软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2011,22(Suppl.(1)):111−121

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel/Fax: +86-10-62562563

一种基于无线传感器网络的防盗技术*

段金晟, 郭龙江+, 刘 勇, 朱敬华

(黑龙江大学 计算机科学技术学院,黑龙江 哈尔滨 150080)
(黑龙江省数据库与并行计算重点实验室,黑龙江 哈尔滨 150001)

Anti-Theft Technology Based on Wireless Sensor Network

DUAN Jin-Sheng, GUO Long-Jiang+, LIU Yong, ZHU Jing-Hua

(Department of Computer Science and Technology, Heilongjiang University, Harbin 150080, China)
(Key Laboratory of Database and Parallel Computing of Heilongjiang Province, Harbin 150001, China)
+ Corresponding author: E-mail: longjiangguo@gmail.com

Duan JS, Guo LJ, Liu Y, ZHU JH. Anti-Theft technology based on wireless sensor network. ***Journal of Software***, **2011,22(Suppl.(1)):111−121.** http://www.jos.org.cn/1000-9825/11012.htm

Abstract: There are shortcomings in traditional anti-theft technology which can not satisfy a user's demand. The common ways of anti-theft are limited in wireless sensor networks. On the topic of the shadowing effect in wireless communication, this paper introduces a anti-theft technology based on wireless sensor networks. System can check intrusion by analyzing received signal strengths. This paper establishes a framework of anti-theft system and studies the key technologies. By defining the graph model in anti-theft system, the agent distribution problem is abstracted into edges partitioned by vertices problem. B-EPV algorithm is proposed for obtaining the optimal solution. Blade algorithm is designed for solving *k*-mode set problem to get steady status of link. This paper constructs experimental environment with real motes and verifies the performance of the system. The result shows low false positives and false negatives in the system.

Key words: wireless sensors networks (WSN); anti-theft technology; shadowing effect; edges partitioned by vertices problem (EPVP); *k*-mode set problem

摘 要: 传统防盗技术存在诸多弊端,无法满足防盗需求.无线传感器网络的常规防盗方式也有着无可避免的局限性.根据无线通信的阴影效应提出一种基于无线传感器网络的防盗技术,通过接收信号强度的变化判断盗贼的入侵.建立了防盗系统的框架,并对其中的关键技术进行研究.通过定义防盗系统的图模型,将代理分配问题抽象为顶点分边问题,并提出 B-EPV 算法求优化解.设计 Blade 算法求解 k-众数集问题,以获得稳定的 RSSI 值范围.搭建了真实实验环境,验证了防盗系统的性能.实验结果表明,系统具有较低的误报率和漏报率.

关键词: 无线传感器网络;防盗技术;阴影效应;顶点分边问题;*k*-众数集问题

科学技术的飞速发展,推动了人们对于安防理念重视的逐渐加大.无线传感器节点体积小、功耗低,属于微型单片机,具有感知自然界物理量和无线通信的功能,人们将其应用于防盗领域十分方便.

* 基金项目: 国家自然科学基金(61033015, 60803015, 61070193); 中国博士后基金(20080430902); 黑龙江省教育厅重点项目(1154Z1001); 黑龙江省博士后基金(LRB08-021); 哈尔滨青年科技创新人才基金(2008RFQXG107); 黑龙江省教育厅项目(11551343)

收稿时间: 2011-05-02; 定稿时间: 2011-07-29

传统防盗方法可以使用摄像头、传感报警器、红外线设备等,但这些传统方法都有局限性,例如摄像头具有观测不到的死角,红外线对物体的穿透性差.使用无线传感器网络进行防盗,传统的方法大致分为:感知光强、震动、距离的变化[1]和红外.根据常规物理量的变化判断某种非法行为的发生,受环境干扰严重.若仅对某一物理量进行判断,则只能适用于少有的几种应用,效果并不理想.

根据无线电波的空间传播特性,如果有物理介质(障碍物或者人)进入通信双方的传输范围内,接收信号强度表现为明显变化,变化程度根据物理介质类别而定.通过判断变化程度,我们可以检测到在监测区域内是否有入侵者.选择无线电波进行防盗的依据是无线电波的频率较高,具有较好的穿透性,不受室内障碍物的影响.另外,传感器节点在使用时可以被隐藏起来.如果我们将传统防盗方式称为显式防盗,则使用无线电波的方式可称为隐式防盗.将节点置于墙壁、家具内部,从外观上看整个系统是不可见的,即隐式防盗系统,解决了基于显式防盗方式的一个缺点——设备易被不法分子发现和破坏.

鉴于当前防盗技术的弊端,本文提出隐式防盗系统的整体解决方案.基于电磁波的特性,建立了基于图的防盗模型和基于无线传感器网络的防盗系统的框架;提出了顶点分边问题和 k–众数集问题,并设计 B-EPV 和 Blade 算法对问题进行解决.本文采用真实节点对系统进行了实现,实验结果表明,误报率和漏报率很低,该系统可以应用于需要较高安全系数的监控环境中,例如博物馆等面积较大的空旷场所.

本文第 1 节为防盗技术的相关研究.第 2 节介绍预备知识和防盗模型.第 3 节建立防盗系统的框架,分别阐述了代理的分配、节点同步、稳态确定和对于异常的处理.第 4 节在真实环境下进行实验并分析了实验结果,最后对全文进行总结.

1 相关研究

目前无线传感器网络领域中防盗技术主要是基于传统意义上的防盗,尚未检索到有文献指出传感器网络防盗技术的整体框架.传统防盗以摄像头的使用居多,此外使用标签式防盗也相当常见,例如超市或书店都允许顾客携带背包入场,管理者主要依据商品上面贴有类似 RFID 的传感贴或磁性条,在顾客出门的时候判断顾客身上有无未结账商品.无线传感器防盗并不常见,原因一是传感器网络技术应用技术尚未成熟,二是目前本领域研究的范围只限于传统意义上的防盗:感知光强、震动、距离.这些被监测对象都属于系统内部的成员(节点和与节点相连的设备等),对于外界行为的感知能力差,而且不成体系,无法大范围推广使用.

