doi:10.3969/j.issn.1000-436x.2014.03.014

基于动态累加器的异构传感网认证组密钥管理方案

钟晓睿[1]，马春光[1,2]
（1. 哈尔滨工程大学 计算机科学与技术学院，黑龙江 哈尔滨 150001；2. 哈尔滨工程大学 国家保密学院，黑龙江 哈尔滨 150001）

摘 要：利用动态累加器的证人能够证明特定累加项是否参与累加的特性，实现了组成员身份认证，提出了一种新的支持节点动态增加和撤销的组密钥管理方案 DAAG。在需要建立组密钥时，所有成员节点提供自己持有的累加项，参与累加计算。DAAG 方案在保证成员节点证人机密性的基础上，通过绑定证人与组密钥更新计算，限制了非成员节点对新密钥的计算能力。安全性和性能分析表明，DAAG 方案虽比 FM 方案消耗更多的通信代价，但能够抵抗伪造、重放和共谋等恶意攻击，提供前后向安全性。

关键词：无线传感器网络；密钥管理；组密钥；动态累加器；认证
中图分类号：TP393.0 **文献标识码**：A **文章编号**：1000-436X(2014)03-0124-11

Dynamic accumulators-based authenticated group key management scheme for heterogeneous wireless sensor network

ZHONG Xiao-rui[1], MA Chun-guang[1,2]
(1. College of Computer Science and Technology, Harbin Engineering University, Harbin 150001, China;
2. College of National Secrecy, Harbin Engineering University, Harbin 150001, China)

Abstract: Witnesses of a dynamic accumulator (DA) can ensure whether an object has been accumulated. On the basis of this, node membership in a cluster was verified and a novel authenticated group key management protocol was proposed, which supports node revocation and addition. In order to establish a group key for a cluster, each member provides their assigned number to join accumulation. DAAG can not only guarantee the confidentiality of witnesses, but also keep non-members from calculating novel group keys by binding witness with group key update. The security and performance analyses show that DAAG is resistant against replay attack, forgery attack and collusion attack, and can provide forward security and backward security.

Key words: wireless sensor network; key management; group key; dynamic accumulators; authentication

1 引言

异构传感网由大量成本低、资源受限的普通节点和一些成本相对较高，资源相对充裕的高能节点组成。这些节点以成簇的方式组成网络，相互协作，共同完成信息的收集与传递。随着异构传感网在军事和日常生活中的应用越来越广、发展越来越快，它已经受到了学术界和工业界的广泛关注。除了点对点单播通信以外，传感网还经常需要进行多播通信，而多播通信具有信道开放的特点，较单播通信更容易遭受窃听攻击、重放攻击和伪造攻击等恶意攻击。安全多播问题已经成为了制约传感网发展的关键问题之一。

异构传感网安全多播主要依靠密码学方法实现，即由组密钥为参与多播的成员提供统一的信息解读权，所有合法组成员共享一个组密钥来实现消息的加解密，以满足消息完整性、保密性等需求，实现安全通信。因此，如何安全高效地建立组密钥并恰当更新是解决传感网安全多播通信的第一步。

结合传感网特征，国内外学者已经着手研究并

收稿日期：2012-11-09；**修回日期**：2013-01-27
基金项目：国家自然科学基金资助项目(61170241)；黑龙江省自然科学基金资助项目(F201229)
Foundation Items: The National Natural Science Foundation of China (61170241); The Natural Science Foundation of Heilongjiang Province (F201229)

设计适合传感网的组密钥管理方案，并取得了阶段性成果。较早的方案主要利用经典密码算法或数据结构来控制组密钥生成。例如，2000 年 Asokan 等人[1]提出的基于口令的组密钥管理方案，无需任何可信中心便可以利用 Diffie-Hellman 算法协商组会话密钥。然而该方案没有考虑组成员关系的变化，无法支持节点的加入和撤销。基于数据结构的组密钥管理方案[2,3]则主要依赖树结构进行密钥建立和更新。这类方案过分依赖数据结构，密钥更新信息量受网络规模的影响较大。较新的研究主要集中在基于身份的组密钥管理[4~6]和自愈组密钥管理[7,8]上。前者允许将一些公开信息（E-mail、身份证等）作为公钥实现加密，避免了从公钥证书中抽取密钥而花费巨额计算开销。但传感网中大量资源受限的节点能否很好地支持大开销的公钥算法还有待考证。后者主要针对传感网信道不可靠的特点，在固定会话期内，利用广播多项式来认证成员身份，利用单向函数来计算前向密钥，达到更新和恢复密钥的目的。由于这类方案必须对每一个加入组的节点预先给定一个固定长度的会话期，并根据会话期数目加载参数，这使得方案的存储开销大，且面临全网参数需要重启的问题，对成员关系变动的支持不好，灵活性欠佳。而利用撤销多项式来验证节点成员身份的方式会随着被撤销节点数目的增多而增大构造难度和构造开销，因而不适合成员关系频繁变动的网络。

综上所述，现有方案虽然在一定程度上实现了安全多播通信，但它们或者没有考虑会话期间网络拓扑结构的动态变化，使得方案对成员关系变动带来的组密钥更新的代价十分巨大, 甚至不可行；或者考虑了动态变化，却没有实现有效的身份认证，容易遭受伪造攻击；或者实现了成员关系认证，但认证消息的长度随时间推移而增加，网络运行越久，负担越重。

为了兼顾性能、有效认证和支持成员关系动态变化，需要设计一种新的有效的组密钥管理方法，文献[9]为笔者提供了思路。但该方案存在严重的前后向不安全性，容易遭受伪造、重放等恶意攻击，因此，本文在前期工作[10, 11]的基础上，基于动态累加器提出了一种新的认证组密钥管理方案 DAAG。该方案能够利用证人信息有效验证成员身份并进行密钥发布，保证即使成员节点收到所有更新信息，也仅能在其成员身份有效的情况下才能计算更新后的组密钥，提供了良好的前后向安全性。由于所提方案完全依赖成员关系来建立密钥，而不依赖所处的会话期，因此初始密钥材料的分配可以持续使用，直到网络消亡，而无需面临在到达固定会话期后重新初始化密钥材料的问题。

2　预备知识

2.1　符号约定

为了便于描述，首先对后文涉及的符号进行约定，如表 1 所示。

表 1　　符号说明

符号	意义
Z_n^*	整数模 n 乘法群
QR_n	Z_n^* 的二次剩余群
$check(A)?B:C$	如果表达式 A 为真，则执行 B，否则执行 C
$y \leftarrow A(x)$	A 接受输入 x 输出结果 y
$y \leftarrow A(x):b(y)$	当 $y \leftarrow A(x)$ 时，布尔表达式 $b(y)$ 的值为真
$(node_i)$	节点 i 进行计算
$a \rightarrow b$	a 向 b 发送消息
$a \rightarrow *$	a 广播消息
$E_k\{M\}$	用密钥 k 加密消息 M
$D_k\{M\}$	用密钥 k 解密消息 M

2.2　动态累加器

2.2.1　累加器定义

Benaloh 和 de Mare[12]首先提出了单向累加器的概念及其构造，后经 Baric 等人[13~17]的进一步研究改进，使其在数字签名和身份认证方面获得了较好的应用。简单来说，累加器将一组输入聚合为一个长度固定的值，对于一个参与累加值计算的元素，存在一个证人能唯一证明它已经加入了该组的事实。

