

Risk Management in Intrusion Detection Applications with Wireless Video Sensor Networks

Abdallah Makhoul
University of Franche-Comté
LIFC Laboratory

Rachid Saadi
INRIA
Rocquencourt

Congduc Pham
University of Pau
LIUPPA Laboratory

Abdallah Makhoul

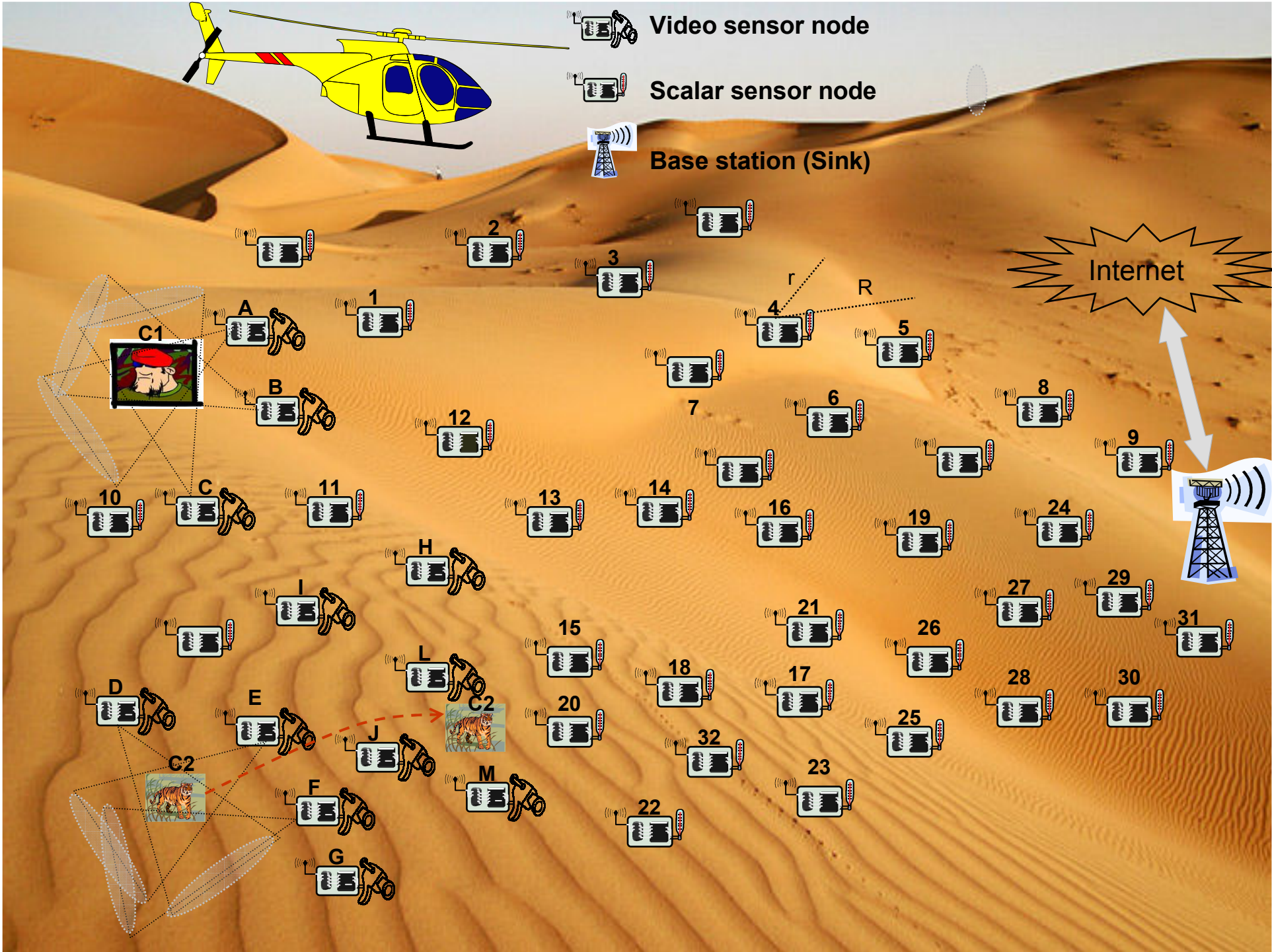
abdallah.makhoul@univ-fcomte.fr

 *Sydney*
AUSTRALIA
18-21 April 2010

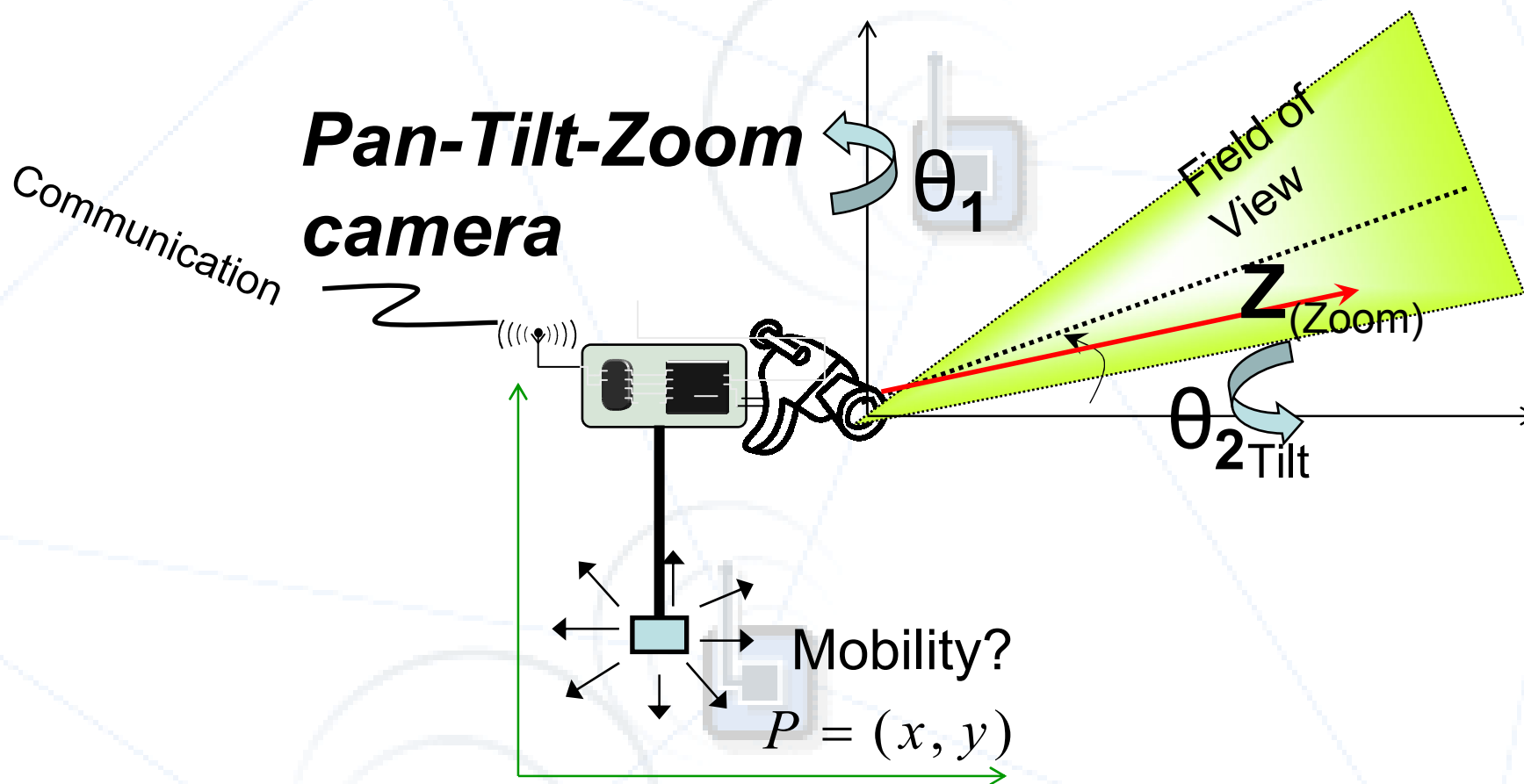
A diagram of a wireless sensor network is overlaid on the slide. It features several blue square nodes, each with a white antenna icon and a small square on its face. These nodes are interconnected by a network of light blue dashed lines. Each node also has several concentric circles around it, representing its communication range. The nodes are distributed across the slide, with some at the top, middle, and bottom. The title 'Overview' is centered at the