基于无证书公钥体制的层簇式 WSN 密钥管理方案

周大伟[1]，魏国珩[1,2]，张焕国[2]
(1. 海军工程大学信息安全系，武汉 430033；2. 武汉大学计算机学院，武汉 430072)

摘 要： 在详细叙述无线传感器网络(wireless sensor network，WSN)密钥管理方案性能衡量指标的基础上，采用层簇式结构，结合无证书公钥算法，提出一种安全的密钥管理方案，通过与其他密钥管理方案的网络联通性、安全性、计算量与存储性能等指标的对比分析，证实了该方案的有效性.

关键词： 无线传感器网络(WSN)；密钥管理；层簇式；公钥体制
中图分类号： TP 309 **文献标志码：** A **文章编号：** 0254－0037(2016)05－0707－06
doi： 10.11936/bjutxb2015070081

Key-management Scheme Based on Public-key Institution to Clustered Wireless Sensor Networks

ZHOU Dawei[1], WEI Guoheng[1,2], ZHANG Huanguo[2]
(1. Information Security Department, Naval University of Engineering, Wuhan 430033, China;
2. School of Computer, Wuhan University, Wuhan 430072, China)

Abstract: On the basis of detailed description of wireless sensor network (WSN) key-management scheme performance measure index, a secure key-management scheme was proposed by using the layer clustered structure and the non-certificate public-key algorithm, the effectiveness of the scheme was confirmed through the comparison and analysis of the network connectivity, security, calculation and storage performance of other key-management Schemes.

Key words: wireless sensor network(WSN); key management; layer clustered; public-key institution

无线传感器网络(wireless sensor network，WSN)技术是物联网感知层的关键技术之一. WSN由大量微型的传感器节点组成，这些节点组成一个移动的无线自组织网络，以实现获取感知对象相关信息的功能. 随着物联网应用的逐步深入，对其安全性也提出了更高要求，对WSN感知技术的安全性研究渐渐成为研究热点. 与传统网络相比，WSN具有传感器节点存储能力和计算能力有限、网络的结构变化快、拓扑复杂、缺乏统一的识别编码等特点. 对WSN的安全保护，需要密钥管理、安全路由、节点认证、入侵检测等多方面共同作用，其中，密钥管理是WSN安全的核心[1].

WSN有分布式和层簇式2种结构模型[2]. 在分布式结构中，每个节点的功能、能量、结构都是相同的，各个节点相互同质；而在层簇式结构中，节点职责分工不同，根据节点具备的不同能力，安排节点完成不同的功能，不同功能的节点分别称为基站、簇头和普通感知节点，簇头是按照一定的算法和协议选出的特殊节点. 层簇式模型如图1所示，适用于网络规模较大的场合，利用多层次消息整合降低通信量，降低节点通信能耗，减少节点通信距离，相比于分布式具有更高的传输效率和

收稿日期： 2015-07-20
基金项目： 国家自然科学基金资助项目(61332019)
作者简介： 周大伟(1980—)，男，讲师，主要从事网络安全方面的研究，E-mail: zdw_xp@163.com

更长的生命周期[3].