定义 1　累加器族是一个满足下述 4 个特性的有限函数集合 $F_k: X_k \times Y_k \rightarrow X_k$。

1) 存在性：存在以安全参数 1^k 为输入的概率多项式时间算法 G，能随机产生若干函数 $f \in F_k$ 以及相应的辅助信息 a_f，即 $(f, a_f) \leftarrow G(1^k)$。

2) 计算有效性：以 $(x, y) \in X_k \times Y_k$ 为输入，函数 f 可在多项式时间内输出结果 $v \in X_k, v = f(x, y)$。

3) 拟交换性：累加值与累加项的累加顺序无关，即：$\forall Y = \{y_1, y_2\} \subseteq Y_k$，$x \in X_k$，$f(x, Y) = f(f(x, y_1), y_2) = f(f(x, y_2), y_1)$。

4) 目击性：$\forall Y=\{y_1,\cdots,y_m\}$，$x\in X_k$，$v=f(x,Y)$，存在$(w_i,y_i)\in X_k\times Y$使得$f(w_i,y_i)=v$成立，不存在$(w_j,y_j)\in X'_k\times(Y'_k-Y)$，使得$f(w_i,y_i)=v$成立。称$w_i$为$y_i$在$v$下的证人或目击者，它证明了$y_i$是累加值$v$的累加项。

定义 2 称一个累加器是单向的，如果$X_k\subset X'_k$，$Y_k\subset Y'_k$，随机给定$(x,y)\in X_k\times Y_k$，$y'\in Y_k$对于任意的概率多项式时间算法A_k，足够大的k和所有多项式$p(k)$，事件“A_k能够在多项式时间内找到$\{Y,w,y\,|\,Y\subset Y_k,\ (w,y)\in X_k\times Y_k)\}$，使得$f(x,Y)=f(w,y)$”的概率是小于$1/p(k)$的，即

$$\Pr[f\leftarrow G(1^k);x\in X_k;(w,y,Y)\leftarrow A(f,X_k,Y_k):Y\subset Y_k;(w,y)\in X_k\times Y_k;f(w,y)=f(x,Y)]<1/p(k)$$

事实上，累加器的单向性保证了从证人计算累加值是容易的，而从累加值计算证人是困难的。

定义 3 称一个单向累加器$f:X_k\times Y_k\to X_k$是动态的，如果存在多项式时间算法D_d和W_d，使得当$x\in X_k$，$Y=\{y_1,\cdots,y_m\}\subset Y_k$，$v=f(x,Y)$时，可删除旧累加项$y_d\in Y$，删除后$v'=D_d(a_f,v,y_d)=f(x,Y-\{y_d\})$，$y_i\in Y-\{y_d\}$的新证人$w'_i=W_d(f,v,v',y_i,y_d,w_i)$，且$f(w'_i,y_i)=v'$。

2.2.2 动态累加器实例

为了解决 FM 方案[9]容易遭受伪造攻击的问题，本文在文献[17]所构造的动态累加器实例的基础上进行了改进，完整的动态累加器实例构造过程如下所示。

1) 算法G随机产生参数(p,p',q,q',n,a_f,f)，其中，p、$p'=(p-1)/2$，q、$q'=(q-1)/2$均为大素数，$n=pq$，$a_f=(x,p,q)$，$f:X_k\times Y_{A,B}\to X_k$，$X_k=\{x\in QR_n\,|\,x\neq 1\}$，$X'_k=Z_n^*$，$Y_{A,B}$是[A,B]上的大素数集，$y\in Y_{A,B}$，$y\neq p',q'$，$A$为大素数，$B<A^2$，$Y'_{A,B}$是包含了$Y_{A,B}$的$[2,A^2-1]$上的整数集族，$f(x,y)=x^y \bmod n$。显然$f$满足拟交换性，且有$f(f(x,y_1)y_2)=f(f(x,y_2)y_1)=x^{y_1y_2}\bmod n$。

2) 添加累加项：向累加项集合Y添加新累加项y_{m+1}，可更新原累加值为$v'=f(v,y_{m+1})=v^{y_{m+1}}\bmod n$，更新$y_i\in Y\cup\{y_{m+1}\}$的证人为$w'=f(w,y_{m+1})=w^{y_{m+1}}\cdot \bmod n$。

3) 删除累加项：从累加项集合Y删除累加项y_j，可更新累加值为$v'=v^{y_j^{-1}\bmod(p-1)(q-1)}\bmod n$，更新$y_i\in Y-y_j$的证人为$w'_i=w_i^{\beta}v'^{\alpha}$，其中，$\alpha$和$\beta$是由扩展 GCD 算法$eGCD(y_i,y_j)=1=\alpha y_i+\beta y_j$产生的整数。

2.3 网络假设

假设网络采用异构层次化的 3 级分簇结构。普通节点在计算能力、通信能力、存储能力和能量资源方面都能够达到目前市面上普通传感器节点的均衡水平，本文采用 Cross 公司旗下的 MICA2 尘埃节点。电量和存储空间充足的高能节点充当簇头（可以是有线固定的节点），且能够保证长期有效的在线状态，支持与其他簇头的高速通信。基站作为无线传感网与外界网络的接口，既是感知数据的目的地，又是整个网络控制信息的起源。基站设备可以是大型服务器、数据中心、笔记本电脑，甚至手持终端。所有普通节点均是全向天线的，支持单播与多播通信，有唯一的标识号，通过空中布撒或定点安装的方式被布置到监测区域中。布置完成后自动进行邻居发现和配对密钥建立。网络以簇为组，簇头为组管理员。

2.4 方案安全性需求

判定一个组密钥方案的安全性主要有前向安全性、后向安全性和抗共谋性三项指标。为了避免二义性，首先给出本文采用指标的确切定义。

1) 前向安全性[18]：一个合法成员节点离开当前组以后，无法获得它离开后更新的组密钥，其身份变为当前组的非成员节点，直到它重新加入组。

2) 后向安全性[18]：一个非成员节点加入当前组以后，无法获得它加入前的组密钥，其身份变为当前组的合法成员节点，直到它离开当前组。

3) 抗共谋攻击：多个合法成员节点相互串谋也不能破解系统。对基于动态累加器的组密钥管理方案来说，是指串谋节点无法计算其他非共谋节点证人和新密钥。

4) 抗重放攻击：仅新鲜的消息能够被节点接收。

5) 抗伪造攻击：仅合法节点能够持有并发布合法消息，包括更新信息、身份信息等。

3 FM 方案

3.1 方案回顾

为了便于描述，称文献[9]所提方案为 FM 方案。该方案采用的累加器与文献[17]相同，主要内容如下所示。

1) 密钥产生：为组$G=\{s_1,\cdots,s_m\}$产生参数

(n,p,q,x)，计算 $\varphi(n)=(p-1)(q-1)$，$n'=\varphi(n)/4$，选择素数集合 $Y=\{y_1,\cdots,y_m\}$，计算证人 $w_i=f(x, Y-\{y_i\})$。分配密钥材料 $(y_i,w_i,n,\varphi(n))$ 给节点 s_i。节点计算组密钥 $v=f(w,y_i)$。

