无线 Ad hoc 网动态密钥管理问题的研究

傅 坚 张 翎
(中国网通集团研究院 北京 100036)

摘 要 作为一类自组织动态网络，无线 Ad hoc 网面临着严重的安全威胁。该文在分析 Ad hoc 网络特点的基础上，提出一种基于扩展 Diffie-Hellman 交换的分级组密钥管理方案(HGKM)。HGKM 协议采用分级架构，利用成员过滤函数维护统一的组密钥，有效减少密钥更新对 Ad hoc 网性能的影响。

关键词 Ad hoc 网，安全，Diffie-Hellman 交换，组密钥管理
中图分类号：TP393, TP309 **文献标识码**：A **文章编号**：1009-5896(2006)05-0815-05

The Research on the Dynamic Key Management of Wireless Ad hoc Network

Fu Jian Zhang Ling
(*China NetCom Group Labs, Beijing* 100036, *China*)

Abstract As a kind of dynamic self-organized network, wireless Ad hoc network is faced with serious security threat. On the basis of analyzing the characteristics of Ad hoc network, a hierarchical group key management solution (Hierarchical Group Controller-Based Group Key Management protocol) based on extended Diffie-Hellman protocol is presented. The HGKM utilizes member filter function and hierarchy to maintain a single group key to adapt to the special requirements for frequent key refresh of Ad hoc network.

Key words Ad hoc network, Security, Diffie-Hellman protocol, Group key management

1 引言

近年来对Ad hoc网的研究成为热点[1－3]。1997年Internet工程任务组——IETF成立了移动Ad hoc网络(Mobile Ad hoc Network)工作组，负责多跳Ad hoc网络的路由算法研究和标准制定，目前已完成了十几个Internet草案标准的制定。Ad hoc网主要应用领域为军用、紧急情况下的组网或其他一些对安全敏感的环境，其它应用例子包括小型传感器网络、虚拟教室等。

作为一种无线网络，传统无线网络中存在的安全问题在Ad hoc网中同样存在，并且由于其特殊性，涉及的安全问题更为复杂[4－6]。文章针对Ad hoc网的密钥管理问题，在分析、比较现有的解决方案基础上，提出一种基于组控制器的分级组密钥管理方案Group Controller based Hierarchical Group Key Management(HGKM) protocol。基于分布式处理，HGKM协议简化了组管理操作，对Ad hoc网络具有很强的适应性，文章最后给出了HGKM方案的性能分析。

2 Ad hoc 网的组密钥管理问题

Ad hoc 网是一类由移动节点组成的动态自治系统，其最大特点是不存在任何固定的网络基础设施(Infrastructure)。与依赖于移动交换中心、基站等网络基础设施的常规无线网络(如 GSM)不同，Ad hoc 网中网内节点通过互相协作实现互联(Interconnect)。如果两个节点位于对方的信号覆盖范围，那么它们之间可以通过无线信道直接通讯，否则依靠邻近节点充当路由器在二者间进行消息转发。Ad hoc 网的另一特点是网络拓扑结构动态变化，移动节点可以随时加入或离开。此外 Ad hoc 网中的节点一般计算能力、内存、电源供给有限。

对Ad hoc网而言，采用组密钥技术有两大优点：(1) 充分利用邻近节点的广播能力，避免对任意节点和其他参与方直接连通性的不切实际假设[5]；(2) 减轻了动态加入/离开节点的密钥更新负担。

超立方体协议[5]利用Diffie-Hellman交换，d轮交互即可使2^d个节点间共享一个组密钥。文献[4]提出了一种基于扩展Diffie-Hellman交换的组密钥建立协议——GDH.2，GDH.2 协议依托线性拓扑结构，N个节点完成组密钥共享只需$N-1$ 条单播消息和一条广播消息。文献[6]提出一种基于二叉树的组密钥分发协议，该协议中根节点负责产生组密钥，并沿树中根到叶子节点的路径分发组密钥。概括起来，这些方案存在以下不足：(1) 依赖某种特殊的网络拓扑结构，如树状结构[6]或立方体结构[4]；(2) 密钥刷新耗时较长，需要重新运行协议[4, 5]；(3) 对动态成员引起的密钥更新缺乏足够的重视[5]。出于维护密钥独立性的考虑[7]，新成员加入或组内现有成员离开，组密钥应立即更换。

