基于路由算法的无线传感器网络伪装研究

段苗莹,何聚厚,何秀青
(陕西师范大学 计算机科学学院,陕西 西安 710062)

摘 要:在研究如何通过无线传感器网络WSN有效获取信息的同时,如何确保敏感地区的信息不被WSN窃取也成为研究者关注的热点问题。基于WSN已有的路由算法,利用其开放的特点在敏感地区设置WSN伪装节点,并使其加入WSN节点的路由构建过程,伪装节点采用路由算法自适应伪装,通过修改数据报中的控制信息进而实现阻止WSN节点构建有效路由,并在最大程度上消耗WSN节点能量的目的。从WSN节点能耗速度和网络生命周期两方面验证了基于路由算法的WSN伪装的有效性。

关键词:无线传感器网络;信息安全;伪装
中图分类号:TP393.08 **文献标识码**:A **文章编号**:1673-629X(2012)11-0105-03

Study on Wireless Sensor Networks' Camouflage Based on Routing Algorithms

DUAN Miao-ying, HE Ju-hou, HE Xiu-qing
(School of Computer Science, Shaanxi Normal University, Xi'an 710062, China)

Abstract: Researchers study on how to access information effectively through the wireless sensor networks, at the same time they also pay their attention on how to protect data in sensitive areas from stealing by WSN. Based on the existing routing algorithms and utilizing its open characteristics, add camouflaging nodes into sensitive areas. The camouflaging nodes join the process of router constructing by using self-adaptive routing protocol, modify the control information of the datagram to stop WSN nodes building an effective routing, and consume the energy of WSN nodes as much as possible. Finally, from energy consumption rate of WSN nodes and the lifetime of the network, the experimental results show that this method can achieve a good result.

Key words: wireless sensor networks; information security; camouflage

0 引 言

无线传感器网络(Wireless Sensor Networks, WSN)是由部署在监测区域大量微型传感器节点组成,这些节点通过飞机抛撒或炮弹发射到观察者不能或不方便到达的数据敏感领域[1,2],通过散落的节点构建自组网实现对该地域信息的窃取和传递[3]。因此无线传感器网络受到学术界、军事部门和工业界的极大关注[4]。人们在研究如何通过WSN传递信息的同时,如何有效保护数据敏感地区的信息不被传感器网络窃取,成为信息安全研究的热点问题之一。

文中提出的"基于路由算法的无线传感器网络伪装模型",是从WSN中节点构建自组网形成信息传递的路由算法出发,在数据敏感领域加入WSN伪装节点,当伪装节点感知WSN节点存在时,主动加入WSN节点构建自组网路由的过程,同时通过伪装节点之间的信息交换和协同工作,实现阻止WSN节点构建有效的路由,进而实现对WSN中节点能量的最大程度消耗,起到保护数据敏感领域信息安全的目的。

1 伪装节点

由于伪装节点是用户自主设置的节点,用户可以采取太阳能供电、周期性更换电池或直接供电等方式对伪装节点进行供电,因此,相对于一般的传感器节点,伪装节点的能量是无限的。

伪装节点有三种状态,休眠、探测和工作。通过一定的算法让节点周期性地休眠、探测和工作以达到节能的效果,节点根据某些参数进行周期性的状态转换。

1.1 感知WSN节点

伪装节点通过截获其通信范围内的数据报并进行简单分析来判断是否有WSN节点存在,通过分析探测到的数据报TTL值,可以得出WSN节点在网络中的大概位置。

收稿日期:2012-02-29;**修回日期**:2012-06-02
基金项目:中央高校基本科研业务费专项资金(GK201002028)
作者简介:段苗莹(1987-),女,硕士研究生,研究方向为计算机网络安全;何聚厚,博士,副教授,研究方向为计算机网络安全。

对于一个具体的无线传感器网络，所有的节点包括 WSN 节点和伪装节点。网络中的节点接收到数据报后，对数据报的处理方式决定了节点的行为特征及其在整个 WSN 中的角色。不同节点对数据报采取的处理方式有：

