移动通信用户身份保密的增强方法

赵源超 李道本
(北京邮电大学信息工程学院 北京 100876)

摘 要： 针对现有移动通信标准中无法完全实现用户身份保密这一问题，该文提出了分别基于公钥密码学和对称密钥密码学的两种改进措施，将用户的真实身份隐蔽在众多的用户标识里，使攻击者不能确切地得到用户身份的具体信息，明显增强了用户身份的保密性，并且分析比较了两种措施的性能。这些改进措施可以用于任何移动通信技术中。

关键词： 用户身份保密性，国际移动用户身份，临时移动用户身份
中图分类号： TN929.5, TN918.91 **文献标识码：** A **文章编号：** 1009-5896(2005)09-1459-04

The Enhanced Methods of User Identity's Confidentiality in Mobile Communication

Zhao Yuan-chao Li Dao-ben
(*Dept of Info. Eng., Beijing Univ. of Posts and Telecom., Beijing* 100876, *China*)

Abstract Focused on the scenario that none of the current standards achieves user identity's confidentiality, two enhanced methods are proposed, respectively based on public key cryptography and symmetric key cryptography, in which each user's real identity is concealed among many users' identities. So attackers can not capture the concrete identity information and user identity confidentiality is improved obviously. The performance of the two methods is analyzed and compared. And the proposed methods can be used in other mobile communication technologies.

Key words User identity confidentiality, International Mobile Subscriber Identity (IMSI), Temporary Mobile Subscriber Identity(TMSI)

1 引言

目前，移动通信技术在全球范围内得到广泛的应用，如欧洲标准的 GSM。移动通信具有可以使用户随时随地接入网络的优点，但是，也正是由于这种“随时随地”的特性再加上无线链路固有的开放性，使得移动通信网络面临比固定网络更加严峻的安全威胁，如：用户的通信可以被攻击者窃听而不被网络和用户觉察、无线链路上传输的信令被破坏和重放等等，甚至网络的安全缺陷可以使得主动攻击者获得对网络服务的使用而不用付费，从而给用户和运营商造成巨大的损失。因此，移动通信的安全特性在国际上已经引起了高度的重视并且得到了广泛的研究，同时新一代的移动通信标准也为安全特性制定了大量的规范。

本文通过对已有的移动通信标准包括第三代移动通信标准的研究发现，在众多的安全特性中，有一个安全特性问题却没有得到完全的解决，这就是用户身份的保密性。在移动通信环境中，攻击者如果能够得到合法用户的身份，就可能利用这种身份信息，定位合法用户的所处位置，而这是合法用户想要避免的事情。如文献[1]所述，“对某些用户而言，通信时所处的位置及时间，都有相当的意义及价值。例如某著名人物到何处休闲的消息，都可因为使用无线通信而泄漏。所以用户的真实身份保密，对某些人而言也是相当重要的。”用户身份的保密性，也被第三代移动通信技术标准的研究人员明确提出[2]。因此，有必要为移动通信环境提出完备的安全方案来确保移动用户身份的保密性。

本文在分析已有的移动通信标准安全特性的基础上，指出了这些技术都无法完全实现用户身份的保密性，这种缺陷也存在于最新的移动通信标准 3GPP 中。针对这一问题，本文提出了相应的改进措施，从而明显增强了用户身份的保密性。而且，本文提出的这些改进措施可以用于任何移动通信技术中。

下面几节分别包括如下内容：

第 2 节以全球移动通信系统(Global System for Mobile

2004-03-25 收到，2004-07-08 改回

Communications, GSM)和第三代合作伙伴计划(3rd Generation Partnership Project, 3GPP)为例，分析已有的移动通信标准中确实存在用户身份保密性的缺陷及其存在的原因；第3节基于密码学原理，提出两种改进措施，并且对性能作了简要的分析；第4节给出了本文的结论。

2 现有移动通信标准的安全缺陷

在任何移动通信系统中，移动用户的身份都要由一个全局唯一的标识号来确定，如GSM和3GPP中的国际移动用户标识(International Mobile Subscriber Identity, IMSI)、DECT(Digital European Cordless Telephone)中的DECT ID(DECT IDentification number)以及USDC(United States Digital Cellular)中的电话序列号(Phone serial number)等等。

下面的讨论以GSM和3GPP为例。

在这两种移动通信系统中，移动用户的身份是由IMSI在全球范围内唯一确定的。移动用户身份的保密性就是指保护合法用户的IMSI，使IMSI不能够被攻击者获得，以免攻击者利用这一信息定位、跟踪合法用户等等。

