基于多路径反馈的无线传感器网络安全数据收集方法

毛郁欣

（浙江工商大学 计算机与信息工程学院，浙江 杭州 310018）

摘 要：针对存在恶意节点的无线传感器网络，提出了一种新型的安全数据收集方法。该方法利用秘密共享算法和多路径路由机制来解决无线传感器网络中的安全数据收集问题。该方法采用了一种“跟踪—反馈”机制，充分利用了无线传感器网络的路由功能，以达到提高数据收集质量的目的。该方法的核心算法易于在资源受限的无线传感器网络环境中实现和执行。通过对应的模拟实现，验证和评价了提出的方法。与现有的同类方法相比，该方法的复杂度更低，安全性更高。

关键词：数据传输；反馈；多路径路由；无线传感器网络

中图分类号：TP393 **文献标识码**：A **文章编号**：1000-436X(2010)8A-0076-05

Secure data collection approach for wireless sensor networks based on multipath routing and feedback

MAO Yu-xin

(School of Computer and Information Engineering, Zhejiang Gongshang University, Hangzhou 310018, China)

Abstract: A novel approach of secure data collection for wireless sensor networks with compromised nodes was proposed. Secret sharing and multipath routing to solve the problem of secure data collection in wireless sensor network was explored. A novel tracing-feedback mechanism was used, which made full use of the routing functionality of wireless sensor networks, to improve the quality of data collection. The algorithms of the approach are easy to be implemented and performed in resource-constrained wireless sensor networks.The performance of the approach with simulation experiments was evaluated. Compared with existing similar methods, the approach provides higher security with less complexity.

Key words: data collection; feedback; multipath routing; wireless sensor network

1 引言

无线传感器网络（WSN）[1]具有无人值守的特性，使得整个网络容易遭受敌对者的恶意攻击。敌对者可以通过物理捕获网络中的部分传感器节点来窃取或破坏信息，而这些被捕获节点（也称为恶意节点）则成为网络中数据收集的“黑洞”[2]。因此，如何检测与处理恶意节点是无线传感器网络安全中的一个重要问题。然而，目前无线传感器网络的入侵技术还并不成熟，由于受到网路自身的资源限制，许多传统网络中智能的入侵检测技术并不适用。针对这一问题，一种替代的解决方法是利用无线传感器网络的路由功能设法绕过或回避这些恶意节点，而不是企图检测这些节点。多路径路由允许在源节点和目标节点之间建立多条路径进行数据传输，通常用于提高数据传输的可靠性、容错性或者实现负

收稿日期：2010-05-21

基金项目：国家自然科学基金资助项目（NSFC60803161）；浙江省教育厅基金资助项目(Y200908082)

Foundation Items: The National Natural Science Foundation of China (NSFC60803161); Educational Commission of Zhejiang Province Program (Y200908082)

载均衡[3]。利用多路径路由的方式，可以在不知道恶意节点具体位置的前提下，将数据分多条路径进行传输，降低数据被恶意节点拦截的机率。

目前，在无线传感器网络研究领域，已经提出了一些利用多路径路由进行安全数据传输[4~7]的方法和算法。但是，现有的解决方案普遍存在算法复杂度较高、对网络性能影响较大的缺点。而本文提出的数据收集方法，针对现有研究的不足提出了改进，利用了秘密共享算法和多路径路由机制来实现无线传感器网络中的安全数据收集。与现有的解决同类问题的方法不同，该方法的创新之处在于提出了一种“跟踪—反馈”机制，充分利用无线传感器网络的路由功能，以达到提高数据收集质量的目的。

