Trusted Routing in IoT

Dr Ivana Tomić

Research Associate

Imperial College London

Email: i.tomic@imperial.ac.uk

In collaboration with:

Prof. Julie A. McCann and

AESE group

Outline

- ❑ Sensors and Sensor Networks – Are these the most Critical Components in IoT?
- ❑ What is the Security & Cyber Risk in IoT?
- ❑ How big is the Loss of Data due to the Break in Routing Paths?
- ❑ How to establish a Trusted Routing in IoT?

Sensors and networks: A value-creation framework

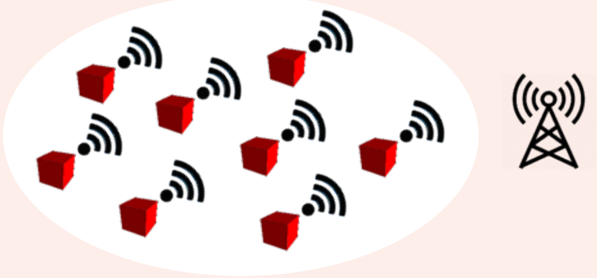
Sources of information

❑ A heavy reliance on **wireless communications** (typically a best-effort network).

❑ A range of **communication protocols** to satisfy the communication needs of diverse applications.

Wireless Sensor Network

many low-cost, low-power devices communicating wirelessly with BS

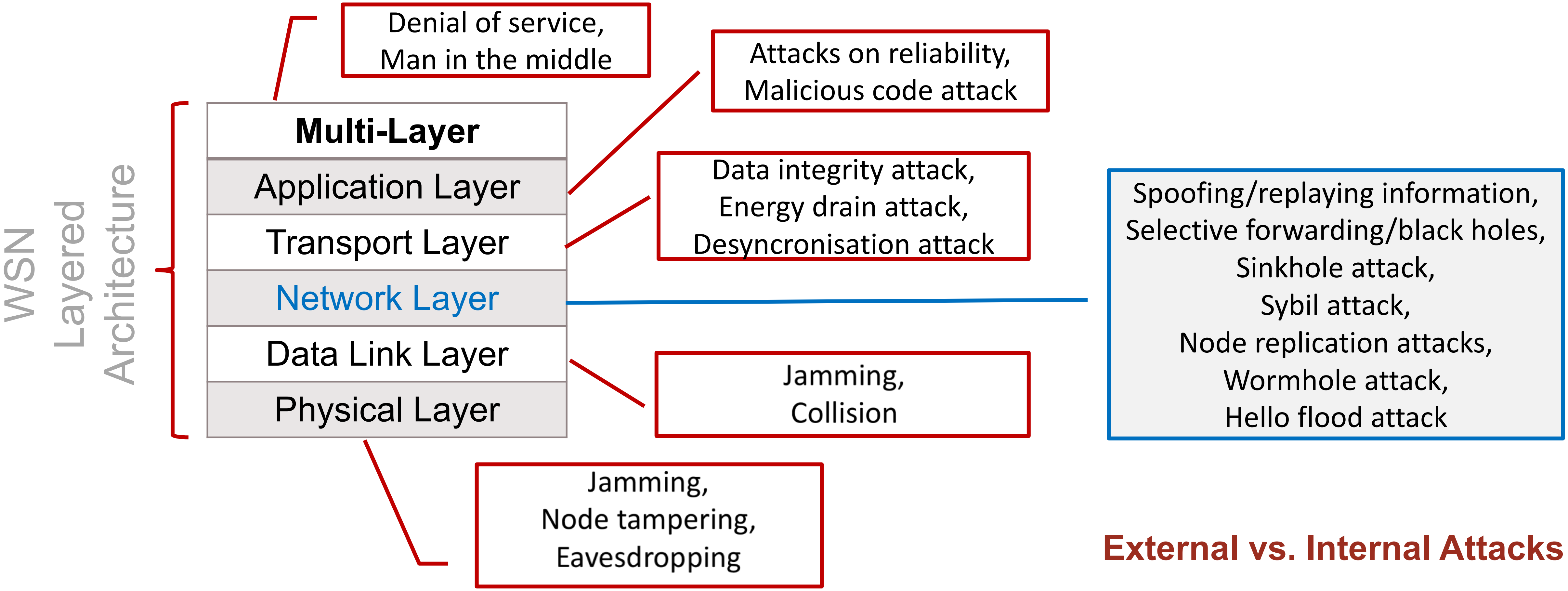


IoT systems differ from traditional IT systems?

