基于低能耗的无线传感器网络安全LEACH协议

王江涛,葛 强,钱 炜,蔡得菊
(中国十七冶集团有限公司信息化部,安徽 马鞍山 243061)

摘 要:针对无线传感器网络分层型路由协议面临的安全威胁和能量有限的问题,提出一种能量优化的安全LEACH协议(SC-LEACH)。该协议通过簇头选举、建立分簇、TDMA时隙分配、信息交互四个阶段的执行,准确设定阈值,解决了最佳簇头数精确选取的问题,同时采用预置共享密钥对方式抵御各种恶意攻击。通过与采用对称密钥加密方式的LEACH协议对比,仿真验证了SC-LEACH算法的有效性,表明该协议在能量优化的同时提高了网络安全性。

关键词:无线传感器网络;网络安全;LEACH;能量优化;簇头选举算法
中图分类号:TP309 **文献标识码**:A **文章编号**:1673-629X(2012)05-0242-03

Secure LEACH Routing Protocol Based on Energy Optimization for Wireless Sensor Network

WANG Jiang-tao, GE Qiang, QIAN Wei, CAI De-ju
(Department of Information Technology of China MCC17 Group Company Limited, Ma'anshan 243061, China)

Abstract: Aiming at the security threats faced by hierarchical model routing protocol and the energy limited of wireless sensor network, put forward the secure LEACH routing protocol (SC-LEACH) based on low-power cluster-head selection algorithm. This protocol gets the four stages of implementation in cluster head election, creating cluster, TDMA time slot allocation and information interaction to accurately set threshold, and solve the accurate selection of optimal cluster number. At the same time use preset shared key on the way to resist all sorts of malicious attacks. Comparing with the LEACH protocol which uses the symmetric keys dispatch, this simulation validates the effectiveness of SC-LEACH and shows that the algorithm optimizes energy as well as improves the security of routing.

Key words: wireless sensor network; network security; LEACH; energy optimization; cluster-head selection algorithm

0 引 言

无线传感器网络(Wireless Sensor Network, WSN)[1]是由部署在监测区域内大量的廉价节点组成,通过无线通信方式形成的一种多跳自组织、自管理的网络。LEACH是WSN中最早的分层型路由协议[2],其他的分层型路由协议PEGASIS[3]、TEEN[4]、LEACH-EE[5]等都是在LEACH的基础上发展起来的。基于LEACH协议,有些专家提出了LEACH的改进算法[6,7],有些专家提出改进分簇路由算法[8~10]。分层型路由协议面临多种恶意攻击,需要做好安全防护方能大范围投入使用[11]。文中提出的新协议在增加安全性能的同时把能量优化作为设计目标,通过在节点部署前预置共享密钥对,增加了协议的安全性。

1 LEACH协议簇头选举算法分析

在LEACH协议中,尚未当选过簇头的节点在本轮(第r轮)成为簇头的概率为:

$$p(r)=\frac{p}{1-p\times[r\bmod(1/p)]}=\frac{k}{N-k*r} \tag{1}$$

由于簇头选举算法是全分布的,单个节点无法获知当前候选簇头节点的个数$N(r)$,采取估算方法计算,令$N(r)=N-k*r$。则:

$$\{x(r)=i\mid i\in[0,N(r)],r\in[0,\frac{N}{k}-1],$$

$$N(r)=N-\sum_{j=0}^{r-1}x(j)\} \tag{2}$$

对于第r轮选举,产生的簇头个数服从二项分布$B(N(r),p(r))$:

$$p(x(r)=k)=C_{N(r)}^{k}p(r)^{k}(1-p(r))^{N(r)-k} \tag{3}$$

在$N(r)$一定的情况下,式(3)中$C_{N(r)}^{k}$为常数,则$p(x(r)=k)$值仅与$p(r)$有关。为了求式(3)的最大值,只需求$p(r)^{k}(1-p(r))^{N(r)-k}$的最大值。假设有连续函数$f(p(r))=p(r)^{k}(1-p(r))^{N(r)-k}$,对该抛物线函数求导,令

$$\frac{df(p(r))}{dp(r)}=kp(r)^{k-1}(1-p(r))^{N(r)-k}+(N(r)-$$

收稿日期:2011-09-22;**修回日期**:2011-12-26
作者简介:王江涛(1978-),男,安徽马鞍山人,高级工程师,博士,研究方向为计算机网络。

