适合P2P环境的动态多秘密共享方案

鲍 洋 卢正鼎 黄保华 李瑞轩 胡和平 路松峰
(华中科技大学计算机学院 武汉 430074)

摘 要 P2P环境中缺少可信的第三方,节点上线率相对较低,而且网络成员与网络规模都处于不断的变动中,这些特性使现有的多秘密共享方案无法有效地工作。针对P2P环境的特点,提出了一种动态多秘密共享方案。首先,该方案无需可信分发者和安全通讯信道,且在保持密文不变的前提下参与者的身份、数量及系统门限值均能动态改变。其次,采用Byzantine Quorum方式在DHT上管理参与者的身份与验证信息,使秘密重构与改变系统参数的操作只需门限个参与者同时在线即可完成。再次,使用基于身份的公钥密码系统与二元多项式,减小了消息开销,同时得以有效地对抗成员欺骗。因此,提出的动态多秘密共享方案能较好地应用于P2P环境。

关键词 对等网,多秘密共享,基于身份的公钥密码系统,门限方案

Dynamic Multi-secret Sharing Scheme for P2P Environment

BAO Yang LU Zheng-ding HUANG Bao-hua LI Rui-xuan HU He-ping LU Song-feng
(College of Computer Science and Technology, Huazhong University of Science and Technology, Wuhan 430074, China)

Abstract Lack of a trusted third party, relatively low node availability and constantly changing membership and network size, make existing multi-secret schemes unsuitable for P2P environment. A dynamic multi-secret sharing scheme was proposed for P2P networks. Neither trusted dealers nor secure communication channels are necessary for the proposed scheme, which allows dynamic changes of participants and the system threshold in keeping ciphertext untouched. In the meantime, the participants' identity and public commitments together with system parameters are managed by Byzantine Quorums, which makes it possible to reconstruct a shared secret, add a participant or change the system threshold with only threshold participants online. Additionally, ID-based public key cryptosystem and bivariate polynomials are used to reduce message traffic and deal with participant cheating. Altogether, the proposed scheme overcomes the drawbacks of the previous schemes in P2P environment.

Keywords Peer-to-peer network, Multiple secret sharing, ID-based public key cryptosystem, Threshold scheme

秘密共享是信息安全中一个重要的研究领域,是分布式系统中数据保密的重要手段。在(t,n)秘密共享方案中,一个秘密s被分成n份,交由一组参与者分别保管,其中任意t个或多于t个参与者联合可容易地重构s,而少于t个参与者则无法获得s的任何信息。

多秘密共享是单个秘密共享的自然延伸,其主要研究内容是如何安全有效地共享多个秘密:不仅参与者持有的子密钥能重复使用,而且即使某个秘密泄漏也不会威胁其它共享秘密的安全[1]。虽然存在许多有效的多密钥共享方案,但这些方案均不适合P2P环境。

1 P2P环境中的多秘密共享

节点动态加入与离开造成的覆盖网的搅动是P2P环境最常见的问题之一。大多数多秘密共享方案要求参与者身份在系统构造时确定且在运行过程中保持不变,将节点的失效/离开视为被敌手攻陷[1-3]。在频繁的节点搅动下,此类方案的门限值将很快被突破,从而无法继续保持理论上的安全特性。

虽然近年来出现了一些允许动态增加参与者的多秘密共享方案[4-6],但真正允许安全地移除参与者,确保被移除的参与者即使公开其秘密份额也无法威胁系统安全性的只有Herzberg提出的主动秘密共享方案[7]。然而该方案中增加参与者和更新秘密份额需要全体成员协作完成,不适合节点上线率相对较低的P2P环境[8]。

正常运行中P2P网络缺少可信的第三方,这为使用需要特定秘密分发者(dealer)来完成加密[3,9]或处理参与者加入[6]的多秘密共享方案带来了直接的困难:即使秘密分发者的行为是可验证的[3],也无法阻止其单方面地泄漏秘密信息或者以Sybil Attack[10]的方式攻击系统。此外,依赖特定的秘密分发者易使该节点成为系统可用性的瓶颈,从而进一步成为拒绝服务攻击的目标。