top in a large blue font. Below the title is a thick blue horizontal line. At the bottom right, there is a small blue number '2'.

Overview

-
- Introduction of wireless video sensor networks
 - Surveillance applications
 - Coverage and scheduling
 - Application Criticality
 - Experimental Results



Video Sensor Node



$$N(P, \Theta_1, \Theta_2, Z)$$

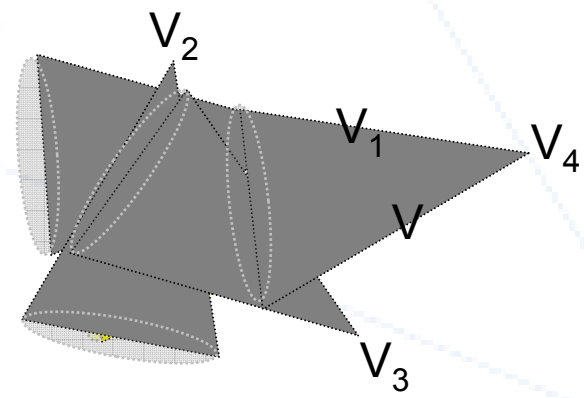
Surveillance Applications

The background features a network diagram with six nodes, each represented by a blue square with a white antenna and a camera lens. The nodes are interconnected by thin blue lines. Concentric circles around each node represent signal waves or coverage areas. The title 'Surveillance Applications' is centered at the top in a large blue font, with a horizontal blue line below it. Another horizontal blue line is at the bottom of the slide.

