第3章

无线网络安全

随着第五代无线通信标准(5th Generation,5G)的不断完善和应用,无线网不仅限于人与人之间的通信,也不再是传统的语音通话,它几乎涵盖了社会生活的方方面面。智能的概念也被越来越多的人熟知和接受。无线通信作为推动世界信息化进程的重要动力之一,发生着日新月异的进步与变化。因此,无线网络的安全既有传统经典的安全问题,也包括很多未知的风险。本章从无线网络发展史,到无线网络安全协议,以及最新的无线智能安全展开阐述,试图给读者一个清晰的无线网络安全脉络,以便进行深入研究。无线网络的安全包括多层的安全加密,物理层采用先进的 MC-CDMA、协作通信 MIMO 设计以及波束赋型算法来提高安全速率,对于 5G 系统会广泛采用的无线传感器网(WSN),在安全技术上考虑了加密协议、路由算法、拓扑结构三大方面。

3.1 无线网络发展历史

无线网络(Wireless Network)指的是任何形式的以电磁波传送信息的网络,它可以和有线网络相连协助传递信息。通常无线网络都对应于移动网络。早在 1897 年,马可尼在陆地和一只拖船之间用无线电进行了消息传输,引领无线通信的开端,至今,无线通信已有 100 多年的历史,在这期间无线通信技术突飞猛进。从 1978 年第一代模拟蜂窝网的诞生,它的发展历史可以概括为以下几个阶段。

(1) 第一代无线网络(1G):包括美国 AMPS、CDPD,英国 TACS,瑞士、荷兰等的 NMT 标准。

(2) 第二代无线网络(2G):包括欧洲 GSM、GPRS、EDGE 等。

(3) 第三代无线网络(3G):包括美国 IS-95、WCDMA、TD-SCDMA、cdmaOne、CDMA2000 等标准产品,3G 标准的国际制定组织有 UMTS、IMT-2000等。

(4) 第四代无线网络(4G):两大主流标准是 TD-LTE 和 WiMAX。

(5) 第五代无线网络(5G):目前 5G 的主流标准还未统一,可以初步认为它是在前几代网络基础上的融合和进一步的创新,从人到人的连接到万物互连,从单纯的通话到多媒体的人机交互,从无线电话网到智慧城市,从微量处理

到海量数据，从基站到云平台，从单天线到大规模 MIMO，从蜂窝网到切片技术，从中心处理到边缘计算，从固定到智能，5G 将给人们带来全新的生活体验。

在此期间，学术界关于无线网络还有其他不同维度的划分，例如无线局域网 WLAN、无线广域网 WBAN、无线个人网 WPAN、无线传感器网 WSN、ZigBee、蓝牙、移动自组织网等，它们一直贯穿在三、四和五代无线网络的发展中，作为主流网络的补充或替代。在技术不断创新发展的三十余年内，历经了第一代无线通信系统（1G）的模拟时代、第二代无线通信系统（2G）的数字时代与第三代无线通信系统（3G）的中低速数据时代，直到 2014 年前后大规模商用的第四代无线通信系统（4G）进入了高速数据时代。而 5G 是在 4G 基础上，对于无线通信提出更高的要求，它不仅在速度而且在功耗、时延等多个方面有了全新的提升。由此互联网的发展也将从移动互联网进入智能互联网时代。国际标准化组织 3GPP 定义了 5G 的三大场景。其中，eMBB（enhanced Mobile Broadband）指 3D/超高清视频等大流量移动宽带业务，mMTC（massive Machine Type Communications）指大规模物联网业务，URLLC（Ultra Reliable Low Latency Communications）指如无人驾驶、工业自动化等需要低时延、高可靠连接的业务。

通过 3GPP 的三大场景定义可以看出，对于 5G，世界通信业的普遍看法是它不仅应具备高速度，还应满足低时延这样更高的要求。从 1G 到 4G，无线通信的核心是人与人之间的通信，个人通信是无线通信的核心业务。但是 5G 的通信不仅仅是人的通信，而且是物联网、工业自动化、无人驾驶等业务的综合，通信从人与人之间通信转向人与物的通信，直至机器与机器之间的通信。

图 3-1 概括了前 4 代无线通信的业务范围。

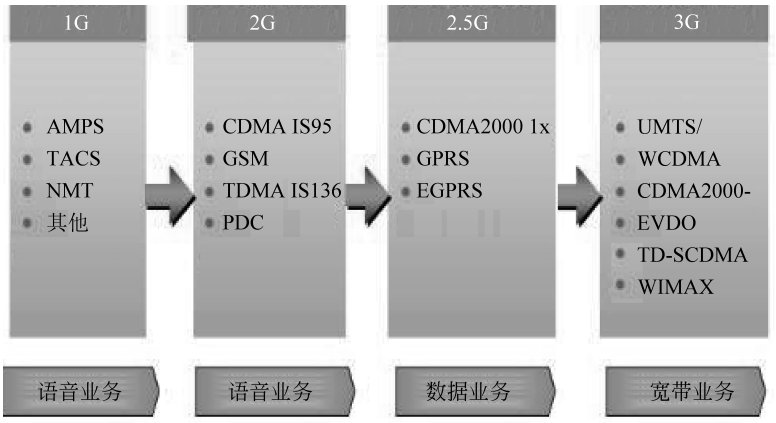


图 3-1　前 4 代无线通信的业务范围

下面介绍一下每一代无线通信标准。

1. 第一代无线通信系统

20 世纪 70 年代末，美国 AT&T 公司通过使用电话技术和蜂窝无线电技术研制了第一套蜂窝移动电话系统，取名为先进的移动电话系统，即 AMPS（Advanced Mobile Phone

Service)系统。第一代无线网络技术的一大成就在于它摆脱了电话线的束缚,用户第一次能够在移动的状态下拨打电话。这一代主要有 3 种窄带模拟系统标准,即北美蜂窝系统 AMPS、北欧移动电话系统 NMT 和全接入通信系统 TACS,我国采用的主要是 TACS 制式,即频段为 890～915MHz 与 935～960MHz。第一代无线通信的各种蜂窝网系统有很多相似之处,但是也有很大差异,它们只能提供基本的语音会话业务,不能提供非语音业务,并且保密性差,容易并机盗打,它们之间还互不兼容,显然移动用户无法在各种系统之间实现漫游。

2. 第二代无线通信系统

为了解决由于采用不同模拟蜂窝系统造成互不兼容无法漫游服务的问题,1982 年北欧四国向欧洲邮电行政会议(Conference Europe of Post and Telecommunications,CEPT)提交了一份建议书,要求制定 900MHz 频段的欧洲公共电信业务规范,建立全欧统一的蜂窝网无线通信系统。同年成立了欧洲无线通信特别小组(Group Special Mobile,GSM)。第二代无线通信数字无线标准主要有 GSM、D-AMPS、PDC 和窄带 IS-95CDMA 等。在我国,现有的 3G 无线通信网络主要以第二代无线通信系统的 GSM 和窄带 CDMA 为主。为了适应数据业务的发展需要,在第二代技术中还诞生了 2.5G,也就是 GSM 系统的 GPRS 和窄带 CDMA 系统的 IS-95B 技术,大大提高了数据传送能力。第二代无线通信系统在引入数字无线电技术以后,数字蜂窝无线通信系统提供了更好的服务,不仅改善了语音通话质量,提高了保密性,防止了并机盗打,而且也为移动用户提供了无缝的国际漫游。

3. 第三代无线通信系统

第三代无线通信技术包括 IMT-2000 和 LTE,提供宽带移动多媒体通信系统,能够实现无缝覆盖和全球漫游。它的数据传输速率高达 2Mb/s,其容量是第二代无线通信技术的 2～5 倍,目前最具代表性的有美国提出的 MC-CDMA(CDMA2000),欧洲和日本提出的 W-CDMA 和中国提出的 TD-SCDMA。H3G 在 2003 年 3 月第一个推出 3G 商用服务,投入使用的有 3G 英国、3G 意大利、3G 奥地利、3G 瑞典等。2007 年,美国 3G 手机用户数量猛增 80%,达到 6420 万部。

