基于单向多汇聚节点的WSN分层路由协议

贺道德[1],武玲玲[2],邓晓衡[3],满君丰[4]
HE Daode[1], WU Lingling[2], DENG Xiaoheng[3], MAN Junfeng[4]

1.贵州工程应用技术学院 信息工程学院,贵州 毕节 551700
2.贵州工程应用技术学院 理学院,贵州 毕节 551700
3.中南大学 信息科学与工程学院,长沙 410083
4.湖南工业大学 计算机与通信学院,湖南 株洲 412007
1.School of Information Engineering, Guizhou University of Engineering Science, Bijie, Guizhou 551700, China
2.College of Science, Guizhou University of Engineering Science, Bijie, Guizhou 551700, China
3.College of Information Science and Engineering, Central South University, Changsha 410083, China
4.School of Computer and Communication, Hunan University of Technology, Zhuzhou, Hunan 412007, China

HE Daode, WU Lingling, DENG Xiaoheng, et al. Wireless sensor network hierarchical routing protocol based on one-way and multiple sink nodes. Computer Engineering and Applications, 2017, 53(12):105-109.

Abstract: Aimed at the weak point of the cluster head node of hierarchical wireless sensor network is easy to become a network bottleneck and restricted the network performance, this paper proposes an energy-efficient routing protocol. This paper constructs network by using multiple sink nodes and the RSSI (Received Signal Strength Indicator) to get the distance between the normal nodes and sink nodes, then divides the scope for each sink node by this distance, and uses the method of the sensor node and its sink node one-way communication to reduce the burden of cluster head node. The simulation results show the proposed routing protocol can effectively overcome the network bottleneck in cluster head, so as to reduce the energy consumption and improve the network lifetime, and this protocol has important value to that wireless sensor network applying large-scale data acquisition networks.
Key words: sink node; received signal strength indicator; network bottleneck; topology

摘 要:针对分层无线传感器网络的簇首节点容易成为网络瓶颈制约网络性能的不足,提出一种低能耗的路由协议。采用多汇聚(Sink)节点模式来构建网络,利用RSSI(接收信号强度指示)测出各传感器节点与各Sink节点之间的距离,并依据距离的远近为Sink节点划分作用域。通过传感器节点单向与所属Sink节点通信来降低簇首节点的负担。仿真实验结果表明提出的路由协议能有效克服簇首节点网络瓶颈问题,从而降低网络能耗,提高网络生存时间,对于无线传感器网络应用于大范围数据收集的网络具有重要的价值。
关键词:汇聚节点;接收信号强度指示;网络瓶颈;拓扑结构
文献标志码:A **中图分类号:**TP393 doi:10.3778/j.issn.1002-8331.1601-0242

无线传感器网络(WSN,Wireless Sensor Network)由一个网络观测区域和分布在该区域外围的汇聚(Sink)节点组成;在网络观测区域内布置大量传感器节点,它们通过无线通信技术组成一个采用多跳路由的自组织智能网络系统;它使用Sink节点来接收并处理传感器节点送来的数据[1-2]。WSN的拓扑结构主要有平面结构与分层结构两种;其中分层结构的WSN因具有通信量少而节能,适合分布式计算且扩展性好等特点而成为

基金项目:国家自然科学基金(No.61379058,No.61350011);贵州省科技厅、毕节市科技局、贵州工程应用技术学院联合基金(No.黔科合LH字[2014]7530号);中央高校基本科研业务费专项资金(No.XDJK2014C002);贵州省重点支持学科(No.黔学位合字ZDXK[2014]26号)。
作者简介:贺道德(1979—),男,副教授,主要研究方向:无线传感器网络技术,网格与Web Services,E-mail:hjabe@163.com。
收稿日期:2016-01-18 **修回日期:**2016-04-18 **文章编号:**1002-8331(2017)12-0105-05
CNKI**网络优先出版:**2016-06-17, http://www.cnki.net/kcms/detail/11.2127.TP.20160617.1550.022.html

