第36卷 第14期 计 算 机 工 程 2010年7月
Vol.36 No.14 Computer Engineering July 2010
·安全技术· 文章编号：1000—3428(2010)14—0132—03 文献标识码：A 中图分类号：TP393

基于密钥连通的WSN簇头选择安全算法

杨 洲[1]，景 博[1]，孙 勇[2]
(1. 空军工程大学工程学院，西安 710038；2. 中国人民解放军 94701部队，安庆 246001)

摘 要：分析无线传感器网络中密钥管理和分簇路由协议存在的安全漏洞，利用模糊推理系统，将簇头与簇内节点的共享密钥数作为重要评判指标，建立一种基于密钥连通的簇头选择安全算法。不同于传统的模糊推理算法，该算法实现了分簇路由协议与密钥管理方案的良好结合，与典型分簇算法相比，能有效降低并均衡簇内的通信能耗、增强通信安全。

关键词：无线传感器网络；密钥管理；分簇；模糊推理

Cluster Head Selection Security Algorithm for Wireless Sensor Networks Based on Key Connection

YANG Zhou[1], JING Bo[1], SUN Yong[2]
(1. College of Engineering, Air Force Engineering University, Xi'an 710038; 2. PLA 94701 Troop, Anqing 246001)

【Abstract】 The security leakage of current key management scheme and clustering routing protocols in Wireless Sensor Networks(WSN) is analyzed, and a cluster head selection algorithm based on key connection is proposed. It takes the number of keys shared between cluster head and cluster nodes as the important index, using the fuzzy inference system. Unlike to the traditional fuzzy inference algorithm, the algorithm achieves a good combination between the clustering routing protocols and key management schemes, effectively lowering and balancing the communication energy in a cluster and improving the communication security compared with the typical clustering algorithm.

【Key words】 Wireless Sensor Networks(WSN); key management; clustering; fuzzy inference

1 概述

无线传感器网络(Wireless Sensor Networks, WSN)作为一门新兴的交叉学科，提供了一种全新的信息获取与处理手段，在军事、农业和医疗等领域都有广阔的应用前景[1]。随着对WSN应用和研究的不断深入，安全问题引起了学者和研究机构的关注。目前，WSN安全研究主要集中在密钥管理、身份认证和数据加密方法、攻击检测与抵御、安全路由协议和隐私问题等方面[2]，密钥管理是研究其他问题的基础。

当节点以簇的形式自组成网时，极大扩展了网络节点的规模和监测范围。每个簇按照一种准则选择合适的节点担任簇头，当簇头剩余能量过低或节点俘获时如何重新选择簇头，具有一定模糊性。簇头主要用于管理或控制簇内成员节点、负责簇内信息的收集、完成数据聚集与转发，要保证信息不被他人获取，必须通过加密和密钥管理。

2 研究现状

WSN 密钥管理按网络拓扑结构可分为分布式密钥管理和分簇型密钥管理。在分布式密钥管理中，节点通信和计算能力是相同的，由预先分布在节点的密钥协作完成共享密钥发现和路由密钥建立及节点密钥的更新与剔除。在分簇式密钥管理中，由具有更多资源的簇头完成上述功能，其功能实现建立在分簇和簇头选择算法上，它的安全直接影响整个密钥管理的安全。

LEACH 是典型的分簇算法[3]，其簇头选择采用概率选择，分簇存在不合理性，文献[4]提出的方案利用模糊推理系统，对LEACH进行改进。但上述算法未考虑信息传输安全，增大了网络威胁。现有路由协议涉及安全问题主要采用密钥管理和安全路由，文献[5]以LEACH为基础，构建密钥预分配模型，设计并实现了一种安全路由算法。但LEACH存在分簇不合理、簇内节点能量不均衡等问题，制约了其效能的实现。

针对现有WSN密钥管理缺乏对安全路由的研究，为使网络具有更好的抗俘获性和较大的网络规模，本文提出一种基于密钥连通的WSN簇头选择安全算法，将簇头选择及密钥管理合为一体，一旦分簇完毕并选择好簇头，即可进行可靠的信息传递，保证簇内的通信安全。

3 簇头选择安全算法

为便于描述，本文采用的相关变量定义如下：

S：密钥池大小；

m：密钥环大小；

ID_i：第 i 个节点的ID；

K_i：第 i 个共享密钥；

K_{ui}：第 i 个节点的私钥；

K_{ci}：第 i 个簇密钥；

K_{share}：2个节点建立安全链路的通信私钥。

3.1 问题的提出

节点分布前，预先从一个很大的密钥池(如 2^{17}~2^{20})随机抽取一定数量密钥构建密钥环。此外，节点还从基站获取一个唯一的私钥 K_{ui} 和ID。假设密钥池大小为 S=1 000，则2个

