The 7th IEEE International Workshop on
Information Forensics and Security

Rome, Italy, 16-19 November, 2015

UNIVERSITY *of* GREENWICH

Cyber-physical intrusion detection on a robotic vehicle

Tuan Vuong, George Loukas and Diane Gan
University of Greenwich,
London, UK

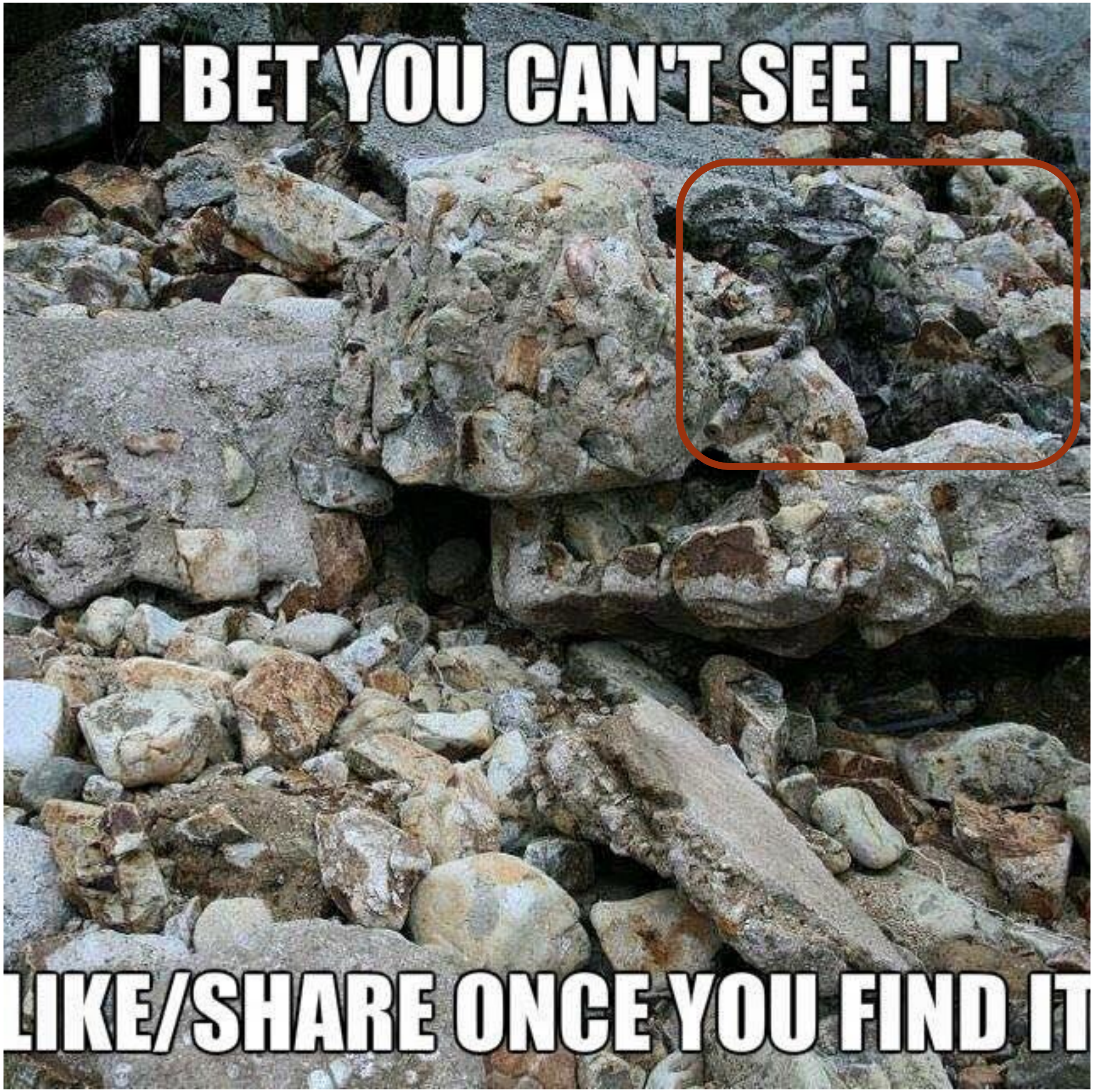
Look for:

- Hidden threat

Source: Internet

How about:

- Motion detection
- Heat map

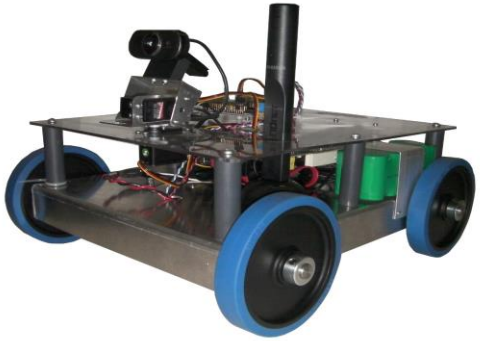


Camouflaged sniper with a rifle

Source: Internet

Robotic vehicles

- Our Cyber-Physical System (CPS) testbed:
  - Computer-control: Linux laptop
  - Control physical entities: Wheels, Batteries, Camera, Accelerometer, …
  - Network of interacting elements: Wifi, Ethernet



- CPS samples:

automated driving

source: Carnegie Mellon University

human-robot collaboration

source: Rethink Robotics

Smart grids

source: Siemens

automated farming

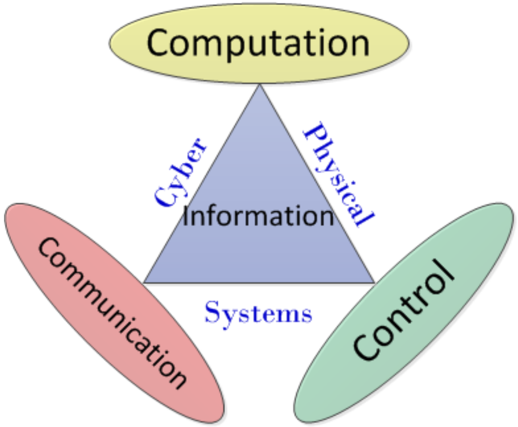
source: Kesmac

surgical robots

source: daVinci

Air traffic control

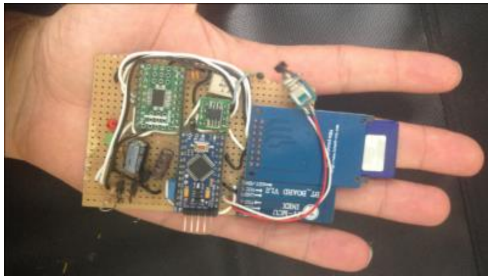
source: NASA



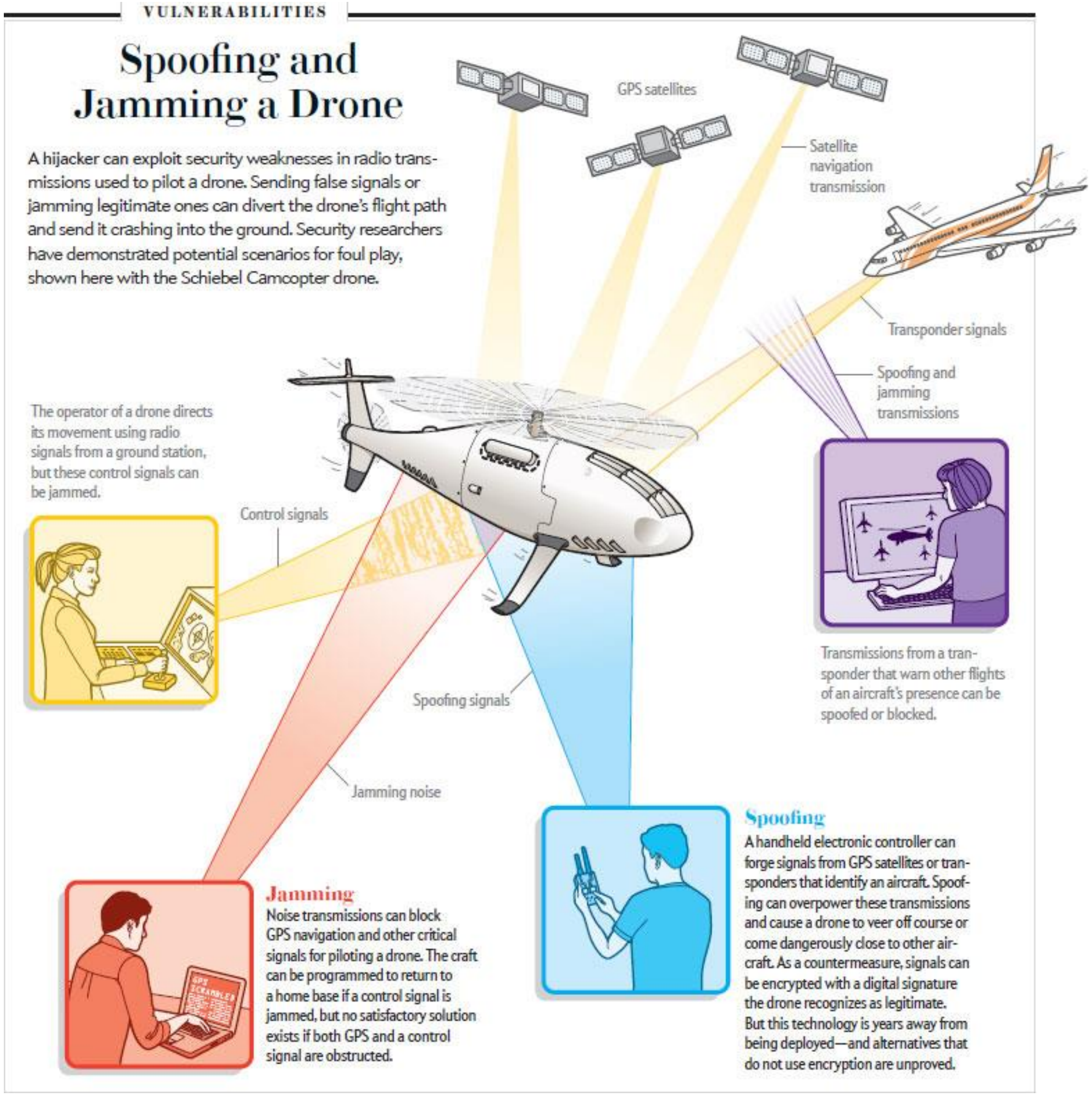
Source: Wu 2011

Security Challenges

- Hack-a-car[1]:
  - 02/2014, Wired, $20
  - Windows, lights, steering, brakes



- Kill a jeep in highway[2]:
  - 07/2015, Wireless
  - Dashboard, steering, brakes, transmission



VULNERABILITIES

Spoofing and Jamming a Drone

A hijacker can exploit security weaknesses in radio transmissions used to pilot a drone. Sending false signals or jamming legitimate ones can divert the drone's flight path and send it crashing into the ground. Security researchers have demonstrated potential scenarios for foul play, shown here with the Schiebel Camcopter drone.

The operator of a drone directs its movement using radio signals from a ground station, but these control signals can be jammed.

Transmissions from a transponder that warn other flights of an aircraft's presence can be spoofed or blocked.

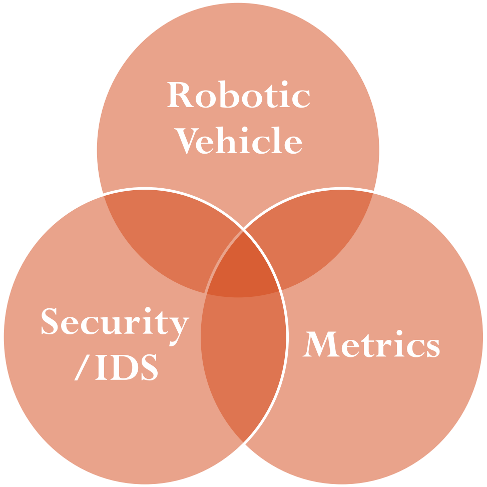
Jamming
Noise transmissions can block GPS navigation and other critical signals for piloting a drone. The craft can be programmed to return to a home base if a control signal is jammed, but no satisfactory solution exists if both GPS and a control signal are obstructed.

Spoofing
A handheld electronic controller can forge signals from GPS satellites or transponders that identify an aircraft. Spoofing can overpower these transmissions and cause a drone to veer off course or come dangerously close to other aircraft. As a countermeasure, signals can be encrypted with a digital signature the drone recognizes as legitimate. But this technology is years away from being deployed—and alternatives that do not use encryption are unproved.

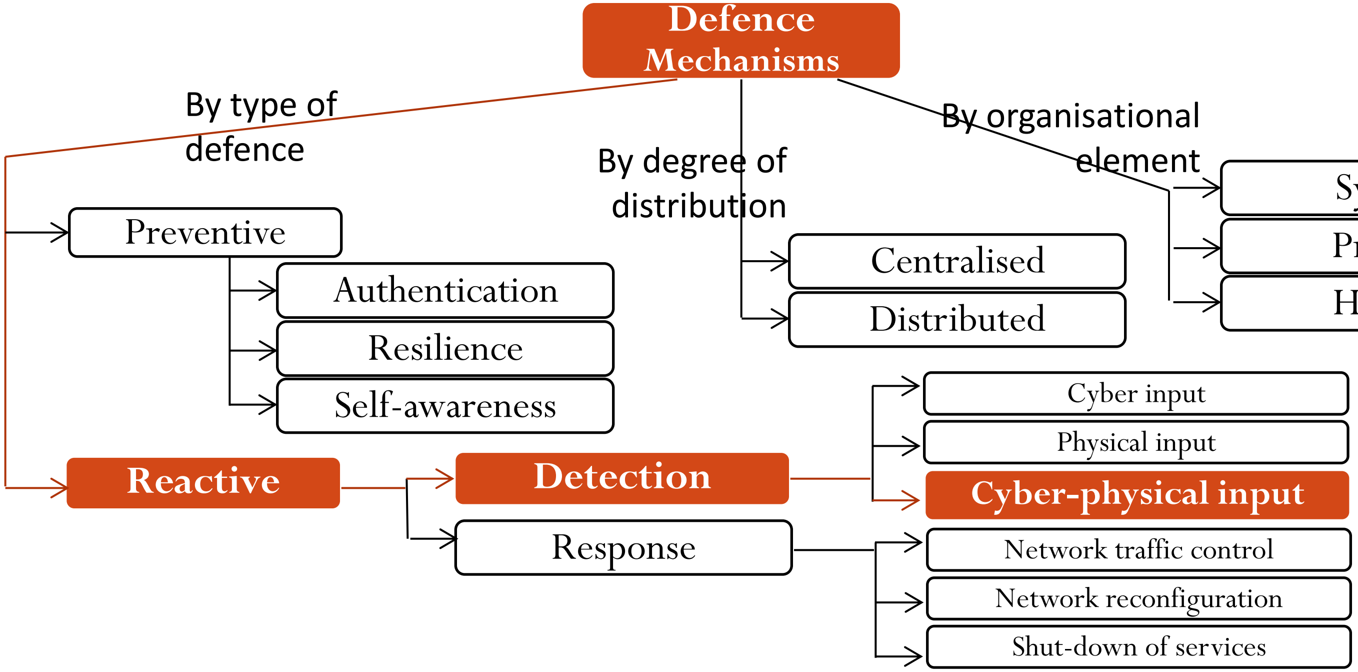
- Spoofing and jamming a drone[3]

