移动通信网中的端端保密通信

余斌霄,王新梅
(1. 西安电子科技大学综合业务网国家重点实验室,陕西西安 710071)

摘 要: 移动通信网络应用范围的不断扩展和新型业务的涌现需要有更多的特殊安全协议来保障其安全性. Yi Mu 和 Vijay Varadharajan 提出了两种分别应用于同一服务区和不同服务区的端端保密通信协议[1,2]. 本文首先分析了其不足之处,然后设计了同时适用于同一归属局和不同归属局移动用户之间进行保密通信的安全协议(分别称为域内和域间保密通信协议),最后,分析了上述协议的各项性能. 与原有协议相比,本文所提出的协议不仅在安全性和其他性能上有较大改进,而且更具普遍性和统一性.

关键词: 移动通信网; 端端保密; 安全协议
中图分类号: TN929.5 **文献标识码**: A **文章编号**: 0372-2112 (2004) 03-0384-04

Secret End-to-End Communications in Mobile Networks

YU Bin-xiao, WANG Xin-mei
(National Key Lab of ISN, Xidian University, Xi'an, Shaanxi, 710071, China)

Abstract: Along with the ceaseless development of application of mobile networks, higher security is required by many jumped-up services of mobile networks, and therefore, sophisticated security protocols for special cases must be designed to fulfill the demand. Two of these are proposed by Yi Mu and Vijay Varadharajan for end-to-end secret communications between two mobile subscribers in same and different service area respectively. We first analyze the defects of them, then we design two new protocols for the same purpose between inter-domain and intra-domain subscribers respectively, and their performance, especially security, is discussed after this. Compared with original ones, ours are improved not only upon security and other performance, but also on universalism and oneness.

Key words: mobile networks; end-to-end communications; security protocols

1 引言

随着移动通信网技术的发展,应用领域的拓展以及人们保护个人隐私意识的增强,在很多应用场合需要进一步提高移动通信的安全程度. Yi Mu 和 Vijay Varadharajan 在文献[1]中提出了在同一服务区内分别利用单钥体制和双钥体制实现端端保密通信的协议,其中单钥体制协议是由所在 VLR 生成保密通信会话密钥并分发给通信双方. 由于移动用户一般缺乏对除其 HLR 之外的 VLR 的信任,这样不仅不能抵御内部攻击,而且相应的 HLR 也缺乏对会话密钥的控制;另外,其中的双钥体制协议多次在移动端进行 DH 密钥生成操作,造成移动端计算负担过重,不太适合于移动通信环境. 关于不同服务区域内的端端保密通信则在文献[2]中有所研究. 上述端端保密通信协议不仅在消息格式和执行过程上差别较大,缺乏统一性;而且在设计协议时仅仅考虑了通信双方的相对物理位置关系(是否处于同一服务区内),没有考虑归属局的相关因素和应当发挥的作用,具有一定的局限性.

本文的目的在于设计安全的、具有普遍意义的端端保密通信协议,其主要特点是以移动用户双方的相对归属关系而不是相对物理位置关系为依据划分不同类型的协议. 这种划分标准简单明了,与其相对位置关系不大,可以克服上述不足. 协议在保障安全性的同时,还要具备良好的不对称性:考虑到移动端和网络端计算能力的巨大差异,我们综合使用单钥体制和双钥体制,在移动端尽可能使用单钥操作,在网络端则同时使用单钥操作和双钥操作;同时在移动端尽量避免费时的双钥签名操作,代之以键控 hash 函数实现认证. 另外,还要保证协议的执行效率和一致性,即协议不能过于复杂,计算量不能过大;同时不同的协议之间本质差别要小,保持统一性,便于实现.

2 前提和假设

本节主要介绍后文讨论所需要的一些相关的前提和假设.

