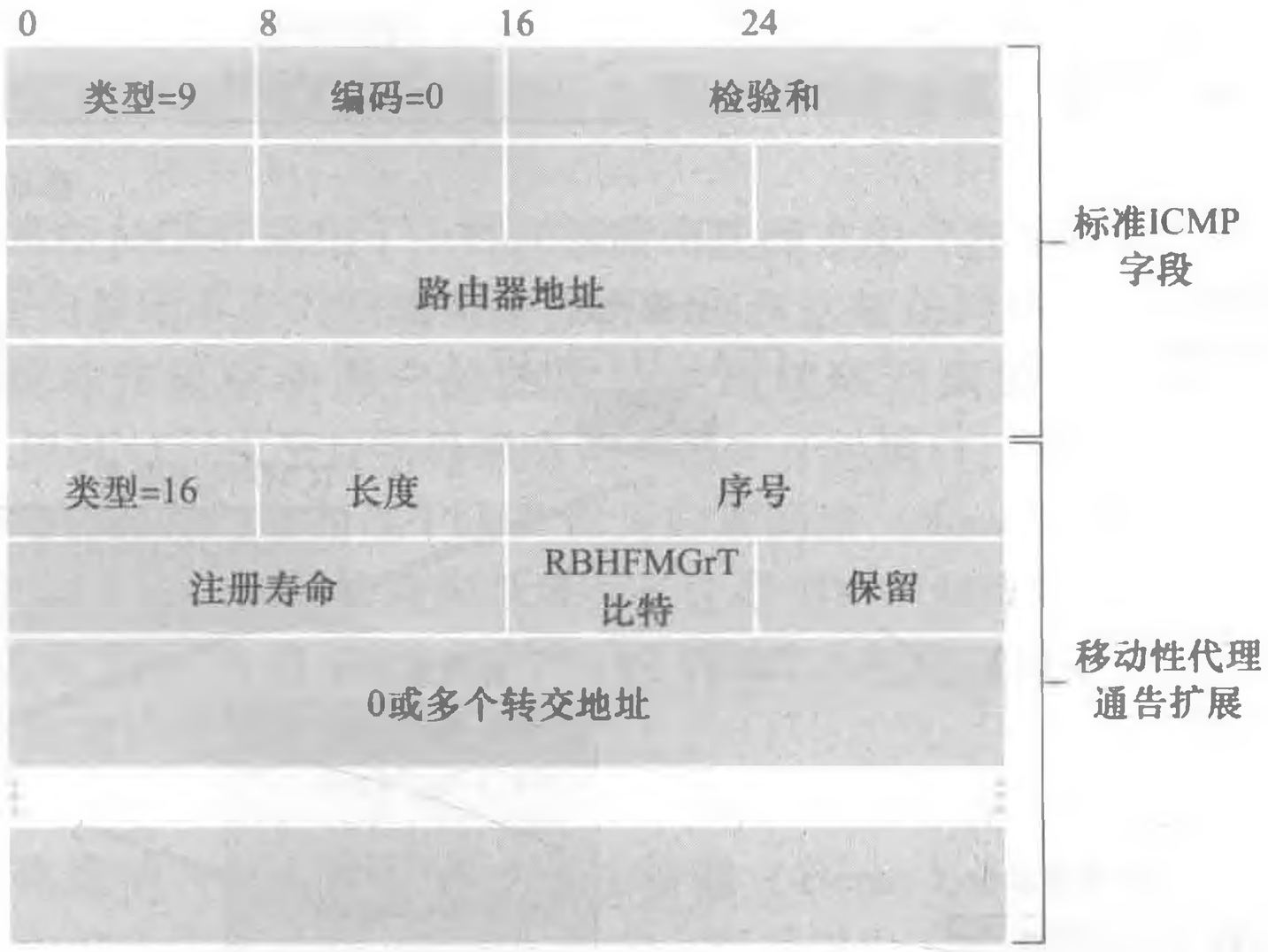


图 7-28 具有移动性代理通告扩展的 ICMP 路由器发现报文

使用**代理请求**（agent solicitation），一个想知道代理的移动节点不必等待接收代理通告，就能广播一个代理请求报文，该报文只是一个类型值为 10 的 ICMP 报文。收到该请求的代理将直接向该移动节点单播一个代理通告，于是该移动节点将继续处理，就好像刚收到一个未经请求的通告一样。

2. 向归属代理注册

一旦某个移动 IP 节点收到一个 COA，则该地址必须要向归属代理注册。这可通过外部代理（由它向归属代理注册该 COA）或直接通过移动 IP 节点自己来完成。我们下面考虑前一种情况，共涉及 4 个步骤。

1）当收到一个外部代理通告后，一个移动节点立即向外部代理发送一个移动 IP 注册报文。注册报文承载在一个 UDP 数据报中并通过端口 434 发送。注册报文携带以下内容：一个由外部代理通告的 COA、归属代理的地址（HA）、移动节点的永久地址（MA）、请求的注册寿命和一个 64 比特的注册标识。请求的注册寿命指示了注册有效的秒数。如果注册没有在规定的时间内在归属代理上更新，则该注册将变得无效。注册标识就像一个序号，用于收到的注册回答与注册请求的匹配（下面会讨论）。

2）外部代理收到注册报文并记录移动节点的永久 IP 地址。外部代理知道现在它应该查找这样的数据报，即它封装的数据报的目的地址与该移动节点的永久地址相匹配。外部代理然后向归属代理的 434 端口发送一个移动 IP 注册报文（同样封装在 UDP 数据报中）。这一报文包括 COA、HA、MA、封装格式要求、请求的注册寿命以及注册标识。

3）归属代理接收注册请求并检查真实性和正确性。归属代理把移动节点的永久 IP 地址与 COA 绑定在一起。以后，到达该归属代理的数据报与发往移动节点的数据报将被封装并以隧道方式给 COA。归属代理发送一个移动 IP 注册回答，该响应报文中包含有 HA、MA、实际注册寿命和被认可的请求报文注册标识。

4）外部代理接收注册响应，然后将其转发给移动节点。

到此，注册便完成了，移动节点就能接收发送到其永久地址的数据报。图 7-29 说明了这些步骤。注意到归属代理指定的寿命比移动节点请求的寿命要小。

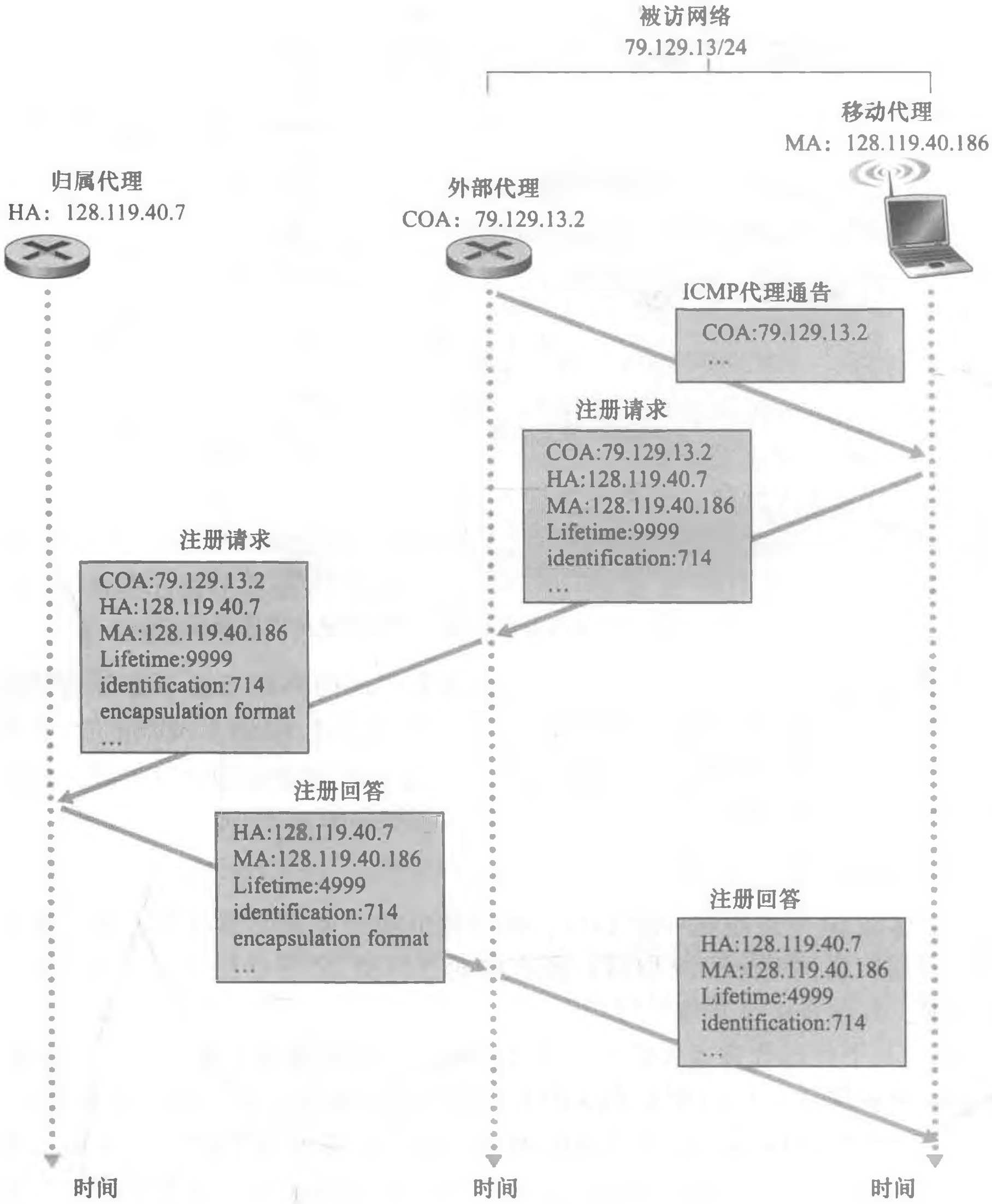


图 7-29　代理通告与移动 IP 注册

当某个移动节点离开其网络时，外部代理无须显式地取消某个 COA 的注册。当移动节点移动到一个新网（不管是另一个外部网络还是其归属网络）并注册一个新 COA 时，上述情况将自动发生。