为了保密移动用户的身份，在3GPP的规范中，系统在无线链路上大多数情况下使用临时移动用户标识(Temporary Mobile Subscriber Identity, TMSI)来确定用户的身份。同时，在用户所处的服务网络的拜访位置寄存器(Visitor Location Register, VLR)的数据库中，保存IMSI和TMSI两者的对应关系，正是由于这个对应关系的存在，使得服务网络既能够确定用户的真正身分，又能够在与移动台的交互中不用直接使用IMSI，从而为移动用户的身份提供了一定程度的保密性。

但是，移动通信系统并不是在任何情况下，都能够只通过使用TMSI来确定用户的身份。当用户不能由临时身份标识的时候，特别是，当用户在服务网络中进行初始注册的时候，或者当服务网络不能由用户在无线链路标识自身的TMSI检索出IMSI的时候(也就是说，在前述的VLR的数据库中不存在相应的TMSI与IMSI的对应关系的时候)，服务网络仍然要求用户提供IMSI，这个传递用户永久身份的过程如图1，其中“ME/USIM”指“移动设备/用户业务身份模块”，而且通俗地说，USIM就是分发给用户的智能卡。这一过程由用户所处服务网络的VLR发起，它要求用户发送自己的永久身份。特别需要引起注意的是，用户的响应中含有IMSI，而且这个IMSI信息是以明文形式传送的。这一点违反了用户身份保密性的原则。

图1 移动用户永久身份的传递过程

实际上，在其他的已有移动通信标准中同样存在以明文传送用户永久身份的缺陷，如DECT、USDC等[1]。

这里分析一下为什么这些系统都要求在空中链路以明文形式传递IMSI，实际上，主要有两方面的原因：

(1) 在移动通信系统中，为了鉴别用户，系统就必须得到用户的身份标识；而且，TMSI的分配以及鉴别与密钥协商过程都是建立在网络已经知道用户的IMSI的基础之上的，因此，移动用户向网络传递自己的IMSI的步骤是必不可少的。同时，由于用户与系统的鉴别信息只是存放在用户的智能卡和归属位置寄存器/鉴别中心(Home Location Register /Authentication Center, HLR/AuC)中，然而，用户和HLR/AuC之间的双向鉴别必须在服务网络的VLR的协助下才能完成(因为很显然用户和归属环境是不能直接通信的)，而VLR和用户之间在初始注册时不存在任何共享秘密，因此不能进行保密通信，所以才使用明文形式进行用户身份的传送；

(2) 当VLR要协助用户和HLR/AuC两者完成鉴别过程的时候，VLR要得到足够的路由信息才能将相关的信令通过核心网传递到移动用户的归属环境。而这种必需的路由信息是包含在用户的身份标识中的。在VLR和用户之间没有建立安全关系之前，这些必需的信息一定要以明文形式传送。

3 移动用户身份保密性的增强方法

本节提出的方法仍然以GSM和3GPP为例，对于其他的标准，方法是完全类似的。

由上一节最后的分析可以看出，之所以对VLR提供明文的IMSI，是因为它提供了服务网络与移动用户建立安全关系时核心网信令所要用到的信息。但是，实际上，我们可以观察到IMSI所提供的信息多于核心网所必需的路由信息。本节提出的改进措施，正是利用将IMSI中所含的信息分成必须明文部分和不必须明文部分，而达到保密用户的身份。其中必须明文的部分在空中链路传送时还是要保持明文形式，而不必须明文的部分就可以被加密处理，隐蔽用户的真实身份。下面就仔细的分析一下IMSI的结构，达到将其分解成必须明文与不必须明文两个部分的目的。ITU-T建议E.212定义了IMSI的结构，如图2[3]示。

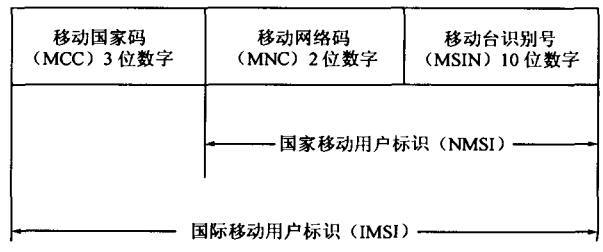

图2 IMSI结构

IMSI 最多可以由 15 位数字组成，包括：3 位数字的移动国家码、2 位数字的移动网络码和 10 位数字的移动台识别号。其中 MSIN 的结构中一般又包括 3 位数字的区域码、3 位数字的局域码和四位数字的个人电话号码这 3 个部分。IMSI 可以通过一个固定的换算方法[3]转换为二进制比特串。

