文章编号:1007-5321(2017)01-0001-17 **DOI**:10. 13190/j. jbupt. 2017. 01. 001

无线传感器网络匿名通信技术研究进展

房卫东[1,2], 李凤荣[1], 单联海[1,3], 何 为[1], 王营冠[1]

(1. 中国科学院 上海微系统与信息技术研究所, 上海 200051;
2. 上海无线通信研究中心, 上海 201210; 3. 上海物联网有限公司, 上海 201899)

摘要: 信息安全(内容安全和通信安全)一直是无线传感器网络(WSN)研究与应用关注的热点. 由于传感器节点能量、计算和内存限制以及部署环境的特殊性,WSN 难以适用复杂度高的安全算法. 内容安全可通过加密方法和认证机制来实现,而匿名通信技术是实现通信安全与隐私保护的一种有效方法. 通过对传统匿名通信技术和 WSN 匿名通信机制的调研,分析了 WSN 关键匿名通信技术的优缺点,并进行了总结和展望.

关 键 词: 无线传感器网络; 安全性; 匿名通信; 隐私

中图分类号: TP393 **文献标志码**: A

Anonymous Communication Technology for Wireless Sensor Network: a Survey

FANG Wei-dong[1,2], LI Feng-rong[1], SHAN Lian-hai[1,3], HE Wei[1], WANG Ying-guan[1]

(1. Key Laboratory of Wireless Sensor Network and Communication, Shanghai Institute of Microsystem and Information Technology, Chinese Academy of Sciences, Shanghai 200051, China;
2. Shanghai Research Center for Wireless Communication, Shanghai 201210, China;
3. Shanghai Internet of Things Company Limited, Shanghai 201899, China)

Abstract: In wireless sensor network (WSN), the information security that involves contents security and communication security becomes the hotspot of research and application. Since the limitation of sensor nodes' resource (energy, computation, et al) and deployment in diverse environments, some complex security algorithms are hardly implemented for WSN. The content security can be realized by various existing encryption approaches and authentication mechanisms, and the anonymous communication technology is a good way to achieve the communication security. The article is to provide a general overview of the anonymous communication in WSN and cover all the relevant work, providing the interested researcher pointers for open research issues in this field. The traditional anonymous communication technologies and WSN's anonymous communication schemes is investigated and reviewed. Furthermore, the advantages and disadvantages of key anonymous communication technologies is analyzed and summarized in WSN.

Key words: wireless sensor network; security; anonymous communication; privacy

收稿日期: 2016-09-01

基金项目: 国家自然科学基金项目(61471346); 上海市自然科学基金项目(17ZR1429100); 上海市青年科技英才扬帆计划项目(15YF1414500); 上海市科技重大项目(15DZ1100400); 中国科学院科技服务网络计划资助项目(kfj-sw-sts-155); 青海省自然科学基金项目(2016-ZJ-922Q)

作者简介: 房卫东(1971—), 男, 博士, 高级工程师, E-mail: weidong. fang@ mail. sim. ac. cn.

随着微机电系统、芯上系统、无线通信技术以及低功耗嵌入式技术的快速发展,传感器的成本下降,性能和可靠性提升,拓展了无线传感器网络(WSN,wireless sensor network)的应用领域. 通常,这些传感器节点部署于检测区域,感知各种信息,如湿度、温度和压力等[1],以无线通信的方式形成自组织多跳的WSN,实现感知信息的传输与汇聚. 目前,WSN广泛应用于军事、工业、农业、医疗等多种领域[2].

随着WSN应用的不断拓展,其信息安全问题日益受到关注. WSN的信息安全分为内容安全和通信安全. 中国工程院院士方滨兴认为"内容安全是指对信息在网络内流动中的选择性阻断,以保证信息流动的可控能力". 内容安全可以通过加密和认证机制来实现,具体实现的方式有多种,如基于单查找表的快速高级加密标准的加密方法[3]、基于组和预分配的传感器网络密钥建立协议[4]等. 而对于通信安全的实现,较为传统的方式是通过对路由协议的改进,实现其信息的传输安全,如基于位置路由机制的衡量可靠性量化度量模型[5]、利用信任模型构建安全路由协议[6]等. 但随着网络规模的不断扩大,尤其是一些敏感关键的应用场景,对通信安全的要求也越来越高. 尽管现有的加密、认证等技术可以实现信息内容安全,有效地预防攻击方获取信息内容,但是无法阻止攻击方通过窃听、流量分析等手段获得节点的位置、身份等重要信息(如军事应用中我方的基地位置等). 匿名通信技术是实现通信安全,尤其是隐私保护的有效技术. 目前,对匿名通信技术已有很多研究,但多数面向传统有限网络(如Internet等),相比较而言,对于WSN的匿名通信技术研究相对较少. 这是因为,WSN的信息传输采用无线通信方式,大多部署于无人值守的地方或敌对区域,节点的计算能力、存储容量以及能量供给有限(能量供给来源于电池供电,且无法更换电池),其部署环境的复杂性及节点资源的受限性等特征使得传统匿名通信技术无法直接应用于WSN,而信息传输媒介的开放性使得WSN匿名通信技术的研究更具有挑战性.

为解决WSN匿名通信技术的诸多问题,国内外研究机构和科研人员从协议、算法、能量有效性等多个方面入手,启动了多个相关项目的研究,取得了多个有价值的技术成果. 例如,美国国防部空军科研办公室、加州大学圣塔芭芭拉分校等机构开展了MURI等项目研究,西班牙科技创新部、国立马拉加大学开展了ARES、SPRINT等项目研究,加拿大开展了ORF-RE WISENSE、NSERC等项目研究,获得一些研究成果[7-9]. 国内的中国科学院信息工程研究所、西安电子科技大学、北京邮电大学和武汉大学等科研院所及高校也相继开展了WSN匿名通信方面的研究. 在关键技术突破方面,主要包括匿名机制与认证协议、匿名性与可用性均衡、匿名机制的计算复杂度与能量有效性分析、隐私信息保护与匿名等. 作为WSN匿名通信技术研究的基础:匿名路由协议、源节点隐私(位置、身份)和基站隐私算法是笔者关注的重点,同时,也关注部分自组织网络路由协议的匿名性.

正如上文表述,WSN匿名通信技术是一个具有挑战性的研究方向,其固有的技术特征,如信道开放性、能量有效性等,使得研究成果散见于各种学术期刊与论著中. 笔者对传统匿名通信技术和现有WSN匿名通信机制进行了较为详尽地调研,综述并分析典型的匿名通信技术,尤其是详细阐述了WSN匿名通信技术的研究进展.

1 匿名通信技术与流程

匿名通信技术主要是通过采取一定的措施隐藏网络节点间关系,使窃听方/攻击方难以获得或推测出任何网络节点的身份、位置及其通信的相互关系.

在20世纪80年代初,Chaum[10]开始注意到现代通信网中匿名需求,之后大量学者开展研究并试图解决这一问题. 王继林等[11]综述2005年以前传统匿名技术研究情况,探讨Crowds、洋葱路由等匿名通信机制,阐述匿名性度量、签名算法、应用中信赖建立等技术,确定进一步研究方向. 根据隐匿对象的不同,Granjal等[2]将匿名技术分为发送方匿名、接收方匿名以及收发方无关联. 本节将简述几种典型的匿名通信技术.

1.1 Mix

1981年,Chaum首次提出了Mix匿名通信技术,该技术基于公钥加密技术,允许电子邮件系统来隐藏通信的参与者和通信的内容,用于不可追踪的电子邮件[10]. 由此技术研制的存储和转发设备,接收用公钥加密的信息,且经过充足的时间段后输出重新排序的批量信息,实现输出和输入之间的相关性隐藏. Mix系统采用单层或多层级联,如图1所示的多层级联中,M1、M2和M3(此处指的是Mix设

备)利用相反顺序中 Mix 的公钥反复加密信息,每层设备 Mix 解密自己的加密层,且在固定延时后输出重排序的批量信息.

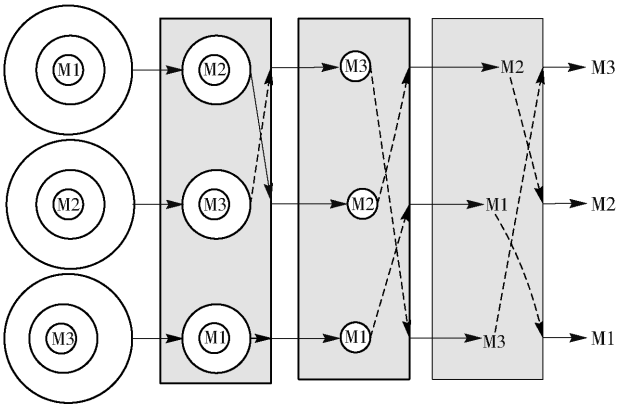

图 1　Mix 级联

现有许多的匿名技术都是以 Mix 技术为研究基础的,如分层加密、消息缓冲池和混淆机制等. 分层加密是通过加密来改变消息的表现形式,然后进行信息混淆. 消息缓冲池则是用来隐藏信息输入和输出的对应时序,增加一定发送延迟. 后来,提出的重加密方法逐渐成为 Mix 研究的重点[12],2004 年 Golle 等[13]对重加密 Mix 又进行了扩充,使得在重加密的过程中不需知道消息加密时所使用的公钥,该机制称为通用重加密.

1.2　Onion Routing 与 Tor

洋葱路由是一种基于洋葱路由器组成网络核心的低延迟匿名通信系统[14-15]. 洋葱路由器的功能类似于 Mix 设备,其区别是 Mix 设备引入较大的延时,而洋葱路由器提供了接近实时的信息转发. 洋葱路由器是面向连接的,一旦匿名连接建立,在给定时间周期内这条路径保持不变. 洋葱路由中,建立匿名连接是通过公钥加密的分层数据结构,该结构提供了洋葱路由、加密密钥和连接的数据流方向. David 等[16-17]提出的洋葱路由多次混淆技术是一种基于 TCP 的新的匿名通信息技术. 洋葱路由采用代理机制、多次混淆技术和加密技术实现路径的匿名和通信双方地址等关键信息的隐藏,其技术原理如图 2 所示.

Tor 是基于电路的低延迟匿名通信服务,是目前互联网较通用的公共匿名通信系统(第二代洋葱路由). Tor 通过增加秘密转发、拥塞控制、目录服务器、完整性检查、可配置退出策略等解决了初始洋葱路由中存在的 Socket 连接实时性、消息生存周期等

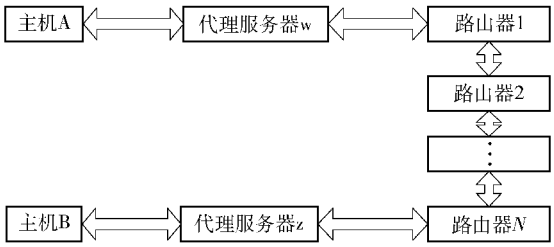

图 2　洋葱路由的实现过程

限制. Tor 工作于实时网络,不需要修改特权或者内核,几乎不需要同步或节点间协调,较好地实现了匿名性、可用性和效率之间的均衡[18-25]. 目前,对洋葱路由或 Tor 的改进,主要是进一步提高匿名性.

