

无线传感器网络中结合信任管理的基于属性基加密方案

黄 丹*

(辽宁师范大学 计算机与信息技术学院, 辽宁 大连 116081)

(*通信作者电子邮箱 huangdan@lnnu.edu.cn)

摘 要:针对无线传感器网络(WSN)中基于属性基加密(ABE)的属性授权与撤销问题,提出了一种结合信任管理的密文-策略 ABE 方案(TM-CP-ABE)。该方案基于密文-策略 ABE,融合了信任管理机制,将信任评估和信任更新与属性授权和属性撤销结合起来。对方案的安全性、复杂性和有效性进行了对比分析,并与目前 WSN 中比较流行的加密方案进行了仿真实验对比,结果表明 TM-CP-ABE 方案较好地解决了无线传感器网络 CP-ABE 的属性撤销问题,并通过属性撤销在一定程度上抑制了恶意节点的破坏行为。

关键词:无线传感器网络;属性基加密;属性撤销;信任管理

中图分类号: TP393.08 **文献标志码:** A

Attribute-based encryption scheme combined with trust management in wireless sensor network

HUANG Dan*

(College of Computer Science and Information Technology, Liaoning Normal University, Dalian Liaoning 116081, China)

Abstract: To solve the attributes authority and attributes revocation of Attribute-Based Encryption (ABE) in Wireless Sensor Network (WSN), a scheme of trust management-based ciphertext-policy ABE (TM-CP-ABE) was proposed. The proposed scheme was based on ciphertext-policy ABE and combined it with trust management mechanism. The procedure and the steps of trust evaluation based attributes authority and trust update based attributes revocation were provided. The security, complexity and validity of the proposed scheme were analyzed. Compared with the popular encryption scheme in WSN through comprehensive simulation, the results show that the proposed scheme is efficient for attribute revocation of CP-ABE in WSN. By attributes revocation, to a certain extent, the attacks of malicious nodes are also inhibited.

Key words: Wireless Sensor Network (WSN); Attribute-Based Encryption (ABE); attribute revocation; trust management

0 引言

以收集信息为目的,无线传感器网络(Wireless Sensor Network, WSN)^[1-2]包括大量通信、计算和能量等资源受限的节点。由于部署环境缺乏物理安全保护,节点很容易受到攻击。因此,如何在资源受限条件下,应对各种安全挑战是 WSN 研究需要解决的问题。

作为一种可选的安全解决方案,WSN 加密方案大多为共享对称密钥^[3]或公钥加密方案^[4]。对称密钥加密的计算和通信量比较小,但节点沦陷后密钥很容易暴露;依赖于非对称密码学方法的公钥加密在网络建立后分配密钥,需要较大的交互和计算存储开销。安全的密钥分发、较少的能耗和密钥存储空间成为 WSN 加密研究的目标之一。

有很多致力于 WSN 密钥协商的研究,其中将基于身份加密技术^[5]用于 WSN 加密是研究的热点。基于身份密码系统的概念最初由 Adi Shamir 于 1984 年提出,使用任意字符串作为公钥。Boneh 等^[6]提出了一个可实现的算法^[6]。Rahman 等^[7]提出了一个椭圆曲线上基于公钥加密的密钥协商方案,任意两个节点可以独立地计算密钥,减少了通信次数和密钥存储空间,但其节点承担的密钥计算开销较大。Oliveira 等^[8]通过基于身份认证的非交互协议协商节点密钥,但身份的认

