计算机网络　第十五周作业　12 月 23 日　周三

PB18151866 龚小航

P6.6 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（即使侦听到信道空闲），CSMA/CA 的设计者是基于怎样的基本原理来考虑的呢?

解：这样的设计主要是出于公平性的考虑。若成功传输帧的站点直接从第一步开始 CSMA/CA 协议，那么它能立即传输第 2 个帧。这会导致一个长帧（例如几十万个帧）将长时间占用信道并且还是不可抢占的，这会出现类似于“护航效应”的现象，即多个需要传输短小帧的站点等待一个传输长帧的站点释放资源。而目前的协议设计能保证每传输一帧都要进行回退，类似于轮转调度，保证了一定的公平性。

P6.8 考虑在图 6－33 中显示的情形，其中有四个无线结点 A、B、C 和 D。这四个结点的无线电覆盖范围显示为其中的椭圆型阴影；**所有结点共享相同的频率**。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。

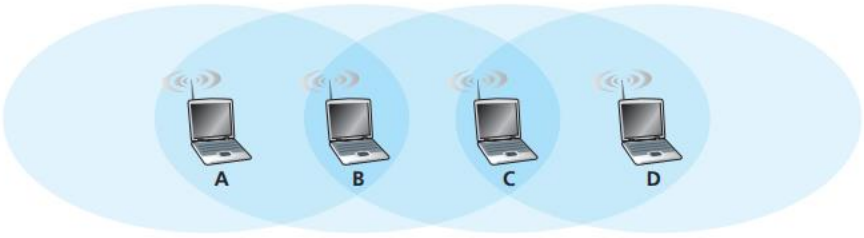


Figure 6.33 ♦ Scenario for problem P8

假定现在每个结点都有**无限多**的报文要向**每个**其他结点发送。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，结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，如果一个结点听到了两个或更多的结点同时发送，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。

($\boldsymbol{a}$) 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结点状态的控制器) 能够命令每个结点去做它(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?

($\boldsymbol{b}$) 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?

($\boldsymbol{c}$) 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?

($\boldsymbol{d}$) 现在假定无线链路由有线链路代替。在此情况下，重复问题 $(a)\sim(c)$。

($\boldsymbol{e}$) 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 $(a)\sim(c)$。

解: 分别分析:

(a) 由题目描述，从 C 到 A 发送报文必须先由 C 发送报文给 B，再由 B 发送报文给 A。再由给出的时隙描述，显然从 C 发送一个报文至 A 需要两个时隙。因此数据报从 C 到 A 的最大传输速率为:

1 数据报/2 个时隙

(b) A 向 B 发送报文且 D 向 C 发送报文时，显然发送方 A 和 D 的信号覆盖范围没有重叠，而且此时 B 恰好只接收得到 A 的信号，C 只接收得到 D 的信号，因此 A 和 D 可以同时发送数据而不受干扰。因此这时流动的组合速率最大为:

2 数据报/1 个时隙

(c) A 向 B 发送报文且 C 向 D 发送报文时，由于所有节点共享相同频率，那么如果 A 和 C 同时发送报文，B 就会同时收到两个信号的混合，出现冲突。因此 A 和 C 不能同时发送数据报。因此此时流动的组合速率最大为:

1 数据报/1 个时隙

(d) 若将无线链路用有线链路代替，即没有距离的限制，每两个节点之间都有一条链路相连。

$C\to A$ 的最大传输速率: 1 数据报/1 个时隙

$A\to B,\ D\to C$ 的最大组合传输速率: 2 数据报/1 个时隙

$A\to B,\ C\to D$ 的最大组合传输速率: 2 数据报/1 个时隙

(e) • 若每个报文都需要一个 ACK，那么从 $C \to A$ 的每步操作还需额外的一个时隙发送接收 ACK 报文。

$C \to A$ 的最大传输速率：　　1 数据报/4 个时隙

• 而 $A \to B, D \to C$ 可以在第一个时隙同时发数据报，但 B 和 C 不能同时发送 ACK 报文。

$A \to B$，$D \to C$ 的最大组合传输速率：　2 数据报/3 个时隙

• 对于 $A \to B$，$C \to D$ 来说，A, C 不能同时发送数据报，因此发送需要两个时隙；但是在发送第二个数据报的同时，第一个数据报的 ACK 报文恰好无冲突可以发送。因此共需三个时隙。

$A \to B$，$C \to D$ 的最大组合传输速率：　2 数据报/3 个时隙

P8.7　(a) 使用 RSA，选择 $p = 3$ 和 $q = 11$，采用对每个字母独立地加密的方法加密短语 'dog'。对已加密报文应用解密算法恢复出原报文。【教材 394，395 页】

