Scientific Research

A New Security Architecture for Cognitive Radio Networks

Li Zhu, Huaqing Mao
Department of information science& technology, Oujiang College, Wenzhou University , Wenzhou, China, 325027
yeah_1397118@hotmail.com,mrmaohuaqing@yahoo.com

Abstract: With rapid development of Wireless communication, more and more wireless standards appear. Cognitive radio networks (CRN) is built on cognitive radio technology which could provide a good solution for heterogeneous networks merging. However, heterogeneous networks merging leads to the various wireless standards are not compatible, and also security architectures of the different standards are not complete compatible. This paper focuses on security issues of heterogeneous networks merging. The paper firstly discusses security architectures of the current wireless standards such as: GSM, WiMAX. Then, a unified security architecture is constructed for the future cognitive radio networks. The new architecture consists of two security sub-layers: security of application layer (sub-layer 1) and physical layer (sub-layer 2). Sub-layer 1 focuses on the encryption algorithms, key management, authentication, data encryption and policy strategies. Sub-layer 2 is responsible for spectrum detection, spectrum distribution, and spectrum recycling. After analysis and discussion, we can conclude that: the proposed architecture is adaptable, scalable, and suitable for cognitive radio networks.

Keywords: Cognitive radio networks; heterogeneous networks merging; security architectures; unified security architecture;

一种新的认知无线网络安全体系结构

朱　丽，毛华庆
温州大学瓯江学院信息系，温州，中国，325027
yeah_1397118@hotmail.com,mrmaohuaqing@yahoo.com

摘　要:无线通信的快速发展导致通信标准不断增多，而各种标准之间并不兼容。认知无线网络是为解决不同标准无线网络融合问题而提出来的，主要针对核心网络的融合以及接入网络的融合。在提供通信服务时，由于各种标准之间的安全体系结构并不能完全兼容，异构网络在融合时会因为安全体系不兼容导致安全隐患。本文重点探讨在未来认知无线网络中，不同无线标准的安全体系兼容问题。本文首先着重介绍现有的 GSM、WiMAX 等标准的安全体系结构，并针对这些安全体系进行分析，在此基础上提出了适用于未来认知无线网络的统一安全体系架构，该结构由安全子层 1 和子层 2 组成：子层 1 由加密算法层、密钥管理层、身份认证层、数据加密层、策略管理层构成;子层 2 主要负责频谱感知、分配和回收。分析表明：该架构能够最大限度的符合未来网络所应具备的可适应性、可扩展性等特点，对未来网络体系结构、网络融合具有指导意义。

关键词：认知无线网络；异构网络融合；安全体系；统一安全体系结构;

1 引言

认知无线网络[1]是为解决网络融合问题而提出，主要针对核心网络的融合以及接入网络的融合。一般认为其以认知无线电[6]为基础构建，由支持认知无线电技术的终端、相关基础设施与控制策略组成无线网络。由于现有的无线通信标准其安全策略并不兼容。对于无线局域网、个人局域网等非商用无线网络，通过身份认证即可接入。而对于 GSM[9]、WCDMA、CDMA2000 等商用网络，具有严格的终端认证以及用户身份认证，

并且将终端认证与用户身份认证区分开来。通过基站端的严格认证来控制终端的合法性，通过 SIM 卡认证[8]来对用户身份、用户接入进行控制。在未来网络中，需要将这些安全标准不同的无线网络融合在一起，因此网络的安全成为隐患。具体来讲，在认知无线网络中，网络融合存在的安全问题主要是由于网络结构不同造成的。在未来认知无线网络中，有两种典型的网络结构：中心型网络和对等型网络。中心型网络存在中心节点，而对等型网络则没有中心节点， 所有用户处于平等状态。在中心型网络中，认知节点通过认知基站或现有基站设备接入现有网络，认知基站与现有核心网络设备可以通过有线连接的方式进行连接。认知基站负责协调所有认知终端，认知终端通过合作或者非合作的方式来感知整个频谱。在对等型网络中，认知节点与现有节点组成 MESH 网络，由现有节点或者终端节点对相关信息进行路由。未来认知无线网络需要解决中心型网络和对等型网络的融合问题，由于这两种结构采用的安全策略不同，简单宽泛的融合会造成安全策略不一致，从而导致安全隐患的出现。本文结合现有无线通信标准的安全机制建立了统一安全体系结构。该安全体系结构能够为网络体系结构、网络融合等提供参考。同时，对现有网络的安全改进也具有重要意义。

