第38卷 第18期
Vol.38 No.18

计 算 机 工 程
Computer Engineering

2012年9月
September 2012

• 安全技术 •

文章编号：1000—3428(2012)18—0123—03 文献标识码：A 中图分类号：TP393

一种低复杂度的安全数据收集算法

王海勇[a,b]，杨 庚[a]，许 建[a]，杨 震[a]

(南京邮电大学 a. 宽带无线通信与传感网技术教育部重点实验室；b. 物联网学院，南京 210003)

摘 要：无线传感器网络中的恶意节点会导致严重的黑洞问题。为此，在SEEM算法的基础上，提出一种低复杂度的安全数据收集算法，采用反馈-确认机制，利用无线传感器网络的多路径路由功能，实现数据的安全传输。实验结果证明，与DRP和SPDC算法相比，该算法的复杂度更低，数据传输性能更好。

关键词：无线传感器网络；数据收集；多路径路由；反馈；SEEM算法

A Low-complexity Secure Data Collection Algorithm

WANG Hai-yong[a,b], YANG Geng[a], XU Jian[a], YANG Zhen[a]

(a. Key Lab of Broadband Wireless Communication & Sensor Network Technology of Ministry of Education;
b. College of Internet of Things, Nanjing University of Posts and Telecommunications, Nanjing 210003, China)

【Abstract】 Compromised nodes in Wireless Sensor Network(WSN) cause black hole. Based on SEEM algorithm, a low-complexity secure data collection algorithm is proposed in this paper. It uses a feedback-acking mechanism, which makes full use of property of multipath routing to achieving security of data transmission. Simulation experiments show that, compared with DRP and SPDC, the algorithm has higher quality of data transmission with less complexity.

【Key words】 Wireless Sensor Networks(WSN); data collection; multipath routing; feedback; SEEM algorithm

DOI: 10.3969/j.issn.1000-3428.2012.18.033

1 概述

无线传感器网络(Wireless Sensor Networks, WSN)是物联网的重要组成部分，它通过大量分散在目标区域内的节点收集有用的信息，以便人们对其进行分析和处理[1]。例如城市交通监控系统利用无线传感器网络监测交通情况，收集并融合交通实时信息，通过分析收集的数据得到相应的解决方法。

无线传感器网络中敌对者通过一些被捕获的节点窃听、破坏或屏蔽接收信息，成为网络中数据收集的“黑洞”，这些被捕获的节点称为恶意节点。如何检测与处理这些恶意节点成为数据安全收集的一个重要问题。常规的密钥密码体制并不能有效解决恶意节点问题，因为节点一旦被捕获，加密/解密密钥也会被敌对者窃取。同时由于无线传感器网络的资源限制以及目前入侵检测技术的不成熟，因此通过无线传感器网络的路由功能规避或绕开这些恶意节点，减少“黑洞”带来的危害，成为解决此问题一个较为有效的替代方法。

目前，基于多路径路由的数据传输算法得到了越来越广泛的研究，如文献[2-9]的方案通过在源节点和汇聚节点间建立多条路径进行数据传输，以降低数据被恶意节点拦截的概率，提高数据传输的可靠性及容错性。但上述方案普通存在算法复杂度高、对网络性能影响大等缺点。为此，本文对SEEM算法进行改进，利用秘密共享算法和多路径路由相结合的算法，实现数据的安全收集。

2 相关研究

文献[3-4]提出的多路径路由算法通过寻找多条节点不相交路径进行数据传输，但是这些算法没有考虑路由安全问题。

文献[5]提出的SPREAD算法利用改进的Dijkstra算法迭代寻找 top-k 条最安全的节点不相交路径。文献[6]对SPREAD算法进行改进，提出了H-SPREAD算法，并考虑了路由安全性和可靠性的需求。文献[7]提出的SEEM算法首先由汇聚节点发送广播数据包，网络中传感器节点对接收到的广播包进行响应，汇聚节点收到响应数据包后

基金项目：国家“973”计划基金资助项目(2011CB302903)；国家自然科学基金资助项目(60873231)；江苏省自然科学基金资助项目(BK2009426)；江苏省高校科技创新计划基金资助项目(CXLX11_0415, CXZZ11_0402, CXLX_0416, CX10B_195Z)；安徽高校省级自然科学研究基金资助项目(KJ2011B115)；南京邮电大学科研基金资助项目(NY207111)

