基于信誉机制的传感器网络安全路由协议设计

李 玲,王新华,车长明
(山东师范大学 信息科学与工程学院,山东 济南 250014)

摘 要:无线传感器网络具有与传统网络不同的特点,传统的安全路由协议不能有效地应用于无线传感器网络,所以无线传感器网络安全问题成为亟待解决的课题。针对无线传感器网络路由面临安全威胁和节点能量有限的不足,提出了一种新的安全路由协议R-GEAR。该协议在GEAR路由算法的基础上,引入了信誉评测机制对攻击节点进行检测;并在能耗方面对其加以改进,通过在数据传输时进行数据融合来节约能量。仿真结果表明,在存在攻击节点的情况下,R-GEAR协议比GEAR协议具有较高的包传输率和较低的包丢失率等属性。

关键词:无线传感器网络;网络安全;安全路由;信誉机制;能耗
中图分类号:TP393 **文献标识码**:A **文章编号**:1673-629X(2010)09-0131-05

A Security Routing Protocol Design Based on Reputation Systems in Wireless Sensor Networks

LI Ling, WANG Xin-hua, CHE Chang-ming
(School of Information Science and Engineering, Shandong Normal University, Jinan 250014, China)

Abstract: Wireless sensor networks are different from traditional networks, so traditional secure routing protocols cannot be applied efficiently to them. Therefore, secure routing issues become emergent in wireless sensor networks. To the problems of threat to routing security and limited energy of the nodes in wireless sensor networks, present a new routing protocol named R-GEAR. This protocol is based on GEAR and reputation evaluation mechanisms are added to GEAR to detect attacking nodes; Moreover, improved GEAR in the energy consumption aspect through data aggregation. The simulation result shows that R-GEAR protocol has higher packet delivery ratio and lower packet drop ratio than GEAR protocol while attacking nodes exist.

Key words: wireless sensor networks; network security; secure routing; reputation mechanism; energy consumption

0 引 言

近年来,无线传感器网络[1](Wireless Sensor Networks,简称WSN)在军事、环境、交通、医疗、商业、家庭等各个领域中得到了广泛的应用。随着其应用范围的不断扩展,对其安全性的需求也越来越高。无线传感器网络的拓扑结构动态变化,并且网络中节点具有能量有限、计算能力有限以及存储能力有限等特点,WSN的这些特点使得当前比较典型的安全机制,像INSENS[2]、SPINS[3]等不能有效地应用于无线传感器网络。另外,由于网络自身也存在着一些安全漏洞,这些漏洞可能会引发不同类型的攻击,其中有很多攻击处在路由层,它们可能会影响到网络的使用甚至导致整个网络的瘫痪。所以,如何建立安全有效的路由协议是在无线传感器网络大规模应用之前亟待解决的问题,具有重要的研究价值。

由于无线传感器的节点具有计算能力、存储能力和通信能力等有限的特点,在采取网络安全措施时尽可能避免采用复杂的密码认证算法。文中借鉴信任模型的思想,在路由中引入了节点信誉评测机制,用于判断节点的优劣,并在此基础上针对GEAR的弱点进行了改进,提出了安全路由协议R-GEAR。

1 相关工作

对于安全路由的研究,目前大多数方法都是在现有的路由基础上,通过增加安全机制来提高路由的安全性。文献[2]提出了一种可以防御通过虫洞的重放攻击的安全路由协议INSENS。该协议结合有效的单向散列链去阻止入侵者发起泛洪攻击,内嵌的MACs可以唯一安全地把一个MAC与某个节点、某个路径

收稿日期:2010-01-06;**修回日期**:2010-04-11
基金项目:山东省自然科学基金资助项目(Y2006G19)
作者简介:李 玲(1984-),女,山东临沂人,硕士研究生,研究方向为无线传感器网络;王新华,博士,教授,研究方向为高性能网络技术和路由算法等。

和特定的OHC号相关联,因此可以防御通过虫洞的重放攻击。它的一个重要特点是,允许网络中的恶意节点威胁它周围的少量节点,但是会通过冗余机制将这种威胁限制在一个小范围内,不会对网络造成太大影响。