- Surveillance video applications :
 - Quality of the captured image
 - Unnecessary to send image with high bandwidth
 - Energy consideration
 - Redundancy and coverage

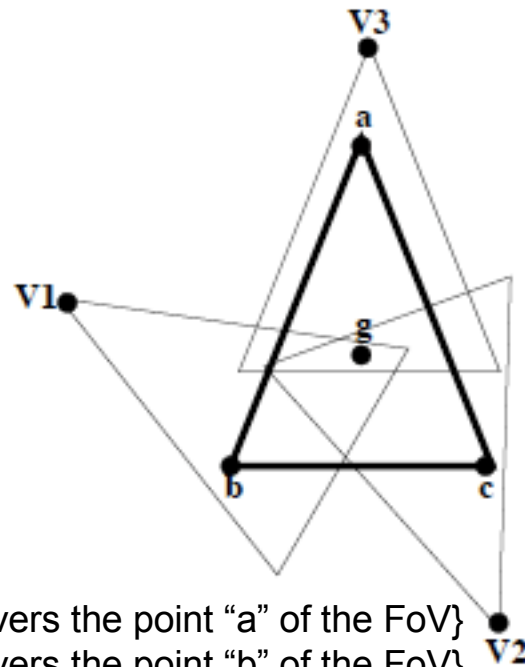
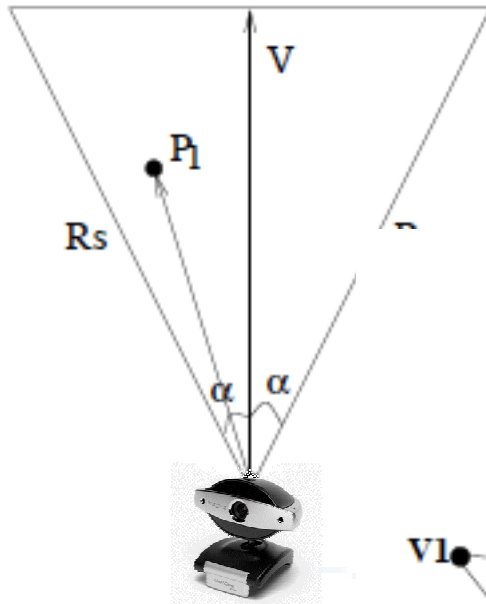
Node's cover set

- Each node v has a Field of View, FoV_v
- $Co_i(v)$ = set of nodes v' such as $\bigcup_{v' \in Co_i(v)} FoV_{v'}$ covers FoV_v
- $Co(v)$ = set of $Co_i(v)$



$$Co(v) = \{V_1, V_2, V_3, V_4\}$$

Finding v's cover set



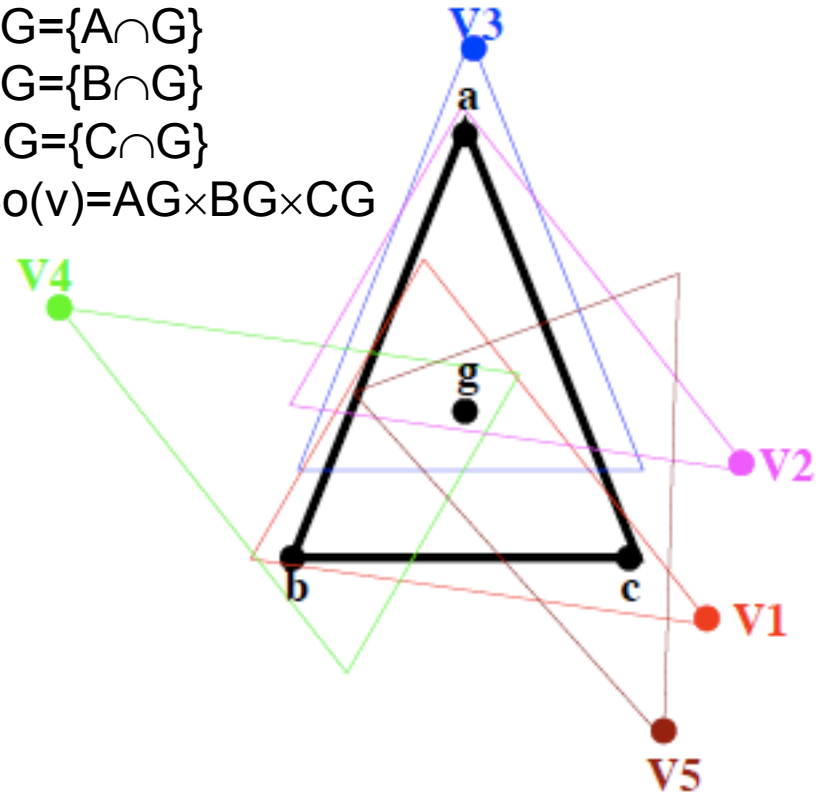
- $A = \{v \in N(V) : v \text{ covers the point "a" of the FoV}\}$
- $B = \{v \in N(V) : v \text{ covers the point "b" of the FoV}\}$
- $C = \{v \in N(V) : v \text{ covers the point "c" of the FoV}\}$
- $G = \{v \in N(V) : v \text{ covers the point "g" of the FoV}\}$