到稿日期:2009-10-16 返修日期:2009-12-29 本文受国家自然科学基金委员会和中国工程物理研究院联合基金(10876012)资助。

鲍 洋 博士生,主要研究方向为对等计算及安全,E-mail:ybao@smail.hust.edu.cn;**卢正鼎** 教授,博士生导师,主要研究方向为分布式计算、软件集成环境、数据库系统、信息安全;**黄保华** 博士,主要研究方向为P2P安全与应用;**李瑞轩** 博士,副教授,主要研究方向为分布式计算、分布式系统安全;**胡和平** 教授,主要研究方向为软件工程、智能决策系统、信息安全、数据库系统;**路松峰** 博士,副教授,主要研究方向为数据挖掘、Web服务与信息安全。

带宽资源是 P2P 系统可伸缩性的最主要限制[11]。Crescenzo 等人将"广播验证信息"限制在参与者 2 hop 内的邻居集合中，极大地减少了方案的消息开销[12]。Saxena 等人针对 P2P 环境使用二元多项式消除了 Herzberg 方案[7]中参与者加入时的广播动作[13]。Daza 等人应用椭圆曲线算法在 P2P 网络中实现了基于身份的公钥密码系统，避免了加密时的密钥协商过程[14]。

在典型 P2P 环境中，节点上线率和网络规模都呈周期性的变化[8]，参与者数量及门限值可变的多秘密共享方案能更加充分地利用网络资源，提供更高的安全性和可用性。Pietro 等人提出了一个可动态增加门限值的秘密共享方案，其中系统节点被划分为 t 类，每类构成一个逻辑上的参与者，以实现 (t,t) 秘密共享[15]。在 Daza 等人提出的基于三元多项式的密码系统中，加密者可通过公开部分解密信息来降低单个秘密的解密门限[5]。

2 公开信息的存储

在多秘密共享领域，公告牌(notice board，bulletin board)机制被广泛用于存储公开信息(通常包括系统参数与验证值)。简单来说，公告牌是一片可靠的存储区域，参与者可以随时查询其内容并信任其返回的结果。

我们使用 Quorum 系统实现 P2P 环境中系统公开信息的可靠存储。Quorum 系统是一个包含一个或多个服务器集合的集合，这个集合中的每个元素叫做一个 quorum，它依靠 quorum 之间充分的相交实现容错[16]。在 P2P 环境中，与经典的基于状态机的方法相比，Quorum 系统工作时产生的消息数更少、操作响应时间更快、节点负载更低，是提高系统可用性和效率的有效工具。下面介绍本文使用的 Byzantine Quorum 算法的基本步骤，其中参与者数量达到了理论最小值，正常情况下读/写操作只需 2/4 次通讯，而基于版本的乐观并发控制保证了并发操作的线性一致性。限于篇幅，这里只给出正常情况下的读写过程，争用的处理及正确性证明请参考我们前期的工作[17]。

假设恶意服务器的数量不多于 f，则系统需要 $n\geqslant 3f+1$ 个服务器来保证操作正确完成。我们采用写证书来阻止恶意用户的 poisonous write[18]：客户 c 向 Quorum 系统中写数据时须先向门限个服务器声明自己的操作内容才能开始实际的写入：

1)申请写许可：客户 c 向所有服务器发送写请求；

2)颁发写许可：收到写请求的服务器 p_i，如果已颁发了对应版本的写许可 G，则反馈拒绝消息 $\langle Refuse,G\rangle_{p_i}$，否则反馈写许可 $G=\langle Grant,ver,hash(v),c\rangle_{p_i}$；

3)构造写证书：客户 c 尝试收集 $n-f$ 个写许可，并使用这些写许可构造一个写证书 C，然后发送写证书 C 给所有服务器；

4)执行写操作：若服务器上数据的版本符合写证书 C 的要求，则执行写操作，并反馈确认消息；

5)确认写操作：客户 c 收集到 $n-f$ 个有效的、符合写证书 C 的确认消息后，写操作成功结束。

客户 c 从 Quorum 系统中读信息时，首先向所有服务器发送读请求 $\langle Read,c.ts\rangle$，其中 $c.ts$ 为客户端时间戳。正确的客户端能保证两次不同的读请求中附加的时间戳不同。收到消息的服务器 p_i 反馈 $\langle Value,c.ts,C\rangle_{p_i}$。当客户 c 成功收集了不少于 $n-f$ 个写证书一致的反馈消息后，读操作成功结束。