2　无线传感器网络模型

一个典型的无线传感器网络通常由两类节点组成：传感器节点和汇聚节点[8,9]。本文研究的方法是基于一个较为简单的无线传感器网络模型。在该模型中，每个传感器节点由独立的电池供电，具备有限的传感、计算和无线通信能力，会定期产生传感数据；而汇聚节点是一个具有足够计算和存储能力的数据收集中心，会定期从各个传感器节点收集数据。同时，假设网络中的恶意节点为了更好地隐蔽和伪装，只是选择性地丢弃一小部分拦截到的数据包。虽然无线传感器网络的路由层会遭受多种类型的攻击，但是本文主要针对存在数据包丢弃行为的攻击进行讨论。

3　基于反馈的数据收集算法

无线传感器网络中的数据收集是一个将数据包从源节点通过中继节点不断转发到达汇聚节点的过程。如果一个数据包通过一条路由路径最终能够成功到达汇聚节点，说明这条路径是相对安全的。因此，可以利用这种数据收集的历史信息来改善后续的数据收集过程。

3.1　基于反馈的安全路径构造

本文提出了一个基于反馈的安全路径构造(FSPC, feedback-based secure path construction)算法，该算法采用了“跟踪—反馈”机制进行安全的数据收集。算法主要基于这样的假设：如果一个数据包从源节点成功达到汇聚节点，那么从源节点到汇聚节点这条路径对于后续的数据传输是潜在安全的。给出算法描述如下（如图 1 所示）。

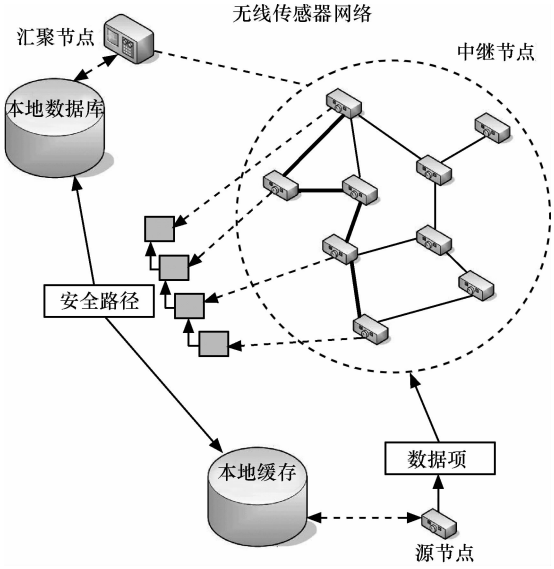

图 1　基于反馈的安全路径构造过程

1) 源节点 S 采用 t-n 门限秘密共享算法[10]将需要传输的数据包 D 进行拆分。同时，S 为拆分后的每个数据项添加一个标识列表 L，L 初始为空。

2) 当传感器节点 S_k 接收到一个数据项时，如果该节点是正常节点，那么将自身的标识 d_k 添加 L 中。

3) 当一个数据项到达汇聚节点时，汇聚节点从数据项中抽取出 $L=\{d_1, d_2, \cdots, d_n\}$ (其中 d_i 表示节点 S_i 的标识)，并将二元组 $<S, L>$ 存储到本地数据库中。

4) 汇聚节点将 L 添加到一个通知消息中，并利用路径 L 发送给 S。

5) 当传感器节点 S_k 接收到通知消息时，如果它的标识 d_j 包含在 L 中，那么从 L 中抽取一条子路径 $P_j=\{d_{j+1}, d_{j+2}, \cdots, d_n\}$，并将 P 存储到本地的缓存中。同时，从 L 中抽取它的下一跳节点 S_{j-1}，节点的标识为 d_{j-1}，并将消息转发给它。

6) 当通知消息达到 S 时，S 从消息中抽取出 L，并存储到本地缓存中。

在上述算法中，路由路径上每个正常的传感器节点都将自己的标识添加到数据包中，当数据包到达汇聚节点时，其中包含了一个由正常节点标识组成的列表。列表对应的路径对于数据收集来说是潜在安全的，并且可以被后续的数据收集重用。因此，本文将这样得到的一条路径称为安全路径。一条路径是安全路径并不意味着这条路径是真正“安全”的。安全路径本身也可能包含恶意节点，因为恶意节点是按照一定的机率丢弃拦截到的数据包的，如果在安全路径的构造过程中，恶意节点没有丢弃而

