基于 Paillier 同态的无线自组网组密钥管理方案

何文才[1] 杜 敏[1,2] 刘培鹤[1] 陈志伟[1,2] 郑 钊[1,2]
(北京电子科技学院通信工程系 北京 100070)[1] (西安电子科技大学通信工程学院 西安 710071)[2]

摘 要 基于 Paillier 密码体制,提出了一种安全有效的同态组密钥管理方案。该方案适用于面向群组和拓扑结构易变的无线自组网,具有抗合谋攻击性、前向保密性与后向保密性。针对无线自组网节点频繁加入和退出的特点,密文上的同态操作提高了组密钥更新的效率和实时性。对其正确性和安全性进行了证明。与其他组密钥管理方案相比,该方案具有交互轮数较少、通信和存储开销小、安全性高等特点。

关键词 无线自组网,Paillier,同态加密,组密钥管理
中图法分类号 TP309 **文献标识码** A

Wireless AD-hoc Network Group Key Management Scheme Based on Paillier Homomorphic

HE Wen-cai[1] DU Min[1,2] LIU Pei-he[1] CHEN Zhi-wei[1,2] ZHENG Zhao[1,2]
(Department of Communication Engineering, Beijing Electronic Science & Technology Institute, Beijing 100070, China)[1]
(School of Telecommunications Engineering, Xidian University, Xi'an 710071, China)[2]

Abstract Based on the Paillier homomorphic cryptography system, we presented a safe and effective homomorphism key management scheme. For the sake of the collusive attack, forward secrecy and backward secrecy, our scheme is suitable for group-oriented and rapid variable topology of wireless mobile Ad-hoc network. The homomorphism operations on the ciphertext improve the efficiency of renewing the group key when the external nodes join the group and the internal members leave the group. The security and correctness of our scheme were discussed in this paper. Compared with other approaches, this new scheme has less interaction frequency, a smaller communication and memory cost and a stronger security.

Keywords Wireless Ad-hoc networks, Paillier, Homomorphic encryption, Group key agreement

1 引言

无线自组网(Wireless Mobile Ad-hoc Network,简称WMANET)是在不依赖任何固定基础设施的情况下,实现移动节点之间临时通信的一种系统。无线自组网具有突破地理局限性、多变的网络拓扑结构等特点。组播技术可以实现一个源节点(通常是服务器节点)同时向多个目标节点提供通信服务,能够有效降低节点发送的数据量,降低其带宽需求和发送能耗,提高网络通信效率。在 WMANET 中,由于无线信道带宽较低和节点通信、计算、能量的限制,上述这些业务无法依靠传统的单播技术来实现,使得组播成为无线自组织网络中应用最广泛的通信技术之一。WMANET 组播也遇到与传统网络的组播一样的安全问题,如组成员如何进行身份认证,组播密钥管理框架的构建和组播密钥的分发与更新。由于 WMANET 网络的节点频繁移动属性,将会造成拓扑更容易变化,节点的加入与离开更加频繁,且要满足对节点离开和节点新加入的前向保密和后向保密[1],因此对组播密钥的实时快速更新与分发提出了更高的要求。

群组密钥协商协议是贡献式的密钥协商机制,存在一个中心机构组管理员 GC(Group Controller),GC 负责为组内的成员产生和分配组密钥,或者负责更新和重发组密钥,其中群组成员计算量和通信开销基本相同。在某些特定网络环境下,无线自组织网络中基站有时会充当 GC 的角色,组合各个移动节点的密钥份额,从而实现密钥协商。本文就是采用移动基站来实现对密钥份额密文的同态操作。

2003 年,Khalili 和 Katz 在文献[2]中首先提出一个用于无线自组网的基于身份的密钥管理方案。此方案的最大缺点是承担 GC 职责的节点固定,不能随意离开网络,无法满足 WMANET 中无线设备的移动性、无线群组成员的动态性的要求。文献[3]中的 LKH 方案和文献[4]中的 OFT 方案采用了层次型密钥管理方案,即一棵具有 N 个成员的深度为 h 的平衡二叉树,密钥服务器需要存储的密钥量与节点成员数呈线性关系:$2N-1$;节点成员退出时密钥服务器 GC 的加密开销和通信量与组成员呈对数关系:$2\log_2 N-1$;一个节点成