(1) WSN 节点：根据节点所绑定的网络服务类型构造相应的响应数据报，并依据数据报中的目的地址将数据报转发给网络中的其他节点；

(2) 伪装节点：根据接收到数据报中的源地址和目的地址分析数据报的流向，决定具体操作，如果数据报流向属于我方网络，则构造响应数据报并进行转发，如果不属于我方网络，则依据数据报的 TTL 值得出 WSN 节点在网络中的大概位置，并构造伪装数据报进行转发。

1.2 路由算法自适应伪装

由于伪装节点要配合 WSN 节点的路由构造，因此采用路由算法自适应伪装，伪装节点根据 WSN 节点选择的路由协议进行配合，自主选择适用的路由协议。路由协议自适应伪装包括状态收集模块和数据转发模块。状态收集模块用来搜集局部网络信息，例如邻居节点的描述(如 id、位置等)和邻居链路可用性(如链路类型、传输速率等)等信息。数据转发模块负责描述路由的转发方式以及下一跳节点的选择标准。

定义 1 伪装节点路由协议特征集合 $F = \{F_1, F_2, \cdots, F_m\}$，$\forall F_i \in F$ 表示现阶段已有的路由协议对应的特征配置。

伪装节点路由自适应过程描述如下：

Step1：接收 N 个数据报，记录并分析其控制信息，提取协议特征，N 的取值是通过多次实验确定的经验值。

Step2：将提取的协议特征与特征集合中的协议特征进行匹配，如匹配成功则输出相应的路由协议并执行 Step3，否则执行 Step4。

Step3：数据转发模块根据输出的路由协议转发数据报，break。

Step4：保留新协议，更新特征集合。

1.3 伪装节点之间的相互认证

每个伪装节点都具有双重身份，对于 WSN 节点感知到的是与其相同的节点并参与 WSN 的路由计算，而对于所有伪装节点，则在获得 WSN 节点的信息并构建路由时以构建“最差”路由为目的。伪装节点收到其他节点发来的数据报时，采用对称密钥机制的点对点认证技术来判断数据发送者的身份，伪装节点之间通过共享的密钥计算和验证消息认证码(Message Authentication Code，MAC)即可完成一次点对点认证过程[5-8]。

1.4 采用 LEACH 算法形成网络拓扑

节点通过 LEACH 算法形成拓扑，周期性地执行：每轮循环分为簇的建立阶段和稳定的数据通信阶段，在簇的建立阶段，相邻节点动态形成簇，随机产生簇头；在数据通信阶段，簇内节点把数据发送给簇头，簇头进行数据融合并把结果发送给汇聚节点[9-12]。

2 无线传感器网络伪装模型

下面给出基于路由算法的无线传感器网络伪装模型的算法描述，分为一个伪装节点和多个伪装节点两种情况。

2.1 一个伪装节点

2.1.1 伪装节点状态转移

定义 2 伪装节点状态集合 $S = \{S_0, S_1, S_2\}$，其中 S_0 表示伪装节点休眠状态，S_1 表示伪装节点探测状态，S_2 表示伪装节点工作状态。