文献[3]提出了一种目前比较流行、实用的传感器网络安全协议SPINS(Security Protocols for Sensor Network),该协议包括安全网络加密协议SNEP(Secure Network Encryption Protocol)以及基于时间的高效的容忍丢包的流认证协议μTESLA(Micro Timed Efficient Streaming Loss - tolerant Authentication Protocol)两个部分。SNEP协议实现消息完整性和点到点认证,并保证数据机密性和新鲜性;μTESLA协议针对WSN中基站需要向所有功能节点广播数据包,实现了WSN中点到多点的广播认证[4]。SPINS安全协议在数据机密性、完整性、新鲜性、可认证等方面都作了充分的考虑,对路由信息的传输提供了一定的保护,但是没有有效地解决密钥管理问题和对传感器节点的访问控制问题。

RFSN[5]是针对不良节点提出的一种联合声誉机制。该声誉机制拥有一个检测模块和一个声誉模块,包括:直接声誉值(由观察者通过直接观察得到)、间接声誉值(由其它节点报告得到)。利用相关策略将这些机制联合起来计算出节点的声誉值,以此来预测节点下一步的行为,从而决定是否与其合作。

EOSR[6]是一种基于能量优化的安全路由算法。该算法通过预置公私密钥对,提高了路由的安全性;同时让能量储备较多的节点承担较多的数据转发任务,可以有效地延长网络生命周期。此外,还有一些安全路由协议,如基于位置的安全路由协议GPSR[7]、基于可信度的路由协议[8]等。

这些路由协议采用不同的安全机制来抵御攻击,在安全性、复杂性和能耗等多个方面之间寻求平衡。因此,研究一种既能抵御各种攻击又适用于资源受限的无线传感器网络的安全路由技术,是一项有挑战性的任务。文中给出了一种节点信誉评价机制,来判断节点的好坏,并在此基础上提出了一个全新的基于信誉机制的安全路由协议R-GEAR。

2 信誉机制评价模型的建立

文中借鉴文献[9]提出的用于移动自组网中节点的信誉评价的思想,针对无线传感器网络的特点对其加以改进,提出了适用于无线传感器网络的信誉机制评价模型。

在无线传感器网络中通常用一个交互的分布式信誉系统实现信誉机制,在这个系统中的每个节点都参与评价其他节点的信誉值。在文中的模型中,每个节点中都包含一个信誉值列表(Reputation List,RL),节点用该信誉值列表保存自己对其他节点的信任度的评价。RL基本结构如表1所示。

表1 节点信誉值列表

NodeID	SR	ER	CR	△CR
NodeID	SR	ER	CR	△CR
.....	.....	.....	.....	.....
NodeID	SR	ER	CR	△CR

在这个信誉值列表中,每个节点的信息包括:NodeID,SR,ER,CR,△CR。其中,NodeID为节点编号;SR(Subjective Rating)为节点的主动监测信誉值;ER(Exchanging Rating)为节点的交换信誉值,即节点从另一个节点处获得的其他节点的信誉值;△CR(Credit Rating)指被评价节点信任度值的改变量;CR指节点对其他节点的信任度,它是节点根据SR和ER的值,对被评价节点做出的一个信誉评价的联合值,计算公式为:

$$CR = W_1 * SR + W_2 * ER \quad (1)$$

其中,$W_1 + W_2 = 1, W_1 > W_2$

W_1代表主动观测值SR的权值,W_2代表从其他节点得到的经验值ER的权值。从直觉上讲,与从其他节点处获得的交换信誉值相比,节点通过直接观测获得的信誉值应该具有更高的权重。

2.1 SR的计算与更新

每个节点对已知节点的SR值初始化为0.5。SR值是通过节点对其邻居节点进行监控获得的,节点打开监控模式,利用监测机制,对其邻居节点进行监控。根据不同的侧重点,对节点的不同功能(如丢包率、吞吐量等)进行监测,获得被监测邻居节点的监测信誉值。

由于使用监控模式,故节点i在向其邻居节点j发送包之前会复制此数据包,并将其保存在缓存中。一定时间内,如果节点i收到节点j发来的已经将数据传输出去的报告,节点i就从缓存中删掉该副本,认为该包被正常传输;若经过一段时间,缓存中还存在着该副本,则认为该包在经过节点j传输时发生了错误。

为了便于表述,做如下符号和定义:

U表示$\triangle T$时间内节点发包的总次数;R表示$\triangle T$时间内节点发包的出错次数;n表示节点的攻击次数,初始值为0;$T_\triangle T$表示事先确定的错误率门限值;V_1表示给正常节点的SR增加的一个变化值;V_2表示使攻击节点的SR指数下降时用到的一个参数