到稿日期:2012-12-06 返修日期:2013-05-09 本文受国家重点基础研究发展规划(973)(2007CB31120),国家密码发展基金密码理论课题,中央高校基本科研业务费专项资金资助。

何文才(1956—),男,教授,主要研究方向为编码理论及其应用、信息安全及保密,E-mail:dumin912@163.com;杜 敏(1987—),女,硕士,主要研究方向为网络通信安全;刘培鹤(1972—),男,实验师,主要研究方向为信息安全;陈志伟(1989—),男,硕士,主要研究方向为密码学;郑 钊(1988—),男,硕士,主要研究方向为信息安全。

员加入时 GC 的加密开销和通信量为 $2\log_2 N$。可以看出，服务器的密钥存储量随着组规模的扩大而增长，同时，对于一个大型的动态组播网络，当成员频繁加入和离开时，这两种方案的加密开销和通信开销也会与变动率成比例增加；对于拓扑极易发生变化的无自组织网络来说，这两种方案是不适用的。

2009 年，文献[6]把单密钥的同态加密算法 $E(x)=(x+rp) \bmod pq$ 应用于无线自组网，实现了一种同态的密钥管理方案，但其安全性是不够的。文献[7]通过随机分段处理明文，改进的同态加密算法大大提高了安全性。Paillier 算法是基于二次剩余困难问题的，其加法同态特性也可以方便快速地处理密文数据，实现密文形式的私钥更新，且能满足更高的安全性要求。

鉴于以上考虑，本文提出了一种基于 Paillier 加密体制的无线自组网密钥协商，其利用 Paillier 同态特性实现对密文的直接操作，减少了密钥更新过程中 GC 处的加解密次数，提高了密钥更新速度和安全强度，支持节点动态事件组密钥更新。

2 同态加密技术

2.1 同态加密机制

秘密同态的思想由 Rivest，Adleman 和 Dertouzos 等[8]提出，即在不解密密文的条件下，通过对密文执行操作，就能够做到对明文数据的各种计算。1998 年，Sander 和 Tschudin 在文献[9]中定义了整数环上的加法、乘法同态加密机制(Homomorphic Encryption Scheme，简称 HES)，来确保两个变量加密后的计算结果与加密前的计算结果相同。描述 HES 如下：

令 R,S 是两个环。其中 R 为明文空间，S 为密文空间。定义 $E:R\rightarrow S$。

(1)加法同态：如果从 $E(x)$ 和 $E(y)$ 通过 PLUS 运算可以计算出 $E(x+y)$，而不需要知道 x,y 的值。

(2)乘法同态：如果从 $E(x)$ 和 $E(y)$ 通过 MULT 运算可以计算出 $E(xy)$，而不需要知道 x,y 的值。

(3)混合乘法同态：如果从 $E(x)$ 和 y 通过 MIXED-MULT 运算可以计算出 $E(xy)$，而不需要知道 x 的值。

(4)代数同态：如果满足加法同态和乘法同态。

分为 4 类的 HES 仅仅有两种操作：加法和乘法。需要指出的是：第一，明文 x 和密文 $E(x)$ 之间是一个一对多的关系，即：对明文，虽然 $E1(x)\neq E2(x)$，但 $D(E1(x))=D(E2(x))$。第二，仅仅有一些元素满足混合乘法同态，否则混合乘法同态和乘法同态产生异常。则在整数集中，当且仅当 $x=1$ 时满足混合乘法同态：$E(xy)=E(x)y$。

2.2 Paillier 同态性分析

密钥生成：(1)随机地选取两个素数 p 和 q，且满足 $gcd(pq,(p-1)(q-1))=1$。

(2)计算 $n=pq$ 和 $\lambda=lcm(p-1,q-1)$。

(3)选取随机数 g ($g\in Z_{n^2}^*$)，且满足 $\mu=(L(g^\lambda \bmod n^2))^{-1} \bmod n$，其中定义函数 L 为 $L(u)=\dfrac{u-1}{n}$。

(4)公钥为 (n,g)，私钥为 (λ,μ)。

加密和解密：对于明文 $m(m\in Z_n)$，选取随机数 $r(r\in Z_n^*)$，则加密为：$c=g^m \cdot r^n \bmod n^2$；解密为：$m=L(c^\lambda \bmod n^2)\cdot \mu \bmod n$。

