

文章编号:1001-9081(2010)03-0688-04

无线传感器网络基于分组协商的数字水印算法

蔡少杰¹, 林亚平^{1,2}, 易叶青¹, 叶松涛¹

(1. 湖南大学 计算机与通信学院, 长沙 410082; 2. 湖南大学 软件学院, 长沙 410082)

(shaojie_lh@126.com; csj_lh@163.com)

摘要:无线传感器网络通常具有分布式数据采集与网内数据处理的特点,因此基于传统数字水印的安全技术难以直接用于传感器网络;针对传感器网络聚类分层的体系结构,通过在簇内建立分组协商机制来生成待嵌入水印,在此基础上实现了一种新的分布式数字水印算法。传感器节点以分组的形式嵌入水印,计算复杂度低,水印具有良好的抗攻击性和对有损压缩的鲁棒性。实验结果表明用该算法嵌入的水印可检测性强,能够成功地鉴别数据是否被非法篡改,保护传感器网络数据安全。

关键词:无线传感器网络;安全;分组协商;数字水印;数据可靠性

中图分类号: TP393 **文献标志码:** A

Group negotiation-based digital watermarking for wireless sensor network

CAI Shao-jie¹, LIN Ya-ping^{1,2}, YI Ye-qing¹, YE Song-tao¹

(1. School of Computer and Communication, Hunan University, Changsha Hunan 410082, China;

2. Software School, Hunan University, Changsha Hunan 410082, China)

Abstract: Traditional digital watermarking cannot be applied directly in Wireless Sensor Network (WSN) that has special features, such as collecting data in distributed sub-clusters and processing data in-network. According to the hierarchical clustering architecture of WSN, a distributed consultative mechanism was established in clusters to generate the proper watermarking; thus, a distributed watermark algorithm was proposed. Sensor nodes of each group were embedded with watermarks with low computational complexity. The watermarks have shown the superiority of resistance to the attacks and the robustness of the lossy data compression. The results of analysis and experiments show that the watermarking proposed is easy to be checked. It can successfully identify whether data had been illegally tampered and thus effectively protect the security of WSN.

Key words: Wireless Sensor Network (WSN); security; group negotiation; digital watermarking; data reliability

0 引言

无线传感器网络(Wireless Sensor Network, WSN)是由一组随机分布的传感器节点通过自组织方式构成的网络,能广泛应用于军事、环境科学、医疗健康、空间探索和灾难拯救等各种领域^[1]。由于传感器节点结构简单,功能有限,通常部署在敏感、复杂的环境之中,无线传感器网络面临着多种特殊的数据安全威胁(如对数据内容恶意篡改、虚假数据攻击等),如何保障其数据的真实性、可靠性、完整性显得尤为重要。

与传统网络不同,这种以数据为中心的新型网络主要目的是收集监测环境的数据,其网内数据具有分布式的特性,为了节约有限的网络资源,在网内通常进行聚合处理,即在网内基于用户兴趣对所采集的数据进行复合子集选择。数字水印技术^[2-3]可在不影响数据原有特性的情况下将水印信息以不可感知的形式嵌入数据集中,仅从表面难以发现水印存在,只有专用的检测算法才能检测出隐藏的数字水印,且无须增加额外的存储和通信开销,这无疑将会给资源受限的新型网络的数据的安全保存和传递开辟一条新的途径。然而,现有的

水印技术主要针对传统网络环境,算法往往是针对一种具体的载体而设计的(比如图像、视频等),具有集中式数据处理的特性,一般不需要考虑网内的聚合处理;而且其所处的网络环境无论是自身的资源还是安全性要比传感器网络更有保障。因此,在无线传感器网络中应用传统数字水印的技术将面临许多问题与挑战,如何设计一种有效解决传感器网络中数据安全问题的水印机制,需要探索新的理论与方法。

本文结合无线传感器网络的体系结构特点对如何在分布式的感知数据中嵌入数字水印进行了深入的研究。无线传感器网络通常采用聚类分层的体系结构,通过对簇内的节点进行进一步的分组,使组中节点以协商方式构造出待嵌入的水印数据,建立了一个传感器节点水印分组协商机制,并在此基础上实现了一种在所有节点上运行的鲁棒的分布式数字水印嵌入算法,能够有效地提高传感器数据的安全性与可靠性。

