一种改进的ZigBee路由优化算法

杜力凯 张 灵 陈云华
(广东工业大学计算机学院 广州 510000)

摘 要 ZigBee网络在运行的过程中,各个节点工作任务不均匀,从而会使能耗不均匀,导致整个网络过早产生分割死亡,因此提出一种均衡负载的路由优化算法。该算法首先通过发送定向RREQ来减少网络风暴,然后基于单个节点剩余能量、整个网络平均能量、多条路由路径能量代价和多个邻居节点能量这几个因素,通过选择动态路径来构建网络的动态路由,从而避免单条链路的压力。NS2仿真实验表明,改进的路由算法在节点死亡数、能耗和生存时间上都得到优化。

关键词 ZigBee,均衡负载,动态路由,定向RREQ
中图法分类号 TP393 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2015.5.030

Improved Optimization Algorithm for ZigBee Routing

DU Li-kai ZHANG Ling CHEN Yun-hua
(College of Computer, Guangdong University of Technology, Guangzhou 510000, China)

Abstract With the operation of network, ZigBee can cause the non-uniformity of node's energy consumption, leading to the problem of network' segmentation death. Therefore, a routing optimization algorithm balancing the network's energy consumption was presented in this paper. This algorithm firstly reduces the network storm by sending directed RREQ, and then based on residual energy of nodes, path forwarding energy consumption and the number of neighbor nodes, it constructs the network routing dynamically. It can avoid the pressure of single link at the same time. By means of the simulation experiment of NS2, the improved routing algorithm is more excellent than the classical routing algorithm of ZigBee in the number of node's death, energy consumption and survival time.

Keywords ZigBee, Load balancing, Dynamic routing, Directional RREQ

1 引言

ZigBee无线传感器网络低成本、低功耗、自组网、高安全性的特点,使得其在物联网领域有着广泛的应用[1]。由于ZigBee具有广泛的生活应用和发展空间,因此ZigBee网络成为很多专家的研究重点[2]。

ZigBee路由协议实现远距离传感器之间的通信,但是ZigBee网络中的传感器采取电池供电,而电池电量有限,因此对ZigBee路由协议优化的关键是充分合理利用网络中的能量,使其发挥最大作用[3]。很多研究学者提出了路由优化方案。李新春等提出了基于节点剩余能量和转发能耗来确定通信代价最小节点转发数据,平衡节点能耗,但其只是基于单个节点,无法从网络整体来均衡能耗[4]。钱志鸿等通过计算目的节点的父节点地址等方法,减少了RREQ,同时设置备用节点保护父亲节点[5];蒋培成等提出基于节点一段时间的能量消耗率、链路质量、跳数构建权值然后选择路由的方法[6],但频繁的能量侦听就要损耗大量能量,且以上两者都未考虑节点剩余能量,若存在剩余能量少但能量消耗速率低的节点,该节点会过早死亡,造成网络分割。刘湘雯等提出应用于Ad hoc网络的能量均衡算法,通过计算本地节点与邻居节点剩余能量的均方差作为衡量能量均衡的指标[7],能获得局部的能量均衡,但算法在约束最小能量路径时需地理信息系统的支持,而多数ZigBee网络并不支持地理信息系统。Xu等提出了一种基于节点分簇的改进策略,选择偶数深度的RN+节点作为簇头节点,奇数的RN+和RN-节点为簇内节点,簇与簇之间通过边界节点进行联系[8],但该方法加重了簇头节点负载,使其比簇内节点更易死亡,从而造成网络能量不均衡。徐艳等将节点的剩余能量划分范围,然后确定RREQ报文发送方向[9],能够减少网络风暴,但在路由时需要收集各个节点的剩余能量,易造成数据拥堵,削弱减轻网络风暴作用;同时因为网络中能量是动态不断减少的,通过节点固定的初始能量来设定阈值,无法确定节点能量在整个网络中的水平,也无法保证选取能耗相对较少的路径。

