无线传感器网络安全研究综述

陈 娟, 张宏莉

(哈尔滨工业大学 计算机科学与技术学院, 150001 哈尔滨, janechen. hit@ gmail. com)

摘 要: 由于无线传感器网络中的节点在计算能力、电池容量以及存储能力上受到限制,使得 WSNs 面临较多的安全威胁. 针对 WSNs 的安全问题首先简要回顾 WSNs 安全问题的早期研究成果;其次,将近年来 WSNs 的安全问题划分为密码算法与密钥管理、安全路由、安全数据融合、安全定位及隐私保护 5 个方面,并深入讨论这 5 个方面的攻、防策略. 最后,指出异构 WSNs、内部攻击攻、防策略以及隐私保护等 3 个方面是 WSNs 安全领域未来的热点研究方向.

关键词: 无线传感器网络;物联网;安全;综述;新进展

中图分类号: TP393. 08 **文献标志码:** A **文章编号:** 0367 - 6234(2011)07 - 0090 - 06

Survey on wireless sensor network security

CHEN Juan, ZHANG Hong-li

(School of Computer Science and Technology, Harbin Institute of Technology, 150001 Harbin, China, janechen. hit@ gmail. com)

Abstract: Wireless sensor networks are composed of sensor nodes which are limited in computational capabilities, power and memory resources, and they are susceptible to a variety of security threats. Security issues in WSNs have are the research focus in academy and industry. First, the early existing research results in wireless sensor network security was briefly surveyed, and then the security issues in WSNs were classified into five categories: cryptography algorithms and key management, secure routing, secure data aggregation, secure location, and privacy preservation. The mechanisms and characteristics of various techniques of these issues were described, while the focus was put on these new techniques that had been developed in recent three years. Finally on the basis of a comprehensive comparison and analysis of these existing techniques, it is points out that the heterogenous WSNs, inside attack and defensive techniques as well as privacy preservation techniques are the hot topics and future research trends in WSNs.

Key words: wireless sensor network; network of things; security; survey; advance

无线传感器网络(Wireless Sensor Networks, WSNs)是由部署在监测区域内的大量廉价微型传感器节点组成的无线 ad hoc 网络. 然而,与一般的 ad hoc 网络不同,WSNs 中的节点在计算能力、电池容量以及存储能力上受到限制,使得 WSNs 更易受到各种安全威胁. 尽管 WSNs 的安全问题较早提出,然而,近年来才引起较多研究者的关注. 尤其是近年来,WSNs 中经典的安全问题得到更多关注,许多新的安全问题如隐私保护等也被提出. 目前,已有一些文献对 WSNs 的安全问题进行综述,提供了有价值的参考资料. 然而,文献[1-2]仅对 2006 年及以前的安全问题进行了综述. 由于相关研究的发展速度很快,有必要对近年来 WSNs 安全问题的最新研究情况进行归纳总结,着重讨论一些重要的发展方向,供研究者参考. 本文重点综述 2006 年以后 WSNs 安全问题的研究新进展,其中,涵盖了大量近年来最新的主要研究成果.

收稿日期: 2010 - 04 - 06.

基金项目: 国家重点基础研究发展规划基金资助项目(2005CB321806, 2007CB311100);国家高技术研究发展计划基金资助项目(2009AA012437).

作者简介: 陈 娟(1982—),女,博士研究生;
张宏莉(1973—),女,教授,博士生导师.

1　WSNs 安全问题的早期研究成果

WSNs 安全问题的早期研究，从网络拓扑结构上而言，主要集中于单层传感器网络（即相对于多层传感器网络而言，网络中所有节点的性能与功能均相同）和静态传感器网络安全问题的研究；从安全解决方案的性能而言，在重点关注安全性能的同时并未足够重视能量的损耗；此外，从使用的技术和方法以及这些技术和方法所满足的安全需求而言，早期的解决方案与近年来的研究也有不同之处. 本文从 WSNs 安全问题的主要研究领域出发，将 2006 年及其以前的研究内容与 2006 年以后的研究内容进行对比，如表 1 所示. 通过表 1 的对比，帮助相关研究者总结早期安全问题研究的重点以及早期解决安全问题所使用的技术方法，同时，帮助研究者把握该领域近年来的研究动态.

