Robust Probabilistic Fake Packet Injection for Receiver-Location Privacy

Ruben Rios[1], Jorge Cuellar[2], Javier Lopez[1]

[1] *NICS Lab – University of Málaga*

[2] *Siemens AG, Munich*

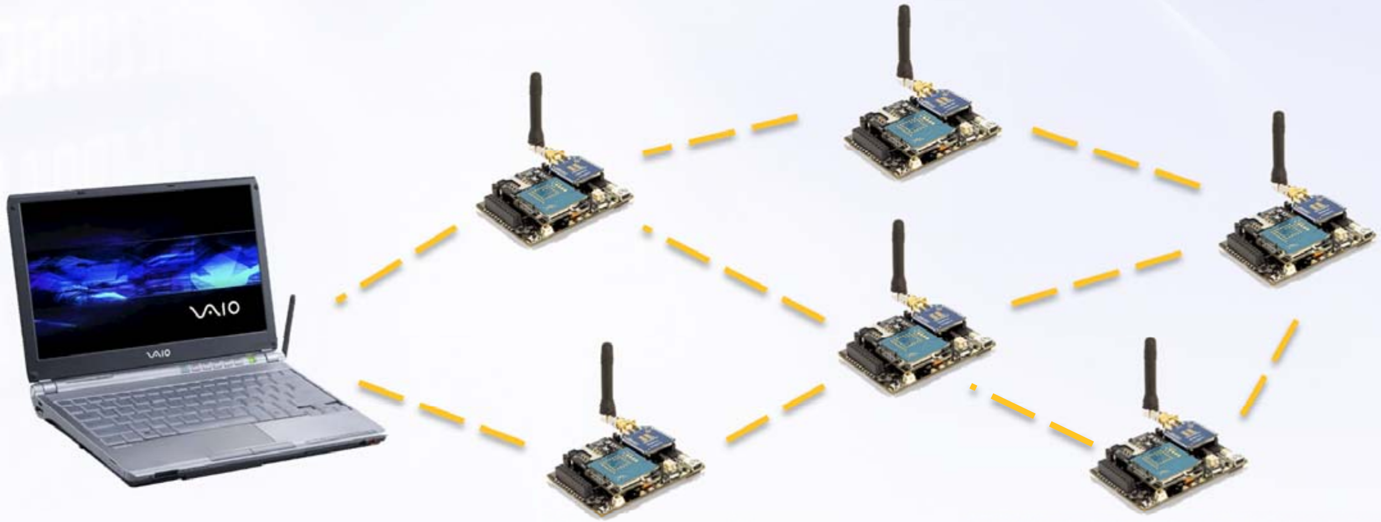
ESORICS 2012 – 10-14 Sept. Pisa (Italy)

Agenda

- Introduction
- Related Work
- Problem Statement
- Homogeneous Injection for Sink Privacy
- Protocol Analysis
- Conclusion

Introduction

- Wireless Sensor Networks (WSN) are ad hoc networks:
  - Sensor nodes: battery-powered devices with limited capabilities
    - measure physical phenomena
    - communicate with nearby nodes using radio interfaces
    - provide routing capabilities
  - Base station: resourceful data sink
    - collects and analyses all data from sensors
    - communication interface to the network



NICS

Introduction

- WSNs are used in applications where sensor nodes are unobtrusively embedded into systems:
  - Monitoring
  - Tracking
  - Collecting
  - Reporting