除了上面所描述的情况，移动 IP 标准还允许许多另外的情形和功能，有兴趣的读者可以参阅［Perkins 1998b；RFC 5944］。

7.7　管理蜂窝网中的移动性

分析了 IP 网络中的移动性管理以后，我们现将注意力转向对移动性支持有更长历史的网络，即蜂窝电话网络。尽管在 7.4 节中我们关注过蜂窝网中的第一跳无线链路，但这里我们关注移动性，并以 GSM 蜂窝网络体系结构［Goodman 1997；Mouly 1992；Scourias 2012；Kaaranen 2001；Korhonen 2003；Turner 2012］作为学习案例，因为它是一个成熟并

被广泛部署的技术。3G 和 4G 网络中的移动性原则上与 GSM 中所使用的移动性类似。与在移动 IP 中的情况类似，我们将会看到 7.5 节指出的许多基本原理都被包含在 GSM 网络体系结构中。

与移动 IP 类似，GSM 采用了一种间接路由选择方法（参见 7.5.2 节），首先将通信者的呼叫路由选择到移动节点的归属网络，再从那到达被访网络。在 GSM 术语中，移动用户的归属网络被称作该移动用户的**归属公共地域移动网络**（home Public Land Mobile Network，home PLMN）。由于首字母缩略词 PLMN 有些拗口，考虑到我们避免缩略词字母表的要求，我们直接将 GSM 归属 PLMN 称为**归属网络**（home network）。移动用户向某个蜂窝网提供商订购了服务，该蜂窝网就成为了这些用户的归属网络（即该提供商就按月提供的蜂窝服务收取用户的费用）。被访问的 PLMN，我们直接称其为**被访网络**（visited network），是移动用户当前所在网络。

与移动 IP 中情况类似，归属网络和被访网络的职责有很大的差别。

- 归属网络维护一个称作**归属位置注册器**（Home Location Register，HLR）的数据库，其中包括它每个用户的永久蜂窝电话号码以及用户个人概要信息。重要的是，HLR 也包括这些用户当前的位置信息。这就是说，如果一个移动用户当前漫游到另一个提供商的蜂窝网络中，HLR 中将包含足够多的信息来获取（通过一个我们即将描述的过程）被访网络中对移动用户的呼叫应该路由选择到的地址。我们将会看到，当一个呼叫定位到一个移动用户后，通信者将与归属网络中一个被称作**网关移动服务交换中心**（Gateway Mobile services Switching Center，GMSC）的特殊交换机联系。同样，为避免拗口的缩略词，我们这里用一个更具描述性的术语来称呼 GMSC，即**归属 MSC**（home MSC）。
- 被访网络维护一个称作**访问者位置注册**（Visitor Location Register，VLR）的数据库。VLR 为每一个当前在其服务网络中的移动用户包含一个表项，VLR 表项因此随着移动用户进入和离开网络而出现或消失。VLR 通常与移动交换中心（MSC）在一起，该中心协调到达或离开被访网络的呼叫建立。

在实践中，一个服务商的蜂窝网络将为其用户提供归属网络服务，同时为在其他蜂窝服务商订购服务的移动用户提供被访网络服务。

7.7.1　对移动用户呼叫的路由选择

现在我们描述一个呼叫如何定位到被访网络中的一个移动 GSM 用户。我们首先考虑下面一个简单的例子，更复杂的例子在［Mouly 1992］中有描述。如图 7-30 所示，这些步骤如下：

1）通信者拨打移动用户的电话号码。该号码本身并不涉及一个特定的电话线路或位置（毕竟电话号码是固定的，而用户是移动的），号码中的前几位数字足以全局地判别移动用户的归属网络。呼叫从通信者通过公共交换电话网到达移动用户归属网络中的归属 MSC。这是呼叫的第一步。

2）归属 MSC 收到该呼叫并查询 HLR 来确定移动用户的位置。在最简单的情况下，HLR 返回**移动站点漫游号码**（Mobile Station Roaming Number，MSRN），我们称其为**漫游号码**（roaming number）。注意到这个号码与移动用户的永久电话号码不同，后者是与移动用户的归属网络相关联的，而漫游号码是短暂的：当移动用户进入一个被访网络后，会给移动用户临时分配一个漫游号码。漫游号码的作用就相当于移动 IP 中转交地址的作用。并

且，与COA类似，它也是对通信者和移动用户不可见的。如果HLR不具有该漫游号码，它返回被访网络中VLR的地址。在这种情况下（未在图7-30中显示出来），归属MSC需要查询VLR以便获取移动节点的漫游号码。但是HLR是如何首先得到漫游号码或VLR地址的呢？移动用户到另一个被访网络后这些值将发生怎样的变化？我们将很快考虑这些重要问题。

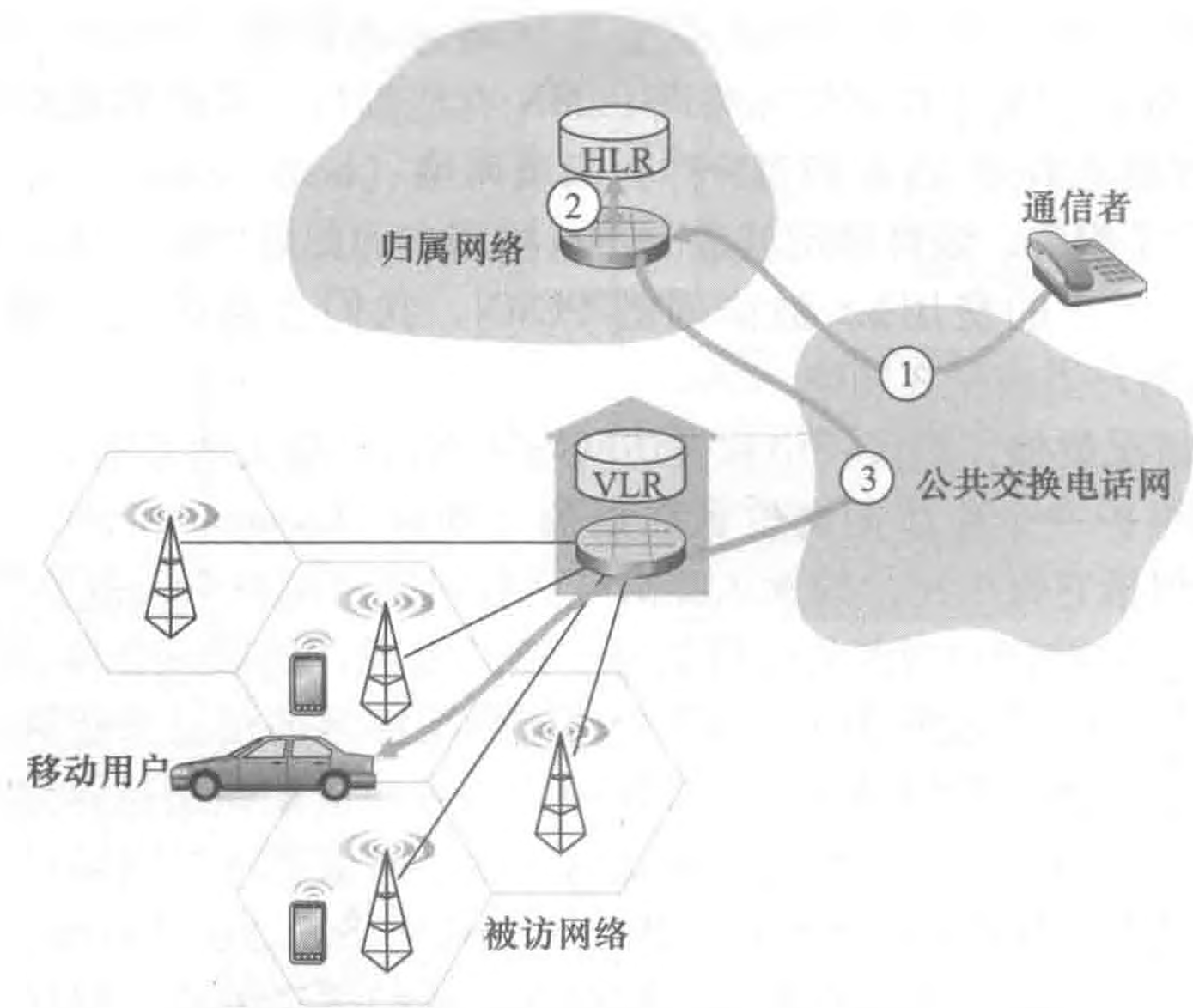


图7-30　将呼叫定位到一个移动用户：间接路由选择

3）给定一个漫游号码，归属MSC通过网络到达被访网络的MSC建立呼叫的第二步。至此，该呼叫已经完成，从通信者到达归属MSC，再从归属MSC到达被访MSC，然后到达为移动用户提供服务的基站。

