5G移动终端认证状态漫游和传递方法

李 强

(北京邮电大学网络与交换技术国家重点实验室 北京 海淀区 100876)

【摘要】移动通信系统通过接入认证和密钥协商在网络与移动终端间建立信任关系，确保通信安全。5G中移动终端在移动过程中可能跨越多种接入方式，需要反复与网络进行认证和协商；物联网应用中存在大量功能相同、行为一致的成组终端，逐一与网络进行认证和协商对网络构成巨大压力。移动终端成功接入网络后，可由网络为其颁发认证状态标识，持该标识的设备可直接通过其他接入方式接入网或将该标识传递给组内成员。该方法可以实现认证状态的漫游，避免成组移动终端与网络逐一认证，从而提高接入效率，避免资源浪费，确保网络安全。

关 键 词 5G； 认证； 密钥协商； 状态标识

中图分类号 TN915.6 文献标志码 A doi:10.3969/j.issn.1001-0548.2018.05.007

5G Mobile Equipment Authentication State Roaming and Transmission Approach

LI Qiang

(State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications Haidian Beijing 100876)

Abstract The mobile communication network establishes a trust relationship between the network and the user equipment with authentication and key agreement. 5G network is a convergence network. User equipment can access the network through a variety of ways and it needs to authenticate with the network repeatedly when it is moving between two access networks. In the application environment of Internet of Thing, a group of user equipment with same characteristics and behaviors need to authenticate with the network one by one, which will over-consumes network resource and lowers access efficiency. To solve this problem, an authentication state identification mechanism is designed. If the user equipment successfully accesses the network, the network grants it a status identification. It can access the network with any way, no need access authentication again for a while. It also can transfer such an identification to the other members of the group, thus avoiding the authentication one by one. This mechanism can improve the efficiency of access, avoid the waste of resources and ensure the security network.

Key words 5G; authentication; key agreement; status identification

移动互联网、物联网的飞速发展迫切需要更大带宽、更高速率、更少时延、更多接入容量的移动通信技术的支撑[1]，尤其需要支持端到端通信和良好的移动性管理。第五代移动通信(5G)应运而生，相比4G，实现了千倍流量密度、百倍传输速率、毫秒级时延、千倍连接数密度。

网络与移动终端进行接入认证和密钥协商，对空口数据和空口信令进行加密和完整性保护是确保移动通信安全的通用技术手段。随着移动通信技术的发展，移动终端与网络间的认证和密钥协商技术不断完善，安全强度不断提高。

为支撑普遍的网络接入，满足不同应用场景的需求，5G将在4G技术基础上进行演进和创新，实现网络和无线传输关键技术的突破[2]。在网络方面，引入服务化网络架构、SDN、NFV、MEC等技术[3-4]。在无线方面，采用大规模天线、超密集组网、非正交多址、高频段通信、新型编码调制等技术[5]。同时，新的网络、空口技术和新的应用场景对5G网络的接入认证和密钥协商机制也提出了新的挑战。

1 移动通信接入认证协商技术发展

第一代移动通信系统(1G)是模拟蜂窝移动通信，只有语音业务，没有数据业务，因此也没有考虑数据网络方面的安全问题。第二代移动通信系统

收稿日期：2016－12－28；修回日期：2018－05－21
基金项目：国家863计划(2014AA01A705)).
作者简介：李强(1984－)，男，博士生，主要从事网络与信息安全、5G接入网方面的研究.

(2G)主要有基于时分多址的GSM系统和基于码分多址的CDMA系统。它不仅能提供清晰、稳定、优质的语音业务，还提供数据业务。同时在接入网设置了网络对用户的认证鉴权机制。第三代移动通信系统(3G)支持高速移动数据传输，可以实现图像、视频等大流量业务。在接入安全机制方面，3G也进行了加强，建立认证和密钥协商机制(authentication and key agreement, AKA)，对空口信令进行了加密和完整性保护。第四代移动通信系统(4G)较3G能够提供更优质的网络服务，满足语音、数据、影像、移动多媒体，以及移动计算、云计算等应用的需求，全面开启移动互联网时代。在网络接入方面，4G(TD-LTE)延用了AKA的思想，使用挑战应答机制，完成用户和网络间身份的双向认证。4G中设计了两层安全保护，NAS安全和AS安全，安全防护能力更强[6-7]。