同态性分析：Paillier 密码体制是具有加法同态性的加密方案。对其加法同态性证明如下：

对明文 m_1 和 m_2 加密后，可以得：$E(m_1)=g^{m_1}x_1^n \bmod n^2$，$E(m_2)=g^{m_2}x_2^n \bmod n^2$。此时，$E(m_1)\cdot E(m_2)=g^{m_1}x_1^n \cdot g^{m_2}x_2^n \bmod n^2=E(m_1+m_2)$。

3 基于 Paillier 同态性的协议设计

3.1 初始化阶段

无线自组网中允许新节点的加入和离开，拓扑结构和网络节点都动态可变。本文采用基于 Paillier 同态性来实现无线自组网中移动基站和各节点间的密钥协商。

设无线自组网中由移动基站和 m 个节点成员组成。假设自组网两两相邻节点间是能相互发送数据包的双向链路。由移动基站建立无线自组网络。

(1)首先进行系统初始化，由 GC 生成 Paillier 的公钥 (n,g)，私钥 (λ,μ)，将公钥和私钥分发给每个节点。而基站仅仅拥有公钥。

(2)对请求加入无线自组网组播的节点 i，利用已有的认证机制由基站完成对节点的认证后，节点 $i(i=1,2,\cdots,m)$ 选取随机数 r_i 组成一一对应数组 (x_i,r_i)，根据 Paillier 加密算法得到 $y_i=g^{x_i}\cdot r_i^n \bmod n^2$，将其作为该节点的临时身份标识，计算完成后，节点 i 要秘密销毁随机数组，并将 y_i 发送给 GC。

同时，移动基站也为自己生成一组随机数组 (x_0,r_0)，加密得 $y_0=g^{x_0}\cdot r_0^n \bmod n^2$，将其作为移动基站的身份标识。

(3)移动基站产生随机数组 (X_0,R_0)，加密得 $Y_0=g^{X_0}R_0^n \bmod n^2$，并将 Y_0 秘密保存起来作为密钥更新的干扰因子。定义 Y_k 为第 k 次密钥更新的干扰因子，当第 k 次密钥更新时，先随机生成 (X_k,R_k)，再计算 $Y_K=g^{X_k}\cdot R_k^n \bmod n^2$，$Y_K$ 需要保密。

(4)基站收到所有节点的身份标识 y_i 后，将其作为每个节点成员计算的中间值：

由于具有 Paillier 的同态特性，因此不用对身份标识进行解密，可直接利用加法同态操作计算得：

$$Z_i=Y_0\cdot\prod_{j=0,j\neq i}^{m}y_j \bmod n^2 (i=1,2,\cdots,m)$$

然后，将 Z_i 安全地返回给每个节点成员 i。

(5)节点成员 i 利用同态性计算共享密钥的密文 $E_P(K)$，即 $E_P(K)=Z_i\cdot y_i \bmod n^2(i=1,2,\cdots,m)$，然后用 Paillier 的私钥 (λ,μ) 解密得到更新后的组密钥 K。

3.2 密钥更新

3.2.1 节点加入

本方案允许新节点加入。新节点请求加入网络时，先向移动基站发送请求，移动基站采用系统初始阶段的方法对新成员认证成功后，允许节点成为第 $m+1$ 个成员加入无线网组播节点。

(1)由基站对新加入节点 $m+1$ 完成认证后，GC 向其分发 Paillier 的公钥和私钥。

(2)该成员产生一组随机数 (x_{m+1},r_{m+1})，加密得：$y_{m+1}=g^{x_{m+1}}\cdot r_{m+1}^n \bmod n^2$；然后将其作为身份标识，这里可以加上增加节点成员标识符 $y_{m+1}\parallel Join$，并将其传送给基站。

(3)移动基站收到 $y_{m+1}\parallel Join$ 后，由移动基站更新干扰因子 (X_0,R_0) 为 (X_1,R_1)，计算 $Y_1=g^{X_1}\cdot R_1^n \bmod n^2$ 和 $Z_{m+1}=Y_1\cdot\prod_{i=0}^{m}y_i \bmod n^2(i=1,2,\cdots,m)$，并将 Z_{m+1} 安全地传送给

