(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 104967517 A
(43)申请公布日 2015.10.07

(21)申请号 201510442987.7

(22)申请日 2015.07.24

(71)申请人 电子科技大学
地址 611731 四川省成都市高新区(西区)西源大道2006号

(72)发明人 许春香 徐辰福 张晓均 金春花 孙丽雪

(74)专利代理机构 成都点睛专利代理事务所(普通合伙) 51232
代理人 葛启函

(51)Int.Cl.
H04L 9/32(2006.01)
H04L 29/06(2006.01)
G06F 17/30(2006.01)

权利要求书4页 说明书9页

(54)发明名称

一种用于无线传感器的网络数据聚合方法

(57)摘要

本发明属于无线通信技术领域，具体的说是涉及一种用于无线传感器的网络数据聚合方法。本发明方法基于椭圆曲线同态加密算法，安全外包算法和基于身份的聚合签名算法，提供了一个可认证的无线传感器网络数据安全聚合方法。本发明的有益效果为，本发明方法通过使用椭圆曲线同态加密算法，基于身份的聚合签名算法和安全外包算法，使得半可信的聚合器不仅能够在较恶劣的网络环境中获得所需的聚合统计数据，而且能够提供保证保密性、数据完整性、数据源可认证性和抗重放攻击，因此在实际应用中具有广泛的应用前景。

CN 104967517 A

1. 一种用于无线传感器的网络数据聚合方法，其特征在于，包括以下步骤：

a. 系统初始化，通过可信第三方生成聚合器节点的公私钥对和中间聚合器节点的公私钥对；可信第三方还产生传感器节点签名私钥、中间聚合器节点签名私钥、系统公共参数和可信第三方私钥；同时可信第三方在系统内设置一个用于生成时间戳的同步时钟；

b. 传感器节点采用聚合器节点的公钥对收集到的秘密信息加密得到中间密文，再使用中间聚合器节点的公钥对中间密文加密得到最终密文；采用最终密文、传感器节点身份信息、中间聚合器节点身份信息和第一时间戳信息构成第一混合密文；

c. 传感器节点使用传感器节点签名私钥对第一混合密文签名获得第一签名，将第一混合密文和第一签名发送到中间聚合器节点；

d. 中间聚合器节点验证接收到的传感器节点发送的第一混合密文和第一签名是否正确，若是，则进入步骤 e，若否，则回到步骤 b；

e. 中间聚合器节点将接收到的所有的第一混合密文中的最终密文相加得到聚合密文，然后使用中间聚合器节点的私钥对聚合密文解密得到中间聚合密文，采用中间聚合密文、中间聚合器的身份信息、聚合器的身份信息和第二时间戳信息构成第二混合密文，中间聚合器节点使用中间聚合器节点的签名私钥对第二混合密文进行签名获得第二签名，将第二混合密文和第二签名发送到聚合器节点；

f. 聚合器验证接收到的中间聚合器节点发送的第二混合密文和第二签名是否正确，若是，则进入步骤 g，若否，则回到步骤 e；

g. 聚合器将接收到的所有中间聚合密文相加得到最终聚合密文，然后使用聚合器的私钥解密最终聚合密文获得所有传感器的明文。

2. 根据权利要求 1 所述的一种用于无线传感器的网络数据聚合方法，其特征在于，所述步骤 d 的具体方法为：

d1. 中间聚合器验证第一混合密文中的中间聚合器节点的身份信息是否正确，若是，则进入步骤 d2，若否，则回到步骤 b；

d2. 中间聚合器验证第一混合密文中的第一时间戳信息是否正确，若是，则进入步骤 d3，若否，则回到步骤 b；

d3. 中间聚合器聚合多个第一签名后验证第一签名是否正确，若是，则进入步骤 e，若否，则回到步骤 b。

3. 根据权利要求 2 所述的一种用于无线传感器的网络数据聚合方法，其特征在于，所述步骤 f 的具体方法为：

f1. 聚合器验证第二混合密文中的聚合器节点的身份信息是否正确，若是，则进入步骤 f2，若否，则回到步骤 e；

f2. 聚合器验证第二混合密文中的第二时间戳信息是否正确，若是，则进入步骤 f3，若否，则回到步骤 e；

f3. 聚合器聚合多个第二签名后验证第二签名是否正确，若是，则进入步骤 g，若否，则回到步骤 e。

4. 根据权利要求 3 所述的一种用于无线传感器的网络数据聚合方法，其特征在于，所述步骤 a 的具体方法为：

a1. 可信第三方产生一个阶为 n 的椭圆曲线点群 G，其中 $n = q_1q_2$，q_1、q_2为可信第三方

生成的大素数；

a2. 随机选择椭圆曲线点群 G 的两个生成元 P_1, P_2，通过公式 $H = q_2P_2$ 获得 H；

a3. 生成聚合器节点的公钥 PK_{AN} 为 $PK_{AN} = \{n, G, P_1, H\}$、私钥 SK_{AN} 为 $SK_{AN} = q_1$；

a4. 随机选择群 G 的第三个生成元 P_3，每个中间聚合器节点选择一个随机的整数值 $d_j, d_j \in [1, n-1]$，通过公式 $Q_j = d_jP_3$ 获得 Q_j，下标 $j = 1, 2, 3, \ldots, l_2$，l_2 为系统中中间聚合器节点的数目；

a5. 生成中间聚合器节点的公钥 PK_{MA_j} 为 $PK_{MA_j} = \{G, P_3, n, Q_j\}$、私钥 SK_{MA_j} 为 $SK_{MA_j} = d_j$；

a6. 可信第三方产生两个阶为 q 的椭圆曲线点群 G_1, G_2 并生成一个双线性对 $\hat{e}: G_1 \times G_1 \to G_2$；

a7. 随机选择椭圆曲线点群 G_1 的一个生成元 P_4 和一个整数 s，$s \in Z/qZ$，通过公式 $P_{pub} = sP_4$ 获得 P_{pub}；

a8. 定义第一安全哈希函数 $H_1: \{0,1\}^* \to G$，第二安全哈希函数 $H_2: \{0,1\}^* \to G$，第三安全哈希函数 $H_3: \{0,1\}^* \to Z/qZ$；