基金项目：陕西省自然科学基金资助项目(2009JM8002-7)；西安市科技创新支撑计划基金资助项目(CXY1011(5))

作者简介：杨 洲(1985－)，男，硕士研究生，主研方向：密钥管理，无线传感器网络安全；景 博，教授、博士后、博士生导师；孙 勇，博士

收稿日期：2009-12-25 **E-mail：**yz-34@163.com

节点至少共享一个密钥的概率为

$$p = p(1)+p(2)+\cdots+p(m)=1-p(0)=1-\frac{C_S^m C_{S-k}^m}{\left(C_S^m\right)^2}=$$

$$1-\frac{\left((S-m)!\right)^2}{(S-2m)!S!}$$

据此，网络的密钥连通性如图 1 所示，其中，S=1 000; m=200。

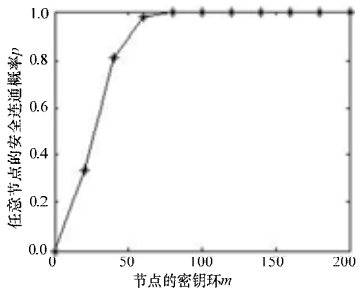

图 1　节点的密钥连通性

由图 1 可知，随着节点密钥环 m 的增大，节点安全连通概率 p 增大。在分簇型网络中，节点要想成为簇头，必须与簇内所有节点至少共享一个密钥，才能建立安全链路、进行安全通信。

现有分簇和簇头选择协议大多只考虑节点物理连通，不考虑密钥安全链路建立，网络易受攻击，导致瘫痪或信息泄露。已有密钥管理方案假定节点按一定路由协议部署，不研究其安全性。因此，要设计一种既考虑簇内密钥链路建立和能量有效，又保证簇内安全通信的簇头选择密钥连通算法。

3.2　簇头选择密钥连通算法

现有簇头选择方案大多将节点划分为高级节点和低级节点，采用固定簇头(由高级节点担当)进行管理，一旦簇头被俘，存储的密钥信息泄露，影响整个簇的安全通信。为有效延长网络寿命，提高节点抗俘获能力，本文设计了一种基于模糊推理的簇头选择算法作为密钥连通的基础，采用节点轮流担当簇头来均衡能耗，避免个别节点因长期担任簇头能耗过大导致网络盲区。与文献[4]不同，本文利用模糊推理系统计算量低的特点，以剩余能量、邻节点数、节点中心度和共享密钥数作为系统输入，以节点成为安全簇头机会作为系统输出。重点考察共享密钥数，结合模糊推理规则，将簇头选择转化为模糊推理。

3.2.1　模糊变量和规则设计

剩余能量包含“低、中等、高”3 个模糊集；邻节点数包含“少、中等、多”3 个模糊集；节点中心度包含“近、中等、远”3 个模糊集；共享密钥数包含“少、中等、多”3 个模糊集；节点成为安全簇头机会包含“很小、小、中等、大和很大”5 个模糊集。对于隶属度函数的选择，根据专家经验“中等”选择三角函数，其他则选择梯形函数，该函数便于实现网络时钟同步。

节点剩余能量=初始能量-消耗能量，消耗能量主要包括节点的通信和计算能量，通常认为通信能耗比计算能耗大 3 个数量级。因此，簇头主要根据接收到的节点数据包估计簇内节点剩余能量。邻节点数为处于节点直接通信范围且属同簇的节点数。节点中心度是节点与所选簇头的欧氏距离，假设节点位置已知。共享密钥数通过比较基站对簇头与簇内成员节点密钥环得到。

模糊规则由专家经验确定，通常剩余能量低、邻节点数目少、中心度远且共享密钥数少的节点成为安全簇头的机会小；反之，当选安全簇头机会大。每个输入模糊变量包含 3 个模糊集，利用“if-then”语句构建模糊规则，用“and”连接前项条件，则该模糊系统共有 3^4=81 条规则。限于篇幅，只列出了部分模糊规则库，见表 1。

表 1　部分模糊规则库

ID	if				then
	剩余能量	邻节点数	中心度	共享密钥数	机会
1	低	少	远	少	很小
2	低	少	远	中等	很小
3	低	少	远	中等	很小
…	…	…	…	…	…