在第二步中，一个未解决的问题是HLR如何获得有关移动用户位置的信息。当一个移动电话切换或进入一个由新的VLR所覆盖的被访网络中以后，移动用户必须向被访网络注册，这是通过在移动用户和VLR之间交换信令报文来实现的。被访VLR随后又向移动用户的HLR发送一个位置更新请求报文。这一报文告知HLR可以用来联系移动用户的漫游号码，或者VLR地址（它可以用来随后查询以获取移动号码）。作为这个交换的一部分，VLR同样从HLR那里获取移动用户的信息，以及确定被访网络应该给予移动用户什么样的服务（如果有的话）。

7.7.2　GSM中的切换

在一个呼叫过程中，移动站点将其关联从一个基站改变到另一个基站时出现**切换**（hand-off）。如图7-31所示，移动用户的呼叫初始时（在切换前）通过一个基站（我们称其为旧基站）路由选择到该移动用户，而在切换以后它经过另一个基站（我们称其为新基站）路由选

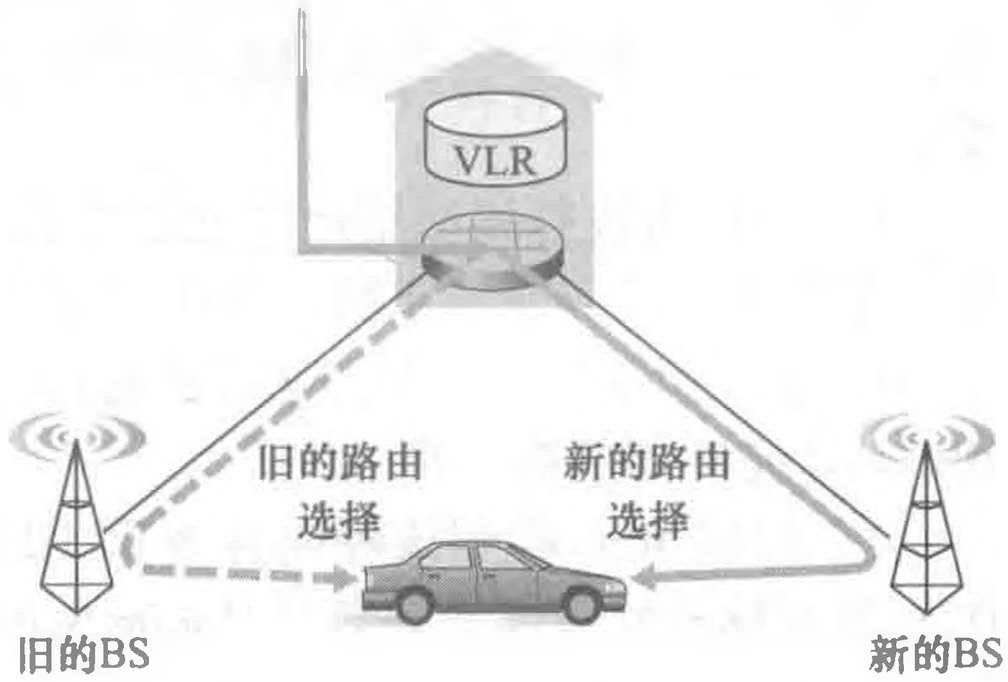


图7-31　具有一个公共MSC的基站间的切换情况

择到移动用户。注意到基站之间的切换不仅导致移动用户向/从一个新的基站传输/接收信号，而且导致正在进行的呼叫从网络中的一个交换点到新基站的重路由选择。我们首先假设新旧基站共享同一个 MSC，并且重路由选择发生在这个 MSC。

有几种原因导致切换的发生，包括：①当前基站和移动用户之间的信号减弱，使得该呼叫有被中断的危险；②一个蜂窝处理的呼叫太多，变得过载。可以通过将一些移动用户切换到邻近不太拥塞的蜂窝中，使这个拥塞得到缓解。

在与一个基站相关联期间，移动用户周期性地测量来自其当前基站和临近它的可以“听得到”的基站的信标信号强度。这些测量以每秒 1～2 次的频率报告给移动用户的当前基站。根据这些测量值、临近蜂窝的移动用户的当前负载以及其他因素，GSM 中的切换由旧的基站发起［Mouly 1992］。GSM 标准并未明确规定基站在确定是否进行切换时所采用的具体算法。

图 7-32 显示了当一个基站决定切换一个移动用户时所包括的步骤：

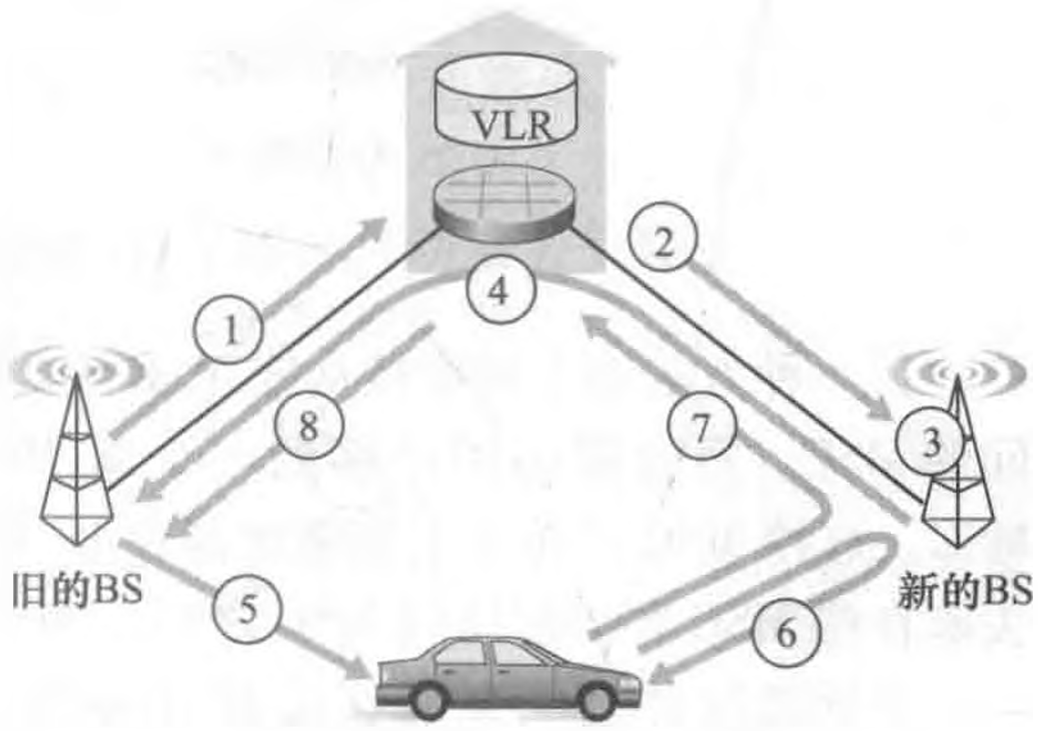


图 7-32　具有一个公共 MSC 的基站间完成一个切换的步骤

1）旧基站（BS）通知被访问 MSC 即将要进行一个切换，通知移动用户将要切换到的 BS（或可能的 BS 集）。

2）被访问 MSC 发起建立到新 BS 的路径，分配承载重路由选择的呼叫所需的资源，以及用信令告知新 BS 一个切换即将出现。

3）新 BS 分配并激活一个无线信道供移动用户使用。

4）新 BS 发出信令返回被访问 MSC 和旧 BS，即已经建立了被访问 MSC 到新 BS 的路径并且移动用户应当被告知即将发生的切换。新 BS 提供移动用户与新的 BS 相关联所需要的所有信息。