表 1　WSNs 安全问题研究内容对比

主要研究领域	早期的主要研究内容	近年来的研究内容
密码与密钥管理	单层传感器网络密钥管理；在考虑安全性能的同时未重点考虑能量损耗.	分层传感器网络密钥管理[3]；轻量级、强安全保障的密钥管理协议[4].
安全路由	单层传感器路由协议；基于可信（reputation-based）的安全路由协议.	多路径安全路由协议[5]；分层传感器网络安全路由协议[6].
安全数据融合	使用纯密码方法提供安全服务；使用基于对称隐私同态（Privacy Homomorphism，PH）密码.	开始考虑受害的融合节点修改数据的情况[7]；使用水印而非 PH 技术实现安全数据融合[8].
安全定位	单层传感器网络安全定位；节点合作检测受害节点保障节点定位的安全性.	分层传感器网络的安全定位[9]；轻量级安全定位方法[10].
隐私保护	极少相关研究.	面向数据的隐私保护[11-12]；面向上、下文的隐私保护[13-14].

2　密码与密钥管理研究新进展

密码与密钥管理是建立 WSNs 安全体系结构的第 1 步，因为所有的加密与认证操作均离不开密码算法与密钥管理. 由于 WSNs 自身硬件资源受限等特点，某些经典的密码算法无法直接用于传感器网络中. 近年来，研究者从不同角度对各种密码算法进行评估，为 WSNs 的密码算法选择提供参考. 与此同时，近年来的密钥管理研究也呈现出一些新的特点如分层传感器网络的密钥管理等，本文对其中具有代表性的一些方法进行介绍.

2.1　密码算法

目前已有许多文献[15-16]对 WSNs 的密码算法进行评估. Ganesan 等对一些密码算法如 RC4、IDEA、RC5、MD5 和 SHA1 的计算开销进行评估且在不同的硬件平台上运行这些密码算法，最终的实验结果表明 RC4 在低端处理器上的性能优于 RC5，而哈希技术需要大约 10 倍于 RC4 的计算开销.

相较于以往只考虑计算开销、能量损耗与安全性能等因素，Liu 等认为 SRAM 对于网络操作具有关键作用并首次将 SRAM 作为一个评估密码算法性能的标准.

2.2　密钥管理

近年来，密钥管理方案在提供安全性保障的同时，更加关注能量的损耗、网络的连通性、占用的存储空间及计算复杂度等问题. 此外，分层传感器网络的密钥管理方案也成为研究的热点.

2.2.1　单层传感器网络密钥管理

对于传统的单层传感器网络，研究者提出一些新的密钥管理方案. 从性能上而言，这些方案具有较低的能量损耗及存储空间需求，同时具有更强的安全保障.

Zhang 等首次将一种基于随机微扰的策略（Random Perturbation-Based，RPB）用于成对（pairwise）密钥建立. RPB 是第 1 个能够同时满足 5 个安全需求的成对密钥建立方案：1）考虑大规模已受害节点的情况；2）保证任意 2 个节点间建立密钥；3）保证节点间直接建立密钥；4）适用由于节点移动造成的网络拓扑改变；5）对于资源抑制的 WSNs 有效. 在该策略中，Zhang 定义了一系列变量：F_q 为预先定义的一个有限域，其中 q 为预先定义的一个很大的素数；l 为满足 $q < 2^l$ 的最小整数；r 为满足 $q > 2^r$ 的最大整数；L 为预先定义的成对密钥的长度；$S \in \{0,1,\cdots,q-1\}$ 为 WSNs 中节点编号的集合；Φ 为微扰多项式集合. 该方法主要分为 3 个阶段：

1）系统初始化阶段：在 F_q 上随机构建 m 个二元对称多项式 $f_i(x, y)(i = 0,\cdots,m-1)$，其中 $m = \lceil l/(l-r) \rceil$，同时在 F_q 上构建单变量微扰多

项式集合 $\boldsymbol{\Phi}$.