是转发了数据包，那么该节点就很可能会被纳入到一条安全路径中。因此，安全路径只是相对而言的、潜在安全的数据收集路径。

3.2 基于安全路径的数据收集

当一个源节点从汇聚节点接收到足够多的安全路径，就可以通过这些路径来进行安全的数据传输。因此，基于 3.1 节提出的安全路径构造算法，进一步提出一个基于安全路径的数据收集算法（SPDC, secure-path based data collection），给出算法描述如下。

1) 当源节点 S 需要发送数据时，首先搜索本地的缓存，如果缓存中有安全路径，那么随机选择一条安全路径 $P=\{d_1, d_2, \cdots, d_n\}$，并且将数据项发送给标识为 d_1 的节点 S_1。如果缓存为空，那么随机选择下一跳节点，同时按照 FSPC 算法构造安全路径。

2) 当传感器节点 S_k 接收到一个数据项时，首先搜索本地缓存，并且随机挑选一条安全路径 $P_k=\{d_{k1}, d_{k2}, \cdots, d_{kn}\}$，并且将数据项发送给标识为 d_{k1} 的节点 S_{k1}。如果缓存为空，那么随机选择下一跳节点，同时按照 FSPC 算法构造安全路径。

a) 如果数据包被成功发送到汇聚节点

3) 当汇聚节点接收到数据包时，如果数据包中没有包含安全路径，说明所有的中继节点的缓存中都存在安全路径，不需用构造新的路径，汇聚节点直接返回一个空的通知消息；否则，汇聚节点从数据包中抽取安全路径，同时更新本地的数据库，并且反馈一个包含安全路径的通知消息给 S。

4) 所有接收到通知消息的中继节点，同时更新本地的缓存。

5) S 接收到通知消息时，从通知消息中抽取安全路径 L，同时更新本地的缓存。

b) 如果数据包没有被成功发送到汇聚节点

S 没有在一个规定周期内收到来自汇聚节点的反馈，说明安全路径 P 上可能存在恶意节点，S 将 P 从本地缓存中删除，重新发送数据。

通过上述算法可以说明，安全路径并非总是安全的。安全路径是否安全，需要根据数据收集的服务质量（QoS）来决定。SPDC 算法利用安全路径实现了相对安全的数据收集。通过尽可能地将恶意节点排除在路由之外来提高数据收集的可靠性。

4 模拟实验与结果分析

为了进一步验证和评价提出的方法，初步设计了一个模拟实验。实验采用的主要评价指标是数据包被拦截率（PIP, packet interception probability），即被恶意节点拦截的数据包数量和源节点发送的数据包总数的比率。为了更好地说明本文提出方法的效率，同时和文献[4]中提出的算法进行了性能上的比较。模拟实验的基本参数设定如表 1 所示，其中丢弃率（drop rate）是指恶意节点选择性丢弃一个数据包的机率。

表 1 模拟实验所需的主要参数

参数	参数值
传感器节点数	50
丢弃率	0.2
源节点集合的基数	10

4.1 数据包被拦截率分析

实验首先针对单一源节点的情况进行分析。通过统计源节点在不同恶意节点数量条件下的数据包被拦截率来分析和比较方法的性能。对于每一组确定的恶意节点数量，针对源节点执行一定次数（约 1 000 次）的数据收集操作，同时计算源节点的平均数据包被拦截率。图 2 给出了源节点在不同恶意节点数量条件下的数据包被拦截率情况。从图中可以看出，当恶意节点数量增多时，数据包的被拦截率也上升，这一点是显然的。当传感器节点中有一半是恶意节点时，大部分数据包都会被拦截。图 2 还将 SPDC 算法（包括 FSPC 算法）和文献[4]给出的 NRRP 算法和 DRP 算法进行了比较。通过比较可以看出，在同一恶意节点数量水平下，SPDC 的性能要优于 DRP 和 NRRP。当恶意节点数量较少时，3 种算法的性能比较接近。但是，当恶意节点数量达到一定程度时，SPDC 的表现要好于后两者。