3 分级组密钥管理方案

基于组控制器的分级组密钥管理方案(以下简称分级方

2004-08-16 收到，2005-06-27 改回
国家“973”项目(G1999035804)和国家自然科学基金(60073049, 90204017)资助课题

案)基本思路可以概括为：相邻的几个移动节点构成一个组，整个 Ad hoc 网由若干个组构成。每个组内有一个组控制器(Group Controller, GC)，组内所有节点都可以与组控制器直接通信。

与组内普通节点不同，具有广播能力的组控制器具备管理功能，包括新加入接点的身份验证和强制注销已有节点，只有通过组控制器的身份验证，新节点才可以加入当前组，强制注销节点被列入黑名单，完全排除在当前组之外。GC 通过广播成员过滤函数控制组密钥的更新，组内成员关系变化，GC 控制的成员过滤函数也相应改变，保证 GC 认可的节点才能获取组密钥。

作为其管理域内(所在组)的核心节点，组控制器另一项主要功能是负责管辖范围内组密钥的更新与分发，组控制器之间通过扩展 Diffie-Hellman 协议完成密钥加密密钥(KEK)的共享，KEK 则被用来在各组之间安全分发组密钥；在组密钥更新之前某一组控制器或者主动发起 KEK 协商或响应其他组控制器发起的 KEK 协商以便最终生成 KEK。

在详细描述HGKM方案之前，首先介绍文中出现的变量： N 为组控制器的个数； n_{ij} 为第 i 组内第 j 个节点，$j\in[1,t_i]$，这里 t_i 代表第 i 组 g_i 的节点总数；不失一般性，假设 n_{i1} 为 g_i 的组控制器。 K 为组控制器共同生成的密钥加密密钥； g_K 为所有成员共享的组密钥； p',p 为大素数，$p'=2p+1$； G 是模 p' 既约剩余系 $Z_{p'}^*$ 的真子群，α 是秩为 p的G的本原元，p, α 公开； x_i 为 第 i 个组控制器生成的秘密随机数，$x_i\in Z_p$； $g_{(i)1-j}$ 为第 i 组组内节点 n_{ij} 与组控制器之间共享的组内初始化密钥， $j\in[2,t_i]$； r_i 为第 i 个组控制器生成并保存的随机数，对普通节点严格保密，新节点加入或退出立即更换； $f_i(x)$ 为 n_{i1} 维护的成员过滤函数，$f_i(x)=\sum_{j=0}^{m}a_{(i)j}x^{m-j} \bmod p$。假设该组有 m 个节点，h 为单向散列函数；组控制器利用过滤参数集 $C_{(i)}=\{C_{(i)0},C_{(i)1},\cdots,C_{(i)m-1}\}$ 和 g_K 来构造 $f_i(x)$，构造公式如下：

$$f_i(x)=\prod_{j=0}^{m-1}(x-h(C_{(i)j}))+g_K \bmod p \tag{1}$$

3.1 初始化

在所有成员共享组密钥之前，必须进行初始化。在分级方案中，初始化过程分为 3 个阶段。

第 1 阶段首先进行组内Diffie-Hellman交换[8]，使组控制器与组内其它成员共享组内初始化密钥。在所有组内的普通节点和该组控制器之间共享 $g_{(i)1-j}$ 后，其中 $i\in[1,N],j\in[2,t_i]$；协议继续进入第 2 阶段。

第 2 阶段采用组间 Diffie-Hellman 交换进行组控制器之间的密钥协商，这里假设在发起协商之前各组控制器已完成身份认证，并确定之间顺序关系； n_{11} 作为第 1 个组控制器，g_i 组的组控制器 n_{i1} 作为第 i 个组控制器，以此类推。组间 Diffie-Hellman 交换由第 1 个组控制器发起，最后 1 个组控制器生成组密钥 g_K 并分发传给其他组控制器后结束，交互过程如下：

