为了具体起见，我们这里将关注 IPsec 的运输模式。使用这种模式，两台主机首先在它们之间创建一个 IPsec 会话。（因此 IPsec 是面向连接的!）使用适当的会话，在这两台主机之间发送的所有 TCP 和 UDP 报文段都享受 IPsec 提供的安全性服务。在发送端，运输层向 IPsec 传递一个报文段。IPsec 然后加密该报文段，在报文段上添加附加的安全性字段，并且在一个普通的 IP 数据报中封装得到的有效载荷。（实际中比上述过程要复杂一点，我们将在第 8 章详细讨论。）发送主机接下来向因特网中发送数据报，因特网则将数据报传送到目的主机。在那里，IPsec 解密报文段并将脱密的报文段传送给运输层。

由 IPsec 会话提供的服务包括：

- *密码技术约定*。这种机制允许两台通信的主机对加密算法和密钥达成一致。
- *IP 数据报有效载荷的加密*。当发送主机从运输层接收到一个报文段时，IPsec 加密该有效载荷。该有效载荷仅能由在接收主机中的 IPsec 解密。
- *数据完整性*。IPsec 允许接收主机验证数据报的首部字段，保证被加密的有效载荷在其数据报从源到目的地的路由器中传输时没有被修改过。
- *初始鉴别*。当一台主机从某受信任的源（具有一个受信任的密钥，参见第 8 章）接收到一个 IPsec 数据报时，该主机确信在数据报中的源 IP 地址是该数据报的实际源。

当两台主机在它们之间创建了一个 IPsec 会话时，在它们之间发送的所有 TCP 和 UDP 报文段将被加密和鉴别。IPsec 因此提供了地毯式覆盖，使这两台主机之间的所有网络应用进行安全通信。

通过使用 IPsec，一个公司能够在非安全的公共因特网中进行安全通信。为了进行说明，我们这里只看一个简单的例子。考虑一个拥有大批销售人员的公司，这些销售人员分布在各地跑业务。假定各种销售人员需要经常查询公司的敏感信息（例如价格和产品信息），这些信息存储在公司总部的一台服务器上。进一步假设销售人员也需要彼此发送敏感文档。使用 IPsec 怎样能够做到这一点呢？如你猜想的那样，我们在这台服务器和所有销售人员的便携机上安装 IPsec。借助于安装在这些主机上的 IPsec，某销售人员无论何时需要与服务器通信或与另一名销售人员通信，这些通信会话将是安全的。

4.5 路由选择算法

到目前为止，我们在本章中主要研究了网络层的转发功能。我们知道当分组到达一台路由器时，该路由器索引其转发表并决定该分组被指向的链路接口。我们也知道路由选择算法在网络路由器中运行、交换和计算信息，用这些信息配置这些转发表。路由选择算法和转发表之间的相互影响如图 4-2 所示。在已经较为深入地研究了转发后，我们将注意力转向本章的其他重要主题，即网络层的至关重要的路由选择功能。不管网络层提供的是数据报服务（在此情况下，在给定源和目的地址之间的不同分组可能采用不同的路由），还是虚电路服务（在此情况下，在给定源和目的地址之间的所有分组将采用相同路径），网络层都必须为从发送方到接收方的分组确定所采用的路径。我们将看到路由选择的工作是：确定从发送方到接收方通过路由器网络的好路径（等价为路由）。

主机通常直接与一台路由器相连接，该路由器即为该主机的**默认路由器**（default router），又称为该主机的**第一跳路由器**（first-hop router）。每当主机发送一个分组时，该分组被传