分簇 Ad Hoc 网络的密钥管理*)

李光松　韩文报
(信息工程大学信息研究系　郑州 450002)

摘　要　Ad Hoc 网络可以不依赖于现有网络基础设施，快速搭建起一个移动通信网络，然而其灵活特性又使其安全性面临着严峻的挑战。密钥管理是 Ad Hoc 网络安全的关键技术，本文首先回顾了 Ad Hoc 网络密钥管理方面的研究，然后基于分簇的网络结构给出了一种新的 Ad Hoc 网络密钥管理方案。方案使用了身份签密的密码算法，不需要公钥证书的存在，用户以其身份标识作为公钥，有效地降低了用户终端计算、存储能力的需求和系统密钥管理的通信开销。基于分簇的结构将网上节点分成一些相对独立的自治域，既提高了安全服务的可用性和可扩充性，也便于对某些紧急情况快速做出反应。

关键词　Ad Hoc 网络，密钥管理，基于身份的密码体制，签密

Cluster-Based Key Management in Ad Hoc Networks

LI Guang-Song　HAN Wen-Bao
(Department of Information Research, Information Engineering University, Zhengzhou 450002)

Abstract　Ad hoc networking can quickly put up a wireless mobile communication network without conventional network infrastructures. However, its flexible characteristics make security a challenge. Robust key management services are central to ensuring privacy protection in wireless Ad Hoc network settings. This paper firstly makes a survey of the recent works about key management for Ad Hoc networks. A new scheme for key management is proposed for cluster-based Ad Hoc networks using id-based signcryption. In this scheme, public key certificates are not needed and every participant can use his identity as public key. It greatly decreases the need of the ability for compution and storage of clients' terminals, as well as communication cost for system key management. Nodes are divided into several autonomous communities based on cluster structure, which not only increases availability and scalability of networks, but also results in quick response to some emergency.

Keywords　Ad Hoc networks, Key management, Identity-based cryptograph system, Signcryption

1　引言

Ad Hoc 网络是一组带有无线收发装置的移动终端组成的多跳的临时性自治系统。它是一种新型无线移动网络，在这种环境中，两个因传输距离有限而无法直接通信的终端可以借助其它终端的分组转发进行通信。它可以在没有或不便利用现有网络基础设施的情况下，通过移动节点间的相互协作快速构建起一个移动通信网络，可广泛应用于教学、医疗、救援、抢险及军事通信等环境中。尤其在未来战场上，Ad Hoc 网络对于高效指挥、协同作战和提高部队机动性具有非常重要的意义。Ad Hoc 网络具有以下主要特征：(1)不依赖于现有网络基础设施；(2)动态变化的网络拓扑结构；(3)网络的分布式控制；(4)链路带宽受限；(5)移动终端的局限性，如计算和存储能力以及供电等。一方面，因为构建费用低廉，使得 Ad Hoc 网络应用有极大的吸引力；另一方面，它的灵活特性给其安全性又带来了巨大的挑战。目前，对于传统的有线或无线网络，已经有了比较完善的安全防护方案，但是 Ad Hoc 网络的特性使得那些方案不能直接应用到 Ad Hoc 网络中。

Ad Hoc 网络是一种特殊的无线网络，不仅面临着传统网络所受到的安全威胁，而且面临着自身一些特殊的安全威胁，主要表现在以下几个方面：

- 无线链路上传输的信息很容易受到窃听、篡改等攻击。
- 移动节点有可能漫游到敌对环境中被俘获破坏，恶意攻击不仅来自网络外部，也有可能来自内部，破坏节点。
- 网络拓扑结构和移动节点数目不断变化，节点的信任关系也随之变化，特别是有节点被检测出为破坏节点时。
- 网络决策和算法的执行往往需要多个节点协作实现，攻击者可以针对协作过程实施新类型的攻击，破坏协作的完成。

Ad Hoc 网络的安全性面临着严峻的挑战，而密钥管理是 Ad Hoc 网络安全的核心技术。在 Ad Hoc 网络中，没有单个可信任的节点，不能像传统网络利用一个在线的可信任的证书机构(Certificates Authority，简称 CA)来实现系统的密钥管理。Zhou 在文[1]中提出了一种基于门限密码体制[2]的部分分布式 CA 密钥管理方案，将 CA 的功能分配给多个节点，这些节点协作构成一个虚拟 CA，完成系统的密钥管理。Luo 假定网络节点相同并且完全对等，给出一种完全分布式 CA 的密钥管理方案[3,4]。网络中所有节点都是服务节点，均持有系统私钥分量。完全分布式 CA 方案尽管在一定程度上提高了系统服务的可用性，但是因为每个节点都持有系统私

