DOI:10.13718/j.cnki.xsxb.2017.01.008

一种高效的无线网络组密钥管理方案①

柯 钢

东莞职业技术学院 计算机工程系,广东 东莞 523808

摘要:为了满足无线网络组播通信的安全,提出一种适用于多跳环境的高效组密钥管理方案.将代理重加密扩展到多跳的无线网络环境中,从而不需要可信的密钥分配中心;在子组的通信中,采用多接收方加密算法,充分利用了无线通信的广播特性,提高了运算效率,大大减少了通信代价.安全分析和效率分析表明,该方案不仅满足前向安全性和后向安全性,而且有效降低了通信复杂度、存储开销和计算量.

关 键 词:组密钥管理;代理重加密;多接收方加密

中图分类号:TP393.8 **文献标志码**:A **文章编号**:1000-5471(2017)01-0047-07

组播技术能有效地解决一个主机向特定多个接收主机高效发送消息的问题,减少不必要的重复发送,有效地利用网络带宽,减轻服务器负荷,降低网络的拥塞,较适合应用在天然具有广播特性的无线网络中.在无线组播安全通信中,组密钥管理成为急需解决的问题.为了防止组播通信内容被非授权用户访问,所有的组成员共享一个组密钥来完成对数据包的加密,并且合法组成员都可以使用该组密钥解密数据包.然而,无线网络的群组经常动态变化,每当有用户加入或离开组播组时,组密钥都必须更新,以满足前向安全性和后向安全性;同时,无线网络缺乏有效的基础设施,难以找到完全可信的中心节点.

现有的组播密钥管理方案可分为集中式、分布式和分簇式 3 种.集中式密钥管理方案[1-2]通过设立一个组管理中心为全部成员产生、分发、更新和撤销密钥.但该方案存在单点失效问题,即一个组播成员发生变化,所有组密钥都需要更新,通信复杂度较高.而分布式密钥管理方案恰恰相反[3-5],没有组管理中心,组密钥由各成员共同协商计算而来,但是方案时间和通信代价将随着组成员数量呈线性上升趋势.分簇式密钥管理方案[6-9]将整个组分成若干个子组,每一个子组由一个管理者控制,该管理者有更强的计算和通信能力,子组中的每个成员共享一个密钥.收到密文时,子组管理者进行解密,并利用子组共享密钥再次加密后发送给组中成员.虽然该类型方案提高了可靠性和扩展性,但是要求管理者节点必须完全可信并能防止密钥泄漏,这仍是一个巨大的挑战.

本文提出了一种分簇式的组密钥管理方案,将代理重加密算法扩展到多跳的环境中,从而不需要可信中心;将多接收方加密算法应用到子组通信中,充分利用了无线的广播特性,提高了密钥更新的效率;采用分层分簇式结构,提高了可用性和扩展性.

1 基础知识

1.1 相关工作

分层分簇式组密钥管理方案可有效地解决网络的可靠性问题,扩大了网络的规模,目前有多个方案提出.

① 收稿日期:2015-10-21
基金项目:东莞市高等院校、科研机构科技计划一般项目(2014106101035).
作者简介:柯 钢(1983-),男,湖北黄石人,硕士,讲师,主要从事网络安全技术、智能算法研究.

Iolus方案[6]要求所有组成员必须完全信任簇头. 为了将分组A的密文传递给分组B,A的簇头必须解密密文,再用分组B的公钥加密,这样传递的信息内容就会泄漏给簇头,存在可信第三方的问题.