(1) n_{11} 产生随机的 x_1 计算 $\alpha^{x_1} \bmod p$，将结果发送到 n_{21}；

(2) n_{i1} 产生 x_i 并依次计算 $\alpha^{x_1x_2\cdots x_i} \bmod p$, $\{\alpha^{x_1x_2\cdots x_i/x_k} \bmod p \mid k\in[1,i]\}$, 这些值被送给下一个组控制器 n_{j1}，其中 $i\in[2,N-1]$, $j=i+1$;

(3) 若 $i\neq N-1$, $i=i+1$; 跳到第(2)步执行，否则继续；

(4) 最后一个组控制器n_{N1}收到前一个组控制器传来的中间值后，利用自己产生的随机数 x_N 计算组间共享密钥 K，另一半公钥 $\{\alpha^{x_1x_2\cdots x_N/x_i} \bmod p \mid i\in[1,N-1]\}$; 然后生成随机的组密钥 g_K 并向其它各组控制器发送一条广播消息：$\{\alpha^{x_1x_2\cdots x_N/x_i} \bmod p \mid i\in[1,N-1]\}$, $K+g_k \bmod p$, 其中 $K=\alpha^{x_1x_2\cdots x_N} \bmod p$ 是所有组控制器共享的一个密钥。

(5) 收到n_{N1}的广播后，组控制器n_{i1}利用自己保存的私钥 x_i 和收到的 $\alpha^{x_1x_2\cdots x_N/x_i} \bmod p$ 计算产生 K，然后解密组密钥 $g_K, i\in[2,N-1]$。

包含 5 个组控制器的组间密钥交换流程如图 1 所示。

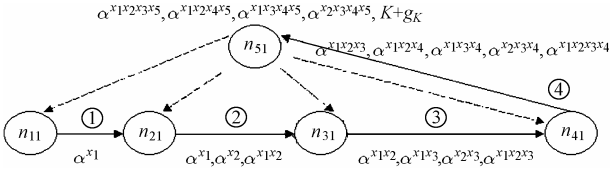

图 1 5 个组控制器间密钥交换消息流程

Fig.1 Message flow among five group controllers

在所有组控制器之间共享 K 和 g_K 后，每个组控制器分别在其控制域内进行第 3 阶段的密钥分发。在分发密钥之前，n_{i1}首先利用与普通节点之间共享的秘钥 $g_{(i)1-j}$ 构建过滤参数集 $C_{(i)},C_{(i)}$ 中每个元素的选择遵循下列条件：

$$\left.\begin{aligned} &C_{(i)0}=r_i \\ &C_{(i)j}=g_{(i)1-j'},\ j'=j+1,\ j\in[1,m-1] \end{aligned}\right\} \tag{2}$$

组控制器然后将 $f_i(x)$ 整理为标准形式 $f_i(x)=\sum_{j=0}^{m}a_{(i)j}x^{m-j} \bmod p$，最后在本组内广播整理后的 $f_i(x)$ 和 $h(g_K)$。

组内普通成员 n_{ij} 收到广播后，如果拥有 $g_{(i)1-j}$ 则计算 $x_{ij}=h(g_{(i)1-j})$，将 x_{ij} 作为变量代入式(1)中，得到的输出 y_i 就是组密钥 g_K：

$$\begin{aligned} y_{(i)} &= fi(x_{ij}) \\ &=(x_{ij}-h(r_i))\prod_{j=2}^{m}(x_{ij}-h(g_{(i)1-j}))+g_K \bmod p=g_K \end{aligned} \tag{3}$$