伪装节点状态转移图如图 1 所示。

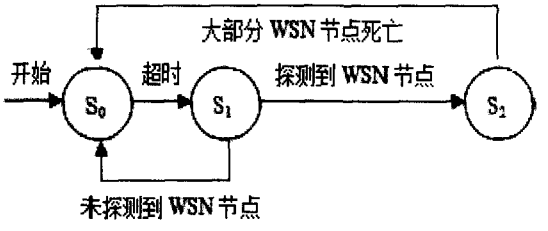

图 1 伪装节点状态转移图

2.1.2 工作过程

伪装节点工作过程描述如下：

Step1：如探测到 WSN 节点已形成网络拓扑，执行 Step3，否则自组织形成拓扑并执行 Step2。

Step2：自组织拓扑过程中，通过修改数据报的目的地址重定向数据报，阻挠拓扑形成并消耗 WSN 节点的能量，如果拓扑形成则执行 Step5。

Step3：周期性广播建立连接的请求报文，得到其他节点回复后执行 Step4。

Step4：收集 WSN 数据报，分析其使用的路由协议，启动路由算法自适应伪装。

Step5：转发数据，将敏感信息发送给簇头，增加簇头负担，尽可能多地消耗簇头能量，如有新一轮簇头选举，执行 Step6，否则执行 Step7。

Step6：主动参与并当选为簇头节点，将收集到的数据报发送给其它簇头，加速整个 WSN 能耗。

Step7：检测到大部分 WSN 节点死亡时，断开与基站的连接并转入休眠状态。

2.2 多个伪装节点

当网络中有两个伪装节点时，两个伪装节点通过相互之间的信息交换和协同工作，阻止 WSN 节点构建

有效路由,最大程度上消耗 WSN 节点的能量。文中只考虑 WSN 节点已形成网络拓扑时伪装节点的工作过程,分别称两个伪装节点为 A 和 B,工作过程描述如下:

Step1: A 广播探测数据报,B 收到数据报后根据共享密钥和消息认证码确定 A 的身份,并向 A 发送响应数据报完成认证文。

Step2: A、B 广播请求报文,获得 WSN 节点的合法认证后参与网络通信。

Step3: A 收到数据报后,修改数据报中的控制信息,将 B 设置为最佳下一跳节点并进行转发。

Step4: B 收到数据报后将其发送给簇头节点,消耗簇头能量,如有新一轮簇头选举,执行 Step5,否则执行 Step6。

Step5: A、B 主动参与并当选为簇头节点,将收集到的数据报发送给其它簇头,加速整个 WSN 能耗。

Step6:网络中大部分 WSN 节点死亡时,A、B 断开与基站的连接并转入休眠状态。

3　实验及结果分析

本模型基于 NS2 实验平台,部署 50 个 WSN 节点并采用 GEAR 路由协议[9]作为 WSN 节点的协议代理,通过脚本场景设置实现伪装模型工作流程。

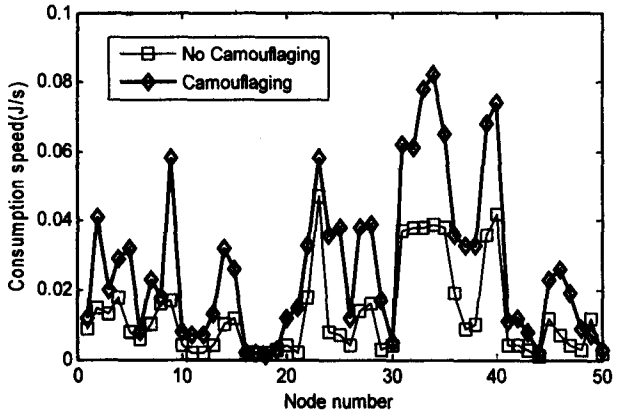

图 2　WSN 节点能耗速度对比图

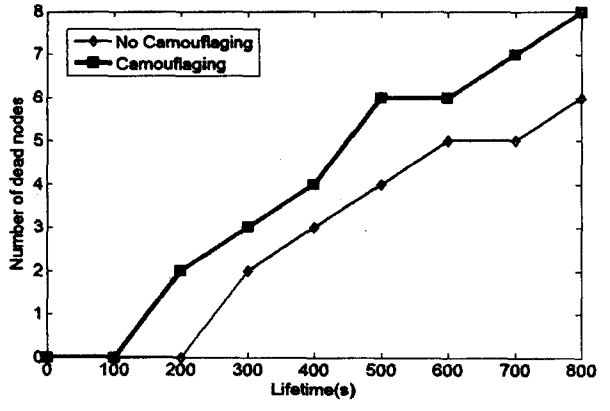

图 3　WSN 网络生命周期对比图

图 2 为在 1 个伪装节点的情况下,WSN 节点的能耗速度对比图,其中 No Camouflaging 表示没有伪装节点,Camouflaging 表示存在伪装节点。图 3 为在 1 个伪装节点的情况下,整个网络的生命周期对比图。图 4 和图 5 分别为在 2 个伪装节点相互配合的情况下,WSN 节点的能耗速度及网络生命周期对比图。

