·安全技术· 文章编号:1000-3428(2014)08-0101-05 文献标识码:A 中图分类号:TP309

无线传感器网中基于隐私同态的数据聚合方案

刘雪艳[1,2],李战明[1]

(1.兰州理工大学电气工程与信息工程学院,兰州 730050;2.西北师范大学数学与统计学院,兰州 730070)

摘 要: DF数据聚合方案在加/解密时采用相同的秘钥,因此不能有效抵抗已知明文攻击、捕获攻击及中间人攻击。为解决该问题,提出一个适用于无线传感器网络的数据聚合方案。该方案利用一次一密的双重加密机制,多资源节点在加/解密时采用不同的密钥,从而有效抵抗明/密文攻击、捕获攻击以及中间人攻击。同时,基于隐私同态技术进行数据加密,使得聚合数据时无需解密,保证了数据机密性和用户的隐私性。分析结果表明,与SDAP和SEDA方案相比,该方案具有较强的前向安全性和较低的存储开销。

关键词: 聚合;簇;捕获攻击;隐私同态;聚合器

Data Aggregation Scheme Based on Privacy Homomorphism for WSN

LIU Xue-yan[1,2],LI Zhan-ming[1]

(1. College of Electrical and Information Engineering,Lanzhou University of Technology,Lanzhou 730050,China;
2. College of Mathematics and Statistics,Northwest Normal University,Lanzhou 730070,China)

【Abstract】 There is only a same key in Domingo-Ferrer(DF) data aggregation scheme while encryption/decryption, therefore it can not resist the known plaintext attack,capture attack,etc. In order to solve these problems,this paper proposes a data aggregation scheme based on Privacy Homomorphism(PH) mechanism. The scheme adopts a double encryption mechanism of one-time pad,multi-resource node uses different key while encryption/decryption,so that it can be effectively against plaintext/ciphertext attack,compromising attack and man-in-middle attack. It does not decrypt while aggregating,so need not the extra decryption overhead,and at the same time it ensures the confidentiality of the data and user's privacy. Analysis result shows that this scheme has strong forward security and lower storage cost compared with the SDAP and SEDA scheme.

【Key words】 aggregation;cluster;compromised attack;Privacy Homomorphism(PH);aggregator

DOI: 10.3969/j.issn.1000-3428.2014.08.019

1 概述

无线传感器网络(Wireless Sensor Network,WSN)由大量传感器节点组成,彼此通过无线链路进行通信,能够实时监测、感知和采集网络分布区域内的各种环境或监测对象信息,并对这些信息进行初步处理,然后将结果送往远方的基站进一步处理[1]。WSN不需要固定网络支持,具有快速展开等特点,广泛应用于工业、交通、环境监测等领域。由于WSN能源受限、带宽有限,因此通常在网内对所采集的数据进行聚合处理,再将聚合结果发送给基站以减少传输能耗[2-3]。

文献[4]提出一个适用于WSN的有效聚合方案,很好地考虑了数据的完整性。文献[5]提出了一个逐跳的数据聚合协议,在该协议中,相比较底层的节点[6],高层节点得到更多的信任。文献[7]提出一个无需持续密码操作的WSN聚合算法,只有当一个欺骗行为被侦测到时,传感器节点才采用一个密码算法,该算法中引入拓扑约束构建了一个安全聚合树(Security Aggregation Tree,SAT),便于数据聚合监测。这些方案都很好地达到了聚合目的,但是,在聚合时都需要解密或者以明文的方式进行,不能保证数据的机密性[8]。

聚合WSN提供了更好的能量保护和高效的通信渠道,但是当传感器网络应用于敏感数据监测时,感知对象通常不希望与其生活、健康等隐私信息相关的

基金项目:国家自然科学基金资助项目(61163038,71263045);教育部人文社会科学研究基金资助项目"西部国家重点生态功能区生态安全预警研究"(12YJCZH282)。