Aims

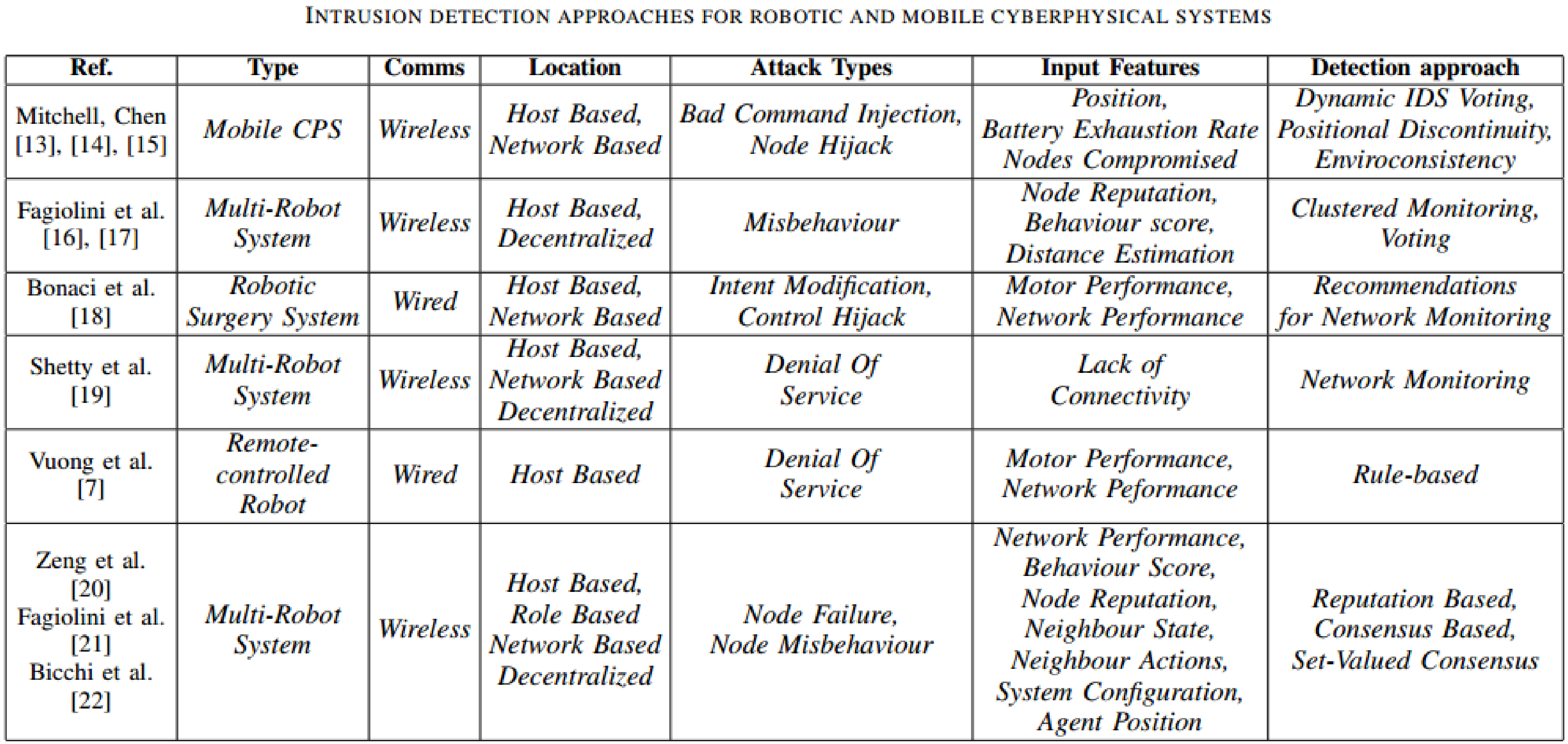
- **Research aims:**
  - Light-weight on-board system for robotic vehicle
  - Cyber attack detection using both cyber and physical features.
  - Performance metrics for intrusion detection in CPS.