目前研究的重点[3-4]。

分层结构的无线传感器网络的优劣主要看其路由算法是否能够降低网络能耗,提高网络生存时间[5]。分层的WSN路由算法将无线传感器网络划分为若干个簇[6],每个簇有一个簇首节点,由该簇首节点来收集本簇成员的数据并传递给Sink节点去处理;因此,簇首节点很容易出现网络瓶颈而制约网络性能[7-8]。此外,分层的WSN为减少通信量而在整个网络一般只设计一个Sink节点来处理网络数据,但这样做带来的负面作用是因单Sink导致簇首负载过重而影响网络性能。

为解决WSN因单一Sink节点带来影响网络稳定性、传输效率及网络生存时间等问题,国内外有很多学者提出在WSN中分配多个Sink节点来处理网络数据[9-11]。但大多数多Sink节点的无线传感器网络协议采用传感器节点多向传输数据给多个Sink节点而带来大量额外的通信量进而不适合分层无线传感器网络。

结合上述背景,本文针对分层WSN因簇首节点负载过重而影响网络性能的问题,在经典WSN分层路由协议的基础之上,提出基于单向多汇聚节点的分层路由协议OWMSRP(One-Way and Multi-Sink Routing Protocol),以达到提高网络性能的目的。

1 相关研究

目前,经典WSN分层路由协议主要以LEACH和PEGASIS协议为代表。在LEACH(Low-Energy Adaptive Cluster Hierarchy)协议的网络中,簇的层级数为1,即网络中的普通节点通过簇首节点传递数据到Sink节点只需2跳[12];此外该协议的簇首节点采用周期性随机轮换的方式选举产生。为减少因簇首节点频繁选举带来的开销,Lindsey S等人提出了PEGASIS(Power-Efficient Gathering in Sensor Information System)协议[13];它使用簇链形式将WSN构成一个多级分簇的网络,因此在该协议的网络中,簇的层级数大于1。

经典WSN分层路由协议的网络由簇或簇链组成,由簇首在普通传感器节点与Sink节点之间传递数据。因此簇首瓶颈问题严重制约着网络的性能。为解决此问题,国内外展开了大量研究。LEACH-C(LEACH-Centralized)协议[14]考虑簇首节点剩余能量和地理位置,由Sink节点来挑选簇首。文献[15]将网络分为不均匀的簇,在簇首选举时,让簇中能量最高的节点当选簇首节点,并由该簇首节点记录整个簇中节点能量的变化情况;在簇首更换时,局部选取能量最高的节点为簇首。文献[16]提出负载均衡感知的容错分簇算法,采用自适应离散粒子群优化的簇首选举机制来确保簇首负载均衡与能耗最低。

上述研究因不能从根本上解决簇首的负载问题,从而不能打破分层无线传感器网络在簇首处的瓶颈。具体分析如下:

(1)在LEACH协议中,由于簇首选举的随机性而使簇首并不是性能最优的节点;并且,因簇首选举的频繁性而给网络带来大量通信量,进而降低网络的生存时间;另外,LEACH需要各簇首的射频功率足够大以保证离Sink再远也能与其通信,这将导致离Sink越远,簇首的功耗也越大。

(2)在PEGASIS协议中,采用多级分簇的方法构建网络使得簇首节点不仅负责簇内信息的收集和处理,还需负责簇间数据转发,而且离Sink节点越近的簇首节点其负载越重。

(3)在LEACH-C协议中,Sink节点从整个网络中挑选出合适数量和最优地理位置的簇首节点集合是一个NP问题。

(4)在文献[15]提出的算法中,簇首更换局限在某一簇内,这并不能保证新更换上的簇首节点相对于整个网络而言是性能最优的节点。

(5)在文献[16]提出的算法中,簇首采用多跳通信的方式与Sink进行通信,这与PEGASIS协议一样,不能解决因到Sink节点的距离不同而导致负载不均衡的问题。