2007年,Junbeorm Hur等[7]使用代理加密提出一个动态网络的组密钥管理方案DGKM. 方案提出了一个多跳的代理加密算法,用来传递密钥信息. 假设有发送方s、接收方u和n个中间代理节点$p_1,p_2,\cdots,p_n$. s加密消息m,输出为$\{c_1,c_2\}=\{g^{r_{init}},m\cdot g^{(r_{init}+PK_{init})\cdot GK^i}\}$. 对于$1\leqslant j\leqslant n$,代理$p_j$转换$\{c_1,c_2\}$为新的密文$\{c'_1,c'_2\}=\{c_1\cdot g^{r_j},c_2\cdot g^{(r_j-PK_{j-1}+PK_j)\cdot GK^i}\}$. 最后当密文到达$u$时,密文为$\{c_1,c_2\}=\{g^{r_{init}+r_1+\cdots+r_n},m\cdot g^{(r_{init}+r_1+\cdots+r_n+PK_n)\cdot GK^i}\}$. 用户$u$恢复$m=\dfrac{c_2}{(c_1\cdot g^{PK_n})^{GK^i}}(\mathrm{mod}\ p)$. 发送者负责为组播组成员分发组密钥,因而不需要密钥分配中心. 但是密钥分配过程中,发送者需要逐个单播组密钥,使得通信量比较大. 当代理节点加入或离开时,相应的代理节点必须发送自己的代理密钥给其它代理节点和组成员,这对于组密钥管理来说太过复杂.

2014年,Abbas Mehdizadeh等人[8]提出一个结合组播和单播通信的无线IPv6无线网络密钥管理方案MUKD,由发送方、簇头节点和组成员组成. 发送方与多个簇头之间通过组播方式进行信息传输,而簇头节点与簇成员绑定MAC物理地址,进行单播通信. 簇头节点作为管理者,负责产生、分发和更新组密钥,而所有成员认为它完全可信. 虽然该方案在密钥管理方面有了效率上的提高,但是存在可信第三方问题.

2014年,郑明辉等人提出一个可扩展的组密钥管理协议KPET[9],包括三类节点:密钥生成中心KDC、演化节点N_i和组成员U_i,其中演化节点N_i与文献[7]的代理节点p_i类似. 在初始化阶段,KDC为演化节点和组成员生成密钥参数,维护一个密钥参数演化树,但是需要进行大量计算,还需要安全通道将参数进行传送,难以适用于缺乏基础设施的无线网络. 该方案解决了可信第三方问题,但也带来了密钥更新复杂的问题. 当组播成员要求加入分组N_i时,KDC需重新配置N_i及其子节点的参数,并重新生成会话密钥;当某个成员离开分组N_i时,KDC需利用单播密钥给其他成员. 此外,方案并未考虑演化节点离开或加入的情况.

1.2 代理重加密

代理重加密是由Blaze等人[10]在欧洲密码会议上提出的. 在代理重加密中,一个拥有代理重加密密钥的半可信代理者(Proxy)可以把Alice的密文转换为Bob对应的同一个明文的密文,而这个代理者不能获得明文. 代理者的半可信,指的是仅仅相信这个代理者一定会按方案进行密文的转换. 代理节点的代理重加密密钥是$RK_{A\to B}$,它可以把Alice用公钥PK_a加密的密文,转化为Bob用自己私钥SK_b解密的密文.

代理重加密具有特殊的转换功能,可以解决很多实际问题,如有效地解决在安全分布式存储和数字版权管理中的跨域操作等问题. 本文将代理重加密多跳扩展后,引入到组密钥管理中,有效解决了中间节点的可信问题.

1.3 多接收方加密

在组播通信中,一个用户要同时向n个用户发送机密数据,直接的方法是应用基本密码算法,分别为每一个接收者产生一则密文并发送出去,这种方法可称之为trivial n-recipient方案或naive方案. trivial n-recipient方案简单直接,但存在缺点,因为点对点场合所考虑的系统模型和攻击者的能力与多用户场合不同,一些在点对点场合中安全的密码方案在多用户场合中仍然不够安全.

2002年,Kurosawa[11]发现用一些密码算法构造多接收方方案(MRES, multi-recipient encryption scheme)时可以提高批量加密的效率,使密文的总体长度和总体计算量降低近一半.