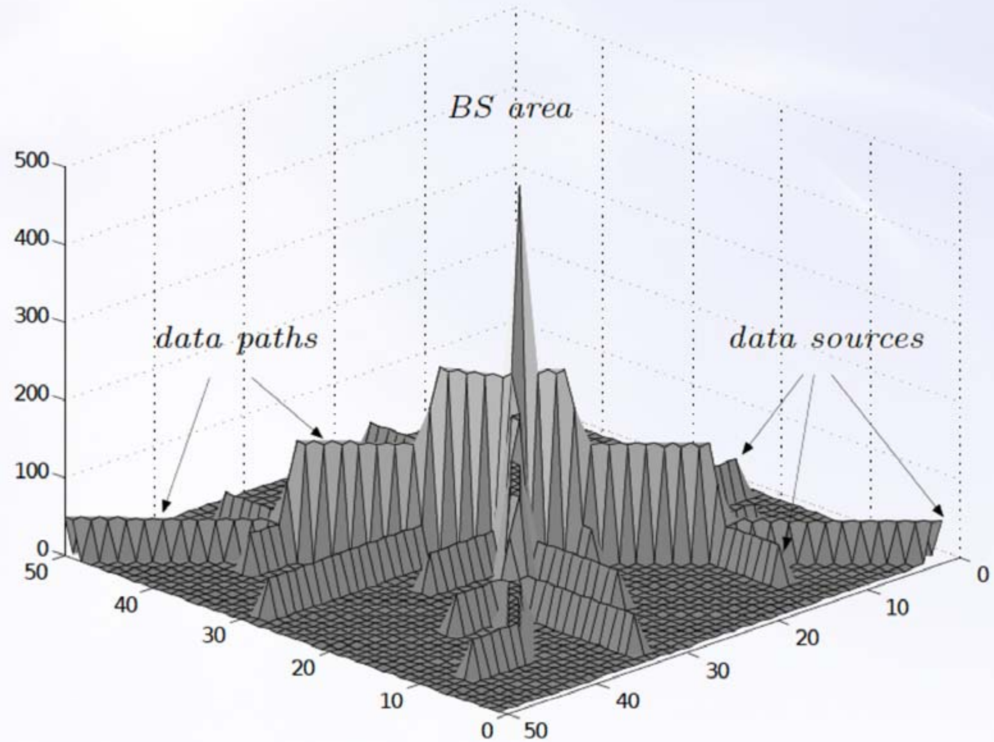
- By sectors, WSNs are used in:
  - Environmental, agriculture, farming,
  - Industrial, critical Infrastructure,
  - Logistics, retailing,
  - Home automation, smart metering, e-health,
  - Homeland security, battlefield monitoring

NICS

Introduction

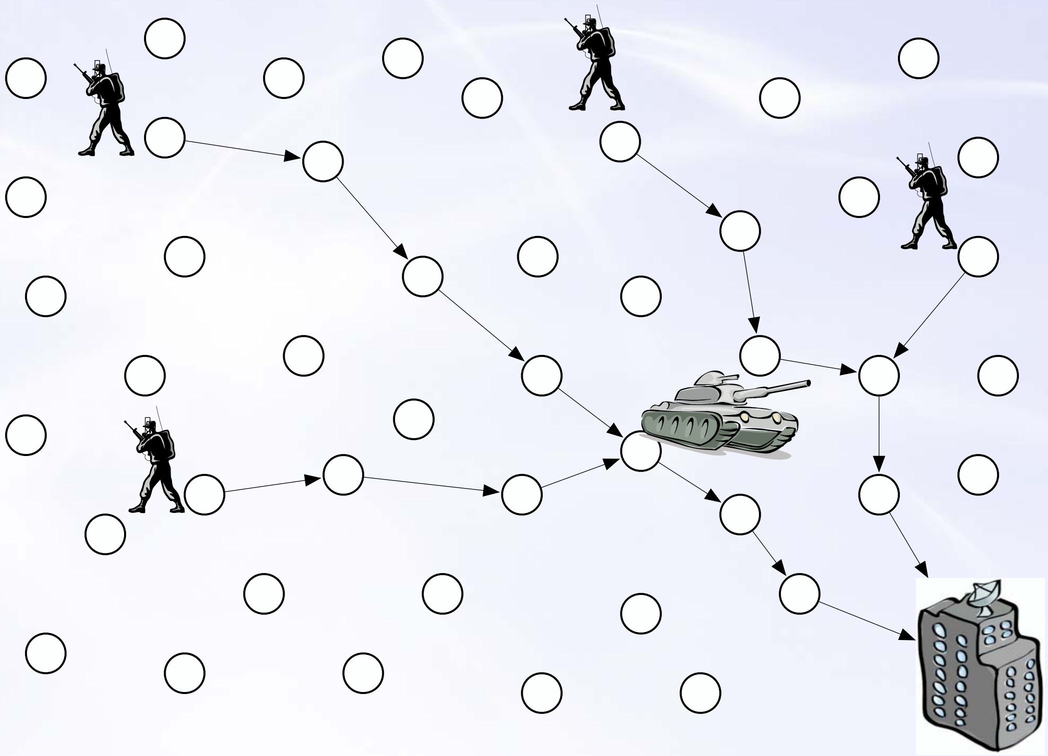
- WSN solutions are designed to maximize the lifetime of the network
  - Data is transmitted using shortest-path routing algorithms