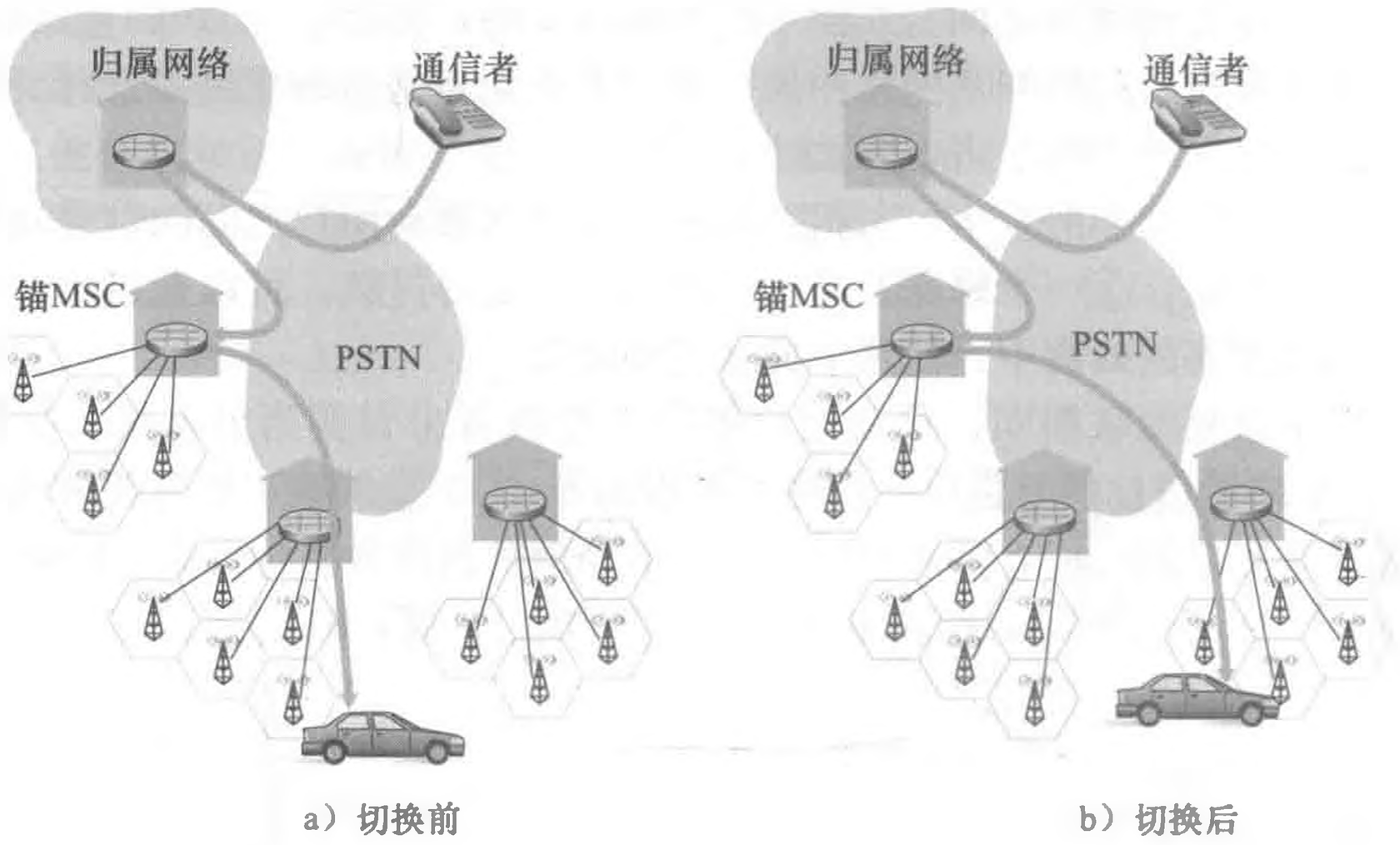
5）移动用户被告知它应当进行一个切换。注意到此时为止，移动用户完全不知网络已经为切换做好所有底层工作（如在新 BS 中分配一个信道，分配一条从被访问 MSC 到新 BS 的路径）。

6）移动用户和新 BS 交换一个或多个报文，以完全激活新 BS 中新的信道。

7）移动用户向新 BS 发送一个切换完成报文，该报文随后向上转发给被访问 MSC。该被访问 MSC 然后重路由选择到移动用户的正在进行的呼叫，使其经过新 BS。

8）沿着到旧 BS 的路径分配的资源随后被释放。

通过考虑如下情况来总结我们对切换的讨论：当移动用户移动到一个不同于旧 BS 的、与不同的 MSC 关联的 BS 中时，并且当这种 MSC 之间的切换多次发生时，考虑这些情况下将发生什么。如图 7-33 所示，GSM 定义了**锚 MSC**（anchor MSC）的概念。锚 MSC 是呼叫首次开始时移动用户所访问的 MSC，它因此在整个呼叫持续过程中保持不变。在整个呼叫持续期间，不论移动用户进行了多少次 MSC 间转换，呼叫总是从归属 MSC 路由选择到锚 MSC，然后再到移动用户当前所在的被访问 MSC。当移动用户从一个 MSC 覆盖区到达另一个 MSC 覆盖区后，正在进行的呼叫被重路由选择，从锚 MSC 到包含新基站的新被访问 MSC。因此，在任何情况下，通信者和移动用户之间至多有 3 个 MSC（归属 MSC、锚 MSC 以及被访问 MSC）。图 7-33 图示了在移动用户所访问的 MSC 之间的一个呼叫的路由选择。



a）切换前　　b）切换后

图 7-33　通过锚 MSC 重路由选择

另一种方法则不用维持从锚 MSC 到当前 MSC 的单一 MSC 跳，将直接链接移动用户访问的 MSC。每当移动用户移到一个新 MSC 后，让旧 MSC 将正在进行的呼叫转发给新 MSC。这种 MSC 链事实上能够出现在 IS-41 蜂窝网络中，通过使用最少步骤的可选路径来去除在锚 MSC 和当前访问 MSC 之间的 MSC［Lin 2001］。

下面通过对比 GSM 和移动 IP 中的移动性管理，来完成我们对 GSM 移动性管理的讨论。表 7-2 中的对比指出了尽管 IP 和蜂窝网络在很多方面有很大的区别，但它们共享数量惊人的公共功能要素和处理移动性的总体方法。

表 7-2　移动 IP 和 GSM 移动性之间的共性

GSM 要素	对 GSM 要素的解释	移动 IP 要素
归属系统	移动用户永久电话号码所归属的网络	归属网络
网关移动（服务）交换中心或简称归属 MSC，归属位置注册器（HLR）	归属 MSC：获取移动用户路由地址的联系点。HLR：归属系统中包含移动用户永久电话号码、个人信息、当前位置和订购信息的数据库	归属代理
被访问系统	移动用户当前所在的非归属系统网络	被访网络
被访问移动（服务）交换中心或简称被访问 MSC，访问者定位记录（VLR）	被访问 MSC：负责建立与 MSC 相关联的发射区中到/从移动节点的呼叫。VLR：访问系统中的临时数据库项，包含每个访问移动用户的订购信息	外部代理
移动站点漫游号码（MSRN），或漫游号码	用于归属 MSC 和被访问 MSC 之间电话呼叫的路由地址，对移动用户和通信者均不可见	转交地址

7.8　无线和移动性：对高层协议的影响

在本章中，我们已经看到了无线网络在链路层（由于无线信道的诸如衰减、多径、隐终端等特性）和网络层（由于移动用户改变与网络的连接点）与有线网络的对应物有重大的区别。但在运输层和应用层是否也有重大差别呢？我们很容易认为这些差别是很小的，因为在有线和无线网络中的网络层均为上层提供了同样的尽力而为服务模式。类似

地，如果在有线和无线网络中都是使用诸如 TCP 和 UDP 的协议提供运输层服务，那么应用层也应该保持不变。在某个方面我们的直觉是对的，即 TCP 和 UDP 可以（也确实）运行在具有无线链路的网络中。在另一方面，运输层协议（特别是 TCP）通常在有线和无线网络中有时会有完全不同的性能。这里，在性能方面区别是明显的，我们来研究一下其中的原因。

前面讲过，在发送方和接收方之间的路径上，一个报文段不论是丢失还是出错，TCP 都将重传它。在移动用户情况下，丢失可能源于网络拥塞（路由器缓存溢出）或者切换（例如，由于重路由选择报文段到移动用户新的网络接入点引入的时延）。在所有情况下，TCP 的接收方到发送方的 ACK 都仅仅表明未能收到一个完整的报文段，发送方并不知道报文段是由于拥塞，或在切换过程中，还是由于检测到比特差错而被丢弃的。在所有情况下，发送方的反应都一样，即重传该报文段。TCP 的拥塞控制响应在所有场合也是相同的，即 TCP 减小其拥塞窗口，如 3.7 节讨论的那样。由于无条件地降低其拥塞窗口，TCP 隐含地假设报文段丢失是由于拥塞而非出错或者切换所致。我们在 7.2 节看到，在无线网络中比特错误比在有线网络中普遍得多。当这样的比特差错或者切换丢失发生时，没理由让 TCP 发送方降低其拥塞窗口（并因此降低发送速率）。此时路由器的缓存的确可能完全是空的，分组可以在端到端链路中丝毫不受拥塞阻碍地流动。