证需要可信的第三方支持。

目前,基于属性基加密(Attribute-Based Encryption, ABE)^[9-10]在 WSN 加密研究领域逐渐受到关注。用户身份也是用户属性的一种,可以把基于身份加密看作 ABE 的一个特例。Hur 等^[11]提出了一种 CP-ABE (Ciphertext-Policy Attribute-Based Encryption) 密钥分发架构用来解决密钥托管问题,将分发密钥的权力分为密钥生成和属性授权两部分,任何一方不能单独决定密钥的发放;但这种方案增加了密钥分发的交互次数。Attrapadung 等^[12]在简单假设下提出了以密文和密钥属性构成正交向量的访问策略,具有基于身份的撤销机制;但方案不具备匿名性。Lin 等^[13]提出一种基于模糊阈值的多授权身份加密方案,属性只有经过若干次不同授权者授权后才能解密数据;但多方授权增加了密钥协商的交互次数。Wang 等^[14]结合基于层次身份加密和 CP-ABE,提出了基于层次的属性加密方案,并给出了属性撤销的方法;但没有研究更高效的表示属性间层次关系的数据结构。Tan 等^[15]从访问策略的细粒度控制以及不同用户不同存取权利的角度,将密钥-策略和密文-策略两种 ABE 进行了对比,认为密钥-策略 ABE 更适合于资源受限的传感器节点上。上面大多数 ABE 设计较为复杂且开销较大,除了属性授权与撤销需要较多交互次数的原因外,ABE 本身也存在一些需要解决的问

题:1) CP-ABE 机制中访问结构由加密者制定,使得加密方的开销与访问结构的复杂性相关,访问结构越复杂开销越大;2) ABE 中用户属性是不断变化的,变化的属性增加了属性授权与撤销的复杂性和开销;3) ABE 中私钥由可信机构集中分发,但从密钥的属性一般无法区分出解密者的身份,因此一旦密钥泄露,将无法追究泄露者的责任,对手容易滥用密钥对网络发起攻击。本文在 CP-ABE^[16] 基础上,提出一种结合信任管理的 CP-ABE 方案,将信任评估和信任更新与属性授权和属性撤销结合起来。理论分析及仿真实验表明,本文方案动态的信任属性授权和属性撤销较好地解决了 WSN 基于密文策略属性加密的属性授权与撤销问题,并一定程度上抑制了恶意节点的攻击。

1 基于信任管理的 CP-ABE 方案

CP-ABE 包括 4 个步骤^[16]: Setup、Encrypt、Key Generation 和 Decrypt,构成了一个关于算法的四元组。其中: Setup 阶段生成主密钥 MK 和公开参数 PK ; Encrypt 阶段使用 PK 把数据明文 m 加密为密文 CT ; Key Generation 阶段利用 PK 生成私钥 SK ; Decrypt 阶段使用私钥 SK 解密密文 CT 得到明文 m 。

信任一般被认为是一种人或事物之间信赖的等级。WSN 中信任管理系统^[17-18] 收集节点行为的反馈并评估信任度。节点的信任也可以看成某种属性。节点的剩余能量、邻居数、行为诚实性以及基站距离等都可作为评估信任度的因素。几种属性值可以加权计算信任值。因此信任本身可以看作是多种属性的综合,信任管理系统负责为信任属性授权。本文假设信任授权机构是可靠的,且节点部署前预设初始信任属性和授权时间为 0 的密钥。方案的基本流程如图 1 所示。

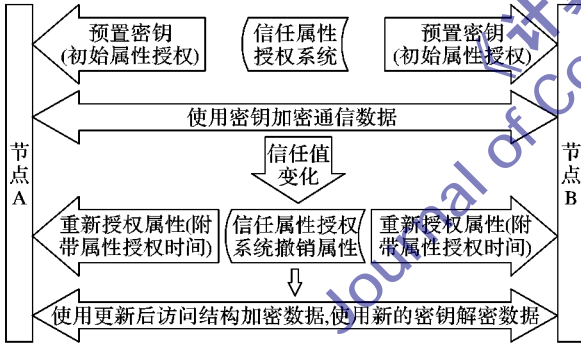


图1 基于信任属性加密的基本流程

下面在随机预言模型下构建基于信任属性的密文策略加密方案,如下:

1) Setup 阶段:信任管理系统选择一个素数阶 p 的群 G 和一个生成元 g ; \mathbb{Z}_p 为素数阶 p 的乘法群;随机选择 $a, \alpha \in \mathbb{Z}_p$; 选择哈希函数 $H: \{0,1\}^* \rightarrow G$, H 为随机预言模型,生成公共参数 $PK = g, e(g, g)^\alpha, g^\alpha$ 和主密钥 $MSK = g^a$; 节点在部署前预置公共参数。