2) 微扰多项式预分配阶段:为每个节点分配1个ID号及 m 个单变量多项式. 如对于ID号为 u 的节点,分配的 m 个多项式为 $g_{u,i}(y) = f_i(u,y) + \phi_{u,i}(y)$, $(i = 0,\cdots,m-1)$, 其中 $\phi_{u,i}(y)$ 为从 $\boldsymbol{\Phi}$ 中随机选取的1个多项式.

3) 成对密钥产生阶段:为了获取 u 与 v 的成对密钥,计算 m 个多项式的值 $g_{u,i}(v) = f_i(u,v) + \phi_{u,i}(v)(i = 0,\cdots,m-1)$, 其中 $g_{u,i}(v)$ 为 l 位. 由于微扰多项式 $\phi_{u,i}(v)$ 的加入,影响对称多项式 $f_i(x, y)$ 的低 r 位,因此选取 $g_{u,i}(v)$ 的高 $l-r$ 位,即 $S_{u,i}(v)$ 作为对称密钥的一部分. 最终,节点 u 与 v 的成对密钥为 m 个部分密钥值的连接 $K_{u,v} = (|S_{u,0}(v)|, |S_{u,1}(v)|,\cdots, |S_{u,m-1}(v)|)$. 之后,Chia 等[17]在此基础上提出一种基于向量的随机微扰成对密钥建立策略,不仅满足上述5个安全需求,同时具有可扩展性和独立于硬件的特性.

2.2.2 分层传感器网络密钥管理

在分层传感器网络中,所有节点被划分为若干簇,每个簇内有一个能力较强的节点,称为簇头,普通节点的密钥分配、协商、更新等都是通过簇头来完成的. 早期的分层传感器网络协议非常少,其中,典型的有 LEAP 协议. LEAP 不仅满足私密性和数据认证的基本安全需求,而且提供不同的通信方案. 然而,该协议在节点部署后的一个特定的时间内必须保留全网的公共密钥,因为公共密钥的泄露会威胁到整个网络的安全. 近年来分层传感器网络尤其是异构传感器网络(Heterogeneous Sensor Networks, HSNs)的密钥管理成为研究的热点.

文献[3]提出一种适用于 HSNs 的成对密钥建立方案,与其他密钥建立方案不同的是,该方案在网络中布置多个微密钥服务器,使得任意相邻节点能够以一个较高的概率在两跳内发现一个微密钥服务器. 同时,该方案使用一个可信当局(Trust Authority, TA)存储密钥的一些基本信息如 s 个 k 比特位的主密钥与认证密钥:$K_1,\cdots, K_s, {}^aK_1,\cdots, {}^aK_s$ 以及1个哈希函数 $h:\{0,1\}^k \times \{0,1\}^k \rightarrow \{0,1\}^k$. 该方案的主要思想为:首先对 WSNs 中的节点进行分组并计算每个节点的私有密钥. 如节点 i 的组号为 $u_i = i \bmod g$, 其中 g 为预先定义的组的个数. 每个节点有 $2s$ 个私有密钥,节点 i 的 $2s$ 个私有密钥为:$K_{u_i,j} = h(K_j, u_i)$ 与 ${}^aK_{u_i,j} = h({}^aK_j, u_i)$, $(j = 1,\cdots,s)$, 可以看出,同一组中的节点具有相同的私有密钥. 其次,TA 为每个节点和每个微密钥服务器分发公共密钥. 最后,2节点 i 与 j 建立通信密钥,过程为:若节点 i 与节点 j 在同一分组中,则节点 i 可产生一个会话密钥并用2节点的公共密钥对该会话密钥进行加密,发送给节点 j,该会话密钥即为2节点间的通信密钥. 若2节点不在同一个分组中,此时建立通信密钥的情况分为3种:1) 若2节点具有共同的公共密钥,则节点 i 产生通信密钥,并用该公共密钥对通信密钥进行加密发送至节点 j; 2) 若2节点没有共同的公共密钥,则节点 i 求助于附近的微密钥服务器建立2节点间的通信密钥;3) 若2节点间没有共同的公共密钥且节点 i 无法与任何的微密钥服务器建立连接,则使用文献[4]的方法为2节点建立路径密钥. 该方案在不使用较多的通信开销和存储开销的同时,有效的提高了网络抵御节点攻击的能力.