- ❑ **Environment:** physical exposure of IoT devices
- ❑ **Resources:** sensors are low-cost, low-power, resource constrained devices
- ❑ **Variety:** more types of devices and different types of networks in IoT
- ❑ **Volume:** billions of IoT devices compared to millions of IT devices
- ❑ **Consequences:** disruption of IoT systems could lead to large economic losses and have a significant impact on the welfare of people

BUT it also creates new opportunities for all that information to be compromised!

The communication protocols have not been designed with a security goal in mind



WSN Layered Architecture

Multi-Layer

Application Layer

Transport Layer

Network Layer

Data Link Layer

Physical Layer

Denial of service,
Man in the middle

Attacks on reliability,
Malicious code attack

Data integrity attack,
Energy drain attack,
Desyncronisation attack

Spoofing/replaying information,
Selective forwarding/black holes,
Sinkhole attack,
Sybil attack,
Node replication attacks,
Wormhole attack,
Hello flood attack

Jamming,
Collision

Jamming,
Node tampering,
Eavesdropping

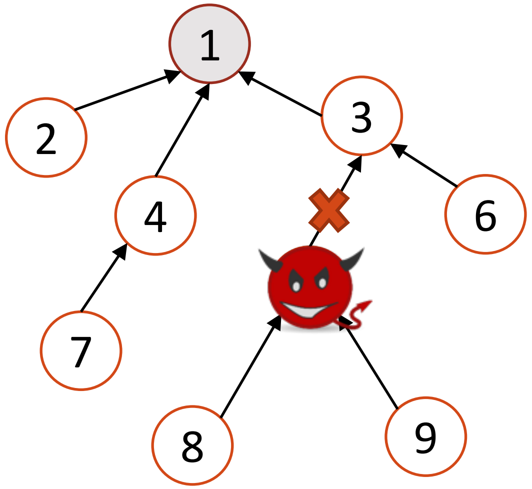
External vs. Internal Attacks

The network level attacks can cause data loss and increase the data collection latency

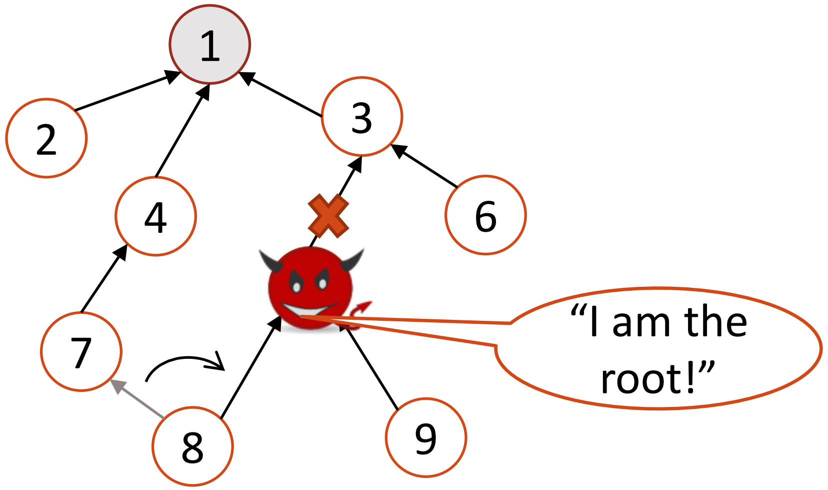
Network communication can be attacked, causing the **loss of data** which can compromise system functionality and cause failure.

?

