

文章编号:1001-9081(2009)03-0638-05

# 无线传感器网络中基于簇协作的分布式组密钥管理方案

曾玮妮<sup>1</sup>, 林亚平<sup>1,2</sup>, 卢秋英<sup>1</sup>

(1. 湖南大学 计算机与通信学院, 长沙 410082; 2. 湖南大学 软件学院, 长沙 410082)

(viol\_v@hotmail.com)

**摘要:**处于敌对环境的传感器网络极易遭到攻击,且不存在长期可信的节点可以担当组管。提出一种分布式组密钥管理方案,方案基于簇形结构,充分利用簇内通信及簇间通信的局部特性,对组密钥协作更新。当妥协节点总数在门限以内的某簇检测出节点妥协时,该簇的簇头发起更新,并通过簇内协作将该节点撤销;当某簇妥协节点数目在门限以上时,由该簇邻居簇的簇头发起更新,并通过簇间通信将该簇妥协节点撤销。与已有方案相比较,此方案能实时地更新组密钥,有着更好的安全性并具有较小的通信开销。

**关键词:**无线传感器网络;组密钥管理;簇内协作;认证数;簇间通信密钥

**中图分类号:** TP393; TP309 **文献标志码:** A

## Distributed group key management scheme based on cluster collaboration in WSN

ZENG Wei-ni<sup>1</sup>, LIN Ya-ping<sup>1,2</sup>, LU Qiu-ying<sup>1</sup>

(1. College of Computer and Communication, Hunan University, Changsha Hunan 410082, China;

2. Software College, Hunan University, Changsha Hunan 410082, China)

**Abstract:** Sensor network is vulnerable to attacks when deployed in unattended fields, and no node can be trusted all the time thus can act as a key server. In this paper, a distributed group key management scheme was proposed. In the new scheme, the group rekeying process took full advantage of the characteristics of the inter-cluster and intra-cluster communication. When the number of the compromised nodes inside one cluster was smaller than  $t$  and a compromised node inside the cluster was detected, the group rekeying would be initiated by the cluster and the compromised nodes would be revoked by inter-cluster collaboration; otherwise, the group rekeying would be initiated by one neighbor cluster of the nodes, and the nodes will be revoked by intra-cluster collaboration. Compared with the existing schemes, the proposed scheme can rekey real-time, provide a high level of security and reduce communication overhead at the same time.

**Key words:** sensor network; group key management; inter-cluster collaboration; authentication number; intra-cluster key

## 0 引言

当无线传感器网络(简称传感器网络)部署在敌对环境时,敌方可能进行各种攻击,比如窃听网络通信、篡改合法消息等,必须将消息加密以确保机密性<sup>[1]</sup>。传感器节点往往密集地部署在目标区域以协同完成各种任务,针对不同任务或不同区域,传感器节点将形成多个通信组<sup>[2-3]</sup>。基站(Base Station, BS)以广播形式发送任务请求给各个特定的组;在组内,任意传感器节点可能广播信息给所有组成员。从机密性角度考虑,将广播信息单独加密发送给每一个组成员并不会增强数据的机密性,相反会增加网络的通信量并可能引起拥塞,为所有组成员共享的组密钥适用于此。组密钥同样可用于加强路由机制的安全性。为了加强网络性能,比如说加强拥塞控制,路由报头通常不会被加密<sup>[4]</sup>;在 TinyOS 1.1.7 中,包含上一跳节点 ID、当前节点 ID、源节点 ID 等信息的路由报头也以明文形式传输。但是当前研究表明,路由报头信息的暴露将暴露位置隐私<sup>[5]</sup>。已有研究表明对称加密计算的使用对于数据传输的时延和吞吐几乎没有影响,可以与消息传输同时进行<sup>[6]</sup>。因此,基于对称加密体制的组密钥的使用可以在保证报头机密性的同时保证路由控制。此外,诸如虚假数据过滤、数据融合等各种服务同样需要用到组密钥<sup>[7-8]</sup>。

因此,传感器网络中的组密钥管理是一个十分有意义的课题。

由于传感器网络中的节点资源有限,传统网络中的组密钥管理机制不适合传感器网络,传感器网络中的组密钥管理引起了研究界的广泛关注,并且已经取得了一些进展<sup>[9-15]</sup>,提出的管理机制主要分为分布式管理机制和集中式管理机制。集中式密钥管理模型由一个专门的组管负责组密钥的生成,并通过特定算法分发给群组中的每个成员,这种机制存在单点失效问题。分布式管理的特点是所有组成员通过密钥协商来共同建立组密钥,一般来说这种模型的安全性更好,但在实现上更为困难。由于传感器网络所处的特点,采用分布式组密钥管理模型更为合适。

已有一些分布式管理方案<sup>[9-11]</sup>,但是均存在着不足。文献[9]中各节点预置当前和未来的组密钥信息,并将其分散在邻居节点中,每个节点通过与邻居节点的协作周期性更新。但是该方案安全性不高,敌方妥协门限个节点就能获取当前及未来的组密钥;其次,每个节点都必须存储多个邻居节点的更新信息;每轮组密钥更新时,组内任意节点都需要多个邻居节点通过对偶链路进行信息支持,通信和存储开销较大。文献[10]提出了一种基于分布式更新权限的组密钥管理方案,各个组节点预置组密钥的更新权限、节点妥协等异常情况发生时由局部网络协商产生一个临时可信的 KS(Key Server),