移动通信系统中的接入认证协商机制，目的是在终端和网络之间建立信任关系，在此基础上采取加密等安全防护措施。从2G到4G，网络需与每一个终端分别进行认证协商。面对5G海量终端的接入需求，将对网络计算能力和效率带来巨大压力。信任传递和信任聚合技术是信任模型中的重要组成部分，尤其随着互联网、P2P、电子商务等应用的发展，越来越受到学术界的重视。文献[8]提出了一种面向无线传感器网络的信任评价传播机制及邻居节点间信任评价聚合方法。通过信任传递，可以为陌生双方提供二手的信任评估[9]，通过信任聚合可以实现信任信息的归集。借鉴信任模型中的信任传递和信任聚合思想，打破网络对终端逐一认证的局限，可有效提升网络的接入能力。

2　5G移动终端接入认证新需求

2.1　5G安全需求

未来，5G将广泛应用于智能制造、车联网、互联网金融等诸多领域，对5G的安全性提出了较高要求。5G作为未来移动互联网的主要载体将面临移动互联网广泛的网络攻击、病毒泛滥、隐私泄露等安全问题；多网异构融合、自组网、SDN、D2D等新技术的引入也为5G网络引入了诸多安全隐患。保证5G安全是保证5G能提供优质可靠服务的前题，也是5G研究的重点内容，受到学术界高度关注。

确保5G安全，从信息安全保障的层面，就是要确保网络安全、身份可信、实体可靠；从网络划分层面，就是要确保核心网安全、接入网安全、移动终端安全。空中接口的开放性导致其很容易受到主动干扰和被动窃听，移动终端的多样性、复杂性和不可控性使接入网络的安全性问题异常复杂。因此，接入认证安全是5G安全的关键环节，接入认证和密钥协商是5G网络安全防护主要手段之一。

2.2　移动终端认证状态漫游需求

5G网络必然是大量异构网络、移动终端等不同层次的网络元素共同构成的一个多层次、高密度、重叠覆盖的异构网络系统。移动终端可以采用有线网络、4G蜂窝网络、5G蜂窝网络、广播电视网络、卫星网络、WIFI网络、蓝牙网络、可见光网络等丰富多样的接入方式接入5G网络[10]。

移动终端支持多种网络接入方式，以便根据具体环境选择不同的接入网络。如：在5G和4G融合的网络中，当移动终端处在有5G网络覆盖的区域时，移动终端可以接入5G网络；当用户移动到没有5G网络覆盖的区域时，可以接入4G网络。移动终端需分别与5G网络和4G网络进行接入认证和密钥协商，如图1所示。在极端情况下(如在行进中的汽车上)，移动终端可能反复在多个接入网络中切换，进而反复与网络进行接入认证和协商。这占用了大量系统资源，影响网络效率，造成资源浪费。

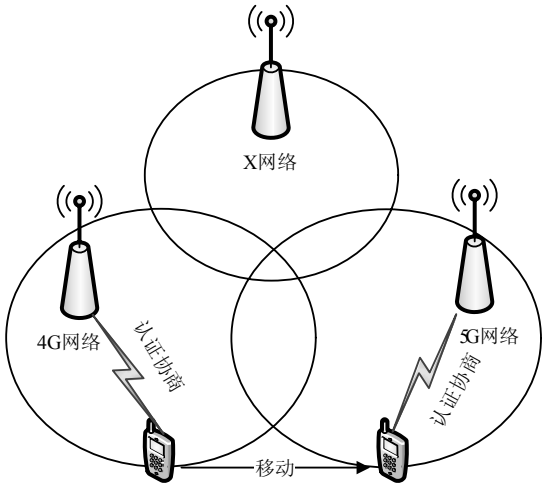

图1　移动终端在融合网络中的认证示意

因此，需要一种能够实现接入认证状态漫游的机制。当移动终端通过一种方式与网络成功完成认证和协商后，这种认证状态可以保持一定时间。当移动终端移动到其他接入网络时避免再次认证和协商。