2 现有的安全体系架构分析

在现有无线通信标准中，由于安全需求等级不一样，其所采用的安全体系架构也有所区别。总体来讲，现有的各种安全体系架构主要分为接入安全、网络安全及用户安全。其中接入安全主要是针对接入过程中的安全问题，包括身份认证[7]、身份识别等。网络安全主要包括传输安全、传输可靠性等。用户安全主要包括用户程序安全、用户身份保密等。未来网络安全体系架构基于现有网络安全体系架构并能兼容现有体系架构。但由于其特殊性，需要面临新的安全问题。通过分析现有的网络安全体系架构，可以对设计未来安全体系架构提供参考。

2.1 第三代移动通信安全体系

第三代移动通信系统[11]的安全体系结构主要包括以下几个方面：

网络接入安全：主要包括用户标识的保密性、实体认证、数据加密、数据完整性；

网络域安全： 包括密钥建立、密钥分配、安全通信三个层次；

用户域安全：提供用户到 USIM 的认证以及 USIM 到终端的链接认证；

应用程序域安全： 终端平台的系统安全，为应用程序开发商以及网络运营服务商所提供的创建应用程序的能力，其安全级别可以由应用程序提供商根据需要选择；

安全可见度与可配置型：包括接入网络加密提示，安全级别提示等；

现有的 3G 安全机制[12]的总体结构如图 1 所示：

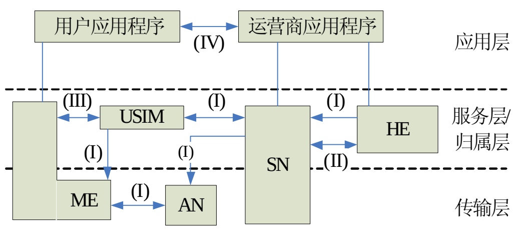

Figure1. 3G security architecture
图 1 现有 3G 网络安全体系结构

由上图可以看出，3G 的网络安全体系由 3 个层面组成：传输层、服务层/归属层和应用层。传输层的安全主要由移动终端以及认证网络接入模块进行保护，主要针对接入网络的过程。服务层/归属层安全主要由用户 USIM 卡进行安全防护，服务层的安全主要是对用户身份进行确认，对用户在网络中的注册地址进行记录。应用层的安全则主要包括用户终端应用程序的安全，主要由用户终端系统进行防范，以及运营商的应用程序安全。

3G 网络相比 2G 网络[10]健壮了许多，包括对用户的身份认证（SIM 认证）以及接入网络的安全改进，但同时也存在安全隐患。主要表现在， 3G 的安全是建立在核心网安全的基础上，核心网络间的数据交换采用有线方式，现有的组网方式认为核心网络属于可信网络，认证向量采用明文方式在各个实体间进行传输。如果攻击者从核心网络入手，获得了某个部分的访问权限，则可以通过对 VLR 和 HLR 之间的消息进行窃听，来获得认证向量 AV，从而可以获得加密密钥 CK 与完整性密钥 IK。整个过程如图 2 所示：