3 安全路由研究新进展

Karlof 等[18]已对早期的 WSNs 路由攻击类型及防御方法进行综述. 近年来,针对传统的单层传感器网络,研究者开始关注安全多路径路由协议并研究如何避开已受害节点和"潜在"受害节点的安全路由协议;此外,分层传感器网络的安全路由协议也是近年来的一个研究重点.

3.1 单层传感器网络路由协议

针对 WSNs 的单路径和多路径路由协议已有较多研究,然而,这些路由协议仅关注传感器网络中每个节点能量的有效使用,并未考虑安全问题. 为此,Nasser 等提出安全的多路径路由协议(Secure and Energy-Efficient Multipath Routingprotocol, SEER),该协议首次综合考虑路由协议的安全性和能量的损耗. 与以往使用源节点或目的节点进行路径发现不同,SEER 使用基站寻找从源节点到目的节点的多条路径. 此后,Shu 等[19]提出安全的随机多路径路由协议,该协议在发现多条随机路径的同时具有较低的能量开销. 由于其随机性,即使攻击者获得路由算法,也无法获得每个数据包的发送路由,因此能有效的避开黑洞攻击.

3.2 分层传感器网络的安全路由协议

大多数分层传感器网络的路由协议均结合密钥算法提供安全服务. Ruan 等在 LEACH 的基础上,使用改进的随机对密钥策略,充分考虑节点资源有限性,在增强路由算法安全性的同时减少了算法的开销. 分层传感器网络由于其结构的特殊性,在为安全解决方案带来便利的同时引入了额外的层次结构管理开销,值得关注.

4　安全数据融合研究新进展

在数据融合过程中，基站发出查询请求，普通节点（General Nodes，GNs）搜集感知数据并发送给数据融合节点（Aggregator Nodes，ANs），ANs 对感知数据进行融合并将融合后的数据发送给基站. 尽管数据融合能够极大地降低通信开销，却带来更多的安全问题. 一般而言，数据融合的攻击可分为 2 类：1）受害的 GNs 修改数据并发送给 ANs；2）受害的 ANs 在数据融合的过程中修改数据并发送给基站. 抵御这 2 类攻击的方法主要有基于明文的方案和基于密文的方案. 对于前者，ANs 能够获得传输数据的内容；对于后者，数据融合是基于加密的数据.

4.1　基于明文的安全数据融合协议

以往，基于明文的安全数据融合协议主要研究受害的 GNs 修改数据的情况，关注使用纯密码方法提供安全服务. 相较于以前的研究，近年来，基于明文的安全数据融合协议开始考虑受害的 ANs 修改数据的情况.

文献[8]研究受害的 ANs 修改融合数据的情况. 其中，Sun 等从入侵检测的角度，提出基于卡尔曼滤波机制的数据检测方法. 并针对不同的融合函数如加、平均、最大、最小等，从理论上得到数据融合值的正常范围，若融合结果超出这个范围，则认定数据被修改.

4.2　基于密文的安全数据融合协议

以往，基于密文的方案大多使用对称的 PH 密码、使用单层的安全数据融合协议. 近年来，研究者尝试使用非对称的 PH 密码方法、使用水印而非 PH 技术实现安全数据融合、扩展单层的数据融合协议到多层的数据融合协议.

基于密文的数据融合方案大多使用 Ferrer[20] 提出的 PH，这是一种特殊的编码转化，允许在加密数据上直接进行加法和乘法计算.

