基于网络切片和无证书公钥密码体制的系统安全控制方法

System Security Control Method Based on Network Slice and Certificateless Public Key Cryptosystem

谢国涛，王首媛，管立军（中讯邮电咨询设计院有限公司，北京 100048）
Xie Guotao，Wang Shouyuan，Guan Lijun（China Information Technology Designing & Consulting Institute Co.，Ltd.，Beijing 100048，China）

摘　要：
随着5G在行业应用中的不断渗透，5G网络切片安全性不足、SLA保障不具备场景化灵活调节能力等问题逐渐凸显。通过虚拟化机制，建立了灵活的安全与路由策略控制方法，以应用系统内外部（应用系统内部以消息对网络性能的需求为基础，进行路由；应用系统外部以消息对网络性能的需求为基础，选择适当的网络切片）整体调度优化网络资源配置为基础，并基于整体安全策略控制，实现系统链路保障、身份认证、访问控制等，即从网络链路的物理和逻辑多层面保障应用系统的整体可靠性、可用性和安全性。

关键词：
5G网络切片；CLA；SLA；身份认证；访问控制
doi：10.12045/j.issn.1007-3043.2022.09.009
文章编号：1007-3043（2022）09-0039-05
中图分类号：TN915.08
文献标识码：A
开放科学（资源服务）标识码（OSID）：

Abstract：
With the continuous penetration of 5G in industrial applications，problems such as insufficient 5G network slicing security and SLA guarantees that do not have the ability to adjust flexibly in scenarios have gradually become prominent. It establishes a flexible security and routing policy control method through virtualization mechanism. Based on the overall scheduling and optimization of network resource allocation inside and outside the application system（inside the application system，routing is performed based on the network performance requirements of messages；outside the application system，based on the network performance requirements of messages，appropriate network slices are selected），and based on the overall security policy control，the system link guarantee，identity authentication，access control，etc. are realized，that is to ensure the overall reliability，availability，and security of the application system from the physical and logical aspects of the network link.

Keywords：
5G network slicing；CLA；SLA；Authentication；Access control

引用格式：谢国涛，王首媛，管立军. 基于网络切片和无证书公钥密码体制的系统安全控制方法[J]. 邮电设计技术，2022（9）：39-43.

1 概述

网络切片是一种按需组网的方式，本质上就是将运营商的物理网络划分为多个虚拟网络，每一个虚拟网络根据不同的服务需求，比如时延、带宽、安全性和可靠性等来划分，以灵活地应对不同的网络应用场景。

CLA是一种基于SM2、不使用双线性对运算的无证书认证体制。在这种体制中，不使用数字证书，不存在密钥托管问题和共谋攻击问题。

但基于CLA的密码体制只能实现业务数据和逻辑链接的安全性，未能结合信道资源，实现业务差异化信道资源保障；同时网络切片的信道安全性，未能结合具体业务场景，无法实现更加灵活的安全策略控制。

本文针对5G网络切片安全性不足、SLA保障不具备场景化灵活调节能力等问题，基于网络切片差异化信道资源保障的优势，和CLA在物联网应用中的高效

收稿日期：2022-07-18

性，实现业务数据和逻辑链接安全性的同时，保障业务差异化信道资源，最终实现更加灵活高效的安全策略控制。

2 5G网络切片安全与SLA现状

2.1 5G网络切片安全

网络切片（Network Slicing，NS）是指5G[1-2]运营商利用软件定义网络（Software Defifined Network，SDN）和网络功能虚拟化（Network Function Virtualization，NFV）技术，在有限物理网络设备上建立多种相互隔离的虚拟网络。不同网络切片达到的网络性能指标不同，提供的通信方式及安全策略也不同。垂直网络切片是指由5G运营商开发并租赁给第三方服务商，专门用来支持不同业务的端到端切片[3-7]。

