doi:10.3969/j.issn.1000-436x.2013.12.008

传感器网络中基于三元多项式的密钥管理方案

关志涛[1]，徐月[1]，伍军[2]
（1. 华北电力大学 控制与计算机工程学院，北京 112206；2. 早稻田大学 国际信息通信研究院，日本 东京 169-0051）

摘 要：提出一种新的密钥管理方案 KMTP(key management based on ternary polynomial)。基站为每个节点建立唯一性标识，保证节点合法性；基于三元多项式设计簇内和簇间密钥预分配算法，可以保证秘密多项式的破解门限值分别大于簇内节点和分簇总数，理论上难以破解；通过构造安全连通邻接表，设计簇间多跳路由选择算法，保证通信阶段的安全；引入更新参数和更新认证数，保证密钥更新阶段的安全。仿真表明，相比已有方案，KMTP 开销较小，且能够提供更高的安全性。

关键词：无线传感器网络；密钥管理；分簇；三元多项式；更新认证数
中图分类号：TP393.08 **文献标识码**：A **文章编号**：1000-436X(2013)12-0071-08

Ternary polynomial based key management scheme for wireless sensor network

GUAN Zhi-tao[1], XU Yue[1], WU Jun[2]
(1. School of Control and Computer Engineering, North China Electric Power University, Beijing 112206, China;
2. Global Information and Telecommunication Institute, Waseda University, Tokyo 169-0051, Japan)

Abstract: A ternary polynomial based key management (KMTP) scheme was proposed, which is effective in cluster based wireless sensor networks. Firstly, the base station will give each node one unique identifier to ensure the validity of the node. Then, algorithm of the inner-cluster and inter-cluster key pre-distribution based on the ternary polynomial of the same order was stated, which can ensure the value of the cracking threshold is bigger than the number of nodes of a cluster and all clusters separately, which means it's very hard to be cracked even all nodes of a cluster or all clusters are compromised. To assure the communication security, inter-cluster multi-hop routing mechanism was designed based on constructing secure conjunct neighbor table. Finally, the updating parameter and the updating authentication number were introduced in rekeying phase. The analysis shows that the proposed scheme can meet the security requirement of key management, and it also has less computation cost and storage cost than the existing schemes.

Key words: wireless sensor network; key management; cluster; ternary polynomial; distance parameter

1 引言

无线传感器网络（WSN, wireless sensor network）被广泛应用于军事、环境监测、医疗健康、城市交通等诸多领域[1]。无线传感器网络作为任务型网络，不仅需要进行数据采集和融合，还要进行数据传输，如何保证数据机密性和传输的安全性，就显得尤为重要。针对这个问题，行之有效的方法就是确定一套合适的密钥管理方案。传统的密钥解决方案，因为通信、存储开销大，管理复杂，而难以在计算能力非常有限的传感器网络上实现。因此很多学者致力于提出适用于传感器网络的密钥管理方案。

预共享密钥模型是较早出现的密钥管理方案[2]，并被成功应用于 SPINS 安全框架协议中。该模型在每对节点间都预共享一个主密钥，用于生成节点间通信密钥。同时，每个节点与基站之间预共享一对主密钥，用以保证节点与基站间的安全通信。该方

收稿日期：2013-07-23；**修回日期**：2013-10-21
基金项目：国家自然科学基金资助项目（61001197）；中央高校基金资助项目（JB2012087）
Foundation Items: The National Natural Science Foundation of China (61001197); Central Government University Foundation (JB2012087)

案计算复杂度低，对节点存储空间占用少，安全引导成功率高。但在多跳网络中，其对 DoS 攻击几乎没有防御能力。为此，Eschenauer 提出随机密钥预分布模型[3]，之后有学者对基本随机密钥预分布模型进行了改进[4~6]，还有学者提出定位信息与密钥分配相结合的方法[7]。

上述方法都是静态的密钥管理方法，难以将妥协或受损节点及时排出网络，而保证传感器网络的每个节点都物理安全是非常困难的[8]。因此，Eltoweissy 在 EBS(exclusion basis systems)[9]和传感器网络分簇结构基础上提出了动态密钥管理的概念[10]，其可以动态且高效地取消任意节点所拥有的全部密钥，从而可以驱逐被敌人捕获的节点[11,12]，提高了网络的安全性能。之后，陆续有学者针对基于 EBS 的动态密钥管理方案进行改进，进一步提升安全性和网络性能[13~17]。然而，基于 EBS 的无线传感器网络动态密钥系统中，存在恶意节点共谋问题，这也是一个棘手的安全难题[17]。还有学者提出基于门限秘密共享的安全密钥管理方案，比如 Zhang 等人提出的 B-PCGR 与增强的 C-PCGR 和 RV-PCGR[18]。文献[19]将混淆技术和秘密共享技术结合，提出了一种基于随机混淆的组密钥管理机制，能突破上面所涉及的门限值问题，但是此机制的开销稍大，且很大程度上依赖于基站保证其安全性，在基站信号弱的外围簇，可能由于信号差而出现安全威胁。