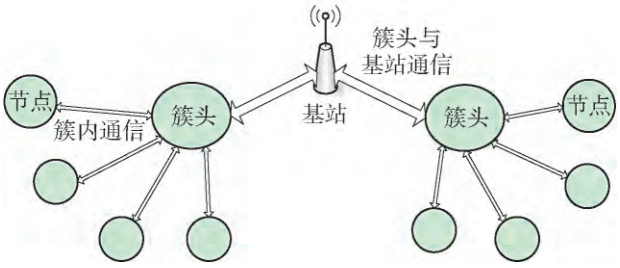

图 1 层簇式 WSN 模型结构

Fig. 1 Layer cluster WSN model structure

近些年来,许多专家学者先后提出了针对 WSN 安全的一系列层簇式结构的密钥管理方案. 李琳等[4]提出的层簇式密钥管理方案运用(t,n)门限方案进行组间通信和认证,满足前向私密性和后向私密性,其密钥更新方式可以抵抗同谋破解,但当节点簇头的能量过低时,某些连接认证无法进行,且各节点没有统一识别码,容易留下安全隐患. 周琴等[5]提出了一种基于分簇的动态密钥分发协议(secure dynamic key distribution,SDKD),运用了一种新的簇头选举算法,在每个回合之后簇头计算各个成员的能量,结合全局位置信息选定新的簇头,成员节点间没有数据交互,通信通过簇密钥加密,可以抵抗 DOS 攻击,但由于使用单跳模式,当网络消息过多时,簇头与基站的信息传输量过大,且无法抵抗同谋破解. 郭宇飞等[6]基于随机密钥预分配和逻辑密钥树(logical key hierarchy,LKH)构建临时分类密钥管理(transitory classified keys management,TCKM)协议,引入睡眠节点召唤和盲因子机制,具有较好的存储优势,但源端认证安全性不够. 柳亚男等[7]提出的方案使用“虚拟簇头”与“物理簇头”相结合的方式完成密钥协商,将节点信息储存于多个虚拟簇头之中,网络部署后,虚拟簇头将共享密钥发送给真实物理簇头,但由于节点能量有限,每形成一个簇密钥就要进行多次通信,无法适用于大型无线传感器网络. Rohbanina 等[8]提出使用公钥密码体制对层簇式 WSN 进行密钥管理,首先构建最短路径,使用基于椭圆曲线的密码方案进行会话密钥分发,但计算量与通信量均较大,影响性能.

这些方案在解决 WSN 的密钥管理方面都有不同的特点,但在某些特殊的应用场合,例如敌方战场地形勘察等,传感器投放的地点在敌方控制区,无法确保基站本身的安全. 因此,需要引入特殊的密钥管理方案.

本文首先阐述了无证书公钥算法,接着提出了一种基于无证书公钥体制的层簇式 WSN 密钥管理方案,将传感节点的私钥生成方式改由系统生成和自身生成 2 部分组成,这样即使基站被敌方捕获,也不会泄露整个网络节点的公钥和私钥,具有较高的鲁棒性;然后对该方案的安全性、效能、方案正确性等进行了详细分析,并就网络联通性、安全性、计算量与存储性能等指标与其他密钥管理方案进行了对比分析,证实了该方案的有效性.

1 无证书公钥算法

1.1 定义

定义 1 k 合谋攻击算法(collusion attack algorithm with k traitors,K-CAA)问题:对于一个 $k\in\mathbb{R}$,$s\in {}^{*}_{q}$,$P\in G_1$. 计算 $P/(s+e)$,其中 $e\notin\{e_i\in Z_q^*\}$,给定$\{sP,P,e_i\in {}^{*}_{q},k,P/(s+e)\}$.

定义 2 计算性迪菲赫尔曼问题[9](computational diffie-hellman problem,CDHP):对于随机给定的$\{P,aP,bP\}$,其中 $a,b\in {}^{*}_{q}$,计算 abP.

定义 3 逆 CDHP 问题[10]:对于一个给定的未知随机数 $a\in {}^{*}_{q}$,$\{P,aP\}$,计算 P/a.

1.2 无证书公钥算法

给定安全参数 k,选择 2 个阶都为素数 $q>2k$ 的群 G_1 和 G_2,一个修改椭圆曲线的 Weil 双线性对 e:$G_1\times G_1\to G_2$,G_1 为一个 q 阶加法群,P 是 G_1 的生成元,G_2 为一个 q 阶乘法群,其中令 $g=e(P,P)$. 挑选 3 个不同的哈希函数

$$H_1:\{0,1\}^{*}\to {}^{*}_{q}$$

$$H_2:\{0,1\}^{*}\times G_1\to {}^{*}_{q}$$

$$H_3:G_2\to\{0,1\}^{*}$$

选择一个随机数 $s\in {}^{*}_{q}$ 作为系统主密钥,并计算得到系统公钥 $P_{pub}=sP\in G_1$,私钥产生器(private key generator,PKG)公布系统参数$\{k,G_1,G_2,e,q,P,g,P_{pub},H_1,H_2\}$,秘密保存 s.

