doi:10.11959/j.issn.1000-436x.2015037

无线传感器网络中匿名的聚合节点选举协议

付帅[1]，马建峰[1,2]，李洪涛[1]，姜奇[1]
（1. 西安电子科技大学 计算机学院，陕西 西安 710071；2. 通信信息控制和安全技术重点实验室，浙江 嘉兴 314033）

摘 要：提出一种分簇无线传感器网络中匿名的簇头选举协议。给出了匿名簇头选举的判定规则及成簇模式，并采用基于双线性对的匿名否决协议对选举结果进行验证以保证存在节点成功当选。设计了相应的匿名数据聚合方案，无需泄露节点身份信息即可完成聚合。分析及仿真结果表明，协议同时实现了簇头选举的匿名性、高效性及安全性，可有效抵抗窃听攻击、节点妥协攻击及合谋攻击等恶意行为。
关键词：无线传感器网络；分簇；数据聚合；匿名否决
中图分类号：TP393.08 **文献标识码**：A

Anonymous aggregator election protocol for wireless sensor networks

FU Shuai[1], MA Jian-feng[1,2], LI Hong-tao[1], JIANG Qi[1]
(1. School of Computer Science and Technology, Xidian University, Xi'an 710071, China;
2. Science and Technology on Communication Information Security Control Laboratory, Jiaxing 314033, China)

Abstract: An anonymous cluster head election protocol in clustered wireless sensor networks was proposed. The protocol detailed the decision rules and mode of cluster construction while an anonymous veto protocol based on bilinear pairings was adopted to verify election results, ensuring the successful election of cluster heads. A corresponding anonymous data aggregation scheme was designed, through which data aggregation can be accomplished without revealing the identities of aggregators. Extensive analysis and simulation results show that the proposed protocol achieves anonymity, energy efficiency and security of cluster heads election simultaneously and can resist eavesdropping attacks, node compromise attacks and collusion attacks effectively.
Key words: wireless sensor networks; cluster; data aggregation; anonymous veto

1 引言

无线传感器网络(WSN, wireless sensor networks)作为物联网的重要组成部分，在国防军事、环境监测、智能家居、医疗卫生、反恐抗灾等领域具有广阔的应用前景[1]。由于传感器节点能量有限且邻近节点采集的原始数据中存在冗余信息，基于分簇的数据收集方法和数据聚合技术[2,3]常应用在无线传感器网络中。在数据聚合过程中，节点需要对获取的数据进行处理，因此在信息安全尤其是数据的隐私保护方面面临极大的挑战。在基于分簇的无线传感器网络中，簇头负责对本簇内的数据进行收集、聚合，并与基站进行通信，所以簇头节点就成为物理破坏攻击或干扰攻击等的主要目标。只要捕获簇头节点，就可以阻止其从整个簇中接收数据。当基站处于离线状态时，安全问题尤为严重。

收稿日期：2013-10-22；**修回日期**：2013-12-11
基金项目：长江学者和创新团队发展计划基金资助项目(IRT1078)；国家自然基金委员会—广东联合基金重点基金资助项目(U1135002)；国家科技部重大专项基金资助项目(2011ZX03005-002)；国家自然科学基金资助项目(61272541，61202389)；中央高校基本科研业务基金资助项目(JY10000903001)；陕西省自然科学基础研究计划基金资助项目(2012JQ8043)
Foundation Items: The Program for Changjiang Scholars and Innovative Research Team in University (IRT1078); The Key Program of NSFC-Guangdong Union Foundation (U1135002); The Major National S&T Program (2011ZX03005-002); The National Natural Science Foundation of China (61272541,61202389); The Fundamental Research Funds for the Central Universities (JY10000903001); The Natural Science Basic Research Plan in Shannxi Province of China (2012JQ8043)

由于簇头必须临时存储数据，攻击者可以选择在特定的时间段内对簇头节点发起攻击，从而导致数据永久丢失。因此，保证簇头的安全成为保护数据隐私安全的重要一环。

目前，已有很多文献[4~7]对无线传感器网络中诸如认证、入侵探测及安全路由等常见的安全问题进行了深入研究，并对传感器网络簇头选举过程中的能耗均衡、选举标准、算法复杂度及簇的稳定性等问题进行了细致分析[8~10]，但几乎没有文献针对分簇无线传感器网络中安全可靠的簇头选举问题提出一个良好的解决方案。现有的基于分簇无线传感器网络的数据聚合协议通常假设网络节点是可信的，不考虑簇头节点身份公开所面临的安全隐患，因此在设计时很少考虑簇头节点失效。同时，由于多数协议对节点参与簇头选举的要求较高，所以难以保证无线传感器网络环境下数据聚合的安全要求。

针对上述问题，提出了一种新的匿名聚合节点选举协议。每个节点首先根据既定规则判定自己能否当选为簇头，然后执行匿名否决协议对选举结果进行验证，以确保至少有一个节点成功当选。同时，针对该匿名选举协议设计了相应的成簇模式和数据聚合方案，能够在不泄露簇头节点身份的同时有效实现数据聚合。安全分析及仿真实验表明，该协议可以在不影响网络寿命的前提下提高簇头节点的安全性，增强了抵抗主动攻击及妥协攻击等恶意行为的能力。

2　预备知识

2.1　理论基础

定义 1　双线性对：假设 G_1，G_2 为具有相同大素数阶 q（k bit，k 为系统安全参数）的群。G_1 为加法群，G_2 为乘法群。假设 P 为 G_1 的任意生成元，aP 表示 P 自加 $a \in Z_q^*$ 次。假定离散对数问题（DLP, discrete logarithm problem）在 G_1 和 G_2 中都是困难的。若映射 $\hat{e}: G_1 \times G_1 \to G_2$ 满足如下性质，则称为双线性对。

1) 双线性：对所有的 $P, Q \in G_1$, $a, b \in Z_q^*$, 满足 $\hat{e}(aP,bQ) = \hat{e}(P,Q)^{ab}$。该性质等价于对所有 $P, Q, R \in G_1$，满足 $\hat{e}(P+Q,R) = \hat{e}(P,R)\hat{e}(Q,R)$，$\hat{e}(P, Q+R) = \hat{e}(P,Q)\hat{e}(P,R)$。