目前，基于 PH 的内网数据融合协议仅适用于一些特定的融合函数，对于大多数基于查询的融合函数无能为力. Zhang 使用水印技术而非 PH 实现安全的数据融合. 该方法的主要思想为：首先，每个节点被赋予一个小的随机值即水印，水印与感知数据相加后作为水印值发送给簇头节点；其次，簇头节点在接收到水印值后，对该值进行压缩并发送给基站；最后，基站对接收到的压缩数据进行评估并确定水印，通过水印验证接收到的数据是否被修改. 图 1 是该方法的一个流程图. 该方法突破了 PH 技术仅对某些特定函数提供安全支持的限制，与此同时，由于水印的嵌入过程非常简单且能量有效，该方法适用于资源抑制的 WSNs.

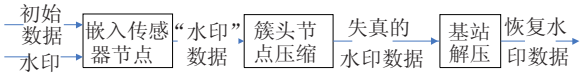

图 1　基于数字水印的数据融合方法工作流程图

5　安全定位研究新进展

在 WSNs 的许多应用中，可靠和精确的位置信息是非常重要的，因此，需要保障节点定位的安全性. 某些传感器节点预先具有自身的位置信息或某些传感器节点使用 GPS 进行自身定位，本文称这类传感器节点为信标节点. 近年来，轻量级安全定位方法、分层传感器网络的安全定位方法以及针对节点定位的新型攻击形式等都是研究的重点.

与以往使用大量节点共同检测已受害节点的方式不同，文献[10] 使用一种松弛标记结构进行节点定位. 算法将 3 个节点分为 1 组，使用松弛标记方法监测这些组的行为. 通过对组内各节点行为的观察进行恶意节点检测. 一旦检测到恶意节点，算法摒弃恶意节点，使用正常节点所传送的报文进行节点定位. 与此同时，基于以往的研究，Sheng 等从理论上证明若恶意信标节点的数量 $> (n-2)/2$，则没有算法能够提供任何程度上的安全定位，其中 n 为信标节点的数量. 同时，他们发现当受害的信标节点数量 $\leqslant (n-3)/2$ 时，存在算法进行节点的安全定位，否则不存在. 这一研究成果为当前及未来基于信标节点的安全定位提供了理论指导.

6　隐私保护研究新进展

以数据为中心的 WSNs，数据在传输、搜集和分析的过程中，数据隐私的保护应当给予足够的重视. 然而，过去几乎没有对 WSNs 隐私保护研究. 目前对 WSNs 数据隐私保护的研究依然较少，针对已有的研究成果，本文将其分为面向数据的隐私保护和面向上、下文的隐私保护.

6.1　面向数据的隐私保护

面向数据的隐私保护用于保护数据内容的隐私. 其中，数据不仅仅是传感器节点搜集的感知数据，也包括用户向 WSNs 所提交的查询信息. 目前，面向数据的隐私保护主要指抵御来自 WSNs 内部的攻击.

He 等提出 2 种数据隐私保护方法：SMART（Slice-mixed Aggregation）与 CPDA（Cluster-based Private Data Aggregation）. 2 种方法均关注加操作且依赖邻节点的合作对原始数据进行隐藏. 在

SMART 方法中,源节点将数据切割成片后加密发送,因而中继节点无法获得完整的数据,从而实现了对数据隐私的保护. SMART 由数据切割、数据混合及数据融合 3 个阶段组成.

1) 数据切割阶段. 首先,每个节点 $i(i = 1, \cdots, N)$ 随机选取距该节点 h 跳内的 j 个节点,该 j 个节点组成节点集合 $S_i(j = |S_i|)$;其次,节点 i 将数据切割成 j 片并对其中的 $j-1$ 片进行加密;最后,节点 i 保留其中的 1 个数据片并将剩余的 $j-1$ 个数据片发送至从 S_i 中随机选取的 $j-1$ 个节点中.

2) 数据混合阶段. 每个节点 j 对搜集到的所有数据片进行解密并计算数据片的总和 $r_j = \sum_{i=1}^{N} d_{ij}$. 其中 d_{ij} 为从节点 i 发送至节点 j 的数据片.

