Energy-efficient Adaptive Encryption for Wireless Visual Sensor Networks

Ms. Danilo de Oliveira Gonçalves, IFBA

Dr. Daniel G. Costa, UEFS

PÓS-GRADUAÇÃO EM
COMPUTAÇÃO APLICADA

Outline

- Wireless visual sensor networks
- Security in WVSN
- Proposed approach
- Confidential Area Association Protocol
- Numerical results
- Conclusions

Wireless visual sensor networks

- Sensor nodes equipped with a low-power camera
  - Perception of sensing radius and redundancy is altered
- A lot of applications:
  - Smart cities, industrial control, visual monitoring, surveillance, tacking, IoT, etc
- Many challenges
  - Energy, memory and processing power, transmission bandwidth, latency, jitter, coding, security, etc

Security in WVSN

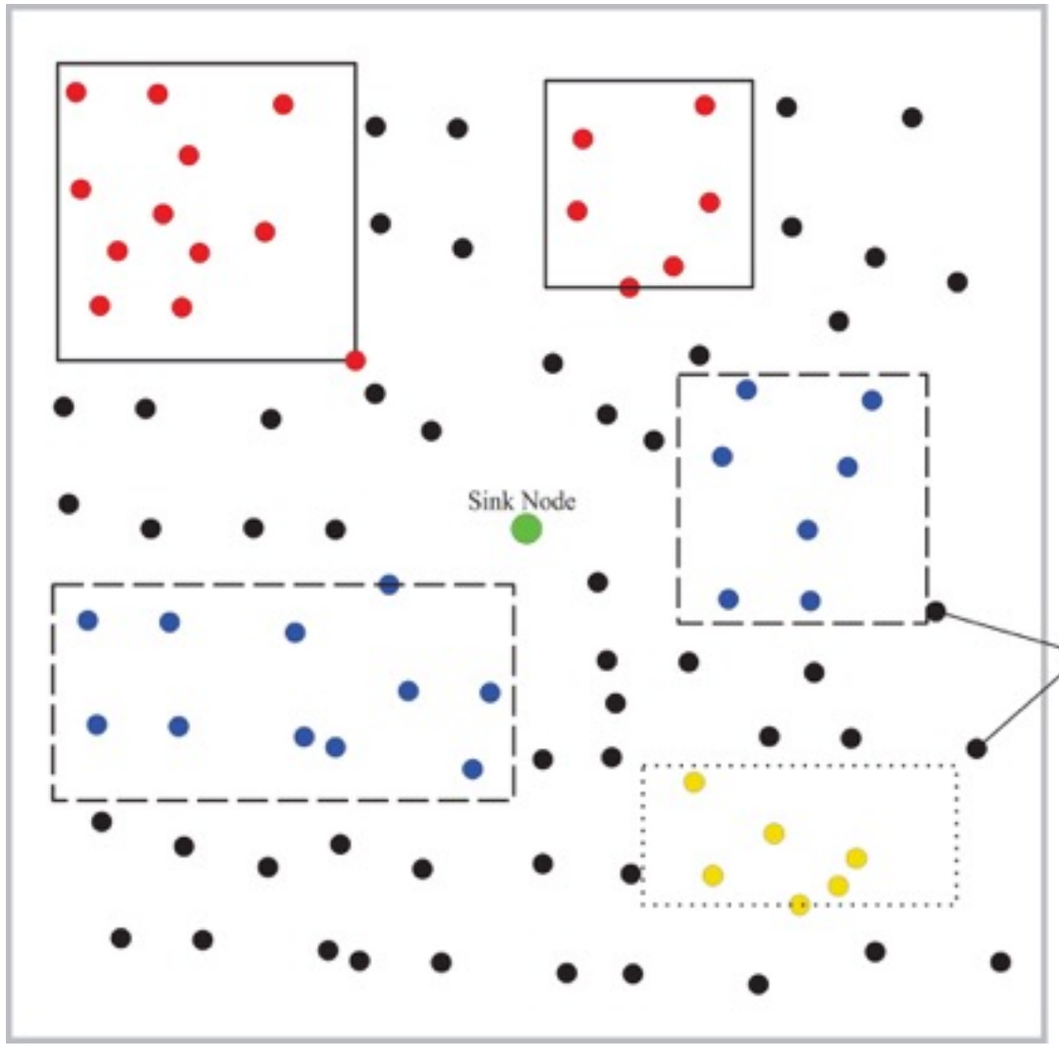
- Many monitoring scenarios demand security
  - **Confidentiality**, integrity, authenticity and availability
- Ensuring security in wireless visual sensor networks is challenging
  - Resource constraints, particularly energy
- Traditional security mechanisms are degrading
  - Does we need to protect the entire network?