(6)上述协议都是从提高簇首节点性能的目的出发来构建网络,并没有考虑如何降低簇首节点的负载来提高网络性能。

2 OWMSRP协议

从第1章对经典WSN分层路由协议及其改进协议的分析来看,分层网络的不足之处主要和簇首节点有关,因为簇首是普通节点与Sink节点之间的桥梁,起着中间转发的功能,从而在簇首节点处很容易出现瓶颈而降低网络的各项性能指标。鉴于此,从降低网络能耗,提高网络生存周期出发,本文以经典WSN分层路由协议LEACH为基础,设计基于单向多汇聚节点的路由协议OSMSRP;采用在无线传感网的观测区域外围分布多个Sink节点,各传感器节点在其所属Sink的作用域范围内,按LEACH的簇首选举与建簇算法构建层级数为1的簇;然后,传感器节点通过其簇首单向与其所属Sink进行通信以减轻簇首的负担,从而解决网络在簇首处的瓶颈问题。

2.1 OWMSRP网络初始架构

OWMSRP网络采取在无线传感器节点观测区外围均匀分布一定数量的Sink节点来初始构建网络。具体如图1所示。

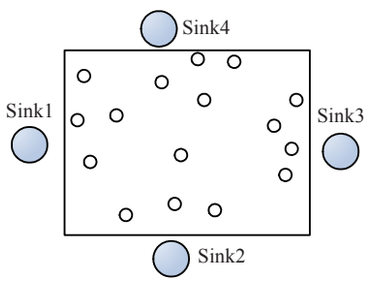

图1 OWMSRP网络初始架构

图1是一网络观测区为矩形的无线传感器网络拓扑图，无线传感器节点随机分布在该区域之内，在该矩形区域的外围四边上分别分配一个Sink节点，以构成基于多Sink节点的无线传感器网络结构。在实际应用环境中，本文提出的协议所支撑的拓扑结构可以是任意观测区域，只要在观测区域外围均匀分布一定数量的Sink节点即满足本文所提出的网络初始架构要求。另外，Sink节点的数量可根据网络的规模来确定。

2.2　确定Sink节点的作用域

在OWMSRP网络初始架构好后，采用RSSI（接收信号强度指示）方法测出各传感器节点与各Sink节点之间的距离，并依据该距离的远近确定各Sink节点的作用域。为实现该任务，Sink节点需维护一个子节点集ChildNodeSet，而普通传感器节点则需缓存该节点的所属Sink节点的相关信息到所属Sink节点域FatherSink，具体结构如表1和表2所示。

表1　Sink节点的子节点集ChildNodeSet

名称	定义
NodeId	该Sink的子节点的节点标识
NodeEN	该子节点的剩余能量值
IsClusterHD	确定该子节点是否为簇首节点标志，该值为1表示节点为簇首，为0为非簇首

表2　传感器节点的所属Sink节点域FatherSink

名称	定义
SinkId	该节点的所属Sink节点标识
Distance	该节点到所属Sink的距离值

各Sink节点发射信号给网络观测区，网络观测区中的传感器节点记录到各Sink节点的RSSI值，并根据该值计算出它们之间的距离，然后选择距离最近的Sink节点为所属Sink节点，记录该Sink节点的相关信息到所属Sink节点域，并单向将自己的相关信息传递给所属Sink节点；而该Sink节点则存储其子节点的相关信息于子节点集，最终确定它的作用域。具体算法如下所示：