值。

定义:$\triangle T$ 时间内节点发包出错次数与发包总数的比值称为节点的错误率 WR(Wrong Rating),计算公式为:$WR = R/U$。

一旦监测到节点 j 发包出错,就开始统计在一段时间 $\triangle T$ 内节点 j 的发包情况。如果节点 j 在 $\triangle T$ 时间内被使用了 U 次,其中发包出错 R 次,就可以根据公式 $WR = R/U$ 计算 $\triangle T$ 内节点 j 的错误率 WR。

根据 $T\_\triangle T$ 的值,判断节点 j 是不是正常节点。若 WR 没有超过 $T\_\triangle T$,则视为网络正常拥塞问题,认为 j 是正常节点,对其进行奖励。SR 线性增加,每次增加一个变化值 V_1,即 $SR = SR + V_1$,然后将攻击次数 n 减 1。若 WR 超过了 $T\_\triangle T$,就可以认为节点 j 具有攻击倾向,为了表示对节点 j 的惩罚,将攻击次数 n 加 1,并使节点 j 的 SR 值随着 n 的增加而呈指数下降,即 $SR = SR - 2^{n-1} * V_2$。在这里,V_2 的值要适当大于 V_1 的值,$\triangle T$ 和 $T\_\triangle T$ 的值根据网络情况和包传输量而定。若 $\triangle T$ 太大,则容易增加误判率,若 $\triangle T$ 太小,则不易检测出异常节点。

2.2　ER 的计算与更新

交换信誉值 ER 是节点从另一个节点处获得的其他节点的信誉值,每个节点对已知节点的 ER 值初始化为 0.5。当节点从其他节点收到信息交换包 MEP 时进行 ER 的更新。对 ER 的值采用触发式更新。

为了便于表述,做如下记号和定义:

$\triangle CR$ 表示 $\triangle$ T 时间内被评价节点信任度值的改变量;$\triangle all\_CR$ 表示每次变化的 $\triangle CR$ 值的累加和,即 $\triangle all\_CR = \triangle all\_CR + \triangle CR$;MEP(message exchange packet)表示信息交换包;$T\_\triangle CR$ 表示事先设定的门限值。

当节点 i 对节点 j 的 SR 改变以后,通过公式(1)计算出节点 i 对节点 j 的信任度值的改变量 $\triangle CR$ 和总的改变量 $\triangle all\_CR$。当 $\triangle all\_CR$ 超过 $T\_\triangle CR$ 时,广播信息交换包 MEP(广播后 $\triangle all\_CR$ 置 0)。如果节点 i 收到节点 j 发来的 MEP 包,则它先对节点 j 的可信度进行评价。评价方法是:根据节点 i 的信誉值列表中的 SR_{ij} 和 ER_{ij} 值,利用公式(1)计算 CR_{ij}。若 CR_{ij} 小于事先确定的门限值 T_CR_{ij},那么节点 i 认为节点 j 是不可信的,丢弃该 MEP 包;若 CR_{ij} 大于事先确定的门限值 T_CR_{ij},那么节点 i 认为节点 j 是可信的,按公式(2)更新 ER:

$$ER_{ik} = ER_{ik} + (CR_{jk} - ER_{ik}) * CR_{ij} \qquad (2)$$

其中,节点 i 为待更新其他节点 ER 值的节点,节点 j 为向 i 发送更新信息的节点,节点 k 为节点 i 要更新其 ER 的节点。ER_{ik} 表示其他节点传递给节点 i 的关于节点 k 的评价值,CR_{ij} 表示节点 i 对节点 j 的信誉评价值。

