# 移动通信网的内生安全共性问题及破解之道

刘彩霞[1,2]，季新生[1]，邬江兴[1]
（1. 国家数字交换系统工程技术研究中心，河南 郑州 450002；2. 军事科学院系统工程研究院，北京 100091）

**摘 要**：基于对移动通信本质特征及移动通信网固有特性的认识，从一个全新的视角剖析了移动通信网固有机制尤其是移动性管理机制存在的基因缺陷，这些基因缺陷不会随着移动通信网的代际发展而消失，因而，又被称为移动通信网的内生安全缺陷或者内生安全共性问题。给出了“信息真实性默认”“数据泛在可见”等安全缺陷可能引入的内生安全威胁，并在网络空间内生安全理论的指导下，提出用“零信任”打破“默认的信任”、以“变隐映射”实现用户数据的“限定可见”等化解移动通信网内生安全共性问题的思路和方法。

**关键词**：移动通信网；5G；内生安全问题；内生安全构造；变隐映射
**中图分类号**：TN929.5
**文献标志码**：A
**DOI:** 10.11959/j.issn.1000−436x.2022176

# Endogenous security common problems and solutions of the mobile communication networks

LIU Caixia[1,2], JI Xinsheng[1], WU Jiangxing[1]
1. National Digital Switching System Engineering &Technological R&D Center, Zhengzhou 450002, China
2. Academy of Military Sciences, Institute of System Engineering, Beijing 100091, China

**Abstract:** Based on the understanding of the mobile communication essential characteristics and the mobile communication network inherent characteristics, from a new perspective, the genetic defects existing in the mobile communication network inherent mechanism, especially in the mobility management mechanism were analyzed. These genetic defects would not disappear with the intergenerational development of mobile communication network, therefore, they were also known as endogenous security defects or endogenous security common problems of mobile communication networks. The endogenous security threats that may be introduced by security defects such as “acquiescence in information authenticity” and “ubiquitous data visibility” were pointed out. Under the guidance of the cyberspace endogenous security theory, the ideas and methods to solve the endogenous security common problems in mobile communication networks were proposed, such as breaking the “default trust” with “zero trust” and realizing the “user data limited visibility” with “variable implicit mapping”.

**Keywords:** mobile communication network, 5G, endogenous security problem, endogenous security structure, variable implicit mapping

## 0 引言

移动通信网作为国家最重要的信息通信基础设施之一，在国家战略、国计民生、国防建设等方面发挥着越来越重要的作用，尤其是进入 5G 移动通信时代，随着新技术的赋能，5G 网络作为国家“新基建”的首选，被赋予为国家经济高质量可持续发展和网络强国建设提供新引擎的重任[1]，并为

**收稿日期**：2022−06−27；**修回日期**：2022−08−19
**基金项目**：国家自然科学基金创新群体基金资助项目（No.61521003）
**Foundation Item:** The National Natural Science Foundation Innovation Group Project (No.61521003)

工业、能源、交通、医疗等垂直行业提供通信服务，成为移动通信网的新使命，移动通信技术发展和网络建设的战略意义达到空前高度。据统计，截至 2022 年 2 月，我国移动通信用户数达到 16.48 亿，其中 5G 用户达到 3.84 亿。

移动通信网的战略地位得到高度重视的同时，其安全问题也成为业界关注的焦点。国外以 3GPP、国际电信联盟电信标准局（ITU-T, Telecommunication Standardization Sector of the International Telecommunications Union）、全球移动通信系统协会（GSMA, Global System Mobile Association），国内以中国通信标准化协会（CCSA, China Communications Standards Association）、IMT-2020(5G)推进组等为代表的标准化组织均成立了专门的移动通信安全研究组，大力开展移动通信系统尤其是 5G 系统的安全和标准化研究工作，已经形成系列研究报告、白皮书和安全标准[2-13]，内容涉及移动终端、IT 化网络基础设施、通信网络、应用与服务、数据、运营管理等多个方面。相对于传统移动通信网，新技术和新标准赋能的 5G、B5G 移动通信网的安全能力大大提升，尤其是 2G/3G/4G 移动通信网普遍存在的空中接口用户信息泄露、核心网缺乏访问控制、网间互通缺乏有效监管等问题得到大大改善，一定程度上弥补了传统移动通信网被业界普遍关注的安全缺陷。但是，移动通信机理决定移动通信网即使代际更新，也依然有其自身固有的通信机制，即使网络架构、协议体系、业务提供方式等发生变化，其固有的通信机制也不会改变，例如，移动通信不会改变其无线通信的特点，也不会改变其“支持用户广泛移动”的特点。根据事物矛盾的双面性，移动通信网固有的通信机制必定存在安全缺陷[14]，本文称之为基因缺陷或者移动通信网的内生安全缺陷或者内生安全共性问题，这些安全缺陷在理论和工程层面不可能依赖“补丁式”或“外挂式”安全机制彻底消除[14]，需要具有“内生安全特性”的体制或者机制来有效规避或化解[15]。

本文基于移动通信网的通信机理和固有通信机制，剖析了移动通信网的内生安全共性问题及可能带来的安全威胁，并在邬江兴院士解决网络空间内生安全问题相关理论[14-15]的指导下，研究提出了解决移动通信网内生安全问题的一些思路和方法。

## 1　移动通信网的内生安全共性问题

“支持终端随意移动”和“依赖用户实时位置提供服务”是移动通信的本质特征。因此，移动通信网的终端接入只能依赖无线通信，而对移动终端或用户实施移动性管理也是移动通信网的固有功能。可以认为，“无线通信”和“用户移动性管理”是移动通信网的固有特性，也就是说，随着代际发展，新技术不断引入，网络架构、协议体系、业务提供模式等不断演进，移动通信网的服务能力越来越强，但其固有特性不会改变。基于“任何事物都是矛盾的统一体”这个共识[16]，移动通信网在提供方便快捷和泛在通信服务的同时，其固有功能或者特性必然存在显式的副作用或者隐式的暗功能。一些非良性的副作用或者暗功能，本文称之为移动通信网的内生安全缺陷或者内生安全共性问题[15]，某种意义上也可以称之为移动通信网的“基因缺陷”。这些内生安全共性问题或者基因缺陷在外部因素的作用下，则可能产生“内生安全威胁”[15]。文献[17]介绍了无线环境的内源性缺陷以及由此引发的无线内生安全问题，本文则主要分析移动通信网“移动性管理”机制的基因缺陷以及相关缺陷可能引入的内生安全威胁。

