(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 101521664 B
(45)授权公告日 2011.11.09

(21)申请号 200810201833.9

(22)申请日 2008.10.28

(73)专利权人 上海电力学院
地址 200090 上海市杨浦区平凉路2103号

(72)发明人 温蜜 唐忠 叶文珺 李红娇
郑燕飞 邱卫东 陈克非

(74)专利代理机构 上海申汇专利代理有限公司
31001
代理人 吴宝根

(51)Int.Cl.
H04L 29/06(2006.01)
H04L 12/28(2006.01)

审查员 胡丽丽

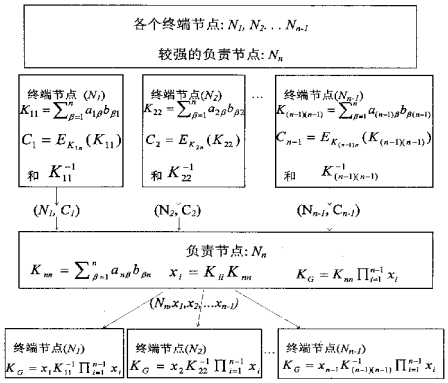
权利要求书 1 页 说明书 4 页 附图 1 页

(54)发明名称

基于传感器网络中协商式组密钥建立的方法

(57)摘要

一种基于传感器网络中协商式组密钥建立的方法，涉及信息安全技术领域；所要解决的是既可保证组密钥安全性也可保证通信中节点的公平性的组密钥建立的技术问题；该组密钥建立方法包括：1）传感器网络中的基站计算出一个在域GF(q)上的n*n的矩阵B和矩阵D，B被当作是公开信息，q是一个小于n的素数；2）完成上述步骤并部署到指定区域后，网络中的每一个节点都计算自己的秘密份额并将其发送给负责计算的节点；利用这些信息，它们就能与其所在组的其他成员节点协商式地完成组密钥的建立。各节点也能验证组密钥的合法性。本发明具有无需可信第三方参与，也不用开销巨大的公钥技术，并能保证组密钥的安全性和组中各成员节点的公平性的特点。



CN 101521664 B

1. 一种基于传感器网络中协商式组密钥建立的方法，其特征在于，方法的步骤如下：

1) 秘密信息的预置：

A) 传感器网络中的基站计算出一个在域 GF(q) 上的 n*n 的矩阵 B，B 被当作是公开信息，q 是一个小于 n 的素数；其中 g^i 是 B 的列生成种子，i = 1，…，n。

B) 基站产生 n 个行生成种子 s_i，i = 1，…，n；基站根据刚才产生的种子构造一个 n*n 的矩阵 D，其每一行的元素都是这些种子的 hash 值；其算法如下：

for(i = 1；i ≤ n；i++)

for(j = 1；j ≤ n；j++)

{if(i > j)，$d_{ij} = H^i(s_j)$；else $d_{ij} = H^i(s_i)$；}

即

$$B=\begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ g & g^2 & g^3 & \cdots & g^n \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ g^{n-1} & (g^2)^{n-1} & (g^3)^{n-1} & \cdots & (g^n)^{n-1} \end{bmatrix}, D=\begin{bmatrix} H^1(s_1) & H^2(s_1) & H^3(s_1)\cdots H^n(s_1) \\ H^2(s_1) & H^2(s_2) & H^3(s_2)\cdots H^n(s_2) \\ \vdots & \vdots & \vdots \\ H^n(s_1) & H^n(s_2) & H^3(s_3)\cdots H^n(s_n) \end{bmatrix};$$