本文提出了一种新的密钥管理方案 KMTP，试图在大幅降低系统开销的前提下，最大化地提升安全性。分析及仿真表明，KMTP 有较好的抗捕获能力、安全性以及较小的系统开销，适用于无线传感器网络。

2 系统模型与假设

2.1 网络模型假设

如图 1 所示，采用分簇结构来进行设计，该结构可扩展性较好，适用于大型组网；再者，采用分簇结构，也易于将侵害范围控制在簇内，提高网络的安全性。

按照在本密钥管理方案中所担功能的不同，节点分为以下四类。

1) 普通节点 ON (ordinary node)：负责最基本的工作，并把收集的数据进行初步处理，发送给本簇簇头节点。

2) 簇头节点 CN(cluster head node)：为所在簇的中心节点，负责簇内外通信；采集簇内节点信息，提交给基站注册。

3) 基站 BS(base station)：为整个网络的密钥分配中心。根据簇头所采集的节点信息，为节点提供注册服务；基站有检测出被攻破或被俘获节点的能力。

4) 密钥管理节点 KMN (key management node)：每个簇内均设有一个 KMN，用于簇内密钥的预分配和更新。

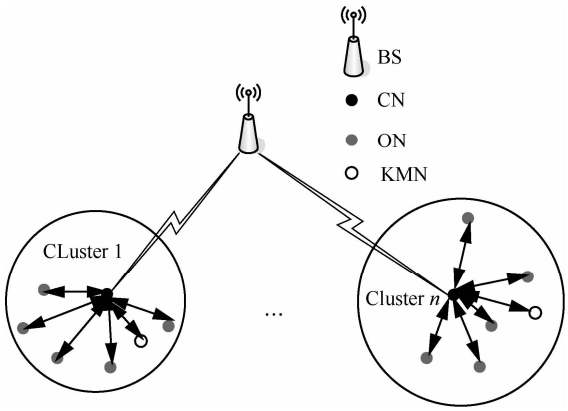

图 1 传感器网络分簇

模型假设：

1) 所有节点固定并且能量有限，基站位置固定，能量不受限；

2) 所有节点具有相似的能力(处理/通信)，并且地位平等；

3) 采用数据融合技术减少传输的数据量；

4) 每个节点周期执行数据采集任务，并始终有数据传送至基站。

2.2 攻击模型假设

传感器节点分布在环境恶劣的地带或敌对区域，容易受到外界攻击，因此提出以下攻击模型假设。

1) 攻击者可窃听网络通信，也可俘获节点。

2) 若节点被俘获，则其上的所有信息，包括密钥信息均被俘获。

3) 普通节点 ON 和簇头节点 CN 均可被俘获。

4) 若有节点被俘获且被识别，则马上进行簇内或簇间密钥更新，且此更新在有新的节点被俘获之前完成。

5) 在节点初始化阶段，节点不会被俘获。

6) 基站始终安全，即基站不会被俘获。

3　KMTP

节点间的通信安全性主要由通信密钥来保证，而通信密钥的安全性主要取决于通信密钥函数。因此，即使某个节点间通信密钥被攻击者获取，只要攻击者未捕获到预分配的多项式，其他节点间通信密钥就不会被破解。

3.1　节点初始化阶段

定义 1　基簇距离 DBSC (distance between base station and cluster)：即基站与某个簇间的距离，记为 $DBSC_i$，其值为基站与簇头节点 CN_i 间的距离。

基站维护一张节点信息表，表中存储各节点的相关信息。在初始化阶段，基站给每个节点分配一个唯一 ID、一个与基站进行身份确认的初始密钥 K_{init}、一个单向散列函数 $H(\cdot)$、一个用于生成簇间初始密钥的单向生成函数 $F(x)$、初始更新参数 $z^{(0)}$、初始更新认证数 A^k 以及 $DBSC_i$(初值为 0)。节点信息表形式如表 1 所示。

表 1　节点信息

序列号	ID 节点	K_{init}	DBSC	$Flag_{CN}$	Reg_Info
1	ID_1	K_1	0	N	NULL
2	ID_2	K_2	0	N	NULL
…	…	…	…	…	…
i	ID_i	K_i	0	N	NULL
…	…	…	…	…	…

3.2　分簇阶段

设定网络被分成若干个局部，每一局部可通过有效方式（如飞行器投放）实现节点的部署，并且节点的分布情况符合高斯分布[20]，即其分布密度函数为 $f(x)=\frac{1}{\sqrt{2\pi}\sigma}\mathrm{e}^{-\frac{(x-\mu)^2}{2\sigma^2}}$，这样的局部为一个簇。CN 和 KMN 的选取采用周期重选的方式以保持能量均衡。

