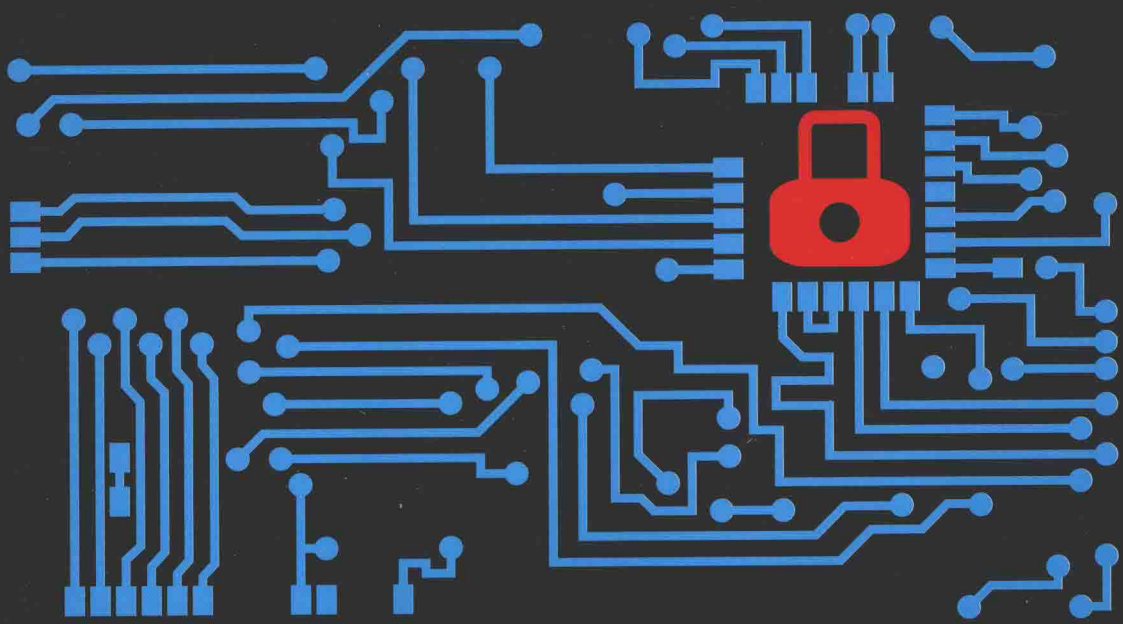
世界著名计算机教材精选

无线移动网络安全（第2版）

Man Young Rhee 著

葛秀慧 等译



WIRELESS MOBILE INTERNET SECURITY

Second Edition

清华大学出版社

WILEY

世界著名计算机教材精选

无线移动网络安全

（第2版）

Man Young Rhee 著
葛秀慧 等译

清华大学出版社
北 京

Man Young Rhee
Wireless Mobile Internet Security, Second Edition
EISBN: 978-1-118-49653-4

图书在版编目(CIP)数据

无线移动网络安全: 第 2 版/(韩)李迈勇著;葛秀慧等译. —北京: 清华大学出版社,2016
书名原文: Wireless Mobile Internet Security, 2nd Edition
(世界著名计算机教材精选)
ISBN 978-7-302-43365-1

Ⅰ. ①无… Ⅱ. ①李… ②葛… Ⅲ. ①无线网—移动网—安全技术—教材 Ⅳ. ①TN929.5

中国版本图书馆 CIP 数据核字(2016)第 074791 号

责任编辑: 龙启铭
封面设计: 傅瑞学
责任校对: 梁 毅
责任印制: 何 芊

出版发行: 清华大学出版社
网 址: http://www.tup.com.cn, http://www.wqbook.com
地 址: 北京清华大学学研大厦 A 座 **邮 编**: 100084
社 总 机: 010-62770175 **邮 购**: 010-62786544
投稿与读者服务: 010-62776969, c-service@tup.tsinghua.edu.cn
质量反馈: 010-62772015, zhiliang@tup.tsinghua.edu.cn
课件下载: http://www.tup.com.cn,010-62795954
印 装 者: 北京密云胶印厂
经 销: 全国新华书店
开 本: 185mm×260mm **印 张**: 24.75 **字 数**: 610 千字
版 次: 2016 年 9 月第 1 版 **印 次**: 2016 年 9 月第1 次印刷
印 数: 1～2000
定 价: 59.00 元