2) 非退化性：若 P 为 G_1 的生成元，则 $\hat{e}(P,P)$ 是 G_2 的生成元，即满足 $\hat{e}(P,P) \neq 1$。

3) 可计算性：对任意 $P, Q \in G_1$，存在有效的算法计算 $\hat{e}(P,Q)$。

满足上述条件的映射可以利用有限域上基于超椭圆曲线的 Weil 对或 Tate 对来构造[11]。

定义 2　双线性 Diffie-Hellman (BDH) 参数生成器：同文献[12,13]，若一个以安全参数 k(k>0)为输入的随机算法 TG，在以 k 的多项式时间内运行，输出关于 2 个群 G_1 和 G_2，它们的共同素数阶 p，以及双线性对 $\hat{e}: G_1 \times G_1 \to G_2$ 的描述，则称该算法为一个 BDH 参数生成器。

定义 3　判定性双线性 Diffie-Hellman (DBDH) 问题：令 $< G_1, G_2, \hat{e} >$ 为上述参数生成器 TG 的输出，且 P 为群 G_1 的生成元。则 $< G_1, G_2, \hat{e} >$ 中的 DBDH 问题为：随机选取 3 个整数 $a,b,c \in Z_p^*$，以及随机元素 $W \in G_2$，给定 $< P, aP, bP, cP, W >$，判断等式 $\hat{e}(P,P)^{abc} = W$ 是否成立。

定义 4　计算性双线性 Diffie-Hellman(CBDH) 问题：假设群 G_1，G_2，生成元 p，以及双线对 $\hat{e}: G_1 \times G_1 \to G_2$ 为所定义的参数。$< G_1, G_2, \hat{e} >$ 中的 CBDH 问题定义为：给定<P,aP,bP,cP>(其中，随机元素 $a,b,c, \in Z_p^*$），计算 $\hat{e}(P,P)^{abc} \in G_2$。

2.2　网络模型

该选举协议基于分簇无线传感器网络结构，并做如下假设：1) 网络是数据驱动的，每个节点都会定期采集并向聚合节点发送数据；2) 节点间可通过合适的密钥协议建立配对密钥；3) 链路是对称的，所有节点都可通过无线信道和邻居节点进行通信；4) 每个节点拥有一个唯一的非零标识符(ID)。

因本文重点关注聚合节点的匿名性，且现已有诸多文献对建立配对密钥等问题进行了大量研究并取得系列成果，所以做出上述假设而不对其进行详细讨论。

2.3　攻击模型

假设攻击者可以发动以下攻击。

1) 窃听攻击：在协议执行过程中，攻击者完全控制参与者的通信。获取所有交互消息副本,但不干预协议的正常执行。攻击者通过对所有监听消息进行分析来获取相关信息。

2) 妥协攻击：敌手通过入侵合法节点将其变成非法节点来获取机密信息。

3) 合谋攻击：多个攻击者借助专用的通信信道

共享已拥有信息，从而合作地发起攻击。

4) 重放攻击：敌手可以通过重放以前的合法消息或假冒合法身份向聚合节点发送虚假消息来发起主动攻击。

3 协议设计

3.1 初始化

初始化阶段主要完成了节点部署前的初始资源配置工作，为节点间信息交换提供了通信信道。为保证消息发送者的匿名性，节点全部采用广播形式进行通信。在无线传感器网络中，广播通信可以通过洪泛等多种方式实现。洪泛路由模式虽然简单，但会导致网络数据的高度冗余，甚至广播风暴[14]等。因此，采用基于连通支配集(CDS, connected dominating set)的模式来实现广播通信。但是，求解MCDS 属于 NP 难问题[15]，在实际应用中常采用近似算法求解[16~18]。由于通过匿名方式选举聚合节点，采用文献[19]提出的基于最小生成树的 CDS 算法构建连通支配集，即通过建立一棵包含较多叶子节点的生成树寻找较小的 CDS。每次成簇后，所有簇都应用该算法构建连通支配集，并基于该 CDS 模式实现数据的匿名聚合。

3.2 匿名聚合节点选举

本文提出的匿名聚合节点选举协议旨在选举出合理簇头的同时保护当选节点的身份不被泄露。该选举过程可分为 2 个阶段。第一，簇头选举：每个节点按照既定规则判定自己是否当选为簇头；第二，选举结果验证：选举结束后运行匿名否决协议，以保证至少成功选举得到一个合法簇头。如果检测到没有节点成功当选，则需重新选举。本节将分别对这 2 个阶段的运行过程进行详细描述。

1) 簇头选举：在每轮选举开始时，节点首先应用式(1)计算本轮的随机阈值 T_{th}。其中，E^i_{res} 和 N^i_{e} 分别表示节点 i 的当前剩余能量和邻居节点数，E_0 表示节点的初始能量，N 为网络中的节点总数。α 和 β 分别表示节点剩余能量比率及其邻居节点密度的权值，其取值随网络规模及场景的变化而变化，$0\leqslant\alpha,\ \beta\leqslant 1$。节点 i 通过与邻居节点进行信息交互得到其邻居数 N^i_{e}。在开始阶段，网络中每个节点在其直接通信范围内广播 Hello 消息，其中包含节点自身的 ID 号、跳数和生存时间等。节点 i 收到周围所有一跳邻居节点广播的 Hello 消息后，就可确定自己的邻居节点数 N^i_{e}。显然，邻居节点密度大的区域内剩余能量值高的节点有更高的概率当选为簇头。

$$T_{\text{th}}=\alpha\frac{E^i_{\text{res}}}{E_0}+\beta\frac{N^i_{\text{e}}}{N} \tag{1}$$

此后，每个节点应用安全加密随机数产生器[20]生成一个 0 和 1 之间的随机数，并判断是否小于该随机阈值。若是，则该节点成功当选为簇头；否则，为普通节点。

2) 选举结果验证：为了在不暴露当选节点身份的前提下保证簇头选举的成功，采用了一种基于双线性对的匿名否决协议[21]对选举结果进行验证，以避免空簇头情况的出现。该协议能够有效抵御簇内恶意成员对表决结果的破坏，并提供可证明安全的簇头匿名性保护。由于分组丢失会对否决协议的运行产生不可忽略的影响，所以假定广播信道能够保证可靠递交。