收稿日期:2008-09-11;修回日期:2008-11-02。 基金项目:湖南省自然科学基金重点项目(06JJ20049)。

作者简介:曾玮妮(1982-),女,湖南邵阳人,博士研究生,主要研究方向:传感器网络; 林亚平(1955-),男,湖南邵阳人,教授,博士生导师,主要研究方向:计算机网络、机器学习; 卢秋英(1986-),女,江西铜鼓人,硕士研究生,主要研究方向:传感器网络。

由KS发起更新。然而,该方案每次更新的数据量较大,很容易受链路影响。文献[11]利用ECC(椭圆曲线加密算法)在节点间两两形成通信密钥对,按照环形拓扑,利用通信密钥对加密组密钥以单播方式在组节点间进行发送。这种机制中组密钥的发送需要节点对间的多个单播,如果某个节点发生故障或妥协等情况都将导致组密钥不能正常生成,容错性不强。

已有一些集中式管理机制<sup>[12-15]</sup>。文献[12]中由网关担当组管,负责组密钥更新,各节点从网关发出的更新广播中获取其更新信息并协同获取组密钥,该机制可能遭到单点失效问题且更新存在大的时延。文献[13]中由普通节点担当组管,并负责组密钥的更新,如果组管妥协则推选新组管,然而远距离组节点很难对新组管的合法性进行检测。文献[14]中,通信组为基站担当根节点的任务树,每棵任务树划分为多个层次,由根节点发起组密钥的更新,并利用各层的层密钥逐层进行。该方案每一层的操作都依赖于祖先节点,如果某祖先节点出现妥协或硬件故障等情况将导致该点以下的操作无法进行,而临时更换祖先节点将导致大的时延和通信开销。文献[15]基于双向哈希链提出了一种集中式组密钥管理机制,该机制由组管周期性发起组密钥更新,主要用于解决包严重丢失环境下组密钥的自修复。由于更新信息以加密单播方式发送,能耗较大,且没有考虑节点妥协等异常情况下的组密钥更新。

为了弥补已有机制的不足,基于对称加密体制,本文提出一种新的适用于传感器网络的分布式组密钥管理方案。为了提高网络的伸缩性、自治性、路由质量等性能,传感器网络往往形成簇形结构<sup>[16-17]</sup>。为了更好地对抗节点妥协,基于簇形结构,本方案充分利用簇内通信及簇间通信的局部特性,构造簇间密钥函数和认证数函数以实现组密钥的更新,并能进行簇内的节点撤销及簇间的节点撤销,为便于描述,简称 GKCC (Group Key management scheme based on Cluster Collaboration)。与已有组密钥管理方案相比较,GKCC 能够提高网络的安全性,并具有较小的通信开销,是一种适合传感器网络的高效的组密钥管理方案。

## 1 系统模型及相关假设

本文考虑静态网络,即传感器节点在网络部署后不再改变物理位置的网路。传感器节点为当前主流的节点类型,如 Berkeley 的 MICA 系列,这些节点一般由 8 MHz 的处理器和 4 KB 的 RAM 构成,由电池供电。节点所拥有的存储空间足够用于保存一些用于组密钥更新的信息。网络部署后,整个网络初始化成多个单跳簇<sup>[16]</sup>,每一个簇有一个簇头,且簇头在簇内轮换。与已有的组密钥管理方案<sup>[9-10]</sup>相似,本文假设:1)网络在部署后的一小段时间内是安全的,在这个时间内足够进行一些网络初始化操作;2)采用分布式的入侵监测机制<sup>[17-19]</sup>对妥协节点进行实时检测和标识,并利用对偶密钥管理机制<sup>[20]</sup>实现节点间信息传输的保密性;3)敌方妥协节点需要一定的时间,在这个时间内足够通信组更新组密钥;4)妥协节点能实时地被检测出,没有被妥协的节点是可以信赖的,也就是说未被妥协的节点能正确地执行预置的算法。

## 2 组密钥管理方案 GKCC

### 2.1 基本思想

传感器节点通信覆盖范围小,且通常只与其邻居节点直接通信,节点出现妥协等故障时,最先发现的往往是其邻居节点,而簇内节点往往互为邻居,因此提出基于簇协作的分布式

组密钥管理方案。方案以簇为单位对组密钥更新信息进行保护。当妥协节点总数在门限以内的簇出现节点妥协时,通过簇内协作将该节点撤销,并协作生成新的认证数向邻居簇发起组密钥更新,任意簇如果收到合法的来自邻居簇的组密钥更新消息,则在簇内协作生成认证数,向其他邻居簇发送该更新消息。当某簇出现妥协节点数目在门限以上时,其邻居簇通过停止与该簇的簇间通信将该簇妥协节点撤销,从而有效提高了安全性。

