将接收到的消息向远离攻击者位置的方向转发.当网络中存在最小安全区域时,所有通过最小安全区域的链路都需要进行路由更新,寻找不经过最小安全区域的通信链路.

文献[28]中给出了基于静默机制的多基站定位网络位置隐私保护协议 CBS&MBS,协议考虑了在以节点为中心和以架构为中心的两种不同网络模型下的内部攻击和外部攻击问题.网络中同时放置了多个活动基站和多个静默基站,静默基站仅仅接收信息而不发送信息.攻击者在进行攻击时,只能确定活动基站的位置,发送相应的误导信号.因此,静默基站和活动基站通过协作可以识别攻击者上传的虚假位置消息.同时,协议还引入了基于活动基站的时间阈消息来抵御外部攻击者的节点位置俘获攻击,引入了节点响应时间附加验证来抵御重放攻击.

3.4.2 跨层路由机制

文献[71]基于 IEEE 802.15.4 协议提出了跨层路由位置隐私保护机制 CLS(cross layer solution).攻击者在进行窃听攻击时一般只关注网络层通信,而不会窃听 MAC 层通信.在 IEEE 802.15.4 协议中,节点可以在睡眠和工作两种状态间切换,以降低网络能耗,节点间周期性地传输信标实现链路维护.信标由帧结构、MAC 层控制信息和负载等部分组成.CLS 协议将所要传输的敏感数据加载在信标的负载部分中.由于信标是按时间间隔发送的,且负载部分的空间有限,单纯依靠信标机制进行数据传输的时延问题比较严重.因此,CLS 协议采用了枢纽节点的方法,源节点在发送消息时,选择一个 h 跳节点作为枢纽节点,并将数据加在信标中首先传送到该枢纽节点,枢纽节点接收到数据后,作为虚假源节点将数据通过网络层转发到基站.

3.4.3 网络编码机制

网络编码机制中,允许节点对所传输的数据包进行重新编码,既可以将一个数据包拆分成多个,通过多条不同路径传输到目的节点,也可以将多个数据包整合成一个,再发送到目的节点.将网络编码机制应用在位置隐私保护中,可以有效防止流量分析攻击,通过中间节点对数据包重新编码,攻击者在全局流量监听时,无法建立接收数据和发送数据之间的对应关系,也就无法分析数据的流向.但是,网络编码机制不能直接应用在位置隐私保

护中,原因是攻击者可以通过全局编码向量GEV(global encoding vectors)[72]获得所需要的敏感信息.因此,Fan等人[72,73]给出了两种适用于传感器网络的基于网络编码机制的位置隐私保护算法 PPSNC(privacy-preserving scheme for network coding)和 SUNC(source un-observability by network coding):

- 在PPSNC算法中,通过对GEV进行同态加密操作,可以同时保证数据流的不可追踪性和数据隐私安全性,有效地阻止流量分析攻击.协议还提供了随机编码功能,基站节点能够以很高的概率恢复源节点数据包;
- SUNC 算法引入了一种特殊的虚假消息机制,虚假消息由同态密文和虚假数据组成,虚假消息与真实数据一起被解码,并且无法区分.节点在感知到敏感数据时直接发送真实数据,在没有感知到敏感数据时发送虚假消息.攻击者既无法通过识别真实消息和虚假消息获得感知数据,也无法通过关联接收数据和发送数据对数据流向进行分析.

需要特别指出的是:网络编码机制在密集型网络中的性能优于稀疏网络;同时,同态加密算法的使用,也对节点的计算能力提出了更高的要求.

3.4.4 定向通信机制

文献[74]给出了一种结合了定向天线、传输控制和数据压缩的源位置隐私保护技术.定向天线的使用可以带来两方面的优势:一是定向发送的特性能够降低数据包被局部攻击者监听的概率;二是定向天线会增加攻击者实现全局监听攻击的难度,并且定向天线波束宽度越小,实现全局监听的难度就越大.为降低网络能耗,文中采用了基于熵的信息压缩方法,只在被监测事物状态发送变化的时刻上传数据,而不是周期性地进行数据传输.定向天线的引入,较好地解决了隐私保护强度和能耗性能之间的均衡问题.

3.4.5 数据中转机制

在 MSS[75]协议中,Li 等人基于局部攻击者共谋的假设提出了半全局攻击模型,然后给出了位置隐私α角度匿名的定义,即真实源节点的位置以均匀概率分布在攻击者认定的方向的正负α角范围内,并基于网络中的移动数据骡(data mules)节点,以一定时延为代价实现了源节点的α角度匿名.MSS 协议的实现分为 3 个阶段:首先,源节点选择任意一个方向来发送数据;接着,中间节点将数据转发给数据骡节点,数据骡节点携带数据继续进行随机游走;最后,数据骡节点将数据发送回普通节点,并由普通节点将数据继续发送到基站.数据骡节点携带数据的距离越长,则攻击者越难确定源节点的位置,但是数据传输的时延也越长.

STAP[29]协议针对车载传感网中的位置隐私保护进行了研究.STAP 的主要思想是:车辆通常会有很高的概率经过一些社会热点区域,例如大型超市、繁忙的十字路口等,因此可以在这些热点区域中放置一些存储和通信能力较强的节点来帮助车辆间进行数据传输.当车辆 A 要发送数据给车辆 B 时,A 先将加密数据包转发到附近的某个车辆 C 上,C 将该数据带到社会热点区域并上传到存储节点,存储节点可以通过路过的车辆将数据拷贝到其他社会热点区域中.当车辆 B 经过存储有该数据包的热点区域时,就可以不泄露位置隐私的完成数据传输任务.在 STAP 协议数据传输过程中,存储节点是可信的,因此能够较好地同时抵御局部攻击和全局攻击.

4 对比分析

近年来无线传感器网络位置隐私保护技术正受到学术界越来越多的关注,已有很多重要的研究成果.网络部署环境、攻击者采用的攻击模式、攻击视角、攻击手段、用户安全需求的多样性,都与位置隐私保护技术的性能有着密切的关系,因此需要从多个角度来对位置隐私保护技术的性能进行综合评价.我们从协议保护对象、实现难度、抵御的攻击手段、隐私保护强度、网络通信质量和能耗控制性能等方面对现有的研究成果进行了对比分析,并采用表格的形式从不同角度对主要协议进行了分类总结.表 1 总结分析了现有研究成果的优缺点.