### 1.1　代理通告机制存在“信息真实性默认”缺陷

“移动性管理功能”是移动通信网为用户提供服务的基础。为支持用户的移动性，避免用户位置信息被频繁传递，移动通信网采用分布式管理模式，包括以下三级：归属域网络功能，如 3G 网络的归属位置寄存器（HLR, home location register）、4G 网络的归属用户服务器（HSS, home subscriber server）、5G 网络的用户数据管理（UDM, user data management）功能，下文统一用 HNF（home network function）表示；拜访地网络功能，如 3G 网络的拜访位置寄存器（VLR, visitor location register）、4G 网络的移动性管理实体（MME, mobile management entity）、5G 网络的接入管理功能（AMF, access management function），下文统一用 VNF（visitor network function）表示；基站子系统（BSS, base station subsystem），如图 1 所示。HNF 存放用户当前所在的 VNF 服务区信息、签约身份标识和签约服务清单，后两者在下文统称为用户身份信息；VNF 存放用户当前所在的基站位置区信息。

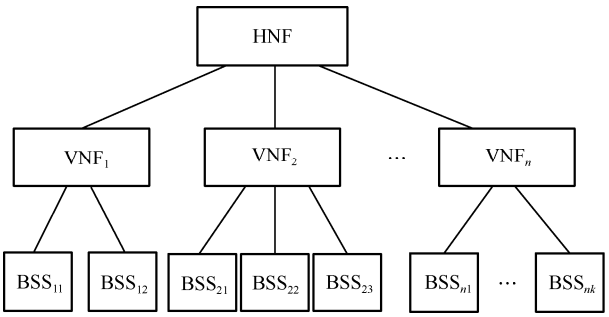



图 1　移动通信网的分布式位置信息管理示意

当用户的位置发生变化时，如果只涉及同一个 VNF 管辖的服务基站，其信息变化只在该 VNF 中处理；当用户跨 VNF 服务区移动时（如图 2 所示），其当前服务 VNF（如图 2 中的 $VNF_2$）会依据终端发起的位置注册或者位置更新请求，向用户的归属 HNF 通告用户的位置变化（图 2 中的过程①），HNF 收到通告后，首先向用户先前的服务 VNF（如图 2 中的 $VNF_1$）发送删除用户位置和身份信息的通告（图 2 中的过程②），然后存储用户更新后的位置信息，并将用户的身份标识和部分签约服务数据（下文简称部分身份信息）通报给 $VNF_2$（图 2 中的过程③）。由图 2 可知，在用户的移动性管理流程中，$VNF_2$ 和 HNF 分别作为“终端代理”间接向 HNF 和 $VNF_1$ 通告终端或者用户的位置信息变化，而 HNF 也作为“运营商代理”向 $VNF_2$ 通告用户的身份信息。本文将上述“通告”流程称为移动通信网的“代理通告”机制。

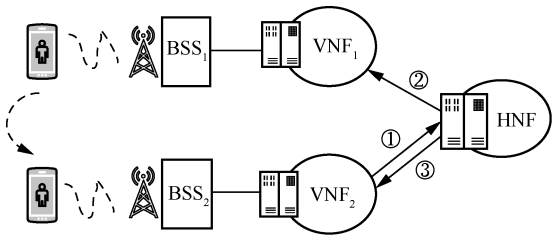



图 2　移动通信用户的位置更新通告流程

通过分析不难看出，移动通信网对用户身份和位置信息的“代理通告”机制会伴随如下安全问题。

1) HNF 可以核实用户签约身份的真实性和合法性，但对用户当前所处位置信息的掌握依赖于 VNF 的通告，对 VNF 通告的用户位置信息默认其是真实准确的，HNF 本身无法实时核实该用户所处位置的准确性。

2) VNF 可掌握终端上报的准确位置信息，但是对 HNF 通报的用户身份信息也是默认真实准确的，在当前的通信机制下，VNF 无法实时核实用户身份信息的真实性。

本文称上述问题为移动通信网的信息“真实性默认”缺陷。这种信息“真实性默认”缺陷在电信运营商管控的封闭环境下，安全问题难以显现。但是随着移动通信网从 1G/2G 发展到 3G/4G 乃至 5G/B5G，移动通信网与互联网逐渐融合走向开放，原有的封闭环境已不复存在，随之而来的“合法网元被挟持攻击”、由漏洞后门引发的“信息篡改攻击”等暴露了这种信息“真实性默认”缺陷极大的安全问题[18]。

为了应对移动通信网复杂开放环境下的弱信任挑战，国际标准组织也在不断努力，主要的措施集中在针对开放环境增加信任措施，例如，添加网络功能间的认证授权机制、增加信息传递过程的机密性和完整性保护机制等[19]，很明显，这些机制可以在一定程度上保证网络功能的合法性和网络功能间信息交互的安全性，但难以保证信息的可信性，也就是说，原理上，这些安全机制无法验证合法的网络功能假冒“代理身份”发起的虚假信息通告，也无法验证合法的网络功能作为“代理身份”通告的信息真实性。

事实上，这种“真实性默认”缺陷也渗透在移动通信网信息访问交流的方方面面，包括移动通信网中各种网元设备之间交互信令消息和协议流程等都秉持默认的真实性，只要收发消息的是“自己人”（即拥有合法网元身份），就不再过多分析判断信息本身、信息行为等的合理性，伴随网络环境的开放和信任边界的模糊，移动通信网的“真实性默认”缺陷已经成为近年来频频曝光的多种移动通信核心网窃密攻击的出发点，事实上也成为当前移动通信网安全防护的“死穴”。