- Routing protocols introduce pronounced traffic patterns, which reveal the location of relevant network nodes
  - Source-location privacy
  - Receiver-location privacy



Introduction

- The criticality of location privacy is evident in the following scenario



- Motivation
  - Physical protection
  - Strategic information

- These problems are extensible to any WSN scenario because they are caused by a network design

Agenda

- Introduction
- **Related Work**
- Problem Statement
- Homogeneous Injection for Sink Privacy
- Protocol Analysis
- Conclusion

NICS

Related Work

- Deng et al. (2006) proposed multi-parent routing which selects the next hop randomly from neighbours closer
  - Always in the direction of the base station
- Fractal Propagation (2006) and Malestrom (2011) create hot-stops to attract adversaries
  - Once reached they can be discarded
- Ying et al. (2011) propose to make every node transmits the same amount of traffic
  - Best protection but at the maximum cost
- Jian et al. (2008) send packets towards the sink with a biased probability and inject fake traffic in the opposite direction
  - Fake traffic is always sent in the opposite direction

NICS

Agenda

- Introduction
- Related Work
- **Problem Statement**
- Homogeneous Injection for Sink Privacy
- Protocol Analysis
- Conclusion

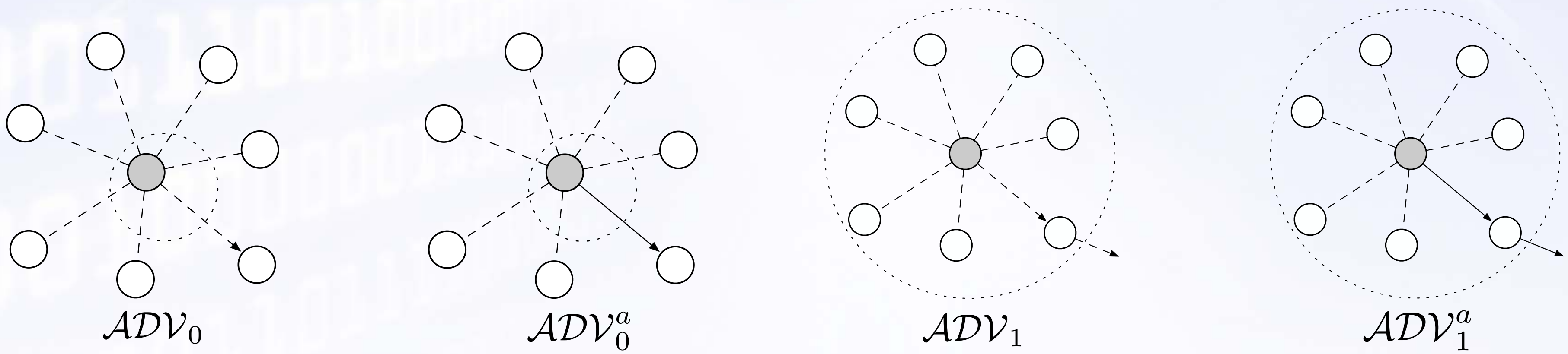
Problem Statement

- We assume a WSN with the following features
  - Sensor nodes are deployed in a vast area
  - The network consists of hundreds of sensor nodes
  - The connectivity of the network is high
  - There is a single base station
  - Event-driven monitoring application
  - Sensor nodes share keys and perform cryptographic operations
  - Real messages are indistinguishable from fake messages