Table 1 Advantages and disadvantages of location privacy-preserving solutions

表 1 位置隐私保护协议的优缺点

协议名称	策略	主要技术	主要优点	主要缺点
PRS&PSRS[2,35]	路径伪装	随机游走	局部攻击隐私保护度较强	无法防御全局攻击
IRL[36]			考虑了节点信任度	存在环路问题
GROW[37]			安全周期长	时延较长;不适用于大规模网络
PRLA[38]			同时考虑了侦听范围和相对角度	需要节点地理位置信息;计算量大
PUSBRF[39]			隐私保护度强,能耗较低	需要节点地理位置信息
NMR[40,41]			同时防御逐跳回溯和热点监听攻击	混合环上节点能量消耗过快
LPSS[42]			可根据需求调整隐私保护强度	容易受网络边界的影响
STaR[43]			能耗控制效果较好;动态更换 ID	虚拟环区域容易成为攻击对象
RRIN[44]			同时防御局部和全局攻击	节点需要维护全网地理位置信息
文献[45]			局部攻击防御较好	握手机制造成冗余时延
SPENA[46]			能够抵御节点俘获攻击	实现较为复杂
文献[47]			考虑了通信时延控制	隐私保护强度需要提高
EELP[48]			基于蚁群算法进行能耗控制	需要节点具备一定计算能力
LPMS[49]			动态的 sink 节点,隐私保护效果好	时延较长
RP&WRS[32]		多路径	局部攻击安全周期较长	泄露方位信息
WRSE[32]			全局攻击隐私保护度较强	没有进行能耗控制
PFSR&SLFSR[35]	陷阱诱导	虚假源/基站	可在保护强度和能耗之间调整	不能保证稳定的保护强度
PeCo[51]			可以实现源和基站位置隐私保护	能耗较大
文献[52]			概率统计模型保证安全性和低能耗	效果依赖概率统计模型
TARP[53]			抵御时间关联分析攻击	攻击者容易被吸引到高通信量区域
DBT&ZBT[55]			隐私保护度较强	能耗较大
文献[56]			隐私保护度较强	流量云能耗较大
GFS[57]			支持 RFID	隐私保护强度与能耗成正比
PPSS[33]			同时保护数据和位置隐私	仅适用于数据聚集操作
文献[60]			交叉节点可以提升安全强度	能耗较高
GAQO&APQO[61]			优化了通信能耗	需要全局位置信息
FPC[25]			有效抵御信号追踪攻击	对节点硬件性能有要求
SLRS[26]			抵御时间关联攻击和信号追踪攻击	仅适用于基站数目较多的网络
CEM[62]		环路陷阱	成功捕获时安全周期长	有一定失败概率
iHIDE[63]			捕获成功率较高,隐私保护度较强	时延较长,冗余能耗多
DCARPS[64]	匿名策略	网络匿名	隐私保护度强	实现复杂
EAC[65]			ID 匿名、防止节点俘获和消息篡改	实现较为复杂
MQA[67]			完全实现 ID 匿名	只适用于最值聚集,上传轮数过多
文献[68]			ID 隐私保护强度高	需要节点具备一定计算能力
TrustMeter[27]			能够抵御恶意攻击	评级操作会增加能耗
ALBS[69]	通信控制	静默机制	网格区域利于确定攻击者位置	需要节点具备额外的攻击检测能力
CALP[70]			网络通信时延较低	寻找新链路时容易导致丢包问题
CBS&MBS[28]			较好的抵御信号追踪攻击	需要移动基站支持
CLS&DCLS[71]		跨层路由	MAC 层通信可以绕过攻击者的监听	通信时延较长
PPSNC[72]		网络编码	同时实现数据隐私和位置隐私	仅适用于密集网络,计算复杂
SUNC[73]			同时实现数据隐私和位置隐私	计算复杂
文献[74]		定向通信	实现了安全、通信和能耗之间的均衡	需要物理层硬件支持
MSS[75]		数据中转	数据骡机制提供了高强度隐私保护	需要移动中转节点,存在冗余时延
STAP[29]			同时抵御局部和全局攻击	需要布置存储节点,通信性能不稳定

表 2 对现有研究成果的保护对象和所抵御的攻击手段进行了汇总对比,其中,保护对象包括源节点位置隐私和基站位置隐私.

Table 2 Security of location privacy-preserving solutions

表 2 位置隐私保护协议的保护对象和抵御的攻击手段

协议名称	策略	主要技术	保护对象		抵御的攻击手段						
			源位置	基站位置	监听	逐跳回溯追踪	流量分析	ID 分析	时间关联分析	节点俘获	数据篡改
PRS&PSRS[2,35]	路径伪装	随机游走	√		√	√					
GROW[37]			√		√	√					
PRLA[38]			√		√	√					
PUSBRF[39]			√		√	√					
NMR[40,41]			√		√	√	√				
LPSS[42]			√	√	√	√					
STaR[43]			√		√	√		√			
RRIN[44]			√		√	√	√				
文献[45]			√		√	√					
SPENA[46]			√		√	√				√	
文献[47]				√	√	√					
EELP[48]			√		√	√					
LPMS[49]				√	√	√	√		√	√	√
RP&WRS[32]		多路径	√		√	√					
WRSE[32]			√		√	√	√		√		
PFSR&SLFSR[35]	陷阱诱导	虚假源/基站	√		√	√					
PeCo[51]			√	√	√		√		√		
文献[52]			√		√		√		√		
TARP[53]			√		√		√		√		
DBT&ZBT[55]			√	√	√	√	√				
文献[56]			√		√		√		√		
GFS[57]			√		√	√					
PPSS[33]			√		√		√			√	
文献[60]				√	√	√					
GAQO&APQO[61]				√	√	√	√				
FPC[25]				√	√	√					
SLRS[26]				√	√	√					
CEM[62]		环路陷阱	√		√	√					
iHIDE[63]			√		√	√	√	√			
DCARPS[64]	网络匿名	网络匿名	√	√	√	√		√			
EAC[65]			√		√		√	√		√	√
MQA[67]			√		√	√		√			
文献[68]			√		√			√		√	
TrustMeter[27]			√		√			√			
ALBS[69]	通信控制	静默机制	√		√	√					
CALP[70]			√		√	√					
CBS&MBS[28]				√	√	√					
CLS&DCLS[71]		跨层路由	√		√		√		√		
PPSNC[72]		网络编码	√		√		√				
SUNC[73]			√		√		√				
文献[74]		定向通信	√		√	√					
MSS[75]		数据中转	√		√	√					
STAP[29]			√		√	√	√				

