一种无证书的移动 Ad hoc 网络密钥管理方案

吴旭光[1],张敏情[1],杨晓元[1,2],韩益亮[1]
WU Xu-guang[1],ZHANG Min-qing[1],YANG Xiao-yuan[1,2],HAN Yi-liang[1]

1.武警工程学院 电子技术系 网络与信息安全武警部队重点实验室,西安 710086
2.西安电子科技大学 网络信息安全教育部重点实验室,西安 710071
1.Key Laboratory of Network & Information Security of APF,Engineering College of APF,Xi'an 710086,China
2.Key Laboratory of Network & Information Security of the Ministry of Education,Xidian University,Xi'an 710071,China
E-mail:wxguang0210@163.com

WU Xu-guang,ZHANG Min-qing,YANG Xiao-yuan,et al.Certificateless key management in mobile Ad hoc networks. Computer Engineering and Applications,2009,45(21):74-76.

Abstract: Combining certificateless signcryption protocol and hierarchical structure,a new key management agreement is proposed.In this scheme,public key certificates are not needed and every participant makes a public key himself.It greatly decreases the need of the ability for computation and storage of terminals,as well as communication cost for system key management.At the same time,the key generator center creates partial private keys for nodes,and then solves the key escrow problem in the identity-based cryptography.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.

Key words: mobile Ad hoc networks;key management;certificateless signcryption

摘 要: 结合无证书签密协议,提出一种分级移动 Ad hoc 网络密钥管理方案。该方案不需要公钥证书,用户自己生成公钥,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;同时密钥生成中心为用户生成部分私钥,解决了基于身份密码体制中的密钥托管问题;分级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: 移动 Ad hoc 网络;密钥管理;无证书签密
DOI: 10.3778/j.issn.1002-8331.2009.21.020 **文章编号:** 1002-8331(2009)21-0074-03 **文献标识码:** A **中图分类号:** TP309

1 引言

移动 Ad hoc 网络是由一组自主的无线节点或移动终端相互合作而形成的,相对于固定的基础设施,是一种自组织、自管理的网络。与有线网络相比,更容易遭到各种攻击,如窃听、篡改、消息重放攻击等。此外移动节点可能会漫游到敌对的环境中,因其脆弱的物理防护而遭到俘虏并被破坏。为了保障 Ad hoc 中信息的可用性、保密性、完整性和认证性,密钥管理受到越来越多的关注。

目前建立在公钥密码体制的基础上的密钥管理,主要有基于传统公钥密码系统(PKI)[1-2]和基于身份密码系统(ID-PKC)[3-4]两种方式。基于传统公钥的密钥管理,将有线网络中基于证书的密钥管理与认证方法移植到 Ad hoc 网络中,其证书管理的高计算量和存贮量,不能满足 Ad hoc 网络的资源受限性和高动态性。基于身份密码系统的密钥管理,虽然避免了证书的使用,减少了证书的计算量和存贮量,但存在密钥托管的局限。

无证书密码系统(CL-PKC)[5],不必使用证书来提供对公钥的认证,同时密钥生成中心(Key Generator Center,KGC)不直接生成用户的私钥,避免了密钥托管,较适合应用在 Ad hoc 网络中。结合无证书签密协议,提出在分级移动 Ad hoc 网络中的密钥管理方案,提高了安全服务的可用性和扩展性,适用于规模较大的移动 Ad hoc 网络。

2 基于无证书的签密协议

基于无证书的密码系统,与传统公钥密码系统相比,用户可将公钥附加在消息后发送给请求者,在密钥管理上可以节省较多的网络资源。与基于身份密码系统类似,它也要依赖于一个拥有主密钥(master-key)的密钥生成中心参与生成用户私钥,但区别在于,这个密钥生成中心不直接生成用户的私钥,只产生与用户身份对应的部分私钥,并将其安全地传送给用户,最终的用户私钥是由部分私钥与用户所选定的秘密值结合起来计算的。这样,不仅有效地解决了基于身份的公钥密码系统中的密钥托管问题,而且节约了网络资源。

基金项目: 国家自然科学基金(the National Natural Science Foundation of China under Grant No.60573032)。
作者简介: 吴旭光(1986-),男,硕士,主研领域为密码学,信息安全;张敏情(1967-),女,教授,研究生导师,主研究域为密码学,信息安全;杨晓元(1959-),男,教授,研究生导师,主研领域为密码学,信息安全;韩益亮,男,讲师,博士研究生,主研领域为密码学,信息安全。
收稿日期: 2009-01-14 **修回日期:** 2009-03-16

签密(Signcryption)能在一个逻辑运算内同时完成加密和签名的双重功能,而复杂度小于两者之和,解决了传统的加密和认证组合方式效率低下和安全性低的不足。

Diego Aranha 等在 2008 年提出了一个高效的无证书签密协议[6],简要介绍如下:

2.1 双线性对

设 G_1 和 G_2 是阶为 q 的加法群,G_T 是阶为 q 的乘法群。P 和 Q 分别是 G_1 和 G_2 的生成元,$e:G_1\times G_2\to G_T$ 称为双线性对映射,假如下面的条件满足:

(1)双线性:对于 $(Q,W)\in G_1\times G_2$ 和 $a,b\in Z_q^*$,有 $e(aQ,bW)==e(Q,W)^{ab}=e(abQ,W)=e(Q,abW)$;

(2)非退化性:存在 P 和 Q,使得 $e(P,Q)\neq 1_{G_T}$;

(3)可计算性:对于所有的 $P\in G_1$,$Q\in G_2$,存在一个有效的算法计算 $e(P,Q)$。

2.2 KGC 设置系统参数

KGC 选取安全随机参数 k,产生一个 k 比特的素数 q;选取 $P\in G_1$,$Q\in G_2$,产生 q 阶双线性组 (G_1,G_2,G_T) 和双线性对 e;选取 3 个哈希函数 $H_1:\{0,1\}^*\to Z_q^*$,$H_2:G_T\to\{0,1\}^n$ 和 $H_3:\{0,1\}^n\times G_1\times G_2\to Z_q^*$;选取随机主密钥 $s\in Z_q^*$ 并计算公钥 $P_{pub}=sP$,此时 $g=e(P,Q)$。最后公布系统参数 $(q,G_1,G_2,G_T,P,Q,e,g,P_{pub},H_1,H_2,H_3)$,保留私钥 s。

2.3 消息处理

签密消息:为了签密消息 M,用户 A 计算:

(1)$r\to_R Z_q^*$,$u\leftarrow r^{-1}$,$U\leftarrow g^u$

(2)$C\leftarrow M\oplus H_2(U)$

(3)$h\leftarrow H_3(C,rP_A,uP_B)$

(4)$T\leftarrow(r+h)^{-1}S_A$

(5)返回得到 (C,rP_A,uP_B,T)。

解签密:当收到签密消息 (C,rP_A,uP_B,T),用户 B 计算:

(1)$h'\leftarrow H_3(C,R,S)$

(2)$V\leftarrow e(R+h'P_A,T)$

(3)$r'\leftarrow e(S,S_B)$

(4)$M'\leftarrow C\oplus H_2(r')$

(5)如果 $V=g$,则返回 M'。否则,返回错误。

3 密钥管理方案设计

3.1 网络模型

无线 Ad hoc 网络的结构一般可分为两种:平面结构和分级结构。在平面结构中,所有节点在网络控制、路由选择和流量管理中作用相同,源节点和目的节点之间一般存在多条路径。它存在着处理能力弱、控制开销大的缺点,并且随着网络规模的扩大,通信能力会急速下降。在分级结构中,网络被划分为簇,每个簇由一个簇头和多个簇成员组成,由簇头节点负责簇间报文的转发。这种结构利用簇减小网络规模,从而减少了开销,并且不同簇内的通信互不影响,克服了平面结构可扩展性差的缺点。

针对分级网络,采取两层密钥管理结构:高级层网络是由通信和计算能力强的移动骨干节点(Mobile Backbone Node,MBN)等簇头组成的控制型无线网络,而低级层网络是由通信和计算能力有限的常规移动节点(Regular Mobile Node,RMN)组成的簇群;在高级层网络中,由一个可信中心作为 KGC 对簇头节点进行集中式管理,在低级层网络中,每个簇头节点作为分支 KGC,负责簇内常规节点密钥的分发、更新、撤销等。

3.2 初始化与公钥、私钥的分发

假设网络中存在一个在线的可信中心,其位置相对固定,在同一时间内与大部分的簇头节点保持通信畅通。它为所有经过认证后的节点颁发唯一的身份标识 ID,并且作为 KGC 公布系统参数 $(q,G_1,G_2,G_T,P,Q,e,g,P_{pub},H_1,H_2,H_3)$,保留私钥 s,以帮助簇头生成公私钥,过程 procedure-1 如下:

步骤 1 对于每个簇头节点 M_i:随机选取 $x_{M_i}\in Z_q^*$,计算公钥 $P_{M_i}=x_{M_i}(H_1(ID_{M_i})+P_{pub})\in G_1$;

步骤 2 $M_i\Rightarrow KGC:ID_{M_i},P_{M_i},H(ID_{M_i}\|P_{M_i})$;

步骤 3 $KGC\Rightarrow M_i:D_{M_i}=(H_1(ID_{M_i})+s)^{-1}Q,H_1(D_{M_i})$;