本文在总结前人研究成果时发现,现阶段都是从各种角度来设置参数从而选择能耗最优或平衡网络能量的路由路径,缺少能真正充分利用网络中能量的方法。由于一味选择

到稿日期:2014-06-16 返修日期:2014-08-19 本文受广东省科技计划国际合作项目(20108050400007),广州市科技计划项目:基于Zigbee的无线传感网络路由协议能效优化研究(科学研究专项)(2014J4100228)资助。
杜力凯(1990-),男,硕士生,主要研究方向为无线传感网,E-mail:carydurant@foxmail.com;张 灵(1968-),女,博士,教授,主要研究方向为无线传感网,E-mail:june4567@163.com;陈云华(1977-),女,博士,讲师,主要研究方向为无线传感网。

能耗最优路径，会存在该路径上出现节点死亡，网络被分割时，其他路径上节点能量仍很充足的现象。同时，现有学者在平衡网络能量时，都提出节点剩余能量的概念，但对其定义过于绝对化，应依据网络实际情况来确定其能量水平。因此，提出基于负载均衡的动态路由优化算法。

2 ZigBee 不足分析

经典的 ZigBee 网路由算法主要是结合 AODVjr 算法和 Cluster-Tree 算法[10]。

2.1 AODVjr 路由算法

AODVjr 算法是简化后的 AODV 算法，相比 AODV 降低了网络的能耗[11]，但在发起路由请求时，仍会盲目广播产生大量 RREQ 分组，造成网络风暴，浪费大量能量。同时，所选取的路由路径过于单一固定[12]，无法依照网络情况动态变化，不能充分利用网络资源，易导致网络分割[13]。

2.2 Cluster-Tree 路由算法

Cluster-Tree 路由算法是 ZigBee 路由网络中簇树节点间的路由算法，它根据判断树中父子节点关系进行路由选择。

假定 C_m 是父节点能拥有的最多子节点数目，其中最多有 R_m 个路由节点，L_m 为网络最大深度。在这种情况下，$Cskip(d)$为父节点分配给子节点的最多地址数，有：

$$R_m=1, Cskip(d)=1+C_m*(L_m-d-1) \tag{1}$$

$$R_m\neq 1, Cskip(d)=\frac{1+C_m-R_m-C_m*R_m}{1-R_m} \tag{2}$$

对于深度为 d、地址为 A_p 的父节点 k。分配给 k 的第 n 个无路由能力节点的网络地址 A_n 为[14]：

$$A_n=A_p+Cskip(d)*R_m+n, 1\leqslant n\leqslant C_m-R_m \tag{3}$$

分配给第 n 个有路由能力节点的网络地址 A_n 为：

$$A_n=A_p+1+Cskip(d)*(n-1), 1\leqslant n\leqslant R_m \tag{4}$$

对于没有路由能力的节点，只能将需要传输的数据交给其父节点进行转发。具有路由能力的节点传输数据报文时，先通过判定下一跳地址再进行转发。

设该节点地址为 A，D 为目的节点地址，d 为深度，若满足式(5)：

$$A<D<A+Cskip(d-1) \tag{5}$$

则对于下一跳的地址有：

$$N=\begin{cases} D, \text{目的节点是子节点} \\ A+1+\left\lfloor \dfrac{D-(A+1)}{Cskip(d)} \right\rfloor * Cskip(d) \end{cases} \tag{6}$$

如果不满足，则父节点就是它的下一跳。可以看出，在 Cluster-Tree 算法中，按照簇树的结构寻找路由，易导致选择结果单一、效率低、能耗高的路由路径[15]。

3 改进算法

3.1 改进算法思想

本文算法先对 AODVjr 的簇间的 RREQ 广播风暴进行了定向限制，对 AODVjr 和 Cluster-Tree 的路由分别进行改进，以达到优化目的。

3.1.1 限制广播风暴思想

在协调器进行广播组网时，可以按照组网的先后顺序对每个节点进行从小到大的分层，设定层数为 L。同时加入网络的划分为同一层数；后入网的为子层，L 递增；之前入网的为父层，L 递减。在路由发起的请求报文 RREQ 中标记发送节点的层数 L，根据 L 来进行选择转发可以避免转发大量重复 RREQ。算法具体思想如下：