2) 新节点加入：节点 s_{m+1} 申请入组，任意组成员随机选择一个 $y*$ 并广播 $E_v\{y*\}$。组成员更新临时新密钥 $v'=f(v,y*)$ 和临时证人 $w_i'=f(w_i,y*)$。s_{m+1} 入簇时，广播 $y**$，v' 作为 s_{m+1} 的证人，剩余节点第二次更新，得到 $v''=f(v',y**)$ 和临时证人 $w_i''=f(w_i',y**)$。

3) 旧节点删除：欲删除组内节点 s_d，所有组成员更新密钥为 $v'=f(v,y_d^{-1} \bmod n')$，根据扩展 GCD 算法计算参数 $(1,a,b)$，更新证人 $w_i'=w_i^{\beta}v'^{\alpha}$。此后，任一组成员再随机选择一个 $y*$ 广播 $E_v\{y*\}$，所有组成员再更新一遍密钥得到 $v''=f(v',y*)$ 和 $w_i''=f(w_i',y*)$。

3.2　存在的问题

虽然 FM 方案实现了组密钥的更新，却难以抵抗伪造攻击和重放攻击，前后向安全性较弱。其存在的问题可归纳如下。

1) 新加入节点易被伪造，破坏了前向安全性。假设新节点 s_{m+1} 对应的累加项为 y_{m+1}，它加入组前，组内密钥更新为 v'，它加入组后，组内密钥更新为 $v''=f(v',y_{m+1})$，而 v' 作为新节点的证人。由于 v' 是组内共享信息，这使得任何旧节点都可以伪造新节点的合法身份 (v',y_{m+1})。只要有新节点加入，旧节点 $s_i(1\leqslant i\leqslant m)$ 就能通过不断复制得到多个新身份。当 s_i 被删除时，即使它不能再用自己的身份获得新密钥，它还可以任意选用一个已被它复制的身份来继续接受网络更新消息，从而保持密钥更新，直到它所有复制来的身份都暴露且被删除为止。可见 FM 方案的前向安全性薄弱。

2) 在删除累加项时，密钥的更新脱离了证人更新，破坏了前后向安全性。假设被删除节点 s_d 对应的累加项为 y_d，其他成员节点的累加项为 $y_i(1\leqslant i\leqslant m, i\neq d)$。FM 方案将密钥材料 $(y_i,w_i,n,\varphi(n))$ 分配给节点，使得任意节点能够解得 (p,q)，并自行计算删除 y_d 以后的新累加值 $v'=f(v,y_d^{-1} \bmod n')$ 和新证人 $w_i'=w_i^{\beta}v'^{\alpha}$。对于 y_d 来说，虽然它无法计算自己的新证人，但累加值 v' 却是可以直接计算的，临时新密钥暴露 v'。虽然再次广播更新消息 $E_{v'}\{y*\}$，但 v' 已经暴露，该消息对 y_d 也不再是秘密的，因此，y_d 最终获得自己离开后的新密钥 $v''=f(v',y*)$，方案失去前向安全性。由于 FM 方案将密钥更新与证人计算相分离，如果 y_d 重新以新节点身份入组，不难发现，在入组前，它已经获得了上一次离开组以后到本次入组之前的所有同步组密钥，方案失去后向安全性。综上所述，在 FM 方案中，证人的证明作用是没有产生效力的，任何节点一旦加入组，则不论它离开还是重新加入，都可以持续获得新组密钥，方案的前后向安全性有待加强。

3) 缺乏对更新信息来源的验证，难以抵抗伪造攻击和重放攻击，容易产生恶意更新。FM 方案不对更新消息的来源进行验证，使得任意一个内部节点都可以伪造更新或重放更新。这些恶意更新的发起将可能导致正常节点被恶意删除，恶意节点被不断恢复，组内成员不能正常工作。此外，频繁的恶意更新还可能造成信息拥堵并迅速耗尽节点能量，最终导致节点死亡。

4　DAAG 方案

针对 FM 方案存在的问题，本节提出了一个新的认证组密钥管理方案 DAAG，它包括了信息初始化、消息验证、新节点加入更新和旧节点撤销更新 4 个部分。

4.1　初始化

在进行组密钥建立之前，需要为节点预加载密钥材料。假设每个组中同时在线的成员数远小于 n，$LG:Z_n\rightarrow Y_{A,B}$ 是一个将 Z_n 中的不同元素唯一映射到 $Y_{A,B}$ 中的算法。一种简单的 LG 算法实现方式如下。

1) 构造 2 个集合 UP 和 UUP，其中，UP 表示已使用的素数集合，UUP 表示尚未使用的素数集合，且满足 $UP\bigcap UUP=\varnothing\wedge UP\bigcup UUP=Y_{A,B}$。

2) 当输入一个数 $s\in Z_n$ 时，从 UUP 中随机选择一个数 y 作为算法 $LG(s)$ 的输出，同时将 y 从 UUP 中移动到 UP 集合中。称 $y=LG(s)$ 为 s 的编码，显然对 s 进行重复编码的结果并不是固定不变的。

完整的初始化过程如下。

1) 基站选定安全参数 k，运行算法 G 随机产生若干组辅助参数 $a_f=(x_0,p,q)$，并随机从中选取一组构建第 g 个组的累加器 $f(x_0,y)=x_0^y \bmod n$。为每个节点分配唯一标识 $s_i\in Z_n$ 并计算编码 $y_i=LG(s_i)$。令 s_{ch}^g 表示第 g 个簇的簇头节点标识。将密钥材料

(a_f, f, y_{ch}) 加载到 s_{ch}^g，将编码 y_i 加载到普通节点 s_i。密钥材料加载完成后将节点布撒到网络。即

$$(Base):\{a_f, f\} \leftarrow G(k), f \in F_k$$
$$Base \rightarrow s_{ch}^g :(a_f, f, y_{ch})$$
$$Base \rightarrow s_i :(y_i)$$

2) s_{ch}^g 经邻居发现收集成员编码列表 $Y=\{y_1,\cdots, y_m\}$，计算初始累加值 $v_1 = f(x,Y)$，以及累加项 y_i 的证人 $w_{i\_1} = f(x, Y-\{y_i\})$。由于 s_{ch}^q 与成员节点之间已建立配对密钥，故 s_{ch}^g 可借由配对密钥加密的安全信道为成员节点发送初始信息。即

$$(s_{ch}^g): Y=\{y_1,\cdots,y_m\}$$
$$v_1 = f(x_0, Y)$$
$$w_{i\_1} = f(x_0, Y-\{y_i\})$$
$$s_{ch}^g \rightarrow s_i : E_{ch,i}\{f, w_{i\_1}\} \| MAC\{f, w_{i\_1}\}$$

3) 成员节点 s_i 解密消息并验证其完整性，如果验证失败，则丢弃该消息；否则保留 w_{i_1} 作为初始证人，计算累加值 v_1 并将其作为第一个会话期的组密钥。即

$$(s_i) : D_{ch,i}\{f, w_{i\_1}\},$$
$$check(MAC)?v_1 = f(w_{i\_1}, y_i) : drop$$