研究人员在 20 世纪 90 年代早期到中期就认识到，由于无线信道的高比特差错率和切换丢失的可能性，TCP 的拥塞控制反应在无线情况下可能会有问题。有三大类可能的方法用于处理这一问题：

- *本地恢复*。本地恢复方法的目标是在比特差错出现的当时和当地（如在无线链路中）将其恢复。如在 7.3 节学习的 802.11 ARQ 协议，或者使用 ARQ 和 FEC 的更为复杂的方法［Ayanoglu 1995］）。
- *TCP 发送方知晓无线链路*。在本地恢复方法中，TCP 发送方完全不清楚其报文段跨越一段无线链路。另一种方法是让 TCP 发送方和接收方知道无线链路的存在，从而将在有线网络中发生的拥塞性丢包和在无线网络中发生的差错/丢包区分开，并且仅对有线网络中的拥塞性丢包采用拥塞控制。在假设端系统能够做出这种区分的情况下，［Balakrishnan 1997］详细研究了多种类型的 TCP。［Liu 2003］研究了在一个端到端路径中区分有线部分丢包和无线部分丢包的技术。
- *分离连接方法*。在分离连接方法中［Bakre 1995］，移动用户和其他端点之间的端到端连接被打断为两个运输层连接：一个从移动主机到无线接入点，一个从无线接入点到其他通信端点（我们假定它是有线的主机）。该端到端连接因此是由一个无线部分和一个有线部分级连形成的。经无线段的运输层能够是一个标准的 TCP 连接［Bakre 1995］，或是一个特别定制运行在 UDP 上的差错恢复协议。［Yavatkar 1994］研究了经无线连接使用运输层选择性重传协议。在［Wei 2006］中的测量报告指出了分离 TCP 连接广泛用于蜂窝数据网络中，通过使用分离 TCP 连接，上述问题的确能够有很大改进。

我们这里有关无线链路上的 TCP 的讨论是十分简要的。在无线网络中有关 TCP 挑战和解决方案的深入展望能够在［Hanabali 2005；Leung 2006］中找到。我们鼓励读者去查阅这些文献以了解这个正在进行的研究领域的详情。

考虑过运输层协议后，我们接下来考虑无线和移动性对应用层协议的影响。这里一个重要的考虑是无线链路经常具有相对较低的带宽，如我们在图 7-2 中所见。因此，运行在

无线链路尤其是蜂窝无线链路上的应用程序，必须将带宽作为稀有物品对待。例如，一个为在 4G 电话上运行的 Web 浏览器提供服务的 Web 服务器，就不能像为运行在有线连接的浏览器那样提供含有大量图片的内容。尽管无线链路的确为应用层提出一些挑战，它们具有的移动性同样使得一大批位置知晓和环境知晓应用成为可能［Chen 2000；Baldauf 2007］。更一般地，无线和移动网络将在未来的泛在计算环境实现中起着重要作用［Weiser 1991］。显然，在谈及无线和移动网络对网络应用及其协议的影响时，公平而论我们仅看到了冰山一角！

7.9　小结

无线网络和移动网络使电话发生了革命性变化，同时也对计算机网络界产生了日益深远的影响。伴随着它们对全球网络基础设施的随时、随地、无缝地接入，它们不仅使网络接入变得更加无所不在，而且催生了一组新的、令人兴奋的位置相关服务。考虑到无线网络和移动网络不断增长的重要性，本章关注用于支持无线和移动通信的原理、通用链路技术以及网络体系结构。

本章以对无线网络和移动网络的介绍开始，描述了由这种网络中通信链路的无线特性所引发的挑战和由这些无线链路带来的移动性之间的重要区别。这使我们能够更好地区分、识别和掌握每个领域中的关键概念。我们首先关注无线通信，在 7.2 节中考虑了无线链路的特征。在 7.3 节和 7.4 节中，我们研究了 IEEE 802.11（WiFi）无线 LAN 标准、两个 IEEE 802.15 个人域网络（蓝牙和 ZigBee），以及 3G 和 4G 蜂窝因特网接入。然后我们将注意力转向移动性问题。在 7.5 节中我们区分了多种形式的移动性，不同的移动性面临不同的挑战，并且看到了不同的解决方案。我们考虑了移动节点的定位和路由选择问题，以及对那些动态地从一个网络接入点移到另一个网络接入点的移动用户的切换问题。在 7.6 节和 7.7 节中，我们分别考察了这些问题在移动 IP 标准和 GSM 中是如何处理的。最后，我们在 7.8 节中考虑了无线链路和移动性对运输层协议和网络应用的影响。

尽管我们用了整整一章来学习无线网络和移动网络，但全面探索这个令人兴奋和快速扩展的领域需要一整本书或更多书的篇幅。我们鼓励读者通过查阅在本章中提供的许多参考资料，对这一领域进行更深入的研究。

课后习题和问题

复习题

7.1 节

R1. 一个无线网络运行在“基础设施模式”下是什么含义？如果某网络没有运行在基础设施模式下，那么它运行在什么模式下？这种运行模式与基础设施模式之间有什么不同？

R2. 在 7.1 节的分类法中，所确定的四种无线网络类型各是什么？你已经使用的是这些无线网络类型中的哪一种？

7.2 节

R3. 下列类型的无线信道损伤之间有什么区别：路径损耗、多径传播、来自其他源的干扰？

R4. 随着移动节点离开基站越来越远，为了保证传送帧的丢失概率不增加，基站能够采取的两种措施是什么？

7.3 ~ 7.4 节

R5. 描述 802.11 中信标帧的作用。

R6. 是非判断：802.11 站在传输一个数据帧前，必须首先发送一个 RTS 帧并收到一个对应的 CTS 帧。

R7. 为什么 802.11 中使用了确认，而有线以太网中却未使用？

R8. 是非判断：以太网和 802.11 使用相同的帧格式。

R9. 描述 RTS 门限值的工作过程。

R10. 假设 IEEE 802.11 RTS 和 CTS 帧与标准的 DATA 和 ACK 帧一样长，使用 CTS 和 RTS 帧还会有好处吗？为什么？

R11. 7.3.4 节讨论了 802.11 移动性，其中无线站点从一个 BSS 到同一子网中的另一个 BSS。当 AP 是通过交换机互连时，为了让交换机能适当地转发帧，一个 AP 可能需要发送一个带有哄骗的 MAC 地址的帧，为什么？

R12. 在某蓝牙网络中的一个主设备和在 802.11 网络中的一个基站之间有什么不同？

R13. 在 802.15.4 ZigBee 标准中超级帧的含义是什么？

R14. 在 3G 蜂窝数据体系结构中，“核心网”的作用是什么？

R15. 在 3G 蜂窝数据体系结构中，RNC 的作用是什么？在蜂窝语音网中 RNC 起什么作用？

R16. 在 4G 体系结构中 eNodeB、MME、P-GW 和 S-GW 的作用是什么？

R17. 3G 和 4G 蜂窝体系结构之间的 3 个重要差别是什么？

7.5 ~ 7.6 节

R18. 如果某节点与因特网具有无线连接，则该节点必定是移动的吗？试解释之。假设一个使用膝上型电脑的用户携带电脑绕着她的住所散步，并且总是通过相同的接入点接入因特网。从网络的角度看，这是移动用户吗？试解释之。

R19. 永久地址与转交地址之间的区别是什么？谁指派转交地址？

R20. 考虑经移动 IP 的一条 TCP 连接。是非判断：在通信者和移动主机之间的 TCP 连接阶段经过该移动用户的归属网络，但数据传输阶段直接通过该通信者和移动主机，绕开了归属网络。

7.7 节

R21. 在 GSM 网络中，HLR 和 VLR 的目的是什么？移动 IP 的什么要素类似于 HLR 和 VLR？

R22. 在 GSM 网络中，锚 MSC 的作用是什么？

7.8 节

R23. 为了避免单一无线链路降低一条端到端运输层 TCP 连接的性能，能够采取的三种方法是什么？

习题

P1. 考虑在图 7-5 中单一发送方的 CDMA 例子。如果发送方的 CDMA 码是（1，-1，1，-1，1，-1，1，-1），那么其输出（对于所显示的两个数据比特）是什么？

P2. 考虑图 7-6 中的发送方 2，发送方对信道 $Z_{i,m}^2$ 的输出是什么（在它被加到来自发送方 1 的信号前）？

P3. 假设在图 7-6 中的接收方希望接收由发送方 2 发送的数据。说明通过使用发送方 2 的代码，（经计算）接收方的确能够将发送方 2 的数据从聚合信道信号中恢复出来。

P4. 在两个发送方、两个接收方的场合，给出一个包括 1 和 -1 值的两个 CDMA 编码的例子，不允许两个接收方从两个 CDMA 发送方提取出初始传输的比特。

P5. 假设有两个 ISP 在一个特定的咖啡馆内提供 WiFi 接入，并且每个 ISP 有其自己的 AP 和 IP 地址块。

a. 进一步假设，两个 ISP 都意外地将其 AP 配置运行在信道 11。在这种情况下，802.11 协议是否将完全崩溃？讨论一下当两个各自与不同 ISP 相关联的站点试图同时传输时，将会发生什么情况。

b. 现在假设一个 AP 运行在信道 1，而另一个运行在信道 11。你的答案将会有什么变化？

P6. 在 CSMA/CA 协议的第 4 步，一个成功传输一个帧的站点在第 2 步（而非第 1 步）开始 CSMA/CA 协议。通过不让这样一个站点立即传输第 2 个帧（如果侦听到该信道空闲），CSMA/CA 的设计者是基

于怎样的基本原理来考虑的呢?