宾夕法尼亚州立大学曹国宏的车辆防盗系统[1],主要是基于判断节点间距离与其链路 RSSI 的关系.车辆泊于停车场,停车场设有基站(BS),车辆内设有传感器节点.车辆进场注册,离开停车场后注销.如果有非法分子将车开走,此过程未经过合法注销,且基站发现车辆从停车场移动出去(根据 RSSI 判断),基站将报警.系统可以应用于同类的几种场所,可是传感器节点需要在车辆内预设,并且不属于室内防盗,这样在通用性上会大打折扣.

圣母大学 Woyach[2]使用 MICA2 和 MICAz 节点,在传感器网络基于 RSSI 感知移动目标领域内做了首次研究并得出结论,当发射机和接收机传输数据时,如果不携带节点的人进入无线传输区域(通常是视距[3],LOS)时,接收机得到的信号强度会发生某种变化,人作为系统外的角色会被系统监测出来.

犹他大学 SPAN 实验室的 Palwari 和 Wilson 基于 Woyach 的实验以及电磁波的一些特性,开发了穿墙定位系统[4].虽然存在误差,但是定位效果还是可以让用户接受.他们对于一个屋子使用了 34 个节点,如果应用于防盗,成本是一个很大的问题.同时,Wilson 使用了复杂的数学模型,完全集中式的系统使得传感器节点和整体网络的工作效率下降,网络数据拥塞.他们没有提出防盗的概念及框架.防盗的关键在于报警的及时与正确,至于定位,开销未免过大.

2 防盗技术模型

先介绍预备知识,这是本文设计防盗系统的主要理论依据,接着介绍防盗监测问题如何演化为抽象的图模型.

2.1 无线通信及阴影效应

无线通信过程至少需要一个无线发射机和一个无线接收机,发送方通过天线将无线信号以电磁波的形式发射到空间,形成一个空间球体[3]向外扩张.当这个具有一定能量(发射功率)的电磁信号撞击在接收机天线上的时候,这个信号会被接收机所接收.接收机可以感知到这个信号的强度,其值称为接收信号强度指标(received signal strength indicator,简称 RSSI).这个值可以被理解为发射功率与衰减能量之差,用单位 dBm 表示,可以由以下方式[4]来表示这个强度:

$$RSSI(dBm) = P - L - S - F - V \tag{1}$$

其中,P 表示发射功率,L 表示距离、天线等能量损失,S 表示阴影效应造成的能量损失,F 指窄带多径环境的干扰,F 表示噪声.从公式中可以看出,发射功率经过一系列做差之后,剩下的能量就是我们所说的 RSSI.

传感器节点在无线通信的过程中,传输区域可以被视为一个椭球体[4],焦点分别为发射机和接收机.当障碍物通过传输区域的时候,会产生阴影效应.阴影效应是由发射机和接收机之间的障碍物造成的,这些障碍物通过吸收、反射、散射和绕射等方式衰减信号功率,严重时甚至会阻断信号[5].本文在验证实验中发现, RSSI 变化程度与信号是否穿墙、发送机与接收机的距离、周围环境及入侵行为的物理介质等都有着紧密的关系.

本文进行一次验证实验,#07(节点编号)不断向#08 发送数据包,当#08 收到#07 的数据包的时候,获得其 RSSI 值,并传回基站.基站可以显示出一条曲线, x 轴为时间, y 轴为 RSSI 值,如图 1 所示.当#07—#08 链路中有人出现的时候,其 RSSI 曲线有相应的波动.图中曲线的 2 个波谷是由于人 2 次穿越传输区域的行为造成的.本文主要根据阴影效应的原理,建立防盗系统的模型.

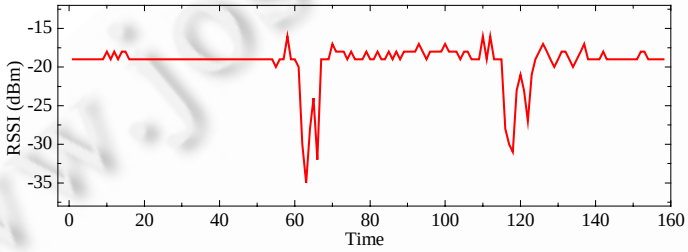


Fig.1 Shadowing effect in wireless communication

图 1 无线通信的阴影效应

2.2 简单模型

此模型由 3 个节点组成,依次为 A,B 和 BS(Base Station, sink 节点).布局如图 2 所示,BS 与 PC 机相连,A 不断地向 B 发送数据包.B 接收到来自 A 的数据包后,将 AB 这条链路的 RSSI 值封包发送给 BS.PC 机上装有 GUI(图形用户界面,Graphical User Interface)程序,当链路 AB 的 RSSI 值发生变化的时候,GUI 程序会显示出 RSSI 的波动情况.

2.3 集中式模型

集中式模型可以视为多个简单模型的累加.该模型含有 m 条链路,共 $2m$ 个节点和 1 个 BS.布局如图 3 所示,该例是 4 个简单模型的累加.

从图 3 中可以看到,链路 1234 的 RSSI 可以被#02、#04、#06 和#08 传送到 BS,进而显示在 GUI 程序上.1234 链路上的无线传输是必要的,因为我们要得到其链路 RSSI 值,但是链路 5678 是不必要的,原因是:

(1) 不一定要在 GUI 程序里时刻观察 1234 链路的状态,可以将这些链路的 RSSI 值保存在#02、#04、#06 和#08 节点中,当链路 RSSI 发生异常时,#02、#04、#06 和#08 才向 BS 报告.