(1) 从总体上看,现有的位置隐私保护研究成果尚未较好地实现隐私保护强度、通信质量和网络能耗控制三者之间的均衡.路径伪装策略基于随机游走机制,由于通信路径变长,对通信质量和能量消耗有一定影响,而且在面对逐跳回溯追踪攻击时,通常只能在一定范围内延长网络的安全周期,位置隐私保护的强度需要进一步提升;陷阱诱导策略可以提供较高强度的位置隐私保护,但是由于使用虚假数据流方法,且隐私保护强度与虚假数据传输量呈正相关,因此难以进行能耗控制.当网络中虚假通信量较大时,还容易引发路由阻塞问题,降低网络的通信质量;网络匿名策略主要针对 ID 分析攻击,对

时间关联、通信热点分析等攻击的防御效果比较一般,并且通常与具体的查询操作类型相关,通用性较差;通信控制策略基于静默、跨层路由、网络编码、定向通信、数据中转等机制实现位置隐私保护,安全强度较高,能量消耗较低,但是改变了最优的数据传输方式,通信时延往往较长,端到端投递率容易受到影响,同时,对硬件支持的要求也较高.

(2) 路径伪装策略中,现有成果以保护源位置隐私为主,对基站位置隐私保护的研究不多.在实现难度方面,随机游走机制实现简单,不需要路由维护操作,节点的计算代价和存储代价较小;多路径机制需要在网络中同时保证多条通信路径的连通,路由维护比较复杂.在抵御的攻击手段方面,所有的路径伪装策略都可以应对逐跳回溯追踪攻击,NMR 和 WRSE 引入了虚假数据流机制来应对流量分析攻击;SPENA 协议通过使用数据包重构机制,可以同时抵御局部攻击和节点俘获攻击;LPMS 利用节点的移动性,可以同时抵御多种攻击.在隐私保护强度方面,多路径机制的位置隐私保护效果强于随机游走机制,在随机游走机制中,PRLA,PUSBRF,NMR,RRIN 和 LPMS 分别引入了侦听范围概念、混合环方法、象限方法和基站移动机制,位置隐私保护强度优于其他协议.在通信质量方面,随机游走和多路径机制受到路径跳数变多的影响,通信时延和丢包率都会有所上升.在能量消耗方面,STaR 协议引入虚拟环区域减小了能量消耗,EELP 协议基于蚁群算法进行了通信能耗优化,而 NMR 和 WRSE 由于使用虚假数据源机制,通信能耗比其他协议大.在适用的网络方面,随机游走机制和多路径机制都只适用于小规模网络,在大规模网络中使用时要引入附加技术来控制路径的长度,以缩短通信时延,节省网络能量.

(3) 陷阱诱导策略中,越来越多的研究开始关注基站位置隐私保护.其中,DBT&ZBT 可以同时实现基站和源位置隐私保护,FPC 协议和 SLRS 协议对车载传感网和多基站传感网的位置隐私保护进行了关注.在抵御的攻击手段方面,多数协议针对流量分析攻击和逐跳回溯追踪攻击.另外,iHIDE 协议使用伪命名空间机制来防止 ID 分析攻击.文献[52]的方案通过控制虚假数据流的传输机制,可以防止时间关联分析攻击.在隐私保护强度方面,虚假数据源/基站机制的隐私保护强度较高,对流量分析攻击和逐跳回溯追踪攻击的防御效果都比较好.其中:PeCo 协议实现了移动轨迹的匿名隐私;环路陷阱机制存在一定的捕获概率,当攻击者被陷阱捕获时,安全周期较长,当攻击者没有被陷阱捕获时,安全周期与路径长度有关,使用逻辑链路的 iHIDE 协议的捕获概率明显高于普通协议 CEM.文献[59]中的研究证明:虚假数据的发送速率并不是越高越好,过高的发送速率会引发路由碰撞问题,导致位置隐私保护强度的降低.在通信质量方面,网络中的虚假数据通信较少时,通信的时延仅与通信路径的长度相关,数据包投递率也较高;当虚假数据通信较多时,路由碰撞问题容易影响网络的正常通信.其中,PeCo 协议、文献[52]的方案和 TARP 协议由于使用了数据传输管理机制,通信时延比其他协议更长.在能量消耗方面,虚假数据源/基站机制和环路陷阱机制的能耗都较高,其中:PRS&PSRS 只进行一跳虚假数据包发送,能耗相对较低,但隐私保护强度也较差;文献[61]通过优化虚假基站定位机制,降低了网络的通信能耗;文献[52]引入了概率统计模型来减少虚假数据的发送量,能耗也相对低一些.

(4) 网络匿名策略中,协议保护源位置和基站位置隐私,在提供 ID 匿名的同时,也针对逐跳回溯追踪和流量分析攻击给出了一些保护方法.在协议实现复杂程度方面:DCARPS 协议共分 6 个阶段实现,同时还使用概率方法和多路径机制,实现较为复杂;EAC 协议基于分段加密机制和 hash 机制生成多重匿名身份,管理过程较为复杂;MQA 协议实现较为简单,但是只能执行网络极值汇聚操作;TrustMeter 协议需要周期性地进行评级操作,节点维护的信息也比较多.在隐私保护强度方面,5 种协议都给出了健壮的 ID 匿名机制,EAC 协议还可以同时防止节点俘获和消息篡改攻击,TrustMeter 协议可以抵御路由风暴、通信时延、数据包删除等恶意攻击.在通信质量方面,MQA 需要在 i 轮查询后才能获得结果,通信的时延较长.在能量消耗方面:DCARPS 提出了负载均衡策略进行能耗控制;EAC 在网络初始化阶段,其通信能耗和计算能耗都比较大;MQA 虽然查询轮数较多,但每次上传的数据量较小,总体能耗不大;文献[68]采用椭圆曲线加密方式,计算能耗较高.