Prioritization in WVSN

- Sensor nodes (segments of the network) may have different relevancies
  - Potential to provide relevant data!
    - *Exploiting the sensing relevancies of source nodes for optimizations in visual sensor networks. Multimedia Tools and Applications, v. 64, p. 549-579, 2013.*
    - *Research Trends in Wireless Visual Sensor Networks When Exploiting Prioritization. Sensors, v. 15, p. 1760-1784, 2015.*
  - Network may be optimized
- Demand for confidentiality IS NOT related to relevance

Proposed Approach

- Employed security according to the **confidentiality** demand
  - Monitoring network defines **Confidential Areas** (CA)
    - Different levels of confidentiality requirements
  - Sensors in a CA apply the same security protection



Confidential Areas

- A Confidential Area delimits a location within the network
  - Defined by application requirements
  - A convex 2D quadrilateral that can change along the time
- Each CA is associated to a Confidentiality Level (CL)
  - Level 0: Without security.
  - Level 1: CA with low security
  - Level 2: CA with moderate security requirements
  - Level 3: CA with maximum security
- Each CL is associated to a Security Scheme

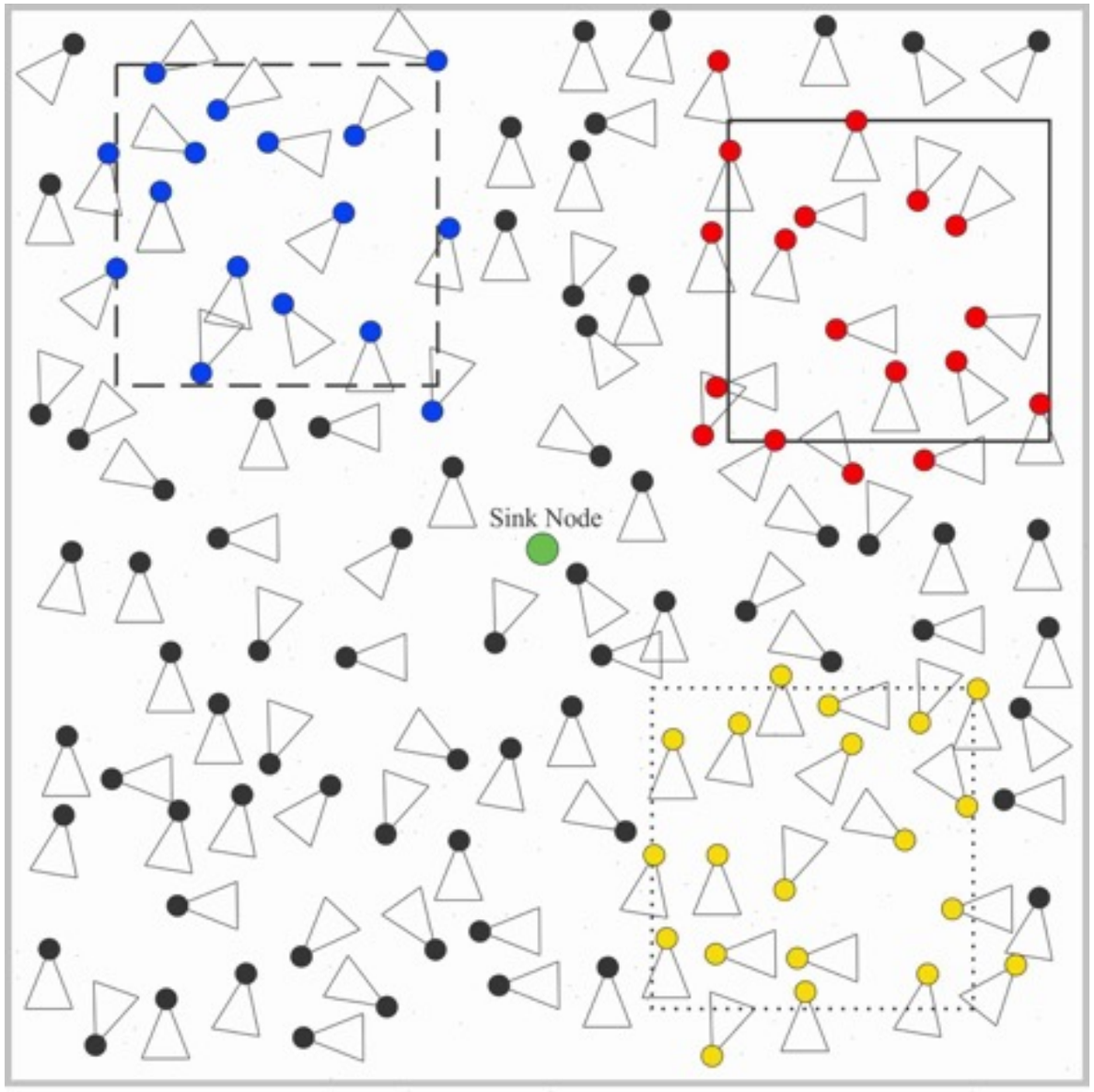
Security schemes

- Any possible combination between CL and a security service

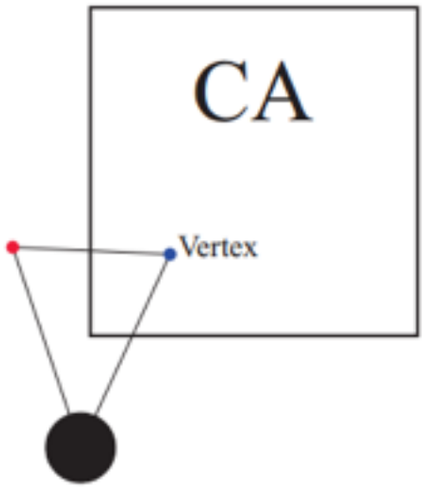
Schema level	Coding	Encryption key size	Collected data type
0	Unencrypted	Unencrypted	Unencrypted
1	DWT at two levels	128-bit key	Encryption of only scalar data
2	DWT at one level	192-bit key	Encryption of scalar data and still images
3	Full image encryption	256-bit key	Encryption of scalar data, still images and video