2.3　成组终端统一接入需求

物联网实现物和物、人和物的互联，是智慧城市、智能交通、车联网等的基础，也是5G的主要应用场景之一。在物联网应用中，存在大量成批、成

组的移动终端[11]。这些移动终端具有相同的属性或行为特征，通常按一定规则或约束条件汇聚在一起，具有相同的应用范围和安全特征。同属一个组的移动终端往往在同一地理位置，同时或近同时接入网络，与网络进行一对一的认证和密钥协商，形成短时的认证协商高峰，对网络造成压力，如图2所示。如：一个居民楼有100个房间，每个房间配备了一台智能电表，每个智能电表需要定时将用户的用电情况通过5G网络上报给电力公司的服务器。该楼内的100台智能电表就可以认为是一个组，其具有相同的功能和行为，地理位置也很接近。100个设备会定期向网络发起接入认证请求，进行认证协商。

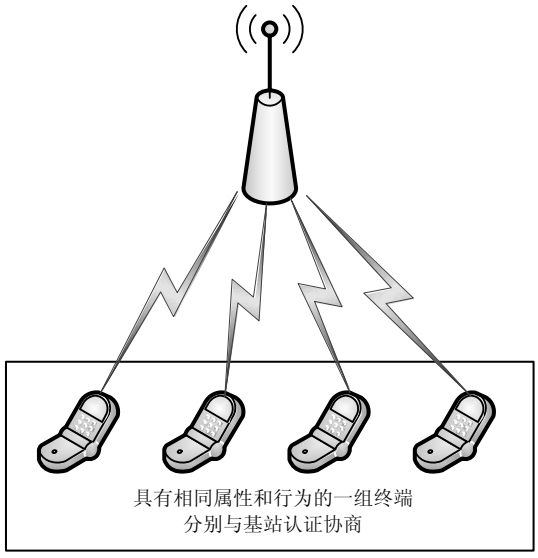

图2 成组终端接入示意

分析物联网的这种应用场景不难发现，一个组内的移动终端具有相同的属性和行为，近乎通过克隆实现。因此，有必要研制相应的接入认证克隆或接入认证聚合机制，实现成组统一接入认证或由组内一个成员代表全组进行接入认证。避免全组设备一对一认证协商的资源浪费。

3 基于标识的认证状态漫游和传递

3.1 统一接入认证和密钥协商协议

为保证5G网络的安全性，不论移动终端以何种方式接入网络，都应进行网络与移动终端间的认证和密钥协商，对交互数据进行加密和完整性保护。但基于5G网络接入方式的多样性，应设计统一的认证和密钥协商协议。认证和密钥协商协议定义认证和密钥协商的过程、交互的数据、交互数据的格式、验证方法等内容。只要通信链路正常，移动终端就可以采用相同的协议与网络进行认证和密钥协商，并实施后续的数据加密和完整性保护。如：移动终端通过5G接入网和通过固定热点接入网络时，虽然采用的通信信道不同，但移动终端应该采用同一套协议与网络进行认证和密钥协商。

3.2 认证状态漫游和传递的基本思路

为便于移动终端在不同接入网络中的移动和实现成组移动终端统一接入，提出基于认证状态标识的移动终端认证状态管理机制，基本思想如下：1) 移动终端在不同接入网络采用同一套协议与网络进行接入认证和密钥协商；2) 移动终端与网络成功认证协商后，建立网络与移动终端间的信任关系，产生后续加密和完整性保护密钥，该信任关系应保持一定的时间，不因移动终端移动和接入方式变化而失效；3) 由网络向通过认证的移动终端签发认证状态标识，该标识由网络统一制做并签发，接入网络可以验证标识的合法性；4) 移动终端在移动过程中，只要所持的认证状态标识不过期，可以直接通过各种方式接入网络，并使用前期协商出的密钥对通信数据进行加密和完整性保护；5) 接入网络在接收到移动终端带有认证状态标识的接入认证后，验证标识的正确性和有效性，验证通过后直接为移动终端提供网络服务。