2) Encrypt 阶段:节点将公共参数 PK 、待加密的信息 m 和 LSSS 访问结构 $A = (M_i, \rho(i))$ 作为输入;映射函数 $\rho(i)$ 是内射的,输入为 M_i 中行 i 所对应的数据,输出为属性集合 S 中的某一属性 x_i ; $\rho(i)$ 至多只能将一个属性关联到 M_i 中的某一行。

本文方案中属性集合 S 有信任属性授权和信任撤销两个属性,密文中 $l \times n$ 维矩阵 M_i 的某一行 M_i 可以通过 $\rho(M_i)$ 映射为相应的属性 x_{M_i} , x_{M_i} 是某一信任属性区间的下限。为了减小计算开销,本文取 $l = 2$ 。同时,为了防止恶意节点通过累积信任值来获得相应属性,信任管理系统授权信任属性时会同时

发布授权时间属性 x_{M_i} 。

节点首先选择一个随机向量 $v = (s, y_2, \dots, y_n) \in \mathbb{Z}_p^n$, 该向量被用于分享秘密 s 。对于参数 i (取值为 u 和 k), 分别计算 $\lambda_i = M_i \cdot v$, 其中 M_i 是 M_i 的行向量。密文表示如下:

$$CT = (C = me(g, g)^\alpha, C' = g^s, C_u = g^{a\lambda_u} H(\rho(u))^{-s}, C_k = g^{a\lambda_k} H(\rho(k))^{-s}) \quad (1)$$

密文含有 $(M_i, \rho(i))$ 。

3) Key Generation 阶段:信任管理系统计算节点 j 的信任值作为其属性 x_u , $x_u = \rho(u) \in S$, x_j 隐含在密钥组件 K_x 中,表示某一信任区间的下限。同样,为了防止恶意节点累积信任值获得相应属性, M_i 中的某一行 k 的映射函数 $\rho(k)$ 对应为信任授权时间属性 x_k , 即 $x_k = \rho(k) \in S$, 以保持信任属性的时效性。

以主密钥 MSK 和属性集合 S_j 为输入,随机选择 $t \in \mathbb{Z}_p$, 生成私钥:

$$K = g^a g^{at}, L = g^t, \forall x \in S, K_x = H(x)^t \quad (2)$$

4) Decrypt 阶段:输入为密文 CT 和密钥 SK 。其中, CT 和 SK 含有各自的 LSSS 访问结构 $(M_i, \rho(i))$, $I \subset \{u, k\}$, 定义 $I = \{u, k: \rho(u) \in S, \rho(k) \in S\}$ 。如果密钥中的属性集合 S_j 是密文 LSSS 访问结构的授权集合,且 $\{\lambda_i\}_{i \in I}$ 是秘密 s 关于 M_i 的有效分享,则可计算 $\sum_{i \in I} \omega_i \lambda_i = s$, 其中 $\{\omega_i\}_{i \in I} \in \mathbb{Z}_p$ 可以在多项式时间内找到。

解密算法首先计算:

$$e(C', K) / \left(\prod_{i \in I} (e(C_i, L) e(C', K_{\rho(i)}))^{w_i} \right) = e(g, g)^{\alpha s} e(g, g)^{\alpha s} / \left(\prod_{i \in I} e(g, g)^{a \lambda_i w_i} \right) = e(g, g)^{\alpha s} \quad (3)$$

然后,可以从 C 中解密出 m 。

2 信任属性加密方案分析

在本文方案中,基站作为权威的信任管理机构收集节点信任反馈进行综合信任评估,并承担授权信任属性和分发密钥的任务。下面分别从安全性、复杂性和有效性等方面对本文提出的 TM-CP-ABE 方案与 TinyPBC^[8] 和 KP-ABE^[15] 进行分析比较。