3G 安全体系的第二个缺陷表现在 CK、IK 的新鲜性依赖于随机数，而随机数又依赖于 SQN，在系统中 SQN 的设计可以保证使用过的鉴权向量不会再次出

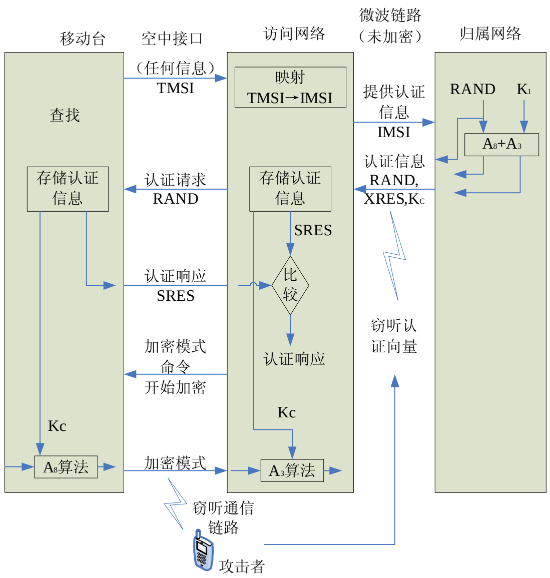

Figure 2. 3G network attack model

图 2 3G 网络攻击示意

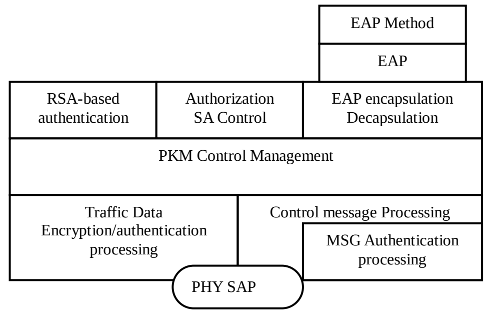

Figure 3. 802.16 security sublayer

图 3 802.16 安全子层示意

从图 3 可以看出，802.16 安全体系结构构建于物理层之上，使用 PKM 管理认证授权[5,7]。终端的身份采用 x.509 证书方式，包括终端的公钥以及 MAC 地址。在建立初始通信连接时，对 MAC PDU 加密，而对 MAC 头信息和管理信息不加密。

现，即重放攻击是无效的。但攻击者可以通过另外的方式来获得：通过劫持可信终端，获得网络的信任，从而获得 CK、IK，来取得鉴权向量给用户鉴权。这样非法用户可以通过合法终端来攻击整个网络。

2.2 802.16 安全体系

在现有的 802.16 协议中[3,4]存在两个版本的安全机制：PKMv1、PKMv2 其中 802.16d 只有 PKMv1 版本，PKMv2[2]版本增加了双向认证机制，以及 EAP 认证方法。在通信过程中所使用的 AK 结合移动终端的 MAC 地址和基站 ID，通过 Dot16KDF 算法获得，而不是由基站随机生成。该方法的优势在于能够避免攻击者伪造基站骗取终端用户的信任，同时能够对企图接入网络的非法终端进行屏蔽，而且密钥的安全强度将得到较大的提高。在 802.16 中， MAC 层包含三个子层：

服务聚合子层（CS：Service-Specific Convergence Sublayer），该子层是下层和高层协议的接口，把通过 CS 服务接入点的上层协议数据包转变或者映射到 MAC 的 SDU（Service Data Unit）；

公共部分子层（CPS：Common Part Sublayer），实现包括系统接入、动态带宽分配、链接建立以及链路维护等 MAC 层的主要功能；

加密子层（PS：Privacy Sublayer），提供与安全有关的功能，包括加密、认证、密钥交换等。

802.16 的安全子层结构如下图所示：

3 认知无线网络安全体系结构构建

未来认知无线网络构建于认知无线电基础之上，因此未来网络除了会存在现有网络的安全问题之外，还会面临物理层的安全问题。对此，本文认为未来网络应针对频谱安全问题，将频谱安全子层分离出来，成为独立的安全子层。同时，未来网络不会脱离于现有的无线网络，因此，网络架构与现有网络会保持一致。在网络安全方面，应对不同的子层设置不同的安全功能模块，负责处理不同的安全问题。

3.1 分层的安全体系结构

认知无线网络除了面临现有网络的各种安全问题，还存在新的安全隐患，即由于工作频谱的不确定性所导致的 DoS 攻击[1]。因此，在未来网络安全体系架构中，需要针对身份认证以及频谱管理设置新的子层。其结构如图 4 所示：

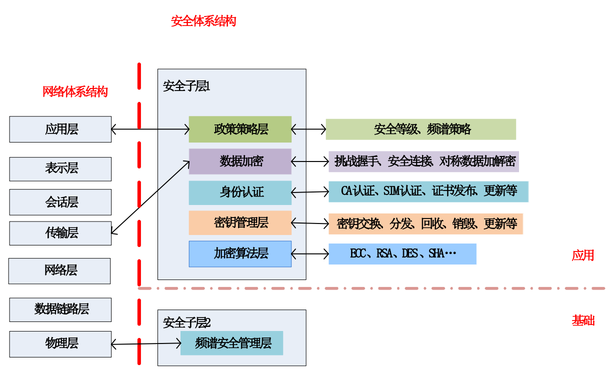

Figure 4.security architecture of cognitive radio networks

图 4 认知无线网络安全体系结构示意

978-1-935068-18-1 © 2010 SciRes.