2.3　基于信誉机制的评价模型流程图

基于信誉机制的评价模型流程图如图 1 所示。

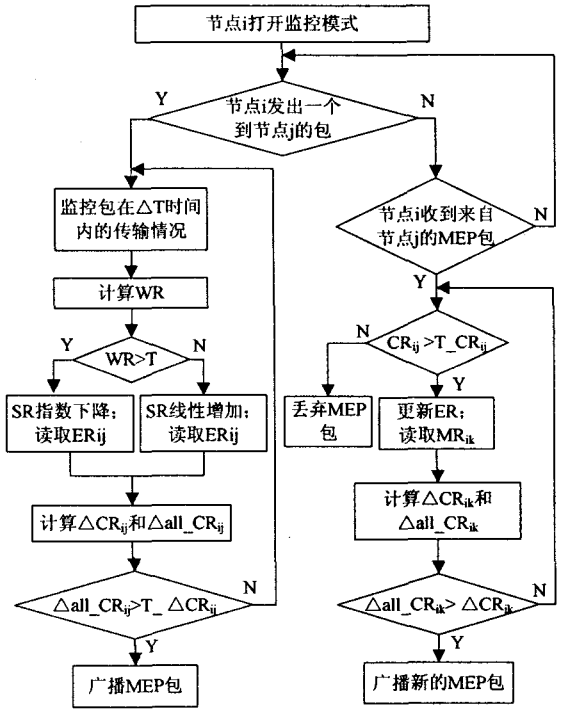

图 1　基于信誉机制的评价模型

3　R－GEAR 协议

3.1　GEAR 路由协议

文献[10]提出了 GEAR(Geographical and Energy Aware Routing)路由协议,该协议在向目标区域散布查询消息的同时考虑了地理位置信息的使用。GEAR 协议的主要思想是利用位置信息,使得"兴趣"只传播到目标区域,而不是传播到整个网络[11]。将查询消息传播到目标区域的所有节点分为两个阶段:

(1)将查询消息发送到目标区域:从 Sink 节点开始的路径建立过程采用贪婪算法[11]。如果节点存在到事件区域的路由代价比自己的小的邻居节点时,则从这些邻居节点中选择路由代价最小的作为下一跳节点;如果节点的所有邻居节点到事件区域的路由代价都比自己的大时,则陷入路由空洞,这时可以使节点在邻居节点中选择到事件区域代价最小的节点作为下一跳节点,并将自己的路由代价设为该节点的一跳通信代价加上该下一跳节点的路由代价。

(2)在目标区域内传送查询消息:如果事件区域内节点密度比较大,则采用递归的、基于地理信息的转发方式;而节点分布较稀疏时,采用泛洪方式路由转发效率更高。这两个阶段完成后,事件区域中的节点采集

的数据沿查询消息的反向路径传送到 Sink 节点。

3.2 R-GEAR 中 Sink 点到目标区域的路由

这个过程建立在上一小节的信誉评测模型的基础上。在进行路由选择时,同时考虑邻居节点到事件区域的代价及其信誉值两个方面,下面的公式(3)综合了这两个方面的因素,节点 N 根据此公式来计算 RC(Reputation Cost) 的值,选择 RC 值最大的邻居节点作为下一跳节点。

$$RC(N_i,R) = \alpha \frac{1}{h(N_i,R)} + (1-\alpha)CR_{NNi} \quad (3)$$

其中,α 是可调权值,其取值范围是[0,1];CR_{NNi} 是节点 N 对其邻居节点 N_i 的信任度;$h(N_i,R)$ 是节点 N 的邻居节点 N_i 到事件区域 R 的代价,取 $\frac{1}{h(N_i,R)}$ 是为了纠正 $h(N_i,R)$ 与 CR_{NNi} 及 $RC(N_i,R)$ 物理意义上的反向性。当尚未建立从 Sink 点到事件区域的代价路径、节点 N 没有关于节点 N_i 的 $h(N_i,R)$ 时,若没有路由空洞,则计算 $h(N_i,R)$ 采用如下公式:

$$h(N_i,R) = \beta d(N_i,R) + (1-\beta)e(N_i) \quad (4)$$

其中,β 是可调权值;$d(N_i,R)$ 是节点 N_i 到事件区域 R 的距离;$e(N_i)$ 为节点 N_i 的剩余能量。当发生路由空洞时,取 $\alpha = 1, \beta = 1$,即采用纯地理路由绕过路由空洞。

3.3 R-GEAR 目标区域内路由

由于无线传感器网络中的节点能量有限,所以如何有效地节省能量成为无线传感器网络的一个重要问题,即传感器网络的低能量特点使节能成为路由协议最重要的优化目标[12]。在数据传输时进行数据融合,减少数据传输量,可以达到节约能量的目的。数据到达目标区域后,采用迭代地理转发机制(节点密度大的情况)或洪泛转发机制(节点密度小的情况)。在迭代地理方式中采用数据融合时,直接以区域中心节点作为数据融合节点即可;对于洪泛方式,采取如下方案:

(1)在事件区域内选出一个能量大于设定的能量阈值、位置在事件区域内而且能对数据进行相应处理的节点作为簇首节点;当选定簇首节点后,对网络中其它节点进行广播,广播数据包中含有该节点成为簇首节点的信息。