2.1 安全性分析

由于本文是在 CP-ABE^[16] 基础上融合了信任管理机制,将信任评估和信任更新与属性授权和属性撤销结合起来。因此,利用文献[16]的方法易知本文提出的方案是选择性安全的。

2.2 复杂性分析

计算复杂性方面,本文方案的加密解密主要通过几个组件进行。无线传感器网络大多数运算集中在通信部分,因此,对于加密组件 $e(g, g)^\alpha$ 和其余 3 个密文组件可以离线计算,且一次计算可用于多次加密,直到下一次信任属性授权。这样,在线部分的加密运算,实际只需要一次 XOR 的计算。同样,解密部分的运算同样只需计算 $e(g, g)^\alpha$ 一次,直至下次属性授权再重新计算 $e(g, g)^\alpha$ 。因此,两次更新之间的时间复杂度分析为 $O(1)$ 。在更新频繁的情况下,时间复杂度可能随更新的频率增加。TinyPBC 利用对称加密的方法,任何两个节点通信前需要首先协商对称密钥,因此其时间复杂度高于采用离线计算方法的本文方案。

2.3 有效性分析

与 TinyPBC 相比,本文方案有如下特性:

1) 本文方案中的公钥是基于信任属性的,信任属性可以灵活变换,相当于很多属性的综合评价。ABE 中的属性授权

分为用户属性授权和系统属性授权:用户属性保证该用户获得该属性对应的权限,不具备该属性的其余用户不具备此权限;系统属性保证拥有该属性的用户都具有某种权限,执行起来比较简单。信任属性正是这样一种系统属性,而每个用户的信任属性更新时间则是用户属性。因此,在设计公钥时,除保留系统信任属性外,只需保留一个所有通信节点的属性授权时间表,密钥存储空间较小,与 TinyPBC 需要为每个通信节点保存公钥所占用的空间大致相当。

2)在私钥方面,TinyPBC 通过离线非交互协商获得两个节点的共享密钥,具有非交互的特点。本文方案在两次信任属性撤销的间隔期间,解密只需重复利用 $e(g, g)^{as}$ 组件,不需要与授权机构交互。虽然为了孤立和抑制不诚实或不信任的节点,信任授权系统会发布密钥更新,但更新频率和节点信任值变化的频率有关,在大多数节点信任值比较稳定的情况下,密钥更新频率较低,比较接近于非交互的密钥协商。

3)TinyPBC 使用双线性映射协商共享对称密钥,但节点沦陷时,对手可能利用泄露的密钥参数与其他节点建立共享密钥。虽然在网络节点数量大且部署范围广时,危害可被控制在较小的范围内,但对节点密度不均匀的场合,骨干节点沦陷将严重影响网络安全性。本文方案中,节点的恶意行为会使其信任属性值大幅降低,这会导致其信任属性被即时撤销并被授权较低的新信任属性值;同时信任管理系统广播发布授权时间通知其他节点更新 LSSS 访问结构中对应信任授权时间的部分,这将使信任属性较低的密钥无法解密密文或只能解密一些信任属性要求较低的密文,从而孤立并抑制恶意节点。这种方法充分利用了 TM-CP-ABE 的解密由授权机构和加密方共同控制的特点。此外,节点在信任属性值被降低后,仍被保留其用户身份,以便信任度增加后再次对其授权较高的信任属性。这种灵活的授权方式可能迫使恶意节点或以长时间非连续的方式保持诚实的行为。

与 KP-ABE 比较:

1)KP-ABE 的访问结构在密钥中,授权的属性在密文中。这种策略的优点是可以较少地限制解密者,并实现复杂的访问结构,支持灵活的访问策略;缺点是加密者不能较好地限制解密权限,仅能够描述用于加密的属性。而本文方案的优点是,加密者通过控制解密策略可以限制解密者的解密权限。