节点成员 $m+1$。

(4)节点成员 $m+1$ 收到 Z_{m+1}，计算出组密钥的密文 $E(K_{new})=(Z_{m+1}\cdot y_{m+1}) \bmod n^2$，用私钥$(\lambda,\mu)$解密即可得到 K_{new}。

(5)移动基站计算 $Z_{Join}=\frac{y_{m+1}\cdot Y_1}{Y_0} \bmod n^2$，向原来的 m 个节点成员广播新成员加入消息 $Z_{Join} \| Join$。其中，除为模逆运算。

(6)原 m 个节点成员收到该广播消息，用共享密钥 K 解密，更新共享密钥的密文 $E_P(K_{new})=E_P(K)\cdot Z_{Join} \bmod n^2$，$i=1,2,\cdots,m$，然后用 Paillier 私钥$(\lambda,\mu)$解密得到更新后组密钥 K_{new}。

此时，节点成员 $m+1$ 加入后的密钥更新工作完成。当再有节点新成员加入时，逐次执行上述节点新成员请求加入过程，并可以扩展到多个节点加入时进行批处理。

3.2.2 节点离开

假设组播节点成员 u 要离开组，此时组内有 m 个成员，成员 u 向基站发送离开请求 $y_u \| Leave$，GC 接收到成员的离开请求后，开始进行密钥更新。节点离开时的密钥更新过程如下：

(1)基站收到 y_u 后不能直接发送给每个节点，需要由基站生成随机数组(X',R')，计算出干扰因子 $Y_1=g^{X'}\cdot R'^n \bmod n^2$。

(2)基站计算出更新值 $Z_{Leave}=\frac{y_u\cdot Y_0}{Y_1} \bmod n^2$(其中除为模逆运算)，通过无线自组网安全信道向除 u 外的其他节点成员广播节点离开消息 $Z_{Leave} \| Leave$。

(3)组内成员收到广播消息 $Z_{Leave} \| Leave$，然后更新密钥的密文：

$$E_P(K_{new})=\frac{E_P(K)}{Z_{Leave}} \bmod n^2 (i=1,2,\cdots,m,i\neq t)$$

然后，用 Paillier 私钥(λ,μ)解密得到更新后组密钥 K_{new}。

当再有节点成员离开时，逐次执行上述节点成员请求离开过程，同时也可以对多个节点离开进行批处理，这样同态特性的优点更会显示出来。

3.2.3 周期性更新

密钥更新的效率对于无线自组网的通信安全非常重要。节点成员在请求加入或者离开网络时，更新密钥。但在节点成员长时间保持不变时也要周期性地更新密钥。周期性更新时，移动基站以一定的时间间隔生成随机数组，并逐次执行上述节点成员请求加入的过程，可以实现满足加法同态性密钥更新的批处理。

周期性更新时，GC 以一定的时间间隔生成新的组密钥，并进行更新。周期性密钥更新过程：

(1)基站定时更新干扰因子，即生成随机数组(X^T,R^T)，计算出干扰因子 $Y_{Timer}=g^{X^T}\cdot (R^T)^n \bmod n^2$。然后，计算出更新值 $Z_{Timer}=\frac{Y_{Timer}}{Y_0} \bmod n^2$。通过无线自组网安全信道向每个节点成员广播定时更新消息 $Z_{Timer} \| Timer$。

(2)节点成员收到 $Z_{Timer} \| Timer$ 后，开始对组密钥进行定时更新，即 $E_P(K_{new})=E_P(K)\cdot Z_{Timer} \bmod n^2$，$i=1,2,\cdots,m$，然后用 Paillier 私钥$(\lambda,\mu)$解密得到更新后组密钥 K_{new}。

这样，整个周期性密钥的更新工作就完成了。

4 正确性分析

本方案的正确性分析结合了文献[10]中密钥协商协议的分析方法，从协议的密钥分发、节点加入和节点离开 3 部分的密钥更新方案来证明正确性。

命题 1 在组密钥生成过程中，每个节点成员都能够正确计算组密钥 K。

证明：已知基站干扰因子 Y_0。组内任意节点成员 s 有：$y_s=g^{x_s}\cdot r_s^n \bmod n^2$，又知从基站处得到：

$$Z_s=Y_0\prod_{j=0,j\neq s}^{m} y_j \bmod n^2=g^{X_0}R_0^n\cdot g^{\sum_{j=0,j\neq s}^{m}x_j}\left(\prod_{j=0,j\neq s}^{m} r_j\right)^n \bmod n^2$$