(b) 重复 (a)，而此时加密 'dog' 作为一个报文 m

解：(a) 按 394 页的加密算法，$p = 3$，$q = 11$ 即可得到 $n = pq = 33$，$z = (p-1)(q-1) = 20$；再取小于 $n\,(33)$ 且与 $z\,(20)$ 互素的数 e，此处从小开始取，令 $e = 3$；此时给定 e，再选择一个 d 使 $ed \bmod z = 1$，此处取 $d = 7$。

此时可以得出生成的公钥 $K^+ = (n, e) = (33,3)$，私钥 $K^- = (n, d) = (33,7)$

参考课本 395 页，将字母以它在字母表中的顺序为 m，列出下表：

RSA 加密，$n = 33$，$e = 3$

明文字母	m:数字表示	m^e	密文 $c = m^e \bmod n$
d	4	64	31
o	15	3375	9
g	7	343	13

再列出解密表：

RSA 解密，$n = 33$，$d = 7$

密文 c	c^d	$m = c^d \bmod n$	明文字母
31	27512614111	4	d
9	4782969	15	o
13	62748517	7	g

(b) 加密算法就是对一个做加密，这与上一问的区别在于本问需要把数据报的所有内容综合视为一个整数再对齐做加密。需要保证 $n > m$，才能确保密文空间不小于明文空间。重新取 p, q

取 $p = 49999$，$q = 1009$ ，$e = 5$，公钥 $K^+ = (n, e) = (50448991,\ 5)$，对文本取 ASCII 码。

RSA 加密，$n = 50448991,\ e = 5$	
明文	dog
m:数字表示	01100100 01101111 01100111 B = 6582119 D
m^e	123545988572207581843046063636465 99
密文 $c = m^e \bmod n$	32872906

$z = 49998 * 1008 = 50{,}397{,}984$ 选取 d 使得 $ed \bmod z = 1$，取 $d = 10079597$。

因此解码时

RSA 解密，$n = 50448991,\ d = 10079597$			
密文 c	c^d	$m = c^d \bmod n$	明文字母
32872906	$(32872906)^{10079597}$	6582119	dog

由于解码时得到的 c^d 太大，此处不展开而写出其形式。

P8.9 在这个习题中，我们探讨 Diffie − Hellman（DH）公钥加密算法，该算法允许两个实体协商一个共享的密钥。该 DH 算法利用一个大素数 p 和另一个小于 p 的大数 g。p 和 g 都是公开的（因此攻击者将知道它们）。在 DH 中，Alice 和 Bob 每人分别独立地选择秘密密钥 S_A 和 S_B。Alice 则通过将 g 提高到 S_A 并以 p 为模来计算她的公钥 T_A。类似地，Bob 则通过将 g 提高到 S_B 并以 p 为模来计算他的公钥 T_B。此后 Alice 和 Bob 经过因特网交换他们的公钥。Alice 则通过将 T_B 提高到 S_A，并以 p 为模来计算出共享密钥 S。类似地，Bob 则通过将 T_A 提高到 S_B 并以 p 为模来计算出共享密钥 S'。

$(\boldsymbol{a})$ 证明在一般情况下，Alice 和 Bob 得到相同的对称密钥，即证明 $S = S'$。

$(\boldsymbol{b})$ 对于 $p = 11$ 和 $g = 2$，假定 Alice 和 Bob 分别选择私钥 $S_A = 5$ 和 $S_B = 12$，计算 Alice 和 Bob 的公钥 T_A 和 T_B。显示所有计算过程。

$(\boldsymbol{c})$ 接着 (b)，现在计算共享对称密钥 S。显示所有计算过程。

$(\boldsymbol{d})$ 提供一个时序图，显示 Diffie − Hellman 是如何能够受到中间人攻击的。该时序图应当具有 3 条**垂直线**，分别对应 Alice, Bob 和攻击者 Trudy。

解： 题中“提高”指取指数运算。列出他们每一步得到的结果，便于证明下面的结论。

	Alice	Bob
私钥	S_A	S_B
公钥	$T_A = g^{S_A} \bmod p$	$T_B = g^{S_B} \bmod p$
共享密钥	$S = T_B^{S_A} \bmod p$	$S' = T_A^{S_B} \bmod p$