CP-ABE 中的策略由加密方制定,使得系统公钥设计的复杂性策略复杂性相关,策略的灵活性使得系统公钥设计复杂,限制了访问结构的设计。为了解决这一问题,本文方案利用信任管理系统将各种策略涉及的属性整合为单一的信任属性,在降低公钥设计复杂性的同时,保留了公钥设计的策略灵活性。密钥拥有相应的信任属性和最新的属性授权时间才能解密密文。加密者不需要与授权机构在线交互就可以利用不同的信任属性策略限制节点的解密权限,以较小的代价实现了灵活的细粒度策略设计。

2)计算方面,在 KP-ABE 中,由于解密者只能进行在线的策略检查,所以本文方案的时间复杂度低于 KP-ABE;同时, KP-ABE 的访问结构计算集中在接收端,很容易耗尽汇聚节点的剩余能量。而本文方案的访问结构在密文中,因此复杂的双线性映射计算被分散在各个发送端,这有利于全网能量的均匀消耗,延长网络寿命。

3 仿真实验及分析

将本文提出的 TM-CP-ABE 方案与 TinyPBC^[8] 和 KP-ABE^[15] 进行比较。在仿真器 NS2 下实现了本文方案及

TinyPBC 和 KP-ABE,实验设备是一台运行 Solaris9 的 Intel I7 2.8 GHz 8 Core 处理器,4 GB DDR3 内存的 PC。

仿真实验根据文献[19]的内部攻击和外部攻击模型来进行分析,主要比较三种方案的能耗和运行时间。仿真环境假设 450 个节点随机均匀部署在一块 400 m × 400 m 的仿真网络区域内,每个节点的传输距离为 40 m,基站位于左上角 (0,0) 坐标,部署基于组的信任管理模式 (Group-based Trust Management Scheme, GTMS)^[18],节点能量消耗采用文献[20]的能量消耗模型,如表 1 所示。为了更好地验证文中提出的加密方案,本文实验中网络拓扑采用单一的基于基站汇聚的方式。

表 1 能耗参数

仿真参数	值
接收一个字节的能耗	580 μ J
发送一个字节的能耗	750 μ J
初始能量	12 J
加密运算开销	10 nJ/b
短距离放大系数	6 pJ/(b · m ²)
长距离放大系数	0.0028 nJ/(b · m ⁴)

在内部攻击模型中,节点面临如下网络层攻击: neglect、greedy 和 misdirection。其中: neglect 攻击指参与网络层协议的恶意节点在回复已收到数据包后,随机或任意丢弃数据包; greedy 攻击是指在丢弃其他节点数据包后,优先转发自己的数据包; misdirection 攻击将数据向错误的方向路由。这三种内部攻击可能造成监测数据与实际数据的偏差。假设监测数据为温度, D_{err} 为实际数据与监测数据偏差的绝对值。采用信任管理系统对 D_{err} 数值进行统计。假设区域温度均匀,图 2 表示三种方案在相同数量的三种内部攻击下,1 200 s 内网络全部节点的 D_{err} 平均值变化情况 (25 s 统计一次)。可以看出 TinyPBC 和 KP-ABE 的 D_{err} 变化较大;而本文方案通过即时的属性撤销机制隔离了恶意节点,从而在 D_{err} 短暂增大后,回到正常水平,因此本文方案可以有效地抵御内部攻击。