### 2.2 相关标记、定义及性质

设节点投放后首次进行的组密钥更新为第一轮更新,第  $(j-1)$  轮更新完成与第  $j$  轮更新完成之间的间隔为第  $j$  阶段,第  $j$  阶段的组密钥记为  $GK_j$ 。所有的 ID 全局唯一,记 ID 为  $i$  的节点为  $v_i$ ,ID 为  $k$  的簇为  $C_k$ ,其簇头为  $CH_k$ ,其簇内通信密钥为  $CK_k$ ,称妥协节点数目小于  $(t+1)$  的簇为合法簇,  $C_k$  合法邻居簇所成集合为  $N^k$ 。节点  $v_i$  与  $v_k$  之间对偶密钥记为  $K_{i,k}$ ;  $C_a$  与  $C_b$  间的通信密钥记为  $CK_{a,b}$ ,  $C_a$  与 BS 间通信密钥为  $CK_{a,BS}$ 。阶段 ID 所成集合与节点 ID 所成集合及簇 ID 所成集合两两相交为空。 $\{M\}_K$  表示用密钥  $K$  加密信息  $M$ 。

**定义 1** 簇间密钥函数。簇间密钥函数  $F(x,y,z)$  是有限素数域  $F(q)$  上的三元对称多项式,  $F(x,y,z) = \sum_{i=0}^t \sum_{j=0}^t \sum_{k=0}^t f_{i,j,k} x^i y^j z^k$ , 且  $f_{i,j,k} = f_{k,j,i}$ 。对于第  $l$  阶段的任意簇  $C_a$ ,定义其簇间密钥函数  $f_{c_{la}}(x) = F(x,l,a)$ ,簇间密钥函数用于计算簇间通信密钥。

**性质 1** 处于阶段  $l$  的任意簇  $C_a$  据  $f_{c_{la}}(x)$  可得其与簇  $C_b$  之间的通信密钥  $f_{c_{la}}(b)$ ,簇  $C_b$  据  $f_{c_{lb}}(x)$  可得其与簇  $C_a$  之间的通信密钥  $f_{c_{lb}}(a)$ ,则有  $CK_{a,b} = f_{c_{la}}(b) = f_{c_{lb}}(a)$ 。

$$\begin{aligned} \text{证明 } f_{c_{la}}(b) &= \sum_{i=0}^t \sum_{j=0}^t \sum_{k=0}^t f_{i,j,k} b^i l^j a^k \\ f_{c_{lb}}(a) &= \sum_{i=0}^t \sum_{j=0}^t \sum_{k=0}^t f_{i,j,k} a^i l^j b^k \end{aligned}$$

因为  $f_{i,j,k} = f_{k,j,i}$ , 所以  $f_{c_{la}}(b) = f_{c_{lb}}(a)$ 。

**定义 2** 认证数函数。认证数函数  $P(x,y) = \sum_{i=0}^{\mu} \sum_{j=0}^t p_{i,j} x^i y^j$ ,第  $l$  阶段的认证数  $N_l = P(l,l)$ ,且  $N_{l-1} = H(N_l)$  ( $\mu \geq l \geq 1$ ),其中  $H(x)$  为单向哈希函数。记任意节点  $v_k$  在网络部署前预置的认证数函数为  $P_k(x,y)$ ,部署后任意簇  $C_a$  的认证数函数为  $P^a(x,y)$ ,第  $l$  阶段的认证数为  $N_l^a$ 。

**定义 3** 妥协节点集。阶段  $l$  的妥协节点所成集合  $C_l = \{c_1, c_2, \dots, c_m\}$ ,其中  $c_i$  ( $1 \leq i \leq m$ ) 为第  $l$  阶段妥协节点的 ID 号。

### 2.3 管理方案 GKCC

#### 2.3.1 网络初始化

任意节点  $v_k$  在网络部署前预置  $F(x,y,k)$ 、 $P_k(x,y)$  及  $GK_0$ 。网络部署后初始化成多个单跳簇<sup>[16-17]</sup>,对于  $\forall C_a$ ,设  $CH_a$  由节点  $v_k$  担当,则  $P^a(x,y) = P_k(x,y)$ ,  $CH_a$  向  $\forall v_i \in C_a$  发送  $\{P^a(x,i)\}_{K_{i,k}}$ ,并向任意邻居簇  $C_b$  发送  $\{a, N_0^a\}_{CK_0}$ ,向 BS 发送  $\{a, k, N_0^a\}_{CK_0}$ 。对于  $\forall v_i \in C_a$ ,计算  $F(i,y,a)$  并删除  $F(i,y,z)$  以及  $p_i(x,y)$ ,计算与邻居簇间的通信密钥、存储邻居簇 ID 及对应  $N_0^{id}$ 。

#### 2.3.2 组密钥更新

当组节点妥协等异常情况发生时,需要进行组密钥的更新。以阶段  $j$  为例进行描述。设妥协节点  $v_r \in C_a$ ,且  $C_a$  为合法簇(即妥协节点数小于  $(t+1)$ ),一旦检测出  $v_r$  妥协,  $CH_a$