设 $K=\{K_1, K_2, \cdots, K_n\}$表示参与者集合。$\hat{e}:G_1\times G_1\to G_2$ 表示定义在 q 阶群 G_1 和 G_2 上的双线性对映射。定义强密码学散列函数：$H:\{0,1\}^*\to G_1$，即任意长度的字符串可以通过 H 映射为 G_1 中的元素。在安全性分析中 H 被视为 Random Oracle。

本文采用 $NIZK\{r:w=g^r\}$表示关于离散对数 r 的非交互式零知识证明。其中 g 表示某素数阶群 G_0 的生成元，且在 G_0 中离散对数问题难解。假定匿名否决协议用到的群 G_1 和 G_2 都满足上述条件。基于双线性对的匿名否决协议在首次执行时包含会话密钥建立阶段和表决阶段 2 轮广播过程。

① 会话密钥建立阶段：每个成员节点 K_i 任取 $r_i\in_R Z_q$，计算 $w_i=r_iQ$ 和零知识证明 $NIZK\{r_i:w_i=r_iQ\}$，并广播给所有邻居节点。待所有成员广播完毕后，首先验证接收的数据是否正确，若出现错误则按 3)中的错误处理方式进行处理；否则，进行如下计算

$$E_i=\xi_iQ=\sum_{j=1}^{n}\operatorname{sgn}(i-j)r_jQ=\sum_{j=1}^{n}\operatorname{sgn}(i-j)w_j \tag{2}$$

其中，$\xi_i=\sum_{j=1}^{n}\operatorname{sgn}(i-j)r_j$。$\operatorname{sgn}\zeta$ 表示符号函数，当 ζ 为正、负和 0 时，函数值分别为 1、−1 和 0。

② 表决阶段：在表决开始前，所有成员节点首先根据预先设定的规则生成一个序列号 SN 作为本轮投票的唯一标识。对于每个成员节点 K_i，如果

K_i 已经当选为簇头，则令 $c_i = s_i \in_R Z_q (s_i \neq r_i)$；如果 K_i 为普通节点，则令 $c_i = r_i$ 。设 $\widetilde{M} = H(SN)$，向其他成员广播 $V_i = \hat{e}(\widetilde{M}, K_i)^{c_i}$ 和证明 $NIZK\{c_i : V_i = \hat{e}(\widetilde{M}, K_i)^{c_i}\}$。待所有成员广播完毕，每个成员对接收到的广播消息进行认证，确认其他成员公布数据的真实性，然后计算最终选举结果 $V = \prod_{i=1}^{n} V_i$。若 V=1，表示没有节点当选为簇头，需重新运行簇头选举协议。若 V≠1,则表示存在簇头节点，本轮选举成功完成。

3) 错误情况处理如下。①若存在成员节点 K_i 在会话密钥阶段发生错误，即未在规定时间内广播 w_i 或广播的零知识证明 $NIZK\{r_i : w_i = r_i Q\}$ 无法通过验证，则重新运行该准备阶段的协议。② 若某个成员节点 K_i 在表决阶段发生错误，即未在规定时间内广播 V_i 或广播的零知识证明 $NIZK\{c_i : V_i = \hat{e}(\widetilde{M}, K_i)^{c_i}\}$ 无效，则正常行为节点按如下方法对选举结果进行计算：假设 K_{fal} 表示异常节点集合，则所有正常行为节点 $K_i \in K - K_{\text{fal}}$ 计算 $R_i = \sum_{K_j \in K_{\text{fal}}} \text{sgn}(i-j) w_j$ 和 $V_i' = \hat{e}(\widetilde{M}, R_i)^{r_i}$ 并构造非交互式零知识证明 $NIZK\{r_i : w_i = r_i Q \wedge V_i' = \hat{e}(\widetilde{M}, R_i)^{r_i}\}$。然后，节点 K_i 将其广播给其他参与节点。选举结束后，选举结果 V 的计算方式修正为 $V = \prod_{K_i \in K - K_{\text{fal}}} V_i / V_i'$。

该匿名否决协议不仅确保了簇头的成功选举，而且保证了当选节点的匿名性。所有节点只能得知是否存在节点成功当选，但无法确定具体哪个节点是簇头。一旦某个节点妥协，攻击者也只能得知该妥协节点是否为簇头，不会得到关于其他节点具体身份或网络中的簇头个数等有价值的信息。

3.3 簇的构建

在一般的分簇无线传感器网络中，节点当选为簇头后要在邻居范围内广播声明消息以完成簇的构建，但该广播过程无疑会引起节点身份的暴露。因此，为了保证簇头节点的匿名性，设计了一种新的 2 轮成簇机制并做如下假设：1) 各节点设置时间为 t_1 和 t_2 的计时器分别应用在 2 轮中；2) 每轮的时长为 T；3) 各节点初始化一个随机的二进制变量 μ 以确定当选簇头节点在哪一轮发布组簇消息，μ 在 2 轮中取值为真的概率相等；4) 所有节点同步，均知晓第一轮的开始时间，T 及 t 的值。

为避免簇头节点因广播声明消息而被外部攻击者识别，要求其他接收消息节点(值不为真的已当选节点和普通节点) 以相同的加密和分发方式在邻居范围内发送虚拟消息。在第一轮，所有值为真的当选簇头节点将在 t_1 超时前于直接通信范围内发布组簇消息，声明自身为簇头。其他收到消息的节点将在邻居范围内发送虚拟消息。若在计时器超时后节点 i 仍未收到任何簇头声明消息且自身并未当选为簇头，也将在一跳范围内发送虚拟消息。第二轮和第一轮的操作过程相同，若节点 i 已当选为簇头且 μ 值在第二轮为真，则在 t_2 超时前于直接通信范围内发布簇头声明消息。否则，节点将只发送虚拟消息。表 1 给出了该成簇算法的伪代码。

表 1　匿名簇头选举成簇算法伪代码

匿名簇头选举成簇算法

```
1) 启动计时器 t1，时长为 T
2) 启动计时器 t2，时长为 T
3) 设定二进制随机值 μ=rand{0,1}
4) 设定簇头节点的 ID ： CHID=−1
5) while t1 未超时 do
6)   if (μ=1) and (CHID=−1)   //μ 在第一轮为真且已当选
7)   then 广播簇头声明消息
8)    CHID 值为发送者自身 ID
9)   else if
10)   接收簇头声明消息
11)    then 广播虚拟消息
12)     else  // t1 超时
13)       广播虚拟消息
14)     end if
15)  end if
16) end while
17)while t2 未超时 do
18)  if(μ=1) and (CHID=−1) then
19)   广播虚拟消息
20)   CHID 为节点自身 ID
21)  else if
22)   接收簇头声明消息 then
23)   广播虚拟消息
24)     else  // t2 超时
25)   广播虚拟消息
26)     end if
27)  end if
28)end while
```

