“On Survivability of Mobile Cyber Physical Systems with Intrusion Detection”

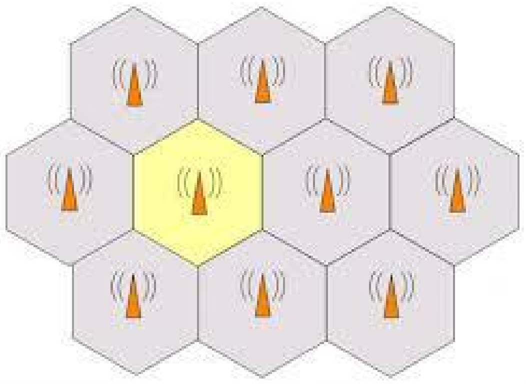
Alex Campbell, 2016-11-17

Presentation Contents

Introduction and Concepts

General Concept:

- Advancing technology leads to increased presence of **Cyber Physical Systems** (CPS)
- **Survivability** becomes more important.
- **Mobile CPSs** complicate the issue of **survivability**



Introduction and Concepts

Cyber Physical System

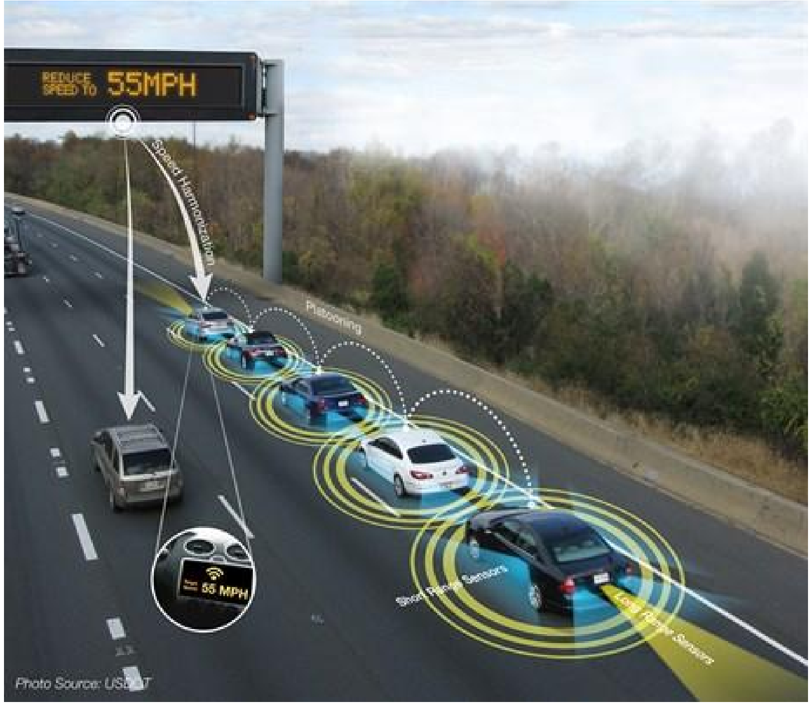
- *"Systems that are built from, and depend upon, the seamless integration of computational algorithms and physical components" [1].*
- Defining Characteristics [3]:
  - Cyber Capability in every component
  - Automated
  - Capable of Large-Scale Networking
  - Capable of optimization through dynamic reconfiguration

[1] https://www.nsf.gov/pubs/2015/nsf15541/nsf15541.htm
[2] Khaitan, S. K., & Mccalley, J. D. (2015). Design Techniques and Applications of Cyberphysical Systems: A Survey. *IEEE Systems Journal, 9*(2), 350-365. doi:10.1109/jsyst.2014.2322503

Introduction and Concepts

CPS Examples

- Process Control Systems
- Medical monitors
- Autonomous (self-driving) Vehicles



Introduction and Concepts

Mobile Cyber Physical System

- Subcategory of a **CPS**
- Inherently mobile
- Examples [4]:
  - Smartphone network
  - Environmental monitoring systems
- Applications[5]:
  - Traffic Measuring System
  - IoT

[4] http://reu-mcps.cs.txstate.edu/home.html
[5] Rose, G. (2006). "Mobile Phones as Traffic Probes: Practices, Prospects and Issues". *Transport Reviews*. **26** (3): 275–291

Problem Statement and Challenges

Problem:

“[Maximize the survivability of] a mobile cyber physical system (MCPS) comprising sensor-carried human actors, vehicles, or robots assembled together for executing a specific mission in battlefield or emergency response situations.”