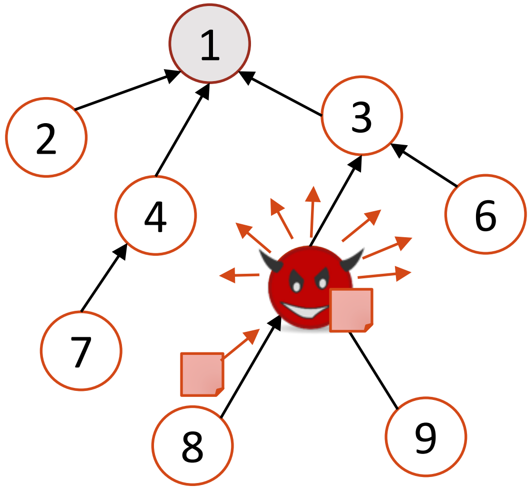
SENSITIVE DATA!
TIME-CRITICAL DATA!



Blackhole attack



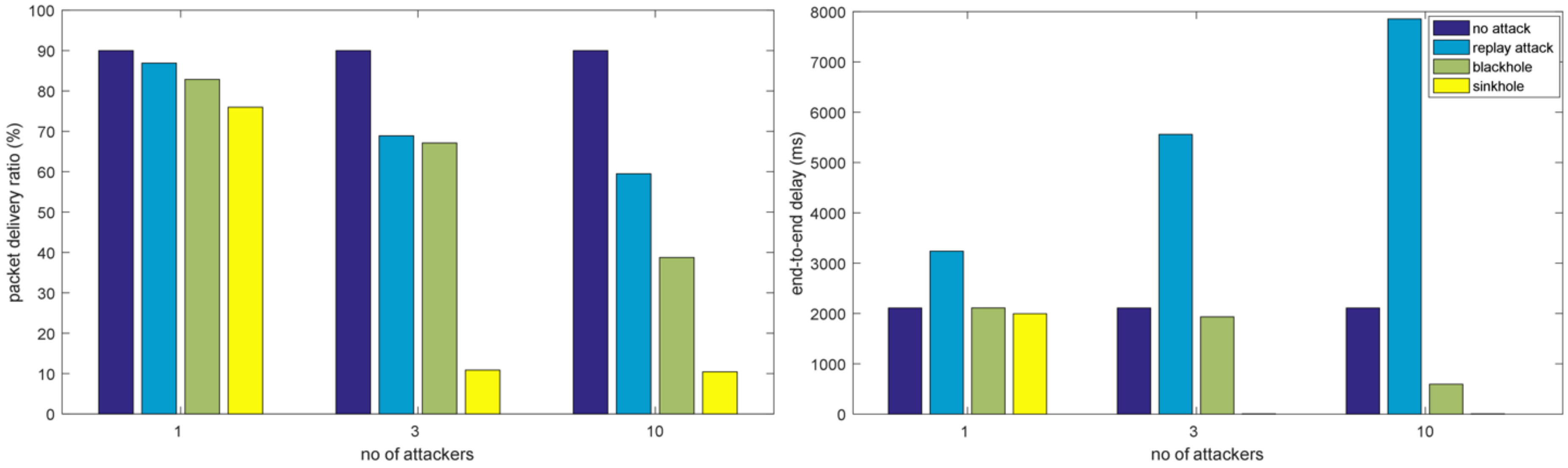
Sinkhole attack



Replay attack

I. Tomić, J. A. McCann. “Trusted Routing In IoT"

Understanding the impact and consequences of an attack helps to prevent possible DoS