本文采用的 2 轮成簇模式保证了成簇过程的完整性。若取消第二轮消息发送过程，节点 i 将会由于在第一轮中只发送或接收了虚拟消息而不能和邻居范围内的簇头节点相关联。同时，随机变量 μ 的引入进一步体现了 2 轮成簇模式的优越性。当选节点随机选择在哪一轮发布簇头声明消息，在一定程度上增大了敌手根据消息发布顺序猜测簇头节

点的难度。由于所有节点对消息的加密和分发方式都相同，外部攻击者只能观察到每个节点都发送了 2 个消息，因此无法利用声明消息的发送过程推测得出哪个节点是簇头。

3.4 数据聚合

在分簇结构的无线传感器网络中，簇头负责对本簇内的数据进行收集和聚合。通过将来自不同成员节点的数据进行压缩、特征提取等处理，聚合技术去除了冗余数据，降低了网络能耗。本节详细描述了如何在不暴露簇头节点身份的前提下，应用 3.1 节提出的基于连通支配集的方法实现簇内数据聚合。图 1 以求均值函数为例，分别给出了聚合过程的 4 个主要步骤：1) 非 CDS 节点向父节点发送数据，数据以（实际平均值，个数）的格式存储；2) 父节点在等待一段随机时间后将聚合值发送给邻居节点；3) 根节点计算最终聚合值，并广播给邻居 CDS 节点；4) CDS 节点将最终聚合结果广播给网络中的所有节点。

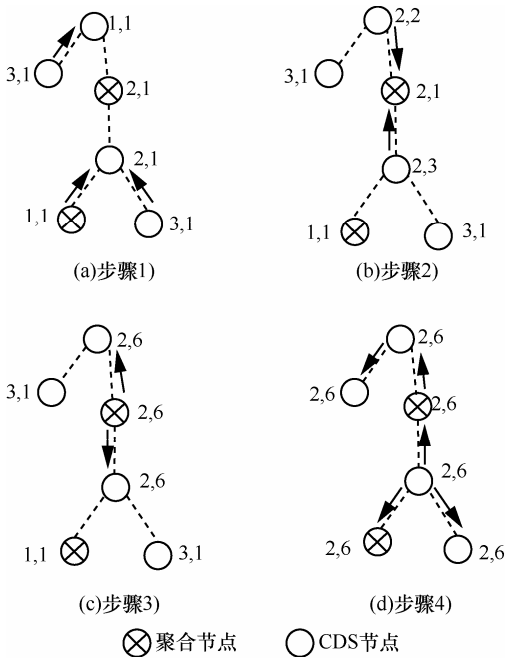


图 1 数据聚合示意

首先，每个非 CDS 节点在其各自分配的时隙内将采集的数据以单播通信的方式发送给与它直接相邻的 CDS 节点（父节点）。待所有非 CDS 节点的数据发送完毕后，CDS 节点先将接收到的数据进行聚合，然后在构造的生成树中应用改进的回波算法计算得到最终结果：CDS 节点在等待一段随机时间后将聚合值发送给其他的邻居节点，即由生成树的叶子节点开始通信，且通信波向生成树的根部传播。这一过程等价于回波算法的第二阶段。当一个节点接收到来自所有邻居节点的子聚合值，而没有其他的邻居节点需要转发时（生成树的根节点），该节点将计算总聚合值，并通过 CDS 节点将最终结果发送到网络中的所有节点。图 2 给出了相应的聚合算法流程。

该聚合过程中最后的广播阶段非常重要，保证了簇中每个节点都接收到相同的最终聚合结果。聚合完成后，每个节点都持有相同的数据，这些数据仅仅是聚合结果本身，并不包含任何有关节点身份的信息。所以，即使某些节点妥协，攻击者也不能通过节点持有的数据准确推断出簇中哪些节点是簇头。

4 协议分析

4.1 匿名簇头选举

1) 安全性

外部攻击：由于每个节点在每轮都发送了一个加密消息，所以虚拟消息的存在使外部攻击者很难通过观察节点的消息发送情况识别簇头节点。但是，敌手仍会试图通过发起合谋攻击综合已知网络信息提高其推测成功的概率。在 3.2 节的簇头选举过程中，节点通过计算自身剩余能量及其邻居节点密度确定本轮的随机阈值。由式(1)可以看出，邻居节点密度大的区域内剩余能量值高的节点有更高的概率当选为簇头。因此，外部攻击者可以通过观察网络拓扑结构对节点的邻居数目进行分析，进而推测出最有可能成为簇头的节点。仿真结果表明，为避免外部攻击者根据已知信息推测，可取 α=0.7，β=0.3，此时节点邻居数目的变化对其能否当选的影响最小且节点具有最高的能量效率。

妥协攻击：敌手可发起妥协攻击在物理上捕获节点，获取其敏感信息。攻击者可能会破坏节点，或修改其内部存储值及聚合函数。如果被捕获节点是簇头，则该节点内部的所有信息将会泄露。从 2 轮成簇过程可以看出，任意 2 个簇头节点间未有特定消息交互，所以妥协的簇头节点不会泄露有关其他簇头的任何信息。如果被捕获的是普通节点，敌手将只获取到与该节点相关联的簇头节点信息，而不会得到关于其他节点具体身份或网络中的簇头个数等信息。