在此阶段，基站向整个网络广播一个“Hello”消息，CN 根据接收到的广播信号强度来计算 DBSC，并将其发送给基站，以更新节点信息表。

3.3　节点注册阶段

定义 2　更新认证数：满足 $A_i^{p-1}=H(A_i^p)$的 A_i^p 称为 CN_i 所在簇的更新认证数。

节点注册阶段用到的符号较多，故将用到的符号统一归纳，如表 2 所示。

表 2　符号定义

符号	含义
T	时间戳
CN_i	第 i 个簇的簇头节点
ON_{ij}	第 i 个簇内的第 j 个普通节点
$\{ON_{ij}\}$	普通节点集合
$\{K\}$	普通节点的初始化密钥集合
$K_{init\_CN_i}$	CN_i 的初始密钥
$K_{init\_ON_{ij}}$	ON_{ij} 的初始密钥
App_{reg}	申请注册信息
$Reg_{ON_{ij}}$	ON_{ij} 的注册信息
Reg_{CN_i}	CN_i 发送的注册信息
Mes	通知注册的消息
A_i^k	CN_i 的初始更新认证数

CN_i 所在簇向基站 BS 注册流程如图 2 所示。

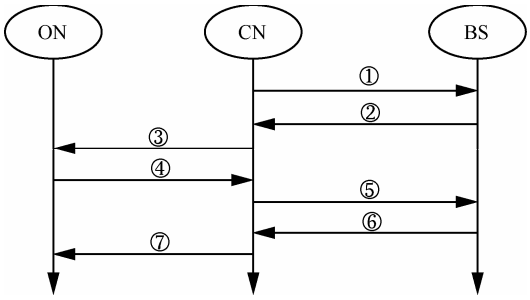

图 2　节点注册流程

① $CN_i \rightarrow BS$:{T, CN_i, {ON_{ij}}, App_{reg}} $K_{init\_CN_i}$

② $BS \rightarrow CN_i$:{T, {ON_{ij}},CN_i , {K}} $K_{init\_CN_i}$

③ $CN_i \rightarrow ON_{ij}$:{T, Mes} $K_{init\_ON_{ij}}$

④ $ON_{ij} \rightarrow CN_i$:{T, $Reg_{ON_{ij}}$} $K_{init\_ON_{ij}}$

⑤ $CN_i \rightarrow BS$: {T, Reg_{CN_i} } $K_{init\_CN_i}$

⑥ $BS \rightarrow CN_i$:{T, Ack} $K_{init\_CN_i}$

⑦ $CN_i \rightarrow ON_{ij}$:{T, Ack, A_i^k } $K_{init\_ON_{ij}}$

CN_i 向基站 BS 申请注册，基站回复其簇内普通节点的初始密钥集合，CN_i 将其记录在自己的存储空间内；ON_{ij} 将自己的注册信息发往 CN_i，CN_i 解密得到其注册信息，将所得注册信息连同自己的注册信息发往基站。此处特别注意，簇头的注册信息中必须包含身份信息 $Flag_{CN}$ =1，即标注自己为簇头节点。基站解密得到所有注册信息，从而完成注册。注册结束后，CN_i 将所存的初始密钥集合全部删除。需要说明的是，KMN 与 ON 的注册过程相同。

3.4 密钥预分配阶段

本方案采用三元多项式作为通信密钥函数，如表 3 所示。

表 3 符号定义

符号	含义
App_{key}	申请通信密钥函数信息
$K_{init\_KMN_i}$	密钥管理节点的初始密钥
f_{ij}	第 i 个簇的第 j 个更新周期的密钥函数

节点获取通信密钥函数的步骤如下。

1) $CN_i \rightarrow BS$:{T, App_{key}} $K_{init\_CN_i}$

2) $BS \rightarrow CN_i$:{T, {f_1,f_2,⋯,f_n} $K_{init\_KMN_i}$} $K_{init\_CN_i}$

3) $CN_i \rightarrow KMN_i$:{T, {f_1,f_2,⋯,f_n} $K_{init\_KMN_i}$ }

4) $CN_i \rightarrow \{ON_{ij}\}$:{$T$, $K_{init\_KMN_i}$} $K_{init\_ON_{ij}}$

5) $KMN_i \rightarrow \{ON_{ij}\}$:{$T$, f_{ij} } $K_{init\_KMN_i}$

6) $ON_{ij} \rightarrow KMN_i$: {$T$, Ack} $K_{init\_KMN_i}$

KMN_i 给所有节点分配密钥多项式，但对分配情况不做记录，以保证即使 KMN_i 被俘获，攻击者也不能获取密钥分配情况。

3.4.1 簇内密钥预分配

定义 3 密钥更新参数：$z^{(p)}=H(z^{(p-1)})$为密钥更新参数，其中 p 为更新次数，$H(\cdot)$为单向散列函数。密钥参数初始值 $z_{ij}^{(0)} = g(z_{CN_i}^{(0)}, z_{ON_{ij}}^{(0)})$，其中 $g(x,y)$为某一对称函数，比如自增或者异或操作。

定义 4 簇内通信密钥函数：ON 与 CN 的通信密钥由簇内通信密钥函数产生，此函数为定义在有限域 $F(2^L)$上的三元多项式，形式如下

$$f(x,y,z)=\sum_{i,j,k=0}^{t} a_{ijk} x^i y^j z^k \tag{1}$$

满足

$$f(x,y,z)=f(y,x,z)$$

其中，$0 \leqslant i,j,k \leqslant t$，$t$=max($N_1$,$N_2$,⋯,$N_m$)，$N_1$,$N_2$,⋯,$N_m$ 为各个簇中的节点个数，x,y 为通信双方的 ID，z 为密钥更新参数。

