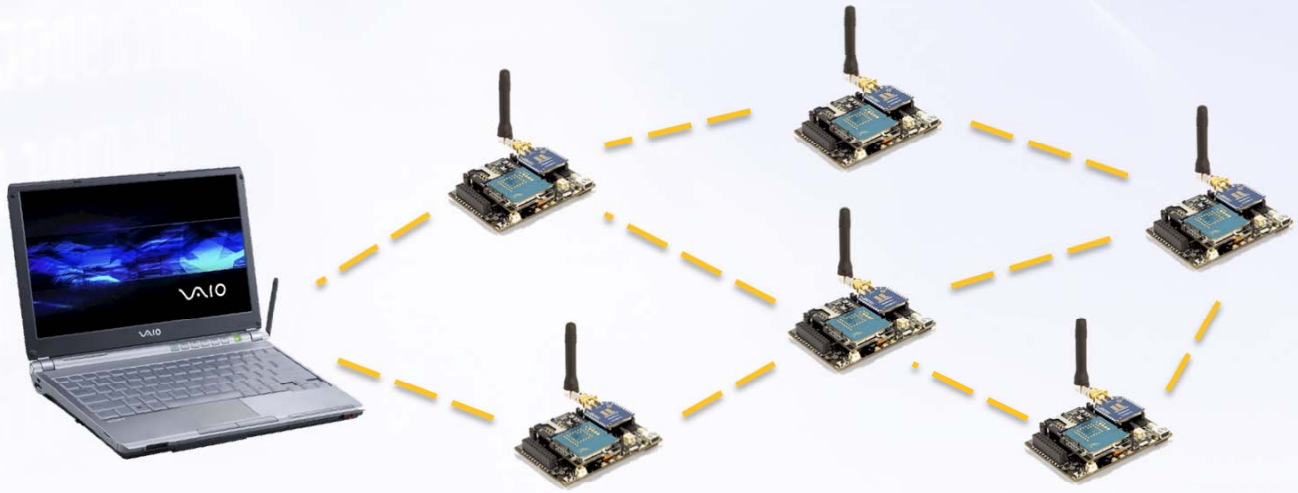
Adecuación de soluciones de anonimato a la privacidad de localización en WSN

Ruben Rios, Javier Lopez
NICS Lab – University of Málaga
http://www.nics.uma.es

Introducción

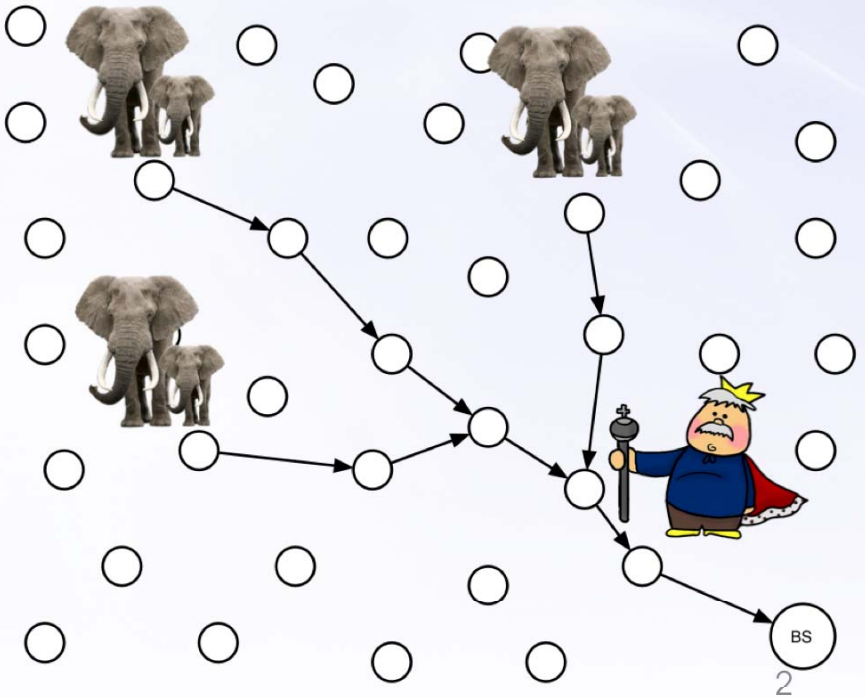
- Las redes de sensores (WSN) son redes ad hoc:
  - Nodos sensores: dispositivos de recursos limitados alimentados por baterías
    - miden fenómenos físicos
    - se comunican con nodos cercanos de manera inalámbrica
    - son capaces de encaminar paquetes
  - Estación base: receptor de información
    - recoge y analiza la información recogida por los sensores
    - interfaz de comunicación con la red y exterior