a9. 计算传感器节点签名私钥 $S_{i,k}$，即 $S_{i,k} = sP_{i,k}$，其中 $k \in \{0,1\}$，$P_{i,k} = H_1(ID_i, k) \in G_1$ 下标 $i = 1, 2, 3, \ldots, l_1$，l_1 为每个中间聚合器节点管理的传感器节点数目，ID 为传感器节点身份标识；

a10. 计算中间聚合器节点签名私钥 $S_{j,k}$，即 $S_{j,k} = sP_{j,k}$，其中 $k \in \{0,1\}$，$P_{j,k} = H_1(ID_{MA_j}, k) \in G_1$，$ID_{MA_j}$ 为中间聚合器节点的身份标识，；

a11. 定义系统公共参数 params 为 $params = \{G_1, G_2, \hat{e}, P_4, P_{pub}, H_1, H_2, H_3\}$，设置可信第三方私钥为整数 s；

a12. 可信第三方在整个系统内部署同步时钟，使得系统内各个用户实时生成当前时间戳。

5. 据权利要求 4 所述的一种用于无线传感器的网络数据聚合方法，其特征在于，所述步骤 b 的具体方法为：

b1. 设传感器节点的身份标识符为 ID_i，传感器采集到的秘密信息为 m_i，i 为传感器节点的编号；采用椭圆曲线算法 BGN，利用聚合器节点的公钥 PK_{MA_j} 对秘密信息 m_i 加密得到中间密文 $C_{BGN}^{i,j}$，其中 $C_{BGN}^{i,j} = (m_iP_1 + r_iH) \in G$，$r_i$ 是一个随机的整数，$r_i \in \{0, 1, 2, 3, \ldots, n-1\}$；

b2. 采用椭圆曲线加密算法 ELG，利用中间聚合器节点的公钥 PK_{MA_j} 对中间密文 $C_{BGN}^{i,j}$ 再次加密得到最终密文 $C_{ELG}^{i,j}$，$C_{ELG}^{i,j} = \{C_{ELG}^{i,j,1}, C_{ELG}^{i,j,2}\}$，其中 $C_{ELG}^{i,j,1} = k_iP_3$，$C_{ELG}^{i,j,2} = C_{BGN}^{i,j} + k_iQ_j$；$k_i$ 是一个随机的整数，$k_i \in [1, n-1]$；

b3. 采用同步时钟生成第一时间戳信息 T_{stamp}，由最终密文 $C_{ELG}^{i,j}$、传感器节点身份信息 ID_i、中间聚合器节点身份信息 ID_{MA_j} 和第一时间戳信息 T_{stamp} 构成第一混合密文 $C_{1,i}$，$C_{1,i} = C_{ELG}^{i,j} \| ID_i \| ID_{MA_j} \| T_{stamp}$。

6. 根据权利要求 5 所述的一种用于无线传感器的网络数据聚合方法，其特征在于，所述步骤 c 的具体方法为：

c1. 传感器节点选择一个虚拟字符串 ω_1，并通过公式 $P_{\omega,1}=H_2(\omega_1)$ 获得哈希值 $P_{\omega,1}$；

c2. 使用第三安全哈希函数 H_3 将第一混合密文 $C_{1,i}$ 及虚拟字符串 ω_1 映射到 Z/qZ，即 $c_i=H_3(C_{1,i},\omega_1)$；

c3. 使用传感器节点签名私钥 $S_{i,k}$ 对第一混合密文 $C_{1,i}$ 签名获得第一签名 σ_i，$\sigma_i=\{S_{MA_j,i},T_{MA_j,i}\}$，$S_{MA_j,i}=r_iP_\omega+S_{i,0}+c_iS_{i,1}$，$T_{MA_j,i}=r_iP_4$，其中 r_i 是一个随机的整数，$r_i\in Z/qZ$；

c4. 传感器节点将第一混合密文 $C_{1,i}$ 及第一签名 σ_i 发送至中间聚合器节点。

7. 根据权利要求 6 所述的一种用于无线传感器的网络数据聚合方法，其特征在于，所述步骤 d 的具体方法为：

d1. 中间聚合器节点接收 l_1 个传感器节点发送的数据后，中间聚合器节点验证接收到的第一混合密文中发送者身份 ID_i 及接收者身份 ID_{MA_j} 是否正确，若是，则进入步 d2，若否，则回到步骤 b；

d2. 通过同步时钟生成本地时间戳 $\hat{T}_{stamp}$，对比本地时间戳 $\hat{T}_{stamp}$ 和接收到的第一时间戳 T_{stamp}，验证是否有恶意第三方进行重放攻击，若否，则进入步骤 d3，若是，则回到步骤 b；

d3. 中间聚合器节点聚合接收到的多个第一签名 σ_i 构成 S_{l_1}，即 $S_{l_1}=\sum_{i=1}^{l_1}S_{MA_j,i},T_{l_1}=\sum_{i=1}^{l_1}T_{MA_j,i}$，然后判断 $\hat{e}(S_{l_1},P)\stackrel{?}{=}\hat{e}(T_{l_1},P_\omega)\hat{e}(P_{pub},\sum_{i=1}^{l_1}P_{i,0}+\sum_{i=1}^{l_1}c_iP_{i,1})$ 是否成立，若是，则判定接收到的第一签名正确，进入步骤 e，若否，则判定接收到的第一签名错误，回到步骤 b，其中 $P_{i,k}=H_1(ID_i,k)$，$k\in\{1,2\}$，$c_i=H_3(C_i,\omega_1)$。