产品编号: 058684-01

目　录

第 1 章　互连网络与分层模型

现在，Internet 是广泛应用的信息基础设施，但本质上，Internet 是一种不安全的发送信息的信道。当从一个 Web 站点向另一个站点发送消息（或数据包）时，在消息中的数据到达目的地之前，要路由通过多个中间站点。Internet 能兼容各种异构平台，从而使得使用不同计算机与操作系统的人们可以互相通信。Internet 的历史比较复杂，主要体现在技术、组织和社区等方方面面的复杂性。随着电子商务、信息获取与社区交互的发展，Internet 也迈上了一个新的台阶。

早期的 ARPANET 研究人员完成了包交换技术的最初示范。在 20 世纪 70 年代后期，Internet 的发展被认可，随后，随着对协调机制需求的增长，感兴趣的研究社区规模也在扩大。美国**国防高级研究计划局**（Defense Advanced Research Projects Agency，DARPA）成立了**国际合作委员会**（International Cooperation Board，ICB），以配合一些专注于数据包卫星研究的欧洲国家的活动，而 **Internet 配置控制委员会**（Internet Configuration Control Board，ICCB）协助 DARPA 管理 Internet 活动。1983 年，DARPA 意识到，Internet 社区的持续增长需要重组协调机制。ICCB 被解散，取而代之的是，根据任务组的主席职位，成立了 **Internet 活动委员会**（Internet Activities Board，IAB）。IAB 使 **Internet 工程任务组**（Internet Engineering Task Force，IETF）有了转机，成为 IAB 成员。到 1985 年，出现了越来越多更实用的 Internet 工程。这种增长导致工作组形式的 IETF 子结构的诞生。DARPA 不再是 Internet 资金的主要来源。从那时起，DARPA 在 Internet 活动中的作用越来越小。IAB 意识到 IETF 越来越重要，重组并确认 **Internet 工程指导小组**（Internet Engineering Steering Group，IESG）作为主要标准的审查机构。除 IETF 之外，IAB 重组成立了 **Internet 研究任务组**（Internet Research Task Force，IRTF）。

最初，Internet 主要用于科学研究，但 20 世纪 80 年代初，Internet 的发展已超出了最初的研究初衷，出现了大量的用户群体，且增加了商业活动。这种增长使商业部门越来越关注相关的标准进程。随着关注越来越多，事情得到进展，最终于 1991 年成立了 **Internet 协会**（Internet Society，IS）。1992 年，重组了 **Internet 活动委员会**（Internet Activities Board，IAB），更名为 **Internet 架构委员会**（Internet Architecture Board，IAB），在 Internet 协会主持下运作。新的 IAB、IESG 与 IETF 间的相互支持关系使之能更好地执行标准的批准、制定服务及一些措施，这些都有利于 IETF 工作的开展。

1.1　互连技术

数据信号通过一种或多种传输介质（双绞线、同轴线和光纤等），从一个设备传输到另一个设备。要传输的消息是网络通信的基本单元。一个消息可能由一个或多个单元、帧或包组成，而这些都是网络通信的基本单位。网络互连技术包括**局域网**（Local Area Networks，LAN）到**广域网**（Wide Area Networks，WAN）。局域网是指有限地理区域内（如单个建筑、

公寓或校园)的网络;广域网是指跨越较大地理区域(如一个国家、一个洲甚至是全世界)的网络。

1.1.1 局域网(LAN)

LAN是一种通信系统,它允许有限地理区域内(如单独的办公楼、仓库或校园)的多个独立设备之间进行直接的相互通信。LAN有三种标准化的体系结构:以太网(Ethernet)、令牌环(token ring)和光纤分布式数据接口(Fiber Distributed Data Interface,FDDI)。

以太网

以太网是一种LAN的标准,最初由Xerox公司开发,后来由DEC、Intel公司和Xerox公司联合开发并扩展。以太网使用的访问机制是**带冲突检测的载波侦听多路访问**(Carrier Sense Multiple Access with Collision Detection,CSMA/CD)。在CSMA / CD中,在一个基站传输数据之前,它必须侦听介质,以确定是否有其他基站正在使用该介质。如果没有其他基站在传输数据,则这个基站可以发送它自己的数据。如果两个或多个基站同时发送数据,就会产生冲突。因此,所有基站都必须不断地监听介质,检测可能产生的任何冲突。如果发生冲突,所有基站会忽略所接收的数据。发送基站需要等待一段时间后,再发送数据。为了减少产生第二次冲突的可能性,发送基站会分别产生随机数,以确定该基站需要等待多久才能重新发送数据。