此外，所有簇头形成一个高级组，该组的管理员是基站，该组组密钥的建立与普通组相同。普通组之间的通信可以通过对密钥加密的簇头间信息交换来实现。

4.2 消息验证

当新节点加入和旧节点撤销时，簇头需要向全组广播更新信息，以通知成员节点进行密钥更新，保证网络的前后向安全。簇头发布密钥更新消息过程必须保证：1) 成员节点能够实现对组管理员的认证，确认更新信息来源；2) 仅合法组成员才能获得正确更新信息。

假设在第 k 个会话期需要进行密钥更新，欲添加或删除节点的编码为 $y*$，第 k 和 k+1 个会话期的累加值（即组密钥）与组管理员证人分别为 v_k、w_{ch_k}、v_{k+1} 和 w_{ch_k+1}，算法 *update* 实现对累加值和证人的更新。本文采用下述策略来实现对更新消息的验证，其中，$update(w,v)$ 表示对第 k 个会话期中节点累加值与证人进行更新。

1) 验证组管理员身份。由组管理员产生随机数 c,计算 $C = f(w_{ch\_k+1}, c)$，并将 (c, C) 发送给成员节点；成员节点判定 $f(C, y_{ch})$ 与 $f(v_{k+1}, c)$ 是否相等，若相等则接收更新消息，否则丢弃。即

$$(s_{ch}^g):(w_{ch\_k+1}, v_{k+1}) \leftarrow update(w_{ch\_k}, v_k)$$
$$c \leftarrow Rand$$
$$C = f(w_{ch\_k+1}, c)$$
$$s_{ch}^g \rightarrow s_i :\{c, C\}$$
$$(s_i):(w_{i\_k+1}, v_{k+1}) \leftarrow update(w_{i\_k}, v_k)$$
$$check\{f(C, y_{ch}) == f(v_{k+1}, c)\} ? accept : drop$$

2) 限制新密钥的可计算性，使非法节点不能更新相关参数，从而无法产生新密钥。将新密钥 v_{k+1} 隐藏在更新信息中，信息接受者必须先自动更新自己的证人，才能从更新信息中恢复新密钥 v_{k+1}。

(a) 当删除旧节点时，簇头节点 s_{ch}^g 广播用于合法成员节点提取新累加值 v_{k+1} 的消息 $\{v_{k+1}r, h(x,\beta')\}$，使得仅未被删除的成员节点能够获得新证人与随机参数 r 的积 $w_{i\_k+1}r^\alpha$，并进一步从密钥隐藏式 $h(x,\beta')$ 中恢复出新累加值 v_{k+1}。即

$$(s_{ch}^g):(w_{ch\_k+1}, v_{k+1}) \leftarrow update(w_{ch\_k}, v_k)$$
$$r \leftarrow Rand, r \in Z*$$
$$e_1 = r^{y*} \bmod n,\ e_2 = r^{-1} \bmod n$$
$$h(x,\beta') = x e_1^{\beta'} e_2$$
$$s_{ch}^q \rightarrow *:\{y*, v_{k+1}r, h(x,\beta')\}$$
$$(s_i):(\alpha,\beta) \leftarrow eGCD(y_i, y*)$$
$$x_i = w_{i\_k}^\beta v_{k+1}^\alpha r^\alpha = w_{i\_k+1} r^\alpha$$
$$v_{k+1} = h(f(x_i, y_i), \beta)$$

其中，$h(f(x_i, y_i), \beta)$ 的计算过程为

$$\begin{aligned} h(f(x_i, y_i), \beta) &= f(x_i, y_i) e_1^\beta e_2 \\ &= f(w_{i\_k+1} r^\alpha, y_i) \cdot r^{\beta y*-1} \bmod n \\ &= (w_{i\_k+1})^{y_i} r^{y_i\alpha} \cdot r^{\beta y*-1} \bmod n \\ &= v_{k+1} r^{\alpha y_i} \cdot r^{\beta y*-1} \bmod n \\ &= v_{k+1} r^{\alpha y_i + \beta y*-1} \bmod n \\ &= v_{k+1} \end{aligned}$$

由于计算参数 (α,β) 是由扩展 GCD 算法产生的，即

$$eGCD(y_i, y*) = 1 = \alpha y_i + \beta y* \quad (1)$$

当 $y* = y_i$，无法找到 2 个整数 (α,β) 使得式(1)成立，故被删除节点不能计算 x_i，更无法进一步计算新密钥 v_{k+1}。

(b) 当添加新节点时，旧节点成员关系未发生变化，拥有 v_k 的节点一定是合法成员节点，故所有成员节点均可以自主生成新证人与新密钥，过程如下

$$s_{ch}^{q} \to *:\{y^*\}$$
$$(s_i): w_{i\_k+1} = f(w_{i\_k}, y^*),$$
$$v_{k+1} = f(v_k, y^*)$$

4.3 节点加入

当节点处于会话期 k 时，只要有新节点加入，则更新会话进入到第 k+1 个会话期。对新节点 s_a 来说，$LG(s_a) = y_a$，s_a 首先向 s_{ch}^{g} 发送入簇申请，获得初始化信息和第 k+1 个会话期的组密钥 v_{k+1}，并由 s_{ch}^{g} 发布更新信息 B_a，接收到的旧节点计算 v_{k+1}，并用它来验证消息是否来自簇头节点，如果是则接受 v_{k+1} 为新密钥，并计算新证人 w_{i_k+1}；否则丢弃 v_{k+1}，继续保留原密钥 v_k

$$s_a \to s_{ch}^{g}: E_{ch,a}\{new, y_a\}$$
$$(s_{ch}^{g}): c \leftarrow Rand, r \in Y_{A,B},\ y^* = y_a r$$
$$v_{k+1} = f(v_k, y_a r),\ w_{ch\_k+1} = f(w_{ch\_k}, y_a r)$$
$$C = f(w_{ch\_k+1}, c),\ \ w_{a\_k+1} = f(v_k, r)$$

$$s_{ch}^{g} \to s_a: E_{ch,a}\{f, w_{a\_k+1}\} \| MAC\{f, w_{a\_k+1}\}$$
$$s_{ch}^{g} \to *\ : B_a = \{y^*, C, c\} \| MAC\{y^*, C, c\}$$
$$(s_i): check(MAC)?(1): drop$$
$$(1): v'_{k+1} = f(v_k, y^*)$$
$$check\{f(C, y_{ch}) == f(v'_{k+1}, c)\}$$
$$?\, w_{i\_k+1} = f(w_{i\_k}, y^*), v_{k+1} = v'_{k+1}: drop$$