（1）各Sink节点在网络观测区内发送作用域划分广播SHello消息；

（2）设置计时器的值为t；

（3）i.FatherSink.SinkId=null；i.FatherSink.Distance=infinite；

/*初始化任意传感器节点i的所属Sink节点域，infinite为无穷大*/

（4）while（t）｛/*在时间t内执行确定任意节点i的所属Sink节点的操作*/

（5）传感器节点i收到任意Sink节点A的SHello消息；

（6）依据i与A之间的RSSI值测出它们之间的距离A.Distance；

（7）if（A.Distance<i.FatherSink.Distance）

（8）｛/*到Sink节点A的距离比到当前所记录的所属Sink节点域的距离短*/

（9）i.FatherSink.SinkId=A.SinkId；i.FatherSink.Distance=A.Distance；

（10）/*节点i的所属Sink域的内容赋值为节点A的相关信息，即节点A为i的当前所属Sink*/｝｝

（11）｛/*任意子节点i在确定其所属Sink节点后，加入由其所属Sink构建的网络区域的过程*/

（12）SinkNode K=new SinkNode（）；

（13）K.SinkId=i.FatherSink.SinkId；/*节点K用于记载i节点的所属Sink的相关信息*/

（14）传感器节点i单向传递加入消息RegSink给Sink节点K；

（15）ChildNode x=new ChildNode（）；/*x节点用于记录子节点i的相关信息*/

（16）x.NodeId=i.NodeId；x.NodeEN=i.NodeEN；

（17）x.IsClusterHD=0；/*在确定Sink节点的作用域时，所有子节点的簇首标志为0，即初始为非簇首*/

（18）K.addChild（x） to ChildNodeSet；/*K将i的信息写入其子节点集*/｝

从上述算法可知，普通传感器节点通过RSSI测距以确定其所属Sink节点，然后Sink节点记录其子节点的相关信息，最终确定Sink节点的作用域。确定好作用域后的OWMSRP网络拓扑图如图2所示。

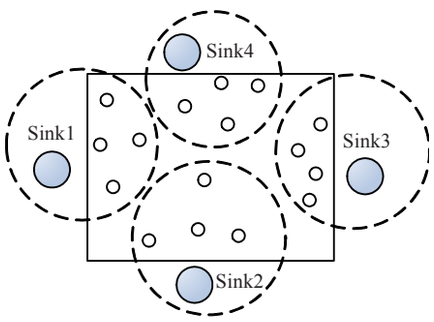

图2　确定Sink作用域后的网络拓扑图

在图2中，各无线传感器节点依据到各Sink节点的距离值来归属于某个Sink节点，图中用虚线圈圈出了各Sink节点的作用域。相比于传统多Sink节点的无线传感器网络，在多Sink节点的情况下，使用RSSI测距以确定Sink节点的作用域，使得普通传感节点只与所属Sink节点通信，从而降低网络通信量；另外，无线传感节点的发射功率有限，因此，使用距离来确定Sink节点作用域范围还能克服网络对发射大功率的要求。

2.3　OWMSRP网络簇首的选举与簇的建立

在确定好各Sink节点的作用域后，OWMSRP网络中的Sink节点应在其作用域范围之内选举簇首节点并构建簇。

在簇首节点选举时，Sink节点根据其子节点集记录的各子节点的NodeEN（子节点的剩余能量值）来计算子节点能量平均值，并将该能量平均值在网络观测区中广播；若某传感器节点为其子节点且其能量高于该平均值，则将其确定为候选簇首节点（即将节点的候选簇首标志IsCandidateClusterHD设为1），所有的候选簇首节点形成候选簇首节点集CandClusHeadSet。然后在候选簇首节点集内，采用LEACH协议的簇首选举方法来选