*)国家自然科学基金资助项目(No. 19971096, No. 90104035)。李光松　博士研究生。研究方向：密码理论、信息安全；韩文报　教授，研究方向：密码理论、信息安全、数论、代数编码。

钥分量，显然使系统的安全性降低。Hubaux 提出一种完全自组织的密钥管理[5,6]，该方案类似于 PGP 信任模型，不需要可信任的 CA。公钥证书的发放是用户的个人行为，两个用户想认证对方公钥时，他们寻找连接双方的证书链。这个方案的优点在于不需要赋予节点特殊的职责，但是在进行用户认证时，连接双方的证书链却不一定能找到，而且较长的证书链可信度很低。利用基于身份的密码体制并结合门限密码体制，Khalili[7]给出一种基于身份的密钥管理机制。在组网时，由 n 个节点分布式生成系统的公钥和私钥，这些节点称为 PKG 节点。系统私钥采用 (n, k) 门限秘密共享的方式为 n 个 PKG 节点共有。分布式的 PKG 节点充当服务节点协作，为用户发放与其身份相应的私钥。用户以身份标识 ID 作为公钥，不需要公钥证书。但是在这种方案中，由 n 个节点协作生成系统密钥，容易受到中间人攻击，恶意用户可以给新入网成员假的系统公钥，而其拥有相应私钥；组网时没有可信任方的参与，不适用于需要较高安全性的网络；该方案也没有给出用户私钥的更新方式。文[8]中我们利用基于身份的签密体制和门限体制给出一种密钥管理方案，解决了用户私钥定期更新的问题，并给出一种新的通信协议，降低分布式更新用户私钥带来的通信开销。但是，由于门限体制的固有缺点，系统通信开销仍很大，并且如果网络拓扑变化频繁，需要更新私钥的用户很可能无法联系足够多的服务节点完成更新。

上述的密钥管理方案采用的都是平面结构，不具有很好的可扩充性，不适合大规模网络。本文不再使用门限体制，利用基于身份的签密机制给出了一种分簇的 Ad Hoc 网络密钥管理方案，提高了安全服务的可用性和可扩充性，适用于大规模的 Ad Hoc 网络。

2 网络模型和假设

Ad Hoc 网络一般有两种结构：平面结构和分级结构。

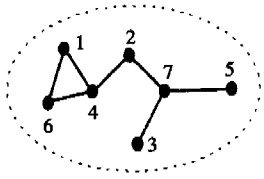

图 1 平面结构

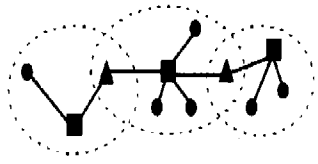

图 2 单频分级结构

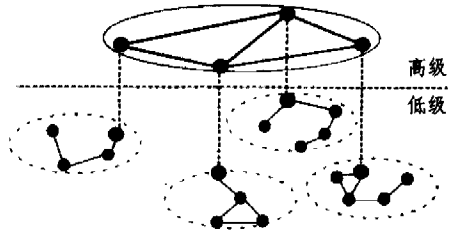

图 3 多频率分级结构

为了使密钥管理方案具有可扩充性，提高安全服务的可用性，我们面向分级结构的 Ad Hoc 网络，给出一种分簇的 Ad Hoc 密钥管理方案。我们的方案采用的是图 3 所示的双频两级网络，与以前的方案相比，在保证安全性的同时更灵活，便于用户私钥的更新。我们的网络模型基于如下假设：

(1)存在一个离线的可信任机构；

(2)网上的节点性能是不同的，存在一些性能优良并且物理安全性高的节点；

(3)网络中节点数目是可变的，不断有新的节点离开或加入网络；

(4)每个节点都具有某种监视机制[9]，可以监视网络的异常情况，尤其是其一跳邻居节点的行为。

网上的节点划分成多个簇，每个簇都有一个控制节点即簇头。这个控制节点性能优于其它节点，包括计算和存储能力、功率和传输范围等，它还具有相对好的物理安全性。网络平面结构中，所有节点的地位平等，也称为对等式结构。而分级结构中，网络被划分为簇，每个簇由一个簇头和多个簇成员组成。簇头节点形成高一级的网络，负责簇间数据的转发。