(5) 通信控制策略中,现有研究成果以保护源位置隐私为主,并且往往需要网络提供相应的支持.例如,静默机制要求节点具备攻击者检测能力,跨层路由假设攻击者不监听 MAC 层通信,网络编码机制要求普通节点具有较强的同态加密计算能力,定向通信和数据中转需要具有相应功能的通信天线系统和节点设备.在抵御的攻击手段方面,静默机制仅针对逐跳回溯追踪攻击,网络编码仅抵御流量分析攻击,定向通信和数据中转机制以防御逐跳回溯追踪攻击为主.在隐私保护强度方面:网络编码机制可以同时实现高强度的位置隐私保护和数据隐私保护;跨层路由机制能够直接绕过攻击者的监听,隐私保护的强度与 MAC 层通信链路的长度呈正相关;静默机制在面对耐心的攻击者或多个攻击者时的隐私保护效果不佳;定向通信和数据中转机制能够提供较高的隐私保护强度.在通信质量方面:静默机制容易引发通信时延、路由断路、丢包等问题;跨层路由机制由于信标结构的负载空间有限,通信时延一般较长;数据中转机制的通信时延受中转节点的影响较大;定向通信和网络编码机制的通信质量较好.在能量消耗方面:通信控制策略的能耗都相对较低;静默机制的能耗与路由重建有关;跨层路由机制的能耗由中枢节点的选择决定,网络编码的计算能耗较高,但通信能耗较低;而定向通信和数据中转机制都不会额外增加网络的通信能耗.

5 未来工作展望

传感器网络位置隐私保护技术属于新兴研究领域,值得关注;同时,物联网的快速发展也给位置隐私保护技术提出了更高的要求,很多挑战性问题需要进一步研究:

(1) 建立位置隐私保护强度评价体系

在进行位置隐私保护强度评价时,现有的研究大多基于各自协议中提出的不同评价参数和标准.随着研究成果的增多,对通用位置隐私保护强度评价体系的需求也越来越迫切.独立于具体应用场景的通用评价体系是对研究成果进行精确性能对比的基础.同时,由于传感器网络应用场景的多样性和复杂性,全面而通用的位置隐私保护强度评价体系的建立也面临着巨大的挑战.文献[41]对提出通用的隐私保护强度评价参数做了尝试,定义了节点位置泄露指数、节点空间泄露指数等安全指标;文献[76]提出了在位置隐私保护中对受攻击的风险进行评估的观点,但是都没有进行更深入的研究.位置隐私保护强度评价体系的建立可以从两个角度入手:一是以攻击手段为中心,分别建立节点在各类型攻击下的安全标准,给出节点安全参数,例如逐跳回溯追踪攻击下的最大通信周期、全局流量分析下的平均定位时间等;二是以保护机制为中心,为各机制制定位置隐私保护评价标准,例如虚假数据源机制下的最小误导距离、数据中转机制下的逃脱概率等.位置隐私保护强度评价体系的建立将是一个长期的并且不断修正的过程.

(2) 位置隐私保护强度与网络通信质量、能耗控制性能的均衡问题

能量、计算能力、存储能力等资源的受限性,是传感器网络的重要特征.然而位置隐私保护算法往往需要较大的通信量、计算量和能量消耗,会明显影响网络的通信性能,并直接缩短网络的生命周期.传感器网络位置隐私保护协议的优化目标是:在安全强度、能耗控制和通信质量三者之间取得平衡,在保证高强度位置隐私保护的前提下,尽量减少能量消耗,降低通信时间延迟,提高数据投递率.现有的基于路径伪装和陷阱诱导的研究成果往往存在着高通信时延或高通信能耗的缺点,为提升协议的性能,需要将研究重点放在改进隐私保护的效率上,通过对伪装路径的合理规划和虚假陷阱的优化定位来增加防御的成功率,减少不必要的冗余虚假通信.

(3) 与物理层相结合的位置隐私保护技术

实现隐私保护强度、能耗控制和通信质量三者之间的均衡,是传感网位置隐私保护研究的目标.现有的基于协议层的研究并不能很好地解决这个问题,而与物理层相结合的位置隐私保护技术为这一目标的实现提供了新的途径.物理层设备的引入,可以改变网络原有的通信模式、数据处理模式和网络结构,从而使攻击者的攻击失效,能够在不增加额外能耗和不影响网络通信性能的前提下达到位置隐私保护的目的.文献[74]将逐跳回溯追踪攻击隐私保护技术与物理层相结合,基于定向通信天线设备,较好地实现了高安全强度低能耗低时延的位置隐私保护协议.目前,尝试与物理层技术结合的位置隐私保护研究还比较少,在未来的研究中,需要根据不

同的攻击方式选择相应的物理层设备,如定向天线、移动存储节点等,从实现网络局部的位置隐私入手,逐步实现全网的位置隐私保护.

(4) 复杂攻击环境下的位置隐私保护技术

随着无线传感器网络的快速发展,网络场景日趋多样化,应用需求日趋复杂化,对网络安全、数据隐私与位置隐私的要求越来越高;同时,攻击者的攻击能力越来越强,攻击方式也越来越复杂.在普通攻击环境下,攻击者仅作为外部节点存在,采用诚信但好奇模型,对网络使用监听、逐跳追踪、流量分析、时间相关性分析、信号传播角度分析等方式进行攻击.但是在复杂攻击环境下,攻击者可以通过俘获、控制、伪造传感器节点进入网络内部,对敏感数据进行窃取和篡改,采用路由风暴攻击和耗尽攻击来影响网络正常通信,甚至直接导致网络瘫痪,严重威胁传感器网络的信息安全和网络安全.现有的研究成果主要针对普通攻击进行防御,对复杂攻击环境下恶意攻击的研究还比较少,也不能很好地满足复杂攻击环境下位置隐私保护的要求.为保证在复杂攻击环境下位置隐私保护协议的安全性能,必须根据位置隐私保护的需求设计相应的信息认证、访问控制和异常节点检测机制,并通过局部成员节点之间的协作,例如簇成员、网格成员、加密链成员等,来提高对重放、耗尽、删除等恶意攻击的防御能力.

(5) 位置隐私保护技术与数据隐私保护技术结合

物联网技术的进步,明显推动了无线传感器网络的发展,传感器网络在军事、智慧城市、智慧交通、智能家居、穿戴式系统等领域的应用范围越来越广泛.在很多应用场景中,攻击者逐渐开始倾向于实施集成了数据窃听、流量分析、节点俘获、逐跳回溯追踪等多种攻击手段的综合式攻击,以达到同时获取网络的数据隐私信息和位置隐私信息的目的.因此,在未来的研究中,必须有针对性地提出既能保护数据隐私又能保护位置隐私的双重隐私保护算法.两种技术结合的难点在于都存在较为复杂的攻击模型,并且数据隐私保护算法通常与具体应用场景有关,如数据聚集、top-*k* 查询、范围查询、连续监测查询等.因此,在与数据隐私保护技术结合时,位置隐私保护技术也必须根据具体的应用场景和攻击者的行为模式来考虑位置隐私泄露的渠道,给出有针对性的位置隐私保护方法.同时,数据隐私保护查询中常用的两层网络结构也给位置隐私保护技术的实现提供新的机遇,由于配备了能量充足、计算能力强的高资源节点,在进行位置隐私保护时,可以选择更多的方法.