本文采用ElGamal的多接收方加密方案对多个接收方的秘密参数分发,在保证安全的情况下提高了效率.

2 多跳代理重加密

本文将Ateniese提出的代理重加密方案[12]扩展到多跳的环境中以适用于组播通信.

如图1所示,n个公私钥对分别为$(P_{p_1},P_{s_1}),(P_{p_2},P_{s_2}),\cdots,(P_{p_n},P_{s_n})$的代理节点$P_1,P_2,\cdots,P_n$组成一条数据链路. 发送者$S(g^s,s)$通过这个链路给目的节点$U(g^u,u)$发送数据,过程见图1.

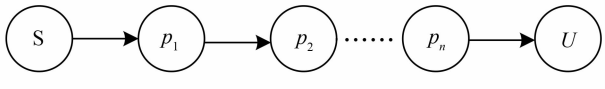

图 1　多跳代理重加密示意图

1) 对于发送方 S，根据接收方 U 公钥 g^u 和自己私钥 s，计算代理重加密密钥 $R=g^{\frac{u}{s}}$；接着选取随机数 k，加密密文 m 后输出密文 $(c_1, c_2)=(g^{sk}, mZ^k)(Z=e(g, g))$，然后将 (c_1, c_2, R) 发送给 P_1.

2) 当代理节点 $P_j(1\leqslant j\leqslant n-1)$ 接收到密文 (c_1, c_2, R) 后，进行如下操作：

a) 计算 $c'_1=c_1^{P_{s_j}}$；

b) 计算 $R'=R^{\frac{1}{P_{s_j}}}$；

c) 将 (c'_1, c_2, R') 作为 (c_1, c_2, R) 发送给下一跳 P_{j+1}；

d) P_{j+1} 重复过程 a) — d)，直到 $j=n$.

3) 当代理节点 P_n 接收 (c_1, c_2, R) 后，计算 $e(c_1, R)=Z^{uk}$，将 $C_u=(\alpha, \beta)=(Z^{uk}, mZ^k)$ 发送给 U.

4) 当目的节点 U 收到 $C_u=(\alpha, \beta)$ 后，使用自己的私钥 u 解密密文，得到消息 $m=\dfrac{\beta}{\alpha^{\frac{1}{u}}}$.

3　方案设计

3.1　网络模型和框架

如图 2 所示，方案的网络模式采用两层分簇式结构. 代理节点因具有较强的通信能力、计算能力和电池供电能力，联合组成一个骨干网络，相互之间通过多跳的无线链路进行通信. 而另外的移动无线节点直接与代理节点连接，通过代理节点与其它移动节点进行通信. 这样，一定数量的移动无线节点与直接连接的代理节点就形成了一个子组. 方案的框架是建立在基于源的多播树网络之上的. 根节点是服务提供商，为客户提供如在线视频点播和远程教育等服务. 网络的中间节点为半可信的代理节点，半可信指的是这些代理节点无法得到组密钥，只能用代理重加密算法将接收到的密文进行转换，并正确发送给下一跳.

