

# Building Dependable Distributed Medical Device Plug-and-Play Environments

Qixin Wang  
Dept. of Computing  
The Hong Kong Polytechnic University  
July 18, 2012



# Contents



Demand



Modeling and Verification



Dependable Medical Wireless Networking



Vision

# Contents



Demand



Modeling and Verification



Dependable Medical Wireless Networking



Vision



Hundreds of thousands of medical devices exist in nowadays hospitals, but are mostly designed for isolated use (proprietary)

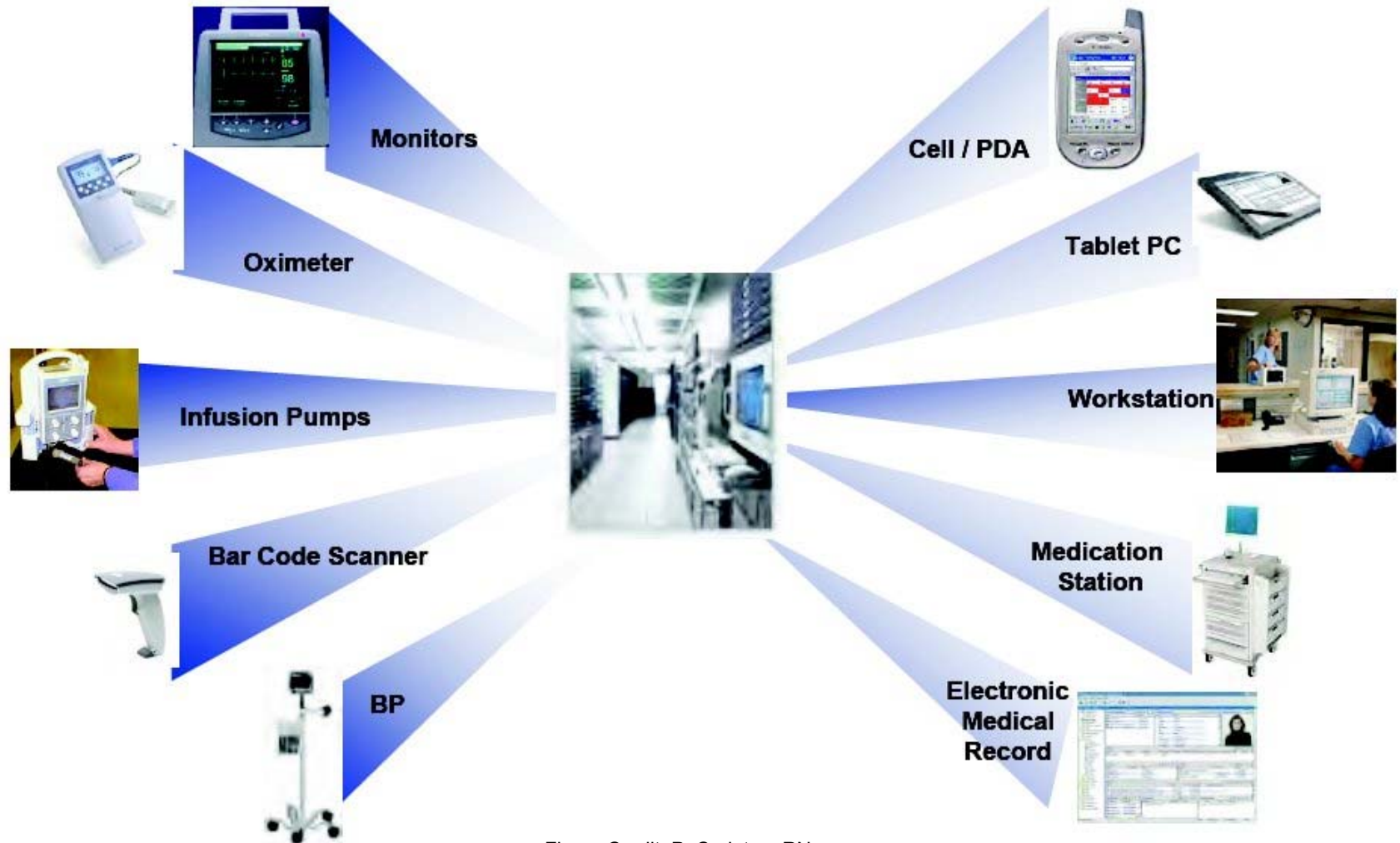


Figure Credit: P. Carleton, RN



# Why do we want Medical Device Plug-and-Play (MDPnP)? (and why wireless MDPnP?)

Safety

Flexibility and expanded medication capability

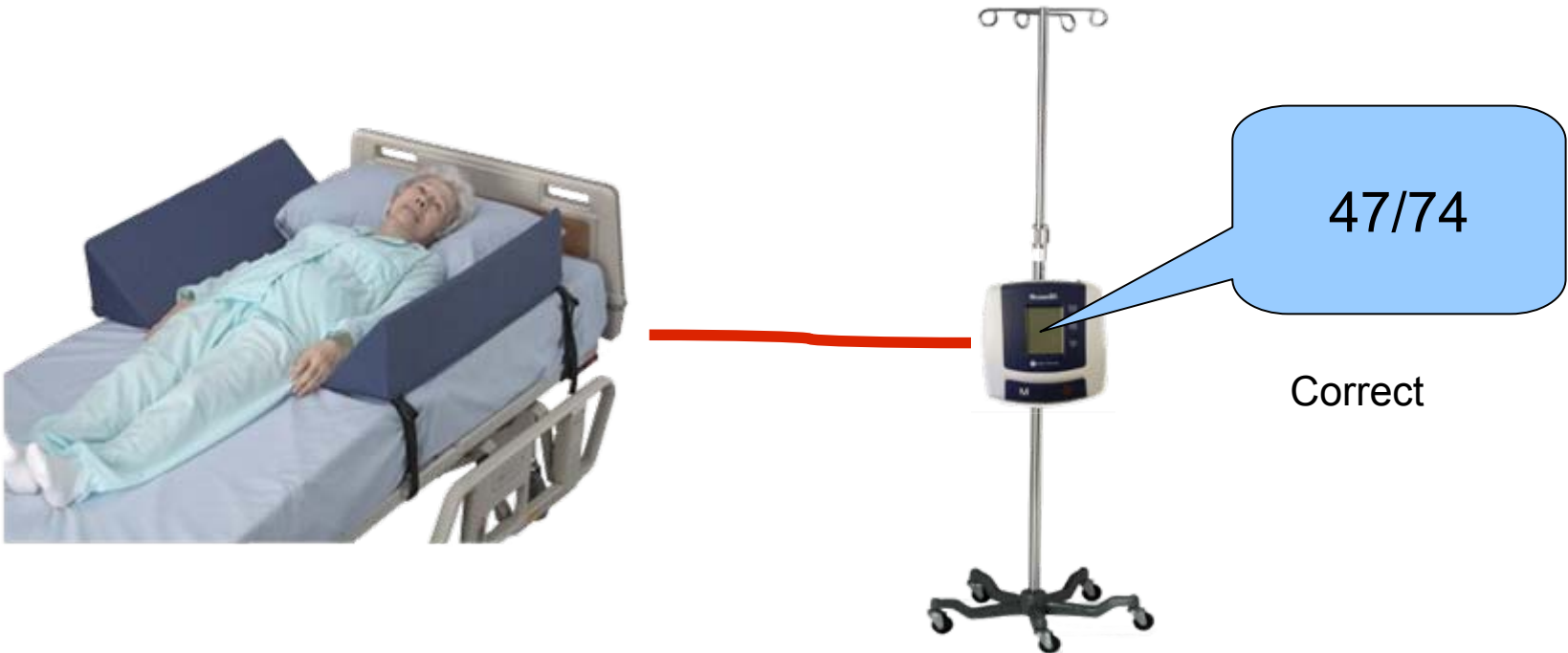
Convenience and Efficiency

Independence from device vendors



We need interconnected/interlocked medical devices to provide **safety**

Blood Pressure Measuring





We need interconnected/interlocked medical devices to provide **safety**

Blood Pressure Measuring





We need interconnected/interlocked medical devices to provide **safety**

Blood Pressure Measuring

Proposal:  
MDPnP interlocked Bed and BP meter



~~49/59~~  
47/74

Offset Corrected





We need interconnected/interlocked medical devices to provide **safety**

Cardiopulmonary Bypass v.s. Ventilator Accident

Heart Lung Machine



Correct Procedure:



Ventilator





We need interconnected/interlocked medical devices to provide **safety**

Cardiopulmonary Bypass v.s. Ventilator Accident

Heart Lung Machine



Correct Procedure:



Ventilator





# We need interconnected/interlocked medical devices to provide **safety**

Cardiopulmonary Bypass v.s. Ventilator Accident

Heart Lung Machine



Correct Procedure:



Ventilator





# We need interconnected/interlocked medical devices to provide **safety**

Cardiopulmonary Bypass v.s. Ventilator Accident

Heart Lung Machine



Absent Minded Procedure:



Ventilator





# We need interconnected/interlocked medical devices to provide **safety**

Cardiopulmonary Bypass v.s. Ventilator Accident

Heart Lung Machine



Absent Minded Procedure:



Ventilator





We need interconnected/interlocked medical devices to provide **safety**

Cardiopulmonary Bypass v.s. Ventilator Accident

Heart Lung Machine



Absent Minded Procedure:



Ventilator







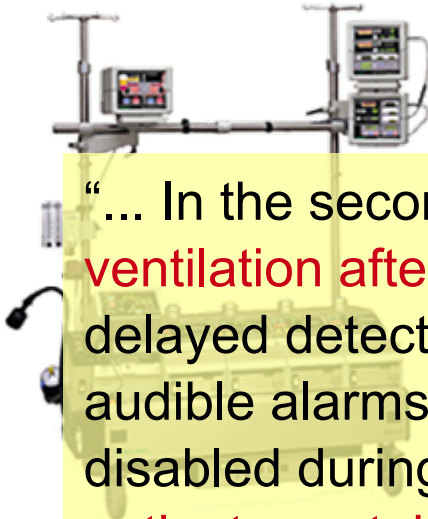
# We need interconnected/interlocked medical devices to provide **safety**

Cardiopulmonary Bypass v.s. Ventilator Accident

Ventilator

Heart Lung Machine

Absent Minded Procedure:



“... In the second case, **the anesthesiologist forgot to resume ventilation after separation from cardiopulmonary bypass.** The delayed detection of apnea was attributed to the fact that the audible alarms for the pulse oximeter and capnograph had been disabled during bypass and had not been reactivated. **Both patients sustained permanent brain damage.**”

Anesthesiology. 87(4):741-748, October **1997**



# We need interconnected/interlocked medical devices to provide **safety**

Cardiopulmonary Bypass v.s. Ventilator Accident

Heart Lung Machine



Capnograph

Proposal:  
MDPnP Interlocked Architecture



MDPnP Control Computer

Ventilator



Oximeter





We need interconnected/interlocked medical devices to provide **safety**

## X-Ray v.s. Ventilator Accident



Picture provided by Mu Sun



We need interconnected/interlocked medical devices to provide **safety**

## X-Ray v.s. Ventilator Accident



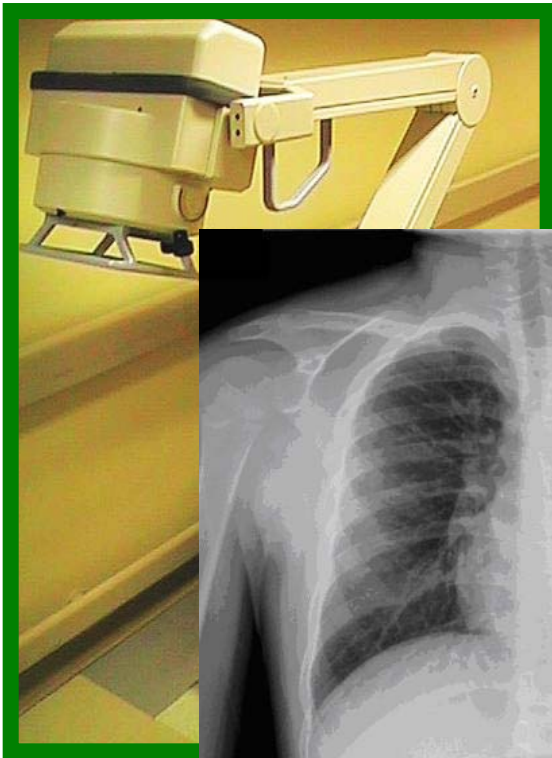
**Blurry Image**





We need interconnected/interlocked medical devices to provide **safety**

## X-Ray v.s. Ventilator Accident

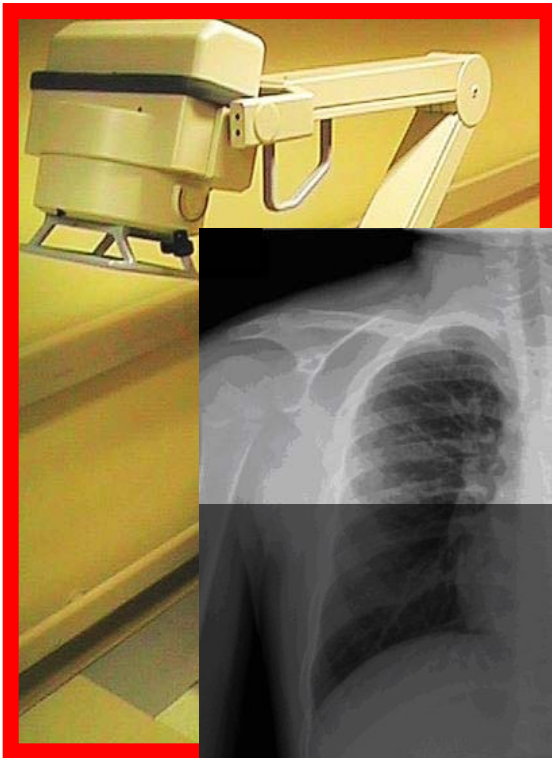


Picture provided by Mu Sun



We need interconnected/interlocked medical devices to provide **safety**

## X-Ray v.s. Ventilator Accident



Picture provided by Mu Sun





We need interconnected/interlocked medical devices to provide **safety**

## X-Ray v.s. Ventilator Accident

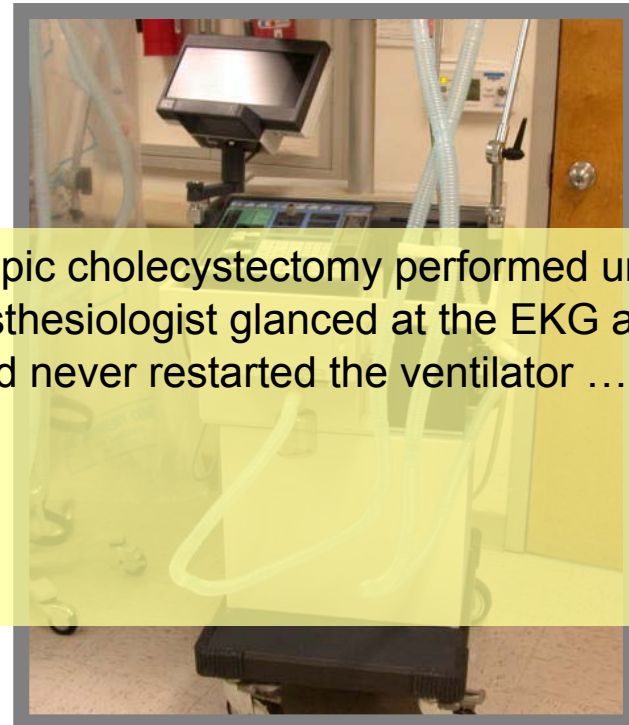


Picture provided by Mu Sun



# We need interconnected/interlocked medical devices to provide **safety**

## X-Ray v.s. Ventilator Accident



“A 32-year-old woman was having a laparoscopic cholecystectomy performed under general anesthesia. ... At some point, the anesthesiologist glanced at the EKG and noticed severe bradycardia. He realized he had never restarted the ventilator ...