P7. 假设一个 802.11b 站点被配置为始终使用 RTS/CTS 序列预约信道。假设该节点突然要发送 1000 字节的数据，并且所有其他站点此时都是空闲的。作为 SIFS 和 DIFS 的函数，并忽略传播时延，假设无比特差错，计算发送该帧和收到确认需要的时间。

P8. 考虑在图 7-34 中显示的情形，其中有 4 个无线节点 A、B、C 和 D。这 4 个节点的无线电覆盖范围显示为其中的椭圆形阴影；所有节点共享相同的频率。当 A 传输时，仅有 B 能听到/接收到；当 B 传输时，A 和 C 能听到/接收到；当 C 传输时，B 和 D 能听到/接收到；当 D 传输时，仅有 C 能听到/接收到。

假定现在每个节点都有无限多的报文要向每个其他节点发送。如果一个报文的目的地不是近邻，则该报文必须要中继。例如，如果 A 要向 D 发送，来自 A 的报文必须首先发往 B，B 再将该报文发送给 C，C 则再将其发向 D。时间是分隙的，报文所用的传输时间正好是一个时隙，如在时隙 Aloha 中的情况一样。在一个时隙中，节点能够做下列工作之一：(i) 发送一个报文（如果它有报文向 D 转发)；(ii) 接收一个报文（如果正好一个报文要向它发送)；(iii) 保持静默。如同通常情况那样，如果一个节点听到了两个或更多的节点同时发送，出现冲突，并且重传的报文没有一个能成功收到。你这时能够假定没有比特级的差错，因此如果正好只有一个报文在发送，它将被位于发送方传输半径之内的站点正确收到。

a. 现在假定一个无所不知的控制器（即一个知道在网络中每个节点状态的控制器）能够命令每个节点去做它（无所不知的控制器）希望做的事情，例如发送报文，接收报文，或保持静默。给定这种无所不知的控制器，数据报文能够从 C 到 A 传输的最大速率是什么，假定在任何其他源/目的地对之间没有其他报文?

b. 现在假定 A 向 B 发送报文，并且 D 向 C 发送报文。数据报文能够从 A 到 B 且从 D 到 C 流动的组合最大速率是多少?

c. 现在假定 A 向 B 发送报文且 C 向 D 发送报文。数据报文能够从 A 到 B 且从 C 到 D 流动的组合最大速率是多少?

d. 现在假定无线链路由有线链路代替。在此情况下，重复问题 (a) ~ (c)。

e. 现在假定我们又在无线状态下，对于从源到目的地的每个数据报文，目的地将向源回送一个 ACK 报文（例如，如同在 TCP 中)。对这种情况重复问题 (a) ~ (c)。

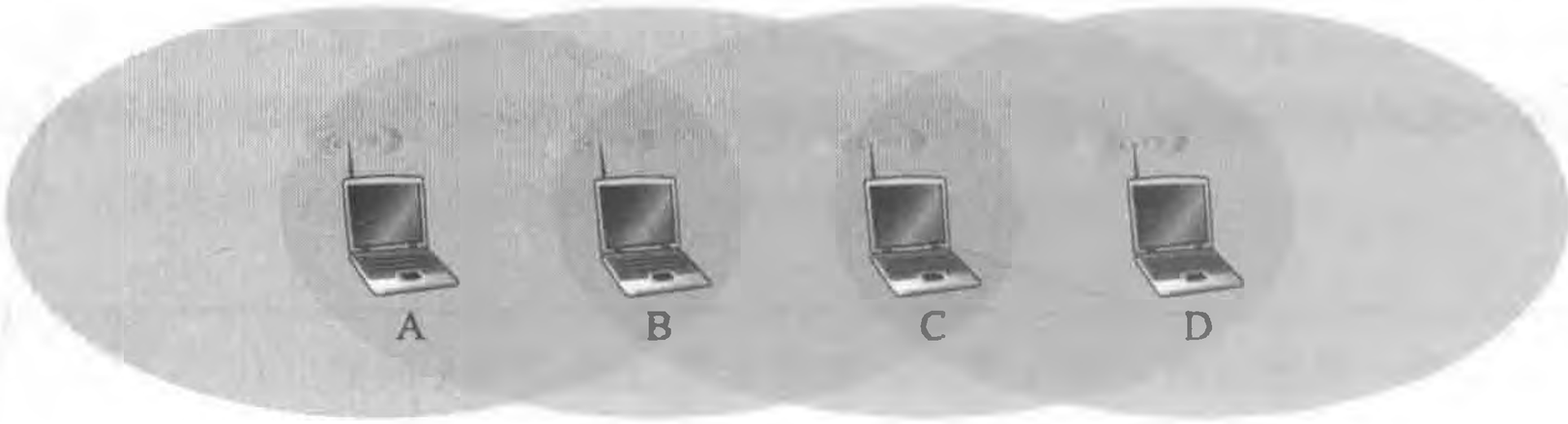


图 7-34　习题 P8 的情形

P9. 描述 802.15.1 蓝牙帧的格式。你必须要阅读某些课外读物来获取这些信息。在帧格式中有哪些因素本质上会限制 802.15.1 网络中主动节点数量为 8 呢? 试解释之。

P10. 考虑下列理想化的 LTE 情形。下行信道（参见图 7-21）划分为时隙，使用了 F 个频率。有 4 个节点 A、B、C 和 D 分别以 10Mbps、5Mbps、2.5Mbps 和 1Mbps 速率在下行信道上可到达基站。这些速率假定基本在所有 F 个频率上能够利用所有时隙只向一个站点进行发送。基站具有无限量的数据向每个节点发送，并且在下行子帧中的任何时隙期间使用 F 个频率中的任何之一能够向这 4 个站点之一发送。

a. 假定基站在每个时隙期间能够向它选择的任何节点发送，它能向节点发送的最大速率是多少? 你的解决方案公平吗? 解释并定义你所指“公平”的含义。

b. 如果有公平要求，即每个站点在每秒期间必须收到等量的数据，在下行子帧期间基站（向所有

节点）的平均传输速率是多少？

c. 假定该公平性准则是在子帧期间任何节点至多能够接收任何其他节点两倍多的数据。在下行子帧期间基站（向所有节点）的平均传输速率是多少？解释你是如何得到答案的。

P11. 在7.5节，一种允许移动用户在外部网络间移动过程中保持其IP地址不变的建议方案是，让外部网络通告一个到该移动用户高度特定的路由，并使用现有的路由选择基础设施在整个网络中传播这一信息。我们将扩展性作为一种关注因素。假设移动用户从一个网络移动到另一个网络后，新的外部网络通告一个到移动用户的特定路由，旧的外部网络丢弃其路由。考虑路由信息如何在一个距离向量算法中传播（尤其是对于跨越全球的网络间的域间路由选择情况）。

a. 一旦外部网络开始通告其路由，其他路由器能否立刻将数据报路由选择到新的外部网络呢？

b. 不同的路由器有可能认为移动用户位于不同的外部网络中吗？

c. 讨论网络中其他路由器最终知道到达移动用户的路径所用的时间范围。

P12. 假设图7-23中通信者是移动的。概述为了将数据报从初始移动用户路由选择到（现在移动的）通信者所需要的额外的网络层基础设施。如图7-24中那样，显示在初始移动用户和（现在移动的）通信者之间数据报的结构。

P13. 在移动IP中，移动性将对数据报在源和目的地间的端到端时延有怎样的影响？

P14. 考虑7.7.2节最后讨论的链的例子。假设一个移动用户访问外部网络A、B和C，当通信者在外部网络A中时，它开始一条与移动用户的连接。列出在外部代理之间和外部代理与归属代理之间，当移动用户从网络A到网络B再到网络C的过程中的报文序列。然后，假设未执行链接，并且通信者（以及归属代理）必须被显式地告知移动用户转交地址的改变。列出在第二种情况下需要交换的报文序列。

P15. 考虑在一个具有外部代理的外部网络中的两个移动节点。在移动IP中，这两个移动节点是否可能使用相同的转交地址？解释你的答案。

P16. 在我们对VLR如何用移动用户当前位置信息更新HLR的讨论中，与VLR地址对HLR相比，提供MSRN所具有的优缺点各是什么？

Wireshark 实验

在本书的配套Web站点上（http://www.pearsonhighered.com/cs-resources），你将找到有关本章的一个Wireshark实验，该实验用于捕获和学习在无线便携机和接入点之间交换的802.11帧。