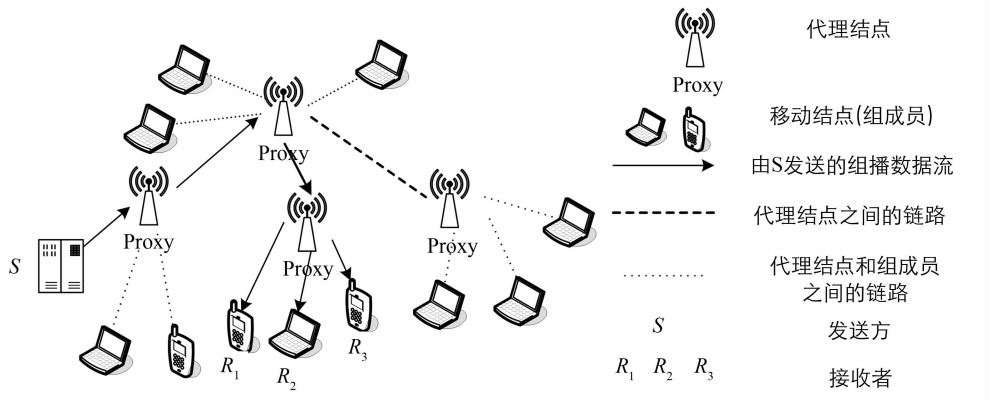

图 2　网络模型

假设在网络部署前，存在一个可信中心，负责为移动无线节点生成一对公私钥，并颁发证书给它们. 这个证书绑定了用户的公钥和身份，用来与代理节点进行认证. 当通过了代理节点认证后，移动无线节点就成为这个子组的组成员. 但他仍然无法得到组播数据，还必须通过服务提供商的认证. 服务提供商认证了用户后，通过安全链路分发组密钥给用户. 在一个组播通信中，服务提供商使用组密钥加密组播数据，然后通过由若干代理节点组成的链路进行传递，最后被拥有组密钥的合法移动节点用户解密.

方案中使用的概念和符号如下：

1) S：服务提供商.

2) Gk：组密钥. Gk 是由服务提供商和组成员之间共享的私钥，而组公钥是 $y=g^{Gk}(\mathrm{mod}p)$. 方案认为代理节点不是组成员，无法得到 Gk，以避免代理节点获取组播数据.

3) R_{s_j}：组成员的私钥. R_{s_j} 是接收者 R_j 的私钥，其公钥为 $R_{p_j} = g^{R_{s_j}} (\mathrm{mod} p)$.

4) P_{s_i}：代理节点 P_i 的代理私钥. 代理节点的公钥为 $P_{p_i} = g^{P_{s_i}} (\mathrm{mod} p)$.

5) r：由服务提供商选取的随机数.

3.2 组密钥分发

由于代理节点是半可信的，因此在本方案中，服务提供商为组播成员分发组密钥. 这在实际应用中是非常合理的，因为只有付费的用户才能获得服务提供商的授权，获取特定的服务. 服务提供商使用多接收方加密算法加密组密钥 Gk，而后发送密文 M 给代理节点. 通信链路中的代理节点不需要重新加解密 M，只需要使用自己私钥计算相应的参数，对密文 M 进行逐次转换. 最后转换后的 M 被传递到离接收组成员最近的代理节点，代理节点解密得到 M 并广播给组成员. 这时合法组成员就可利用自己私钥正确地获取 Gk. 过程如下：

1) 服务提供商选取随机数作为组密钥 Gk，并且用多接收方加密算法加密 Gk，输出密文为 $M = (g^r, Gk \cdot R_{P_1}^r, \cdots, Gk \cdot R_{P_n}^r)$.

2) M 沿着通信链路被传递给 P_n. 这个过程使用了 4.2 节中的多跳代理重加密算法.

3) P_n 解密得到 M，然后广播给组成员.

4) 正确接收到 M 后，组成员 R_i 可得到 $(a, b) = (g^r, Gk \cdot R_{P_i}^r)$，使用私钥 R_{s_i} 对之解密，得到 $Gk = \dfrac{b}{a^{R_{s_i}}}$.

3.3 密钥更新

当组播成员加入或离开组播子组时，组播密钥应该及时更新，以确保前向安全性和后向安全性.

3.3.1 成员加入

为了加入一个安全组播，移动客户端要向附近的代理节点发送JOIN消息，申请加入组播组. 如果通过了代理节点的认证，移动客户端就成功地加入了这个组播组. 然后代理节点将 JOIN 消息转发给信息服务商. 信息服务商确认新节点可信后，发送更新消息给组播成员，进行组密钥更新. 提出的密钥更新算法详细过程如下：

a) 所有拥有 Gk 的组播成员使用哈希算法，更新组密钥 $Gk' = Hash(Gk)$；

b) 信息服务商计算 $Gk' = Hash(Gk)$；

c) 信息服务商使用安全单播，发送 Gk 给新节点.