3) 数据融合阶段. 采用基于树的路由协议,每个节点对其所接收到的所有数据 $r_i(i = 1, \cdots, N)$ 进行融合处理并发送至父节点,最后的融合数据发送至查询服务器. SMART 与 CPDA 均为原始数据提供一定的隐私保护,然而它们均只支持加操作,此外,它们抵御共谋攻击的能力有限. 之后,Zhang 等提出一种抵制共谋攻击的隐私保护技术,能够支持多种融合函数.

6.2 面向上、下文的隐私保护

面向上、下文的隐私保护即对数据发送和转发的时间和位置等信息进行保护. 根据上、下文信息内容的不同,主要分为位置隐私保护和时间隐私保护.

6.2.1 位置隐私保护

敌方能够通过所获取的数据推断出数据源或基站的位置信息. 文献[15]通过改进洪泛路由和单路径路由协议对数据源的位置进行保护. 路由协议分为:

1)随机转发阶段. 数据包从数据源节点被随机转发若干跳.

2)依概率转发阶段,使用洪泛路由或单路径路由协议对随机转发后的数据包进行路由,其中,每个节点仅以一定的概率广播或转发数据包,因此,敌方无法获取参与转发数据包的节点集合,继而无法追踪到数据源的位置. 然而,文献[21]表明:经过若干步纯粹的随机转发后,数据包依然位于数据源节点附近,因而很容易泄露源节点的位置信息. Xi 等对此进行了改进,提出一种双路贪婪随机转发方案.

6.2.2 时间隐私保护

时间隐私为数据源产生数据的时间、节点接收到数据的时间以及数据发送到基站的时间. Pandurang 提出一种速率可控的自适应时间隐私保护方案. 在该方案中,数据包经过中继节点后,不直接被转发,而是缓存一个随机时间 t, 因此,数据包在每个节点的传输时延各不相同,避免时间信息的泄露.

7 结 论

1)在安全路由协议方面,目前的安全路由协议均考虑受害节点已被检测的情况,对于尚未检测到的已受害节点,安全的路由协议如何避开?

2)分层传感器网络利用其特殊的网络结构为解决安全问题提供便利,同时也带来簇管理开销等一系列问题.

3)隐私保护技术涉及多学科交叉且发展时间较短,目前,WSNs 的隐私保护,国内外的研究均处于起步阶段.

参考文献:

[1] 李 平, 林亚平, 曾玮妮. 传感器网络安全研究[J]. 软件学报, 2006, 17(12): 2577 - 2588.

[2] DJENOURI D, KHELLADI L, BADACHE A N. A survey of security issues in mobile ad hoc and sensor networks[J]. IEEE Communications Surveys & Tutorials, 2005, 7(4): 2 - 28.

[3] ESCHENAUER L, GLIGOR V. A key-management scheme for distributed sensor networks [C]//Proceedings of the 9th ACM Conference on Computer and Communications Security. New York, NY: ACM, 2002: 41 - 47.

[4] ZHANG W S, TRAN M, ZHU S C, *et al.* A random perturbation-based scheme for pairwise key establishment in sensor networks [C]//Proceedings of the 8th ACM International Symposium on Mobile ad Hoc Networking and Computing. New York, NY: ACM, 2007: 90 - 99.

[5]NASSER N, CHEN Y F. Secure multipath routing protocol for wireless sensor networks nasser [C]//Proceedings of the 27th International Conference on Distributed Computing Systems Workshops (ICDCSW'07). Washington DC: IEEE Computer Society, 2007: 12 - 12.

[6] ZHANG K, WANG C, WANG C, *et al.* A secure routing protocol for cluster-based wireless sensor networks using group key management [C]//Proceedings of the 4th International Conference on Wireless Communications, Networking and Mobile Computing(WiCOM'08). Washington, DC: IEEE, 2008: 12 - 14.