然后，根据自身身份标识 y_s 计算组密钥密文：

$$\begin{aligned}E_P(K)&=Z_s\cdot y_s\\&=g^{X_0}R_0^n\cdot g^{\sum_{j=0,j\neq s}^{m}x_j}\left(\prod_{j=0,j\neq s}^{m} r_j\right)^n\cdot g^{x_s}r_s^n \bmod n^2\\&=g^{\sum_{j=0}^{m}x_j+X_0}\left(\prod_{j=0}^{m} r_jR_0\right)^n \bmod n^2\end{aligned}$$

节点 s 用 Paillier 私钥(λ,μ)解密得到组密钥：

$$Dec(\lambda,\mu,E_P(K))=\sum_{j=0}^{m}x_j+X_0$$

由于节点 s 是组内任意一个成员，因此每个节点计算出来的 $\sum_{j=0}^{m}x_j+X_0$ 都是相同的，即为组密钥。

命题 2 新节点加入后，其他节点需要进行组密钥更新，只要没有异常发生，则最后计算出的组密钥就是 K_{new}。

证明：(1)对于刚加入节点 $m+1$，有：$y_{m+1}=g^{x_{m+1}}\cdot r_{m+1}^n \bmod n^2$，又从基站处得到：

$$Z_{m+1}=Y_1\cdot\prod_{i=0}^{m} y_i \bmod n^2=g^{\sum_{j=0}^{m}x_j+X_1}\left(\prod_{j=0}^{m} r_jR_1\right)^n \bmod n^2$$

然后计算 $m+1$ 节点，得：

$$\begin{aligned}E(K_{new})&=Z_{m+1}y_{m+1}\\&=g^{\sum_{j=0}^{m}x_j+X_1}\left(\prod_{j=0}^{m} r_jR_1\right)^n g^{x_{m+1}}r_{m+1}^n \bmod n^2\\&=g^{\sum_{j=0}^{m+1}x_j+X_1}\left(\prod_{j=0}^{m+1} r_jR_1\right)^n \bmod n^2\end{aligned}$$

解密后得到组密钥 $\sum_{j=0}^{m+1}x_j+X_1$。

(2)对于组内其他节点成员 s，收到广播消息：

$$Z_{Join}=\frac{y_{m+1}\cdot Y_1}{Y_0}=\frac{g^{x_{m+1}}r_{m+1}^n\cdot g^{X_1}R_1^n}{g^{X_0}R_0^n} \bmod n^2$$

$$=g^{x_{m+1}+X_1-X_0}r_{m+1}^n\left(\frac{R_1}{R_0}\right)^n \bmod n^2$$

然后：

$$\begin{aligned}E_P(K_{new})&=E_P(K)\cdot Z_{Join} \bmod n^2\\&=g^{\sum_{j=0}^{m}x_j+X_0}\left(\prod_{j=0}^{m} r_jR_0\right)^n\cdot g^{x_{m+1}+X_1-X_0}r_{m+1}^n\left(\frac{R_1}{R_0}\right)^n \bmod n^2\\&=g^{\sum_{j=0}^{m}x_j+X_0+x_{m+1}+X_1-X_0}\left(\prod_{j=0}^{m} r_jr_{m+1}R_0\frac{R_1}{R_0}\right)^n \bmod n^2\\&=g^{\sum_{j=0}^{m+1}x_j+X_1}\left(\prod_{j=0}^{m+1} r_jR_1\right)^n \bmod n^2\end{aligned}$$