3.3.2 成员离开

当有组成员离开组播组时，密钥更新机制可被看作是一个新的组密钥分发过程，可以使用 3.2 的组密钥分发协议进行密钥更新. 但是，考虑到代理节点比普通移动客户端具有更强的计算和通信能力，我们提出了一个新的更新算法，有效减少通信包的长度和降低客户端的计算量. 算法详细过程如下：

a) 信息服务商选取随机数 k'，使用 Elgamal 加密算法，传递 k' 给代理节点 P_n；

b) P_n 解密得到 k'，计算密文 $M = (g^r, Gk \cdot R_{P_1}^r, \cdots, Gk \cdot R_{P_n}^r)$ 并广播给组成员；

c) 所有合法节点使用自己的私钥 R_{s_i} 解密 k'，然后计算新的组密钥 $Gk' = Hash(Gk \oplus k')$.

3.4 网络动态管理

在动态网络内，组成员和代理节点都可以动态地离开或加入网络，这给密钥管理带来了巨大的挑战. 特别是代理节点随时离开或加入组播树，改变了组播树的拓朴结构. 因此一个好的密钥管理方案应该能及时消除代理节点加入和离开所造成的影响，做到不中断组播数据的传递，减少动态管理所需通信量和计算量.

3.4.1 代理节点加入

在正在运行的组播网络中，一个新的代理节点可以随时加入网络. 根据网络实际情况的不同，这个代理节点可能作为叶子节点或非叶子节点. 如果代理节点作为叶子节点加入网络，那么父代理节点需要认证该节点，并修改下一跳为该节点. 如果新的代理节点作为非叶子节点加入网络，那么父代理节点和子代理节点都需要认证该节点. 假如成功通过了认证，父节点和子代理节点分别修改下一跳和上一跳为该新代理

节点. 同时该节点修改自己的上一跳和下一跳分别为父代理节点和子代理节点. 图 3 说明了代理节点 P_i 加入 P_1 和 P_2 之间的例子.

3.4.2　代理节点离开

当代理节点离开组播树时，由信息服务商到组成员的多播路径将中断，因此其它的代理节点应迅速修复这条链路. 父代理节点修改它的下一跳为离开节点的子代理节点，同时离开节点的子代理节点修改上一跳为离开节点的父节点. 图 4 说明了代理节点 P_2 离开 P_1 和 P_3 之间的例子.