### 1.2　“分布式管理”机制导致用户数据泛在可见

如前所述，移动通信网为支持用户移动或者漫游，对与用户身份和位置信息关联的用户数据采用分布式的三级管理机制。当用户移动到一个新的基站无线信号覆盖区或者拜访地服务区时，不仅终端要逐级通告自身的实时位置标识，用户的身份标识也会从归属 HNF 流向用户拜访地的 VNF；网络为用户提供服务的过程中，用户的身份标识、位置标识、签约数据、动态业务数据等会在移动通信网的不同网络功能或者基站的无线覆盖环境中传递和使用。也就是说，随着用户移动，用户数据可能在用户可达的所有网域和

网络功能中广泛传递、存储和使用。表 1 为用户数据在 3G 网络不同网元的分布情况，表 2 为用户数据在 5G 网络不同网络功能的分布情况。

尤其是当用户漫游到境外网络时，用户的身份和位置等关联数据也会如图 3 虚线箭头所示，在境内、境外网络的传输通道以及境内、境外网络的不

**表 1　　用户数据在 3G 网络不同网元的分布情况**

| 网元名称 | 静态存储或者动态获取的用户数据类型 | 备注 |
| --- | --- | --- |
| VLR | 1) 用户标识数据：私有身份标识，公开身份标识，终端标识，临时身份标识，路由标识；<br>2) 用户位置信息：基站小区标识，基站位置区标识等；<br>3) 用户鉴权数据：AKA 鉴权向量；<br>4) 用户签约数据：签约业务清单，业务或者漫游权限 | 随用户在境内、境外网络漫游，相关用户数据会遍布用户所到的所有 VLR |
| HLR | 1) 用户标识数据：IMSI，MSISDN，IMEI 等；<br>2) 用户位置信息：MSC 号码，VLR 号码，MSCID，BSID<br>3) 用户鉴权数据：根密钥，鉴权算法；<br>4) 用户签约数据：签约业务清单（电信业务、补充业务、智能网业务等），业务权限，漫游权限等 | |
| 短消息中心（SMSC, short message service center） | 用户标识数据，用户位置信息，短消息内容 | |
| 智能网业务控制点（SCP, service control point） | 用户签约的智能网业务数据，用户标识数据，用户位置信息 | |
| 全球移动定位中心（GMLC, global mobile location center） | 用户定位业务签约数据，用户身份标识，用户位置信息 | |

**表 2　　用户数据在 5G 网络不同网络功能的分布情况**

| 网络功能 | 静态存储或者动态获取的用户数据类型 | 备注 |
| --- | --- | --- |
| AMF | 1) 用户标识数据：私有身份标识，公开身份标识，终端标识，临时身份标识；<br>2) 用户位置信息：基站小区标识，跟踪区标识等；<br>3) 用户 UE 上下文信息：为用户服务的 UDM、AUSF、PCF、SMF 等标识，会话状态相关数据；<br>4) 用户鉴权数据：AKA 鉴权向量，EAP 鉴权向量；<br>5) 用户签约数据：签约业务清单，业务权限，漫游权限等；<br>6) 切片相关信息 | 随用户在境内、境外网络漫游，相关用户数据会遍布用户所到的所有 AMF |
| UDM | 1) 用户标识数据：SUPI，GPSI，PEI 等；<br>2) 用户鉴权数据：根密钥，鉴权算法标识，SUPI 隐私保护计算密钥，SUPI 加密算法标识等；<br>3) 用户签约数据：用户切片信息，用户 5G 业务签约信息，签约切片列表，默认网络切片等；<br>4) 用户签约的短消息业务参数；<br>5) 会话管理签约数据：签约的 DNN 列表，PDU 会话类型，SSC 模式，QoS 参数、计费特性，静态 IP 地址等；<br>6) 用户服务网络网元地址：用户在 3G 网络、4G 网络和 5G 网络的服务网元标识；<br>7) 用户当前服务 AMF 相关数据；<br>8) 用户当前服务 SMF 相关数据；<br>9) 用户当前服务 SMSF 相关数据 | |
| 统一数据存储（UDR, unified data repository）功能 | 用户鉴权数据，用户会话数据，用户策略数据，用户营账操作记录数据等 | |
| 网络注册功能（NRF, network register function） | 1) 用户不同服务网络功能 NF 的注册信息：SUPI, GPSI, DNN, sNSSAI, AMF 区域, AMFSetID 等；<br>2) NF 订阅的其他 NF 的状态信息。 | |
| 会话管理功能（SMF, session management function） | 用户会话管理签约数据，用户身份标识，会话管理动态数据 | 随用户在境内、境外网络漫游，相关用户数据会遍布用户所到的所有 SMF |
| 短消息服务功能（SMSF, short message service function） | 用户短消息签约数据，用户身份标识，用户位置标识 | |
| GMLC | 用户定位业务签约数据，用户身份标识，用户位置信息 | |