Applying Machine Learning to Robotic Vehicle's Intrusion Detection



Intrusion detection approaches



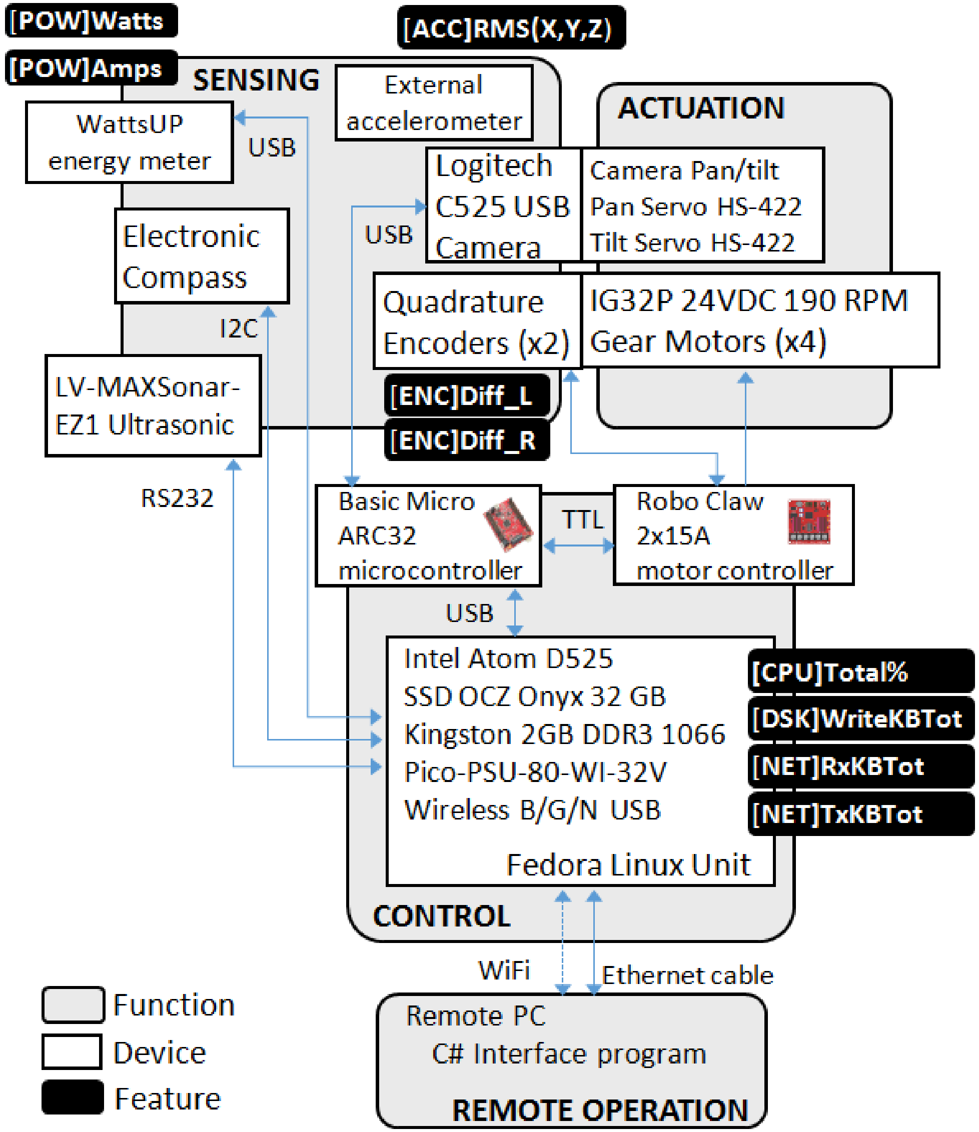
INTRUSION DETECTION APPROACHES FOR ROBOTIC AND MOBILE CYBERPHYSICAL SYSTEMS

Year:	Ref.	Type	Comms	Location	Attack Types	Input Features	Detection approach
2011-2013	Mitchell, Chen [13], [14], [15]	*Mobile CPS*	*Wireless*	*Host Based, Network Based*	*Bad Command Injection, Node Hijack*	*Position, Battery Exhaustion Rate Nodes Compromised*	*Dynamic IDS Voting, Positional Discontinuity, Enviroconsistency*
2008-2009	Fagiolini et al. [16], [17]	*Multi-Robot System*	*Wireless*	*Host Based, Decentralized*	*Misbehaviour*	*Node Reputation, Behaviour score, Distance Estimation*	*Clustered Monitoring, Voting*
2015	Bonaci et al. [18]	*Robotic Surgery System*	*Wired*	*Host Based, Network Based*	*Intent Modification, Control Hijack*	*Motor Performance, Network Performance*	*Recommendations for Network Monitoring*
2014	Shetty et al. [19]	*Multi-Robot System*	*Wireless*	*Host Based, Network Based Decentralized*	*Denial Of Service*	*Lack of Connectivity*	*Network Monitoring*
2014	Vuong et al. [7]	*Remote-controlled Robot*	*Wired*	*Host Based*	*Denial Of Service*	*Motor Performance, Network Peformance*	*Rule-based*
2014 2014 2008	Zeng et al. [20] Fagiolini et al. [21] Bicchi et al. [22]	*Multi-Robot System*	*Wireless*	*Host Based, Role Based Network Based Decentralized*	*Node Failure, Node Misbehaviour*	*Network Performance, Behaviour Score, Node Reputation, Neighbour State, Neighbour Actions, System Configuration, Agent Position*	*Reputation Based, Consensus Based, Set-Valued Consensus*

- Intrusion Detection goals

1. **Common attacks**
2. **Light-weight**
3. **On-board**
4. **Cyber &physical features**

Components



[POW]Watts

[POW]Amps

SENSING

WattsUP energy meter

USB

External accelerometer

[ACC]RMS(X,Y,Z)

Electronic Compass

I2C

Logitech C525 USB Camera

USB

Quadrature Encoders (x2)

[ENC]Diff_L

[ENC]Diff_R

LV-MAXSonar-EZ1 Ultrasonic

RS232

ACTUATION

Camera Pan/tilt
Pan Servo HS-422
Tilt Servo HS-422

IG32P 24VDC 190 RPM Gear Motors (x4)

Basic Micro ARC32 microcontroller

TTL

Robo Claw 2x15A motor controller

USB

Intel Atom D525
SSD OCZ Onyx 32 GB
Kingston 2GB DDR3 1066
Pico-PSU-80-WI-32V
Wireless B/G/N USB

Fedora Linux Unit

[CPU]Total%

[DSK]WriteKBTot

[NET]RxKBTot

[NET]TxKBTot

CONTROL

WiFi

Ethernet cable

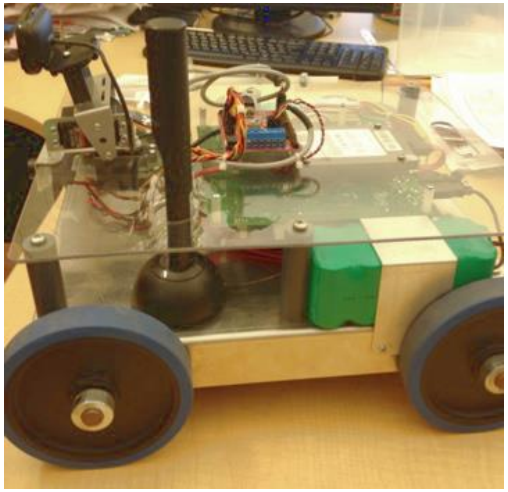
Remote PC
C# Interface program

REMOTE OPERATION

▭ Function

□ Device

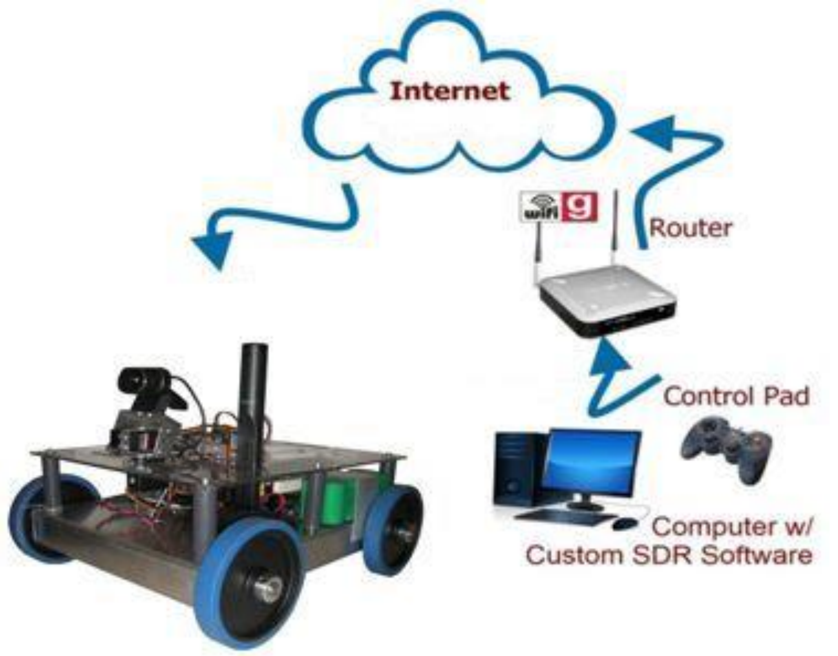
■ Feature



Indicators	Function	Data Sources
Encoders	Sensing	Robot
Power	Sensing	PC
Accelerometers	Sensing	Smart Phone
CPU Data	Control	Robot
Network	Control	Robot
Disk Data	Control	Robot