NICS

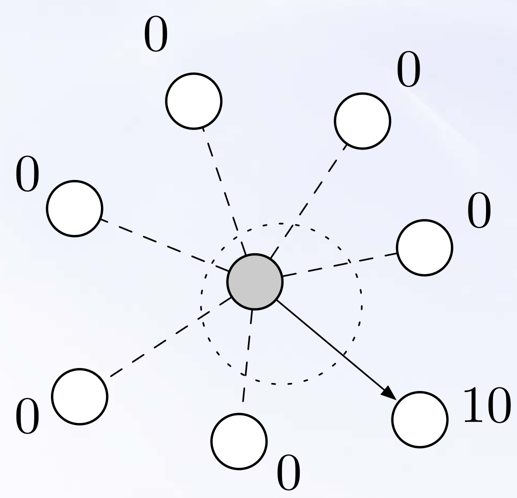
Problem Statement

- We assume the adversary
  - Has a partial view of the communications ($\mathcal{ADV}_1$)
  - Cannot decrypt data packets
  - Can determine the data sender based on features of the signal
  - Can determine the data recipient using header information or the transmission times of nodes
  - Can count the number of packets sent by a particular node
  - Moves according to a particular strategy at a reasonable speed



Problem Statement

- The movement strategy of the adversary is determined by the type of traffic analysis attack performed
  - Time-correlation attack
    - A node transmits shortly after receiving a packet
  - Rate-monitoring attack
    - Nodes closer to the base station receive more packets
    - Less efficient because it requires several observations before moving



Agenda

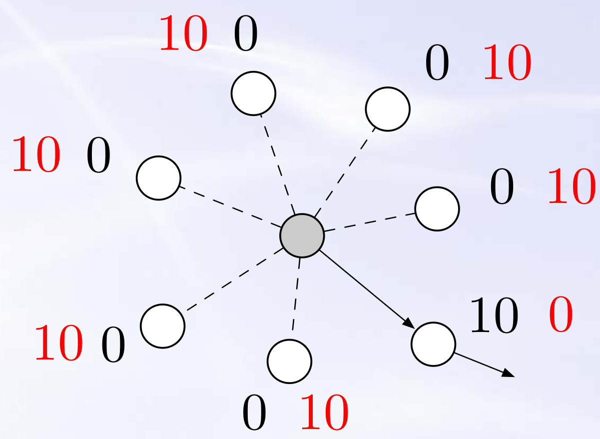
- Introduction
- Related Work
- Problem Statement
- **Homogeneous Injection for Sink Privacy**
- Protocol Analysis
- Conclusion

NICS

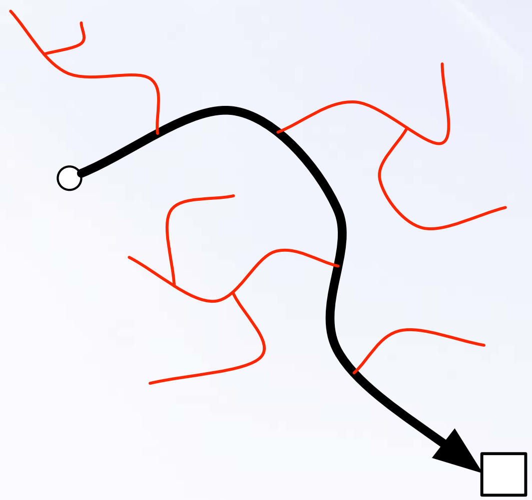
Homogeneous Injection for Sink Privacy

- The HISP idea is to locally homogenise the number of packets sent by a node to its neighbours

1. Fake traffic hides the flow of real packets
   - Two messages (real, fake)
   - Controlled by a parameter



2. Real packets are sent using a biased random walk
   - More likely to reach the BS
   - Static path + fake branches are eventually discarded by the adversary