$k)p(r)^k(1-p(r))^{N(r)-k-1}$

$=p(r)^{k-1}(1-p(r))^{N(r)-k-1}(kp(r)-(N(r)-k)(1-p(r)))=0$

解此方程可得:

$$p(r)=\frac{k}{N(r)} \tag{4}$$

因此,在每轮选举中,当$p(r)=\frac{k}{N(r)}$时,选举出k个簇头节点的概率最大,而不是LEACH协议认为的$p(r)=\frac{k}{N-n*k}$。并且从式(3)可以看出$x(r)$的值和$p(r)$、$N(r)$值都有关。

2 基于低功耗簇头选举算法的安全LEACH协议(SC-LEACH)

2.1 改进LEACH协议的簇头选举算法

通过以上分析可知,在WSN中若想使选出最优簇头数的概率最大,节点就需要知道全网当前参加选举的节点个数。在WSN的分簇建立阶段,当新当选簇头节点A的簇头身份确立后,向全网广播当选信息,并在广播信息尾部添加已当选簇头节点总个数$ch(r)$,周围节点根据信号强度大小自行决定加入相应簇。簇头节点A以最大功率向全网发送当选信息,尽量让全网节点都能收到其发布的信息。当簇头节点B收到A节点广播信息后,与A节点数据包中的$ch(r)$值比较,如果比自己的$ch(r)$值大,则将自己的$ch(r)$值更新为A的$ch(r)$值,如果相等则把自己的值设为$ch(r)+1$,从而确保新当选簇头节点建立分簇时$ch(r)$值为最新。

2.2 改进簇头选举算法的LEACH协议算法分析

设$E(p(r))$、$D(p(r))$分别为LEACH协议第r轮选举出簇头节点数的期望值与方差,$E(p'(r))$、$D(p'(r))$为改进LEACH协议第r轮簇头节点数的期望值与方差,则有:

$$E(p(r))=E(E(p(r)/N(r)))=E(N(r)p(r))=E(N(r))*p(r) \tag{5}$$

$$E(p'(r))=E(E(p'(r)/N(r)))=E(N(r)p'(r))=k \tag{6}$$

对于式(5),通过递推公式可得:

$$E(N(r))=E(E(N(r)/N(r-1)))=N-k*r \tag{7}$$

将式(7)分别代入式(5)得

$$E(p(r))=E'(p(r))=k$$

从而LEACH协议和改进簇头选举算法的LEACH协议每轮簇头数的均值都为k。由方差公式$D(x)=E(D(x/y))+D(E(x/y))$,可得到下面公式:

$$D(p(r))=\frac{k(n-rk)}{n} \tag{8}$$

$$D(p'(r))=kE(\frac{N-N(r)-k}{N-N(r)}) \tag{9}$$

为了比较两者的大小,计算两者之差:

$$\delta=D(p(r))-D(p'(r))=k^2E(\frac{N(r)}{N(N-N(r))}) \tag{10}$$

显然$\delta>0$,即改进LEACH协议的方差比LEACH协议小,也就是说每轮选举出的节点更加接近于最佳簇头数k。因此,采用改进簇头算法的LEACH协议簇头选举概率为$p'(r)=\frac{k}{N(r)}$时,可以确保每轮选举出k个簇头节点的概率最大。

2.3 SC-LEACH协议描述

SC-LEACH采用预置共享密钥对的方法[12],SC-LEACH协议执行分为四个阶段。

(1) 簇头选举。

节点H以明文方式向全网广播宣布自己为簇头节点,发布{sequence|ID_H|$ch(r)$}报文告诉周围节点当前选举轮数sequence、密钥标志ID_H、已当选过簇头节点的个数$ch(r)$。