令牌环

令牌环是一种LAN标准,最初由IBM公司开发,它使用逻辑环形拓扑结构。CSMA/CDP所用的访问方法可能会产生冲突。因为,基站在捕获完美的传输链路之前,可能尝试多次发送数据。如果数据流量很大,这种冗余会产生不确定长度的延迟。因此,CSMA/CD没有办法预测冲突发生,也没有办法预测由多个基站试图同时捕获链路所产生的延迟。而令牌环通过让基站轮流发送数据来解决CSMA / CD存在的这种不确定性问题。

作为一种访问方法,令牌按顺序从一个基站传递到另一个基站,直到它遇到需要发送数据的基站为止。要发送数据的基站都必须等待令牌。当一个基站捕获令牌后,就能发送自己的数据帧。这个数据帧绕着环继续前行,每个基站都重新生成该数据帧。中间的每个基站都检查目的地地址,如果发现这个数据帧是对另一个基站寻址,就将它中继到其相邻的基站。预定接收的基站识别自身的地址,复制该消息、进行差错校验,并修改数据帧中最后一个字节的四位,表示该地址已被确认,且复制了数据帧。然后,完整的数据包继续在环中前行,直到返回发送它的基站。

光纤分布式数据接口

光纤分布式数据接口(FDDI)是一种由**美国国家标准协会**(American National Standards Institute,ANSI)和ITU-T提出的标准化LAN协议。它支持100 Mbps的数据速率,并提供了替代以太网和令牌环的高速网络。当设计FDDI时,需要使用光纤电缆以支持100 Mbps的数据速率。

FDDI的访问方法也称为**令牌传递**(token passing)。在令牌环网络中,基站每次捕获令牌时,只能发送一个帧。在FDDI中,令牌传递机制略有不同,其访问是定时的。每个基站

维护一个计时器，来显示令牌必须离开基站的时间。如果基站接收令牌的时间早于预定时间，则它可以持有令牌并发送数据，直到预定的离开时间为止。另一方面，如果基站在预定时间或更晚的时间接收到令牌，则它必须将令牌传递给下一个基站，并等待令牌的下一轮到来。

FDDI 的实现是一个双环。在大多数情况下，数据传输都使用主环。主环发生故障的情况下才使用备用环。当主环出现问题时，将激活备用环来完成数据传输和维护服务。

1.1.2　广域网(WAN)

WAN 提供跨越广阔地理区域的数据、语音、图像与视频信息的远距离传输，其跨越的地理区域可能是一个国家、一个洲乃至全世界。相比之下，局域网依靠自己的硬件进行传输，而广域网则利用公共的、租赁的或专用通信设备进行传输，且往往混合使用这些通信设备。

PPP

点对点协议(Point-to-Point Protocol，PPP)设计用于处理使用异步调制解调器链路或高速同步租赁线路的数据传输。PPP 帧使用如下的格式：

- 标志字段(Flag field)：每个帧以一个字节的标志作为开始，其值是 7E(01111110)。该标志用于在位级上同步发送方与接收方。
- 地址字段(Address field)：该字段的值为 FF(1111 1111)。
- 控制字段(Control field)：该字段的值为 03(0000 0011)。
- 协议字段(Protocol field)：这是两个字节的字段，其值为 0021(0000 0000 0010 0001)，表示**传输控制协议/网际协议**(Transmission Control Protocol/Internet Protocol，TCP/IP)。
- 数据字段(Data field)：数据字段多达 1500 个字节。
- CRC：这是两个字节的**循环冗余校验**(Cyclic Redundancy Check，CRC)。CRC 在物理层实现，但用于数据链路层。在数据单元末尾附加冗余位(CRC)序列，使所得的数据单元能被预定的二进制数整除。在其目的地，输入数据单元除以相同的数。如果没有余数，就接收这个数据单元。如果有余数存在，那么这个数据单元在传输中已被破坏，因此必须拒绝接收这个数据单元。

X.25

X.25 是广泛用于 WAN 的包交换协议。在 1976 年，ITU-T 开发了 X.25。X.25 是数据终端设备与数据电路终端设备之间的接口，用于数据包模式下公共数据网络的终端操作。

X.25 定义了数据包模式终端如何连接到数据包网络以进行数据交换。它描述了建立连接、数据交换、确认、流控制和数据控制所需的过程。

帧中继

帧中继是一种 WAN 协议，其设计目标是弥补 X.25 的缺陷。X.25 提供了扩展的差错校验和流控制。在数据包路由经过的每个基站，都要对数据包进行准确性校验。每个基站都保留原始帧的一个副本，直到它收到下一个基站的确认，证实该帧已完好无缺地到达为

