第34卷 第12期 计 算 机 工 程 2008年6月
Vol.34 No.12 Computer Engineering June 2008
·安全技术· 文章编号：1000—3428(2008)12—0135—03 文献标识码：A 中图分类号：TP309

Ad Hoc网络中的密钥管理策略

于行国[1]，冯昌盛[2]
(1. Motorola(中国)有限公司南京软件中心，南京 211102；2. 南京嘉环科技有限公司，南京 210002)

摘 要：作为一种无线移动自组织网络，移动Ad Hoc网的密钥管理与传统网络有很大差异，该文分析Ad Hoc网络密钥管理的特点，结合常用密钥管理机制，提出一种新型的密钥管理策略——YWCR，保证密钥管理的有效性，适用于Ad Hoc网络。实验结果证明了该策略的有效性。

关键词：Ad Hoc网络；密钥管理；YWCR策略

Key Management Strategy in Ad Hoc Network

YU Xing-guo[1], FENG Chang-sheng[2]
(1. Nanjing Software Centre of Motorola(China) Electronics Ltd., Nanjing 211102; 2. Nanjing Bestlink Technologies Co., Ltd., Nanjing 210002)

【Abstract】 Mobile Ad hoc network is a new kind of wireless mobile self-organization network. Its key management is quite different from that in traditional networks. Based on the properties of the key management in Ad Hoc network, it analyzes the used mechanism and proposes a new key management scheme——YWCR, which is effective and more suited to Ad Hoc network. Experimental results show that the strategy is effective.

【Key words】 Ad Hoc network; key management; YWCR strategy

Ad Hoc是一种新型的网络构架技术，由于移动Ad Hoc网络(Mobile Ad Hoc NETwork, MANET)大多运用于高安全需求领域，因此其安全性是焦点问题。作为诸多安全解决方案的关键，密钥的分配和管理得到了普遍的关注[1]。本文介绍了Ad Hoc网络中密钥管理的特点和常用的密钥管理机制，借鉴部分分布密钥管理机制的思想，提出YWCR策略。

1 Ad Hoc 网络中的密钥管理机制

1.1 Ad Hoc网络中密钥管理机制的特点

Ad Hoc网络具有网络安全需求高、网络拓扑结构多变、网络节点资源有限等特点。

因此，密钥管理机制具有以下3个特点[2]：

(1)安全性

Ad Hoc网络对于安全性要求很高，因此密钥管理机制必须提供足够的安全保证。所谓安全性，表现在网络中出现节点的恶意攻击时，攻破密钥的难度。难度越大，密钥管理机制的安全性越强，恶意节点窃听节点通信的可能性越小。

(2)节点移动性

在Ad Hoc网络中，各个节点高速运动，网络的拓扑结构不断变化，不会长时间固定在某一网络的节点。因此，密钥管理机制必须支持节点位置的动态变化。

(3)节点能源

在Ad Hoc网络中，各个节点使用电池或其他易损耗能源作为能量提供源，其计算能力和存储能力有限，因此，密钥管理机制必须最大限度地节省各个节点的能源。机制中的实施策略必须考虑数据的计算量和传输量，过于复杂的实施策略必然带来过多的能源消耗。

1.2 常用的网络密钥管理机制

(1)集中密钥管理机制

把网络中的信任关系集中在可信任的第三方认证服务器(Certificate Authority, CA)上。CA为节点颁发证书提供认证服务，各节点的私有密钥和公共密钥对在证书的基础上生成。

在该机制中，Ad Hoc网络采用单个CA作为第三方认证服务器，如果CA提供的服务不可用，节点将不能获得其他节点的公开密钥，从而导致网络信任关系瘫痪；如果CA被入侵，将有可能导致整个密钥管理系统的私密密钥全部泄漏，将给网络带来致命的威胁。可见，该机制的安全性比较差。

另外，由于需要确定的CA作为整个网络的认证基础，因此要求CA节点长时间固定在网络中，这限制了CA节点的可移动性。

(2)自发分布式密钥管理机制

为了解决单个CA带来的问题，文献[3]提出了一种自发分布式管理机制，这是一种完全自组织形式的机制，不需要CA的参与。

节点之间同样通过证书来建立信任关系，而证书的颁发是基于单个节点之间的互相信任，网络节点不需要扮演任何特殊角色。这种机制适合于自发的、完全自组织形式的Ad Hoc网络。