(2)簇内节点将采集的数据传送给簇首节点,由簇首节点对这些数据进行压缩整合,除去冗余数据后传送给第一个接收这些数据的节点;

(3)以时间间隔 T 为周期,将在[0,T] 时间内收到的数据缓存起来,在下一个时间间隔内对这些数据进行整合并转发。

在理想的融合情况下,簇首节点可以把 m 个长度相等的输入数据分组合并成一个等长分组,传输这个分组只需消耗不进行融合时所需时间的 $1/m$;最坏的情况下,融合后不能减少传输数据,但减少了所需传输的分组个数,从而可以降低信道的协商或竞争过程所带来的能量开销。所以在数据传输时进行数据融合,可以减少通信次数,降低通信开销。

4 R-GEAR 仿真实验

4.1 仿真环境及性能参数

根据 GEAR 路由协议以及一些 WSNs 的相关文献的实验场景设置,文中在 500m * 500m 的范围内随机放置 20 个节点。其中一个 Sink 节点不停地向目标区域发送兴趣数据包,传感器节点发送相应数据包,兴趣数据包和相应数据包的长度分别为 32 字节和 64 字节。每个节点的通信范围是 100 个单位,目标区域是一个半径为 50 个单位的圆形区域,传输带宽为 2M。设节点初始能量为 2J,发送和接收一个数据包消耗 0.001J,总模拟时间为 600s。每个节点对已知节点的 SR、ER 值均初始化为 0.5。

在对 R-GEAR 的模拟实验中,分三种情况进行测试:网络中存在 1 个内部攻击节点、网络中存在 2 个内部攻击节点、网络中存在 3 个内部攻击节点。攻击方式为:攻击节点收到数据包后并不对其进行转发,而是将其丢弃。

为了比较存在内部攻击节点时 GEAR 协议与 R-GEAR 协议的性能,使用下列性能参数进行评价:

(1)包传输率(Packet Delivery Ratio)。

网络中所有目的节点收到的数据包数量之和与源节点发出的数据包总数的比值。

(2)包丢失率(Packet Drop Ratio)。

内部攻击节点丢弃的数据包总数与源节点发出的数据包总数的比值。

4.2 模拟结果及性能分析

在下面的图中,用 GEAR(i)、R-GEAR(i) 分别表示网络中存在 i 个内部攻击节点时 GEAR 协议的性能曲线和 R-GEAR 协议的性能曲线。图 2、图 3 分别给出了网络中存在内部攻击节点时 GEAR 协议和 R-GEAR 协议在包传输率、包丢失率方面的比较。

从图 2 可以看出,随着时间的增加,GEAR(1)、GEAR(2)和 GEAR(3)的包传输率逐渐降低,当攻击节点数达到 3 个时,GEAR 的包传输率下降到 33%左右,这是因为网络中存在的内部攻击节点对接收到的包不进行转发而是将其丢弃。而在 R-GEAR 中却有不同的情况产生,R-GEAR(1)、R-GEAR(2)和 R-GEAR(3)的包传输率先是随着时间的推移逐渐降低,200s 后开始逐渐上升。之所以出现这种情况,是因为

在 R－GEAR 中引入了信誉评测机制,在选路时将节点信誉值作为其中的一个考虑因素。内部攻击节点信誉值会不断降低,随着信誉值的降低它被选为下一跳节点的几率也不断降低,逐渐被排除在传送数据包的路径之外,从而使得包传输率有所上升。从图中可以看出,当存在内部节点时,R－GEAR 包传输率比 GEAR 高 25%左右。