(2) 建立分簇。

每个节点可能会收到多个簇头节点的报文,选取信号最强的簇头读取其相关参数,确定密钥S,发送{sequence|S}信息加入该簇。其他簇头收到H发布的报文后,与H中的$ch(r)$值比较,如比自己的大,则将自己值置为H的$ch(r)$值,如相等则置为$ch(r)+1$。

(3) TDMA时隙分配。

簇头节点向簇内成员节点发送调度信息

{ID_H|[sequence|CDMA code|TDMAschedule|$ch(r)$]},分配用于信息交互的TDMA时隙。

(4) 信息交互。

分簇建立后,簇内成员节点采集数据,加密后发送到簇头。簇头节点解密收到的信息,剔除无效、重复的数据后将有用信息发送到基站。

3 实验结果及分析

3.1 网络仿真环境

仿真工具采用NS-2平台,操作系统为Linux。E_{elec}是发送电路和接收电路消耗的能量,由于实际相差不大,在这里简化为两者相等。在簇头节点取3~5个时,所消耗的总能量最小[2],文中仿真时取最优簇头个数为4。表1列出了仿真中使用的参数。

3.2 仿真过程及数据分析

主要通过以下三个指标:每轮节点存活数、节点消

耗的总能量值、每轮产生的簇头节点个数，综合分析比较两种算法的性能。

表1 仿真中使用的参数

仿真节点数	100个
撒布范围	100m * 100m
基站坐标	(50,175)
选举时间间隔	10m
E_{elec}	50nJ/bit/m
传输功放 ε_{amp}	0.0013pJ/bit/m^2
报文融合消耗 E_{da}	5nJ/bit/signal
初始能量	2J
最优簇头数	4
带宽	1Mkbs

(1) 每轮剩余存活节点数比较。

WSN每轮存活的节点数越多，参与选举的簇头数就多，则网络的生命期就越长。由图1可以看出，采用LEACH协议的WSN网络在418秒时节点开始死亡，到582秒时节点全部死亡。而采用SC-LEACH协议的WSN网络，在563秒时才有节点死亡，到745秒时节点全部死亡。说明采用SC-LEACH协议的WSN网络生命期比采用LEACH协议的要长。

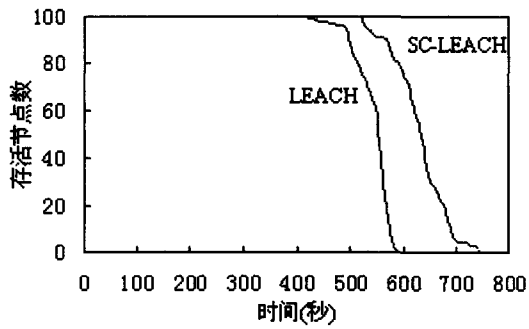

图1 每轮节点存活数比较

(2) 节点总能耗比较。

WSN全网节点总能耗越少生命期就约长。由图2可以看出，LEACH协议总能耗曲线在297秒时突变，能耗随之突增。采用SC-LEACH协议的总能耗曲线相对平滑，从而节点每轮消耗的能量相对稳定，全网总能耗较低。

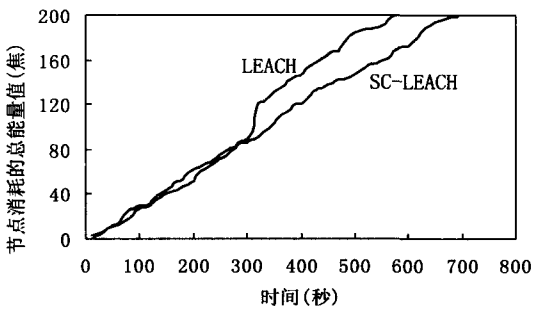

图2 节点消耗的总能量比较

(3) 每轮产生的簇头节点个数比较。

每轮产生的簇头数越接近最优簇头数，网络的整体能耗就小，生命期就长。由图3可以看出，两种协议产生的簇头节点数都在4左右摆动，但是SC-LEACH协议摆动的幅度要小得多。