1.3　Crowds

Crowds 匿名通信机制是基于组群和重路由的方法实现发送方匿名[26],该机制通过对 Web 交互匿名的实现来保护 Internet 用户隐私. 其本质思路是“Blending into a crowd”即“混在人群中”,通过把使用者分组到大且地域多元化的组中,用组群代替其成员发起问题请求,故 Web 服务器无法获知请求的真实源. 因为问题请求也可能来自该组群的任何成员,甚至合作的群成员也无法区别请求的发起者,这是由于一个成员可能仅仅代表其他成员转发请求,其系统结构如图 3 所示.

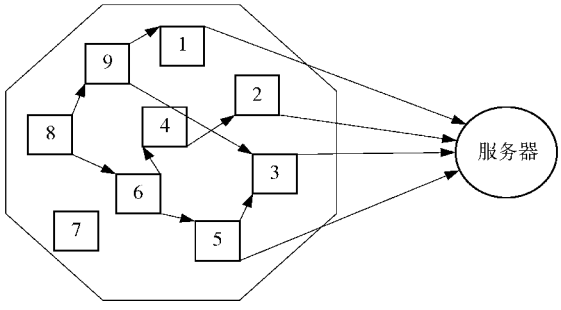

图 3　Crowds 匿名通信机制结构示意图

Crowds 匿名通信机制具有较低的通信延迟和较高的系统通信效率,且扩展性好,通过在群组中匿名提高发送方的匿名性,有效地抵抗流量分析. Hordes 协议[27]在 Crowds 模型基础上加入多播的思想来减少发送应答消息的时延和消耗. 陶颋等[28]提出基于 Crowds 的重路由匿名通信协议,该协议兼顾了通信的匿名性与效率,克服了 Crowds 匿名通信机制抗攻击性差的缺点. 吴云霞等[29]则结合了 Mix 匿名通信技术和随机数填充技术提出一种基于 Crowds 的改进匿名通信系统.

除上述 3 种典型匿名机制外,还有其他一些匿

名通信机制陆续被提出. 其中,DC-Net(dining cryptographers network)协议是一种广播性匿名通信协议[30],该协议是将发送方和接收方隐藏在大量参与者中,经研究发现,若参与者中混有恶意节点,其匿名性会降低. 在对等(P2P,peer-to-peer)网络匿名技术研究中,Tarzan 是一个 P2P 匿名的 IP 网络覆盖[31],Tarzan 利用分层加密和多跳路由实现匿名性,信息发起者选择节点路径,建立起静态隧道,生成大量的虚拟信息流来提供匿名性. 陆天波等[32]提出了基于 P2P 匿名通信的 WonGoo 协议,该协议利用分层加密和随机转发相结合的方法,实现了 Mix 的强抗攻击性和 Crowds 的低延迟、高通信效率. 综上可见,Mix、Onion Routing 和 Tor 提供发送方的匿名;DC-Net 和 Tarzan 实现了发送方、接收方以及双方通信关系的匿名;WonGoo、Crowds 和 Hordes 主要实现发送方的匿名. 除此之外,传统网络的匿名通信协议还有许多,如 Mixmaster[33]、MorphMix[34]、PipeNet[35]、Mixminion[36]等.

2 WSN 匿名机制

信息安全是 WSN 需要解决的关键问题之一,其目标是 WSN 具备数据机密性、认证性、完整性、及时性和网络容侵性[37].

匿名通信技术是解决通信安全,尤其是隐私保护的一种有效技术. 尽管传统网络匿名通信技术已有较多研究,但对于 WSN 来说,由于其固有特征使得传统的匿名通信技术无法直接应用,所以,WSN 匿名通信技术是近年来信息安全领域关注的研究热点之一. WSN 匿名通信机制可分为匿名路由机制、源节点隐私保护的匿名通信机制和基站隐私保护的匿名通信机制,其中,隐私包括位置、身份等.

2.1 匿名路由机制

在 WSN 信息传输过程中,匿名路由机制是在已建立路由上对参与转发的所有节点标识实现匿名,以防止跟踪者进行定位与反向跟踪.

早期匿名路由机制主要通过加密技术等实现节点标识的匿名性[38]. STR(Skinny TRee)是基于 DH(Diffie-Hellman)密钥交换的分布式组密钥管理协议机制[39],它的非平衡树结构使得密钥更新过程变得简单,密钥树结构维护更加容易. 分层机制可以降低 STR 协议的计算开销,也可以减小大规模组场景下的组密钥更新的延迟. Tu 等[40]采用分层机制与 STR 协议相结合,降低了密钥管理产生的通信量和计算量,但是存在单点失效问题[41-42],安全性得不到保障. 麻常莎等[43]提出了一种基于 STR 的混合组密钥管理机制——H-STR(Hybrid Skinny TRee),该密钥树沿用 STR 协议的非平衡结构,分为主树与子树,压缩了树高,在继承 STR 协议低通信开销特点同时,提高了组密钥的更新效率,降低了节点活动对其他节点的影响,从而节省了节点活动造成的计算开销,适用于节点活动频繁的大规模组网通信环境.

随着研究的深入,假名机制逐渐受到了关注. Misra 和 Xue[44]提出了分簇 WSN 的简单匿名机制(SAS,sample anonymity scheme),SAS 主要采用了假名(Pseudonmy)机制和共享密钥机制,通过假名策略来隐藏节点真实的身份,使得通信链路中的传感器节点完全匿名. 为了确保匿名性,他们提出在网络中所有节点使用"K"位的假名机制,使得假名的空间范围是 $0 \sim 2^K - 1$ 共 2^K 个假名,且对于每个节点 ID 对应的子区间假名是非连续的,如图 4 所示. 该机制较好地实现了发送方的匿名,但是未实现基站的匿名.

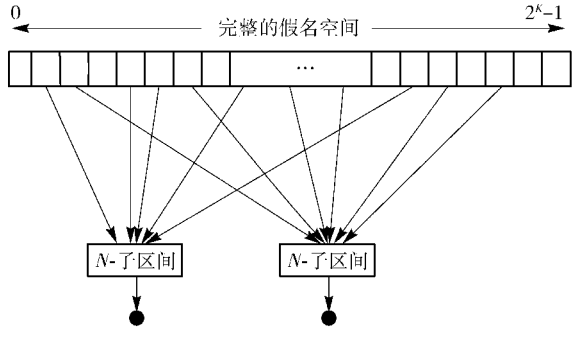

图 4 SAS 非连续假名分配示意图

在 SAS 部署前,每个节点预分配一定数量的非重叠假名范围;部署之后,在设置阶段,节点与它的其中一个邻居关联某个假名范围,每两个相邻节点交换关于分配假名范围的信息. 若节点想要发送信息到邻节点,它利用已关联假名范围的随机假名代替接收方和发送方的 ID. 此外,Misra 和 Xue[45]还提出了另一种匿名机制:加密匿名机制(CAS,cryptographic anonymity scheme). 在 CAS 机制中,利用密钥散列函数 H_K,在预映射基础上生成假名:

$$\text{Pseudonmy} = H_{K_{uv}}(x_{uv} \oplus S_{uv}) \tag{1}$$

其中:K_{uv}为两个通信节点 u 和 v 之间的共享密钥,x_{uv}为节点 u 和 v 之间的一个随机种子,S_{uv}为节点 u 和 v 之间通信的当前序列号,$\oplus$代表异或操作. 与

SAS 相比，CAS 需要更多的计算量，但节约了存储空间，这是由于在 SAS 中，每个节点需要保存若干不同的已关联的假名空间.

Shi 等[46]提出了分簇 WSN 中基于假名的匿名增强机制，分为簇内通信阶段与簇间通信阶段.

1）簇内通信阶段

簇内通信阶段包含 5 个部分：①节点 i 与簇头(CH，cluster head)形成假名对(fc_chid 与 f_id)，共享假名对的使用时间，簇头保有假名对的映射列表；②节点 i 参照共享假名对的使用时间，用假名替换自身真实 ID 与簇头真实 ID；③当时间超出了共享假名对的使用时间时，则由节点 i 发送虚假节点请求消息，然后由簇头更新假名对及映射表，并对请求进行响应；④当节点 i 接收到该响应消息时，更新假名对并重置时间戳；⑤当簇状态发生改变时，再次执行①～④过程.

2）簇间通信阶段

簇间通信是指簇头与基站的通信. 其中，基站负责簇头假名分配. 每个簇头与基站共享一个密钥，当簇头发送消息时，它用密钥 K 加密消息. 该过程也包含 5 个部分：①当簇形成过程结束时，每个簇头发送一个消息到基站，该消息包括自身 ID 以及与基站的距离；②当基站收到此消息时，会为簇头生成一个假名 jbs_chid，并根据距离为簇头选择下一跳. 基站在假名表存储该信息. ③基站发送响应消息至簇头，该消息包含假名 jbs_chid 与选择它下一跳假名 fn_chid. ④当簇头接收到消息时，它获取 jbs_chid 和下一跳 fn_chid. 在传输中，簇头使用 jbs_chid 来代替真实 ID，而下一跳使用 fn_chid. 该消息被密钥 K 加密. 簇头在自身的假名表保有 fbs_chid 和 fn_chid，每当需要更新时，基站完成 jbs_chid 和下一跳 fn_chid 更新，同时发送到相应的簇头. ⑤更新机制与簇内通信阶段类似. 该机制可以较好地保护簇头和簇成员的隐私信息.

Abdullahi 和 Wang[47]提出了一种轻量级的匿名路由机制(LANDER，lightweight anonymous on-demand routing scheme)实现匿名通信，首先利用 Bloom 过滤器隐藏路径上传感器节点的身份，然后基于椭圆曲线密码体制生成每一跳的假链接标识符，进而实现 WSN 中机密信息的交换. 该机制的目的是构建能量有效的路由机制，阻止敌对方获得数据包发送方和接收方的身份信息，保证敌对方没有能力跟踪数据流，以回溯到发送方及接收方，确保路由上节点的匿名性. LANDER 机制采用了基于信誉和信任的概念，仅仅允许可靠的节点参与所有路由和数据包转发过程，增强抵御内部攻击的能力，提高了数据传输的安全性，优化了传输的可靠性.

Yuan[48]提出了基于认证密钥的安全匿名路由协议. 该协议为了适应存在主动攻击和被动攻击的复杂环境，利用公钥建立路由，取代了以往自组织网络认证路由[7]等协议中使用共享密钥建立路由的方法. 该协议隐藏了参与方及其关联的网络拓扑信息，接收方通过对发送方的认证，确保发送方身份的合法性，故不需建立获取私有密钥过程，中间节点通信前也无需匿名邻居节点，该协议具有较好的扩展性.