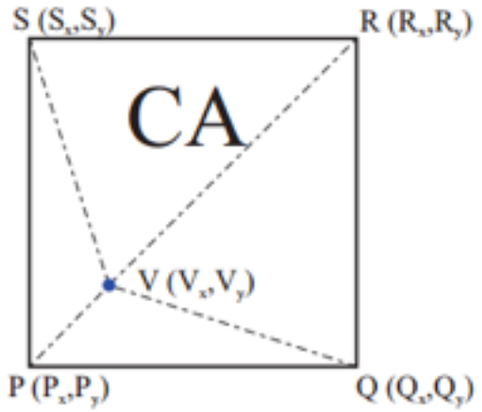
Confidential Areas

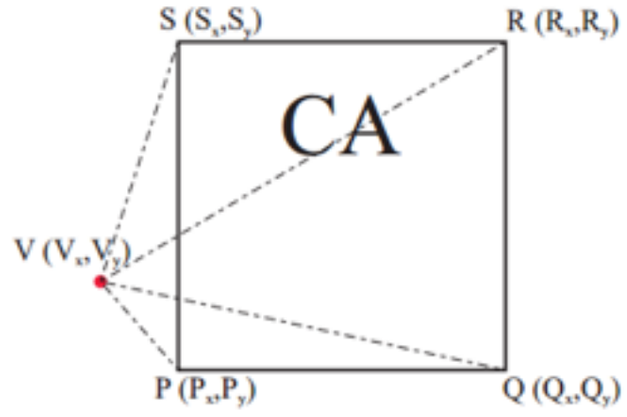
- A big challenge is how to associate sensors to confidential areas
  - A 2D mathematical model was defined
  - Problem: how to properly associate ONLY ONE CA to each visual sensor?
    - We compute FoV



Confidential Areas







- If a visual sensor views more than one CA, it is associated to the CA with highest confidentiality level
- Association is computed in a central unit (sink)
  - Knows information of the network
  - We propose an association protocol: Confidential Area Association Protocol (CAAP)

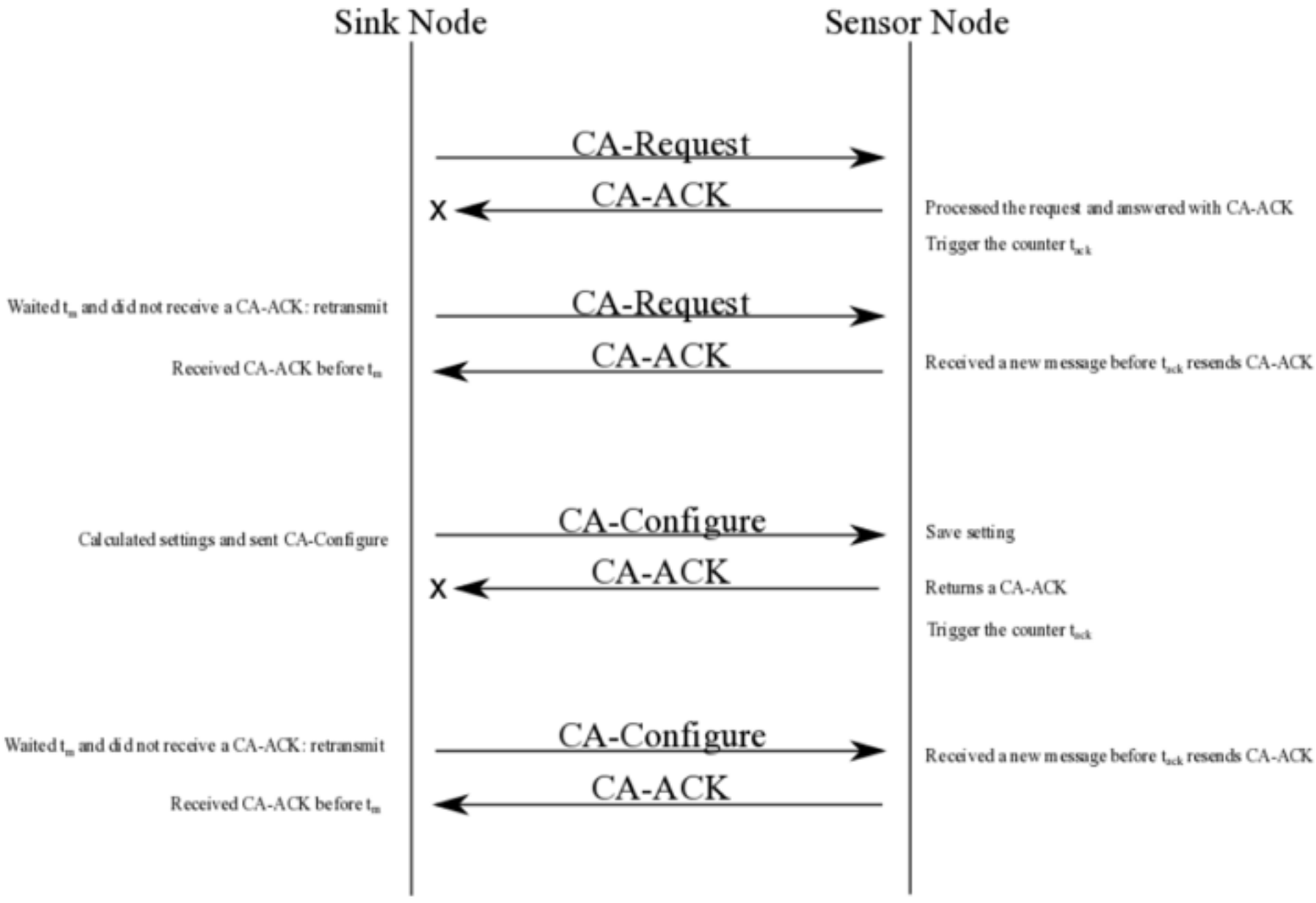
Confidential Area Association Protocol - CAAP