3.3 4G(LTE)认证和密钥协商过程

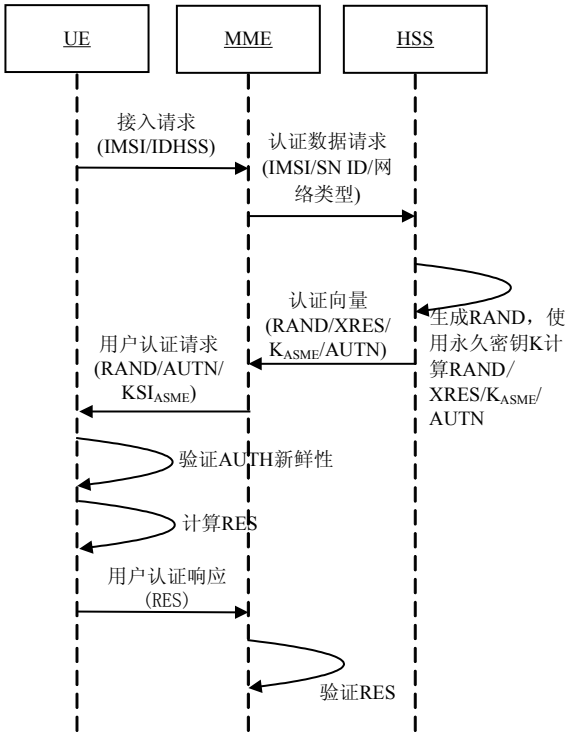

图3 LTE认证和密钥协商过程

以TD-LTE接入认证和密钥协商过程为例，进行优化和改进，实现认证状态漫游和成组统一接入，

首先对LTE接入过程回顾如图3所示。

1) UE(user equipment) 向 MME(mobility management entity) 发送 IMSI(international mobile subscriber identification number) 与 HSS(home subscriber serve)的标识IDHSS等身份信息，请求接入；

2) MME在本地查询是否有该IMSI对应的认证向量，如果没有向对应的 HSS请求认证数据；

3) HSS收到认证请求后，验证IMSI与SNID的合法性，通过后生成认证向量组(含多个认证向量)发回给MME，每个认证向量包括RAND、XRES、K_{ASME}、AUTN四元组；

4) MME收到应答后，存储认证向量组，并从中选择一个认证向量，将RAND、AUTN、K_{ASME}发送给UE；

5) UE收到后，验证AUTN的新鲜性，验证通过后计算RES与K_{ASME}，将RES传给MME；

6) MME将收到的RES与XRES进行比较，如果一致，则通过认证；

7) 认证通过后，MME与UE使用K_{ASME}根据约定的算法派生出加密密钥与完整性保护密钥，随后进行加密通信。

3.4　可漫游的认证协商过程

对现有LTE接入认证和密钥协商协议进行改进，在现有认证向量4元组的基础上添加认证状态标识，形成5元组。认证状态标识由网络使用非对称密码机制生成，接入网络可以对标识进行合法性验证。

改进后的认证和密钥协商过程如图4所示。

1) 初始时，HSS生成公私钥对，私钥保存在本地，公钥分发给各个MME；

2) HSS在生成认证四元组后，并为每个认证向量生成一个认证状态标识ASI，形成五元组，发给MME，认证状态标识的生成方法为：使用私钥对RAND、IMSI和失效时间EXPIRATION进行签名，使用签名值和EXPIRATION做为接入认证标识；

3) UE和MME完成认证协商，建立信任关系后，MME将ASI发给UE做为UE后续接入网络的凭证；

4) UE再次需要接入网络时，首先查看ASI中的过期时间是否已到，如果已过期，重新向网络发送认证请求，如果没有过期则使用之前协商出的加密密钥和完整性保护密钥对ASI进行加密和完整性保护，并将IMSI和密文ASI发送给MME；