4. 第四代无线通信系统

从核心技术来看,通常 3G 技术主要采用 CDMA(Code Division Multiple Access,码分多址)技术,而业界对新一代无线通信核心技术的界定主要是指采用 OFDM(Orthogonal Frequency Division Multiplexing,正交频分复用)调制技术的 OFDMA 多址技术,可见 3G 和 4G 技术最大的区别在于采用的核心技术完全不同,因此从这个角度来看 WiMAX、LTE-Advanced 和 IEEE 802.16m 等技术均可被视为 4G;不过从标准的角度来看,ITU 对 IMT-2000(3G)系列标准和 IMT-Advanced(4G)系列标准的区别并不以核心技术为参考,而是通过能否满足一定的技术要求来区分,ITU 在 IMT-2000 标准中要求,3G 技术必须满足传输速率在移动状态 144kb/s、步行状态 384kb/s、室内 2Mb/s,而

ITU 正在制定的 IMT-Advanced(4G)标准中要求在使用 10MHz 信道带宽时,理论传输速率达到 1.5Gb/s。

在 2008 年 2 月,ITU-RWP5D 正式发出了征集 IMT-Advanced 候选技术的通函。经过两年的准备时间,ITU-RWP5D 在其第六次会议上(2009 年 10 月)共征集到六种候选技术方案,它们分别来自两个国际标准化组织和三个国家。这六种技术方案可以分成两类:基于 3GPP 的技术方案和基于 IEEE 的技术方案。

(1) 3GPP 的技术方案:LTE Release 10 & beyond (LTE-Advanced),该方案包括 FDD 和 TDD 两种模式。由于 3GPP 不是 ITU 的成员,该技术方案由 3GPP 所属 37 个成员单位联合提交,包括我国三大运营商和四个主要厂商。3GPP 所属标准化组织以文稿的形式表态支持该技术方案。韩国政府也以文稿的形式支持。最终该技术方案由中国、3GPP 和日本分别向 ITU 提交。

(2) IEEE 的技术方案:802.16m,该方案同样包括 FDD 和 TDD 两种模式。BT、KDDI、Sprint 等 51 家企业,日本标准化组织和韩国政府以文稿的形式表态支持该技术方案,我国企业没有参加。最终该技术方案由 IEEE、韩国和日本分别向 ITU 提交。

经过 14 个外部评估组织对各候选技术的全面评估,最终得出两种候选技术方案完全满足 IMT-Advanced 技术需求。2010 年 10 月的 ITU-RWP5D 会议上,LTE-Advanced 技术和 802.16m 技术被最终确定为 IMT-Advanced 阶段国际无线通信标准。我国主导发展的 TD-LTE-Advanced 技术通过了所有国际评估组织的评估,也被确定为 IMT-Advanced 国际无线通信标准。

无线网络的发展方向之一就是“万有无线网络技术”,也就是将各种不同的无线网络统一在一个设备。Intel 公司正在开发的芯片采用软件无线电技术,可以在同一个芯片上处理 WiFi、WiMAX 和 DVB-H 数字电视等不同无线技术。

在第二次世界大战期间,无线通信改变了传统战争的模式,显示了科技的强大威力。而无线网络的持续发展,在人们生活中所占比例也越来越大。现如今,校园、商场、高楼,无线网几乎遍布世界的所有陆地区域。卫星通信、微波通信、室内无线局域网通信,通过主干有线网的有力支撑使得世界范围内万物互联不再只是梦想。

图 3-2 显示了从第二次世界大战时期到今天无线网络的发展,从最初的战场通信,到现在的移动支付、无人驾驶,无线网络在人类生活中扮演着重要角色。

5. 应急无线网络

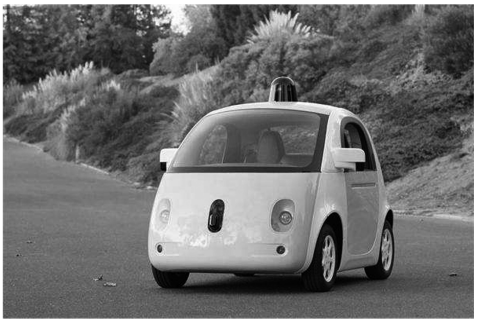
上述所说 4 代网络中并没有特别强调自然界突发危机状况下组建网络。诸如在当今地震、洪水、狂风、冰雹等灾难不断发生的环境下,如何应用无线移动自组织网络及时快速救援,也使得对于无线通信的研究领域另辟蹊径,相辅相成。

无线网络的重要应用之一还包括为基础电信建设贫乏或缺乏资源的发展中国家和落后地区提供一个快速便捷的通信互连环境。由于世界范围内标准林立,厂家众多,强者凌弱,各自为政,也使得在使用无线网络时,兼容性的问题不断浮现。不同的制造厂商所生产的组件可能无法在同一个平台使用。这一问题也许会在 5G 网络时代得到解决。

(a) 战争时代的通信

(b) 现代手机

(c) 利用无线网络完成收付款



(d) 无线网络完成无人驾驶

图 3-2 无线网络的发展示例

3.2 无线网络标准简述

3.2.1 AMPS

AMPS(高级移动电话系统)是由美国 AT&T 开发的最早的蜂窝电话系统标准。AMPS 是第一代蜂窝技术,使用单独的频带,或者说信道为每次对话服务。因此它需要相当的带宽来支持一个大数量的用户群体。在通用术语中,AMPS 常常被当作更早的 OG 改进型移动通信服务,只不过 AMPS 使用更多的计算功率来选择频谱、切换到 PSTN 线路的通话以及处理登记和呼叫建立等。

真正将 AMPS 从更早的 OG 系统中区分出来的是最后的呼叫建立功能。在 AMPS 中,蜂窝中心可以根据信号强度灵活地分配信道给每个手持终端,允许相同的频率在完全不同的位置复用,并且没有干扰。这使得在一个地区内,大数量的手持终端被同时支持成为可能。AMPS 的创始者们发明了“蜂窝”这个术语正是因为它在一个基站系统里使用的都是小的六边形“蜂窝”形状。

AMPS 由于模拟通信的固有缺陷曾受指责。首先它是一个模拟标准,它很容易受到静电和噪声的干扰,而且也没有安全措施阻止扫描式的偷听。一些肆无忌惮的偷听者采

用特制的设备可以截取手持设备的电子序列号和移动标识码(也叫电话号码),并复制和克隆到一个不同的手持电话然后在别的地方建立呼叫,逃避电信付费。后来问题变得越发严重以至于一些运营商不得不要求客户在打电话前使用 PIN。渐渐地,蜂窝网络公司建立了一个系统叫作 RF 指纹识别,它可以确定一部电话和另一个电话信号的细微差别,然后切断一些克隆者的电话。一些合法的用户虽然对自己的电话做了设置,但在手机更换电池或者天线后问题又会再次出现。

3.2.2 CDPD

CDPD(Cellular Digital Packet Data,蜂窝数字分组数据)系统是第一代分组数据网络的典型代表。CDPD 最早是美国电报电话公司(AT&T)为满足计算机用户对移动数据通信的需求而开发的。它与美国的 AMPS 共用一个频段,共用一套基站和天线,利用移动电话的空闲信道传送数据。当移动电话话音需要占用某个信道时,CDPD 系统就另找一条新的空闲信道,并且利用信道切换技术自动切换到新的空闲信道上进行数据的传送,直到数据传输完毕。这种系统在美国获得较为广泛的应用。1993 年,美国电信工业协会和电子工业协会(TIA/EIA)通过了 CDPD 的业务规范。此后,CDPD 系统在硬件和软件上都有了很大的进展。