- Energy-efficient protocol
  - CAAP is an application-level protocol with simple request/confim operation
- Three messages
  - CA-Request
    - Sent by the sink to request information (localization and sensing parameters) from sensor nodes
  - CA-Configure
    - Sent by the sink indicating the computed configuration for the sensor nodes
  - CA-ACK
    - Confirmation and responses from sensor nodes

Confidential Area Association Protocol - CAAP

- It is controlled by two timers
  - $\mathbf{t_m}$ sets the time that the sink node should wait for the receiving of a CA-ACK message
  - $\mathbf{t_{ack}}$ sets the time required to ensure that a CA-ACK message was received by the sink node
- Retransmission will occurs:
  - If a CA-request or CA-Configure message is lost (dropped or corrupted) during transmission;
  - If a CA-ACK message is lost;
  - If a CA-ACK message is received after tm.

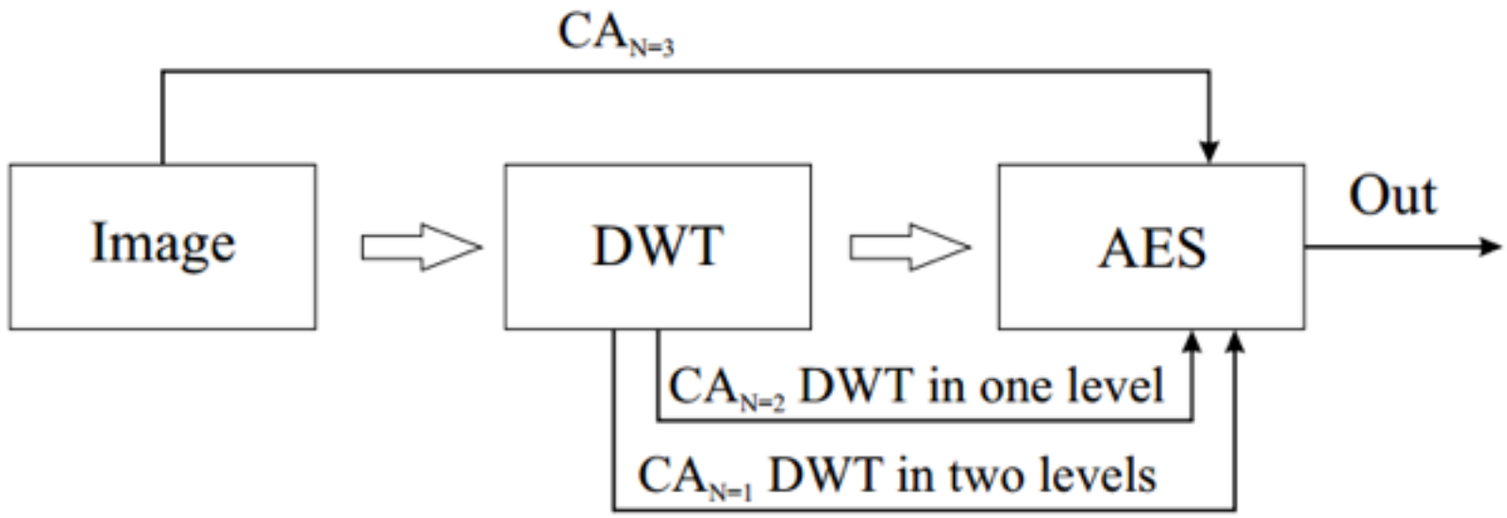
Confidential Area Association Protocol - CAAP



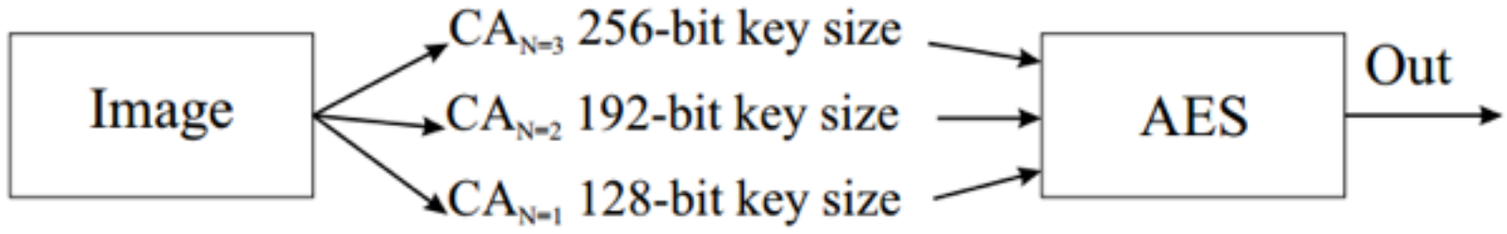
Numerical Results

- WVSN simulated in Matlab. Cryptography with AES.
- Two security schemes were implemented

