 DOI: https://doi.org/10.36956/iser.v2i1.363

# Research on Security System and Countermeasures of Mobile Communication System

**Yuning Zhou**

Huazhong University of Science and Technology, Wuhan, Hubei, 430074, China

**Abstract**

The conceptual security architecture framework (OSI/RM) proposed in the Open System Interconnection Reference Model defines five groups of security services: authentication services, confidentiality services, data integrity services, access control services, and non-repudiation services. The information security architecture based on the seven-layer protocol of the OSI reference model is a three-dimensional matrix composed of security attributes, OSI protocol layers and system components. It has important guiding significance for the information security architecture of the specific network environment. According to the characteristics of the mobile communication system, the paper gives the three-dimensional framework structure of the mobile communication system security system with reference to the 3G security domain structure and the OSI security system structure.

**Keywords**

mobile communication system; network security; system; countermeasures

# 移动通信系统的安全体系及对策研究

周宇宁

华中科技大学，中国 · 湖北 武汉 430074

**摘　要**

开放系统互联参考模型中提出的概念性安全体系结构框架（OSI/RM）定义了 5 组安全服务：认证服务、保密服务、数据完整性服务、访问控制服务、抗抵赖服务。基于 OSI 参考模型的七层协议之上的信息安全体系结构由安全属性、OSI 协议层和系统部件组成的三维矩阵，它对具体网络环境的信息安全体系结构有重要的指导意义。论文根据移动通信系统的特点，参考 3G 安全域结构和 OSI 的安全体系结构给出了移动通信系统安全体系的三维框架结构。

**关键词**

移动通信系统；网络安全；体系；对策

## 1 引言

随着电子信息技术的发展，各种网路技术不断融入到移动通信系统中，3G 移动通信系统得到广泛的应用，移动通信的用户也是越来越多，移动通信系统的网络安全问题已经受到人们的关注和重视，研究移动通信系统的网络安全问题对于提升通信安全具有十分重要的作用和意义。

## 2 移动通信系统的安全体系概述

安全服务轴（S）包括认证（鉴权）、访问控制、数据完整性、数据保密性和不可否认 5 个元素，各元素之间的关系是层次关系。安全需求轴（N）参照接口协议的分层和 OSI 参考模型的分层模型，包括物理层安全、链路层安全、控制层安全、用户层安全和管理层安全。安全域轴（F）由不同的安全域组成，安全域的划分由具体的安全策略确定。整个 TETRA 系统的安全域可以初步划分为网络接入域、网络域和用户域。

系统的任何一个安全措施都可以映射成这个三维空间的一个点，可以解释为每个安全措施都是在某个安全域内，为满足某个层次上的安全需求而提供的某种安全服务。

下面从安全服务、安全需求以及安全域三个方面详细讨论移动通信安全体系所涉及的要素和逻辑关系以及相关的安全技术。

## 3 安全服务

移动通信安全体系的安全服务包括认证和密钥管理服务、访问控制服务、数据完整性服务、数据保密性服务以及

 DOI: https://doi.org/10.36956/iser.v2i1.363

不可否认性服务等方面。各种安全服务之间存在相互依赖的关系，单独采用其中的一种安全服务无法满足移动通信系统的安全需求。这些安全服务之间的关系可以看成是一种层次关系。

其中实体 1 或实体 2 可以根据不同的安全域代表移动通信系统中不同的构件。例如，在用户域内可能分别代表安全模块和移动终端 . 在接入域内代表移动终端和网络基础设施，在网络域内则可以代表两个交换机或交换机和基站。所有的移动通信系统的安全服务都依赖主体与客体的身份标识和认证，主要实现的技术有系统和移动终端之间的鉴权协议、公钥基础设施和智能卡技术等 ; 访问控制是整个安全系统的核心，其目标是防止对任何资源进行非授权的访问，它对数据保密性和完整性所起的作用是十分明显的；数据的完整性和保密性确保数据在流通中不被篡改和窃取，它们是认证和访问控制有效性的重要保证，可以采用的技术包括空中接口加密和端到端加密等；不可否认服务是数字集群通信系统一个必不可少的安全服务，一般采用合法的监听来防止用户否认自己的通话。具体讨论如下。