解密得到组密钥 $\sum_{j=0}^{m+1}x_j+X_1$。至此，证明出新加入节点和组内任意一个节点的组密钥计算值都是相同的，即为 K_{new}。

命题 3 节点离开后，其他节点需要进行组密钥更新，只要没有异常发生，则最后计算出的组密钥就是 K_{new}。

证明：节点离开后，组内任意其他节点成员 s 会收到广播消息：

$$Z_{Leave}=\frac{y_u \cdot Y_0}{Y_1}=\frac{g^{x_u} r_u^n \cdot g^{X_0} R_0^n}{g^{X_1} R_1^n} \bmod n^2$$

$$=g^{x_u-X_1+X_0} r_u^n (\frac{R_0}{R_1})^n \bmod n^2$$

然后：

$$E_P(K_{new})=\frac{E_P(K)}{Z_{Leave}} \bmod n^2$$

$$=\frac{g_{j=0}^{m} x_j+X_0 (\prod_{j=0}^{m} r_j R_0)^n}{g^{x_u-X_1+X_0} r_u^n (\frac{R_0}{R_1})^n} \bmod n^2$$

$$=g_{j=0,j\neq u}^{m} x_j+X_1 (\prod_{j=0,j\neq u}^{m+1} r_j R_1)^n \bmod n^2$$

解密得到组密钥 $\sum_{j=0,j\neq u}^{m+1} x_j+X_1$。由于 s 可以是组内任意一个节点，因此证明出组内任意一个节点的组密钥计算值都是相同的，即为 K_{new}。

周期性更新密钥更新协议是节点离开协议的一种特殊形式，同理也是正确的。至此，整个协议的正确性得到了证明。

5 安全性分析

本文协议是利用 Paillier 加法同态性来实现的无线自组网的密钥协商。在假定计算和判断 $Z_{n^2}^*$ 上的 n 次剩余问题是困难的条件下，Paillier 加密体制具有较强的安全性[11,12]。因此在传输信道上的安全性能够得到保障，包括群组密钥的前向保密性和后向保密性。其次，提出的方案满足抗合谋攻击，即任意组成员只持有自身的密钥份额和剩余组成员的部分密钥和，无法判定系统内的成员个数以及其他成员的密钥份额。下面将具体分析本文协议的安全性。

(1)抗离开节点和新加入节点的合谋攻击

首先，设 t_1 时间点之前离开的节点的集合为：$L\subseteq(L_{t_1}\cup L_{t_1-1}\cup\cdots\cup L_1)$，$t_2$ 时间点之后加入的节点集合为：$J\subseteq(J_{t_2+1}\cup J_{t_2+2}\cup\cdots)$，且 $|L\cup J|\leqslant m$，$t_1<t_2$。如图 1 所示，合谋攻击[13]就是指在 t_1 时刻之前离开的节点和 t_2 时刻之后新加入的节点被捕获或合谋想得到它们未知的 $t_1\sim t_2$ 时段的阴影部分会话($t_1<t<t_2$)时的组密钥。要获得($t_1<t<t_2$)时段的组密钥 K_t，必须知道该时段任何的 Z_t：显然集合 L 中节点能够计算出 $\sum_{j=0,j\neq t}^{m+1} x_j+X_t$；然而，$B\cup C$ 中的节点虽然拥有 t_1 时刻前和 t_2 时刻后的广播消息 Z_{t_1,t_2}，却无法得到 t 时段正确的干扰因子 Y_t。若 $B\cup C$ 想通过恢复 t 时段的组密钥 K_{new}，必须暴力破解得到 t 时段可能有的新加入节点密钥份额 y_t 和该时段的干扰因子，所以 $B\cup C$ 是无法恢复 K_{new} 的。进而 $B\cup C$ 合谋无法计算出 $t(t_1<t<t_2)$ 时段的组密钥 K_{new}。因此，该协议能够抵抗合谋攻击。

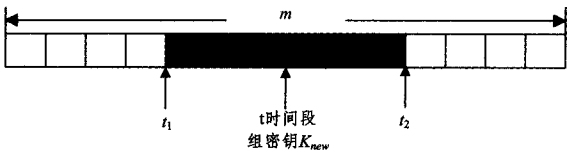

图 1 节点的密钥协商阶段举例

(2)前向保密性

当任意节点成员 s 离开后，移动基站通过安全线网络单播信道向所有成员发送消息($Z_{Leave}\parallel Leave$)，其中，$Z_{Leave}=\frac{y_s \cdot Y_1}{Y_0} \bmod n^2$。组内其他节点成员得到消息后，将组密钥更新为：$E_P(K_{new})=\frac{E_P(K)}{Z_{Leave}} \bmod n^2$。

节点成员 s 得不到消息($Z_{Leave}\parallel Leave$)，也无法得到移动基站产生的新干扰因子。因此，节点成员 s 不能得到新的组播密钥，从而保证了更新密钥 K_{new} 在广播消息时不被泄露，则该密钥更新方案是前向安全的。