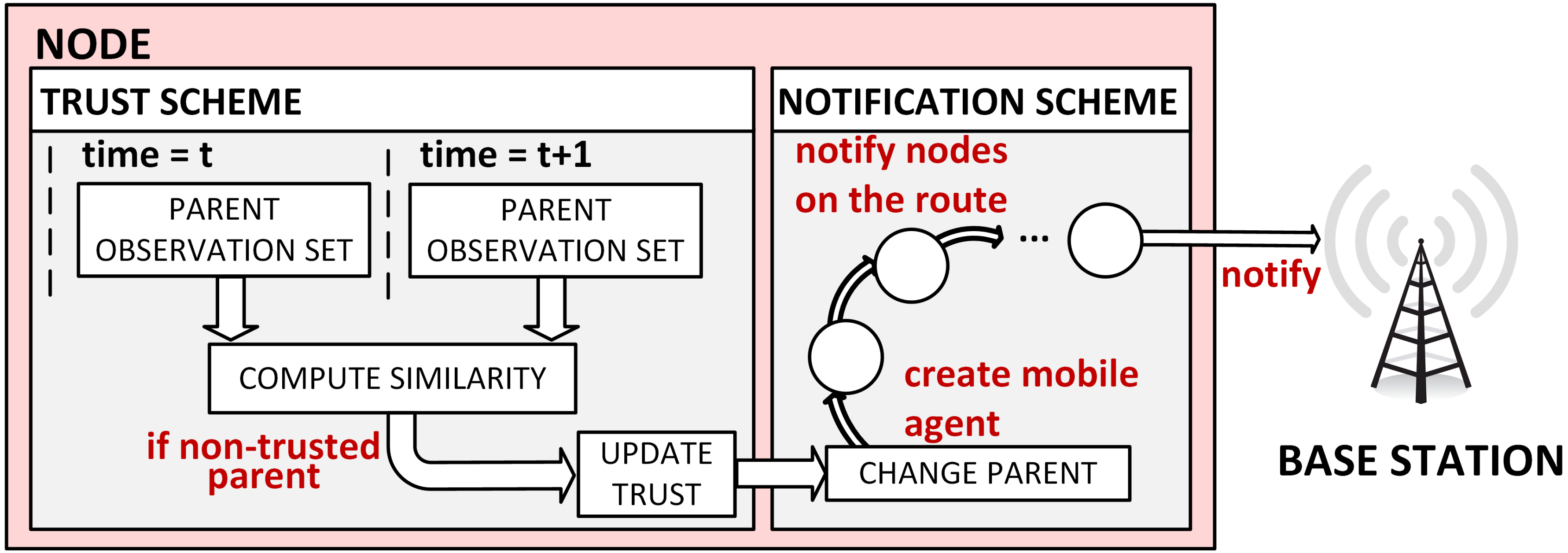


Implementation: Contiki OS & Cooja (Contiki simulator), 100nodes random topology

Observations:

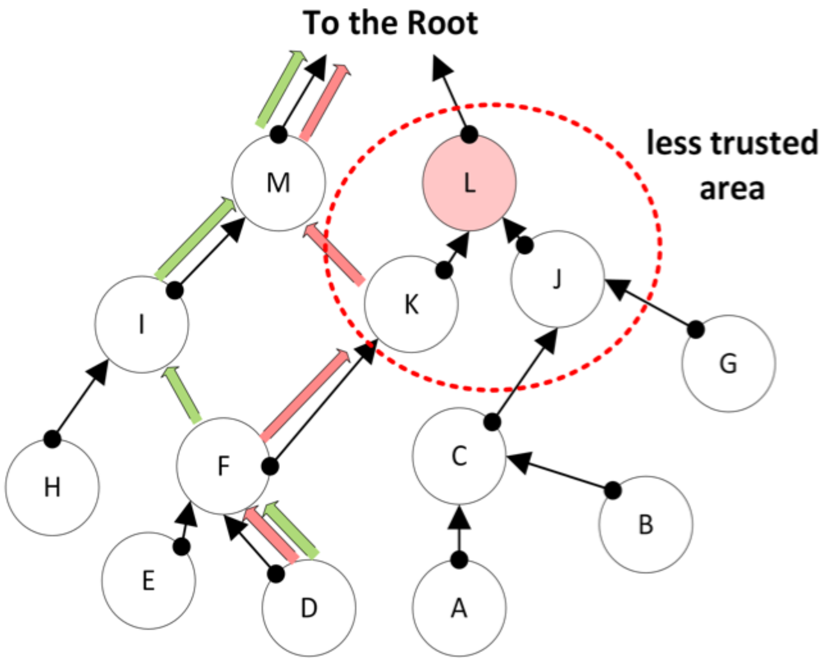
- Each attack has it’s own signature wrt to the network performance.
- Two groups: 1. attacks that introduce additional data → reduced PDR and increased E2E delay 2. attacks that reduce no. of packets → reduced PDR and reduced E2E delay.