步骤 1 节点初始私钥(extract partial private key)的建立

对于给定节点身份 $\mathrm{ID}\in(0,1)^{*}$,PKG 计算

$$Q_{\mathrm{ID}}=H_1(\mathrm{ID})$$

$$d_{\mathrm{ID}}=P/(s+Q_{\mathrm{ID}})$$

在传感器节点生成时,通过安全信道,将节点身份信息 ID 及其私钥 d_{ID} 注入与节点之中.

步骤 2 节点完整密钥(generate user keys)的建立

节点收到到身份信息 ID 及其私钥 d_{ID} 之后,选

取一个随机数 r 作为其秘密值，则该节点的用户私钥为

$$\mathrm{SK_{ID}}=(d_{\mathrm{ID}},r)$$

则公钥

$$\mathrm{PK_{ID}}=(P_{\mathrm{pub}}+Q_{\mathrm{ID}}P)\times r$$

节点将公钥发送给 PKG，PKG 将各节点公钥发送给基站(base station，BS)，基站保存节点公钥.

步骤 3　无证书签密算法

1) 签密算法(signcrypt)

用户 A 随机选择一个值

$$z\in {}^{*}_{q}$$

$$C_1=H_3(g^z)\oplus m$$

$$h=H_2(m)$$

$$S=\frac{d_{\mathrm{A}}}{r_{\mathrm{A}}+h}$$

$$C_2=\mathrm{PK_A}\parallel z\mathrm{PK_B}$$

计算发送消息 $\delta=(C_1,h,S,C_2,\mathrm{ID_A})$ 给 B.

2) 解密验证算法(unsigncrypt)

B 接受 A 的消息进行验证，如果

$$e(S,\mathrm{PK_A}+h(P_{\mathrm{pub}}+Q_{\mathrm{ID_A}}P))=e(P,P)=g$$

则确认 A 为正确用户，然后计算

$$e(z\mathrm{PK_{ID_s}},\mathrm{SK_{ID_z}})=e(P,P)^{z}=g^z$$

$$m=H_3(g^z)\oplus C_1$$

2　基于无证书公钥算法的密钥管理方案

2.1　系统初始化阶段

WSN 节点在分配到各个位置之后，使用自身携带的 GPS 模块获取位置信息，节点计算自身能量，能量值记为 E，$m=\mathrm{GPS}\parallel E$. 节点随机选择一个秘密值 $z\in {}^{*}_{q}$，计算

$$h=H_2(m)$$

$$S=\frac{d_{\mathrm{A}}}{r_{\mathrm{A}}+h}$$

$$C_2=\mathrm{PK_A}\parallel z\mathrm{PK_{BS}}$$

$$C_1=H_3(g^z)\oplus m$$

发送 $\delta=(C_1,h,S,C_2,\mathrm{ID_A})$ 基站，基站解密消息，获取各节点的位置信息及能量信息. 本协议使用 LEACH 协议中轮的概念，每轮分为分配成簇阶段、节点和簇头建立簇密钥阶段等 2 个阶段.

1) 选择簇头

本方案使用分簇式结构，每个簇拥有一个簇头，簇中节点根据簇头能量判断自己是否有能力担当簇头，如果有足够能量则向基站报告自己的位置和可以担当簇头请求.

基站将簇员消息发送给簇头

$$m=(\mathrm{PK}_i\parallel \mathrm{ID}_i)\parallel K_{\mathrm{BS}}$$

式中 K_{BS} 为簇头与基站之间通信密钥，基站随机选择一个秘密值 $z\in {}^{*}_{q}$，然后，计算

$$C_1=H_3(g^z)\oplus m$$

$$h=H_2(m)$$

$$S=d_{\mathrm{BS}}/(r_{\mathrm{BS}}+h)$$

$$C_2=S\parallel z\mathrm{PK}_{\mathrm{CH}_i}$$

发送消息 $\delta=(C_1,h,S,C_2,\mathrm{ID_{BS}})$ 给簇头 CH_i.