接着，利用 B 和 D 构造一个对称矩阵 K = $(DB)^T B$，能证明 K = $(DB)^T B = B^T D^T B = B^T DB = (AB)^T = K^T$；令 A = $(DB)^T$，则 K = AB；于是，对同一个组中的节点的秘密信息的预置过程如下：

a) 将矩阵 A 中的第 i 行元素预存在节点 Ni 中，A 中的第 i 行可表示为 $r_i(A)$，即 $r_i(A) = [a_{ij}]$；j = 1，…，n；

b) 将矩阵 B 中的第 i 列的列生成种子 g^i 存放在节点 Ni 中；

2) 组密钥建立的过程如下：

A) 每一个节点 Ni，需要计算一个对密钥 K_{in} 和两个自己的私密信息 $K_{ii} = \sum_{\beta=1}^{n} a_{i\beta} b_{\beta i}$ 和 K_{ii}^{-1}；接着，Ni 会发送一个信息 (Ni，$c_i = E_{K_{in}}(K_{ii})$) 给节点 Nn，这里 1 ≤ i ≤ n-1，而 K_{ii}^{-1} 则暂时保存在自己的内存中；

B) 节点 Nn 也会计算自己的私密信息 K_{nn}；一旦接收到各个节点提供的秘密信息 (Ni，c_i)，节点 Nn 分别用它与这些节点的对密钥来解密这些信息；然后计算 $x_i = K_{nn} K_{ii}$；进而，节点再计算 $K_G = K_{nn} \prod_{i=1}^{n-1} x_i$；然后节点将广播一个信息 (Nn，$x_1$，……，$x_{n-1}$) 给所有的其他节点；

C) 一旦接收到 Nn 的广播消息，每一个节点 Nj，都能计算出共享的组密钥 $K_G = x_j K_{jj}^{-1} \prod_{i=1}^{n-1} x_i$，这里 1 ≤ j ≤ n-1。

基于传感器网络中协商式组密钥建立的方法

技术领域

[0001] 本发明涉及信息安全技术，特别是涉及一种传感器网络中的组密钥的建立和验证的方法，尤其是适用需要采用投票方式选择簇头或者用在采样等需要保证各节点的公平性的领域中时，进行信息广播的传感器网络。

背景技术

[0002] 在无线传感器网络中，密码机制作为一种基础的安全机制可以通过用秘密密钥加密消息的方式为我们提供安全通信服务。近年来对于节点间一对一的对密钥的研究非常的广泛和深入，但是组内的通信中除了需要安全的一对一的通信以外经常还需要一对多和多对多的安全多播通信。虽然依赖于对密钥也可以实现安全多播通信，但是消息会被途的接受者逐一地解密和加密后才能安全地到达目标接受者，这样效率太低，网络中的通信负担也太重。如果这个组的全体成员都能共享一个组密钥(group key)，那么多播通信就会非常简单，只需要将消息用组密钥加密就可以了。因此，组密钥的建立对于组内的多播通信是非常重要的。

[0003] 当前的组密钥管理方案主要分为两大类：一类是组密钥分发(group keydistribution 或称分发式组密钥）方案，另一类是组密钥协商（group key agreement 或称协商式组密钥）方案。在组密钥分发方案中，其中的一个参与者或者有一个密钥服务器（key server）负责预先计算或者生成一个组密钥，然后再将此组密钥分发给各个成员。这个方法的特点是简单，通信和计算开销小。但是如果组密钥计算者被攻击或者其恶意地选择一个对攻击者有力的密钥来代替计算出的合法组密钥，成员节点并不知道，因为它们无法验证组密钥的合法性，因此，组密钥分发方法的安全性容易受到威胁。而在组密钥协商方案中，所有的参与者共同协作的完成组密钥的 建立；每一个参与者都要奉献一部分秘密份额，然后由其中一个能力较强的节点负责把所有参与者的秘密份额综合起来生成组密钥，并且每一个参与者能够验证自己所奉献的秘密份额包含在其中。因此以密钥协商得方式建立组密钥的一个好处就是组密钥不能由任何一个参与者独立生成或替换，这样既可以保证了组密钥的安全性也可以保证通信中节点的公平性。但是当前的传感器密钥管理方案并没有这样的好方法，基于这一现状，本发明提供了这样一种新颖的方法。

发明内容

[0004] 针对上述现有技术中存在的缺陷，本发明所要解决的技术问题是提供一种无需可信第三方的参与，也不用开销巨大的公钥技术的，并能保证组密钥的安全性和组中各成员节点的公平性的基于传感器网络中协商式组密钥建立的方法。