在建立了输入输出变量及其隶属度函数构造完模糊规则后，即可执行模糊推理。本文采用“极大-极小”合成为模糊推理规则，模糊推理算法为 Mamdani 算法，去模糊化方法为面积中心法。

3.2.2　模糊推理算法仿真

当簇头选定进入稳定传输，一旦簇头剩余能量低于阈值或被俘，即触发簇头选择。当基站重新选择簇头，原簇头作为普通节点继续参与监测，负责感知、传递数据。当网络平均能量较低，这些节点依据其剩余能量不同仍有机会再次当选簇头。基于模糊推理的簇头选择算法流程如图 2 所示。节点成为安全簇头的机会如图 3 所示。

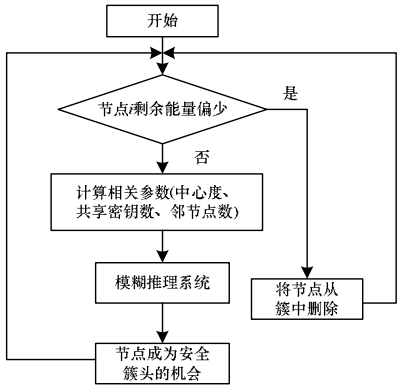

图 2　簇头选择算法流程

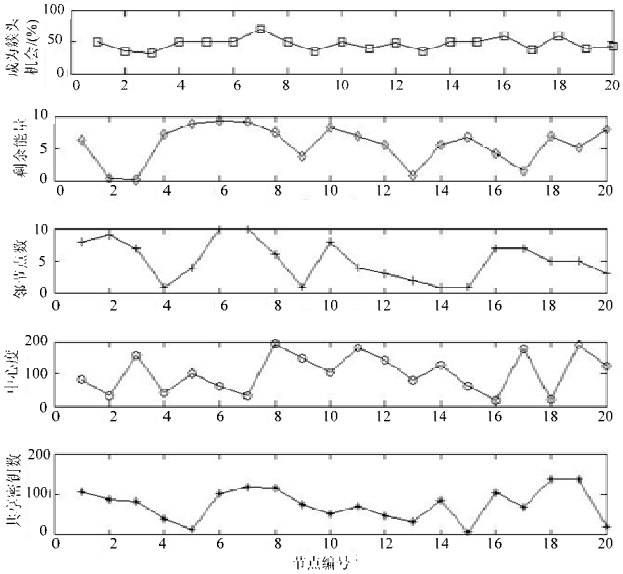

图 3　节点成为安全簇头的机会

在图 3 中 20 个节点的簇内，当簇头 2 剩余能量低于阈值，假设基站能够检测该事件，并利用模糊推理在簇内重新选择簇头时，各节点成为安全簇头的机会与剩余能量、邻节点数、中心度和共享密钥数有关。在本轮簇头选择中，节点 7 当选簇头。当节点成为簇头机会相同时，共享密钥数大的节点当选安全簇头。不仅要保证节点物理连通，而且要保证密钥连通，才能建立安全链路，确保信息传递安全可靠。

当一轮簇头选择完成即在簇内形成完全密钥连通图，满足以下条件：(1)所有簇内节点都在簇头直接通信范围内；(2)建立的网络都是密钥连通的。

当安全链路建立后，由簇头与簇内节点的共享密钥对来建立链路的通信私钥 K_{share}，而 $K_{share}=Hash(K_1|K_2|\cdots|K_i)$。节点将自身私钥 K_{ui} 加密传给簇头：$K_{ci}=message(ID|K_{ui})_{Kshare}$。簇头将收到的簇内节点信息给基站：$message(ID_{cl}|K_{c1}|K_{c2}|\cdots|K_{ci})_{Kui}$，由基站对其进行加密运算，将簇密钥 $K_c=Hash(message\ (ID_{cl}|K_{c1}|K_{c2}|\cdots|K_{ci})_{Kui})$传给簇头，簇头通过和簇内节点形成的密钥对将其分配给簇内节点，建立簇密钥保证整簇安全通信。

3.3 节点的加入与退出

定义 共享密钥集 由簇头节点与簇内成员节点所有共享密钥构成的集合。

当有新节点加入，首先由基站随机从密钥池选取一定密钥组成密钥环，并判断是否有密钥属于当前共享密钥集。计算加入节点的相关变量，利用模糊推理系统判断能否与簇头建立安全链路。一旦节点被俘获或能量耗尽退出，即触发密钥更新。基站删除该节点 ID 和共享密钥，建立新的共享密钥集重新进行簇头选择，从而保证被俘节点不会对网络安全产生影响。算法流程如图 4 所示。