随即生成新的  $CK_a$ , 并通过对偶密钥将新的  $CK_a$  发送给  $C_a$  中的任意节点  $v_k$  ( $k \neq r$ )。随即,  $C_a$  发起组密钥的更新, 如下:

**步骤 1**  $C_a$  内任意节点  $v_i$  向  $CH_a$  发送  $\{F(i, j, a), P^a(j, i)\}_{K_i, CH_a}$ 。 $CH_a$  据拉格朗日插值原理计算认证数函数  $P^a(j, y)$  以及  $f_{c_{ja}}(x)$ , 据  $P^a(j, y)$  计算  $N_j^a$ , 据  $f_{c_{ja}}(x)$  计算  $CK_{a,b} = f_{c_{ja}}(b)$  ( $b \in N^a$ ), 并在簇内广播  $\{N_j^a, CK_{a,b} (b \in N^a), GK_j\}_{CK_a \circ C_a}$  内合法节点存储  $N_j^a$  并删除  $N_{j-1}^a$ 。

记  $T$  为当时时间,  $CH_a$  向 BS 发送  $\{GK_j, T, N_j^a, C_j\}_{CK_a, BS}$ , 向任意合法邻居簇  $C_b$  发送  $\{a, N_j^a\} \cup \{GK_j, T, N_j^a, C_j\}_{CK_a, b}$ , 发起组密钥的更新。

**步骤 2**  $C_a$  的任意合法邻居簇  $C_b$  在收到  $\{a, N_j^a\} \cup \{GK_j, T, N_j^a, C_j\}_{CK_a, b}$  后, 首先验证  $N_{j-1}^a = H(N_j^a)$  是否成立, 如果成立,  $C_b$  内任意节点  $v_i$  向  $CH_b$  发送  $\{F(i, j, b), P^b(j, i)\}_{K_i, CH_b}$ , 存储  $N_j^b$  并删除  $N_{j-1}^b$ 。同步步骤 1,  $CH_b$  计算认证数  $N_j^b$  以  $CK_{b,e} (e \in N^b)$ , 在簇内广播  $\{CK_{b,e} (e \in N^b)\}_{CK_b}$ ,  $C_b$  内节点据  $CK_{b,a}$  即可获取  $\{GK_j, T, N_j^b, C_j\}$ 。

$CH_b$  向任意合法邻居簇  $C_e$  发送  $\{b, N_j^b\} \cup \{GK_j, T, N_j^b, C_j\}_{CK_{b,e}}$ 。

**步骤 3** 对于非  $C_a$  邻居簇的合法簇  $C_e$ , 设  $C_e$  收到  $\{b, N_j^b\} \cup \{GK_j, T, N_j^b, C_j\}_{CK_{b,e}}$ , 则  $C_e$  内节点首先验证  $N_{j-1}^b = H(N_j^b)$  是否成立。如果成立, 存储  $N_j^b$  并删除  $N_{j-1}^b$ , 获取  $\{GK_j, T, N_j^b, C_j\}$ , 并发送  $\{P^e(j, i)\}_{K_i, CH_e}$  给  $CH_e$ 。

$CH_e$  计算并验证认证数  $N_j^e$ , 向任意合法邻居簇  $C_f$  发送  $\{e, N_j^e\} \cup \{GK_j, T, N_j^e, C_j\}_{CK_{e,f}}$ 。重复步骤 3, 直至整个组。

**步骤 4** 算法结束。

如果在第  $j$  阶段, 分属不同簇的几个节点同时被妥协, 由上述更新过程可知, 各妥协节点所在簇将分别发起组密钥的更新, 这时  $GK_j$  为时间  $T$  最早的组密钥更新广播中的组密钥。如果某簇  $C_e$  的妥协节点数达到  $(t+1)$ , 其邻居簇将发起组密钥的更新, 过程同上, 这时  $C_e$  的认证数将被其邻居簇删除, 任何由其发起的组密钥更新视为非法更新。

### 3 算法分析

#### 3.1 安全性分析

在传感器网络中评价一种密钥管理方案的安全性, 通常考虑四个方面的因素: 反俘获性、抗复制性、剔除性和伸缩性<sup>[1]</sup>。下述定理证明了本方案有着很好的反俘获性。

**定理 1** 簇间密钥函数  $F(x, y, z)$  被暴露, 当且仅当:

(1) 至少  $(t+1)$  个簇有节点被妥协, 且每个簇至少妥协  $(t+1)/2$  个节点或至少  $(t+1)/2$  个簇有节点被妥协, 且每个簇至少妥协  $(t+1)$  个节点; 或者 (2)  $(t+1)^3/2$  个簇间密钥被捕获。

**证明** 要想获得簇间密钥函数  $F(x, y, z)$ , 必须获取其各系数项。  $F(x, y, z) = \sum_{i=0}^t \sum_{j=0}^t \sum_{k=0}^t f_{i,j,k} x^i y^j z^k$ ,  $f_{i,j,k} = f_{k,j,i}$  故其系数共有  $(t+1)^3/2$  项, 这相当于要求解一个  $(t+1)^3/2$  元方程组。