- Maximize uptime of MCPS
- Mission critical scenarios
- Protect against malicious attacks, unauthorized intrusions

Problem Statement and Challenges

Challenges:

- Distributed architecture
- Large Scale
- Rough / Dangerous environmental Conditions
- Resource Constraints

Main point: scenarios include possibilities of:

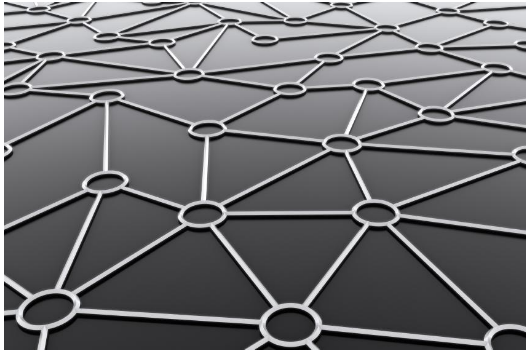
- Compromised / captured nodes
- Inability to replenish nodes

A REMBASS-II sensor

Literature Overview

<u>Literature: For survivability, design MCP systems that promote:</u>

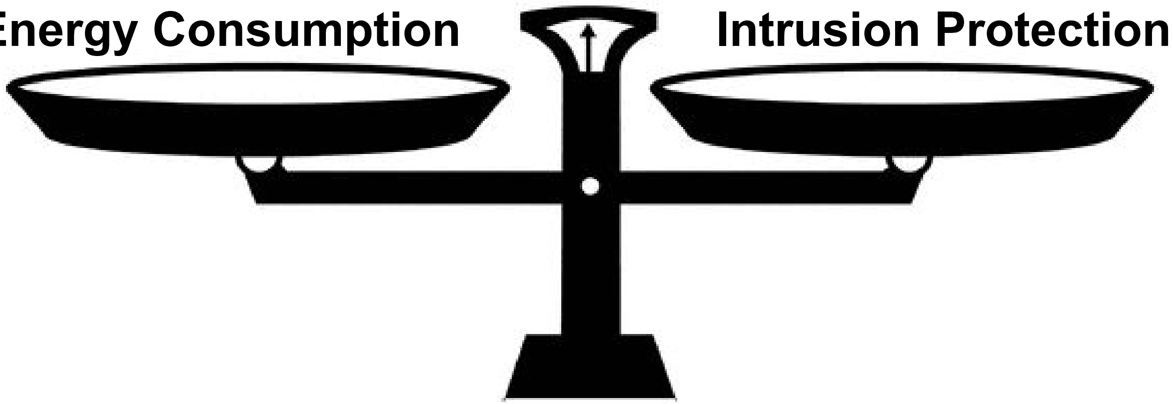
- Intrusion Prevention
- Intrusion Detection
  - Application-specific Intrusion detection
  - Anomaly-based detection
- Intrusion Tolerance
  - Static / Structural
    - Redundancy: component, path, data
    - Threshold Cryptography (cooperative decryption).
    - Decentralization
  - Dynamic / Responsive:
    - Self-Organization
    - Dynamic Routing
    - Forward / Backward Recovery



Literature Overview

Complicating Factor absent from Literature:

Survivability



Both **Energy Depletion** and **Security Failures** constitute failure of an MCPS!

Proposed Solution

Solution: Perform a mathematical-model-based analysis to maximize **Survivability**

- Model an MCPS with Dynamic Voting-based Intrusion Detection
- Optimally balance intrusion detection energy conservation