举簇首节点和构成簇。最后,簇首节点向所属Sink节点宣告身份,而Sink节点则在子节点集中将该节点的IsClusterHD值(簇首标志)设为1。建簇算法具体如下所示:

```
(1)AveNodeEN=0;/*平均能量值赋初值为0*/
(2)for(j=0;j<A.ChildNodeSet.Length;j++)
(3){/*遍历Sink节点A的子节点集,求其平均能量值*/
(4)AveNodeEN=AveNodeEN+A.ChildNodeSet[j].NodeEN;}
(5)AveNodeEN=AveNodeEN/A.ChildNodeSet.Length;
(6)A.aveEnergy(A.SinkId,AveNodeEN) to Network Area;/*A向网络观测区广播其子节点平均能量值*/
(7)i.IsCandidateClusterHD=0;/*任意传感器节点i初始将候选簇首标志设为0*/
(8)i.IsClusterHD=0;/*任意传感器节点i的簇首标志初始设为0*/
(9)if(i.SinkId==A.SinkId&&i.NodeEN>AveNodeEN)
(10){/*若节点为A的子节点且剩余能量高于平均能量值,将其加入候选簇首节点集*/
(11)IsCandidateClusterHD=1;
(12)添加节点i到候选簇首节点集CandClusHeadSet;}
(13)leachClusterHD(CandClusHeadSet,A.SinkId);
/*在候选簇首节点集内调用LEACH协议的簇首选举算法选举簇首*/
(14)leachCluster(A.SinkId);/*调用LEACH协议的建簇算法在Sink节点A的作用域内建簇*/
(15)if(i.IsClusterHD==1){/*若某传感器节点i为簇首,向其所属Sink节点宣告簇首身份*/
(16)SinkNode A=new SinkNode();
(17)A.SinkId=i.FatherSink.SinkId;/*节点A用于记载i节点的所属Sink的相关信息*/
(18)i.myIsClusterHD(i.nodeId) to A;/*发myIsClusterHD消息给所属Sink节点A,告知其为簇首*/
(19)for(j=0;j<A.ChildNodeSet.Length;j++)/*遍历Sink节点A的子节点集,将子节点i的簇首标识设为1*/
(20)if(A.ChildNodeSet[j].NodeId==i.nodeId)
(21){A.ChildNodeSet[j].IsClusterHD=1;break;}}
```

在上述算法中,为选择最优的节点为簇首,算法首先由各Sink确定其作用域的能量下限,然后根据这个下限将符合条件的节点选为候选簇首;为继承LEACH协议在小范围内运行具有优秀性能的特征,本算法在Sink作用域范围内调用LEACH协议的簇首选择和建簇算法来构建簇。在簇建立工作完成后的OWMSRP网络拓扑图如图3所示。

在图3中,在无线传感器节点观测区内形成多个簇,并且每个簇因处于不同的Sink节点的作用域内而分布在网络观测区的不同区域。当传感器节点需汇聚数据时,只需通过簇首节点单向将数据传给其所属Sink节点;因此传感器节点汇聚数据到Sink只需2跳即可完成。

2.4　OWMSRP协议与经典WSN分层路由协议比较

OWMSRP协议采用单向多Sink节点技术,能有效地解决簇首节点处的网络瓶颈问题,相比于经典WSN分层路由协议及其改进协议,其优点具体如下:

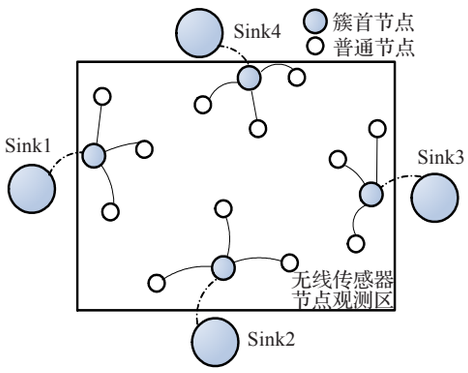

图3　OWMSRP网络拓扑结构图

(1)在簇首节点选举过程中,OWMSRP网络选举能量值超过平均能量值的节点为候选簇首节点,再从候选簇首节点集中采用随机轮换的方法选举簇首,这将保证簇首节点有充足的能量来完成其转发数据的任务,从而避免了因簇首能量不足而降低网络性能的情况出现;另外,也避免了簇首选择的NP问题。

(2)由于Sink节点均匀分布在网络观测区的外围,并且采用RSSI测距来划分其作用域范围,这势必使得各Sink节点能获得一个相对均匀的作用域,从而使得簇首节点分布在不同Sink节点的作用域之内,进而避免簇首节点集中在网络的某个区域。

(3)由于每个Sink节点的作用域范围有限,因此传感器节点通信只能局限在该作用域,这将降低网络对射频大功率的要求,从而也降低网络通信的能耗。

(4)本协议的簇首选举局限在其所属Sink节点的作用域范围内进行;并且各普通传感节点通过簇首只和其所属Sink节点单向传递数据;等等上述因素,使得本协议相比于传统分层路由协议,减少了网络通信量,提高了网络生存时间。