Homogeneous Injection for Sink Privacy

- We require three properties during data transmission
  - *Prop 1:* Convergence

$$E(dist(x', BS)) < E(dist(x, BS))$$

  - *Prop 2*: Homogeneity

$$\forall y, z \in neigh(x) \quad Frec_m(x, y) \simeq Frec_m(x, z)$$

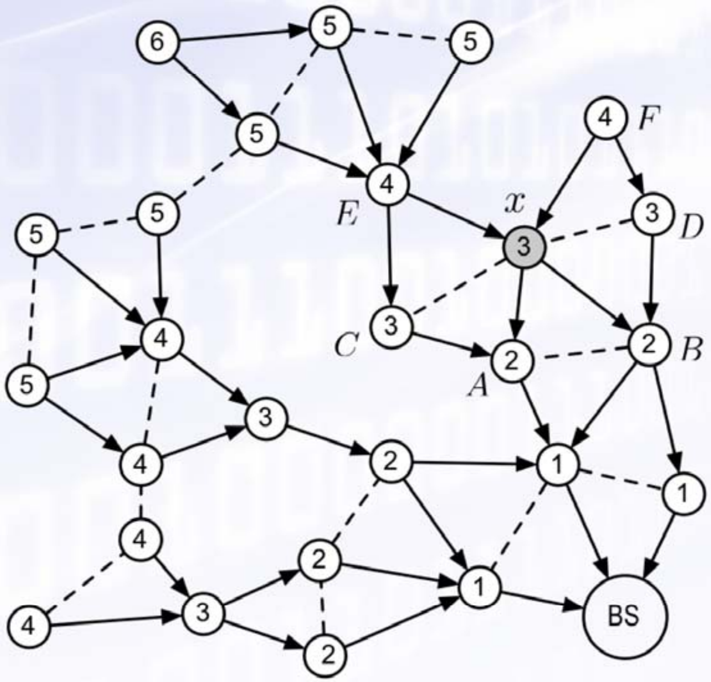
  - *Prop 3*: Exclusion

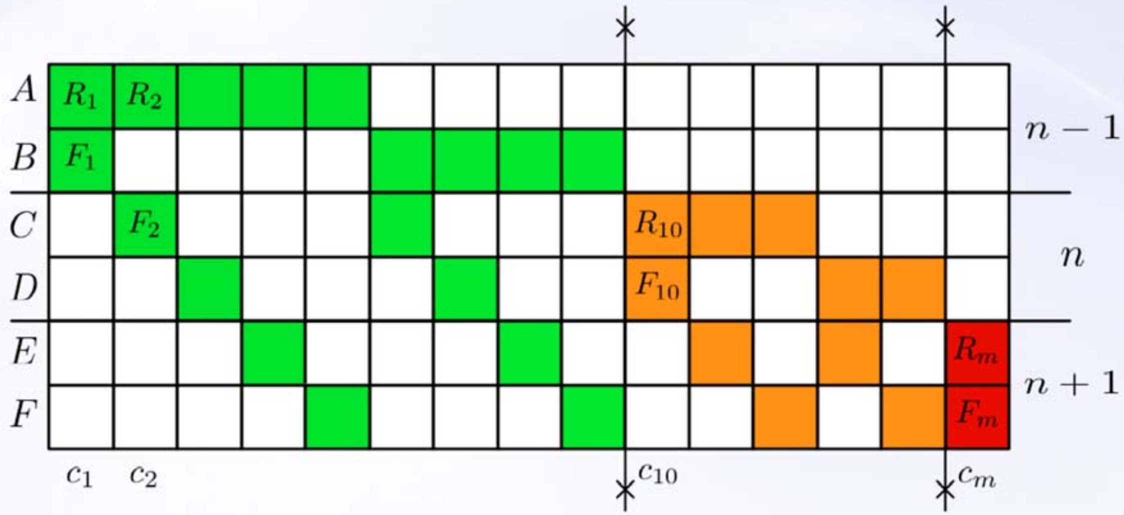
$$\forall m, m', x, y, t \quad send(m, x, y, t) \wedge m \neq m' \\ \Rightarrow \neg send(m', x, y, t)$$

NICS

Homogeneous Injection for Sink Privacy

- A computationally inexpensive approach ensures the previous properties
  - Sorted combinations without repetition of two neighbours
  - Select one of the combinations randomly





Homogeneous Injection for Sink Privacy

- The proposed algorithm introduces a network parameter to control the amount of fake traffic
  - Depends on the hearing range of the adversary