1)当源节点发起路由请求时，直接广播 RREQ，然后进入 2)。

2)当其他节点收到 RREQ 分组时，若自己是目的节点，发送 RREP 进行回复，建立路由；否则，转向 3)。

3)若 RREQ 分组中 L 和该节点 L 相同，表示发送节点来自同一层，节点不转发 RREQ，直接进入 4)。

4)若 RREQ 分组中 L 比节点中的 L 小，直接转发 RREQ 分组给 L 较大的节点；否则，进入 5)。

5)若 RREQ 分组中的 L 比节点中 L 大，直接转发 RREQ 给 L 较小的节点；否则，进入 6)。

6)当为目的节点时，发送 RREP 回复建立路由；否则转向 2)。

在发起路由请求时，RREQ 一般会同时发给节点和其同一层的邻居节点，若该节点把请求发回给上一个发送 RREQ 的节点或同一层的邻居节点，都会造成大量能量浪费。确定 RREQ 的发送方向，能够减少大部分没用的 RREQ。

3.1.2 路由算法思想

网络组建运行后，收发数据等任务不同会导致网络中节点能量的不均匀，出现当有部分节点死亡，使得一个网络分割或者效率极低时，仍有部分节点是有很多能量的。它们的能量若能得到有效利用，势必会延长网络的寿命。

若出现网络平均能量很低，但某些节点能量相对整个网络平均能量较高，那么，在考虑网络能量路径的前提下，这些能量较高的节点应得到有效利用，尽可能多地分担网络中的任务，减轻其他节点的能耗压力，待其能量相对较少时让其休息。

若网络平均能量很高，但是网络中某些节点因过多任务而能耗严重，剩余能量相对网络处于较低水平，那么这些节点如果继续参与传输数据，将很快耗尽能量，以导致网络被分割。应让这些节点休息，保存能量，以保证网络能量平衡，在其能量相对网络较合适时继续参与工作。

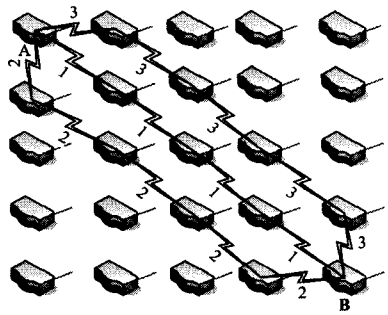

图 1 改进算法策略

在图 1 改进算法策略所示的网络中，节点 A 发送给节点 B 的数据会选择最短路径 1，但是长时间工作后，路径 1 上的节点会因能量耗尽死亡，导致网络被分割，影响了其他与路径 1 有交叉的路由路径，从而造成网络能耗急剧上升，大大降低了网络质量。如果在路径 1 能量相对偏低时选择不是最优的路径 2 和路径 3 分担一些任务，那么 A 到 B 的数据传输任务压力就得到了分担，路径 1 中的节点得到了能量保护，延长了

节点生存时间。等到其他路径能量相对较低，路径 1 能量相对较高时让它重新工作，这样网络能量可最大程度上得到利用，网络生存时间得到延长。因此将单条路由路径的能耗压力合理地分摊给整个网络，使网络中处在工作状态的路由路径的节点是网络中能量相对充足的节点，可以保护能量相对较少的节点，使网络的整体能量得到充分应用。这样可以避免节点能量过早耗尽死亡导致的网络分割的现象，保证了网络的各方面性能。

根据上面的分析，在 ZigBee 路由算法中，对采取 AODVjr 算法的部分采用多路径寻优算法进行改进，对 Cluster-Tree 算法部分采用规避等待算法进行改进，从而将改进算法思想融入整个 ZigBee 路由算法中。