作者简介:刘雪艳(1978-),女,副教授、博士研究生,主研方向:密码协议形式化分析,智能电网信息安全;李战明,教授、博士生导师。

收稿日期:2013-07-12 修回日期:2013-09-03 E-mail:liuxy@nwnu.edu.cn

(C)1994-2022 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

数据暴露，因此，节点所采集的数据需对其他节点保密。然而，传统加密体系不能在保证数据隐私性的同时支持数据聚合；基于安全多方计算等技术的隐私保护方案由于开销昂贵也不适用于传感器网络[9]。数据聚合对传感数据的隐私性保护提出了新的挑战，加密/隐藏数据聚合成为学者们关注的热点。

在加密机制[10-12]中，中间聚合器无需对加密数据进行解密，而是应用一些聚合函数完成加密数据聚合，因为聚合器不拥有数据发送者和基站(BS)间的共享秘钥。在文献[11-12]中，采用基于椭圆曲线的公钥密码隐藏节点的读数，这些机制提高了 WSN 抵抗单个节点攻击的保密性，因为捕获单个节点或一个节点集并不能揭露只有 BS 知道的解密钥。文献[13]提出了能量有效的基于模式码安全数据汇聚协议(ESPDA)。节点建立与原始数据对应的模式码并将其发往簇头，簇头不需要对加密数据进行解密，根据模式码实现了数据汇聚。但在该方案中，每个节点都发送模式码导致能耗不够理想，同时，没有考虑到多跳转发的数据认证，可能导致主动攻击及 DoS 攻击。文献[14]提出端到端的加密算法，允许汇聚节点通过对密文的操作完成数据汇聚，保护了数据的隐私性，但该算法中指数级的计算复杂度导致过大的计算开销，且该算法在唯密文攻击下并不安全；文献[15]提出安全的加密数据汇聚(Secure Encrypted Data Aggregation，SEDA)方案，该方案使用散列函数与异或操作在不对密文解密的情况下完成数据汇聚，保护了数据的隐私性且能耗较优。但该方案存在以下问题：(1) 要求汇聚节点预装入($N-1$)对密钥异或值，N 为网络中节点总数，网络的可扩展性差；(2) 没有提供数据认证，不能抵抗主动攻击及 DoS 攻击等恶意行。

文献[16-18]等协议使用了隐私同态(Privacy Homomorphism，PH)加密，聚合数据时不需要解密数据。文献[16-17]采用对称隐私同态加密机制对加密数据进行聚合。然而，DF 方案[16]要求加/解密时采用相同的秘钥，对于已知明文攻击、捕获攻击和重放攻击是脆弱的；在文献[17]中，聚合数据时允许使用不同的加密钥，基于加法模 n 操作，使用了一个扩展的一次性加密技术，但没有解决一些实际问题。此外，对于专门的参数集，基于隐私同态的对称秘钥方案对于选择明文攻击是不安全的。文献[18]提出的方案基于隐私同态依赖非对称秘钥，但需要一个单个的公钥对分层的数据进行聚合。

本文提出一个具有数据隐藏功能的隐私同态聚合方案。该方案修改了 DF 的同态方案，在聚合前，利用只有加密节点和 BS 之间的共享秘钥生成一个类似一次一密的掩盖值，掩盖要加密的数据，然后采用 DF 方法进行二次加密。在传输过程中，聚合器无需解密，而是采用隐私同态聚合收到的加密数据，之后传给上一级聚合器。BS 在收到聚合的机密数据后，利用和各节点共享的密钥完成解密工作。在该方案中，每个节点加密的同时生成一个承诺，BS 用于对数据的完整性和资源进行认证和故障诊断。对方案中采用的参数和各类攻击进行安全性分析，且对方案达到的安全要求和存储开销与已有经典方案进行比较。