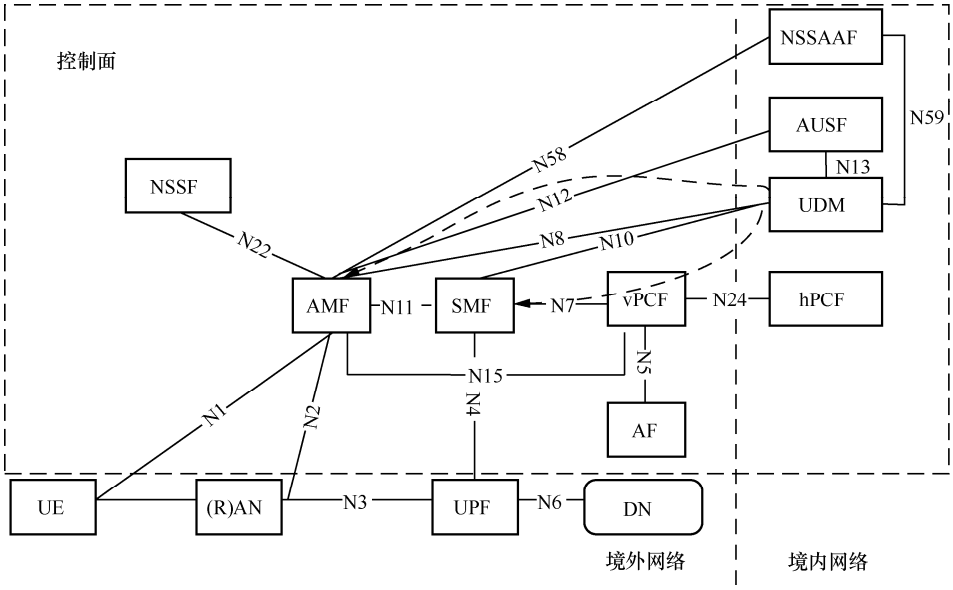



图 3 5G 网络漫游组网示意

同网元设备（如图 3 中的 AMF 和 SMF）中传递、存储和使用。

综上可以看出，移动通信网用户数据分布式管理机制的好处是网络功能在业务提供过程可以“就近取材”，减少数据使用中的检索还原层次和频次，缺陷是带来用户数据“泛在分布”，导致用户数据“泛在可见”。尤其是手机等移动通信终端通常与用户紧密捆绑，位置和身份关联数据直接涉及用户隐私，因而，移动通信用户的隐私安全问题也是移动通信体制机制伴随的安全问题。

受移动通信“效率优先”和“服务优保”设计理念以及网络处理能力的限制，用户数据的分布式管理和代理通告机制在短期内很难改变，至少目前正在建设的 5G 网络依然如此。

## 2 移动通信网内生安全共性问题的破解之道

根据网络空间内生安全理论[15,20]，网络空间内生安全问题与其本征功能实体间是事物内部之间互相依赖又互相排斥的矛盾性表达，具有不可分割性，只可能演进转化而不可能彻底消除。通过上面的分析，移动通信网存在的“信息真实性默认”“数据泛在可见”问题，本质上是由移动通信网的“代理通告”机制和用户数据组织管理机制造成的，因而要破解这 2 个安全问题，要从“通告代理”和数据组织管理机制着手，从机制层面将“默认信任”转化为“默认不信任”、将“泛在可见”转化为“限定可见”。

### 2.1 以零信任打破“默认的信任”

零信任作为一种安全概念，以“默认不信任”的安全防护理念，受到业界广泛关注。其具有如下安全防护原则[21]。

1) 永不信任，持续验证——构建以资源为中心的安全边界，对访问主体的身份、位置、设备、数据源、服务或工作负载等进行持续验证，资源包括但不限于业务应用、服务接口、操作功能和数据。

2) 最低权限授权访问——基于访问主体的属性、业务逻辑、应用上下文以及受访资源的属性和访问控制策略进行最小范围授权。

3) 持续信任评估、动态访问控制——实时评估访问主体和资源的安全状态，根据安全状态动态设立访问控制策略。

不难得出以下结论：用零信任的“默认不信任”安全防护理念对抗移动通信网的信息“真实性默认”缺陷，必有化解之道。

当前，基于零信任增强移动通信网的安全防护能力这一思路得到业界的广泛认可，文献[22]给出了单包授权、异常流量监控、网络功能信任评估等 7 个潜在方向作为 5G 核心网安全的零信任增强；文献[23]给出了 5G 网络切片安全零信任保护机制；文献[24]提出了一种基于零信任的 5G 网络网元功能信任评估方法；IMT-2020(5G)推进组于 2022 年 4 月发布了“5G 零信任安全技术研究”报告[12]，给出了零信任在 5G 网络中的可能应用场景和部分应用场景的解决方案。从目前业界的研究着重点看，已有

的移动通信网零信任安全增强机制均意在加强对信息交互过程中网元身份、网元行为合法性和合理性的判定，没有针对网络中交互的信息内容、信息行为等真实性的判别。因而，要化解移动通信网信息“真实性默认”缺陷，需要在当前移动通信网“代理通告”机制的基础上，引入“信息持续核实”机制，包括信息产生真实性的核实和信息本身真实性的核实。

基于移动通信网“合法网元被挟持攻击”“信息篡改攻击”（下文简称信息攻击）等产生的原理，本文基于内生安全构造机理，通过打造具有动态异构冗余（DHR, dynamic heterogeneous redundancy）构造的信息通告代理，实现对代理产生的信息内容和信息行为的“持续核实”。

#### 2.1.1　移动通信网的信息攻击原理

根据图 1 和图 2，基于如图 4 所示的 5G 用户终端位置更新过程，给出移动通信网基于代理的信息通告一般模型，如图 5 所示。

图 4 中，5G 用户终端发生跨 AMF 服务区的位置变化，首先通告无线信号覆盖区的 5G 基站（gNB），gNB 再通告核心网的 AMF，AMF 被授权后，访问 UDM，通过 UDM 将用户位置变化信息通告 UDR，UDR 存储用户新的位置。为描述问题的针对性，图 4 省略了用户的鉴权认证过程和网络功能的服务访问授权过程。

基于图 4 所示的用户终端位置更新流程，本文可以把 gNB 看作终端位置信息通告的第一个代理，AMF 看作第二个代理，UDM 看作第三个代理。为此，给出移动通信网基于代理的信息通告一般模型。不同的信息（行为）从触发起点到信息终点需要经过的代理个数 $K$ 可能不同。

假设信息传递路径均采用机密性和完整性保护机制且可以实现信息防篡改，从图 5 可以看出，移动通信网的信息代理通告机制产生的“信息攻击”可能来自信息传递路径上的任何一个信息（行为）转发代理。事实证明，这些具备信息（行为）转发代理功能的网元或者网络功能，不仅可能篡改从信息（行为）触发起点或者前一个信息（行为）转发代理收到的信息数据，也可能构造虚假的信息（行为）对信息（行为）终点进行信息攻击。

#### 2.1.2　采用 DHR 构造的内生安全代理实现信息核实

动态异构冗余架构[15]是在功能等价条件下通过软硬件层级化的异构冗余资源部署，配合输出裁决、反馈控制和多维动态重构等机制，实现“测量感知、误差识别、反馈迭代”等，能够同时应对“基于暗功能的人为攻击”和软硬件随机性失效引发的故障，可提供传统可靠性与网络安全性一体化的功能安全，其抽象模型[15]如图 6 所示。基于 DHR 架构构造的信息系统也被称为内生安全构造系统。