1 相关工作

目前对于传感器网络中数字水印技术的应用研究仍处于探索阶段,已经在传感器网络中出现的一些数字水印技术如下。

收稿日期:2009-09-01;修回日期:2009-10-26。

基金项目:国家自然科学基金资助项目(60973031);湖南省自然科学基金资助项目(09JJ6097);湖南省科技计划项目(2009FJ3083)。

作者简介:蔡少杰(1983-),男,河南漯河人,硕士研究生,主要研究方向:无线传感器网络;林亚平(1955-),男,湖南邵阳人,教授,博士生导师,CCF高级会员,主要研究方向:计算机网络、机器学习;易叶青(1976-),男,湖南邵阳人,博士研究生,主要研究方向:数字水印、无线传感器网络安全;叶松涛(1983-),男,河南郑州人,博士研究生,主要研究方向:无线传感器网络。

Wong 等人^[4]提出利用传感器节点定位时允许距离的期望值与测量值之间有一定误差,通过修改测量值嵌入水印。该方法利用传感器节点感知数据可能有微量误差的特性,只要嵌入水印时引入的误差在限定范围内,就不会影响感知数据的正常使用;文献[5]在无线图像传感器网络中,从减小能耗角度考虑,利用基于小波自适应水印算法,对传输的数据嵌入可识别的图像标志水印信息。文献[6]作者以误差最小化为目标,根据传感器网络采集数据和处理数据阶段给系统添加附加的限制条件,嵌入水印信息。文献[7]论述了采用基于跳频扩频技术的数字水印、基于数字水印的认证技术来保障无线传感器网络的安全,并给出了一个简单数字水印设计实例。此外,易叶青等人^[8]提出了多重半脆弱水印机制用于过滤无线传感器网络中的虚假数据,在探讨无线传感器网络中的数字水印机制方面取得了一定的进展。

以上方法表明在无线传感器网络中采用数字水印技术来保护传感器网络中的感知数据是一种切实可行的方法,但上述多数方法只是沿袭了传统水印的思想,没有充分考虑传感器网络中节点分布式的采集,存储数据的特点;同时在无线传感器网络中还会对要传输的数据进行网内有损压缩来降低通信能耗,嵌入的水印必须具有一定的鲁棒性;目前已出现的水印算法并不适合传感器网络特点,无法直接将水印信息嵌入到传感器网络中随机分布的节点的数据包中。

2 簇内节点分组协商机制

2.1 网络体系结构与条件假设

假设无线传感器网络被部署在一个节点密集撒播的物理环境,该网络采用 LEACH (Low Energy Adaptive Clustering Hierarchy)^[9]路由协议实现聚类分层的组织方式(如图1)。图中整个网络被划分为一定数目的节点簇,每个簇内由簇头节点负责收集、处理传感器节点定期采集的数据,然后以多跳中继的形式向 Sink 节点转发聚合处理后的数据, Sink 节点位置比较安全,不容易被俘获妥协。

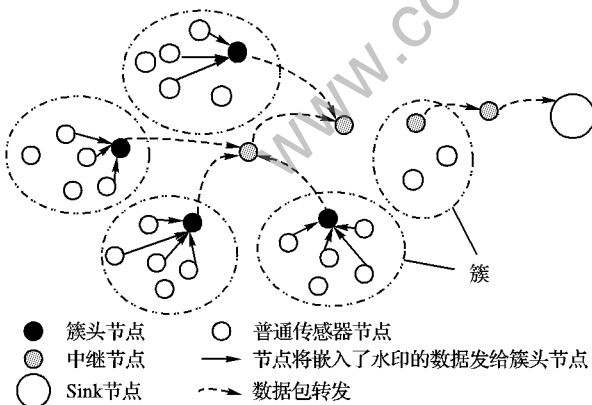


图1 网络聚类分层的体系结构

另外,假设所有的节点时间同步,节点向 Sink 发送感知数据包中含有自己的身份标识字段,网络在刚部署后的一段时间内是安全的,这段时间主要用来完成相应的初始化操作。节点与 Sink 节点可以进行加密通信,邻居节点之间通过建立对偶密钥加密节点之间的交换信息,如文献[10]所述。