Designing the System Model

Reference System: Distributed network of 128 nodes, where each node contains

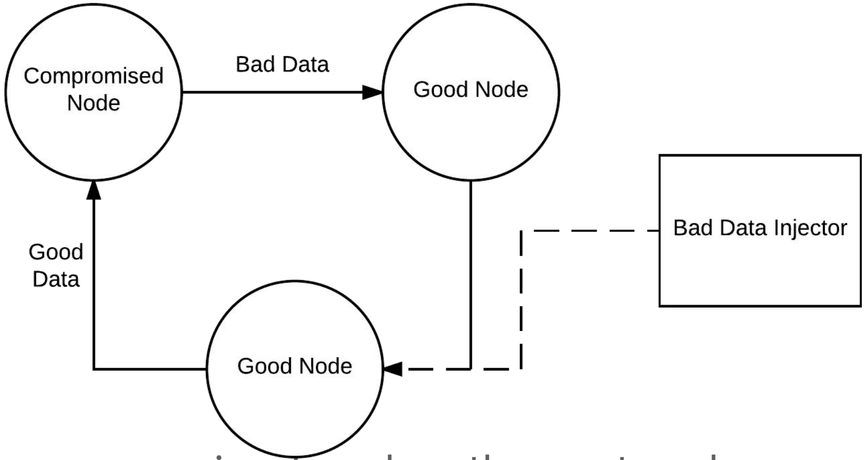
- 600 MHz Analog Devices Blackfin DSP Processor
- 8MB flash memory
- 64MB SDRAM
- GPS Receiver
- 7.5 V battery
- Sensors (inertial, barometric, physiological, radiological, environmental).

Purpose: Detect nearby phenomena, transmit information to neighbors to perform localization and remote sensing (collect data without making physical contact with the object [Wikipedia].

Designing the System Model

<u>Attack Model:</u> Two Types:

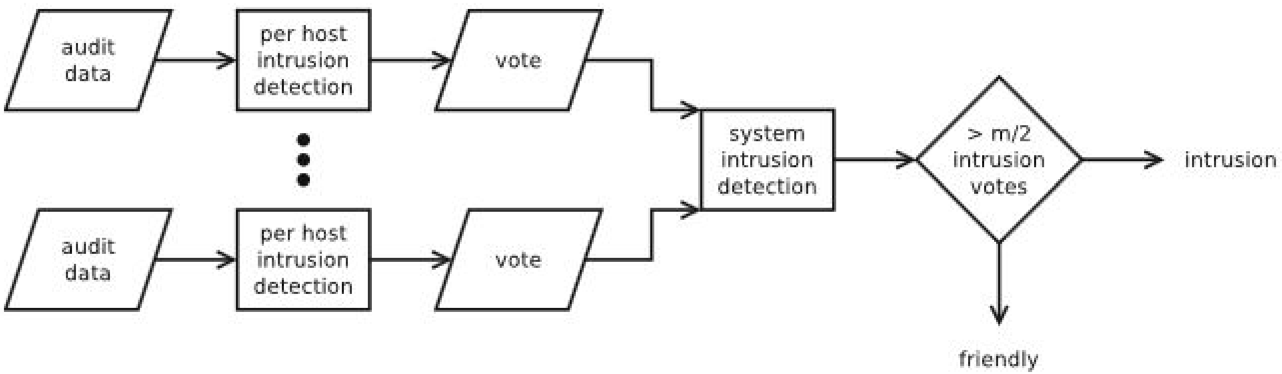
- Node Capture
  - Defeats Authentication
  - Creates Insider Threats
- Bad Data Injection
  - Defeats integrity of data
  - Defended against by insiders



Assumption: When the system contains ⅓ compromised nodes, the system has failed (Byzantine Fault Model). Once a consensus cannot be reached (due to fear of malicious nodes), the system has failed.

Designing the System Model

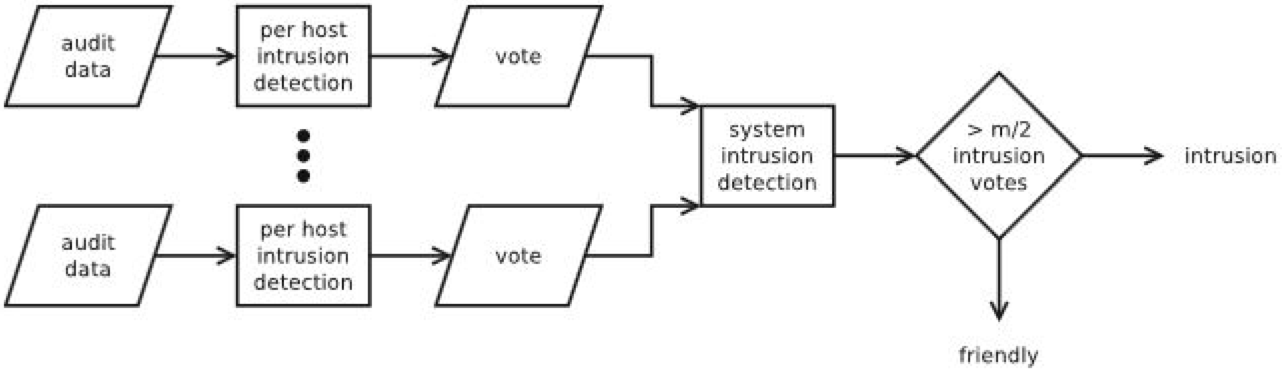
Intrusion Detection Technique: Dynamic voting-based intrusion detection