人物专访

Deborah Estrin

DeborahEstrin是位于纽约城的Cornell工学院的计算机科学教授，同时是Weill Cornell医学院的公共卫生学教授。她是Cornell工学院健康技术中心的创始人和非营利组织创业公司Open mHealth的联合奠基人。她从MIT获得了计算机科学博士学位（1985年），并从加州大学伯克利分校获得学士学位（1980年）。Estrin的早期研究集中在多播和域间路由选择等网络协议的设计。在2002年，Estrin创建了美国国家自然科学基金资助的科学技术中心CENS（http://cens.ucla.edu）。CENS开创了多学科计算机系统研究的新领域，从用于环境监测的传感器网络到用于居民科学的分享感知。她当前致力于移动健康和小数据，促进移动设备和用于健康及生活管理的数字交互的普适性，正如她在2013 TEDMED演讲中所描述的。Estrin教授是美国艺术和科学研究院（2007年）、国家工程院（2009年）的当选成员，是IEEE、ACM和AAAS的会士。她被选为首名ACM-W雅典娜讲师（2006年），获得Anita Borg学院的妇女远见创新奖（2007年），被引入WITI名人纪念馆（2008年），被授予EPFL（2008年）和Uppsala大学（2011年）的荣誉博士。

- 请描述您职业生涯中干过的几个最令人激动的项目？

20世纪90年代中期当我在USC和ISI的时候，非常荣幸地与像Steve Deering、Mark Handley和Van Jacobson这样的人物在一起工作，设计多播路由选择协议（特别是PIM）。我试图将多播体系结构设计中的许多经验教训借鉴到生态监视阵列中，这是我首次真正开始全身心地进行应用和多学科的研究。那让我对社会和技术领域中的联合创新感兴趣，它们激发我对近期的研究领域——移动健康的研究兴趣。这些项目中的挑战随问题领域不同而不同，但它们的共同之处是需要睁大我们的眼睛，当我们在设计、部署、制作原型和试用之间重复时关注对问题的定义是否正确。没有一个问题能够借助于模拟或者构造的实验室实验加以分析解决。面对凌乱的问题和环境要保持清晰的体系结构，它们都对我们的能力提出挑战，并且它们都需要广泛的协作。

- 未来在无线网络和移动性方面您预见将会发生什么变化和创新？

在前个版本的专访中曾说过我从来对预测未来不具太多信心，但我的确继续推测，随着智能手机变得越来越强大和因特网基本接入点增多，我们可能看到特色电话（即那些不可编程和仅能用于语音和文本信息的电话）的终结，并且很快在今天这个推测显然已经成真。我也认为我们将看到嵌入式SIM的继续迅速增长，各种设备通过嵌入式SIM经过蜂窝网络能够以低数据率通信。而这种情况已出现，我们看到许多设备和“物联网”，它们使用嵌入式WiFi和其他低功率、短距离以及各种形式连接到本地中心。我并不期待出现大型可穿戴消费市场的时代。但到了本书下个版本出版的时间，我期待着在物联网和其他数字设备数据的促进下，个人应用软件会有极大的增长。

- 您预见网络和因特网未来将往何处发展？

我仍然认为向后看和向前看是有用的。以前我观察到在命名数据和软件定义网络方面的努力将出现成果，产生更可管理、可演化和更丰富的基础设施，并且更一般地表现为推动体系结构的角色向协议栈较高层发展。在因特网初期时，体系结构包括第四层及以下，位于顶端的应用程序更为竖井式/独块式。现在则是数据和分析控制着传输。SDN的采用已经超出了我一直以来的预期，在本书的第7版中包含SDN的内容使我由衷地感到高兴。然而，从协议栈向上看去，我们占优势的应用越来越多地生存在带围墙的花园之中，无论是移动应用还是如脸书那样的大型消费者平台。随着数据科学和大数据技术的发展，由于与其他应用和平台连接的价值，它们可能有助于引导这些应用跳出藩篱。

- 是谁激发了您的职业灵感？

有三个人出现在我的脑海中。第一个人是Dave Clark，他是因特网界的秘方和无名英雄。早期我有幸在他的左右，看到他在IAB的组织规范和因特网管理方法方面所起的作用，成为大致共识和运行编码的引导者。第二个人是Scott Shenker，他的智慧才华、正直和坚持令我印象深刻。我努力却很难像他那样清晰地定义问题和给出解决方案。无论问题大和小，我发电子邮件征求建议，他总是第一个回复的人。第三个人是我的姐姐Judy Estrin，她将创造性和勇气投入到她的职业，将想法和概念带入市场。没有Judy这类人，因特网技术将不会改变我们的生活。

- 您对进入计算机科学和网络领域的学生有什么忠告？

首先，在你的学术工作中构建一个坚实的基础，与你能够得到的任何、每个现实世界的工作经验相权衡。当你寻找一个工作环境时，在你真正关心的问题领域寻找机会，并且参与到你能够从中学习的思维敏捷的团队中。

第8章

Computer Networking: A Top-Down Approach, Seventh Edition

计算机网络中的安全

早在1.6节我们就描述了某些非常盛行和危险的因特网攻击，包括恶意软件攻击、拒绝服务、嗅探、源伪装以及报文修改和删除。尽管我们已经学习了有关计算机网络的大量知识，但仍然没有考察如何使网络安全，使其免受那些攻击的威胁。在获得了新的计算机网络和因特网协议的专业知识后，我们现在将深入学习安全通信，特别是计算机网络能够防御那些令人厌恶的坏家伙的原理。

我们首先介绍一下 Alice 和 Bob，这俩人要进行通信，并希望该通信过程是“安全”的。由于本书是一本网络教科书，因此 Alice 和 Bob 可以是两台需要安全地交换路由选择表的路由器，也可以是希望建立一个安全传输连接的客户和服务器，或者是两个交换安全电子邮件的电子邮件应用程序，所有这些学习案例都是在本章后面我们要考虑的。总之，Alice 和 Bob 是安全领域中两个众所周知的固定设备，也许因为使用 Alice 和 Bob 更为有趣，这与命名为“A”的普通实体需要安全地与命名为“B”的普通实体进行通信的作用是一样的。需要安全通信的例子通常包括不正当的情人关系、战时通信和商业事务往来；我们宁愿用第一个例子而不用后两个例子，并使用 Alice 和 Bob 作为发送方和接收方，以第一种情况为背景来讨论问题。

我们说过 Alice 和 Bob 要进行通信并希望做到“安全”，那么此处的安全其确切含义是什么呢？如我们将看到的那样，安全性（像爱一样）是多姿多彩的东西；也就是说，安全性有许多方面。毫无疑问，Alice 和 Bob 希望他们之间的通信内容对于窃听者是保密的。他们可能也想要确保当他们进行通信时，确实是在和对方通信，还希望如果他们之间的通信被窃听者篡改，他们能够检测到该通信已被篡改破坏。在本章的第一部分，我们将讨论能够加密通信的密码技术，鉴别正在与之通信的对方并确保报文完整性。

在本章的第二部分，我们将研究基本的密码学原则怎样用于生成安全的网络协议。我们再次采用自顶向下方法，从应用层开始，逐层（上面四层）研究安全协议。我们将研究如何加密电子邮件，如何加密一条 TCP 连接，如何在网络层提供覆盖式安全性，以及如何使无线 LAN 安全。在本章的第三部分，我们将考虑运行的安全性，这与保护机构网络免受攻击有关。特别是，我们将仔细观察防火墙和入侵检测系统是怎样加强机构网络的安全性的。

8.1 什么是网络安全

我们还是以要进行“安全”通信的情人 Alice 和 Bob 为例，开始网络安全的研究。这确切地意味着什么呢？显然，Alice 希望即使他们在一个不安全的媒体上进行通信，也只有 Bob 能够理解她所发送的报文，其中入侵者（入侵者名叫 Trudy）能够在该媒体上截获从 Alice 向 Bob 传输的报文。Bob 也需要确保从 Alice 接收到的报文确实是由 Alice 所发送的，并且 Alice 要确保和她进行通信的人的确就是 Bob。Alice 和 Bob 还要确保他们报文的内容在传输过程中没有被篡改。他们首先要确信能够通信（即无人拒绝他们接入通信所需

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其所声称的身份。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时，邮件服务器如何证实该用户就是他所声称的那个人呢？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，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 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。