3 适合 P2P 环境的多秘密共享方案

系统存在 4 类节点：负责初始化工作的系统节点、执行加密与秘密重构的客户节点、提供解密服务的解密节点和负责维护公共信息的管理节点。节点类别是一种逻辑身份，仅用于表示节点的职责。某个实际节点可同时属于多个类别。

加解密运算使用基于身份的公钥密码系统：每个节点的 ID 同时也是其公钥[14]。系统以不同的组的形式同时提供多安全级的秘密共享服务，每个组有固定的 ID 以及可变的解密节点与管理节点集合。管理节点以 Quorum 系统的形式工作于可抗 Byzantine 失效的 DHT 系统[19,20]上，通过本文第 2 节中的读写协议维护组的公共信息，包括解密节点集合、验证参数、门限值等。

加密时，客户节点使用某个组 ID 加密明文；秘密重构时，客户节点请求该组的解密节点根据密文计算解密分片，在收集到门限个有效的解密分片后即可获得原始明文。

3.1 系统初始化

系统的初始化参数为 $\langle T,q,P,e,H_1,H_2,H_3,H_4\rangle$，其中 T 为基于身份的公钥密码系统的安全门限，e 是 q 阶的双线性对，P 为其加法群的一个生成元，H_1,H_2,H_3,H_4 均为 hash 函数。初始化时所有的节点均为系统节点，系统初始化步骤如下：

1)任意节点 i 随机选择 $\frac{T(T+1)}{2}$ 个有限域 Z_q 上的数。这组随机数唯一确定了一个 $T-1$ 次二元多项式 $f_i(x,y)=\sum_{j,k=0}^{T-1}a_{ijk}x^jy^k$，其中 $a_{ijk}=a_{ikj}$，于是有 $f_i(x,y)=f_i(y,x)$。

2)任意节点 i 发送一元多项式 $f_i(x,H_1(ID_j))$ 的系数给另一节点 j，并公开验证值 $Y_i=f_i(0,0)P$，$A_{ijk}=a_{ijk}P$；

3)节点 j 使用 A_{ijk} 验证收到的多项式系数的正确性；

4)节点 j 将获得的所有一元多项式相加，并秘密保存。

令 $F(x,y)=\sum f_i(x,y)$，当所有节点完成了全交换后，每个系统节点 j 都有了自己的秘密 $F(x,H_1(ID_j))$，而任何人都不知道系统的私钥 $s=F(0,0)$。系统的公钥 $P_{pub}=sP=\sum_{i=0}^{T-1}Y_i$。

如果节点 i 在初始化完成后请求加入系统节点集合，i 需要向现存的系统节点验证自己的身份。若系统节点 j 同意节点 i 的请求，则反馈 $F(H_1(ID_i),H_1(ID_j))$。节点 i 同样使用 A_{ijk} 验证反馈的有效性，在收集到 T 个有效的 $F(H_1(ID_i),H_1(ID_j))$ 后，即可插值得到一元 $T-1$ 次多项式 $F(H_1(ID_i),x)=F(x,H_1(ID_i))$。

3.2 组初始化

给定组 SG、初始门限值 t、基数为 T 的系统节点集合 SN 以及基数为 n 的候选解密节点集合 EN_{SG}，解密节点集合的初始化步骤如下：

1)与系统初始化过程类似，节点 $i\in SN$ 随机构造一个有限域 Z_q 上的 $t-1$ 次二元多项式 $g_i(x,y)=\sum_{j,k=0}^{t-1}b_{ijk}x^jy^k$，满足 $b_{ijk}=b_{ikj}$，$b_{i00}=L_i^0F(0,H_1(ID_i)H_1(ID_{SG}))$，其中 $L_i^0=\prod_{j\in SN/\{i\}}$

$\frac{-H_1(ID_j)}{H_1(ID_i)-H_1(ID_j)}$(即点 $H_1(ID_i)$在 0 处的拉格朗日插值系数)；

2)节点 $i\in SN$ 发送一元多项式 $g_i(x,H_1(ID_j))$的系数给节点 $j\in EN_{SG}$，并向 EN_{SG}中的所有节点公开验证值 $Y'_i=g_i(0,0)P$，$B_{ijk}=b_{ijk}P$；