止。这种基站到基站的校验是在**开放系统互连**(Open Systems Interconnect,OSI)模型的数据链路层实现,但 X.25 只在网络层对发送方与接收方进行差错校验。发送方一直保留源数据包的副本,直到它接收到来自最终目的地的确认为止。X.25 网络中的大部分流量都专用于差错校验,以确保服务的可靠性。帧中继在数据链路层不提供差错校验或进行确认。相反,所有差错校验都留给使用帧中继服务的网络层和传输层协议。帧中继只工作于物理层和数据链路层。

异步传输模式

异步传输模式(Asynchronous Transfer Mode,ATM)是一种具有创新性的重构数据通信基础设施的想法。它旨在支持数据、语音和视频能在高数据率传输媒介(光纤电缆)上传输。ATM 是一种信元传输协议。信元是一个长度为 53 字节的小数据单元,由 5 个字节的报首部和 48 个字节的有效载荷组成。报首部包含一个**虚拟路径识别符**(Virtual Path Identifier,VPI)和**虚拟信道识别符**(Virtual Channel Identifier,VCI)。根据这两个标识符,路由器将信元路由到网络的最终目的地。

ATM 网络是面向连接的信元交换网络。这意味着,数据单元既不是包交换网络的数据包,也不是帧中继的帧,而是信元。但是,ATM 与 X.25 和帧中继一样,也是一种面向连接的网络,也就是说,在两个系统进行通信之前,必须先建立连接。为了启动连接,系统使用 20 字节的地址。在建立连接之后,VPI/VCI 的组合可以将信元从其源端引导到最终目的地。

1.2 互连设备

互连设备用于将各个网段连接起来或将网络连接成互连网络。这些设备分为五类:交换机、中继器、网桥、路由器和网关。除了交换机之外,其余设备都与 OSI 模型中不同层的协议进行交互。

中继器转发所有电信号且只工作于物理层。网桥存储和转发完整的数据包,并影响着单个局域网的流量控制。网桥工作于物理层和数据链路层。路由器为两个独立局域网之间提供链路,它工作于物理层、数据链路层和网络层。最后,网关为不兼容的局域网或应用之间提供转换服务,它工作于所有层。

互连设备与 OSI 模型不同层的协议进行交互的示意图如图 1.1 所示。

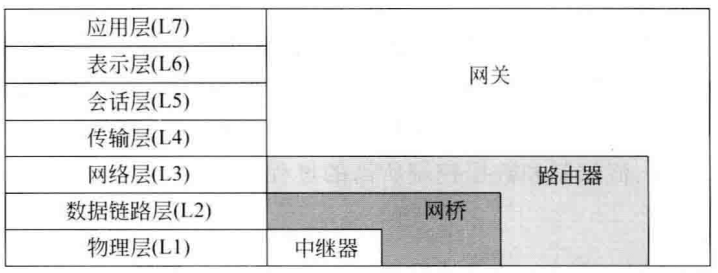


图 1.1 互连设备

1.2.1　交换机

交换网络由一系列互连的交换机组成。交换机是一种硬件/软件设备，能够在两个或多个与交换机相连的设备之间建立临时连接，但不是建立交换机之间的连接。交换机制一般分为三种方法：电路交换、数据包交换和消息交换。

- 电路交换：电路交换是在两个设备（如电话或计算机）之间建立直接的物理连接。一旦两个系统之间建立了连接，电路交换就在两个终端用户之间建立了专用路径。只要终端用户需要，就可以一直使用这条路径。
- 数据包交换：数据包交换为数据传输提供了一种更为合理的解决方案。在数据包交换网络中，数据以离散的、长度可变的分组（称为数据包）为单元进行传输。每个数据包不仅包含数据，还包含含有控制信息的首部。数据包被发送到网络，从一个节点传输到另一个节点。在每个节点，在根据数据包的首部信息对数据包进行发送之前，都会对数据包进行临时存储。

  在数据包交换的数据报方法中，对每个数据包都进行单独处理，就像它单独存在一样。在数据包交换的虚电路方法中，如果在会话开始时，发送方与接收方只选择了一条线路，则所有数据包都沿着这条线路逐个传输。虽然电路交换和虚电路方法看似相同，但两者之间存在着本质区别。在电路交换中，两个终端用户之间的路径只有一个信道。在虚电路中，线路并非是两个用户专用。线路被分为多个信道，每个信道只是使用了线路中的一个信道。
- 消息交换：消息交换被称为**存储与转发方法**（store and forwarding method）。在这种方法中，计算机（或节点）接收消息时，一直会存储消息，在合适的线路空闲之后，再把消息发送出去。现在，这种方法已被淘汰。