(5)OWMSRP协议是单层级分簇路由协议,即簇首节点只需负责簇内信息的收集与处理,而没有簇间数据转发的需要,因此,本协议降低了簇首节点的负载。

3　仿真与性能分析

从本文的设计与分析来看,OWMSRP协议相比于经典WSN分层路由协议及其改进协议能够有效解决因簇首节点而带来的网络瓶颈问题;但设计的效果会受到实际环境及相关网络参数的影响,因此,本文设计了仿真实验来测试LEACH、PEGASIS、LEACH-C与OWMSRP的网络性能。

实验确定无线传感器网络的观测区为:1 200 m×1 000 m,500个无线传感器节点随机分布在该区域,当测试LEACH、PEGASIS和LEACH-C时,整个网络只有一个Sink节点,该Sink节点的坐标为(0,800),观测区的传感器节点将信息发给该Sink节点进行处理。当测

试OWMSRP时,在观测区外围均匀分布4个Sink节点,每个Sink节点在其作用域范围内负责数据的处理。在测试时,为了能对各协议进行合理比较,各协议采用的仿真参数相同;在仿真过程中,各节点分多轮发送数据与Sink节点通信,每轮发送10帧,每帧大小为50个字节,信道速率为1 MB/s。

3.1 不同协议之间的能耗比较

OWMSRP协议下的簇首选举与簇的建立都局限在所属Sink节点的作用域范围之内完成;另外,在数据传输时,传感器节点通过簇首节点采用就近原则将信息传给其所属Sink节点;从而使得分层传感器网络在簇首节点处的瓶颈问题得以打破,进而降低网络节点能耗。为验证该效果,本仿真实验测试了在四种不同协议下的网络节点能量消耗随时间变化的情况。具体如图4所示。

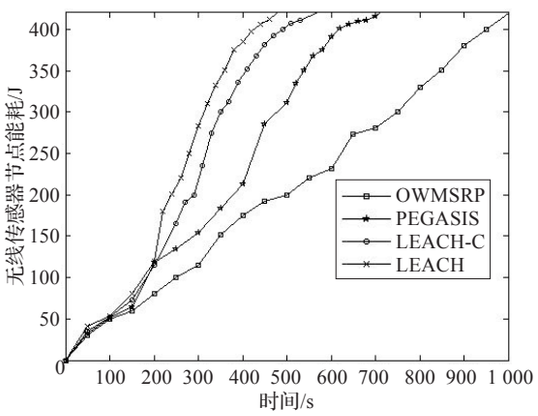

图4 不同协议的能耗比较

图4为在OWMSRP、LEACH、PEGASIS和LEACH-C下,网络在整个工作过程中,节点能耗随时间变化的情况。从图4可以看出,在测试的初始阶段,各协议下的节点剩余能量值没有太大差距;但随着测试时间的不断增加,OWMSRP协议明显放慢了能量消耗的速度;这是因为OWMSRP通过在无线传感器网络观测区域的外围均匀分布多个Sink节点,网络中的各簇首就近与其所属Sink节点交换数据,从而克服了传统单Sink协议因簇首负载过重而带来的网络瓶颈,使能量得到合理利用从而降低网络能耗。

3.2 不同协议的网络生存时间比较

分层路由协议最大的不足为簇首节点负载过重使得簇首节点的能量消耗非常快,进而导致簇首节点失效而影响网络的生命周期。因此,为衡量OWMSRP协议的网络性能,不仅要测试其网络节点的能量消耗情况,而且还需通过测试网络节点的生存时间来评估网络。具体如图5所示。

图5为在OWMSRP、LEACH、PEGASIS和LEACH-C下,无线传感器网络的节点存活数随时间变化的情况。从图5可以得知,与其他协议相比较,OWMSRP协议因拥有2.4小节所分析的优点,从而高效率地考虑簇首节点的网络瓶颈问题,明显延长了网络各节点的生存时间,进而提高了网络的生命周期。