簇内通信密钥生成过程如下，以 ON_{ij} 和 CN_i 为例，如下所示。

1) ON_{ij} 向 CN_i 发送一条加密消息，协商生成双方通信密钥。

$$M=\{T, ID_{ON_{ij}}, ID_{CN_i}, z_{ON_{ij}}^{(0)}, rand, r\} K_{init\_ON_{ij}}$$

其中，$rand$ 为随机产生的 L 位数字，r 为 $H(rand)$。

2) CN_i 收到消息后，解密得到($rand$', r')，验证 $H(rand$')是否等于 r'，若不等，则视此消息为无效，予以丢弃；否则，CN_i 将 ID_{CNi},ID_{ONij},和 $z_{ij}^{(0)}$，代入通信密钥函数，计算出 CN_i 与 ON_{ij} 的通信密钥 $Ka_{ij}=f(ID_{CNi},ID_{ONij},z_{ij}^{(0)})$。之后给 ON_{ij} 发送一条用初始密钥加密的确认消息

$$\{T, ID_{CN_i}, ID_{ON_{ij}}, z_{CN_i}^{(0)}, rand, r\} K_{init\_ON_{ij}}$$

3) ON_{ij} 收到回复消息，解密验证（验证过程同上）后得到 $z_{CN_i}^{(0)}$,同上计算得到 ON_{ij} 与 CN_i 的通信密钥 Ka_{ij}。

3.4.2 簇间密钥预分配

定义 5 簇间通信密钥函数：用于生成簇头之间通信密钥，此函数为定义在有限域 $F(2^L)$上的三元多项式，形式如下

$$f(x,y,z)=\sum_{p,q,r=0}^{m} b_{pqr} x^p y^q z^r \tag{2}$$

其中，m 为簇的数量。此函数由基站统一分配给各簇头节点。

在密钥预分配前，基站向所有的簇头节点发送用于生成簇间初始密钥 K_{init_clu} 的参数 M_{nei}，各簇头节点将 M_{nei} 代入 $F(x)$，得到 $K_{init\_clu}=F(M_{nei})$。各簇头基于 K_{init_clu} 进行簇间密钥预分配，算法过程为：CN_i 将自己的 ID 和 $z_{CN_i}^{(0)}$ 附带着验证信息，发送给 CN_j，要求建立通信，CN_j 接收这个信息，首先验证是否合法，若不合法，则直接予以丢弃；否则将自己的 ID 和 $z_{CN_j}^{(0)}$ 回复给 CN_i，并计算得到通信密钥，CN_i 接收到回复信息后同样操作，得到通信密钥。

3.5 通信建立阶段

KMTP 采用簇内单跳和簇间多跳数据传输方式，因此涉及到两类通信，一类是 ON 和 CN 之间的通信，另一类是 CN 之间的通信。

3.5.1 簇内单跳通信

设定 ON 之间不可直接通信，ON 需直接与 CN 通信。ON 所收集的信息经簇内通信密钥加密发送给 CN，CN 解密获得信息后，做进一步处理。

3.5.2 簇间多跳通信

对一个簇头节点而言，它并不需要与所有邻居节点建立通信密钥，只需与它和基站信息传输路径上的节点建立通信密钥，这样可大幅减少整个网络的通信密钥建立开销。由此引入簇间多跳路由算法。

定义 6 簇间多跳路由：若簇头节点 u 是簇头节点 v 所有邻居中能够通信并且距离基站最近的节点，则 u 就在 v 到基站的簇间多跳路由路径上。

采用分布式策略建立簇间多跳路由，目标是找到一条能耗最优路径，以减小簇间数据传输量，降低能耗。簇间多跳路由算法的是邻接表，表中为邻居节点的关键信息，包括节点 ID、DBSC 值和剩余能量值等，表项按 DBSC 升序、能量降序的方式排列。邻接表的建立过程如图 3 所示。