Zhang 等[49]提出了 WSN 多路径冗余安全匿名路由协议(MPRSARP，multiple-path redundancy secret anonymous routing protocol)，该协议利用多路径冗余来建立路由路径，克服了单路径的一些弊端，如路由中任意节点的失败将导致整个路径的失败等. MPRSARP 中使用了假名机制、加密机制和多路径机制，使用了散列函数操作和异或操作，源节点和目的节点之间采用了共享的会话私钥机制，同时还增加了时间戳来保证实时性. 后续，他们进一步提出了基于双线性映射和异或操作 WSN 的安全匿名路由协议[50]，该协议不仅可以提供路由匿名、源节点和目的节点位置隐私和身份的匿名性，而且具有后向和前向安全性. 在 MPRSARP 中，使用对称私钥代替非对称私钥，异或操作代替模指数操作，因此该协议明显改善了计算复杂度，更适用于 WSN. Gagneja 提出了安全匿名通信协议(SACP，secure anonymity communication protocol)[51]，该协议不仅实现了源节点、目的节点以及通信相关的匿名性，与匿名路径路由协议[52]、SAS[44]和 CAS[45]等加密匿名机制相比，具有较少的内存占用、较低的通信开销以及较小的计算量.

Jiang 等[52]提出了 WSN 匿名路径路由协议，该协议包括 3 个基本机制：①匿名一跳通信；②匿名多跳通信；③匿名数据转发. Yang 等[53]提出了节点不相关的假名对机制(NUCPP，node-uncorrelated pseudonym pair-wise mechanism)的安全匿名路由协议，该协议利用不相关节点的假名对机制来表述特定通信体(节点)间的直接通信关系，而不是用假名来表示特定的节点. Pan 等[54]提出了对抗局部或全局攻击的保护源节点隐私的匿名通信协议，在该协议中，

考虑到传感器节点在活动模式和睡眠模式之间转换,实现对抗局部或全局攻击方的目标,遵循一个简单的原则:在活动模式下,每个节点正确地传输一个固定大小的数据包,而不关心它是数据发送或者转发. Manjula 和 Datta 利用虚拟源概念和 α 角度匿名概念,提出了能量有效的隐私保护路由算法[55]. 另外,Nakamura 等[56]利用单路径树形拓扑提出了通信效用优先的匿名路由协议.

从上面的分析可以看出,匿名路由的实现主要通过加密/解密、假名机制、多路径机制等隐藏通信双方的关系或传输路径. 对于加密/解密机制而言,无论是椭圆曲线密码机制,还是公钥/私钥机制,都会增加计算量和内存占用,同时,密钥的生成与分发等必然增加通信开销,因此,低复杂度、高安全性的加密/解密机制是 WSN 匿名路由的研究方向之一. 假名机制在某种意义上是真实节点 ID 的随机化虚拟映射,该机制基本不增加通信开销,但保证其动态的更新则是需要面对的问题. 多路径机制是通过增加冗余路径来实现通信双方的关系或传输路径的隐藏,该机制一方面可以防止单路径中节点损坏造成的链路中断;另一方面通过路径的冗余增加路径反跟踪的难度. 值得注意的是,与传统网络不同,WSN 的路由节点除了具备路由及转发的功能外,还具有位置信息,这些信息一方面是需要保护的对象;另一方面也可作为潜在的备用信息应用于匿名路由技术研究中.

2.2 源节点隐私保护的匿名通信机制

WSN 源节点隐私保护技术的匿名通信机制既要隐藏真实的通信模式,防止敌对方通过对通信模式的监听和数据流量的分析,获得感知数据的源节点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、数据分组丢失率和能量消耗[57].

Alomair 等[58]提出了用以分析评估传感器网络匿名性的框架,该框架的创新之处在于 2 个方面:①引入了"时间不可区分"的概念,提出了一种用以 WSN 建模的定量方法;②通过多余参数(nuisance parameters)将源匿名映射到二元假设检验的统计问题. Ozturk 等[59]和 Kamat 等[60]提出了幻影路由(PR, phantom routing)协议和幻影单路径路由(PSPR, phantom single-path routing)协议,他们将随机游走方法引入到源位置隐私保护中,源节点随机选择周围临近区域,并在选定区域内随机选择邻居节点作为转发节点,直至达到一定的跳数或者不能继续转发为止. 上述随机区域内选定的转发节点称为源节点转发数据的幻影源节点,幻影源节点将数据包洪泛或单播方式发送到基站节点,该方法较好地实现了源节点匿名. 马春光等[61]提出了基于 Voronoi 图预分配的静态用户和动态用户协作的匿名方法,该方法采用锚节点代替源节点真实位置,实现源节点的匿名性. 周长利等[62]针对基于位置查询服务中构造的匿名框或选取的锚点仍位于敏感区域而导致的位置隐私泄露问题,提出了基于敏感位置多样性的锚点选取算法,该算法根据用户访问数量和访问高峰时段,对不同敏感位置进行定义和筛选,选择具有相似特征的其他敏感位置构成多样性区域,并以该区域形心作为查询锚点,提高用户在敏感位置出现的多样性. Niu 等[63]提出了一种针对时延敏感 WSN 的基于最优簇的源匿名协议,该协议通过调整传输速率和不均等簇的半径,实现网络流量和实际事件报告延迟之间的平衡,以减少网络流量.

Mahmoud 和 Shen[64]提出了一种 WSN 的源节点位置隐私保护机制,该机制采用了加密操作,通过改变每一跳传输的数据包外观(packets' appearance)来预防数据包之间的关联性;该机制还采用了虚假流云将源节点隐藏在云的节点组中,虚假流云的形状不规则,大小也不固定,源节点可以从云的节点中选择一个虚假的源节点,将感知数据匿名地发给它. 该机制利用基于双线性对的身份加密来生成任意两节点之间的共享密钥,节点之间通信采用假名策略. 该机制在预部署和引导阶段,每个传感器节点有自己独特的身份、与基站的共享密钥和私钥,部署后基站广播信标数据包用来建立节点到基站的路径,为了分配虚假源节点需要执行虚假节点请求数据包、虚假节点请求回复数据包和虚假节点分配数据包;数据传输阶段,真实的源节点匿名发送事件到虚假的源节点,然后发送到汇聚节点,且同时激活虚假数据包云来保护源节点的位置. 该机制的假名利用节点的共享密钥 K_{AB}、随机数 R 和散列函数 $H(\cdot)$创建,通过迭代操作可以生成一系列假名,假名的同步是通过一个滑动窗口的匹配实现的. 节点 A 和 B 的共享密钥 K_{AB}可以创建以下一系列假名:

$$P_{AB}^{(1)},\ P_{AB}^{(2)},\ P_{AB}^{(3)},\cdots,P_{AB}^{(n)}$$

这里的 $P_{AB}^{(i)}$是经过第 i 次迭代后的假名.

$$P_{AB}^{(i)}=H(K_{AB},P_{AB}^{(i-1)}) \tag{2}$$

其中 $P_{AB}^{(1)}=H(K_{AB},R)$. 由(2)式可见,由于随机数

R 的不同，2 个节点可以利用相同的密钥生成不同的假名. 假名不仅用于识别发送节点与接收节点，而且识别利用不同的随机数产生的不同传输路径. 该机制通过限制每个虚假包的传输次数，以减少资源的消耗.

Kang[65] 提出了关于大规模 WSN 位置隐私支持机制（LPSS，location privacy support scheme），主要通过多样化可能路由路径的数量调整系统参数，实现发送延迟和保护强度之间的均衡. LPSS 机制中，每个传感器节点将其邻居节点分为 3 个等级：小的梯度值集 S、相等的梯度值集 I、大的梯度值集 L，其中梯度值指的是当前节点到汇聚节点的最小跳数. 当节点传输数据包时，以概率 p_i 在 I 集中选择下一跳节点，或者以概率 $1-p_i$ 在 S 集中选择下一跳节点，这里 p_i 是预先设定的系统参数，通过调整其值来均衡发送延时和位置隐私. 对于安全路径数的计算如下：

$$y_x = (1-p_i)n_S y_{x-1} + p_i n_I (1-kx) y_x \qquad (3)$$

其中：y_x 为预期的安全路径数，k 表示此跳在预期安全路径上的不确定性，x 为当前节点距离汇聚节点的跳数，n_I 和 n_S 分别为相等梯度值集和小的梯度值集节点的数量. y_x 的取值范围为

$$((1-p_i)n_S)^{x-m} \leqslant y_x \leqslant \left((1-p_i)\frac{n_S}{p_i n_I}\right)^{x-m} \qquad (4)$$

其中 m 为该节点的梯度值. 安全路径数随着源节点到汇聚节点距离的增加以指数的方式增加，其位置的隐私度也就越好，因为路径数越多对于节点的隐私保护越好. LPSS 机制同时采用虚假数据包注入的机制. 虚假数据包的引入可以抵抗数据包流的分析，把攻击方引导到错误的方向，同时对于虚假数据包的移动跳数进行限制. 在 LPSS 研究的基础上，Kang 进一步证明汇聚节点和源节点的相关性，发现某个源节点暴露给攻击方，则传统的虚假数据包注入机制对于保护汇聚节点往往是无用的.

Tan 等[66] 提出一种路径扩展方法用以保障源位置隐私，在该方法中，当源节点发送事件消息到基站后，动态生成虚假源节点，通过一些虚假路径上的虚假源节点诱导敌对方远离真正的源节点，如图 5 所示. 该方法可以有效地保护源节点的位置隐私，具有较小的信息传递延迟和可接受的计算开销.

Li 和 Ren[67] 提出了源位置隐私保护机制，主要采用在信息发送到基站之前随机选择中间节点的方法，提出了 3 种基于动态路由的机制来保护源位置隐私.

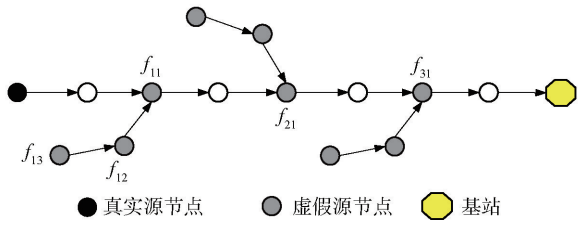

图 5　路径扩展方法中虚假路径示意图

第 1 种是随机中间节点路由机制. 该机制中，选择中间节点的原则是基于传感器节点的相对位置，希望中间节点远离源节点的最小距离（$d_{\min}$）越大越好，以使得敌对方难以获得真实源节点的位置信息，但其仅仅可以提供局部的位置隐私.

第 2 种是基于相角的多中间节点路由机制，如图 6 所示. 该机制中，最大相角 β 指的是源节点到基站和最后一个中间节点到基站之间的角度. 由于源节点是动态的，所以最大相角 β 也是变化的. 以基于相角的方法来选择中间节点，若最大的相角 β 越大，实现位置隐私的级别就越高，图 7 所示的阴影区域为源节点可能的位置. 该机制比第 1 种机制更加可靠，能耗较低，而且数据发送率高.