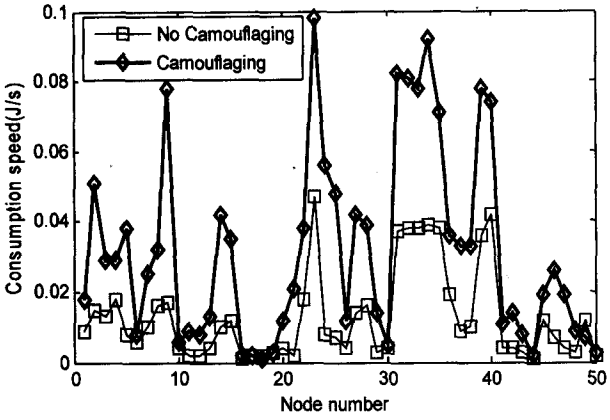

图 4　WSN 节点能耗速度对比图(2 个伪装节点)

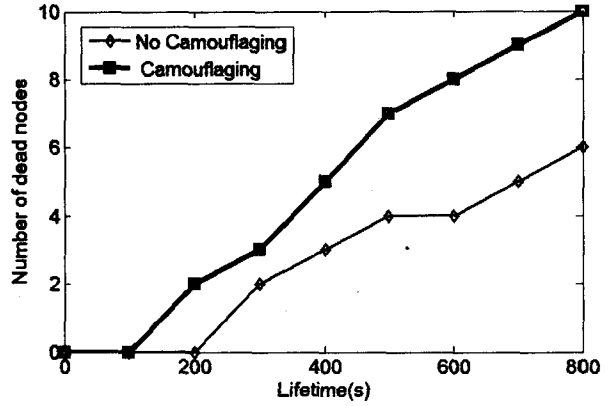

图 5　WSN 网络生命周期对比图(2 个伪装节点)

实验数据对比如表 1 所示。

表 1　WSN 伪装模型实验数据对比

WSN 节点相关参数	平均能耗速度(1 个伪装节点)(J/s)	平均能耗速度(2 个伪装节点)(J/s)	平均每 100s 死亡的节点数(1 个伪装节点)	平均每 100s 死亡的节点数(2 个伪装节点)
No Camouflaging	0.01278	0.01302	3	3
Camouflaging	0.02714	0.0318	4	6

由表 1 可以看出,存在伪装节点时,WSN 节点能耗速度明显加快,单位时间内网络中死亡的 WSN 节点较多,说明伪装节点在一定程度上消耗了 WSN 节点的能量。随着伪装节点个数的增加,效果更加明显。

4　结束语

文中提出了基于路由算法的无线传感器网络伪装模型,通过在 WSN 中加入伪装节点达到保护数据敏感领域信息安全的目的。伪装节点具有“双重身份”,一

(下转第 112 页)

与优化思想,搭建了人群模拟系统的静态框架,最后引入几何方法来制定碰撞规避的规则,从而对人群模拟仿真的真实度加以提升。最后对不同的出口条件下人群的疏散进行仿真,仿真结果表明该系统对疏散出口优化设计、人员疏散引导和待疏散人员选择正确的疏散策略有一定的指导作用。

虽然文中已经建立了全局路径,但是对于多房间的环境下研究还不够,未来希望通过建立三维建筑物的平面拓扑结构图来对全局路径进行分层,以加快路径计算效率。此外,所建立的碰撞规避规则还过于简单,对于以后的建模应当更多地加入个体心理因素的相互作用来制定更加完善的规则。在特殊环境下,例如火灾、煤气泄露、爆炸等情况下的烟雾,火势对人群移动是如何产生影响这一问题也值得深入研究。

参考文献:

[1] Amkraut S, Girard M, Karl G. Motion Studies for a Work in Progress Entitled 'Eurythmy'[C]//SIGGRAPH Video Review. [s. l.]:[s. n.],1985.

[2] Reynolds C W. Flocks, birds and schools: a distributed behavioral model[J]. Computer Graphics, 1987(21):25-34.

[3] EXODUS[EB/OL]. 2010. http://fseg. gre. ac. uk/index. html.

[4] Thompson P A, Marchant E W. Computer and Fluid Modeling of Evacuation[J]. Safety Science, 1995, 18(4):277-289.

[5] 方 正,卢兆明. 建筑物避难疏散的网格模型[J]. 中国安全科学学报,2001,11(4):10-13.