Scheme 1



Scheme 2



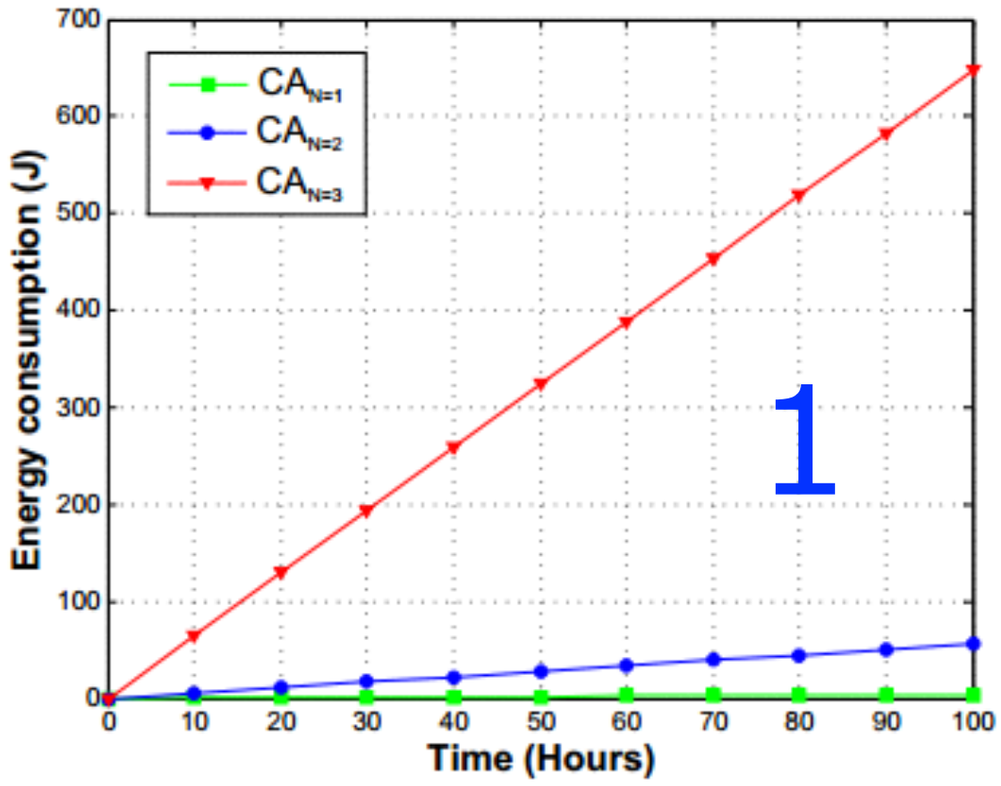
Energy consumption with AES

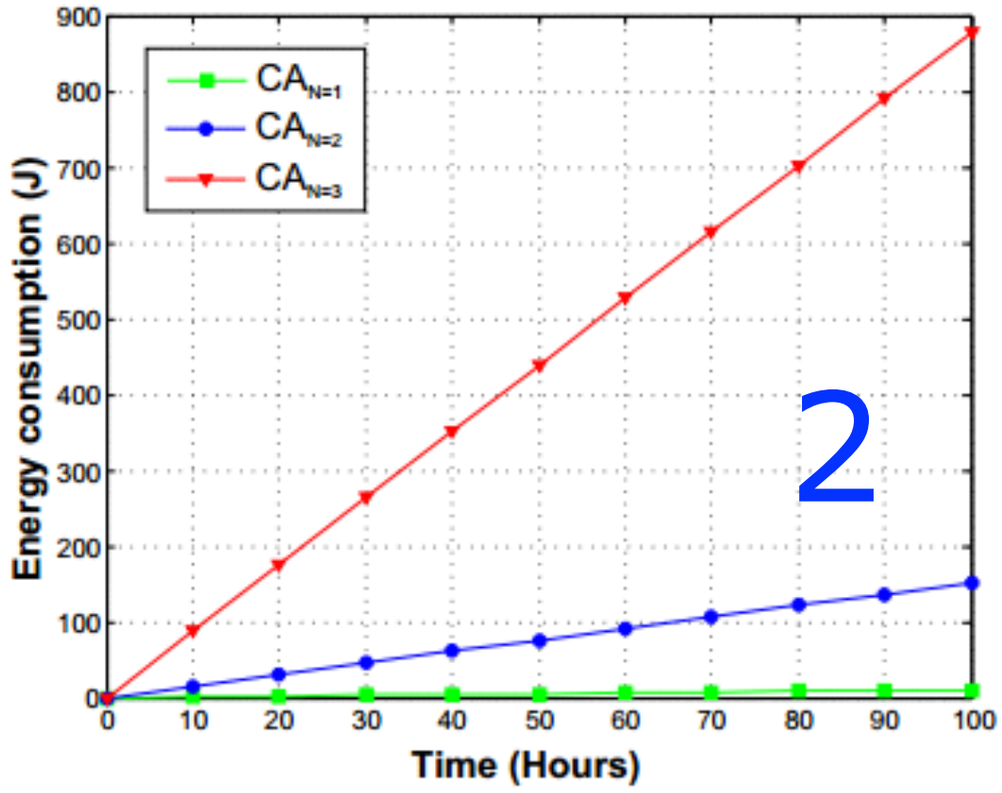
$$EnergyCost_{(Si)} = EKey_{(Si)} + (EByte_{(Si)} * Size_{(Data)})$$