尽管 CDPD 是在 AMPS 模拟蜂窝移动电话网上提供分组数据服务的一种系统,但它并不影响话音通信,而是利用 AMPS 中未被使用的资源提供数据通信。CDPD 的最大信道速率为 19.2kb/s。CDPD 的基本原理是按一定的规则,把要传送的数据分成若干定长的数据段,并给每一数据段加上收、发终端地址及其他控制信息,以“分组”为单位,在 AMPS 的空闲信道上进行传输。在一次数据接续中,每个数据分组可以通过不同的无线信道进行传送。由于各数据分组不需要单独占用信道,所以可以与其他用户共同享用信道。因此能充分利用信道,提高通信效率,降低数据通信的费用。现在 CDPD 系统既可以使用业务信道,也可以使用专用信道进行通信。

CDPD 系统主要由移动终端、固定终端、移动数据基站、管理服务器、信息服务器、网络管理系统等组成。每个管理服务器可支持 8 个分组服务器,每个分组服务器可支持 32 个移动基站,一个基站拥有 6 个信道,每个信道约 2000～3000 个用户。CDPD 采用 IP 高层网间协议,各部分的通信靠 TCP/IP 来连接。外部主机与 CDPD 网之间可采用 X.25 协议或 Internet 互连。CDPD 具有标准性好、开放性强、传输效率高等特点。

尽管 CDPD 在其他国家没有得到广泛采用,但其思想和技术为进一步发展蜂窝分组数据业务打下了基础。

3.2.3 GSM

GSM(Global System for Mobile Communications,全球移动通信系统)在中国俗称全球通。

它是由欧洲电信标准组织 ETSI 制定的一个数字无线通信标准。空中接口采用时分多址技术。自 20 世纪 90 年代中期投入商用以来,被全球超过 100 个国家采用。GSM 标准的设备占据当前全球蜂窝无线通信设备市场 80%以上。

GSM是当前应用最为广泛的移动电话标准。全球超过10亿人正在使用GSM电话。GSM标准的无处不在使得在移动电话运营商之间签署“漫游协定”后用户的国际漫游变得很平常。GSM较之它以前的标准最大的不同是它的信令和语音信道都是数字式的，因此GSM被看作是第二代移动电话系统。GSM是一个当前由3GPP开发的开放标准。

3.2.4 GPRS

GPRS(General Packet Radio Service,通用分组交换无线数据业务)标准代表通用分组交换无线数据业务，又称2.5G，特点是传输速率高，每个信道最大传输速率21.4kb/s，要求最大数据吞吐量每用户171kb/s，现实的最高吞吐量为115kb/s。可以提供彩信收发和邮件接收等业务，采用分组交换，多个用户可分时共享一个时隙，或者一个用户最多可使用八个时隙，接入速度快，费用低。

GPRS是GSM在第二阶段提供的分组数据业务。欧洲早在1993年就提出了在GSM网上开通GPRS业务，标准化工作始于1994年，1997年取得重大进展，1997年10月，ETSI(European Telecommunications Standards Institute,欧洲电信标准化协会)发布了GSM02.60 GPRS Phase1的业务描述。GPRS的标准化工作分3个阶段进行，这3个阶段分别制定18个新标准并对几十个现有标准进行修订。修改的标准包括：05系列无线接口物理层，04.08MAC/RLC和第三层移动性管理，09.02MAP增加Gr和Gd接口协议，04.04-04.07GPRS系统和时间信息安排，03.20安全方面，03.22空闲模式过程，11.10TBR-19MS测试，11.2XBSS测试，11.11SIM，12.XX0&M，01.61加密算法等。ETSI已完成GPRS各个阶段的标准化工作，随同GSM的其他标准，从2001年开始全部移交给ITU，由ITU的3GPP等组织继续发展和版本的更新。

GPRS的现状已经非常成熟。不管人们如何评价GPRS在无线通信发展历程上的作用，目前，全世界已有近百个运营商开通了GPRS商用系统、试商用系统或实验系统。从1999年开始，英国的BTCellNET、德国的T-Mobile、荷兰的TELFORT以及法国、西班牙、意大利、俄罗斯、澳大利亚、新加坡、菲律宾等国家和地区的运营商，纷纷在其GSM网叠加发展GPRS。2001年各运营商有了非常大的发展，2002年基本进入商用化。

2001年，英国BTCellNET和瑞典Telia公司向其几百万用户提供GPRS业务；土耳其最大的无线通信运营商TurkCell投资约700万美元在土耳其提供商用GPRS业务；泰国总接入通信公司TAC为移动用户开办GPRS业务；AT&T无线公司为美国的用户提供GPRS业务。另外，BT和AT&T联合成立的Concert公司提供GPRS业务批发，Concert向运营公司提供批发30个国家的GPRS移动漫游业务，用户可以通过单一的虚拟GPRS漫游交换连接到IP骨干网。

GPRS是一种采用分组交换模式传输高速、低速数据及信令的高效率方式。它克服了电路交换型数据传输速率低、资源利用率差的缺陷，也不像短消息、USSD那样无法适应大量数据应用而仅适合于少量突发数据应用。与现有GSM数据业务相比，GPRS具有如下优势。

(1) 资源共享，频率利用率高。GPRS的信道分配原则是“多个用户共享，按需动态分配”。它的基本思想是将一部分可用的GSM信道专门用于传送分组数据，由MAC协

议来管理多址接入，多用户可以协调对带宽的利用。GPRS的上、下行信道独立分配，同一时隙的上、下行方向可以服务于不同的用户，方式更加灵活，减小了资源的浪费。

(2) 采用数据流量计费。用户可以保持一直在线，只有在读取数据的时候占用资源和进行付费，改变以往按连接时间计费的方式，这将节约用户资费，从而吸引更多用户。

GPRS为GSM网向第三代演进打下了基础。

GPRS是GSM移动电话用户可用的一种移动数据业务。GPRS可以说是GSM的延续。GPRS和以往连续在频道传输的方式不同，是以分组(Packet)式来传输，因此使用者所负担的费用是以其传输资料单位计算，并非使用其整个频道，理论上较为便宜。

3.2.5 EDGE

EDGE(Enhanced Data Rate for GSM Evolution，改进数据率GSM服务)是一种介于现有的第二代移动网络与第三代移动网络之间的过渡技术，比“二代半”技术GPRS更加优良，因此也有人称它为“2.75代”技术。传输速率是GPRS的3倍，传输速率最高可达384kb/s。主要业务为邮件接收、视频/音乐下载、快速上网。

3.2.6 UMTS

UMTS(Universal Mobile Telecommunications System，通用无线通信系统)是国际标准化组织3GPP制定的全球3G标准之一。作为一个完整的3G无线通信技术标准，UMTS并不仅限于定义空中接口。它的主体包括CDMA接入网络和分组化的核心网络等一系列技术规范和接口协议。除WCDMA作为首选空中接口技术获得不断完善外，UMTS还相继引入了TD-SCDMA和HSDPA技术。

3.2.7 IS-95A

1993年7月高通公司开发了窄带CDMA蜂窝体制，该体制被采纳为北美数字蜂窝标准，定名为IS-95A。

IS-95A是由高通公司发起的第一个基于CDMA数字蜂窝标准，IS-95A也叫TIA-EIA-95。基于IS-95A的第一个品牌是CDMAOne。它是一个使用CDMA的2G无线通信标准。IS-95A CDMA系统的工作频段是800MHz，采用频分双工的模式，采用码片速率为1.2288Mb/s的PN码进行扩频，系统带宽为1.25MHz。

IS-95A系统承载的业务主要为话音业务，话音速率为速率集1(RS1)，也称为8k速率集。RS1的话音速率有4种：9.6kb/s、4.8kb/s、2.4kb/s和1.2kb/s。具体的话音速率是在进行码激励线性预测(CELP)编码时，根据话音当时的属性由声码器做出判断。IS-95A CDMA系统也支持基于电路方式的有限速率数据业务，最大可到9.6kb/s。IS-95A及其相关标准是最早商用的基于CDMA技术的无线通信标准，它或者它的后继CDMA2000也经常被简称为CDMA。

1994年3月中国开始试验CDMA，1998年11月试运营网(133网)开通，2002年4月联通新时空CDMA网络正式运营，2004年用户数超过400万。1998年全球CDMA用户达到500多万，CDMA的研究和商业进入高潮。1999年CDMA在日本和美国形成增

