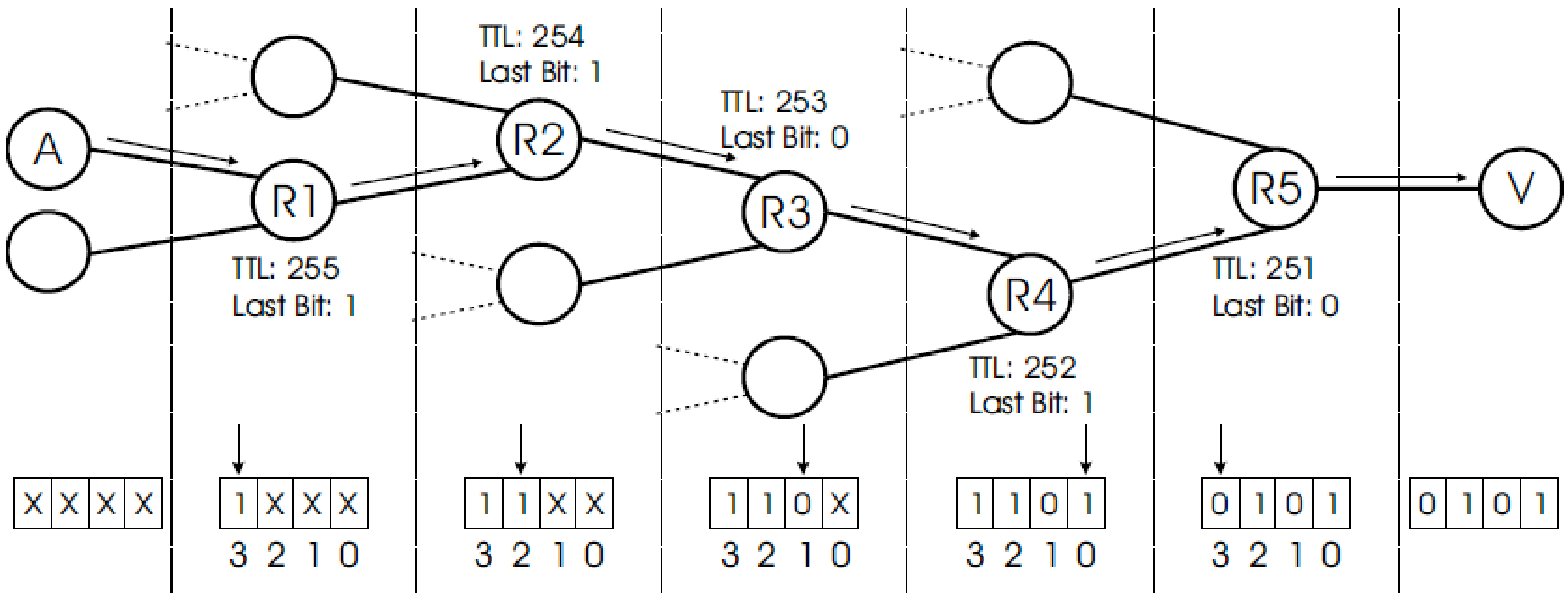
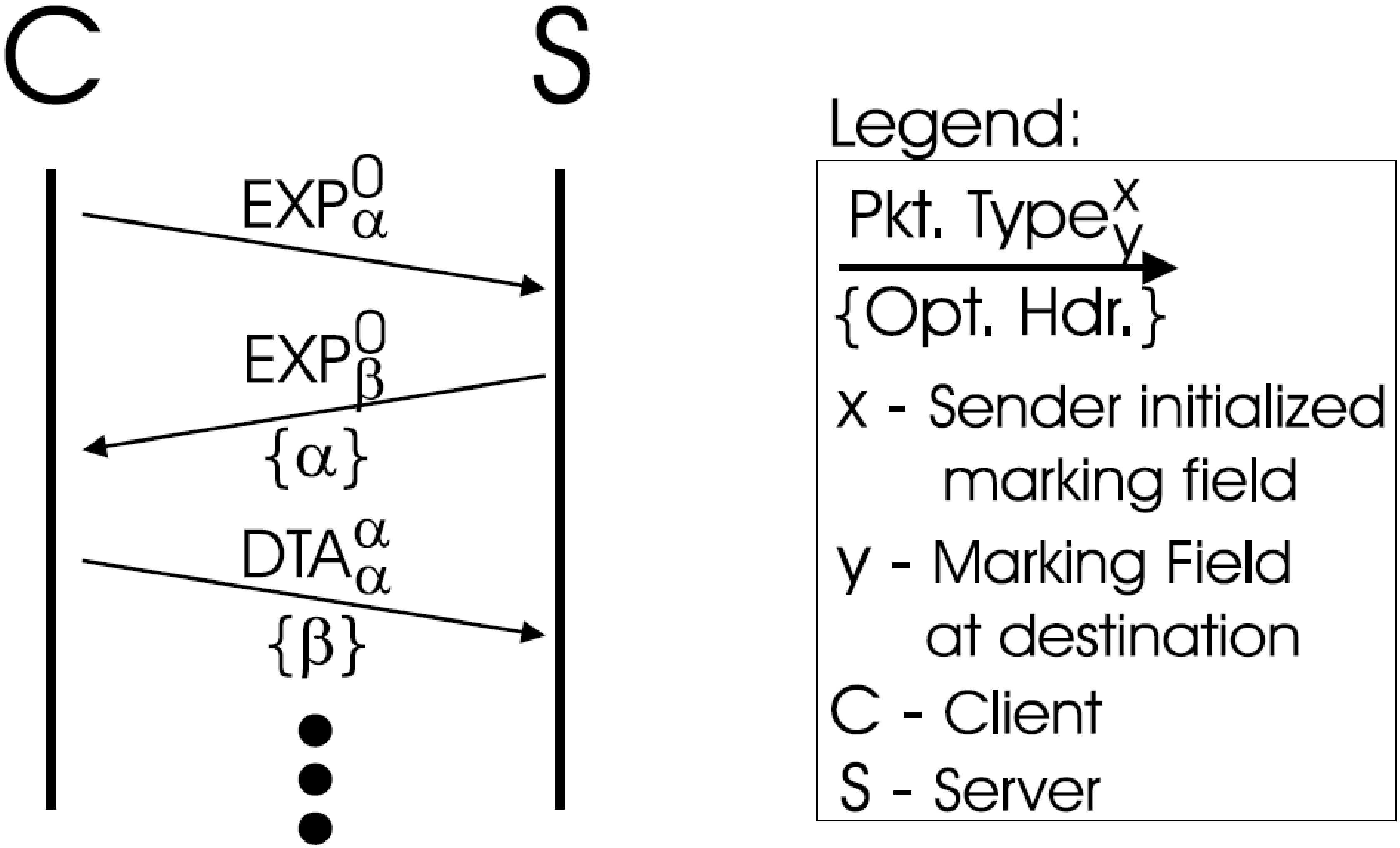