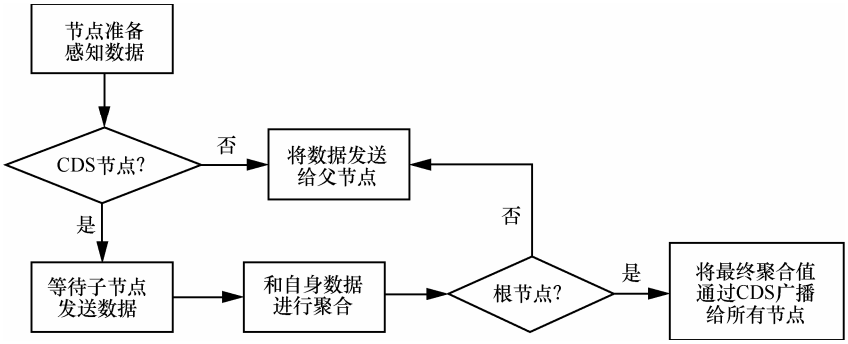


图 2　聚合算法流程

2) 消息复杂度

由于该匿名选举协议是消息驱动的，所以对协议的消息复杂度进行分析，假设 M 表示单个簇中的节点数。在簇头选举时，每个节点要在其直接通信范围内广播 Hello 数据分组，所以簇内每个节点都会收到 M 个消息；在选举结果验证过程中，每个节点分别在会话秘钥建立阶段和表决阶段广播一个零知识证明消息和表决消息；而在之后的 2 轮成簇过程中，每个节点每轮都发送一个消息(簇头声明消息或虚拟消息)，因此该阶段收发的消息总数为 M+2M+2M=5M，由于 M 为常数，所以成簇过程的消息复杂度为 $O(1)$。而在进行数据聚合时，由于必须首先接收并存储簇内所有成员节点发来的数据(M 个)，所以聚合过程的消息复杂度也为 $O(1)$。由此可知，该协议具有较低的消息复杂度。

4.2　匿名否决协议

1) 正确性

定理 1　若所有成员节点均遵守该匿名否决协议且没有节点当选为簇头，则选举结果 V=1；若有一个或一个以上的节点当选为簇头，则 $V\neq 1$ 的概率为 $1-q^{-1}$。

证明　若没有节点当选为簇头，则对任意 $1\leqslant i\leqslant n$，有 $c_i=r_i$。已知

$$V=\sum_{i=1}^{n}V_i=\sum_{i=1}^{n}\hat{e}(\widetilde{M},K_i)^{r_i} \tag{3}$$

将式(2)代入式(3)，得

$$V=\sum_{i=1}^{n}V_i=\sum_{i=1}^{n}\hat{e}(\widetilde{M},K_i)^{r_i}=\sum_{i=1}^{n}\hat{e}(\widetilde{M},\sum_{j=1}^{n}\mathrm{sgn}(i-j)r_jQ)^{r_i}$$

$$=\hat{e}(\widetilde{M},Q)^{\sum_{i=1}^{n}\sum_{j=1}^{n}\mathrm{sgn}(i-j)r_jr_i}$$

$$\sum_{i=1}^{n}\sum_{j=1}^{n}\mathrm{sgn}(i-j)r_jr_i$$

$$=\sum_{i=1}^{n}[\mathrm{sgn}(i-1)r_1r_i+\mathrm{sgn}(i-2)r_2r_i+\cdots+\mathrm{sgn}(i-n)r_nr_i]$$

$$=[-r_2r_1-r_3r_1-\cdots-r_nr_1]+[r_1r_2-r_3r_2-\cdots-r_nr_2]+\cdots+$$

$$[r_1r_{n-1}+r_2r_{n-1}+\cdots-r_nr_{n-1}]+[r_1r_n+r_2r_n+\cdots+r_{n-1}r_n]$$

$$=0$$

所以，$V=\hat{e}(H(SN),Q)^0=1$

若存在簇头节点，不妨将这些节点标记为 $U_1,U_2,\cdots,U_t(t\leqslant n)$。假定 $U_i(1\leqslant i\leqslant t)$ 在投票表决时任取 $c_i=s_i=s_i'+r_i$，则表决结果可以表示为

$$V=\hat{e}(\widetilde{M},Q)^{\sum_{i=1}^{n}\sum_{j=1}^{n}\mathrm{sgn}(i-j)r_ir_j}\hat{e}(\widetilde{M},Q)^{\sum_{i=1}^{t}\sum_{j=1}^{n}\mathrm{sgn}(i-j)s_i'r_j}$$

$$=\hat{e}(\widetilde{M},Q)^{\sum_{i=1}^{t}s_i'\xi_i} \tag{4}$$

由于 s_i' 和 ξ_i 是 Z_q 上相互独立的随机变量，因此，$\sum_{i=1}^{t}s_i'\xi_i$ 等于 0 的概率为 q^{-1}。所以，若有一个或一个以上的节点当选为簇头，最终表决结果 $V\neq 1$ 的概率为 $1-q^{-1}$。 因 q 足够大，则 $1-q^{-1}\approx 1$。所以，该匿名否决协议能够准确反应簇头的选举情况。

2) 匿名性

定理 2　在双线性 Diffie-Hellman 决策问题假设和 Random Oracle 模型下，如果除目标节点 U_i 外，簇中至少有一个节点是安全的，那么攻击者能够推测出 U_i 是否为簇头节点的概率是可忽略的。

证明　攻击者能够得到的有关节点 U_i 的信息包括 $r_iQ, K_i=\xi_iQ(\xi_i=\sum_{j=1}^{n}\mathrm{sgn}(i-j)r_j)$，$V_i$ 以及 U_i 广播的相关零知识证明，但这些证明不能为攻击者的猜测提供任何帮助。假定 $\widetilde{M}=H(SN)=\lambda Q$，在

Random Oracle 模型下，攻击者无法预知随机变量 λ 的值。除目标节点 U_i 外，记簇中存在的另一安全节点为 U_t，由于攻击者无法获得 r_t 的值,所以无法计算 ξ_i。若攻击者要判断 U_i 是否为簇头节点，则要面临解如下判定双线性 Diffie-Hellman 问题：给定 Q、r_iQ、ξ_iQ 和 λQ，判断 V_i 是否等于 $\hat{e}(Q,Q)^{r_i\xi_i\lambda}$。

3) 顽健性

定理 3 基于 G_1 上的离散对数问题假设和 Random Oracle 模型，若 U_i 为簇头，则即使攻击者可以控制除 U_i 外的其他所有节点，他能够使选举结果 V=1（否决结果被破坏）的概率是可忽略的。

证明 采用反证法。设 A 表示一个具有多项式运行时间的攻击算法，且 A 破坏否决结果的概率是不可忽略的。假定 A 可以控制除 U_i 外的其他所有节点且在 U_i 投否决票的情况下能够使表决结果 V=1。下面分析如何用 A 解 G_1 上的离散对数问题，即给定 λQ，求 λ 的值。