2 预备知识

2.1 基本假设

除了基站(Base Station，BS)，所有传感器节点拥有有限的存储、计算、通信能力和对攻击的脆弱性，因此作如下假设：

(1) WSN 中包含大量的资源受限的传感器节点。

(2) 存在一个强有力的基站 BS。

(3) 所有的传感器节点是固定的。

(4) 簇头拥有较高的安全性，扮演聚合器的角色。

(5) 每个传感器节点只能发送数据给聚合器。

2.2 网络模型

本文采用的网络拓扑为基于簇的传感器网络，如图 1 所示。在该体系结构中，只包含 3 类角色：基站 BS，聚合器 Agg 和传感器节点。整个网络被划分为非重叠的簇，每个簇有一个聚合器(或簇头)，比传感器节点功能强一些，从传感器节点接收数据，聚合后传给 BS。

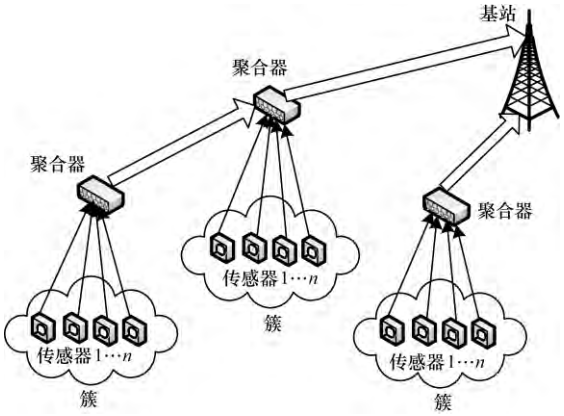

图 1 基于簇的网络拓扑

2.3 攻击模型

攻击者的目的是阅读、插入或者修改传感器节点的读数，所以，除了可以窃听、截获所有经过网络的消息外，还具备以下知识和能力[19]：

(1) 熟悉网络中各节点的 ID。

(2) 具有密码分析的知识和能力。

(3) 熟悉加/解密、散列等密码操作。

(4) 由于邻近节点可能得到相同的数据且攻击

(C)1994-2022 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

者可以得到节点发送的密文信息，因此攻击者可以发动已知明/密文攻击。

（5）攻击者可以捕获一个或者一小部分传感器节点，获得相应的秘密信息。

（6）攻击者可以通过物理操作改变传感器节点的读数（比如加热时的温度升高）。

（7）攻击者可以重放以前的合法消息或者假冒合法节点向聚合器发送虚假消息而发起主动攻击。

3　基于隐私同态的数据聚合方案

文中符号说明如表 1 所示。

表 1　符号说明

符号	说明
S_i	第 i 个节点
s_i	第 i 个节点与 BS 的共享密钥
r	所有节点与 BS 的共享密钥
τ, H	单向函数
r_i^u	第 i 个节点、第 u 次用于掩盖数据的值
$\hat{m}_i$	第 i 个节点被掩盖的数据
C_i	第 i 个节点的密文
ω_i^u	第 i 个节点第 u 次的承诺值

3.1　DF 方案

DF 是一个适用于 WSN，采用对称密钥的隐私同态方案。

Parameter 公钥：整数 $d \geqslant 2$，大整数 M；私钥：整除 M 的 $g, r \in Z_M$ 和 $r^{-1} \in Z_M$。

Encryption 将 m 划分为 d 部分 $m_1 m_2 \cdots m_d$，满足：

$$\sum_{i=1}^{d} m_i \bmod g = m$$

$$C = [C_1, C_2, \cdots, C_d] = [m_1 r \bmod M, m_2 r^2 \bmod M, \cdots, m_d r^d \bmod M]$$

Decryption $m = (C_1 r^{-1} + C_{2r}{}^{-1} + \cdots + C_d r^{-d}) \bmod g$。

Aggregation $C_{12} = C_1 + C_2 = [(C_{11} + C_{21}) \bmod M, \cdots, (C_{1d} + C_{2d}) \bmod M]$。