平面结构(图 1)的网络比较简单，网络中所有节点是对等的，原则上不存在瓶颈，所以比较健壮。平面结构的最大缺点是网络规模受限。网络规模越大，路由维护的开销就越大。当网络的规模增加到某个程度时，所有的带宽都可能会被路由协议消耗掉。分级结构的最大优点是可扩充性好，可以通过增加簇的个数或级数来提高网络的容量。分级结构(图 2 和图 3)中，簇内成员的功能比较简单，基本上不需要维护路由，这大大减少了网络中路由控制信息的数量。簇头节点复杂一些，它要维护到达其它簇头的路由，还要知道所有节点与簇的从属关系。但总的来说，在相同网络规模的条件下，路由开销要比平面结构的小。分级结构是无中心和有中心模式的混合体，可以采用两种模式的技术优势。虽然采用分级结构后网络有了相对的控制中心—簇头，但是簇头和簇成员是动态变化的，节点仍是自动组网的。

根据不同的硬件配置，分级结构可分为单频分级和多频分级两种。单频分级网络(图 2)只有一个通信频率，所有节点使用同一个频率通信；为了实现簇头之间的通信，要有网关节点(同时属于两个簇的节点)的支持。簇头和网关形成高一级的网络，称为虚拟骨干。而在多频率分级网络中(图 3)，不同级采用不同的通信频率。低级节点的通信范围较小，高级节点要覆盖较大的范围。高级节点同时处于多个级中，有多个频率，用不同的频率实现不同级的通信。在图 3 所示的两级网络中，簇头节点有两个频率：频率 1 用于簇头与簇成员的通信，频率 2 用于簇头之间的通信。军事通信中，一般采用分级的 Ad Hoc 网络，高级节点有多个通信频率。

中普通节点分属于这些簇，类似多个自治域，由簇头节点负责本簇节点的密钥管理；簇头与簇成员的从属关系可以是动态的，一个簇的成员也可以加入其它的簇。簇头节点构成高一级的网络，簇头节点之间是对等的。为了使系统对某些紧急情况可以迅速做出反应(有些场合下，需要对恶意节点迅速做出反应，使损失减到最小，如战场、抢险等)，本文不再使用门限体制，而是赋予簇头节点一定的自治权力，对簇内节点的安全性实施有效的控制。假定簇头节点有较大的功率，互相都在对方的通信范围之内，可以直接通信。

3 基于身份的签密体制

这节中我们简要介绍本文所使用的 Boyen[10]基于身份的签密体制。设 G_1 和 G_2 是两个阶为素数 p 的群，群的运算用乘法表示，G_1 和 G_2 两个群的单位元都用 1 表示。假定离散对数问题在两个群上都是困难的。

定义 1 设 g 是 G_1 的生成元，映射 $e:G_1\times G_1G_2$，称为双线性对映射，如果 e 满足下面的性质：

(1)双线性：$e[x^a,y^b]=e[x,y]^{ab}$，对于 $\forall x,y\in G_1$，$\forall a,b\in Z$；

(2)非退化性：$e[g,g]\neq 1$，即它是 G_2 的生成元；

(3)可计算性：存在一种算法，对于所有 $x,y\in G_1$ 都可以有效地计算 $e[x,y]$。

定义 2 双线性 Diffie-Helleman 问题(BDH 问题)。设 g 是 G_1 的生成元，随机选择 $a,b,c\in F_p^*$，给定 $g^a,g^b,g^c\in G_1$，计算 $e[g,g]^{abc}$。

BDH 问题在某些椭圆曲线群上是困难的，即没有多项式时间的算法能解决 BDH 问题。利用 BDH 问题的困难性，Boyen 给出了一种有效的基于身份的签密体制。该体制中用户不需要使用公钥证书，直接使用身份标识作为公钥，可以实现不可否认的保密通信；签名方案可独立使用，认证用户的身份。该方案基于椭圆曲线群的运算，与其它密码体制相比较，有较短的签名长度、密文长度。

假定有一个可信任的密钥生成机构 PKG(Private Key Generation Service)，为系统和用户生成密钥。PKG 构造上述的 p 阶群 G_1,G_2，使得 BDH 问题是困难的。设 $e:G_1\times G_1\to G_2$，是双线性对映射，g 是 $G1$ 的生成元，随机选择 $\sigma\in F_p^*$，令 g^σ 作为系统公钥，σ 作为系统私钥。PKG 选择 5 个 Hash 函数：