Algorithm 1 Transmission strategy

Input: $packet \leftarrow receive()$
Input: $combs \leftarrow combinations(sort(neighs), 2)$
Input: MAX_TTL

$\{neigh1, neigh2\} \leftarrow select\_random(combs)$
if $isreal(packet)$ **then**
    $send\_random(neigh1, packet, neigh2, fake(MAX\_TTL))$
else
    $TTL \leftarrow get\_time\_to\_live(packet) - 1$
    if $TTL > 0$ **then**
        $send\_random(neigh1, fake(TTL), neigh2, fake(TTL))$
    end if
end if

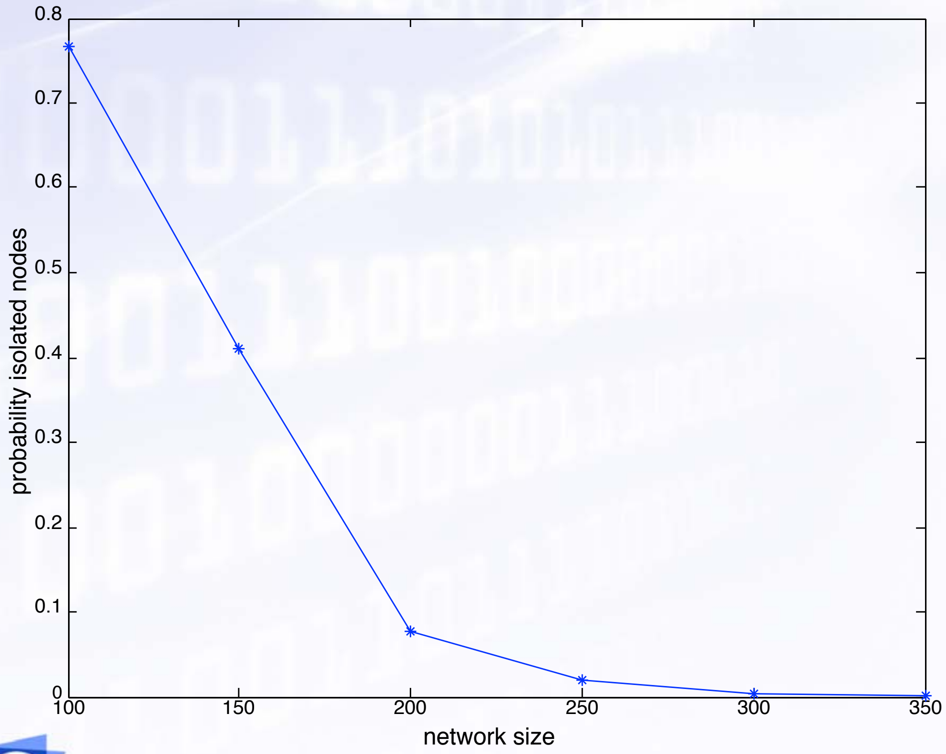
Agenda

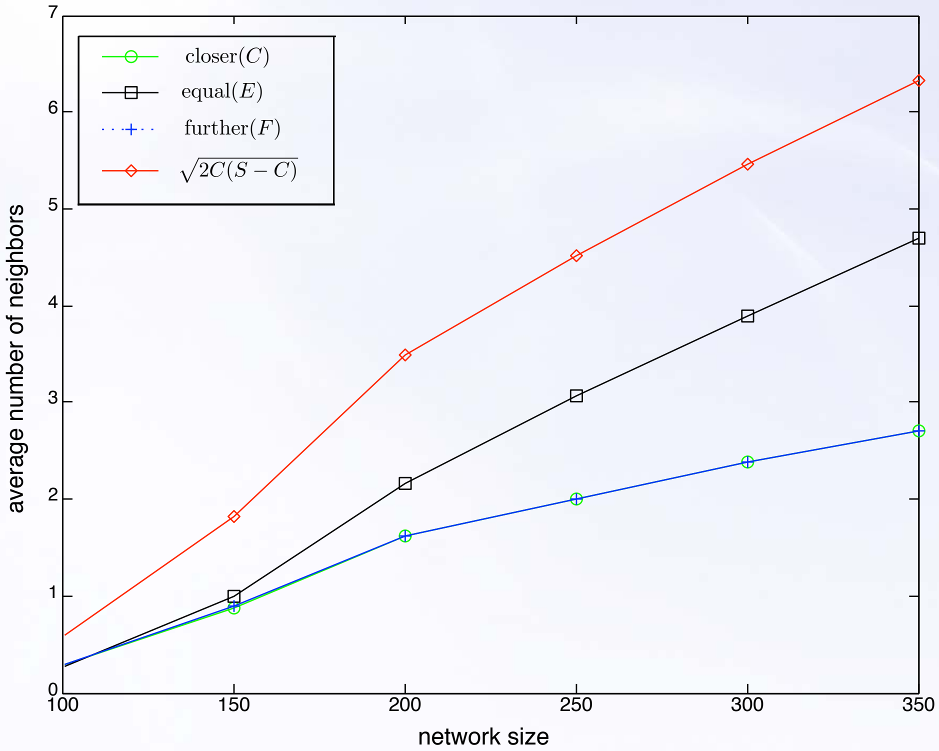
- Introduction
- Related Work
- Problem Statement