4.4 节点撤销

当在第 k 个会话期要删除节点 s_d 时，s_{ch}^{g} 计算随机参数构造密钥隐藏式 $g(x,y,z)$ 并发动更新，广播被删除的节点信息。各成员节点首先验证更新消息来源，若来自簇头节点，则进一步计算各自新证人 w_{i_k+1} 和证人参数 (α,β)，从密钥隐藏式中恢复第 k+1 个会话期组密钥 v_{k+1}；否则丢弃该信息，保持原有密钥和证人。详细过程如下

$$(s_{ch}^{q}): r, c \leftarrow Rand$$
$$v_{k+1} = v_k^{y_d^{-1} \bmod (p-1)(q-1)} \bmod n$$
$$(\alpha,\beta) \leftarrow A(y_{ch}, y_d)$$
$$w_{ch\_k+1} = w_{ch\_k}^{\beta} v_{k+1}^{\alpha}, C = f(w_{ch\_k+1}, c)$$
$$h(x,\beta') = x e_1^{\beta'} e_2$$

$$s_{ch}^{q} \to *\ : B_d = \{y_d, C, c, v_{k+1} r, h(x,\beta')\} \|$$
$$MAC\{y_d, C, c, v_{k+1} r, h(x,y,z)\}$$
$$(s_i)\quad : check(MAC)?(1): drop$$
$$(1): (\alpha,\beta) \leftarrow eGCD(y_i, y_d)$$
$$x_i = w_{i\_k}^{\beta}(v_{k+1} r)^{\alpha},\ v'_{k+1} = h(f(x_i, y_i), \beta)$$
$$check\{f(C, y_{ch}) == f(v'_{k+1}, c)\}$$
$$?\, w_{i\_k+1} = w_{i\_k}^{\beta} v_{k+1}^{\alpha}, v_{k+1} = v'_{k+1}: drop$$

5 安全性分析

基于改进的动态累加器，DAAG 方案保证了仅组内合法成员节点 s_i 才具有当前组密钥 v_k 下的证人 w_{i_k}，才能正确计算 v_k，从而提供了良好的安全性。

引理 1　在强RSA假设下，动态累加器 $f(x,y) = x^y \bmod n$ 是安全的，即对于攻击者 A，

$$\Pr[f \leftarrow G(1^k); x \in X_k; (w,y,Y) \leftarrow A(f, X_k, Y_k):$$
$$Y \subset Y_k; (w,y) \in X_k \times Y_k; f(w,y) = f(x,Y)] < 1/p(k)$$

证明　根据强RSA假设可知，寻找满足 $v \equiv w^y \cdot \bmod n$ 的 (w,y) 的问题是多项式时间内难解的。$\forall Y = \{y_1, \cdots, y_m\}$，$v = f(x,Y)$，如果存在攻击者 A 能够找到一对 $(w,y) \in X_k \times Y_{A,B}$，使得 $v = f(w, y) = w^y \bmod n$，其中，$n$ 是一个 rigid 数，则强 RSA 假设为假。因此在强 RSA 假设下，给定 v 和 y，要找到一个 w 使得 $v = f(w,y)$ 是困难的，动态累加器 $f(x,y) = x^y \bmod n$ 是一个安全累加器。证毕。

引理 2　在强 RSA 假设下，任意 2 个已参与累加的累加项的证人是彼此秘密的。

证明　对于累加项集合 $Y = \{y_1, \cdots, y_m\}$，累加值 $v = f(x,Y)$，$\forall y_i, y_j \in Y$，有 $v = f(w_i, y_i) = f(w_j, y_j)$。根据引理 1 可知，对于 y_i 来说，给定 (v, w_i, y_i, y_j) 要找到一个值 w'_j 使得 $f(w_i, y_i) = f(w'_j, y_j)$ 在强 RSA 假设下是困难的。同理，y_i 也难以找到满足条件的 w'_i。因此任意 2 个已累加项的证人是彼此秘密的。证毕。

引理 3　在强 RSA 假设下，任意累加项 y_i 和新累加项 y_a 的证人是彼此秘密的。

证明　令 y_a 参与累加前的累加值为 v_k，根据累加器的目击性可知，不存在 y_a 在 v_k 下的证人。由于 y_a 没有当前累加值的相关知识，组内通信又均不涉及直接传递累加值或证人信息，故未

参与累加的 y_a 无法获知其他累加项的证人及累加值信息。

参与累加后，y_a 得到证人 $w_{a\_k+1}=f(v_k,r)$，$y_i\in Y$ 更新累加值 $v_{k+1}=f(v_k,y_ar)$ 和证人 $w_{i\_k+1}=f(w_{i\_k},y_ar)$。

对于 y_i 来说，一方面，虽然 y_i 获得 $y_ar(y_a,r\in Y_{A,B})$，但根据大整数因子分解的困难性可知寻找 y_a 和 r 是困难的，y_i 无法通过计算 $f(v_k,r)$ 获得 w_{a_k+1}。另一方面，虽 y_i 能够更新 $v_{k+1}=f(v_k,y_ar)=f(w_{a\_k+1},y_a)$，但基于强 RSA 假设可知，给定 (v_k,y_ar) 寻找 (w_a,y_a) 的问题也是难解的。

对于 y_a 来说，寻找 y_i 新证人 w_{i_k+1} 的问题如引理 2 所述是难解的。同样根据强 RSA 假设可知，虽然 $v_{k+1}=f(w_{a\_k+1},y_a)=f(v_k,y_ar)=f(f(w_{i\_k},y_i),y_ar)$，给定 (w_{a_k+1},y_a,y_ar,y_i) 寻找 y_i 的旧证人 w_{i_k} 的问题仍然是难解的。综上所述，新累加项 y_a 与旧累加项 y_i 的证人是彼此秘密的。证毕。

引理 4 在强 RSA 假设下，任意累加项 y_i 和被删除累加项 y_d 的证人是彼此秘密的。

证明 令 $Y=\{y_1,\cdots,y_m\}$，$y_i,y_d\in Y$，y_d 被删除以前，$v_k=f(x,Y)=f(w_{i\_k},y_i)=f(w_{d\_k},y_d)$。根据引理 2，$w_{i\_k}$ 与 w_{d_k} 是相互秘密的。当 y_d 被删除，y_i 首先根据扩展 GCD 算法获得参数对 (α,β)，再更新得到 $v_{k+1}=g(w_{i\_k}^{\beta}v_{k+1}^{\alpha}r^{\alpha},\beta)$ 和 $w_{i\_k+1}=w_{i\_k}^{\beta}v_{k+1}^{\alpha}$。

对于 y_d 来说，一方面，p 和 q 的值是未知的，又受到随机数 r 的干扰作用，无法直接获得 v_{k+1}；另一方面扩展 GCD 算法不能找到满足 $\alpha y_d+\beta y_d=1$ 的 (α,β)，故 y_d 在 v_{k+1} 下的证人不存在，进而无法计算新累加值 v_{k+1}。因此，y_d 所持有的组密钥知识仅有 $(v_k,v_{k+1}r,w_{d\_k})$，根据强 RSA 假设，在这种情况下寻找满足 $v_k=f(w_{i\_k},y_i)$ 的 w_{i_k} 和满足 $v_{k+1}=f(w_{i\_k+1},y_i)$ 的 w_{i_k+1} 的问题均是难解的。

综上所述，被删除的累加项 y_d 与任意参与累加的累加项 y_i 的证人是相互秘密的。证毕。

定理 1 DAAG 方案能够抵抗伪造攻击。

证明 DAAG 方案能够有效地抵御下述伪造攻击。

1) 编码为 $y*$ 的非成员恶意节点谎称自己是编码为 y_a 的新节点，申请入簇，企图伪造 y_a 的身份。由于申请入簇信息由 y_a 与组管理员之间的对密钥加密，$y*$ 根本无法伪造该申请信息，组管理员也就不会产生更新响应，伪造失败。