步骤 4 M_i:验证 D_{M_i} 后,计算私钥 $S_{M_i}=x_{M_i}D_{M_i}\in G_2$,显然 $e(P_{M_i},S_{M_i})=g$。

在簇头节点 M_i 拥有自己的公私钥后,成为网络中的分支 KGC。它公布簇内参数 $(q,G_1,G_2,G_T,P,Q,e,g,P_{M_i},H_1,H_2,H_3)$,并为申请加入簇的 RMN 节点分配簇内密钥,过程与 Procedure-1 类似。至此,网络组建完毕,可以看出网络初始化的过程也是网络密钥分配的过程。

3.3 认证与会话密钥协商协议

3.3.1 簇内节点之间的认证与会话密钥协商协议

同一簇 RGN 节点 R_a 和 R_b 进行通信,使用无证书签密协议签密对称密钥 K_{ab},可以实现认证功能,与其他先签名再加密的方法相比,提高了效率。其过程 Procedure-2 如下:

步骤 1 R_a 向 R_b 发送通信请求;

步骤 2 R_b 同意通信请求后,选取会话密钥 K_{ab},并对其签密;

步骤 3 R_a 对收到的消息解签密,先验证签名是否正确,如果正确则通过认证,并解密得到 K_{ab},用 K_{ab} 加密响应消息发给 R_b;如果未通过认证,则丢弃消息。

3.3.2 簇间节点之间的认证与会话密钥协商协议

不同簇之间的 RGN 节点 R_a 和 R_b 进行通信,由于它们分属簇的公钥不同,无法直接进行签密和解签密。在文献[7]的会话密钥交换协议基础上,提出适合方案的会话密钥协商协议,其过程 Procedure-3 如下:

步骤 1 R_a:随机选择 r_a',$\alpha\in_R Z_p^*$,计算 $v_a=\alpha^{r_a'}\bmod p$,向 M_j 发送消息 $\{ID_{R_a},ID_{R_b}v_a$,归属簇 $M_i\}$;

步骤 2 M_j 哈希与 R_b 之间的对称密钥 K_{jb},得到 $h_j=H(K_{jb})$,并发给 R_b 消息 $\{ID_{R_a},v_a$,簇 $M_i,h_j\}$;

步骤 3 R_b 选择 r_b',$\beta\in_R Z_p^*$,计算 $v_b=\beta^{r_b'}\bmod p$,向 M_i 发送消息 $\{R_a,v_b,T_{cur}$ 归属 $M_j\}$;

步骤 4 M_i 哈希与 R_a 消息之间的对称密钥 K_{ia},得到 $h_i=H(K_{ia})$,并发给 R_a 消息 $\{ID_{R_b},v_{bj}$ 簇 $M_j,h_i\}$;

步骤 5 R_a 计算 $K_{ab}=v_a^{h_j}\cdot v_b^{h_a}(\bmod p)\equiv v_a^{h_j}\cdot v_b^{h_i}(\bmod p)$,因为 $h_a=H(K_{ia})=h_i$;

步骤 6 R_b 计算 $K_{ab}=v_b^{h_i}\cdot v_a^{h_b}(\bmod p)\equiv v_a^{h_j}\cdot v_b^{h_i}(\bmod p)$，因为 $h_b=H(K_{jb})=H_j$。

3.4 恶意节点的处理和密钥更新

移动 Ad hoc 网络中，RGN 节点设备简单、性能较差、安全性低，容易被俘获并受攻击者控制。而 MBN 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 RGN 节点。因此假定簇头节点不易被破坏或俘获，并且能通过入侵检测及时发现簇内的恶意节点。

在簇内，所有的 RGN 节点拥有一个诚实身份列表 IDHL（ID Honesty List），用以记录本簇内的诚实节点。簇头发现恶意 RGN 节点后，将其从 IDHL 列表中删除，向簇内各 RGN 节点广播发送 IDHL，并联合 KGC 更新自己公私钥。各个 RGN 节点更新 IDHL 后，申请密钥更新。密钥更新过程 Procedure-4 如下：

步骤 1 簇头节点 M_i 用旧的公私钥与 KGC 相互认证身份并协商会话密钥 K_{ci}，具体协议见 3.3.1；

步骤 2 KGC 计算部分私钥 D'_{M_i}，并把 $E_{K_{ci}}(D'_{M_i})$ 发送给 M_i；

步骤 3 簇头 M_i 解密得到 D'_{M_i}，随机选取 $x_{M_i}\in Z_q^*$，计算公私钥对 (S_{M_i},P_{M_i})；

步骤 4 重复步骤 1~步骤 3 的过程，簇内各节点 R_i 与作为分支的 KGC 的簇头联合产生新的簇内节点公私钥。

3.5 节点的漫游

当 M_i 簇内节点 R_a 长时间地漫游到 M_j 簇时，R_a 可向簇头 M_j 申请加入簇，其过程 Procedure-5 如下：

步骤 1 R_a 向簇头 M_j 发送加入请求 {加入标识 $JOIN$，ID_{R_a}，归属 M_i}；

步骤 2 M_j 向 M_i 发送消息 $E_{K_{ij}}(ID_R,T_{cur},JOIN)$，用以验证 R_a 是否属于 M_i；

步骤 3 如果 R_a 属于 M_i，则 M_i 把与 R_a 的会话密钥加密后发给 M_j，消息是 $\{E_{K_{ij}}(K_{ia})\}$；如果 R_a 不属于 M_i，则发给 M_j 消息 {否认标识 Deny}；