(6) 新型网络中的位置隐私保护技术

随着传感器网络技术的发展和应用领域的拓展,出现了多基站传感网、车载传感网、参与式传感网等新型网络.在这些新型网络中,数据存储、链路选择、路由机制、消息类型等数据传输模式将发生重大变化,攻击者可能采用新型攻击方式进行攻击,因此,网络中将会出现新的隐私保护内容和隐私泄漏渠道.例如:多基站定位传感网中,攻击者欺骗或俘获基站的可能性增大,基站位置隐私保护将成为重点研究内容;车载传感网中,除通信模式变化外,信息的实时性显得更加重要,对位置隐私保护算法时延控制性能的要求更高;参与式传感网可能拥有更多用户类型,用户位置、身份信息和查询模式等敏感信息的保护将变得更加重要.多种新型网络应用的出现,也对组件式位置隐私保护技术和个性化位置隐私保护技术的研究提出了要求.当前的研究大多基于特定的应用场景和特定的攻击类型,移植性较差,能够具有广泛适用范围的、与具体应用场景无关的组件式位置隐私保护技术是未来重要的研究方向.新型网络应用正逐步进入人们的日常生活,对于相同的应用,不同的用户可能会有不同的位置隐私保护需求,相同的用户在不同的时间和地点也可能有不同的位置隐私保护需求.如何根据用户的不同需求提供个性化的位置隐私保护,也正在成为未来研究的一个重点.

致谢 本文部分工作是在作者访问中国人民大学的萨师煊大数据管理和分析中心时完成的,该中心获国家高等学校学科创新引智计划(111 计划)等资助.

References:

[1] Ren FY, Huang HN, Lin C. Wireless sensor networks. Ruan Jian Xue Bao/Journal of Software, 2003,14(7):1282−1291 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/14/1282.htm

[2] Ozturk C, Zhang Y, Trappe W. Source-Location privacy in energy-constrained sensor network routing. In: Proc. of the 2nd ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN 2004). IEEE, 2004. 88−93. [doi: 10.1145/1029102.1029117]

[3] Fan YJ, Chen H, Zhang XY. Data privacy preservation in wireless sensor networks. Chinese Journal of Computers, 2012,35(6): 1131−1146 (in Chinese with English abstract). [doi: 10.3724/SP.J.1016.2012.01131]

[4] He WB, Liu X, Nguyen H, Nahrstedt K, Abdelzaher T. Pda: Privacy-preserving data aggregation in wireless sensor networks. In: Proc. of the 26th IEEE Int'l Conf. on Computer Communications INFOCOM. IEEE, 2007. 2045−2053. [doi: 10.1109/INFCOM. 2007.237]

[5] Zhang F, He L, He WB, Liu X. Data perturbation with state-dependent noise for participatory sensing. In: Proc. of the 32th IEEE Int'l Conf. on Computer Communications INFOCOM. IEEE, 2012. 2246−2254. [doi: 10.1109/INFCOM.2012.6195610]

[6] Liu CX, Liu Y, Zhang ZJ, Cheng ZY. High energy-efficient and privacy-preserving secure data aggregation for wireless sensor networks. Int'l Journal of Communication Systems, 2013,26(3):380−394. [doi: 10.1002/dac.2412]

[7] Yang DJ, Fang X, Xue GL. Truthful incentive mechanisms for *k*-anonymity location privacy. In: Proc. of the 32th IEEE Int'l Conf. on Computer Communications INFOCOM. IEEE, 2013. 2994−3002. [doi: 10.1109/INFCOM.2013.6567111]

[8] He WB, Nguyen H, Liu X, Nahrstedt K, Abdelzaher T. iPDA: An integrity-protecting private data aggregation scheme for wireless sensor networks. In: Proc. of the 2008 IEEE Int'l Conf. on Military Communications Conf. MILCOM. IEEE, 2008. 1−7. [doi: 10. 1109/MILCOM.2008.4753645]

[9] Yang G, Wang AQ, Chen ZJ, Xu J, Wang HY. An energy-saving privacy-preserving data aggregation algorithm. Chinese Journal of Computers, 2011, 34(5):792−800 (in Chinese with English abstract). [doi: 10.3724/SP.J.1016.2011.00792]

[10] Castelluccia C, Mykletun E, Tsudik G. Efficient aggregation of encrypted data in wireless sensor networks. In: Proc. of the 2th IEEE Int'l Conf. on Mobile and Ubiquitous Systems: Networking and Services. MobiQuitous: IEEE, 2005. 109−117. [doi: 10.1109/ MOBIQUITOUS.2005.25]

[11] Feng TM, Wang C, Zhang WS, Ruan L. Confidentiality protection for distributed sensor data aggregation. In: Proc. of the 27th IEEE Int'l Conf. on Computer Communications INFOCOM. IEEE, 2008. 56−60. [doi: 10.1109/INFOCOM.2008.20]

[12] Papadopoulos S, Kiayias A, Papadias D. Secure and efficient in-network processing of exact SUM queries. In: Proc. of the 27th IEEE Int'l Conf. on Data Engineering (ICDE 2011). IEEE, 2011. 517−528. [doi: 10.1109/ICDE.2011.5767886]

[13] Fan YJ, Chen H. Verifiable privacy-preserving top-*k* query protocol in two-tiered sensor networks. Chinese Journal of Computers, 2012,35(3):423−433 (in Chinese with English abstract). [doi: 10.3724/SP.J.1016.2012.00423]

[14] Sheng B, Li Q. Verifiable privacy-preserving range query in two-tiered sensor networks. In: Proc. of the 27th IEEE Int'l Conf. on Computer Communications INFOCOM. IEEE, 2008. 46−50. [doi: 10.1109/INFOCOM.2008.18]

[15] Shi J, Zhang R, Zhang YC. Secure range queries in tiered sensor networks. In: Proc. of the 28th IEEE Int'l Conf. on Computer Communications INFOCOM. IEEE, 2009. 945−953. [doi: 10.1109/INFCOM.2009.5062005]

[16] Zhang R, Shi J, Zhang YC. Secure multidimensional range queries in sensor networks. In: Proc.of the 10th ACM Int'l Symp. on Mobile Ad Hoc Networking and Computing. ACM Press, 2009. 197−206. [doi: 10.1145/1530748.1530777]