$H_0:\{0,1\}^*\to G_1^*$，$H_1:G_1^*\times\{0,1\}^*\to F_p^*$，$H_2:G_2^*\to\{0,1\}^{\lceil\log p\rceil}$，$H_3:G_2^*\to F_p^*$，$H_4:G_1\to\{0,1\}^*$，公开参数$\{G_1,G_2,p,e,g,g^\sigma,H_0,H_1,H_2,H_3,H_4\}$。设用户身份标识为 $ID\in\{0,1\}^*$，则其对应私钥如下计算：$i_{ID}=H_0(ID)$，$d_{ID}=(i_{ID})^\sigma$，d_{ID}为用户的私钥。

假设用户 A 欲给用户 B 发送签密的消息 m，用户 A 和用户 B 身份标识分别为 ID_A,ID_B，相应的私钥分别为 d_A,d_B。下面算法中⊕表示模 2 加，H_4 输出看作比特流。

签名算法：

对于用户 A，$i_A=H_0(ID_A)$，$d_A=i_A^\sigma$，

随机选取 $r\in F_p^*$，令 $j=i_A^r\in G_1^*$，计算 $h=H_1[j,m]\in F_p^*$，$v=d_A^{r+h}\in G_1$

A 对消息 m 的签名为$\langle j,v\rangle$。

加密算法：

计算 $i_B=H_0(ID_B)$，$u=e[d_A,i_B]\in G_2^*$，$k=H_3[u]\in F_p^*$，

令 $x=j^k\in G_1^*$，$w=u^{kr}\in G_2^*$，计算 $y=H_2[w]\oplus v$，$z=H_4[v]\oplus\langle ID_A,m\rangle$

A 对消息 m 加密后的密文为$\langle x,y,z\rangle$

解密算法：

B 收到密文$\langle\hat{x},\hat{y},\hat{z}\rangle$，计算 $\hat{w}=e[\hat{x},d_B]$，

恢复 $\hat{v}=H_2[\hat{w}]\oplus\hat{y}$，$\langle\hat{ID}_A,\hat{m}\rangle=H_4[\hat{v}]\oplus\hat{z}$，$\hat{i}_A=H_0(\hat{ID}_A)$，

计算 $\hat{u}=e[\hat{i}_A,d_B]$，$\hat{k}=H_3[\hat{u}]$，$\hat{j}=\hat{x}^{\hat{k}^{-1}}$

输出消息 $\hat{m}$、签名$\langle\hat{j},\hat{v}\rangle$和恢复的发送者身份 $\hat{ID}_A$

验证签名：

由上得到 $\hat{i}_A=H_0(\hat{ID}_A)$，再计算 $\hat{h}=H_1[\hat{j},m]$

检验 $e[g,\hat{v}]=e[g^\sigma,(\hat{i}_A)^{\hat{h}}\hat{j}]$是否成立，

如果成立，验证通过，消息为用户 A 发送，否则断定消息并非用户 A 发送。

上面的方案中，签名算法可独立使用，在消息不需要保密但是需要其他用户确认发送消息的用户身份时，只使用签名算法，不必要对消息加密。另外，如果只需要消息的完整性和匿名保密通信时，可以用公开参数$\langle g,g^\sigma\rangle$替代$\langle i_A,d_A\rangle$的使用，由于 $d_A=i_A^\sigma$，所以算法中的关系均成立，从而可以保证消息的完整性和匿名的保密通信。

4 分簇的密钥管理

在本节中，我们利用 Boyen 的签密体制，给出一种分簇的 Ad Hoc 网络密钥管理方案。这里我们采用的是一种双频分级的分簇网络结构。本文的密钥管理方式是一种中心化与分布式相结合的混合模式。为了获得有效性，簇内密钥管理采用的是中心式的模式，由簇头节点管理。簇头节点因具有良好性能的设备，是相对独立的，采用分布式协商方式生成会话密钥获得保密性，可以减小单点失效带来的危害。

4.1 初始化

组网时，为网络配置 n 个性能优良的节点，这些节点有相当强的计算能力、存储能力和功率，物理安全性较好，并且使用两个通信频率。由这些节点充当簇头节点，建立一个两级的网络。例如在战地环境中，存在通信车、装甲车、士兵用通信终端等多类移动节点，性能优良的节点如通信车、装甲车这样的设备，可以充当簇头节点。网上节点按位置或业务分为 n 个簇，分别归属于这些簇头节点。簇头与簇头之间通信使用一个频率，簇头与簇内节点通信使用另外一个频率。