但是由于证书的签发完全依赖于用户之间的信任，因此恶意节点很容易通过伪造错误证书造成整个系统的破坏。

到目前为止，还没有提出安全有效的证书建立机制。

(3)部分分布密钥管理机制

该机制介于集中密钥管理机制和自发分布式密钥管理机制之间，基于分布式信任模型，将信任分布到多个节点，因此，不会因为单个CA而造成系统瓶颈。该机制引入CA集合

作者简介：于行国(1979－)，男，学士，主研方向：嵌入式系统，移动设备软件开发；冯昌盛，学士

收稿日期：2007-08-27 **E-mail：**royule@yahoo.com.cn

的概念，CA由一组选定的节点共同承担。模型由 2 个部分组成[4]：

(1)(N, T)门限 RSA 数字签名系统。

(2)普通节点。

在网络中，公开密钥 K 为所有节点共知，而私有密钥被分成 N 个部分，由(N, T)门限 RSA 数字签名系统中的 N 个节点分别拥。如果恶意节点试图得到网络的私密密钥，必须攻破所有 N 个 CA 集合节点。

虽然这种机制对系统的安全性有所加强，但是对于节点移动性的限制仍然存在：网络节点在建立安全通信的整个过程中，都需要 CA 集合提供认证服务。CA 集合节点固定，不能随意离开网络。

可以看出，Ad Hoc 密钥管理机制的成功与否，很大程度上取决于：在保证系统安全性的基础上，如何让机制适应网络节点的移动性。

笔者采用部分分布密钥管理机制的思想，提出了一种高效的密钥预分配策略——YWCR，使原有门限 RSA 数字签名系统在提供认证服务的同时，更加适合 Ad Hoc 网络，并对其实现细节进行了描述和评估。

2 YWCR 策略

YWCR 策略基于部分分布密钥管理机制。在系统的通信节点中建立私有密钥、公共密钥对，利用 RSA 数字签名的办法实现安全通信。将密钥的管理分成网络初始化和网络运行 2 个阶段。

在网络初始化阶段，主要工作如下：

(1)由担当门限 RSA 数字签名系统的 CA 集合产生系统的主密钥，将其信任分散到各个 CA 节点。

(2)CA 集合为网络中的节点生成私有密钥。

在网络运行阶段，节点通过计算，产生公共密钥，实现网络的安全通信。

2.1 系统主密钥的产生

YWCR策略中主密钥在网络初始化阶段由CA集合中的节点共同产生，其产生过程为：在Ad Hoc网络中，假设存在N个普通节点$\{n_1,n_2,\cdots,n_N\}$，每个节点有其相应的网络ID号。任意选择L个节点$\{R_1,R_2,\cdots,R_L\}$担当门限RSA数字签名系统，组成CA集合。每个CA集合中的节点R_i，采用BBS(Blum, Blum, Shub)随机数发生器产生随机数M_i，将L个随机数的集合$<M_1,M_2,\cdots,M_L>$作为系统的主密钥。

2.2 网络节点私有密钥的产生

网络节点的私有密钥也在网络初始化阶段产生。在描述其产生过程之前，首先给出 3 个定义：

定义 1(单路 Hash 函数) 具有以下性质的函数 H，对于任意给定值 x，可以计算 $y=H(x)$；同时，当给定 y 和函数 H 时，计算 x 的复杂度很大。

定义 2(多值函数) 具有以下性质的函数F，对于任意给定值x，可以计算$Y=F(x)$；Y是由$<y_1,y_2,\cdots,y_n>$组成的有序序列；其中，$y_i\in V$，V为函数的值域。

定义 3 对于序列$<M_1, M_2, \cdots, M_L>$，定义$M_i^j=H(H(H(H(M_i))))$，即对M_i利用单路Hash函数H进行j次Hash计算后得到的结果。

网络建立之初，整个网络系统共享节点的 ID 号集合和两个函数：单路 Hash 函数 H，多值函数 F。担当门限 RSA 数字签名系统系统的 CA 集合为节点 j 产生私有密钥的具体过程如下：