2.1 CA 结构和证书管理

CA 体系呈倒置的树状结构:顶层为根 CA,具备权威性和公正性,其公钥证书由自己签发;各归属局的公钥证书 HCAi 由根 CA 签发;移动用户的公钥证书 MCAj 则经其归属局审验

收稿日期:2002-11-29;修回日期:2003-06-02
基金项目:国防重点实验室基金项目(No. 51434060103DZ01)

注册材料后由其归属局 CA 签发.

根 CA 保存自己和各归属局的公钥证书;各归属局保存根 CA、自己以及其注册用户的公钥证书;移动端则保存根 CA、归属局和自己的公钥证书.归属局可以向根 CA 索要其他归属局的公钥证书,也可以向其他归属局索要其注册用户的的公钥证书;移动端可以通过其归属局索要本域或其他域内移动用户的公钥证书.由于归属局相对固定且为数不多,而且索要其他归属局证书的过程较为简单,我们假设每个归属局都保存有其他归属局的最新公钥证书.

2.2 Hash 函数的安全特性[4]

本文用到三种 hash 函数: $KH\_MA_K(M)$、$KH\_KC_K(M)$ 和 $KH\_KG_K(M)$,分别用于消息认证、密钥确认和密钥生成.根据需要,我们假设其分别具有如下安全特性:

$KH\_MA_K(M)$:满足单向性和弱认证属性;

$KH\_KC_K(M)$:满足单向性、无碰撞性和弱认证属性;

$KH\_KG_K(M)$:满足局部单向性、无碰撞性、弱认证属性和弱伪随机属性.

2.3 基本 AKE 协议

端端保密通信协议是以基本 AKE 协议[3]作为基础设计的,协议流程和对应的描述如图 1 所示.有关该协议的详细情况见文献[3].

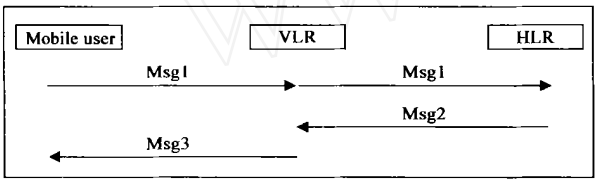

图 1　基本 AKE 协议

Msg1: UID_{TEMP}, $\{r_{UID} \| c\}_{KUID}$, $KH\_MA_{KUID}((UID_{TEMP} \| r_{UID}) \oplus c)$;

Msg2: HLR $\| k_S$, $\{UID'_{TEMP} \| r_H \| r_{UID}\}_{KUID}$, $KH\_KC_{KS}(UID_{TEMP} \| UID'_{TEMP} \| r_H \| r_{UID})$;

Msg3: $\{UID'_{TEMP} \| r_H \| r_{UID}\}_{KUID}$, $KH\_KCKS(UID_{TEMP} \| UID'_{TEMP} \| r_H \| r_{UID})$;

其中 UID'_{TEMP}和 UID_{TEMP}分别为移动用户 UID 的新生成的和已使用的临时身份; k_{UID}移动用户 UID 和其归属局之间的共享密钥; r_H、r_{UID}、c 和 c 均为一次性随机数; $k_S = KH_KG_{KUID}(UID \| UID'_{TEMP} \| r_{UID} \| r_H)$为本次会话密钥,下同.

2.4 归属局和拜访局间的通信安全

我们假设其间通信信道是安全的;否则可利用双钥加密和签名使其变为安全信道.由于 HLR 和 VLR 通常具备较强的运算能力,因而采用双钥体制保障其安全性是切实可行的.后文中我们仅仅考虑归属局和拜访局内存在的内部攻击,不再考虑针对其间通信信道的攻击.

3 域内保密通信协议

本文所提出的域内保密通信协议适用于同一归属局的移动用户(A 和 B)之间进行保密通信的情况.协议以基本 AKE 协议为基础,与双方各自具体漫游位置无关.