首先，运行 A 在会话密钥建立阶段的算法，任取 $r_i \in_R Z_q$ 并计算 $w_i = r_iQ$，得到 A 选择的$(n-1)$个 r_j 和 $w_j = r_jQ, j \neq i$。然后，运行 A 在表决阶段的算法得到$(n-1)$个输出 $V_j = \hat{e}(\widetilde{M}, K_j)^{c_j}$。若令 U_i 的输出 $V_i = \hat{e}(\widetilde{M}, \xi_i\lambda Q) = \hat{e}(\widetilde{M}, K_i)^{\lambda}$，即假定 $c_i = \lambda$，则必然满足 $V = V_i\Pi_{j\neq i}V_j = 1$，即 $c_i\xi_i + \sum_{j\neq i} c_j\xi_j = 0$。另外，通过 A 可以得到 $c_j(j \neq i)$，否则在 Random Oracle 模型下 A 能够提供有效证明 $NIZK\{c_j : V_j = \hat{e}(\widetilde{M}, K_j)^{c_j}\}$ 的概率是可忽略的。由于已知 $c_j(j \neq i)$ 和任意的 r_i，可进一步计算任意的 $\xi_i = \sum_j \mathrm{sgn}(i-j)r_j$，进而成功求得 λ 的值：$\lambda = c_i = \xi_i^{-1}\sum_{j\neq i} -c_j\xi_j$。

因此，即使一个内部攻击者控制了除簇头 U_i 外的其他所有节点，也不能对选举结果造成破坏。定理得证。

5 仿真实验

5.1 仿真环境

本文使用 OMNET++对提出的匿名选举协议进行仿真，实验的基本参数设置如表 2 所示。仿真实验主要从能量消耗和节点邻居数对随机阈值的影响 2 个角度对提出的匿名选举协议进行验证。初始化完成后节点的邻居数目分布情况如图 3 所示。

表 2 仿真参数

参数	参数值
节点数	100
网络规模	100 m×100 m
基站位置	95
数据分组长度/byte	500
节点初始能量/J	0.25
无线收发电路能耗/(nJ·bit^{-1})	50
自由空间模型放大器能耗/(pJ·bit^{-1}·m^{-2})	10
多路径衰减模型放大器能耗/(pJ·bit^{-1}·m^{-1})	0.001 3
融合单位长度数据能耗/(nJ·bit^{-1})	5
最大通信距离/m	15

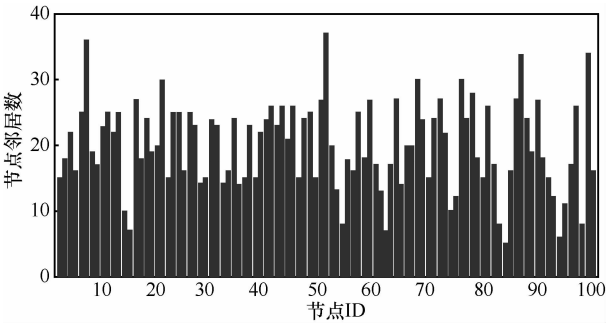


图 3 节点邻居数分布

5.2 仿真结果

1) 节点单轮能量消耗

图 4 给出了本文提出的簇头选举算法与基于权重的分簇算法 EECA 和 LEACH-C 在节点单轮能量消耗方面的比较结果。由于 LEACH-C 要向基站发送能量和位置信息，而 EECA 不仅与邻居节点交换信息，还要计算彼此之间的距离等，提出的簇头选举算法在运行前期（800 轮之前）节点的能量消耗是最优的。而在运行后期，所提算法因限于本地运算而未综合考虑影响能耗的其他因素，使节点平均剩余能量略小于 EECA 和 LEACH-C。从整体上看，该簇头选举算法并不会因为匿名性的要求而对节点寿命造成较大影响。图 4 是仿真过程中结果与 50 次仿真平均值最接近的一次实验原始数据，为进一步研究节点邻居数对当选概率的影响提供了数据依据。

2) 网络寿命

图 5 是 α 与 β 分别取不同值时节点生命周期的统计结果。由图可知，α 与 β 分别取值为（0.7，0.3）时，节点的生命周期较长。这是因为随剩余能量所占比率的增大，节点当选为簇头的概率也相应增

加，网络的整体能耗就越均衡。所以，80%节点死亡前，α 与 β 取值为（0.7，0.3）时节点生存周期是最长的。而当 80%的节点死亡后，取该值的节点生命周期缩短，因为此时节点剩余能量所占比率越大其 T_{th} 值越小，节点当选的概率也随之减小，导致重新选举簇头的频率增加，加速了节点的死亡。