3.2 AODVjr 多路径寻优路由算法

根据 3.1.2 节的路由算法思想，运行 AODVjr 算法的簇间，将节点和网络的平均剩余能量比作为重要的考虑因素，同时因为节点的邻居节点将是节点转发数据的对象，因此邻居节点也应在考虑的对象里面。设 E_n 为节点的剩余能量，E_{nb} 为节点的邻居节点平均能量，网络中所有节点的平均剩余能量为 E_{ave}，它反映了网络的能量水平。对于路由路径中的单个节点，其能量平衡函数有：

$$f=\alpha\frac{E_n}{E_{ave}}+\beta(\frac{E_{nb}}{E_{ave}})^2 \tag{7}$$

其中，α,β 是影响因子，$0<\beta<\alpha$，一条路径的平衡能量代价是

$$\sum_{i=1}^{n}\frac{1}{f_i} \tag{8}$$

其中，$f_1,f_2,f_3,\cdots,f_n$ 为路径中第 $1,2,3,\cdots,n$ 个节点的能量平衡函数，$\frac{1}{f_i}$ 为平衡能量代价。同时，可以得到一条路由路径的整体能量为 $\sum_{i=1}^{n}E_i$，其中，$E_1,E_2,E_3,\cdots,E_n$ 为路径中第 $1,2,3,\cdots,n$ 个节点的能量，取其倒数 $\frac{1}{E_i}$ 作为路径能耗代价，能量越低代价越大。对于路径中的能耗代价有：

$$\sum_{i=1}^{n}\frac{1}{E_i} \tag{9}$$

同时，设置节点的能量平衡比：

$$V=\frac{E_n}{E_{ave}} \tag{10}$$

节点能量安全平衡比为 ε，$0<\varepsilon<0.3$。V_{safe} 是节点能量相对网络的安全值，当 $V<V_{safe}$ 时，该节点能量相对于整个网络处于一个很低的状态，已造成能量的不均衡，应得到能量保护，其中 ε 在节点初始能量较多，数据转发耗能较少时，取小值；在节点初始能量较少，数据转发耗能较多时，取大值。那么所选取的路由路径在路径中满足 $V<V_{safe}$ 节点数目最少，同时满足下式：

$$\mathrm{MIN}(\mu\sum_{i=1}^{n}\frac{1}{f_i}+\lambda\sum_{i=1}^{n}\frac{1}{E_i}),\mu>\lambda>0 \tag{11}$$

其中，当节点初始能量较小，网络节点较少时，μ 相对 λ 差值取大；当节点初始能量较小，网络中较多时，μ 相对 λ 差值取小。因为 E_n、E_{nb}、E_{ave} 是随着网络运行动态变化的，所以节点的 V 值、路径平衡代价也是依据网络实际情况动态变化的，动态地选择最优路径保证了充分利用网络中的能量。AODVjr 动态多路径寻优路由算法的流程如图 2 所示。

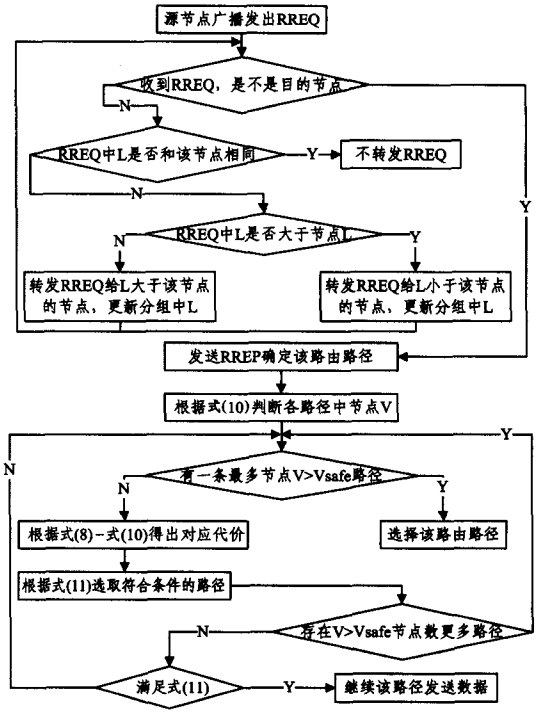

图 2 AODVjr 动态多路径寻优算法流程

3.3 Cluster-Tree 规避算法

在传统的 ZigBee 网络的树路由中，因为节点的路由能力有限，只通过父子关系进行路由选择，建立的路由不够优化，会造成较大的路由损耗。如果目的节点在邻居节点中，可以直接通过邻居表来确认下一条，因此，引入邻居表，也就是当目的节点在自己邻居表中时，不通过树路由，直接进行传输。