依据网络的层次特点,对感知数据植入水印可以有以下两种方式。

1) 仅由每个簇的簇头节点对收集到的数据嵌入水印,

这样操作起来比较简单,因为簇内节点数据已经在簇头集中起来,只需要选择适当的水印算法,但这种方式存在很大的弊端:一方面,总是由簇头节点对数据植入水印,使得簇头的负担过重,增加了簇头节点的能量消耗,缩短了簇头的生存时间,容易引起频繁地更换簇头的问题,造成网络资源的浪费,减少网络整体生存时间;另一方面,一旦簇头节点被俘获或者被妥协,敌方很容易获得水印信息与密钥,伪造数据并植入水印信息,严重破坏网络中数据的真实性。

2) 另一种方式即在簇内传感器节点上进行数字水印的嵌入,更适合传感器网络体系结构的特点,簇头节点不知道簇内节点与数字水印相关的信息,只负责对节点数据的聚合处理与转发,这样在避免簇头节点负担过重的同时也降低了簇头被妥协时伪造数据、非法植入数字水印信息成功欺骗 Sink 节点的几率。

如果由每个节点自己负责生成水印数据与密钥,这样又过于分散,不利于管理,因此,折中地采用分组的方式来生成水印。在网络初始化阶段,分簇完成后紧接着对簇内节点进一步分组,组内节点通过密钥通信来协商生成要嵌入的水印信息,完成网络的初始化。

2.2 节点分组协商机制

2.2.1 节点参数预置

1) 每个节点都有一个 (FID, GID) 对,其中 GID 是节点唯一的身份标识号, FID 是节点的伪标识号,也是唯一的,该参数对在节点撒播前写入节点内部。Sink 节点中保存所有节点的 (FID, GID) 对应表。

2) 节点内置分组函数 $groupFunc(n_i, G, N) = G_i$ ($1 \leq G_i \leq G$), n_i 表示簇内传感器节点序号(节点序号不等于节点标识号), N 为簇内节点总数, G 为分组的总数, G_i 是分组函数对应输入 n_i 与 G 的输出,即所属组号码。

其中,参数 G 与 N 用来保证分组的结果使所有组的节点数量接近平均,因为如果某个组内节点过少,该组的数据占簇内总数据量的比例就偏小,当簇头对的所有嵌入水印后的数据进行有损压缩时,节点数目少的组因有损压缩而丢失水印的几率增大,容易导致整个簇的感知数据中的水印信息不完整。

2.2.2 分组协商过程

簇头先根据簇内节点总数确定合理的分组个数 G , 分组步骤如下。

第1步 每个节点用自己的伪标识号 FID 从簇头处注册获取一个序号 n_i , 节点的 n_i 值唯一并根据注册先后次序保持递增。簇头将 (n_i, G, N) 打包发给 FID 所属节点, 将所有节点的 (FID, n_i) 对和簇的 G, N 值发给 Sink 节点。

第2步 节点根据自己获得的序号 n_i 用分组函数 $groupFunc(n_i, G, N)$ 计算出所属的组号 G_i 。

第3步 同一组的节点用 FID 作为身份标识通过密钥通信相互获得组内其他节点的信息, 确认小组成员与通信密钥。

第4步 同一组的节点采用组密钥共同协商生成向感知数据中嵌入的水印信息, 组节点将水印信息通过密钥通信传递给 Sink 节点。

第5步 分组协商结束, 初始化工作完成, 分组后的效果如图2所示。

3 基于分组协商机制的数字水印算法

以第2章描述的分组协商机制为基础,设计并实现了一个新颖的分布式数字水印算法,具体内容如下所述。

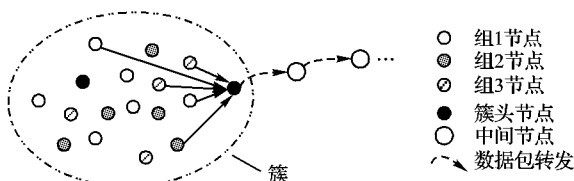


图2 节点分组效果

3.1 数字水印嵌入算法

算法描述如下。

输入 (x, d, w) 。 x 是要嵌入水印的感知数据; w 表示要嵌入的水印信息; d 为节点内部的一个参数,用作嵌入水印时的一个调制值,节点 i 的调制值表示为 d_i ,网络部署前每个节点的 d 值为 Sink 节点所已知(节点具有不同的 d 值,由 Sink 负责初始化)。