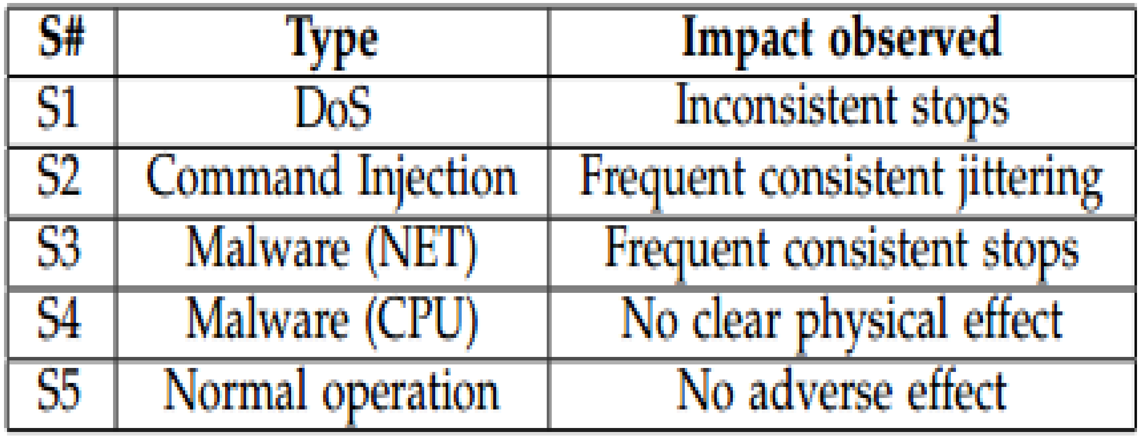
Attacking scenarios

Attacking Computers



EXPERIMENTAL SCENARIOS

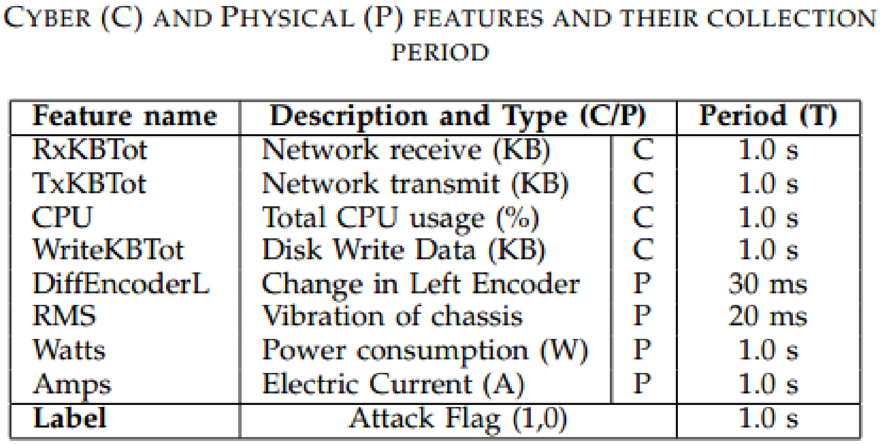
Conditions
TCP traffic flood
Rogue cmd “STOP” or “LEFT”
Modify NET control setting
Resource-demanding tasks
Camera feed + legitimate cmd



S#	Type	Impact observed
S1	DoS	Inconsistent stops
S2	Command Injection	Frequent consistent jittering
S3	Malware (NET)	Frequent consistent stops
S4	Malware (CPU)	No clear physical effect
S5	Normal operation	No adverse effect

Features & Labelling

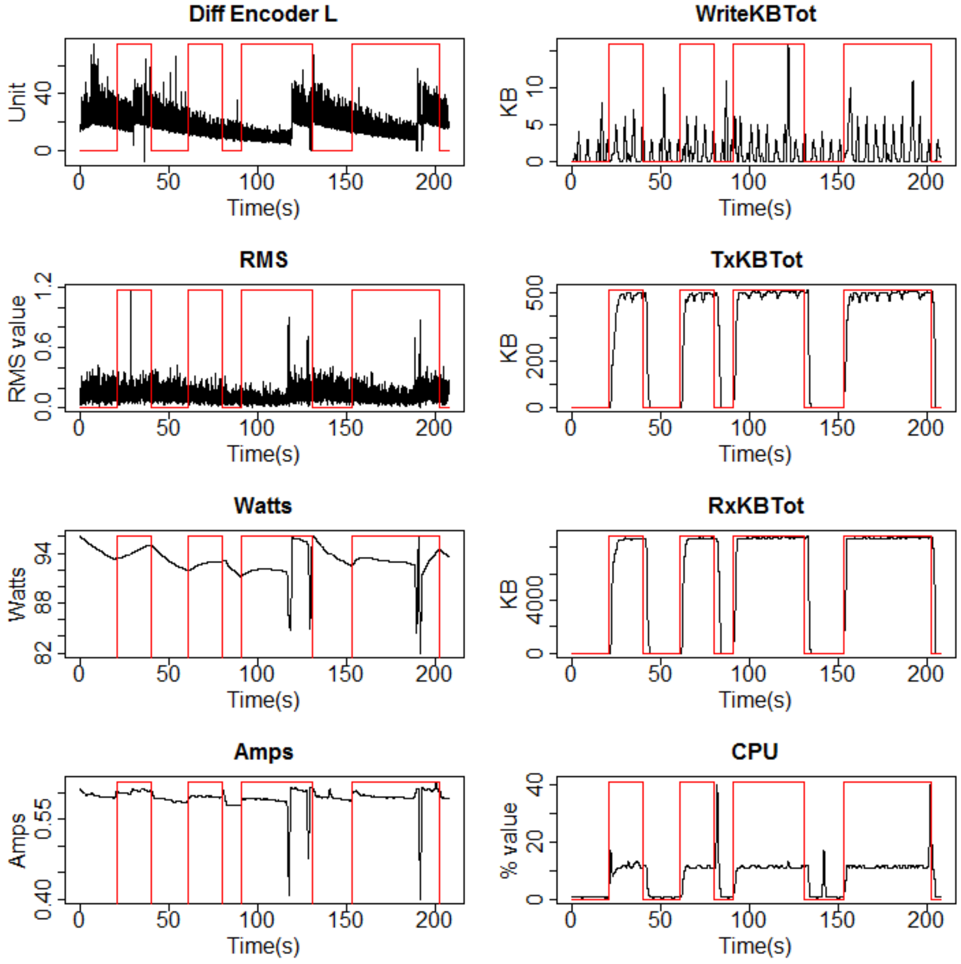
- Data collection
  - Features: 8 + 1 labelling (ground truth)
  - Each has different sample rate
  - Collected 52,215 points per feature