长的高峰期，全球的增长率高达250%，用户达到2000万。

3.2.8 CDMA2000

CDMA2000由美国提出，是由IS-95A系统演进而来的，并向下兼容IS-95A系统。CDMA2000系统继承了IS-95A系统在组网、系统优化方面的经验，并进一步对业务速率进行了扩展，同时通过引入一些先进的无线技术，进一步提升系统容量。在核心网络方面，它继续使用IS-95A系统的核心网作为其电路域来处理电路型业务，如语音业务和电路型数据业务，同时在系统中增加分组设备(PDSN和PCF)来处理分组数据业务。因此在建设CDMA2000系统时，原有的IS-95A的网络设备可以继续使用，只要新增加分组设备即可。在我国，联通公司在其最初的CDMA网络建设中就采用了这种升级方案，在2008年中国电信行业重组时，由中国电信收购了中国联通的整个CDMA2000网络。2000年10月韩国SK Telecom公司就推出了世界上第一个商用CDMA2000 1X网络。2001年4月，LG电信也推出了CDMA2000 1X服务。目前，韩国已经开通CDMA2000 1X EVDO服务。经过合并，韩国形成了以3个全国范围的移动运营商为主的格局。

CDMA系统是基于码分技术(扩频技术)和多址技术的通信系统，系统为每个用户分配各自特定地址码。地址码之间具有相互准正交性，从而在时间、空间和频率上都可以重叠；将需传送的具有一定信号带宽的信息数据，用一个带宽远大于信号带宽的伪随机码进行调制，使原有的数据信号的带宽被扩展，接收端进行逆向解扩解调操作，增强了抗干扰的能力。

CDMA，一开始建网是IS-95A，然后升级到CDMA2000 1X，再到了现在已经开始的CDMA2000 1X EVDO，比起GSM，CDMA辐射小。在射频部分完全兼容，不需要重新建基站。技术上，CDMA2000 1X采用扩频速率为SR1，即指前向信道和反向信道均用码片速率1.2288Mb/s的单载波直接系列扩频方式。因此它可以方便地与IS-95(A/B)后向兼容，实现平滑过渡。CDMA2000 1X采用了反向相干解调、快速前向功控、发送分集、Turbo编码等新技术，网络部分引入分组交换，可支持移动IP业务。在相同条件下，对普通话音业务而言，容量大致为CDMA(IS-95)系统的2倍。CDMA2000 1X手机上网的传输速率可达144kb/s，比现有CDMA产品高出10倍。

3.2.9 WCDMA

欧洲电信标准委员会(ETSI)在GSM之后就开始研究其3G标准，其中有几种备选方案是基于直接序列扩频码分多址的，而日本的第三代研究也是使用宽带码分多址技术的，其后，以二者为主导进行融合，在3GPP组织中发展成了第三代无线通信系统UMTS，并提交给国际电信联盟(ITU)。国际电信联盟最终接受WCDMA(Wideband Code Division Multiple Access，宽带码分多址)作为IMT-2000 3G标准的一部分。目前。WCDMA是世界范围内商用最多、技术发展最为成熟的3G制式。在我国，中国联通公司在2008年电信行业重组之后，开始建设其WCDMA网络。日本在2000年12月以招标方式颁发了3G牌照，2001年10月，日本的NTT DoCoMo在世界上第一个开通了WCDMA服务。3年后，3G正逐渐走出发展初期的低谷。日本是世界上3G网络起步最

早的国家之一。

3.2.10　TD-SCDMA

TD-SCDMA(Time Division-Space Code Division Multiple Access,时空码分多址)是中国提出的第三代无线通信标准,也是 ITU 批准的 3 个 3G 标准中的一个,以我国知识产权为主,被国际上广泛接受和认可。它是我国电信史上重要的里程碑。相对于另两个主要 3G 标准(CDMA2000 和 WCDMA),它的起步较晚。

该标准的原标准研究方为西门子公司。为了独立出 WCDMA,西门子公司将其核心专利卖给了大唐电信。之后在加入 3G 标准时,信息产业部(现工业和信息部)以爱立信、诺基亚等电信设备制造厂商在中国的市场为条件,要求他们给予支持。1998 年 6 月 29 日,中国邮电部电信科学技术研究院(现大唐电信科技产业集团)向 ITU 提出了该标准。该标准将智能天线、同步 CDMA 和软件无线电(SDR)等技术融于其中。

TD-SCDMA 的发展始于 1998 年初,在当时的邮电部科技司的直接领导下,由电信科学技术研究院组织队伍在 SCDMA 技术的基础上,研究和起草符合 IMT-2000 要求的我国 TD-SCDMA 建议草案。该标准草案以智能天线、同步码分多址、接力切换、时分双工为主要特点,于 1998 年 6 月 30 日提交到 ITU,从而成为 IMT-2000 的 15 个候选方案之一。

经过一年多的时间,经历了几十次工作组会议,几百篇提交文稿的讨论,在 2001 年 3 月棕榈泉的 RAN 全会上,随着包含 TD-SCDMA 标准在内的 3GPPR4 版本规范的正式发布,TD-SCDMA 在 3GPP 中的融合工作达到了第一个目标。

至此,TD-SCDMA 不论在形式上还是在实质上,都已在国际上被广大运营商、设备制造商所认可和接受,形成了真正的国际标准。

但是由于 TD-SCDMA 的起步比较晚,技术发展成熟度不及其他两大标准,同时由于市场前景不明朗导致相关产业链发展滞后,最终导致了 TD-SCDMA 虽然成为第三代无线通信国际三大标准之一,但除了在中国由中国移动进行商用之外,并没有其他商用市场。

TD-SCDMA 由于采用时分双工,上行和下行信道特性基本一致。因此,基站根据接收信号估计上行和下行信道特性比较容易。此外,TD-SCDMA 使用智能天线技术有先天的优势,而智能天线技术的使用又引入了 SDMA 的优点,可以减少用户间干扰,从而提高频谱利用率。

3.2.11　LTE

LTE(Long Term Evolution,长期演进项目)标准是 3G 的演进,始于 2004 年 3GPP 的多伦多会议。LTE 并非人们普遍误解的 4G 技术,而是 3G 与 4G 技术之间的一个过渡,是 3.9G 的全球标准,它改进并增强了 3G 的空中接入技术,采用 OFDM 和 MIMO 作为其无线网络演进的唯一标准。在 2MHz 频谱带宽下能够提供下行 326Mb/s 与上行 86Mb/s 的峰值速率。改善了小区边缘用户的性能,提高小区容量和降低系统延迟。LTE 将大大提升用户对无线通信业务的体验,为运营商带来更大的技术优势和成本优

势，巩固蜂窝移动技术的主导地位，改善目前通信业务的 IPR 格局。

与 3G 相比，LTE 具有如下关键技术特征。

(1) 通信速率有了提高，下行峰值速率为 10Mb/s，上行峰值速率为 5Mb/s。

(2) 提高了频谱效率，下行链路为 5(b/s)/Hz，上行链路为 2.5(b/s)/Hz。

(3) 简单的网络架构和软件架构，以信道共用为基础，以分组域业务为主要目标，系统在整体架构上将基于分组交换。

(4) 通过系统设计和严格的 QoS 机制，保证实时业务(如 VoIP)的服务质量。

(5) 系统部署灵活，能够支持 1.4～2MHz 间的多种系统带宽，可支持对称和非对称的频谱分配，保证了将来在系统部署上的灵活性。

(6) 非常低的网络时延。子帧长度为 0.5ms 和 0.675ms，解决了向下兼容的问题并降低了网络时延。

(7) 增加了小区边界比特速率，在保持目前基站位置不变的情况下增加小区边界比特速率，OFDM 支持的单频率网络技术可提供高效率的多播服务。

(8) 强调向下兼容，支持已有的 3G 系统和非 3GPP 规范系统的协同运作，支持自组网(Self-organising Network)操作。

针对 LTE 扁平化的网络架构，LTE 系统采用了用户层与控制层分离的策略，网元连接用户设备，作为中转站使用户能够与核心网相连，其中用户的控制层信令通过 S1-MME 接口传输至 MME(Mobility Management Entity，移动管理实体)，用户层数据通过 S1-U 接口传输至服务网关(Service Gateway，SGW)。控制层和用户层传输的协议不尽相同。