2) 编码为 $y*$ 的成员恶意节点企图复制成员节点的身份。根据引理 2 可知，任意一个已参与累加的成员的证人对 $y*$ 都是秘密的，恶意节点缺少目标节点累加项的证人，身份伪造失败。

3) 编码为 $y*$ 的成员恶意节点企图复制新加入节点的身份。根据引理 3 可知，新累加项的证人对 $y*$ 都是秘密的，缺少目标节点累加项的证人，身份伪造失败。

4) 编码为 $y*$ 的恶意节点企图在离开时复制合法成员节点的身份。根据引理 4 可知，成员节点持有的证人对 $y*$ 都是秘密的，恶意节点缺少目标节点累加项的证人，身份伪造失败。

5) 恶意节点企图伪造更新消息，控制组密钥更新。不论是增加节点还是删除节点，组密钥更新信息都包含了用来验证更新信息来源的信息 (C,c)，由于 $C=f(w_{ch\_k+1},c)$，根据强 RSA 假设，恶意节点不能从 (C,c) 中解得组管理员的证人 w_{ch_k+1}，即 (C,c) 不能根据恶意节点的需要进行伪造。对于新节点加入更新 $B_a=\{y*,C,c\}$ 来说，恶意节点替换 $y*$ 为 $y**$，则收到消息的节点计算一个新的 v'_{k+1}，验证 $f(C,y_{ch})=f(v'_{k+1},c)$ 就会失败。同理，对于伪造的删除更新 $B_d=\{y_d,C,c,v_{k+1}r,g(x,y,z)\}$，不论修改了除 (C,c) 之外的任何一项，都将影响节点计算得到的新累加值 v'_{k+1}，导致验证失败。

综上所述，DAAG 方案成功抵抗上述 5 种场景下的伪造攻击，使得其既能保证 4 类节点（从未加入过的节点、正参与组通信的节点、加入过又离开的节点和离开后又加入的节点）均无法伪造它人身份，又能保证更新信息不被伪造。证毕。

定理 2 DAAG 方案可以抵抗重放攻击。

证明 每次更新消息中的 (C,c) 都携带了当前组的正确累加值 v_{k+1}。如果恶意节点重放更新消息，则接收到该消息的节点各自计算新的累加值 v'_{k+1}，将是 v_{k+1} 重复累加一个累加项或重复删除一个累加项的结果，即 $v'_{k+1}\neq v_{k+1}$，此时验证 $f(C,y_{ch})=f(v'_{k+1},c)$ 失败。因此，DAAG 方案能够有效抵抗重放攻击。证毕。

定理 3 DAAG 方案能够抵抗大规模共谋攻击。

证明 共谋节点相互分享各自的证人，作为

一个整体，获得当前组的更新消息。攻破系统的关键在于找到当前组所选累加器的辅助信息 $a_f=(x_0, p, q)$。只要任意共谋节点获得了 a_f，它就能避开身份认证直接计算新密钥。然而，一方面在强 RSA 假设下，不论共谋节点的数目有多少，它们都不能逆向计算 $v=f(w, y)$，恢复基底 x_0；另一方面，参数 p、q 的安全性由大整数因子分解困难性保证，共谋节点无法获得。考虑最坏的情况下，仅组管理员是非共谋节点，其他所有组成员像一个节点一样共享信息。此时，网络可以看作一个组管理员和一个恶意节点，根据引理 2，组管理员的证人仍然安全，如果新添加非共谋节点，其证人也始终安全。共谋节点一旦被完全删除，它们立刻失去对新密钥的计算能力。综上所述，非组管理员的成员节点共谋仅能实现身份共享，而不能攻破网络。DAAG 方案仅在组管理员参与共谋时才被攻破。

定理 4　DAAG 方案是前向安全的。

证明　当一个节点离开组时，它不能利用扩展 GCD 算法计算参数 (α,β)，从而无法更新证人，也就无法更新自己的组密钥。同时根据引理 4，被删除节点不能复制任何合法成员节点的身份。因此，被删除节点既不能正常更新组密钥，也不能通过伪造身份获取组密钥，方案是前向安全的。

定理 5　DAAG 方案是后向安全的。

证明　当新节点加入，它能够获得新累加值 $v_{k+1}=f(v_k,y_a r)$ 和证人 $w_{a\_k+1}=f(v_k,r)$。在强 RSA 假设下，给定 $(v_{k+1},y_a r,r)$ 寻找 v_k 的问题是难解的。因此新节点不能获得旧组密钥 v_k，DAAG 方案是后向安全的。

定理 6　DAAG 方案能够抵抗恶意更新。

证明　每次节点的加入与删除都需要进行全组密钥更新。DAAG 方案从两方面入手防止恶意更新：1) 利用配对密钥加密入簇申请信息，屏蔽了伪造节点的入簇申请；2) 利用身份认证手段对组管理员身份进行验证，防止了恶意节点伪造组管理员或重放更新信息发起恶意更新。综上所述，DAAG 方案能够抵抗恶意更新。证毕。

表 2 显示了 DAAG 方案与 FM 方案在安全性方面的对比情况。其中，“√”表示方案具有该特性，“×”表示方案不具有该特性。

表 2　安全性对比

安全性	DAAG 方案	FM 方案
前向安全性	√	×
后向安全性	√	×
抗重放攻击	√	×
抗伪造攻击	√	×
抗共谋攻击	仅当组管理员共谋时网络才被攻破	×

6　性能分析

设所有参数、密钥、多项式和 MAC 消息的平均大小为 L byte。Md 表示模运算代价，Mc 表示 MAC 运算代价，$AES\ E/D$ 为 AES-128 对称加/解密代价，N 表示组规模，S 表示每发送 1 byte 数据的代价，R 表示每接收 1 byte 数据的代价，G 表示 eGCD 算法代价。

6.1　存储开销分析

令 C_{str} 表示存储开销。节点的存储空间主要耗费在存储预分配密钥材料和变量上。在 DAAG 方案中，组管理员存储信息 (f,a_f,y_{ch},w_{ch},v)，普通成员存储的信息 (f,y_i,w_i,v)。FM 方案中所有成员节点存储相同的信息 $(f,y_i,w_i,\varphi(n),v)$。因此，在一个有 N 个成员的组中，2 种方案的节点平均存储开销分别为

$$C_{str}(DAAG)=\frac{5L+4(N-1)L}{N}=4L+L/N \quad (2)$$

$$C_{str}(FM)=5L \quad (3)$$

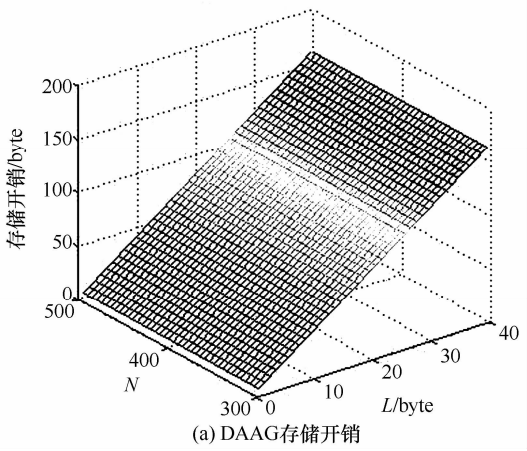
图 1 给出了 DAAG 方案与 FM 方案的存储开销对比情况。其中，L 的取值范围为 1~40 byte，组成员数目变化范围为 305~500。显然，DAAG 方案要比 FM 方案消耗更少的存储空间。当 N 极大时，DAAG 方案的存储开销将接近 $4L$，此时，DAAG 的 L 上限约为 128 KB，FM 的 L 上限约为 102 KB。