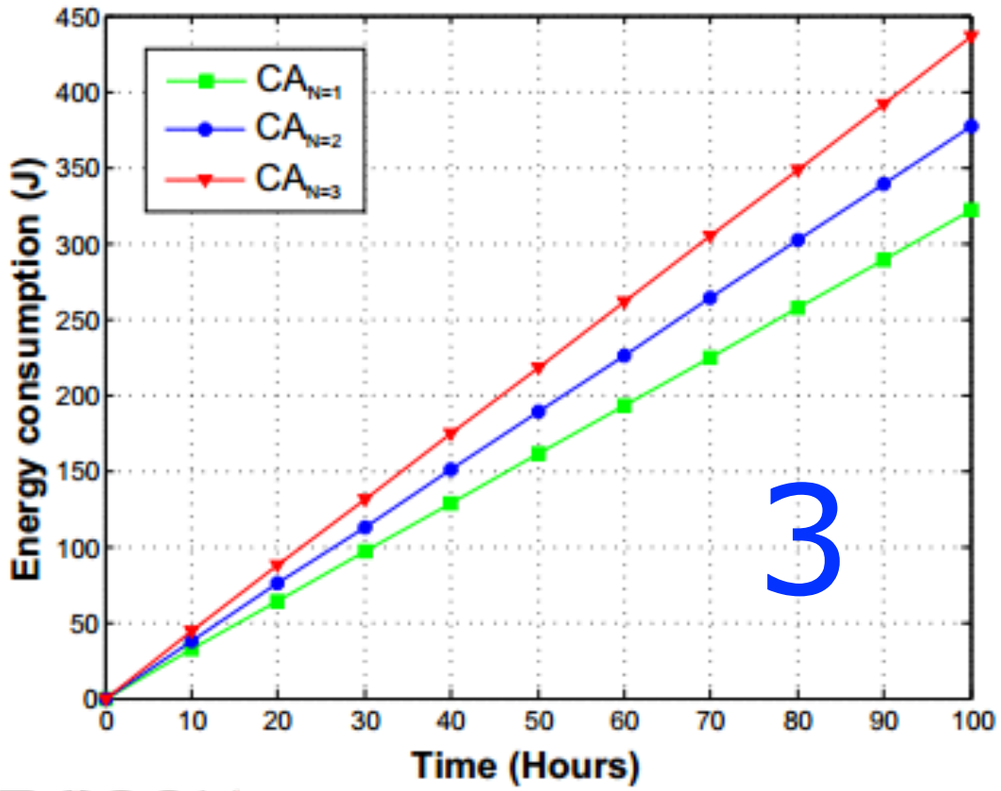
Key Size (bits)	EKey(AES) (µJ)	EByte(AES) in ECB mode (µJ/B)	EByte(AES) in CBC mode (µJ/B)	EByte(AES) in CFB mode (µJ/B)	EByte(AES) in OFB mode (µJ/B)
128	7.83	1.21	1.62	1.91	1.62
192	7.87	1.42	2.08	2.30	1.83
256	9.92	1.64	2.29	2.31	2.05