一张垂直网络切片由终端切片、接入网切片、核心网切片和数据网切片等水平切片组成；5G网络切片终端侧主要包含用户移动设备和各种物联网终端；接入网切片主要包含由各种接入技术提供的接入网，帮助用户终端接入核心网切片；核心网切片由多种虚拟网元构成，将网络分为控制层和用户数据层，控制层负责管控用户数据层的通信和安全，用户数据层负责为用户终端和外部服务器之间创建会话；数据网切片主要由云服务器构成，其主要作用是提供用户所需的服务数据，并存储大量的用户信息。4种切片在提供不同服务的同时，也带来许多安全问题[8]。

2.2 5G网络切片SLA

切片服务等级保障（Service Level Assurance，SLA）使得5G网络切片可以给行业应用提供可定制、可感知、可预期的通信服务质量，并将其作为完整业务系统中的一环，实现对业务质量的端到端管控[9-12]。

网络切片SLA作为提供通信服务的服务协议，需要把运营商与网络切片客户签约的业务需求信息传递到运营商的网络中。对于需要新创建一个切片的场景，切片管理系统根据租户对切片的SLA要求（如切片列表、PLMN列表、最大用户数、切片服务区域、切片端到端时延、切片中终端的移动等级、切片资源共享等级）进行各域（接入网、传输网、核心网等）的SLA分解，进而进行各域资源配置，包括带宽、时延等[13]。

2.3 现有基于5G网络切片的系统安全与SLA保障体系存在的问题

当前对于基于5G网络切片的系统安全与SLA保障体系，主要研究点在于5G网络本身的安全和服务等级保障；但对于利用5G网络切片安全和SLA保障，实现业务系统高安全性和差异化服务保障的研究较少；同时5G网络切片不能实现非常灵活的调度，否则将消耗大量的5G网络运营调度资源；但业务系统对于安全和SLA保障存在着丰富的需求，主要包括以下3个方面。

a）业务系统需要具备身份认证、数据加解密、访问控制等功能，这些功能是多层次的、灵活动态的，不同业务系统的策略、实现机制也不同。

b）对于业务系统的交互消息，需要具备SLA，SLA参数受消息载荷、发送消息的主体、时空间等因素影响，这些因素存在变化，甚至这些因素与SLA的关联策略也存在变化，因此需要业务系统的SLA实现灵活的调整。

c）业务系统的安全和SLA保障并非独立，可能存在关联关系，比如对于安全性要求较高的交互消息，可能也需要较高SLA保障，但这种交互消息对资源占用较多。

简而言之，业务系统更加了解自身交互需求，基于本文提供的机制，能利用5G网络切片的安全性和SLA保障，实现更加灵活、高效的安全和SLA保障体系。

3 PKI/CLA无证书密码技术

CLA是一种基于SM2、不使用双线性对运算的无证书认证体制，融合自证公钥密码体制和无证书公钥密码体制的密钥生成和密钥使用机制，借鉴PKI/CA系统的管理体系架构而构建的一种新型公钥基础设施。采用现有SM2椭圆曲线密码算法，不使用数字证书，不使用双线性对运算，兼具PKI/CA、IBC的优点。生成短格式的数字签名数据包，适合于各种签名应用，而验签时不需要密钥管理中心的支持，验签者可以直接对签名进行验证，极大地方便了接收者对签名的验证。建设成本低，计算效率高，占用资源少，可用于对海量用户的密钥管理，满足大规模、大范围的云计算、物联网和移动互联网环境下的身份认证、数据防篡改、防抵赖等安全应用需求[14]。

4 基于网络切片和无证书公钥密码体制的系统安全控制设计

4.1 方法设计

4.1.1 标识说明

首先说明3个标识。

a）应用标识：表征具有清晰边界和业务内聚性应用的标识，应用一般以B/S结构组成，包括客户端APP和应用系统，称为ID_{APP}；应用集合的子集，称为APP组，其标识记为$ID_{APP组}$；下文UE的安全模块中涉及的虚拟应用，称为虚拟APP，其标识记为$ID_{虚拟APP}$。

b）切片标识，即网络切片选择辅助信息（Single Network Slice Selection Assistance Information，S-NSSAI）标识，该信息进一步包括如下2部分信息。