6.2　计算开销分析

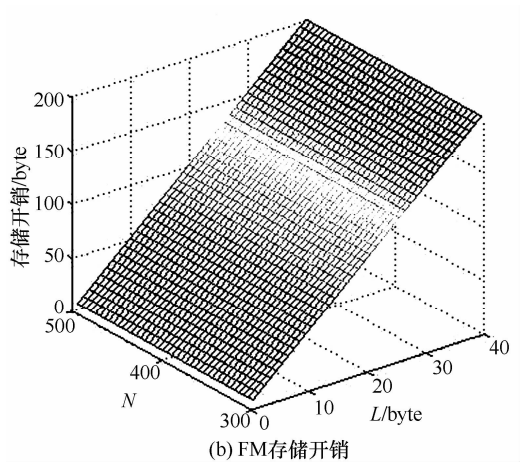
令 C_{comp} 表示计算开销。在初始化阶段，FM 方案只需要 1 次模运算来计算初始密钥，DAAG 方案还需多执行 1 次 MAC 运算。即

$$C_{\text{comp}}(DAAG)=Mc+Md \quad (4)$$

$$C_{\text{comp}}(FM)=Md \quad (5)$$



(a) DAAG存储开销



(b) FM存储开销

图 1 存储开销对比

在新节点加入时，FM 方案的每个成员节点运行 4 次模运算和 1 次解密运算。DAAG 方案需要 2 次模运算获得密钥和证人更新，2 次模运算用来验证更新信息来源，1 次 MAC 运算和 1 次解密运算。即

$$C_{\text{comp}}(DAAG)=D+Mc+4Md \tag{6}$$

$$C_{\text{comp}}(FM)=D+4Md \tag{7}$$

在删除节点时，FM 方案执行 1 次解密运算、3 次模运算，并运行 1 次 GCD 算法。DAAG 方案需要 1 次 GCD 运算、1 次 MAC 计算以及 3 次模运算。即

$$C_{\text{comp}}(DAAG)=G+Mc+3Md \tag{8}$$

$$C_{\text{comp}}(FM)=G+3Md+D \tag{9}$$

6.3 通信开销分析

令 C_{comm} 表示节点的通信开销。由于 FM 方案的初始化是离线完成的，因此不存在通信开销。在 DAAG 方案中，基站进行的材料分配也是离线的，因此只需要关注在线成组过程。对于有 M 个成员的组，组管理员需要广播 $3L$ 的信息，因此初始化阶段 DAAG 方案的平均通信开销为

$$C_{\text{comm}}(DAAG)=\frac{3LS+3LR(N-1)}{N} \tag{10}$$

$$C_{\text{comp}}(FM)=0 \tag{11}$$

在新节点加入阶段，FM 方案需要广播 2 次大小为 L 的信息，第一次的接受者有 N−1 个，第二次有 N 个。DAAG 方案需广播一次 $4L$ 的消息，接受者为 N−1 个。即

$$C_{\text{comm}}(DAAG)=\frac{4L(S+R(N-1))}{N} \tag{12}$$

$$C_{\text{comp}}(FM)=\frac{L(2S+R(N-1)+RN)}{N} \tag{13}$$

在节点删除阶段，FM 方案广播 2 次大小为 L 的信息，接受者均为 N−2 个。DAAG 方案需广播 1 次 $6L$ 的消息，接受者为 N−2 个。即

$$C_{\text{comm}}(DAAG)=\frac{6L(S+R(N-2))}{N} \tag{14}$$

$$C_{\text{comp}}(FM)=\frac{L(2S+2R(N-2))}{N} \tag{15}$$

6.4 可扩展性分析

FM 方案是将整个网络看作一个组，离线为节点初始化证人信息。这意味着网络不具有划分动态子组的能力。与之不同，DAAG 方案是在线建立组，动态收集邻居节点信息，由组管理员动态组织成组，能够支持节点移动和多级子组建立。因此，对于相同的一组，最多能够支持 M 个成员节点的密钥材料来说，FM 方案只能支持一个组共 M 个节点建立组密钥，而 DAAG 方案能够支持的节点数是 M 的指数级。

综上所述，DAAG 方案的存储开销要小于 FM 方案，计算开销则相当。初始化和新节点加入时，DAAG 的计算开销分别比 FM 方案仅多 1 次 MAC 运算。但为了保证前向安全性，DAAG 方案需要传递更多的信息来帮助合法节点恢复组密钥，因此通信开销要大于 FM 方案。

6.5 仿真分析

本节借助 OMNET++平台定量分析 DAAG 方案的寿命以评测其可行性。根据 2.3 节网络假设，本文选择 Cross 公司的 MICAz 节点（ATmega128L，2.4 GHz，传输速率 250 kbit/s，存储器 512 Kbyte）

作为普通传感器节点，以有线供电节点作为簇头节点，建立测试网络。在测试过程中，只需考虑 MICAz 节点的性能问题，数值和仿真分析涉及的参数分别来自文献[19~21]，如表 3 所示。

表 3　　仿真参数

参数	值	参数	值
S	8.528 μJ / byte	电池	1.5 V, 2 500 mAH
R	4.424 μJ / byte		
Md	13.95 mJ	MICAz 内存	512 KB
AES E/D	1.62/2.49 μJ / byte	*r*	80 m

一次 RSA 加解密运算的平均代价约为 13.95 mJ。一只普通 AA 电池的能量约为 1.5×2.5×3 600 = 13 500 J，一个普通的 MICAz 是两节 AA 电池供电的，能量能够达到 27 000 J。图 2 给出了在 OMNET++ 中对所提方案进行仿真分析的运行场景，整个网络由 3 个簇组成，并分簇持续执行所提方案，直到第一个成员节点死亡。初始组密钥只建立 1 次，之后簇头以平均 10 s、1 min 和 1 h 的时间间隔发起组密钥添加或删除事件。由于各个成员节点中组密钥的建立与更新仅发生在接收到簇头广播的更新消息之后，由节点自身完成，故每个组成员节点的数目多少不影响协议的性能分析结果。仿真过程以网络中第一个节点的死亡时间为网络寿命长短的标识，相应的仿真测试结果如表 4 所示。

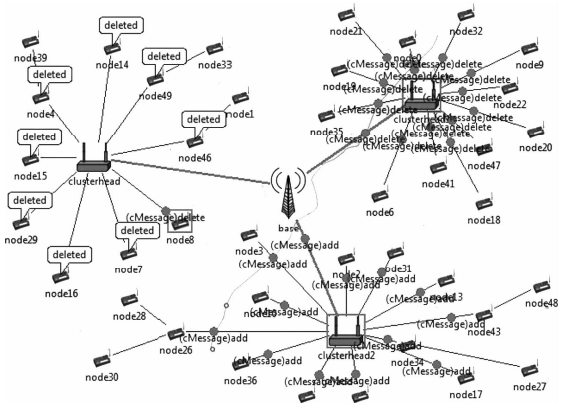


图 2　仿真场景

表 4　　仿真结果

更新间隔	网络寿命/天			
	测试 1	测试 2	测试 3	平均
10 s	15.321	14.287	15.098	14.902
1 min	96.750	96.875	97.128	96.918
10 min	968.546	968.133	968.574	968.418