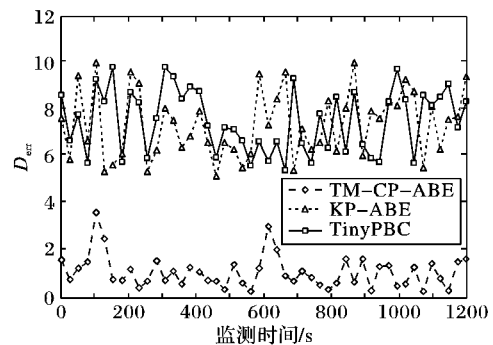


图 2 运行三种方案的网络在内部攻击下的监测偏差

在外部攻击模型中,网络面临物理层攻击,如 Tampering 攻击等。Tampering 攻击为真正的暴力破坏,攻击者可以物理破坏或破解传感器节点进而得到密钥监听渗透网络。假定攻击者渗透网络的目的是定位更多的节点并使其 fail-silent。采用基站对 fail-silent 节点数量 N_{fs} 进行统计。设定节点每成功破解一个节点(破解时间为 3 s 以内的随机值)后,会定位下一个节点继续攻击。图 3 是三种方案在受到 Tampering 攻击时,1 000 s 内 N_{fs} 的变化情况。可以看出: TinyPBC 在节点被破解后,攻击者可以随意地定位攻击下一个节点, N_{fs} 上升较快; KP-ABE 由于访问结构由解密者决定,因此同样无法阻止 N_{fs} 的上升;在本文的方案中,授权机构监测出节点信任属性变化

较大后,即时撤销用户属性,在重新授权用户属性后,对手无法定位更多的节点, N_{fs} 的上升因此得到了有效抑制。

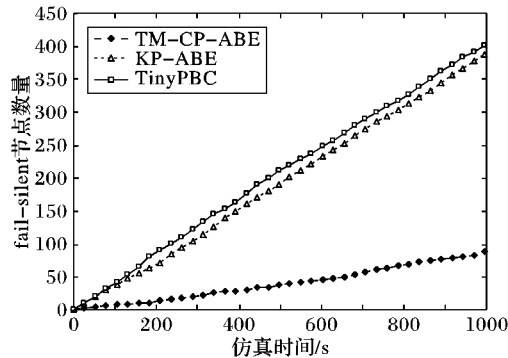


图3 运行三种方案的网络在外部攻击下的静默节点数

表2对节点的能耗、运行时间等参数进行了统计,表中数据为15次实验后的平均值。

表2 平均能耗及运行时间

方案	能量消耗/ (J · s ⁻¹)	初始化 时间/s	加密 时间/s	解密 时间/s	总运行 时间/s
TinyPBC	0.0064	28.0023	0.0054	0.0054	1875
KP-ABE	0.0103	6.0063	0.0108	0.0122	1165
TM-CP-ABE	0.0055	5.0054	0.0033	0.0017	2181

从表2可以看出,本文方案的平均能耗最小,原因之一是在属性撤销不频繁的情况下,本文的加密解密只需要一次简单的异或运算;其次是采用对称加密方案的 TinyPBC; KP-ABE 因为解密需要较多的在线计算,因此平均能耗最多。在加密和解密方面,本文方案所用时间最少, TinyPBC 其次, KP-ABE 最多。

4 结语

本文针对 WSN 基于属性加密的属性授权与撤销问题提出了基于信任属性的加密方案。与目前无线传感器网络中比较典型的对称密钥加密以及 KP-ABE 的理论分析与仿真对比实验表明,本文结合信任管理系统的即时属性授权与撤销机制在降低公钥设计复杂性的同时,通过加密者与授权机构非交互的解密设计提供了基于信任等级的细粒度策略控制;并能通过隔离或抑制恶意节点一定程度上抵御内部和外部攻击,为无线传感器网络提供安全保障。本文实验环境采用基于单一的基站汇聚方式组网,该方案实现比较简单,实验结果较好。分析表明,该方案在多跳路由并有基站管理的组网环境下可以得到相同的结论。本文方案可以通过属性撤销有效抑制恶意节点破解密钥后进行的攻击或消极行为,但无法阻止恶意节点单纯的监听行为,因此如何在节点沦陷的情况下,更好地保护网内信息及策略的隐私是下一步的研究重点。

参考文献:

- [1] MANOLAKOS E S, LOGARAS E, PASCHOS F. Wireless sensor network application for fire hazard detection and monitoring [C]// SENSAPPEAL 2009: Proceedings of the 2009 International Conference on Sensor Applications, Experimentation, and Logistics. Berlin: Springer-Verlag, 2010: 1-15.
- [2] JENNIFER Y, BISWANATH M, DIPAK G. Wireless sensor network survey [J]. Computer Networks, 2008, 52(12): 2292-2330.
- [3] OLIVEIRA L B, WONG H C, LOUREIRO A A F, et al. On the design of secure protocols for hierarchical sensor networks [J]. International Journal of Security and Networks, 2007, 2(3/4): 216-227.