5) MME根据IMSI查找加密和完整性保护密钥解密ASI，并验证完整性，验证通过，说明ASI与IMSI对应关系成立，接着使用HSS的公钥验证ASI的合法性，验证通过，说明ASI是HSS签发的合法标识，最后再验证ASI是否过期，如果没有过期，说明UE具有合法的认证状态，安全可信，直接提供通信服务。

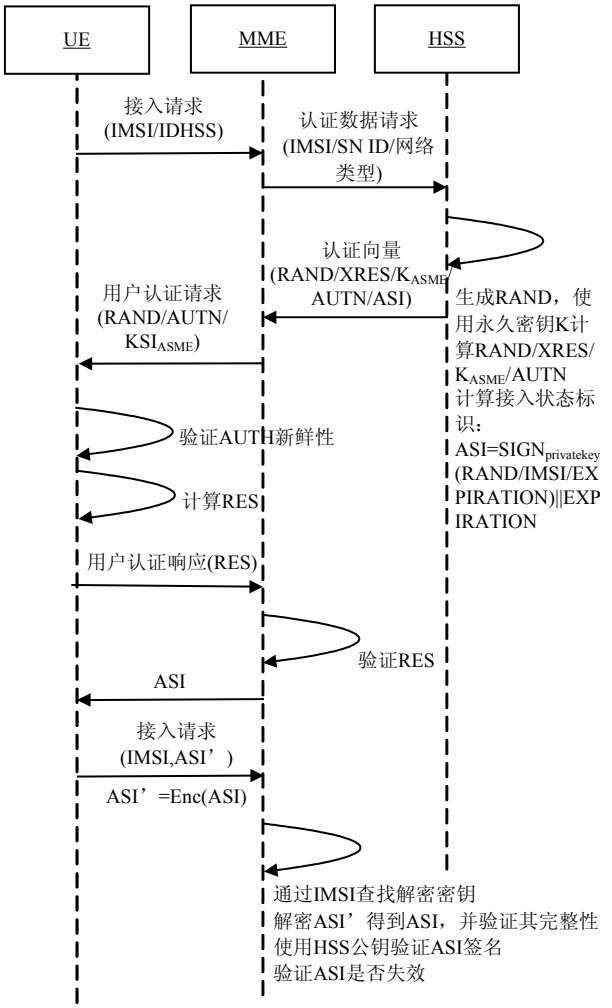

图4　可漫游的认证协商过程

3.5　成组统一接入认证过程

成组移动终端统一接入时采用与单个设备接入时相似的接入过程，区别在于成组接入时需要同时上传所有组内设备的IMSI，以便于MME和HSS掌握组内设备的情况，将协商的密钥与各个设备的IMSI建立绑定关系，具体过程如图5所示。

1) 组内设备通过选举或指定确定一个移动终端代表，该设备代表全组设备进行接入认证协商；

2) 代表设备向MME发送全组设备的IMSI和IDHSS，请求接入；

3) HSS发现MME的接入请求数据中含一组设备的IMSI，确定这是一个成组接入请求，将各个IMSI异或后做为一个IMSI，计算其接入认证标识ASI，将接入向量发送给MME，并记录K_{ASME}与各个设备IMSI的对应关系；

4) MME记录K_{ASME}与各个设备IMSI的对应关系；

5) UE与MME完成接入认证和密钥协商后，将ASI发送给UE；

6) UE可以将该ASI传递给组内的其它成员；

7) 组内任何一个其它成员需要使用网络时，将密文ASI和IMSI发送给MME；

8) MME通过IMSI查询对应的密钥(如果没有可以向HSS申请)，通过解密密文ASI并验证其完整性确定IMSI与ASI的对应关系，再通过HSS的公钥验证ASI的合法性以及是否超时，验证通过后直接为UE提供网络服务。