- Homogeneous Injection for Sink Privacy
- **Protocol Analysis**
- Conclusion

Analysis of Potential Limitations

- The topology of the network might negatively impact the convergence of real packets
  - Theorem: Real messages reach the base station if $F < \sqrt{2C(S-C)}$

- Validation on randomly deployed networks





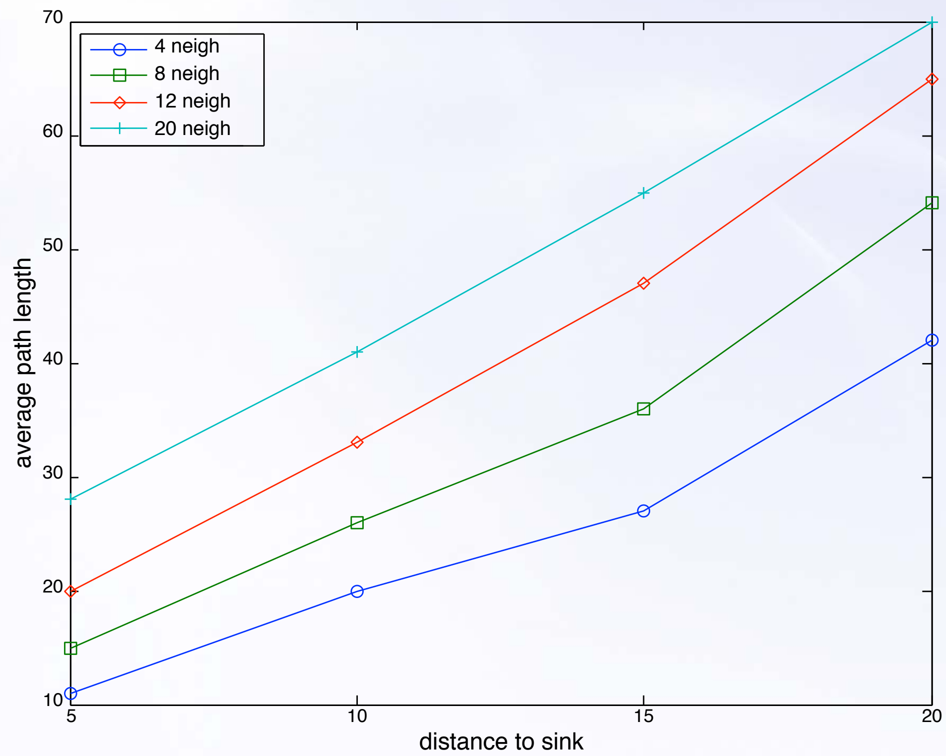
Analysis of Potential Limitations

- Message delivery time is affected by the probabilistic nature of the protocol

$$x_n = 1 + px_{n-1} + qx_n + rx_{n+1}$$

- The values of *p,q,r* might differ for each node due to the network configuration