[17] Chen F, Liu AX. SafeQ: Secure and efficient query processing in sensor networks. In: Proc. of the 29th IEEE Int'l Conf. on Computer Communications INFOCOM. IEEE, 2010. 1−9. [doi: 10.1109/INFCOM.2010.5462094]

[18] Subramanian N, Yang K, Zhang W, Qiao D. ElliPS: A privacy preserving scheme for sensor data storage and query. In: Proc. of the 28th IEEE Int'l Conf. on Computer Communications INFOCOM. IEEE, 2009. 936−944. [doi: 10.1109/INFCOM.2009.5062004]

[19] Zhou AY, Yang B, Jin CQ, Ma Q. Location-Based service: Architecture and progress. Chinese Journal of Computers, 2011,34(7): 1155−1171 (in Chinese with English abstract). [doi: 10.3724/SP.J.1016.2011.01155]

[20] Wang L, Meng XF. Location privacy preservation in big data era: A survey. Ruan Jian Xue Bao/Journal of Software, 2014,25(4): 693−712 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/4551.htm [doi: 10.13328/j.cnki.jos.004551]

[21] Gruteser M, Grunwald D. Anonymous usage of location-based services through spatial and temporal cloaking. In: Proc. of the 1st ACM Int'l Conf. on Mobile Systems, Applications and Services. ACM Press, 2003. 31−42. [doi: 10.1145/1066116.1189037]

[22] Dewri R. Local differential perturbations: Location privacy under approximate knowledge attackers. IEEE Trans. on Mobile Computing, 2013,12(12):2360−2372. [doi: 10.1109/TMC.2012.208]

[23] Zhu ZC, Cao GH. Toward privacy preserving and collusion resistance in a location proof updating system. IEEE Trans. on Mobile Computing, 2013,12(1):51−64. [doi: 10.1109/TMC.2011.237]

[24] Zhang JM, Zhao YJ, Jiang HB, Jia XD, Wang LM. Research on protection technology for location privacy in VANET. Journal of Communications, 2012,33(8):180−189 (in Chinese with English abstract).

[25] Taha S, Shen X. A physical-layer location privacy-preserving scheme for mobile public hotspots in NEMO-based VANETs. IEEE Trans. on Intelligent Transportation Systems, 2013,99:1−16. [doi: 10.1109/TITS.2013.2265311]

[26] Holiday M, Mittal N, Venkatesan S. Secure location verification with randomly-selected base stations. In: Proc. of the 18th IEEE Int'l Conf. on Distributed Computing Systems Workshops (ICDCSW 2011). IEEE, 2011. 119−122. [doi: 10.1109/ICDCSW. 2011. 44]

[27] Christin D, Pons-Sorolla DR, Hollick M, Kanhere SS. TrustMeter: A trust assessment scheme for collaborative privacy mechanisms in participatory sensing applications. In: Proc. of the 9th IEEE Int'l Conf. on Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP 2014). IEEE, 2014. 1−6. [doi: 10.1109/ISSNIP.2014.6827614]

[28] Zeng YP, Cao JN, Hong J, Zhang S, Xie L. Secure localization and location verification in wireless sensor networks: A survey. The Journal of Supercomputing, 2013,64(3):685−701. [doi: 10.1007/s11227-010-0501-4]

[29] Lin XD, Lu RX, Liang XH, Shen XM. STAP: A social-tier-assisted packet forwarding protocol for achieving receiver-location privacy preservation in VANETs. In: Proc. of the 30th IEEE Int'l Conf. on Computer Communications INFOCOM. IEEE, 2011. 2147−2155. [doi: 10.1109/ INFCOM.2011.5935026]

[30] Groat MM, He W, Forrest S. KIPDA: *k*-indistinguishable privacy-preserving data aggregation in wireless sensor networks. In: Proc. of the INFOCOM. IEEE, 2011. 2024−2032. [doi: 10.1109/INFCOM.2011.5935010]

[31] Radio direction finder. http://en.wikipedia.org/wiki/Radio_direction_finder

[32] Wang HD, Sheng B, Li Q. Privacy-Aware routing in sensor networks. Computer Networks, 2009,53(9):1512−1529. [doi: 10.1016/ j.comnet.2009.02.002]

[33] Li S, Zhu HJ, Gao ZY, Guan XP, Xing K, Shen XM. Location privacy preservation in collaborative spectrum sensing. In: Proc. of the 31th IEEE Int'l Conf. on Computer Communications INFOCOM. IEEE, 2012. 729−737. [doi: 10.1109/INFCOM.2012. 6195818]

[34] Hong XY, Wang P, Kong JJ, Zheng QW, Liu J. Effective probabilistic approach protecting sensor traffic. In: Proc. of the 2005 IEEE Int'l Conf. on Military Communications Conf. (MILCOM 2005). IEEE, 2005. 169−175. [doi: 10.1109/MILCOM.2005. 1605681]

[35] Kamat P, Zhang Y, Trappe W, Ozturk C. Enhancing source-location privacy in sensor network routing. In: Proc. of the 25th IEEE Int'l Conf. on Distributed Computing Systems (ICDCS 2005). IEEE, 2005. 599−608. [doi: 10.1109/ICDCS.2005.31]

[36] Shaikh RA, Jameel H, d'Auriol BJ, Lee H, Lee S, Song YJ. Achieving network level privacy in wireless sensor networks. Sensors, 2010,10(3):1447−1472. [doi: 10.3390/s100301447]

[37] Xi Y, Schwiebert L, Shi W. Preserving source location privacy in monitoring-based wireless sensor networks. In: Proc. of the 20th IEEE Int'l Conf. on Parallel and Distributed Processing Symp. (IPDPS 2006). IEEE, 2006. [doi: 10.1109/IPDPS.2006.1639682]

[38] Wang WP, Chen L, Wang JX. A source-location privacy protocol in WSN based on locational angle. In: Proc. of the 2008 IEEE Int'l Conf. on Communications (ICC 2008). IEEE, 2008. 1630−1634. [doi: 10.1109/ICC.2008.315]

[39] Chen J, Fang BX, Yin LH, Su S. A source location privacy preservation protocol in wireless sensor networks using source based restricted flooding. Chinese Journal of Computers, 2010,33(9):1736−1747 (in Chinese with English abstract). [doi: 10.3724/SP.J. 1016.2010.01736]