每个簇以簇头的标识作为簇的标识，例如一个簇头节点的标识为 CH，则它所在的簇标识为 CH。每个簇成员节点有一个唯一的网上身份标识 ID。

离线的可信任机构(称为 PKG)，生成系统的主密钥 σ 和公钥 g^σ。簇头节点拥有三个私钥：高级私钥、簇主密钥、低级私钥。高级私钥用于簇头节点间的安全协议以及簇头与初入网节点的认证。离线的 PKG 为所有簇头节点生成高级私钥。设一个簇头节点身份标识为 CH，其高级私钥如下生成：$i_{CH}=H_0(CH)$，$d_{CH}=(i_{CH})^\sigma$，d_{CH}为这个簇头的高级私钥。假定网上共有 n 个簇 CH_j，$j=1,2,\cdots,n$。每个簇头节点 CH_j 分别选择一个随机的簇主密钥 σ_j，簇的公钥为 g^{σ_j}，$j=1,2,\cdots,n$。簇主密钥用于簇内节点私钥的生成和更新。低级私钥用于和簇内节点的认证和加密。簇头节点的低级私钥为：$d_{ch}=(i_{CH})^{\sigma_j}$。

入网前普通用户都必须到 PKG 处注册身份，PKG 认证用户的身份，然后由系统私钥 σ 和用户的身份 ID 计算供用户短期使用的私钥 d_{ID}。计算方法如下：$i_{ID}=H_0(ID)$，$d_{ID}=(i_{ID})^\sigma$。PKG 把这个私钥以及系统公钥 g^σ 秘密分发给用户。

4.2 新节点加入和私钥更新

每个簇头节点 CH_j 周期性地广播簇的信令消息，包括簇头信息、簇公钥、簇时钟 t，使用高级私钥 d_{CH} 对上述信息的签名。Cluster-message$=\{CH_j,g^{\sigma_j}$，簇内时钟 t，前面信息的签名$\}$。我们的方案使用上一节中基于身份的签密方案。该方案中的签名方案可独立使用，不必对签名的消息进行加密。由于系统不需要公钥证书，任何人都可以由节点的身份标识和系统公钥 g^σ 验证签名。通过检验签名的正确性，可以认证节点的身份。簇成员节点都保存有系统公钥 g^σ，可以验证信令消息的真实性。

新节点 A 从离线可信任机构注册后入网，注意侦听簇头的信令消息，寻找自己需要加入的簇。如果接收到需要的簇头信息，首先利用系统公钥 g^σ 和簇头身份验证一下消息的真

实性，然后向簇头节点发出加入申请。因为普通节点与簇头节点之间的链路是非对称的，申请消息不能直接到达簇头节点，需要其它节点转发。申请节点 A 与簇头节点 CH_j 使用签名算法执行一个双向的 Challenge-Response 协议，相互认证对方身份。

A 的申请消息：{A，JOIN 标志，随机数 r_1}，A 发送申请消息给 CH_j。

CH_j 收到申请消息后发送响应消息到 A。响应消息为{CH_j，随机数 r_1，随机数 r_2，前面信息的签名}。这里签名的计算使用高级私钥 d_{CH}。

A 验证消息，如果正确则发送回应消息{A，随机数 r_2，前面信息的签名}。这里的签名使用的是离线信任机构产生的私钥 d_A，其中 $d_A=(i_A)^{\sigma}$，$i_A=H_0(A)$。

CH_j 接收并验证消息，若正确则允许节点 A 加入，并为其产生以后使用的私钥。网络的生存时间按 T 分成若干时间段，假定当前时段为 T_m。节点 A 此时使用临时身份 $A\parallel T_m$，也即当前时段 A 的公钥。簇头据此计算出节点当前时段使用的私钥 $d'_A=(i'_A)^{\sigma_j}$ 其中 $i'_A=H_0(A\parallel T_m)$。簇头将 A 的私钥 d'_A 用 d_{CH} 和 A 的公钥 i_A 签密后，发给节点 A。

节点 A 利用 d_A 解密并验证其正确性，以防止消息被恶意篡改。如果上述过程都验证通过，节点 A 便加入了簇。节点 A 销毁原来离线机构分发的私钥，以后使用 CH_j 分发的私钥。CH_j 维护一张本簇成员列表，在表中添加节点 A。

节点 A 使用的私钥由 CH_j 定期更新，在私钥有效期到期之前 CH_j 为节点 A 生成下一时段使用的私钥，用低级私钥 d_{ch} 签密后发送给节点 A。簇主密钥 σ_j 也可以定期由 CH_j 更换，若 σ_j 更换，CH_j 需要为簇内节点生成新的私钥并秘密分发。