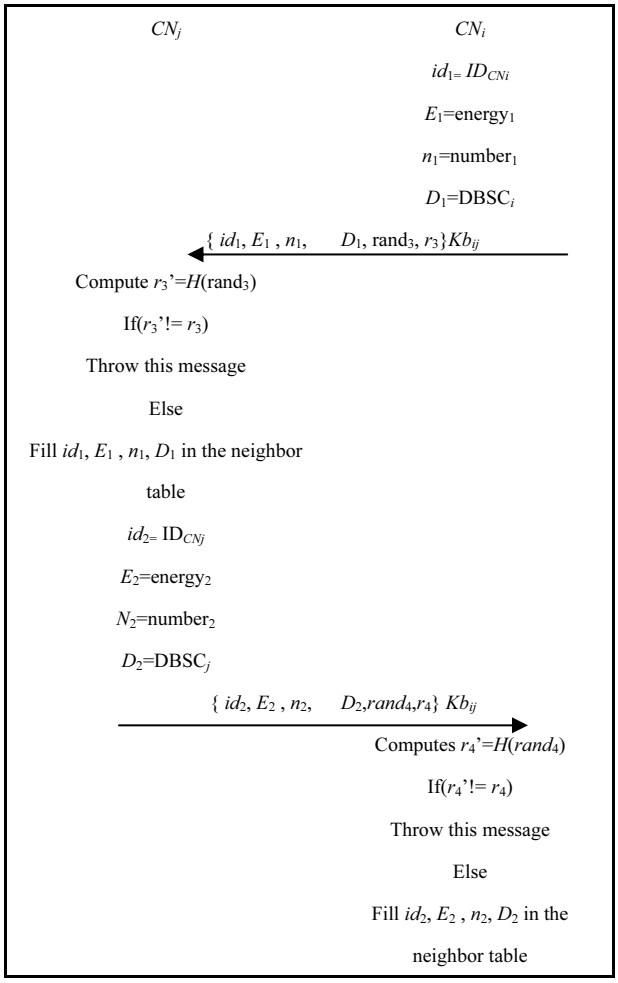

图 3　邻接表建立算法

簇头依据邻接表进行路由选择，下一跳首选表中靠前的节点，若该节点能量不足或通信繁忙，再依次选择表中后续节点，最后直接传送给基站。

3.6　密钥更新阶段

密钥更新包括 2 种模式：一是周期性更新，设定更新周期 T，定时进行密钥更新；二是触发性更新，当发生触发性事件时，需立即进行密钥更新。默认情况下，设定为周期性更新。

3.6.1　周期性密钥更新

簇内周期性密钥更新过程如下。

1) CN_i 向簇内广播一条通信密钥更新消息，此消息用簇内通信密钥加密发送，格式如下：

ID_{CN_i}	$Update_p$	A_i^p

ID_{CNi} 表示 CN_i 的 ID，$Update_p$ 表示第 p 轮更新，A_i^p 为更新认证数。

2)KMN_i 接收到密钥更新消息后，解密得到消息内容，验证 $H(A_i^p)$的值是否与本地所存的 A_i^{p-1} 相等，若不等，则抛弃该消息；若相等，则更新 CN_i 的更新认证数为 A_i^p，并给 CN_i 加密回复一条更新响应消息，格式如下：

ID_{KMN_i}	R_p	A_i^p

R_p 表示对 CN_i 发起的更新进行响应。KMN_i 向簇内广播新一轮的通信密钥函数 $f'(x,y,z)$。

之后按照密钥预分配阶段的方式，簇内节点与簇头建立新一轮的通信密钥。

进行簇间通信密钥更新时，即让基站发挥类似于 KMN 的作用，其更新过程与簇内通信密钥更新过程类似，此处不再赘述。

3.6.2　触发性密钥更新

进行簇内触发性密钥更新的前提是有触发性事件发生，包括 2 种情况：一是簇内节点发生变化，如有新节点加入或簇头节点更替等事件；二是出现安全威胁，如检测到某节点被俘获或通信被监听，为了保证网络的安全，此时需立即进行密钥更新。

触发簇间通信密钥更新的事件一般为：1)某簇产生新的簇头节点；2)簇头节点被俘获。情况 1)由新产生的簇头节点向基站发送更新请求；情况 2)则由被俘获簇头节点的邻居向基站发送更新请求。基站收到请求信息后，首先验证其有效性，若为有效请求，则由基站向全网发起簇间通信密钥更新。

触发性密钥更新过程与周期性密钥更新相同，此处不做赘述。

3.7　新节点加入

新节点加入分为 2 种情况，一种是替换被撤销或失效的节点，另一种是为了扩充簇的范围。首先分配第一种新节点，使得簇范围能够保持原有稳定水平，然后将第二种新节点向簇平均分配。

为保证网络的安全性，新节点初始化之后需要按照前述步骤进行加入，具体步骤见触发性密钥更新。特殊的是，替换那些因为能量耗尽而失效节点的新节点，可以直接继承原节点的密钥和信息。

4 安全性分析

通过下面 2 个定理证明 KMTP 安全性很高，被攻破的概率很小。

定理 1 攻击者不能攻破某个簇,除非突破其安全阈值 t+1。

证明 通过前面对通信密钥函数的定义知道,此函数为满足：$f(x,y,z)= f(y,x,z)$的三元多项式函数,它具有安全阈值 t+1,攻击者必须获得超过 t+1 个节点信息，才能攻破此簇；否则无法解出通信密钥函数的任何信息。由于 t=max($N_1, N_2,\cdots, N_m$)，攻击者不可能得到同一周期同一簇内 t+1 个节点，即无法攻破此簇。