8. 根据权利要求 7 所述的一种用于无线传感器的网络数据聚合方法，其特征在于，所述步骤 e 的具体方法为：

e1. 中间聚合器节点采用椭圆曲线加密算法 ELG 对接收到的第一混合密文中的最终密文 $C_{ELG}^{i,j}$ 聚合获得聚合密文 C_{ELG}^{j}，$C_{ELG}^{j}=\{C_{ELG}^{j,1},C_{ELG}^{j,2}\}$，即 $C_{ELG}^{j,1}=\sum_{i=1}^{l_1}C_{ELG}^{i,j,1},C_{ELG}^{j,2}=\sum_{i=1}^{l_1}C_{ELG}^{i,j,2}$；

e2. 使用中间聚合器节点私钥 SK_{MA_j} 对聚合密文 C_{ELG}^{j} 解密得到中间聚合密文 C_{BGN}^{j}，$C_{BGN}^{j}=C_{ELG}^{j,2}-d_jC_{ELG}^{j,1}=\sum_{i=1}^{l_1}C_{BGN}^{i,j}$；采用同步时钟生成第二时间戳信息 T_{stamp}，构成第二混合密文 $C_{2,j}$ 为 $C_{2,j}=C_{BGN}^{j}\|ID_{MA_j}\|ID_{AN}\|T_{stamp}$，$ID_{AN}$ 为聚合器节点的身份标识；

e3. 中间聚合器节点选择一个虚拟字符串 ω_2，并通过公式 $P_{\omega,2}=H_2(\omega_2)$ 获得哈希值 $P_{\omega,2}$，然后使用第三安全哈希函数 H_3 将第二混合密文 $C_{2,j}$ 及虚拟字符串 ω_2 映射到 Z/qZ，即 $c_j=H_3(C_{2,j},\omega_2)$；

e4. 使用聚合器节点的签名私钥 $S_{j,k}$ 对第二混合密文 $C_{2,j}$ 签名获得第二签名 σ_j，

$\sigma_j=\{S_{MA_j},T_{MA_j}\}$，$S_{MA_j}=r_jP_\omega+S_{j,0}+c_jS_{j,1},T_{MA_j}=r_jP_4$，其中 r_j 是一个随机的整数，$r_j\in Z/qZ$；中间聚合器节点将第二混合密文 $C_{2,j}$ 签名获得第二签名 σ_j 发送至聚合器节点。

9. 根据权利要求 8 所述的一种用于无线传感器的网络数据聚合方法，其特征在于，所述步骤 f 的具体方法为：

f1. 聚合器节点接收 l_2 个中间聚合器节点发送的第二混合密文 $C_{2,j}$ 签名获得第二签名 σ_j 后，聚合器节点验证接收到的第二密文中聚合器节点身份信息 ID_{MA_j} 及聚合器节点身份信息 ID_{AN} 是否正确，若是，则进入步骤 f2，若否，则回到步骤 e；

f2. 通同步时钟生成本地的时间戳 $\hat{T}_{stamp}$，将本地时间戳 $\hat{T}_{stamp}$ 和接收到的第二时间戳 T_{stamp} 进行对比，验证是否有恶意第三方进行重放攻击，若否，则进入步骤 f3，若是，则回到步骤 e；

f3. 聚合器节点将收到的 l_2 个第二签名 σ_j 聚合为 S_{l_2}，即 $S_{l_2}=\sum_{j=1}^{l_2}S_{MA_j},T_{l_2}=\sum_{j=1}^{l_2}T_{MA_j}$；然后批量认证 $\hat{e}(S_{l_2},P)\stackrel{?}{=}\hat{e}(T_{l_2},P_\omega)\hat{e}(P_{pub},\sum_{j=1}^{l_2}P_{j,0}+\sum_{j=1}^{l_2}c_jP_{j,1})$ 是否成立，若是，则判定收到的第二签名正确，进入步骤 g，若否，则判定收到的第二签名错误，回到步骤 e，其中 $P_{j,k}=H_1(ID_{MA_j},k),k\in\{1,2\},c_j=H_3(C_j,\omega_2)$。

10. 根据权利要求 9 所述的一种用于无线传感器的网络数据聚合方法，其特征在于，所述步骤 g 的具体方法为：

聚合器节点首先聚合收到的 l_2 个中间聚合密文 C_{BGN}^j，得到最终聚合密文 C_{BGN}，即 $C_{BGN}=\sum_{j=1}^{\ell_2}C_{BGN}^j$，然后利用椭圆曲线算法 BGN，使用聚合器的私钥 SK_{AN} 解密 C_{BGN} 得到传感器明文的最终聚合统计数据 SUM，即 $SUM=\log_{q_1P_1}(q_1C_{BGN})=\sum_{i=1}^{\ell_1*\ell_2}m_i$。

一种用于无线传感器的网络数据聚合方法

技术领域

[0001] 本发明属于无线通信技术领域，具体的说是涉及一种用于无线传感器的网络数据聚合方法。

背景技术

[0002] 无线传感器网络 (WSN) 是由各种计算和存储能力有限，电量存储也有限的传感器设备组成的一种分布式传感网络。WSN 中的传感器通过无线网络进行通信，因此具有网络设置灵活，设备移动性强的特点。WSN 也可以与互联网进行无线或有线方式的连接。通过无线通信方式可以形成一个多跳自组织网络，因此可以广泛的应用于军事，交通，环境监控等多个领域。

[0003] 对于无线设备而言，电池的使用寿命有限，而无线传感器节点大部分的电量消耗都是在无线通信模块。有研究表明，传感器节点传送数据远比执行计算耗能，将 1bit 数据传送 100 米消耗的能量大约相当于执行 3000 条计算指令需要的能量，因此，在面向应用的，以数据为中心的无线传感器网络中，通过数据聚合技术实现节点间的协作，将处理后的信息而不是原始采集的信息报告给终端用户的方法研究具有十分重要的意义。

[0004] 在很多应用场景中，传感器设备采集到的数据是需要保密的，因此需要采用加密传输的方式聚合。另外，无线传感器设备通常被部署在网络状况恶劣的环境中，传感器设备容易遭到各种各样的攻击，例如重放攻击、伪装攻击等，因而数据聚合方案需要实现数据完整性、数据新鲜性、数据可用性及实体认证。

[0005] 早期的数据聚合方案都假设聚合器是可信的，因此聚合器将成为系统的瓶颈。近十年来，数据聚合方案都假设聚合器是不可信或者是半可信的，这就要求聚合器不仅能够计算得出聚合统计数据，而且不能威胁到单个传感器设备的隐私数据。例如 :2013 年，Li 等使用将解密密钥分割的思想提出一个有效而且简单的数据聚合方案 (Efficient and Privacy-Aware Data Aggregation in Mobile Sensing)。另外，传感器设备通常被部署在恶劣的网络环境中，很容易遭受到各种各样的物理攻击和网络攻击，因此数据聚合方案应当保证数据的新鲜性，完整性，可认证性。例如 :2013 年，Niu 等利用同态哈希和基于身份的聚合签名提出一个基于身份的安全聚合方案 (Lossy data aggregation integrity scheme in wireless sensor networks)。最后由于传感器设备的可移动性，如何有效的解决传感器节点动态加入和退出也将是一个必须解决的问题。