从仿真结果可以发现，以平均 10 s 的时间间隔触发更新事件时，网络中最早因能量耗尽的节点拥有约 15 天的寿命。随着更新事件触发间隔的增长，网络寿命也随之延长。当以 10 min 的时间间隔触发更新时，寿命下限约为 2.5 年。与移动 ad hoc 网不同，现实中无线传感网节点的位置常是相对固定的，节点的新增与删除仅在需要补充节点和移除妥协与死亡节点的情况下发生，其平均触发时间间隔一般大于 1 min 甚至 10 min。可见，所提方案在实际的传感网安全应用中是可行的。

7　结束语

针对 FM 方案中节点身份易伪造、不能提供前后向安全性等问题，本文改进了动态累加器构造，提出了一种支持节点动态加入和撤销的认证组密钥管理方案 DAAG。该方案充分考虑了组密钥更新过程中可能存在的攻击场景，具有下述优势：1) 限定了合法信息来源，能够严格依靠动态累加器证人信息实现节点成员身份合法性鉴定；2) 限制了非成员节点对更新消息的解读权和对新密钥的恢复能力，能够在保障前后向安全性的前提下支持成员关系的动态变化；3) 能够抵抗伪造攻击、重放攻击、共谋攻击和恶意更新攻击。

总的来说，DAAG 方案能够在耗费一定性能代价的基础上，提供较 FM 方案更好的安全性。此外，由于组密钥更新多采用多播方式发布更新消息，而传感网信道又存在不同程度的不稳定性，某些更新信息可能未到达或未能完整到达成员节点，使得合法节点只能重新申请入组才能获得新的组密钥。因此，在后续的研究中将重点为 DAAG 方案提供自愈能力，以实现智能、安全、轻量的密钥自愈。

参考文献：

[1] ASOKAN N, GINZBOORG P. Key agreement in ad hoc networks[J]. Computer Communications, 2000, 23(17): 1627-1637.

[2] WONG C K, GOUDA M, LAM S S. Secure group communications using key graphs[J]. IEEE/ACM Transactions on Networking, 2000, 8(1): 16-30.

[3] SHERMAN A T, MCGREW D A. Key establishment in large dynamic groups using one-way function trees[J]. IEEE Transactions on Software Engineering, 2003, 29(5): 444-458.

[4] DU X, WANG Y, GE J, *et al*. An ID-based broadcast encryption scheme for key distribution[J]. IEEE Transactions on Broadcasting, 2005, 51(2): 264-266.

[5] YANG G, WANG J, CHENG H, *et al*. An identity-based encryption scheme for broadcasting[A]. NPC 2007[C]. Dalian, China, 2007.123-126.

[6] ZHANG Y H N M L Y. Identity-based boradcast encryption with shorter transmissions[J]. Journal of Shanghai Jiaotong University (Science), 2008, 13(6): 641-645.

[7] 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]. Security Issues in Sensor and Ad Hoc Networks, 2007, 5(1):14-23.

[8] DUTTA R, CHANG E C, MUKHOPADHYAY S. Efficient self-healing key distribution with revocation for wireless sensor networks using one way key chains[A]. LNCS 4521[C]. Zhuhai, China, 2007. 385-400.

[9] 冯涛, 马剑锋. 基于单向累加器的移动 ad hoc 网络组密钥管理方案[J]. 通信学报, 2007, 28(11A): 103-107.
FENG T, MA J F. One-way accumulators based group key agreement scheme for mobile ad hoc network[J]. Journal on Communications, 2007, 28(11A):103-107.

[10] 马春光, 王九如, 钟晓睿等. 基于单向累加器的传感网密钥管理协议[J]. 通信学报, 2011, 31(11A): 184-189.
MA C G, WANG J R, ZHONG X R, *et al*. One-way accumulators-based key management protocol for wireless sensor networks[J]. Journal on Communications, 2011,31(11A):184-189.

[11] 马春光, 蔡满春, 武朋. 基于单向累加器的无向可传递闭包图认证[J]. 通信学报, 2008, 29(3): 63-69.
MA C G, CAI M C,WU P. Transitively closed undirected graph authentication based on one-way accumulators[J]. Journal on Communications, 2008,29(3):63-69.

[12] BENALOH J, MARE M D. One-way accumulators: a decentralized alternative to digital signatures[A]. EUROCRYPT'93 Workshop on the Theory and Application of Cryptographic Techniques on Advances in Cryptology[C]. New York, USA, 1994.274-285.

[13] BARIC N, PFITZMANN B. Collision-free accumulators and fail-stop signature schemes without trees[A]. The 16th Annual International Conference on Theory and Application of Cryptographic Techniques[C]. Konstanz, Germany, 1997.480-494.

[14] GOODRICH M T, TAMASSIA R, HASIC J. An efficient dynamic and distributed cryptographic accumulator[A]. The 5th International Conference on Information Security[C]. Springer-Verlag London, UK, 2002.372-388.

[15] YUM D H, SEO J W, LEE P J. Generalized combinatoric accumulator[J]. IEICE Transactions on Information and Systems, 2008, E91-D(5): 1489-1491.

[16] CAMENISCH J, KOHLWEISS M, SORIENTE C. An accumulator based on bilinear maps and efficient revocation for anonymous credentials[A]. LNCS 5443[C]. Irvine, CA, United States, 2009.481-500.

[17] JAN C, LYSYANSKAYA A. Dynamic accumulators and application to effcient revocation of anonymous credentials[J]. Lecture Notes in Computer Science, 2002, 2442: 61-76.

[18] 温涛, 张永, 郭权等. WSN 中同构模型下动态组密钥管理方案[J]. 通信学报, 2012, 33(6): 164-173.
WEN T, ZHANG Y, GUO Q, *et al*. Dynamic group key management scheme for homogeneous wireless sensor networks[J]. Journal on Communications, 2012, 33(6):164-173.

[19] KAYALVIZHI R, VIJAYALAKSHMI M, VAIDEHI V. Energy analysis of RSA and ELGAMAL algorithms for wireless sensor networks[J]. Communications in Computer and Information Science, 2010, 89:172-180.

[20] ARVINDERPAL S, WANDER N G H E. Energy analysis of public-key cryptography for wireless sensor networks[A]. PerCom2005[C]. Kauai Island, HI, United States,2005.324-328.

[21] HAAPOLA J, SHELBY Z, POMALAZA-RÁEZ C. Cross-layer energy analysis of multi-hop wireless sensor network[A]. EWSN 2005[C]. Istanbul, Turkey, 2005.33-44.

作者简介：

钟晓睿（1987-），女，四川自贡人，哈尔滨工程大学博士生，主要研究方向为无线网络安全、协议性能评测。

马春光（1974-），男，黑龙江双鸭山人，博士，哈尔滨工程大学教授、博士生导师，主要研究方向为密码学、信息安全、网络编码等。