2) 构建簇密钥

当簇头收到来自于基站的消息之后，解密消息并获取属于其簇内的节点公钥及身份号，簇头 CH_i 随机选择一个随机数 N 和秘密值 $z\in {}^{*}_{q}$，计算

$$S=\frac{d_{\mathrm{CH}_i}}{r_{\mathrm{CH}_i}+h}$$

$$\delta=(C_1,h,S,C_2,\mathrm{ID}_i)$$

$$C_1=H_3(g^z)\oplus m$$

$$h=H_2(m)$$

$$C_2=\mathrm{PK}_{\mathrm{CH}_i}\parallel z\mathrm{PK}_{\mathrm{ID}_i}$$

式中：$m=\mathrm{ID}_{\mathrm{CH}_i}\parallel K_{\mathrm{CH}_i}\parallel N\parallel T$；$T$ 为该节点回复簇头时间段；δ 发送给节点 ID_i.

节点收到消息之后解密消息，并从消息中获取簇密钥 K_{CH_i} 及随机数 N 节点将随机数使用簇密钥加密发送给簇头，即 $C_{K_{\mathrm{CH}_i}}(N)$ 发送给簇头，簇头验证 N 是否正确，如正确则簇密钥协商完成，自此首轮基于无证书的层簇式 WSN 的密钥管理初始化完成.

2.2　网络安全通信

在系统完成初始化之后，系统进入稳定的运行状态，成员节点在其时间段里将所有消息或数据加密后发送给簇头，簇头将这些消息进行整合压缩发送给基站.

1) 簇头与节点之间通信

在系统稳定运行时，每个成员等待自己时间段，其余时间处于休眠状态，降低能量消耗，当到自身通信时隙时，节点向簇头发送加密消息，使用簇密钥加密明文 m

$$C=C_{K_{\mathrm{CH}_i}}m$$

$$S=\frac{d_{\mathrm{ID}_i}}{r_{\mathrm{ID}_i}+h}$$

$$\delta=(C,h,S,\mathrm{ID}_{\mathrm{ID}_i})$$

$$h=H_2(m)$$

簇头通过对节点发过来消息对节点进行合法认证，

并对明文进行整合，去除冗余数据；如果发现节点认证错误，则在下一轮初始化开始删除该节点，并通知基站删除该节点. 同样簇头与基站通信与此类似.

2) 新节点加入与旧节点退出

当有新的节点想加入 WSN 时，新的节点向基站发送请求，基站根据其地理位置情况[11]，选择最合适的簇，并将该节点公钥及其 ID 发送给簇头，簇头执行将簇密钥分发给节点，自此新的节点加入.

当某一节点失效或者被敌方俘获时，簇头将该节点公钥及其身份信息删除，此后失效节点或者被俘获节点将无法完成会话.

3 方案的性能分析

3.1 正确性分析

验证等式

$$e=(S,\mathrm{PK}_{\mathrm{A}}+h(P_{\mathrm{pub}}+Q_{\mathrm{ID}_{\mathrm{A}}}P))=e(P,P)=g$$
$$e(z\mathrm{PK}_{\mathrm{ID}_{\mathrm{B}}},\mathrm{SK}_{\mathrm{ID}_{\mathrm{B}}})=g^{z}$$

的正确性，设节点解出的明文消息为 m'.

认证

$$e(S,\mathrm{PK}_{\mathrm{A}}+h(P_{\mathrm{pub}}+Q_{\mathrm{ID}_{\mathrm{A}}}P))=$$
$$e(S,r+h(P_{\mathrm{pub}}+Q_{\mathrm{ID}_{A}}\mathrm{P}))=$$
$$e\left(\frac{d_{\mathrm{A}}}{r_{\mathrm{A}}+h},(r_{A}+h)(P_{\mathrm{pub}}+Q_{\mathrm{ID}_{\mathrm{A}}}P)\right)=$$
$$e\left(\frac{P}{r_{\mathrm{A}}+h(S+Q_{\mathrm{ID}_{\mathrm{A}}})},(r_{\mathrm{A}}+h)(S+Q_{\mathrm{ID}_{\mathrm{A}}})P\right)=$$
$$e(P,P)=g \tag{1}$$

