PARIS: Privacy Augmented Relaying of Information from Sensors

WINLAB WIRELESS INFORMATION NETWORK LABORATORY

Pandurang Kamat, Yanyong Zhang and Wade Trappe

Privacy Issues in Sensor Networks

Content-oriented privacy

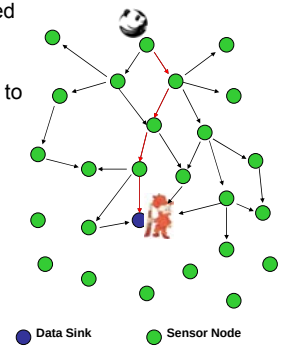
- Issues that arise because an adversary can observe and manipulate the content of the messages in the network.
- Best addressed through cryptography and network security.

Contextual privacy

- Issues that arise because an adversary observes the **context** surrounding creation and transmission of a sensor message.
- Source-Location Privacy: The physical location of communication participants may be sensitive.
- Temporal Privacy: Temporal information corresponding to the creation of message might be sensitive.
- Traffic Privacy: The size and number of messages originating from a sensor may be sensitive.

A generic asset monitoring sensor network

- Consider a sensor network deployed to monitor a panda habitat.
- Sensors periodically send Panda_Here messages, forwarded to sink.
- The hunter observes packets and traces his way back to the panda.
- Messages may be encrypted to protect the content.
- The headers may be in plaintext to avoid cost of hop-by-hop decryption/encryption
- Privacy Goal: Make it difficult for Hunter to track down the panda.
- Longer tracking time means stronger privacy.



Formal Model for Source-Location Privacy

Asset monitoring network is a 6 tuple : (*N, S, A, R, H, M*)

- N = network of sensor nodes
- S = Sink to which all messages are routed to
- A = The asset being monitored
- R = The routing strategy used by sensors
- H = The hunter or adversary whose movements are governed by a set of rules M.

Safety period

Number of new messages initiated by the source node(s) monitoring the asset before the adversary captures the asset (if at all)

Likelihood of capture

The likelihood that the adversary will trace the asset successfully in a given period of time.

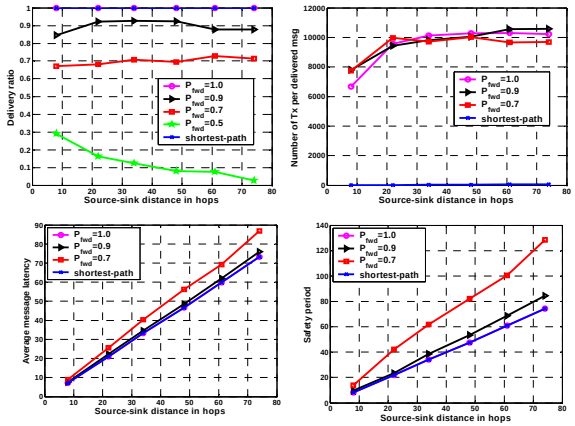
Baseline routing techniques

Shortest Path routing

- Single path routing with minimum number of hops to sink or highest gradient as criteria.
- Minimum amount of network energy expended
- Minimum message delivery latency
- Worst safety period !!

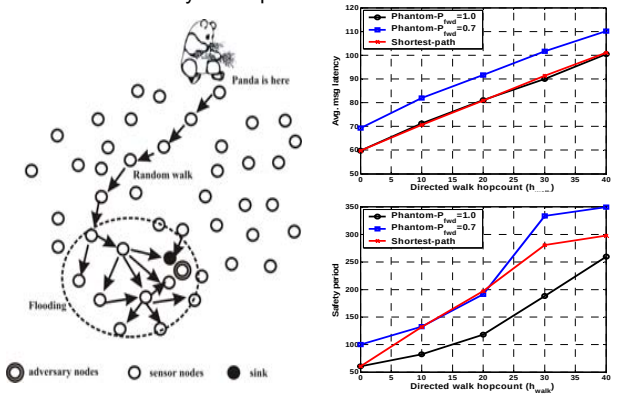
Probabilistic flooding

- Each node forwards a received sensor packet with probability $P_{forward}$ to all its neighbors, the first time it receives it.
- Small $P_{forward}$ means reduced energy consumption but also means lower network reacheability, lower message delivery ratio and higher delivery latency.

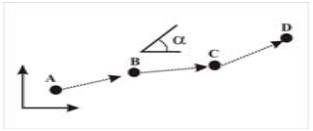


Phantom Routing

- The source message is sent out on a **directed random walk** for "h" hops before being flooded or sent down to shortest path. Thus a **phantom source** is created for every "new" message that's sent out.
- Combines the best of flooding and shortest path strategies but without any of the problems.



Moving Target Scenario



Source-Sink separation 48 hops

∂ = time interval after which the target moves

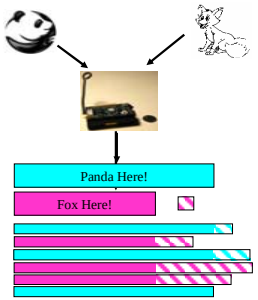
T = time interval after which new source msgs originate

Slower target speed means larger value of ∂ /T.

Routing Techniques	∂/ T = 2		∂/ T = 6		∂/ T = 18	
	L	Φ	L	Φ	L	Φ
Flooding	1.0	54	1.0	50	1.0	47
Phantom-flooding	1.0	92	1.0	75	1.0	78
Single-path	0.43	51	0.80	50	1.0	51
Phantom-single	0.40	134	0.67	169	1.0	107

Future Direction: Traffic Privacy

- Sensor networks may report different types of data
- **Contextual Privacy Issue:** An adversary may correlate packet size and traffic with the type of data
- Example: Pandas and Foxes
- Need to vary **what** you send
- Traffic Shaping :
  - Uniform Message Size
  - Randomized Message Size
  - Privacy-Preserving Source Coding



Future Direction: Temporal Privacy

- Sensor networks may store, aggregate and forward data.
- **Contextual Privacy Issue:** An adversary may infer time-of-creation context by observing and correlating traffic.
- Forwarding delay also translates into source-location ambiguity
- Need to change **when** you send/route/forward.
  - Delay at the source
  - Random delay in routing