(1)利用多值函数F和ID_j产生$<j_1,j_2,\cdots,j_L>=F(ID_j)$。

(2)利用单路Hash函数和$<j_1,j_2,\cdots,j_L>$产生序列为

$<M_1^{j1}, M_2^{j2},\cdots,M_L^{jL}>$

其中，$<M_1, M_2,\cdots,M_L>$为系统主密钥。

(3)将$<M_1^{j1},M_2^{j2},\cdots,M_L^{jL}>=<K_j^1,K_j^2,\cdots,K_j^L>=K_j$发送给节点 j。

节点 j 的私有密钥即为

$<K_j^1,K_j^2,\cdots,K_j^L>=K_j$

2.3 通信节点公共密钥的产生

在网络运行阶段，必须为通信节点建立 RSA 认证的公共密钥，从而在节点之间建立信任认证，如图 1 所示。

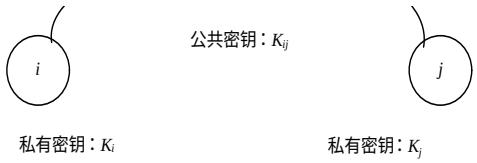

图 1 公共密钥的产生

节点 i、节点 j 生成公共密钥的过程如下：

(1)节点i、节点j交换各自ID号ID_i, ID_j。

(2)节点i计算$<j_1,j_2\cdots,j_L>=F(ID_j)$；节点$j$计算$<i_1, i_2,\cdots,i_L>=F(ID_i)$。

(3)节点 i、节点 j 生成新序列为

$<g_1,g_2,\cdots,g_L>$

其中，$g_i=\max(i_i, j_i)$。

(4)节点i、节点j在K_i, K_j的基础上计算序列，即

$<M_1^{g1},M_2^{g2},\cdots, M_L^{gL}>=<K_{ij}^1,K_{ij}^2,\cdots,K_{ij}^L>=K_{ij}$

对于节点j而言：如果$g_n=j_n$，则$K_{ij}^n=K_j^n$；如果$g_n>j_n$，则$K_{ij}^n=H\cdots H(K_j^n)$，即对$K_j^n$进行$g_n$-$j_n$次Hash运算的结果。

节点 i、节点 j 之间的公共密钥为

$<K_{ij}^1,K_{ij}^2,\cdots,K_{ij}^L>=K_{ij}$

2.4 密钥重组

为了加强YWCR密钥管理策略的安全性，防止恶意节点破坏网络的安全性，引入密钥重组机制[5]：

每隔时间段T，网络重新任意选择L个担当门限RSA数字签名系统的CA集合节点。由此，重新产生系统主密钥，并采用BBS(Blum, Blum, Shub)随机数发生器产生新的密钥：$<T_1,T_2,\cdots,T_L>$，重组网络安全认证。

3 YWCR 策略评估

从 Ad Hoc 网络密钥管理策略的 3 个特点(安全性、节点移动性、节省节点能源)对 YWCR 策略进行评估。

3.1 YWCR 策略安全性评估

密钥管理可分为 2 个阶段：

(1)网络初始化阶段

为了建立节点之间的安全通信，笔者引入了 4 个信息：单路 Hash 函数 H，多值函数 F，节点序列号 ID，CA 集合节点生成的系统主密钥。

前 3 个信息为网络中所有节点共享，网络的安全性能主要取决于系统主密钥。在 N 个网络节点中任意选择 L 个作为 CA 集合节点，节点单独生成主密钥为

$<M_1,M_2,\cdots,M_L>$

由于密钥M_i由单个节点生成，不需要与其他CA集合节点共享信息，因此在网络初始化阶段，如果存在恶意节点试图

获取密钥信息，必须正确地攻击L个CA集合节点。成功的概率为

$$r(N,L)=\binom{L}{N}\xi^{L}(1-\xi^{N-L}) \tag{1}$$

其中，$\xi=L/N$。对于 Ad Hoc 网络，N 表示网络结构大小，L 表示 CA 集合的大小，N 越大，L 越小，直接攻破的概率越小，所以，YWCR 策略更加适合节点较多、结构较大的网络。而当 L=1 时，YWCR 策略退化成集中密钥管理机制。

(2)网络运行阶段

恶意节点的攻击主要体现在攻破通信节点的公共密钥，对通信信息进行监听。因为 L 值体现了私有密钥和公共密钥对的位数，所以其直接决定了攻破概率的大小。对于穷举攻击而言，概率为

$$r=2^{-L} \tag{2}$$

根据式(1)和式(2)，得出结论：YWCR策略的安全性能主要取决于L值，称L为策略中的安全因子。当安全因子L=64，节点个数为 1×10^{6}时：

(1)计算式(1)，得出概率约为 1.3×10^{-41}；

(2)计算式(2)，概率为 $2^{-64}<10^{-20}$。

YWCR 策略适合于高安全需求的 Ad Hoc 网络。

3.2 YWCR 策略移动性能评估

YWCR 策略在网络初始化时任意选取 L 个节点作为门限 RSA 数字签名系统的 CA 集合节点，以此为基础实现安全通信。在网络运行阶段，由通信节点各自产生公共密钥，不再需要 CA 集合节点提供认证。