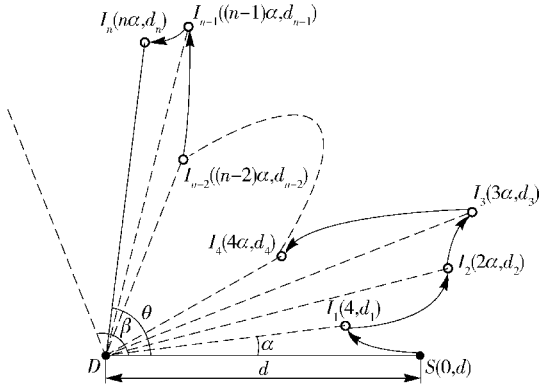

图 6　基于相角的多中间节点路由机制示意图

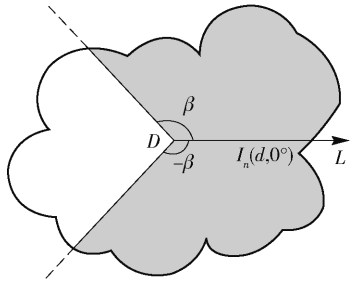

图 7　基于相角法的可能源位置示意图

第 3 种是基于象限的多中间路由机制. 该机制

中,整个网络依据源节点和汇聚节点的位置划分成4个象限. 基于相角和基于象限的多中间节点路由机制,均可以实现全局位置隐私,仿真结果表明,基于象限的多中间节点路由机制提供的匿名性优于基于相角的多中间节点路由机制.

Park 等[68]利用虚拟 IDs(IDentities)和简单消息认证码(SMAC, simple message authentication code)技术来抵抗窃听攻击,保护源节点的隐私,通过使用虚拟 IDs 技术来抵抗流量分析攻击,并且通过创建冗余的 IDs 来混淆敌对方;利用 SMAC 代替数据帧的循环冗余检查(CRC, cyclic redundancy check)确保数据的完整性. 源节点的真实 ID 用虚拟 ID、隐藏矢量(HV, hidden vector,用 α_{HV} 表示)和时间戳(TS, time stamp,用 α_{TS} 表示)代替,其中 HV 的计算式为

$$\alpha_{HV}=\alpha_{SID}\oplus K_D\oplus R \tag{5}$$

其中:SID 为源节点真实 ID(用 α_{SID} 表示),K_D 为目的节点私钥,R 为随机数,$\oplus$ 表示异或操作.

HV 保证了只有目的节点可以识别源节点,SID 只有源节点持有,而 K_D 只有目的节点持有,只要 K_D 不泄露,源节点的隐私就不会泄露,R 的泄露不会影响源节点的隐私. HV 通过 R 的改变而定期的改变,这样可以有效地预防重放攻击. 虚拟 ID 即 PID,用 α_{PID} 表示,每个传感器节点在初始化后,其 PID 为

$$\alpha_{PID}=q^{\alpha_{SID}}\bmod p \tag{6}$$

其中 p 和 q 为相邻节点间的密钥对. 每个节点都储存在邻近传感器节点 PID 的映射表,并且 PID 定期更新. 对于 SMAC(用 α_{SMAC} 表示)的创建和识别通过如下过程实现,其中 AV 为节点 A 的矢量,用 α_{AV} 表示.

1)创建(传感器)

$$K=\alpha_{AV}\bmod p \tag{7}$$

$$\alpha_{SMAC}=H(K\oplus\alpha_{TS}) \tag{8}$$

2)识别(基站)

$$K'=\alpha_{PID}^{K_D}\bmod p \tag{9}$$

$$\alpha_{SMAC'}=H(K'\oplus\alpha_{TS}) \tag{10}$$

其中 $H(\cdot)$ 是散列函数.

通过 SMAC 和 SMAC 之间的对比确保信息的完整性. 在图8中 D 和 G 是窃听方,即便 PID、HV、R、SMAC 和 TS 的值泄露给局部窃听方 D 和 G,但它们仍然无法获得传感器节点的真实 ID.

Park 等[69]提出了对抗全局窃听方/攻击方的保护源节点和汇聚节点位置隐私的匿名方法(PASSAGE, preserving anonymity of sources and sinks against global eavesdroppers),采用了少量的隐秘渗透性信道(如虫洞和消息摆渡)来分散、转向和隐藏通信事件,因此可以利用 PASSAGE 特性,使用虫洞来建立一个隐秘的安全通信信道. PASSAGES 机制能够很好地实现源节点和汇聚节点的隐私保护,而且不会增加额外开销,但由于消息摆渡的使用会增加时延,不适用于时延敏感的网络. Gurjar 和 Patil[70]提出了基于分簇 WSN 的源位置隐私保护机制,主要利用随机身份来代替真实身份,通过簇头选择连续不相交的数字范围,分配给每个节点,预期传输信息的节点随机选择一个数字用来代替节点的身份,且节点分配的数字范围是周期性变化的,这样有效地预防了节点位置和数字范围的相关性. Zhang 等[71]提出了全代理机制,通过在每个传感器节点执行信息过滤,改善了有效性,提高了真实信息的发送率,而且减少了通信开销. Reindl 等[72]提出了通过增加短控制数据包协调传播时间的方法,该方法使得攻击方只能获知已经发生的事件,但是不能获知是何事件或是在何处发生. Shinganjude 和 Theng[73]分析了 WSN 源匿名的几种方式,建议采用信息伪装的最低有效位和源签名技术,实现源匿名的改进. Kazemi 和 Azmi[74]针对多汇聚节点的 WSN,通过使用标签交换路由方法来提供每个簇中的汇聚节点匿名. Pongaliur 和 Xiao[75]不使用传统开销密集的方法,而使用较低开销的密码技术隐藏源信息,该方法动态选择中间节点,通过选择的节点修改路由中的数据包,使得敌对方难以通过恶意追踪数据包而发现源节点,并可以防止分组欺骗. Amahmoud 和 Shen[76]提出了一个基于云计算的匿名通信机制,用以保护源节点的位置隐私以对抗热点定位攻击,该机制能够提供比基于路由机制更强的隐私保护和比基于全球对抗计划更少的能量需求. Li 等[77]提出了在基于路由的源位置隐私(SLP, source-location

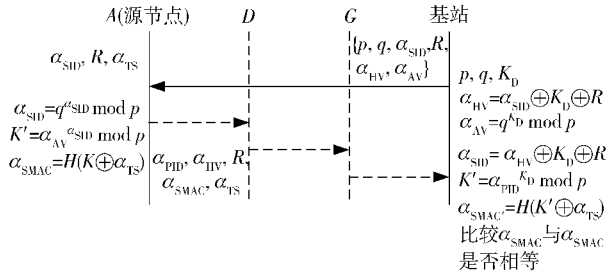

图8 从节点(A)到基站的数据传输

privacy)保护机制中,定量地测量源位置信息泄露的模型,通过该模型分析给出了某些知名 SLP 保护机制的漏洞,随后采用了路由到一个随机选择中间节点和网络混合环的方法,提出了改进的 SLP 保护机制. 该方法具有一定的安全性,并可以达到较高的信息传输率.

从上面的分析可以看出,源节点隐私保护的匿名通信机制主要通过数据流加/解密、数据包加/解扰、虚拟 IDs、随机身份变更、假名机制、洪泛路由协议等方式实现. 其中,数据流加密的方法是一种较为传统的方法,其较高的算法复杂度是它应用于资源受限 WSN 的一个瓶颈;数据包加/解扰是一种信息变换或部分信息的替代,其计算量通常会比加/解密少一些;虚拟 IDs、随机身份变更某种意义上与假名机制类似,其本质是用虚拟的信息替代关键的信息,如节点真实 ID 等;洪泛路由协议通过增加数据的冗余来增强匿名性. 但是,目前大多数源匿名通信机制的研究很少考虑算法的能量消耗,这对于能量供给受限的 WSN 而言,是需要进一步开展的研究.

2.3　基站隐私保护的匿名通信机制

基站在 WSN 中所处位置十分重要,它不但是整个网络信息汇聚的中心,而且是整个网络信息安全模型建立过程中被认定为“安全”的基础. 基站隐私保护的匿名通信机制实现基站或网关节点的位置与身份的匿名,以防止敌对方通过流量分析、数据跟踪对基站进行定位.

Gottumukkala 等[78]针对 WSN 中基站位置隐私提出了一种保护技术,该技术的核心思想是通过使基站周围所选择传感器节点集的传输范围多样化,实现对敌对方的混淆,即创建不能被全局攻击方识别的虚假基站集合,如图 9 所示. 该技术的关键点在于利用爆发节点来保护基站隐私的安全. 在该技术中,网络中节点分成 2 个节点集,即普通节点集和爆发节点集. 爆发节点集是在一个环形或圆形区域,真实的基站(不一定在中心)混淆在爆发节点中. 普通节点集中每个普通节点的传输范围为 t_x,爆发节点集中每个爆发节点的传输范围是 $M \times t_x$,其中 M 可以是任意值,只要满足乘积 $M \times t_x$ 在传感器节点所能传输的最大范围内即可,乘积 $M \times t_x$ 设置为图 9 所描述的爆发半径,普通节点可以基于它们到目的地(图 9 中灰色区域中的任意爆发节点)的距离从其邻居中选择下一跳节点. 数据传输过程

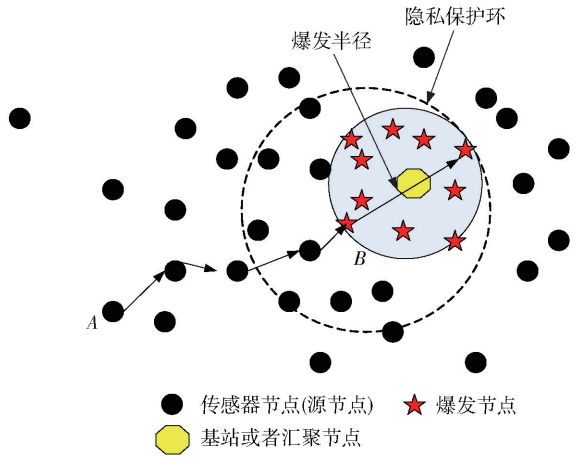

图 9　利用爆发节点的数据包传输

分为 2 个阶段:第 1 阶段,数据包从源节点发送到目的区域(见图 9 中灰色区域)的爆发节点,使用源节点到爆发节点之间最短的路径,且使用定向的随机路径来增加隐私,在该阶段中,目的区域的爆发节点是随机选择的,因此每次传输选择的路径不相同;第 2 阶段,爆发节点在环内(隐私保护环内)广播数据包,环内的每个节点包括真实的基站将得到数据包,这样敌对方就不易跟踪到基站(这是由于环内的每个爆发节点都可能是基站). 因此,基站在爆发节点的混淆下是安全的. 第 1 阶段采用的是最短的路径,这个技术与其他保护基站隐私的技术相比延时较小;第 2 阶段中,只有爆发节点在环内传输数据包时,需要一定的能量,在其他的节点并没有增加能量消耗,能量消耗也较少. 此外,Shahare 等[79]通过增加最短路径算法和高效分簇机制,修改了传统的爆发节点处理技术,获得较小的能量消耗和分组延迟.