[0006] 本发明方法通过调用安全外包算法使得计算能力有限的传感器设备能够使用非对称密码学对隐私数据加密且签名，不仅能够提供数据保密性，数据完整性保护，数据源认证，抗重放攻击，而且任意传感器设备的动态加入和退出都不会对其他传感器设备的数据隐私产生威胁。

发明内容

[0007] 本发明所要解决的，就是针对上述问题，基于椭圆曲线同态加密算法提出一种用

于无线传感器的网络数据聚合方法。

[0008] 为实现上述目的，本发明采用如下技术方案：

[0009] 一种用于无线传感器的网络数据聚合方法，其特征在于，包括以下步骤：

[0010] a. 系统初始化，通过可信第三方生成聚合器节点的公私钥对和中间聚合器节点的公私钥对；可信第三方还产生传感器节点签名私钥、中间聚合器节点签名私钥、系统公共参数和可信第三方私钥；同时可信第三方在系统内设置一个用于生成时间戳的同步时钟；

[0011] b. 传感器节点采用聚合器节点的公钥对收集到的秘密信息加密得到中间密文，再使用中间聚合器节点的公钥对中间密文加密得到最终密文；采用最终密文、传感器节点身份信息、中间聚合器节点身份信息和第一时间戳信息构成第一混合密文；

[0012] c. 传感器节点使用传感器节点签名私钥对第一混合密文签名获得第一签名，将第一混合密文和第一签名发送到中间聚合器节点；

[0013] d. 中间聚合器节点验证接收到的传感器节点发送的第一混合密文和第一签名是否正确，若是，则进入步骤 e，若否，则回到步骤 b；

[0014] e. 中间聚合器节点将接收到的所有的第一混合密文中的最终密文相加得到聚合密文，然后使用中间聚合器节点的私钥对聚合密文解密得到中间聚合密文，采用中间聚合密文、中间聚合器的身份信息、聚合器的身份信息和第二时间戳信息构成第二混合密文，中间聚合器节点使用中间聚合器节点的签名私钥对第二混合密文进行签名获得第二签名，将第二混合密文和第二签名发送到聚合器节点；

[0015] f. 聚合器验证接收到的中间聚合器节点发送的第二混合密文和第二签名是否正确，若是，则进入步骤 g，若否，则回到步骤 e；

[0016] g. 聚合器将接收到的所有中间聚合密文相加得到最终聚合密文，然后使用聚合器的私钥解密最终聚合密文获得所有传感器的明文。

[0017] 进一步的，所述步骤 d 的具体方法为：

[0018] d1. 中间聚合器验证第一混合密文中的中间聚合器节点的身份信息是否正确，若是，则进入步骤 d2，若否，则回到步骤 b；

[0019] d2. 中间聚合器验证第一混合密文中的第一时间戳信息是否正确，若是，则进入步骤 d3，若否，则回到步骤 b；

[0020] d3. 中间聚合器聚合多个第一签名后验证第一签名是否正确，若是，则进入步骤 e，若否，则回到步骤 b。

[0021] 更进一步的，所述步骤 f 的具体方法为：

[0022] f1. 聚合器验证第二混合密文中的聚合器节点的身份信息是否正确，若是，则进入步骤 f2，若否，则回到步骤 e；

[0023] f2. 聚合器验证第二混合密文中的第二时间戳信息是否正确，若是，则进入步骤 f3，若否，则回到步骤 e；

[0024] f3. 聚合器聚合多个第二签名后验证第二签名是否正确，若是，则进入步骤 g，若否，则回到步骤 e。

[0025] 更进一步的，所述步骤 a 的具体方法为：

[0026] a1. 可信第三方产生一个阶为 n 的椭圆曲线点群 G，其中 $n = q_1q_2$，q_1、q_2为可信第三方生成的大素数；

[0027] a2. 随机选择椭圆曲线点群 G 的两个生成元 P_1, P_2，通过公式 $H = q_2P_2$ 获得 H；

[0028] a3. 生成聚合器节点的公钥 PK_{AN} 为 $PK_{AN} = \{n, G, P_1, H\}$、私钥 SK_{AN} 为 $SK_{AN} = q_1$；

[0029] a4. 随机选择群 G 的第三个生成元 P_3，每个中间聚合器节点选择一个随机的整数值 $d_j, d_j \in [1, n-1]$，通过公式 $Q_j = d_jP_3$ 获得 Q_j，下标 $j = 1,2,3,...,\ell_2, \ell_2$ 为系统中中间聚合器节点的数目；

[0030] a5. 生成中间聚合器节点的公钥 PK_{MA_j} 为 $PK_{MA_j} = \{G, P_3, n, Q_j\}$、私钥 SK_{MA_j} 为 $SK_{MA_j} = d_j$；

[0031] a6. 可信第三方产生两个阶为 q 的椭圆曲线点群 G_1, G_2 并生成一个双线性对 $\hat{e}: G_1 \times G_1 \to G_2$；

[0032] a7. 随机选择椭圆曲线点群 G_1 的一个生成元 P_4 和一个整数 s，$s \in Z/qZ$，通过公式 $P_{pub} = sP_4$ 获得 P_{pub}；

[0033] a8. 定义第一安全哈希函数 $H_1: \{0,1\}^* \to G$，第二安全哈希函数 $H_2: \{0,1\}^* \to G$，第三安全哈希函数 $H_3: \{0,1\}^* \to Z/qZ$；其中 Z/qZ 为密码学中的固定表达式，无特殊含义。

[0034] a9. 计算传感器节点签名私钥 $S_{i,k}$，即 $S_{i,k} = sP_{i,k}$，其中 $k \in \{0,1\}$，$P_{i,k} = H_1(ID_i, k) \in G_1$ 下标 $i = 1,2,3,...,\ell_1, \ell_1$ 为每个中间聚合器节点管理的传感器节点数目，ID 为传感器节点身份标识；