考虑与现有网络体系结构的对应，新的安全体系结构应该具有两个安全子层。安全子层 1 主要负责网络传输安全以及身份认证安全，安全子层 2 主要负责网络频谱安全。

安全子层 1 包括以下几部分：

加密算法层：整个安全体系结构的核心，包括各种对称和非对称加密算法、报文摘要算法等。该层应囊括现有无线通信标准所采用的各种加解密算法。其它各层均从加密算法层获取加解密方法。值的注意的是，这些加密算法需要得到各种标准组织的认可，并且按照其加密强度区分安全等级。上层根据不同的安全需要以及计算能力选择合适的算法；

密钥管理层：主要负责在通信双方交换密钥，包括密钥的分发、回收、销毁、更新等。密钥管理依赖于加密算法。同时应采用非对称加密算法对密钥进行传输。部分无线通信标准由于安全等级较低，通常密钥管理不需要单独作为一层来处理。

身份认证层：为核心网络的主要安全保障。应结合现有 Internet 的 CA 认证[13]以及 GSM 的 SIM 身份认证。未来网络中，将逐步统一为第三方认证方法。主要包括证书的发布、更新、验证、销毁等。

数据加密层：在连接建立后进行的数据交换按照安全等级可以分为安全连接、非安全连接。对于安全等级较高的安全连接，所有数据将进行加密处理，而对于非安全连接，只有部分机要数据进行加密处理。在此层中，还需要进行挑战握手的管理，改进的挑战握手机制一直存在于通信过程中。

政策策略层：包括应用程序所需要采用的安全等级、物理层对频谱的管理策略等。该层在安全体系结构中，主要负责依据通信要求选择合适的安全等级。

安全子层 2 包括：

频谱安全管理层：包括对各种频段的监控，根据历史信息以及相关共享信息，对终端节点周围的频谱使用情况做出判断，当频谱使用情况出现较大异常时，应及时采取措施对其进行控制。

3.2 加密算法层

加密算法层主要负责整个通信过程中的加密算法，包括对称加密和非对称加密算法。其中对称加密主要用于对数据的加密，非对称加密主要用于密钥的交换、身份的认证等过程。摘要算法，比如 MD5，SHA 等，主要用于对数据安全性的保障，能够保证数据不被篡改。加密算法层具有扩展性，除了能够兼容现有的各种方法外，还应该支持用户自定义算法以及扩展算法。其组成如下图 5 所示：

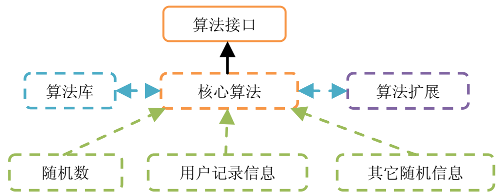

Figure 5. Components of Encryption algorithm layer
图 5 加密算法层组成框图

核心算法为上层应用提供算法接口，根据用户需要调用算法库中的各种加解密算法进行相关运算。算法扩展模块为用户提供自定义算法接口，用户可以自己根据需要确定相关的算法并纳入到核心算法库中。

核心算法依赖的随机数、用户记录信息、其它随机信息等作为整个加密算法层的支撑。在认知无线网络中，可以以用户的位置信息、频谱信息等信息作为随机数的发生种子。

3.3 密钥管理层

密钥管理层主要负责对整个通信过程中各类密钥进行分发、管理、更新以及销毁。密钥在使用过程中可能存在暴露、重复等问题，因此需要对其定期进行更新。此外，随着通信过程的结束，需要将密钥销毁。可以看出：密钥管理层在整个密钥生存周期内，承担重要的职责。其业务流程如图 6 所示：

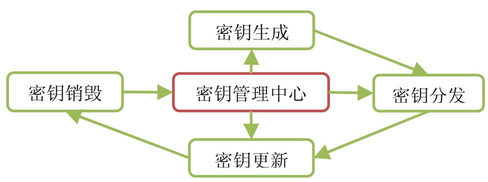

Figure 6.Business process of key management
图 6 密钥管理层业务流程

密钥管理中心的业务流程分为两类：正常业务流程和非正常业务流程。

正常业务流程： 密钥生成后使用非对称加密算法进行分发，用户获得密钥后正常使用；密钥管理中心根据业务需要定期更新密钥；会话结束后对密钥进行销毁；

非正常业务流程：密钥产生并分发后，发现密钥存在暴露、破解、重复等问题时，立即更新密钥生成算法，

并对密钥重新进行分发。

密钥管理中心一般由位于网络中的第三方来承担，因此第三方的安全应作为整网安全的基石。

3.4 身份认证层

身份认证层包括基站用户对终端用户的认证以及终端用户对基站用户的认证。对于终端用户身份，可以采用 EAP-SIM[8]的认证方式，即每个终端配备独立的身份识别卡。对于基站用户，采用第三方的身份认证方法，即通过 CA 为基站用户颁发证书。其组成框架如图 7 所示：

