DISSN: A Dynamic Intrusion Detection System for Shared Sensor Networks

Claudio Farias, Renato Pinheiro, Rafael Costa, Igor Leão

PPGI- iNCE/DCC-IM Universidade Federal do Rio de Janeiro, Rio de Janeiro, Brazil

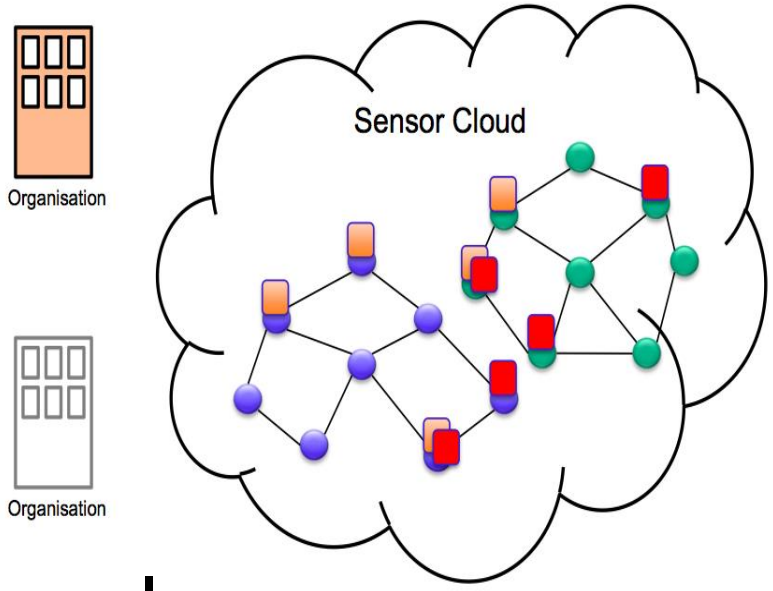
Schedule

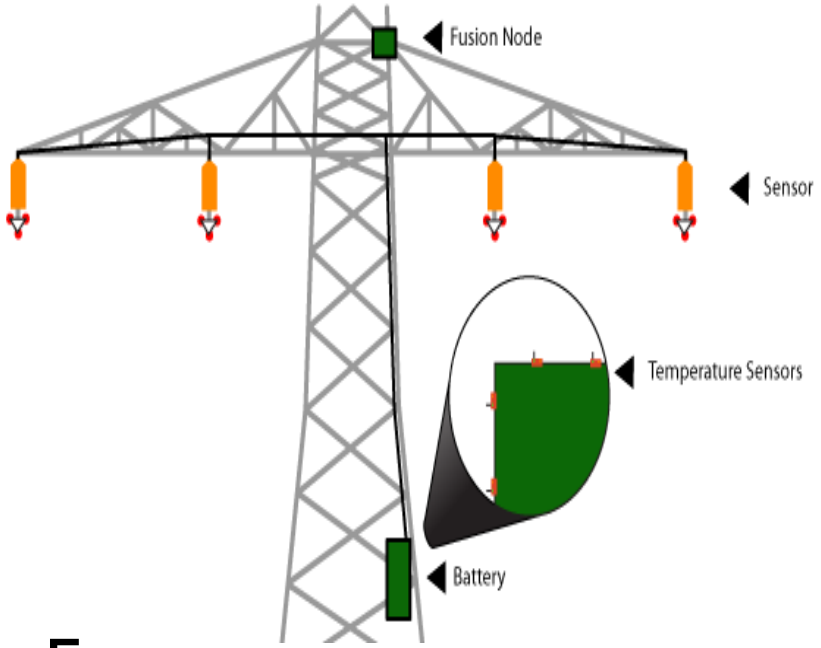
- Introduction
- Proposal - DISSN
- Tests
- Conclusion

Introduction -Wireless sensor Networks

- Low-cost small-sized sensors
- Sensing, processing and communicating capabilities through wireless
- Tens to thousands of sensors
- Monitoring diverse types of applications – including Buildings

Introduction -Shared Sensor Networks





Increases

- Number of applications
- Number of transmissions (energy)
- Data volume
- processing

Ex:
Batery Monitoring (BM) – 40 -144 °C
Overhead Transmission Line Monitoring (OPLM) - 60 - 80 °C