- The speed decreases as the packet approaches the sink

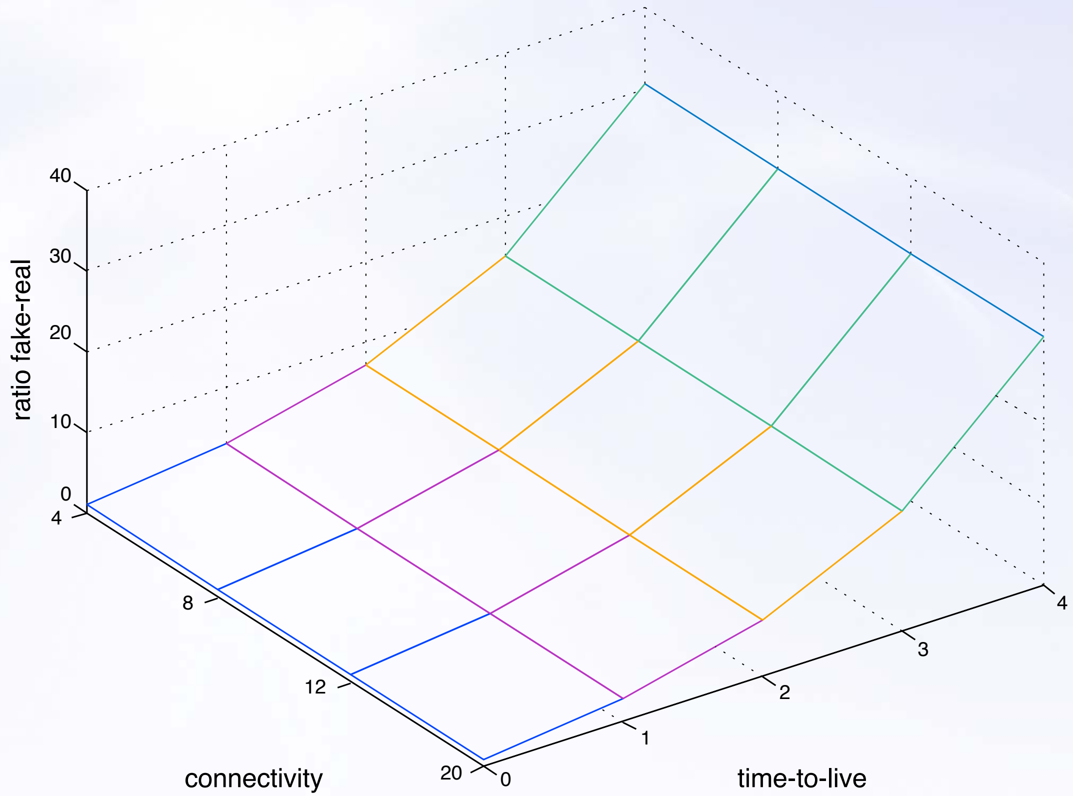


Analysis of Potential Limitations

- The use of fake traffic impacts the lifetime of the network

- The durability of fake traffic is controlled by a parameter, *MAX_TTL*, which is dependent on the hearing range of the adversary ($\mathcal{ADV}_n$)

- Ratio $\mathcal{O}(2^{n+1})$ can be reduced by half



Analysis of Potential Limitations

- We analyse the privacy protection against a local adversary

- Time-correlation
  - Packets flow in any direction
  - Fake and real packets are indistinguishable

- Rate-monitoring
  - Evenly distributes packets among neighbours
  - Random walk blurs the band of fake messages

Agenda

- Introduction
- Related Work
- Problem Statement
- Homogeneous Injection for Sink Privacy
- Protocol Analysis
- **Conclusion**

NICS

Conclusion

- We present a new receiver-location privacy solution called HISP based on fake traffic and biased random walks
- HISP has been validated analytically and experimentally
- Future work
  - Reduce fake traffic
  - More powerful adversaries
  - Node compromise attacks
  - Topology discovery process

Thanks for your attention!

Ruben Rios[1], Jorge Cuellar[2], Javier Lopez[1]

[1]NICS Lab – University of Málaga

[2]Siemens AG, Munich