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
Overview

• Introduction of wireless video sensor networks
• Surveillance applications
• Coverage and scheduling
• Application Criticality
• Experimental Results
Video Sensor Node

Pan-Tilt-Zoom camera

Communication

Mobility?

$P = (x, y)$

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

- 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, $\text{FoV}_v$
- $\text{Co}_i(v) = \text{set of nodes } v' \text{ such as } \bigcup_{v' \in \text{Co}_i(v)} \text{FoV}_{v'} \text{ covers } \text{FoV}_v$
- $\text{Co}(v) = \text{set of } \text{Co}_i(v)$
Finding v’s cover set

\[ AG = \{ A \cap G \} \]
\[ BG = \{ B \cap G \} \]
\[ CG = \{ C \cap G \} \]
\[ Co(v) = AG \times BG \times CG \]

\[ A = \{ v \in N(V) : v \text{ covers the point “a” of the FoV} \} \]
\[ B = \{ v \in N(V) : v \text{ covers the point “b” of the FoV} \} \]
\[ C = \{ v \in N(V) : v \text{ covers the point “c” of the FoV} \} \]
\[ G = \{ v \in N(V) : v \text{ covers the point “g” of the FoV} \} \]

\[ Co(V) = \{ \]
\[ \{ V \}, \]
\[ \{ V 2, V 1 \}, \]
\[ \{ V 3, V 1 \}, \]
\[ \{ V 2, V 4, V 5 \}, \]
\[ \{ V 3, V 4, V 5 \} \} \]
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) Sentry node: Node with high speed capture (high cover set).
Idle node: Node with low speed capture.

(B) Alerted node: Node with high speed capture (alert intrusion).

(C) 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: \( r^2 = 0 \)
Alert mode: \( r^2 = R^2 \)
Hibernate mode (after intrusion): \( r^2 = 0 \)
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
• \( r^0 \) 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

| $r^0$ | \( |C_0(v)| \) | 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

- Full coverage
- Battery decreases by 1 unit/round
Percentage of coverage

![Graph showing percentage of coverage over rounds for different densities. The graph plots percentage of coverage on the y-axis and round on the x-axis. There are lines for Density 50, Density 100, Density 150, and Density 200, each with a different symbol and line style.]
Average capture speed

- 150 nodes
- 75m*75m
- Max frame capture speed = 6fps
- Battery decreases by 1 unit/frame

4.63 fps in average
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