Broadcast authentication

$$\mathrm{Po}(k;\lambda) = \frac{\lambda^k}{k!}e^{-\lambda}$$

C. Gunter, S. Khanna, K. Tan, S. S. Venkatesh (2004)

Broadcast authentication

$$\mathrm{Po}(k;\lambda) = \frac{\lambda^k}{k!}e^{-\lambda}$$

C. Gunter, S. Khanna, K. Tan, S. S. Venkatesh (2004)

- Cryptographic protection
  - Provides guarantees of confidentiality and integrity of information.
  - Cost: but it is computationally intensive.

Broadcast authentication

$$\mathrm{Po}(k;\lambda) = \frac{\lambda^k}{k!}e^{-\lambda}$$

C. Gunter, S. Khanna, K. Tan, S. S. Venkatesh (2004)

- Cryptographic protection
  - Provides guarantees of confidentiality and integrity of information.
  - Cost: but it is computationally intensive.
- An opportunity for a Denial of Service (DoS) attack: overwhelm the server with a flood of spurious signature packets.

Broadcast authentication

$$\mathrm{Po}(k;\lambda) = \frac{\lambda^k}{k!}e^{-\lambda}$$

C. Gunter, S. Khanna, K. Tan, S. S. Venkatesh (2004)

- Cryptographic protection
  - Provides guarantees of confidentiality and integrity of information.
  - Cost: but it is computationally intensive.

- An opportunity for a Denial of Service (DoS) attack: overwhelm the server with a flood of spurious signature packets.

- Randomised selective authentication: The case for the defence — exploit the mismatch in the needs of the attacker and the client.
  - The attacker's need: have the receiver examine the vast majority of the spurious packets. Defang the attack by having the receiver randomly rejects a fraction $1 - p$ of incoming packets. [Reject rate determined by the spare computational capacity at the receiver and the maximum attack rate. For example, if $p = 0.1$ then only ten percent of the attack gets through.]
  - The sender's need: have one signed packet validated by the receiver. Sender sends n copies of her cryptographically signed packet. The probability that at least one signed packet is verified is approximately $1 - \mathrm{Po}(0; \lambda) = 1 - e^{-\lambda}$ where $\lambda = np$ is the Poisson parameter. [If $p = 0.1$ and $n = 25$ there is a 92% chance that a signed packet makes it through the blockade; if $n = 40$ the chance jumps to 98%.]