$$AG = \{A \cap G\}$$

$$BG = \{B \cap G\}$$

$$CG = \{C \cap G\}$$

$$Co(v) = AG \times BG \times CG$$

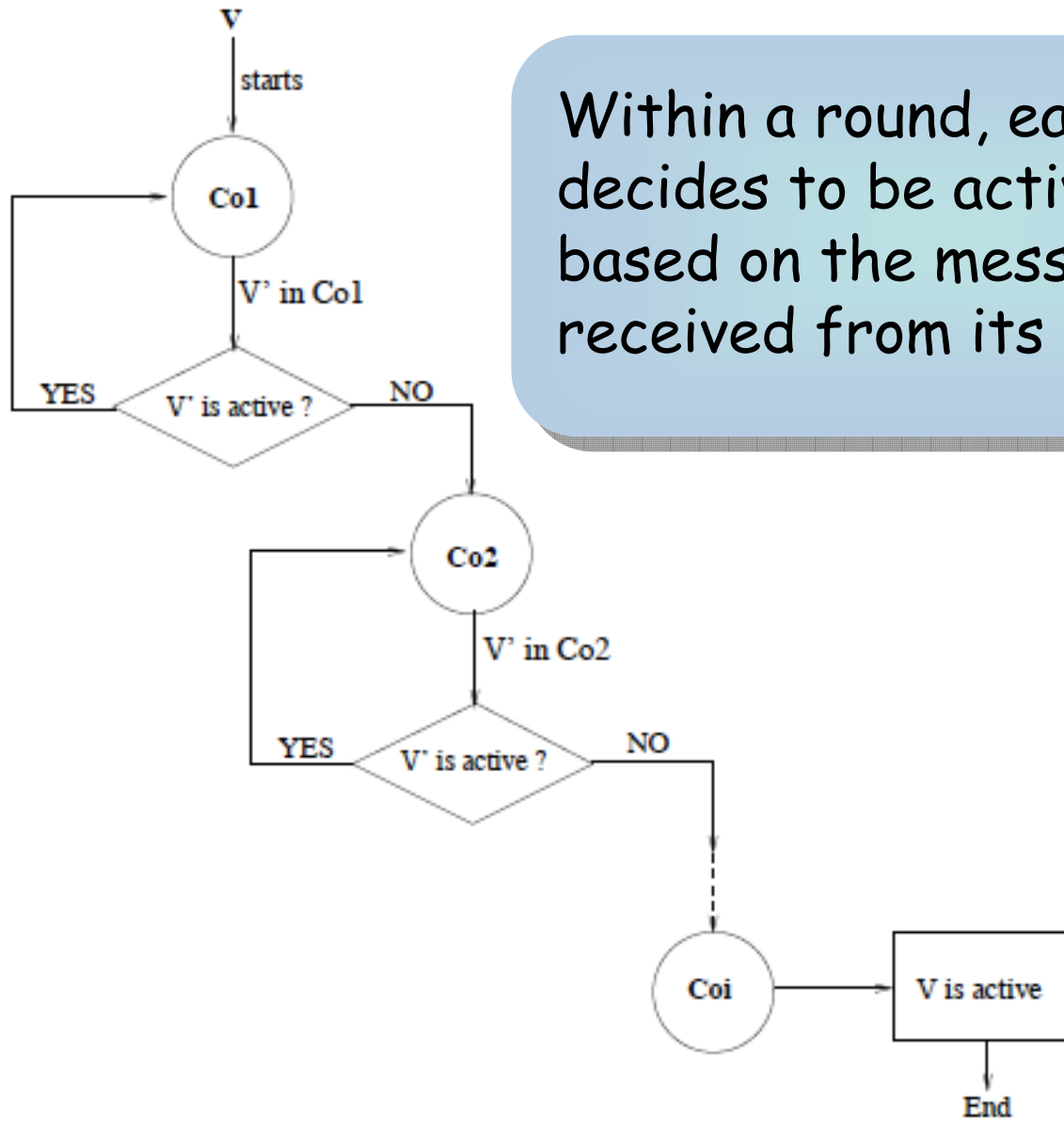


$$Co(V) = \{$$

- $\{V\},$
- $\{V2, V1\},$
- $\{V3, V1\},$
- $\{V2, V4, V5\},$
- $\{V3, V4, V5\}$

$$\}$$

Active node selection



Within a round, each node decides to be active or not based on the messages received from its neighbors

Application's criticality



- All surveillance applications may not have the same criticality level, $r^0 \in [0, 1]$
 - Environmental, security, healthcare,...
- Capture speed should decrease when r^0 decreases
- Sensor nodes could be initialized with a given r^0 prior to deployment

How to meet app's criticality

- Capture speed can be a « quality » parameter
- Capture speed for node v should depend on the app's criticality and on the level of redundancy for node v
- V 's capture speed can increase when as V has more nodes covering its own FoV - cover set

Evolution of the video network nodes

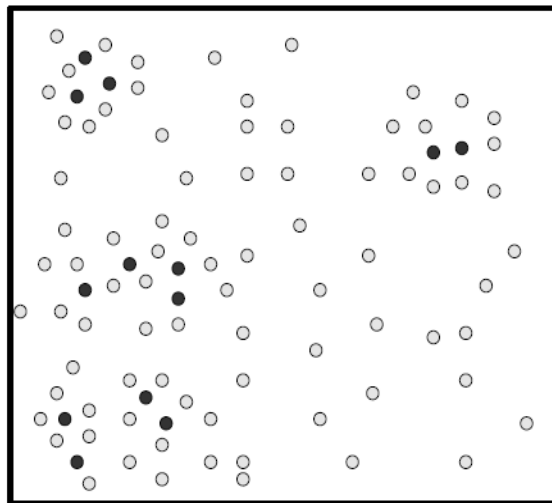
(A)

(B)

(C)

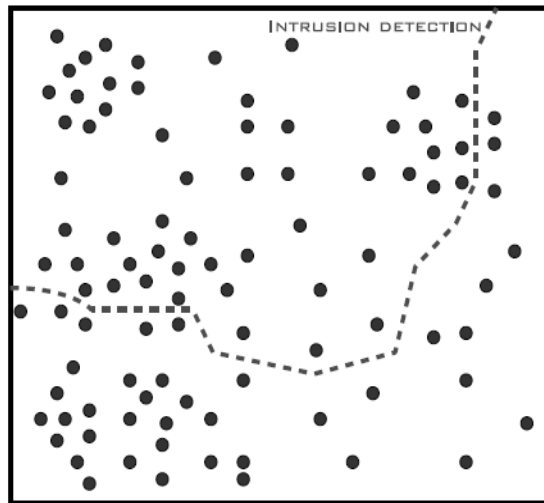
● SENTRY NODE: NODE WITH HIGH SPEED CAPTURE (HIGH COVER SET).