- [4] CHIEN H-Y, LIN R-Y. Improved ID-based security framework for Ad Hoc network [J]. Ad Hoc Networks, 2008, 6(1): 47-60.
- [5] HU L, LIU Z, SUN T, et al. Survey of security on identity-based cryptography [J]. Journal of Computer Research and Development, 2009, 46(9): 1537-1548. (胡亮, 刘哲理, 孙涛, 等. 基于身份密码学的安全性研究综述[J]. 计算研究与发展, 2009, 46(9): 1537-1548.)
- [6] BONEH D, FRANKLIN M. Identity based encryption from the Weil pairing [J]. SIAM Journal of Computing, 2003, 32(3): 586-615.
- [7] RAHMAN S M, KHALILI E K. Private key agreement and secure communication for heterogeneous sensor networks [J]. Journal of Parallel and Distributed Computing, 2010, 70(8): 858-870.
- [8] OLIVEIRA L B, ARANHA D F, CONRADO P L, et al. TinyPBC: pairings for authenticated identity-based non-interactive key distribution in sensor networks [J]. Computer Communications, 2011, 34(3): 485-493.
- [9] GOYAL V, PANDEY O, SAHAI A, et al. Attribute-based encryption for fine-grained access control of encrypted data [C]// CCS06: Proceedings of the 13th ACM Conference on Computer and Communications Security. New York: ACM, 2006: 89-98.
- [10] BETHENCOURT J, SAHAI A, WATERS B. Ciphertext-policy attribute-based encryption [C]// SP07: Proceedings of the IEEE Symposium on Security and Privacy. Washington, DC: IEEE Computer Society, 2007: 321-334.
- [11] HUR J, KOO D, HWANG S O, et al. Removing escrow from ciphertext policy attribute-based encryption [J]. Computers & Mathematics with Applications, 2012, 34(6): 260-264.
- [12] ATTRAPADUNG N, LIBERT B. Functional encryption for public-attribute inner products: achieving constant-size ciphertexts with adaptive security or support for negation cached [J]. Journal of Mathematical Cryptology, 2011, 5(2): 115-158.
- [13] LIN H, CAO Z, LIANG X, et al. Secure threshold multi authority attribute based encryption without a central authority [J]. Information Sciences, 2010, 180(13): 2618-2632.
- [14] WANG G, LIU Q, WU J, et al. Hierarchical attribute-based encryption and scalable user revocation for sharing data in cloud servers [J]. Computers & Security, 2011, 30(5): 320-331.
- [15] TAN Y L, GOI B M, KOMIYA R, et al. A study of attribute-based encryption for body sensor networks [J]. Communications in Computer and Information Science, 2011, 251(2): 238-247.
- [16] WATERS B. Ciphertext-policy attribute-based encryption: an expressive, efficient, and provably secure realization [C]// Proceedings of 14th International Conference on Practice and Theory in Public Key Cryptography, LNCS 6571. Berlin: Springer, 2011: 53-70.
- [17] GANERIWAL S, BALZANO L K, SRIVASTAVA M B. Reputation-based framework for high integrity sensor networks [J]. ACM Transactions on Sensor Network, 2008, 4(3): 1-37.
- [18] SHAIKH R A, JAMEEL H, AURIOLURI B J, et al. Group-based trust management scheme for clustered wireless sensor networks [J]. IEEE Transactions on Parallel and Distributed Systems, 2009, 20(11): 1698-1712.
- [19] WOOD A D. Denial of service in sensor networks [J]. Computer Date of Publication, 2002, 35(10): 54-62.
- [20] KALPAKIS K, DASGUPTA K, NAMJOSHI P. Efficient algorithms for maxinluin lifetime data gathering and aggregation in wireless sensor networks [J]. ACM Computer Networks, 2003, 42(6): 697-716.