作者简介：王海勇(1979－)，男，博士研究生，主研方向：无线传感器网络，信息安全；杨 庚，教授、博士；许 建，博士研究生；杨 震，教授、博士

收稿日期：2011-12-14 **修回日期**：2012-02-07 **E-mail**：whynjupt@njupt.edu.cn

构建网络拓扑，每次数据传输均需汇聚节点和网络中相应节点进行通信，再由汇聚节点根据节点剩余能量和跳数来决定数据收集时间和数据传输路径，以应对某些网络内部攻击，比如虫洞攻击、选择性重发。

文献[8]提出一种基于秘密共享算法和随机多路径路由的安全数据收集方法，该方法利用源节点的随机传播和 Min-Hop 路由算法，但仅对单个源节点进行了模拟分析，没有考虑多个源点发送数据的情况，同时没有考虑到网络中存在恶意节点离汇聚节点较近时，很容易截获足够多的数据项，秘密共享算法不再安全。文献[9]通过源节点随机传播数据项，汇聚节点对每一个收到的数据项进行跟踪反馈确认建立相对安全路由，但该方法加重了网络负荷。

3 无线传感器网络模型

本文方法基于一个汇聚节点和若干传感器节点所构成的无线传感器网络模型。其中，汇聚节点配备足够的资源，如能量、计算能力、存储空间，而每个传感器节点由独立的电池供电，具备有限的能量、计算和通信能力、存储空间等，周期性地上传感知的信息。无线传感器网络中每个节点都具有唯一的标识。假设节点间使用密钥体系进行可靠的点对点传输。网络中被捕获的恶意节点为了伪装自己以会一定概率选择性地丢弃收到的数据包。本文主要针对恶意节点丢包行为进行研究。

4 安全数据收集算法

由于每个传感器节点的能量和通信能力有限，节点感知的数据需要经过中间节点的转发到达汇聚节点，因此距离汇聚节点近的网络节点需更多地参与网络数据的传输，这个特性往往会被敌对者所利用，通过捕获距离汇聚节点近的网络节点，达到窃听、破坏或屏蔽接收更多网内信息目的。本文在设计多路径路由时尽可能多地考虑这些易成为捕获目标的网络节点的负荷平衡问题，降低由于这些节点成为恶意节点引起的数据收集不安全性，而这往往是多路径路由算法[8-9]所忽视的。

4.1 多路径安全路由的构建

无线传感器网络节点部署以后，节点的位置信息以及节点之间的连接性是未知的，可以通过给每个节点配备 GPS 或者定位算法来实现，但由于价格因素和定位的精确度问题，在实际中往往采用 SEEM 算法中的方法，通过汇聚节点发送一个 ND(Neighbors Discovery)消息在网络中以泛洪方式传播来获得位置信息。本文利用汇聚节点的广播信息构建多路径安全路由，具体的描述如下：

(1)汇聚节点首先广播发送 m 个 ND 数据包，其中，m 为汇聚节点的度数，即汇聚节点的邻居节点数。对每一个 ND 数据包采用随机扩散机制进行下一跳节点的选择。ND 信息包中包含 ND 序列号、一个 R 路由列表和上一跳节点邻居列表。

(2)当中间节点 S_k 收到节点 S_j 传来的 ND 数据包时：

1)检查 S_j 是否在自己的邻居列表中，如果不在，则添加 S_j 到邻居列表。

2)检查是否已收过此 ND 数据包，如果收到过，则将此数据包丢弃不进行转发，结束；否则转步骤 3)。

3)存储数据包中 R 路由列表到本地数据库，将自身的标识添加到 R 路由列表中。

4)在邻居列表中任选一个不在上一跳节点邻居列表中的节点进行 ND 数据包转发。

5)用 S_k 邻居列表更新上一跳节点邻居列表。

(3)当网络中无 ND 数据包转发或超过设定时间阈值时，每一个节点都存储了本节点到汇聚节点的多条安全路由。

在上述多路径安全路由的构建方法中，每个网络节点都会将自己的标识添加到转发数据包中，同时得到路由列表中汇聚节点至本节点的路径，这条路径将在以后数据收集过程中用于网络节点传输数据到汇聚节点，且认为是相对安全的。本文中网络节点得到的路径称为相对安全路径，这是由于网络中的恶意节点是按照一定的概率来丢弃数据包，有可能对接收的广播数据包不进行丢弃而是选择转发，这就使恶意节点有可能被纳入到路由列表的路径中，因此安全路径是相对的。