本文基于 DHR 架构的多异构执行体运行环境、输出裁决、反馈控制等机制，设计具有信息内容和信息行为真实性核实机制的移动通信网络信息代理（网元或者网络功能）。下面，以 5G 网络的 UDM 网络功能为例，给出基于 DHR 构造的内生安全代理的实现方案及信息真实性核实原理。

基于 DHR 构造的内生安全 UDM 如图 7 所示。为简化系统设计，选用 3 个异构 UDM 执行体（增加异构 UDM 执行体的数量，可以增强内生安全构造 UDM 的抗攻击能力，但也会增加系统的复杂性），分别执行标准的 UDM 功能，具体包括输入信令处理；构造新的信令数据向下一个信息代理转发；依据信息行为操作需求，访问 UDR 数据库；向上一个信息代理反馈信令处理结果等。其中，3 个 UDM 执行体要求尽可能避免具有相同的软硬件漏洞或者设计缺陷，目的是尽可能降低同时被攻击者挟持且产生共模攻击的可能性。工程实现过程，“输出比对”可以采用大数判决方法，即如果一个 UDM 执行体的输出与其他 2 个不同，则认为这个 UDM 执行体可能发生了“信息篡改攻击”；如果一个

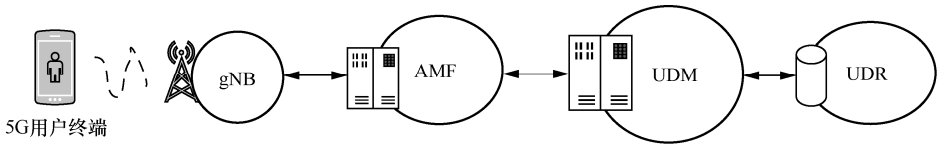



图 4　5G 用户终端位置更新过程

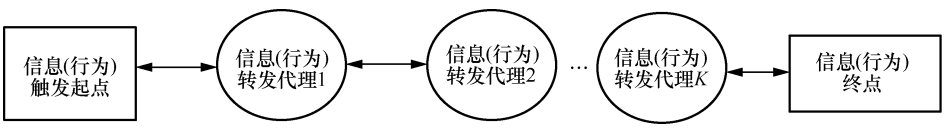



图 5　移动通信网基于代理的信息通告一般模型

UDM 执行体产生信令输出，其他 UDM 执行体没有输出，则认为这个 UDM 执行体可能发生了“信息行为伪造攻击”。基于负反馈控制功能，可以根据输出比对判别结果控制输入代理的信令分发以及控制异构 UDM 执行体的运行。

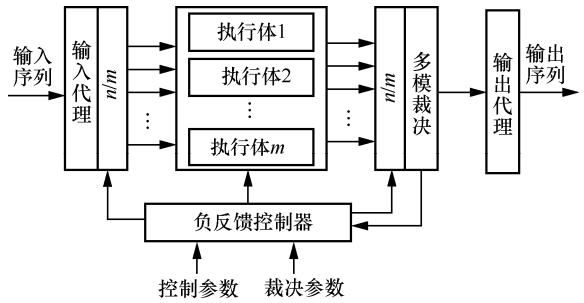



图 6　DHR 架构的抽象模型

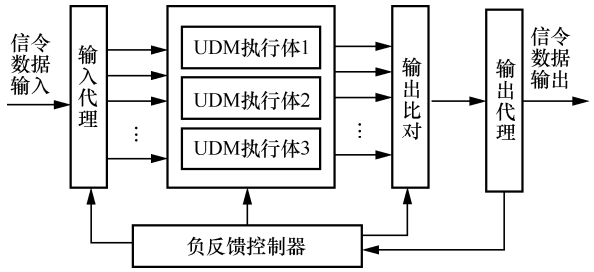



图 7 基于 DHR 构造的内生安全 UDM

不难看出，基于 DHR 构造的内生安全信息代理，不仅能够在一定程度上保证输出信息的真实性，还能够监测是否发生攻击事件。基于 DHR 构造的网络功能的工程实现、性能和效能评估等可以参考文献[15]。

### 2.2　以“变隐映射”实现用户数据的“限定可见”

#### 2.2.1　用户数据“变隐映射”机制

要实现用户数据在移动通信网络中的“限定可见”，最理想的情况是对于可确认正常的通信过程或者通信设备，用户数据可见；对于不可确认或者不可控的通信过程或通信设备，用户数据不可见。而对于当前位于公众移动通信网中的通信路径和通信设备而言，均应该认为是不可控通信过程和通信设备[25]。

进一步分析，因作为通信标识的手机号码对外公开，由表 1 和表 2 可知，在通信过程和数据存储环节，手机号码作为公开标识（MSISDN 或 GPSI）与用户私有标识（IMSI 或 SUPI）、用户位置标识等其他数据全部或者部分在网络中显性直接关联，因而，知道手机号码，就可以从用户数据的存储、传输及使用过程中获取与其关联的其他数据。因而，要解决用户数据的“泛在可见”问题，一个有效途径是打破或者隐匿已知用户数据与其他用户数据的显性关联关系。

进一步从人类行为学分析，攻击者实施攻击通常是以特定人、特定群体或特定网络作为目标，因而代表特定目标的身份标识应该被认为是已知信息。移动通信用户数据保护实质上是保护移动通信网中与特定身份标识（用户标识或者网络标识）关联的核心数据，这里的核心数据是指需要保护的用户数据。

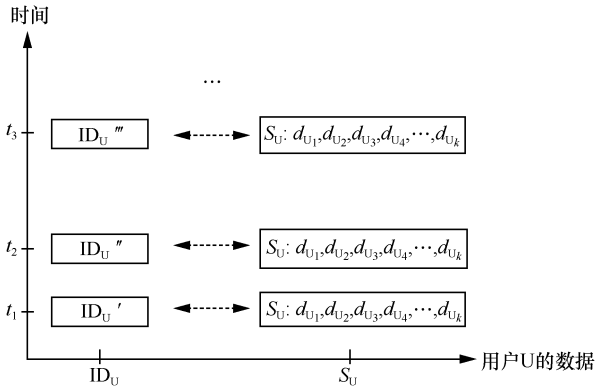
基于对用户数据公开性与隐秘性共存并交织这一本质特征的认识，本文提出以有效隐藏并动态改变用户数据关联关系为突破口，基于“变隐映射”实现用户数据关联关系主动隐藏[25]。其核心思想是通过特定机制隐藏已知身份标识与核心用户数据集合间的关联关系，并通过网络或者系统可控的机制动态改变该隐性关联关系，确保非可控的通信过程或者通信设备中用户信息呈现不完整、不确定、不关联和非真实等特性。