3.1 协议流程

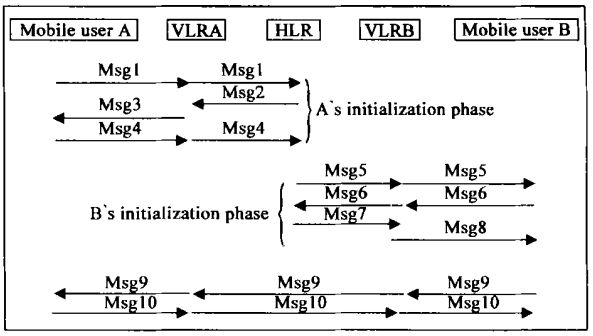

图 2　域内端端保密通信协议

Msg1: A_{TEMP}, $\{B \| r_A \| c'_A\}_{KA}$, $KH\_MA_{KA}((A_{TEMP} \| r_A) \oplus c_A)$;

Msg2: $A_{TEMP} \| k_{SA} \| Cert_B$, $\{A'_{TEMP} \| r_H \| r_A \| Cert_B\}_{KA}$, $KH\_KC_{KSA}(A_{TEMP} \| A'_{TEMP} \| r_H \| r_A \| Cert_B)$;

Msg3: $\{A'_{TEMP} \| r_H \| r_A \| Cert_B\}_{KA}$, $KH\_KC_{KSA}(A_{TEMP} \| A'_{TEMP} \| r_H \| r_A \| Cert_B)$;

Msg4: A_{TEMP}, $E_{PB}\{A \| B \| r_1\}$;

Msg5: $\{A \| r'_H\}_{KB}$;

Msg6: B_{TEMP}, $\{A \| r_B \| c'_B\}_{KB}$, $KH\_MA_{KB}((B_{TEMP} \| r_B \| r'_H) \oplus c_B)$;

Msg7: $B_{TEMP} \| k_{SB} \| Cert_A$, $\{B'_{TEMP} \| r_H \| r_B \| Cert_A\}_{KB}$, $KH\_KC_{KSB}(B_{TEMP} \| B'_{TEMP} \| r_H \| r_B \| Cert_A)$, $E_{PB}\{A \| B \| r_1\}$;

Msg8: $\{B'_{TEMP} \| r_H \| r_B \| Cert_A\}_{KB}$, $KH\_KC_{KSB}(B_{TEMP} \| B'_{TEMP} \| r_H \| r_B \| Cert_A)$, $E_{PB}\{A \| B \| r_1\}$;

Msg9: $E_{PA}\{B \| A \| r_2\}$, $KH\_KC_{KAB}\{A \| B \| r_1 \| r_H \| r_2\}$;

Msg10: $KH\_KC_{KAB}\{A \| B \| r_1 + 1 \| r_H + 1 \| r_2 + 1\}$;

其中 k_A、k_{SA}、P_A、S_A 和 k_{AB}分别为 A 和 HLR 的共享秘密钥、本次会话密钥、公钥、私钥和与 B 的保密会话密钥, E_{PA}和 S_{SA}分别表示 A 的公钥加密和私钥签名. B 的情况亦然.

3.2 协议描述

协议执行过程可大致分为三个阶段:移动用户 A 的初始化阶段,移动用户 B 的初始化阶段以及 AB 握手阶段,分别进行描述:

3.2.1 移动用户 A 的初始化阶段

(1) 发起方 A 通过拜访局 VLR_A 向归属局 HLR 传送 A_{TEMP}、包括对方真实身份 B 的密文$\{B \| r_A \| c'_A\}_{KA}$以及认证 hash 值 $KH\_MA_{KA}((A_{TEMP} \| r_A) \oplus c_A)$;

(2) HLR 在核实 A 的身份之后生成 A'_{TEMP}和 r_H,计算 $k_{SA} = KH\_KG_{KA}(A \| A'_{TEMP} \| r_A \| r_H)$,然后向 VLR_A 发送 Msg2;

(3) VLR_A 向 A 转发 Msg3;

