<<认知无线电技术与应用>>

图书基本信息

书名：<<认知无线电技术与应用>>

13位ISBN编号：9787302264200

10位ISBN编号：7302264201

出版时间：2012-1

出版时间：清华大学出版社

作者：党建武，李翠然，谢健骊 编著

页数：227

字数：371000

<<认知无线电技术与应用>>

内容概要

《认知无线电技术与应用》是一本专门讲授认知无线电技术及其应用的技术书籍。

《认知无线电技术与应用》共分6章，包括认知无线电技术概述、频谱感知策略、频谱管理和频谱移动性管理、频谱共享等认知无线电关键技术，以及认知无线电网络关键技术（路由协议、传输层协议、跨层设计和网络安全技术），同时还对认知无线电技术的典型应用实例进行了分析。

《认知无线电技术与应用》在选材上，参考了大量最新的相关文献，在内容上充分反映了认知无线电技术的最新研究进展。
本书适合作为高等院校工科通信工程、计算机工程、电子工程和其他相近专业高年级本科生和研究生教材，也可作为相关专业的教师和科研、工程人员的参考书。

<<认知无线电技术与应用>>

书籍目录

章节摘录

当前对网络的攻击主要分为两类：主动攻击和被动攻击。
主动攻击是指攻击者通过有选择地修改、删除、延迟、乱序、复制、插人数据流或数据流的一部分以达到其非法目的。
主动攻击有中断、篡改、伪造3种形式。
中断是指阻断发送方到接收方的信息流，使接收方根本不知道有人给他发过信息，这是通过破坏信息的可用性来实现的；篡改是指攻击者修改、破坏由发送方到接收方的信息流，使接收方接收的是错误的信息，这是通过破坏信息的完整性来实现的；伪造是指攻击者假冒发送方给接收方发送信息，使接收方误以为是信任的一方通信从而接收信息，这是通过破坏信息的真实性来实现的。
被动攻击主要是攻击者监听网络上传递的信息流，从而获得信息的内容或者进行流量分析得到信息流的长度、传输频率等数据，这是通过破坏信息的保密性来实现的。
网络安全是一个系统工程，认证和加密、防火墙和入侵检测系统是网络安全的3道防线。
①认证就是验证实体的真实性和信息交换的合法性。
认证机制是以密码术为基础的，对实体的某些参数进行有效性验证。
认证技术包括：身份认证、报文认证、访问授权和数字签名。
身份认证是通过认证进行用户身份的识别，通常确认用户的身份是在允许用户访问网络资源之前，一般采用用户名和口令等方法；报文认证主要是通信双方对通信的信息内容进行验证，以保证报文是由确认的发送方产生的，报文内容在传送过程中没有被修改，报文传送到了欲达的接收方；访问授权是指用户的身份通过认证后，确定该用户对信息资源的访问权限；数字签名主要是防止冒名顶替，保证在报文传输过程中，接收方能够对公正的第三方（仲裁方）证明其接收的报文的真实性和发送源的真实性而采用的一种安全措施。
②数据加密技术作为网络安全技术，是提高网络系统数据的保密性、防止秘密数据被外部破译所采取的主要技术手段。
③防火墙是在内部网和外部网之间实施安全防范的系统，用于加强网络间的访问控制，防止外部用户非法使用内部网的资源，保护内部网的设备不被破坏，防止内部网络的敏感数据被盗取。
④入侵检测系统是一种主动的网络安全防护措施，是防火墙的合理补充，它从系统内部和各种网络资源中主动采集信息，从中分析可能的网络入侵或攻击，扩展了系统管理员的安全管理能力（包括安全审计、监视、进攻识别和响应），提高了信息安全基础结构的完整性。
无线网络摆脱了有线的束缚，给人们的生活带来了很大的方便，但同时也带来了一些固有的缺陷，其中比较突出的是较差的安全性。
无线网络安全的脆弱性源于无线传输媒介的开放性、终端的移动性以及网络拓扑结构的动态变化。
无线网络的开放性使其更容易受到恶意攻击、非法信息截取；移动性使得安全管理难度加大，在跨区域漫游时，移动节点可能被窃听、破坏和劫持；网络拓扑的动态变化，使效率较高的集中式安全管理机制难于实现。
当前对无线网络的主要攻击可以归纳为以下几种。
①网络信息容易遭到窃听。
无线网络的电磁辐射难以精确地控制在某个范围内，攻击者只需架设一副天线即可窃取数据。
②网络中窃听行为难于检测。
对于窃听这种被动攻击行为，在无线网络中检测的难度远大于有线网络。
因为在有线网络中窃听数据必须靠近传输线，而在无线网络中攻击者可在远处隐蔽地窃听数据。
……

<<认知无线电技术与应用>>

版权说明