[0035] a10. 计算中间聚合器节点签名私钥 $S_{j,k}$，即 $S_{j,k} = sP_{j,k}$，其中 $k \in \{0,1\}$，$P_{j,k} = H_1(ID_{MA_j}, k) \in G_1$，$ID_{MA_j}$ 为中间聚合器节点的身份标识，；

[0036] a11. 定义系统公共参数 params 为 $params = \{G_1, G_2, \hat{e}, P_4, P_{pub}, H_1, H_2, H_3\}$，设置可信第三方私钥为整数 s；

[0037] a12. 可信第三方在整个系统内部署同步时钟，使得系统内各个用户实时生成当前时间戳。

[0038] 更进一步的，所述步骤 b 的具体方法为：

[0039] b1. 设传感器节点的身份标识符为 ID_i，传感器采集到的秘密信息为 m_i，i 为传感器节点的编号；采用椭圆曲线算法 BGN，利用聚合器节点的公钥 PK_{MA_j} 对秘密信息 m_i 加密得到中间密文 $C_{BGN}^{i,j}$，其中 $C_{BGN}^{i,j} = (m_iP_1 + r_iH) \in G$，$r_i$ 是一个随机的整数，$r_i \in \{0, 1, 2, 3, \ldots, n-1\}$；

[0040] b2. 采用椭圆曲线加密算法 ELG，利用中间聚合器节点的公钥 PK_{MA_j} 对中间密文 $C_{BGN}^{i,j}$ 再次加密得到最终密文 $C_{ELG}^{i,j}$，$C_{ELG}^{i,j} = \{C_{ELG}^{i,j,1}, C_{ELG}^{i,j,2}\}$，其中 $C_{ELG}^{i,j,1} = k_iP_3$，$C_{ELG}^{i,j,2} = C_{BGN}^{i,j} + k_iQ_j$；$k_i$ 是一个随机的整数，$k_i \in [1, n-1]$；

[0041] b3. 采用同步时钟生成第一时间戳信息 T_{stamp}，由最终密文 $C_{ELG}^{i,j}$、传感器节点身份信息 ID_i、中间聚合器节点身份信息 ID_{MA_j} 和第一时间戳信息 T_{stamp} 构成第一混合密文 $C_{1,i}$，$C_{1,i} = C_{ELG}^{i,j} \| ID_i \| ID_{MA_j} \| T_{stamp}$。

[0042] 更进一步的，所述步骤 c 的具体方法为：

[0043] c1. 传感器节点选择一个虚拟字符串 ω_1，并通过公式 $P_{\omega,1}=H_2(\omega_1)$ 获得哈希值 $P_{\omega,1}$；

[0044] c2. 使用第三安全哈希函数 H_3 将第一混合密文 $C_{1,i}$ 及虚拟字符串 ω_1 映射到 Z/qZ，即 $c_i=H_3(C_{1,i},\omega_1)$；

[0045] c3. 使用传感器节点签名私钥 $S_{i,k}$ 对第一混合密文 $C_{1,i}$ 签名获得第一签名 σ_i，$\sigma_i=\{S_{MA_j,i},T_{MA_j,i}\}$，$S_{MA_j,i}=r_iP_\omega+S_{i,0}+c_iS_{i,1}$，$T_{MA_j,i}=r_iP_4$，其中 r_i 是一个随机的整数，$r_i\in Z/qZ$；

[0046] c4. 传感器节点将第一混合密文 $C_{1,i}$ 及第一签名 σ_i 发送至中间聚合器节点。

[0047] 更进一步的，所述步骤 d 的具体方法为：

[0048] d1. 中间聚合器节点接收 ℓ_1 个传感器节点发送的数据后，中间聚合器节点验证接收到的第一混合密文中发送者身份 ID_i 及接收者身份 ID_{MA_j} 是否正确，若是，则进入步 d2，若否，则回到步骤 b；

[0049] d2. 通过同步时钟生成本地时间戳 $\hat{T}_{stamp}$，对比本地时间戳 $\hat{T}_{stamp}$ 和接收到的第一时间戳 T_{stamp}，验证是否有恶意第三方进行重放攻击，若否，则进入步骤 d3，若是，则回到步骤 b；

[0050] d3. 中间聚合器节点聚合接收到的多个第一签名 σ_i 构成 S_{11}，即 $S_{l_1}=\sum_{i=1}^{l_1}S_{MA_j,i},T_{l_1}=\sum_{i=1}^{l_1}T_{MA_j,i}$，然后判断 $\hat{e}(S_{l_1},P)\stackrel{?}{=}\hat{e}(T_{l_1},P_\omega)\hat{e}(P_{pub},\sum_{i=1}^{l_1}P_{i,0}+\sum_{i=1}^{l_1}c_iP_{i,1})$ 是否成立，若是，则判定接收到的第一签名正确，进入步骤 e，若否，则判定接收到的第一签名错误，回到步骤 b，其中 $P_{i,k}=H_1(ID_i,k)$，$k\in\{1,2\}$，$c_i=H_3(C_i,\omega_1)$。

[0051] 更进一步的，所述步骤 e 的具体方法为：

[0052] e1. 中间聚合器节点采用椭圆曲线加密算法 ELG 对接收到的第一混合密文中的最终密文 $C_{ELG}^{i,j}$ 聚合获得聚合密文 C_{ELG}^{j}，$C_{ELG}^{j}=\{C_{ELG}^{j,1},C_{ELG}^{j,2}\}$，即 $C_{ELG}^{j,1}=\sum_{i=1}^{\ell_1}C_{ELG}^{i,j,1},C_{ELG}^{j,2}=\sum_{i=1}^{\ell_1}C_{ELG}^{i,j,2}$；

[0053] e2. 使用中间聚合器节点私钥 SK_{MA_j} 对聚合密文 C_{ELG}^{j} 解密得到中间聚合密文 C_{BGN}^{j}，$C_{BGN}^{j}=C_{ELG}^{j,2}-d_jC_{ELG}^{j,1}=\sum_{i=1}^{\ell_1}C_{BGN}^{i,j}$；采用同步时钟生成第二时间戳信息 T_{stamp}，构成第二混合密文 $C_{2,j}$ 为 $C_{2,j}=C_{BGN}^{j}\|ID_{MA_j}\|ID_{AN}\|T_{stamp}$；