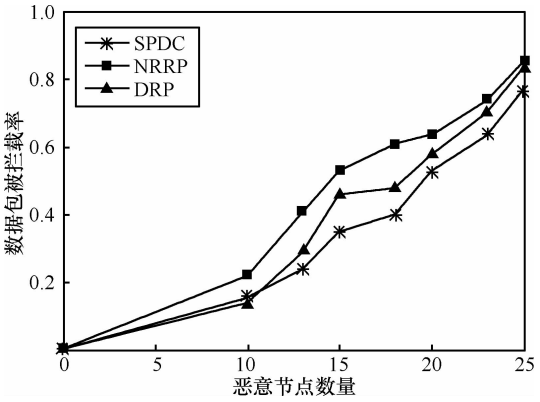

图 2 算法在不同数量的恶意节点条件下的数据包被拦截率比较

4.2　不同丢弃率下的性能分析

当恶意节点的丢弃率发生变化时，被丢弃的数据包的数量也会有所变化。较大的丢弃率意味着恶意节点会丢弃较多的数据包，因此，数据包被拦截率也会随着丢弃率的增大而增大。模拟实验通过改变丢弃率来分析各种算法的性能。图 3 给出了 3 种算法在 2 个不同丢弃率的性能。从图中可以看出，当丢弃率从 0.2 上升到 0.5 时，SPDC 的性能要明显好于 DRP 和 NRRP。而且 SPDC 在丢弃率 0.5 下的性能和丢弃率 0.2 下的性能非常接近，与此形成对比的是，当丢弃率从 0.2 上升到 0.5 时，DRP 和 NRRP 的数据包被拦截率有明显提高，说明这 2 种算法在高丢弃率下的性能较差。因为当丢弃率较大时，在构造安全路径时能够比较容易地将恶意节点排除在外，从而使得 SPDC 获得较好的性能，抵消了由于丢弃率上升所导致的被丢弃数据包增多的影像。而对于 DRP 和 NRRP 而言，较大的丢弃率就意味着被丢弃的数据包较多，从而导致性能下降。

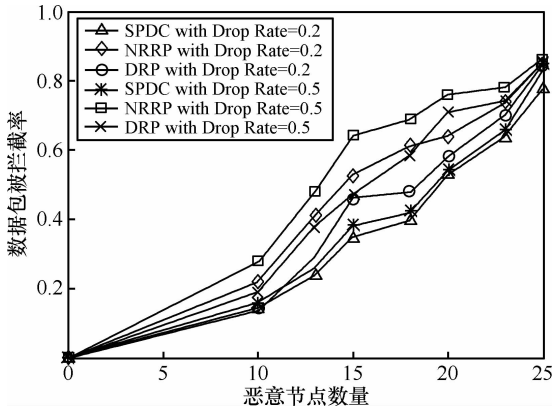

图 3　算法在不同丢弃率下的数据包被拦截率比较

4.3　源节点集合的性能分析

文献[4]的方法在进行模拟实验时，只针对单一源节点发送数据给汇聚节点的情况进行模拟。然而，使用单一源节点并不能很恰当地模拟无线传感器网络的情况。在实际应用中，无线传感器网络中的数据往往是由分布式的传感器节点产生的。事实上，对于单一源节点而言，只要存在安全路径，那么 SPDC 算法总能达到很好的性能。因此，为了更好地评价方法，还必须对多个源节点或者一个源节点集合进行模拟实验。按照表 1 的设定，选取了 10 个源节点，每个源节点都会产生数据和接受数据收集。通过统计源节点集合的整体性能来进一步验证方法，对于源节点集合进行模拟的过程和单一源节点是完全类似的。通过将所有源节点的模拟结果进行累加和归一化，就是最终的整体性能。通过图 4 可以发现，在相同恶意节点数量条件下，SPDC 的性能要优于 DRP 和 NRRP。但是，在作用于源节点集合时，3 种算法的性能差距并不明显。