○ IDLE NODE: NODE WITH LOW SPEED CAPTURE.



HIBERNATE MODE
 $r^o=0$

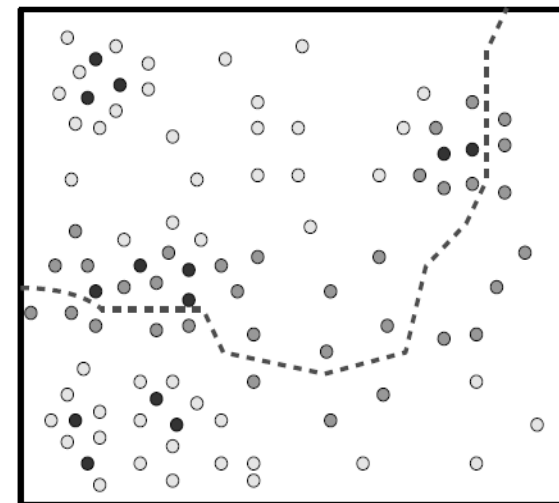
● ALERTED NODE: NODE WITH HIGH SPEED CAPTURE (ALERT INTRUSION).



ALERT MODE
 $r^o=R^o$

● SENTRY NODE: NODE WITH HIGH SPEED CAPTURE (HIGH COVER SET).
● CRITICAL NODE: NODE WITH HIGH SPEED CAPTURE (NODE THAT DETECTS THE INTRUSION).

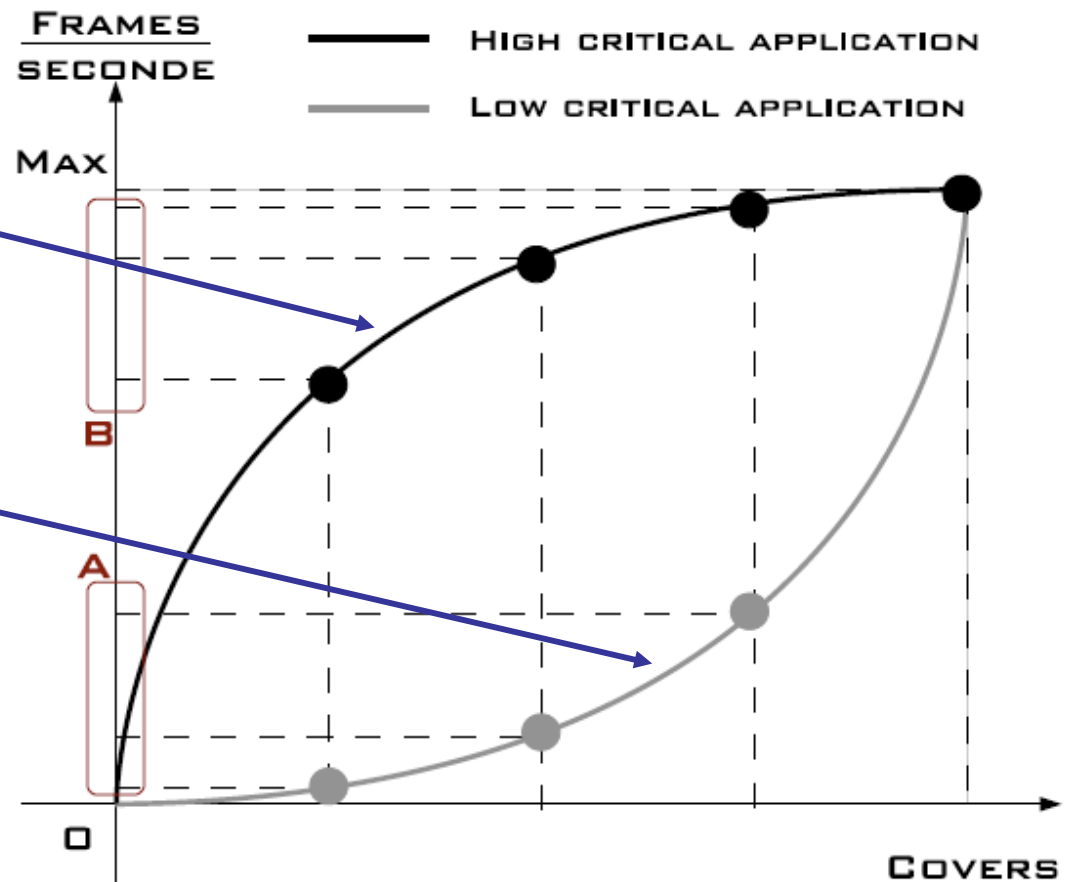
○ IDLE NODE: NODE WITH LOW SPEED CAPTURE.