**The patient ultimately died.”**

APSF Newsletter, Winter, 2005.



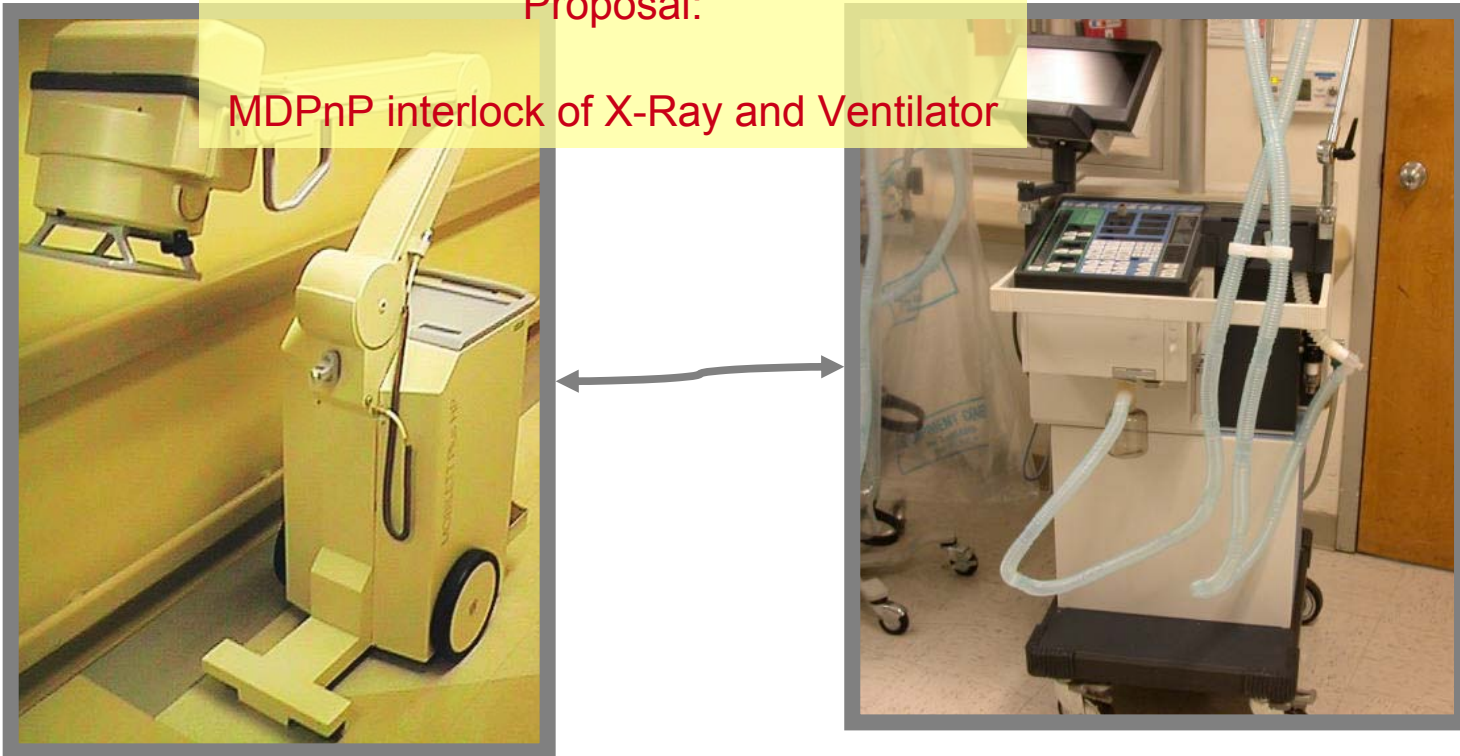


We need interconnected/interlocked medical devices to provide **safety**

## X-Ray v.s. Ventilator Accident

Proposal:

MDPnP interlock of X-Ray and Ventilator





We need interconnected/interlocked medical devices to provide **safety**

Laser v.s. Oxygen Concentration Accident

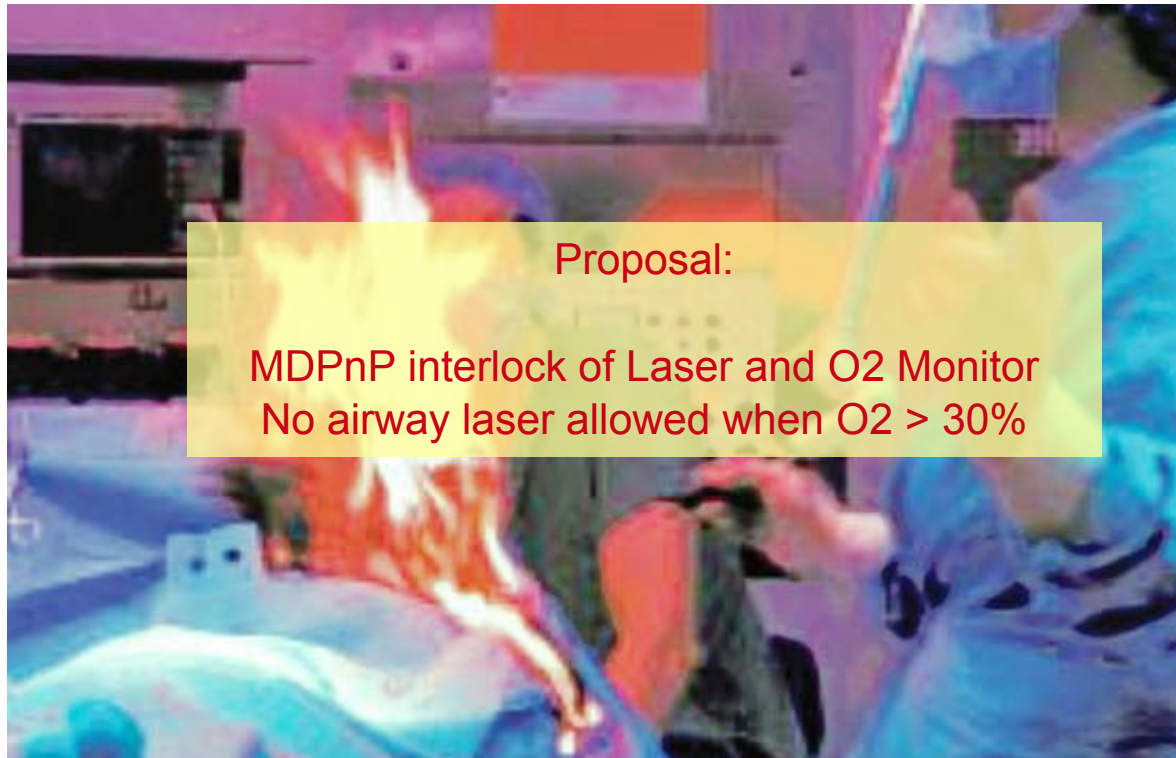






We need interconnected/interlocked medical devices to provide **safety**

## Laser v.s. Oxygen Concentration Accident





We need interconnected/interlocked medical devices to provide **safety**

Contangoous patient calls nurse for help





# We need interconnected/interlocked medical devices to provide **safety**

Contagious patient calls nurse for help



Contagious,  
must wear mask!





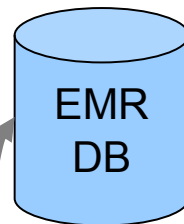
# We need interconnected/interlocked medical devices to provide **safety**

Contagious patient calls nurse for help

Contagious,  
must wear mask!



Nurse Station



Proposal:

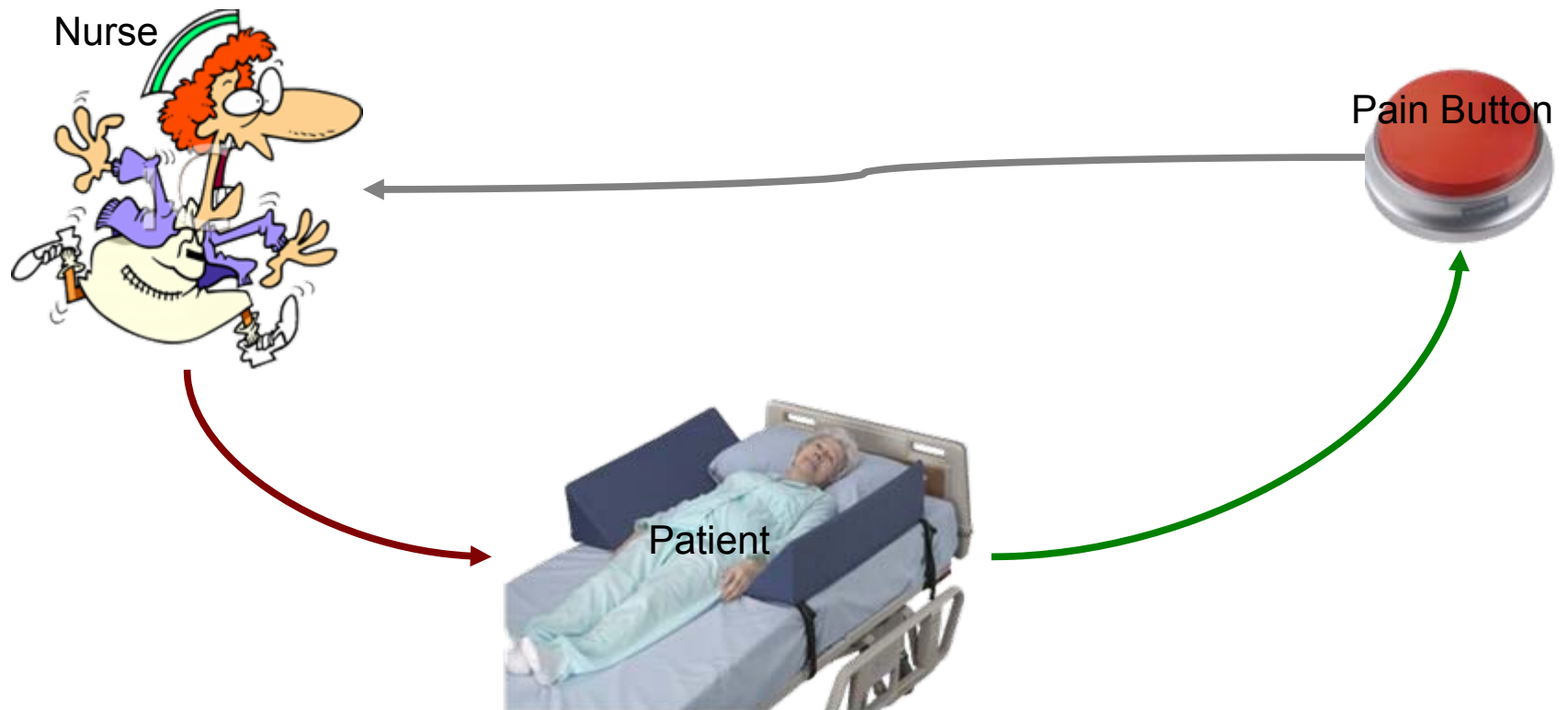
MDPnP connection of EMR DB,  
Nurse Station, and Vital Sign  
Monitors





# Flexible composition of medical devices expands medication capability by enabling new methods/apps

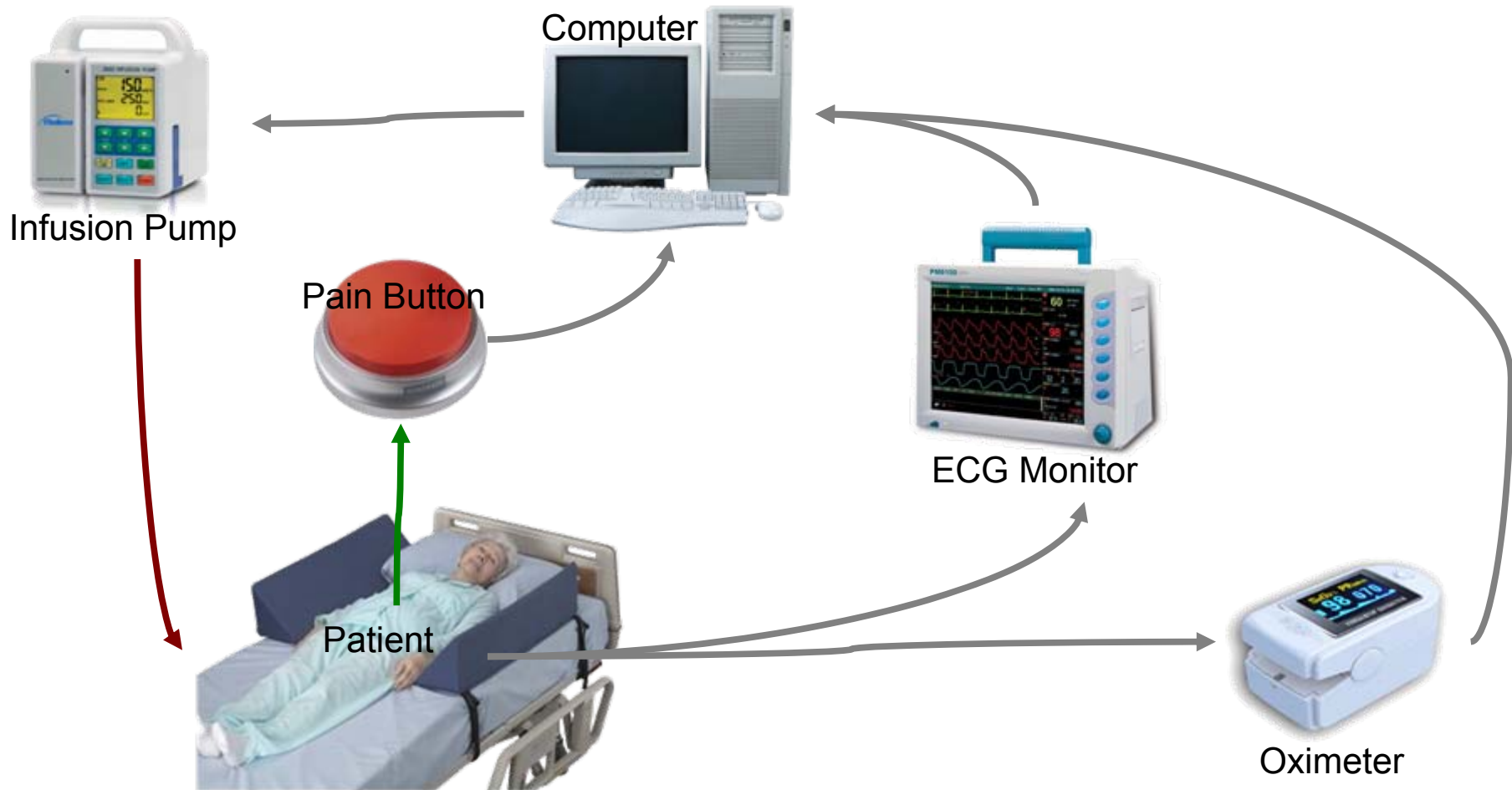
## Patient Controlled Anesthesia (PCA)





# Flexible composition of medical devices expands medication capability by enabling new methods/apps

## Patient Controlled Anesthesia (PCA)







# MDPnP, particularly wireless MDPnP, improves convenience and efficiency

Messed Up Operation Room

High-acuity care today:  
How do we prevent errors?  
How do we keep track of all this?