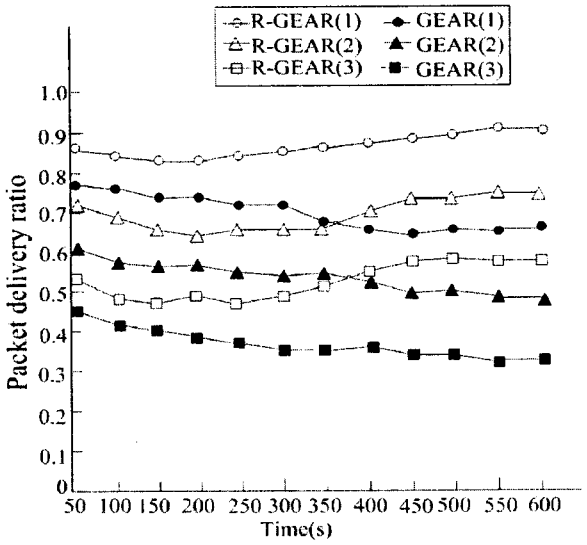

图 2　GEAR 与 R－GEAR 协议包传输率的比较

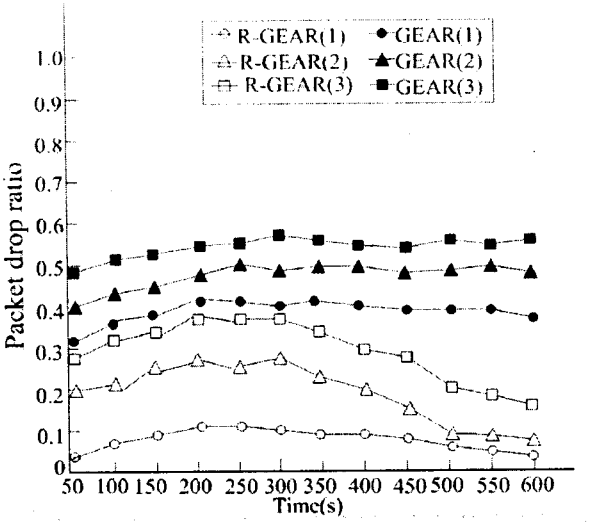

图 3　GEAR 与 R－GEAR 协议包丢失率的比较

从图 3 可以看出,随着内部攻击节点数目的增加,丢包率不断增大。当有 1 个攻击节点时,GEAR 协议中丢包率在 38%左右,当攻击节点数达到 3 个时,GEAR 协议中丢包率高达 55%左右。而在 R－GEAR 中,存在 1 个攻击节点时,丢包率为 15%左右,当攻击节点数达到 3 个时,丢包率占 35%左右。由此可以看出,R－GEAR 协议的丢包率比 GEAR 协议的丢包率小很多,之所以产生这种差别,是因为在 R－GEAR 中用节点信誉值这一因素将大部分内部攻击节点排除在网络之外,对内部攻击节点的使用明显减少。

从以上的模拟实验结果可以看出,网络中存在内部攻击节点时,R－GEAR 在包传输率和包丢失率方面都比 GEAR 好,R－GEAR 协议比 GEAR 协议具有更好的性能。

5　结束语

文中在 GEAR 基础上引入了信誉评测机制和密钥机制,并对 GEAR 的选路策略加以修改,提出了 R－GEAR 安全路由协议。仿真实验表明,该协议的路由安全性较高,比 GEAR 路由协议具有更好的包传输率和包丢失率等属性。

参考文献:

[1] 任丰原,黄海宁,林　闯.无线传感器网络[J].软件学报,2003,14(7):1282－1290.

[2] Deng J, Han R, Mishra S. INSENS: Intrusion－Tolerant Routing in Wireless Sensor Networks[R]. Colorado: Department of Computer Science, University of Colorado, 2002.

[3] Perrig A, Szewczyk R, Wen V, et al. SPINS: Security Protocols for Sensor Networks[J]. Wireless Networks Journal, 2002, 8(5):521－534.

[4] 彭志娟,王汝传,孙力娟.无线传感器网络 SPINS 安全协议分析与改进[J].无线通信技术,2007,16(1):14－21.

[5] Ganeriwal S, Srivastava M. Reputation－based framework for high integrity sensor networks[C]//In: Proc. of the 2nd ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN 2004). New York: ACM Press, 2004:66－77.

[6] 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.

[7] Karp B, Kung H. GPSR: Greedy perimeter stateless routing for wireless networks[C]//In: Proc. of the 6th Annual Int'l Conf. on Mobile Computing and Networking. Boston: ACM Press, 2000:243－254.

[8] 王　潮,贾翔宇,林　强.基于可信度的无线传感器网络安全路由算法[J].通信学报,2008,29(11):105－112.

[9] 王建新,张亚男,王伟平,等.移动自组网中基于声誉机制的安全路由协议设计与分析[J].电子学报,2005,33(4):596－601.

[10] Yu Y, Govindan R, Estrin D. Geographical and Energy－Aware Routing: A Recursive Data Dissemination Protocol for Wireless Sensor Networks[R]. California: UCLA Computer Science Department, 2001:1－23.

[11] 赵海霞.无线传感器网络 GEAR 协议的一种改进方案[J].传感器与微系统,2006,25(9):61－63.

[12] 储昭勋,胡艳军.无线传感器网络技术[J].计算机技术与发展,2006,16(4):64－66.