相反，如果某个节点没有与组控制器共享密钥，即使收到广播并选取随机数 x' 进行计算，只能得到一个无效值，无法获得组密钥。

组成员可以通过计算 $h(y_i)$，并与收到的 $h(g_K)$ 比较，判断是否获得正确的组密钥。在所有组 $g_i, i\in[1,N]$ 完成组内广

播后，整个网络所有节点共享一个密钥 g_K；任意两个节点或多个节点之间，可以使用该密钥对它们之间传送的消息进行加密保护。

3.2 新节点加入

Ad hoc 网络的一个重要特点是新节点可以随时加入网络，这对密钥管理提出了新的挑战。如果不改变组密钥，新成员加入后，可以使用 g_K 不受限制地访问截获的加密的旧消息，破坏消息的机密性。所以组成员关系发生改变后，有必要更换组密钥。

要加入 g_i 的新节点 n_{ix}，首先向组控制器n_{i1}提出加入申请；通过加入申请n_{i1}对新节点的身份进行必要认证，通过认证的节点获准加入当前组，否则被排除在当前组之外。获准加入的新节点与n_{i1}进行一次Diffie-Hellman交换，建立双方共享密钥 $g_{(i)1-x}$。

接下来n_{i1}产生新的组密钥 g'_K 并在整个网络内进行分发，在保证网络内所有节点安全接收更新的组密钥前提下，为提高分发效率，组密钥更新采取组内广播和组间广播两种形式：

组间广播针对网络内其它组控制器，广播的内容是 $K+g_Kg'_K \bmod p$；收到n_{i1}的广播后，其余组控制器首先利用自己保存的 K 解密，然后在其控制域内广播 $g_Kg'_K \bmod p$ 将新密钥 g'_K 安全分发给每一个普通节点。拥有旧密钥 g_K 的任意节点，均可以解密组控制器的广播消息来获取新密钥，实现组密钥的同步更新。

n_{ix}加入 g_i 后，该组的成员控制函数 $f_i(x)$ 必须改变以反映当前组内成员关系。组控制器首先改变过滤参数集 $C'_{(i)}=\{r'_i, g_{(i)1\text{-}2}, g_{(i)1\text{-}3}, \cdots, g_{(i)1\text{-}m}, g_{(i)1\text{-}x}\}$，接着利用式(1)重新构建成员控制函数 $f'_i(x)$ 并在本组内广播 $f'_i(x)$ 和 $h(g'_K)$。

组内所有成员包括新加入的节点因为和组控制器之间共享组内初始化密钥，可以从 $f'_i(x)$ 推导出新的组密钥 g'_K。需要指出一点：新节点只能获得 g'_K，无法得到旧密钥 g_K。

3.3 删除节点

由于某种原因(某个节点遭到恶意攻击或节点主动离开)，组控制器可能需要删除当前组内的节点。与新节点加入类似，此时也需更新组密钥以保证组密钥的独立性。

一种可能的做法是直接利用旧密钥来安全分发新密钥，这样做的不利之处在于无法阻止拥有旧密钥的节点通过非法窃听获取新密钥，分级方案采取了另外一种办法：

假设 n_{im} 被从 g_i 中删除，组控制器n_{i1}首先产生新组密钥 g'_K 并向全网分发。在开始组内分发密钥之前，n_{i1}重新生成 r'_i 并将元素 $\{g_{(i)1-m}\}$ 从过滤参数集 $C'_{(i)}$ 删除，然后基于式(4)重新计算成员过滤函数 $f'_i(x)$，n_{i1}最后广播成员过滤函数 $f'_i(x)$ 和 $h(g'_K)$ 实现控制域内组密钥的安全分发。除了节点 n_{im}，组内其他节点 n_{ij} 均能由 $f'_i(x)$ 推导出新的组密钥 g'_K。

$$f'_i(x)=(x-h(r'_i))(x-h(g_{(i)1-2}))(x-h(g_{(i)1-3}))\cdots(x-h(g_{(i)1-(m-1)}))+g'_K \bmod p \quad (4)$$