4.2 基于多路径安全路由的数据收集算法

在构造的多路径路由上传输数据时，采用(t, n)门限 Shamir 秘密共享算法，将数据拆分成 n 个数据项，汇聚节点只要收到至少 t 个数据项便能还原原始数据。n 个数据项在传输过程中，只要 $n-t+1$ 个数据项绕开恶意节点，敌对者便无法还原原始数据，实现数据的安全收集。由于每个节点至汇聚节点的多路径路由是随机产生的，因此敌对者无法根据路由算法在相应的路由上部署恶意节点以达到窃听、破坏或屏蔽接收信息的目的。汇聚节点对已接收的全部数据项进行统计分析，将未能正确接收的数据项反馈给源节点，在此基础上，本文提出一种基于“反馈-确认”安全路径的数据收集算法 MERS(Multi-error Report Simultaneously)，算法具体描述如下：

(1)源节点 S 发送一个数据时，首先根据(t,n)门限秘密共享算法将此数据包 D 拆分成 n 个数据项，给每个数据项按 1~n 进行编号。

(2)搜索本地缓存，如果缓存中存在安全路径，则随机从路由列表选择一条安全路径 $R=\{ID_1, ID_2, \cdots, ID_n\}$进行数据项发送，将数据项发送给标志为 ID_1 的节点 S_1。并记录下每个数据项所选择的安全路径。

(3)中间节点 S_k 收到一个数据项后，在路由项中找到自身的标志 ID_k，将数据项转发给标志为 ID_{k+1} 的节点 S_{k+1}，以此类推，直至所有数据项传送到汇聚节点。

(4)若有 e 个数据项$(n-t<e<n)$没有成功发送到汇聚节点，则汇聚节点重新构建多路径安全路由；否则，执行步骤(5)。

(5)若有 n 个数据项成功传送至汇聚节点，则汇聚节点

不进行任何信息反馈；否则，执行步骤(6)。

(6)若有 e 个数据项($0<e<n-t+1$)没有成功发送到汇聚节点，则汇聚节点随机选择一条正确接收数据项的安全路径发送一个反馈通知消息给源节点 S，反馈消息包含未正确接收到的数据项编号。

(7)在一个规定时间周期内，若源节点 S 没有收到来自汇聚节点的反馈信息，说明选择发送的路由都是安全的；若收到反馈信息，则将反馈消息中数据项编号所在的路径从本地缓存中删除。

5　模拟实验结果与分析

为了对本文算法的效果进行验证和评价，初步设计了一个模拟实验。采用被恶意节点拦截数据包数量和源节点一共发送数据包数量的比率，即数据被拦截率作为主要衡量指标。将本文算法和 DRP 算法[8]、SPDC 算法[9]进行对比。模拟实验的基本参数设置如表 1 所示，其中丢弃率指恶意节点按此概率选择性地丢弃收到的数据包。

表 1　模拟实验中的基本参数

参数	参数值
区域	200 m×200 m
传感器节点数	400
丢弃率	0.2
源节点集合数	10

5.1　不同门限值 n 下的算法性能分析

首先设置不同门限值 n，对单一源节点在网络中数据包被拦截的情况进行实验。图 1 为在一个确定门限值 n 的前提下，源节点进行 1 000 次数据发送操作，平均数据包被拦截的统计情况。