对于 CA 集合节点移动性的限制只在网络初始化和网络进行密钥重组时产生，网络初始化完成，进入运行阶段时，各个节点不需要扮演任何特殊角色。因此，YWCR 策略适合于自发的、完全自组织形式的 Ad Hoc 网络。

3.3 YWCR 策略能源消耗评估

YWCR 策略的计算量和数据传输量具有以下局限：

(1)对于数据的计算量，引入的 BBS 随机数发生器、单路 Hash 函数、多值函数计算简单、计算量小，可以在短时间内完成。

(2)对于网络数据传输量，网络初始化时，需要传输各个节点的私有密钥，即

$<M_1,M_2,\cdots,M_L>$

大小由安全因子 L 决定，当 L=64 时，传输的数据即为 64 位，网络运行时，设置各个节点的 ID 号为 8 位，为了生成通信节点的公共密钥，传输的数据即为 8 位。

通过模拟实验来观察 YWCR 策略实施前后网络中能源消耗的情况。

实验采用：

(1)NS-2 模拟器；

(2)仿真环境：

1)节点个数：30；

2)节点所处空间：2 000×2 000 m^2。

(3)传输能量：14 dBm；

(4)模拟时间：300 s；

(5)MAC 层协议：802.11 协议。

在网络层实现 YWCR 策略时，简单起见，忽略恶意节点的攻击。

如图 2 所示，选择网络中 4 个节点进行比较，虚线为没有加入 YWCR 密钥管理策略时各个节点消耗能源的情况，实线为加入后的情况。

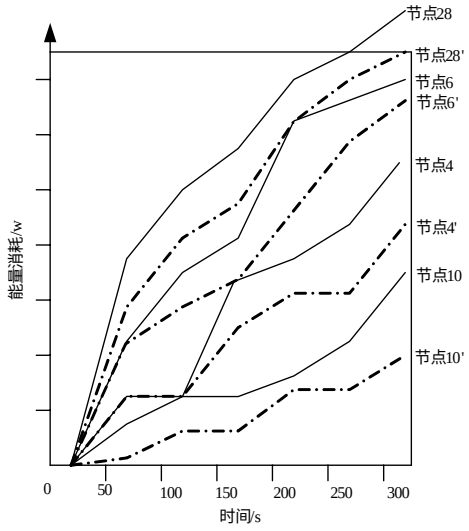

图 2 能源消耗的对比

可以看出，各个节点的能源消耗并没有因为 YWCR 策略的加入而明显增加。因此，YWCR 适合于节点能源有限的 Ad Hoc 网络。

4 结束语

Ad Hoc 网络的安全性研究主要集中在两个方面：安全的路由技术和密钥管理技术。而作为诸多安全机制核心的密钥管理技术大多针对某种具体应用环境提出。因此，缺乏普遍适合于 Ad Hoc 网络的有效密钥管理机制。YWCR 策略通过简单函数的方法在节点之间建立公共密钥和私有密钥，为网络安全通信奠定了牢固的基础。

参考文献

[1] Wu Bing, Wu Jie. Secure and Efficient Key Management in Mobile Ad Hoc Networks[C]//Proceedings of the 19th IEEE International Parallel and Distributed Processing Symposium. Colorado, USA: [s. n.], 2005: 17.

[2] George C. A Framework for Key Management in Mobile Ad Hoc Networks[C]//Proceedings of the International Conference on Information Technology: Coding and Computing. Las Vegas, Nevada, USA: [s. n.], 2005: 568-573.

[3] Capkun S. Self Organized Public-key Management for Mobile Ad Hoc Networks[C]//Proceedings of ACM International Workshop on Wireless Security. [S. l.]: ACM Press, 2003: 52-64.

[4] Jing Deng, Richard H, Mishra S. A Performance Evaluation of Intrusion-tolerant Routing in Wireless Sensor Networks[C]//Proc. of the IEEE 2nd International Workshop on Information Processing in Sensor Networks. Palo Alto, CA, USA: [s. n.], 2003: 33-41.

[5] Ramkumar M, Memon N. An Efficient Key Predistribution Scheme for Ad Hoc Network Security[J]. IEEE Journal on Publication. 2005, 23(3): 611- 621.