(4) A 解密$\{A'_{TEMP} \| r_H \| r_A \| Cert_B\}_{KA}$得到 A'_{TEMP}、B 的公钥证书 $Cert_B$、r_H 和 r_A:若 r_A 不相符,则终止协议;否则计算 k_{SA}并验证其确认哈希值是否相等:若不等则终止协议;否则经 VLR_A 向 HLR 发送 Msg4,其中 r_1 作为部分密钥材料以及 A 对 B 的认证数据;

3.2.2 移动用户 B 的初始化阶段

(5) HLR 收到 Msg4 后通过 B 所在的拜访局 VLR_B 向其发送 $\{A \| r'_H\}_{KB}$;

(6) B 解密 $\{A \| r'_H\}_{KB}$ 得到 A 的身份和 r'_H,随后通过 VLR_B 向 HLR 发送 Msg6;

(7) HLR 解密 $\{A \| r_B \| c'_B\}_{KB}$ 得到 A 和 r_B,然后计算认证 hash 值并与收到的 hash 值进行比较:不符则从第(5)步重新开始;否则生成 B'_{TEMP},计算 $k_{SB} = KH_{KB}(B \| B'_{TEMP} \| r_B \| r_H)$,然后向 VLR_B 发送 Msg7;

(8) VLR_B 向 B 转发 Msg8;

3.2.3 AB 握手阶段

(9) B 在验证 k_{SB} 后生成 r_2,计算 $k_{AB} = KH_{KRH}(A \| B \| r_1 \| r_2)$,然后向 A 发送 Msg9;

(10) A 解密 $E_{PA}\{B \| A \| r_2\}$ 得 r_2,同样计算 k_{AB},计算认证 hash 值并与收到的相比较:若相符则向移动用户 B 发送认证 hash 值 $KH_{KAB}\{A \| B \| r_1 + 1 \| r_H + 1 \| r_2 + 1\}$;否则协议出错终止.

3.3 协议功能

协议实现了以下特定于端端保密通信的功能:

实体交互认证:通信双方通过 HLR、VLR_A 以及 VLR_B 传递认证关系,实现交互认证;保密会话密钥生成:根据密钥材料 A、B、r_1、r_H 和 r_2 各自生成,保证密钥控制和新鲜性;保密会话密钥认证:通过传送只有意定接收者才能得到的密钥材料实现,具备隐式认证性质;保密会话密钥确认:在握手阶段通过使用保密会话密钥构造 hash 认证值实现.

3.4 协议分析

3.4.1 安全性

基本 AKE 协议的安全性分析见文献[3],这里主要介绍其他方面.

(1) 内部攻击:本协议中归属局或拜访局的内部攻击不再有效. 拜访局仅仅知道双方身份和本端会话密钥,归属局则缺乏由双方公钥加密保护的两部分密钥材料,区别于文献[1]中的方式;

(2) 外部攻击:主要讨论无线接口上的攻击. 攻击者无法得知通信双方的真实身份(见文献[3])和 r_H,也无法得知 r_1 和 r_2 以生成保密会话密钥窃听通信内容;

(3) 其他:$E_{PA}\{B \| A \| r_2\}$ 和 $E_{PB}\{A \| B \| r_1\}$ 没有私钥签名,但由于其中包括了双方各自选定的一次性随机数,因而是不可伪造的. 关于重放攻击、中间人攻击和伪基站攻击的分析见文献[3].

3.4.2 效率

考虑到无线接口两端计算能力的差异,我们仅仅考虑移动端的情况. 本协议与文献[1]中方案的效率比较见表 1.

计算量标准:内嵌 5MHz 协处理器 SLE44CR80S 的智能卡可以在 40ms 内完成 512 比特的 RSA 双钥操作[5];而 RSA 操作要比 DES 慢大约 1000 倍,MD4 大约比 DES 快三倍[6]. 据此我们假设双钥操作、单钥操作和 hash 操作分别需要 40ms、40μs 和 10μs. 由于交互次数相差不多,为简单起见,我们不考虑无线接口及网内时延.