3.2　本文方案

本文方案分为 Setup，Encryption，Aggregation 和 Decryption 4 个阶段，验证工作在 Decryption 中根据情况进行。

Setup 公钥：整数 $d \geqslant 2$，大整数 M；私钥：整除 M 的数 $g, r \in Z_M$ 和 $r^{-1} \in Z_M$；BS 为每个节点 S_i 随机生成共享秘钥 s_i，选择 2 个单向函数，$H: \{0,1\}^* \times Z_M \to Z_M$，$\tau: Z_M \to Z_M$，将 $s_i, r, \tau()$ 和 H 预先装入节点 $S_i, i = 1, 2, \cdots, n$。

Encryption S_i 第一次加密时计算种子掩盖值 $r_i^1 = H(ID_i || s_i)$，然后在每次加密前计算 $r_i^u = \tau(r_i^{u-1})$，随后删除 r_i^{u-1}。

利用 r_i^u 掩盖要加密的数据 m_i：$\hat{m}_i = (m_i + r_i^u) \bmod M$。将 $\hat{m}_i$ 划分为 d 部分 $m_{i1} m_{i2} \cdots m_{id}$，满足 $\sum_{j=1}^{d} m_{ij} \bmod g = \hat{m}_i$，然后加密 $\hat{m}_i$：

$$C_i = [C_{i1}, C_{i2}, \cdots, C_{id}] = [m_{i1} r \bmod M, m_{i2} r \bmod M, \cdots, m_{id} r^d \bmod M]$$

且计算承诺：$\omega_i^u = (r_i^u + s_i) \bmod g$，发送 $C_i || \omega_i^u$ 给聚合器 Agg_k。

Aggregation Agg_k 聚合收到的 l 个消息：

$$C_{12 \cdots l} = \sum_{i=1}^{l} C_i = [\sum_{i=1}^{l} C_{i1}, \sum_{i=1}^{l} C_{i2}, \cdots, \sum_{i=1}^{l} C_{id}] = [C_{l1}, C_{l2}, \cdots, C_{ld}] = [\sum_{i=1}^{l} m_{i1} r \bmod M, \cdots, \sum_{i=1}^{l} m_{id} r^d \bmod M]$$

发送 $C_{12 \cdots l} || \omega_1^u || \omega_2^u || \cdots || \omega_l^u$ 给 BS。

Decryption 基站收到各聚合器发来的信息，计算 $r_i^u = \tau(r_i^{u-1})$，$i = 1, 2, \cdots, l$，然后验证：

$$(\sum_{i=1}^{l} \omega_i^u - \sum_{i=1}^{l} s_i) \bmod g \stackrel{?}{=} \sum_{i=1}^{l} r_i^u \tag{1}$$

（1）如果式（1）相等，则解密：

$$m = (C_{l1} r^{-1} + C_{l2} r^{-2} + \cdots + C_{ld} r^{-d} - \sum_{i=1}^{l} r_i^u) \bmod g \tag{2}$$

然后，判断 m 是否属于某个既定的现实意义区间 $[L, R]$。如果属于该区间，则接受；否则利用式（2）解密各簇的值 m_k，再次判断 m_k 是否属于区间 $[L, R]$，根据情况可以追踪到每个节点，从而判断哪个节点被捕获或者发生其他故障问题。

（2）如果式（1）不相等，BS 根据式（1）验证各个簇值的正确性，从而发现有问题的簇，进而多次利用式（1）判断有问题的节点，当然对于验证通过的簇，还要进行和情况（1）类似的 m_k 判断。

4　安全性分析

安全性分析主要针对 2.3 节的攻击模型进行，并在安全要求和存储开销方面与已有方案进行比较。

4.1　相关攻击分析

相关攻击分析具体如下：

（1）选择明/密文攻击分析

方案中只涉及 2 类秘钥：s_i 和 r，s_i 是传感器节点 S_i 与 BS 之间的共享秘钥，而 r 是所有节点和 BS 共享的秘钥。它们在明/密文攻击下的安全性如下：秘钥 s_i 用于生成掩盖值 r_i^u，在节点 S_i 没有妥协时，获得 s_i 的难度等同于单项函数求逆运算，因此 s_i 是明/密文攻击安全的。r 存在于密文 C_i 中，要获得它等同于大整数分解，因而是安全的。