# MDPnP, particularly wireless MDPnP, improves convenience and efficiency

Messed Up OR v.s. Vital Sign Bulletin Board



Picture quoted from [www.mdnpn.org](http://www.mdnpn.org)

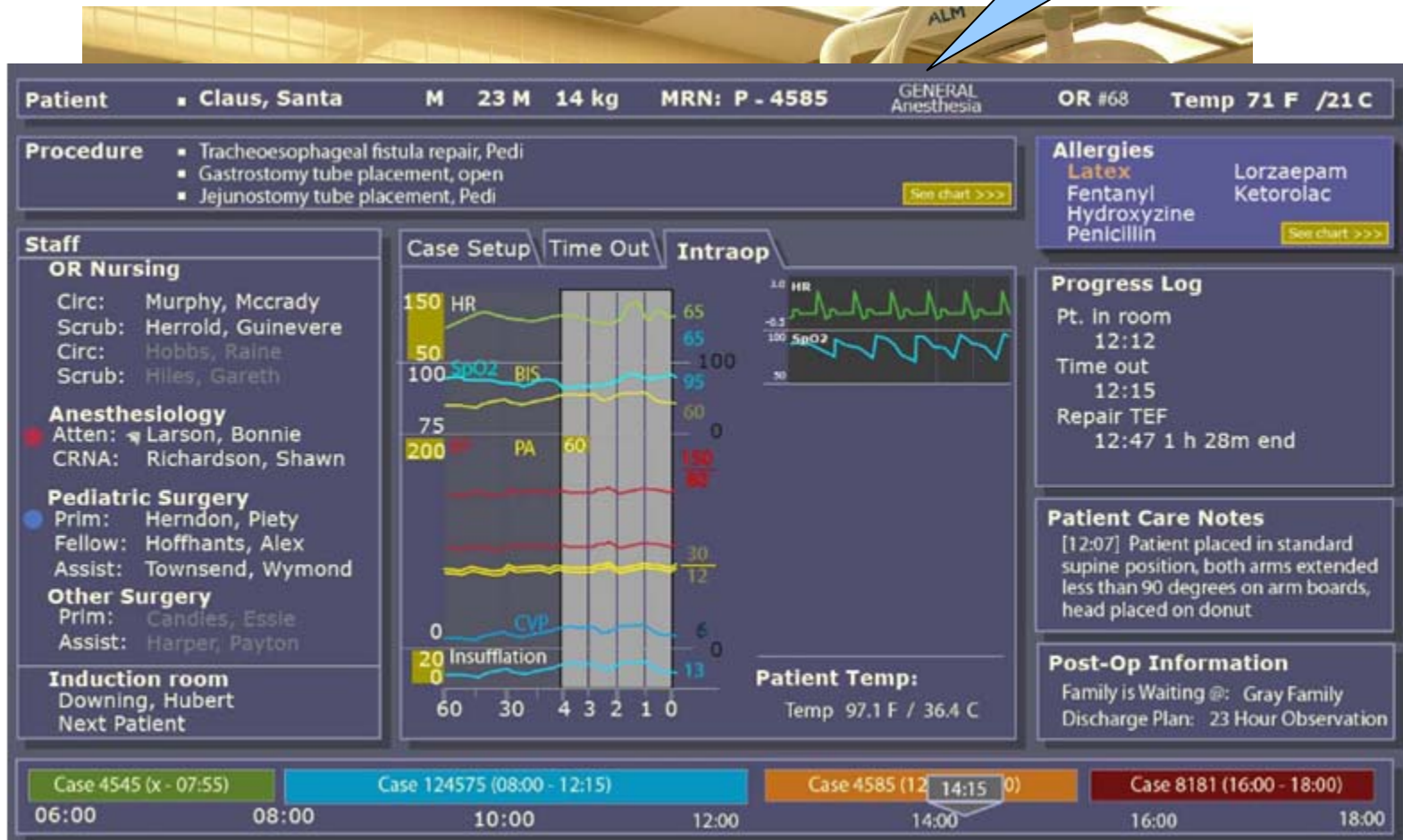




# MDPnP, particularly wireless MDPnP, improves convenience and efficiency

LiveData OR Dashboard

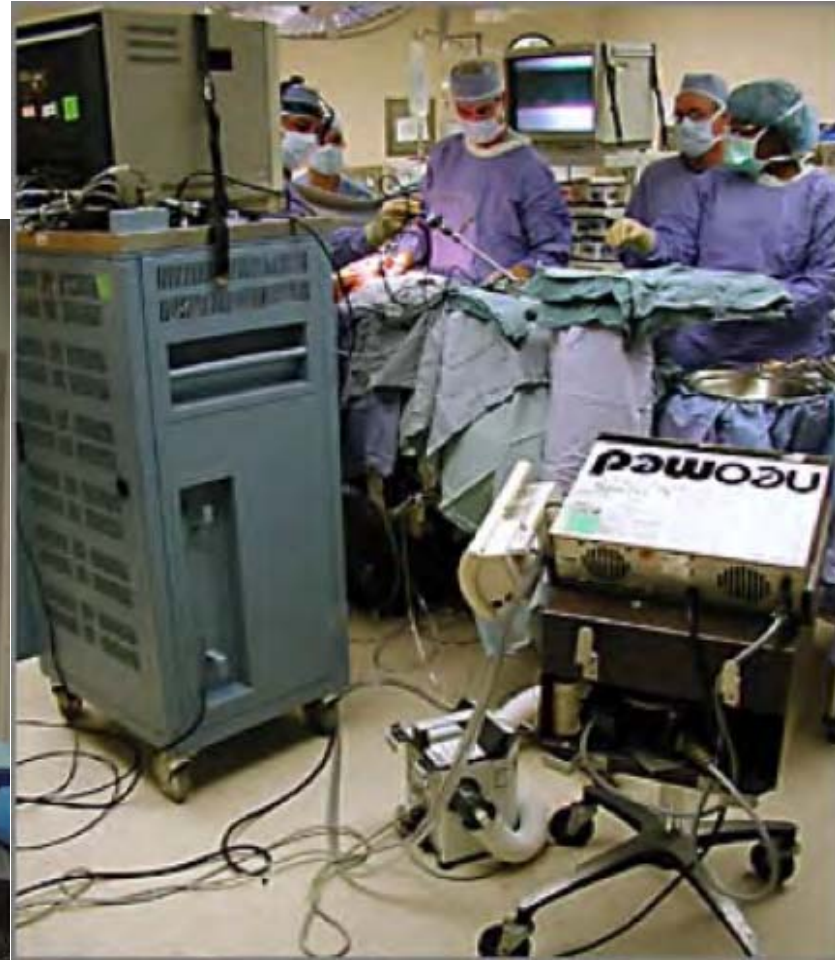
Messed Up OR v.s. Vital Sign Bulletin Board





# MDPnP, particularly wireless MDPnP, improves convenience and efficiency

## The Operation Room Spider Web

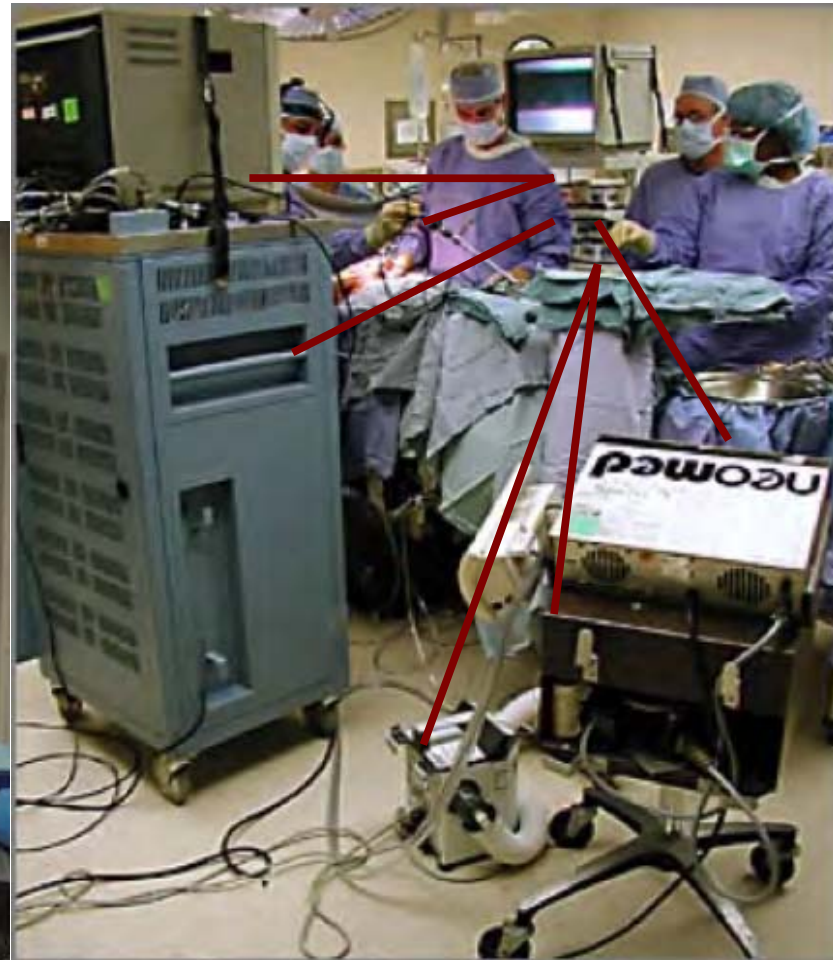
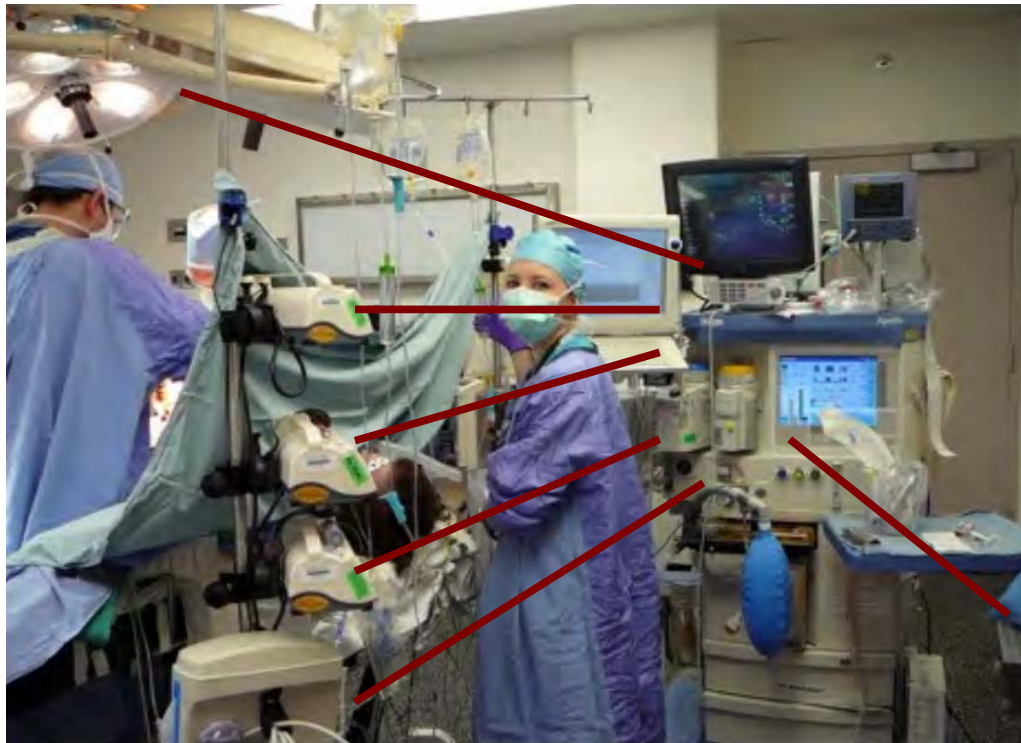






# MDPnP, particularly wireless MDPnP, improves convenience and efficiency

The Operation Room Spider Web,  
after MDPnP safety interlocks





MDPnP, particularly wireless MDPnP, improves  
**convenience and efficiency**

Spider Web OR v.s. Wireless OR



Picture quoted from [www.mdpnp.org](http://www.mdpnp.org)



**Independence:** hospitals need hundreds of thousands of types of medical devices; don't want to be controlled by one vendor.