综上，如果用户 U 的已知身份标识（如手机号码）用 $\mathrm{ID_U}$ 表示，其他核心数据的集合用 $S_\mathrm{U}$ 表示，即 $S_\mathrm{U}=\left\{d_{\mathrm{U}_1},d_{\mathrm{U}_2},d_{\mathrm{U}_3},\cdots,d_{\mathrm{U}_k}\right\}$，$d_{\mathrm{U}_i}\left(i=1,2,\cdots,k\right)$ 表示集合中的核心数据，$k$ 表示与 $\mathrm{ID_U}$ 关联的核心用户数据个数。通过在不可控的通信过程或者通信设备中隐匿或者打破 $\mathrm{ID_U}$ 与 $S_\mathrm{U}$ 或者 $\mathrm{ID_U}$ 与 $S_\mathrm{U}$ 的某个子集间的关联关系，就可以大大增加攻击者对用户数据的攻击难度，可以想象，如果这种关联关系可以动态改变，攻击者获取用户数据的难度就会进一步增强。因而，实现移动通信用户数据“限定可见”的核心思想就是在不可控的通信过程或者通信设备中建立 $\mathrm{ID_U}$ 与 $S_\mathrm{U}$ 或者 $\mathrm{ID_U}$ 与 $S_\mathrm{U}$ 的某个子集间的“动态虚拟映射”，也就是通过某种机制动态改变 $\mathrm{ID_U}$ 与 $S_\mathrm{U}$（或者 $S_\mathrm{U}$ 的子集）间的显性映射关系，以构建不确定的“用户数据虚拟关系谱”，进而提高攻击者获取信息的难度。

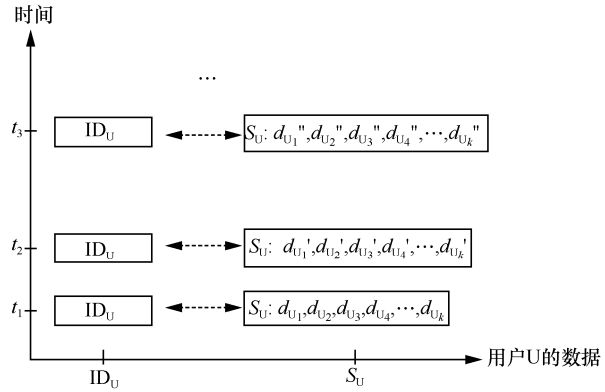
进一步，本文提出采用用户数据“动态变体”作为实现“动态虚拟映射”的基本方法，即通过“动态变体”特定用户数据，使单个网元设备无法组合多维真实信息，确保非可控网元设备中用户信息呈现不完整、不确定、不关联和非真实等特性。

不难看出，建立用户已知身份标识与用户核心数据集合间的“动态虚拟映射”有 2 种实现方式，一种是通过动态改变用户的已知身份标识，隐藏用户身份；另一种是通过动态改变用户的核心数据集

合或者子集合，隐藏核心用户数据，如图 8 所示。图 8(a)中的 $ID_U'$、$ID_U''$等分别表示用户 U 身份标识的不同取值；图 8(b)中的 $d_{U_i}$、$d'_{U_i}$、$d''_{U_i}$（$i$=1,2,⋯,$k$）等分别表示用户的某个核心数据的不同取值。




(a) 动态改变用户已知身份标识




(b) 动态改变用户的核心数据集合或者子集合

图 8　动态虚拟映射的 2 种实现方式

基于上述思想，进一步需要解决的核心问题是在当前的移动通信机制下，用户数据能否动态变体以及动态变体需要满足什么样的条件。

下面，本文从分析用户数据的属性、时空特性和时空关联特性入手，解决上述问题。

### 2.2.2　用户数据的属性、时空特性和关联特性

基于典型制式移动通信网的通信流程和业务提供机制，本文挖掘了移动通信用户的手机号码（MSISDN 或 GPSI）、私有身份标识（IMSI 或 SUPI）、不同位置标识（MSCID、BSID、CellID 或 AMFID、NR CGI、5G TAI 等）、业务路由（MSRN、MSCNUM）等用户核心数据的本质属性（用 A 表示）和在不同应用场景的内在功能（用 F 表示），分析了其相互关联使用和关联索引的内因。

其中，用户数据的“本质属性”包括数据的定义、结构、来源等。用户数据的“内在功能”根据移动通信场景可以是身份验证功能、路由寻址功能、计费功能、号码显示功能、定位功能、辅助功能等。相互关联使用和关联索引的内因包括“正向索引需求”“反向索引需求”“双向索引需求”。所谓“正向索引需求”指需要通过本数据，查阅或者请求其他数据；“反向索引需求”指需要通过其他某数据，查阅或者请求本数据；“双向索引需求”指既具有“正向索引需求”，又具有“反向索引需求”。

此外，本节还分析了在特定场景和特定网元设备中，用户不同数据的角色（R）及相互间关联属性。其中，移动通信的特定场景可以用时间域描述，特定网元设备可以用空间域描述。

用户数据在特定时空中的“角色”可用主导（M）、辅助（A）或者可选（O）描述，如 3G 中用户 A 拨打用户 B 的场景，用户 A 的服务 MSC/VLR 需要利用用户 B 的 MSISDN 号码寻址用户 B 的 HLR，获取用户 B 的路由。此时，本文称在用户 B 作为被叫的场景，用户 B 的 MSISDN 号码在用户 A 的服务 MSC/VLR 中处于主导角色，而其他数据，如用户 B 的 IMSI 和位置信息等，在用户 A 的服务 MSC/VLR 中的主要作用是计费，此时，本文称在用户 B 作为被叫的场景，用户 B 的 IMSI 和位置标识在用户 A 的服务 MSC/VLR 中处于辅助角色。移动通信机制决定当用户数据在某个特定时空中处于主导角色时，该数据是不能改变的。