Ngai[80]主要通过在路由表中省略汇聚节点的地址,实现其身份和位置隐私的保护,提出了隐藏地址的随机路由机制(RRHA, randomized routing with hidden address),可以有效地防止敌对方通过捕获数据包,进而分析目的字段获得接收方的地址,或者通过观测网络流向来预测汇聚节点的位置. 在该机制中,当传感器节点 i 想要传输信息(数据包)到基站时,节点 i 不需知道基站位置或 ID,它首先使用与基站共享的对称密钥 K_i 加密待传输的数据包,然后数据包沿着一条随机路径传输. 节点 i 只是随机地把数据包发送给它的任意一个邻居节点 j,然后邻居节点 j 也随机地选择一个邻居节点作为下一跳,相应地,数据包的跳数 H 增加 1(H 在源节点处初始化为 0),上述转发过程一直重复,直到 H 达到预定义

的最大跳数 L. 在这个传输过程中,数据包可能到达任意某个基站,也可能无法传输到任何基站. 节点 i 发送数据包的格式为 $<i\,|\,Y_{\text{type}}\,|\,H\,|\,Yk_i>$,其中 i 为源节点的 ID,Y_{type} 为数据包的信息类型,Y_{K_i} 为节点 i 用对称密钥 K_i 加密信息,H 为数据包传输过程中的跳数. 信息类型允许基站来辨别出数据包的内容,基站仅仅解密它感兴趣的数据包. 为了增加数据包能到达基站的概率,每个节点可以选择多个邻居节点发送数据包,即使用多路径传输代替单路径传输.

多路径随机路由传输机制如图 10 所示. 该机制与采用虚假数据包注入机制相比能量消耗较少,但是可能会产生较大的延时,由于每个节点都是随机转发数据包,无法确保采用最短的路径,甚至数据包存在无法到达基站的可能.

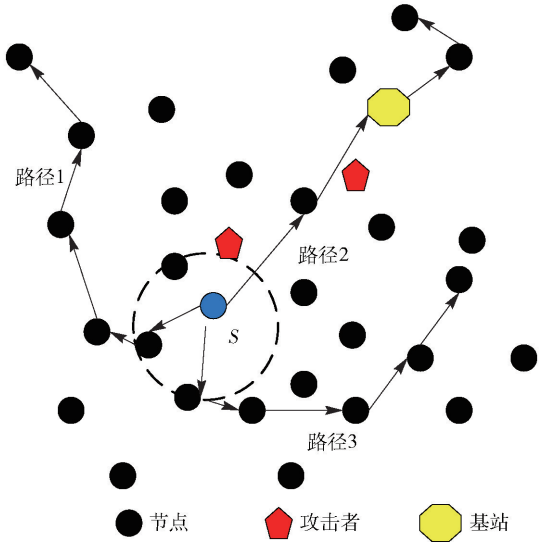

图 10 多路径随机路由示意图

Ying 等[9]提出了汇聚节点位置隐私保护协议(SLPP, sink location privacy protection protocol),可以有效地迷惑局部攻击方或全局攻击方,每个节点产生的假消息数目依赖其邻节点的数量. 仿真结果表明,尽管假消息的传输会消耗额外的节点能量,但网络的生命周期不会受到影响.

Gu 等[81]提出了节点移动 WSN 的基站匿名保护机制. 由于移动控制协议是为了获得最优的部署位置,在该协议执行过程中,通过使能量消耗最小化而实现传感器节点位置的重新部署. 经分析发现,移动控制协议会泄露基站位置的隐私,为了保护基站隐私,他们提出了用虚假的基站来混淆真实基站位置,而把真实的基站隐藏在匿名区域 Φ_P 来欺骗敌对方,如图 11 所示.

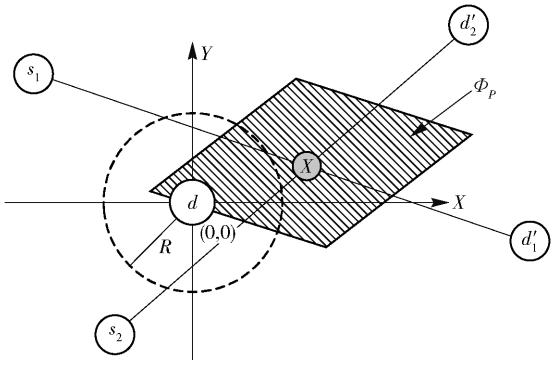

图 11 虚假基站与匿名区域示意图

Ren 和 Younis[82]考虑到基站在 WSN 中的重要性,分析并阐述了基站数量以及移动性能对基站匿名性的影响,他们通过开展基站数量对匿名性影响的实验,发现可以利用多个基站增加匿名性,这是由于在 WSN 中若存在多个基站,可以将数据包发给不同的汇聚方,从而使得网络流量分布更均匀,而且在基站附近不会创建明显的热点区域;通过基站移动性的实验表明,基站的移动性是增加匿名的有效方法,但若存在多个移动基站的情况下,基站匿名性可能反而得不到增加,这是由于多个移动基站有可能会造成创建相同热点区域的情况,从而使得攻击方更容易发现基站的位置.

Acharya 和 Younis[83]提出了增强基站匿名性的方法,通过选择数据包的重传,增强基站的匿名性,但增加了通信的能耗. Ebrahimi 和 Younis[84]提出了一种利用提高传感器节点发射功率来增强基站匿名性的方法,在该方法中,传感器节点通过提高发射功率增加其邻居的数量,降低敌对方试图通过评估节点链路质量,以寻找抵达基站路由的能力. 除此之外,他们还提出了应对流量分析并提高基站匿名性的方法[85],该方法的核心是为了使攻击方流量分析无效,并增强混淆攻击方的能力,在某些传感器节点活动不频繁的区域发起虚假的数据流. 由于该方法仅在一些选择的区域传输虚假数据包,故网络总体的能量开销较低. 任艳丽等[86]基于素数阶群与非对称双线性映射假设,提出了基于身份匿名的加密机制,该机制实现了数据保密性和接收者的匿名性,有效地降低了计算开销. Ward 和 Younis[87-88]提出了利用分布式波束成形与跨层协作技术增强基站的匿名性,在分布式无线网络中,分布式波束成形技术是一种增大通信范围、提高数据传输速率与能量有效性、增强物理层安全和减少干扰的有效方法.

Zhong 和 Younis[89] 提出了 3 种方法用以提升基站的匿名性：①探索多基站节点的部署，提供了资源占用与匿名性折衷的指导，以确定最合适的基站数目；②利用基站节点的移动性，分类了基站节点重定位到最低匿名区域的效果；③采用动态传感器集群重关联技术，改变了流量模式迷惑攻击方，提升了基站匿名性. 考虑到攻击方可以通过流量分析识别基站的情况，Ward 和 Younis[90] 提出了一种增强的证据理论——应答感知证据理论. 在该理论中，他们给出了基于应答的 WSN 中基站匿名性的评估指标，该指标较好地表征了带确认机制的基站匿名性，并证明了证据理论的鲁棒性. 随后，他们使用证据理论分析并研究了 2 种常用协议——参考广播同步协议与传感器网络的时序同步协议，给出了 WSN 同步对基站匿名性的影响[91]，仿真结果表明，通过合理配置上述 2 种同步协议参数，实现基站的匿名性不需要增加额外的能量消耗.

由 WSN 技术组成可知，其“数据流向”一定是 Multipoint-to-Point 形式. 其中，Multipoint 指的是众多感知节点，而这里的 Point 指的则是基站（或汇聚节点），因此，如何抵御流量分析成为实现基站匿名性的关键. 目前，实现基站匿名的方法大多采用虚假基站、虚假数据包注入、沿随机路径发送数据包等方法，这些方法的目的在于隐藏真实数据流向使得攻击方难以通过流量分析定位基站，或是提供虚假数据流向误导攻击方定位于错误的基站. 由于这些方法的本质是通过增加冗余的虚假信息来实现匿名性，尽管可以提高基站的匿名性，但是会带来一些附加的通信能量消耗，并且一定程度上降低了有效信息的传输性能.

通过分析发现，以上 3 种匿名通信机制在实现过程中，所使用的知识信息基本上来源于路由层或网络层，基本上没有使用到物理层信息，而 WSN 与传统网络的重要区别之一就是其开放无线传输媒介的动态物理层参数. 因此，可以预见基于跨层的 WSN 匿名通信技术，尤其是结合物理层的跨层匿名通信技术研究将是未来 WSN 信息安全研究的方向之一.

3　匿名通信技术分析

由于传统网络和 WSN，无论在通信方式，还是应用场景等存在较大的差异. 因此，传统网络成熟的匿名技术不能直接应用于 WSN. 下面将在对传统网络的匿名通信技术分析基础上，重点给出 WSN 匿名通信机制的对比与分析.

3.1　传统网络匿名通信技术分析

Mix 能够很好地实现发送方匿名，但具有较高的时间延迟. 这是由于 Mix 报文输出规则采用以下 3 种方式：阈值 Mix、缓冲池 Mix、停止转发 Mix，因此适用于时延不敏感的电子邮件系统. Mix 利用公钥加密技术隐藏通信的参与者和通信内容，因此节点需要有较强的计算能力和较大的存储空间. 另外，为了预防攻击，Mix 通过检测数据包的大小来跟踪数据流的方向，就必须对解密后的信息进行填充，这样就增大了节点的开销.

与 Mix 相比较，Onion Routing 的延迟较小，具有传输的实时性，因此许多实时性要求较高的无线网络采用类似洋葱结构实现其自身的匿名性[8]. Onion Routing 中使用了定长数据包和掩饰流来抵抗复杂的通信流分析；使用加密技术隐藏 IP 包地址，实现了抵抗流量分析攻击和窃听. 但是 Onion Routing 对于以扰乱为目的的主动攻击的抵抗能力非常脆弱，不支持路径重排，而且 Onion Routing 代理易成为敌对方攻击的重点.

Crowds 可以实现发送方匿名，但无法实现接收方匿名. 由于路径的随机建立，Crowds 对路径的长度没有制约，当建立的路径长度过长时，各个成员之间频繁的加解密将会影响网络性能. Crowds 扩展性好，节点可以随时申请加入成员组. 通过对 Web 交互匿名实现 Internet 用户保护，Crowds 适用于较低通信延迟和较高通信效率环境. 另外，DC-Net 协议实现了发送方、接收方以及双方通信关系的匿名，但很容易因不诚实的参与者，而使其匿名性遭到破坏，该协议容易受到拒绝服务攻击，而且扩展性差. 表 1 给出了几种传统匿名通信机制的分析.

由表 1 可以看出，每种匿名通信机制都有各自的优缺点，但是它们的内存和计算等的开销普遍比较大，不适用于 WSN；同时，WSN 是实时性通信系统，对于延迟的要求更加严格. 因此，WSN 匿名需要考虑的因素更多，也更为复杂.

3.2　WSN 匿名机制分析

通过对现有 WSN 匿名通信机制的研究发现，匿名路由机制主要是通过假名机制、加/解密以及多路径机制等方式实现. 源节点隐私保护的匿名通信机制有基于洪泛的路由协议（基线洪泛、概率洪泛、假消息洪泛和基于虚拟的洪泛）、基于数据扰乱的数

表1 传统的匿名路由协议的比较

匿名协议	优点	缺点
Mix	较好地实现匿名,抗攻击性强	延迟大,对抗合谋攻击能力较弱,开销大
Onion	实时性通信,延迟较小	代理易成为攻击重点,抵抗扰乱网络的攻击较差
Tor	匿名好,实时性通信,延迟较小	系统的抗滥用能力不高,计算与通信开销大
Crowds	扩展性好,通信效率高,开销较低	接收方不能实现匿名
DC-Net	理论安全的匿名保护,传输效率高	易受拒绝服务攻击,扩展性差
Tarzan	匿名性较好,开销较低	静态隧道失败时会使计算开销大,延迟大
WonGoo	低延迟,扩展性好,强匿名性	转发路径过长时,系统负载开销变大,延迟变大

据流掩饰、基于假名的策略等. 而基站隐私保护的匿名通信机制大多采用虚假基站、虚假数据包注入、沿随机路径发送数据包等方法. 表2定性地概括了文中涉及的主要匿名机制的匿名性、能量消耗、存储空间、计算量、安全性、实现机制等特性的比较. 其中,网络拓扑是指该匿名通信机制所适用的WSN的拓扑形式,“-”表示原文中未明确指明是何种拓扑.