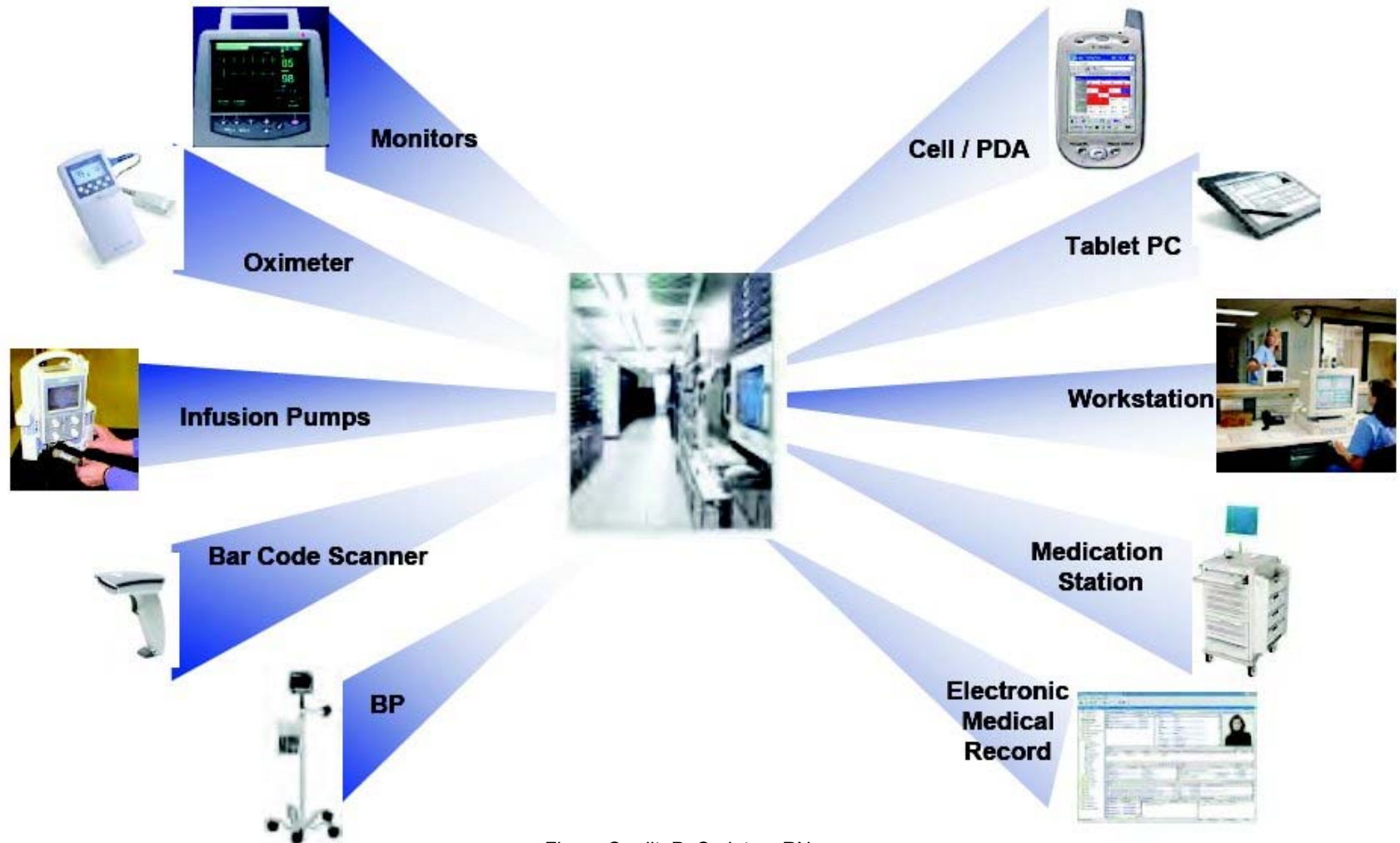


Figure Credit: P. Carleton, RN



## MDPnP benefits whom?

Hospitals:	independence, medication capability, safety
Doctors:	medication capability, safety, convenience
Patient:	medication capability, safety, cost
Government:	tracktability, cost
Vendors:	larger market
Academia:	typical case of cyber-physical systems

# Contents



Demand



Modeling and Verification



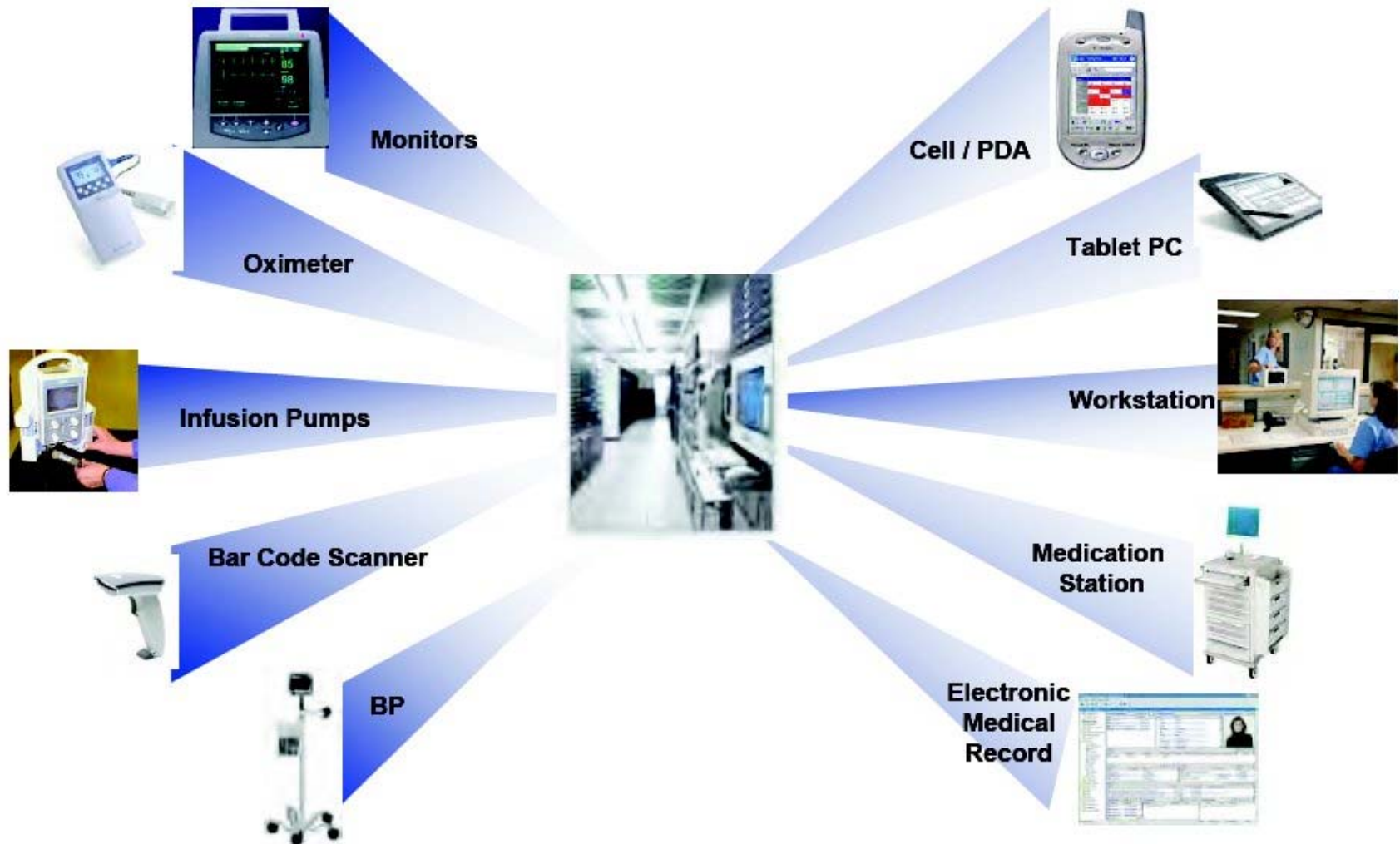
Dependable Medical Wireless Networking



Vision



✓✗ MDPnP leads to better safety, capability, and convenience of medical settings.

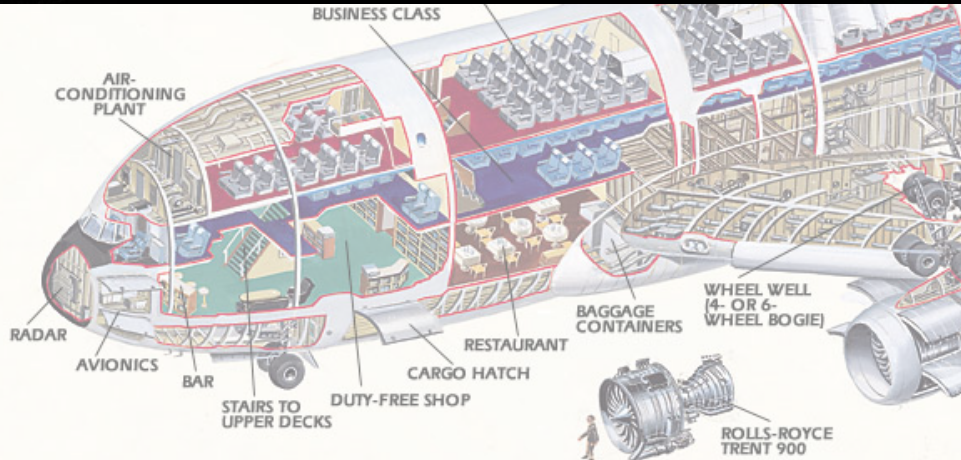
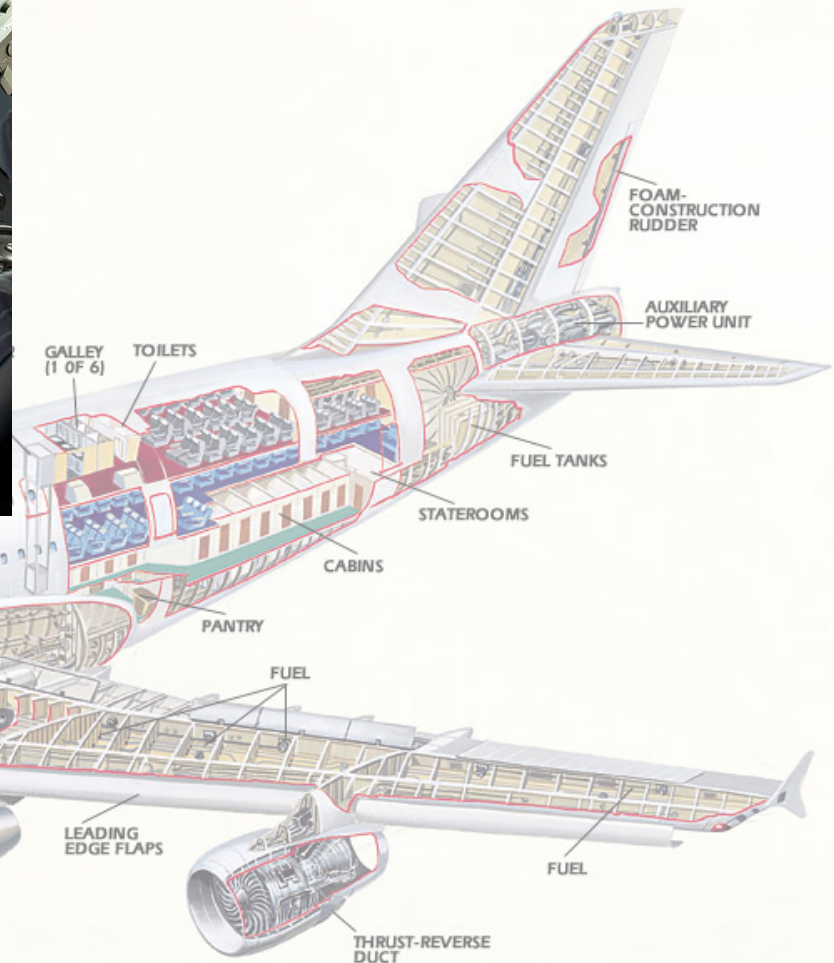




✔✘ MDPnP can help prevent many serious/lethal accidents in medical settings.

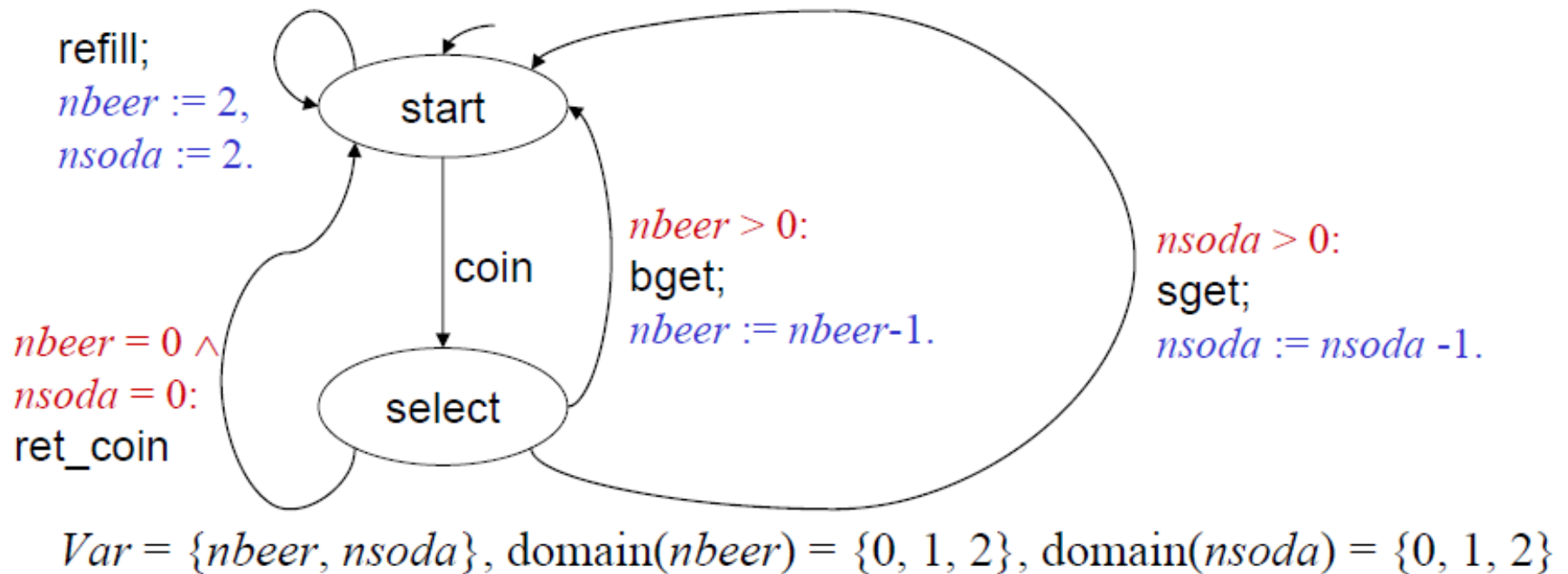


✓✗ Following the success of requiring avionics to be **verifiably** safe → MDPnP to be verifiably safe.