HIBERNATE MODE (AFTER INTRUSION)
 $r^o=0$

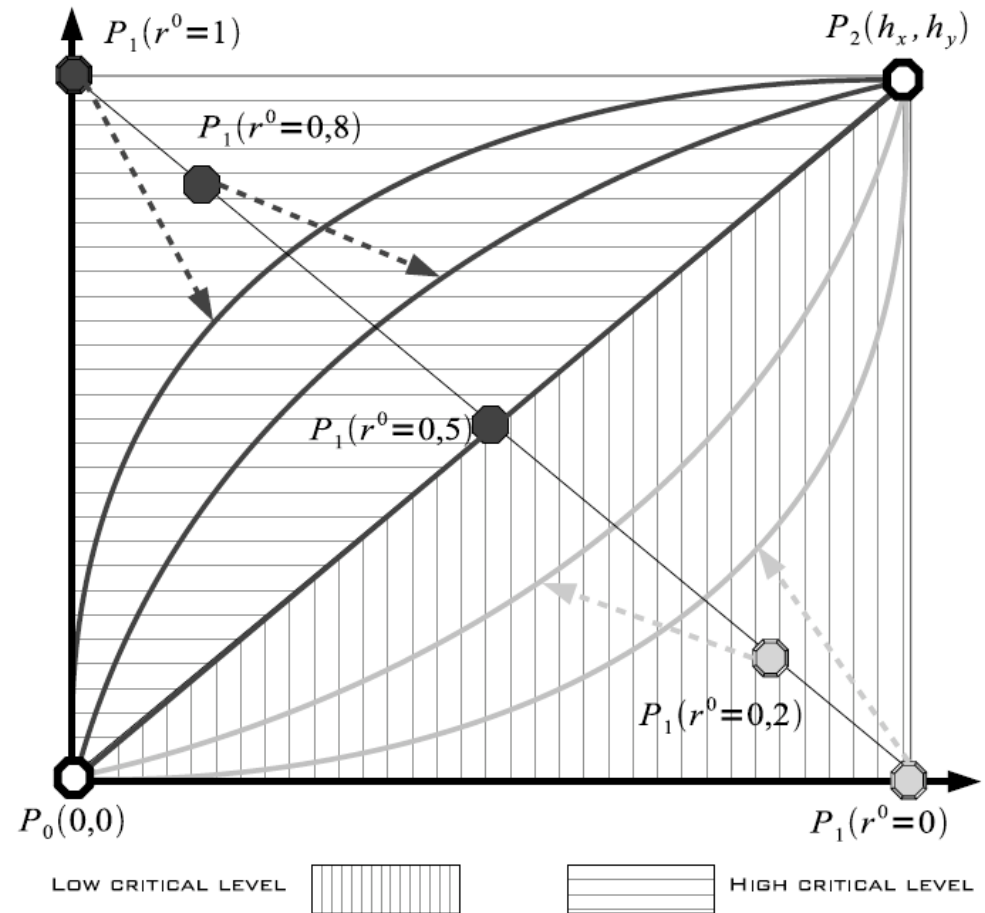
Criticality model (1)

- Link the capture rate to the size of the cover set
- High criticality
 - Convex shape
 - Most projections of x are close to the max capture speed
- Low criticality
 - Concave shape
 - Most projections of x are close to the min capture speed
- Concave and convex shapes automatically define sentry nodes in the network



Criticality model (2)

- r^0 can vary in $[0, 1]$
- Behavior functions (BV) defines the capture speed according to r^0
- $r^0 < 0.5$
 - Concave shape BV
- $r^0 > 0.5$
 - Convex shape BV
- We propose to use Bézier curves to model BV functions