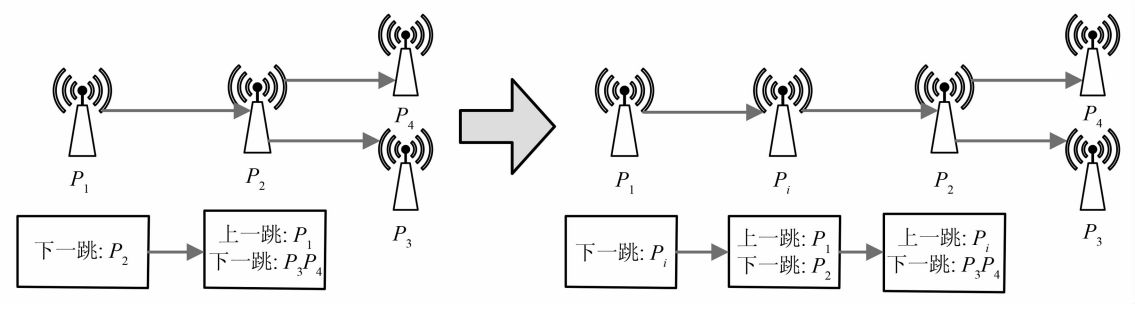

图 3　代理节点加入

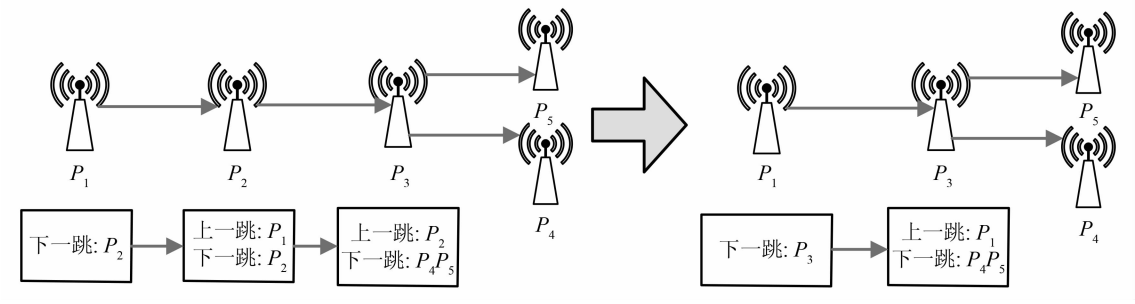

图 4　代理节点离开

4　方案分析

4.1　安全性分析

在本节，对提出方案进行了安全性分析，分析结果显示该方案满足前向安全性和后向安全性.

4.1.1　前向安全性

当一个移动客户端加入组播组时，信息服务商更新组密钥为 $Gk' = Hash(Gk)$. 新加入的移动客户端即使接收到新组密钥 Gk'，并且存储了之前的加密组播数据，但因无法得到 Gk，而不能解密这些组播数据. 如果一个攻击者在知道 Gk' 的情况下要得到 Gk，必须从哈希算法 $Gk' = Hash(x)$ 中计算 x. 但是目前破解单向哈希算法是不可行的. 因此，攻击者在知道 Gk' 的情况下，无法得到之前的密钥 Gk'.

另一种获取先前组密钥的可能是攻击者截获密钥分发消息 $M = (g^r, Gk \cdot R^r_{P_1}, \cdots, Gk \cdot R^r_{P_n})$. 为了获得 Gk，攻击者需要在不知道任何一个组成员私钥的情况下，攻破多接收方加密方案. 显然，多接收方加密方案的安全性等同于 Diffie-Hellman 困难问题，它在多项式时间内是无法被计算出来的. 因此，本方案满足前向安全性.

4.1.2　后向安全性

当一个组成员离开组播组时，服务提供商选择并传递随机数 k' 至 P_n. P_n 使用多接收方加密算法加密 k'，得到 M 并广播给组成员. 所有组成员成功接收后，计算新的组密钥 $Gk' = Hash(Gk \oplus k')$. 即使攻击者知道 Gk，但不能作为密文 M 的接收者，从而无法用自己私钥解密出 k'. 上文已分析过哈希算法是无法被攻破的，因此攻击者无法得到新的组密钥. 对于代理节点来说，虽然拥有随机数 k'，但因没有先前的组密钥 Gk 而无法计算出 Gk'.

4.2　效率分析

如表 1 所示，本方案与其它方案进行比较，包括是否提供数据加密、是否需要密钥生成中心、密钥更新

时的通信量和密钥存储等方面. 表1中N代表全部组成员的数量，M代表子组成员的平均数量，P_1代表代理节点的预期子节点数量，P_2代表代理节点所在密钥树的深度.

本方案由信息服务商负责分发组密钥，因此本方案不需要传统的密钥分配中心，避免了单点失效问题. 通信链路上的代理节点是部分可信的，无法获取传递的信息内容，解决了可信第三方的问题，而且将多接收方加密算法应用在子组通信中，大大降低了通信代价.

当普通移动节点加入组播组时，本方案只需要单播新的组密钥给该节点. 组成员离开组播组时，信息服务商传递一个随机数给代理节点，然后代理节点广播给剩余组成员. 因此，当组成员离开时，方案的通信量仅需一次单播和一次广播.