3)节点 $j\in EN_{SG}$用 B_{ijk}验证收到的多项式系数的正确性；

4)节点 $j\in EN_{SG}$将获得的所有一元多项式相加得到：$s_j(x)=\sum_{k=0}^{t-1}c_{jk}x^k$。节点 j 秘密保存其秘密份额 $s_j(x)$并向 EN_{SG}中的所有节点公开 $y_j=e(s_j(0),P)$。

令 $G(x,y)=\sum_{i\in SN}g_i(x,y)$，显然有 $G(x,y)=G(y,x)$。当解密节点完成初始化后，每个解密节点 j 都有了自己的秘密份额 $s_j(x)=G(x,H_1(ID_j))$，而任何人都不知道组私钥 $G(0,0)$。

给定组 SG 及容错参数 f，管理节点集合被定义为 DHT 上负责对象$\{ID|ID=ID_{SG}+\frac{i}{3f+1},0\leqslant i\leqslant 3f+1\}$的节点的集合，即 $3f+1$ 个管理节点在 P2P 的 ID 空间[0,1)上均匀分布。管理节点的初始化仅需要组参数版本号 $ver=0$、门限值 t、解密节点集合 EN_{SG}及对应的验证值 y_j，$C_{jk}=\sum_{i=0}^{T-1}B_{ijk}$使用本文第 2 节中的写协议写入即可。因为初始化管理节点集合所需的信息均为公开信息，所以该过程可以由任一节点执行(例如 ID 最小的解密节点)，而任何解密节点均能通过读协议验证初始化的正确性。

3.3 加密与秘密重构

在基于身份的公钥密码系统下，加密过程由客户节点独立完成，无需公钥证书或密钥协商过程：给定明文 m 与组 SG，客户节点随机选择 $r\in Z_q$，计算 $k=e(rP_{pub},H_1(ID_{SG}))$，$U=rP$，$V=H_2(k)\oplus m$，$W=rH_3(U,V)$即得到密文 $C=(U,V,W)$。与之对应，已知密文 C 与组 SG，客户节点 c 秘密重构的步骤为：

1)客户节点 c 首先使用 ID_{SG}定位管理节点的位置，然后用第 2 节中的读协议获取组的公共信息，以定位该组现有的解密节点集合 EN_{SG}。接着向 EN_{SG}中的节点发送密文 $C=(U,V,W)$，请求解密分片。

2)验证客户节点 c 的身份与权限后，解密节点 $i\in EN_{SG}$，验证 $e(P,W)=e(U,H_3(U,V))$。若不相等，则拒绝提供解密服务；如果通过，则随机选择 T_i，计算解密分片 $k_i=e(U,s_i(0))$，同时给出 $\tilde{k}_i=e(U,T_i)$，$\tilde{y}_i=e(P,T_i)$，$\lambda_i=H_4(k_i,\tilde{k}_i,\tilde{y}_i)$，$L_i=T_i+\lambda_i s_i(0)$。将$(ver,k_i,\tilde{k}_i,\tilde{y}_i,\lambda_i,L_i)$反馈给客户节点 c，其中 ver 为节点 i 所知组参数的版本号。

3)客户节点 c 检查版本号与 1)中读取的值是否一致，必要时重新读取组公共信息。接着验证 $\lambda_i=H_4(k_i,\tilde{k}_i,\tilde{y}_i)$，$\frac{e(L_i,U)}{k_i^{\lambda_i}}=\tilde{k}_i$，$\frac{e(L_i,P)}{y_i^{\lambda_i}}=\tilde{y}_i$，丢弃过时的与无效的解密分片。

4)在收集到多于 t 个有效的解密分片 k_i 后，客户节点 c 即可插值算出 $k=e(U,G(0,0))$，从而得到 $m=V\oplus H_2(k)$。

3.4 增加解密节点

当 P2P 网络中的某节点 m 希望为某个组 SG 提供解密服务时，m 首先通过 ID_{SG}定位管理节点集合，接着读取该 Quorum 系统以定位该组现有的解密节点集合 EN_{SG}，然后向 EN_{SG}中的节点发出加入申请。