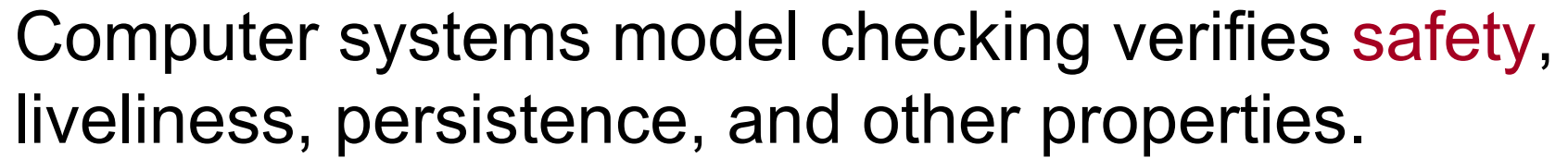




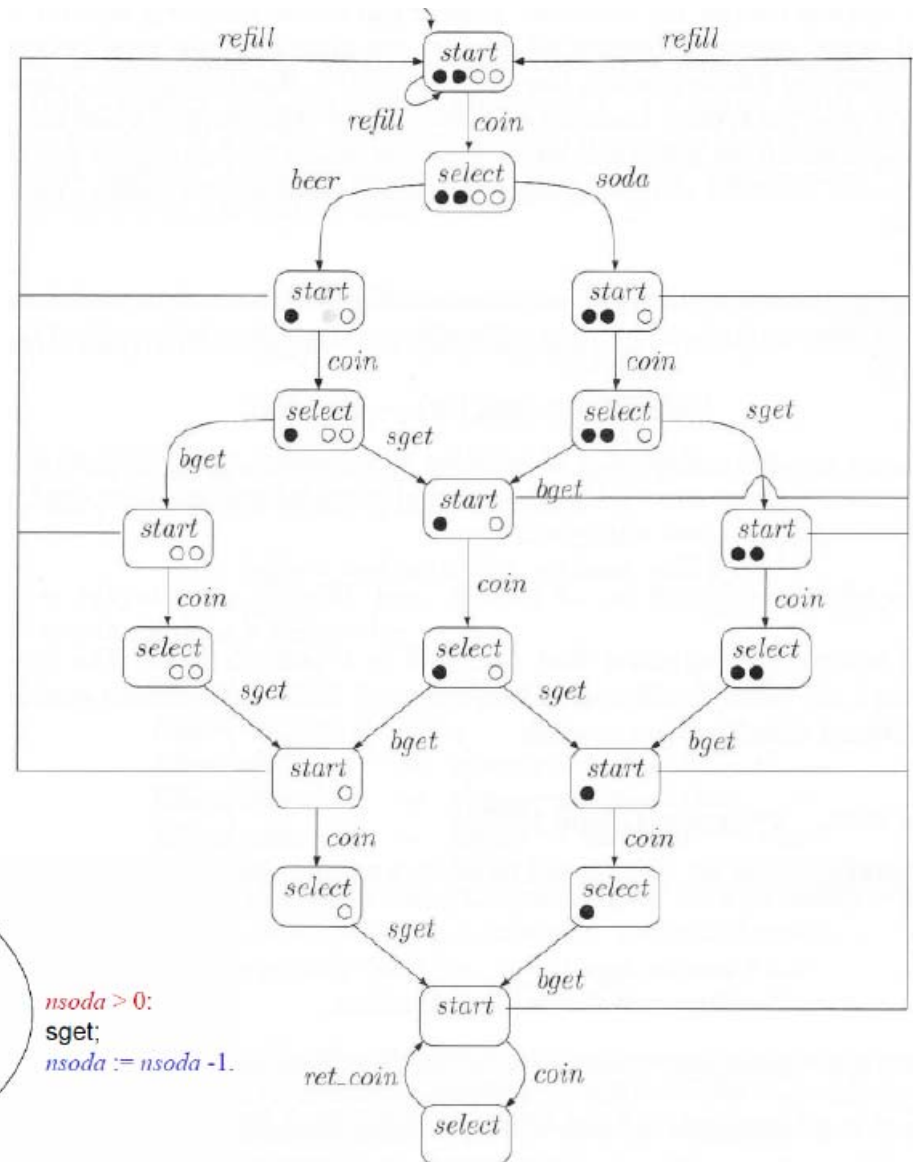
A key tool for traditional computer systems verification is model checking.



$$PG = (Loc, Act, Effect, \rightarrow, Loc_0, g_0)$$



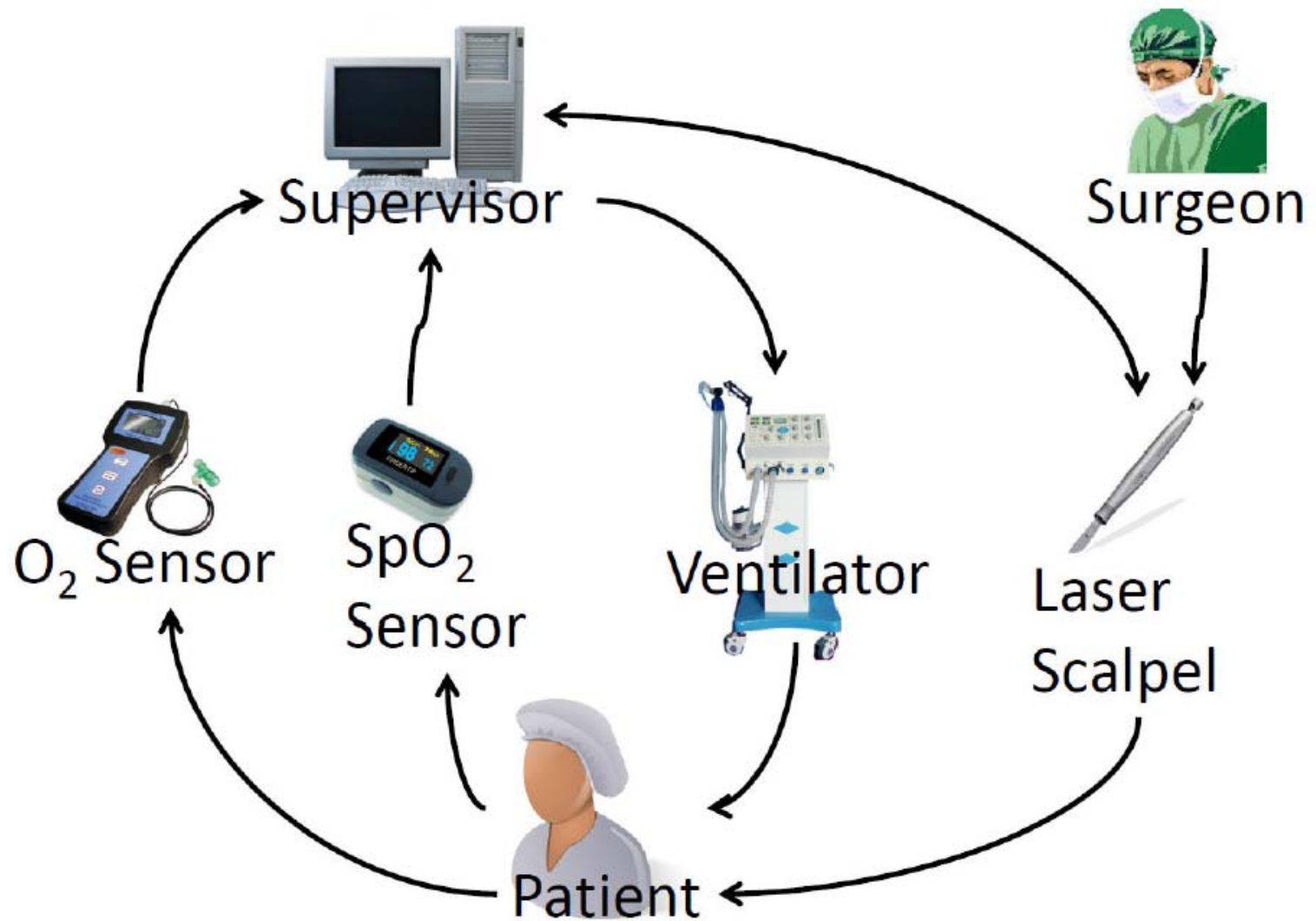
Note the combinatorial explosion of size.







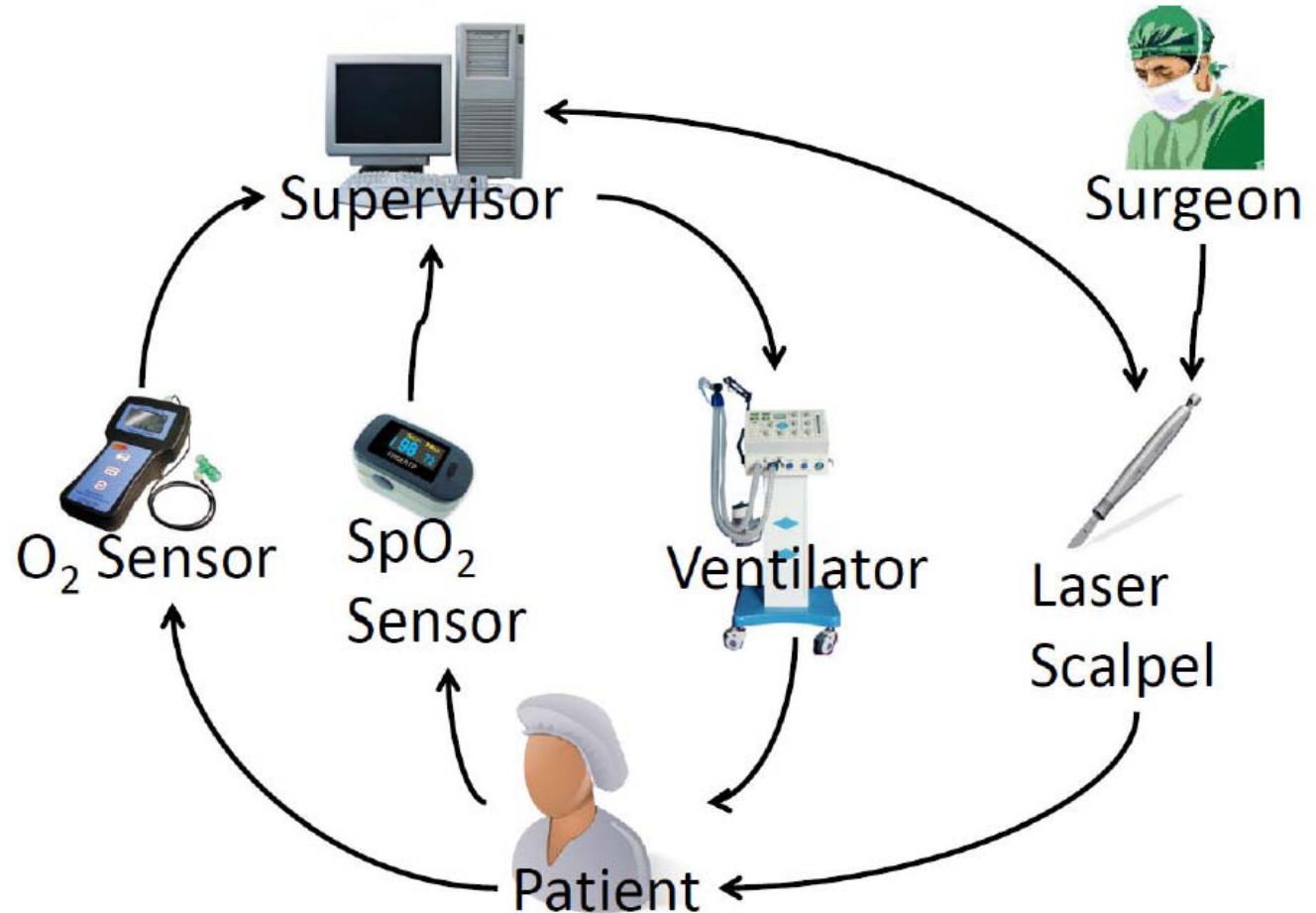
MDPnP is not just a computer system, it is a hybrid of computer & other systems, i.e., CPS.



Laser Tracheotomy MDPnP

✓✗ MDPnP is not just a computer system, it is a hybrid of computer & other systems, i.e., CPS.

Computer



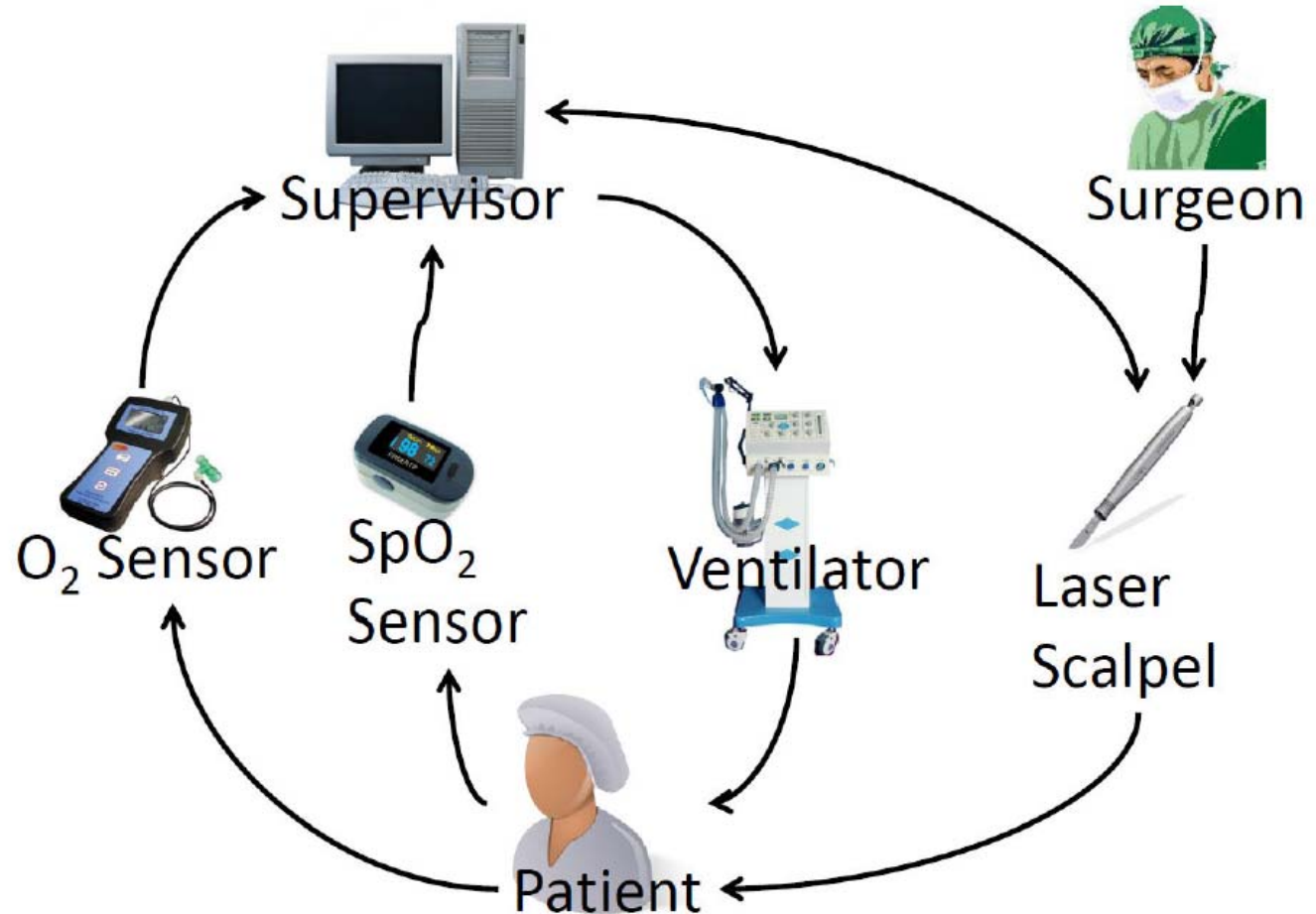
Laser Tracheotomy MDPnP



✓✗ MDPnP is not just a computer system, it is a hybrid of computer & other systems, i.e., CPS.