（a）Slice/Service Type（SST），表征对应切片特征和业务期待的网络切片行为。

（b）Slice Differentiator（SD），该功能可选，它是对SST的补充，进一步区分相同SST的多个切片。

c）CLA用户标识，即CLA系统中用于标识用户实体身份的信息，称为ID_{CLA}。

4.1.2 思路说明

本文设计方法的主要实现思路为：CLA用户标识ID_{CLA}可以融合网络切片的切片标识（S-NSSAI），以切片标识（S-NSSAI）和应用标识（ID_{APP}）组合形成CLA用户标识（ID_{CLA}），实现切片识别及差异化安全认证方案；其优势在于：通过5G端到端切片SLA实现底层通信链路差异化保障，实现业务识别适配；以切片S-NSSAI为桥梁，作为用户安全标识的一部分，关联多业务差异化安全与切片差异化SLA，实现多切片场景下的自定义差异化安全策略。具体结构及交互示意如图1所示。

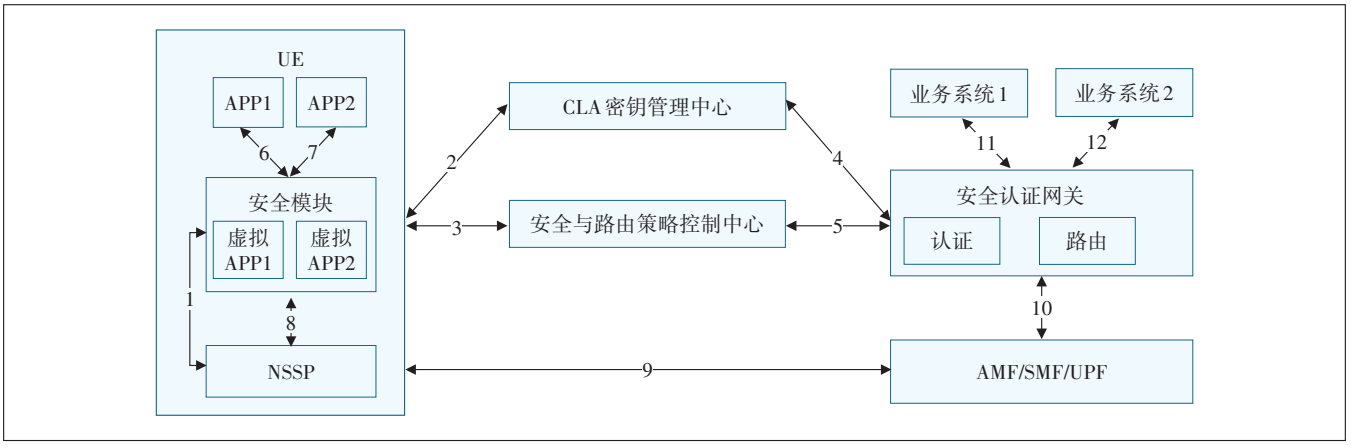

图1 基于网络切片和无证书公钥密码体制实现的系统结构与交互图

4.1.2.1 初始化阶段

a）安全策略控制中心对应用（图1中为APP1、APP2）进行分组，形成多个应用组，这些应用组为应用集合的子集；应用组可为空，即不包含任何应用，或包含全部应用；UE中的安全模块基于图1中接口3，从安全策略控制中心获取应用分组配置信息；该安全策略控制被称为应用系统静态分组配置。

b）UE中的安全模块与网络切片选择策略（Network slice selection policy，NSSP）模块交互（基于图1中接口1），获取UE支持的S-NSSAI列表和S-NSSAI所标识的网络切片SLA参数信息。

c）UE中的安全模块基于应用分组配置信息和UE支持的S-NSSAI列表信息，生成虚拟APP列表，其生成策略基于图1中接口3，从安全策略控制中心获取；譬如，基于组合策略可形成如表1所示的虚拟APP。