组控制器n_{i1}通过组间广播 $K+g_K+g'_K \bmod p$ 向其它组控制器分发新密钥。收到n_{i1}的组间广播消息后，第 j 组的组控制器n_{j1}首先解密获取新密钥 g'_K；然后生成新随机数 r'_j 并根据式(5)计算成员过滤函数 $f'_i(x)$，最后在本组内广播 $f'_i(x)$ 和 $h(g'_K)$ 来分发新组密钥 g'_K。

$$f'_i(x)=(f_j(x)-g_K)(x-h(r'_j))\big/(x-h(r_j))+g'_K \bmod p \quad (5)$$

3.4 组控制器变更

若某个组控制器离开或处于失控状态，出于安全考虑，必须隔离该组控制器，随之产生一个新问题——新组控制器如何产生。假设组 g_i 的组控制器 n_{i1} 被隔离，则该组内其它节点 $\{n_{ij} \mid 1<j\le m\}$ 开始选举产生新组控制器，选举主要依据候选节点的处理能力和安全特性，第 1 个符合条件的节点成为该组的组控制器 n'_{i1}。若通过选举依然无法产生新组控制器，则剩余节点移动到就近组控制器 $\{n_{j1} \mid j\ne i\}$ 周围，申请加入组 g_j。

选举产生新组控制器后面临组密钥更新问题。如果不更新 K，仍然使用 $K+g'_K \bmod p$ 分发新密钥，拥有 K 的 n_{i1} 照样可以获取 g'_K，密钥更换失去了意义。

本方案中组控制器变更后密钥变新是通过重新运行初始化协议实现的，除了新产生组控制器的组外，其它组无需运行第1阶段的初始化。n_{i1} 被排除在第2阶段初始化过程外，第 2 阶段初始化由第 1 个组控制器发起，最后一个组控制器生成组密钥 g'_K，向其它所有组控制器广播 $K'+g'_K \bmod p$。

第 k 组的组控制器 $\{n_{k1} \mid k\ne i\}$ 解密 g'_K 后，根据式(5)重新生成成员过滤函数 $f'_i(x)$，然后在组内广播 $f'_i(x)$ 和 $h(g'_K)$ 来分发新组密钥。

新组控制 n'_{i1} 运行第 3 阶段的初始化，利用与节点 $\{n_{ij} \mid 1<j\le m-1\}$ 共享的组初始化密钥构造新成员过滤函数，然后通过广播 $f'_i(x)$ 和 $h(g'_K)$ 在本组内安全分发 g'_K。

若隔离 n_{i1} 后剩余节点全部加入其它组，等同于多个新节点加入，限于篇幅不再重复。

3.5 密钥更新

密钥一般需要预先设定寿命，寿命过期之前，密钥必须立即更新。

组密钥的更新可以由任意组控制器发起，发起方同时负责生成新密钥 g'_K，然后在组内和组间广播 $g_K+g'_K \bmod p$。收到发起组控制器的广播消息后，各组控制器除了解密获取新密钥外，还继续在其控制域内广播该消息；对节点 n_{ij} 而言，无论是否处于发起组控制器的控制域，只要其拥有 g_K 就可以解密广播消息获取更新后的组密钥 g'_K。

4 方案分析

4.1 安全性

分级方案的安全性依赖于Diffie-Hellman交换和成员过滤函数的安全性。Diffie-Hellman交换的数学基础是有限域离散对数计算难题[8]，文献[4]还进一步指出根据Diffie-Hellman

判定假设：给定 Z_p 域内 3 个随机数 $a,b,c,<\alpha^a,\alpha^b,\alpha^c>$ 和 $<\alpha^a,\alpha^b,\alpha^{ab}>$ 是多项式不可分离的。