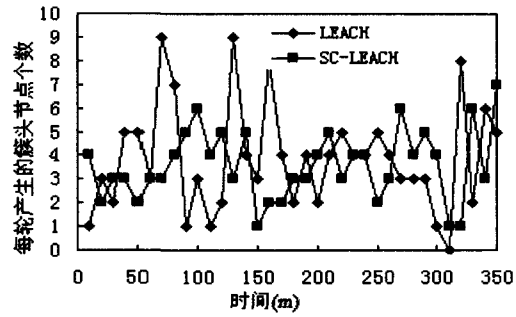

图3 每轮产生的簇头节点个数比较

4 结束语

文中提出的SC-LEACH协议在LEACH基础上改进了WSN簇头选举算法及加密方式。通过与采用对称密钥加密方式的LEACH协议对比的仿真结果表明，SC-LEACH协议采用的在簇头选举时相互协作获取当前参加选举的节点总数，及通过预置共享密钥对加密机制，可以在优化全网能耗的同时提高路由安全性。

参考文献：

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

[2] Heinzelman W, Chandrakasan A, Balakrishnan H. Energy-efficient communication protocol for wireless micro sensor networks[C]//Proceedings of the 33rd Annual Hawaii International Conference on System Sciences. Hawaii: [s. n.], 2000: 1-10.

[3] Lindsey S, Raghavendra C S. PEGASIS: power efficient gathering in sensor information systems[C]//Proceedings of IEEE Aerospace Conference. [s. l.]: [s. n.], 2002: 1125-1130.

[4] Manjeshwar A, Agrawal D P. TEEN: *a routing protocol for enhanced efficiency in wireless sensor network*[C]//Proceedings of the 15th Parallel and Distributed Processing Symposium. [s. l.]: [s. n.], 2001: 2009-2015.

[5] 李 岩，张曦煌，李彦中. LEACH-EE-基于LEACH协议的高效聚类路由算法[J]. 计算机应用，2007，27(5)：1103-1105.

[6] 武春涛，胡艳军. 无线传感器网络LEACH算法的改进[J]. 计算机技术与发展，2009，19(3)：80-83.

[7] 金 骥，徐昌庆，葛颖君. 无线传感器网络基于类的LEACH路由算法研究[J]. 计算机应用与软件，2006，23(11)：137-138.

[8] 李 雷，付东阳. 基于分层模型的无线传感器网络分簇路由算法[J]. 计算机技术与发展，2010，20(1)：135-138.

(下转第249页)

[9] 林德敬,林柏钢,林德清.3GPP系统全系列信息安全及其算法设计与应用[J].重庆邮电学院学报,2003,15(4):18-23.

[10] 王　冉,李小文.基于TD-SCDMA系统的完整性保护算法的研究[J].信息技术,2005(10):66-69.

[11] 姚惠明,隋爱芬,杨义先.3GPP网络AKA协议中若干算法的设计[J].北京邮电大学学报,2002,25(3):98-102.

[12] 万仁福,李方伟,马剑光,等.GPRS与UMTS系统网络接入安全机制的比较与研究[J].电讯技术,2004(4):42-46.

[13] 万仁福,李方伟.GPRS与UMTS系统网络接入安全机制的比较与研究[J].重庆邮电学院学报,2004,17(1):42-45.

[14] 戴沁芸.第三代移动通信系统网络接入安全机制分析[J].现代电信技术,2010(4):12-17.

[15] Zhang Muxiang, Fang Yuguang. Security Analysis and Enhancements of 3GPP Authentication and Key Agreement Protocol[J]. IEEE Transactions on Wireless Communication, 2005,4(2):734-742.

[16] Huang C M,Li J W. Authentication and key agreement protocol for UMTS with low bandwidth consumption[C]//Proc. of the 19th Int'l Conf. on Advanced Information Networking and Applications. Washington:IEEE Computer Society Press, 2005:392-397.