表1 应用组标识与网络切片标识组合表

应用组标识	网络切片标识	虚拟APP标识（组成部分）
IDAPP组1	S-NSSAI1	ID虚拟APP1（IDAPP组1-S-NSSAI1）
IDAPP组1	S-NSSAI2	ID虚拟APP2（IDAPP组1-S-NSSAI2）
IDAPP组2	S-NSSAI1	ID虚拟APP3（IDAPP组2-S-NSSAI1）
IDAPP组2	S-NSSAI2	ID虚拟APP4（IDAPP组2-S-NSSAI2）

d）UE中的安全模块以虚拟APP ID（$ID_{虚拟APP}$）作为CLA用户标识（ID_{CLA}）或作为CLA用户标识（ID_{CLA}）的一部分（可基于统一规则加入其他标识，譬如在“$ID_{APP组1}$-S-NSSAI1”标识前部或后部加入UE特征标识），通过图1中接口2，与CLA密钥管理中心交互，最终生成$ID_{虚拟APP}$对应的公私钥对。

e）安全认证网关，采用网关的CLA用户标识（ID_{CLA}），通过图1中接口4，与CLA密钥管理中心交互，最终生成网关CLA公私钥对。

4.1.2.2 系统运行阶段

a）UE 中的 APP，通过图 1 中接口 6、7，将需要发送到业务系统的信息，发送到安全模块。

b）UE 中的安全模块，获取到 APP 发送的消息，能够识别发送者身份（IDAPP），基于初始化阶段从安全策略控制中心获取的应用分组配置信息和系统当前运行阶段，安全策略控制中心配置的应用与应用组之间的映射偏好策略（称为应用系统消息动态分组偏好配置），确定应用与应用组之间的唯一映射关系（IDAPP→IDAPP 组），即运行时发生的消息只能属于某个应用系统分组。

c）UE 中的安全模块，通过图 1 中的接口 3，获取安全策略控制中心配置的应用组 SLA 参数，选择适当的虚拟 APP；选择过程为：通过系统运行阶段步骤 b）确定 IDAPP 组，基于从获取安全策略控制中心配置的应用组 SLA 参数要求，并结合网络切片 SLA 参数信息，确定网络切片标识 S-NSSAI，基于 IDAPP 组和 S-NSSAI，确定 ID 虚拟 APP；最后将消息通过该虚拟 APP 发出。

d）UE 中的安全模块，通过图 1 中的接口 8，将虚拟 APP 的消息发送给 NSSP，NSSP 基于切片选择策略将消息通过网络切片（图 1 中的接口 9）发送到 5G 网络中。

e）5G 网络将消息路由至安全认证网关（图 1 中的接口 10）。

f）安全认证网关基于从安全策略控制中心获取的身份认证与访问控制策略（通过图 1 中的接口 5），对接收到的消息进行认证；可能包括如下情形。

（a）消息无需认证，直接转发。

（b）消息仅需要身份认证；基于 CLA 认证算法，对消息进行身份认证；如果身份认证通过，则转发该消息；如果身份认证不通过，则返回认证失败信息。

（c）消息需要身份认证，且需要验证消息发送者的合法性（譬如，消息发送者是否在白名单且不属于黑名单）；身份认证通过后，验证消息发送者是否合法（譬如，消息发送者 ID_{APP} 或 $ID_{APP组}$ 属于白名单且消息发送者 ID_{APP} 或 $ID_{APP组}$ 不属于黑名单），如果发送者身份合法性验证成功，则转发消息；如果发送者身份验证失败，则返回身份合法性失败信息；身份认证不通过，返回认证失败信息。

其中，需要说明的是，基于 CLA 的身份认证能够识别消息发送者（ID_{APP}）所在的应用组（$ID_{APP组}$）是否为系统中已经注册的应用组；身份合法性判定则是基于身份认证通过后的细粒度访问控制策略。

g）安全认证网关将通过身份认证与访问控制的消息，通过图 1 中接口 11 和 12，转发给相应的业务系统。

4.2 一种实现说明

为方便说明，一种实现方式如图 2 所示。

其中，系统包括 2 个应用软件，其客户端软件分别为 APP1、APP2。

安全与路由策略控制中心对应用软件进行分组，分为 2 个组：APP 分组 1（包括 APP1、APP2）和 APP 分组 2（包括 APP1）。

安全模块获取 UE 支持的网络切片为切片 1（S-NSSAI1）和切片 2（S-NSSAI2），形成 4 个虚拟 APP，分别为虚拟 APP1、虚拟 APP2、虚拟 APP3、虚拟 APP4，虚拟 APP ID 在本例中包括 APP 组 ID 和切片 ID 各种组合（本例中有 2 个 APP 组、2 个切片，因此为 4 个组合）。安全模块，基于虚拟 APP ID，与 CLA 系统合作生成对应密钥对。