表2 WSN匿名机制比较分析

匿名机制	匿名性	能量消耗	存储空间	计算量	安全性	实现机制	网络拓扑
SAS	中	中	大	小	中	假名机制、密钥共享	簇状(Cluster)
CAS	中	中	小	大	中	假名机制、密钥共享	簇状(Cluster)
LANDER	较好	大	大	小	较好	Bloom Filter、虚假链路标识	网格(Grid)
MPRSARP	好	大	中	中	中	假名机制、多路径	网状(Mesh)
Mahmoud[64]	较好	大	小	中	较好	虚假包、假名机制	网状(Mesh)
LPSS	中	大	小	大	较好	虚假包、多路径	—
Li[67]	中	大	小	中	中	随机选择中间节点	网状(Mesh)
Park[68]	较好	中	中	大	好	虚拟的IDs、SMAC技术	—
Gottumukkala[78]	较好	中	小	小	中	虚假基站	网状(Mesh)
RRHA	好	大	小	小	中	随机路由、隐藏基站地址	网状(Mesh)
PR & PSPR	较好	中	小	小	中	随机路由、隐藏源地址	网状(Mesh)
SACP	较好	小	小	小	中	假名机制、密钥共享	簇状(Cluster)
SLPP	中	小	中	小	中	虚假包	网状(Mesh)
Gu[81]	中	中	中	中	较好	虚假基站	网状(Mesh)

根据对现有WSN匿名通信机制的分析可知,目前对于其匿名性的实现大多数都是采用虚假数据包、虚假源(基站)、虚假多路径等方法,但是这对于资源受限的WSN来说,有较大的通信、计算开销,不利于保障网络的生命周期. Zhang等[49]提出的多路径机制在一段时间内也只采用了一条安全路径通信,造成路径的冗余,仅适用于大规模网络. 假名策略则需要定期地更新假名,这会增加计算或内存开销. 为了对抗流量分析攻击,大多数的策略都是采用延时、虚假数据流、重加密等,这些方法不能有效地对抗计算能力强大的全局攻击方.

作为WSN节点隐私保护手段之一的匿名通信机制与其他传统网络,如Internet隐私保护技术相比,充分考虑了自身的网络特性,如传播媒介的开放性、网络拓扑的动态性以及节点资源的受限性等,借助成熟的加/解密、混淆、多路径、假名等匿名策略,在加/解密技术的适用性、假名生成与映射等方面,开展了较多有意义的研究工作. 此外,近年来被广泛关注的直接匿名证明(DAA, direct anonymous attestation)机制,可提供较强的正确性、安全性和匿名性,但由于其设计复杂度高,计算开销大,无法直接应用于资源受限的传感器节点. 因此,针对WSN而

言，在保证安全性与匿名性的前提下，有效地降低 DAA 计算复杂度是一个有意义的研究方向，如宋成等[92]采用双线性对密码机制，以双线性对为工具，提出了一种改进的 DAA 机制.

未来，WSN 节点隐私保护技术的研究不仅要关注隐私保护的强度，而且要综合考虑节点的能量消耗、计算能力、传输延时等方面，要以降低内存和计算等开销、提高传输效率、提升安全性(匿名性)、减少时延为研究目标.

4　WSN 匿名通信安全建议

随着 WSN 的发展，越来越多的研究人员开始关注 WSN 的匿名通信，同时提出了不少新颖的匿名算法、机制与技术，但目前该领域的研究尚处于起步阶段，笔者认为未来潜在的研究热点包括以下几个方面.

4.1　基于能量有效性的匿名通信技术

能量供给、计算能力、存储能力等资源受限是 WSN 的重要特征，能量受限已成为制约大范围、长期部署 WSN 的最主要因素，而能量消耗和通信安全是 WSN 最为敏感的因素. 传统网络的匿名技术，无论提供发送方匿名的 Mix、Onion Routing 和 Tor，还是实现发送方、接收方以及双方通信关系匿名的 DC-Net 和 Tarzan，它们的内存占用与计算开销等都比较大，不适用于 WSN. 而已有的匿名通信算法往往需要较大的通信能量消耗，从而影响了 WSN 的生命周期.

目前，WSN 匿名通信机制大多数采用虚假数据包、虚假源(基站)等方法，也存在通信、计算开销较大的情况，同时，针对现有的匿名技术缺乏有效的能效分析机制. 笔者认为，进一步研究基于能量有效性的匿名通信技术，建立能量有效性分析评估机制，对未来的相关研究将提供更加有效的技术支撑. 另外，在能效有限的基础上，开展针对低复杂度、高安全性的加密/解密机制，构建多路径机制增加冗余路径，提高路径反跟踪的难度等方向的研究，将更加有助于减少能量消耗，降低通信时间延迟，提升算法的综合性能.

4.2　WSN 跨层匿名通信机制

跨层设计是根据具体应用通过将 2 个或多个网络功能层融合为一层，对整个层次体系进行整合. WSN 跨层匿名通信机制的研究将探索建立一种可靠、可长期利用的参考模型，同时结合其节点计算能力、存储能力、通信能力以及能量供给等约束条件，将采用信息变换或部分信息的加/解扰方式，逐步替代复杂的加解密运算，如散列函数、数字签名等，利用节点仅能获取的局部拓扑信息、无线传输媒介与动态的物理层参数等，进行跨层匿名通信机制的设计. 所设计的匿名通信机制应对原有通信协议栈的影响尽可能小，计算、通信的开销尽可能少；针对不同应用服务质量需求，使用不同优化尺度；通过信息的共享与交换，层与层之间联合优化，提高各个层的适应性，同时满足不同组网形式、网络协议下抵御潜在攻击的安全需要，提高整个网络的安全性能，为 WSN 的规模应用提供有力的技术基础.

4.3　基于位置的匿名路由

无线通信技术和智能移动终端的广泛应用，出现了车载传感网、参与式传感网等各种新型网络，同时，各种基于位置服务也得到飞速发展与普及. 现有 WSN 基于位置隐私保护的匿名技术存在一定的安全隐患，攻击方已具有一定的应对措施，从而直接破解或者绕过一般的隐私保护技术. 现有的大部分攻击模型可以分为隐私保护算法漏洞的攻击、利用辅助信息的攻击、伪装用户攻击、拒绝服务攻击等，但相对的防御手段较为单一，如对抗流量分析攻击，大多数的策略都是采用延时、虚假数据流、重加密等，这些方式不能有效地对抗计算能力强大的全局攻击方.

进一步研究基于位置的匿名路由，将位置信息作为潜在的知识应用于匿名路由的设计中，同时综合考虑隐私保护强度、能量消耗、计算能力、延时等因素. 根据用户需求、时间、地点不同，设计出具有较高弹性的匿名路由协议，实现对节点隐私信息的有效保护的同时，又能根据现有的位置信息发现与其关联的潜在知识，进而为最终用户的个性化服务提供有效的支持.

5　结束语

尽管对匿名通信技术已有较多的研究，但是在 WSN 领域的研究相对较少. 笔者主要阐述了传统网络匿名通信技术与现有 WSN 匿名机制的研究进展，并且对它们进行较为系统地分析. 虽然传统网络的匿名技术相对成熟，但不能直接应用于 WSN，而现有的一些 WSN 匿名通信机制是以牺牲网络其他性能来换取节点的匿名性或隐私保护，但这可能导致 WSN 的生命周期无法得到保障.

WSN匿名通信技术需要满足的条件:WSN是实时性网络,所以必须具有较小的时延;传感器节点自身条件的限制,对于内存、计算和能量的开销希望尽量少. 通过对现有的匿名通信机制分析发现,可以借助传统网络匿名通信机制的思想/策略,将其进一步研究、优化,应用于WSN的匿名通信机制中,如Mix中的混淆思想、Crowds中的组播思想、多路径策略、动态假名机制等. 因此,在将来的工作中,将基于分片、混淆、多路径开展匿名性和可靠性均衡的安全路由协议研究,并将继续关注未来WSN匿名技术的研究热点,包括基于能量有效性的匿名技术、跨层匿名机制以及基于位置的匿名路由等.

参考文献:

[1] AL-Fuqaha A, Guizani M, Mohammadi M, et al. Internet of things: a survey on enabling technologies, protocols, and applications[J]. IEEE Commu Sur Tut, 2015, 17(4): 2347 -2376.

[2] Granjal J, Monteiro E, Silva J S. Security in the integration of low-power wireless sensor networks with the Internet: a survey[J]. Ad Hoc Networks, 2015, 24: 264-287.

[3] 罗新强, 齐悦, 万亚东, 等. 面向工业无线网络的低开销快速AES加密方法[J]. 北京邮电大学学报, 2015, 38(1): 55-60.
Luo Xinqiang, Qi Yue, Wan Yadong, et al. Low-ocst and fast AES encryption method for industrial wireless network[J]. Journal of Beijing University of Posts and Telecommunications, 2015, 38(1): 55-60.

[4] 刘志宏, 马建峰, 庞辽军, 等. 密钥传播在传感器网络中的应用[J]. 通信学报, 2009, 30(11): 56-63.
Liu Zhihong, Ma Jianfeng, Pang Liaojun, et al. Key infection and its applications in sensor networks[J]. Journal on Communications, 2009, 30(11): 56-63.

[5] 曾勇, 马建峰. 基于位置的无线传感器网络可靠性区分服务机制[J]. 通信学报, 2008, 29(2): 56-63.
Zeng Yong, Ma Jianfeng. Location based reliability differentiation service for WSN[J]. Journal on Communications, 2008, 29(2): 56-63.

[6] 余旺科, 马文平, 严亚俊, 等. 利用信任模型构建安全路由协议[J]. 北京邮电大学学报, 2010, 33(3): 48-51.
Yu Wangke, Ma Wenping, Yan Yajun, et al. Constructing secure routing protocol using trust model[J]. Journal of Beijing University of Posts and Telecommunications, 2010, 33(3): 48-51.

[7] Sanzgiri K, Laflamme D, Dahill B. et al. Authenticated routing for ad hoc networks[J]. IEEE J Sel Area Comm, 2005, 23(3): 598-610.

[8] Rios R, Lopez J. (Un) suitability of anonymous communication systems to WSN[J]. IEEE Syst J, 2013, 7(2): 298-310.

[9] Ying B, Makrakis D, Mouftah H T. A protocol for sink location privacy protection in wireless sensor networks[C]// GLOBECOM 2011. Houston, TX: IEEE Press, 2011: 1-5.