(3)后向保密性

当节点 s 加入时，节点得到消息 $y_{m+1}\parallel Join$，每个节点更新后，得到新的组密钥 $K_{new}=\sum_{j=0}^{m+1} x_j+X_1$，而旧的组密钥为 $K_{old}=\sum_{j=0}^{m} x_j+X_0$，由于新成员 s 从基站得到的信息 Z_{m+1} 中不包含更新前的干扰因子，因此节点成员 s 无法计算更新前的组密钥 K_{old}。所以我们的密钥更新方案是后向安全的。

6 性能分析

6.1 计算复杂性

在密钥协商过程中，只需要进行常数次加解密运算，所以计算开销主要由 Paillier 加密算法的运算效率决定，并且不会随着问题规模的增大而快速增长。群组密钥管理协议中成员之间的消息交互次数应尽可能少。新方案中组密钥协商协议只需 2 轮，这表明成员间的消息交互次数与群组成员个数无关，所以协议的操作可以并行执行，这减少了组密钥的交换时间，提高了协议的执行效率。

协议中许多运算都是在密文上直接操作的，这是不含有加法同态属性的 DES、AES 和 RSA 等密码体制无法做到的，而且密文上的同态操作，可直接计算出节点成员的中间值，无需解密，提高了密钥分发的速度，同时也增加了频繁的解密造节点密钥份额的泄漏。

Paillier 与其他密码算法的加解密复杂度对比如表 1 所列，虽然 Paillier 的加解密复杂度较高，但是密文的同态操作减少了大量的加解密次数，所以次数不多的加解密耗时是可以接受的，且密文的同态操作避免了读取用户明文形式的密钥份额。当有多个节点离开或加入时，基于同态技术的批处理密钥分发方案以其较少的加解密开销将更具优势。

表 1 Paillier 加密算法的计算复杂度比较[14]

	RSA(n,e)	ELGamal	Paillier
	$\|n\|,\|p\|=512,e=2^{16}+1$	$\|n\|,\|p\|=512$	$\|n\|,\|p\|=512$
加密	17	1536	5120
解密	192	768	768

说明：表中数值为进行加解密运算所需要进行模($|n|=512$)乘运算的次数

表 2 中符号说明：m 为成员数；h 为密钥树高度；d 为密钥树的度数；O 代表一次单向 Hash 函数的代价；E 表示基于进行一次加密(或解密)运算的代价；R 表示产生一个随机数的代价；A 表示进行一次四则运算的计算代价。其中计算量大小依次排序为：$E>R>O>A$。

从表 2 中可以看出，文献[15]协议每个节点的计算开销略小于本文提出的协议，在假设基站计算能力足够大的情况下，其也是很有效的一个方案。但是，往往基站的计算能力也

是有限的，此时本文方案的优势便体现出来。从与文献[3-5，15]中方案的对比可知，在节点离开和加入的过程中，基站这一端，本文提出的协议中加解密操作次数少于所有的方案。Paillier同态性的利用使得基站只需进行一次的加密和若干次的同态密文操作即可完成密钥更新，提高了系统的实时性，使其更适用于无线终端。

表2 同类协议性能比较

方案	保密性		是否抵御合谋攻击	运算开销			
				节点加入		节点离开	
	前向	后向		GC或基站	成员	GC或基站	成员
文献[3]	√	√		hR+dhE	hE	hR+dhE	hE
文献[4]	√	√		R+hE+2hO	hE+hO	R+hE+2hO	hE+hO
文献[5]	√			2R+(h+2)E+A	2E+hA	2R+2h(d−1)E+A	2E+hA
文献[15]	√	√	√	(h+x)E	0	R+(d−1)hE+A	E+hA
本文协议	√	√	√	E+3A	A+E	E+2A	E+A

说明：运算只与消息加解密有关，并未包含密钥生成和密钥更新的运算。

6.2 存储与通信开销

从表3中可以看出，在存储复杂度上本文提出的协议占用的节点资源相比其他方案少，但是GC的存储开销与文献[3,4]相当，比文献[5]的多。在通信复杂度的比较中，本文协议不占有明显优势，但是本文通信的数据可以采用占用计算资源较少的广播。在节点离开和节点加入时本文协议的通信开销是一样的，由系统节点数目决定。而其他的方案还取决于拓扑结构，这样拓扑结构的合理有效生成也是一个难以解决的问题。而本文协议拓扑结构相对简单，更适应于快速组建的无线自组织网络。