LTE 的标准化研究始于 2004 年，于 2008 年 12 月推出第一个 LTE 标准 Release 8 版本。Release 8 版本是 LTE 标准的基础版本，该版标准里定义了 LTE 采用的核心技术，包括帧结构、正交频分复用技术、MIMO 技术、高阶调制技术、先进信道编码技术、功率控制技术等。此后，LTE 相关技术与标准不断发展，后续版本皆是对已提出的技术进行强化，对 LTE 通信系统的传输速率和系统容量进一步增强，提高系统性能。2009 年 12 月，3GPP 推出 Release 8 版协议的增强版本 Release 9 版本。Release 9 版本与基础版本 Release 8 版相比，只做了少量修改，加入一些新的技术，包括终端定位技术、自组织网络、家庭基站等技术。

2011 年 3 月，在 Release 9 版本的基础上，对其进行局部增强后，推出的 Release 10 版本被接纳为真正的 4G 标准，也被称为 LTE-A 的基础版本，之后在其基础上，又相继不断推出 Release 11 演进版本、Release 12 演进版本和 Release 13 演进版本。

3.2.12 TD-LTE

TD-LTE 即 TD-SCDMA Long Term Evolution，第四代无线通信标准之一。TD-LTE 得到了大家的一致关注。

TD-LTE 系统分为控制层和用户层，其中控制层用于传输与控制相关的信令等控制信息，在整个系统的工作中有至关重要的作用。控制层协议栈即为控制层数据在传输过

程中严格遵守的协议，通过研究控制层协议栈中网元接口、重要控制流程，进而达到优化控制流程、特殊场景应用等相关目的。第四代无线通信系统由于采用了正交频分复用(Orthogonal Frequency Division Multiplexing，OFDM)等技术，使得系统拥有了更高的通信速率，从而进入高速数据时代。第四代无线通信系统中按照接入方式的不同分为两种标准——LTE-TDD 和 LTE-FDD，其中，LTE-TDD 上下行采用在相同频点而在不同时隙间切换，进行发送和接收数据，其由 TD-SCDMA 进化演进而来，在国内习惯称为 TD-LTE(Time Division Long Term Evolution，时分长期演进)；LTE-FDD 的上下行采用不同的频点分别进行数据的发送和接收。由于 TD-LTE 通信系统对通信速率与时延提出了较高的要求，其中下行速率需达 100Mb/s，上行速率需达 50Mb/s，时延 10ms 内，故 TD-LTE 系统的物理层方面也采用了全新的技术，包括 OFDM 技术、新型多址接入技术、MIMO 技术、波束赋形技术、载波聚合技术等。这些技术构成了 LTE 系统的核心技术，使得 TD-LTE 系统相比于 3G 通信系统出现了质的飞跃，不仅速率得到了极大提升，频谱利用效率、小区间干扰等问题也得到有效解决。

语音业务在 TD-LTE 系统网络建设初期由于各种限制，无法在分组域实现语音业务，而现有的 2G/3G 网络如果不加以利用，将造成资源极大的浪费。因此，在 TD-LTE 系统协议制定之初的 Release 8 版协议中，就提出了电路域语音回落(Circuit Switch FallBack，CSFB)方案进行 TD-LTE 系统语音业务的演进过渡。CSFB 方案目前承担了 TD-LTE 系统中的大部分语音业务，由于网络建设缓慢和用户终端设备的支持，CSFB 方案在 TD-LTE 系统中还将继续长期承担主要的语音业务。

由于控制层协议栈在系统中起到的主要作用，控制层信息内容丰富，控制层协议栈分析与应用研究作为 TD-LTE 系统的研究重点之一，科研院所和研究机构均对此投入巨大精力，并涌现了大批成果。

用户在 TD-LTE 系统中的服务类型包括数据业务、通话业务及短信业务，其中数据业务包括 UE 发起的服务请求、UE 接收数据业务即寻呼、VoLTE 通话业务。

作为 TD-SCDMA 的演进技术，TD-LTE 目前已经成为 3GPP 里面唯一的基于 TDD 技术的 LTE 标准。中国已经全面启动的 TD-LTE 产业与国际 LTE 产业基本同步，而且已被国际广泛接受。TD-LTE 将为中国在引领无线通信产业的发展带来很重要的机遇。2008 年 3 月，工业和信息化部电信研究院和中国移动牵头的 TD-LTE 工作组成立。一年多来，该工作组从国家发展策略、技术和产业路线的研究、加快推动标准制定等各方面大力推动 TD-LTE 的技术和产业化发展。2009 年，TD-LTE 在国际标准化、技术创新、整体测试、产业化方面已经取得了一系列突破性的进展。

TD-LTE 一方面继承了 TD-SCDMA 智能天线、特殊时隙等的核心专利；另一方面，由于中国企业在国际标准化组织中的实力不断增强，且参与 LTE 的研发工作较早，从而在一些 3G 时代并不占据优势的技术领域获得了新的专利。因此，总体看来，TD-LTE 有望实现中国自主专利整体比重的进一步提升。现在我国自主研发 TD-LTE 标准的进展比较顺利。同时也得到了国际制造企业的鼎力支持，包括国内企业大唐、华为、中兴等在内的厂商等，均已投入到 TDD-LTE 和 LTE FDD 的融合研发中来。由中国移动牵头、沃

达丰等运营商参加的 TDD 和 FDD 融合的发展之路，进一步推动了 TD-LTE 和 LTE FDD 的融合发展。可以说，具有自主知识产权、以我国为主的 TD-LTE 标准技术的形成，为 TD-SCDMA 技术的后续发展演进明确了方向。TD-LTE 既继承并发展了 TD-SCDMA 的中国自主知识产权技术，又很好地与 FDD LTE 技术实现了协同发展，为 TD-SCDMA 可持续发展、我国自主创新技术走向全球市场开辟了重要空间，创造了历史机遇。TD-LTE 已经成为国际产业广泛关注的 TDD 技术。印度、日本、韩国、欧美等国家和地区的海外运营商已经与我国产业建立了 TD-LTE 合作，多家运营商计划在 2010 年启动试验网建设乃至实际网络部署。TD-LTE 国际市场机遇已经显现。

3.2.13 WiMAX

WiMAX 的全称是 Worldwide Interoperability for Microwave Access(微波存取全球互通)，又称为 IEEE 802.16 无线城域网，是一种为企业和家庭用户提供的宽带无线连接方案。WiMAX 的技术起点较高，WiMAX 所能提供的最高接入速率是 7Mb/s，这个速率是 3G 所能提供的宽带速率的 30 倍。

WiMAX 网络在网络覆盖面积和网络的带宽上优势巨大，WiMAX 也成为 4G 的两大主流标准之一。

3.2.14 BT

蓝牙(Bluetooth)技术是世界著名的 5 家大公司——爱立信(Ericsson)、诺基亚(Nokia)、东芝(Toshiba)、国际商用机器公司(IBM)和英特尔(Intel)于 1998 年 5 月联合宣布的一种无线通信新技术。蓝牙设备是蓝牙技术应用的主要载体，常见蓝牙设备有计算机、手机等。蓝牙产品容纳蓝牙模块，支持蓝牙无线电连接与软件应用。蓝牙设备连接必须在一定范围内进行配对。这种配对搜索被称为短程临时网络模式，也被称为微微网，可以容纳设备最多不超过 8 台。蓝牙设备连接成功，主设备只有一台，从设备可以有多台。蓝牙技术具备射频特性。采用了 TDMA 结构与网络多层次结构，在技术上应用了跳频技术、无线技术等，具有传输效率高、安全性高等优势，所以被各行各业所应用。