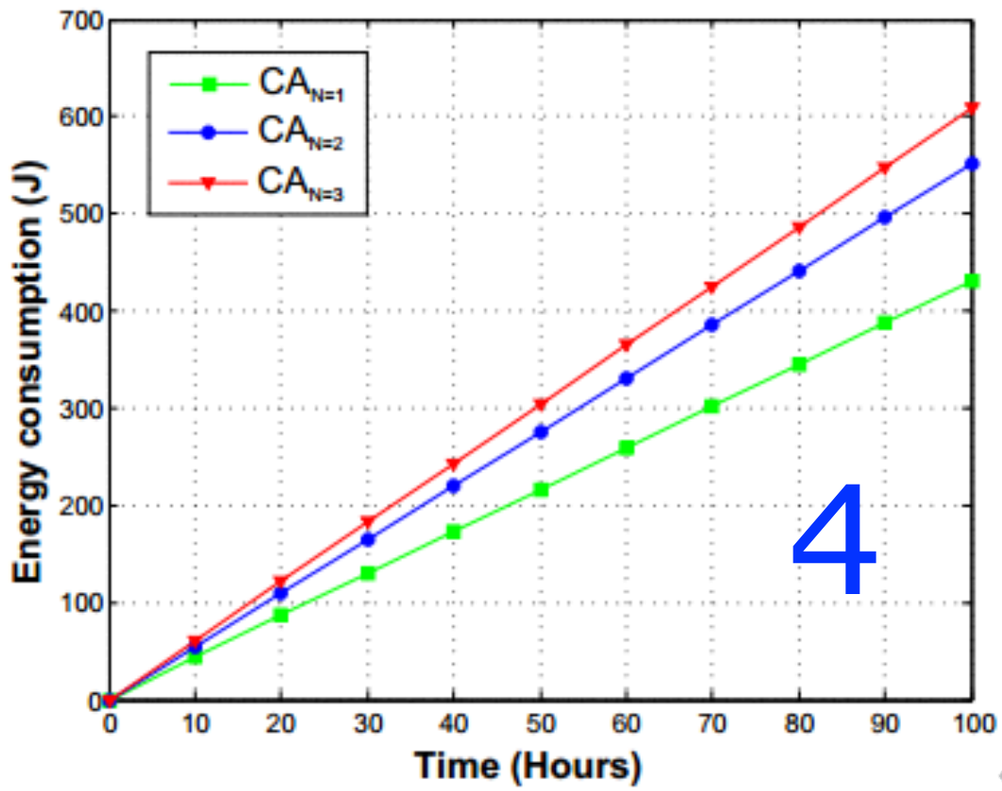
Validation scenarios

Scenario	Security Scheme	Image resolution	Key size	CA $_{N=1}$	CA $_{N=2}$	CA $_{N=3}$	Algorithm
1	1	128 x 128 x 8	128 bits	125	125	125	AES/ECB
2	1	256 x 256 x 4	256 bits	125	125	125	AES/ECB
3	2	128 x 128 x 4	vary	90	90	90	AES/ECB
4	2	128 x 128 x 4	vary	90	90	90	AES/CBC