Computer

Biochemical



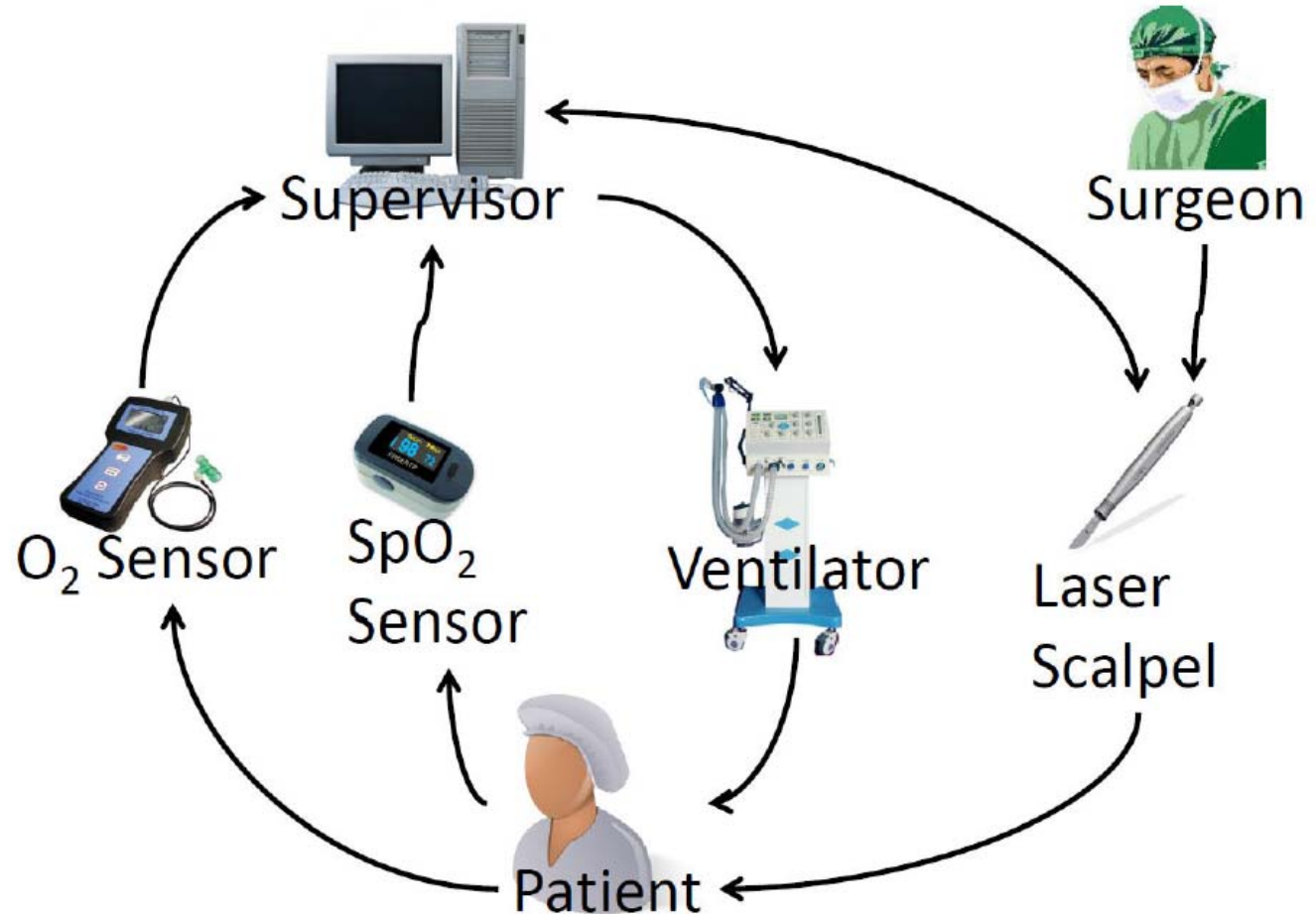
Laser Tracheotomy MDPnP

✔✘ MDPnP is not just a computer system, it is a hybrid of computer & other systems, i.e., CPS.

Computer

Biochemical

Mechanical



Laser Tracheotomy MDPnP

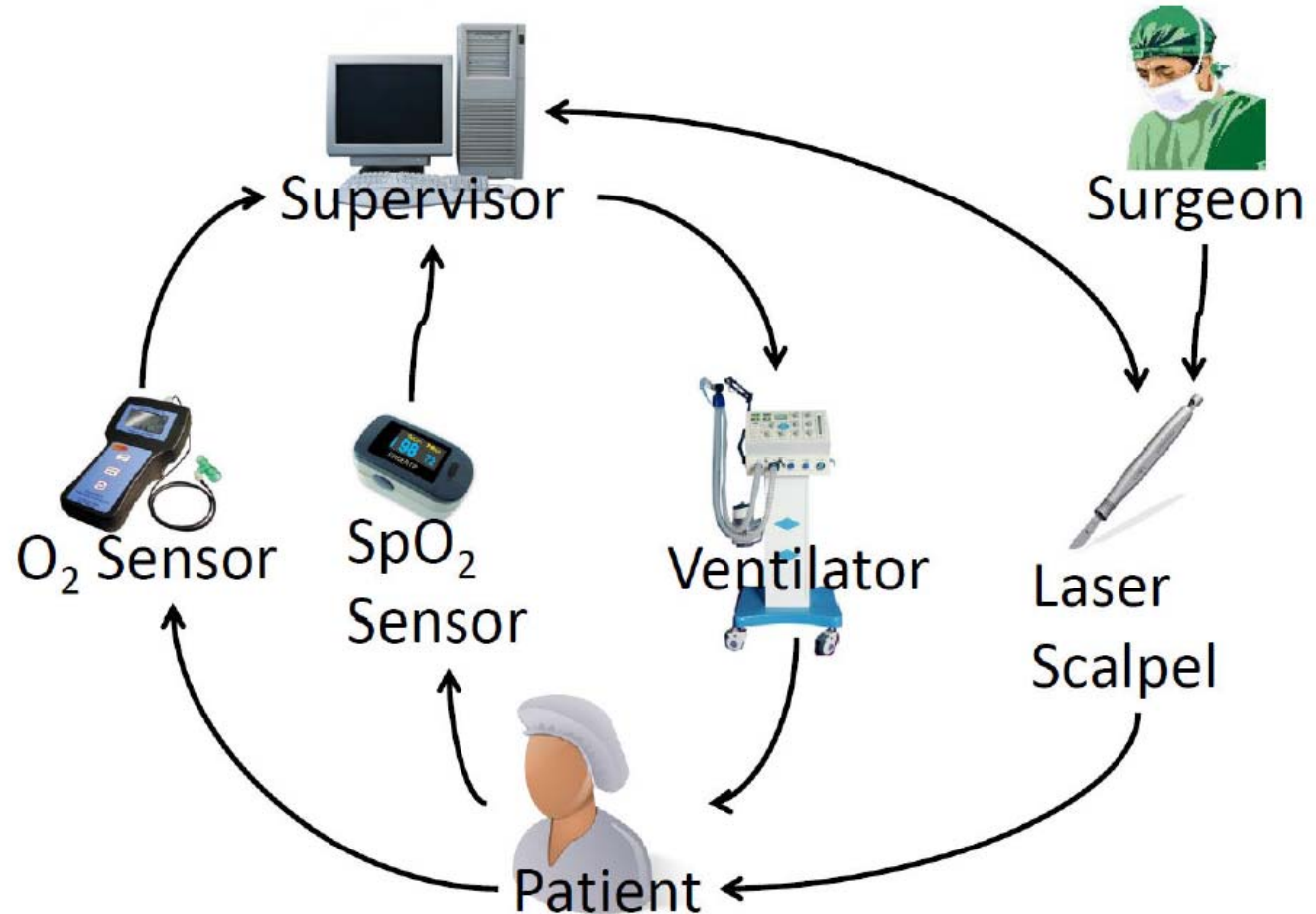
✔✘ MDPnP is not just a computer system, it is a hybrid of computer & other systems, i.e., CPS.

Computer

Biochemical

Mechanical

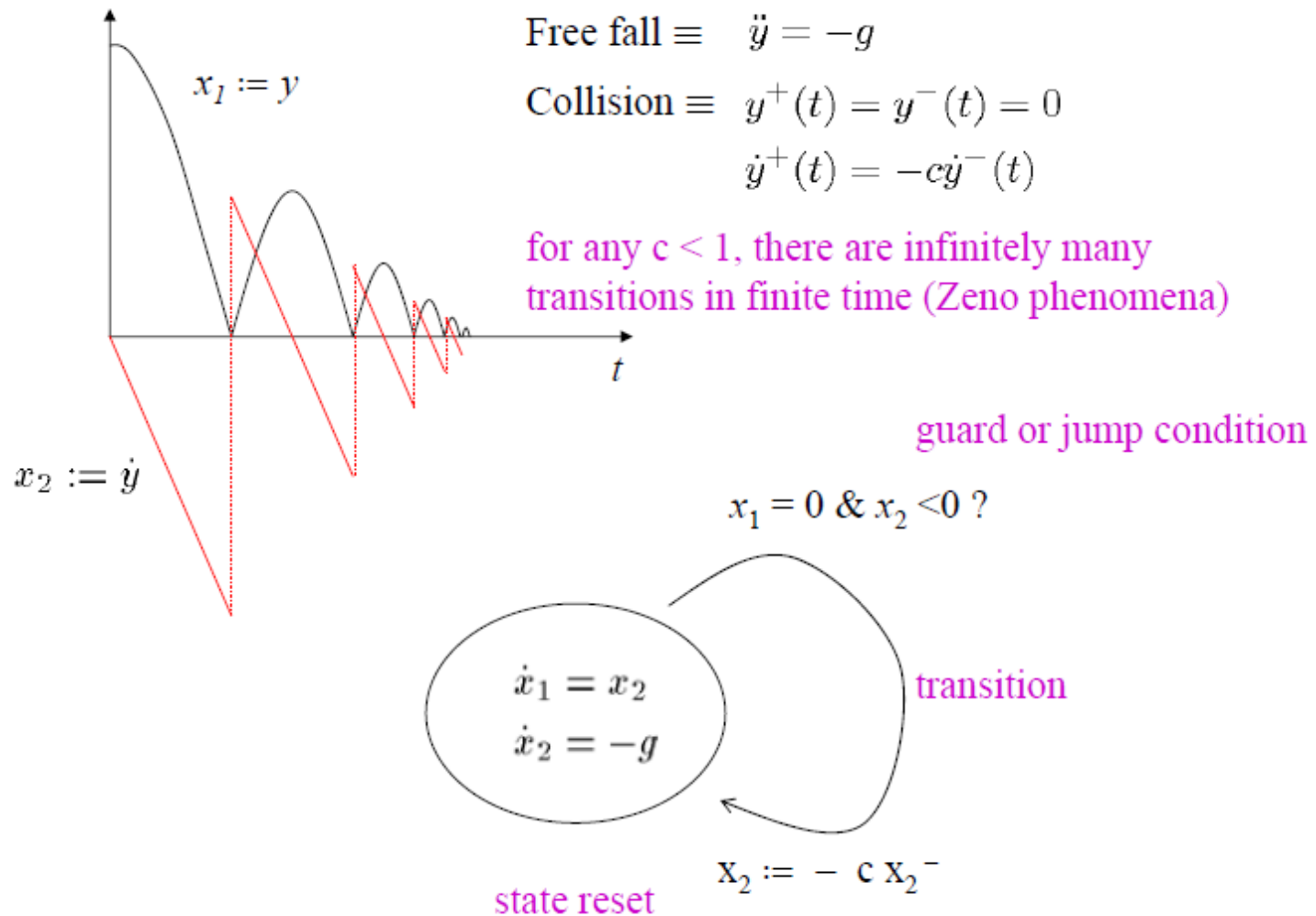
Communication



Laser Tracheotomy MDPnP

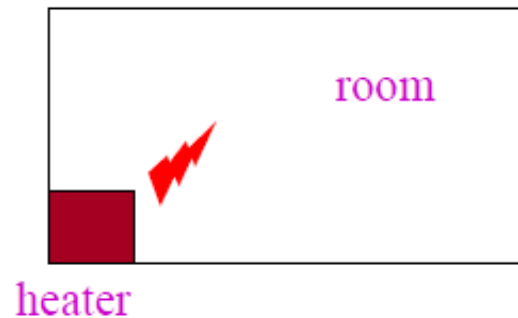
✓✗ A state-of-the-art CPS model checking is Hybrid  
Systems Model Checking: Comp + Fdbk Ctrl.