节点 $i\in EN_{SG}$若同意 m 的申请，则反馈 $s_i(H_1(ID_m))=G(H_1(ID_m),H_1(ID_i))$以及自己所知组参数的版本号 ver。节点 m 检查版本号后，使用 C_{jk}验证反馈值的有效性。一旦收集到了多于 t 个有效反馈，m 即可通过插值获得一元 $t-1$ 次多项式 $G(H_1(ID_m),x)=G(x,H_1(ID_m))=s_m(x)$。

最后，m 向 EN_{SG}中的所有节点公开验证值 $y_m=e(s_m(0),P)$，并将收集到的 $s_i(H_1(ID_m))$乘 P 后公开给管理节点，以证明新身份得到了多于 t 个解密节点的承认，同时将新的版本号：$ver+1$，EN_{SG}以及 y_m 的值写入。

3.5 移除解密节点与门限值变更

与增加解密节点不同，为了安全地移除一个或多个解密节点，剩余的解密节点必须变换其秘密份额，使被移除节点的秘密份额失效而同时保持组秘密不变[7]。于是移除解密节点的过程与门限值变更的过程完全一致。

变换解密节点的秘密份额，使新门限值 t'的过程与本文 3.2 节中的解密节点集合初始化过程基本一致，只是基数为 T 的系统节点集合由基数为 t 的解密节点集合取代，而且节点 i 选择的 $g_i(0,0)$中 $b_{i00}=L_i^0G(0,H_1(ID_i))$。这样，新的 $G(x,y)$与原始的二元多项式在原点上取值一致，而原始的秘密份额与新的秘密份额不存在其它任何关系，无法联合起来获取组密钥。

值得注意的是，上述过程无需系统节点参与，仅在组的解密节点之间进行。若某个解密节点在上述变换期间不在线，那么其秘密份额也将失效。当其重新上线后，需重新执行解密节点的加入协议。

4 分析与讨论

4.1 正确性分析

首先，因为 $G(0,0)=\sum_{i=0}^{T-1}b_{i00}=F(0,0)$，$H_1(ID_{SG})=sH_1(ID_{SG})$，由双线性变换的性质有 $e(U,G(0,0))=e(rP,sH_1(ID_{SG}))=e(sP,H_1(ID_{SG}))^r=e(P_{pub},H_1(ID_{SG}))^r=k$，即本方案能解密得到正确的明文。

其次，因为少于 t 个节点联合无法通过拉格朗日插值获得 $t-1$ 次多项式 $G(0,0)$的任何信息，而 t 个或多于 t 个解密节点即可顺利提供解密服务，所以本方案是门限秘密共享方案。

最后，由于在多次秘密共享中，解密节点 i 仅需维护一份秘密份额 $s_i(x)$，只要每次加密时的随机数 r 不同，那么即使某个秘密的明文被公开，敌人也无法获得关于其它秘密的任何信息，因此本方案是有效的多秘密共享方案。

4.2 安全性分析

我们假设在双线性对 e 的加法群上离散对数问题(DLP)与计算性 Diffie-Hellman 问题(CDHP)是困难的，而判定性 Diffie-Hellman 问题(DDHP)可在多项式时间内解决(利用椭圆曲线上的 Weil 对或 Tate 对可构造满足上述性质的双线性映射)。

已知 y_j 求解 $s_j(x)$为计算性 Diffie-Hellman 问题。除此之外，本方案中所有的验证信息与对应的秘密信息之间均为解离散对数关系，所以通过公开信息来求解秘密信息是困难的。

本方案以 Baek 等人基于身份的门限解密方案为算法基

础，在上述困难问题成立的前提下，可以证明解密算法在随机预言模型下同样是不可区分适应性选择密文安全的[4]。只要攻击者无法收集到某个密文的门限个解密分片，那么任何计算对应明文的方法都无法在多项式时间内完成。

本方案的秘密共享与重构过程无需秘密分发者，虽然系统初始化及组管理过程需要由某个节点来发起，并最终将结果写入管理节点集合，但由于所涉及的内容均为公开信息，不存在泄密问题，且任何节点均可验证其行为的正确性，因此管理员欺骗的攻击方式对本方案无效。