1.2.2　中继器

中继器是一种电子设备，它只工作于 OSI 模型的物理层。中继器将来自一个网段的传输信号放大，再继续将信号转发到另一个网段。因此，中继器可以扩展网络的物理距离。由于噪声及数据信号的衰减，携带信息的信号在网络中只能传输有限的距离。中继器就是在信号失真之前，接收信号，重新生成信号的原始的比特模式，并在链路中对再生的信号副本进行转发。

1.2.3　网桥

网桥工作在 OSI 模型的物理层和数据链路层。单个网桥就能将不同类型的网络连接在一起，并提升网络间的互连性。网桥将大型网络划分成较小的网段。与中继器不同，网桥包含逻辑，从而使每个网段都保持独立的流量。网桥有足够的智能，能将数据帧转发给预定的接收者，还能过滤流量。事实上，这种过滤操作使网桥功能增加，能控制拥塞、隔离有问题的链路，并且通过这种对流量的分割，提升网络的安全性。

网桥可以访问与之相连的所有基站的物理地址。当一个数据帧到达网桥时，网桥不仅再生信号，还会检查目的地址，并将新副本转发到该地址所属的网段。当网桥遇到数据包

时,它读取数据帧所包含的地址,并把该地址与和它相连的两个网段中所有基站表进行比较。当找到匹配的基站,它会找到基站所属的网段,并只将数据包转发到这个网段。

1.2.4 路由器

路由器工作在OSI模型的物理层、数据链路层和网络层。路由器所连接的各种网络形成了Internet。数据报从源端到目的地的过程中,在到达附属于目的网络的路由器之前,会经过多个路由器。路由器决定数据包所经由的路径。路由器在多个互连的网络中转发数据包,特别是IP路由器在与之相连的网络中转发IP数据报的情况。路由器使用数据报的目的地址来选择转发数据报的下一跳。数据包要从一个网络的基站发送到相邻网络的另一个基站,先要经过两个网络共有的路由器,该路由器会将数据包交换到目的网络。事实上,构造Internet的最简单方法就是用路由器连接两个或多个网络。路由器能连接多种不同类型的物理网络:以太网、令牌环、点对点链路和FDDI等。

- 路由模块接收来自处理模块的IP数据包。如果数据包将被转发,则它必须将IP数据包传递给路由模块。它先在要转发的数据包中找到下一个基站的IP地址和接口号。然后,将含有信息的数据包发送给拆分模块。拆分模块参照MTU表,找到特定端口号的**最大传输单元**(Maximum Transfer Unit,MTU)。
- 路由模块使用路由表来确定数据包的下一跳地址。每个路由器都维护一个路由表,该表的每一项都对应一个目的地网络。每个表项包括目的地网络的IP地址、到达目的地的最短距离(以跳数计)和数据包要到达最终目的地必须经过的下一个路由器(下一跳)。跳数是数据包从源端到最终目的地所经过的网络数。当路由器准备转发数据包时,它必须有路由表作为参考。路由表应当指定数据包的最佳路径。路由表可以是静态的,也可以是动态的。静态路由表是不经常改变的。当Internet的某处发生变化时,动态路由表会自动更新。现在,Internet所需的是动态路由表。
- 路由开销:路由开销是通过网络的成本。特定路由器的总开销等于包含了该路由器的所有网络的开销总和。路由器选择最小开销(最小值)的路径。分配给每个网络的路由开销取决于协议的类型。**路由信息协议**(Routing Information Protocol,RIP)将每个网络看作一跳。因此,如果数据包经过10个网络到达目的地,则总成本为10跳。**开放式最短路径优先**(Open Shortest Path First,OSPF)协议允许管理员根据网络所需服务类型,为所经过的网络分配成本。这样,通过网络的路由有不同的成本。OSPF允许路由器根据所需服务的类型拥有几种路由表。**边界网关协议**(Border Gateway Protocol,BGP)定义的路由开销完全不同。在BGP中,策略标准由管理员设置。这个策略定义了应选择的路径。

1.2.5 网关

网关工作于OSI模型的所有层中。传统上,将Internet上所有的路由设备都称为**网关**(gateway)。网关是一个协议转换器,它连接两个或多个异构系统,并负责这些系统之间的转换。因此,网关是指设备间执行协议转换的设备。网关接收一个协议格式的数据包,并在转发数据包之前,将其转换为另一个协议格式的数据包。网关知道连接到路由器的每个网