

# Redes de Comunicación

Es importante proteger las comunicaciones para que no quede rastro de las comunicaciones. A nivel de aplicación puede ser necesario reforzar el sistema. Se le debe permitir a un usuario acceder a una red sin revelar su identidad. El problema de estos sistemas es que si accede algún mal actor no es posible identificarlo.

## Anonimidad

Supone no ser capaz de distinguir a una persona dentro de un conjunto de personas.

## Unobservabilidad

Un objeto de interés no es distinguible de otros elementos de interés

## Pseudonimidad

El estado de usar un pseudónimo como identificador

## Tipos de ataques en redes de comunicación

- Tipo 1 Pasivo: Se pueden observar los enlaces de comunicación
- Tipo 2 Atacante pasivo con capacidades de envío: Un observador que puede inyectar paquetería
- Tipo 3 atacante activo: Puede controlar enlaces de comunicación, eliminar paquetes, enviar o retrasar otros paquetes.

## Requerimientos para la anonimidad en redes de comunicación

- Tráfico cubierto: Se añade tráfico adicional a la red para enmascarar una transmisión, funciona siempre y cuando el atacante no controle la red
- Efectividad. No se deben meter más de cierta cantidad de mensajes ya que se puede volver completamente ineficiente la comunicación.  $K/N$  nos dice cuanta paquetería es buena de verdad. Si  $K/N=1$  Entonces es completamente eficiente, todos los paquetes son reales y no hay

ningún dummy.

- Si hay nodos comprometidos, tiene que haber al menos uno honesto, siendo lo más recomendable un mínimo de 2.

## Redes Mix

From:

<https://www.knoppia.net/> - **Knoppia**

Permanent link:

<https://www.knoppia.net/doku.php?id=pan:niideaxd&rev=1731515732>

Last update: **2024/11/13 16:35**