(2) 集中式模型中,每增加一个简单模型,都要额外增加一个向 BS 传输的过程,即每次观察一个被检测的链路,要增加 2 个节点,这种开销很大.

所以,在设计布局及任务分配中不使用集中式模型.鉴于集中式模型的缺点,本文提出代理的概念.

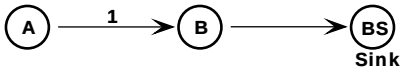


Fig.2 Simple model

图 2 简单模型

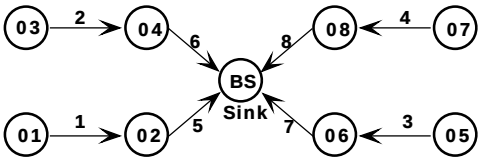


Fig.3 Centralized model

图 3 集中式模型

定义 1(代理). 一个链路的代理是一个节点,这个节点记录并监控该链路的 RSSI 值,发现异常时向 BS 报告.对于需要被监控的链路 a 来说,一定有且只有一个代理来对链路 a 进行监控.一个节点可以代理多条链路的监控工作.节点 A 对其代理链路的另一端的节点感兴趣.

由代理定义得知,当节点 A 代理链路 a 时,节点 A 应该是链路 a 的一个端点.

2.4 图模型

在实际应用中,确定节点个数与布局的方法是:在监控区域 S 内根据情景需要设置出一些感兴趣的子区域,这些子区域可以抽象成为线段,即需要被监测的链路.我们把这些线段的端点设置成为传感器节点,各节点间进行通信.根据设置的节点与链路,模型进而被抽象成一个无向图 $G.G$ 包含 n 个顶点和 m 条边, n 为传感器节点数, m 为被监控的链路数,如图 4 所示,n=5, $m=8$.

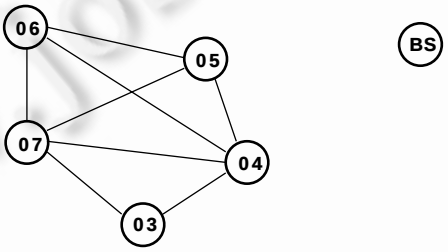


Fig.4 Graph model

图 4 图模型

现在我们已经有了代理的概念,对于每一条链路 a 都要找到一个代理节点.如果#06 代理链路(04,06)但不代理链路(03,06),#06 收到来自#04 的数据包后要对该链路 RSSI 进行分析;而#06 收到#03 的数据包后,检查出#06 对#03 不感兴趣,则将收到#03 的数据包丢弃.

3 防盗系统框架

在前面介绍的数学模型基础之上,接下来将要设计防盗系统的框架.如图 5 所示,用户操控一个连有 BS 的 PC 机,GUI 程序在 PC 机上运行.明确了代理的任务分配后,用户通过 GUI 程序手动绘制实验布局,输入系统参数,将这些数据下发到代理节点.代理节点主要包含 3 种机制:适应过程、节点同步和 OM 算法.适应过程的目的是确定稳态;节点同步保证节点间无冲突通信;对异常的处理使用 OM 算法.本文将在此框架内设计防盗系统.

系统的工作流程分为 3 个阶段:参数设置、适应过程、监视链路.用户启动 GUI 程序后,通过手动绘制添加实验拓扑及节点间关系,输入相应参数.PC 机通过 BS 将信息下发到代理节点.适应过程:代理节点开始按照兴趣表的顺序进行时间同步,依次发送数据包;当每个代理节点对于其代理的每个链路都收集到 M 个 RSSI 样本后结束适应过程,运行 Blade 算法确定稳态.监视链路:代理节点继续按照兴趣表的顺序依次发送数据包,且每一个代理节点都要使用 OM 算法分析其得到的链路 RSSI 值,监控其感兴趣的链路,检查链路是否出现异常.若发现异常,则在下次广播数据的时候将警报传送给 BS.若某代理对于链路 AB 报警,则报警数据包含有链路 AB 的信

息,GUI 程序会以图形的方式显示出边 AB 处存在异常,并发出警报声通知用户.

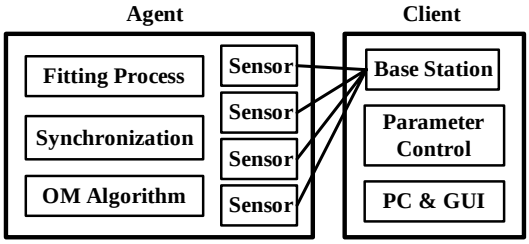


Fig.5 Framework of anti-theft system

图 5 防盗系统框架

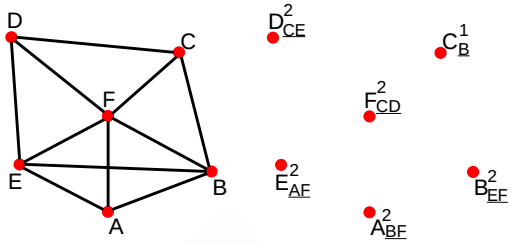


Fig.6 An example of EPVP

图 6 顶点分边问题的一个实例

3.1 代理的分配: 均衡的顶点分边问题

通过前面介绍的图模型和代理的概念,可知问题已被抽象成无向图的形式.但是哪些节点作为代理,而这些节点代理哪些链路呢?为了保证用户感兴趣的链路监控任务平均分配给所有节点,使得各节点之间的任务量尽可能均衡,本文提出顶点分边问题:一个无向图 G,定义所有顶点与边的归属关系——对于其中某一条边 AB,边 AB 只能从属于顶点 A 或顶点 B 的其中一个,任一顶点不能从属于某条边.

图 6 是顶点分边问题的例子:左边的图是输入 G,右边是输出.顶点 F 右上方的数字表示 F 有 2 个从属于自己的边;F 右下方的字母表示边 FC、边 FD 从属于自己,亦表示 F 对 C、D 感兴趣.下面给出一些符号的定义.