表3 存储复杂度和通信复杂度比较

方案	存储复杂度		通信复杂度	
	GC或基站	节点	节点加入	节点离开
文献[3]	O(m)	$O(\log_d m)$	$O(d\log_d m)$	$O(d\log_d m)$
文献[4]	O(m)	$O(\log_2 m)$	$O(\log_2 m)$	$O(\log_2 m)$
文献[5]	O(2)	$O(\log_d m)$	$O(\log_d m)$	$O(d\log_d m)$
本文协议	O(m+4)	O(3)	O(m+1)	O(m−1)

结束语 本文基于Paillier加法同态性，结合无线自组网通信的特点，提出了一种新的高效快速无线自组网密钥协商方案。与一般的密钥协商方案相比，本文方案在满足密钥安全的前提下，具有更高的密钥协商效率。同态加密算法的特性使得我们可以方便地处理密文数据，实现密文形式的私钥更新，满足了更强的安全策略要求，且密钥管理方便，计算量小，适用于大规模和恶意环境下建立无线网络，实现群组密钥协商。

参考文献

[1] 崔国华，郑明辉. 移动自组网络中的分布式安全组密钥管理[J]. 小型微型计算机系统，2007，7(6)：299-306

[2] Khalili A，Katz J，Arbaugh W A. Toward secure key distribution in truly Ad-Hoc networks[C]//Proceedings of The Symposium on Applications and the Internet Workshops. Los Alamitos：IEEE Computer Society Press，2003：342-346

[3] Wong C K，Gouda M，Lam S S. Secure group Communications using key graphs[J]. IEEE ACM Trans Networking，2000，8(1)：16-30

[4] Balenson D，McGrew，Sherma A. Keymanagement for large dynamic groups：one-way function trees and amortized initialization[Z]. Internet-Draft Internet Engineering Task Force，Mar. 1999

[5] Tseng Y-M. A scalable key-management scheme with minimizing key storage for secure group communications[J]. International Journal of Network Management，2003，13(6)：419-425

[6] 胡焰智，马大玮，等. 基于同态加密机制的无线群组密钥分配协议[J]. 计算机工程，2009(4)：158-160

[7] Domingo-Ferrer J，Herrera-Joancomarti J. A new privacy homomorphism and application[J]. Information Processing Letters，1996，60(5)：227-282

[8] Rivest R L，Adleman L，Dertouzos M L. On data banks and privacy homomorphisms[A]//De-millo R A et al. Foundations of Secure Computation[C]. New Youk：Academic Press，1978：169-179

[9] Sander T，Tschudin C. Protecting Mobile Agents Against Malicious Hosts[C]//the Proceedings of the 1998 IEEE Symposium of Research in Security and Privacy. Oakland，1998

[10] 冯涛，马建峰，等. 一种新的基于椭圆曲线密码体制的Ad hoc组密钥管理方案[J]. 电子学报，2009，37(5)：918-924

[11] Catalano D，Gennaro R，Grahamn H. The bit security of paillier encryption scheme and its application[C]//Advances in CryptologyEurocrypt'01，Aarhus，Denmark，LNCS2045. Berlin：Springer-Verlag，2001：229-243

[12] Cramer R，Shoup V. Universal hash proofs and a paradigm for adaptive chosen ciphertext secure public-key encryption[C]//Advances in Cryptology-Eurocrypt'02，Amsterdam Netherlands，LNCS 2332. Berlin：SpringerVerlag，2002：45-94

[13] 曹帅，张申绒，等. 具有抗合谋攻击能力的自治愈群组密钥管理方案[J]. 计算机应用，2011，31(10)：2692-2777

[14] Paillier P. Public-key cryptosystems based on Composite degree residuosity classes[C]//Proceedings of Eurocyypt'99，Prague，Czech Republic，LANCS 1592. Berlin：SpringerVerlag，1999：223-228

[15] 武涛，郑雪峰，等. 一种高效的组密钥分发协议[J]. 小型微型计算机系统，2010，31(10)：2030-2033