SSN security Challenges

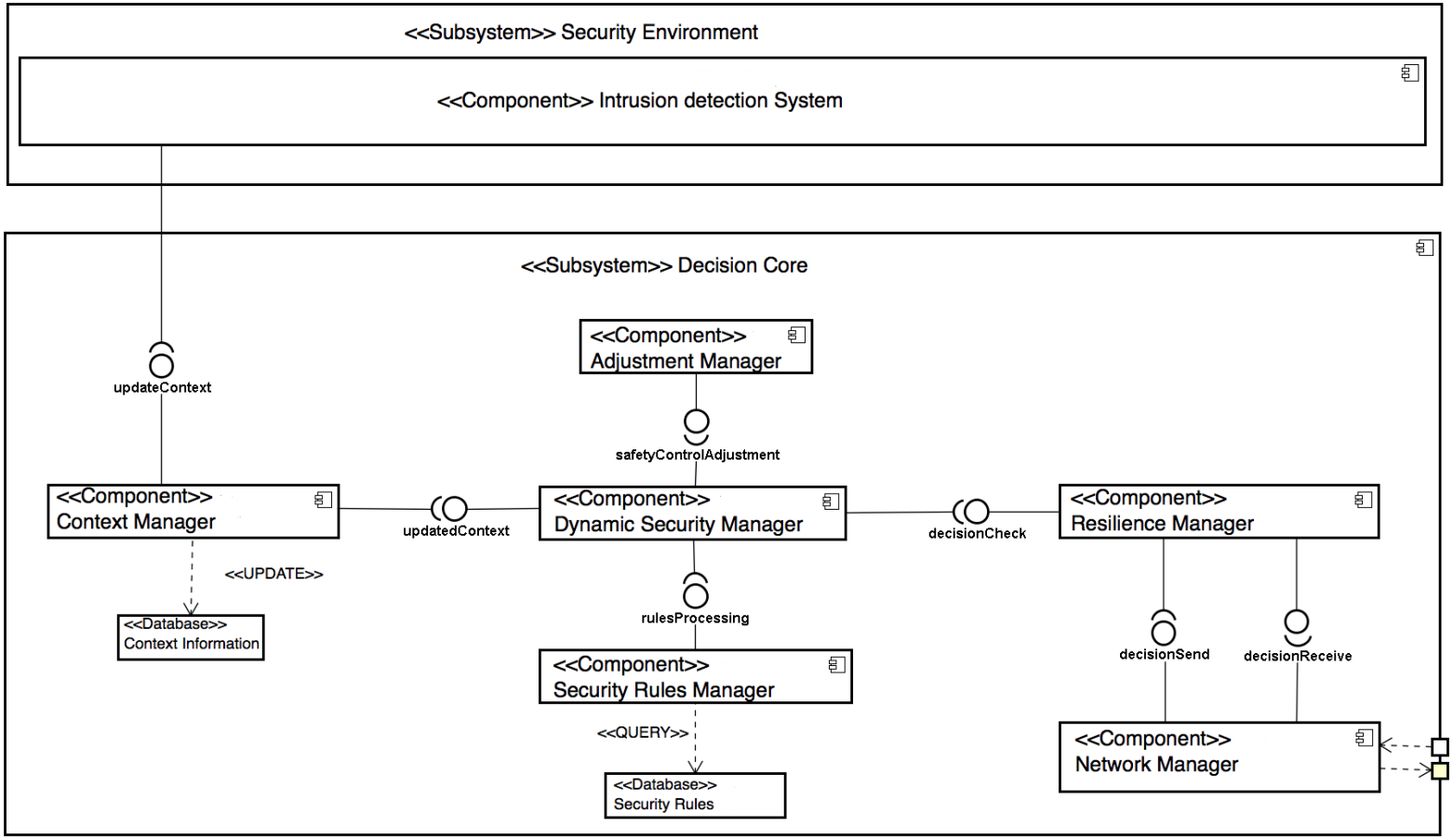
- limited resources of sensors
- vulnerabilities associated with wireless communication

- Solution: intrusion detection system
  - able to manage the availability, integrity and confidentiality of multiple applications according to the context information

Proposal - DISSN

- Dynamic IDS for Shared Sensor Networks
- Consider:
  - security requirements of the running applications;
  - information provided by the IDS
  - the amount of resources available sensors.

Logical Architecture



Tests - Metrics

- Efficacy
  - TP – activate countermeasure correctly
  - TN – Did not activate correctly
  - FP - activate countermeasure and it should
  - FN - Did not activate and it should
- Efficiency
  - Energy Consumption
  - Memory Consumption
  - Incresead Number of messages

Tests - Scenario

- SUN SPOT
- SSN varied 6 to 12 sensors
- 1 to 6 with DISSN
- arranged in the same rows equidistant from each other.
- one node was provided inaccurate context information.
- DISSN send messages every 10 seconds.
- confidence interval of 95%
- Repeats 30 times each simulation.

Tests - Efficiency

- Three scenarios
  - without using DISSN and with disabled security controls,
  - without using the DISSN and all the security controls enabled
  - using the DISSN to enable and disable security controls dynamically.

