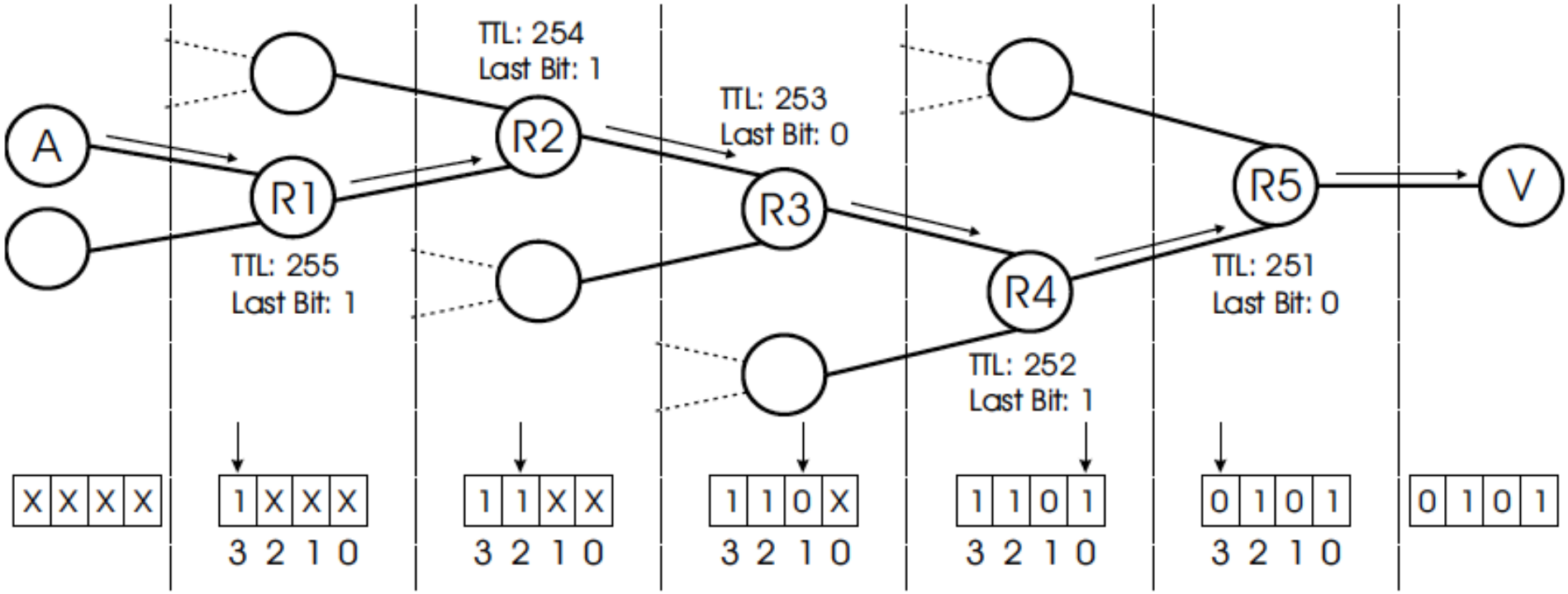


Figure 3. Example of our initial marking scheme. The packet travels from the attacker A to the victim V across the routers R1 to R5. Each router uses the TTL value of the packet to index into the IP identification field to insert its marking. In this example we show a 1-bit marking in a 4-bit field for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