在此基础上，根据 3.1.2 节的算法路由思想，如果邻居表中没有目的节点，同时要转发的下一跳节点（可能是子节点或父节点）在这个时刻 V_1 有 $V_1<V_{safe}$ 时，说明该节点的能量已处于相对较低的水平，如果继续传输数据，其能量将很快耗尽，很可能导致整个子树因父节点或子节点死亡脱离网络。此时设置规避时间 t：

$$t=V_1t_0 \tag{12}$$

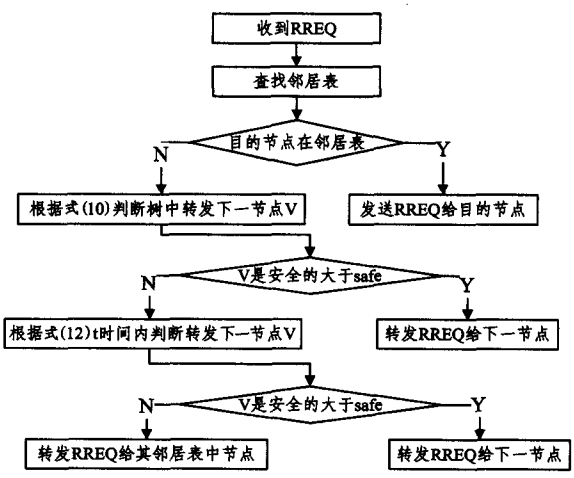

图 3 簇树规避算法流程

按照这种能耗速率，理论上 t 后节点能量耗尽，t_0 为网络已经运行的时间。让节点等待时间 t 后，若父节点（子节点）能量平衡比 $V_2>V_1$，说明节点相对能量得到改善，再通过其发送，使其得到休息。若 t 之后 $V_2<V_1$，把数据转发给邻居表

中节点，让邻居表中节点，通过其他能量相对较高的路径发送，使簇树生存时间得到延长。簇树规避算法的流程如图 3 所示。

4 仿真分析

为了有效评估本文路由算法性能，应用 NS2.33，分别对 ZigBee 的经典路由算法、有代表意义的文献[16]中改进算法、本文算法进行网络仿真比较。在网络覆盖面积为 200m×200m 的仿真场景中，设定 100 个随机位置的固定节点，设置 50 个 CBR 数据信息源，数据包长度为 80 个字节，网络中簇树参数 $L_m=3, C_m=R_m=4$，所有的节点起始能量为 5J，发送数据功率 0.6W，节点接收数据功率 0.3W，仿真时间 1200s，设置本文算法参数 $\varepsilon=0.2, \alpha=10, \beta=5, \mu=2, \lambda=1$，参考文献[16]中算法设定其因子 $\alpha=0.5, \beta=0.25, \gamma=0.1, \mu=10, n=2, K=0.2$。网络运行完后，对各项数据提取分析得到以下结果。网络场景如图 4 所示。

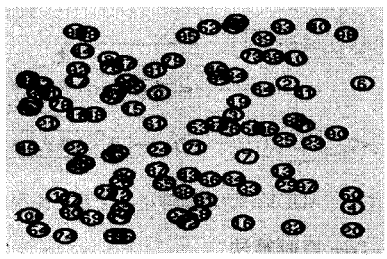

图 4 网络场景

从图 5 可以看出，随着网络中数据的传输，出现了能量耗尽的死亡节点，文献和本文算法都优于经典算法。文献算法减少了 RREQ，保护了能量偏低的节点，但是路由路径的单一导致一些节点过早死亡。本文算法在减少 RREQ 的前提下，动态选择能量相对较高的节点来分担那些能量相对较低节点的任务，使负载比较均衡地分担到了整个网络中，节点死亡时间得到推迟，网络生存时间得到最大化。