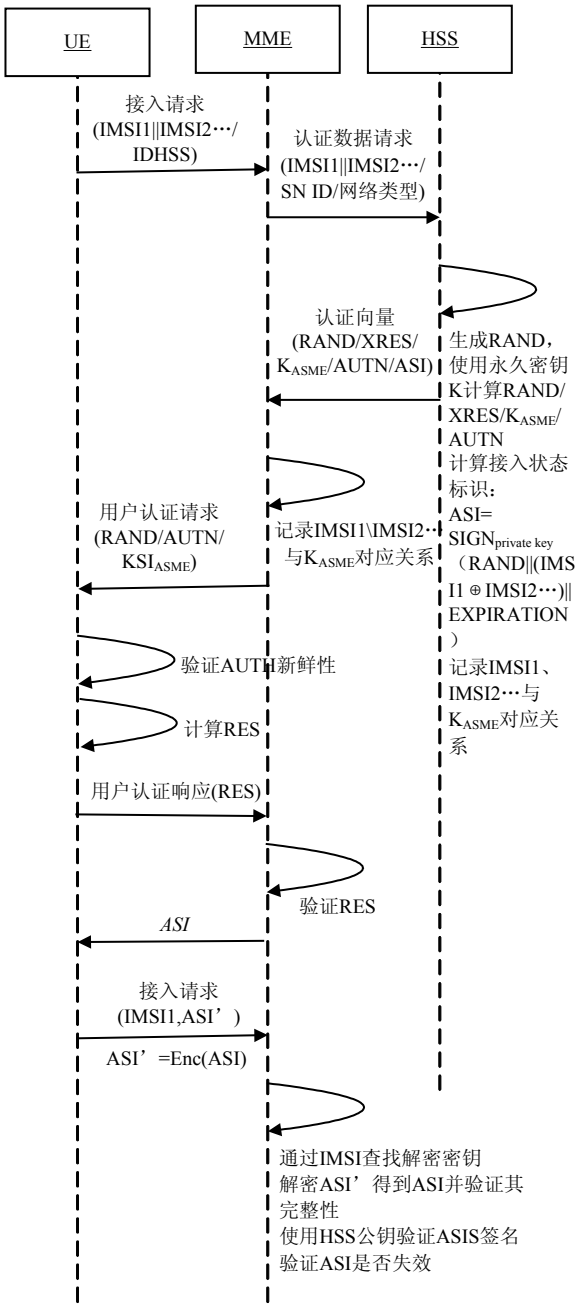

图5 成组统一接入认证过程

3.6 安全性和性能分析

网络向认证通过的移动终端颁发具有一定时效的认证状态标识，实现终端在不同接入方式之间的漫游和成组终端统一认证。认证标识具有可重复使用(有效期内)、可传递的特性，是实现认证状态漫游和组内传递的关键。网络对终端的信任状态也主要依赖于对认证状态标识的验证。因此，其安全风险主要有两个方面：一方面来自认证状态标识的伪造，也即非法终端伪造认证状态标识，欺骗网络实现接入；另一方面来自终端对合法认证状态标识的非法使用，即非法终端借用合法终端的认证状态标识欺骗网络实现接入认证。

对于认证状态标识伪造的风险，方法中的认证状态标识是在移动终端与网络成功认证协商之后，由网络颁发的，并且网络采用非对称密码机制，使用私钥对其进行了签名，私钥存储于HSS本地。终端持有认证状态标识向网络证明可信状态时，网络对认证状态标识中的签名进行验证，确保认识状态标识的合法性。因此，只要存储于网络的私钥不丢失，可以从密码机制上保证认证状态标识的真实性。

对于非法终端对合法认证状态标识的借用风险，方法中持有认证标识的设备，需使用前期协商出的密钥对认证标识进行加密和完整性保护后，再发给网络验证，网络通过解密和验证完整性，可以确定用户IMSI与对应密钥的对应关系；认证状态标识是网络对终端信息进行签名实现的，签名内容包括IMSI。验签成功，说明终端发送的IMSI和认证状态标识的对应关系成立，从而有效防止了非法用户借用合法标识接入网络。