## Bouncing Ball Example



# ✓✗ The state-of-the-art CPS model checking is Hybrid Systems Model Checking: Comp + Fdbk Ctrl.

## Thermostat Example



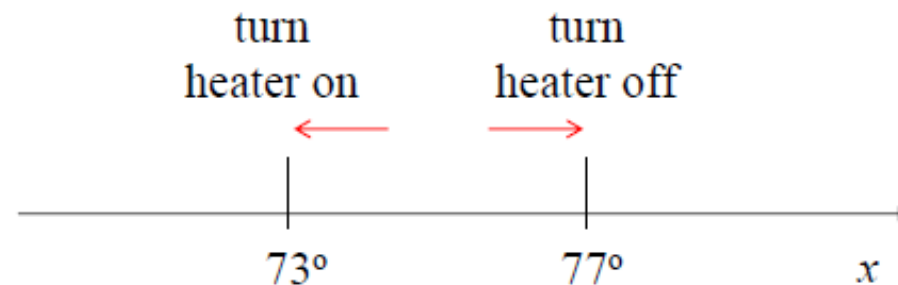
goal  $\equiv$  regulate temperature around  $75^\circ$

$x \equiv$  mean temperature

when heater is off:  $\dot{x} \approx -x + 50$  ( $x \rightarrow 50^\circ$ )

when heater is on:  $\dot{x} \approx -x + 100$  ( $x \rightarrow 100^\circ$ )

event-based control

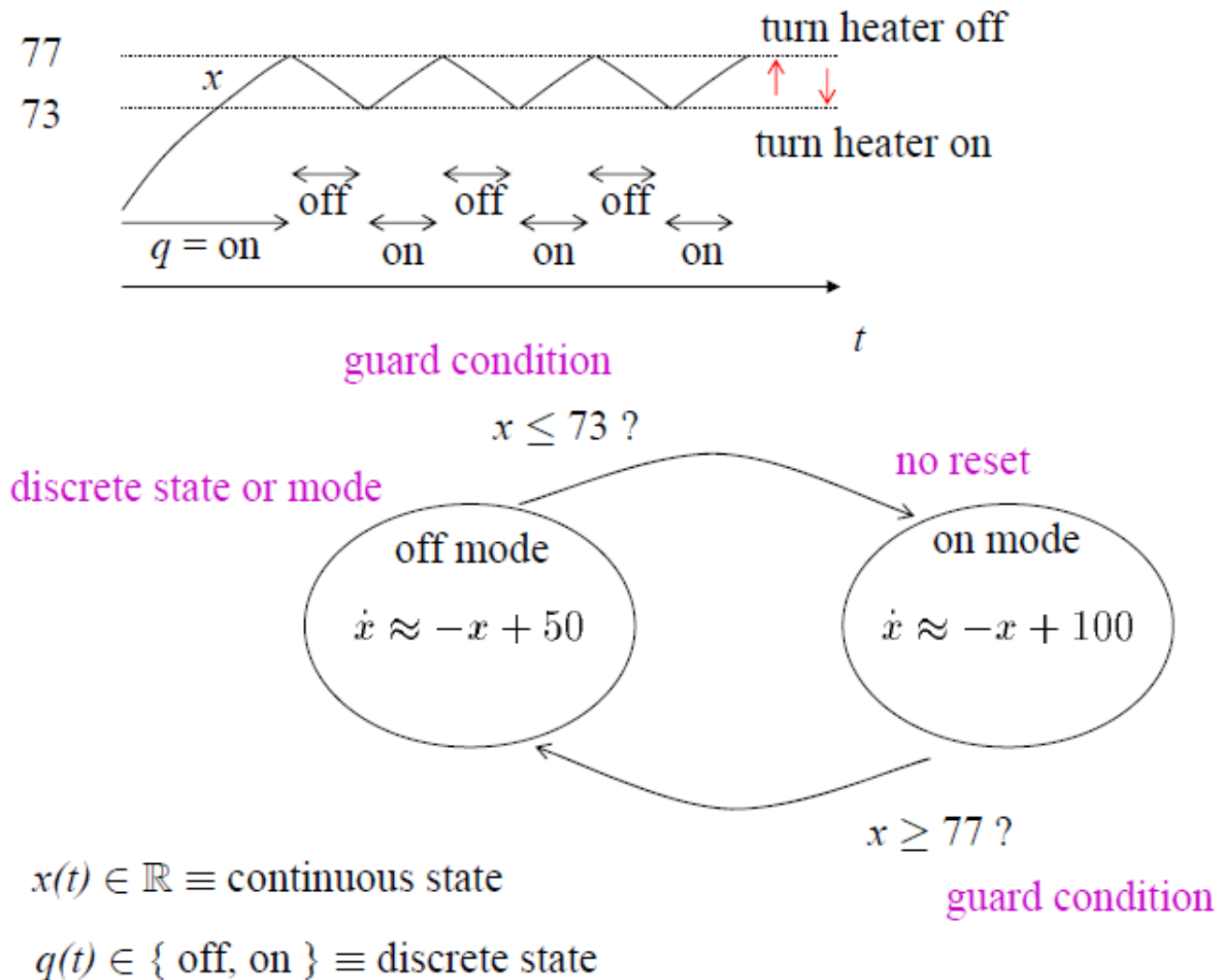






# The state-of-the-art CPS model checking is Hybrid Systems Model Checking: Comp + Fdbk Ctrl.

## Thermostat Example





However, existing hybrid systems model checking (computer + fdbk ctrl) doesn't very well fit MDPnP.

✓✗ However, existing hybrid systems model checking (computer + fdbk ctrl) doesn't very well fit MDPnP.

Existing model checking:

Offline (partly due to lack of time cost bound),

Time-Unbounded Behavior (Long-Run Future)



✓✗ However, existing hybrid systems model checking (computer + fdbk ctrl) doesn't very well fit MDPnP.

Existing model checking:

Offline (partly due to lack of time cost bound),

Time-Unbounded Behavior (Long-Run Future)

Challenge 1: No good offline models for complex biomedical systems of human body.

  However, existing hybrid systems model checking (computer + fdbk ctrl) doesn't very well fit MDPnP.

Existing model checking:

Offline (partly due to lack of time cost bound),

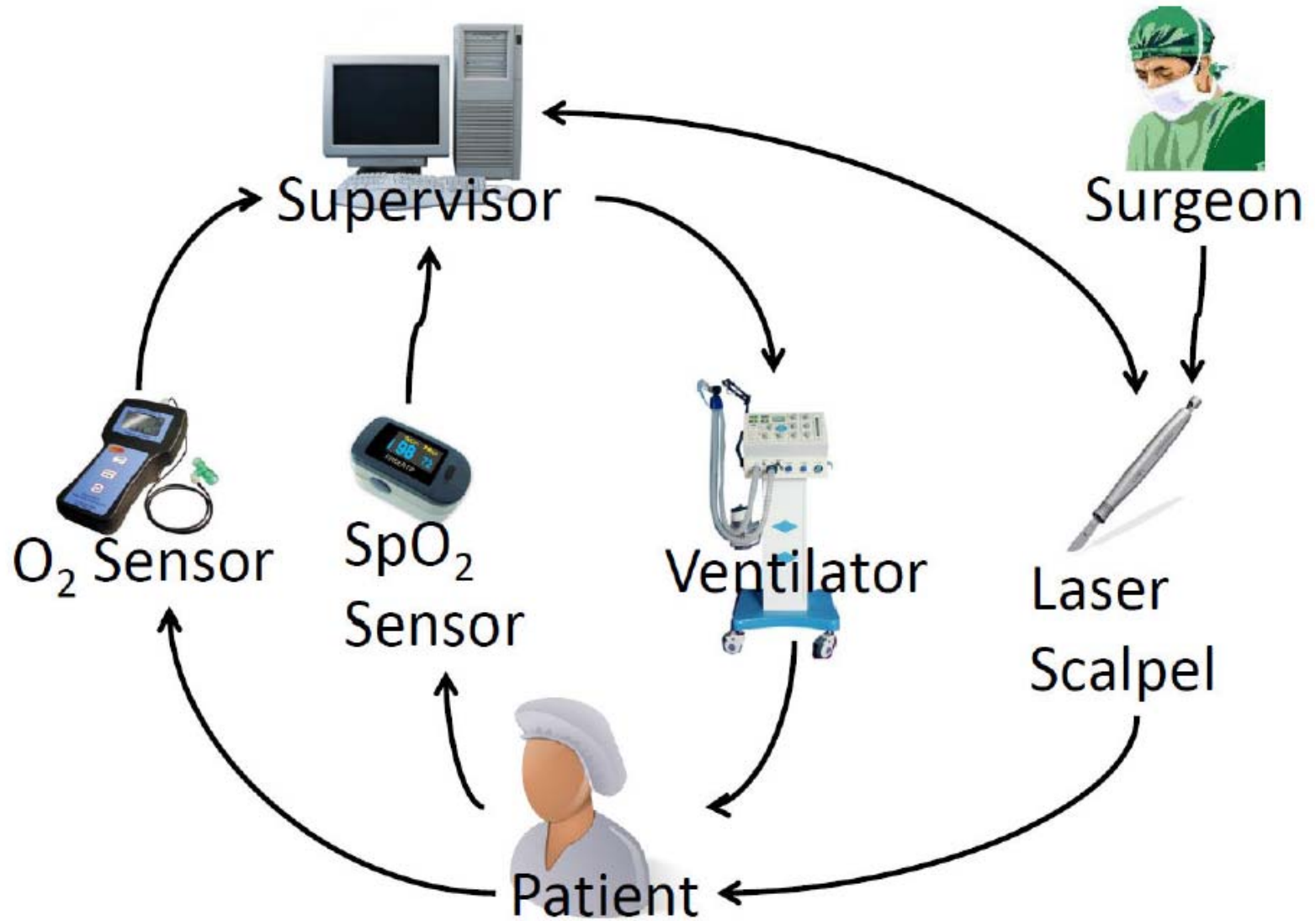
Time-Unbounded Behavior (Long-Run Future)

Challenge 1: No good offline models for complex biomedical systems of human body.

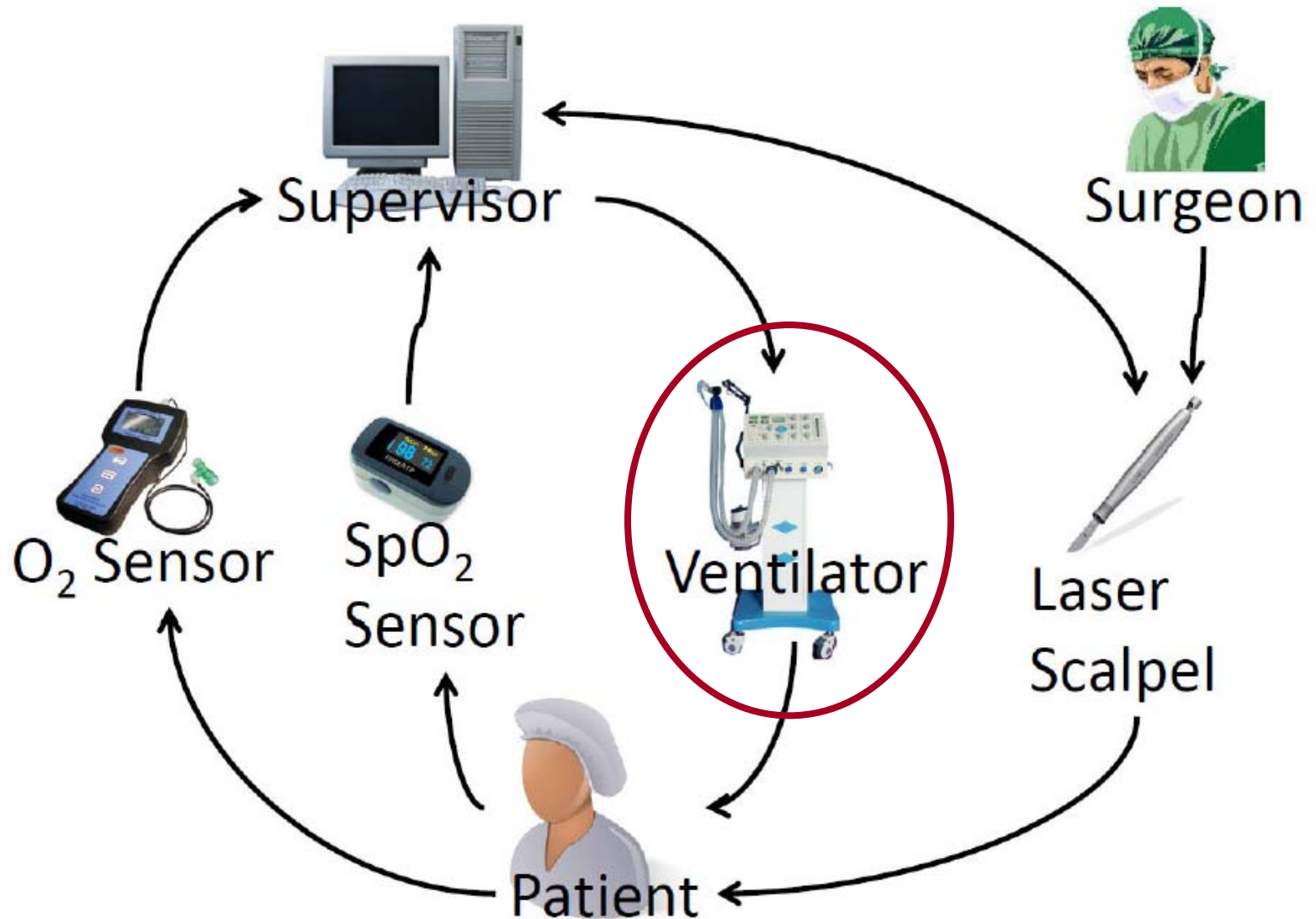
Challenge 2: Verification state space easily explode.



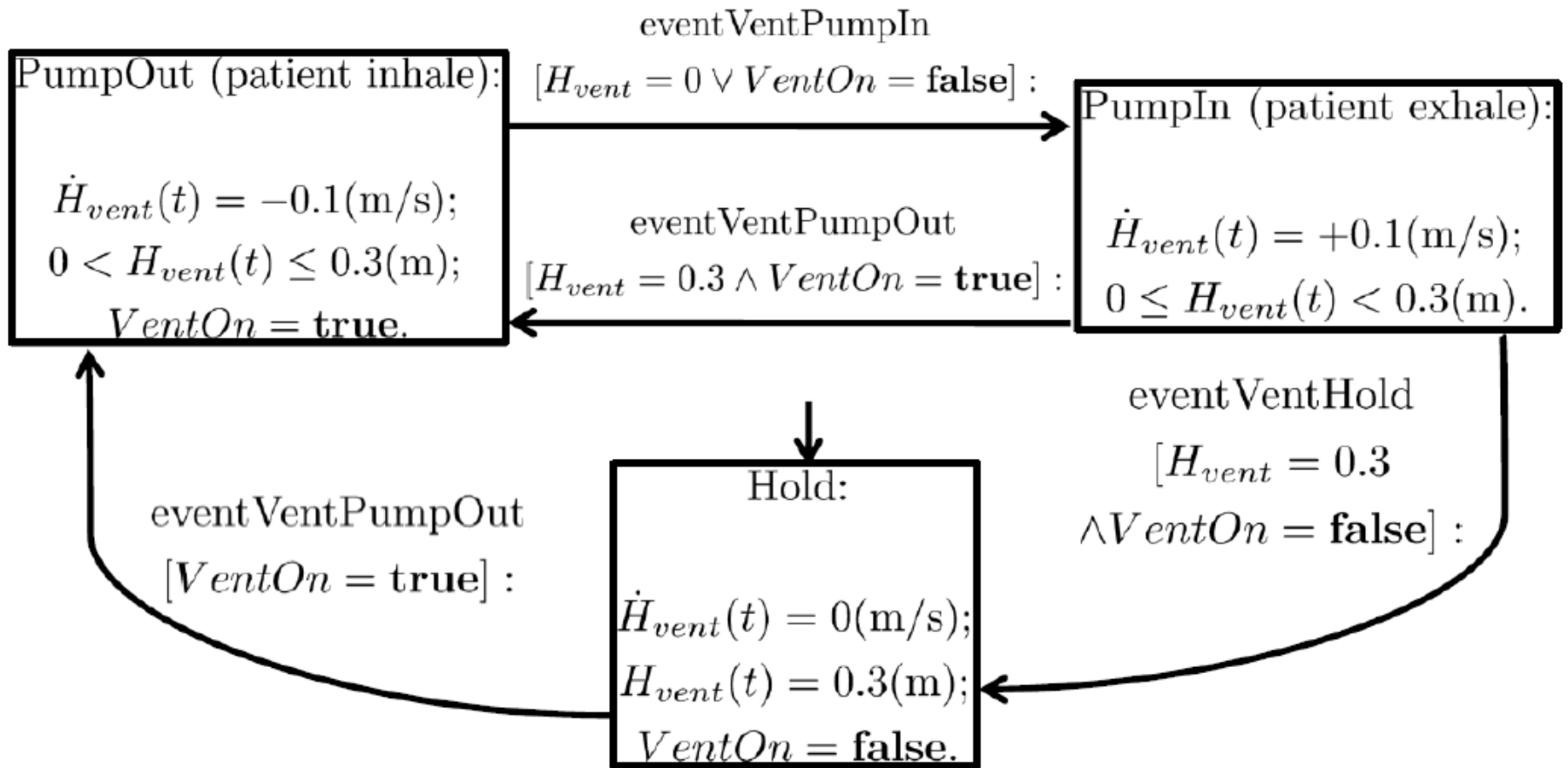
✓✗ Take laser tracheotomy offline hybrid systems modeling as an example.