可以看出,除交互次数外,与文献[1]中的双钥方案相比,本协议的其他各项性能均有较大幅度提高,而且可以以较小的代价(0.1ms 时延)实现越区切换而不必终止保密通话.

表 1 本协议与文献[1]中协议的性能比较

主叫/被叫		交互次数	消息长度	计算量 hash 运算	计算量 单钥操作	计算量 双钥操作	呼叫建立时延	越区切换时延
本协议		5/5	较短	4/3	2/3	2/2	160.27ms	0.1ms
文献	单	5/3	较长	8/6	10/7	N/A	0.82ms	N/A
文献	双	5/3	较长	5/3	6/3	4/3	280.44ms	N/A

3.4.3 普遍性和通用性

当移动端发生越区切换时,本协议可以不加修改地适用于各种情况. 另外,消息格式和流程相对统一,便于模块化实现. 事实上,更具普遍性和通用性的是下文将要介绍的域间保密通信协议,本协议仅仅作为其一个特例:通信双方归属局相同的情况.

4 域间保密通信协议

域间协议适用于通信双方归属局不一定相同的情况,可以看作是域内协议的拓展和推广,较前者更具普遍性和通用性. 不同之处在于:由于可能涉及到两个归属局,需要在其间进行某些信息交互,密钥材料的提供方式和用法也稍有区别. 由于两种协议间的相似性,其安全性和其他性能的分析和结果极其类似. 限于篇幅,这里仅仅给出协议流程,然后指出不同之处,不再作深入分析.

4.1 协议流程

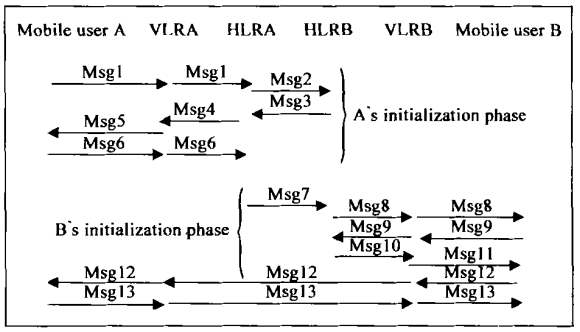

图 3 域间端端保密通信协议

Msg1: $A_{TEMP}, \{B \| r_A \| c'_A\}_{KA}, KH_{MA_{KA}}((A_{TEMP} \| r_A) \oplus c_A)$;

Msg2: $HLR_A, HLR_B, E_{PHB}\{HLR_A \| HLR_B \| S_{SHA}(B \| r_{HA})\}$;

Msg3: $HLR_B, HLR_A, E_{PHA}\{HLR_B \| HLR_A \| S_{SHB}(Cert_B \| r_{HA} \| r_{HB})\}$;

Msg4: $A_{TEMP} \| k_{SA} \| Cert_B, \{A'_{TEMP} \| r_{HAB} \| r_A \| Cert_B\}_{KA}, KH_{KC_{KSA}}(A_{TEMP} \| A'_{TEMP} \| r_{HAB} \| r_A \| Cert_B)$;

Msg5: $\{A'_{TEMP} \| r_{HAB} \| r_A \| Cert_B\}_{KA}, KH_{KC_{KSA}}(A_{TEMP} \| A'_{TEMP} \| r_{HAB} \| r_A \| Cert_B)$;

Msg6: $A_{TEMP}, E_{PB}\{A \| B \| r_1\}$;

Msg7: $HLR_A, HLR_B, E_{PHB}\{A \| S_{SHA}(Cert_A \| r_{HB})\}, E_{PB}\{A \|$

$B \| r_1\}$;

Msg8:$\{A \| r'_{HB}\}_{KB}$;

Msg9:$B_{TEMP}, \{A \| r_B \| c'_B\}_{KB}$, $KH\text{-}MA_{KB}((B_{TEMP} \| r_B \| r'_{HB}) \ominus c_B)$;