[7] SUN B, JIN X, WU K, *et al.* Integration of secure in-network aggregation and system monitoring for wireless

sensor networks [C]//Proceedings of IEEE International Conference on Communications (IEEE ICC'07). Washington, DC: IEEE, 2007: 1466 – 1471.

[8] ZHANG W, LIU Y H, DAS S K, *et al.* Secure data aggregation in wireless sensor networks: A watermark based authentication supportive approach [J]. Pervasive Mobile Computing, 2008, 4(5): 658 – 680.

[9] CHANG C-C G, SNYDER W E, WANG C. A new relaxation labeling architecture for secure localization in sensor networks [C]//Proceedings of the Communications (ICC'07). Washington, DC: IEEE, 2007: 3076 – 3081.

[10] ZHONG S, JADLIWALA M, UPADHYAYA S, *et al.* Towards a theory of robust localization against malicious beacon nodes [C]//Proceedings of the 27th Conference on Computer Communications. Washington, DC: IEEE, 2008: 1391 – 1399.

[11] HE W B, LIU X, NGUYEN H, *et al.* PDA: Privacy-preserving data aggregation in wireless sensor networks [C]//Proceedings of the 26th IEEE International Conference on Computer Communications. Washington, DC: IEEE, 2007: 2045 – 2053.

[12] ZHANG W S, WANG C, FENG T M. GP2S: Generic privacy-preservation solutions for approximate aggregation of sensor data (concise contribution) [C]//Proceedings of the Sixth Annual IEEE Communications (PerCom). Washington, DC: IEEE, 2008: 179 – 184.

[13] KAMAT P, XU W Y, TRAPPE W, *et al.* Temporal privacy in wireless sensor networks [C]//Proceedings of the 27th International Conference on Distributed Computing Systems (ICDCS). Washington, DC: IEEE, 2007: 23 – 23.

[14] KAMAT P, ZHANG Y Y, TRAPPE W, *et al.* Enhancing source-location privacy in sensor network routing [C]//Proceedings of the 25th IEEE International Conference on Distributed Computing Systems (ICDCS). Washington, DC: IEEE, 2005: 599 – 608.

[15] GANESAN P, VENUGOPALAN R, PEDDABACHAGARI P, *et al.* Analyzing and modeling encryption overhead for sensor encryption overhead for sensor network nodes [C]//Proceedings of the 2nd ACM International Conference on Wireless Sensor Networks and Applications. New York, NY: ACM, 2003: 151 – 159.

[16] LIU W, LUO R, YANG H Z. Cryptography overhead evaluation and analysis for wireless sensor networks [C]//Proceedings of the 2009 WRI International Conference on Communications and Mobile Computing. Washington, DC: IEEE Computer Society, 2009: 496 – 501.

[17] YU C M, CHI T Y, LU C S, *et al.* A constrained random perturbation vector-based pairwise key establishment scheme for wireless sensor networks [C]//Proceedings of the 9th ACM International Symposium on Mobile ad hoc Networking and Computing. New York: ACM, 2008: 449 – 450.

[18] KARLOF C, WAGNER D. Secure routing in wireless sensor networks: Attacks and countermeasures [J]. Elsevier's Ad Hoc Networks Journal, Special Issue on Sensor Network Applications and Protocols, 2003, 1(2/3): 293 – 315.

[19] SHU T, LIU S S, KRUNZ M. Data collection in wireless sensor networks using randomized dispersive routes [C]//The 28th Conference on Computer Communications (INFOCOM'09). Washington, DC: IEEE, 2009: 2846 – 2850.

[20] FERRER J D. A provably secure additive and multiplicative privacy homomorphism [C]//Proceedings of the 5th International Conference on Information Security. London, UK: Springer-Verlag, 2002: 471 – 483.

[21] XI Y, SCHWIEBERT L, SHI W S. Preserving source location privacy in monitoring-based wireless sensor networks [C]//Proceedings of the 20th International Parallel and Distributed Processing Symposium (IPDPS). Washington, DC: IEEE, 2006: 25 – 29.

（编辑　张　红）