解密

$$e(z\mathrm{PK}_{\mathrm{ID}_{\mathrm{B}}},\mathrm{SK}_{\mathrm{ID}_{\mathrm{B}}})=$$
$$e\left(z(P_{\mathrm{pub}}+Q_{\mathrm{ID}_{\mathrm{B}}}P)r_{\mathrm{B}},\frac{d_{\mathrm{B}}}{r_{\mathrm{B}}}\right)=$$
$$e\left(z(P_{\mathrm{pub}}+Q_{\mathrm{ID}_{\mathrm{B}}}P)r_{\mathrm{B}},\frac{P}{s+Q_{\mathrm{ID}_{\mathrm{B}}}r_{\mathrm{B}}}\right)=$$
$$e(P,P^{z})=g^{z} \tag{2}$$
$$m=H_{3}\cdot(g^{z})\oplus C_{1} \tag{3}$$

采用等式证明方法，证明节点解出的明文 $e(S,\mathrm{PK}_{\mathrm{A}}+h(P_{\mathrm{pub}}+Q_{\mathrm{ID}_{\mathrm{A}}}P))=g$，$m'\equiv m$，因此，本文提出的基于无证书层簇式 WSN 的密钥管理方案可行.

3.2 安全性分析

在无线传感器网络中，节点常遇到捕获攻击，从而攻击者能够轻易地获取节点中的密钥信息，如果这些密钥存在于一些节点的密钥环中，一个节点被捕获后会危及其他节点，整个网络的安全性将受到威胁.

本方案中当某一节点被敌方俘获时，簇头将删除该节点信息，失效节点将无法完成会话，降低了对其他节点的影响. 每个节点的信息都存储在簇头中，在网络安全通信阶段，如果簇头被捕获，它所存储的所有信息将被敌方获取，因此本方案簇头与基站间，节点与簇头间采取相同的通信方式，及时删除错误节点，增强了抗攻击性.

WSN 是由无数传感节点组成，一般而言 WSN 的密钥管理必须满足 4 个安全特性，分别为可验证性(availability)、不可否认(non-reputation)、认证(authentication)和机密性(confidentiality)[12]. 下面以本方案在实际应用中遇到捕获攻击时为例，对以上 4 个安全特性进行分析.

1) 可验证性

通过 3.1 节的等式证明，方案在理论上是可以验证的.

2) 不可否认性

本方案将消息哈希值 h 加入计算之中，$h=H_{2}(m)$，$S=d_{\mathrm{A}}/(r_{\mathrm{A}}+h)$，且与各节点秘密值相结合，有且仅有合法认证的消息才能完成加解密运算，因此该方案具有不可否认性[13].

3) 认证

WSN 中使用无证书公钥密码体制，使用节点自身私钥对消息进行签名；在验证时，使用节点公钥进行解密，只有掌握节点私钥的合法节点才能对消息完成签名.

由于私钥中节点的秘密值由节点自己选择，其他节点无法模仿，即使一个节点被捕获，也无法获取其他节点的秘密值，因此，该方案可以完成对节点的双向认证.

4) 机密性

本方案通过签名方式对节点合法性进行认证，签名方案在基于逆 CDHP、K-CAA 难题下的攻击具有抗伪造性. 方案加密基于 CDHP 难题和哈希函数，因此攻击者希望找到 Z^{*}，使得等式成立 $e(P,P)^{z^{*}}=e(P,P)^{z}$ 是困难的，找到 $H_{3}(g^{z^{*}})=H_{3}(g^{z})$ 也是困难的. 根据逆 CDHP 难题，知道 $z\mathrm{PK}_{\mathrm{B}}$ 和 PK_{B}，得出 $Z^{*}=Z$ 也是困难的，所以在理论上破解该加密系统是不可行的.