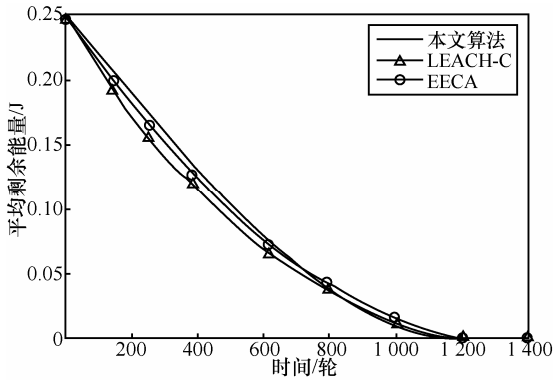


图 4　节点单轮能量消耗

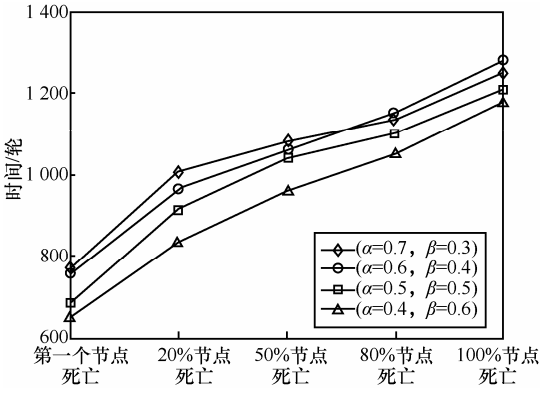


图 5　α、β 与网络寿命的关系

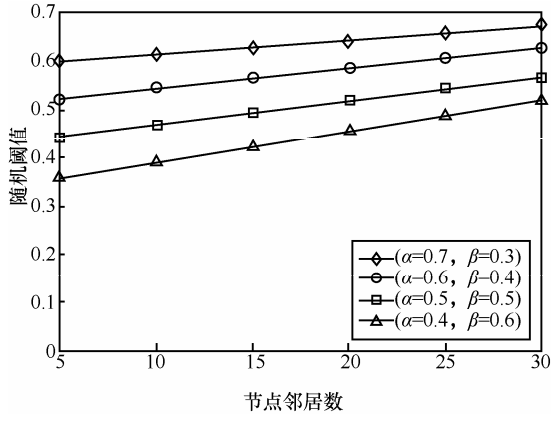


图 6　协议运行 210 轮时 α、β 与 T_{th} 值的关系

3) 节点邻居数及权值因子 α、β 对当选概率的影响

因节点当选概率与随机阈值的变化成正比，所以重点分析节点邻居数的变化对随机阈值的影响。图 6~图 10 给出了节点具有不同剩余能量时其值随 α、β 及邻居数变化的情况。由图可见，在节点邻居数和剩余能量都相同时，β 所占比值越大其值越小。同时，当节点具有相同邻居数时，剩余能量越少，α 与 β 取不同值时其值的差别也越小。由此判断，能量是影响随机阈值的决定性因素，即节点邻居数对当选概率的影响较小。

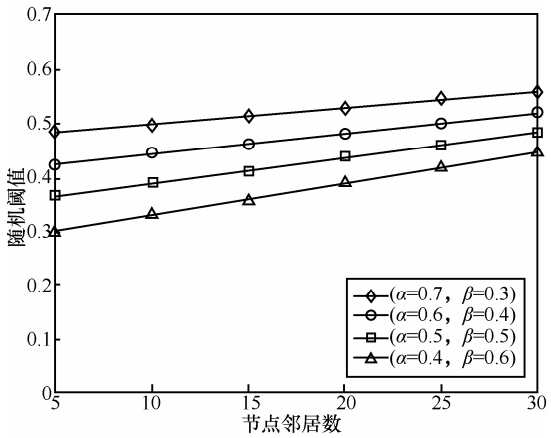


图 7　协议运行 320 轮时 α、β 与 T_{th} 值的关系

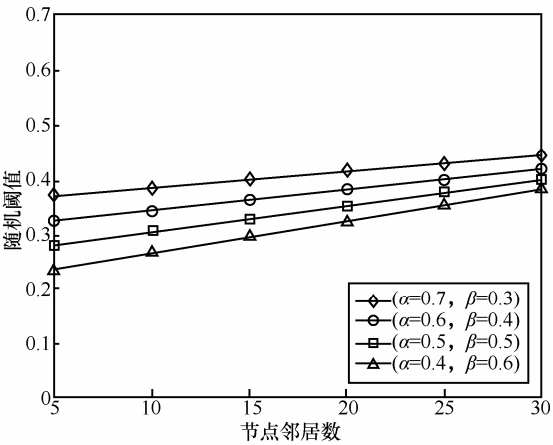


图 8　协议运行 430 轮时 α、β 与 T_{th} 值的关系

从图 6~图 9 可以看出，在节点剩余能量较多时，α 所占比值越大，曲线越平缓，节点的值受其邻居节点数变化的影响越不明显。但当协议运行 620 轮后，其值的变化与节点的邻居密度紧密相关。由图 10 可知，在节点的邻居数大于 15 后，其值随 α 的减小而增大。这是因为节点的剩余能量都很小时，邻居数成为首要考虑因素。此时，若敌手利用已掌握信息对簇头节点进行猜测，成功概率较大。但当节点剩余能量极少时，网络在实际应用中已失去意义，可以认为该网络生命周期结束。

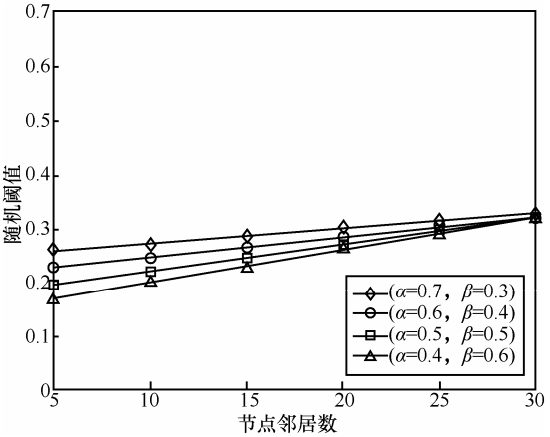


图 9 协议运行 620 轮时 α、β 与 T_{th} 值的关系

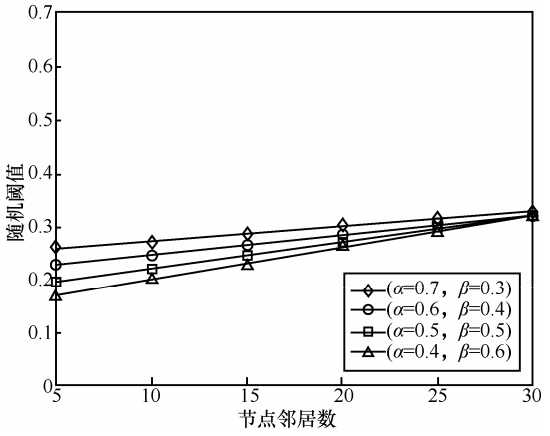


图 10 协议运行 820 轮时 α、β 与 T_{th} 值的关系

通过以上仿真实验可知，对于该匿名簇头选举协议，节点邻居数的变化对其当选概率的影响较小，且在权值因子 α=0.7、β=0.3 时抵抗外部攻击能力最强，此时敌手通过综合分析已知基本信息成功推测簇头节点是困难的。

5 结束语

本文提出了一种分簇无线传感器网络中的匿名簇头选举协议，并设计了相应的数据聚合方案。每个节点首先根据既定规则判定自身能否当选为簇头，然后共同执行匿名否决协议验证本簇中是否至少有一个节点成功当选。成簇阶段的 2 轮消息发布模式有效解决了因簇头发布声明消息而造成的身份泄露问题，可靠地保证了聚合数据的安全。分析和仿真实验表明，该协议可以有效抵御外部和内部攻击，具有较高的安全性。为了保证簇头节点的匿名性，所设计的簇头选举规则只考虑了剩余能量和邻居节点数 2 个因素。如何在保证簇头匿名的基础上进一步减少节点在协议运行过程中的能量消耗将是下一步的工作目标。

参考文献：

[1] YICK J, MUKHERJEE B, GHOSAL D. Wireless sensor networks survey[J]. Computer Networks, 2008, 52(12): 2292-2330.