[0005] 为了解决上述技术问题，本发明所提供的一种基于传感器网络中协商式组密钥建立的方法，其特征在于??? ，方法的步骤如下：

[0006] 1）秘密信息的预置：

[0007] A）传感器网络中的基站（充当可信的分发者）计算出一个在域 GF(q) 上的 n*n 的

矩阵 B，B 被当作是公开信息，q 是一个小于 n 的素数；范德蒙行列式就是矩阵 B 的最好的例子，其中 $b_{ij} = (g^j)^i \bmod q$；

[0008] B) 基站产生 n 个行生成种子 s_i，i = 1，…，n；基站根据刚才产生的种子构造一个 n*n 的矩阵 D，其每一行的元素都是这些种子的 hash 值；其算法如下：

[0009] for(i = 1；i ≤ n；i++)

[0010] for(j = 1；j ≤ n；j++)

[0011] {if(i>j)，$d_{ij} = H^i(s_j)$；else$d_{ij} = H^j(s_i)$；}

[0012] 即

[0013] $$B=\begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ g & g^2 & g^3 & \cdots & g^n \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ g^{n-1} & (g^2)^{n-1} & (g^3)^{n-1} & \cdots & (g^n)^{n-1} \end{bmatrix}, D=\begin{bmatrix} H^1(s_1) & H^2(s_1) & H^3(s_1) \\ H^2(s_1) & H^2(s_2) & H^3(s_2) \\ H^3(s_1) & H^3(s_2) & H^3(s_3) \end{bmatrix};$$

[0014] 接着，利用 B 和 D 构造一个对称矩阵 $K = (DB)^T B$，能证明 $K = (DB)^T B = B^T D^T B = B^T DB = (AB)^T = K^T$；令 $A = (DB)^T$，则 K = AB；于是，对同一个组中的节点的秘密信息的预置过程如下：

[0015] a) 将矩阵 A 中的第 i 行元素预存在节点 Ni 中，A 中的第 i 行可表示为 ri(A)，即 ri(A) = [aij]；j = 1，…，n。

[0016] b) 将矩阵 B 中的第 i 列的列生成种子 g^i 存放在节点 Ni 中；

[0017] 2) 组密钥建立的过程如下：

[0018] A)(轮一) 每一个节点 Ni(1 ≤ i ≤ n-1) 需要计算一个对密钥 K_{in} 和两个自己的私密信息 $K_{ii} = \sum_{\beta=1}^{n} a_{i\beta} b_{\beta i}$ 和 K_{ii}^{-1}；接着，Ni 会发送一个信息 (Ni，$c_i = E_{K_{in}}(K_{ii})$) 给节点 Nn；而 K_{ii}^{-1} 则暂时保存在自己的内存中；

[0019] B)(轮二) 节点 Nn 也会计算自己的私密信息 K_{nn}；一旦接收到各个节点提供的秘密信息 (Ni，Ci)，节点 Nn 分别用它与这些节点的对密钥来解密这些信息；然后计算 $x_i = K_{nn} K_{ii}$；进而，节点再计算 $K_G = K_{nn} \prod_{i=1}^{n-1} x_i$；然后节点将广播一个信息 (Nn，$x_1$，……，$x_{n-1}$) 给所有的其他节点；

[0020] C)(轮三) 一旦接收到 Nn 的广播消息，每一个节点 Nj(1 ≤ j ≤ n-1) 都能计算出共享的组密钥 $K_G = x_j K_{jj}^{-1} \prod_{i=1}^{n-1} x_i$。

[0021] 本发明提供的基于传感器网络中协商式组密钥建立的方法具有以下有益效果：

[0022] 1) 由于本发明是采用的预分发的方式，在传感器节点撒布在具体区域之前就预置了秘密信息，然后利用对称密钥的性质来建立密钥，无需可信第三方的参与，也不用开销巨大的公钥技术。

[0023] 2) 本发明提供的协商式组密钥建立的方法是一种真正意义上的密钥协商，每一个成员节点根据自己预置的秘密信息计算自己的秘密份额，并且能够验证自己的份额是否包含所建立的组密钥中。这样可以保证组密钥的安全性和组中各成员节点的公平性。