Msg10:$B_{TEMP} \| k_{SB} \| Cert_A; \{B'_{TEMP} \| r_{HAB} \| r_B \| Cert_A\}_{KB}$, $KH\text{-}KC_{KSB}(B_{TEMP} \| B'_{TEMP} \| r_{HAB} \| r_B \| Cert_A)$;

Msg11:$\{B'_{TEMP} \| r_{HAB} \| r_B \| Cert_A\}_{KB}$, $KH\text{-}KC_{KSB}(B_{TEMP} \| B'_{TEMP} \| r_{HAB} \| r_B \| Cert_A)$, $E_{PB}\{A \| B \| r_1\}$;

Msg12:$E_{PA}\{B \| A \| r_2\}$, $KH\text{-}KC_{KAB}\{A \| B \| r_1 \| r_{HAB} \| r_2\}$;

Msg13:$KH\text{-}KC_{KAB}\{A \| B \| r_A + 1 \| r_{HAB} + 1 \| r_B + 1\}$.

4.2　协议性能

这里我们只讨论所增加的归属域之间的交互对协议性能的影响.

4.2.1　安全性

根据假设,归属局之间的通信信道是安全的,在其间所传送消息的关键部分均进行了加密和签名保护,还使用了一次性随机数防止重放,因此域间协议至少和域内协议同样安全.

4.2.2　效率

归属局之间的交互对协议效率影响不大,考虑到归属局的计算能力,所增加的三次交互基本不对其构成负担;而在无线接口上的消息传输是相同的.因此,域间协议的各项效率和性能基本与域内协议相同.

5　结束语

本文在分析以往研究成果的基础上提出了一种新的端端保密通信协议.该协议的主要特点是:以移动用户所属域的关系为依据建立保密连接,与用户之间相对位置无关;改变了以往由拜访局生成会话密钥并进行分配或由双方通过 DH 方案生成会话密钥的做法,使得通信双方和各自的归属局均有能力对会话密钥进行控制;同时使用了单钥体制和双钥体制,既保证了安全性,又兼顾了不对称性.分析表明,协议概念简单,易于理解,不仅具备更高的安全性,同时还可以不加修改地适用于各种不同情况,具有普遍意义.

参考文献:

[1] Yi Mu, Vijay Varadharajan. On the design of security protocols for mobile communications [A]. ACISP'96 [C]. NSW, Australian: LNCS 1172, Springer, Wollongong, June 1996. 134 - 145.

[2] Vijay Varadharajan, Yi Mu. Design of secure end-to-end protocols for mobile systems [A]. Canberra, Australia: IFIP Congress 1996, 1996. 258 - 266.

[3] 余斌霄,王新梅. 移动通信网中的认证与密钥建立协议[J]. 西安电子科技大学学报,2004,31(1):124 - 128.

[4] Gunther Horn, Bart Preneel. Authentication and payment in future mobile systems[J]. Journal of Computer Security, July 2000. 183 - 207.

[5] Choonsik Park: On certificate-based security protocols for wireless mobile communication systems [J]. IEEE Network, September/October 1997:50 - 55.

[6] Bruce Schneier. 应用密码学(第二版)[M]. 北京:机械工业出版社,2000. 251 - 336.

作者简介:

余斌霄　男,1975 年 3 月生于陕西长安,1997 年 7 月毕业于西安工业学院计算机系计算机及应用专业,获工学学士学位,2000 年 4 月毕业于西安工业学院计算机科学与工程系计算机应用技术专业,获工学硕士学位;2001 年起在西安电子科技大学攻读博士学位,研究方向为无线网络安全、移动商务和密码学.

王新梅　男,1937 年 11 月生于浙江,1960 年毕业于中国人民解放军军事电讯工程学院,现任西安电子科技大学教授、博士生导师,主要从事通信、纠错码和密码的教学和科研,在国内外著名期刊和有关国际会议上发表论文 60 余篇,著有多部专著,主持了国家八五攻关、国家自然科学基金、国家密码学发展基金、电子部基金等多项科研项目.