- Detection informed by location/distance data anomalies between neighbors
- A “coordinator” node is chosen amongst neighbors at random to prevent specific targeting by attackers
- Coordinator selects *m* random nodes to participate in labeling nodes as good/bad

Designing the System Model

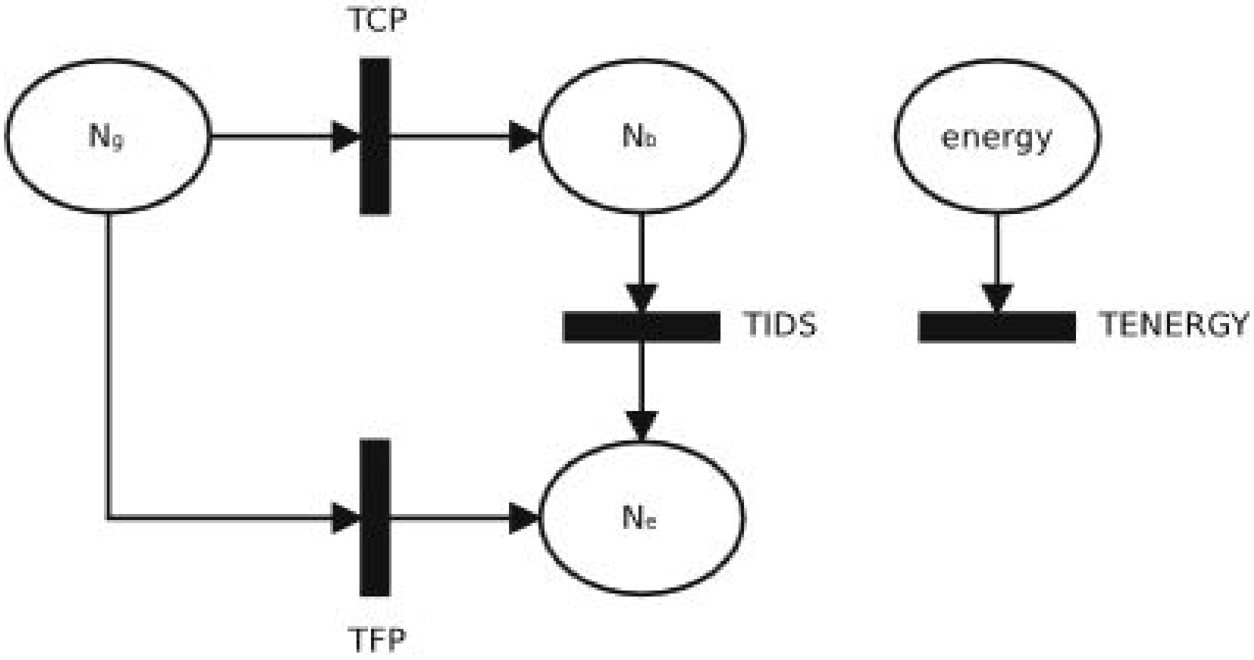
Intrusion Detection Technique: Dynamic voting-based intrusion detection



Main Point: Predict the number of good/bad nodes as a result of compromising events happening in the system, coupled with voting-based intrusion detection.