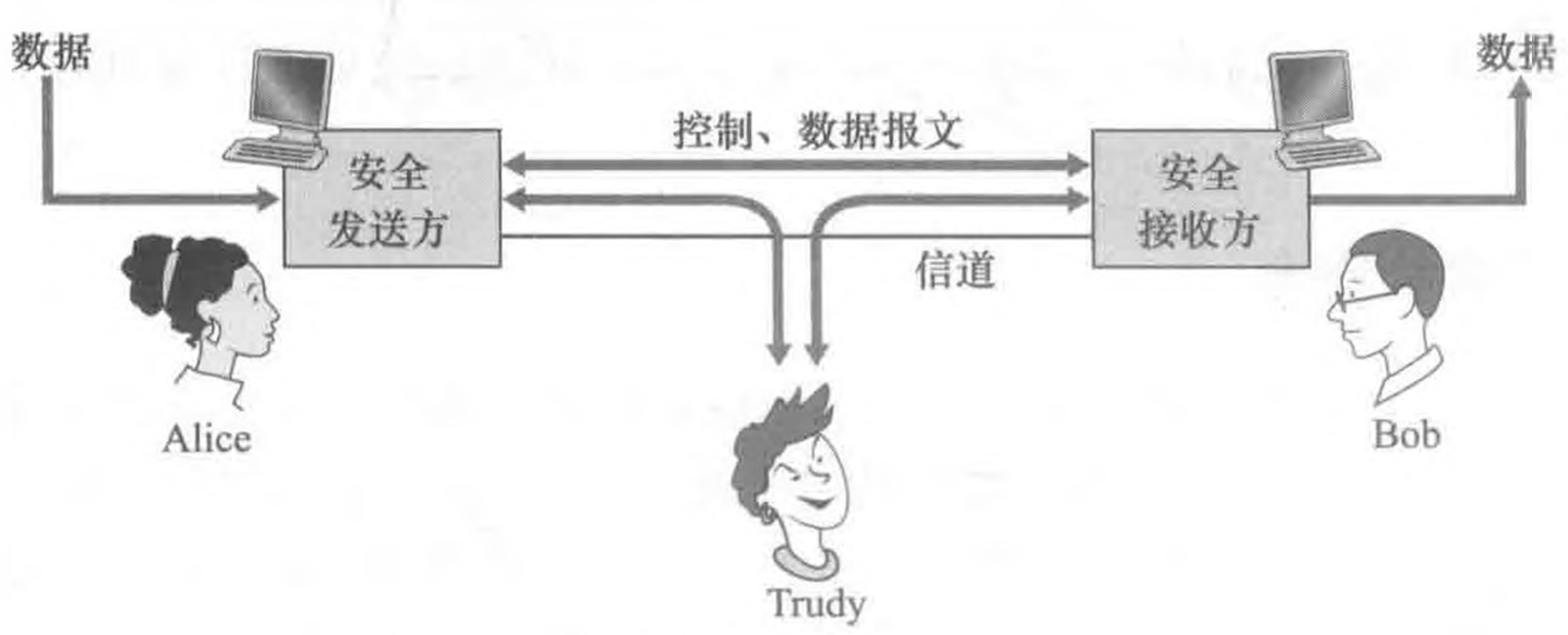


图 8-1　发送方、接收方和入侵者（Alice、Bob 和 Trudy）

如我们将看到的那样，除非采取适当的措施，否则上述能力使入侵者可以用多种方式

发动各种各样的安全攻击：窃听通信内容（可能窃取口令和数据），假冒另一个实体，“劫持”一个正在进行的会话，通过使系统资源过载拒绝合法网络用户的服务请求等等。CERT 协调中心对已报道的攻击进行了总结［CERT 2016］。

已经知道在因特网中某处的确存在真实的威胁，则 Alice 和 Bob（两个需要安全通信的朋友）在因特网上的对应实体是什么呢？当然，Alice 和 Bob 可以是位于两个端系统的人类用户，例如，真实的 Alice 和真实的 Bob 真的需要交换安全电子邮件。他们也可以参与电子商务事务。例如，真实的 Bob 希望安全地向一台 Web 服务器传输他的信用卡号码，以在线购买商品。类似地，真实的 Alice 要与银行在线交互。需要安全通信的各方自身也可能是网络基础设施的一部分。前面讲过，域名系统（DNS，参见 2.4 节）或交换路由选择信息的路由选择守护程序（参见第 5 章）需要在两方之间安全通信。对于网络管理应用也有相同的情况，第 5 章讨论了该主题。主动干扰 DNS 查找和更新（如在 2.4 节中讨论的那样）、路由选择计算［RFC 4272］或网络管理功能［RFC 3414］的入侵者能够给因特网造成不可估量的破坏。

建立了上述框架，明确了一些重要定义以及网络安全需求之后，我们将深入学习密码学。应用密码学来提供机密性是不言而喻的，同时我们很快将看到它对于提供端点鉴别、报文完整性也起到了核心作用，这使得密码学成为网络安全的基石。

8.2　密码学的原则

尽管密码学的漫长历史可以追溯到朱利叶斯·凯撒（Julius Caesar）时代，但现代密码技术（包括今天的因特网中正在应用的许多技术）基于过去 30 年所取得的进展。Kahn 的著作《破译者（The Codebreakers）》（［Kahn 1967］和 Singh 的著作《编码技术：保密的科学——从古埃及到量子密码（The Code Book：The Science of Secrecy from Ancient Egypt to Quantum Cryptography）》［Singh 1999］回顾了引人入胜的密码学的悠久历史。对密码学的全面讨论需要一本完整的书［Kaufman 1995；Schneier 1995］，所以我们只能初步了解密码学的基本方面，特别是因为这些东西正在今天的因特网上发挥作用。我们也注意到，尽管本节的重点是密码学在机密性方面的应用，但我们将很快看到密码学技术与鉴别、报文完整性和不可否认性等是紧密相关的。

密码技术使得发送方可以伪装数据，使入侵者不能从截取到的数据中获得任何信息。当然，接收方必须能够从伪装的数据中恢复出初始数据。图 8-2 说明了一些重要的术语。

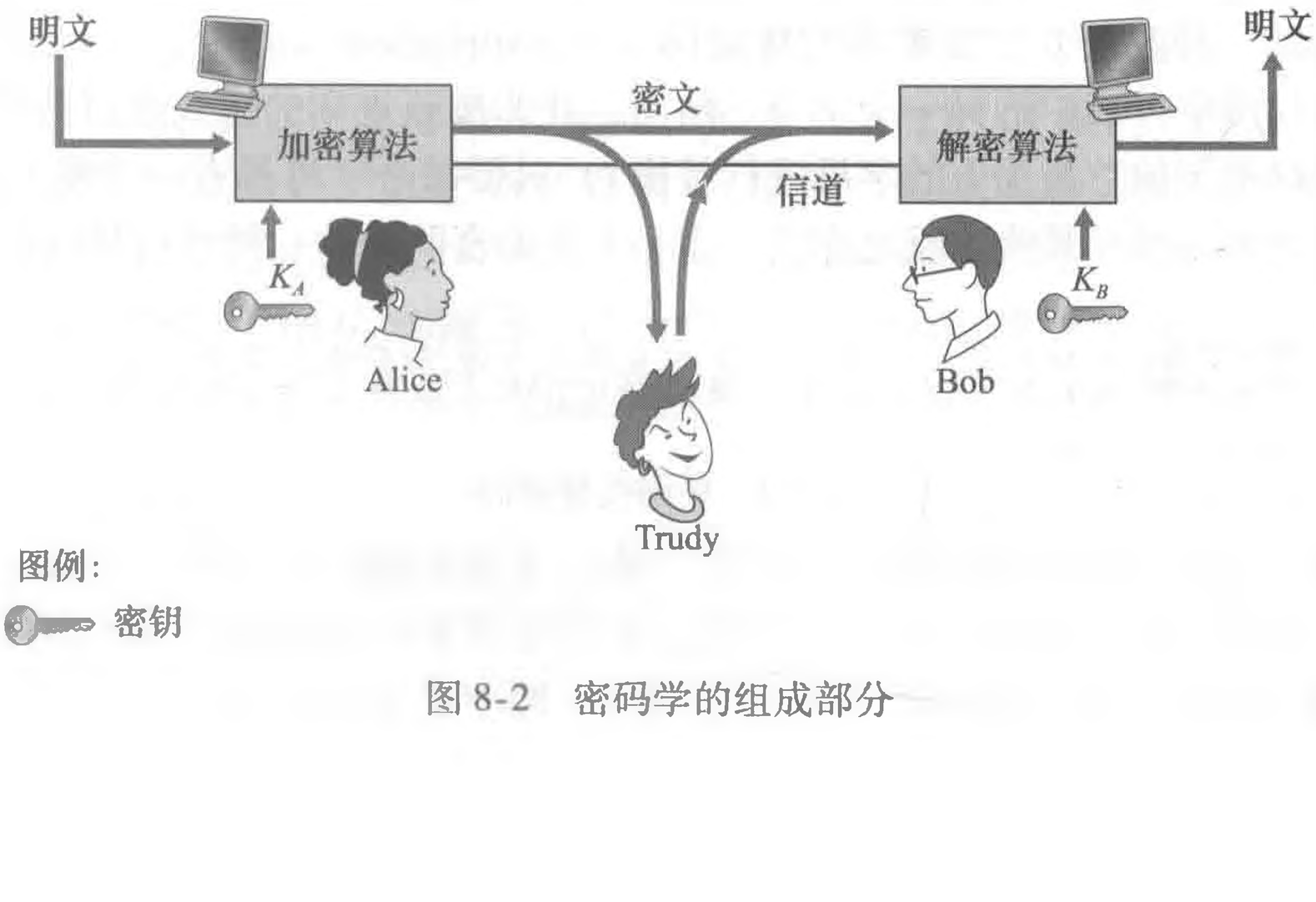


图 8-2　密码学的组成部分