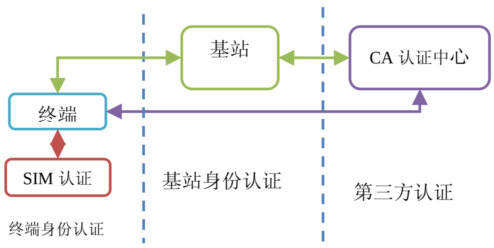

Figure 7.Process of authentication layer
图 7 身份认证层流程

在身份认证过程中，基站与核心网络连接，由核心网络中身份认证鉴别单元对终端上传的相关身份信息进行认证，这些认证信息包括终端身份和用户身份两部分。在现有的 3G 网络中，通过 HLR 以及权鉴单元来实现对终端和用户的认证。终端用户通过终端设备唯一编号 IMSI 进行认证，用户身份通过 USIM 进行认证。

引入第三方认证主要有以下两种目的：1.对基站身份的认证；如果潜在的攻击者模拟基站用户，诱骗终端接入网络从而获取用户信息，则通过对 CA 中心颁发的数字证书可以避免此类安全隐患。用户在接入网络时，获取基站的相关信息，并将信息与第三方颁发的信息进行对比，以此确认基站是否合法。2.认证中心对终端的认证；这里的认证是指对终端设备的认证。可以在终端制造时，将证书写入终端设备，这样可以保证终端设备的合法性。

CA 中心位于核心网络中，因此需要保证现有网络的权鉴单元与 CA 认证中心的连接安全。对于核心网络的安全，由于其采用有线连接的方式，因此面临的安全攻击会小很多。

3.5 数据加密层

数据加密层与网络体系结构中传输层对应，主要包括传输过程中的安全连接、对称的数据加解密等过程。数据加密层以身份认证层为基础。在通信双方身份得到认证和保证的前提下，对通信数据进行加密。

数据加密层根据应用层的需求，对不同的数据采取不同的加密方式。对于系统信令相关的数据，采用最高等级的加密，对于一般的数据流，根据需要可以采用流密钥进行加密，而对于视频、语音等信号，在保证网络流量的基础上，只需要进行扰乱、卷积等运算即可。

值得注意的是，通信双方在建立连接后，可能因为异常因素导致连接被重置，此种情况下，身份认证层需重新对通信双方进行身份认证。

为了保证通信过程的安全，在数据传输过程中，数据加密层定期对网络连接进行重置。以防范可能存在的连接冒充、篡改等安全隐患。

3.6 政策策略层

政策策略层主要包括通信过程所采用的整体安全策略，以及对于未来网络，频谱政策的理解和应用。其中，网络所采用的整体安全策略关系到整个通信过程的严密性和安全性，需要考虑众多因素。

此外，频谱政策也是政策策略层应考虑的因素。对于工作频段，未来的频谱政策可能会放宽条件，但同时也存在众多的限制条件，比如工作时段限制、功率限制等，策略层需要依据用户对频段的需求以及网络所能提供的工作频段综合考虑，选择适合的安全策略和频谱策略。

频谱策略管理主要针对在未来网络中，可用频谱和已授权频谱的管理问题。针对需要接入网络的认知设备，除了对其发射功率、接收功率、可工作频段做出强制性的规则，以避免被攻击者所利用。对发射功率的控制能够保证接入设备不会成为其他正常工作网络设备的干扰源，对接收功率的控制能够保证其不能监听大范围、远距离的其它设备。工作频段的确定能够让设备工作于某些指定的频段，以免非全频段的设备对国防、海事、卫星等的正常通信造成干扰。

频谱策略的管理是整个安全管理的宏观指导方法，应由标准化组织确定，各国依据自己情况进行细化。该标准尚未冻结，还有很大的研究空间。

3.7 频谱安全管理层

频谱安全管理层主要解决未来网络可能面临的动态频谱问题。如果工作频段可以移动，则攻击者可通过加大功率，让通信网络的各个节点处于无频段可用的状

978-1-935068-18-1 © 2010 SciRes.