Some typical capture speed

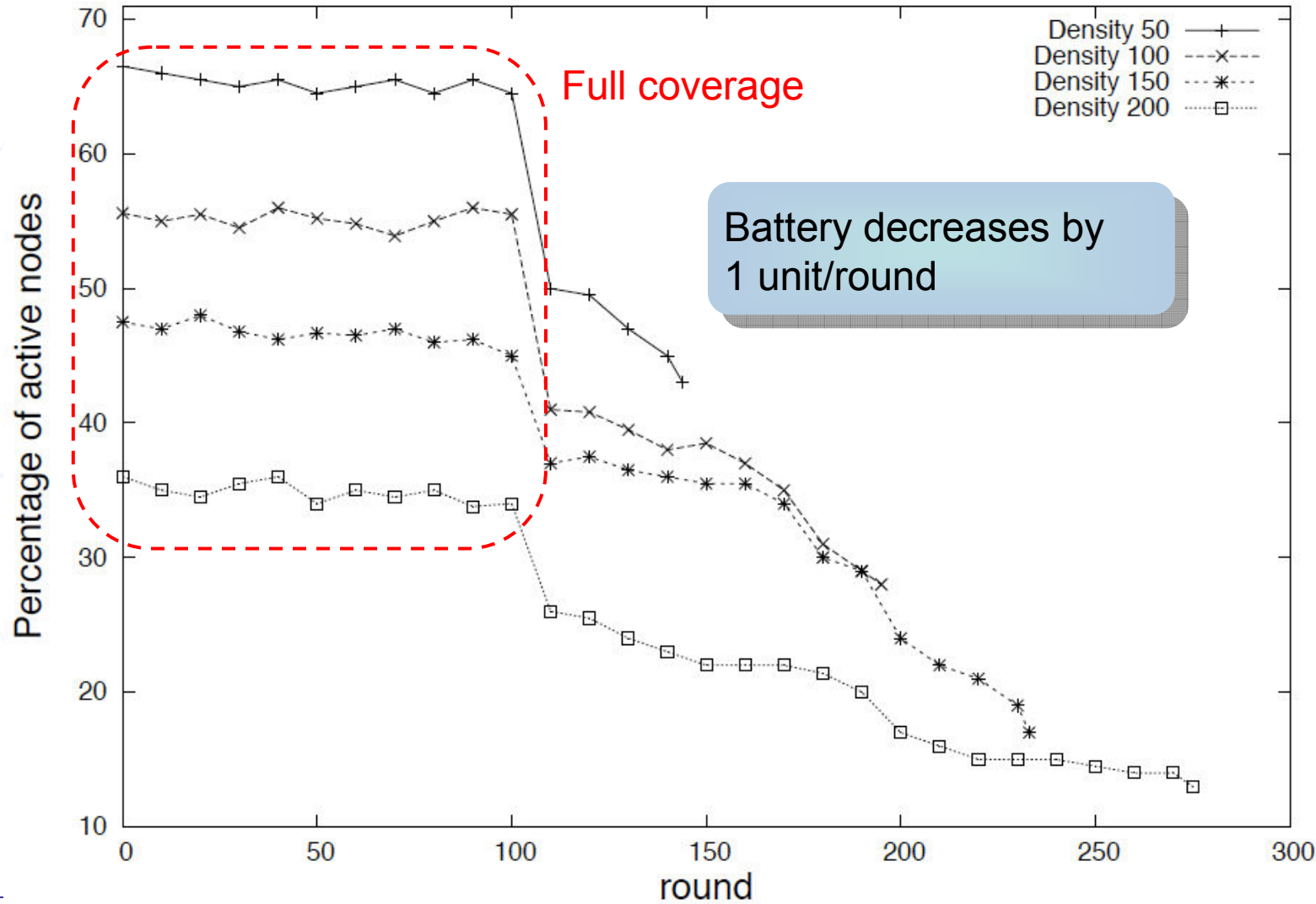
- Maximum capture speed is 6fps
- Nodes with size of cover set greater than 6 capture at the maximum speed

r^0 \ $ Co(v) $	1	2	3	4	5	6
0.0	0.05	0.20	0.51	1.07	2.10	6.00
0.2	0.30	0.73	1.34	2.20	3.52	6.00
0.5	1.00	2.00	3.00	4.00	5.00	6.00
0.8	2.48	3.80	4.66	5.27	5.70	6.00
1.0	3.90	4.93	5.49	5.80	5.95	6.00