[0054] e3. 中间聚合器节点选择一个虚拟字符串 ω_2，并通过公式 $P_{\omega,2}=H_2(\omega_2)$ 获得哈希值 $P_{\omega,2}$，然后使用第三安全哈希函数 H_3 将第二混合密文 $C_{2,j}$ 及虚拟字符串 ω_2 映射到 Z/qZ，即 $c_j=H_3(C_{2,j},\omega_2)$；

[0055] e4. 使用聚合器节点的签名私钥 $S_{j,k}$ 对第二混合密文 $C_{2,j}$ 签名获得第二签名 σ_j，$\sigma_j=\{S_{MA_j},T_{MA_j}\}$，$S_{MA_j}=r_jP_\omega+S_{j,0}+c_jS_{j,1}$，$T_{MA_j}=r_jP_4$，其中 r_j 是一个随机的整数，$r_j\in Z/qZ$；中间聚合器节点将第二混合密文 $C_{2,j}$ 签名获得第二签名 σ_j 发送至聚合器节点。

[0056] 更进一步的，所述步骤 f 的具体方法为：

[0057] f1. 聚合器节点接收ℓ_2个中间聚合器节点发送的第二混合密文$C_{2,j}$签名获得第二签名 σ_j后，聚合器节点验证接收到的第二密文中聚合器节点身份信息ID_{MA_j}及聚合器节点身份信息ID_{AN}是否正确，若是，则进入步骤 f2，若否，则回到步骤 e；

[0058] f2. 通同步时钟生成本地的时间戳$\hat{T}_{stamp}$，将本地时间戳$\hat{T}_{stamp}$和接收到的第二时间戳T_{stamp}进行对比，验证是否有恶意第三方进行重放攻击，若否，则进入步骤 f3，若是，则回到步骤 e；

[0059] f3. 聚合器节点将收到的ℓ_2个第二签名σ_j聚合为S_{l_2}，即$S_{l_2}=\sum_{j=1}^{l_2}S_{MA_j}, T_{l_2}=\sum_{j=1}^{l_2}T_{MA_j}$；然后批量认证$\hat{e}(S_{l_2},P)\stackrel{?}{=}\hat{e}(T_{l_2},P_\omega)\hat{e}(P_{pub},\sum_{j=1}^{l_2}P_{j,0}+\sum_{j=1}^{l_2}c_jP_{j,1})$是否成立，若是，则判定收到的第二签名正确，进入步骤 g，若否，则判定收到的第二签名错误，回到步骤 e，其中$P_{j,k}=H_1(ID_{MA_j},k)$，$k\in\{1,2\}$，$c_j=H_3(C_j,\omega_2)$。

[0060] 更进一步的，所述步骤 g 的具体方法为：

[0061] 聚合器节点首先聚合收到的ℓ_2个中间聚合密文C_{BGN}^j，得到最终聚合密文C_{BGN}，即$C_{BGN}=\sum_{j=1}^{\ell_2}C_{BGN}^j$，然后利用椭圆曲线算法BGN，使用聚合器的私钥$SK_{AN}$解密$C_{BGN}$得到传感器明文的最终聚合统计数据 SUM，即$SUM=\log_{q_1P_1}(q_1C_{BGN})=\sum_{i=1}^{\ell_1*\ell_2}m_i$。

[0062] 在本发明的方案中，传感器节点在加密和签名的过程中调用安全的外包算法将椭圆曲线的贝点运算外包至半可信的外包服务器，因此传感器节点只需极小的计算开销加密隐私数据。

[0063] 本发明的有益效果为，本发明方法通过使用椭圆曲线同态加密算法，基于身份的聚合签名算法和安全外包算法，使得半可信的聚合器不仅能够在较恶劣的网络环境中获得所需的聚合统计数据，而且能够提供保证保密性、数据完整性、数据源可认证性和抗重放攻击，因此在实际应用中具有广泛的应用前景。

具体实施方式

[0064] 本发明的一种用于无线传感器的网络数据聚合方法，其特征在于，包括以下步骤：

[0065] a. 系统初始化，通过可信第三方生成聚合器节点的公私钥对和中间聚合器节点的公私钥对；可信第三方还产生传感器节点签名私钥、中间聚合器节点签名私钥、系统公共参数和可信第三方私钥；同时可信第三方在系统内设置一个用于生成时间戳的同步时钟；

[0066] b. 传感器节点采用聚合器节点的公钥对收集到的秘密信息加密得到中间密文，再使用中间聚合器节点的公钥对中间密文加密得到最终密文；采用最终密文、传感器节点身份信息、中间聚合器节点身份信息和第一时间戳信息构成第一混合密文；

[0067] c. 传感器节点使用传感器节点签名私钥对第一混合密文签名获得第一签名，将第一混合密文和第一签名发送到中间聚合器节点；

[0068] d. 中间聚合器节点验证接收到的传感器节点发送的第一混合密文和第一签名是否正确，若是，则进入步骤 e，若否，则回到步骤 b ；

[0069] e. 中间聚合器节点将接收到的所有的第一混合密文中的最终密文相加得到聚合密文，然后使用中间聚合器节点的私钥对聚合密文解密得到中间聚合密文，采用中间聚合密文、中间聚合器的身份信息、聚合器的身份信息和第二时间戳信息构成第二混合密文，中间聚合器节点使用中间聚合器节点的签名私钥对第二混合密文进行签名获得第二签名，将第二混合密文和第二签名发送到聚合器节点 ；