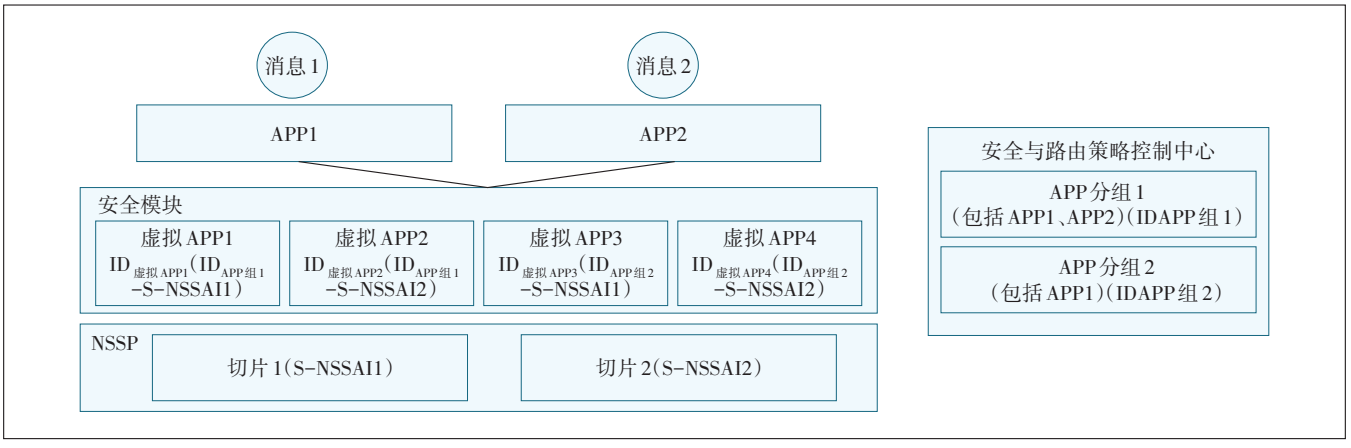

图 2　本方法的一种实现

系统运行时，UE上的安全模块，发现“APP分组1”和“APP分组2”中均包括“APP1”，同时基于安全与路由策略控制中心的“应用系统消息动态分组偏好配置”，判断来源于APP1的“消息1”，应该归入哪个APP分组，不失一般性的假设，将“消息1”归入“APP分组2”；同时UE上的安全模块，基于安全与路由策略控制中心的“应用系统消息动态SLA策略”，根据切片1和切片2的SLA与消息SLA的符合程度，最终选择使用“虚拟APP1”或“虚拟APP2”中的一个进行消息处理；UE上的安全模块，基于安全与路由策略控制中心的“消息签名与加密策略”，对消息进行签名、加密，经由通信模组将消息发出。

4.3 本方法的优点

本方法关注切片SLA与消息SLA的动态符合程度，通过“虚拟APP”的适配策略，选择适当的具备网络SLA属性的虚拟APP（该虚拟APP的网络SLA属性预计与承载该虚拟APP的切片SLA属性一致或接近），满足消息的动态SLA需求；消息SLA动态变化的频率，明显大于运营商能够承载的切片SLA变化频率。

本文关注应用系统层面的逻辑安全，并不关注网络传输管道本身是否安全，或者说对传输数据进行了签名/加密处理；其次本文通过安全策略中心，实现对消息动态的安全策略控制；再次，本文基于安全与路由策略控制中心的“安全认证网关的身份认证与访问控制策略”，通过安全认证网关进行消息身份认证、消息发送者合法性验证；即本方法不仅可以实现消息签名/验签、加密/解密，还能够对消息发送者合法性验证；同时通过安全与路由策略控制中心动态的安全策略控制，实现消息级别的灵活的安全策略。