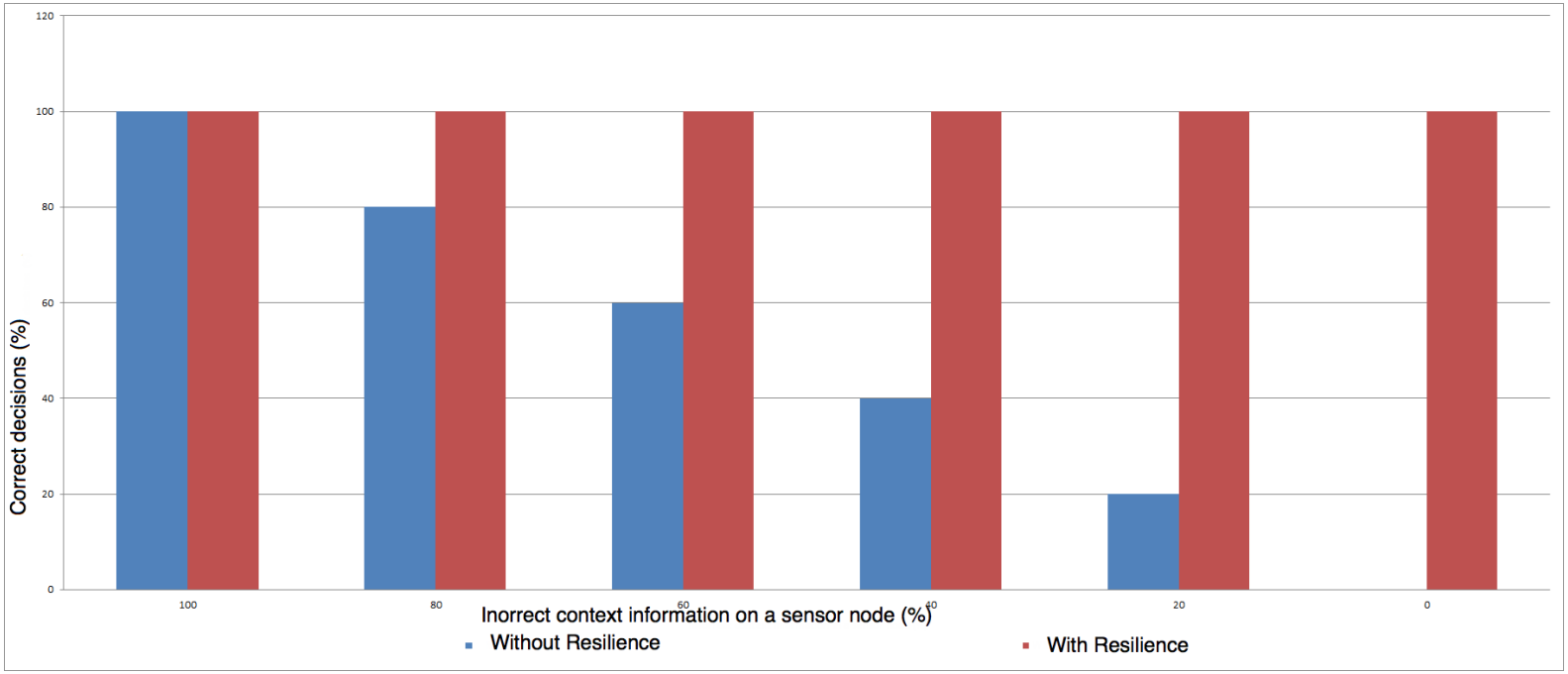
Tests - Efficiency

- DISSN is 26 kbytes in size
- less messages were consumed than when simply using the maximum level of security
- 18 messages while without using DISSN we had 50 messages

Testes - Efficacy

% of correct messages sent by a comproised sensor						
	100%	80%	60%	40%	20%	0%
VP	48	30	37	13	3	0
VN	52	50	23	27	7	0
FP	0	13	12	28	51	32
FN	0	7	28	32	39	68

Tests - Efficacy after consensus



Conclusions

- DISSN
  - adjusts security according to the context;
  - ensures through the consensus among the nodes in the SSN, that even in the occurrence of compromised nodes the decision of security adjustments is carried out correctly;

Future Work

- Energy expenditure and efficiency of the IDS resilience.
- Determine IDS resource consumption
- Compare of DISSN to other works in literature.

DISSN: A Dynamic Intrusion Detection System for Shared Sensor Networks

Claudio Farias, Renato Pinheiro, Rafael Costa, Igor Leão

PPGI- iNCE/DCC-IM Universidade Federal do Rio de Janeiro, Rio de Janeiro, Brazil