4.3 节点的漫游

簇头节点互相在通信范围之内，它们周期性交换时钟信息、簇公钥和簇成员信息。本文约定采用最快的时钟，以达到系统的同步。

当一个簇 CH_1 的成员节点 A 移动到另外一个簇 CH_2 的范围内，也就是说节点 A 收到了簇头 CH_2 的簇信令信息或簇 CH_2 成员节点的信息。如果 A 需要加入簇 CH_2，执行下面的过程：

A 首先向簇头 CH_2 发送一个申请消息：{A，JOIN 标志，归属簇 CH_1，随机数 r_1}。簇头 CH_2 收到申请消息后发送响应消息到 A。响应消息为{CH_2，随机数 r_1，随机数 r_2，前面信息签名}。这里的签名的计算使用低级私钥 d_{ch2}。

A 利用 CH_2 簇公钥 g^{σ_2}、当前时间段 T_m 和 CH_2 的身份验证消息，如果正确则发送回应消息{A，随机数 r_2，前面信息签名}。这里的签名使用的是 CH_1 为 A 产生的私钥。

CH_2 接收消息后，用 CH_1 的簇公钥 g^{σ_1} 和当前时间段 T_m，以及 A 的身份验证消息，若正确允许节点 A 加入。CH_2 计算出当前时间段 A 应该使用的私钥 $d_A=i_A^{\sigma_2}$，$i_A=H_0(A\parallel T_m)$。由 3 节最后一段所述，CH_2 可利用$\langle g,g^{\sigma_1}\rangle$将生成的私钥加密发送给 A。

节点 A 解密后，检验 $e[i_A^{\sigma_2},g]=e[i_A,g^{\sigma_2}]$是否成立，以验证收到的私钥的正确性，防止信息被恶意篡改。

如果上述过程都验证通过，节点 A 便加入了簇 CH_2。

4.4 端到端保密通信

网上两个用户 A、B 要进行保密通信时，分下面两种情况获得一次性会话密钥：

在同一簇 CH_j 内

(1)协商会话密钥

方式一：设 δ 是 F_p^* 的生成元，A 随机选择 $x\in F_p^*$，计算 δ^x，并用私钥对 δ^x 做签名，将 δ^x 和对它的签名发给 B。B 随机选择 y，计算 δ^y，用私钥对其签名，将 δ^y 和对它的签名发送给 A。A 和 B 收到消息后，先验证对方的签名。如果与对方身份相符，则分别计算$(\delta^y)^x$ 和$(\delta^x)^y$，作为会话密钥。

方式二：A 随机选择 $x\in F_p^*$，计算 i_A^x 发送给 B；B 随机选择 y，计算 i_B^y 发送给 A。A 和 B 收到消息后，分别计算 $e[d_A,i_B^y i_B]$和 $e[i_A^x i_A,d_B]$，作为会话密钥。易验证 $e[d_A,i_B^y i_B]=e[i_A^x i_A,d_B]$。

(2)由一方生成会话密钥　由 A 或 B 一方生成随机的会话密钥，并对会话密钥和时间戳签密，发送给对方。

(3)利用非交互的共享秘密　A 和 B 分别计算 $e[d_A,i_B]$、$e[i_A,d_B]$，易验证 $e[d_A,i_B]=e[i_A,d_B]$。A 和 B 用 $e[i_A,d_B]$作为共享秘密信息，记为 k。把 k 作为加密密钥的密钥，采用对称加密方式交互形成会话密钥。设 E 为双方采用的对称加密算法，k_s 为双方协商生成的会话密钥，h 为强的单向 Hash 函数。采用下面的协议生成会话密钥 $k_s=h(n_1,n_2)$，n_1 为 A 选择的随机数，n_2 为 B 选择的随机数。该协议是一个认证的密钥协商协议。

$A\rightarrow B$：A，$E_k(A,n_1)$

$B\rightarrow A$：B，$E_k(B,n_{1+1},n_2)$

$A\rightarrow B$：$E_{k_s}(n_2+1)$

不在同一簇内

假定 A 在簇 CH_1 内，B 在簇 CH_2 内，可通过如下方式建立会话密钥：

(1)协商会话密钥　设 δ 是 F_p^* 的生成元，A 随机选择 $x\in F_p^*$，计算 δ^x，并用私钥对 δ^x 做签名，将 δ^x 和对它的签名发给 B。B 从 CH_2 获得 CH_1 的簇公钥 g^{σ_1}，用 g^{σ_1} 和 A 的标识可验证 A 的签名。如果正确，B 随机选择 y，计算 δ^y，用私钥对其签名，将 δ^y 和对它的签名发送给 A。A 收到消息后，从 CH_1 获得 CH_2 的簇公钥 g^{σ_2}，用 g^{σ_2} 和 B 的标识可验证 B 的签名。如果验证都通过，则 A，B 分别计算$(\delta^y)^x$ 和$(\delta^x)^y$，作为会话密钥。