[2] 郭江鸿，马建峰. 安全透明的无线传感器网络数据汇聚方案[J]. 通信学报，2012,33(10):51-59.
GUO J H, MA J F. Secure and transparent data aggregation for wireless sensor networks[J]. Journal on Communications, 2012, 33(10): 51-59.

[3] 杨军，张德运，张云翼等. 基于分簇的无线传感器网络数据汇聚传送协议[J].软件学报, 2010, 21(5): 1127-1137.
YANG J, ZHANG D Y, ZHANG Y Y，*et al*. Cluster-based data aggregation and transmission protocol for wireless sensor networks[J]. Journal of Software, 2010, 21(5):1127−1137.

[4] XUE K P, MA C S, HONG P L, *et al*. A temporal-credential-based mutual authentication and key agreement scheme for wireless sensor networks[J]. Journal of Network and Computer Applications, 2013, 36(1):316-323.

[5] WANG S S, YAN K Q, WANG S C, *et al*. An integrated intrusion detection system for cluster-based wireless sensor networks[J]. Expert Systems with Applications, 2011, 38(12):15234-15243.

[6] PANTAZIS N A, NIKOLIDAKIS S A, VERGADOS D D. Energy-efficient routing protocols in wireless sensor networks: a survey[J]. IEEE Communications Surveys &Tutorials, 2013, 15(2): 551-591.

[7] GUERMAZI A, ABID M. An efficient key distribution scheme to secure data-centric routing protocols in hierarchical wireless sensor networks[J]. Procedia Computer Science, 2011, 5: 208-215.

[8] ZHANG P F, XIAO G X, TAN H P. Clustering algorithms for maximizing the lifetime of wireless sensor networks with energy-harvesting sensors[J]. Computer Networks, 2013, 57(14): 2689-2704.

[9] KACIMI R, DHAOU R, BEYLOT A L. Load balancing techniques for lifetime maximizing in wireless sensor networks[J]. Ad Hoc Networks, 2013, 11(8): 2172-2186.

[10] DARABKH K A, ISMAIL S S, Al-SHURMAN M, *et al*. Performance evaluation of selective and adaptive heads clustering algorithms over wireless sensor networks[J]. Journal of Network and Computer Applications, 2012, 35(6): 2068-2080.

[11] DUTTA R, BARUA R, SARKAR P. Pairing-Based Cryptographic Protocols: A Survey[R]. Cryptology Eprint Archive, Report 2004/064, 2004.

[12] BONEH D, FRANKLIN M. Identity based encryption from the weil pairing[J]. SIAM Journal of Computing, 2003, 32(3): 586-615.

[13] 王圣宝. 基于双线性配对的加密方案及密钥协商协议[D]. 上海: 上海交通大学, 2008.
WANG S B. Research on Cryptosystems and Key Agreement Protocols from Bilinear Pairings[D]. Shanghai: Shanghai Jiaotong University, 2008.

[14] CHANG D, CHO K, CHOI N, *et al*. A probabilistic and opportunistic flooding algorithm in wireless sensor networks[J]. Computer Communications, 2012, 35(4): 500-506.

[15] GAREY M R, JOHNSON D S. Computers and Intractability: A Guide to the Theory of NP-Completeness[M]. New York: W H Freeman &Co, 1979.

[16] ZHENG C, SUN S X, HUANG T Y. Constructing distributed connected dominating sets in wireless ad hoc and sensor networks[J]. Journal of Software, 2011, 22(5):1053-1066.

[17] YIN B, SHI H C, SHANG Y. An efficient algorithm for constructing a connected dominating set in mobile ad hoc networks[J]. Journal of Parallel and Distributed Computing, 2011, 71(1): 27-39.

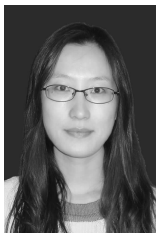
[18] ZOU F, WANG Y X, XU X H, *et al*. New approximations for minimum weighted dominating sets and minimum-weighted connected dominating sets on unit disk graphs[J]. Theoretical Computer Science, 2011, 412(3):198-208.

[19] 高文宇. 基于最小生成树的连通支配集求解算法[J]. 计算机应用, 2009, 29(6): 1490-1493.
GAO W Y. Novel connected dominating set algorithm based on minimum spanning tree[J]. Journal of Computer Applications, 2009, 29(6): 1490-1493.

[20] FRANCILLON A, CASTELLUECIA C. TinyRNG: a cryptographic random number generator for wireless sensors network nodes[A]. Proceedings of the 5th International Symposium on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks (WiOpt '07)[C]. Limassol, 2007.1-7.

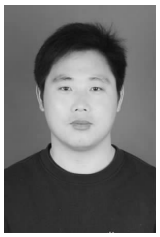
[21] 杨浩淼, 孙世新, 李洪伟. 双线性 Diffie-Hellman 问题研究[J]. 四川大学学报(工程科学版), 2006, 38(2): 137-140.
YANG H M, SUN S X, LI H W. Research on bilinear Diffie-Hellman problem[J]. Journal of Sichuan University (Engineering Science Edition), 2006, 38(2):137-140.

作者简介：

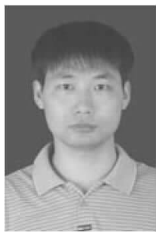


付帅（1986-），女，河北衡水人，西安电子科技大学博士生，主要研究方向为无线传感器网络、数据聚合、隐私保护等。

马建峰（1963-），男，陕西西安人，博士，西安电子科技大学教授、博士生导师，主要研究方向为计算机安全、密码学、移动与无线网络安全。



李洪涛（1985-），男，山东临沂人，西安电子科技大学博士生，主要研究方向为数据发布、隐私保护、无线网络安全等。



姜奇（1983-），男，安徽全椒人，博士，西安电子科技大学讲师，主要研究方向为安全协议分析、无线网络安全等。