CYBER (C) AND PHYSICAL (P) FEATURES AND THEIR COLLECTION PERIOD

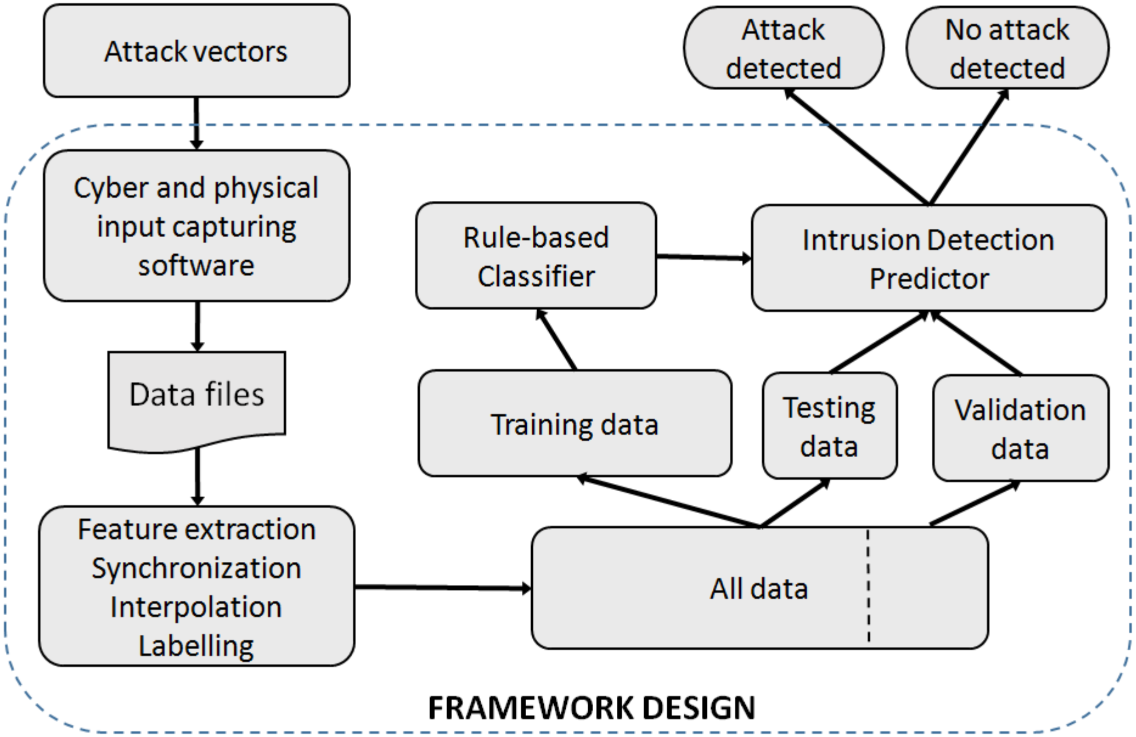
Feature name	Description and Type (C/P)		Period (T)
RxKBTot	Network receive (KB)	C	1.0 s
TxKBTot	Network transmit (KB)	C	1.0 s
CPU	Total CPU usage (%)	C	1.0 s
WriteKBTot	Disk Write Data (KB)	C	1.0 s
DiffEncoderL	Change in Left Encoder	P	30 ms
RMS	Vibration of chassis	P	20 ms
Watts	Power consumption (W)	P	1.0 s
Amps	Electric Current (A)	P	1.0 s
Label	Attack Flag (1,0)		1.0 s

- Data during DoS attack scenario



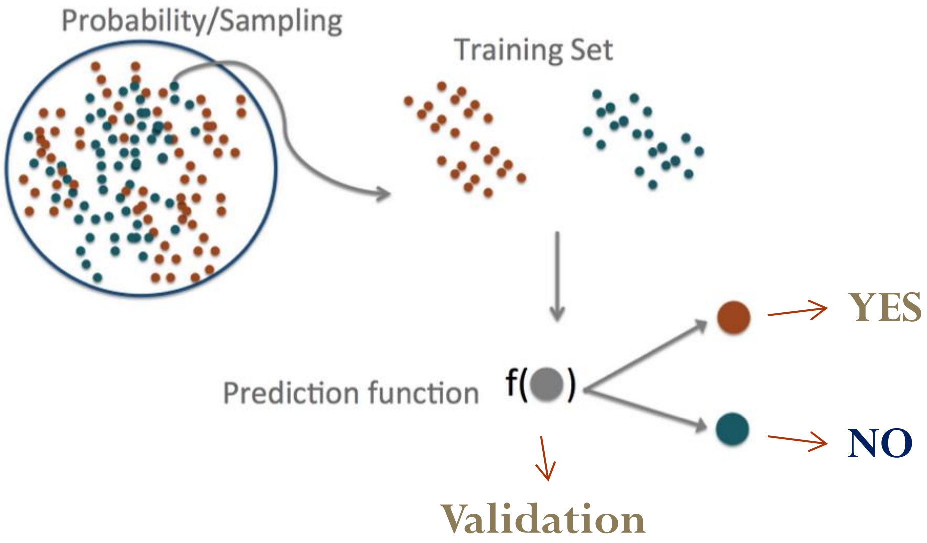
Framework

- Data preparation:
  - 5 scenarios
  - Cyber & physical data from different sources
  - Feature extraction
  - Synchronization
  - Interpolation
  - Labelling

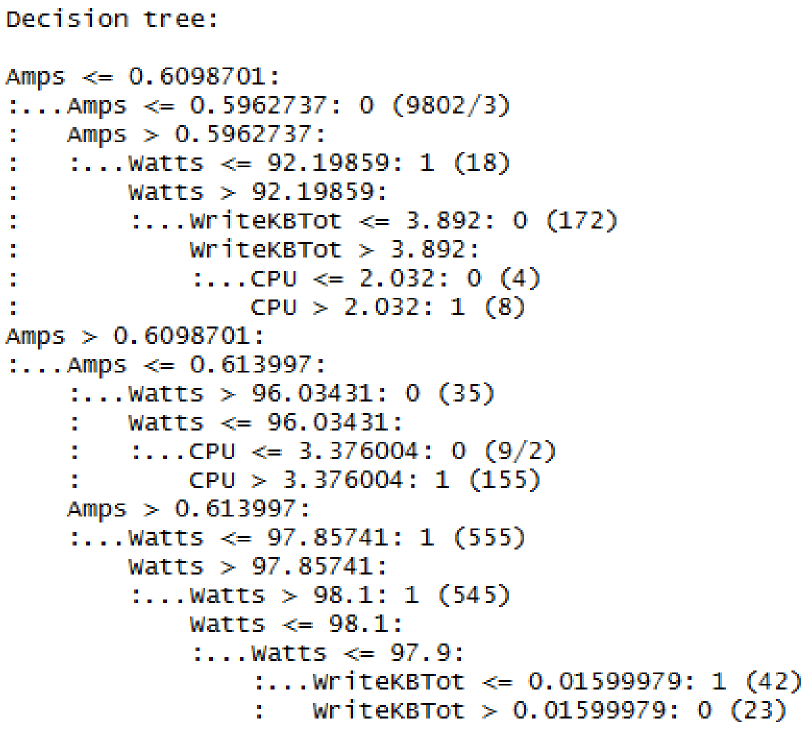


- Prediction study design
  - 80% for training (70% randomly) and testing (30%)
  - 20% for validation

Machine Learning Algorithm



- Algorithm consideration:
  - Performance
  - Data/features: transformation
  - Type: Binary classification



```
Decision tree:

Amps <= 0.6098701:
:...Amps <= 0.5962737: 0 (9802/3)
:   Amps > 0.5962737:
:   :...Watts <= 92.19859: 1 (18)
:       Watts > 92.19859:
:       :...WriteKBTot <= 3.892: 0 (172)
:           WriteKBTot > 3.892:
:           :...CPU <= 2.032: 0 (4)
:               CPU > 2.032: 1 (8)
Amps > 0.6098701:
:...Amps <= 0.613997:
    :...Watts > 96.03431: 0 (35)
    :   Watts <= 96.03431:
    :   :...CPU <= 3.376004: 0 (9/2)
    :       CPU > 3.376004: 1 (155)
    Amps > 0.613997:
    :...Watts <= 97.85741: 1 (555)
        Watts > 97.85741:
        :...Watts > 98.1: 1 (545)
            Watts <= 98.1:
            :...Watts <= 97.9:
                :...WriteKBTot <= 0.01599979: 1 (42)
                :   WriteKBTot > 0.01599979: 0 (23)
```

