通常必须相互鉴别。此处，鉴别应当在报文和数据交换的基础上，作为某**鉴别协议**（authentication protocol）的一部分独立完成。鉴别协议通常在两个通信实体运行其他协议（例如，可靠数据传输协议、路由选择信息交换协议或电子邮件协议）之前运行。鉴别协议首先建立相互满意的各方的标识；仅当鉴别完成之后，各方才继续下面的工作。

同第3章中我们阐释可靠数据传输协议（rdt）的情况类似，我们发现阐释各种版本的鉴别协议——我们将称为 ap（authentication protocol）——是有启发的，并随着我们学习的深入指出各个版本的漏洞。（如果你喜欢这种逐步式的设计演化，你也许喜欢看[Bryant 1988]，这本书虚构了开放网络鉴别系统的设计者间的故事，以及他们对许多相关奇妙问题的发现。）

我们假设 Alice 要向 Bob 鉴别她自己的身份。

8.4.1 鉴别协议 ap1.0

也许我们能够想象出的最简单的鉴别协议就是：Alice 直接发送一个报文给 Bob，说她就是 Alice。这个协议如图 8-15 所示。这个协议的缺陷是明显的，即 Bob 无法判断发送报文“我是 Alice”的人确实就是 Alice。例如，Trudy（入侵者）也可以发送这样的报文。

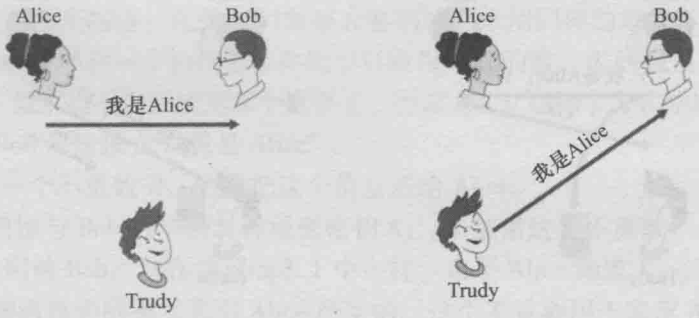

图 8-15 协议 ap1.0 和一种失败的情况

8.4.2 鉴别协议 ap2.0

如果 Alice 有一个总是用于通信的周知网络地址（如一个 IP 地址），则 Bob 能够试图通过验证携带鉴别报文的 IP 数据报的源地址是否与 Alice 的周知 IP 地址相匹配来进行鉴别。在这种情况下，Alice 就可被鉴别了。这可能阻止对网络一无所知的人假冒 Alice，但是它却不能阻止决定学习本书的学生或许多其他人！

根据我们学习的网络层和数据链路层的知识，我们就会知道做下列事情并不困难（例如，如果一个人能够访问操作系统代码并能构建自己的操作系统内核——比如 Linux 和许多其他免费可用的操作系统）：生成一个 IP 数据报，并在 IP 数据报中填入我们希望的任意源地址（比如 Alice 的周知 IP 地址），再通过链路层协议把生成的数据报发送到第一跳路由器。此后，具有不正确源地址的数据报就会忠实地向 Bob 转发。这种方法显示在图 8-16 中，它是 IP 哄骗的一种形式。如果 Trudy 的第一跳路由器被设置为只转发包含 Trudy 的 IP 源地址的数据报，就可以避免 IP 哄骗［RFC 2827］。然而，这一措施并未得到广泛采用或强制实施。Bob 可能因为假定 Trudy 的网络管理员（这个管理员可能就是 Trudy 自己）已经配置 Trudy 的第一跳路由器，使之只能转发适当地址的数据报而被欺骗。