一个组播成员需要存储自身私钥和本组的代理节点密钥. 这里就不再考虑组密钥的存储问题，因为对所有的方案都需要存储组密钥. 对于代理节点来说，它除存储自身的代理密钥外，还需要存储M个组成员的公钥以进行广播通信. 在表1中，本方案中的组成员存储的密钥量少于其它方案，但代理节点的密钥存储量却多于其它方案. 因为在本方案的网络模型中，代理节点比普通移动客户端有更强的存储能力、计算能力和通信能力.

在表1中，本文首先对安全特性进行比较：KPET，DGKM和本方案提供数据加密功能，Iolus，DGKM和本方案无需密钥分配中心，故只有DGKM和本方案同时满足这两个安全特性. 在效率理论分析方面，本方案在密钥更新时，通信量最少. 本文使用PBC函数库(http://crypto.stanford.edu/pbc/down.html)编程模拟实现了3个方案的密钥更新算法，并不区分节点，所有运算均在在联想开天M6600的计算机上运行，其CPU为Interl® Core ™2 CPU 1.86 GHz、内存为1.00 GB. 算法中使用的私钥为20byte、公钥为30byte、组密钥为32byte. 计算结果如图5所示，横坐标为组成员的数量，分别为1,5,10,15,20,25,30；纵坐标表示所有节点的计算所消耗的时间. 从该图可以看出，本方案所需时间最少，并且随着组成员数量的逐渐增多效率优势愈发明显.

表1 安全特性和效率比较表

	Iolus	MUKD	KPET	DGKM	本方案
数据加密	否	否	是	是	是
密钥分配中心	否	是	是	否	否
可信代理	完全可信	可信	部分可信	部分可信	部分可信
组节点加入时密钥更新通信量/byte	$M+P_1$	2	P_1+1+M	2	1
组节点离开密钥更新通信量/byte	$M+P_1$	1	P_2+M	$2\log(M+P_1)+1$	2
代理节点密钥存储量/byte	P_1	M	P_1	2	M
组成员节点密钥存储量/byte	1	1	1	$\log M+1$	2

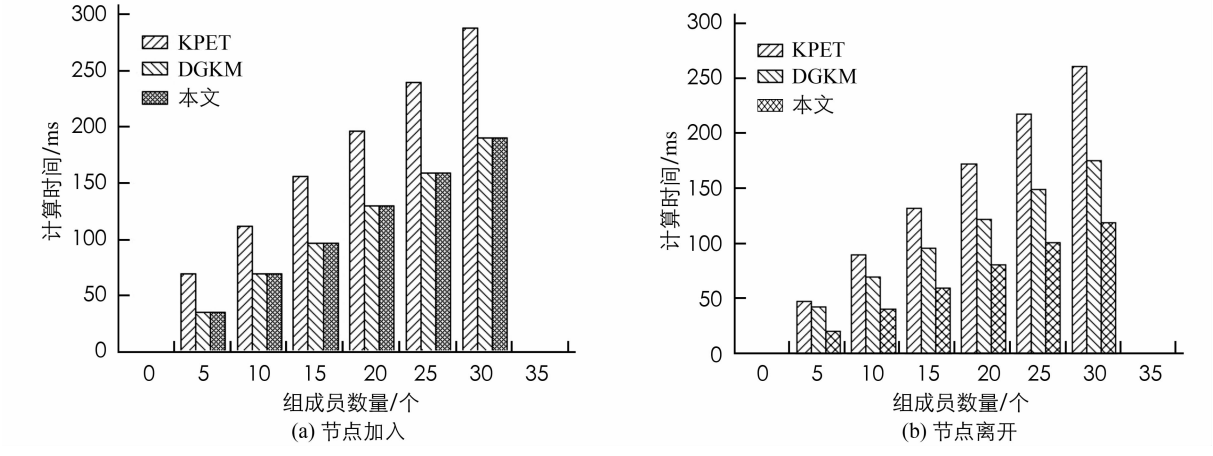

图5 组密钥更新消耗时间对比图

5 总 结

本文设计了一种新的组密钥管理方案，采用分层分簇式网络结构，具备良好的可扩展性；利用代理重

加密的半可信性，将它扩展应用于多跳的无线网络环境，从而不需要可信的密钥分配中心；使用多接收方加密算法，用于安全参数的秘密分发，充分利用了无线通信的广播特性，提高了运算效率，大大减少了通信代价. 分析和实验表明，本方案在保证安全性的前提下，比其他方案效率更高.