A novel self-healing scheme that detects and recovers from common attack scenarios



Each sensor builds a trust model of its neighbourhood to adapt routing decisions

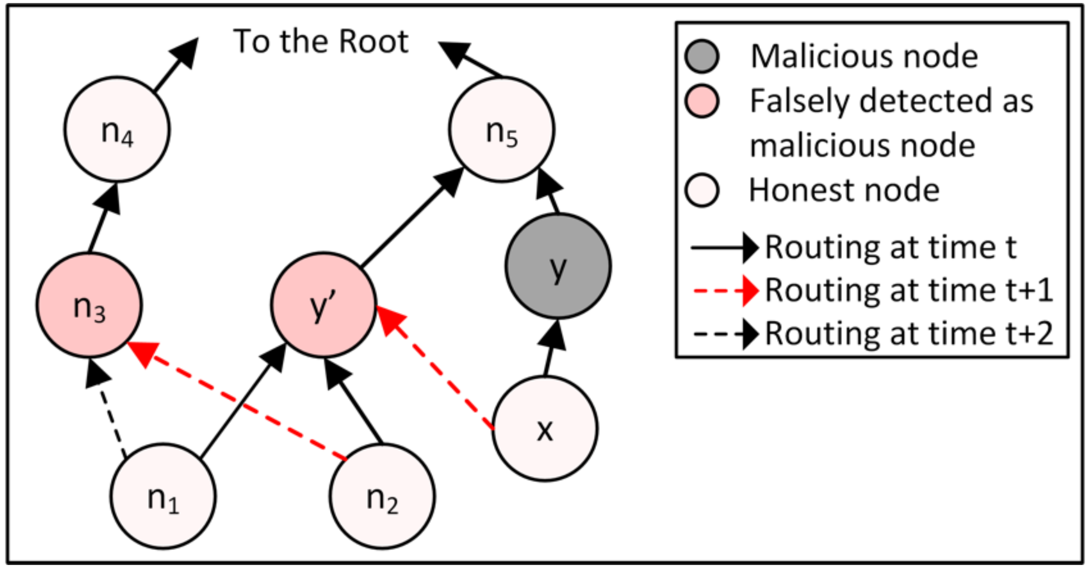
- ❑ Pairwise trust between a node and its neighbours.
- ❑ Choose your routing paths accordingly.
- ❑ This allows data to **flow around** regions of the network affected by an attack.



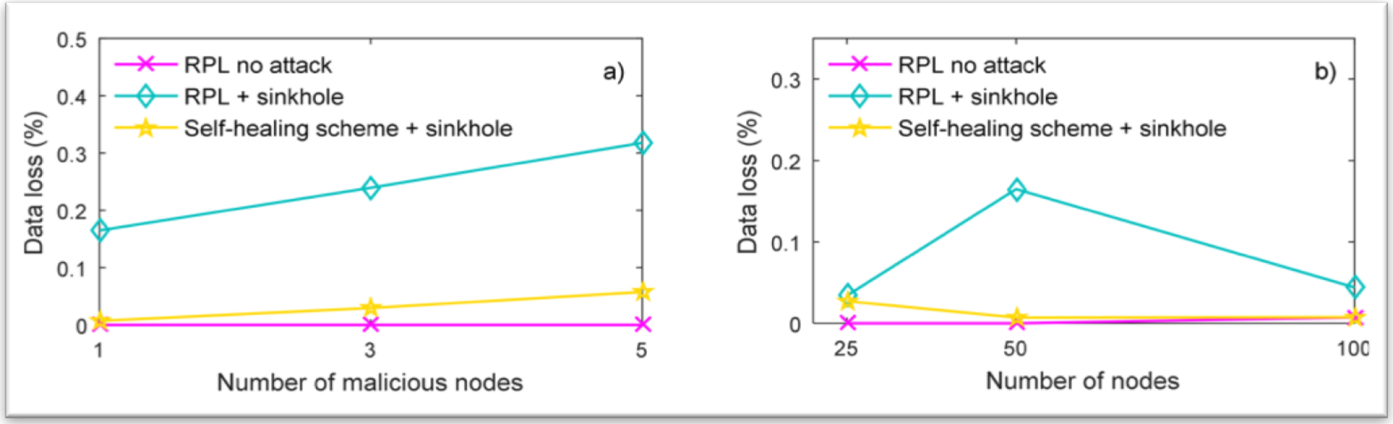
Imperial College London

A simple notification scheme propagates routing decisions from the affected areas to the sink