[10] Chaum D L. Untraceable electronic mail, return addresses, and digital pseudonyms[J]. Commu ACM, 1981 (2): 84-90.

[11] 王继林, 伍前红, 陈德人, 等. 匿名技术的研究进展[J]. 通信学报, 2005, 26(2): 112-118.
Wang Jilin, Wu Qianhong, Chen Deren, et al. A survey on the technology of anonymity[J]. Journal on Communications, 2005, 26(2): 112-118.

[12] Blaze M, Bleumer G, Strauss M. Divertible protocols and atomic proxy cryptography[C]// Lecture Notes in Computer Science: Vol 1403. Berlin Heidelberg: Springer, 1998: 127-144.

[13] Golle P, Jakobsson M, Juels A, et al. Universal re-encryption for mixnets[C]// Lecture Notes in Computer Science: Vol 2964. Berlin Heidelberg: Springer, 2004: 163-178.

[14] Reed M, Syverson P, Goldschlag D. Anonymous connections and onion routing[J]. IEEE J Sel Area Comm, 1998, 16(4): 482-494.

[15] Goldschlag D, Reed M, Syverson P. Hiding routing information[C]// Lecture Notes in Computer Science: Vol 1174. Berlin Heidelberg: Springer, 1996: 137-150.

[16] Goldschlag D, Reed M, Syverson P. Onion routing for anonymous and private internet connections[J]. Commu ACM, 1999, 42(2): 39-41.

[17] Dingledine R, Mathewson N, Syverson P. Tor: the second-generation onion router[C]// SSYM 2004. Berkeley: ACM Press, 2004: 21-21.

[18] 赵福祥, 王育民, 王常杰. 可靠洋葱路由方案的设计与实现[J]. 计算机学报, 2001, 24(5): 463-467.
Zhao Fuxiang, Wang Yumin, Wang Changjie. An authenticated scheme of onion routing[J]. Chinese Journal of Computers, 2001, 24(5): 463-467.

[19] 时金桥, 方滨兴, 郭莉, 等. 抵御MIX重放攻击的混合结构消息报文机制[J]. 通信学报, 2009, 30(3): 21-26.
Shi Jinqiao, Fang Binxing, Guo Li, et al. Hybrid-struc-

tured onion scheme against replay attack of MIX[J]. Journal on Communications, 2009, 30(3): 21-26.

[20] 李龙海, 付少锋, 苏锐丹, 等. 对一种混合结构洋葱路由方案的密码学分析[J]. 通信学报, 2013, 34(4): 88-98.
Li Longhai, Fu Shaofeng, Su Ruidan, et al. Cryptanalysis of a hybrid-structured onion routing scheme[J]. Journal on Communications, 2013, 34(4): 88-98.

[21] Kurve A, Griffin C, Miller D J, et al. Optimizing cluster formation in super-peer networks via local incentive design[J]. Peer-to-Peer Networking & Applications, 2015, 8(1): 1-21.

[22] Soltani M, Najafi S, Jalili R. Mid-defense: mitigating protocol-level attacks in TOR using indistinguishability obfuscation[C]// ISCISC 2014. Piscataway: IEEE Press, 2014: 214-219.

[23] Haraty R A, Zantout B. The TOR data communication system[J]. Journal of Communications and Networks, 2014, 16(4): 415-420.

[24] Ling Zhen, Luo Junzhou, Yu Wei, et al. Tor bridge discovery: extensive analysis and large-scale empirical evaluation[J]. IEEE T Parall Dist, 2015, 28(7): 1887-1899.

[25] Emura K, Kanaoka A, Ohta S, et al. Secure and anonymous communication technique: formal model and its prototype implementation[J]. IEEE Trans on Emerging Topics in Computing, 2016, 4(1): 88-101.

[26] Reiter M K, Rubin A D. Crowds: anonymity for web transactions[J]. ACM T Inform Syst Se, 1998, 1(1): 66-92.

[27] Shields C, Levineb N. A protocol for anonymous communication over the Internet[C]// CCS 2000. New York: ACM Press, 2000: 33-42.

[28] 陶颋, 包仁丹, 孙乐昌. S-Crowds 匿名通信协议的性能研究[J]. 海军工程大学学报, 2008, 20(2): 109-112.
Tao Ting, Bao Rendan, Sun Lechang. Research on performance of S-Crowds anonymous communication protocol[J]. Journal of Naval University of Engineering, 2008, 20(2): 109-112.

[29] 吴云霞, 黄明和, 汪浩. 一种基于 Crowds 的改进匿名通信系统[J]. 江西师范大学学报(自然科学版), 2009, 33(1): 88-91.
Wu Yunxia, Huang Minghe, Wang Hao. An improved anonymous communication system based on Crowds[J]. Journal of Jiangxi Normal University (Natural Sciences Edition), 2009, 33(1): 88-91.

[30] Chaum D. The dining cryptographers problem: unconditional sender and recipient untraceability[J]. Journal of Cryptology, 1988(1): 65-75.

[31] Freedman M J, Morris R. Tarzan: a peer-to-peer anonymizing network layer[C]// CCS 2002. New York: ACM Press, 2002: 193-206.

[32] 陆天波, 方滨兴, 孙毓忠, 等. 点对点匿名通信协议 WonGoo 的性能分析[J]. 计算机工程, 2006, 32(2): 26-29.
Lu Tianbo, Fang Binxing, Sun Yuzhong, et al. Performance analysis of a peer-to-peer anonymous communication protocol WonGoo[J]. Computer Engineering, 2006, 32(2): 26-29.

[33] Rennhard M, Plattner B. Introducing morphmix: peer-to-peer based anonymous internet usage with collusion detection[C]// WPES 2002. New York: ACM Press, 2002: 91-102.

[34] Moller U, Cottrell L, Palfrader P. Mixmaster protocol-version 2[EB/OL]. (2003-12-15)[2016-02-09]. http://www.eskimo.com/rowdenw/crypt/Mix/draft-moeller-mixmaster2-protocol-00.txt.

[35] Dai Wei. PipeNet 1.1[EB/OL]. (1996-08-05)[2016-01-06]. http://www.eskimo.com/~weidai/pipenet.txt.

[36] Danezis G, Dingledine R, Mathewson N. Mixminion: design of a type III anonymous remailer protocol[C]// IEEE SP 2003. Berkeley: IEEE Press, 2003: 2-15.

[37] Perrig A, Stankovic J A, Wagner D, Security in wireless sensor networks[J]. COMMUN ACM, 2004, 47(6): 53-57.

[38] Karlof C, Wagner D. Secure routing in wireless sensor networks: attacks and countermeasures[J]. Ad Hoc Network, 2003, 1(2/3): 293-315.

[39] Kim Y, Perrig A, Tsudik G. Group key agreement efficient in communication[J]. IEEE T COMPUT, 2004, 53(7): 905-921

[40] Tu Shanshan, Ma Chunbo, Ao Faliang, et al. The research of hierarchical group key management for Ad hoc networks[C]//ICISS 2010. Guilin: IEEE Press, 2010: 121-124.

[41] 李慧贤, 庞辽军, 王育民. 适合 Ad hoc 网络无需安全信道的秘钥管理方案[J]. 通信学报, 2010, 31(1): 112-117.
Li Huixian, Pang Liaojun, Wang Yumin. Key management scheme without secure channel for ad hoc networks[J]. Journal on Communications, 2010, 31(1): 112-117.

[42] 袁珽, 马建庆, 钟亦平, 等. 基于时间部署的无线传感器网络密钥管理方案[J]. 软件学报, 2010, 21(3): 516-527.
Yuan Ting, Ma Jianqing, Zhong Yiping, et al. Key management scheme using time-based deployment for wireless sensor networks[J]. Journal of Software, 2010, 21(3): 516-527.

[43] 麻常莎, 薛开平, 洪佩琳, 等. 基于STR非平衡树结构的混合组密钥管理方案[J]. 中国科技大学学报, 2011, 41(7): 582-588.
Ma Changsha, Xue Kaiping, Hong Peilin, et al. Hybrid group key management scheme based on STR unbalanced tree structure[J]. Journal of University of Science and Technology of China, 2011, 41(7): 582-588.

[44] Misra S, Xue Guoliang. SAS: a simple anonymity scheme for clustered wireless sensor networks[C]// ICC 2006. Istanbul: IEEE Press, 2006: 3414-3419.

[45] Misra S, Xue Guoliang. Efficient anonymity schemes for clustered wireless sensor networks [J]. International Journal of Sensor Networks, 2006, 1(1/2): 50-63.

[46] Shi Leyi, Fu Wenjing, Jia Cong, et al. A sensor anonymity enhancement scheme based on pseudonym for clustered wireless sensor network[J]. China Communications, 2014, 11(9): 6-15.

[47] Abdullahi M B, Wang Guoqing. A lightweight anonymous on-demand routing scheme in wireless sensor networks[C]// TrustCom 2012. Liverpool: IEEE Press, 2012: 978-985.

[48] Yuan Wei. An anonymous routing protocol with authenticated key establishment in wireless ad hoc network[J]. Int J Distrib Sensor N, 2014: 10.

[49] Zhang Zhiming, Jiang Changgen, Deng Jiangang. Multiple-path redundancy secret anonymous routing protocol for wireless sensor networks [C] // WiCOM 2010. Chengdu: IEEE Press, 2010: 1-4.

[50] Zhang Zhiming, Jiang Changgen, Deng Jiangang. A secure anonymous path routing protocol for wireless sensor networks[C] // WCNIS 2010. Beijing: IEEE Press, 2010: 415-418.

[51] Gagneja K K. Secure communication scheme for wireless sensor networks to maintain anonymity[C]//ICNC2015. Anaheim: IEEE Press, 2015: 1142-1147.

[52] Sheu J P, Jiang J R, Tu C. Anonymous path routing in wireless sensor Networks [C] // ICC 2008. Beijing: IEEE Press, 2008: 2728-2734.

[53] Yang Guang, Geng Guining, Song Jing, et al. A secure anonymous routing protocol in WSN[C] // ICIA 2013. Yinchuan: IEEE Press, 2013: 415-418.

[54] Pan P, Boppana R V. ACP: anonymous communication protocol for wireless sensor networks[C]//CCNC 2011. Las Vegas: IEEE Press, 2011: 751-755.

[55] Manjula R, Datta R. An energy-efficient routing technique for privacy preservation of assets monitored with WSN[C] // TechSym 2014. Kharagpur: IEEE Press, 2014: 325-330.

[56] Nakamura S, Hori Y, Sakurai K. Communication efficient anonymous routing protocol for wireless sensor networks using single path tree topology [C] // WAINA 2012. Fukuoka: IEEE Press, 2012: 766-771.

[57] 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 Hui, Chen Hong, Zhang Xiaoying, et al. Location privacy preservation in wireless sensor network [J]. Journal of Software, 2015, 26(3): 617-639.

[58] Alomair B, Clark A, Cuellar J, et al. Toward a statistical framework for source anonymity in sensor networks[J]. IEEE Trans Mobile Comput, 2013, 12(2): 248-260.