Table 1 Symbol definition

表 1 符号定义

无向图	顶点数	边数	顶点度	分边均值	v_i 已分到的边数	G 当前边数
$G=(V,E)$	$n=\|V\|$	$m=\|E\|$	d_i(变量)	$\varphi=m/n$	w_i(变量)	e(变量)

定义 2(顶点分边问题,edges partitioned by vertices problem,简称 EPVP).输入:一个无向图 G.输出:一个 G 中边集的划分 $\varepsilon=(\varepsilon_1,\ldots,\varepsilon_n)$,$\varepsilon$是 EPVP 的解.其中 ε_i 是一个边集,表示顶点 v_i 分到的边,满足 $|\varepsilon_i|\leqslant d_i$, $\sum_{i=1}^{n}|\varepsilon_i|=m$,$\varepsilon_i$ 中任意一边的某端点是 ε_i.

定义 3(EPVP 的可行解). $\varepsilon'=(\varepsilon'_1,\ldots,\varepsilon'_n)$ 是 EPVP 的可行解,满足: $\min\sum_{i=1}^{n}\left(|\varepsilon'_i-\varphi|\right)^2$.

$\varphi=m/n$ 称为分边均值,即理想情况下每个节点平均得到边的个数.在图 6 中 $\varphi\approx1.83$,令 $y(\varphi)=\sum_{i=1}^{n}\left(|\varepsilon_i|-\varphi\right)^2$ 是一个关于 φ 的函数,$y(\varphi)$表示图 G 分边情况与均值的总体偏差,φ为总体分边情况的均值.对 $y(\varphi)$取导数,令 $y'(\varphi)=-2\sum_{i=1}^{n}\left(|\varepsilon_i|-\varphi\right)=0$,得 $\varphi=m/n$.又因 $y''(\varphi)\big|_{\varphi=m/n}>0$,当 $\varphi=m/n$ 时 $y(\varphi)$有最小值.

定义 4(EPVP 的可行因子). 设 ε'是 EPVP 的可行解,对于 $i\neq j$,当 $d_i\leqslant d_j$ 时,有 $|\varepsilon'_i|\leqslant|\varepsilon'_j|$,称$(i,j)$为 ε'的一个可行因子.令 ε''是同输入的 EPVP 的另一可行解,若 ε''的可行因子数大于 ε'的可行因子数,称 ε''比 ε'具有更强的可行性.

定义 5(EPVP 的优化解). $\varepsilon=(\varepsilon_1,\ldots,\varepsilon_n)$是 EPVP 的优化解,首先 ε是 EPVP 的可行解,并且 ε满足:对 $\forall i\neq j$,当 $d_i\leqslant d_j$ 时,$|\varepsilon_i|\leqslant|\varepsilon_j|$.$\varepsilon$可行因子数为 C_n^2.

使用 B-EPV 算法,可求得 EPVP 的优化解.算法 1 中 v_i 原始度为 G 初始化时的 d_i,算法开始后 d_i 是变量.每次将边(v_i,v_j)分给 v_i 时,w_i++,边(v_i,v_j)被删除,图 G 中边数 e––,所以图 G 在算法计算的过程中是变化的,变化包括 d_i,和 e.算法在每次外层循环的开始部分选出 V_i 集合,从中随机选出 v_i.在 v_i 邻居集合 N_i 中选出 *Temp* 集合.通过贪心法确定分给 v_i 的边数 $r(r=|\varepsilon_i|)$,从 *Temp* 中取 r 个点与 v_i 形成边分给 v_i.再将 *Temp* 中剩余的点与 v_i 形成边,分给 *Temp* 中这些剩余的点.通过 B-EPV 算法求得优化解,可以获得代理任务量的平均分配.

算法 1. B-EPV 算法,均衡分边算法.

输入:无向图 $G=(V,E)$.

输出:n 个三元(v_i,ε_i,w_i)组.

初始化:$e=m$,对于$\forall i$ 有 $w_i=0,\varphi=m/n$.

WHILE $e>0$ **DO**

1 选出 G 中具有非 0 最小度的顶点集合 V_i

2 保留 V_i 中原始度最小的那些顶点

3 从 V_i 中随机选出一个顶点 v_i

4 找到令$(w_i+r-\varphi)^2$ 最小化的最大整数 $r,r=\min\{r,d_i\}$

5 选出集合 N_i,N_i 是 v_i 邻居顶点集 **WHILE** $r>0$ **DO**

6 选出 N_i 具有最大顶点度的子集 *Temp*

7 从 *Temp* 中随机选出一个顶点 v_j

8 将边(v_i,v_j)分给 v_i

9 更新 N_i,r--

END WHILE

10 对于所有 $v_k\in N_i$,将边(v_i,v_k)分给 v_k

END WHILE

引理 1(分边与原度的保序性). 假设ε为 B-EPV 求得的解,那么当 $d_i\leqslant d_j(\forall i\neq j)$时,$\varepsilon$满足:$|\varepsilon_i|\leqslant|\varepsilon_j|$.

证明:从 B-EPV 算法分析,可以分为以下 4 种情况:

① 假设得到绝对平均情况 I(即$\forall i\neq j,\varphi=\lfloor\varphi\rfloor=\lceil\varphi\rceil=|\varepsilon_i|=|\varepsilon_j|$).无论 $d_i<d_j$ 或 $d_i\geqslant d_j$,都满足保序性.

② 假设得到绝对平均情况 II(即 G 是一个完全图,$\forall i\neq j,d_i=d_j,|\varepsilon_i|=\lfloor\varphi\rfloor$或$|\varepsilon_i|=\lceil\varphi\rceil$),满足保序性.