参考文献：

[1] McGreW D A, SHERMAN A T. Key Establishment in Large Dynamic Groups Using One-Way Function Trees [J]. IEEE Transactions on Software Engineering, 2003, 29 (5): 444－458.

[2] LIU N, CHEN J S, ZHANG J H, etal. An Efficient Distributed Group Key Management Using Hierarchical Approach with ECDH and Symmetric Algorithm [J]. IEEE Transactions on Industrial Electronics, 2013, 60(10): 4746－4756.

[3] UDAY P S, RAJKUMAR S R. An Efficient Distributed Group Key Management Using Hierarchical Approach with ECDH and Symmetric Algorithm [J]. Computer Engineering and Intelligent Systems, 2012, 3(7): 32－38.

[4] NIU Q. ECDH-based Scalable Distributed Key Management Scheme for Secure Group Communication [J]. Journal of Computers, 2014, 9(1): 153－160.

[5] GUO C, CHANG C C. An Authenticated Group Key Distribution Protocol Based on the Generalized Chinese Remainder Theorem [J]. International Journal of Communication Systems, 2014, 27(1): 126－134.

[6] MITTRA S. Iolus: A Framework for Scalable Secure Multicast [J]. ACM Computer Communication, 1997, 27(3): 277－288.

[7] HUR J, SHIN Y, YOON H. Decentralized Group Key Management for Dynamic Networks Using Proxy Cryptography [C]// Q2swinet'07-Proceedings of the Third ACM Workshop on Q2s and Security for Wireless and Mobile Networks. Providence: ACM Press, 2007: 123－129.

[8] ABBAS M, FAZIRULHISYAM H , MOHAMED O. Light Weightd Ecentralized Multicast-Unicast Key Management Method in Wireless IPv6 Networks [J]. Journal of Network and Computer Applications, 2014, 42: 59－69.

[9] 郑明辉，周慧华，宋庆燕. KPET：一种新的可扩展组密钥管理协议 [J]. 武汉大学学报(理学版)，2014，60(6)：513－517.

[10] BLAZE M, BLEUMER G, STRAUSS M. Divertible Protocols and Atomic Proxy Cryptography [J]. Lecture Notes in Computer Science, 1998, 1403: 127－144.

[11] KUROSAWA K. Multi-Recipient Public Key Encryption with Shortened Ciphertext [C]//Proceedings of the 5th International Workshop on Practice and Theory in Public Key Cryptosystems. London: Springer-Verlag, 2002: 7－38.

[12] GIUSEPPE A, KEVIN F, MATTHEW G, etal. Improved Proxy Re-Encryption Schemes with Applications to Secure Distributed Storage [J]. ACM Transactions on Information and System Security, 2006, 9(1): 1－30.

An efficient group key management scheme for wireless networks

KE　Gang

Department of Computer Engineering, Dongguan Polytechnic, Dongguan Guangdong 523808, China

Abstract: For secure group communication in wireless networks, an efficient group key management scheme suited for multi-top environment has been proposed. A proxy re-encryption to multi-hop environment has been extended, and then a distributed protocol been developed for key distribution. In local group communication, a multi-recipients encryption has been used to broadcast key information reducing communication cost. Though analyzing the proposed scheme with the previous schemes, the result indicates that the proposed scheme can not only satisfy the forward security and backward security, but also has advantages with regard to the rekeying cost, storage overhead and computation efficiency.

Key words: group key management; proxy re-encrypiton; multi-recipient encryption

责任编辑　张　枸