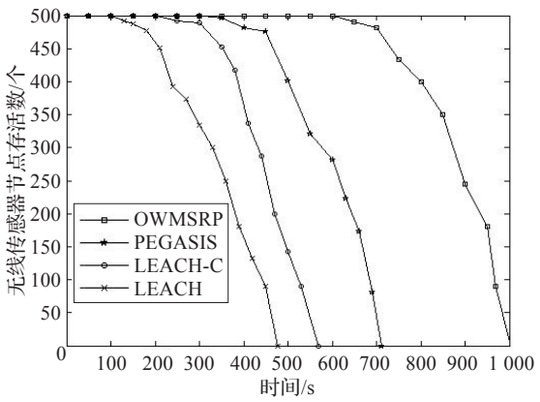

图5 不同协议的网络生存时间比较

4 结论

本文提出的OWMSRP协议,采用在无线传感器网络的观测区外围均匀分布多个Sink节点的方法来构建网络;使用RSSI技术来为每个Sink节点划分作用域范围;采用平均能量阈值的方法选举簇首节点并建立簇;采用传感器节点通过簇首节点单向与所属Sink节点通信。经分析,本文提出的这些技术,有效克服了在簇首节点处的瓶颈问题,减少了网络通信量,均衡了网络中各节点的负载,从而提高了网络生存时间。下一步的研究重点是将该协议应用到三维以及更复杂的无线传感器网络中。

参考文献:

[1] Potdar V,Sharif A,Chang E.Wireless sensor networks:a survey[C]//Proc of 2009 International Conference on Advanced Information Networking and Applications Workshops.Washington D C,USA:IEEE Computer Society,2009.

[2] 崔勇,张鹏.无线移动互联网原理、技术与应用[M].北京:机械工业出版社,2012.

[3] Li Chenmin.Analyzing cluster-head selection mechanisms and improving the LEACH[C]//Proc of ICECC'11.[S.l.]:IEEE Press,2011.

[4] 蒋畅江,石为人,唐贤能,等.能量均衡的无线传感器网络非均匀分簇路由协议[J].软件学报,2012,23(5):1222-1232.

[5] Sardar S,Sarker A,Bahar A N.Hierarchical routing protocol in wireless sensor network-a survey[J].International Journal of Scientific & Engineering Research,2015,6(2):184-189.

[6] 杨晗,杨天明.依托路由规则的自适应能量优化分簇无线传感器网络路由算法[J].计算机应用研究,2015,32(2):585-588.

[7] Younis O,Fahmy S.Heed:a hybrid,energy-efficient,distributed clustering approach for Ad-Hoc sensor networks[J].IEEE Transactions on Mobile Computing,2004,3(4):660-669.

(下转120页)

就可实现上述的“全或无”共享性,即:知道其中一个用户的私钥就可以求出另一个用户的私钥,而没有其中任何一个私钥的用户不能获得内部用户的私钥信息。

5 结语

本文引入了一类新的函数族并证明了CS-DCR方案关于这类函数族具有相应的KDM-CCA安全性。虽然这类函数族不能包含所有的仿射函数族,但是他们对于某些应用如匿名证书协议已经足够了。希望以后能够证明该方案关于更大类的函数族具有相应的KDM安全性。

参考文献:

[1] Goldwasser S, Micali S.Probabilistic encryption[J].Journal of Computer System Sciences,1984,28(2):270-299.

[2] Naor M, Yung M.Public-key cryptosystems provably secure against chosen ciphertext attacks[C]//STOC 1990, 1990: 427-437.

[3] Rackoff C, Simon D.Non-interactive zero-knowledge proof of knowledge and chosen ciphertext attact[C]//Crypto 1991, 1991,576:433-444.

[4] Boneh D, Halevi S, Hamburg M, et al.Circular secure encryption from decision diffie-hellman[C]//CRYPTO 2008, 2008,18:108-125.

[5] 常金勇,薛锐,史涛.ElGamal加密方案的KDM安全性[J].密码学报,2014,1(3):235-243.