成员过滤函数实际上属于有限域模运算问题[9]。在第 i 组内，非法节点可以接收到广播的成员过滤函数 $f_i(x)$ 的标准形式： $a_0x^m+a_1x^{m-1}+\cdots+a_{m-1}x+a_m \bmod p$ ，其中的常数项为 $h(r_i)h(g_{(i)1\text{-}2})\,h(g_{(i)1\text{-}3})\cdots h(g_{(i)1\text{-}m})+g_K \bmod p$，除非非法节点拥有 $h(r_i)h(g_{(i)1\text{-}2})\,h(g_{(i)1\text{-}3})\cdots h(g_{(i)1\text{-}m})$, 否则无法从常数项中分离出 g_K。另一方面，非法用户即使获得某个过滤参数 $h(g_{(i)1\text{-}j})$ ，也无法利用单向的散列函数h，反向推导出 n_{i1} 与 $n_{i(j+1)}$ 间共享的密钥 $g_{(i)1\text{-}j}$，并进一步从 $f_i(x)$ 中推导出 g_K。

删除节点 n_{im} 后，即使该节点 n_{im} 保存了 $g_{(i)1-m}$， g_K 以及 $f_i(x)$，并通过窃听获取更新的成员过滤函数 $f_i'(x)$；由于 r_i 是每次更新的随机数，n_{im} 无法利用公式 $f_i'(x)-g_K' \bmod p=\left\{(f_i(x)-g_K)(x-h(r_i'))\Big/\left[\left(x-h(g_{(i)1-m})\right)(x-h(r_i)\right]\right\}\bmod p$ 计算获取 g_K' 。

由于 r_i 由组控制器产生并严格保密， n_{im} 即使移动到其他组也无法获取 g_K' 。首先它无法解密组间广播消息 $K+g_K+g_K' \bmod p$ 获取 g_K'; 其次由 $f_i'(x)$ 的计算式(5)可知，即使该节点在移动到 g_j 之前预先窃听了 $f_j(x)$ 并拥有旧密钥 g_K， 移动到 g_j 后又获取 $f_i'(x)$，没有 r_j 同样无法解密 g_K' 。

4.2 性能

无线Ad hoc网络的最大特点是节点不断移动，节点间链路情况不断变化。为了更好检验HGKM协议的实际性能，采用通用的ns-2 网络模拟软件[10]进行了模拟。

首先简要描述一下模拟环境：每个移动节点的物理特征(如无线网络接口的接收灵敏度和天线传输能力)与 AT&T Wave LAN 标准类似，节点最大移动速度 10m/s，节点等停时间为 5s。模拟空间随节点数量变化而变化，总模拟时间为 1500s。由于密钥管理方案属于高层应用，需要在 ns-2 提供的代码接口基础上编写应用 Agent。在实现过程中，节点间通信采用基于 UDP 协议的组播和广播。

无线 Ad hoc 网络规模以节点个数表征，在分级方案中节点总数为各组节点数之和。假设每个组控制器平均控制 4 个普通节点，则组控制器个数的变化就对应了网络规模的变化。组密钥的更新过程由新节点加入、离开或组控制器加入触发，触发节点随机选择。根据文献[11]，在 8 位微处理器的典型终端 512 位模幂运算大约耗时约 0.1s。因为远远小于通信延迟，协议运算对性能的影响可忽略不计。

当节点变化幅度为 5 节点个数从 25 变到 80 时，图 2—图 4 分别给出了普通节点加入、普通节点删除、组控制器删除情况下组密钥平均更新延迟变化曲线，这里组密钥平均更新延迟代表所有节点接收并解密 g_K' 所用时间的均值。上述 3 图中，HGKM协议分别与GDH.2 协议，CKD协议[12]比较了组密钥更新延迟。