[6] 朱 艺,杨立中,李 健. 不同房间结构下人员疏散的 CA 模拟研究[J]. 火灾科学,2007,16(3):175-179.

[7] 王兆其,毛天露,蒋 浩,等. 人群疏散虚拟现实模拟系统-Guarder[J]. 计算机研究与发展,2010,47(6):969-978.

[8] Hughes R L. A continuum theory for the flow of pedestrians [J]. Transportation Research Part, 2002(36):507-535.

[9] Gayle R, Sud A, Andersen E, et al. Real-time navigation of independent agents using adaptive roadmaps [J]. IEEE TVCG, 2009(10):34-38.

[10] Jiang Hao, Xu Wenbin, Mao Tianlu, et al. Continuum crowd simulation in complex environments[J]. Computers & Graphics, 2010(34):537-544.

[11] 陈 育,陶 平,张小英. 大型商场人员安全疏散的计算机仿真研究[J]. 计算机技术与发展,2010,20(10):211-214.

[12] 褚龙现,刘高原. 基于 Agent 的应急疏散模型研究[J]. 计算机技术与发展,2011,21(9):201-207.

[13] 皱 海,徐 军,褚维翠. 基于 OpenGL 的三维地形的模拟[J]. 计算机技术与发展,2011,21(6):239-241.

[14] 于 君,刘 弘. 基于 ABC 算法的群体动画研究与应用[J]. 计算机技术与发展,2011,21(10):222-225.

[15] 杨 晓,廉静静,张新宇. 基于 OSG 的虚拟场景中包围盒碰撞检测的研究[J]. 计算机技术与发展,2011,21(9):32-35.

[16] Fruin J J. Designing for Pedestrians: a Level - of - Service [C]//Highway Research Record 355. [s. l.]:[s. n.], 1971:1-15.

(上接第 107 页)

方面配合 WSN 节点,参与其路由计算,另一方面通过伪装节点之间的相互协作,在获得 WSN 节点信息的同时,构建最差路由。通过 NS2 平台实现模型的仿真实验,根据 WSN 节点的能耗及整个网络的生命周期等参数验证了伪装模型的有效性。

参考文献:

[1] Akylidiz I F, Su Weilian, Sankarasubramaniam Y, et al. A Survey on Sensor Networks[J]. IEEE Communications Magazine, 2002, 40(8):102-114.

[2] Tilak S, Abu-ghazaleh N B, Heinzelman W. A Taxonomy of Wireless Micro-sensor Network Models[J]. Mobile Computing and Communications Review, 2002, 1(2):1-8.

[3] 任丰原,黄海宁,林 闯. 无线传感器网络[J]. 软件学报,2003,14(7):1282-1291.

[4] 孙利民,李建中,陈 渝. 无线传感器网络[M]. 北京:清华大学出版社,2005:1-18.

[5] Yang G, Wang J T, Cheng H B. Identity-based Key Agreement and Encryption for Wireless Sensor Networks[J]. Journal of China Universities of Posts and Telecommunications, 2006, 13(4):54-60.

[6] Zhang Y C, Liu W, Lou W J, et al. Location-based Compromise-tolerant Security Mechanisms for Wireless Sensor Networks[J]. IEEE Journal on Selected Areas in Commnuications, 2006, 24(2):247-260.

[7] 赵小伟,王绍斌. 基于标识算法的密钥管理体系和 CPK 认证[J]. 信息安全与通信保密,2007(6):200-202.

[8] 周文粲. 一种改进的无线传感器网络密钥管理方案[J]. 计算机工程,2011,37(24):123-125.

[9] 敬海霞,胡向东. 无线传感器网络的路由协议研究[J]. 计算机技术与发展,2007,17(10):150-154.

[10] Heinzelman W, Chandrakasan A, Balakrishnan H. Energy efficient communication protocol for wireless microsensor networks[C]//Proceedings of the 33rd Annual Hawaii International Conference on System Sciences. MA, USA:[s. n.], 2000:3005-3014.

[11] Yu Y, Govindan R, Estrin D. Geographical and energy aware routing: a recursive data dissemination protocol for wireless sensor networks[R]. [s. l.]:UCLA, 2001.

[12] 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.