输出 嵌入水印后的感知数据 wx 。

第1步 如果 x 为小数,则将 x 分为整数部分 z 与小数部分 r 。

第2步 对整数 z 进行模 d 运算,运算结果为 m , m 对 2 求余得到 k , m 减去 $d/2$ 得到 dx 。

第3步 对 x 减去 dx 得到 wx 。

第4步 如果 k 等于 w 则转到第5步,否则将 wx 值增加 d 。

第5步 对 x 嵌入水印后的值 wx 添加一个正态分布的误差 $\Delta\lambda$,返回。

数字水印嵌入函数如下:

$$F(x, d, w) = \begin{cases} x - [(z \bmod d) - d/2], & k = w \\ x + d - [(z \bmod d) - d/2], & k \neq w \end{cases} \quad (1)$$

其中: z 为对 x 的取整结果; $k = (x \bmod d) \% 2$ 。

数据嵌入水印例子 假设某传感器网络节点对周围的温度、光度与湿度进行感知后获得数据 (T, H, L) , 其中: T 表示温度; H 表示湿度; L 表示光强度。接下来采用本小节提出的算法对传感器温度、湿度与光强数据嵌入水印。具体嵌入过程如下。

$$T = \begin{bmatrix} T_0 & T_1 \\ T_2 & T_3 \end{bmatrix} \text{表示簇内同一组的节点 } node[0, 1, \dots, 3]$$

的温度数据,这里为简单起见令所有节点的 d 值都取 2,假设初始数据为 $O: \begin{bmatrix} 25.2 & 23.0 \\ 24.5 & 26.1 \end{bmatrix}$,水印信息 $w = 1$,用函数 $F(O, w, d)$ 对 O 进行水印嵌入运算:

$$\begin{bmatrix} 25.2 & 23.0 \\ 24.5 & 26.1 \end{bmatrix} \xrightarrow{\text{嵌入}} \begin{bmatrix} 27.2 & 23.0 \\ 26.5 & 26.1 \end{bmatrix}$$

$$\text{输出结果为 } O + w: \begin{bmatrix} 27.2 & 23.0 \\ 26.5 & 26.1 \end{bmatrix}.$$

同上,湿度与光强数据采用同样的嵌入方式。

3.2 嵌入算法安全性与鲁棒性分析:

Sink 节点已知所有节点的 $pair(FID, n_i)$ 和 $pair(FID, UID)$,根据接收到的节点的 UID 信息,Sink 节点通过上边两个对应关系可以通过分组函数 $groupFunc()$ 计算得到相应节点的分组号 G_i 。根据 G_i 组在协商时密钥通信传递过来的水印

信息 w ,Sink 节点可以直接对数据中的水印真伪进行鉴别,判定感知数据是否可信。算法安全性分析如下。

1) 假设某个组的节点 a 被妥协,因为同一组节点间采用 FID 身份进行秘密通信,如果在通信范围内位置不相邻, a 无法通过窃听获知同组其他节点的 UID ,也无从知晓其 d 值,这时成功伪造同组节点的数据不太可能。如果 a 窃听它邻居节点 b 的数据包(a, b 在不同组),比较彼此监测的相同对象的数据,根据式(1)二者相减得到 $\Delta wdata = z \bmod d_b - z \bmod d_a + E_a - E_b + \Delta$,其中 Δ 是 a 与 b 两节点监测数据的测量误差,节点 a 根据 d_a 与 w 可以确定 E_a 大小。 E_b 未知,表示为 $d_b/2$ 或 $3d_b/2$ 。化简后用 E 代替已知量,可以得到 $E = z \bmod d_b - E_b + \Delta$ 。由上式可见必须根据具体的 Δ 才能算出 d_b 值,由于又在嵌入算法中对数据添加了干扰 $\Delta\lambda$,要得到准确的 d_b 难度很大。

2) 如果网络运行期间簇头被妥协,则它可获知节点 i 的 UID ,要成功伪造节点 i 的数据还需要知道节点的 w 值与 d_i 值;在仅有簇头被妥协情况下,簇头通过比较与自己空间非常相邻的节点数据所能得到的结果如 1) 中所述。如果簇头与节点 a 同时被妥协,对于 a 所在的组,簇头已知其嵌入的 w ,而在分组过程中,由于同一组节点的位置是随机的,当且仅当妥协节点与同一组节点邻近时才有可能使用 1) 中的分析方法计算其 d 值,而这种情况的概率约为 $P = \frac{N \times P_1}{G \times P_2}$, P_1 为节点监测范围, P_2 簇监测区域总面积, N 为簇节点总数, G 是分组总数。