[0024] 附图说明

[0025] 图 1 为本发明实施例基于传感器网络中的组密钥协商建立的过程框图。

具体实施方式

[0026] 以下结合附图说明对本发明的实施例作进一步详细描述，但本实施例并不用于限制本发明，凡是采用本发明的相似方法及其相似变化，均应列入本发明的保护范围。

[0027] 本发明实施例的基于传感器网络中协商式组密钥建立的方法中每一个节点都为组密钥的建立提供一份秘密信息（称之为秘密份额），并且当组密钥建立成功以后各节点可以验证其奉献的秘密份额是否包含在这个组密钥中，这对于检验组密钥的安全性和保证网络中个节点的公平性都提供了有效的手段。不失一般性，假设 N = {N1，N2，……，Nn} 是一个组中所有参与节点的初始集合。其中有一个强有力的节点 Nn 我们称为组头，还有 n-1 个普通节点。

[0028] 本发明实施例的基于传感器网络中协商式组密钥建立的方法，包括 1) 秘密信息的构造和预置；2) 节点部署到指定区域后，根据预置的秘密信息建立组密钥；具体的运行步骤如下：

[0029] 1) 秘密信息的预置：

[0030] 首先，传感器网络中的基站（充当可信的分发者）首先计算出一个在域 GF(q) 上的 n*n 的矩阵 B，B 被当作是公开信息，q 是一个小于 n 的素数；范德蒙行列式就是矩阵 B 的最好的例子，其中 $b_{ij} = (g^j)^i \bmod q$；

[0031] 然后，基站产生 n 个行生成种子 s_i，i = 1，…，n。基站根据刚才产生的种子构造一个 n*n 的矩阵 D，其每一行的元素都是这些种子的 hash 值；其算法如下：

[0032] for(i = 1；i ≤ n；i++)

[0033] for(j = 1；j ≤ n；j++)

[0034] {if(i>j)，$d_{ij} = H^i(s_j)$；else $d_{ij} = H^j(s_i)$；}

[0035] 即

[0036] $$B=\begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ g & g^2 & g^3 & \cdots & g^n \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ g^{n-1} & (g^2)^{n-1} & (g^3)^{n-1} & \cdots & (g^n)^{n-1} \end{bmatrix}, D=\begin{bmatrix} H^1(s_1) & H^2(s_1) & H^3(s_1) \\ H^2(s_1) & H^2(s_2) & H^3(s_2) \\ H^3(s_1) & H^3(s_2) & H^3(s_3) \end{bmatrix}$$

[0037] 接着，利用 B 和 D 构造一个对称矩阵 K = $(DB)^T B$，可以证明 K = $(DB)^T B = B^T D^T B = B^T DB = (AB)^T = K^T$。这里令 A = $(DB)^T$，这样 K = AB。于是，对同一个组中的节点的秘密信息的预置过程如下：

[0038] 第一步；将矩阵 A 中的第 i 行元素预存在节点 Ni 中，A 中的第 i 行可表示为 ri(A)，即 ri(A) = [aij]；j = 1，…，n。

[0039] 第二步；将矩阵 B 中的第 i 列的列生成种子 g^i 存放在节点 Ni 中；

[0040] 2) 如图 1 所示，组密钥的建立：

[0041] 完成上述步骤并部署到指定区域后，网络中的每一个节点都计算自己的秘密份额并将其发送给负责计算的节点；利用这些信息，它们就能与其所在组的其他成员节点一起完成组密钥地建立；具体过程如下：

[0042] 第一步（轮一）：首先，每一个节点 Ni(1 ≤ i ≤ n-1) 需要计算一个对密钥 K_{in} 和两个自己的私密信息 $K_{ii} = \sum_{\beta=1}^{n} a_{i\beta} b_{\beta i}$ 和 K_{ii}^{-1}。接着，Ni 会发送一个信息 (Ni，$c_i = E_{K_{in}}(K_{ii})$) 给节点 Nn；而 K_{ii}^{-1} 则暂时保存在自己的内存中；