③ 假设得到非绝对平均情况 I(即$\exists i,j,|\varepsilon_i|<\varphi,|\varepsilon_j|>\varphi;0<\lceil\varphi\rceil-\varphi\leqslant 0.5$).算法第 4 行:$r=\min\{r,d_i\},\exists i\neq j$,对于 $d_i<\varphi$有 $d_i\leqslant\lfloor\varphi\rfloor$,选择$|\varepsilon_i|=d_i$.对于 $d_j>\varphi$有 $d_j\geqslant\lceil\varphi\rceil$,选择$\varepsilon_j=\lceil\varphi\rceil$.可知对于 i 和 j 有$|\varepsilon_i|=d_i\leqslant\lfloor\varphi\rfloor<\lceil\varphi\rceil\leqslant d_j$.

④ 假设得到非绝对平均情况 II(即$\exists i,j,|\varepsilon_i|<\varphi,|\varepsilon_j|>\varphi;0<\varphi-\lfloor\varphi\rfloor<0.5$).算法第 4 行:$r=\min\{r,d_i\},\exists i\neq j$,对于 $d_i<\varphi$有 $d_i\leqslant\lfloor\varphi\rfloor$,选择$|\varepsilon_i|=d_i$.对于 $d_j>\varphi$有 $d_j\geqslant\lceil\varphi\rceil$,选择$\varepsilon_j=\lfloor\varphi\rfloor$.可知对于 i 和 j 有$|\varepsilon_i|=d_i\leqslant\lfloor\varphi\rfloor=\varepsilon_j\leqslant d_j$.引理得证. □

引理 2(可交换性). 仅考虑分边数量,设ε'是 EPVP 的一个可行解,若$\exists i\neq j,d_i\leqslant d_j$ 且$|\varepsilon'_i|>|\varepsilon'_j|$时,称分边数量$|\varepsilon'_i|$和$|\varepsilon'_j|$是可交换的.

证明:交换$|\varepsilon'_i|$和$|\varepsilon'_j|$得新解ε''(其中$|\varepsilon_i''|=|\varepsilon'_j|,|\varepsilon_j''|=|\varepsilon'_i|,|\varepsilon_i''|<|\varepsilon_j''|$),由已知得$|\varepsilon'_j|<|\varepsilon'_i|\leqslant d_i\leqslant d_j$,推出:① $|\varepsilon'_i|\leqslant d_i\leqslant d_j$,$|\varepsilon'_i|\leqslant d_j,|\varepsilon_j''|\leqslant d_j$;② $|\varepsilon'_j|<|\varepsilon'_i|\leqslant d_i,|\varepsilon'_j|\leqslant d_i,|\varepsilon_i''|\leqslant d_i$,则 $d_i\leqslant d_j,|\varepsilon_i''|=|\varepsilon''_j|,\varepsilon''$比$\varepsilon'$有更强的可行性.□

定义 6(*k*-选择). 对于长度为 n 的序列 A 中的一个元素 A_i,如果 A_i 是 k-选择的,那么满足:

① 存在至少 $k-1$ 个元素不大于 A_i;② 存在至少 $n-k$ 个元素不小于 A_i.

直观地说,A_i 是 k-选择的,等价于 A_i 是 A 中第 k 小的元素(A_i 与对 A 升序排序后第 $k-1$ 位置上的元素相等).在 A 中 k-选择的元素可能不唯一,但它们都相等.

引理 3(优化解的存在性). 假设ε'是 EPVP 的可行解,通过使用一系列交换动作,可以使ε'转化为优化解ε.

证明:ε'按$|\varepsilon'_i|$排序后,如果在解ε'中ε'_i是从左端开始第 1 个非 i-选择的,那么从ε'_{i+1}到ε'_n必存在一个ε'_j是 i-选择的.可知$|\varepsilon'_i|>|\varepsilon'_j|$,对二者交换,由引理 2 得$\varepsilon''$比$\varepsilon'$具有更强的可行性.当进行一系列交换动作之后,最终可将ε'转化为优化解ε. □

引理 4. EPVP 的优化解ε具有最优子结构.

证明:$\varepsilon=(\varepsilon_1,\ldots,\varepsilon_n)$是满足 $\min\sum_{i=1}^{n}\left(|\varepsilon_i|-\varphi\right)^2$ 的优化解,只需证明解ε的子结构$(\varepsilon_2,\ldots,\varepsilon_n)$也是可以满足 $\min\sum_{i=2}^{n}\left(|\varepsilon_i|-\varphi\right)^2$ 的优化解即可.

反证:假设$(\varepsilon_2,\ldots,\varepsilon_n)$不是满足 $\min\sum_{i=2}^{n}\left(|\varepsilon_i|-\varphi\right)^2$ 的优化解,那么存在$(\varepsilon'_2,\ldots,\varepsilon'_n)$是满足 $\min\sum_{i=2}^{n}\left(|\varepsilon'_i|-\varphi\right)^2$ 的优化解,使得 $\sum_{i=2}^{n}\left(|\varepsilon'_i|-\varphi\right)^2<\sum_{i=2}^{n}\left(|\varepsilon_i|-\varphi\right)^2$.在不等式左右分别加上 $\left(|\varepsilon_1|-\varphi\right)^2$ 得 $\left(|\varepsilon_1|-\varphi\right)^2+\sum_{i=2}^{n}\left(|\varepsilon'_i|-\varphi\right)^2<\sum_{i=1}^{n}\left(|\varepsilon_i|-\varphi\right)^2$.但已知$\varepsilon=(\varepsilon_1,\ldots,\varepsilon_n)$是满足 $\min\sum_{i=1}^{n}\left(|\varepsilon_i|-\varphi\right)^2$ 的优化解,假设与前提矛盾.所以,$(\varepsilon_2,\ldots,\varepsilon_n)$是满足

$\min\sum_{i=2}^{n}\left(|\varepsilon_i|-\varphi\right)^2$ 的优化解,EPVP 的优化解ε具有最优子结构. □

定理 1. B-EPV 算法是一个贪心算法,根据 B-EPV 算法我们可以得到 EPVP 的优化解ε.