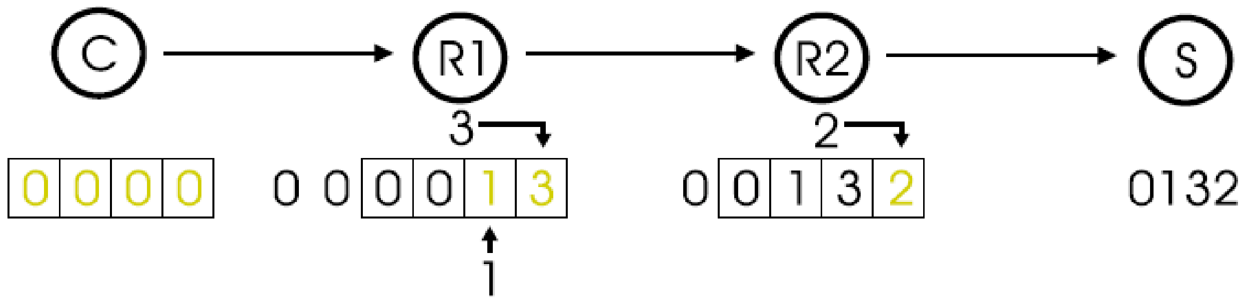
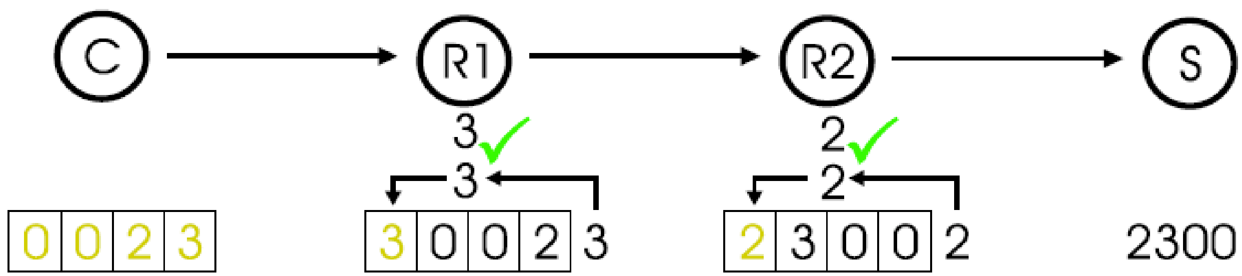