假设攻击者控制了某个解密节点 i 并尝试通过提供错误的解密分片 $k_i'=e(U,x)$，其中 $x\neq s_i(0)$，来干扰客户获得正确的明文。如果节点 i 使用 $s_i(0)$ 来计算 L_i，则 $\frac{e(L_i,U)}{k_i^{\lambda_i}}=\frac{e(T_i,U)e(s_i(0),U)^{\lambda_i}}{e(U,x)^{\lambda_i}}\neq\tilde{k}$，$k_i'$ 将无法通过客户节点的验证；若使用 $x=s_i(0)$ 来计算 L_i，则 $\frac{e(L_i,P)}{y_i^{\lambda_i}}=\frac{e(T_i,P)e(x,P)^{\lambda_i}}{e(s_i(0),P)^{\lambda_i}}\neq y_i$，$k_i'$ 依然将被丢弃，所以本方案可以有效地检测成员欺骗。

4.3 解密节点变更与门限值调整

在相同的节点失效率下，安全移除解密节点的能力使本方案能长时间安全地运行于节点搅动环境。相应地，允许动态增加解密节点，使系统能保持长期可用，同时更充分地利用网络资源。通过使用二元多项式，新增的解密节点无法利用现有节点的反馈值反推组密钥，从而消除了 random shuffling[7] 的必要，有效地减小了消息开销。

但是动态增加解密节点同时也引入了新的问题：敌人的攻击对象不再局限于现有参与者。敌人可以首先选择网络中相对容易攻陷的节点进行攻击，控制多个节点之后再操纵其申请加入解密节点集合。所以，当网络规模增大时，有必要增加系统的门限值，以保持系统的安全性。

本方案使用 Byzantine Quorum 算法确保了组参数版本号的全局唯一性。这样，即使某个节点在组参数改变时不在线，它也可以随后通过版本号判断自己信息的有效性。本方案中组的初始化，解密节点的增加、移除，门限值的变更，秘密重构都仅需门限个解密节点同时在线，达到了门限方案的最小值，适合节点上线率相对较低的 P2P 环境。显然，系统是否可用，取决于当前是否存在门限个在线的参与者。当节点不断离开，网络规模逐渐缩小时，应考虑减小门限值，以保持系统的可用性。

结束语 针对现有多秘密共享方案在 P2P 环境中的不足，本文提出了一种新的动态多秘密共享方案。首先，方案无需可信分发者和安全通讯信道，能有效对抗成员欺骗，适合无中心、自组织的网络环境。其次，针对节点上线率相对较低的问题，该方案采用 Byzantine Quorum 方式在 DHT 上管理组参数，使操作只需门限个参与者同时在线即可完成。再次，针对网络的节点和网络规模的变化问题，该方案允许动态地加入和移除参与者，动态地改变系统门限值，从而更加充分地利用网络资源，提供更高的安全性和可用性。最后，该方案使用基于身份的公钥密码系统与二元多项式，减小了消息开销，提高了系统的可伸缩性。因此，本文所提出的动态多秘密共享方案能够更好地满足 P2P 环境的应用需求。

参 考 文 献

[1] Zheng Y, Hardjono T, Seberry J. Reusing Shares in Secret Sharing Schemes[J]. The Computer Journal, 1994, 37(3): 199-205

[2] Hwang R-J, Chang C-C. An On-line Secret Sharing Scheme for Multi-secrets[J]. Computer Communications, 1998, 21(13): 1170-1176

[3] Harn L. Efficient sharing(broadcasting) of multiple secrets[J]. IEE Computers and Digital Techniques, 1995, 142(3): 237-240

[4] Baek J, Zheng Y. Identity-based Threshold Decryption[A]// Public Key Cryptography-PKC 2004[C]. Springer Berlin/Heidelberg, 2004: 262-276

[5] Daza V, Herranz J, Morillo P, et al. Cryptographic techniques for mobile ad-hoc networks[J]. Computer Networks: The International Journal of Computer and Telecommunications Networking, 2007, 51(18): 4938-4950

[6] 王锋，张建中. 基于 RSA 的可验证的动态多重秘密共享方案[J]. 计算机应用研究，2008，25(6)：1806-1811

[7] Herzberg A, Jarecki S, Krawczyk H, et al. Proactive Secret Sharing Or: How to Cope With Perpetual Leakage[A]// Proceedings of the 15th Annual International Cryptology Conference on Advances in Cryptology[C]. Santa Barbara, California, USA: Springer-Verlag, 1995: 339-352