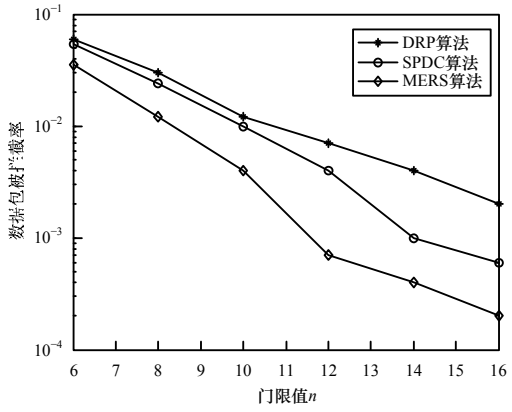

图 1　单源节点时不同 n 值下的数据包被拦截率比较

由图 1 可以看出，随着 n 的增大，数据被拦截率明显下降，这点是显然的，当源节点数据包被拆分成数据项的数量增大时，意味着有更多的安全路径参与数据项传输。另外，在 n 相同的情况下，MERS 的性能优于 DRP 和 SPDC。当 n 取值较大时，3 种算法性能比较接近，但随着 n 的增大，相应的数据项开销也会增加，将给网络带来更大的消耗，因此实际中 n 不宜取较大值。当 n 取值小到一定程度时，MERS 性能明显优于 DRP 算法和 SPDC 算法。

5.2　不同恶意节点数量下的算法性能分析

网络中恶意节点数量的增加表现为网络环境的恶化，被敌对者捕获的节点数量增加，随之而来的就是数据包被拦截率的上升。图 2 为在单一源节点情况下，网络中恶意节点数量发生变化时，平均数据包被拦截的统计情况。

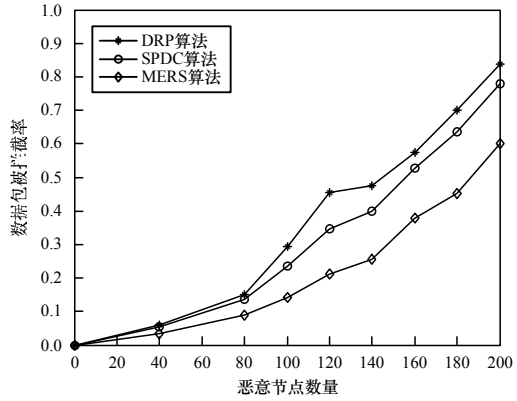

图 2　单源节点时不同恶意节点数量下的数据包被拦截率比较

由图 2 可以看出，网络中恶意节点数量较少时，3 种算法数据包被拦截率较为接近。随着恶意节点数量的增加，3 种算法的数据包被拦截率都在上升，但 MERS 算法增长较为缓慢。这是因为恶意节点数目增加，靠近汇聚节点的恶意节点数目也随之增加，DRP 算法和 SPDC 算法没有考虑到这一点，SPDC 算法中只要本地缓冲有一条安全路径，便使用剩余的安全路径进行数据传输，易造成多个数据项从同一条路径传输，使被拦截率迅速提高。MERS 充分考虑了靠近汇聚节点的传感器节点承担较多的数据转发工作和源节点本地缓存中安全路径较少情况下的情形，当恶意节点数量相同时，MERS 算法性能优于 DRP 算法和 SPDC 算法。

5.3　多源节点情况下的算法性能分析

在实际应用中，汇聚节点接收的数据是由网络中大量分布的传感器节点产生的，为了更加真实地反映网络中多个源节点发送数据的实际数据传输场景，选取 20 个源节点进行模拟实验。最后将所有源节点的模拟结果进行累加归一化，作为算法的整体性能。由图 3 可以看出，在恶意节点数量较少的情况下，MERS 性能优于 DRP 算法和 SPDC 算法，但 3 种算法性能相差不大。在恶意节点数量较多的情况下，MERS 的性能明显好于 DRP 和 SPDC。

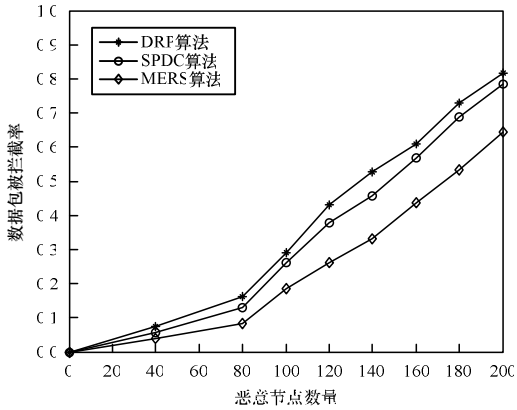

图 3　多源节点时不同恶意节点数量下的数据包被拦截率比较

(下转第 129 页)