态。为解决此问题，需要在未来网络中专门增加频谱安全管理层。其结构如图 8 所示：

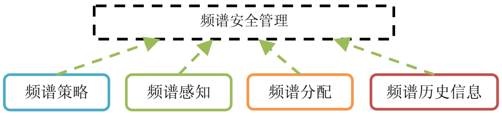

Figure 8. Spectrum security management layer
图 8 频谱安全管理层示意

频谱策略层主要用于对可用频谱的管理以及频谱礼仪的管理。对于未来网络，具有认知能力的设备具有动态的频谱接入能力，但绝非所有频段均可接入。频谱策略即从宏观上规定哪些频段可以接入、何时可以接入等问题。此外，对于可用的空白频段，多个认知设备之间该如何进行接入，即接入的频谱礼仪，也需要进行规定。

频谱感知用于解决未来网络中多个频谱感知信息的融合。对于不同的终端节点，其感知到的频谱信息不尽相同，为了获得最准确的频谱信息，需要对虚假信息以及异常信息进行排除，使用权重融合算法等对频谱信息进行融合，从而保证信息的准确。频谱感知的安全应能够有效对攻击节点上报的频谱信息进行防范。

频谱分配主要是针对网络中的节点，使其频谱分配保持在一个范围内，而非按需索取，这样能够防范潜在的攻击者非法获取可用频谱，造成其它正常工作节点的频谱资源耗尽。频谱分配能够保证频谱在认知节点和主用户节点之间得到有效、公平、安全的利用。

由于在随机数产生过程中采用了终端及基站节点记录的频谱历史信息，因此保证历史信息的安全是频谱安全管理的重点。如果攻击者能够获得终端节点的历史记录信息，则可能会对通信过程中的随机数进行猜测。从而导致一系列的安全隐患。频谱历史信息的安全采用两种方式来进行保护：1）对终端节点历史记录的访问需要采用相应的授权机制；2）终端节点与基站节点应进行历史记录的同步与扰乱。

4 结论

本文针对未来认知无线网络需要兼容现有无线网络的特点，提出了一种统一的分层安全体系结构。该结构由加密算法层、密钥管理层、身份认证层、数据加密层、策略管理层以及物理频谱安全管理层组成。此安全体系结构融合了现有的无线网络、有线网络安全体系结构特点，采用分离设计的方式，最大限度的保证了未来网络的安全体系能够兼容现有的网络，同时，使现有网络以最小化的成本升级到更可靠的安全体制结构上。

References (参考文献)

[1] Chen R., Park J. M., Defense against primary user emulation attacks in cognitive radio networks, IEEE Journal on Selected Areas in Communications, 2008, 26(1), pp. 25～37.
[2] Ke Fang, Rong Wang, Formal analysis of IEEE802.16 security authentication protocol, Netinfo Security, 2008, (9).
[3] Zhang Lirong Fang Ailian Research on Information Secruity of Wimax/802．16e, Computer&Digital Engineering, 2008, 36(9).
[4] Jiang Yichuan Wang Xuping, Research on the security in WMAN IEEE802．16, Computer Applications and Software, 2008, 25(11).
[5] Mandin J., 802.16 e Privacy key management (PKM) version 2, IEEE C802. 16e-02/131r1, 2002 .
[6] Cordeiro C., Challapali K., Birru D., et al., IEEE 802.22: an introduction to the first wireless standard based on cognitive radios, Journal of communications, 2006, 1(1), pp.38～47.
[7] Johnston D, Walker J., Overview of IEEE 802. 16 security, IEEE Security & Privacy Magazine, 2004, 2(3), pp.40～48.
[8] Haverinen H, Salowey J, EAP SIM Authentication, Work in Progress, 2004.
[9] Zhang Yi，Cui Tian-xi， Mutual authentication in GSM based on Elliptic Curve Cryptography and combined public key technology, Computer Engineering and Applications，2008.
[10] Liu Dong-su, Wei Bao-dian, An amendment of authentication and key agreement protocol of 3G mobile communications system，Journal of china institute of communications, 2002.
[11] Lai Xin, Ruan Zhigang， The Improvement 3G Authentication Protocol based on Public Key Cryptosystem ， China information security，2006
[12] Hu Xilei, A Security Countermeasure for E—Government Based on Internet，Computer security，2009