Figure 3. Example of our initial marking scheme. The packet travels from the attacker A to the victim V across the routers R1 to R5. Each router uses the TTL value of the packet to index into the IP identification field to insert its marking. In this example we show a 1-bit marking in a 4-bit field for simplicity.

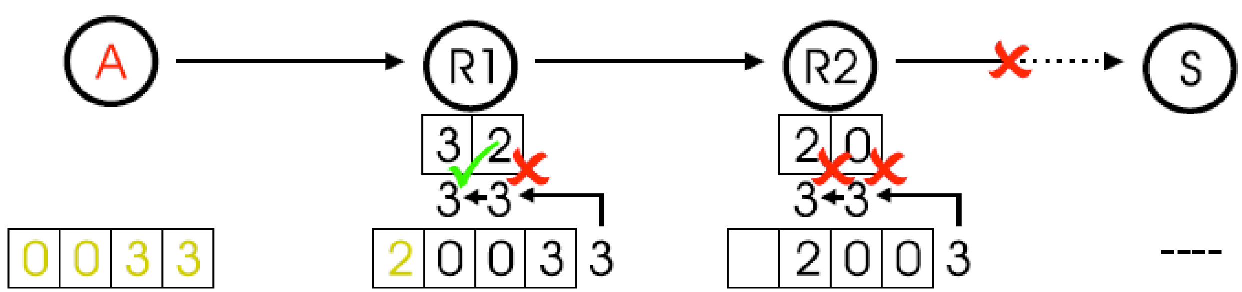

C
S
EXP $^{0}_{\alpha}$
EXP $^{0}_{\beta}$
$\{\alpha\}$
DTA $^{\alpha}_{\alpha}$
$\{\beta\}$
Legend:
Pkt. Type $^{x}_{y}$
{Opt. Hdr.}
x - Sender initialized marking field
y - Marking Field at destination
C - Client
S - Server



(a) Marking scheme for EXPLORER packets. Routers push their markings into the least significant bits of the capability field. Packets with a capability field of all zeros get marked with an additional 1 bit.