（2）捕获攻击分析

一般地，传感器网络节点被捕获难以避免，因此当网络中一个或多个节点被捕获，攻击者可获得节点的所有秘密信息。各节点与基站的配对秘钥 s_i 是

(C)1994-2022 China Academic Journal Electronic Publishing House. All rights reserved.　http://www.cnki.net

由基站随机生成的，因此从捕获节点无法获取未捕获节点与基站共享的秘钥；其次，即使作为聚合器的簇头被捕获，它拥有的只是 $C_i||\omega_i^u$，因为也无法获得未捕获节点与基站的共享秘钥，所以对于捕获攻击是安全的，同理中间人攻击也是安全的。

（3）主动攻击分析

在该方案中，节点每次将 $C_i||\omega_i^u$ 发往聚合器，都会通过更新 $r_i^u=\tau(r_i^{u-1})$ 进而更新 $\omega_i^u=(r_i^u+s_i)\bmod M$，聚合器通过简单比较，可以过滤重放消息；攻击者冒充节点 S_i 向聚合器发送虚假消息，攻击者在不知道节点与基站的共享秘钥 s_i 和 r 的情况下，伪造正确 $C_i||\omega_i^u$ 的概率是一个可忽略的量，BS 通过散列计算可以将该消息过滤；即使攻击者捕获了一个或者多个节点，可以发送多个含有正确 ω_i^u 的消息，但是无法通过 BS 的 m_i 检测。综上所述，该方案可以有效地抵抗主动攻击。

（4）前向安全

在该方案中，节点每次加密前先计算 $r_i^{u+1}=\tau(r_i^u)$，然后删除 r_i^u，所以，即使节点被捕获，只能获得当前的 r_i^{u+1}，要获得 r_i^u 相当于关于单向函数求逆运算，从而保证了方案的前向安全。

4.2 方案比较

方案比较具体如下：

（1）安全性能分析

表 2 给出了本文方案与 SDAP、SEDA 方案的安全性比较。本文方案具有较高的安全性。每个节点发送的 $C_i||\omega_i^u$ 中包含每次更新的 r_i^u，保证了数据的完整性和新鲜性，并且提供承诺用于认证；采用该方案，类似于 Sybil 的攻击都会被抵抗；因为每个簇头即为聚合器，所以可用性很容易满足。

表 2 安全性能比较

方案	机密性	新鲜性	完整性	资源认证	可用性
SDAP[6]					
SEDA[15]					
本文方案					

（2）存储开销分析

设节点 ID 的长度为 2 Byte，秘钥长度为 8 Byte，单项函数存储开销为 h_1，簇内节点数目为 l，n 表示网络内节点总数，其他开销为 x。

表 3 给出了本文方案与 SDAP、SEDA 方案的存储开销比较。在本文方案中，每个节点需要预先装入 ID、与基站的配对秘钥 s_i 和 r，单项函数 $\tau()$ 和 H，簇头不需要预装信息。在 SDAP 方案中，每个节点需要预装入 ID、与簇内节点的 $(l-1)$ 个配对秘钥，2 个单项函数 $f_g()$ 和 H，簇头也是普通传感器根据簇策略生成，且为了安全需要不时变动，所以，簇头存储的信息量和节点的信息量是一样的。在 SEDA 方案中，每个节点需要预装入 ID、与基站的配对秘钥及单项函数 $f()$，且每个簇头需预装秘钥序列 L，其大小等同于 $(n-1)$ 个秘钥所需的空间，当 n 比较大时，传感器节点无法承受该秘钥序列的开销。

表 3 存储开销比较 Byte

方案	节点	簇头
SDAP[6]	$(2\times h_1+x+2+8(l-1))$	$(2\times h_1+x+2+8(l-1))$
SEDA[15]	(h_1+10l)	(h_1+8n+2)
本文方案	$(2\times h_1+26)$	无