3) 水印的嵌入过程只对感知数据进行了简单的取模运算与加法运算,不涉及循环处理,算法的计算复杂度为 $O(n)$,Sink 获得传感数据后可以依据 d 与 w 信息对感知数据通过逆运算进行很接近的还原,数据失真较小。水印遍布全部节点数据,而且是重复嵌入水印数据,嵌入位置是数据的整数有效位,有损数据压缩不会对水印造成太大影响;如果在传递过程中丢失了部分数据,因为水印的重复嵌入依然能够保证检测出完整的水印,水印的鲁棒性较强。

3.3 水印的提取与检测

Sink 节点接收到由中间节点转发过来的数据包,首先对数据包进行解压,接着对从相同簇获得的数据进行水印的提取。

在同一簇内,节点 i 的分组信息 G_i ,Sink 节点可以通过分组函数计算出来,与具体分组对应的 w 信息已经由组内节点通过加密通信传给 Sink 节点。

令 w' 表示测试出的水印, r_k (取值 1 或者 0) 表示感知数据 x 中检出的水印 w' 是否与 w 一致, p 表示检测的出的水印与原嵌入水印相比的正确率。

提取检测步骤如下。

第1步 对于节点 i 的数据 x ,对 x 取整得到 z ,提取嵌入的信息 $w' = (z \bmod d_i) \% 2$ 。因为簇内同一组的节点嵌入的是共享的同一个 w ,所以水印的检测也以组为单位。

第2步 验证单个水印数据,对同一组的每个感知数据有:如果 $w = w'$,令 $r_k = 1$,否则 $r_k = 0$ 。

第3步 验证全组水印数据,设待测数据中属于同一组的数据个数为 n ,则统计出同一分组的正确检出水印的数据

$$\text{个数 } sum = \sum_{k=0}^n r_k.$$

第4步 计算本组水印正确校验的比率 p ,如果 $p =$

$sum/n > 0.5$, 认为本组数据中含有水印信息 $w = w'$, 否则判定为水印错误, 该组数据不可信。

第5步 将整个簇中的各个分组的水印合并来生成同一簇内感知数据中的完整水印信息。

4 模拟实验与结果分析

本节对提出的水印算法进行仿真实验, 试验平台采用 OMNET++ 离散事件模拟环境。实验主要测试水印算法遇到数据丢失时的完整性与数据被修改时敏感性验证。实验场景: 在一个 500×500 的监测范围内随机分布 1000 个传感器节点, 实验用 100 个节点来仿真一个簇。每个簇内将节点共分为 10 组, 每组有 10 个节点, 同一组内节点间通过协商来生成水印信息。协商过程完成后, 每个节点每隔 10 s 产生一组 $\langle T, H, L \rangle$ (温度、湿度和光强度) 数据, 在数据中植入水印信息后向簇头发送数据包。簇头节点对数据压缩处理后通过中继节点转发收到的含有感知数据的数据包直到 Sink 节点。

第一个实验多次重复地按照 1%、3%、5%、10%、15%、20% 和 30% 的比例随机地对传感数据进行提取来检测数字水印的完整性, 这样可以模拟因为网络的原因 Sink 节点只获得了一部分感知数据时数据水印的完整度。

在图 3 中可以明显地看到, 由于本文提出的数字水印算法将水印信息扩展到每个节点的数据中, 因此随机地从整体数据中抽取一定比例的数据来检测能够获得很好的检测效果, 当随机抽取 5% 的数据时, 检出的数据完整性约为 45%, 随着抽取数据比例的增加, 水印数据的完整性越来越好, 在模拟实验中当抽取比例为 20% 时, 检出的水印完整性已经达到 95%。