(2)由一方生成会话密钥　以 A 为例，由 A 生成随机的会话密钥，先对其签名，然后用$\langle g,g^{\sigma_2}\rangle$对会话密钥、签名和时间戳加密发送给 B。B 可以利用其私钥解密，并使用 g^{σ_1} 和 A 的标识验证 A 的签名。如果验证通过，可以作为会话密钥。

4.5 恶意节点处理

Ad Hoc 网络中任意节点都有被破坏或俘获的可能。簇头节点性能优良，计算和存储能力以及物理安全保障等方面均优于普通节点。假定簇头节点不易被破坏或俘获、具有一定可靠性是合理的。其它移动节点设备简单、性能较差、安全性低，容易被俘获受攻击者控制。

为抵抗被俘获节点的内部攻击，采用下面的检测和响应措施：

假定每个节点都具有某种监视机制，例如装备有入侵检测机制[9]，可以监视其一跳邻居节点。簇头节点均在彼此一跳通信范围内，互为邻居节点，它们之间互相监督。如果簇头 CH_1 发现某个簇头节点 CH_2 有恶意行为，则分别将签密的控告消息发给其它的簇头节点。文[10]中基于身份的签密方案，对于同一消息签密发送给多个接收者有一种优化算法，可

(下转第 96 页)

中蓝色曲线代表原始流量，红色曲线代表预测值。蓝线上的红色粗圆点表示检测到的异常。其中异常程度即风险级别的定义如上文，图中没有标出异常点的风险级别。利用本文的算法，正如所期待的，检测到了流量异常。

总结与展望 本文介绍了一种基于异常流量检测方法的骨干网早期预警系统 ESTAB 算法和框架设计，详细论述了基于周期性和非周期性业务流量的异常检测方法，并用来自骨干网的真实数据进行了测试验证。结果进一步说明，该方法是可行的。今后的工作将继续对模型的适应性进行改进，以实现更精准的检测，并进一步完善系统的性能。

参 考 文 献

1 Moore D, Shannon, et al. Code-Red: a case study on the spread and victims of an Internet worm. IMW, 2002

2 Moore D, Paxson V, et al. The Spread of the Sapphire/Slammer Worm. CAIDA, ICSI, Silicon Defense, UC Berkeley EECS and UC San Diego CSE, 2003

3 Weaver N, Paxson V, Staniford S, et al. A Taxonomy of Computer Worms. In: Proc. ACM CCS Workshop on Rapid Malcode, 2003

4 http://www.cnn.com/2001/TECH/internet/10/31/new.nimda.idg/

5 http://www.cnn.com/2003/TECH/internet/01/25/internet.attack/

6 Security firm: MyDoom worm fastest yet. http://edition.cnn.com/2004/TECH/internet/01/28/mydoom.spreadwed/index.html

7 Barford P, Kline J, Plonka D, et al. A signal analysis of network traffic anomalies. In: Internet Measurement Workshop, 2002

8 Madhusudan B, Lockwood J, et al. Design of a System for Real-Time Worm Detection. In: 12th Annual IEEE Symposium on High Performance Interconnects (Hot-I), Stanford, CA, 2004. 77～83

9 Lakhina A, Papagiannaki K, Crovella M, et al. Structural analysis of network traffic flows. Proc ACM SIGMETRICS, 2004

10 http://www.itl.nist.gov/div898/handbook/pmc/section4/pmc42.html

11 http://www.cert.org

（上接第 82 页）

以减少计算量，适合这里的需要。根据具体安全需求，选定门限值 k_1。如果有 k_1 个簇头节点对 CH_2 进行控告，则 CH_2 不再被信任，其簇内的节点也不再被信任。簇头 CH_2 内的普通节点需要重新离线注册或经其它簇头节点用辅助方法认证（旁路安全信道：红外线、视频、音频等），才能重新加入网络。

簇头节点安全性较高，为本簇内所有节点信任。簇成员节点因设备简单、保护措施差，易被俘获。对普通节点的信任关系由簇头节点控制。如果一个节点发现了其邻居节点有恶意行为，或是与其通信节点的恶意行为，则向簇头节点发出一个控告消息，并对该消息签密。