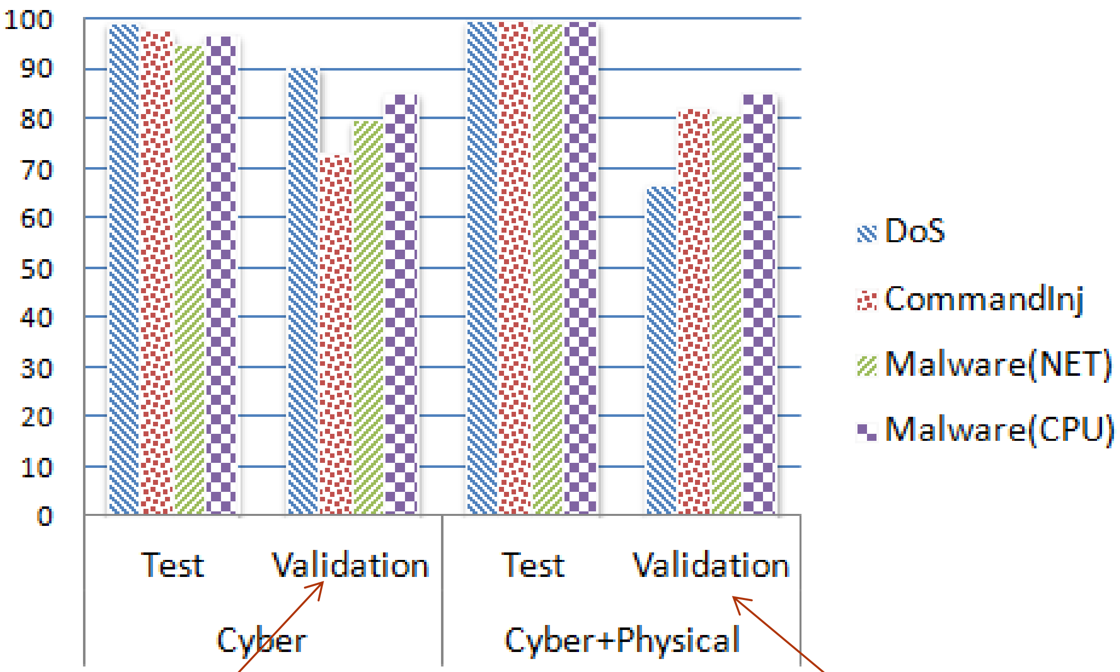
- Decision Tree C5.0 using R programming language (widely used for data analysis)
  - Transformation less important, robust to set of attributes
  - Fast, compact when trained
  - Simple to understand/interpret
  - Problem: over-fitted

Evaluation: Confusion matrix

- Confusion matrix

	Predicted 1	Predicted 0
True 1	TP	FN
True 0	FP	TN

- Result:



DETECTION RESULTS USING ONLY CYBER INPUT FEATURES

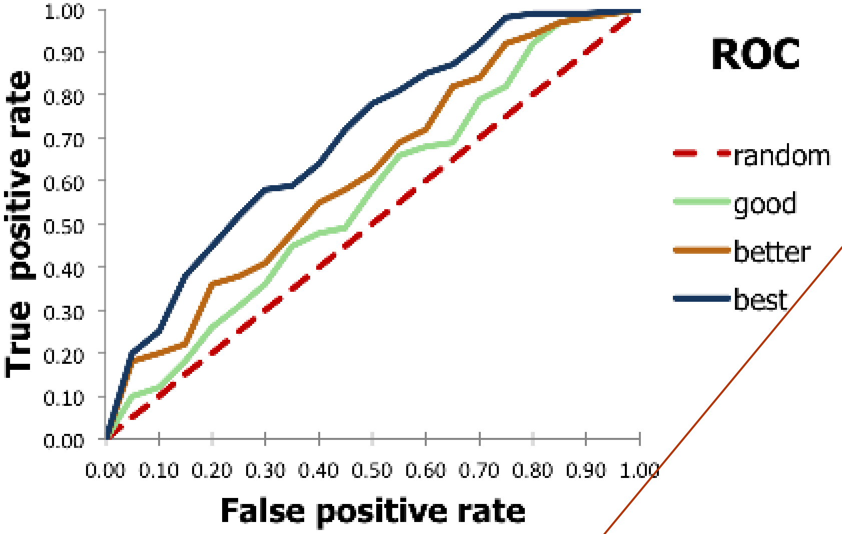
	Test	Validation		
Attack	ACC%	FPR%	FNR%	ACC%
DoS	99.45	15.77	7.26	90.47
Command inj.	97.58	31.79	22.34	72.80
Malware (NET)	94.99	21.42	18.99	79.70
Malware (CPU)	97.03	21.16	6.76	85.31

DETECTION RESULTS USING BOTH CYBER AND PHYSICAL INPUT FEATURES

	Test	Validation		
Attack	ACC%	FPR%	FNR%	ACC%
DoS	99.84	10.76	41.44	66.70
Command inj.	99.53	29.60	5.74	81.99
Malware (NET)	99.20	25.70	11.31	80.92
Malware (CPU)	99.72	5.43	26.18	85.24

Receiver Operating Characteristic (ROC) Curves

- ROC curves

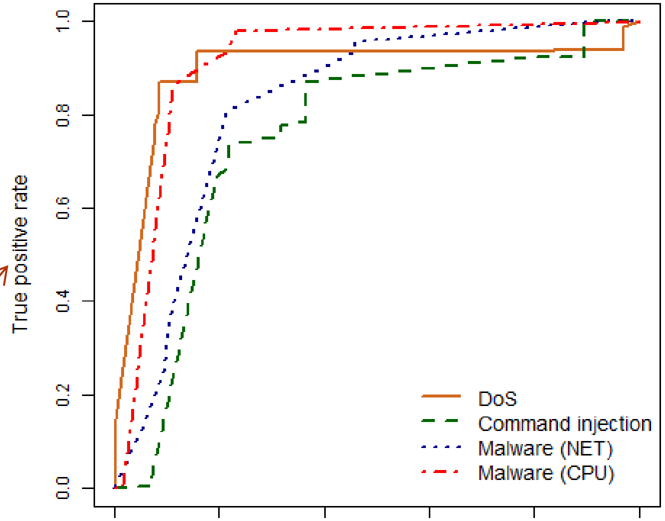


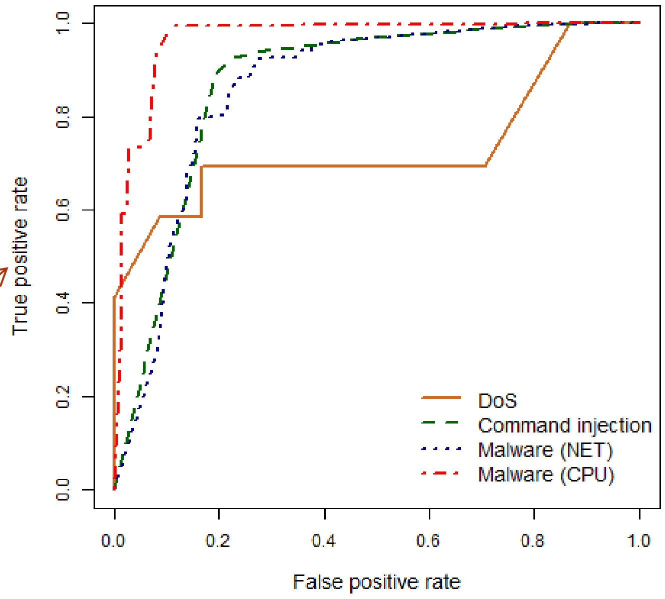
- AUC (Area under the curve)