[59] Ozturk C, Zhang Yanyong, Trappe W, et al. Source-location privacy in energy-constrained sensor network routing [C] // SASN 2004. Washington: ACM Press, 2004: 88-93.

[60] Kamat P, Zhang Yanyong, Trappe W, et al. Enhancing source-location privacy in sensor network routing[C] // ICDCS2005. Columbus: IEEE Press, 2005: 559-608.

[61] 马春光, 周长利, 杨松涛, 等. 基于Voronoi图预划分的LBS位置隐私保护方法[J]. 通信学报, 2015, 36(5): 5-16.
Ma Chunguang, Zhou Changli, Yang Songtao, et al. Location privacy-preserving method in LBS based on Voronoi division[J]. Journal on Communication, 2015, 36(5): 5-16.

[62] 周长利, 马春光, 杨松涛. 基于敏感位置多样性的LBS位置隐私保护研究[J]. 通信学报, 2015, 36(4): 129-140.
Zhou Changli, Ma Chunguang, Yang Songtao. Research of LBS privacy preserving based on sensitive location diversity[J]. Journal on Communication, 2015, 36(4): 129-140.

[63] Niu Xiaoguang, Wei Chuanbo, Feng Weijiang, et al. OSAP: optimal-cluster-based source anonymity protocol in delay-sensitive wireless sensor networks[C]//WCNC 2014. Istanbul: IEEE Press, 2014: 2880-2885.

[64] Mahmoud M E, Shen Xuemin. Secure and efficient source location privacy-preserving scheme for wireless

sensor networks[C] // ICC 2012. Ottawa & Ontario: IEEE Press, 2012: 1123-1127.

[65] Kang Lei. Protecting location privacy in large-scale wireless sensor networks[C] // ICC 2009. Dresden: IEEE Press, 2009: 1-6.

[66] Tan Wei, Xu Ke, Wang Dan. An anti-tracking source-location privacy protection protocol in WSNs based on path extension[J]. IEEE Internet of Things Journal, 2014, 1(5): 461-471.

[67] Li Yun, Ren Jian. Source-location privacy through dynamic routing in wireless sensor networks[C] // INFOCOM 2010. San Diego, CA: IEEE Press, 2010: 1-9.

[68] Park J H, Jung Y H, Lee K H, et al. A new privacy scheme for providing anonymity technique on sensor network[C] // UCMA 2011. Daejeon: IEEE Press, 2011: 10-14.

[69] Park H, Song Sejun, Choi B Y, et al. PASSAGES: preserving anonymity of sources and sinks against global eavesdroppers[C] // INFOCOM 2013. Turin: IEEE Press, 2013: 210-214.

[70] Gurjar A, Patila A R B. Cluster based anonymization for source location privacy in wireless sensor network[C] // CSNT 2013. Gwalior: IEEE Press, 2013: 248-251.

[71] Zhang Yihua, Price M, Opyrchal L, et al. All proxy scheme for event source anonymity in wireless sensor networks[C] // ISSNIP 2010. Brisbane: IEEE Press, 2010: 263-268.

[72] Reindl P, Du Xiaojiang, Nygard K, et al. Light weight source anonymity in wireless sensor networks[C] // GLOBECOM 2011. Houston, TX: IEEE Press, 2011: 1-5.

[73] Shinganjude R D, Theng D P. Inspecting the ways of source anonymity in wireless sensor network[C] // CSNT2014. Bhopal: IEEE Press, 2014: 705-707.

[74] Kazemi M, Azmi R. Privacy preserving and anonymity in multi sinks wireless sensor networks with master sink[C] // ICCCNT 2014. Heifei: IEEE Press, 2014: 1-7.

[75] Pongaliur K, Xiao Li. Maintaining source privacy under eavesdropping and node compromise attacks[C] // INFOCOM 2011. Shanghai: IEEE Press, 2011: 1656-1664.

[76] Amahmoud M M E, Shen Xuemin. A cloud-based scheme for protecting source-location privacy against hotspot-locating attack in wireless sensor networks[J]. IEEE Trans Parall Distr, 2012, 23(10): 1805-1818.

[77] Li Yun, Ren Jian, Wu Jie. Quantitative measurement and design of source-location privacy schemes for wireless sensor networks[J]. IEEE Trans Parall Distr, 2012, 23(7): 1302-1311.

[78] Gottumukkala V P V, Pandit V, Li Hailong, et al. Base-station location anonymity and security technique (blast) for wireless sensor networks[C] // ICC 2012. Ottawa, Ontario: IEEE Press, 2012: 6705-6709.

[79] Shahare P C, Chavhan N A. An approach to secure sink node's location privacy in wireless sensor networks[C] // CSNT 2014. Bhopal: IEEE Press, 2014: 748-751.

[80] Ngai E C H. On providing sink anonymity for sensor networks[C] // IWCMC 2009. New York: ACM Press, 2009: 269-273.

[81] Gu Qijun, Chen Xiao, Jiang Zhen, et al. Sink-anonymity mobility control in wireless sensor networks[C] // WIMOB 2009. Marrakech: IEEE Press, 2009: 36-41.

[82] Ren Z, Younis M. Effect of mobility and count of base-stations on the anonymity of wireless sensor networks [C] // IWCMC 2011. Istanbul: IEEE Press, 2011: 436-441.

[83] Acharya U, Younis M. An approach for increasing base-station anonymity in sensor networks[C] // ICC 2009. Dresden: IEEE Press, 2009: 1-5.

[84] Ebrahimi Y, Younis M. Increasing transmission power for higher base-station anonymity in wireless sensor network[C] // ICC 2011. Kyoto: IEEE Press, 2011: 1-5.

[85] Ebrahimi Y, Younis M. Using deceptive packets to increase base-station anonymity in wireless sensor network [C] // IWCMC 2011. Istanbul: IEEE Press, 2011: 842-847.

[86] 任艳丽, 张新鹏, 钱振兴. 素数阶群中基于身份的匿名加密方案[J]. 北京邮电大学学报, 2013, 36(5): 96-98.
Ren Yanli, Zhang Xinpeng, Qian Zhenxing. Anonymous identity-based encryption scheme in groups of prime order[J]. Journal of Beijing University of Posts and Telecommunications, 2013, 36(5): 96-98.

[87] Ward J R, Younis M. On the use of distributed beam forming to increase base station anonymity in wireless sensor networks[C] // ICCCN 2013. Nassau: IEEE Press, 2013: 1-7.

[88] Ward J R, Younis M. Increasing base station anonymity using distributed beamforming[J]. Ad Hoc Networks, 2015, 32(9): 53-80.

(下转第 27 页)

表 4　计算所得左右两侧二杆组的设计参数

序号		r_1/r_2	a/d	b/c	μ_1/μ_2	φ_0/ψ_0
	1	19.509 8	3.473 5	3.793 1	1.043 8	1.876 6
左侧	2	15.855 1	0.925 1	5.527 0	0.847 4	1.198 7
参数	3	10.307 3	1.012 5	16.448 0	0.077 4	1.128 2
	4	20.043 8	0.780 6	1.685 0	0.997 3	−0.076 3
	1′	19.885 6	1.167 1	2.280 8	1.009 5	1.309 4
右侧	2′	20.634 5	1.081 8	1.424 9	1.016 2	−0.343 5
参数	3′	26.845 5	1.901 2	14.836 6	0.437 0	−1.045 5
	4′	21.521 2	2.049 2	3.054 0	0.904 7	−0.796 4

通过仿真程序对综合所得机构进行运动分析，发现左右两侧均取第 3 组参数时组成的平面五杆机构生成轨迹与目标轨迹最为接近，且不存在分支和逆序问题，满足设计要求. 图 5 所示为目标轨迹与机构生成轨迹的比较.

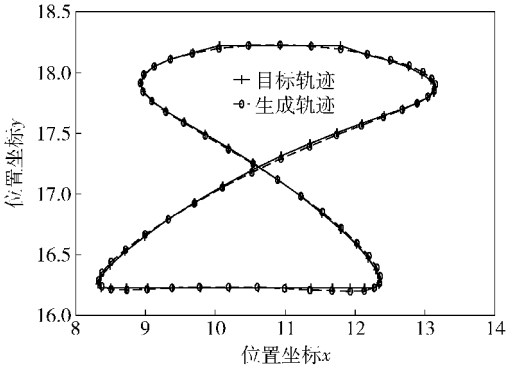

图 5　目标轨迹与综合机构生成轨迹比较

5　结束语

建立了一种基于傅氏级数的平面五杆机构轨迹综合代数求解新方法. 通过将平面五杆机构分解为两个二杆组，对轨迹综合设计变量进行解耦. 在此基础上，分析得到机构尺寸与连杆曲线谐波参数间的函数关系，依据这一关系建立了不同传动比条件下平面五杆机构轨迹综合设计的新方程，通过配析消元法进一步将方程化简为一元四次代数方程，得到了平面五杆机构轨迹综合设计参数计算的通用公式. 与已有的综合方法相比，该方法在实现多点轨迹综合的同时，采用解析方法求解，无需给定初值和建立数值图谱库，具有求解精度高，计算速度快，便于计算机编程的特点；同时，其可得出多组可行方案，为机构的进一步筛选和优化提供了前提.

参考文献：

[1] 辛洪兵，余跃庆. 平面五杆并联机器人运动学导论[M]. 北京：国防工业出版社，2007.

[2] Starns G, Flugrad D R. Five-bar path generation synthesis by continuation methods [J]. Journal of Mechanical Design, 1993, 115(4): 988-994.

[3] Buśkiewicz J. Use of shape invariants in optimal synthesis of geared five-bar linkage [J]. Mechanism and Machine Theory, 2010, 45(2): 273-290.

[4] Lin Wenyi. Optimum path synthesis of a geared five-bar mechanism [J]. Advances in Mechanical Engineering, 2013(2): 1-13.

[5] Chu Jinkui, Sun Jianwei. Numerical atlas method for path generation of spherical four-bar mechanism [J]. Mechanism and Machine Theory, 2010, 45(6): 867-879.

[6] 褚金奎，孙建伟. 连杆机构尺度综合的谐波特征参数法[M]. 北京：科学出版社，2010.

[7] McGarva J, Mullineux G. Harmonic representation of closed curves [J]. Applied Mathematical Modelling, 1993, 17(4): 213-218.

(上接第 17 页)

[89] Zhong Ren, Younis M. Exploiting architectural techniques for boosting base-station anonymity in wireless sensor networks[J]. International Journal of Sensor Networks, 2012, 11(4): 215-227.

[90] Ward J R, Younis M. A metric for evaluating base station anonymity in acknowledgement -based wireless sensor networks [C] // MILCOM 2014. Baltimore: IEEE Press, 2014: 216-221.

[91] Ward J R, Younis M. Examining the effect of wireless sensor network synchronization on base station anonymity [C] // MILCOM 2014. Baltimore: IEEE Press, 2014: 204-209.

[92] 宋成，李静，彭维平，等. 基于双线性对的直接匿名认证方案[J]. 北京邮电大学学报，2014，37(6)：72-76.
Song Cheng, Li Jing, Peng Weiping, et al. Research on direct anonymous attestation scheme based on bilinear pairing[J]. Journal of Beijing University of Posts and Telecommunications, 2014, 37(6): 72-76.