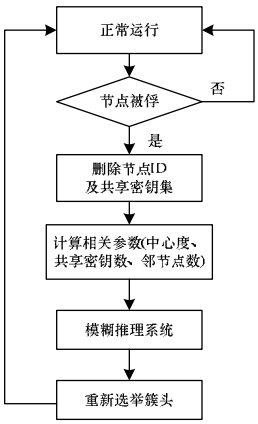

图 4 节点加入与退出

3.4 密钥更新

当簇头剩余能量低于阈值，由其向基站发起请求，基站根据模糊推理系统重新进行簇头选择，并将新产生的簇内通信密钥 K_{new} 和簇头 ID 广播给簇内节点。节点收到后替换原有密钥和 ID，原有簇头降级为普通节点继续参加网络监测。

4 仿真及性能分析

4.1 计算性能和能量消耗

该算法引入模糊推理系统选择簇头，由基站完成以减轻节点的运算负担，较好地满足 WSN 轻量级的处理要求，并采用与 LEACH 相同的能耗模型和相关参数设置[3]，运用 Matlab 仿真，见图 5。由图 5 可知，相比 LEACH 算法，利用模糊推理系统使簇头选择趋于合理，较好地平衡了节点能耗，传统 WSN 密钥管理以一定路由协议为基础，节点能量消耗较大。本方案在路由建立时考虑安全连通，将链路建立与密钥共享相结合，降低了网络通信能耗，延长了节点寿命。

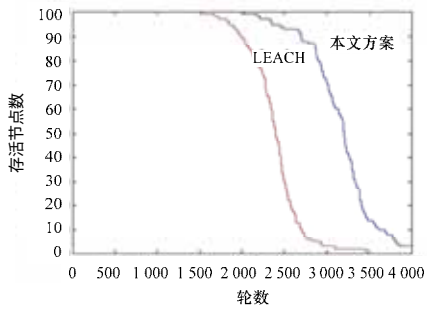

图 5 网络存活节点比较

4.2 簇头分布

分簇完毕后各节点将信息发给基站，作为模糊系统的输入变量，基站根据模糊推理系统，决策节点成为安全簇头的机会。当 2 个节点成为簇头机会相等时，重点考虑其安全问题，着重选择共享密钥多的节点成为簇头，解决了文献[4]中的安全问题。在选举簇头时有效避免了 LEACH 算法簇头分布的随机性，更加贴近实际。

4.3 信息安全

节点和簇头通信采用 Hash 函数进行加密运算，利用 Hash 函数单向性避免敌人窃听传递信息，防止敌人注入虚假信息。此外，簇头轮换机制也可有效抵御网络流量分析，避免泄漏拓扑结构。根据不同应用场景的安全需求，设立不同的共享密钥数，实现不同等级的安全性能。亦可运用不同的密钥共享机制提高网络中节点的抗俘获性，与路由协议相结合构建可靠的安全链路。因此，该方案具有较好的安全适应性和体系开放性。

5 结束语

本文在同构传感器网络中利用模糊推理系统，将共享密钥引入簇头选择，使其更加公平合理，保密性更强，并有效降低节点成本。簇头选择由基站完成，进一步降低了网络通信能耗，提高网络的密钥连通和安全等级。但存储过多密钥会占用节点有限内存，如何寻找最优共享密钥数并设计更有效的基于密钥联系的安全路由协议是未来研究的重点。

参考文献

[1] Akyildiz I F. Wireless Sensor Networks: A Survey[J]. Computer Networks, 2002, 38(4): 393-422.

[2] 李建中, 高 宏. 无线传感器网络的研究进展[J]. 计算机研究与发展, 2008, 45(1): 6-7.

[3] Heinzelman W R, Chandrakasan A, Balakrishnan H. Energy-efficient Communication Protocol for Wireless Microsensor Networks[C]//Proceedings of the 33rd Hawaii International Conference on System Sciences. Hawaii, USA: [s. n.], 2000: 3005-3014.

[4] Gupta I, Riordan D, Sampalli S. Cluster-head Election Using Fuzzy Logic for Wireless Sensor Networks[C]//Proc. of the 3rd Annual Communication Networks and Services Search Conference. Washington, USA: IEEE Computer Society, 2005.

[5] Oliveira L B, Marco A F. SecLEACH——On the Security of Clustered Sensor Networks[J]. Signal Processing, 2007, 87(12): 2882-2895.

编辑 张正兴