（3）参数分析

在 DFPH 方案中，消息大小为 $d\cdot\bar{m}$，d 份中的每一份为 $\bar{m}$ Byte，安全参数组合后的消息会变得非常大。而在本文中，由于引入了掩盖值，相当于双重加密，且不同节点拥有不同的秘钥，因此消息长度无需增加。

5 结束语

为能在带宽有限的、开放的、甚至是恶意的环境中进行数据的安全高效传输，数据聚合、保证数据的机密性或者用户的隐私性都是十分重要的，综合考虑两方面因素可以提高 WSN 的传输效率，并且保证数据的隐私性和安全性。本文采用隐私同态机制，提出一个适用于传感器网络的数据聚合方案。该方案具有如下优点：(1) 采用隐私同态机制，聚合器不需要解密收到的加密数据，以及额外的解密开销；(2) 聚合器没有解密钥，不可能获得数据的任何信息，保证了数据的机密性；(3) 方案中采用了一次一密的双重加密机制，使得该方案有效抵抗明/密文攻击和捕获攻击；(4) BS 可利用节点提供的承诺完成认证和故障诊断；(5) 将 DF 方案的多资源节点采用相同秘钥扩展到采用不同密钥，抵抗中间人攻击。此外，本文对方案达到的安全要求与存储开销与已有经典方案进行了比较，由比较结果得出本文方案的安全性更高，存储开销明显低于其他 2 个方案，尤其是簇头无需任何存储开销。

参考文献

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

[2] Tang Xueyan, Xu Jianliang. Extending Network Lifetime for Precision Constrained Data Aggregation in Wireless sensor Networks [C]//Proceedings of the 25th IEEE International Conference on Computer Communications. Piscataway, USA: IEEE Press, 2006: 131-146.

[3] Hu Lingxuan, Evans D. Secure Aggregation for Wireless Networks [C]//Proceedings of Workshop on Security and Assurance in Ad hoc Networks. Orlando, USA: IEEE Press, 2003: 384-390.

(C)1994-2022 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

[4] Przydatek B,Song D,Perrig A. SIA:Secure Information Aggregation in Sensor Networks [C] //Proceedings of SenSys'03. [S. l.]:IEEE Press,2003:255-265.

[5] Yang Yi,Wang Xinran,Zhu Sencun,et al. SDAP: A Secure Hop-by-Hop Data Aggregation Protocol for Sensor Networks [C] //Proceedings of MOBIHOC'06. [S. l.]:ACM Press,2006:1-30.

[6] Westhoff D, Girao J, Acharya M. Concealed Data Aggregation for Reverse Multicast Traffic in Sensor Networks: Encryption, Key Distribution and Routing Adaptation [J]. IEEE Transactions on Mobile Computing,2006,5(10):1417-1431.

[7] Wu K,Dreef D,Sun B,et al. Secure Data Aggregation Without Persistent Cryptographic Operations in Wireless Sensor Networks [J]. Ad Hoc Networks,2007,5(1):100-111.

[8] Ozdemir S. Secure, Reliable Data Aggregation for Wireless Sensor Networks [M] //Ichikawa H,Cho We-Duke,Satoh I. Ubiquitous Computing Systems,Tokyo, Japan: [s. n.],2007:25-28.

[9] He W,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. Piscataway,USA:IEEE Press,2006:165-168.

[10] Girao J,Westhoff D,Schneider M. CDA: Concealed Data Aggregation in Wireless Sensor Networks [C] // Proceedings of ACM Workshop on Wireless Security. Philadelphia,USA:IEEE Press,2004:3044-3049.

[11] Mykletun E,Girao J,Westhoff D. Public Key Based Cryptoschemes for Data Concealment in Wireless Sensor Networks [C] //Proceedings of IEEE International Conference on Communications. Istanbul,Turkey:IEEE Press,2006:2288-2295.

[12] Sang Y, Shen H, Inoguchi Y, et al. Secure Data Aggregation in Wireless Sensor Networks: A Survey [C] //Proceedings of the 7th International Conference on Parallel and Distributed Computing,Applications and Technologies. Washington D. C.,USA:IEEE Computer Society,2006:315-320.