步骤 4 如果 R_a 属于簇 M_i，M_j 为 R_a 生成部分私钥 $D_{R_a}=(H_1(ID_{R_a})+s_{M_j})^{-1}Q$，使用 K_{ia} 加密后发给 R_a；

步骤 5 如果 R_a 是冒充者，他将不能解开 K_{ia} 加密的密文，得不到部分私钥，无法加入簇 M_j。否则，R_a 通过解密得到部分私钥，然后随机选择 $x_{R_a}\in Z_q^*$，计算公私钥对 (S_a,P_a)，与簇头 M_j 相互认证并协商会话密钥。

4 分析

4.1 安全性分析

以下分三个方面讨论本文密钥管理方案的安全性：(1)向前/后安全性。每个节点 ID 是唯一的，可信中心以 ID 为节点计算部分私钥，使得不会出现相同的公私钥对，因而节点不能解密在它加入之前的秘密信息，保证了向前安全。可信中心设置密钥更新的时间，以保证节点在失效后不能参加通信，同时分支 KGC 在发现恶意 RGN 节点后，删除节点 ID，并向簇内各节点和其他簇头广播 ID，这样保证了向后安全。(2)节点公私钥的安全性。节点选取随机数作为秘密值，结合 KGC 的公开参数生成公钥；KGC 为节点生成部分私钥，而用户最终的私钥是由部分私钥和秘密值计算而来，这样私钥只有节点知道，其他任何节点包括 KGC 都无法知道，满足了密钥的保密性。(3)会话密钥的安全性。会话密钥协商时使用签密算法，只有经过签名认证后才能建立会话密钥，并使用签密加密保证了会话密钥的安全性。

4.2 效率分析

4.2.1 通信开销

移动 Ad hoc 网络中进行较多的是密钥会话协商。在这方面，基于传统公钥密码体制的密钥管理中节点双方需要两次的证书传递和验证，以进行 3 次握手协议。而该方案不需要证书，减少了约三分之一的通信量，提高了通信效率。同时使用签密算法，与传统先签名再加密的组合方式相比，又提高了计算效率。

4.2.2 计算复杂度

由于采用分级分簇式结构，每个簇头作为分支 KGC，负责簇内各个节点的密钥管理，因此计算复杂度大大降低。在密钥更新时，簇头只需更新簇内节点和自己私钥。假如簇内有 m 个节点，则计算复杂度为 $O(m)$。

文献[4]的密钥管理方案使用了基于身份的签密算法。分别从双线性对计算 e、指数运算 α^x、群中的乘法运算 kP，Z_q^{a-1} 中的求逆 a^{-1} 和 Hash 函数 H 等方面与其进行比较，结果如表 1。

表 1 计算复杂度比较

算法	方案	e	α^x	kP	a^{-1}	H
签密	文献[4]	1	4	0	0	6
	本文	0	1	3	2	2
解签密	文献[4]	3	1	0	0	6
	本文	2	0	1	0	2

在这几项指标中，双线性对计算 e 计算量最大、耗费时间最多，算法在签密计算时不需要双线性对计算，而在解签密时需要 2 次计算，总的双线性对计算次数相对于文献[4]减少了一半；虽然 kP 和 a^{-1} 与文献[4]相比次数有所增加，但总体上本文算法比文献[4]算法计算量小、效率更高。

5 结束语

基于无证书签密协议，提出了分级移动 Ad hoc 网络密钥管理方案，相比基于传统公钥密码管理和基于身份的密钥管理方案，该方案不仅避免了繁琐的证书管理方式，而且解决了密钥托管问题，同时使用签密算法提高了效率。下一步将结合门限方案，解决可信中心的安全问题，并对无证书签密算法的安全性做进一步研究证明。

参考文献：

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

[2] S Yi,R Kravets.Key management for heterogeneous Ad hoc wireless networks[C]//10th IEEE International Conference on Network Protocols (ICNP 2002),2002.

[3] 李光松,韩文报.基于签密的 Ad hoc 网络密钥管理[J].计算机工程与应用,2005,41(12):160-167.

（下转 84 页）