通过在接入认证过程中设置认证状态标识的方法实现已接入终端的接入状态漫游和成组终端的统一接入认证。可在保证安全的前提下，有效提升网络的接入能力。一方面，已经与网络进行接入认证，建立信任关系的终端，在有效期内再次接入网络只需发送一次数据给网络，就可实现信任关系的延续，大大简化了终端与网络的交互流程，数据交互量降低到30%左右，节省信道资源和交互开销。另一方面，在终端处于高速移动或处于复杂网络环境中，需要在不同网络间频繁切换时，通过认证状态标识可以实现信任状态快速建立，有效提升终端移动性和通信效率，切换越频繁，优势越明显。同时，在物联网环境下，大量成组终端通过认证状态标识传递实现成组接入，避免逐一接入认证，有效降低网络接入认证压力。

4 结 束 语

网络与移动终端间的认证和密钥协商做为移动通信安全防护的主要手段，在5G中需要进行加强和改进。采用基于状态标识的接入认证状态漫游和传递机制可以有效降低终端在多种接入方式间切换时重复认证协商造成的资源浪费，实现物联网成组设备的统一接入认证。

为适应未来广泛的应用需求，提供优质、便捷、高效的网络服务，5G接入认证和密钥协商机制还需进行不断优化和完善，如设计可分级的接入认证机制、建立D2D和M2M时终端间的认证和加密机制等。

参 考 文 献

[1] 尤肖虎, 潘志文, 高西奇, 等. 5G移动通信发展趋势与若干关键技术[J]. 中国科学: 信息科学, 2014, 44(5): 551-563.
YOU Xiao-hu, PAN Zhi-wen, GAO Xi-qi, et al. Development trends and several key technologies of 5g mobile communication[J]. Scientia Sinica(Informationis), 2014, 44(5): 551-563.

[2] IMT-2020(5G) Promotion Group. 5G Vision and requirementswhite paper[EB/OL]. [2015-03-21]. http://www.IMT-2020.cn.

[3] 王胡成, 徐晖, 程志密, 等. 5G网络技术研究现状和发展趋势[J]. 电信科学, 2015, 9: 156-162.
WANG Hu-cheng, XU Hui, CHENG Zhi-mi, et al. Current research and development trend of 5G network technologies[J]. Telecommunications Science, 2015, 9: 156-162.

[4] 赵国锋, 陈婧, 韩远兵, 等. 5G移动通信网络关键技术综述[J]. 重庆邮电大学学报(自然科学版), 2015, 27(4): 441-452.
ZHAO Guo-feng, CHEN Jing, HAN Yuan-bing, et al. Prosective network techniques for 5G mobile communication: a survey[J]. Journal of Chongqing University of Posts and Telecommunications(Natural Science Edition), 2015, 27(4): 441-452.

[5] PIRINEN P. A brief overview of 5G research activities[C]// International Conference on 5g for Ubiquitous Connectivity. [S.l.]: ICST, 2015.

[6] 王映民, 孙韶辉. TD-LTE技术原理与系统设计[M]. 北京: 人民邮电出版社, 2010.
WANG Ying-min, SUN Shao-hui. TD-LTE principles and system design[M]. Beijing: People's Posts and Telecommunications Press, 2010.

[7] PARK Y, PARK T. A survey of security threats on 4G networks[C]//GLOBECOM Workshops. [S.l.]: IEEE, 2007.

[8] 蒋黎明, 张琨, 徐建, 等. 证据信任模型中的信任传递与聚合研究[J]. 通信学报, 2011, 32(8): 91-100.
JIANG Li-ming, ZHANG Kun, XU Jian, et al. Research on trust transitivity and aggregation in evidential trust model[J]. Journal on Communications, 2011, 32(8): 91-100.

[9] 王进, 孙怀江. 基于Jφsang信任模型的信任传递与聚合研究[J]. 控制与决策, 2009, 24(12): 1885-1889.
WANG Jin, SUN Huai-jiang. Trust transitivity and aggregation research based on Jφsang's trust model[J]. Control and decision, 2009, 24(12): 1885-1889.

[10] ASAI T. 5G radio access network and its requirements on mobile optical network[C]//International Conference on Optical Network Design and Modeling. [S.l.]: IEEE, 2015.

[11] ZENG L Y. A security framework for internet of things based on 4G communication[C]//International Conference on Computer Science and Network Technology. [S.l.]: IEEE, 2012.

编 辑 税 红