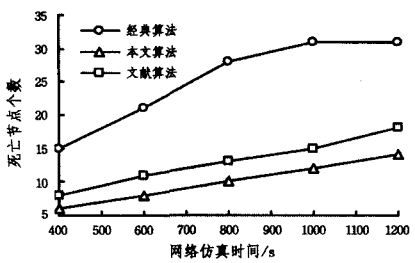

图 5 死亡节点数目随仿真时间变化

如图 6 所示，经典算法网络能量消耗在前 400s 快速增长，到后期网络死亡，能耗趋于平缓。文献算法减少了 RREQ 的泛洪，能量消耗较少，也趋于平缓。但从图 5 可知，本文算法死亡节点数目最少，有更多节点保持工作，网络效率较高，总体消耗能量总处于比较理想状态。

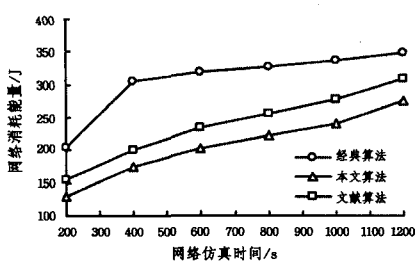

图 6 网络消耗能量随仿真时间变化

如图 7 所示，经典路由算法没有设置能量规避，前 400s 端到端的时延较小，但随着网络运行，网络中死亡节点增多，时延大大超过了其他两个算法。本文算法的路由是根据网络中的平均能量动态调整的，前期略大，因为均衡负载，死亡节点数目、能耗最少，网络的生存质量较高，后面大部分时间延迟最小。

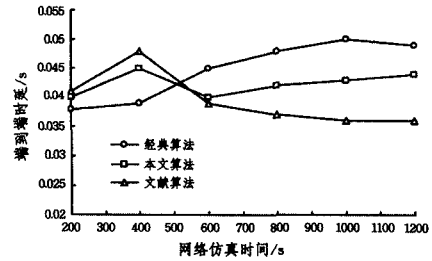

图 7 网络时延随仿真时间变化

结束语 本文从均衡 ZigBee 经典路由协议算法的能量消耗，充分利用网络中能量，延长网络生存时间的角度出发，提出了基于网络能量平衡的优化算法。本文算法在经典算法的基础上，限制了 RREQ 广播风暴，同时针对网络能耗均衡问题，对平衡代价、能耗代价综合寻优，动态选择合理路径，同时设置规避时间，最大程度上利用网络中能量。虽然会产生一些额外的控制和管理开销，但整体提升了网络效率，减少消耗。下一步将会在本文的基础上，研究改善算法时延，提升网络吞吐量并结合具体的硬件平台进行应用。

参 考 文 献

[1] Zahia B, Hafid H, Maimour, et al. Node disjoint mufti-path routing for ZigBee Cluster-Tree wireless sensor networks[C]// International Conference on Multimedia Computing and Systems Proceedings. 2011

[2] Medagliani P, Martalo M, Ferrari G. Clustered ZigBee networks with data fusion: Characterization and performance analysis [J]. Ad Hoc Networks, 2011, 7(9): 1083-1103

[3] Zhang Feng-hui, Zhou Hui-ling, Zhou Xiao-guang. A routing algorithm for ZigBee network based on dynamic energy consumption decisive path[C]// Proceedings of the 2009 International Conference on Computational Intelligence and Natural Computing(CINC 2009). Wuhan, China, 2009: 429-432

[4] 李新春，杨洪，李元诚. 基于通信代价的 ZigBee 网状网络路由选择算法[J]. 计算机工程与设计，2013，34(7)：2354-2357

[5] 钱志鸿，朱爽，王雪. 基于分簇机制的 ZigBee 混合路由能量优化算法[J]. 计算机学报，2013，36(3)：485-493

[6] 蒋培成，陈鸣，李兵. 一种优化 ZigBee 性能的综合加权路由算法[J]. 小微型计算机系统，2013，34(9)：2014-2017

[7] 刘湘雯，薛峰，李彦，等. 一种分布式无线传感器网络能量均衡路由算法[J]. 计算机科学，2010，37(1)：122-125

[8] Xu X, Yuan D, Wan J. An Enhanced Routing Protocol for ZigBee/IEEE 802.15.4 Wireless Networks[C]// The Second International Conference on Future Generation Communication and Networking(FGCN). Volume 1, 2008: 294-298