由以上的结构可以看出，IMSI 中的移动国家码、移动网络码、区域码和局域码的组合已经提供了所需的路由信息，足以使得 VLR 找到 HLR/AuC，这 4 个部分的组合是必须用明文传送的，为了下面叙述的方便，我们将这 4 部分组合形成的二进制串称作 IMSIr，其中小写的 r 指“路由信息”。也就是说，IMSI 由 IMSIr 和个人电话号码两个部分组成。这时，就可以加密个人电话号码部分，实现用户身份的保密性。这里给出两种方法。

方法 1　基于公钥算法的方法　在这个方法中应该为每一个 HLR/AuC 配置一个公钥，而且要在分发给用户的智能卡中存储相应的 HLR/AuC 的公钥，过程如图 3。其中 KuAuc 是 HLR/AuC 的公钥，enc( )是公开密钥加密函数，它的第一个参数是公钥，第二个参数是要被加密的内容，符号“‖”表示两个二进制串的串接，Rand 是由用户端产生的固定长度的随机数。

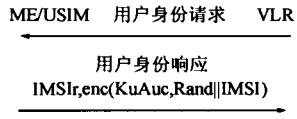

图 3　基于公钥算法的方法 1

当用户收到 VLR 的身份请求后，用户作出响应，其中包含明文的 IMSIr 和用 KuAuc 加密的 Rand||IMSI；VLR 收到这个响应以后，根据 IMSIr 的路由信息将 enc(KuAuc, Rand||IMSI)发送到 HLR/AuC，后者使用解密函数 dec(KrAuc, enc(KuAuc, Rand||IMSI))得到 IMSI 的明文，其中 KrAuc 是相应于公钥 KuAuc 的解密私钥；然后可以由 IMSI 从数据库中索引出相应的鉴别信息，完成后续的鉴别和密钥协商过程。Rand 的值在解密后弃置不用，发送端使用它的原因如下：如果我们不使用 Rand 而直接发送 enc(KuAuc, IMSI)，那么尽管攻击者无法解密出明文的 IMSI，但是攻击者在连续的窃听当中将得到同样的密文，从而能够对同一个用户进行跟踪定位，这会间接地危及用户身份的保密性。

方法 2　基于对称密钥算法的方法　在这个方法中，不需要额外配置密钥信息，只需要利用智能卡和 HLR/AuC 中的对称主密钥 K。这个方法的主要思想在于通过将 IMSI 中的个人电话号码部分进一步划分为加密部分和明文部分，将用户的真实身份标识隐蔽在一组用户的身份标识当中。例如我们可以将个人电话号码比特串的最后 5bit 保留为加密部分，前面的其余比特保持为明文传送，这两个部分分别记作 IMSIuni 和 IMSIi，其中小写的“uni”和“i”分别指 unimportant 和 important，即 IMSI 由 IMSIr、IMSIi 和 IMSIuni 三个部分组成。这时，加密保护 IMSIuni 部分，实现用户身份的保密性，过程如图 4。其中 K 是用户和 HLR/AuC 共享的主密钥，enc( )是对称密钥加密函数，而且采用密码分组链接(Cipher BIock Chaining, CBC)工作模式，它的第一个参数是密钥，第二个参数是要被加密的内容，Rand 是由用户端产生的固定长度的随机数，它的作用与方法 1 中的相同。

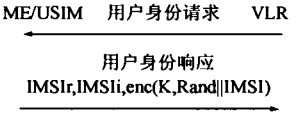

图 4　基于对称密钥算法的方法 2

当用户收到 VLR 的身份请求后，用户作出响应，其中包含明文的 IMSIr 和 IMSIi 以及用 K 加密的 Rand||IMSI，与图 3 中最大的不同在于传送了明文的 IMSIi；VLR 收到这个响应以后，根据 IMSIr 的信息将 IMSIi 和 enc(K, Rand||IMSI)一起发送到 HLR/AuC，但是这时 HLR/AuC 不可能通过直接使用解密函数 dec(K, enc(K, Rand||IMSI))立即得到 IMSI 的明文，因为此时没有完整的用户身份信息，因此也就不能立即从数据库中得到 K。然而，HLR/AuC 知道这个用户可能是哪些用户之一，所以只要在所有可能用户范围内遍历一遍(在上面的例子中，IMSIuni 为 5bit，所以可能用户的数量为 32)，而且用相应密钥解出的 IMSI 符合一定的条件的用户就是目标用户，这个处理过程可以用图 5 所示流程图说明。