### 3.1 认证服务和密钥管理

对一个实体进行鉴权就是接收到该实体的标识后证明该标识是真实的。在移动通信系统的接入域中，根据实际需要，鉴权可以是双向的，也可以是单向的。一般在移动终端接入网络或一次通话开始时需要鉴权，由系统的安全策略来决定鉴权的频度。密钥管理是产生、分发、选择、删除和管理在鉴权和加 / 解密的过程中使用的密钥的过程。没有发送和接收密钥的双方的双向鉴权就无法安全分发密钥。因此密钥管理和鉴权的关系非常紧密。

移动通信系统中的认证服务包括用户和网络之间签权、网络实体之间的认证以及在终端内安全服务模块和终端的认证等。密钥管理包括空中接口鉴权密钥的密钥管理、空中接口机密性和完整性服务的密钥管理、端到端保密通信的密钥管理等部分。

### 3.2 访问控制

访问控制的目标是防止对任何资源（这里主要是通信资源和信息资源）进行非授权访问。非授权访问包括未经授权的使用、泄露、修改、销毁以及颁发指令等。访问控制直接支持数据保密性、数据完整性、数据可用性以及合法使用的安全目标。在移动通信系统中访问控制的需求广泛存在，例如，为了保护系统基础设施，网络运营商需要：

防止对无线资源的非授权使用；

防止对服务的非授权使用；

对数据库需要进行访问控制；

对配置和网络管理需要进行访问控制；

终端的使能 / 禁用。

### 3.3 完整性服务

数据完整性是指接收方接收到的数据和发送方发送的数据保持一致。数据源鉴别用来检查数据源标识的真实性和发送该级别数据的资格。显然，只有在进行通信的双方进行鉴权后，数据完整性和数据源鉴别服务才有用。鉴权过程可用来提供安全参数和所需的密钥。

移动通信系统中的完整性服务主要是指信令数据的完整和数据源的鉴别功能，该服务可以确保和检查终端与核心网络之间的控制信息的完整性，并提供检查信息源的方法。

### 3.4 数据保密性服务

移动通信系统保密性服务的目的是保护敏感数据，防止存储在系统内和传输过程中的敏感数据被某个无权得到该数据的用户、实体或过程故意或偶然获得。一般采用加 / 解密来实现保密性服务。保密性服务需要和其他安全服务共同配合才能达到保护敏感数据的目的。例如，采用访问控制机制来防止对存储的数据和用来进行加解密的过程的非授权访问，在终端进行通信前需要进行鉴权，一般鉴权协议执行过程会产生进行空中接口加密的会话密钥。

移动通信系统的保密性服务不仅包括移动终端和核心网络之间（即空中接口）的语音、信令和数据保密，还包括端到端的语音和数据保密通信，以及用户标识和组标识的保密性服务等。其中用户标识的保密性服务是指，保证移动通信的个人用户标识或个人用户短标识不被非授权的个人、实体和过程获得 ; 组标识的保密性服务特指在集群移动通信系统中，组用户标识不被非授权的个人、实体和过程获得，而且保证从个人用户标识无法得到组用户标识，反之亦然，当然，组标识的保密可以通过部分信令的保密性服务来实现。

### 3.5 不可否认性服务

不可否认性服务的主要目的是保护通信用户免遭来自系统其他合法用户的威胁，而不是来自未知攻击者的威胁。具

 DOI: https://doi.org/10.36956/iser.v2i1.363

体是指，防止参与某次通信交换的一方事后否认曾经发生过本次交换。

在专有网络中经常采用合法的监听来防止用户否认自己的通话。一般某个组织管理者需要监听其组织内部的流量和通信，调度台用户需要监听其所管理的各个组的流量和通信，某个授权用户需要监听他所在的组或其他组的流量和通信情况。在某种程度上监听与机密性等安全服务有些对立，这需要系统的规划者、管理者和使用者合理设计、实施和使用这些安全服务。