[13] Cam H,Ozdemir S. Energy-efficient Security Protocol for Wireless Sensor Networks [C] //Proceedings of the 58th Vehicular Technology Conference. New York, USA:IEEE Press,2003:2981-2984.

[14] Acharya M,Girao J. Secure Comparison of Encrypted Data in Wireless Sensor Networks [C] //Proceedings of the 3rd International Symposium on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks. Trentino,Italy:IEEE Press,2005:47-53.

[15] Huang S I,Shiuhpyng S,Tygar J D. Secure Encrypted-data Aggregation for Wireless Sensor Network [J]. Wireless Networks,2010,16(4):915-927.

[16] Domingo-Ferrer J. 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.

[17] Castelluccia C, Mykletun E, Tsudik G. Efficient Aggregation of Encrypted Data in Wireless Sensor Networks [C] //Proceedings of the 2nd Annual International Conference on Mobile and Ubiquitous Systems: Networking and Services. [S. l.]:IEEE Press,2005: 109-117.

[18] Ozdemir S. Concealed Data Aggregation in Heterogeneous Sensor Networks using Privacy Homomorphism [C] // Proceedings of IEEE International Conference on Pervasive Services. Istanbul,Turkey:IEEE Press,2007: 165-168.

[19] 郭江鸿,马建峰. 安全透明的无线传感器网络数据汇聚方案 [J]. 通信学报,2012,33(10):51-59.

编辑　陆燕菲

(上接第 100 页)

参考文献

[1] 李文仲,段朝玉. ZigBee2006 无线网络与无线定位实战 [M]. 北京:北京航空航天大学出版社,2008.

[2] Baronti P,Pillai P,Chook V W C,et al. Wireless Sensor Networks:A Survey on the State of the Art and the 802.15.4 and Zigbee Standards [J]. Computer Communications,2007, 30(7):1655-1695.

[3] 蒋　挺,赵成林. ZigBee 技术及其应用 [M]. 北京:北京邮电大学出版社,2006.

[4] 陈　波. Zigbee 路由算法分析及改进 [D]. 天津:南开大学,2009.

[5] Chakeres I D,Berndt K. AODVjr,AODV Simplified [J]. Mobile Computing and Communication Review,2002,6 (3):100-101.

[6] 王　芳,柴乔林,班艳丽. 一种改进的 ZigBee Mesh 网络路由算法 [J]. 计算机应用,2008,28(11): 2788-2794.

[7] 李予东,黄宏光,向西西. 基于能量均衡的 Zigbee 路由算法优化 [J]. 计算机工程与设计,2011,32(2): 397-400.

[8] Ran P,Sun M H,Zou Y M. ZigBee Routing Selection Strategy Based on Date Services and Energy Balanced Zigbee Routing [C] //Proceedings of 2006 IEEE Asia Pacific Conference on Services Computing. Washington D. C.,USA:IEEE Computer Society,2006: 400-404.

[9] Ha J Y,Park H S,Choi S,et al. Enhanced Hierarchical Routing Protocol for ZigBee Mesh Networks [J]. IEEE Communications Letters,2007,11(12):1028-1030.

[10] 张　擎,刘淑美,柴乔林. 能量高效的 Zigbee 网络改进路由策略 [J]. 计算机工程,2010,36(7):108-111.

[11] Ashraf U,Abdellatif S,Juanole G. An Interference and Link-quality Aware Routing Metric for Wireless Mesh Network [C] //Proceedings of the 68th Vehicular Technology Conference. [S. l.]:IEEE Press,2008:1-5.

[12] 谢　川. Zigbee 中改进的 Cluster-Tree 路由算法 [J]. 计算机工程,2011,37(7):115-117.

编辑　陆燕菲

(C)1994-2022 China Academic Journal Electronic Publishing House. All rights reserved.　http://www.cnki.net