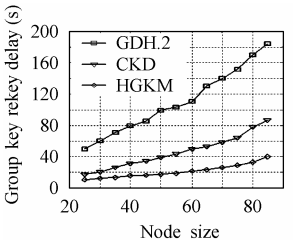

图 2 普通节点加入组密钥更新延迟

Fig.2 Group key rekey delay when new node join

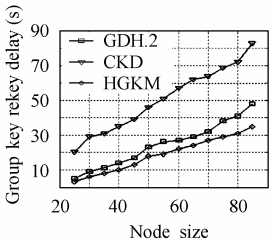

图 3 普通节点离开组密钥更新延迟

Fig.3 Group key rekey delay when node leaves

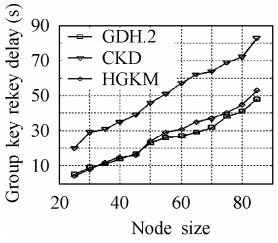

图 4 组控制器离开组密钥更新延迟

Fig.4 Group key rekey delay when group controller leaves

分析上述模拟结果可以发现，无论是新节点加入还是普通节点离开，分级方案的组密钥更新延迟要好于其它两种方案。这是因为，分级方案将较大的密钥分发范围细分为若干较小的分组，在每个分组内很好利用了处理能力强的移动节点——组控制器，减少了普通节点的处理负担，组密钥分发大量采用了广播的形式，有效减少了组密钥在传输过程中可能遇到的各种延迟，加速密钥的分发。

对于组控制器离开，因为只有 HGKM 协议存在组控制器，对其它两种协议比较采用普通节点离开条件下组密钥更新延迟的数据。当组控制器离开后，因为需要重新运行协议，分级方案与 GDH 2 性能基本相当，但优于 CKD 协议。

5 结束语

迅速发展的无线 Ad hoc 网对密钥管理提出了特殊的要求，文章在分析 Ad hoc 网的特性基础上，综合现有的解决方案，提出一种基于组控制器的分级组密钥管理方案(HGKM)。HGKM 方案在兼顾安全性的同时，采用灵活的分级成员管理方法，在组控制器和普通节点间不对称地分配运算量，有效控制了密钥管理对节点性能的影响。今后研究的重点是进一步提高效率。

致谢

本文在写作过程中得到胡正名教授、杨义先教授精心指点，特此致谢！

参 考 文 献

[1] Stajano F, Anderson R. The resurrecting duckling: security issues for Ad-hoc wireless networks. Proceedings of 7th International Workshop on Security Protocols, Berlin Germany, Springer-Verlag, 1999: 172−194.

[2] Fordigh M, Johansson P, Larsson P. Wireless Ad hoc networking

——the art of networking without a network. *Ericsson Review*, 2000: 125−131.

[3] Charles Perkins, Ad hoc networks. Addison Wesley Editions, 2001.

[4] Steiner M, Tsudik G, Waidner M. Diffie-Hellman key distribution extended to group communication. 3rd ACM Conference on Computer and Communications Security, New Delphi, India, 1996: 31−37.

[5] Jalel Ben Othman, Xiaoyun Xue. Security equipment in Ad hoc networks, IEEE VTC 2002: 1819−1823.

[6] Mike Burmester, Yvo Desmedt. A secure and efficient conference key distribution system. Advances in Cryptology-EUROCRYPT ’94, Perugia, Italy, 1994, 950: 275−286.

[7] Klaus Becker, Uta Wille. Communication complexity of group key distribution. Proc. 5th ACM Conference on Computer and Communications Security, San Francisco, USA, 1998: 1−6.

[8] Diffie W, Hellman M. New directions in cryptography. *IEEE Trans. on Information Theory*, 6(1976), 644−654.

[9] Kuen-Pin Wu, Shang-Jang Ruan, Feipei Lai, *et al*.. On key distribution in secure multicasting. 25th Annual IEEE Conference on Local Computer Networks, 2000: 208−212.

[10] Fengji Ye, Su Yi, Biplab Sikdar. Improving spatial reuse of IEEE 802.11 based ad hoc networks. GLOBECOM 200, IEEE Global Telecommunications Conference, 2003, 22(1): 1013−1017.

[11] Beller M J, Yacobi Y. Fully-fledged two-way public key authentication and key agreement for low-cost terminals. *Electronics Letters*, 1993, 29(11): 999−1001.

[12] Y. Amir, G Ateniese, D Hasse, *et al*.. Secure group communication in asynchronous networks with failures: Integration and experiments. IEEE ICDS, 2000: 330−343.

傅　坚：　男，1976 年生，工学博士，主要从事网络安全、网络运营支撑系统等方面研究.

张　翎：　男，1962 年生，高级工程师，长期从事传送与接入技术研究工作.