$(\boldsymbol{a})$ 由上面得到的表达式，只需证明 $S = S'$：由教材 394 页的结论：

$$[(a \bmod n) + (b \bmod n)] \bmod n = (a + b) \bmod n$$
$$[(a \bmod n) - (b \bmod n)] \bmod n = (a - b) \bmod n$$
$$[(a \bmod n) \cdot (b \bmod n)] \bmod n = (a \cdot b) \bmod n$$
$$(a \bmod n)^d \bmod n = a^d \bmod n,$$

$$S - S' = \left(T_B^{S_A} - T_A^{S_B}\right) \bmod p = \left((g^{S_B} \bmod p)^{S_A} - (g^{S_A} \bmod p)^{S_B}\right) \bmod p$$
$$= \left(g^{S_A S_B} \bmod p - g^{S_A S_B} \bmod p\right) \bmod p = 0$$

即他们得到的共享密钥必然是一样的。

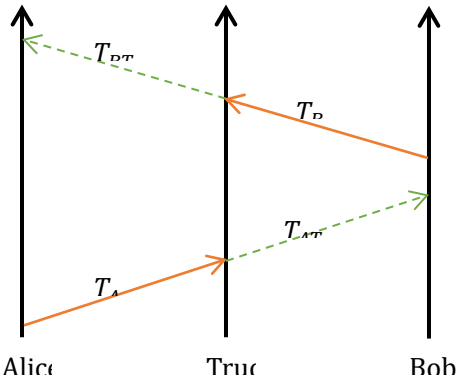
$(\boldsymbol{b})(\boldsymbol{c})$ $p = 11$，$g = 2$，$S_A = 5$，$S_B = 12$

计算他们得到的公钥以及共享密钥，直接由上面得出的表代入数值计算：

	Alice	Bob
私钥	$S_A = 5$	$S_B = 12$
公钥	$T_A = g^{S_A} \bmod p = 10$	$T_B = g^{S_B} \bmod p = 4$
共享密钥	$S = T_B^{S_A} \bmod p = 1$	$S' = T_A^{S_B} \bmod p = 1$

$(\boldsymbol{d})$ 此时这种通信存在严重的缺陷，这是由于没有使用公钥认证造成的。攻击者 Trudy 可以简单的冒充任意一方。例如下图所示：

两条虚线表示攻击者拦截下通信双方发送的公钥，并将自己的公钥发送过去。由于没有数字签名和



公钥认证，Alice 和 Bob 都以为自己正在和对方通信，实际上他们都在和 Trudy 通信，而攻击者可以做他想做的任何事，包括拦截，修改，伪造，监听等等。

P8.12 假定 Alice 和 Bob 共享两个秘密密钥：一个鉴别密钥 S_1 和一个对称加密密钥 S_2。扩充图 8－9，使之提供完整性和机密性。

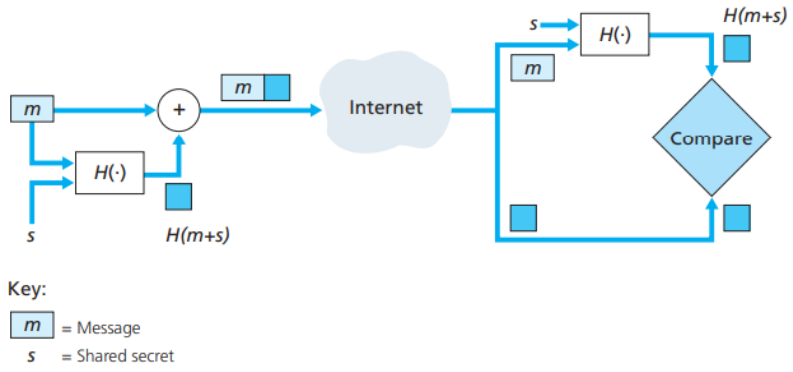


Figure 8.9 ♦ Message authentication code (MAC)

解：如图：

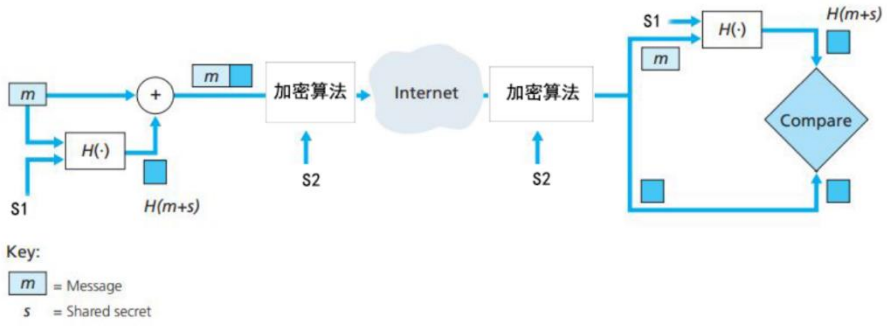


Figure 8.9 ♦ Message authentication code (MAC)