[9] 徐艳，王茜，武剑. ZigBee 路由协议优化仿真研究[J]. 计算机仿真，2013，30(60)：292-295

[10] Lee K K, Kim S H, Park H S. Cluster label based ZigBee routing protocol with high scalability[C]// Proceedings of the 2nd International Conference on Systems and Networks Communications (ICSNC 2007). Cap Esterel, France, 2007: 12

（下转第 168 页）

身份 ID_b 的选择有 $q_{H_1^B}$ 种可能，且至少有一个身份没执行 *Extract* 询问。因此 $\mathscr{A}$ 不对 ID_b 进行 *Extract* 询问的概率大于 $\frac{1}{q_{H_1^B}}$（进行 H_1^B 询问的次数）。此外，$\mathscr{A}$ 选择身份 ID_b 进行挑战的概率为 $\frac{1}{q_{H_1^B}}$。

在第二阶段，如果 $\mathscr{A}$ 对 $w=e_B(P_B,P_B)^{abc}$ 执行 H_2^B 询问，$\mathscr{C}$ 将失败。同理，$\mathscr{A}$ 不对 $w=e_B(P_B,P_B)^{abc}$ 执行 H_2^B 询问的概率大于 $\frac{1}{q_{H_2^B}}$（执行 H_2^B 询问的次数），因此，$\mathscr{C}$ 解决 BDH 问题的优势至少为 $\varepsilon\frac{1}{q_{H_1^B}q_{H_2^B}}$。在 $\mathscr{C}$ 的计算时间方面，每次 *Singcrypt* 询问需要 1 次双线性对运算，每次 *UnSingcrypt* 询问需要 4 次双线性对运算。

同理可证，管理域 B 中用户给管理域 A 中用户发送签密文仍然满足机密性。

证毕。

(2)不可伪造性

不可伪造性是指任何攻击者都不能伪造一个来自发送方的对消息的签密。本方案在适应性选择消息攻击下抗存在性伪造。如果存在一个敌手能够伪造一个我们的签名，则他也能够伪造下面的一个签名方案，该签名方案是 Hess 签名方案的一个变体。

签名：签名者随机选取 $r_1^{Alice}\in Z_{q_A}^*$，计算 $R_1^{Alice}=r_1^{Alice}P_A$ 和 $\sigma_{Alice}=r_1^{Alice}Pub_A+h_{Alice}S_{Alice}$，对消息 m_{Alice} 的签名为 $(R_1^{Alice},\sigma_{Alice})$。

验证：当收到签名 $(R_1^{Alice},\sigma_{Alice})$ 时，验证者计算 $h_{Alice}=H_3^A(c_{Alice},R_1^{Alice})$，并检验等式 $\sigma_{Alice}=r_1^{Alice}Pub_A+h_{Alice}S_{Alice}$ 是否成立。

由于 Hess 方案在适应性选择消息攻击下抗存在性伪造，因此我们的方案也同样抗存在性伪造。

(3)不可否认性

不可否认性是指任何人都不能够否认其发送过该签密消息。由于本方案满足签密的不可伪造性，只有本人 Alice 能够发送签名消息，因此只要 Bob 正确验证了 Alice 的签名，Alice 就不能否认曾经发过这个消息。

(4)公开验证性

只需要将 $\{c_{Alice},R_1^{Alice},R_2^{Alice},\sigma_{Alice}\}$ 给第三方验证者，验证 $e_A(P_A,\sigma_{Alice})=e_A(R_1^{Alice},Pub_A)e_A(Pub_A,Q_{Alice})^{H_3^A(c_{Alice},R_1^{Alice})}$ 是否成立，即可确认该消息是否是 Alice 签名的，该过程不需要 Bob 私钥的参与，也无需访问明文，即在保密性的基础上实现了公开验证性。