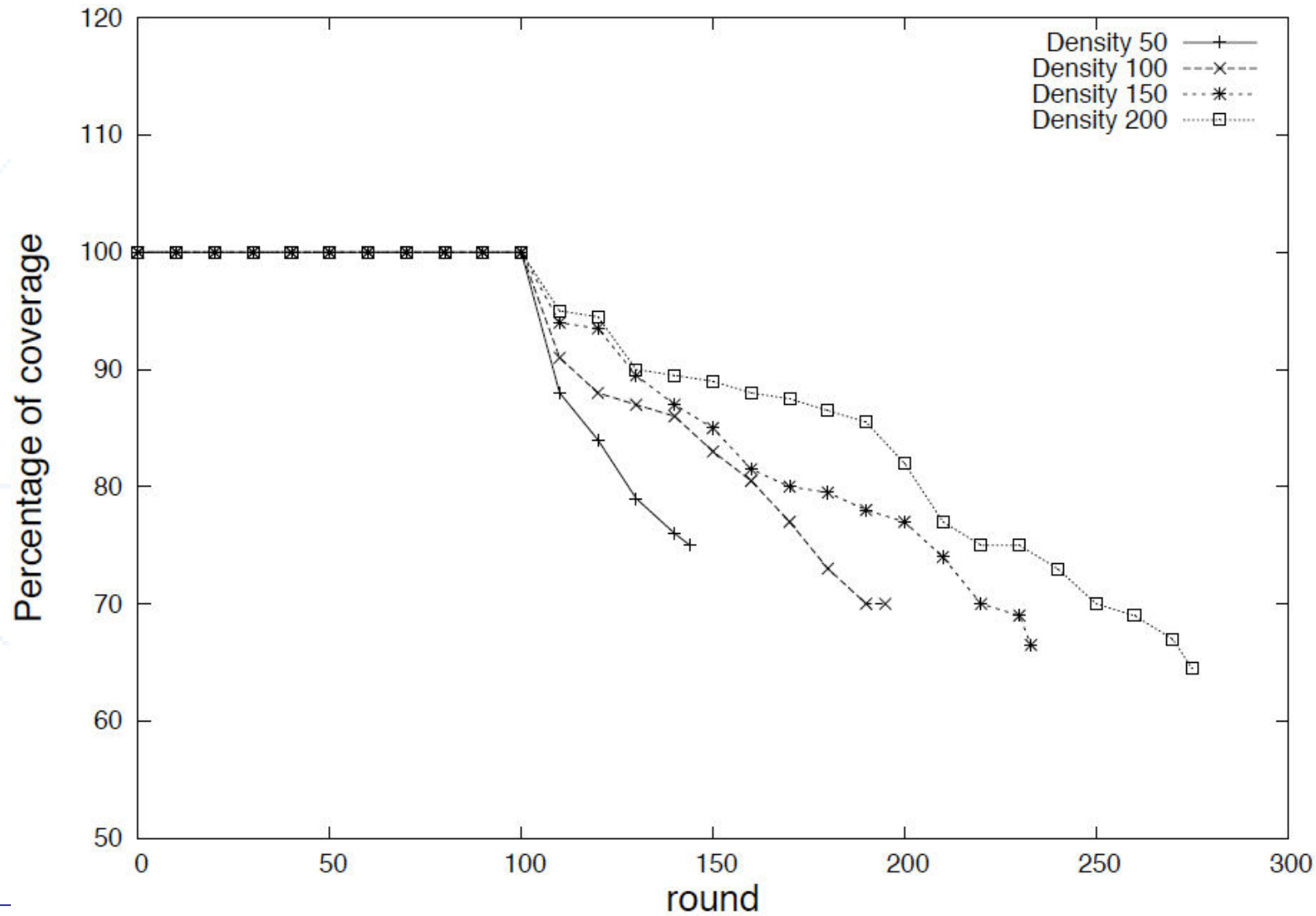
Simulation settings

- OMNET++ simulation model
- Video nodes have communication range of 30m and video sensing range of 25m, FoV is a sector of 60°
- Battery has 100 units
- Full coverage is defined as the region initially covered when all nodes are active

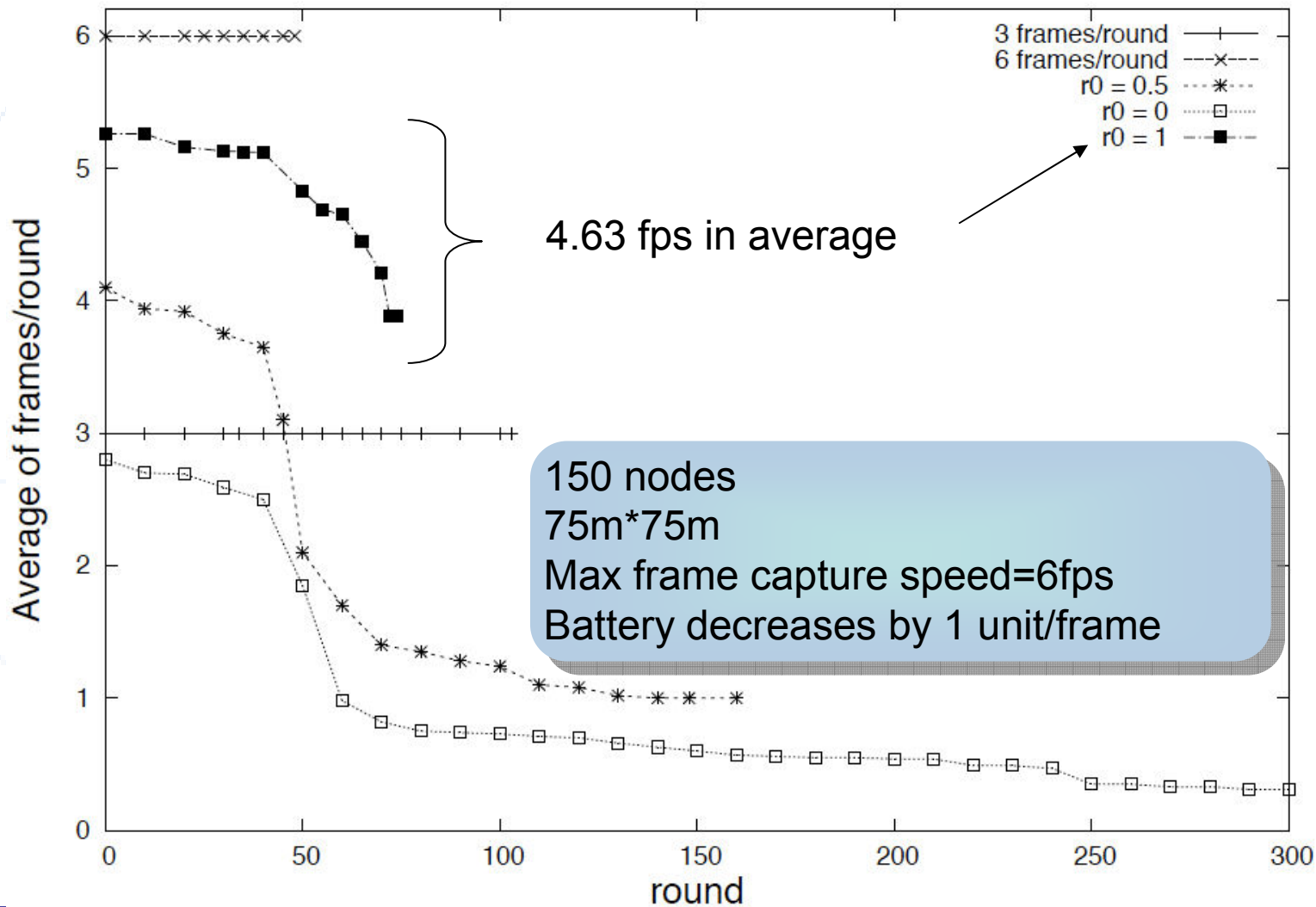
Percentage of active nodes



Percentage of coverage



Average capture speed



Conclusions & future works

- Criticality model with adaptive scheduling of nodes
- Optimize the resource usage by dynamically adjusting the provided service level
- Extension for risk-based scheduling in intrusion detection systems
- Congestion control