特定用户的某个数据与其他数据在特定时空中的关联属性可用关联和非关联表示。例如，在用户 A 作为主叫的场景，用户 A 的 IMSI 与其位置标识在用户 A 的服务 MSC/VLR 中是关联的，而其位置标识与签约业务清单是不关联的。

通过对用户数据“内在属性”“内在功能”及“关联使用和关联索引”的分析，可以明确定位其在不同时空坐标中的角色以及与其他数据的关联属性。基于用户数据的时空特性和关联特性，可以得到用户数据的“时空关系序列”，该关系序列清楚地表示了用户数据在特定场景、特定网元设备中的属性、功能、角色以及相互关联关系。“时空关系序列”为分析特定用户数据在特定时空能否动态变体提供了依据。

### 2.2.3　用户数据动态变体的时机和条件

基于上述分析，结合移动通信的协议体系和业务提供模式，本节提出了用户数据动态变体方法。该方法描述为基于某用户的身份标识或者其核心

数据集合中的某个（或某些）用户数据在“时空关系谱”序列中的“来源”属性、角色和关联特性，对“非本地产生”、在网络中具备“动态变更身份”且处于“非主导角色”的用户身份标识或者核心数据进行“动态变体”。

所谓“非本地产生”是指在用户数据的“时空关系谱”序列中，用户数据不是当前网元产生的，对来源为终端设备的用户数据归类为“本地产生”；具备“动态变更身份”是指在现有移动通信协议体系中，用户终端设备或者网络可以通过标准的通信流程对该数据进行修改。

图 9 以 3G 网络为例，标注了用户数据“来源”属性（图 9 括号中的标示）的时空关系序列，其中，T 表示数据来自移动终端设备，H 表示数据来自归属网络网元 HLR，$V_1$ 表示数据来自 $MSC_1/VLR_1$（主叫用户的服务 MSC/VLR），$V_2$ 表示数据来自 $MSC_2/VLR_2$（被叫用户的服务 MSC/VLR），O 表示数据是网元设备自身存储的，S 表示数据是本网元自行临时分配的。上述的主叫用户特指发起语音或者其他业务呼叫的用户，被叫用户指与主叫用户建立通信联系的用户。

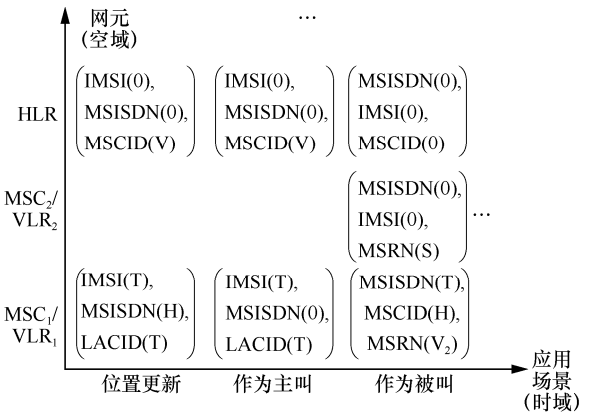



图 9 3G 网络中用户数据在特定场景时空坐标中的关系序列

下面，基于用户作为被叫场景，示例用户数据“动态变体”的时机和条件。

图 9 中 $MSC_1/VLR_1$ 中关联了被叫用户的手机号码 MSISDN、被叫用户的位置信息 MSCID 以及被叫用户的路由信息 MSRN，其中，MSISDN 是主叫用户拨打的号码，来自发起呼叫的终端设备；MSCID 是 $MSC_1/VLR_1$ 以 MSISDN 为索引，通过标准的信令流程从被叫用户的 HLR 中申请的；MSRN 也是通过 MSISDN 为索引，通过标准的信令流程经 HLR 请求 $MSC_2/VLR_2$ 临时分配的。

用户数据“动态变体”的一个执行例就是根据前面分析的用户数据属性及角色，MSISDN 作为被拨打的号码，在用户作为被叫的应用场景，其主要功能是寻址被叫用户的 HLR，处于“主导”角色，不具备“动态变体”条件，而 MSCID 和 MSRN 作为“辅助”角色，同时满足“非本地产生”“在网络中具备‘动态变更身份’”2 个条件，因而可对其进行“动态变体”。

通过对 MSCID 和 MSRN 进行动态变体，实现了在主叫用户的服务 MSC/VLR 以及通信协议传递路径中用户身份与位置信息的虚拟关联，达到了隐匿被叫用户真实位置和真实路由的目的。

不难分析，在所有制式移动通信网的用户位置更新场景，同样可以通过对用户的 MSISDN 号码（或 GPSI 号码）进行“动态变体”，建立虚拟用户的数据关联关系[26]，达到隐藏用户真实位置、真实路由、私有标识 IMSI（或 SUPI）等核心数据的目的。

此外，要对特定用户数据进行动态变体，除了该数据要满足上述条件外，还需要研究用户数据如何动态变体以及变体后如何保证网络和用户的正常通信，即用户数据实现“变隐映射”后的工程实现及可行性验证。由于篇幅所限，本文省略了相关内容。作者研究团队基于典型制式的移动通信网络，通过研制原理样机，验证了本文提出的用户数据“变隐映射”安全机制的可行性。基于 MSISDN 动态变体实现用户数据“限定可见”安全机制的方法、工程实现及安全性分析可以参考文献[26]，相关方法同样适用于 5G 网络对应的应用场景。

## 3 结束语

网络空间内生安全是网络空间安全领域的新发展范式[27]，网络空间内生安全问题的研究和挖掘是网络空间内生安全体制和机制创新的基础。本文基于移动通信机理和移动通信网络服务特性，剖析了移动通信网特有机制尤其是移动性管理机制存在的内生安全问题或内生安全缺陷，指出了这些安全缺陷可能带来的安全威胁，这些内生安全问题或缺陷也可以认为是移动通信网存在的共性内生安全问题。此外，本文从问题化解的角度，提出了解决这些内生安全问题的思路和方法，开拓了移动通信网安全问题研究的新视角，希望为业界开展 B5G、6G 等新一代移动通信网内生安全机制研究提供思路和参考。

## 参考文献：


[1] 刘彩霞. 网络空间安全专题导读[J]. 无线电通信技术, 2020, 46(4): 377.
LIU C X. Introduction to special topics on cyberspace security[J]. Radio Communication Technology, 2020, 46(4): 377.