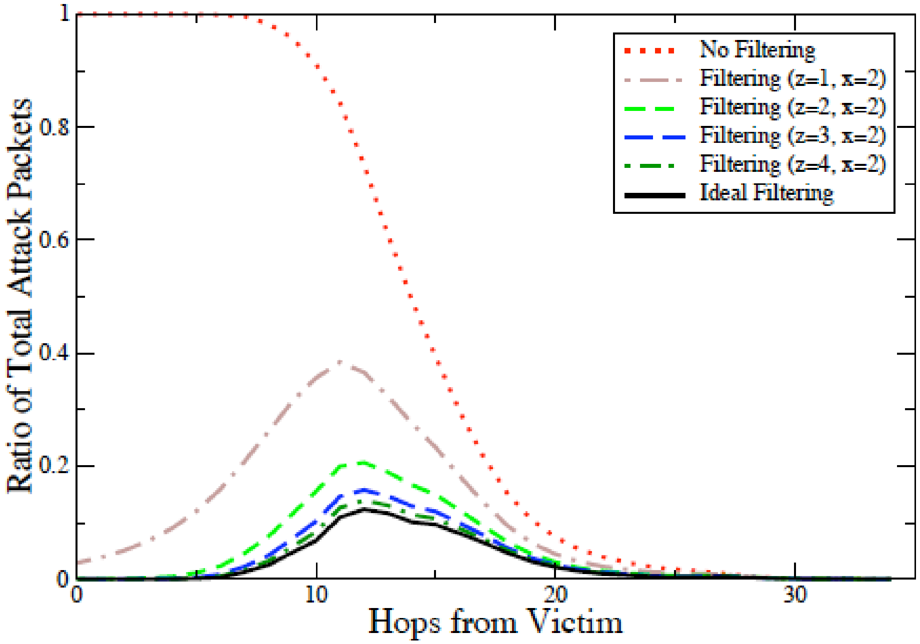


(b) Authentication scheme for DATA packets. Routers check the marking in the least significant bits of the capability field, and rotate it into the most significant bits, if it is equal to what the marking would be for an EXPLORER packet.

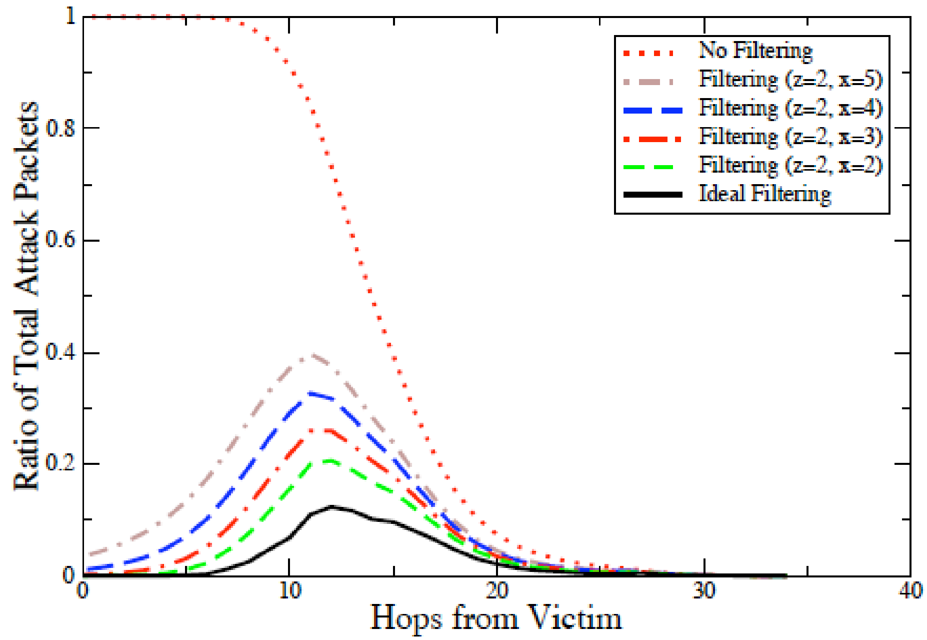


	$x = 2$	$x = 3$	$x = 4$	$x = 5$
$z = 1$	0.7500	0.8750	0.9375	0.9688
$z = 2$	0.4375	0.5781	0.6836	0.7627
$z = 3$	0.2344	0.3301	0.4138	0.4871
$z = 4$	0.1211	0.1760	0.2275	0.2758

Table 1. Evaluation of $P(x, z)$ (the probability to pass one router with a forged probability), for common values of x and z.



(a) Performance for various values of z, ($x = 2$).



(b) Performance for various values of x, ($z = 3$).

The probability that the client can connect after k tries is:

$$P(\text{ connect after k tries}) \\ = 1 - (1 - P(\text{connect after 1 try}))^k \\ = 1 - (1 - (1 - \epsilon_i)^i)^k$$

the required number of connection attempts is:

$$k = \frac{\log(1 - P(connect))}{\log(1 - (1 - \epsilon_i)^i)}$$