[8] Bhagwan R, Savage S, Voelker G M. Understanding Availability [A]// Peer-to-Peer Systems II[C]. Heidelberg: Springer Berlin, 2003: 256-267

[9] 施荣华. 一种多重密钥共享认证方案[J]. 计算机学报，2003，26(5)：552-556

[10] Douceur J R. The Sybil Attack[A]// Proceedings of the First International Workshop on Peer-to-Peer Systems[C]. Cambridge, MA, USA: Springer-Verlag, 2002: 251-260

[11] Blake C, Rodrigues R. High Availability, Scalable Storage, Dynamic Peer Networks: Pick Two[A]// Proceedings of the 9th Workshop on Hot Topics in Operating Systems (HotOS-IX)[C]. Lihue, Hawaii, USA: USENIX Association Berkeley, CA, USA, 2003: 1-6

[12] Crescenzo G D, Arce G, Ge R. Threshold Cryptography in Mobile Ad Hoc Networks[A]// Security in Communication Networks[C]. Heidelberg: Springer Berlin, 2005, 91-104

[13] Saxena N, Tsudik G, Yi J H. Efficient Node Admission for Short-lived Mobile Ad Hoc Networks[A]// Proceedings of the 13th IEEE International Conference on Network Protocols(ICNP'05)[C]. Boston, Massachusetts, USA: IEEE Computer Society, 2005: 269-278

[14] Daza V, Morillo P, Rafols C. On Dynamic Distribution of Private Keys over MANETs[J]. Electronic Notes in Theoretical Computer Science(ENTCS), 2007, 171(1): 33-41

[15] Pietro R D, Mancini L V, Zanin G. Efficient and Adaptive Threshold Signatures for Ad hoc Networks[J]. Electronic Notes in Theoretical Computer Science(ENTCS), 2007, 171(1): 93-105

[16] Malkhi D, Reiter M. Byzantine quorum systems[J]. Distributed Computing, 1998, 11(4): 203-213

[17] Bao Y, Lu Z-D, Huang B-H, et al. Quorum-based Optimistic Concurrency Control in Replicated DHTs[A]// Proceedings of The First International Symposium on Information Engineering and Electronic Commerce(IEEC 2009)[C]. Ternopil, Ukraine: IEEE Computer Society, 2009: 40-45

(下转第 62 页)

辨率和测量精度。

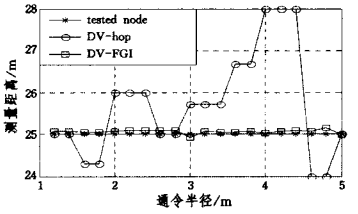

图 5　不同通讯半径下的节点间距离测量值

图 6 为待测节点处于不同位置时节点间距离测量的仿真结果，图 7 为待测节点处于不同位置时的距离测量误差，其中，“DV-FGI(REV)”曲线为边沿节点或近边沿节点用“代测”节点校正后的曲线。由图 6 与图 7 可见，DV-FGI 算法的测量结果明显优于 DV-hop 算法。

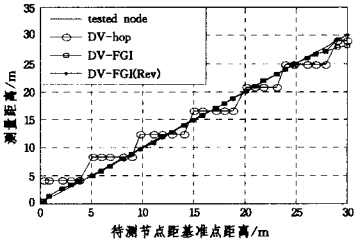

图 6　不同待测节点位置时的节点间距测量值

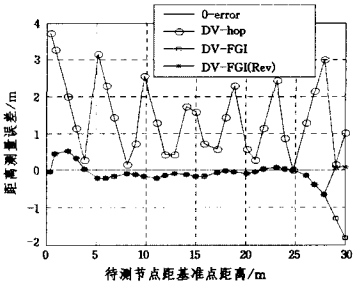

图 7　不同待测节点位置时的节点间距测量误差

结束语　理论分析和仿真结果表明，在最小跳数梯度场中，处于梯度层次中不同径向位置的节点具有的精细化梯度值不同，DV-FGI 算法将最小跳数梯度场中节点的精细化梯度值用于传感器网络节点间的距离测量，与 DV-hop 算法相比，在不增加传感器节点任何物理功能模块的前提下，能将节点距离测量的分辨率从节点通信半径 R 提高到节点间距 D_1，而且只在待测节点为网络边沿节点或近边沿节点时增加少许通信开销，在节点密集分布的无线传感器网络中，能极大地提高节点间距离测量和节点定位的精度，并提供了节点间相互区别的能力，用此方法得到的节点定位值可具有节点 ID 的部分功能。该算法具有低成本、低能耗、低通信开销、低处理开销和低时延的优点，在资源严格受限的无线传感器网络中无疑具有一定的应用前景。