定理 2 攻击者想要破解簇间密钥函数，至少需要捕获 m+1 个簇头节点。

证明 在某一特定更新周期 $Update_k$ 内，簇头 CN_i 与其他簇头间的通信密钥可以表示为 $f(CN_i, CN_1,z_k), f(CN_i, CN_2, z_k),\cdots, f(CN_i, CN_m,z_k),$，攻击者想要攻破簇间通信密钥函数 $f(x,y,z)=\sum_{p,q,r=0}^{m} b_{pqr}x^p y^q z^r$，由拉格朗日插值法可知，其至少需要俘获 m+1 个节点，得到 $f(CN_i, y, z_k)$，再由函数的对称性可得到 $f(x,CN_i,z_k)$。但簇头节点总数为 m，因此不可能有超过 m 个簇头节点被俘，即无法得到簇间密钥函数的任何信息。

此外，还有以下安全性问题需解决：

1) 普通节点失效或被俘获；

2) 簇头节点失效或被俘获；

3) KMN 失效或被俘获。

针对问题 1)，簇头将中断与其所有通信，并从自身存储区删除其 ID 等信息，同时向基站报告此节点 ID，基站从注册表中清除此节点的注册信息。

对于问题 2),基站向全网广播此簇头节点的 ID，一切通信被禁止。簇内重新选举簇头，基站清除注册表中其注册信息，新簇头节点向基站重新注册。

对于问题 3)，由于 KMN_i 对密钥多项式的分配情况不做记录，因此 KMN 节点被捕获时，攻击者无法获得有效的密钥信息。若 KMN_i 所存储的密钥多项式个数为 w_i 个，簇个数为 m 个，则攻击者在俘获了所有 KMN 的情况下，攻占系统的概率 $p=\prod_{i=1}^{m}\frac{1}{w_i}$。

类似方案 B-PCGR 能够行之有效是有条件的：1)节点不会同 μ+1 或者更多个邻居节点同时被捕获；2)攻击者无法得到同一个组的 t+1 或者更多个通信密钥。但无线传感器网络大多部署在敌方区域，这些条件很难满足，为了解决限制 1)，提出了 C-PCGR，为了解决限制 2)，提出了 RV-PCGR。两者的安全性均较 B-PCGR 高，但相应的开销较大。

5 开销评估

密钥管理方案中只有密钥更新是不断进行的，因此本文主要就密钥更新的开销问题展开讨论。不同的三元多项式作为通信密钥函数会产生数量级完全不同的开销,因此在这里选择了一种简单的三元多项式 $f(x,y,z)=\sum_{i=j=0}^{t} a_{ijk}x^i y^j z^k$ (k 取不大于 t 的任意整数)，显然其满足 $f(x, y, z)= f(y, x, z)$，可以作为此方案的通信密钥函数。比较对象为与 KMTP 类似的密钥管理方案 B-PCGR，C-PCGR 和 RV-PCGR。为叙述方便，特用以下符号表示，L 为密钥长度，m 为簇个数，t 表示多项式次数，n 是 B-PCGR，C-PCGR 和 RV-PCGR 的可信邻居节点的个数。各方案开销情况如表 4 所示。

5.1 存储和计算开销

5.1.1 存储开销

KMN_i 存储了 w_i 个密钥函数，每个密钥函数只需存储其系数及 k 值即可,则 KMN_i 的存储开销为 $(t+2)Lw_i$，因此整个网络的 KMN 存储开销为 $(t+2)L\sum_{i=0}^{m} w_i$，其他节点由于不需要存储任何函数，其存储开销均为 $O(1)$。取 KMN 所存储多项式个数 w=300，$\mu=20$。从图 4 可明显地看出，KMTP 的存储开销明显小于其余三者。

表 4 更新阶段各密钥管理方案开销比较

开销	B-PCGR	C-PCGR	RV-PCGR	KMTP
计算开销	n 次解密操作；$F(q)$上复杂度为 $O(\mu^3)$ 的乘/除运算 ($q>2^L$)	n 次解密操作；$F(q)$上复杂度为 $O(\mu^3)$ 的乘/除运算	n 次解密操作	$F(2^L)$上复杂度为 $O(1)$的加解密操作；$O(t^2)+O(m^2)$的乘/除运算
存储开销	$(n+1)(t+1)NL$	$(2n+1)(t+1)NL$	$2(n+1)(t+1)NL$	$(t+2)L\sum_{i=0}^{m} w_i$
通信开销	nNL	$2nNL$	$2nNL$	$(t+2)L(N-m)+(m+2)Lm$

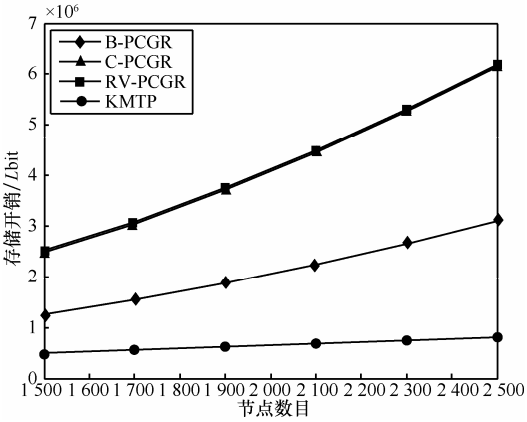

图 4　各方案的存储开销比较

5.1.2　计算开销

更新阶段，每个节点的计算开销主要包括以下几个方面。

1) 解密 KMN 发送来的通信密钥函数，开销为 $O(1)$。

2) 计算与簇头的通信密钥，需要 $O(t^2)$乘法。

3) 簇头需要与前后的通信邻居建立簇间通信密钥，其计算开销为 $O(m^2)$。

所以，KMTP 的计算开销为在有限域 $F(2^L)$上述三者之和。从表 4 可以看出，KMTP 的计算开销高于 RV-PCGR，但明显低于 B-PCGR 和 C-PCGR。