Pi: A Path Identification Mechanism to Defend against DDoS Attacks

Abraham Yaar Adrian Perrig Dawn Song

Carnegie Mellon University

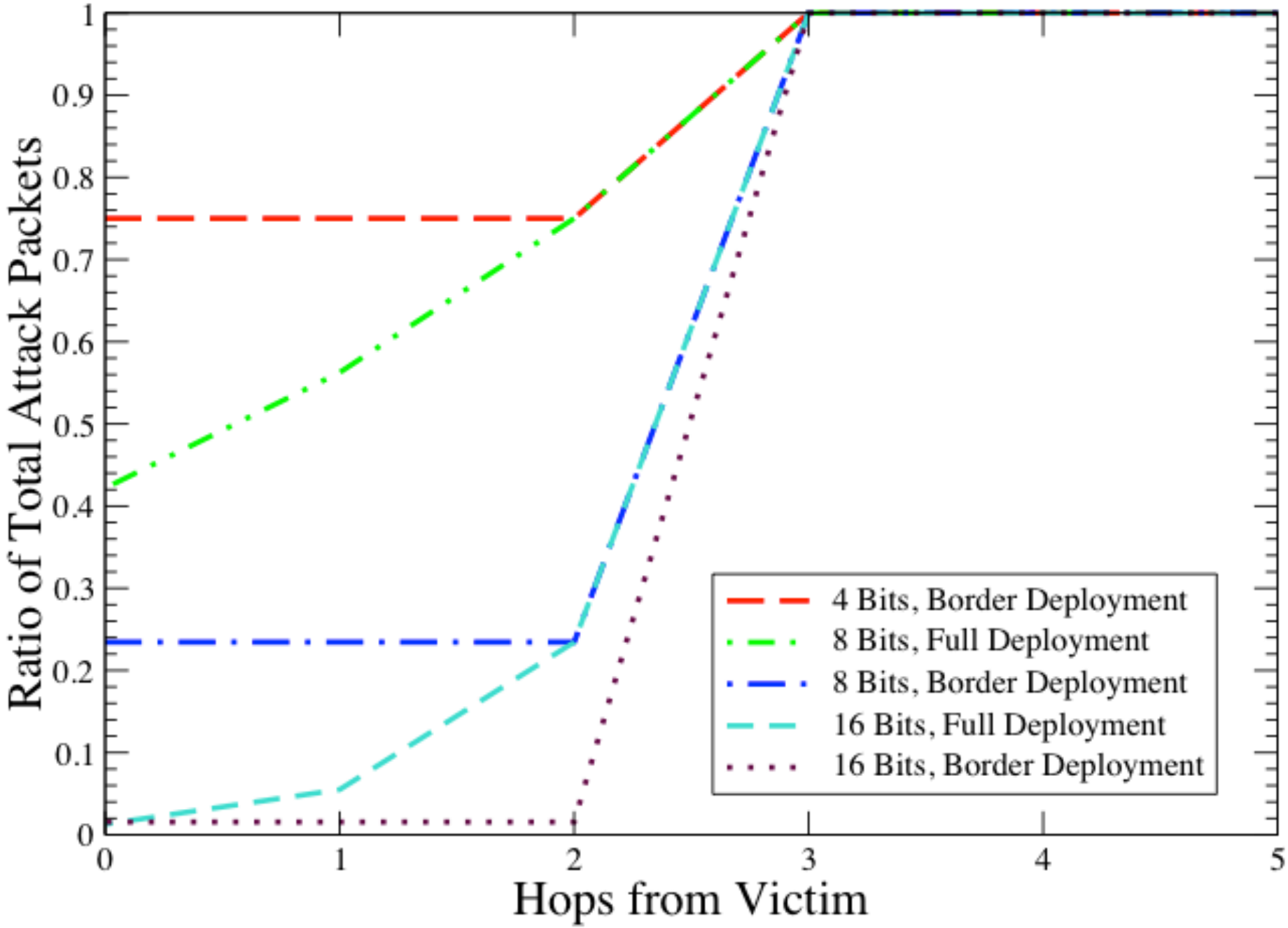
{ayaar, perrig, dawnsong}@cmu.edu

SIFF: A Stateless Internet Flow Filter to Mitigate DDoS Flooding Attacks*

Abraham Yaar Adrian Perrig Dawn Song

Carnegie Mellon University

{ayaar, perrig, dawnsong}@cmu.edu


Ratio of Total Attack Packets
Hops from Victim
0
0.1
0.2
0.3
0.4
0.5
0.6
0.7
0.8
0.9
1
0
1
2
3
4
5
4 Bits, Border Deployment
8 Bits, Full Deployment
8 Bits, Border Deployment
16 Bits, Full Deployment
16 Bits, Border Deployment

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

$$\begin{aligned} &P(\text{ connect after k tries}) \\ &\quad = 1 - (1 - P(\text{connect after 1 try}))^k \\ &\quad = 1 - (1 - (1 - \epsilon_i)^i)^k \end{aligned}$$

the required number of connection attempts is:

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

A nice feature of this formula is that the expected number of connection attempts depends logarithmically on the connection probability, which indicates that even for large ϵ_i, a determined client can get a connection after a moderate waiting time.