[0043] 第二步（轮二）：节点 Nn 也会计算自己的私密信息 K_{nn}；一旦接收到各个节点提供

的秘密信息 (Ni，Ci)，节点 Nn 分别用它与这些节点的对密钥来解密这些信息；然后计算 $x_i = K_{nn}K_{ii}$；进而，节点再计算 $K_G = K_{nn}\prod_{i=1}^{n-1}x_i$；然后节点将广播一个信息 (Nn，$x_1$，……，$x_{n-1}$) 给所有的其他节点；

[0044] 第三步（轮三）：一旦接收到 Nn 的广播消息，每 3 一个节点 Nj(1 ≤ j ≤ n-1) 都可以计算出共享的组密钥 $K_G = x_j K_{jj}^{-1}\prod_{i=1}^{n-1}x_i$。

[0045] 本发明中基于传感器网络中协商式组密钥建立的方法的合法性的验证过程：

[0046] 下面要证明通过运行 2) 中的过程，所有的参与节点都可以建立一个唯一的组密钥；并且每一个节点都可以验证它奉献的秘密份额是包含在该组密钥中的。

[0047] 证明：根据 2) 中的方法，节电 Nn 把消息 (Nn，，x_1，……，x_{n-1}) 广播给所有的节点，并且每一个节点 Ni(1 ≤ i ≤ n-1) 能用自己的私密信息K_{ii}^{-1}来计算出组密钥 K_G。一旦这个组密钥 K_G 建立成功以后，那就意味着下面的等式成立：

[0048] $K_G = x_1 K_{11}^{-1}\prod_{i=1}^{n-1}x_i = x_2 K_{22}^{-1}\prod_{i=1}^{n-1}x_i = \cdots = x_{n-1}K_{n-1n-1}^{-1}\prod_{i=1}^{n-1}x_i$

[0049] 因此，可以得出值 $V=K_G(\prod_{i=1}^{n-1}x_i)^{-1}$。并且 $V=x_1K_{11}^{-1}=x_2K_{22}^{-1}=\cdots\cdots x_{n-1}K_{n-1n-1}^{-1}$。

[0050] 所以有：

[0051] $x_1 = VK_{11}$

[0052] $x_2 = VK_{22}$

[0053] …….

[0054] $X_{n-2} = VK_{(n-2)(n-2)}$

[0055] $X_{n-1} = VK_{(n-1)(n-1)}$

[0056] 从上式能发现，每一个 x_i 包含了参与者 Ni 的秘密份额信息 K_{ii}；由于对于节点 Nj(1 ≤ j ≤ n-1) 都可以计算 $K_G = x_j K_{jj}^{-1}\prod_{i=1}^{n-1}x_i$，可以得到 $K_G = V\prod_{i=1}^{n-1}x_i$。因此，组密钥 K_G 包含了所有参与节点的秘密份额信息 K_{ii}，故而每一个参与节点都可以验证其奉献的秘密份额是包含在这个组密钥中的。

[0057] 本发明适用的环境有：需要进行信息广播的传感器网络，特别是传感器网络采用投票方式选择簇头或者用在采样等需要保证各节点的公平性的领域中时本发明非常适用。