(1) 不妨设  $F(i, y, a) = u_0 + u_1 y + u_2 y^2 + \dots + u_t y^t$ , 则有:

$$\begin{cases} f_{000} + if_{100} + af_{001} + i^2 f_{200} + a^2 f_{002} \dots + i^t a^t f_{00t} = u_0 \\ f_{010} + if_{110} + af_{011} + i^2 f_{210} + a^2 f_{012} \dots + i^t a^t f_{01t} = u_1 \\ \vdots \\ f_{0t0} + if_{1t0} + af_{0t1} + i^2 f_{2t0} + a^2 f_{0t2} \dots + i^t a^t f_{0tt} = u_t \end{cases}$$

$$\det \begin{pmatrix} 1 & \dots & i^t a^t \\ \vdots & & \vdots \\ 0 & \dots & i^t a^t \end{pmatrix} = (t+1)$$

因此若想获取  $F(x, y, z)$ , 必须妥协  $(t+1)$  个簇, 且每个簇至少妥协  $(t+1)/2$  个节点或妥协  $(t+1)/2$  个簇, 且每个簇必须妥协至少  $(t+1)$  个节点。

(2) 与 (1) 同理, 略。

方案 B-PCGR 及 DRA 在  $t$  个节点妥协时即被攻破。在本方案中, 妥协节点必须通过簇间通信密钥获取组密钥, 从定理 1 可知, 方案 GKCC 有着更好的反俘获性。假设敌方妥协了合法簇  $C_a$  中节点  $v_r$ , 并企图利用  $v_r$  发起虚假的组密钥更新广播, 由于  $v_r$  不能获取认证数  $N_j^a$ , 更新广播在局部范围将被抛弃, 不会对网络造成大的影响。而要想获取  $N_j^a$ , 敌方必须在  $C_a$  内妥协至少  $(t+1)$  个节点。假设敌方企图利用  $v_r$  篡改组密钥更新时的广播, 如果  $v_r$  篡改  $N_j^a$  或  $x$ , 则接收到的节点通过哈希运算将检测出这一篡改, 并抛弃该信息; 如果  $v_r$  仅篡改  $\{GK_j, T, N_j^a, C_j\}_{CK_{a,x}}$ , 则接收节点通过核对  $N_j^a$  值即可判断。

方案 GKCC 还具有很好的剔除能力。如果合法簇中某节点被妥协, 其所在簇将更新簇内密钥, 并协作生成新的簇间密钥, 妥协节点不能获取新的簇密钥, 必不能获取新的簇间通信密钥及新的组密钥, 这样就被从组通信中剔除。如果某簇被妥协节点达到了  $(t+1)$ , 则其邻居簇将删除该簇的认证数, 将该簇从簇间通信中删除。删除该簇的通信信息并不会影响到组内其他簇的后续更新。

方案 GKCC 同样具有很好的伸缩能力。当阶段  $j$  有新的节点  $v_k$  需要加入网络中某区域, 该区域所在簇为  $C_a$ , BS 只需在  $v_k$  中预置  $C_a$  及其邻居簇的认证数函数、簇间密钥函数以及这些簇下一阶段的认证数  $N_{j+1}^a$ , 即可将  $v_k$  投放入网络。投放后节点  $v_k$  的邻居节点根据  $N_{j+1}^a$ , 即可接纳  $v_k$  为合法邻居节点, 并更新组密钥。而  $v_k$  根据所在簇信息即可局部化预置信息, 如已有网络节点一样工作。

最后, 本方案具有很好的抗复制能力。假设敌方妥协了一个传感器节点, 然后对这个传感器节点进行复制, 投放入网络中各个区域, 企图对整个传感器网络进行控制。由于复制节点没有新的位置所在簇的私有信息, 不会被邻居节点所接纳, 从而不能加入簇, 参与簇协作, 获取组密钥。

#### 3.2 性能分析及比较

为方便分析和比较, 记组节点数为  $N$ , 每个节点的平均邻居节点数为  $n_1$ , 簇数目为  $N_c$ , 每个簇的平均邻居簇数目为  $n_c$ , 簇内平均转发次数为  $h$ ; 密钥长、认证数长、多项式系数和多项式值均为  $L$  (位); 每条广播信息抵达全组的转发次数为  $r$ 。方案 GKCC 中任意节点  $v_i \in C_a$  需要存储一元  $\mu$  次多项式  $P^a(x, i)$  及一元  $t$  次多项式  $F(i, y, a)$ 、 $(n_c + 1)$  个认证数和簇内密钥  $CK_a$ , 故其存储开销为  $(t + \mu + n_c + 4)L$ 。接下来考虑计算开销, 节点需要对来自  $n_c$  个邻居簇的更新广播进行解密并对认证数进行验证, 这需要  $n_c$  次哈希运算及  $n_c$  次解密; 如果节点担当簇头, 还需要计算新的认证数并向邻居簇发送组密钥更新广播, 计算开销分别为  $F(q)$  域上运算复杂度为  $O(t^2)$  的乘除运算以及  $n_c$  次加密。妥协节点所在簇及其邻居簇的簇头数目很小, 其额外计算开销忽略不计。每个节点总的计算开销最多为:  $F(q)$  域上运算复杂度为  $O(t^2)$  的乘除运算、 $n_c$  次哈希运算及  $2n_c$  次加解密。方案 GKCC 的通信开销分为两个部分:

第一部分, 各簇协作获取该簇的认证数, 组内总的开销最

多为  $hNL$ ;

第二部分,组密钥更新广播在簇内及簇间加密发送,由于时间  $T$ 、节点ID及簇ID都是很小的数字,其长度之和考虑为

$2L$ ,则广播长度为  $4L$ ,这一过程所需开销最多为  $4(n_c + h)N_c$ ,故总的通信开销  $S_c = (hN + 4(n_c + h)N_c)L$ 。对方案 GKCC、B-PCGR<sup>[9]</sup>、DRA<sup>[10]</sup> 各项开销的比较见表1。

表1 性能比较

性能比较项	方案	方案	方案
	B-PCGR	DRA	GKCC
是否分布式	是	是	是
整个网络的通信开销(最大)	$Nn_1L$	$(\frac{19}{2}t + 8)rL$	$hN + 4(n_c + h)N_c$
每一个节点的存储开销/位	$(n_1 + 1)(t + 1)L$	$12L$	$(t + \mu + n_c + 4)L$
每一个节点的计算开销(最大)	$2n_1$ 次加密/解密, $F(q)$ 域上乘除运算复杂度为 $O(\mu^3 + (n_1 + 1)t^2)$	$F(q)$ 域上乘除运算复杂度为 $8O(t^2)$	$2n_c$ 次加密/解密, $n_c$ 次哈希运算, $F(q)$ 域上乘除运算复杂度为 $O(t^2)$

结合表1,通过分析可以发现,方案 GKCC 其存储和计算开销略高于 DRA;计算开销低于 B-PCGR,由于  $n_1 \geq 2t$ ,取等号,当  $\mu < 2t^2$  时,存储开销低于 B-PCGR。GKCC 的通信开销是与簇数目  $N_c$ 、邻居簇数目  $n_c$  及簇大小相关的一个值,这取决于网络覆盖范围和分簇算法,为方便比较,对  $(n_c + h)N_c$  进行理论上的估计。由于非正方形区域总可以分割成正方形区域之和,不妨取正方形区域作为传感器网络的覆盖区域进行估计,并记区域边长为  $a$ 。记传感器节点的通信半径为  $R$ ,假设簇内节点互为邻居节点,因而簇所在区域总是在以  $R$  为半径的圆域以内,不妨将簇所在区域抽象为半径  $R$  的圆的内接正方形,则  $n_c = 8$ ,考虑单跳簇,则信息抵达全簇的簇内平均转发次数  $h = 4$ ,于是  $(n_c + h)N_c = 6a^2/R^2$ ,方案 GKCC 总的通信开销  $S_c = (hN + 24a^2/R^2)L$ 。

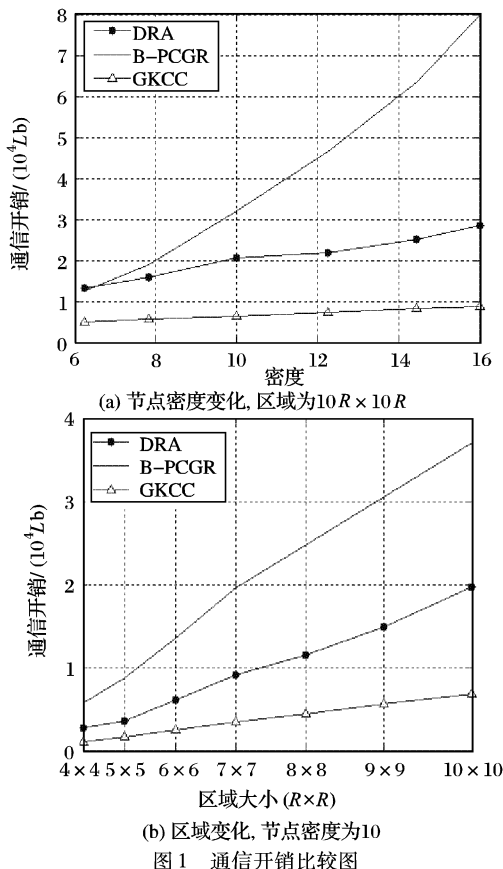
$10R \times 10R$  间变化,  $N$  在 625 和 1600 之间变化,按照文献[22]中成簇算法成簇,对方案 GKCC 的更新过程进行模拟。图1(a)显示了传感器节点均匀分布于大小为  $10R \times 10R$  的区域,  $N$  在 625 和 1600 之间变化(即网络密度在 6.25 和 16 之间变化)时,各方案通信开销的变化情况。图1(b)显示了网络密度固定为 10,网络覆盖区域  $a$  在  $4R \times 4R$  到  $10R \times 10R$  之间变化时各方案通信开销的变化情况。从图1(a)可以看出,  $S_c$  随密度变化不大,且随密度增大略有降低,这是由于  $S_c$  主要与簇数目及各簇的平均邻居簇相关,在网络连通的前提下,当区域大小及节点通信半径固定时,簇数目及各簇的平均邻居簇固定,  $S_c$  的大小只随广播转发次数  $r$  变化,而  $r$  随密度增大略有降低。从图1(b)可以看出,  $S_c$  的大小随区域基本呈线性变化,这是由于簇数目随区域基本呈线性变化。可见无论区域规模或节点疏密,方案 GKCC 在通信开销上均优于已有方案 B-PCGR 及 DRA。