证明:使用算法进行选择分边数量的时候,都是选择使 $\sum_{i=1}^{n}\left(|\varepsilon_i|-\varphi\right)^2$ 最小化的分边数量$|\varepsilon_i|$,且根据引理 1 可得解的保序性.由引理 1~引理 3 可得 B-EPV 算法的贪心选择性[6],由引理 4 可得解的优化子结构. □

3.2 节点同步

节点的发送功率不同,通信半径也不同,多数节点的通信半径可以达到 100m 以上.由于室内的面积有限,室内防盗系统的模型都是设计在一跳范围内.所有节点处于同一个冲突区域,如果没有配置良好的调度与同步,当两个节点同时发送数据的时候,很容易发生信号碰撞.这里设计同步的目标就是要在任一时槽至多有一个节点在发送数据包.

本文根据 B-EPV 算法得出的结果见表 2,节点 ID 表示某个顶点 v_i,兴趣列表内容是 v_i 感兴趣的节点.当 v_i 收到来自其兴趣列表内节点发来的数据包的时候,v_i 会采取一些行动(记录或检测).例如对于#05 来说,当它收到#03 或#04 广播的数据包时,它将采取一些行动:将该数据包解封,检查此链路的 RSSI 值;但是当#05 收到#06 广播的数据时,由于#05 对#06 不感兴趣,所以将该数据包丢弃.

节点同步策略如图 7 所示,节点个数为 n=4,节点的工作周期为 $n\times t_{sleep}$,每一个节点广播数据后,在 t_{sleep} 时间后下一个节点进行广播.在调度顺序上,第 i 个节点在第 $i+\theta\times n$(θ为系统已运行的周期数)个时间区域上进行数据的广播.图 7 表示了表 2 的同步图,可知节点按照序号进行广播,达到节点间的同步.

Table 2 Interest table (output of B-EPV algorithm)
表 2 兴趣表(B-EPV 算法的输出)

序号	节点 ID	分边数	兴趣列表
0	#03	1	6
1	#04	1	3
2	#05	2	3, 4
3	#06	1	5

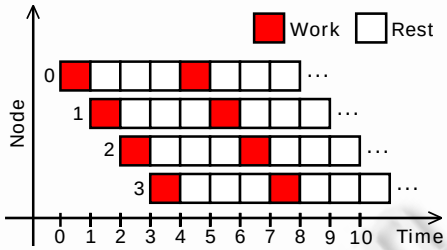


Fig.7 Synchronization of sensors
图 7 节点同步

3.3 稳态确定

通过使用在第 3.2 节设计的同步方式,所有节点按照调度顺序广播数据包.当某节点接收到感兴趣的数据包时,获取该链路 RSSI 值,检查这条兴趣链路是否存在异常.

定义 7(链路状态). 链路状态分为稳态和混态.某链路的稳态是一个三元组(α,β,δ),当链路 RSSI 值存在关系 $\alpha-\delta\leqslant RSSI\leqslant\beta+\delta$时,称该链路处于稳态.混态被描述为该链路 $RSSI\leqslant\alpha-\delta$或 $RSSI\geqslant\beta+\delta$.当链路处于混态时,称此链路异常.

由于室内无线通信模型比较复杂[7],室内测量的 RSSI 值往往与节点距离无固定比例关系.为了识别链路的状态,首先要确定稳定状态.系统对每一条链路进行一次适应过程,并且整个适应过程需要在环境不变(检测区域无人,节点要放置于相对稳定的位置)的前提下进行.由于传感器节点计算能力有限,无法使用复杂的机器学习模型,本文使用如下适应过程:设每个链路都需要进行一次适应过程,每个链路的适应过程均需要收集 M 个 RSSI 样本,采用直方图模型,当一个 RSSI 样本到达的时候,将该样本放入直方图相应的“柱”内.例如在某链路收集了 $M=223$ 个数据,适应过程结束后形成的直方图如图 8 所示,6 个柱的样本总数是 M .样本数相对较多的那几个柱的样本值(样本−13,−12,−11 具有绝对多于其他样本的样本数)被视为处于稳定范围内,因为在无人环境下样本值几乎完全平稳在该范围内,且该范围内的样本数绝对多于范围外的样本数.作者在其他实验(由于篇幅有限,本文不予列出具体实验过程)中测量了 RSSI 被人体干扰的平均振幅大约是 15dBm~20dBm,所以图中其余

的 3 个样本值(−15,−14,−10)仅被视为环境噪声,而并非异常.这里使用 δ 作为一种阈值,在本例中,$\alpha=-13$, $\beta=-11$, $\delta=2$ 可以达到比较好的效果(δ 值的选取比较复杂,我们暂时从经验获得).

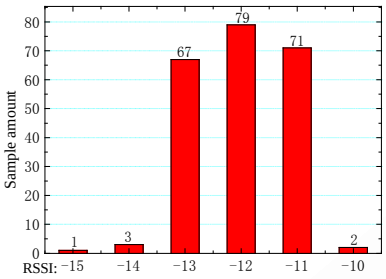


Fig.8 Histogram of fitting process, unit of sample: dBm

图 8 适应过程的直方图,样本单位: dBm

定义 8(*k*-众数集问题).

输入:$k>0$,集合 $S=\{s_1,s_2,\ldots,s_n\}$,$\forall s_i \geqslant 0$.

输出:S 的一个划分$\{S_A,S_B\}$,满足:对于 $\forall s_i \in S_A$,有 $s_i > k\sum_{s_j \in S_B} s_j$.