[40] Li Y, Ren J. Mixing ring-based source-location privacy in wireless sensor networks. In: Proc. of the 18th IEEE Int'l Conf. on Computer Communications and Networks (ICCCN 2009). IEEE, 2009. 1−6. [doi: 10.1109/ICCCN]

[41] Li Y, Ren J, Wu J. Quantitative measurement and design of source-location privacy schemes for wireless sensor networks. IEEE Trans. on Parallel and Distributed Systems, 2012,23(7):1302−1311. [doi: 10.1109/TPDS.2011.260]

[42] Kang L. Protecting location privacy in large-scale wireless sensor networks. In: Proc. of the 2009 IEEE Int'l Conf. on Communications (ICC 2009). IEEE, 2009. 1−6. [doi: 10.1109/ICC.2009.5199372]

[43] Lightfoot L, Li Y, Ren J. Preserving source-location privacy in wireless sensor network using STaR routing. In: Proc. of the 2010 IEEE Global Telecommunications Conf. on GLOBECOM. IEEE, 2010. 1−5. [doi: 10.1109/GLOCOM.2010.5683603]

[44] Li Y, Ren J. Source-Location privacy through dynamic routing in wireless sensor networks. In: Proc. of the 29th IEEE Int'l Conf. on Computer Communications INFOCOM. IEEE, 2010. 1−9. [doi: 10.1109/INFCOM.2010.5462096]

[45] Spachos P, Song L, Bui FM, Hatzinakos D. Improving source-location privacy through opportunistic routing in wireless sensor networks. In: Proc. of the 2011 IEEE Symp. on Computers and Communications (ISCC 2011). IEEE, 2011. 815−820. [doi: 10. 11 09/ISCC.2011.5983942]

[46] Pongaliur K, Xiao L. Maintaining source privacy under eavesdropping and node compromise attacks. In: Proc. of the 29th IEEE Int'l Conf. on Computer Communications INFOCOM. IEEE, 2011. 1656−1664. [doi: 10.1109/INFCOM.2011.5934959]

[47] Lopez J, Rios R, Cuellar J. Preserving Receiver-Location Privacy in Wireless Sensor Networks. Information Security Practice and Experience: Springer-Verlag, 2014. 15−27. [doi: 10.1007/978-3-319-06320-1_3]

[48] Zhou LM, Wen QY. Energy efficient source location privacy protecting scheme in wireless sensor networks using ant colony optimization. Int'l Journal of Distributed Sensor Networks, 2014. [doi: 10.1155/2014/920510]

[49] Ngai ECH, Rodhe I. On providing location privacy for mobile sinks in wireless sensor networks. Wireless Networks, 2013,19(1): 115−130. [doi: 10.1145/1641804.1641825]

[50] Shi R, Goswami M, Gao J, Gu XF. Is random walk truly memoryless-traffic analysis and source location privacy under random walks. In: Proc. of the 32th IEEE Int'l Conf. on Computer Communications INFOCOM. IEEE, 2013. 3021−3029. [doi: 10.1109/ INFCOM.2013.6567114]

[51] Mehta K, Liu D, Wright M. Protecting location privacy in sensor networks against a global eavesdropper. IEEE Trans. on Mobile Computing, 2012,11(2):320−336. [doi: 10.1109/TMC.2011.32]

[52] Shao M, Yang Y, Zhu S, Cao G. Towards statistically strong source anonymity for sensor networks. In: Proc. of the 27th IEEE Int'l Conf. on Computer Communications INFOCOM. IEEE, 2008. [doi: 10.1109/INFOCOM.2008.19]

[53] Majeed A, Liu K, Abu-Ghazaleh N. Tarp: Timing analysis resilient protocol for wireless sensor networks. In: Proc. of the 2009 IEEE Int'l Conf. on Wireless and Mobile Computing, Networking and Communications (WIMOB 2009). IEEE, 2009. 85−90. [doi: 10.1109/WiMob.2009.24]

[54] Silvija KF, Fabrice LF, Predra S. The quality of source location protection in globally attacked sensor networks. In: Proc. of the 2011 IEEE Int'l Conf. on Pervasive Computing and Communications Workshops (PERCOM 2011). IEEE, 2011. 44−49. [doi: 10.1109/PERCOMW.2011.5766931]

[55] Chen H, Lou W. On protecting end-to-end location privacy against local eavesdropper in wireless sensor networks. In: Proc. of the Pervasive and Mobile Computing. 2014. [doi: 10.1016/j.pmcj.2014.01.006]

[56] Mahmoud ME, Shen X. Secure and efficient source location privacy-preserving scheme for wireless sensor networks. In: Proc. of the 28th IEEE Int'l Conf. on Communications (ICC 2012). IEEE, 2012. 1123−1127. [doi: 10.1109/ICC.2012.6363763]

[57] Xiao WC, Zhang H, Wen Q, Li WM. Passive RFID-supported source location privacy preservation against global eavesdroppers in WSN. In: Proc. of the 28th IEEE Int'l Conf. on Broadband Network & Multimedia Technology (IC-BNMT 2013). IEEE, 2013. 289−293. [doi: 10.1109/ICBNMT.2013.6823959]

[58] Shi E, Chan THH, Rieffel EG, Chow R, Song D. Privacy-Preserving aggregation of time-series data. In: Proc. of the Annual Network & Distributed System Security Symp. (NDSS 2011). 2011. 4.

[59] Thomason A, Leeke M, Bradbury M, Jhumka A. Evaluating the impact of broadcast rates and collisions on fake source protocols for source location privacy. In: Proc. of the 12th IEEE Int'l Conf. on Trust, Security and Privacy in Computing and Communications (TrustCom 2013). IEEE, 2013. 667−674. [doi: 10.1109/TrustCom.2013.81]

[60] Yao L, Kang L, Shang P, Wu G. Protecting the sink location privacy in wireless sensor networks. Personal and Ubiquitous Computing, 2013,17(5):883−893. [doi: 10.1007/s00779-012-0539-9]

[61] Chai GF, Xu M, Xu WY, Lin ZY. Enhancing sink-location privacy in wireless sensor networks through k-anonymity. Int'l Journal of Distributed Sensor Networks, 2012. [doi: 10.1155/2012/648058]

[62] Ouyang Y, Le ZY, Chen GL, Ford J, Makedon F. Entrapping adversaries for source protection in sensor networks. In: Proc. of the 2006 Int'l Symp. on on World of Wireless, Mobile and Multimedia Networks (WOWMOM 2006). IEEE, 2006. 23−34. [doi: 10.1109/WOWMOM.2006.40]