Introducción

- Las soluciones para WSN están diseñadas para maximizar el tiempo de vida de la red
  - Los datos se envían por el camino más corto a la estación base

- La observación de los patrones de tráfico revela la ubicación de los nodos que se comunican
  - Origen de mensajes
  - Ubicación de estación base



Introducción

- Los sistemas de comunicación anónima (ACS) tradicionales tienen como objetivo ocultar los patrones de tráfico

- Objetivo:

  ¿Son aplicables los ACS al problema de la privacidad de localización en WSN?

Origen del problema

- Las WSN presentan características originales que difieren de las redes convencionales
  - Restricciones HW
  - Naturaleza desatendida
  - Proximidad nodos
  - Transmisiones inalámbricas
  - Flujo de datos muchos-a-uno
  - Información en tiempo real

Gama	CPU	RAM	ROM	Energía
Baja	4 MHz	1 KB	4-16 KB	1.5 mA
Media	4-8 MHz	4-10 KB	48-128 KB	2-8 mA
Alta	13-180 MHz	256-512 KB	4-32 MB	40 mA

Modelos de Atacante

- Los atacantes se limitan a realizar análisis del tráfico y no interrumpen activamente a las comunicaciones

- Atacantes internos
  - Visión local
  - Acceso al contenido de paquetes

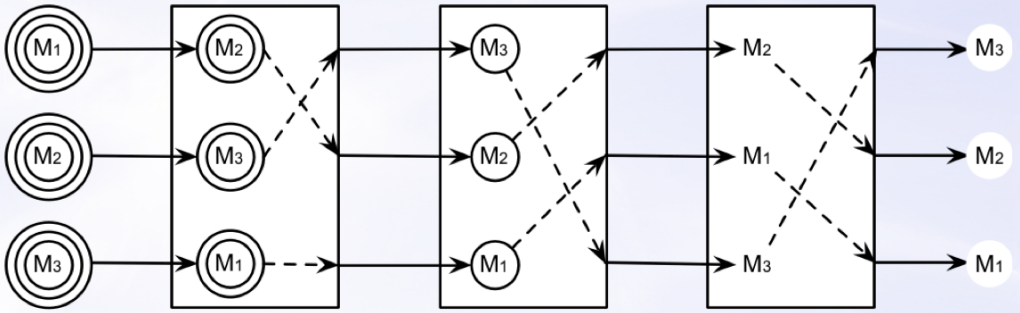
- Atacantes externos
  - Visión local o global
  - No acceso al contenido de paquetes
  - Capacidad de movimiento según
    - Ángulo de llegada señales
    - Número de paquetes
    - Correlación de tiempos

NICS

Onion Routing

- Sistema centralizado formado por un conjunto de dispositivos situado entre emisores y receptores

- Onion routers
  - Pequeños retrasos
  - Capas de criptografía simétrica
  - Establecimiento de circuitos



- El objetivo principal es proteger la relación entre emisores y receptores (unlinkability)

Onion Routing

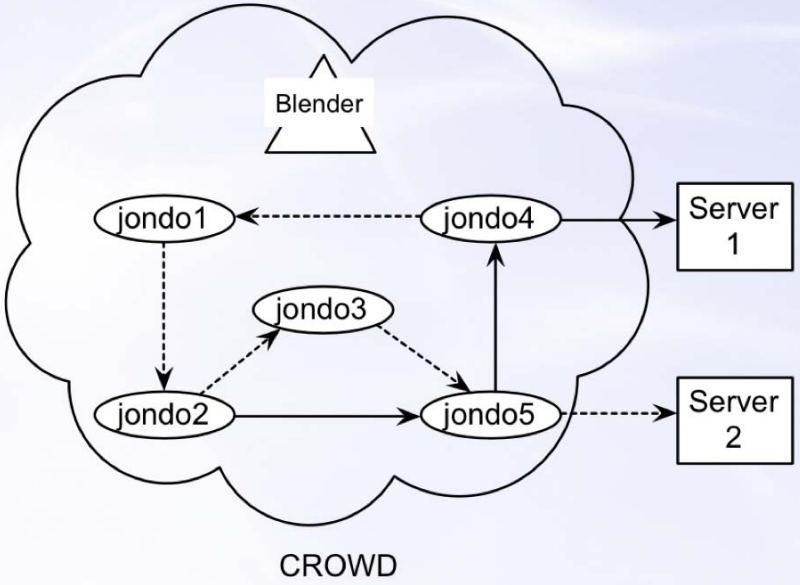
- Computacionales
  - Principalmente recaen en nodos fuente
    - Realizar 1 cifrado por cada nodo intermedio
    - Visión global de red para el establecimiento de circuitos
    - Acceso y almacenamiento de públicas y de circuito