Energy consumption (J)
Time (Hours)
CA$_{N=1}$
CA$_{N=2}$
CA$_{N=3}$
1

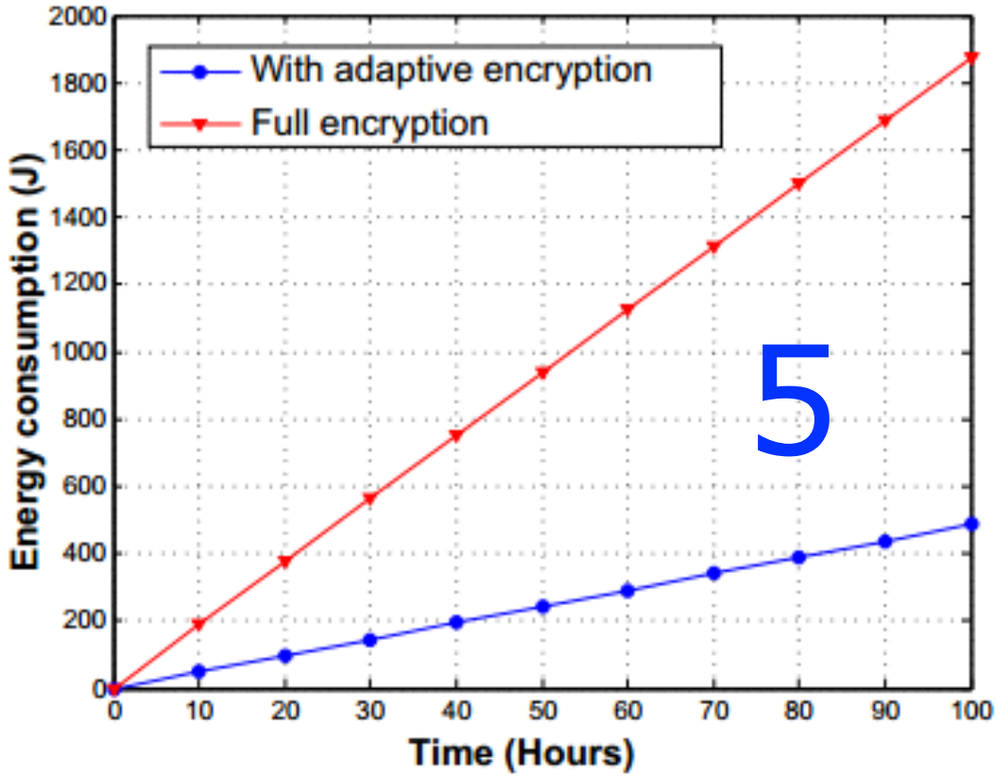

Energy consumption (J)
Time (Hours)
CA$_{N=1}$
CA$_{N=2}$
CA$_{N=3}$
2

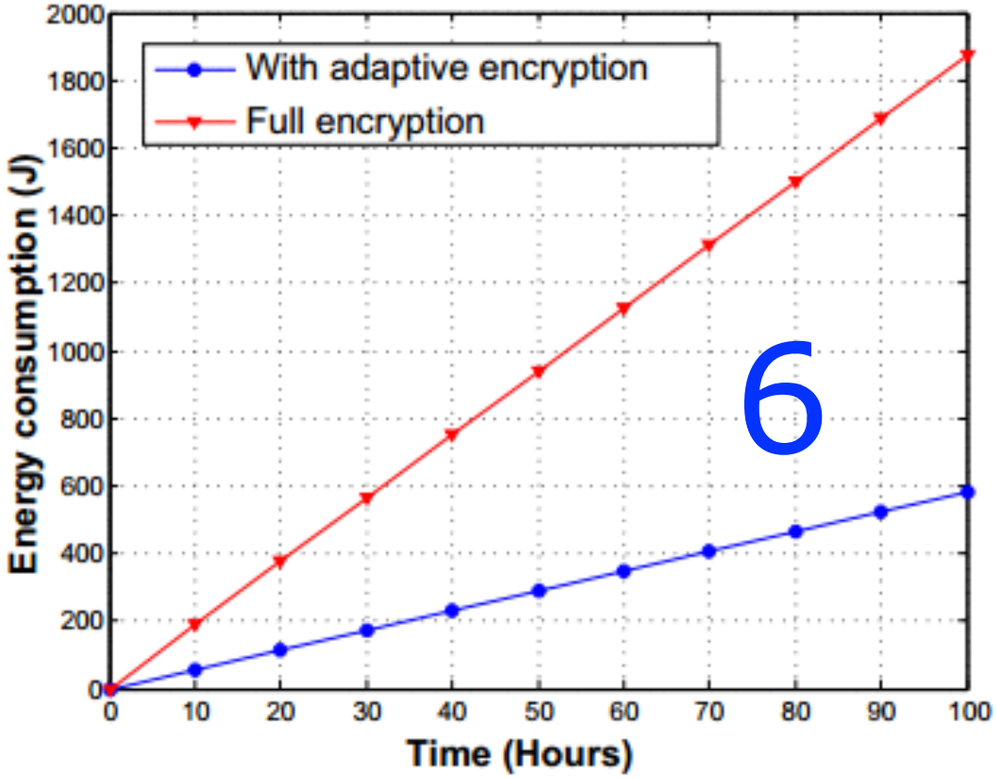

Energy consumption (J)
Time (Hours)
CA$_{N=1}$
CA$_{N=2}$
CA$_{N=3}$
3

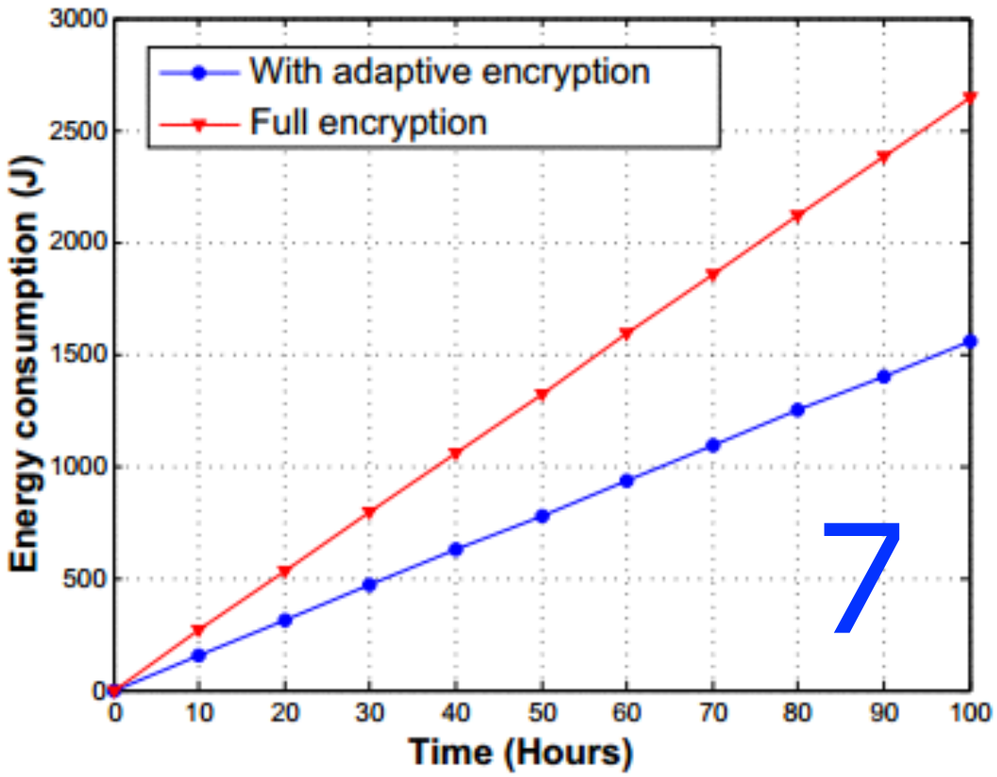

Energy consumption (J)
Time (Hours)
CA$_{N=1}$
CA$_{N=2}$
CA$_{N=3}$
4

Validation scenarios

Scenario	Security Scheme	Image resolution	Key size	CA $_{N=1}$	CA $_{N=2}$	CA $_{N=3}$	Algorithm
5	1	128 x 128 x 8	128 bits	46	32	67	AES/CBC
6	1	128 x 128 x 8	128 bits	41	56	79	AES/CBC
7	2	128 x 128 x 4	vary	41	56	79	AES/CBC


With adaptive encryption
Full encryption
Energy consumption (J)
Time (Hours)
0
200
400
600
800
1000
1200
1400
1600
1800
2000
0
10
20
30
40
50
60
70
80
90
100
5


With adaptive encryption
Full encryption
Energy consumption (J)
Time (Hours)
0
200
400
600
800
1000
1200
1400
1600
1800
2000
0
10
20
30
40
50
60
70
80
90
100
6


With adaptive encryption
Full encryption
Energy consumption (J)
Time (Hours)
0
500
1000
1500
2000
2500
3000
0
10
20
30
40
50
60
70
80
90
100
7

Conclusions

- Adaptive encryption may bring significant results for wireless visual sensor networks
  - Energy saving, while strongly protecting sensed data with highest confidentiality requirements
    - CAAP results can be found in: *Um Protocolo Genérico Eficiente de Energia para Aplicações em Redes de Sensores sem Fio sem Restrição de Tempo de Resposta. Revista de Tecnologia da Informação e Comunicação, v. 5, p. 8-15, 2015.*
- Future works will be concerned with:
  - Additional validation with more scenarios
    - Mobility, heterogeneous networks, different encryption algorithms, etc
  - Implementation of the proposed approach in physical sensors

Thank you!

- Danilo de Oliveira Gonçalves
  - daniloxm@gmail.com

- Daniel G. Costa
  - danielgcosta@uefs.br