接入通信所需的资源）。考虑了这些问题后，我们能够指出**安全通信**（secure communication）具有下列所需要的特性。

- 机密性（confidentiality）。仅有发送方和希望的接收方能够理解传输报文的内容。因为窃听者可以截获报文，这必须要求报文在一定程度上进行**加密**（encrypted），使截取的报文无法被截获者所理解。机密性的这个方面大概就是通常意义上对于术语安全通信的理解。我们将在8.2节中学习数据加密和解密的密码学技术。
- 报文完整性（message integrity）。Alice和Bob希望确保其通信的内容在传输过程中未被改变——或者恶意篡改或者意外改动。我们在可靠传输和数据链路协议中遇到的检验和技术在扩展后能够用于提供这种报文完整性，我们将在8.3节中研究该主题。
- 端点鉴别（end-point authentication）。发送方和接收方都应该能证实通信过程所涉及的另一方，以确信通信的另一方确实具有他们所声称的身份。人类的面对面通信可以通过视觉识别轻易地解决这个问题。当通信实体在不能看到对方的媒体上交换报文时，鉴别就不是那么简单了。当某用户要访问一个邮箱，邮件服务器如何证实该用户就是他或她所声称的那个人呢？我们将在8.4节中学习端点鉴别技术。
- 运行安全性（operational security）。几乎所有的机构（公司、大学等）今天都有了与公共因特网相连接的网络。这些网络都因此潜在地能够被危及安全。攻击者能够试图在网络主机中安放蠕虫，获取公司秘密，勘察内部网络配置并发起DoS攻击。我们将在8.9节中看到诸如防火墙和入侵检测系统等运行设备正被用于反制对机构网络的攻击。防火墙位于机构网络和公共网络之间，控制接入和来自网络的分组。入侵检测系统执行“深度分组检查”任务，向网络管理员发出有关可疑活动的警告。

明确了我们所指的网络安全的具体含义后，我们接下来考虑入侵者可能要访问的到底是哪些信息，以及入侵者可能采取哪些行动。图8-1阐述了一种情况。Alice（发送方）想要发送数据给Bob（接收方）。为了安全地交换数据，即在满足机密性、端点鉴别和报文完整性要求的情况下，Alice和Bob将交换控制报文和数据报文（以非常类似于TCP发送方和接收方双方交换控制报文和数据报文的方式进行）。通常将这些报文全部或部分加密。如在1.6节所讨论的那样，入侵者能够潜在地执行下列行为：

- 窃听——监听并记录信道上传输的控制报文和数据报文。
- 修改、插入或删除报文或报文内容。

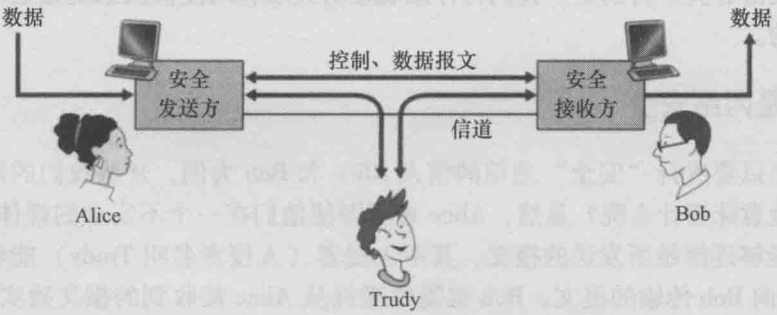


图8-1 发送方、接收方和入侵者（Alice、Bob和Trudy）