#### 4 结语

无线传感器网络中的组密钥管理有利于通信组内安全、快速的通信。本文基于簇协作提出了一种新的分布式组密钥管理方案 GKCC,此方案具有以下特点。1) GKCC 能实时地进行组密钥更新。2) GKCC 能更好地对抗节点妥协,当妥协节点总数在门限以内的簇出现节点妥协时,通过簇内协作可以将该节点撤销;当某簇妥协节点数目在门限以上时,通过簇间通信可以将该簇妥协节点撤销。3) GKCC 中组密钥更新数据包很小,在相同发送次数的前提下,通信开销要小,且受链路误差影响小。本文致力于设计满足应用需求、低能耗的组密钥管理方案,下一步工作将针对特定的传感器网络应用背景,并结合传感器网络的运行特性,考虑其底层局限性,研究有效的组密钥管理方案。

#### 参考文献:

- [1] CHAN H, PERRIG A. Security and privacy in sensor networks[J]. IEEE Computer, 2003, 36(10): 103–105.
- [2] LIU JUAN, LIU JIE, REICH J E, et al. Distributed group management for track initiation and maintenance in target localization applications[C]// Proceedings of the Second International Workshop on Information Processing in Sensor Networks (IPSN'03), LNCS 2634. Berlin: Springer, 2003: 113–128.
- [3] 李小龙, 林亚平, 胡玉鹏, 等. 基于分组的分布式节点调度覆盖算法[J]. 计算机研究与发展, 2008, 45(1): 180–187.
- [4] WOO A, TONG T, CULLER D. Taming the underlying challenges of reliable multihop routing in sensor networks[C]// The ACM Conference on Embedded Networked Sensor Systems 2003. New York: ACM, 2003: 14–27.



方案 DRA 中通信开销与广播转发次数  $r$  相关,文献[21]中广播值的获取基于 OMNET 仿真工具,引用其值。为方便比较,同文献[21]中实验参数,基于 OMNET 仿真工具设计试验如下:传感器节点均匀分布,网络覆盖区域在  $4R \times 4R$  和

- [5] KAMAT P, XU W, TRAPPE W, *et al.* Temporal privacy in wireless sensor networks [C]// Proceedings of the 27th International Conference on Distributed Computing Systems (ICDCS'07). Washington, DC: IEEE Computer Society, 2007: 22–23.
- [6] PERRIG A, STANKOVIC J, WAGNER D. Security in wireless sensor networks [J]. *Communications of the ACM*, 2004, 47(6): 53–57.
- [7] YE FAN, LUO HAIYUN, LU SONGWU, *et al.* Statistical en-route filtering of injected false data in sensor networks [J]. *IEEE Journal on Selected Areas in Communication*, 2005, 24(4): 732–744.
- [8] KRISHNAMACHARI B, ESTRIN D, WICKER S. The impact of data aggregation in wireless sensor networks [C]// DEBS'02. Washington, DC: IEEE Computer Society, 2002: 575–578.
- [9] ZHANG WENSHENG, CAO GUOHONG. Group rekeying for filtering false data in sensor networks: A predistribution and local collaboration-based approach [C]// IEEE INFOCOM'05. Miami, FL, USA: IEEE, 2005: 503–514.
- [10] 曾玮妮, 林亚平, 胡玉鹏, 等. 传感器网络中一种基于分布式更新权限的组密钥管理方案 [J]. *计算机研究与发展*, 2007, 44(4): 606–614.
- [11] ARAZI O, QI H. Self-certified group key generation for ad hoc clusters in wireless sensor networks [C]// 14th International Conference on Computer Communications and Networks. San Diego, CA, USA: IEEE, 2005: 359–364.
- [12] CHADHA A, LIU Y H, DAS S K. Group key distribution via local collaboration in wireless sensor networks [C]// SECON 2005: 2005 Second Annual IEEE Communications Society Conference on Sensor and Ad Hoc Communications and Networks. Santa Clara, CA, USA: IEEE, 2005: 46–54.
- [13] LI H, CHEN K F, ZHENG Y F, *et al.* A locally group key management with revocation and self-healing capability for sensor networks [C]// ICSNC 2006: 2nd International Conference on Systems and Networks Communications. Washington, DC: IEEE Computer Society, 2006: 29–29.
- [14] HUANG J H, BUCKINGHAM J, HAN R. A level key infrastructure for secure and efficient group communication in wireless sensor networks [C]// 1st International Conference on Security and Privacy for Emerging Areas in Communications Networks. Washington, DC: IEEE Computer Society, 2005: 249–260.
- [15] JIANG Y X, LIN C, SHI M H, *et al.* Self-healing group key distribution with time-limited node revocation for wireless sensor networks [J]. *Ad Hoc Networks*, 2007, 5(1): 14–23.
- [16] SEEMA B, COYLE E J. An energy efficient hierarchical clustering algorithm for wireless sensor networks [C]// Proceedings of IEEE INFOCOM 2003. San Francisco, CA, USA: IEEE, 2003: 1713–1723.
- [17] McCUNE J M, SHI E, PERRIG A, *et al.* Detection of denial-of-message attacks on sensor network broadcasts [C]// IEEE Symposium on Security and Privacy. Washington, DC: IEEE Computer Society, 2005: 64–78.
- [18] WANG G, ZHANG W, CAO G, *et al.* On supporting distributed collaboration in sensor networks [C]// IEEE Military Communications Conference. Boston: IEEE, 2003: 752–757.
- [19] MAHESHWARI R, GAP J, DAS S R. Detecting wormhole attacks in wireless networks using connectivity information [C]// IEEE INFOCOM'07. Anchorage Alaska, USA: IEEE, 2007: 2391–2395.
- [20] DU W L, DENG J, HAN Y S, *et al.* A key management scheme for wireless sensor networks using deployment knowledge [C]// IEEE INFOCOM 2004. Piscataway: IEEE Press, 2004: 586–597.
- [21] DURRESI A, PARUCHURI V K, IYENGAR S S, *et al.* Optimized broadcast protocol for sensor networks [J]. *IEEE Transactions on Computers*, 2005, 54(8): 1013–1024.
- [22] XU Y, HEIDEMANN J, ESTRIN D. Geography-informed energy conservation for Ad-Hoc routing [C]// The Seventh Annual ACM/IEEE International Conference on Mobile Computing and Networking. New York: ACM, 2001: 70–84.