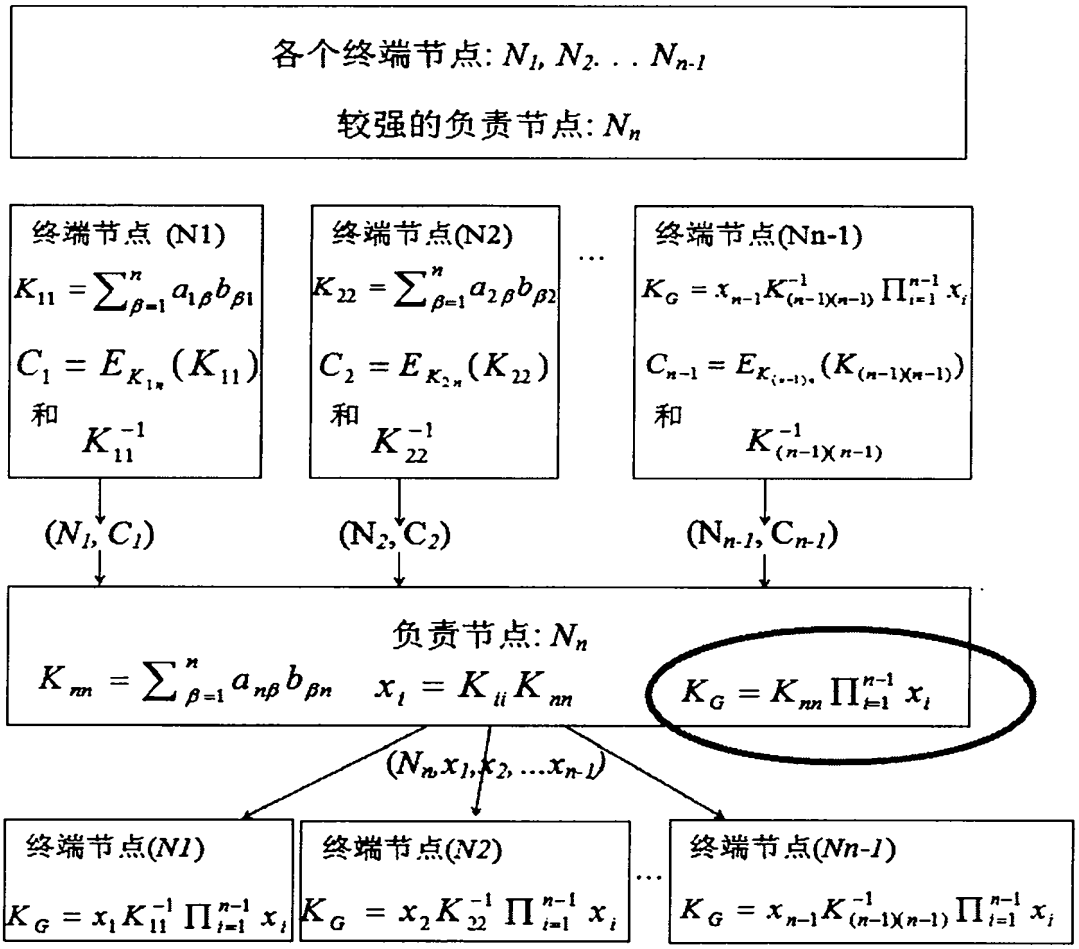

各个终端节点: $N_1, N_2 \ldots N_{n-1}$
较强的负责节点: N_n
终端节点 (N1)
$K_{11} = \sum_{\beta=1}^{n} a_{1\beta} b_{\beta 1}$
$C_1 = E_{K_{1n}}(K_{11})$
和 K_{11}^{-1}
终端节点(N2)
$K_{22} = \sum_{\beta=1}^{n} a_{2\beta} b_{\beta 2}$
$C_2 = E_{K_{2n}}(K_{22})$
和 K_{22}^{-1}
...
终端节点(Nn-1)
$K_G = x_{n-1} K_{(n-1)(n-1)}^{-1} \prod_{i=1}^{n-1} x_i$
$C_{n-1} = E_{K_{(n-1)n}}(K_{(n-1)(n-1)})$
和 $K_{(n-1)(n-1)}^{-1}$
(N_1, C_1)
(N_2, C_2)
(N_{n-1}, C_{n-1})
负责节点: N_n
$K_{nn} = \sum_{\beta=1}^{n} a_{n\beta} b_{\beta n}$ $x_i = K_{ii} K_{nn}$
$K_G = K_{nn} \prod_{i=1}^{n-1} x_i$
$(N_n, x_1, x_2, \ldots x_{n-1})$
终端节点(N1)
$K_G = x_1 K_{11}^{-1} \prod_{i=1}^{n-1} x_i$
终端节点(N2)
$K_G = x_2 K_{22}^{-1} \prod_{i=1}^{n-1} x_i$
...
终端节点(Nn-1)
$K_G = x_{n-1} K_{(n-1)(n-1)}^{-1} \prod_{i=1}^{n-1} x_i$

图 1