Designing the System Model

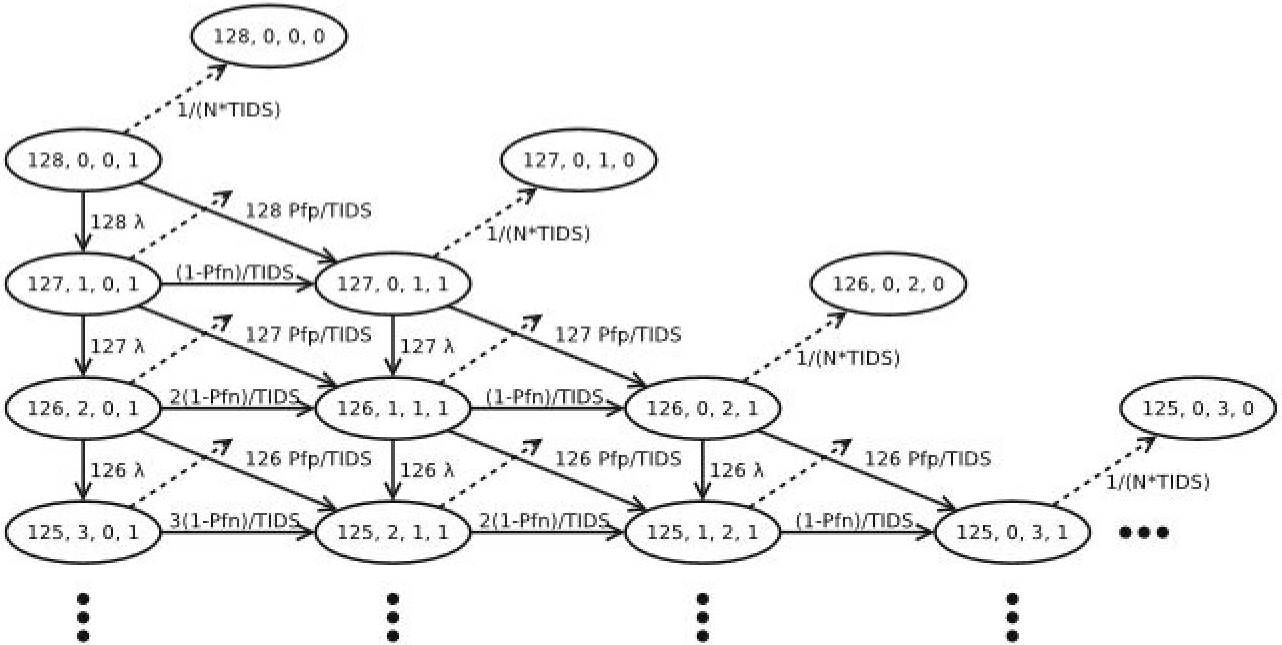
Modeling the system in regards to intrusions and energy consumption:

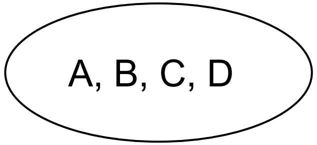


Ng	# Good Nodes
Nb	# Bad Nodes
Ne	# Nodes Evicted
T_{IDS}	Intrusion Detection Interval
energy	Binary, 1=full energy, 0=exhaustion
λ	Compromise Rate
Pfn	P(false negative)
Pfp	P(false positive)
TIDS	Dynamic Voting Invocation Interval
TCP	Good node get compromised. Rate: **λ x Ng**
TIDS	Evict Bad Node: $\frac{N_b \times (1-\mathcal{P}_{fn})}{T_{IDS}}$
TFP	Evict Good Node: $\frac{N_g \times \mathcal{P}_{fp}}{T_{IDS}}$
TENERGY	Energy is Exhausted: $\frac{1}{N \times T_{IDS}}$

Designing the System Model

Equivalent Semi-Markov Model:

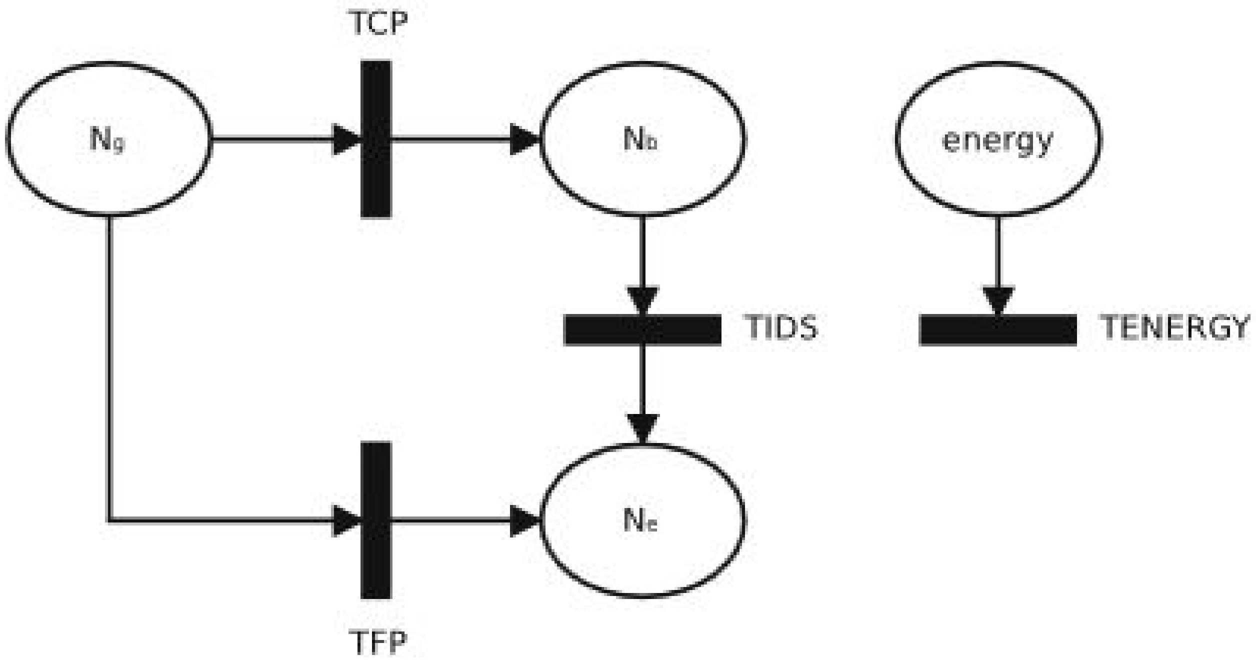




A	Ng
B	Nb
C	Ne
D	energy

Designing the System Model

Modeling the system in regards to intrusions and energy consumption:



Important Concepts:

- Tokens = nodes in MCPS
- Initialize 128 Good nodes
- Pfn, Pfp, and λ are used as input parameters to the underlying markov chain.
- Use to calculate expected values for each state at time *t.*
- Use these expected values to solve for Pfn and Pfp at time *t*.
- Adjust Transitions TIDS and TFP to model changes to Pfn and Pfp.

Designing the System Model

Solving for Pfn and Pfp:

$$\mathcal{P}_{\mathrm{fn}} = \sum_{i=0}^{m-N_{\mathrm{maj}}} \left[\frac{\binom{N_{\mathrm{b}}}{N_{\mathrm{maj}}+i}\binom{N_{\mathrm{g}}}{m-(N_{\mathrm{maj}}+i)}}{\binom{N_{\mathrm{g}}+N_{\mathrm{b}}}{m}} \right] + \sum_{j=0}^{m-N_{\mathrm{maj}}} \left[\frac{\binom{N_{\mathrm{b}}}{j} \sum_{k=N_{\mathrm{maj}}-j}^{m-j} \left[\binom{N_{\mathrm{g}}}{k} (p_{\mathrm{fn}})^k \binom{N_{\mathrm{g}}-k}{m-j-k} (1-p_{\mathrm{fn}})^{(m-j-k)} \right]}{\binom{N_{\mathrm{g}}+N_{\mathrm{b}}}{m}} \right] \quad (1)$$

Probability of a false negative due to selecting a majority of bad nodes

Probability of a false negative due to:

1. *Selecting a majority of good nodes that cast incorrect votes*
2. *Including some bad nodes*

$$\mathcal{P}_{\mathrm{fp}} = \sum_{i=0}^{m-N_{\mathrm{maj}}} \left[\frac{\binom{N_{\mathrm{b}}}{N_{\mathrm{maj}}+i}\binom{N_{\mathrm{g}}}{m-(N_{\mathrm{maj}}+i)}}{\binom{N_{\mathrm{g}}+N_{\mathrm{b}}}{m}} \right] + \sum_{j=0}^{m-N_{\mathrm{maj}}} \left[\frac{\binom{N_{\mathrm{b}}}{j} \sum_{k=N_{\mathrm{maj}}-j}^{m-j} \left[\binom{N_{\mathrm{g}}}{k} (p_{\mathrm{fp}})^k \binom{N_{\mathrm{g}}-k}{m-j-k} (1-p_{\mathrm{fp}})^{(m-j-k)} \right]}{\binom{N_{\mathrm{g}}+N_{\mathrm{b}}}{m}} \right] \quad (2)$$

Probability of a false positive due to selecting a majority of bad nodes

Probability of a false positive due to:

1. *Selecting a majority of good nodes that cast incorrect votes*
2. *Including some bad nodes*

Designing The System Model

Calculate MTTF via Reward Assignments:

- Recall that we want to optimize the MCPS Survivability
- Survivability is equivalent to the system's expected lifetime, or MTTF
- Let Ri, reward assignment at state i, be:
  - Ri = 1 if the system is alive in state i
  - Ri = 0 if the system is dead in state i
  - System is dead when:
    - Place "Energy" does not have a token
    - The number of tokens when Nb > (⅓)(Nb + Ng)
      - Number of bad nodes comprises at least 1.3 of all nodes in system
- P_{fp}, P_{fn}, and T_{IDS} all affect transition rates, and therefore MTTF

Designing the System Model

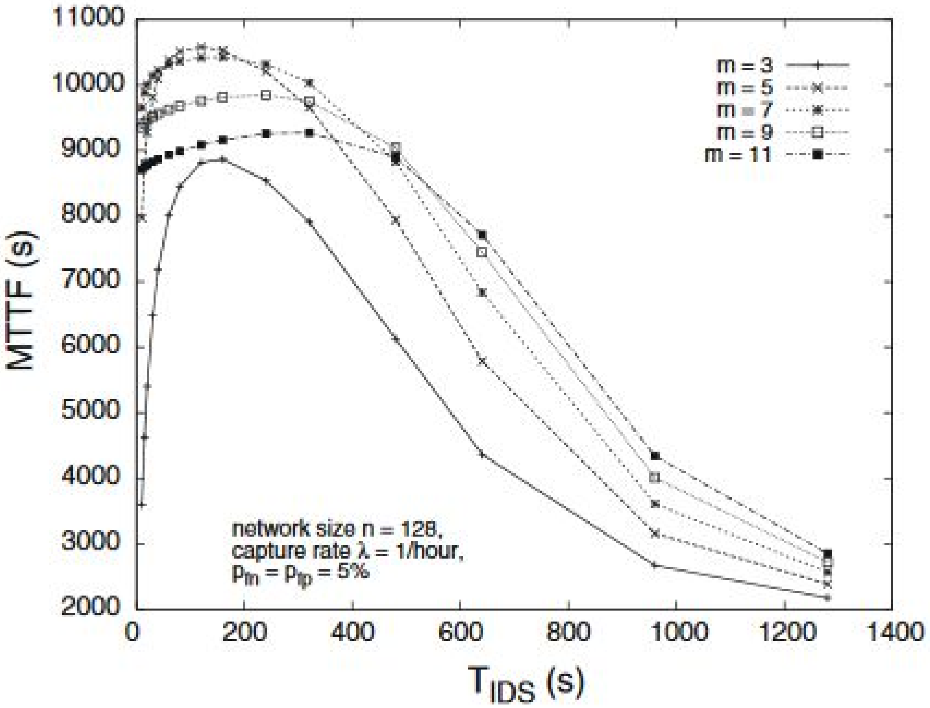
Parameter	Meaning	Default value
n	Network size	128
$\bar{n}$	Number of neighbors within radio range	32
p_{fn}	Per-host false negative probability	[1–5]%
p_{fp}	Per-host false positive probability	[1–5]%
λ	Per-node capture rate	[1–24]/day
T_{IDS}	Intrusion detection interval	[0–700] s
m	Number of intrusion detectors per node	[3,11]
α	Number of ranging operations	5
E_{t}	Energy for transmission per node	0.000125 J
E_{r}	Energy for reception per node	0.00005 J
E_{a}	Energy for analyzing data per node	0.00174 J
E_{s}	Energy for sensing per node	0.0005 J
E_{o}	Initial system energy	16,128 kJ
$\mathcal{P}_{\mathrm{fn}}$	System false negative probability	Eq. 1
$\mathcal{P}_{\mathrm{fp}}$	System false positive probability	Eq. 2
MTTF	Mean time to failure	Eq. 3
N	Maximum cycles before energy exhaustion	Eq. 4
$E_{T_{\mathrm{IDS}}}$	Energy consumed per T_{IDS}	Eq. 5

$$E_{\mathrm{detection}} = m \times (E_{\mathrm{t}} + \bar{n} \cdot E_{\mathrm{r}}) + m \times (E_{\mathrm{t}} + (m-1) \cdot (E_{\mathrm{r}} + E_{\mathrm{a}})). \qquad (8)$$

Running the simulation

Theoretical Results:

- m = #nodes selected for voting
- Optimal Intrusion detection interval (T_{IDS}) is roughly 200 seconds
- Optimal T_{IDS} value decreases as m decreases: weaker intrusion detection means more invocations
- Optimally, m = 5. Best balance of energy exhaustion and security failure.