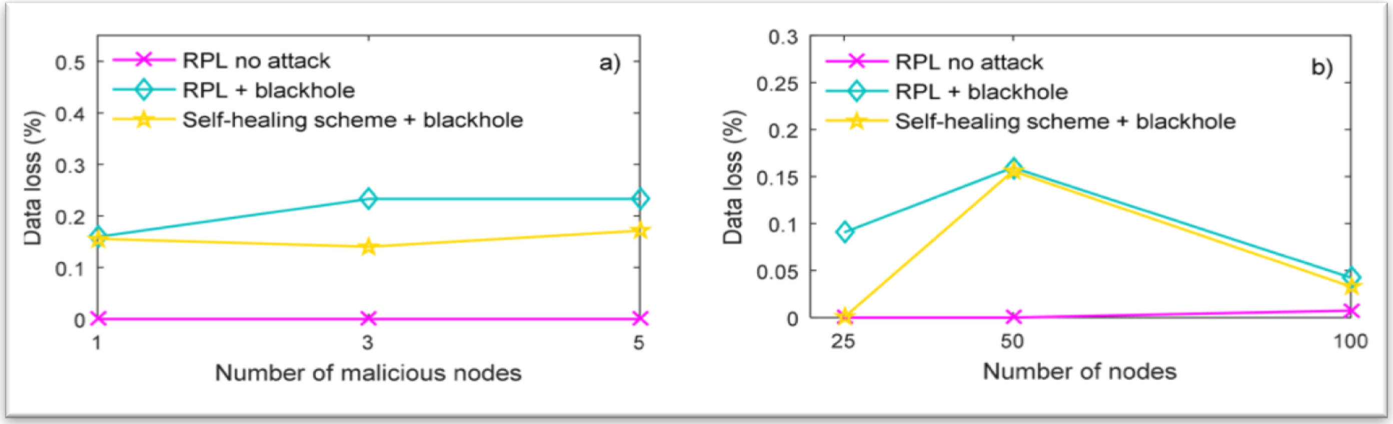
- ❑ Change due to a potentially malicious activity in the neighbourhood triggers the creation of mobile agents.
- ❑ They spread the information in network so that the damage of an attack is bounded.



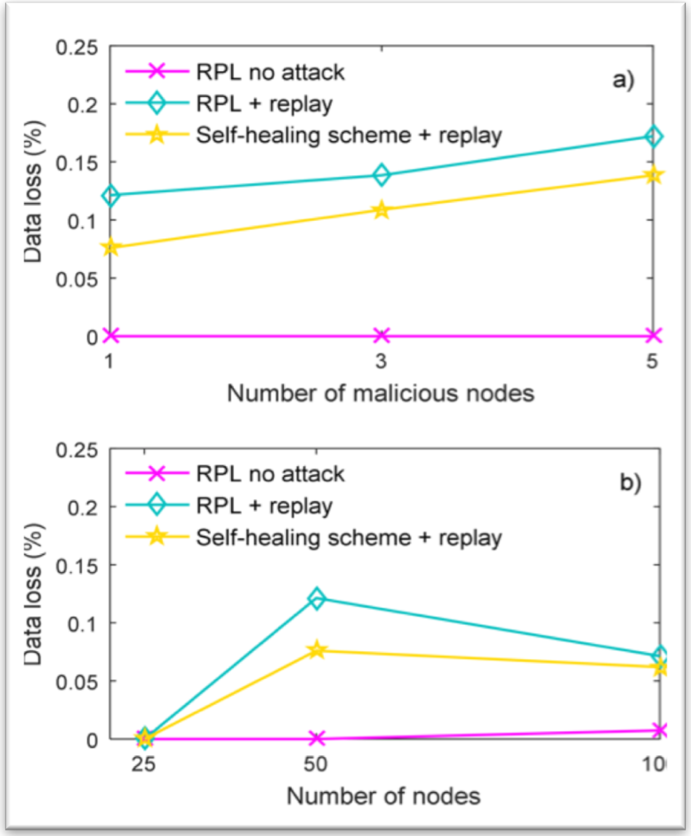
Our solution reduces data loss due to the varied attack scenarios down to 1% (5% on average)