性能分析

几种跨信任域签密方案的计算性能分析如表 1 所列。从比较中可以看到，本文提出的方案与其他方案相比最多只有 1 次点乘运算的差别，但其他几种跨信任域的签密方案都对 PKG 作了如下假设：各 PKG 使用相同的参数，仅有主密钥和私钥不同。而本方案在与其他跨信任域签密方案计算开销相当的情况下，不但实现了跨信任域的签密，并且对各 PKG 参数不作限制。

表 1　几种跨信任域签密方案的性能分析

方案	加密、签名			解密、验证			PKG 参数限制
	对运算	点乘运算	指数运算	对运算	点乘运算	指数运算	
文献[6]	1	4	0	4	0	1	有
文献[7]	1	3	1	4	0	1	有
文献[9]	1	5	0	4	0	1	有
本方案	1	5	0	4	0	1	无

结束语　本文提出了一种跨信任域的签密方案以及密钥生成方法，该方案不受 PKG 参数一致的假设制约，各个信任域可以具有完全不同的系统参数。下一步的研究重点是将该方案应用于异构无线网络安全切换，预期取得良好效果。

参 考 文 献

[1] Adi S. Identity-based cryptosystems and signature schemes [C] // Advances in Crypto'84. Springer-Verlag, 1984: 47-53

[2] Dan B, Matt F. Identity based encryption from the Weil paring [C] // Advances in Crypto'01. Springer-Verlag, 2001: 213-229

[3] Zheng Yu-liang. Digital Signcryption or How to Achieve Cost (Signature & Encryption)<<Cost(Signature)+Cost(Encryption) [C] // Advances in Crypto'97. Springer-Verlag, 1997, 1294: 165-179

[4] Malone-Lee John. Identity-based signcryption [R]. Cryptology ePrint Achive, Report 2002/098

[5] Hess Florian. Efficient identity based signature scheme based on Parings[C] // Proceeding of the 9th Workshop on Selective Areas on Cryptography (SAC 2002). Springer-Verlag, 2002, 2595

[6] 路晓明，冯登国. 一种基于身份的多信任域网格认证模型[J]. 电子学报，2006，34(4)：577-581

[7] Li Fa-gen, HuYu-pu, Zhang Chuan-rong. An identity based signcryption scheme for multi-domain Ad Hoc Networks[C] // Proceeding of ACNS 2007. 2007, 4521: 373-384

[8] Sunder L, Prashant K. Multi-PKG based signcryption [R]. Cryptology ePrint Archive, Report 2008/050

[9] 张红旗，张文波，等. 网格环境下基于身份的跨域认证研究[J]. 计算机工程，2009，35(17)：160-162

[10] 朱重，吴国新. 分布式多信域管理技术研究综述[J]. 计算机科学，2011，38(4)：38-92

(上接第 156 页)

[11] 鲍凤卿. 基于 Ns2 的 ZigBee 网络节点接入的研究[J]. 信息技术，2008(11)：95-98

[12] 徐沛成，胡国荣. 改进的 ZigBee 网络路由算法[J]. 计算机工程与设计，2013，34(9)：3019-3023

[13] Lj X, Hong S H, Fang K L. WSNHA-GAHR: a greedy and A* heuristic routing algorithm for wireless sensor networks in home automation[J]. IETCommunieations, 2011, 21(5): 1797-1805

[14] Lee J S, Su Y W, Shen C C. A comparative study of wireless protocols: bluetooth, UWB, ZigBee, and WiFi[C] // Proc of the International Conference on Information Networking (IECON'07). Taiwan: IEEE, 2007: 46-50

[15] Bhatia A, Kaushik P. A cluster based minimum battery cost AODV routing using multipath route for ZigBee[C] // Proceedings of the 2008 16th International Conference on Networks(ICON 2008). New Delhi, India, 2008: 1-7

[16] 刘兆孟. ZigBee 无线传感网路由协议研究与设计[D]. 无锡：江南大学，2013