- Funcionales
  - La propiedad de unlinkability no impide la detección
  - Los observadores globales consiguen su objetivo
  - Los puntos de entrada y salida son críticos
  - Protección frente a atacantes

Crowds

- Sistema descentralizado en el que los participantes colaboran para mantener el anonimato de sus miembros

- Sistema basado en
  - Establecimiento aleatorio de caminos
  - Renombrado de cabeceras
  - Criptografía simétrica



- El objetivo principal es ocultar la identidad del emisor al receptor (anonimato)

Crowds

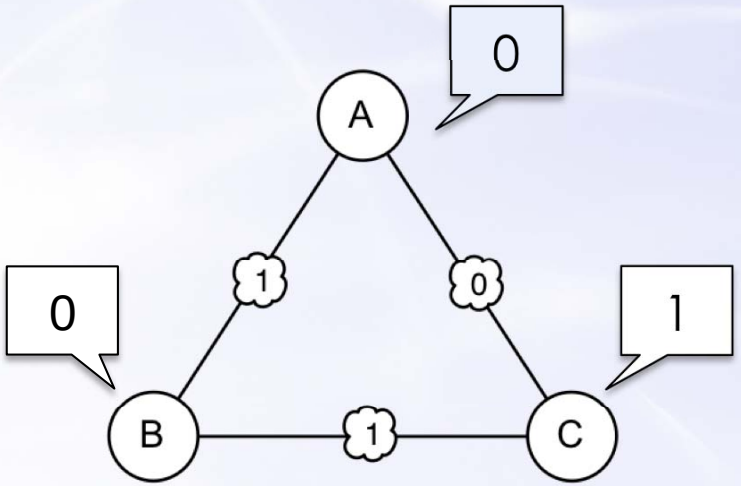
- El modelo Crowds tiene unos requisitos asequibles
  - Descifrado y cifrado simétrico
  - Almacenamiento de las claves dependiente del tamaño de la red

- Funcionales
  - El anonimato frente a la BS es contraproducente
  - No resiste un modelo de atacante móvil
  - Es vulnerable a atacantes globales

DC-nets

- Sistema descentralizado que permite a un grupo compartir información al tiempo que se oculta al emisor del mensaje

- Sistema basado en
  - Broadcasts simultáneos
  - Sumas módulo 2 (xor) de bits secretos
  - Inversiones



- El objetivo principal es ocultar el origen de datos a cualquier observador (unobservability)

DC-nets

- Coste computacional reducido con requisitos elevados de memoria
  - 3 operaciones booleanas por mensaje
  - Compartición de [2, N-1] secretos por mensaje

- Limitaciones funcionales
  - La propiedad de undetectability previene la localización
  - Fiabilidad del medio de transmisión
  - Sincronización precisa
  - Todos los participantes en el rango de transmisión
  - Soporte de comunicaciones simultáneas

Conclusión

- Los sistemas tradicionales no son aplicables a WSN

	Limitaciones	Atacante		
		Global	Local	Interno
Onion routing	↑↑↑	×	×	√
Crowds	↓	×	×	≈
DC-nets	↑↑↑	√	√	√

- Trabajo futuro
  - Abordar nuevas soluciones tradicionales
  - Aplicación sobre nodos reales
  - Nuevas soluciones específicamente diseñadas

¡Gracias!

Ruben Rios, Javier Lopez
NICS Lab – University of Málaga
http://www.nics.uma.es

NICS