[0070] f. 聚合器验证接收到的中间聚合器节点发送的第二混合密文和第二签名是否正确，若是，则进入步骤 g，若否，则回到步骤 e ；

[0071] g. 聚合器将接收到的所有中间聚合密文相加得到最终聚合密文，然后使用聚合器的私钥解密最终聚合密文获得所有传感器的明文。

[0072] 其中，所述步骤 d 的具体方法为 ：

[0073] d1. 中间聚合器验证第一混合密文中的中间聚合器节点的身份信息是否正确，若是，则进入步骤 d2，若否，则回到步骤 b ；

[0074] d2. 中间聚合器验证第一混合密文中的第一时间戳信息是否正确，若是，则进入步骤 d3，若否，则回到步骤 b ；

[0075] d3. 中间聚合器聚合多个第一签名后验证第一签名是否正确，若是，则进入步骤 e，若否，则回到步骤 b。

[0076] 所述步骤 f 的具体方法为 ：

[0077] f1. 聚合器验证第二混合密文中的聚合器节点的身份信息是否正确，若是，则进入步骤 f2，若否，则回到步骤 e ；

[0078] f2. 聚合器验证第二混合密文中的第二时间戳信息是否正确，若是，则进入步骤 f3，若否，则回到步骤 e ；

[0079] f3. 聚合器聚合多个第二签名后验证第二签名是否正确，若是，则进入步骤 g，若否，则回到步骤 e。

[0080] 所述步骤 a 的具体方法为 ：

[0081] a1. 可信第三方产生一个阶为 n 的椭圆曲线点群 G，其中 $n = q_1q_2$，q_1、q_2为可信第三方生成的大素数 ；

[0082] a2. 随机选择椭圆曲线点群 G 的两个生成元 P_1，P_2，通过公式 $H = q_2P_2$ 获得 H ；

[0083] a3. 生成聚合器节点的公钥 PK_{AN} 为 $PK_{AN} = \{n, G, P_1, H\}$、私钥 SK_{AN} 为 $SK_{AN} = q_1$；

[0084] a4. 随机选择群 G 的第三个生成元 P_3，每个中间聚合器节点选择一个随机的整数值 d_j，$d_j \in [1, n-1]$，通过公式 $Q_j = d_jP_3$ 获得 Q_j，下标 $j = 1,2,3,...,\ell_2,\ell_2$ 为系统中中间聚合器节点的数目 ；

[0085] a5. 生成中间聚合器节点的公钥 PK_{MA_j} 为 $PK_{MA_j} = \{G, P_3, n, Q_j\}$、私钥 SK_{MA_j} 为 $SK_{MA_j} = d_j$；

[0086] a6. 可信第三方产生两个阶为 q 的椭圆曲线点群 G_1，G_2 并生成一个双线性对 $\hat{e}: G_1 \times G_1 \to G_2$；

[0087] a7. 随机选择椭圆曲线点群 G_1 的一个生成元 P_4 和一个整数 s，$s \in Z/qZ$，通过公式

P_{pub}= sP_4获得 P_{pub}；

[0088] a8. 定义第一安全哈希函数 H_1:{0,1}*→ G，第二安全哈希函数 H_2:{0,1}*→ G，第三安全哈希函数 H_3:{0,1}*→ Z/qZ；

[0089] a9. 计算传感器节点签名私钥 $S_{i,k}$，即 $S_{i,k}$= $sP_{i,k}$，其中 k ∈ {0,1}，$P_{i,k}$= $H_1(ID_i,k) \in G_1$下标 $i=1,2,3,...,\ell_1,\ell_1$为每个中间聚合器节点管理的传感器节点数目，ID 为传感器节点身份标识；

[0090] a10. 计算中间聚合器节点签名私钥 $S_{j,k}$，即 $S_{j,k}$= $sP_{j,k}$，其中 k ∈ {0,1}，$P_{j,k}=H_1(ID_{MA_j},k)\in G_1$，$ID_{MA_j}$为中间聚合器节点的身份标识，；

[0091] a11. 定义系统公共参数 params 为 $params=\{G_1,G_2,\hat{e},P_4,P_{pub},H_1,H_2,H_3\}$，设置可信第三方私钥为整数 s；

[0092] a12. 可信第三方在整个系统内部署同步时钟，使得系统内各个用户实时生成当前时间戳。

[0093] 所述步骤 b 的具体方法为：

[0094] b1. 设传感器节点的身份标识符为 ID_i，传感器采集到的秘密信息为 m_i，i 为传感器节点的编号；采用椭圆曲线算法 BGN，利用聚合器节点的公钥 PK_{MA_j} 对秘密信息 m_i加密得到中间密文 $C_{BGN}^{i,j}$，其中 $C_{BGN}^{i,j}=(m_iP_1+r_iH)\in G$，$r_i$ 是一个随机的整数，r_i∈ {0,1,2,3,...,n-1}；

[0095] b2. 采用椭圆曲线加密算法 ELG，利用中间聚合器节点的公钥 PK_{MA_j} 对中间密文 $C_{BGN}^{i,j}$ 再次加密得到最终密文 $C_{ELG}^{i,j}$，$C_{ELG}^{i,j}=\{C_{ELG}^{i,j,1},C_{ELG}^{i,j,2}\}$，其中 $C_{ELG}^{i,j,1}=k_iP_3$，$C_{ELG}^{i,j,2}=C_{BGN}^{i,j}+k_iQ_j$；$k_i$是一个随机的整数，$k_i$∈ [1,n-1]；

[0096] b3. 采用同步时钟生成第一时间戳信息 T_{stamp}，由最终密文 $C_{ELG}^{i,j}$、传感器节点身份信息 ID_i、中间聚合器节点身份信息 ID_{MA_j} 和第一时间戳信息 T_{stamp}构成第一混合密文 $C_{1,i}$，$C_{1,i}=C_{ELG}^{i,j}\| ID_i\| ID_{MA_j}\| T_{stamp}$。

[0097] 上述步骤中传感器节点在加密过程中调用安全外包算法将椭圆曲线贝点运算外包至半可信的外包服务器。

[0098] 所述步骤 c 的具体方法为：

[0099] c1. 传感器节点选择一个虚拟字符串 ω_1，并通过公式 $P_{\omega,1}$= $H_2(\omega_1)$ 获得哈希值 $P_{\omega,1}$；

[0100] c2. 使用第三安全哈希函数 H_3将第一混合密文 $C_{1,i}$及虚拟字符串 ω_1映射到 Z/qZ，即 c_i= $H_3(C_{1,i},\omega_1)$；

[0101] c3. 使用传感器节点签名私钥 $S_{i,k}$对第一混合密文 $C_{1,i}$签名获得第一签名 σ_i，$\sigma_i=\{S_{MA_j,i},T_{MA_j,i}\}$，$S_{MA_j,i}=r_iP_\omega+S_{i,0}+c_iS_{i,1}$，$T_{MA_j,i}=r_iP_4$，其中 r_i是一个随机的整数，r_i∈ Z/qZ；