(上接第 632 页)

- [44] SARDAR B, SAHA D. A survey of TCP enhancements for last-hop wireless networks [J]. *IEEE Communications Surveys & Tutorials*, 2006, 8(3): 20–34.
- [45] FU C, LU W, LEE B. TCP veno revisited [C]// IEEE Global Telecommunications Conference, 2003. San Francisco, California: IEEE, 2003, 6: 3237–3241.
- [46] WU E, CHEN M. JTCP-based TCP for heterogeneous wireless networks [J]. *IEEE Journal on Selected Areas in Communications*, 2004, 22(4): 757–766.
- [47] KOPPARTY S, KRISHNAMURTHY S, FALOUTOUS M, *et al.* Split TCP for mobile Ad Hoc networks [C]// IEEE Global Telecommunications Conference 2002. [S.l.]: IEEE, 2002, 1: 138–142.
- [48] XIE FEI, JIANG NING, YAO HUA, *et al.* Semi-split TCP: Maintaining end-to-end semantics for split TCP [C]// 32nd IEEE Conference on Local Computer Networks 2007 (LCN 2007). Washington, DC: IEEE Computer Society, 2007: 303–314.
- [49] ALTMAN E, JIMENEZ T. Novel delayed ACK techniques for improving TCP performance in multihop wireless networks [C]// Proceedings 2003 IEEE of Personal Wireless Communications, LNCS 2775. Berlin: Springer, 2003: 237–253.
- [50] KYU-HAN K, SHIN K G. PRISM: Improving the performance of inverse-multiplexed TCP in wireless networks [J]. *IEEE Transactions on Mobile Computing*, 2007, 6(12): 1297–1312.
- [51] GOZUPEK D, PAPAVALASSILOU S, ANSARI N, *et al.* A power efficient QoS provisioning architecture for wireless Ad Hoc networks [C]// IEEE International Conference on Communications 2006. [S.l.]: IEEE, 2006, 8: 3873–3877.
- [52] ZHANG QIAN, CHEN QING, YANG FAN, *et al.* Cooperative and opportunistic transmission for wireless Ad Hoc networks [J]. *IEEE Network*, 2007, 21(1): 14–20.
- [53] MORGAN Y L, KUNZ T. A proposal for an Ad-Hoc network QoS gateway [C]// IEEE International Conference on Wireless and Mobile Computing, Networking and Communications, 2005. [S.l.]: IEEE, 2005, 3: 221–228.
- [54] MORGAN Y L, KUNZ T. A design framework for wireless MANET QoS gateway [C]// SNPD/SAWN 2005. Washington, DC: IEEE Computer Society, 2005: 420–427.
- [55] DOMINGO M C, ROMONDO D. A cooperation model and routing protocol for QoS support in Ad Hoc networks connected to fixed IP networks [C]// Proceedings of the Advanced Industrial Conference on Telecommunications/Service Assurance with Partial and Intermittent Resourced Conference/ E-Learning on Telecommunications Workshop. Washington, DC: IEEE Computer Society, 2005: 390–395.
- [56] KIM D, BAE H, TOH C K. Improving TCP-Vegas performance over MANET routing protocols [J]. *IEEE Transactions on Vehicular Technology*, 2007, 56(1): 372–377.