[63] Kazatzopoulos L, Delakouridis C, Marias GF, Georgiadis P. iHIDE: Hiding sources of information in WSNs. In: Proc. of the 2th Workshop on Security, Privacy and Trust in Pervasive and Ubiquitous Computing (SECPERU 2006). 2006. 8−48. [doi: 10.1109/SECPERU.2006.11]

[64] Nezhad AA, Miri A, Makrakis D. Location privacy and anonymity preserving routing for wireless sensor networks. Computer Networks, 2008,52(18):3433−3452. [doi: 10.1016/j.comnet.2008.09.005]

[65] Chen J, Du X, Fang B. An efficient anonymous communication protocol for wireless sensor networks. Wireless Communications and Mobile Computing, 2012,12(14):1302−1312. [doi: 10.1002/wcm.1205]

[66] Mei Y, Jiang GZ, Zhang W, Cui YQ. A collaboratively hidden location privacy scheme for VANETs. Int'l Journal of Distributed Sensor Networks, 2014. [doi: 10.1155/2014/473151]

[67] Di PR, Viejo A. Location privacy and resilience in wireless sensor networks querying. Computer Communications, 2011,34(3):515−523. [doi: 10.1016/j.comcom.2010.05.014]

[68] Li J, Li Y, Ren J, Wu J. Hop-by-Hop message authentication and source privacy in wireless sensor networks. IEEE Trans. on Parallel and Distributed Systems, 2014,25(5):1223−1232. [doi: 10.1109/TPDS.2013.119]

[69] Dutta N, Saxena A, Chellappan S. Defending wireless sensor networks against adversarial localization. In: Proc. of the 11th IEEE Int'l Conf. on Mobile Data Management (MDM 2010). IEEE, 2010. 336−341. [doi: 10.1109/MDM.2010.75]

[70] Rios R, Lopez J. Exploiting context-awareness to enhance source-location privacy in wireless sensor networks. The Computer Journal, 2011:55. [doi: 10.1093/comjnl/bxr055]

[71] Shao M, Hu W, Zhu S, Cao G, Krishnamurth S, La Porta T. Cross-Layer enhanced source location privacy in sensor networks. In: Proc. of the 6th IEEE Int'l Conf. on Sensor, Mesh and Ad Hoc Communications and Networks (SECON 2009). IEEE, 2009. 1−9. [doi: 10.1109/SAHCN.2009.5168923]

[72] Fan Y, Jiang Y, Zhu H, Shen X. An efficient privacy-preserving scheme against traffic analysis attacks in network coding. In: Proc. of the 28th IEEE Int'l Conf. on Computer Communications INFOCOM. IEEE, 2009. 2213−2221. [doi: 10.1109/INFCOM.2009.5062146]

[73] Fan Y, Chen J, Lin X, Shen X. Preventing traffic explosion and achieving source unobservability in multi-hop wireless networks using network coding. In: Proc. of the 2010 IEEE Int'l Conf. on Global Telecommunications Conf. (GLOBECOM 2010). IEEE, 2010. 1−5. [doi: 10.1109/ GLOCOM.2010.5683317]

[74] Rana SS, Vaidya NH. A new ‘Direction’ for source location privacy in wireless sensor networks. In: Proc. of the 2012 IEEE Int’l Conf. on Global Communications Conf. (GLOBECOM 2012). IEEE, 2012. 342–347. [doi: 10.1109/GLOCOM.2012.6503136]

[75] Li N, Raj M, Liu D, Wright M, Das SK. Using Data Mules to Preserve Source Location Privacy in Wireless Sensor Networks. Distributed Computing and Networking. Springer-Verlag, 2012. 309–324. [doi: 10.1007/978-3-642-25959-3_23]

[76] Jiang R, Luo J, Wang XP. An attack tree based risk assessment for location privacy in wireless sensor networks. In: Proc. of the 8th IEEE Int’l Conf. on Wireless Communications, Networking and Mobile Computing (WiCOM 2012). IEEE, 2012. 1–4. [doi: 10. 1109/WiCOM.2012.6478402]

附中文参考文献:

[1] 任丰原,黄海宁,林闯.无线传感器网络.软件学报,2003,14(7):1282–1291. http://www.jos.org.cn/1000-9825/14/1282.htm

[3] 范永健,陈红,张晓莹.无线传感器网络数据隐私保护技术.计算机学报,2012,35(6):1131–1146. [doi: 10.3724/SP.J.1016.2012.01131]

[9] 杨庚,王安琪,陈正宇,许建,王海勇.一种低耗能的数据融合隐私保护算法.计算机学报,2011,34(5):792–800. [doi: 10.3724/SP.J.1016.2011.00792]

[13] 范永健,陈红.两层传感器网络中可验证隐私保护 Top-*k* 查询协议.计算机学报,2012,35(3):423–433. [doi: 10.3724/SP.J.1016.2012.00423]

[19] 周傲英,杨彬,金澈清,马强.基于位置的服务:架构与进展.计算机学报,2011,34(7):1155–1171. [doi: 10.3724/SP.J.1016.2011.01155]

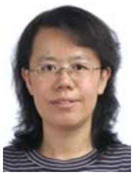
[20] 王璐,孟小峰.位置大数据隐私保护研究综述.软件学报,2014,25(4):693–712. http://www.jos.org.cn/1000-9825/4551.htm [doi: 10.13328/j.cnki.jos.004551]

[24] 张建明,赵玉娟,江浩斌,贾雪丹,王良民.车辆自组网的位置隐私保护技术研究.通信学报,2012,33(8):180–189.

[39] 陈娟,方滨兴,殷丽华,苏申.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.计算机学报,2010,33(9):1736–1747. [doi: 10.3724/SP.J.1016.2010.01736]

彭辉(1986－),男,山东曲阜人,博士生,主要研究领域为无线传感器网络,隐私保护,数据管理.

范永健(1978－),男,博士,副教授,CCF 会员,主要研究领域为无线传感器网络,隐私保护.



陈红(1965－),女,博士,教授,博士生导师,CCF 高级会员,主要研究领域为数据库,数据仓库,无线传感器网络.

李翠平(1971－),女,博士,教授,博士生导师,CCF 高级会员,主要研究领域为社会网络,数据挖掘.

张晓莹(1987－),女,博士生,CCF 会员,主要研究领域为无线传感器网络,隐私保护.

李德英(1965－),女,博士,教授,博士生导师,CCF 高级会员,主要研究领域为无线传感器网络,组合优化.