AUC COMPARISON USING CYBER ONLY AND BOTH CYBER AND PHYSICAL INPUT FEATURES

Attack	AUC	
	Cyber only	Cyber + Physical
DoS	0.89	0.73
Command inj.	0.75	0.87
Malware (NET)	0.82	0.86
Malware (CPU)	0.91	0.97

- Result:

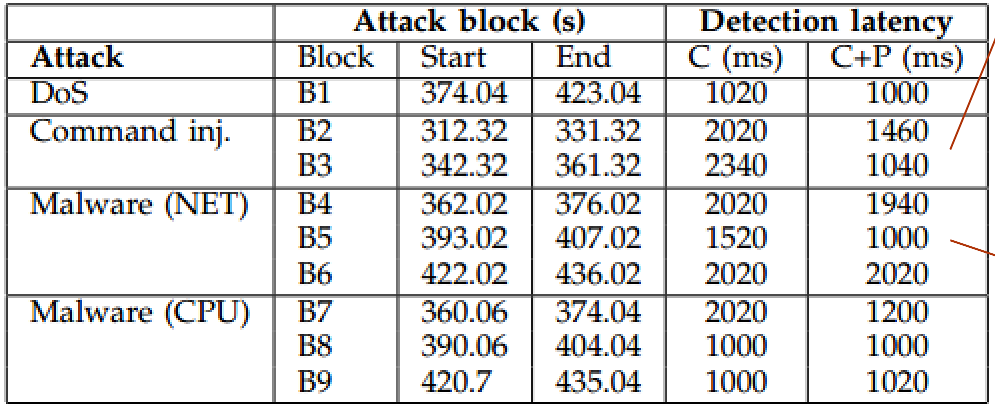




Detection Latency

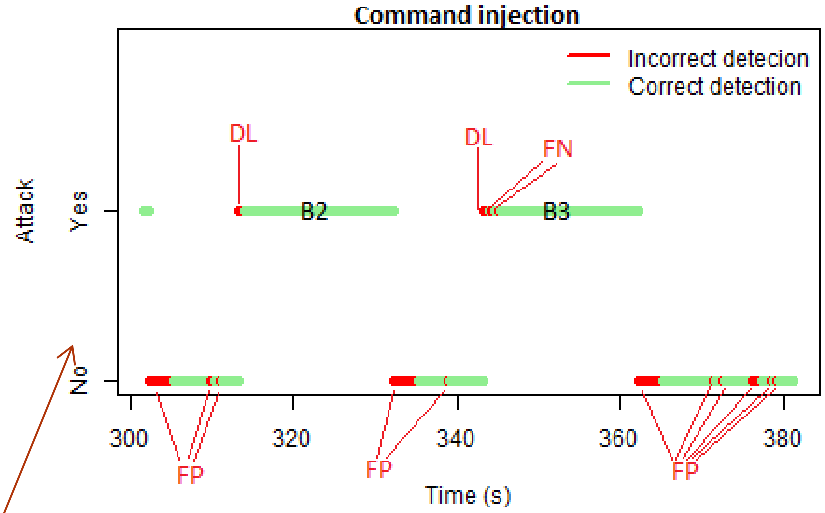
- Real-time for CPS
- Various factors:
  - Data collection time (gathering & measuring): different frequency per feature
  - Preparation time: pre-processing (cleaning scaling, normalizing), interpolation,
  - Detection accuracy: TP (true positive) vs. FN (false negative)

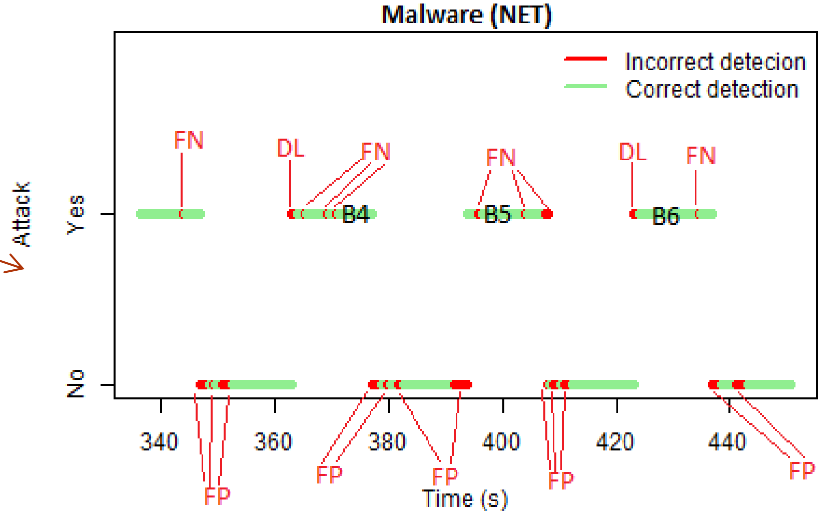
DETECTION LATENCY (MS) FOR DIFFERENT ATTACK TYPES (CYBER ONLY VS. CYBER + PHYSICAL)



	Attack block (s)			Detection latency	
Attack	Block	Start	End	C (ms)	C+P (ms)
DoS	B1	374.04	423.04	1020	1000
Command inj.	B2	312.32	331.32	2020	1460
	B3	342.32	361.32	2340	1040
Malware (NET)	B4	362.02	376.02	2020	1940
	B5	393.02	407.02	1520	1000
	B6	422.02	436.02	2020	2020
Malware (CPU)	B7	360.06	374.04	2020	1200
	B8	390.06	404.04	1000	1000
	B9	420.7	435.04	1000	1020

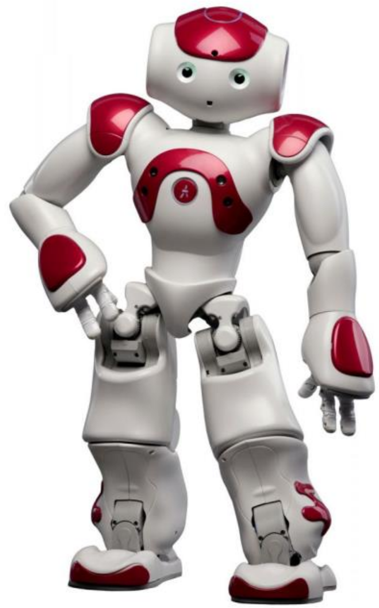
- Detection result:
  - **DL: Detection Latency**
  - **FP : False Positive**
  - **FN: False Negative**





Conclusion and future work

- Conclusion:
  - Light-weight on-board intrusion detection for robotic vehicle
  - Four attacks and detection performance with and without physical features
  - Performance metrics: Confusion matrix, ROC Curve, and Detection latency
- Future work:
  - Improve current technique (over-fitted, time-series)
  - More attack types (communication jamming, relay attacks..)
  - Unknown attack, other detection methods
  - Additional test beds



Q&A

Thank you!