集合 S_A 称为集合 S 的众数集,k 表示 S_A 中某元素值多于 S_B 中元素值总和的程度.对于上面例子使用下面的 Blade 算法可以解决这个问题,得出 $S_A=\{67,71,79\}$,$S_B=\{1,2,3\}$,这里 k 取 1.5 即可.至此,稳态可以被确定.

算法 2(Blade 算法).

输入:$k>0$,集合 $S=\{s_1,s_2,\ldots,s_n\}$.

输出:有序集合 S' 及 S' 中最小众数下标 *blade*.

初始化:$sum=0$,$i=0$.

1 对 S 按元素值进行升序排序,得有序集合 S'.

WHILE $i<0$ **DO**

IF $s_i' > k \times sum$

2 $blade=i$

3 $sum+=s_i'$

END WHILE

算法 3(OM 算法, Other Mess Algorithm)

输入:信号强度 *RSSI*,链路编号 l_no .

输出:链路是否报警——*Warn* .

IF $premess == TRUE$

IF RSSI 异常

1 $Warn = TRUE$

ELSE

2 以概率 $P = om/m$ 使 $Warn = TRUE$

ELSE

IF RSSI 异常

$premess = TRUE$

3 **ELSE**

4 $premess = FALSE$

3.4 异常处理

现在已经可以通过 Blade 算法得到稳态的 RSSI 范围了,接下来就是如何针对超出稳态的样本进行处理.若系统对于单一的混态样本判断为警报,实验表明系统过于灵敏,误报率将会很高.如果凭借同一个链路连续发现两个混态样本进行判断,则系统灵敏度大大下降.由于篇幅原因,这两种方法不予展示.本文使用一种折中的方式,判断准确且灵敏度可以被用户接受.OM 算法根据某链路 a 的状态结合其他所有链路状态进行判断,即对全局进行权衡.若网内混态的链路数较多,且当前链路前一时刻处于混态,当前时刻为稳态,则其代理节点以较高的概率报警.算法中 *premess* 表示上一时刻链路 l_no 是否异常. *om* 为从上次当前节点广播数据包到当前时刻其他异常链路的个数, m 为总链路数.

4 实 验

实验环境如图 9 所示,图中圆圈指示节点.在实验中使用的节点为 Crossbow 公司的 TelosB[8].该节点拥有 IEEE802.15.4 协议标准,通过 CC2420 芯片发射 2.4GHz 频率无线信号.节点被固定在一个高为 0.9m 的木架上面,保证在空间内有足够大的传输范围.节点程序在 TinyOS2.x[9]环境下编写,Blade 算法参数 k=1.5.实验中节点的布局如图 10 所示,节点个数分别为 4、5、6.假设布局已优化,可以覆盖整个区域.屋子的面积为 7.23×7.45m^2,每一条线段,都是要被监测的链路.由于信号穿墙实验的开销与空间需求比较大,本文实验设计为非穿墙实验.信号是否穿墙的原理均相同,同时根据无线通信的阴影效应来处理 RSSI 的衰落程度,只是穿墙实验中节点收到的 RSSI 值普遍较低.文中使用 B-EPV 算法对实验布局进行代理分配(GUI 程序完成),分配的结果见表 3.对于布局 1 中#05,表 3 布局 1 中#05 列的数字表示#05 对#03、#04 感兴趣.

Fig.9 Testbed

图 9 实验环境

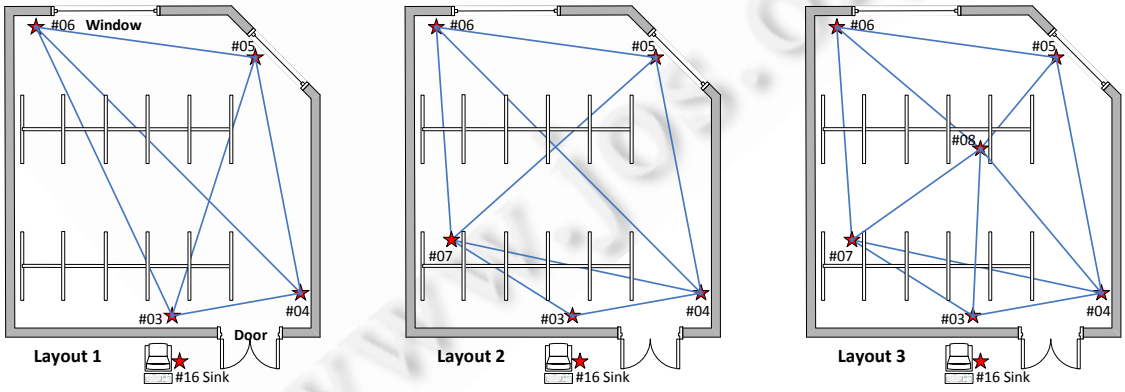


Fig.10 Layouts of experiment

图 10 实验布局

响应时间指系统运行时,从目标进入监测区域到系统首次提示报警的时间.响应时间是防盗技术的一个重

要指标,它标志着系统报警的及时性.图 11 显示的是目标在 1m/s 和 2m/s 的移动速度下系统测量响应时间的实验结果(M=30).因为人移动的速度处于一个固定的范围($0 \leqslant v \leqslant 10$m/s 室内环境下人移动的速度是很慢的),网络扫描周期(从节点 i 广播至下次节点 i 广播的时间间隔)为 $n \times t_{sleep}$,其中 n 为节点个数.如果人在网络中移动的时间小于网络扫描周期,系统则无法发现人的行为.实验布局 3 中网络扫描时间 0.6s(t_{sleep}=100ms),倘若人移动速度高达 10m/s,从理论上讲,系统仍可以对环境进行监控.我们可以从结果中得出结论:对于同一个布局,在相同参数的情况下,系统对快速移动目标的响应时间比对慢速移动目标的响应时间要短;休息时间(t_{sleep},图 11 中的 sleep)越长,响应时间越长.

