所谓**SNMP应用程序**（SNMP application）是由命令产生器、通知接收器和代理转发器（这些通常位于管理实体中）、命令响应器和通知源发器（这两者通常位于代理中）以及其他可能的应用程序组成的。命令产生器产生我们在9.3.3节讨论过的GetRequest、GetNextRequest、GetBulkRequest和SetRequest PDU，并处理对这些PDU接收到的响应。命令响应器在代理中执行，接收、处理和（用Response报文）回答接收到的GetRequest、GetNextRequest、GetBulkRequest和SetRequest PDU。代理中的通知源发器应用程序产生Trap PDU；这些PDU最终由管理实体中的通知接收器应用程序接收和处理。代理转发器应用程序转发请求PDU、通知PDU和响应PDU。

由SNMP应用程序发送的PDU在经过适当的运输协议发送之前，接下来通过SNMP“引擎”传递。图9-5显示了由命令产生器应用程序产生的一个PDU先进入调度模块，在那里决定SNMP的版本。然后该PDU在报文处理系统中进行处理，在这里该PDU被封装在包括SNMP版本号、报文ID和报文长度信息的报文首部中。如果需要加密或鉴别，还要包括针对这些信息的适当首部字段信息；详见［RFC 3411］。最后，SNMP报文（应用程序产生的PDU加上首部信息的报文）被传递到适当的运输协议。携带SNMP报文的首选运输协议是UDP（即SNMP报文被作为UDP数据报的负载传送），用于SNMP的首选端口号是端口161。端口162用于陷阱报文。

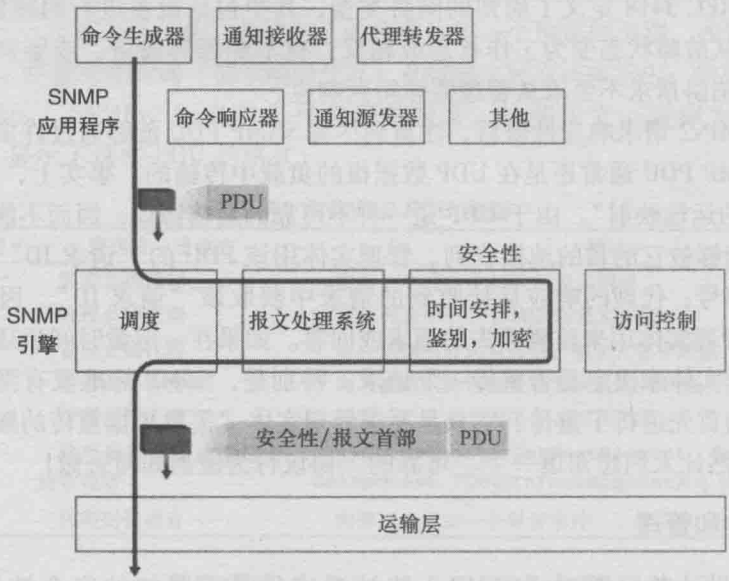

图9-5 SNMPv3引擎和应用程序

前面我们已经看到SNMP报文不仅能用于监视，也能用于控制（例如，通过SetRequest命令）网络元素。显然，若一个入侵者能够截获SNMP消息和/或产生它自己的SNMP报文并向管理基础设施发送，它就可能会对网络造成损害。因此，安全地传输SNMP报文是至关重要的。令人惊奇的是，仅在SNMP最近的版本中，安全性才得到应有的注意。SNMPv3的安全性被称为**基于用户的安全性**（user-based security）［RFC 3414］，这是因为它应用了用户的传统概念（用户采用用户名来标识），还有相关的口令、密码值或访问权限等安全信息。SNMPv3提供了加密、鉴别、对重放攻击的防护（参见8.3节）和访问控制功能。