5.2　通信开销

KMTP 更新阶段的通信开销主要包括 2 个方面，一是簇内 KMN 广播簇内通信密钥函数，若用 N 表示节点总数，则此部分的通信开销为$(t+2)L(N-m)$；另一方面即为基站广播簇间通信密钥函数，通信开销为$(m+2)Lm$，两者之和即为 KMTP 更新阶段主要的通信开销。

现设计如下仿真实验：基站部署在区域角落，节点通信半径为 50 m，将网络分为 50 m×50 m 多个簇。通过飞行器部署网络节点，设各簇节点服从标准方差为 $\sigma_x=\sigma_y=10$ 的二维高斯分布。实验分两组：1) 部署区域固定为 500 m×500 m，节点数在 1 500~2 500 之间变化，因此，共有 100 个簇；2) 每个簇的大小固定为 50，部署区域在 500 m×500 m ~ 800 m×800 m 之间变化。当部署区域为 800 m×800 m 时，相应的簇数目为 256，取 $\mu=20$，KMTP 的簇内通信函数次数 $t=N/m$。

图 5 和图 6 给出了 KMTP、B-PCGR、C-PCGR 在不同实验条件下通信开销的变化情况（因 RV-PCGR 与 C-PCGR 通信开销相同，故略去 RV-PCGR 结果）。由图可以看出，KMTP 的通信开销均低于 B-PCGR 和 C-PCGR。

图 5 显示当网络的覆盖面积不变，节点个数递增时，KMTP 的通信开销也递增，这是因为多项式次数 t 随着簇内节点数目的增加而增加，在簇覆盖范围固定的情况下，节点密度越大，KMTP 的通信开销越大。相同地，B-PCGR 和 C-PCGR 受到节点密度的影响也较大，从而显示出于较 KMTP 更为明显的增长趋势。从图 6 可以发现，三者都呈现线性增长，但 KMTP 的开销均低于其余两者，这是由于当簇内节点数一定时，t 的值固定，通信开销主要受到节点总数的影响，而 B-PCGR 和 C-PCGR 当节点密度较大时其可信邻居节点数目也随之增加，从而通信开销偏高。

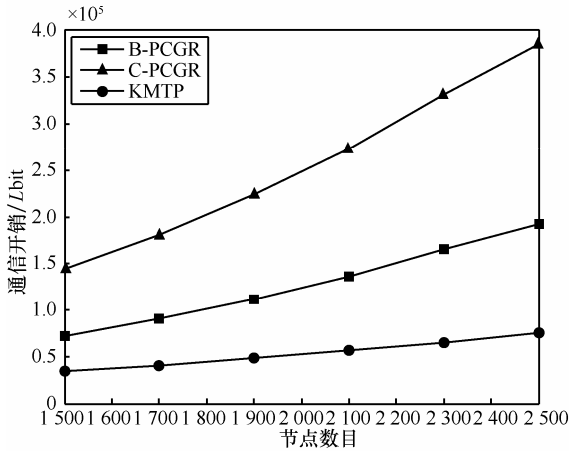

图 5　节点数目不同时各方案的通信开销比较

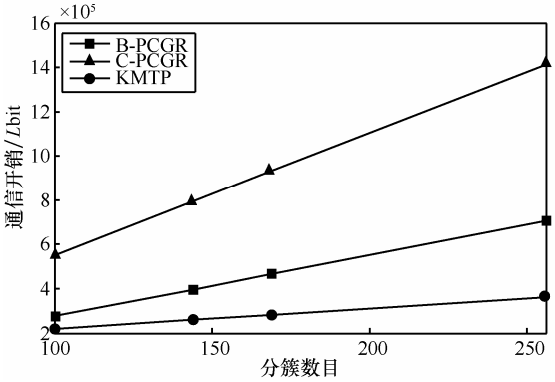

图 6　簇数目不同时各方案的通信开销比较

分析与仿真结果表明，与 B-PCGR，C-PCGR 和 RV-PCGR 相比，KMTP 可以提供更高的安全性；计算开销，通信开销与存储开销均为最小；总之，KMTP 在总体开销较小的前提下，能够提供更高的安全性，适用于无线传感器网络。

6 结束语

本文提出了一种基于三元多项式、兼具良好的安全性和可扩展性的无线传感器网络密钥管理方案，其主要特点为：1) 构造了一系列函数和算法，有效地保证密钥的保密性和节点通信的安全性；2) DBSC 的引入使得整个网络的能量消耗平衡化；3) 分析表明，该方案有很强的抗捕获性和安全性，并且与类似的方案相比开销较低，适用于分簇式无线传感器网络。

参考文献：

[1] 任丰原,黄海宁,林闯.无线传感器网络[J].软件学报,2003,14(7): 1282-1291.
REN F Y, HUANG H N, LIN C. Wireless sensor networks[J]. Journal of Software, 2003,14(7):1282-1291.