WSN 密钥管理方案需要同时满足前向私密性、端源认证、鲁棒性、抗同谋破解、易扩展性、后向私密性、低功耗等特性，表 1 为本文方案与其他方案的特性对比.

表 1　本文方案与其他方案安全特性对比

Table 1　Comparison of security features

方案	前向私密性	后向私密性	抗同谋破解	端源认证	鲁棒性	可扩展性	低功耗
文献[7]	√	√		√	√	强	
文献[14]	√	√			√	弱	
文献[15]	√					弱	√
文献[16]	√		√	√	√	较强	√
本文	√	√	√	√	√	强	√

3.3　效率分析

密钥管理方案的效率包括计算复杂性和存储开销等 2 个方面.

1）计算复杂性分析

本文方案使用簇密钥进行节点和簇头之间加密通信，大大降低了计算量，簇密钥的安全性通过系统周期性进行广播并重新广播分簇来保证. 方案中的运算主要包括: hash 函数运算 H、双线性对运算 P、XOR 运算 X、乘法运算 PM 等，表 2 列出了本方案使用的运算量及与其他方案的对比.

表 2　计算复杂性比较

Table 2　Comparison of computational complexity

算法来源	轮数	计算量	通信量
文献[17]方案	1	$2P+3H+nX$	n
文献[8]方案	1	$(n-1)(2H+PM+P)$	$n(n-2)/2$
文献[7]方案	1	$(n-1)(H+4PM+P)$	$n(n-2)/2$
本文方案	1	$2P+3H+3PM+2X$	n

2）方案的存储开销分析

基于对称密钥的系统节点需要存储所有预分配密钥，在本方案中，普通节点只需存储自身身份消息、公钥、私钥以及簇密钥，相比其他存储所有密钥对的方案来说，存储开销相对较小. 同时，本方案采用椭圆曲线算法实现，相比于诸如文献[4]等基于 RSA 方案所需的密钥长度要小很多. 且本方案使用的是协商簇密钥方式，因此密钥的建立与网络的规模无关.

4　结论

1）提出了一种基于无证书公钥体制的层簇式 WSN 密钥管理方案，采用椭圆曲线算法生成密钥，使用无证书公钥算法进行签密验证，改革传感节点的私钥生成方式，降低基站被敌方捕获带来的密钥泄露风险，同时满足可验证性、不可否认性、认证性、机密性等安全特性.

2）与其他类似方案的安全特性和计算量与存储性能等效率指标的对比分析. 通过对比结果表明，本文方案具备良好的安全特性，在计算复杂性、存储开销等方面有较好的表现，且符合大规模 WSN 的应用，是一个安全有效的层簇式密钥管理方案，在 WSN 技术的物联网感知层安全应用中具有较高的应用价值.

参考文献:

[1] 米波，曹建秋，段书凯，等. 无线传感器网络密钥管理问题综述[J]. 计算机工程与应用，2011，47(13)：77-82.
MI B，CAO J Q，DUAN S K，et al. Survey on key management of wireless sensor networks [J]. Computer Engineering and Applications，2011，47(13)：77-82. (in Chinese)

[2] 冯国军，熊冬青，张大勇. 军事物联网解决方案[J]. 物联网技术，2012(6)：70-72.
FENG G J，XIONG D Q，ZHANG D Y. Research on military internet of things [J]. Internet of Things Technology，2012(6)：70-72. (in Chinese)

[3] AZARDERSKNSH B，REYHANI-MASOLLEH A. Secure clustering and symmertic key establishment in heterogeneous wireless sensor networks [C] // EURASIP Journal on Wireless Communication and Networking. Nasr city：Hindawi Publishing Corporation，2011：48-52.