[2] 3GPP. 5G security assurance specification (SCAS): TS33.512-522[S]. 2019.

[3] 3GPP. Study on 5G security enhancements against false base stations: TR33.809[S]. 2018.

[4] 3GPP. Study of privacy of identifiers over radio access: TR33.870[S]. 2021.

[5] 3GPP. Study on enhanced security aspects of the 5G service based architecture (eSBA): TR33.875[S]. 2021.

[6] 3GPP. Study on security aspects of the 5G service based architecture (SBA): TR33.855[S]. 2020.

[7] 3GPP. Study on security impacts of virtualization: TR33.848[S]. 2018.

[8] 3GPP. Study on authentication enhancements in the 5G system: TR33.846 [S]. 2021.

[9] 3GPP. Study on security aspects of 5G network slicing management: TR33.811[S]. 2018.

[10] 全国信息安全标准化技术委员会(通信安全标准工作组). 5G 网络安全标准化白皮书[R]. 2021.
National Information Security Standardization Technical Committee (Communication Security Standard Working Group). White paper on 5G network security standardization[R]. 2021.

[11] IMT-2020(5G)推进组. 5G 行业专网安全技术研究报告[R]. 2022.
IMT-2020 (5G) Advance Group. Research report on private network security technology in 5G industry[R]. 2022.

[12] IMT-2020(5G)推进组. 5G 零信任安全技术研究报告[R]. 2022.
IMT-2020 (5G) Advance Group. Research report on 5G zero-trust security technology[R]. 2022.

[13] 中国通信学会. 5G 数据安全防护白皮书[R]. 2022.
China Communications Society. White paper of 5G data security protection[R]. 2022.

[14] 邬江兴. 网络空间拟态防御原理-下册: 广义鲁棒控制与内生安全[M]. 2 版. 北京: 科学出版社, 2018.
WU J X. Principles of cyberspace mimic defense: generalized robust control and endogenous safety & security[M]. 2ed. Beijing: Science Press, 2018.

[15] 邬江兴. 网络空间内生安全-上册: 拟态防御与广义鲁棒控制[M]. 北京: 科学出版社, 2020.
WU J X. Cyberspace endogenous safety and security: mimic defense and general robust control[M]. Beijing: Science Press, 2020.

[16] 肖前, 李秀林, 汪永祥. 辩证唯物主义原理[M]. 北京: 人民出版社, 1981.
XIAO Q, LI X L, WANG Y X. Principles of dialectical materialism[M]. Beijing: People's Publishing House, 1981.

[17] JIN L, HU X Y, LOU Y M, et al. Introduction to wireless endogenous security and safety: problems, attributes, structures and functions[J]. China Communication, 2021, 18(9): 88-99.

[18] Adaptive Mobile Security.Hidden art SS7 spoofing[R]. 2022.

[19] 3GPP. Security architecture and procedures for 5G system: TS33.501[S]. 2018.

[20] WU J X. Cyberspace endogenous safety and security[J]. Engineering, 2021, doi.org/10.1016/j.eng.2021.05.015.

[21] 冀托. 白话零信任[M]. 北京: 电子工业出版社, 2022.
JI T. Zero trust in vernacular[M]. Beijing: Publishing House of Electronics Industry, 2022.

[22] 刘建华. 基于零信任架构的 5G 核心网安全改进研究[J]. 邮电设计技术, 2020(9): 75-78.
LIU J H. Research on security improvement of 5G core network based on zero trust architecture[J]. Designing Techniques of Posts and Telecommunications, 2020(9): 75-78.

[23] 单英. 基于零信任的 5G 安全切片架构设计[J]. 通信管理与技术, 2022(1): 47-49, 59.
SHAN Y. Design of 5G security slicing architecture based on zero trust[J]. Communications Management and Technology, 2022(1): 47-49, 59.

[24] 张奕鸣. 5G 网络服务化接口安全增强技术研究[D]. 郑州: 信息工程大学, 2022.
ZHANG Y M, Research on security enhancement technology of 5G network service based interface[D]. Zhengzhou: Information Engineering University, 2022.

[25] LYU X J, DI L, LIN Z L, et al. Characteristic model based all-coefficient adaptive control of an AMB suspended energy storage flywheel test rig[J]. Science China (Information Sciences), 2018, 61(11): 113-127.

[26] 刘彩霞, 季新生, 邬江兴. 一种基于 MSISDN 虚拟化的移动通信用户数据拟态防御机制[J]. 计算机学报, 2018, 41(2): 275-287.
LIU C X, JI X S, WU J X. A mimic defense mechanism for mobile communication user data based on MSISDN virtualization[J]. Chinese Journal of Computers, 2018, 41(2): 275-287.

[27] 邬江兴. 网络空间内生安全发展范式[J]. 中国科学: 信息科学, 2022, 52(2): 189-204.
WU J X. Development paradigms of cyberspace endogenous safety and security[J]. Scientia Sinica (Informationis), 2022, 52(2): 189-204.


[作者简介]

**刘彩霞**（1974− ），女，山东烟台人，国家数字交换系统工程技术研究中心研究员、博士生导师，主要研究方向为移动通信网络新技术、网络与信息安全。

**季新生**（1968− ），男，河南驻马店人，国家数字交换系统工程技术研究中心教授、博士生导师，主要研究方向为移动通信网络新技术、网络与信息安全。

**邬江兴**（1953− ），男，安徽金寨人，中国工程院院士，国家数字交换系统工程技术研究中心教授，主要研究方向为网络新技术、网络空间内生安全。