簇头节点维护一张恶意节点列表，表中每项包括的内容有：节点 ID、控告节点列表、行为状态。根据具体安全需求，选定另一门限值 k_2。如果恶意节点列表中节点 A 的控告列表少于 k_2 个合法的控告者，那么节点 A 被标记为可疑节点，行为状态标记为 0；否则，认为这个节点为恶意节点，不再信任此节点，行为状态标记为 1。如果有节点 A 受到 k_2 个合法节点的控告，簇头节点就在簇内广播一条签名的撤消节点 A 簇成员身份的消息，也需要向其它的簇头节点广播这一消息。消息格式如下：{节点 ID，恶意节点标记，签名}。节点 A 在整个网络中都不再被信任。这 k_2 个节点可以是其一跳邻居节点或是和它有过联系、发现它有恶意行为的节点。每个节点都存有一张被簇头节点确认的恶意用户列表，拒绝与这些节点的连接。需要选择合适的门限 $k2$，以确保合法节点不会被敌手节点的虚假信息损害。如果簇头节点发现一个节点有恶意行为，则直接把这个节点标记为恶意节点，广播签名的公告消息。

簇成员节点完全信任簇头节点，通过簇头节点维护恶意用户列表维持本簇内的信任关系。如果节点 A 被标记为恶意节点，那么它发出的控告信息都被视为无效，并且 A 将被从控告节点列表中清除。被标记为恶意节点的节点在对其控告列表中节点减少至 k_2 个以下时，可以变为可疑节点。簇头节点广播相应的签名消息，通告其行为状态。

结束语 Ad Hoc 网络是一种新型无线移动网络，它面临的特殊威胁导致了传统网络中的安全机制不再适用。现有 Ad Hoc 网络密钥管理方案多数是针对某种应用环境提出的，而且所提出的方案中有不少漏洞，目前尚缺乏有效的密钥管理方案。基于文[7,8]中的密钥管理方案，利用文[10]中的基于身份的签密体制，我们针对双频分级的 Ad Hoc 网络给出了一种分簇的密钥管理方案。方案不需要公钥证书，节省了用户的计算量、存储容量和系统的通信开销，并对恶意节点给出了有效的处理机制，而且可以对用户私钥进行有效的更新。方案具有良好的扩充性，适用于大规模的网络。我们在另一篇文章里研究了单频分级 Ad Hoc 网络的密钥管理问题。在以后的工作中，我们将进一步分析和改进分簇 Ad Hoc 网络的密钥管理方案，尤其是通信协议的仿真和优化以及方案的软件实现和效率分析。

参 考 文 献

1 Zhou L, Haas Z J. Securing Ad hoc Networks. IEEE Networks, 1999, 13(6): 24～30

2 Desmedt Y. Threshold cryptography. European Transactions on Telecommunications, 1994, 5(4): 449～457

3 Luo H, Zerfos P, Kong J, et al. Self-securing Ad Hoc Wireless Networks. In: 7th IEEE Symp on Computers and Communications, 2002. 567～574

4 Luo H, Lu S. Ubiquitous and Robust Authentication Services for Ad Hoc Wireless Networks: [UCLA-CSD-TR-200030]. 2000 http://www.cs.ucla.edu/wing/publication/papers/Luo.TR200030.pdf

5 Hubaux J P, Buttyan L, Capkun S. Self-organized Public-Key Management for Mobile Ad hoc Networks. In: IEEE Transactions on Mobile Computing, 2003. 52～64

6 Hubaux J P, Buttyan L, Capkun S. The Quest for Security in Mobile Ad hoc Networks. http://www.gta.ufrj.br/～eric/tese/artigos/QuestForSecurityInMobileAdhocNetworks.pdf

7 Khalili A, Katz J, Arbaugh W A. Towards Secure Key Distribution in Truly Ad Hoc Networks. In: Proc. of IEEE Workshop on Security and Assurance in Ad hoc Networks, 2003. http://www.gta.ufrj.br/～eric/tese/artigos/id threshold.ps.gz

8 Li Guangsong, Han Wenbao. A New Scheme for Key Management in Ad Hoc Networks. In: Proceeding of 4th International Conference on Networking, LNCS 3421, 2005. 242～249

9 Zhang Y, Lee W, Huang Y. Intrusion Detection Techniques for Mobile Wireless Networks. ACM/Kluwer Wireless Networks Journal, 2003. 545～556

10 Boyen X. Multipurpose Identity-Based Signcryption: A Swiss Army Knife for Identity- Based Cryptography. In: Proceedings of Crypto '03, LNCS 2729, 2003. 383～399