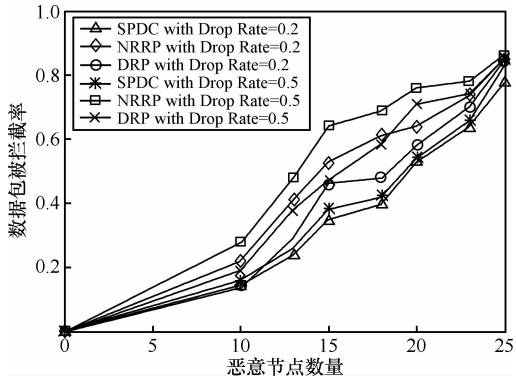

图 4　算法作用于源节点集合时的数据包被拦截率比较

5　结束语

针对无线传感器网络中的数据收集问题，提出了一种新型的基于多路径反馈的安全数据收集方法。该方法的核心内容是一种新的“跟踪—反馈”机制，该机制充分利用了无线传感器网络的路由功能，改善了数据传输的质量，提高了数据收集的可靠性。这种方法的主要优势在于，安全路径的构造是数据收集过程的“副产品”，本身并不会对网络的性能造成过分的影响，却为后续的数据收集提供了潜在安全的路由路径。安全路径的构造过程复杂性低，对传感器节点的性能影响相当有限。和一般的随机多路径路由方法相比，却更加安全可靠。与现有的相关工作相比较，该方法的算法复杂度较低，能够适应传感器节点资源受限的特征。根据模拟实验的结果，该方法的性能要优于类似的方法。

参考文献：

[1] LOW K S, WIN W N, ER M J. Wireless sensor networks for industrial environments[J]. Mater Sci Forum, 1992,119: 83-87.

[2] AKYILDIZ F, SU W, SANKARASUBRAMANIAM Y, *et al*. A survey on sensor networks[J]. IEEE Communications Magazine, 2002, 40(8): 102-114.

[3] TSIRIGOS A, HAAS Z J. Multipath routing in the presence of frequent topological changes[J]. IEEE Communication Magazine, 2001, 39(11): 132-138.

[4] SHU T, LIU S, KRUNZSECURE M. Data collection in wireless sensor networks using randomized dispersive routes[A]. Proc IEEE INFOCOM Conference[C]. Brazil, 2009. 2846-2850.

[5] LOU W, KWON Y. H-spread: a hybrid multipath scheme for secure and reliable data collection in wireless sensor networks[J]. IEEE Transactions on Vehicular Technology, 2006, 55(4): 1320-1330.

[6] LEE P C, MISRA V, RUBENSTEIN D. Distributed algorithms for secure multipath routing in attack-resistant networks[J]. IEEE/ACM Transactions on Networking, 2007, 15(6): 1490-1501.

[7] NASSER N, CHEN Y. SEEM: secure and energy-efficient multipath routing protocol for wireless sensor networks[J]. Computer Communications, 2007, 30(11-12): 2401-2412.

[8] AKYILDIZ I F, SU W, SANKARASUBRAMANIAM Y, *et a1*. Wireless sensor networks: a survey[J]. Computer Networks, 2002, 38(4): 393-422.

[9] IOANNIS K, DIMITRIOU T, FREILING F C. Towards intrusion detection in wireless sensor networks[A]. Proc the 13th European Wireless Conference[C]. France, 2007.

[10] SHAMIR A. How to share a secret[J]. Communication of the ACM, 1979, 22(11): 612-613.

作者简介：

毛郁欣（1980-），男，浙江龙泉人，博士，浙江工商大学讲师，主要研究方向为语义 Web、无线传感器网络。