## 4 安全需求

移动通信系统安全体系结构的 N 轴从下到上分别对应物理层、链路层、控制层、用户层和管理层。

相应的安全需求定义如下：

### 4.1 管理层

管理层位于安全需求的最上层，包括对安全威胁的管理和制定合理的管理标准。管理层对所有信息的安全负责，确定移动通信系统与其他系统连接时可能会暴露的漏洞，确定被保护的资源和使用的安全技术。

### 4.2 用户层

用户层安全提供事务处理的端到端安全。如果安全业务是应用层特有的，或者需要经过应用中继，则其安全性需要在本层上进行设置。移动通信系统中的端到端保密通信需求一般处在这个层面上。如果对通话内容进行端到端的保护，只有通信的端用户知道所用的密钥，则尽管信息经过了基站、交换机等中继系统，但因为这些中继系统对所用的密钥一无所知，因此也无法了解通信的内容。在其他基于用户层的应用中，如数据检索等需要保护特定服务的信息和处理，可能的安全服务包括验证、加密、数字签名、日志以及恢复机制等。有些安全服务，如不可抵赖只能在用户层实现。

### 4.3 控制层

负责网络过程。其中鉴权和用户管理等安全服务需要在该层的子网络接入功能中实现。

### 4.4 链路层

链路层主要保证数据在无线电线路上传输的正确性和安全性，一般采用 TDMA 帧同步、交织 / 去交织、信道编码、差错保护、空中接口加密等技术来实现。

### 4.5 物理层

移动通信系统的物理层由定时结构、无线电射频发射和接收等部分组成，其安全主要是防止物理通路的损坏、对物理通路的窃听和攻击干扰等。防止机房、电源、监控等场地设施和 UPS 周围环境的破坏，同时应具备对系统关键设备的备份手段。

## 5 安全域

### 5.1 网络接入域安全

网络接入域安全主要提供安全接入服务，包括用户身份保密性、用户认证、在网络接入信道和设备间传输数据的保密性和完整性、移动设备的鉴定。主要是通过临时身份号码来保证用户身份号码的保密性；采用基于对称密钥算法的双向认证协议来进行用户接入的认证和加密密钥与完整性密钥的协商。利用国际移动设备号来鉴别移动设备。

### 5.2 网络域安全

主要提供网络实体间（如交换机和基站之间，交换机和交换机之间）的认证、数据传输保密性和完整性、攻击信息的监视等安全机制。

### 5.3 用户域安全

主要提供终端安全服务模块（可能是终端内的模块或智能卡）与用户间的认证以及终端安全服务模块与移动终端间的认证。用户与终端安全服务模块间认证通常采用 PIN（个人识别码），而终端安全服务模块与移动终端间的认证通常采用共享秘密信息的方法。

## 6 移动通信系统的网络安全策略研究

### 6.1 移动通信系统的数据完整性研究

在执行密匙协商的过程中能够实现移动通信系统用户数据完整性的密匙协商，在用户和网络之间的安全模式协商机制能够实现完整性算法协商，而移动通信系统中的网络和 MS 之间的多数指令信息都需要提供完整性保护，在 3G 移动通信系统中为了确保用户和网络之间的信息指令不会被篡改，可以通过消息认证的方式来实现。

首先需要数据信息发送方将需要传递的数据信息使用完整性密匙将 F9 算法产生的消息认证码 MAC 附在发出数据信

 DOI: https://doi.org/10.36956/iser.v2i1.363

息的后面，数据信息接收方只需要将接收到的信息使用同样的方法得到 XMAC，然后将 XMAC 和 MAC 进行比较，如果两者相同，则表示数据信息的完整性，反之数据信息不完整。3G 移动通信系统数据信息的完整性主要表现在完整性算法协商、数据和指令的完整性以及完整性密匙协商三个方面。