Running the simulation

- Use a simulation modeling library, SMPL, to:
  - Track node state (goodness, membership)
  - Schedule events
  - Monitor system failure based on events:
    - Security failure
    - Exhausted Energy
    - All nodes have been evicted
- Parameterize values:
  - λ from 1/day to 1/10 minutes
  - m from [3,11]
  - T_{IDS} from 10s to 1280s
- Apply BMA for 95% confidence level and 10% accuracy:
  - 100 MTTF Observations

Running the simulation: SMPL Results

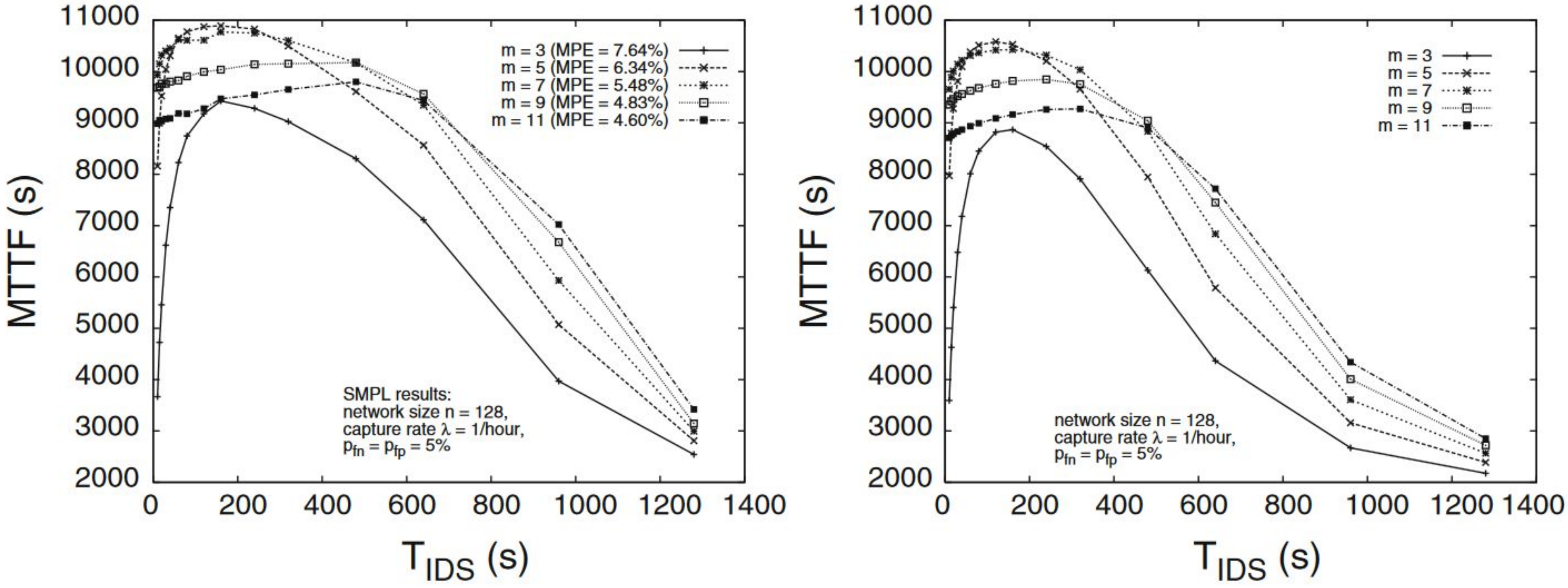


Fig. 7 Simulation and theoretical MTTF versus T_{IDS} and m

Running the simulation

Remarks:

- Theoretical and Simulation plot shapes are very similar
- For both, MTF peaks near TIDS = 160s between 9000 and 11,000s
- m = 5 is the optimal value for m in both cases
- The Mean Percentage Error (MPE) between the two is between 4.60 and 7.64%

Main Point: Survivability analysis methodology is validated due to similarities between results.

Conclusions and Future Work

- This paper demonstrated the feasibility of the authors' survivability model for Mobile Cyber Physical Systems with voting-based intrusion detection.
  - Given known values for false alarm probabilities and node compromise rates, the model can determine the best intrusion detection interval and the best number of detectors to maximize MTTF.
- Future work may include discussions concerning design principles for intrusion detection protocols in both homogenous AND heterogenous MCPSs.