[4] 李琳，王汝传，姜波，等. 无线传感器网络层簇式密钥管理方案研究[J]. 电子信息学报，2006，28(12)：2394-2397.
LI L，WANG R C，JIANG B，et al. Research of layer-cluster key management scheme on wireless sensor networks [J]. Journal of Electronics & Information Technology，2006，28(12)：2394-2397. (in Chinese)

[5] 周琴，李腊元，程真. 一种基于分簇的无线传感器网络动态密钥分发协议[J]. 传感技术学报，2009，22(7)：1002-1006.
ZHOU Q，LI L Y，CHENG Z. A cluster-based dynamic key distribution protlcol in wireless sensor networks [J]. Chinese Journal of Sensor and Actuators，2009，22(7)：1002-1006. (in Chinese)

[6] 郭宇飞，王换招，曹宁，等. 簇状传感器网络临时分类密钥管理协议[J]. 北京邮电大学学报，2008，31(3)：63-66.
GUO Y F，WANG H Z，CAO N，et al. Transitory

classified keys management for clustered wireless sensor network [J]. Journal of Beijing University of Posts and Telecommunications, 2008, 31(3): 63-66. (in Chinese)

[7] 柳亚男，王箭，张楠楠. 层次型传感器网络簇内密钥协商方法 [J]. 系统工程与电子技术，2011，33(7)：1633-1637.
LIU Y N, WANG J, ZHANG N N. Intra-cluster key agreement in hierarchical sensor networks [J]. Systems Engineering and Electronics, 2011, 33(7): 1633-1637. (in Chinese)

[8] ROHBANINA M R, KHARAZMI M R, KESHAVARZ-HADDAD A, et al. Watchdog-LEACH: a new method based on LEACH protocol to secure clustered wireless sensor networks [J]. ACSIJ Advances in Computer Science, 2013(2): 105-117.

[9] 胡亮，赵阔，袁巍，等. 基于身份的密码学 [M]. 北京：高等教育出版社，2011：10-20.

[10] 孙天一. 无线传感器网络 LEACH 协议的探讨及改进 [D]. 济南：山东大学，2004.
SUN T Y. Discussion and improvement of LEACH protocol for wireless sensor networks [D]. Jinan: Shandong University, 2004. (in Chinese)

[11] 屈玉贵，翟羽佳，蔺智挺，等. 一种新的无线传感器网络传感器放置模型 [J]. 北京邮电大学学报，2004，27(6)：2-6.
QU Y G, ZHAI Y J, LIN Z T, et al. A novel sensor placement model in wireless sensor network [J]. Journal of Beijing University of Posts and Telecommunications, 2004, 27(6): 2-6. (in Chinese)

[12] 张华，温巧燕，金正平. 可证明安全算法与协议 [M]. 北京：科学出版社，2012：131-137.

[13] LU Z, GE J H. Synchronization and channel estimation for MIMO OFDM wireless LAN systems [J]. Journal of Harbin Institute of Technology, 2009, 16(6): 799-803.

[14] 丁汉城，杨庚，李斌. 一种动态分簇无线传感器网络密钥管理方案 [J]. 计算机工程与应用，2008，44(3)：157-160.
DING H C, YANG G, LI B. Key management scheme for dynamically clustering wireless sensor networks: KMDC [J]. Computer Engineering and Applications, 2008, 44(3): 157-160. (in Chinese)

[15] 刘伟，罗嵘，杨华中. 一种轻量级的无线传感器网络密钥建立协议 [J]. 电子与信息学报，2010，32(4)：869-873.
LIU W, LUO R, YANG H Z. A lightweight key establishment protocol for wireless sensor networks [J]. Journal of Electronics & Information Technology, 2010, 32(4): 869-873. (in Chinese)

[16] ZHANG Y, LIU W, LOU W. Location-based compromise tolerant security mechanisms for wireless sensor networks [J]. IEEE JSAC, 2006, 24(2): 247-260.

[17] 邓邵江，王宇，田袁，等. 基于 EBS 的分组分层 WSN 密钥管理策略 [J]. 计算机工程，2013，39(9)：64-68.
DENG S J, WANG Y, TIAN Y, et al. Grouping and layered key management strategy in WSN based on EBS [J]. Computer Engineering, 2013, 39(9): 64-68. (in Chinese)

（责任编辑 吕小红）