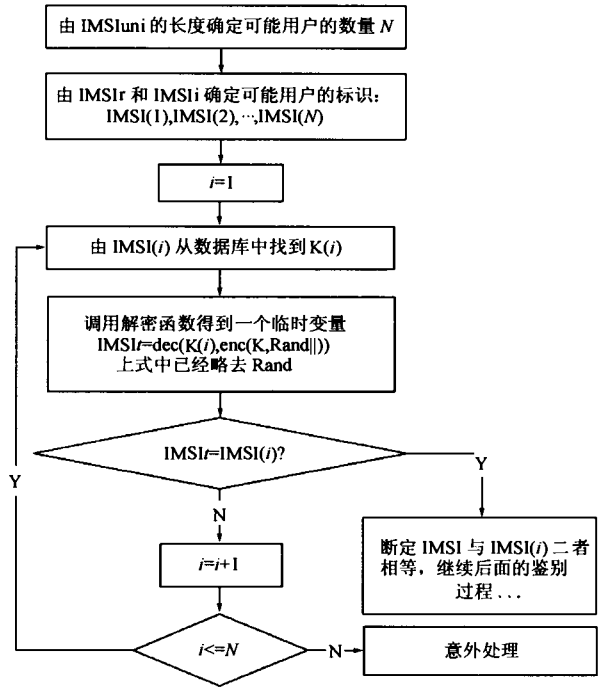

图 5　方法 2 中 HLR/AuC 的处理流程

为了提高加密解密算法的性能，对于方法 1 可以采用 Rabin 的模平方根密码体制[4]。这种密码体制的优点在于它是一种非对称的算法，即用户端加密的开销远小于网络端的解密开销，对于用户端有限的处理能力和有限的电池蓄电能力而言尤其适合。而方法 2 本身明显是非对称的算法，即用户端只运行一次加密算法，网络端平均运行 $N/2$ 次解密算法。由于方法 2 是对称加密体制，所以在同样加密强度下，方法 2 的运算速度会比方法 1 的速度快。再有，一般来说，VLR 要求用户提供 IMSI 的情况并不会频繁出现，所以本文提出的方法的运算开销对系统影响很小，它们是可行的方法。如果由于 VLR 的数据库出现问题导致 VLR 要求用户提供 IMSI 的情况频繁出现，那么采用方法 2 仍然是可行的。

4 结束语

本文提出的两种方法都是对用户身份保密性的增强方法，虽然它们都是以明文形式来传送用户的归属信息，即 HLR/AuC 的位置，但是它们都将用户的真实身份隐蔽在几十个用户标识(方法 2)甚至成千上万个用户标识(方法 1)里，使得攻击者不能确切地得到用户身份的具体信息。对于攻击者来说，他已经不能确保跟踪定位同一个用户，对一群潜在的合法用户跟踪定位，显然对于攻击者已经没有什么意义了。可见，这两种方法都明显比现有移动通信标准增强了用户身份的保密性。

实际上，要想将包括归属环境的路由信息在内的整个用户身份标识全部保护起来，只有一个方法能够做到：利用公钥密码学，每个 VLR 广播自己的加密公钥，用户就可以用这个公钥将自己的标识加密后传送给 VLR，如文献[5]中提到的方法。但是，由于用户与 VLR 间预先不存在任何信任关系，所以 VLR 不能只是广播自己的公钥，而是应该广播自己的公钥证书。这样一来，就需要有一个可信的第三方——证书权威机构(Certification Authority, CA)。使用公钥证书，一方面，会增加运营商的成本，另一方面，还有待成熟的公钥基础设施(Public Key Infrastructure, PKI)的出现，这还需要一段很长的时间才能成为现实。

因此，采用本文提出的方法是目前达到加强用户身份保密性的比较有效而实际的选择。

参 考 文 献

[1] 赖溪松，韩亮，张真诚，张玉清，肖国镇改编. 计算机密码学及其应用. 北京：国防工业出版社，2001：178－184.

[2] 3GPP TS 33.102 (V6.0.0): 3rd Generation Partnership Project (3GPP); Technical Specification Group (TSG) SA; 3G Security; Security Architecture. Sep. 2003, URL: http://www.3gpp.org/ftp/Specs/archive/33_series/33.102/

[3] Rhee M Y 著，袁超伟等译. CDMA 蜂窝移动通信与网络安全. 北京：电子工业出版社，2002：241－243.

[4] Stinson D R 著，冯登国译. 密码学原理与实践. 北京：电子工业出版社，2003：172－176.

[5] Curtis H W. Subscriber authentication and security in digital cellular networks and under the mobile Internet protocol. [Master Thesis], The University of Texas at Austin, May 2001, URL: http://www.portelligent.com/forms/HCThesis.pdf

赵源超： 男，1971 年生，博士生，从事移动通信安全方面的研究.

李道本： 男，1939 年生，教授，博士生导师，主要从事 Las-CDMA 移动通信系统的研究.