蓝牙是一种支持设备短距离通信(一般 10m 内)的无线电技术。能在包括移动电话、PDA、无线耳机、笔记本计算机、相关外设等众多设备之间进行无线信息交换。利用蓝牙技术，能够有效地简化无线通信终端设备之间的通信，也能够成功地简化设备与网络之间的通信，从而数据传输变得更加迅速高效。蓝牙采用分散式网络结构以及快跳频和短包技术，支持点对点及点对多点通信，工作在全球通用的 2.4GHz ISM(即工业、科学、医学)频段。其数据速率为 1Mb/s。采用时分双工传输方案实现全双工传输。

3.2.15 ZigBee

在蓝牙技术的使用过程中，人们发现蓝牙技术尽管有许多优点，但仍存在许多缺陷。对工业、家庭自动化控制和工业遥测遥控领域而言，蓝牙技术太复杂、功耗大、距离近、组网规模太小等。而工业自动化，对无线数据通信的需求越来越强烈，对于工业现场，无线

传输必须是高可靠的，并能抵抗工业现场的各种电磁干扰。因此，经过人们长期努力，ZigBee(紫蜂)协议在2003年正式问世。

ZigBee是一种低速短距离传输的无线网上协议，底层是采用IEEE 802.15.4标准规范的媒体访问层与物理层。主要特点是低速、低耗电、低成本、支持大量网上节点、支持多种网上拓扑、低复杂度、快速、可靠、安全。ZigBee与蓝牙相类似，是一种新兴的短距离无线通信技术，用于传感控制应用，例如5G中的智能农业网、智能家居、智慧交通、智能停车网等。它由IEEE 802.15工作组提出，并由下属TG4工作组制定规范。

2001年8月，ZigBee Alliance成立；2004年，ZigBee V1.0诞生，它是ZigBee规范的第一个版本。由于推出仓促，存在一些错误；2006年，推出ZigBee 2006；2007年年底，推出ZigBee PRO；2009年3月，推出ZigBee RF4CE，具备更强的灵活性和远程控制能力；2009年开始，ZigBee采用了IETF的IPv6 6LoWPAn标准作为新一代智能电网Smart Energy(SEP 2.0)的标准，致力于形成全球统一的易于与互联网集成的网络，实现端到端的网络通信。

ZigBee在数千个微小的传感器之间相互协调实现通信。这些传感器只需要很少的能量，以接力的方式通过无线电波将数据从一个网络节点传到另一个网络节点，所以它们的通信效率非常高。它的低成本可使每块芯片的价格大约为2美元。ZigBee工作在20～250kb/s的速率，分别提供250kb/s(2.4GHz)、40kb/s(915MHz)和20kb/s(868MHz)的原始数据吞吐率，满足低速率传输数据的应用需求。传输范围一般介于10～100m，在增加发射功率后，亦可增加到1～3km，这指的是相邻节点间的距离。如果通过路由和节点间通信的接力，传输距离将可以更远。ZigBee的响应速度较快，一般从睡眠状态转入工作状态只需15ms，节点连接进入网络只需30ms，进一步节省了电能。ZigBee可采用星状、片状和网状网络结构，由一个主节点管理若干子节点，最多一个主节点可管理254个子节点；同时主节点还可由上一层网络节点管理，最多可组成65 000个节点的大网。ZigBee提供了三级安全模式，包括安全设定、使用访问控制清单(Access Control List，ACL)防止非法获取数据以及采用高级加密标准(AES 128)的对称密码，以灵活确定其安全属性。使用工业科学医疗(ISM)频段，915MHz(美国)、868MHz(欧洲)、2.4GHz(全球)。由于此三个频带物理层并不相同，其各自信道带宽也不同，分别为0.6MHz、2MHz和5MHz，分别有1个、10个和16个信道。这三个频带的扩频和调制方式亦有区别。扩频都使用直接序列扩频(DSSS)，但从比特到码片的变换差别较大。调制方式都用了调相技术，但868MHz和915MHz频段采用的是BPSK，而2.4GHz频段采用的是0QPSK。在发射功率为0dBm的情况下，蓝牙通常能有10m的作用范围。ZigBee在室内通常能达到30～50m的作用距离，在室外空旷地带甚至可以达到400m。所以ZigBee可归为低速率的短距离无线通信技术。

简单地说，ZigBee是一种高可靠的无线数传网络，类似于CDMA和GSM网络。ZigBee数传模块类似于移动网络基站。通信距离从标准的75m到几百米、几千米，并且支持无限扩展。ZigBee是一个由可多到65 000个无线数传模块组成的一个无线数传网络平台，在整个网络范围内，每一个ZigBee网络数传模块之间可以相互通信，每个网络节

点间的距离可以从标准的 75m 无限扩展。

与无线通信的 CDMA 网或 GSM 网不同的是，ZigBee 网络主要是为工业现场自动化控制数据传输而建立。因此，它必须具有简单、使用方便、工作可靠、价格低的特点。无线通信网主要是为语音通信而建立，每个基站价值一般都在百万元人民币以上，而每个 ZigBee 基站却不到 1000 元。每个 ZigBee 网络节点不仅本身可以作为监控对象，例如其所连接的传感器直接进行数据采集和监控，还可以自动中转别的网络节点传过来的数据资料。除此之外，每一个 ZigBee 网络节点还可在自己信号覆盖的范围内，和多个不承担网络信息中转任务的孤立的子节点无线连接。

ZigBee 技术所采用的自组织网原理可以举一个简单的例子来说明，当一队伞兵空降后，每人持有一个 ZigBee 网络模块终端，降落到地面后，只要他们彼此间在网络模块的通信范围内，通过彼此自动寻找，很快就可以形成一个互连互通的 ZigBee 网络。而且，由于人员的移动，彼此间的联络还会发生变化。因此，模块还可以通过重新寻找通信对象，确定彼此间的联络，对原有网络进行刷新，这就形成自组织网。

网状网通信实际上就是多通道通信，在实际工业现场，由于各种原因，往往并不能保证每一个无线通道都能够始终畅通，就像城市的街道一样，可能因为车祸、道路维修等，使得某条道路的交通出现暂时中断，此时由于有多个通道、车辆(相当于控制数据)仍然可以通过其他道路到达目的地，而这一点对工业现场控制而言非常重要。因此，ZigBee 技术采用自组织网来通信，并采用动态路由的方式。动态路由是指网络中数据传输的路径并不是预先设定的，而是传输数据前，通过对网络当时可利用的所有路径进行搜索，分析它们的位置关系以及远近，然后选择其中的一条路径进行数据传输。在网络管理软件中，路径的选择使用的是“梯度法”，即先选择路径最近的一条通道进行传输，如传不通，再使用另外一条稍远一点的通路进行传输，以此类推，直到数据送达目的地为止。在实际工业现场，预先确定的传输路径随时都可能发生变化，或者因各种原因路径被中断了，或者过于繁忙不能进行及时传送。动态路由结合网状拓扑结构，就可以很好地解决这个问题，从而保证数据的可靠传输。

ZigBee 适合的应用领域为传感和控制。市场上的 ZigBee 射频收发“芯片”实际上只是一个符合物理层标准的芯片，它只负责调制解调无线通信信号，所以必须结合单片机才能完成对数据的接收发送和协议的实现。而单芯片也只是把射频部分和单片机部分集成在了一起，不需要额外的一个单片机，它的好处是节约成本、简化设计电路，但这种单芯片也并没有包含 ZigBee 协议在里面。这种情况需要用户根据单片机的结构和寄存器的设置并参照物理层部分的 IEEE 802.15.4 协议和网络层部分的 ZigBee 协议自己去开发所有的软件部分。

除了上述标准外，还需要了解一些常用无线网的概念，例如 WLAN(Wireless Local Area Networks，无线局域网)，家用无线路由器就是无线局域网的一种应用。WLAN 是利用射频技术来取代传统双绞铜线所构成的局域网络，WLAN 的数据传输速率现在已经能够达到 11Mb/s，最高速率可达 54Mb/s。它是对有线联网方式的一种补充和扩展，使互联端口具有一定的可移动性。