[0102] c4. 传感器节点将第一混合密文 $C_{1,i}$及第一签名 σ_i发送至中间聚合器节点。

[0103] 所述步骤 d 的具体方法为：

[0104] d1. 中间聚合器节点接收ℓ_1个传感器节点发送的数据后，中间聚合器节点验证接收到的第一混合密文中发送者身份 ID_i及接收者身份 ID_{MA_j}是否正确，若是，则进入步 d2，若否，则回到步骤 b；

[0105] d2. 通过同步时钟生成本地时间戳$\hat{T}_{stamp}$，对比本地时间戳$\hat{T}_{stamp}$和接收到的第一时间戳 T_{stamp}，验证是否有恶意第三方进行重放攻击，若否，则进入步骤 d3，若是，则回到步骤 b；

[0106] d3. 中间聚合器节点聚合接收到的多个第一签名 σ_i构成 S_{l_1}，即 $S_{l_1}=\sum_{i=1}^{l_1}S_{MA_j,i}, T_{l_1}=\sum_{i=1}^{l_1}T_{MA_j,i}$，然后判断 $\hat{e}(S_{l_1},P)\stackrel{?}{=}\hat{e}(T_{l_1},P_\omega)\hat{e}(P_{pub},\sum_{i=1}^{l_1}P_{i,0}+\sum_{i=1}^{l_1}c_iP_{i,1})$ 是否成立，若是，则判定接收到的第一签名正确，进入步骤 e，若否，则判定接收到的第一签名错误，回到步骤 b，其中 $P_{i,k}=H_1(ID_i,k), k\in\{1,2\}, c_i=H_3(C_i,\omega_1)$。

[0107] 所述步骤 e 的具体方法为：

[0108] e1. 中间聚合器节点采用椭圆曲线加密算法 ELG 对接收到的第一混合密文中的最终密文$C_{ELG}^{i,j}$聚合获得聚合密文C_{ELG}^{j}，$C_{ELG}^{j}=\{C_{ELG}^{j,1},C_{ELG}^{j,2}\}$，即$C_{ELG}^{j,1}=\sum_{i=1}^{\ell_1}C_{ELG}^{i,j,1}, C_{ELG}^{j,2}=\sum_{i=1}^{\ell_1}C_{ELG}^{i,j,2}$；

[0109] e2. 使用中间聚合器节点私钥SK_{MA_j}对聚合密文C_{ELG}^{j}解密得到中间聚合密文 C_{BGN}^{j}，$C_{BGN}^{j}=C_{ELG}^{j,2}-d_jC_{ELG}^{j,1}=\sum_{i=1}^{\ell_1}C_{BGN}^{i,j}$；采用同步时钟生成第二时间戳信息 T_{stamp}，构成第二混合密文 $C_{2,j}$为 $C_{2,j}=C_{BGN}^{j}\|ID_{MA_j}\|ID_{AN}\|T_{stamp}$；

[0110] e3. 中间聚合器节点选择一个虚拟字符串 ω_2，并通过公式 $P_{\omega,2}=H_2(\omega_2)$ 获得哈希值 $P_{\omega,2}$，然后使用第三安全哈希函数 H_3将第二混合密文 $C_{2,j}$及虚拟字符串 ω_2映射到 Z/qZ，即 $c_j=H_3(C_{2,j},\omega_2)$；

[0111] e4. 使用聚合器节点的签名私钥 $S_{j,k}$对第二混合密文 $C_{2,j}$签名获得第二签名 σ_j，$\sigma_j=\{S_{MA_j},T_{MA_j}\}$，$S_{MA_j}=r_jP_\omega+S_{j,0}+c_jS_{j,1}, T_{MA_j}=r_jP_4$，其中 r_j是一个随机的整数，$r_j\in Z/qZ$；中间聚合器节点将第二混合密文 $C_{2,j}$签名获得第二签名 σ_j发送至聚合器节点。

[0112] 所述步骤 f 的具体方法为：

[0113] f1. 聚合器节点接收ℓ_2个中间聚合器节点发送的第二混合密文 $C_{2,j}$签名获得第二签名 σ_j后，聚合器节点验证接收到的第二密文中聚合器节点身份信息 ID_{MA_j}及聚合器节点身份信息 ID_{AN}是否正确，若是，则进入步骤 f2，若否，则回到步骤 e；

[0114] f2. 通同步时钟生成本地的时间戳$\hat{T}_{stamp}$，将本地时间戳$\hat{T}_{stamp}$和接收到的第二时间戳 T_{stamp}进行对比，验证是否有恶意第三方进行重放攻击，若否，则进入步骤 f3，若是，则回到步骤 e；

[0115] f3. 聚合器节点将收到的 ℓ_2 个第二签名 σ_j 聚合为 S_{l_2}，即 $S_{l_2}=\sum_{j=1}^{l_2}S_{MA_j}, T_{l_2}=\sum_{j=1}^{l_2}T_{MA_j}$；然后批量认证 $\hat{e}(S_{l_2},P)\stackrel{?}{=}\hat{e}(T_{l_2},P_\omega)\hat{e}(P_{pub},\sum_{j=1}^{l_2}P_{j,0}+\sum_{j=1}^{l_2}c_jP_{j,1})$ 是否成立，若是，则判定收到的第二签名正确，进入步骤 g，若否，则判定收到的第二签名错误，回到步骤 e，其中 $P_{j,k}=H_1(ID_{MA_j},k)$，$k\in\{1,2\}$，$c_j=H_3(C_j,\omega_2)$。

[0116] 更进一步的，所述步骤 g 的具体方法为：

[0117] 聚合器节点首先聚合收到的 ℓ_2 个中间聚合密文 C_{BGN}^j，得到最终聚合密文 C_{BGN}，即 $C_{BGN}=\sum_{j=1}^{\ell_2}C_{BGN}^j$，然后利用椭圆曲线算法 BGN，使用聚合器的私钥 SK_{AN} 解密 C_{BGN} 得到传感器明文的最终聚合统计数据 SUM，即 $SUM=\log_{q_1P_1}(q_1C_{BGN})=\sum_{i=1}^{\ell_1*\ell_2}m_i$。