[17] Saraireh J A,Yousef S. Extension of authentication and key agreement protocol (AKA) for universal mobile telecommunication system(UMTS)[J]. Int'l Journal of Theoretical and Applied Computer Sciences,2006,1(1):109-118.

[18] Lee C C,Hwang M S,Yang W P. Extension of authentication protocol for GSM[J]. IEEE Proc. of Communications,2003, 150(2):91-95.

[19] Zhang M X,Fang Y G. Security analysis and enhancements of 3GPP authentication and key agreement protocol[J]. IEEE Trans. on Wireless Communications,2005,4(2):734-742.

[20] Juang W S,Wu J L. Efficient 3GPP authentication and key agreement with robust user privacy protection[C]//Proc. of the IEEE Wireless Communications and Networking Conf.[s. l.]:[s. n.],2007:2722-2727.

[21] Bais A,Penzhorn W T,Palensky P. Evaluation of UMTS security architecture and services[C]//Proc. of the IEEE Int'l Conf on Industrial Informatics. Washington: IEEE Computer Society Press,2006:570-575.

[22] Jiang R,Li J H,Pan L. Formal analysis of 3GPP authentication and key agreement based on the strand space model[J]. Journal of Shanghai Jiaotong University,2006,40(5):791-795.

[23] Yuan Y F,Lian Y Z. Logic analysis of authentication key agreement protocol of 3G mobile communication[J]. Journal of Information Engineering University,2004,5(4):15-17.

[24] Liu F,Li D X. Amelioration of authentication and key agreement protocol in 3G[J]. Computer Engineering and Design, 2006,27(14):2705-2707.

[25] Marques V,Aguiar R L,Garcia C,et al. An IP-based QoS architecture for 4G operator scenarios[J]. IEEE Wireless Communications,2003,10(3):54-62.

[26] Bravo A M,Moreno J I,Soto I. Advanced positioning and location based services in 4G mobile-IP radio access networks [C]//Proc. of Int. Symposium on Personal,Indoor and Mobile Radio Communicaitons. Lisbon, Portugal: IEEE, 2004: 1085-1089.

[27] Dell'Uomo L,Scarrone E. An all-IP solution for QoS mobility management and AAA in the 4G mobile network[C]//Proc. of Int. Symposium on Wireless Personal Multimedia Communication. Hawaii,USA:IEEE,2002:591-595.

[28] Santhi K R,Kumaran G. S. Migration to 4G:Mobile IP Based Solutions[C]//Proc. of Int. Conf. on Internet and Web Applications and Services. Guadeloupe, French: IEEE Computer Society,2006:76-76.

[29] Kojen G M,Haslestad T. Security Aspects of 3G-WLAN Interworking[J]. IEEE Communication Magazine,2003,41(5):82-88.

[30] Salkintzis A K. Interworking Techniques and Architecture for WLAN/3G Intergration Torward 4G Mobile Data Networks [J]. IEEE Wireless Communication,2004,11(3):50-61.

[31] Salkintzis A K,Fors C,Pazhyannur R. WLAN-GPRS Integration for Next-Generation Mobile Data Networks[J]. IEEE Wireless Communication,2002,9(5):112-124.

[32] Kambourakis G,Rouskas A,Kormentzas G,et al. Advanced SSL/TLS Communication[J]. IEEE Proceedings,2004,151 (5):501-506.

(上接第244页)

李成法,陈贵海.一种基于非均匀分簇的无线传感器网络路由协议[J].计算机学报,2007,30(1):88-91.

[10] 杨菊英,吕光宏.无线传感器网络分层路由协议研究[J].计算机技术与发展,2008,18(6):115-118.

[11] 周贤伟,覃伯平.基于能量优化的无线传感器网络安全路由算法[J].电子学报,2007,35(1):54-57.

[12] Imamoto K,Sakurai K. A Design of Diffie-Hellman Based Key Exchange Using One-time ID in Pre-shared Key Model [C]//The 18th International Conference on Advanced Information Networking and Applications.[s. l.]:[s. n.],2004: 327-333.