误报率(false positive)指监测区域内无人时系统分析数据后,将结果确定为报警的概率.漏报率(false negative)指当有人进入区域时,系统分析数据后并未做出报警的概率.误报率和漏报率反映了系统报警的准确性,目前未发现明显影响误报率的因素.对于误报率的测量,本文进行了 3 组实验,共扫描网络 8000 次,仅产生 1 次误报,误报率为 0.0125%.在进行的 260 入侵动作中,系统工作正常,尚未发现漏报.

在实验中有这种情况发生:当目标通过 AB 边而未通过 CD 边(AB 与 CD 无公共顶点),[A,B]报警而[C,D]也同时报警.原因主要是 CD 传输范围过大,甚至与 AB 的传输范围有交集,称这种[C,D]的报警形式为偏差报警.偏差报警的个数占整体报警个数的百分比称为偏差率.如图 12 所示,在相同的实验布局中,偏差率与适应过程所收集的数据量 M 成反比.偏差率并不是防盗系统的重要参数,若要在 GUI 程序中根据报警的边表示出大致入侵行为的位置,误差率会体现出定位的精度.

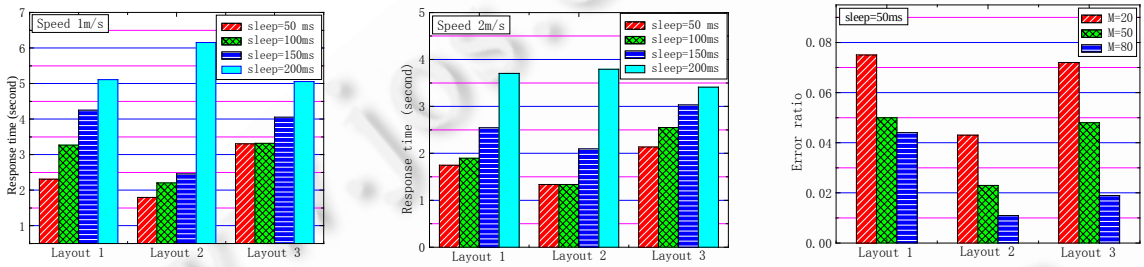


Fig.11 Response time of target with speed at 1m/s and 2m/s

图 11 目标以 1m/s 和 2m/s 速度时的响应时间

Fig.12 Error ratio

图 12 偏差率

Table 3 Agent distributions in 3 layouts

表 3 各布局代理的分配情况

布局	#03	#04	#05	#06	#07	#08
布局 1	6	3	3, 4	4, 5	—	—
布局 2	7	3, 7	4	4, 5	5, 6	—
布局 3	4, 8	7, 8	4	5, 7	3, 8	5, 6

5 结 论

根据无线通信阴影效应的特性,人移动到通信区域内,对于接收信号强度有不同程度的影响.此特性应用在无线传感器网络中,可以实现防盗的功能.本文建立了无线传感器网络隐式防盗技术的框架,对关键技术进行了必要的分析.首次提出描述无向图中顶点与边从属关系的顶点分边问题,本文在理论上证明了 B-EPV 算法是一个贪心算法,可以得到优化解.本文提出了 k-众数集问题及解决该问题的 Blade 算法.实验结果表明,节点休息时间越长,响应时间越长;人移动速度越快,响应时间越短;适应过程 M 值越大,偏差率越小.

今后的研究工作可以从以下几个方面开展:进行更多的实验,研究影响误报率和漏报率的因素;通过系统长期的运行,测定、分析系统健壮性;对多个感兴趣的区域同时进行监控,用户在系统上进行多路查询.

References:

[1] Song H, Zhu S, Cao G. SVATS: A sensor-network-based vehicle anti-theft system. In: Proc. of the INFOCOM 2008. Phoenix: IEEE, 2008. 2128−2136.

[2] Weisman CJ. The Essential Guide to RF and Wireless. 2nd ed., Upper Saddle River: Prentice Hall PTR Press, 2002.

[3] Wilson J, Palwari N. See-Through walls: Motion tracking using variance-based radio tomography networks. IEEE Trans. on Mobile Computing, 2011,10(5):612−621.

[4] Goldsmith A. Wireless Communications. Cambridge: Cambridge University Press, 2005.

[5] Woyach K, Puccinelli D, Haenggi M. Sensorless sensing in wireless networks: Implementation and measurements. In: Proc. of the Modeling and Optimization in Mobile, Ad Hoc and Wireless Network, the 4th Int'l Symp. Boston: IEEE, 2006. 1−8.

[6] Cormen H, Leiserson E, Rivest L, *et al*. Introduction to Algorithms. 2nd ed., Cambridge: The MIT Press, 2001.

[7] Zanca G, Zorzi F, Zanella A, Zorzi M. Experimental comparison of RSSI-based localization algorithms for indoor wireless sensor networks. In: Proc. of the REALWSN 2008. Glasgow: ACM, 2008. 1−5.

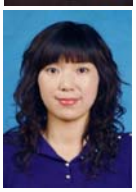
[8] TelosB Datasheet. http://www.willow.co.uk/html/telosb_mote_platform.html

[9] Hill J, Szewczyk R, Woo A, Levis P, Madden S, Whitehouse C. TinyOS: An open operating system for wireless sensor networks. In: Proc. of the 7th Int'l Conf. on Mobile Data Management (MDM 2006). Nara: IEEE Computer Society, 2006.

段金晟(1986－),男,黑龙江齐齐哈尔人,硕士生,主要研究领域为无线传感器网络.

郭龙江(1973－),男,博士,教授,CCF 会员,主要研究领域为并行与分布式计算,传感器网络,数据挖掘,数据库.

刘勇(1975－),男,博士,副教授,主要研究领域为数据挖掘,信息检索.



朱敬华(1976－),女,博士,副教授,主要研究领域为无线传感器网络,嵌入式计算.