通常计算机组网的传输媒介依赖铜缆或光纤来构成有线局域网。但某些场合布线受

限，如工程量大、线路容易损坏、网中的各节点不可移动等。特别对于相离较远的节点，敷设专用通信线路的布线施工难度大、费用高、耗时长、后期维护难等对正在迅速扩大的联网需求形成了严重的瓶颈阻塞。这时架设无线局域网络就成为最佳解决方案。它安装便捷，使用灵活，经济节约，易于扩展。在中国最近几年，WLAN 已经在政府、军队、油田、酒店、医院、商场、工厂和学校等不适合网络布线的场合得到了广泛的应用。

在一个典型的 WLAN 环境中，有一些进行数据发送和接收的设备，称为接入点（Access Point，AP）。通常，一个 AP 能够在几十至上百米的范围内连接多个无线用户。在同时具有有线和无线网络的情况下，AP 可以通过标准的 Ethernet 电缆与传统的有线网络相连，作为无线网络和有线网络的连接点。WLAN 的终端用户可通过无线网卡等访问网络。在距离较远的无线网络环境中，通过室外无线网桥来实现几千米、几十千米的远端局域网连接中心局域网。

无线网络在给人们带来便利生活的同时，它的安全性也不容忽视。例如伪基站的肆虐、无线破解、无线钓鱼、流氓 AP 等数十种基于 WLAN 的无线攻击行为等都触犯了法律的底线。因为任何人在无须抵达实际地点的情况下都可以尝试去入侵无线网络的信号。许多网络提供有线等效加密（WEP）防护系统，但它也仍然容易受到攻击。另一种无线网络防护系统为 WPA（WiFi Protected Access）提供了比 WEP 更安全的无线网络环境，而这道防火墙可以帮助易受入侵的无线网络修补漏洞。

下面就对各种无线网络安全协议进行介绍。

3.3　无线网络安全协议

3.3.1　无线传输层安全协议

无线传输层安全协议（Wireless Transport Layer Security Protocol，WTLS）的作用是保证传输层的安全，用作 WAP（Wireless Access Protocol，无线通信协议）栈的传输层向上层提供安全传输服务的接口。WTLS 是以安全协议 TLS 1.0 标准为基础发展而来的，提供通信双方数据的机密性、完整性和通信双方的鉴权机制。WTLS 在 TLS 的基础上，根据无线环境、长距离、低带宽、自身的适用范围等增加了一些新的特性，如对数据报文的支持、握手协议的优化和动态密钥的刷新等。

无线传输层安全协议版本 18-2-2000 是从 TLS 1.0 协议演化而来的，它的主题框架和握手流程模仿了 TLS 1.0 协议中的内容，但又针对无线应用这一特殊领域的要求做了相应的调整。WTLS 为两个通信应用提供保密、数据完整性和认证服务。它为无线通信协议 WAP 上层提供了一个安全传输服务接口且屏蔽其下层的传输服务接口。另外，WTLS 提供一个管理安全连接（创建、撤销）的接口，主要服务有客户方和服务器的合法性认证，使得通信双方能够确信数据将被送到正确的客户方或服务器上。客户方和服务器都有各自的数字证书。为了达到验证用户的目的，WTLS 要求通信双方交换各自的数字证书以进行身份认证，并可由此可靠地获取对方的公钥。对数据进行加密，WTLS 协议使用的加密技术既有对称加密算法，也有非对称加密算法。具体地说，在安全的通信连

接建立起来之前，双方先使用非对称加密算法加密握手过程中的报文信息和进行双方的数字签名及验证等。安全的通信连接建立起之后，双方使用对称加密算法加密实际的通信内容，以达到提高通信效率的目的。保证数据的完整性，WTLS 协议采用消息摘要函数提供数据的完整性服务，同时也达到节省通信带宽，提高通信效率的目的。WTLS 协议是一个分层协议，被分为四层。

(1) 应用数据协议(Application Protocol)，这是一个从相邻层接收原始数据的协议，它仅在连接状态下运行。连接状态是指 WTLS 记录协议的运行环境，它规定压缩算法、加密算法和 MAC 算法。另外，这些算法的参数也是已知的。MAC 的密码、体加密密钥以及读写双向安全连接的 IV。它将所接收到的数据进行压缩、加/解密、鉴别和数据完整性处理，然后向上层转交或向下层发送。本协议进行的有关处理完全按照在握手协议中通信双方所协商一致的处理流程和算法进行。逻辑上，通常有两个连接状态很重要：当前状态和未决状态。所有的记录都在当前状态下进行处理，未决状态的安全参数由 WTLS 被重新初始化为空状态。最初的当前状态通常都指明不使用加密、压缩或 MAC。

(2) 握手协议(Handshake Protocol)，所有与安全相关的参数都是在握手阶段协商一致的。这些参数包括协议版本号、使用的加密算法、鉴别的信息和由公开密钥技术生成的密钥素材。握手阶段从客户方与服务方进行 Hello 消息应答开始，在两个 Hello 消息中，通信双方商定一致的会话方式。当客户方发送 Client Hello 消息以后，它等待接收 Server Hello Done 消息。服务方如果需要鉴别，可以发一个代表自己的服务器证书给客户方，也可以要求客户方鉴别自己。Server Key Exchange 用于向客户方提供公开密钥。当客户方收到 Server Hello Done 消息后，返回 Client Certificate 消息以让服务方鉴别自己；随后，客户方发送一个 Client Key Exchange 消息，包含由服务方用公开密钥加密过的共享主密钥和其他一些信息，以使双方完成密钥交换；最后，客户方发送一个包含验证前面所有数据的 Finished Message，服务方也同样发送一个 Finished Message 证实交换和计算的信息来回应客户方。

(3) 报警协议(Alert Protocol)，记录协议的警报消息主要有错误、严重、致命三种。警报消息使用当前的安全状态发送。如果警报消息的类型是“致命”，则双方将结束安全连接。同时，其他使用安全会话的连接可以继续，但会话标识必须设成无效，以防用已经终止的安全对话建立新的安全连接。当警报消息的类型为“严重”时，当前的安全连接结束，而其他使用安全会话的连接可以继续，会话标记也可以保存，用于建立新的安全连接。警报信息的传送可以有当前连接状态(如压缩和加密)指定或采用无密码(如不进行压缩与加密)。WTLS 中的出错处理是基于警报消息的，当发现错误时，发现者发送包含出现错误的警报消息，进一步地处理依赖于出现错误的级别和类型。

(4) 改变密码规范协议，此协议应用在加密算法中，用来在无线通信会话的双方间进行加密策略改变的通知，仅使用一种改变密码标准消息。此消息在双方的安全参数协商一致后，在握手阶段由客户方或服务方发送给对方实体，用于通知另一方以后的数据记录将采用新协商的密码规范和密钥。在握手时，经过双方同意安全参数后并在最后校验信息发送前，改变后的密码规范信息才被传送。运行中必须检查改变密码规范信息的发送或接收是否在最后校验信息发送或接收之前进行，这样，已结束和接下来的信息将受新的

密码规范和密钥的保护。当消息到达时,发送消息的一方设定当前的写状态为待决状态,接收消息的一方设定当前的读状态为待决状态。

WTLS的保密性依靠加密通信通道来实现,所使用的加密方法和计算共享密钥所需的值在握手时进行交换。首先,客户端和服务器交换Hello消息,此后,客户端和服务器交换预主密钥(Pre-master Secret),这个值用来计算主密钥(Master Secret),计算所使用的加密算法在服务器的Hello消息中进行选择。在这条消息中,服务器通知客户端已经选择了一个密码组,客户端向服务器提供一个密码组列表。如果服务器未发现合适的密码组,则握手失败,连接关闭。当前常用的大批量加密算法有:支持40、56和128位密钥的RC5,支持40和56位密钥的DES,支持40、56和128位密钥的3DES和IDEA。所有的算法都是分组加密算法,加密密钥在密钥分组的基础上进行操作,密钥分组根据协商的密钥刷新频率在一段时间后重新运算。