[6] Camenishch J, Lysyanskaya A.An efficient system for non-transferable anonymous credentials with optional anonymity revocation[C]//EUROCRYPT 2001,2001,2045:93-118.

[7] Cash D, Green M, Hohenberger S.New definitions and separations for circular security[C]//PKC 2012,2012,7293: 540-557.

[8] Galindo D, Herranz J, Villar J.Identity-based encryption with master KDM security and leakage-resilience[C]// ESORICS 2012,2012:627-642.

[9] 来齐齐,陈原,裴庆祺,等.标准模型下KDM安全的对称加密方案[J].电子与信息学报,2011,33(6):1277-1281.

[10] Black J, Rogaway P, Shrimpton T.Encryption-scheme security in the presence of key-dependent messages[C]// SAC 2002,2002:62-75.

[11] Camenisch J, Chandran N, Shoup V.A public key encryption scheme secure against key dependent chosen plaintext and adaptive chosen ciphertext attacks[C]//Eurocrypt 2009,2009,5479:351-368.

[12] Hofheinz D.Circular chosen-ciphertext security with compact ciphertexts[C]//Eurocrypt 2013,2013,7881:520-536.

[13] Brakerski Z, Goldwasser S.Circular and leakage resilient public-key encryption under subgroup indistinguishability-(or:Quadratic residuosity strikes back)[C]// Crypto 2010,2010:1-20.

[14] Brakerski Z, Goldwasser S, Kalai Y.Black-box circular-secure encryption beyond affine functions[C]//TCC 2011, 2011:201-218.

[15] Barak B, Haitner I, Hofheinz D, et al.Bounded key-dependent message security[C]//Eurocrypt, 2010, 2010: 423-444.

[16] Qin Baodong, Liu Shengli, Huang Zhengan.KDM-CCA security of the Cramer-Shoup cryptosystem[C]//ACISP 2013,2013:136-151.

[17] Chang Jinyong, Xue Rui.Practical key-dependent message chosen-ciphertext security based on decisional composite residuosity and quadratic residuosity assumptions[J].Security and Communication Networks, 2015, 8 (8):1525-1536.

[18] Cramer R, Shoup V.Universal hash proofs and a paradigm for adaptive chosen ciphertext secure public key encryption[C]//Eurocrypt 2002,2002,2332:45-64.

(上接109页)

[8] Xia D, Vlajic N.Near-optimal node clustering in wireless sensor networks for environment monitoring[C]//AINA International Conference on Advanced Information Networking and Applications.Washington DC: IEEE Computer Society,2007:632-641.

[9] Grilo A, Macedo M, Nunes M.An energy-efficient low-latency multi-sink MAC protocol for alarm-driven wireless sensor networks[C]//LNCS 4396: Wireless and Mobility, 2007:87-101.

[10] Emanuele C, Francesca C.Topology characterization and performance analysis of IEEE 802.15.4 multisink wireless sensor networks[C]//The Sixth Annual Mediterranean Ad Hoc Networking Workshop,2007:196-203.

[11] Akyildiz F, Kasimoglu H.Wireless sensor and actor networks: research challenges[EB/OL].[2004-05-19].http://www.docin.com/p-347054477.html.

[12] Heinzelman W, Chandrakasan A, Balakrishnan H.Energy-efficient communication protocol for wireless microsensor networks[C]//Proc of the 33rd Annual Hawaii International Conference on System Scineces.Maui: IEEE Computer Society,2000:3005-3014.

[13] Lindsey S, Raghavendra C S.PEGASIS: Power-efficient gathering in sensor information systems[J].IEEE Aerospace and Electronic Systems Society,2002:1125-1130.

[14] Heinzeiman W.Application-specific protocol architectures for wireless networks[D].Boston: Massachusetts Institute of Technology,2000.

[15] 姚光顺,温卫敏,张永定,等.改进的无线传感器网络簇首选择策略及其路由算法[J].计算机应用,2013,33(4): 908-911.

[16] 苏金树,郭文忠,余朝龙,等.负载均衡感知的无线传感器网络容错分簇算法[J].计算机学报,2014,37(2):445-456.