[2] PERRIG A, SZEWCZYK R, TYGAR J D, *el al*. SPINS: security protocols for sensor network[J]. Wireless Networks, 2002,8(5): 521- 534.

[3] ESCHENAUER L, GLIGOR V D. A key-management scheme for distributed sensor networks[A]. Proc of the 9th ACM Conf. on Computer and Communications Security[C]. Washington, 2002. 41-47.

[4] CHAN H W, PERRIG A, SONG D. Random key predistribution schemes for sensor networks[A]. Proc 2003 IEEE Symp on Security and Privacy[C]. 2003. 197-214.

[5] DU W L, DENG J, *et al*. A pairwise key pre-distribution scheme for wireless sensor networks[A]. Proc 19th ACM Conf on Computer and Communications Security[C]. Washington, 2003. 42-51.

[6] LIU D G, NING P. Location-based pairwise key establishments for static sensor networks[A]. Proc 1st ACM Workshop on Security of Ad Hoc and Sensor Networks[C]. Fairfax, Virginia, 2003. 72-82.

[7] MI Q, STANKOVIC J, STOLERU R. Practical and secure localization and key distribution for wireless sensor networks[J]. Ad Hoc Networks, 2012, 10: 946-961.

[8] ZHANG Y T, YANG J, LI W J, *et al.* An authentication scheme for locating compromised sensor nodes in WSN[J]. Journal of Network and Computer Applications, 2010, 33: 50-62.

[9] ELTOWEISSY M, HEYDARI H, MORALES L, *et al.* Combinatorial optimization of key management in group communications[J]. Journal of Network and Systems Management, 2004,12(1):33-50.

[10] ELTOWEISSY M, MOHARRUM M, MUKKAMALA R. Dynamic key management in sensor networks[J]. IEEE Communications Magazine, 2006, 44(4):122-130.

[11] TIAN B M, HAN S, HU J K, *et al*. A mutual-healing key distribution scheme in wireless sensor networks[J]. Journal of Networks and Computer Applications, 2011, 34: 80-88.

[12] 李林春, 李建华, 潘军. 无线传感器网络中具有撤销功能的自愈组密钥管理方案[J]. 通信学报, 2009, 30(12):12-17.
LI L C, LI J H, PAN J. Self-healing group key management scheme with revocation capability for wireless sensor networks[J]. Journal on Communications, 2009, 30(12):12-17.

[13] RAAZI S M K, LEE H, LEE S, *et al*. MUQAMI+: a scalable and locally distributed key management scheme for clustered sensor networks[J]. Annals of Telecommunications, 2010, 65(1/2):101-116.

[14] LO C, HUANG C, CHEN S. An efficient and scalable EBS-based batch rekeying scheme for secure group communications[A]. Proc of IEEE Military Communications Conference[C]. Taiwan, China 2009. 1-7.

[15] YOUNIS M F, GHUMMAN K, ELTOWEISSY M. Location-Aware combinatorial key management scheme for clustered sensor networks[J]. IEEE Trans on Parallel and Distributed Systems, 2006, 17(8):865-882.

[16] 孔繁瑞, 李春文. 无线传感器网络动态密钥管理方法[J].软件学报,2010,21(7):1679-1691.
KONG F R, LI C W. Dynamic key management scheme for wireless sensor network[J]. Journal of Software,2010,21(7):1679-1691.

[17] ELTOWEISSY M, MOHARRUM M, MUKKAMALA R. Dynamic key management in sensor networks[J]. IEEE Communications Magazine, 2006,44(4):122-130.

[18] ZHANG W S, CAO G H. Group rekeying for filtering false data in sensor networks: a predistribution and local collaboration-based approach[A]. Proc of the IEEE INFOCOM 2005[C]. Piscataway, 2005. 503-514.

[19] 曾玮妮, 林亚平, 余建平等.传感器网络中基于随机混淆的组密钥管理机制[J]. 软件学报,2013,24(4):873-886.
ZENG W N, LIN Y P, YU J P, *et al*. Group key management based on random perturbation in wireless sensor networks[J]. Journal of Software, 2013,24(4):873-886.

[20] DU W L, DENG J, HAN Y S, *et al*. A key management scheme for wireless sensor networks using deployment knowledge[A]. Proc of the IEEE INFOCOM 2004[C]. Piscataway, 2004. 586-597.

作者简介：

关志涛（1979-），男，博士，辽宁沈阳人，华北电力大学讲师，主要研究方向为信息安全、无线传感器网络安全、电力 CPS 安全。

徐月（1989-），女，山东泰安人，华北电力大学硕士生，主要研究方向为无线传感器网络安全。

伍军（1979-），男，博士，湖南湘潭人，日本早稻田大学研究员，主要研究方向为物联网信息安全。