为了保证安全的联系通道,加密密钥或计算密钥的初始值必须以安全方式进行交换。WTLS的密钥交换机制提供了一种匿名交换密钥的方法。在密钥交换过程中,服务器发送包含服务器公钥的服务器密钥交换消息。密钥交换算法可能是RSA、Diffie-Hellman或Elliptic Curve Diffie-Hellman。在RSA和匿名RSA中,客户端用服务器的公钥加密预主密钥,并在客户密钥交换消息中将其返回给服务器。在基于Diffie-Hellman的算法中,客户端和服务器在一个私钥和相应的公钥基础上计算预主密钥。

如果客户端列出了它所支持的用密码写的密钥交换方法,服务器可以选择是使用基于客户请求的方法,还是定义另一种方法。如果客户端并未提出任何方法,则服务器必须指明。

WTLS的身份鉴别依靠证书实现。身份鉴别可以在客户端和服务器之间进行,也可以在服务器允许的情况下,只由客户端鉴别服务器,服务器还可以要求客户端向服务器证明自己。在WTLS规范中,身份鉴别是可选的。当前所支持的证书类型包括X.509v3、X9.68和WTLS证书。在客户端和服务器之间交换Hello消息之后,鉴别过程随即开始。当使用鉴别时,服务器发送服务证书消息给客户端。根据WTLS规范,为了优化流量和客户处理,服务器一次只发送一个证书。服务器证书由CA(Certificate Authority,认证中心)公司独立分发的公钥进行鉴别。服务器也可以发送证书请求消息给客户端以鉴别。此时,客户端发送客户证书消息返回给服务器,客户端证书遵循与服务证书相同的结构。

数据完整性通过使用消息验证码(Message Authentication Code,MAC)算法而得到保证,MAC算法同时也被认为是加密算法。客户端发送一列所支持的MAC算法,服务器在返回的Hello消息中标出所选的算法。WTLS支持通用的MAC算法,MAC在压缩的WTLS数据上产生。

在安全协商后,会话通信双方将拥有同样的安全状态。当前状态通过安全参数产生,并持续更新。

3.3.2 有线等效协议

有线等效协议(Wired Equivalent Privacy,WEP)是对在两台设备间无线传输的数据

进行加密的方式，用于防止非法用户窃听或侵入无线网络。

WEP 使用 RC4(Rivest Cipher)算法进行加密，并使用 CRC32(循环冗余校验)校验来保证数据的正确性。

1. WEP 的加密过程

(1) WEP 工作在数据链路的介质接入控制层(Media Access Control，MAC)，从上层获得传输的明文数据后，首先使用 CRC 进行计算，利用 CRC 算法生成的 32 位 ICV (Integrity Check Value，完整性检查值)和明文连接在一起作为将要被加密的数据。

(2) WEP 利用 RC4(一种流加密算法 Rivest Cipher 4 的缩写)产生伪随机序列流，用伪随机序列流和(1)中处理过后的明文进行异或计算，产生密文。RC4 密钥分成两部分：一部分是 24 位的初始向量(Initial Value，IV)，一部分是用户密钥。由于相同的密钥生成的伪随机序列流是一样的，所以使用不同的初始向量来确保生成的伪随机序列流是不相同的，从而使其用于加密其他的数据帧。

(3) 密文和初始化向量一起传输给接收方，WEP 的加密过程如图 3-3 所示。

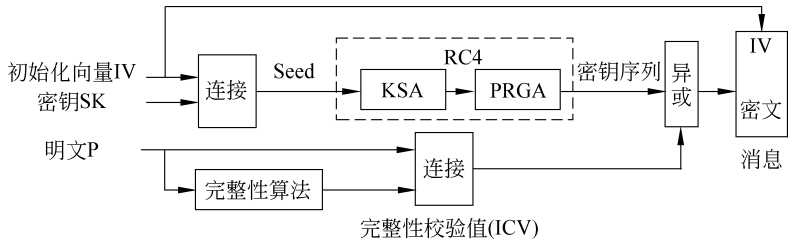


图 3-3 WEP 的加密过程

2. WEP 的解密过程

WEP 的解密过程和加密过程刚好相反，WEP 的解密过程如图 3-4 所示。

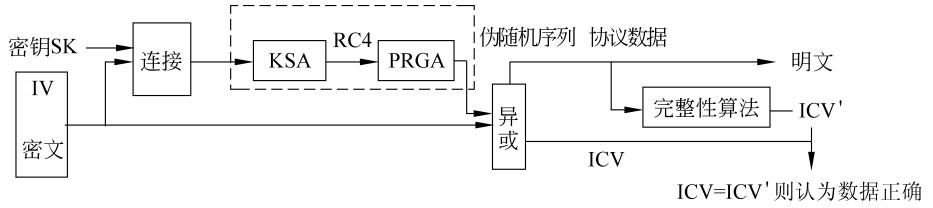


图 3-4 WEP 的解密过程

(1) 进行帧的完整性校验，从中取出 IV 和使用的密钥编号，将 IV 和对应的密钥组合成解密密钥流。

(2) 通过 RC4 算法计算伪随机序列流，进行异或计算，计算出载荷以及 ICV 内容。

(3) 对解密出的内容使用 WEP 加密的(1)步方法生成 ICV'，比较 ICV'和 ICV，若相同则认为数据正确。

3. WEP 缺陷

1）密钥重复

WEP 加密基于 RC4 的序列加密算法，加密的原理是使用密钥生成伪随机密钥流与明文数据逐位进行异或来生成密文。如果攻击者获得相同的密钥流加密后的两段密文，将两段密文进行异或，生成的也就是明文的两段异或，因此能消去密钥的影响。通过统计分析以及对密文中冗余的信息进行分析，就可以推出明文，因此重复使用相同的密钥是不安全的。

2）WEP 缺乏密钥管理

在 WEP 机制中，对应密钥的生成和分发没有任何规定，对于密钥的使用也没有明确规定，密钥使用情况比较混乱。

数据加密主要使用两种密钥：Default Key 和 Mapping Key。数据加密密钥一般使用默认密钥中的 Key ID 为 0 的 Default Key，也就是所有的用户使用相同的密钥。而且这种密钥一般使用人工装载，更新也少，增加了用户站点之间密钥重用的概率。

3）IV 重用问题

IV 重用问题，即不同的数据帧加密时使用的 IV 值相同，使用相同的数据帧加密密钥是不安全的。数据帧加密密钥是基密钥和 IV 值串联而成的，一般用户使用的基密钥是 Key ID 为 0 的 Default Key，因此不同的数据帧加密使用相同的 IV 值是不安全的。除此之外，IV 值是明文传输的，攻击者可以通过观察来获得使用相同数据帧加密密钥的数据帧获得密钥，所以要避免使用相同的 IV 值，这不仅要同一个站点避免使用重复的 IV，也要避免其他用户站点使用曾经使用过的 IV。但 IV 的可选范围值只有 224 个，理论上来说只要传输 224 个数据帧后就会发生一次 IV 重用，所以 WEP 是非常不安全的。

WEP 是针对无线网络而开发的，1999 年 9 月获准成为 WiFi 安全标准。WEP 理论上应当提供与有线网络同等的安全等级，但是其中却存在很多众所周知的问题，而且这些问题同样也易于破解且配置困难。尽管已经尽一切努力来提升 WEP 系统，它仍然是高度脆弱的解决方案。依赖于此协议的系统在安全升级无法实现的时候应当予以升级或替换。WEP 于 2004 年正式被 WiFi 联盟予以放弃。

3.3.3　WiFi 保护设置

WiFi 保护设置（WiFi Protected Setup，WPS）是由 WiFi 联盟推出的全新 WiFi 安全防护设定标准。该标准推出的主要原因是为了解决长久以来无线网络加密认证设定的步骤过于繁杂的缺点，使用者可能会因为设定过程太过麻烦而放弃进行加密安全设定，从而引发安全问题。

1. WPS 工作原理

WPS 加密就是使客户端连接 WiFi 时，连接过程变得非常简单。用户只需按一下无线路由器上的 WPS 键，或者输入一个 PIN 码，就能快速地完成无线网络连接，并获得 WPA2（WiFi Protected Access 2，无线保护接入）级加密的无线网络。WPS 支持两种模