本文针对节点近似均匀分布的最小跳数路由无线传感器网络，借助网络节点精细化梯度值的分布特征，将节点精细化梯度值与距离间的关系简化为分段线性关系，描述了一种基于精细化梯度的节点距离测量算法，分析并验证了该算法的有效性。围绕该算法，在以下两个方面还有待进一步深入研究：

(1)该算法用于节点非均匀分布网络的效果分析以及适用程度。

(2)如何根据网络的实际状况，在将节点精细化梯度值-距离关系的线性化过程中，选择更优的线性化方法，并引入自适应校正因子，以进一步提高算法在各类无线传感器网络中的测量效果。

参 考 文 献

[1] Niculescu D, Nath B. Ad hoc positioning system [C]// IEEE Globe COM101. San Antonio, Texas: IEEE Press, 2001, 5: 2926-2931

[2] Xu Guochang. GPS theory algorithms and applications[M]. Berlin: Springer-Verlag, 2003

[3] Girod L, Estrin D. Robust range estimation using acoustic and multimodal sensing[C]// Proceedings of IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS101). Maui. Hawaii, USA: IEEE Computer Society, 2001, 3: 1312-1320

[4] Dorigo M, Maniezzo V, Colomi A. Ant system optimization by a colony of cooperating agents[J]. IEEE Transactions on Systems, man, and Cybemetics, 1996, 26(1): 29-41

[5] Girod L, Byehovskiy V, Elson J, et al. Locating tiny sensors in time and space: a case study[C]// Werner B, ed. Proc. of the 2002 IEEE Int'l Conf. on Computer Design: VLSI in Computers and Processors. Freiburg: IEEE Computer Society, 2002: 214-219

[6] Bulusu N, Heidemann J, Estrin D. GPS-less low cost outdoor localization for very small devices[J]. IEEE Personal Communications Magazine, 2000, 7(5): 28-34

[7] Sun Y J, Sun Y G, Chen B J, et al. Research on the one vertex and two vertices connectivity reliability in the wireless sensor networks [J]. Chinese Journal of Sensors and Actuators, 2003, 4: 379-385

[8] Han K H, Ko Y B, Kim J H. A novel gradient approach for efficient data dissemination in wireless sensor networks[C]// IEEE VTC2004-Fall. Los Angeles: IEEE Press, 2004, 4: 2979-2983

[9] Heinzelman W R, Kulik J, Balakrishnan H. Adaptive protocols for information in wireless sensor networks[C]// Proceedings of the ACM Mobicom'99. Seattle: ACM Press, 1999: 174-185

[10] Nagpal R, Shrobe H, Bachrach J. Organizing a global coordinate system from local information on an Ad Hoc sensor network[C]// Proceedings of 2nd International workshop on Information Processing in Sensor Networks(IPSN'03). Palo Alto: IEEE Press, 2003: 333-348

[11] Zhu H S, Sun L M, Xu Y J, et al. Mechanism and analysis on fine-grain gradient sinking model in wireless sensor networks [J]. Journal of Software, 2007, 18(5): 1138-1151

(上接第 43 页)

[18] Martin J-P, Alvisi L, Dahlin M. Minimal Byzantine Storage[A]// Proceedings of the 16th International Conference on Distributed Computing[C]. Toulouse, France: Springer-Verlag, 2002: 311-325

[19] Awerbuch B, Scheideler C. Towards a Scalable and Robust DHT [A]// Proceedings of the Eighteenth Annual ACM Symposium on Parallelism in Algorithms and Architectures[C]. Cambridge, Massachusetts, USA: ACM Press, 2006: 318-327

[20] Dolev D, Hoch E N, Renesse R V. Self-stabilizing and Byzantine-tolerant Overlay Network[A]// Principles of Distributed Systems[C]. Heidelberg: Springer Berlin, 2007: 343-357