总体而言，本方法通过APP静态分组、APP动态分组适配、虚拟APP抽象、安全认证网关的身份认证与访问控制等技术，在应用系统层面，以消息为粒度，实现动态、丰富的安全控制与网络服务。

5 结束语

基于网络切片差异化信道资源保障的优势和CLA在物联网应用中的高效性，实现业务数据和逻辑链接安全性的同时，保障业务差异化信道资源，最终实现更加灵活高效的安全策略控制。

参考文献：

[1] IMT-2020(5G)推进组. 5G概念白皮书[EB/OL]. [2022-04-25]. https://wenku.baidu.com/view/5bde7aa901d276a20029bd64783e0912a3167c44.html.
[2] 3GPP. Study on scenarios and requirements for next generation access technologies: 3GPP TR 38.913[S/OL]. [2022-04-25]. ftp://ftp.3gpp.org/Specs/.
[3] IMT-2020(5G)推进组. 5G网络安全需求与架构白皮书[EB/OL]. [2020-04-25]. https://download. csdn. net/download/qq_38341856/10213128.
[4] 3GPP. Security architecture and procedures for 5G system(Release 15): 3GPP TS 33.501[S/OL]. [2022-04-25]. ftp://ftp. 3gpp. org/Specs/.
[5] 刘建伟，王育民. 网络安全：技术与实践[M]. 3版. 北京：清华大学出版社，2017.
[6] China Mobile, Huawei, Deutsche Telekom, et al. 5G service-guaranteed network slicing whitepaper [EB/OL]. [2022-04-25]. https://www. huawei. com/uk/technology-insights/industry-insights/outlook/mobile-broadband/insights-reports/5g-service-guaranteed-network-slicing-whitepaper.
[7] 3GPP. 5G security assurance specification(SCAS); access and mobility management function(AMF): 3GPP TS 33.512[S/OL]. [2022-04-25]. ftp://ftp.3gpp.org/Specs/.
[8] 刘建伟，韩祎然，刘斌，等. 5G网络切片安全模型研究[J]. 信息网络安全，2020，20(4)：1-11.
[9] IMT-2020(5G)推进组. 基于AI的智能切片管理和协同白皮[EB/OL]. [2022-04-25]. https://wenku.baidu.com/view/09e7c98d6d1aff00bed5b9f3f90f76c660374c1a. html? fr=income2-wk_app_search_ctrX-search.
[10] 中国移动，华为，腾讯，等. 网络切片分级白皮书[EB/OL]. [2022-04-25]. https://max.book118.com/html/2021/1106/52443042340041 01.shtm.
[11] 中国信息通信研究院. 5G端到端切片SLA行业需求研究[EB/OL]. [2022-04-25]. https://wenku.baidu.com/view/30e98df9773231126edb6f1aff00bed5b8f37349. html? fr=income1-wk_app_search_ctr-search.
[12] 3GPP. System architecture for the 5G system(5GS); Stage 2(Release 15): 3GPP TS 23.501[S/OL]. [2022-04-25]. ftp://ftp. 3gpp. org/Specs/.
[13] 夏旭，梅承力. 面向智能化切片的服务化等级保障技术增强和研究[J]. 移动通信，2021，45(1)：6-10.
[14] 熊荣华. 一种无双线性对运算的无证书公钥密码体制的实现方法：CN201410772127.5[P]. 2014-12-16.

作者简介：
谢国涛，毕业于浙江大学，工程师，硕士，主要从事5G物联网密码与数据安全创新技术研究与应用工作；王首媛，毕业于北京邮电大学，工程师，硕士，主要从事5G物联网密码与数据安全创新技术研究与应用工作；管立军，毕业于东南大学，工程师，硕士，主要从事5G+工业互联网方案设计与产品开发工作。