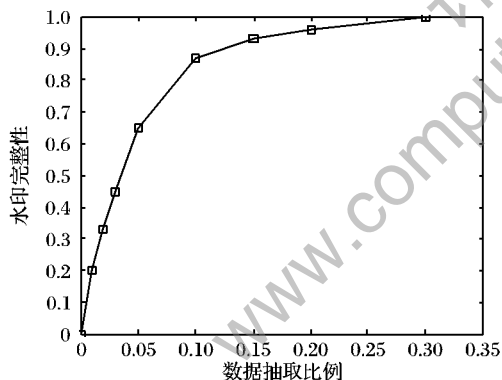


图3 不同数据抽取比例下水印的完整性

第二个实验对恶意篡改数据包内容的攻击行为进行检测, 检验水印对篡改数据攻击的敏感性。假设簇头被妥协并试图修改不同比例的传感器数据。

图4是对于虚假数据的实验结果, 攻击者在无法取得组水印与 UID 信息情况下如果强行修改数据值, 很容易使修改数据的水印数据破坏, 在 Sink 节点一端通过对水印的提取可以鉴别出数据是否被篡改。而在簇的分组内节点的水印数据跟 d_i 值密切相关, 妥协节点无法获知其他节点的 d_i 值, 很难控制嵌入值, 因此易于检测出虚假数据。实验结果显示当虚假数据比例超过 15% 时, 正确识别虚假数据率超过 60%。

5 结语

通过对现有技术的分析, 数字水印技术在无线传感器网络具有较好的应用前景, 可以很好地保证感知数据的真实性,

提高无线传感器网络的数据安全。本文对无线传感器网络的体系结构特点研究后提出的水印算法具有一定的创新性, 易于实现。实验表明, 该分布式数字水印算法很好地结合了传感器网络分布式数据存储处理的特点, 数字水印在数据包发生一定比例的损失时仍然具有很强的完整性, 同时也能有效地对检出对数据的非法篡改, 提高了传感器网络数据的可靠性与真实性。

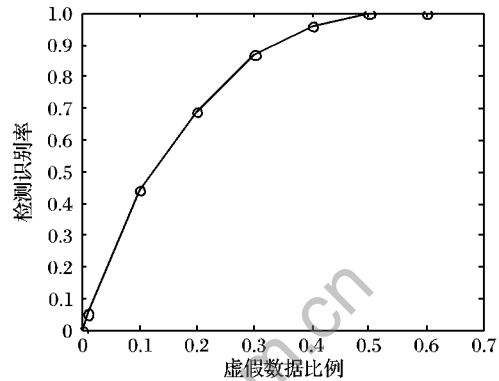


图4 不同比例虚假数据的识别率

参考文献:

- [1] 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.
- [2] 尹浩, 林闯, 邱峰, 等. 数字水印技术综述[J]. 计算机研究与发展, 2005, 42(7): 1093-1099.
- [3] ROY S, SETIA S, JAJODIA S. Attack resilient hierarchical data aggregation in sensor networks [C]// Proceedings of the 4th ACM Workshop on Security of Ad Hoc and Sensor Networks. New York: ACM Press, 2006: 71-82.
- [4] WONG J L, FENG J, KIROVSKI D, et al. Security in sensor networks: Watermarking techniques [M]// Wireless sensor networks. Norwell, MA, USA: Kluwer Academic Publishers, 2004: 305-323.
- [5] WANG H G, PENG D M, SHARIF H, et al. Energy-aware adaptive watermarking for real-time image delivery in wireless sensor networks [C]// IEEE 2008 International Conference on Communications. Washington, DC: IEEE Computer Society, 2008: 1483-1497.
- [6] KLEIDER J E, GIFFORD S, CHUPRUN S, et al. Radio frequency watermarking for OFDM wireless networks [C]// INFOCOM 2004: IEEE 2004 International Conference on Acoustics, Speech, and Signal Processing. Piscataway, NJ: IEEE Computer Society, 2004: 397-400.
- [7] 彭志娟, 王汝传, 王海艳. 基于数字水印技术的无线传感器网络安全机制研究[J]. 南京邮电大学学报: 自然科学版, 2006, 26(4): 69-72.
- [8] 易叶青, 林亚平, 彭舸, 等. 无线传感器网络中不依赖 MAC 认证的虚假数据过滤算法[J]. 通信学报, 2009, 30(6): 53-63.
- [9] HEINZELMAN W, CHANDRAKASAN A, BALAKRISHNAN H. Energy efficient communication protocol for wireless microsensor networks [C]// The 33rd Hawaii International Conference on System Sciences. Maui: IEEE Computer Society, 2000: 3005-3014.
- [10] DU W L, DENG J, HAN Y S, et al. A pairwise key pre-distribution schemes for wireless sensor networks [J]. ACM Transactions on Information and System Security, 2005, 8(2): 228-258.