### 6.2 移动通信系统的用户身份保密性研究

用户身份保密性主要涉及到以下几个主要方面。（1）用户身份的机密性，确保移动通信系统的用户的真实身份不会在无线链路中被盗用和窃听；（2）用户所处位置的机密性，确保所有移动通信系统的用户的即时位置在无线接入链路中使用窃听等手段来确定；（3）用户信息的不可追溯性，确保入侵移动通信系统的人无法通过无线接入链路得出用户的信息。移动通信系统为了确保用户身份的机密性，往往是通过设置常用的临时身份来识别用户身份，对于用户信息的可追溯性问题，系统可以应用不同的临时身份来识别和判断某一位用户的方法来解决，此外对于可能泄露用户身份的所有数据信息在无线接入链路上都应该采取加密措施，来提升信息传输和接受的安全性。

### 6.3 移动通信系统的认证系统

为了避免移动通信系统受到伪基站的攻击，提升移动通信系统的通信安全，可以采用双向认证方式，对 MS 和基站以及基站和 MS 进行认证，移动通信系统应该保证用户和网络之间建立的每一个连接的假设实体认证机制都能够发挥作用。双向认证鉴权向量的 5 个参数分别为期望相应、RAND、加密密匙、鉴权令牌和完整性密匙，其中完整性密匙能够对无线接入链路的数据的完整性提供有效保护，无疑增强了移动通信系统用户对网络测合法性的鉴权，大大确保网络安全。

### 6.4 移动通信系统数据保密性研究

3G 移动通信系统在密匙长度加长的同时，引入加密算法协商机制，提供基于端到端的全网加密方式，采用以交换设备为主的安全机制来确保数据信息在网络中的传输安全。3G 移动通信系统中的网络接入部分数据保密有加密密匙协商机制、机密算法协商机制、信息质量数据加密机制和用户数据加密机制四个方面。

## 7 结语

移动通信系统有确保自身信息传输和终端接入网络以及用户信息传递和接入网络的安全性，如何解决这些网络安全问题是影响移动通信系统发展的关键所在。

## 参考文献

[1] 谢磊 . 移动通信系统的网络安全问题研究 [J]. 信息通信 ,2013 (010):208.

[2] 张绍林 . 对移动通信系统中常见安全问题的思考 [J]. 中国新通信 ,2014 (011):56+57.

[3] 朱里奇 . 第三代移动通信系统 (3G) 安全性研究 [D]. 武汉 : 华中科技大学 ,2004.

[4] 黎杰文 . 超宽带无线通信系统中同步若干关键技术的研究 [D]. 重庆 : 重庆邮电大学 ,2008.

[5] 钱芳 . 移动通信系统的安全性研究 [J]. 计算机安全 ,2012 (004):25−28.

[6] 张振波 .4G 无线网络安全若干关键技术研究 [J]. 科技创业家 ,2014(05):7.

[7] 刘忠明 . 基于 3G 移动通信系统的安全问题研究 [J]. 信息与电脑 : 理论版 ,2013(006):67−68.

[8] 高建辉 , 祁建华 .3G 移动通信中的安全问题研究 [J]. 内江科技 ,2010(12):132−133.

[9] 范明钰 . 第三代移动通信系统的安全体系 [J]. 信息安全与通信保密 ,2000(03):1−4.

[10] 邓所云 , 胡正名 , 钮心忻 , 等 . 移动通信中的双向认证与密钥协商新协议 [J]. 北京邮电大学学报 ,2002,25(2):54−56.

[11] 安华萍 , 贾宗璞 .3G 移动网络的安全问题 [J]. 科学技术与工程 ,2005,5(6):375−378.

[12] 3G 移动通信系统的安全体系与防范策略 . 信息安全与通信保密 [J],2009(8):22−23.