Sinkhole attacks: a) 50 nodes, multiple attackers b) 25, 50 and 100 nodes, single attacker

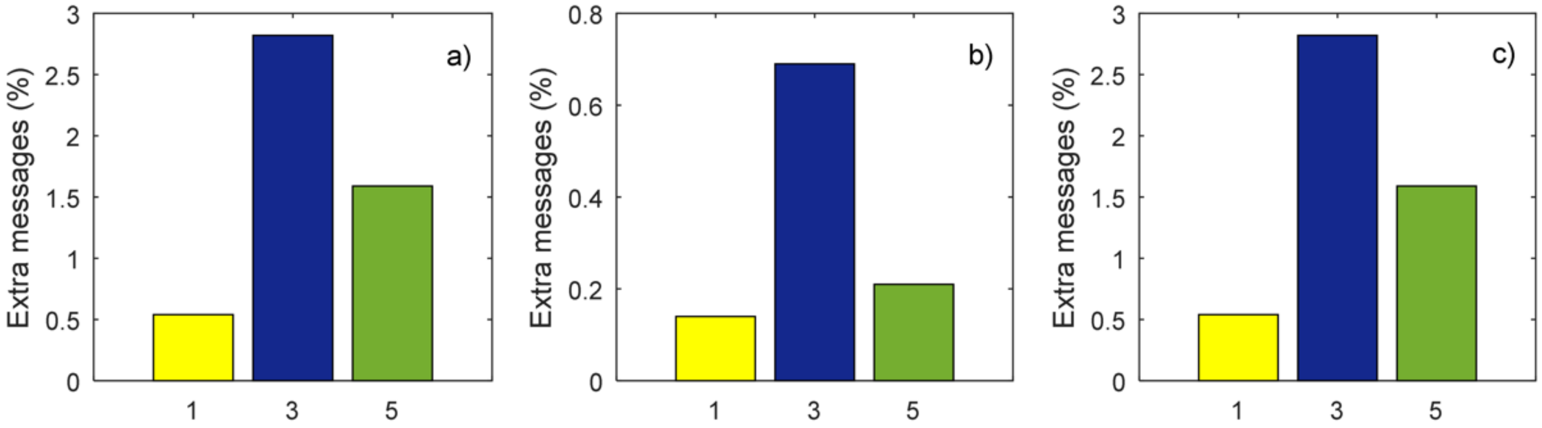


Blackhole attacks: a) 50 nodes, multiple attackers b) 25, 50 and 100 nodes, single attacker



Replay attacks: a) 50 nodes, multiple attackers b) 25, 50 and 100 nodes, single attacker

It achieves low overheads of 1% and a detection reliability of 99.3% tested across scenarios



Overhead in 50 nodes network, multiple attackers a) sinkhole attack b) blackhole attack c) replay attack

The **sensitivity** of our solution can be adjusted per user requirements by setting a sensitivity parameter α. While α = 0.9 gives the lowest number of false positives, we opted for more conservative approach and α = 0.7 which ensures a good sensitivity to all attacks with 99.3% detection reliability.

To conclude…

Our experimental results showed **high effectiveness** in terms of data loss rate requiring **low operational overheads** for varied attack scenarios.

- CISCO/Silicon Valley Community Foundation “Fog to FIELD”
- S4 (EPSRC Programme Grant): Science for Sensor Systems Software

[1] **I. Tomić** and J. A. McCann. “A Survey of potential security issues in existing wireless sensor network protocols”, IEEE Internet of Things Journal, 2017.

[2] **I. Tomić** et al. “Run time self-healing security for wireless sensor networks”. July 2017. Under review.

[3] https://labs.ripe.net/Members/ivana_tomic/iot-turning-evil

Thank you for your attention!