✔✘ Take laser tracheotomy offline hybrid systems modeling as an example.



✔✘ Take laser tracheotomy offline hybrid systems modeling as an example.



Legend:

→ (w/ source location) Event;  
(w/o source location) Initial  
location indicator



Location

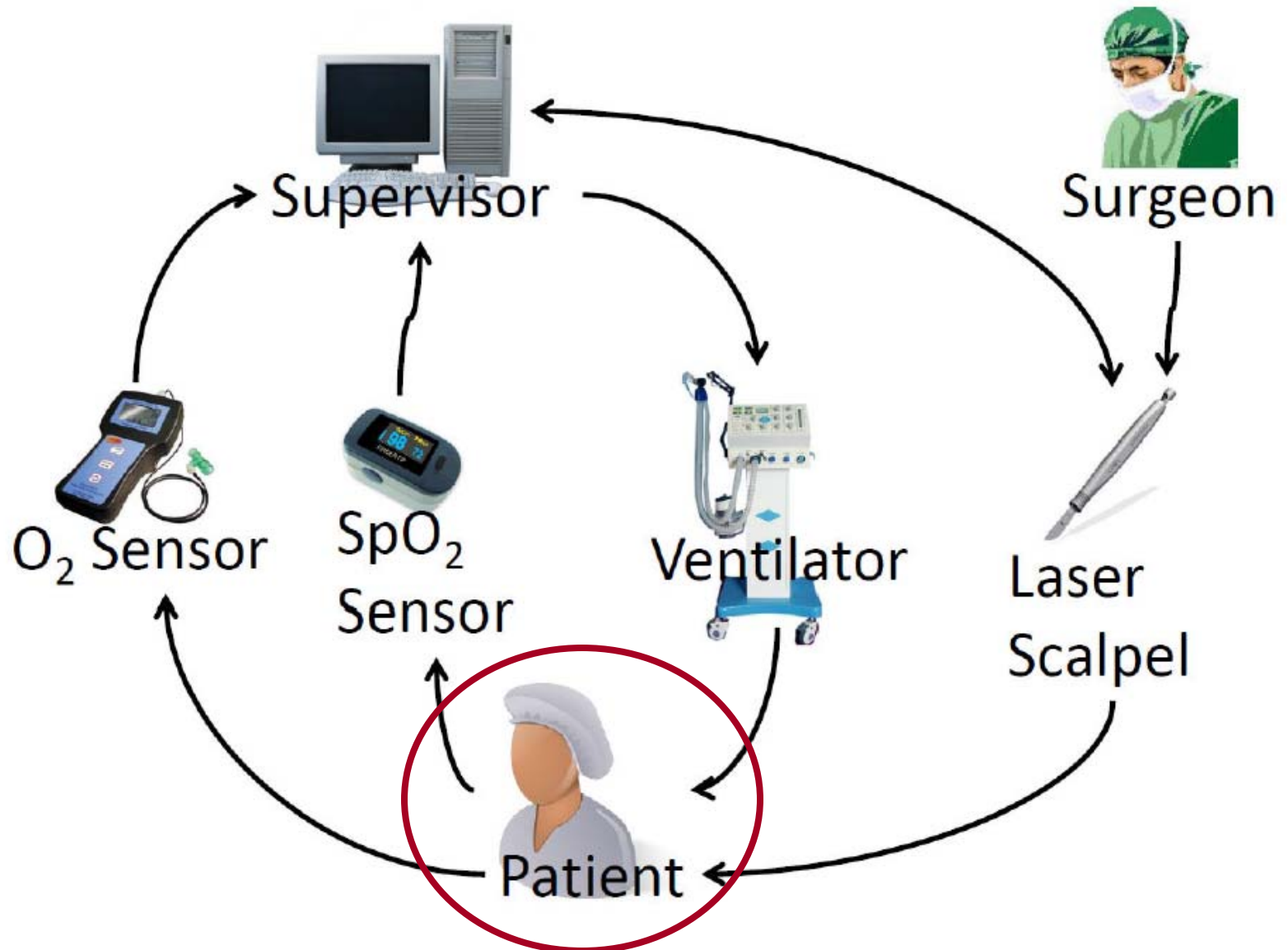


Event guard (event triggering condition)



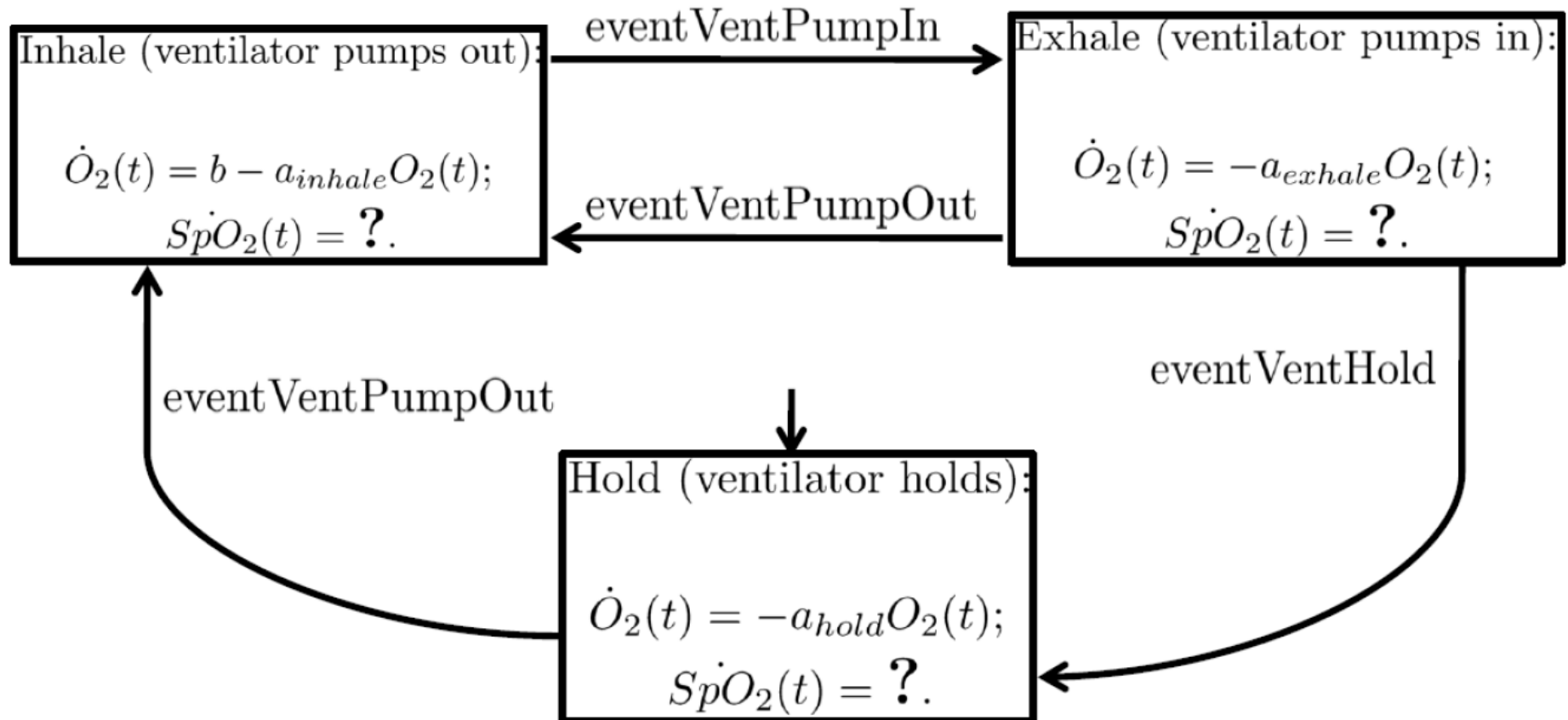
Variable value update

✓✗ Take laser tracheotomy offline hybrid systems modeling as an example.





Take laser tracheotomy offline hybrid systems modeling as an example: model  $\text{SpO}_2$  offline?





✓✗ Online periodical real-time hybrid systems model checking of time-bounded (i.e., short-run) future!

✓✗ Online periodical real-time hybrid systems model checking of time-bounded (i.e., short-run) future!

Traditional model checking vs. Ours:

Offline	↔	Online Periodical Real-Time
Long-Run Future	↔	Short-Run Future

✓✗ Online periodical real-time hybrid systems model checking of time-bounded (i.e., short-run) future!

Traditional model checking vs. Ours:

Offline	↔	Online Periodical Real-Time
Long-Run Future	↔	Short-Run Future

Challenge 1: No good offline models for complex biomedical systems of human body.

✓✗ Online periodical real-time hybrid systems model checking of time-bounded (i.e., short-run) future!

Traditional model checking vs. Ours:

Offline	↔	Online Periodical Real-Time
Long-Run Future	↔	Short-Run Future

Challenge 1: No good offline models for complex biomedical systems of human body.

Most vital signs' online short-run behavior is easy to predict.

✓✗ Online periodical real-time hybrid systems model checking of time-bounded (i.e., short-run) future!

Traditional model checking vs. Ours:

Offline	↔	Online Periodical Real-Time
Long-Run Future	↔	Short-Run Future

Challenge 1: No good offline models for complex biomedical systems of human body.

Most vital signs' online short-run behavior is easy to predict.

Challenge 2: Verification state space easily explode.



# Online periodical real-time hybrid systems model checking of time-bounded (i.e., short-run) future!

Traditional model checking vs. Ours:

Offline	↔	Online Periodical Real-Time
Long-Run Future	↔	Short-Run Future

Challenge 1: No good offline models for complex biomedical systems of human body.

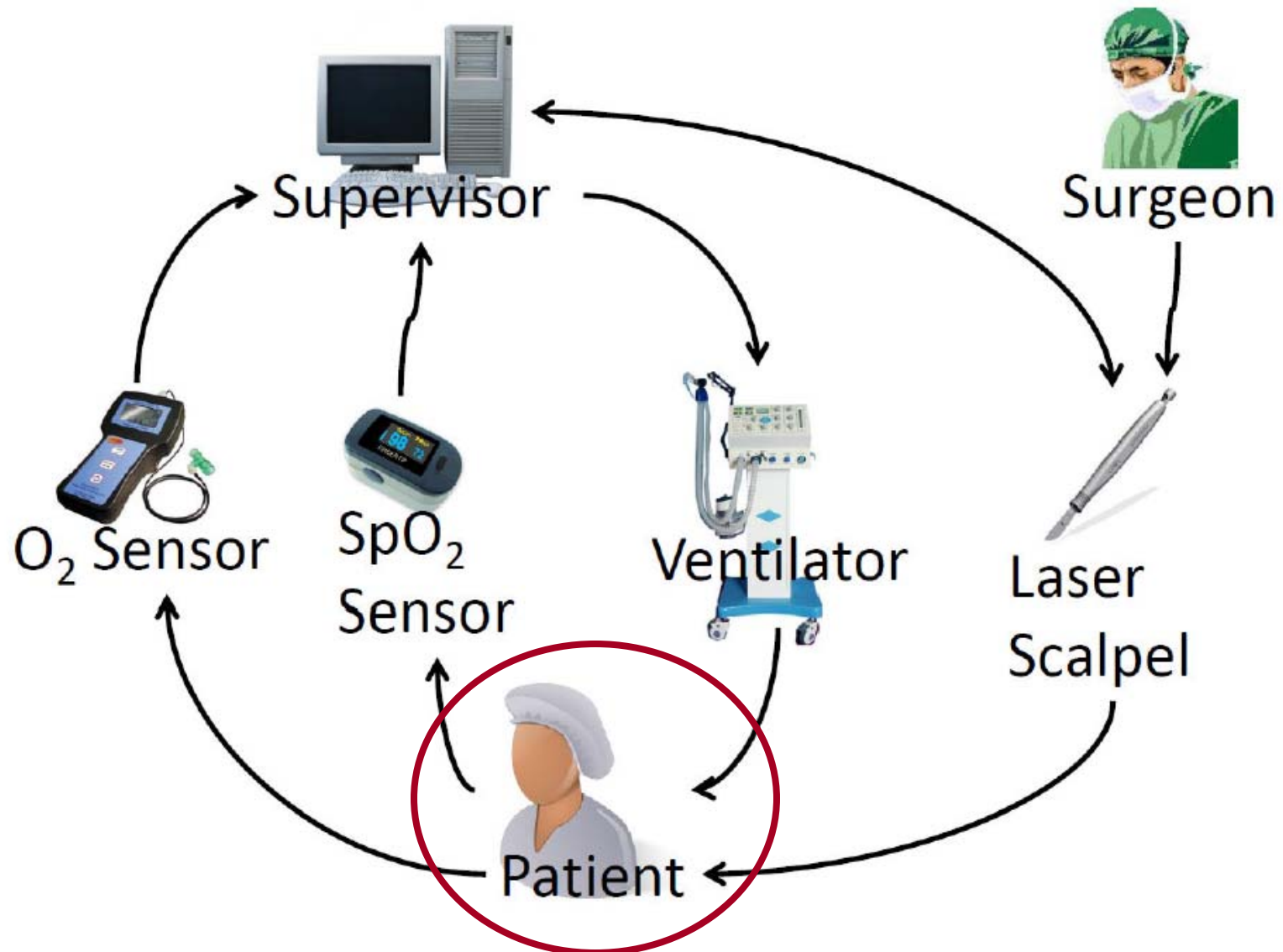
Most vital signs' online short-run behavior is easy to predict.

Challenge 2: Verification state space easily explode.

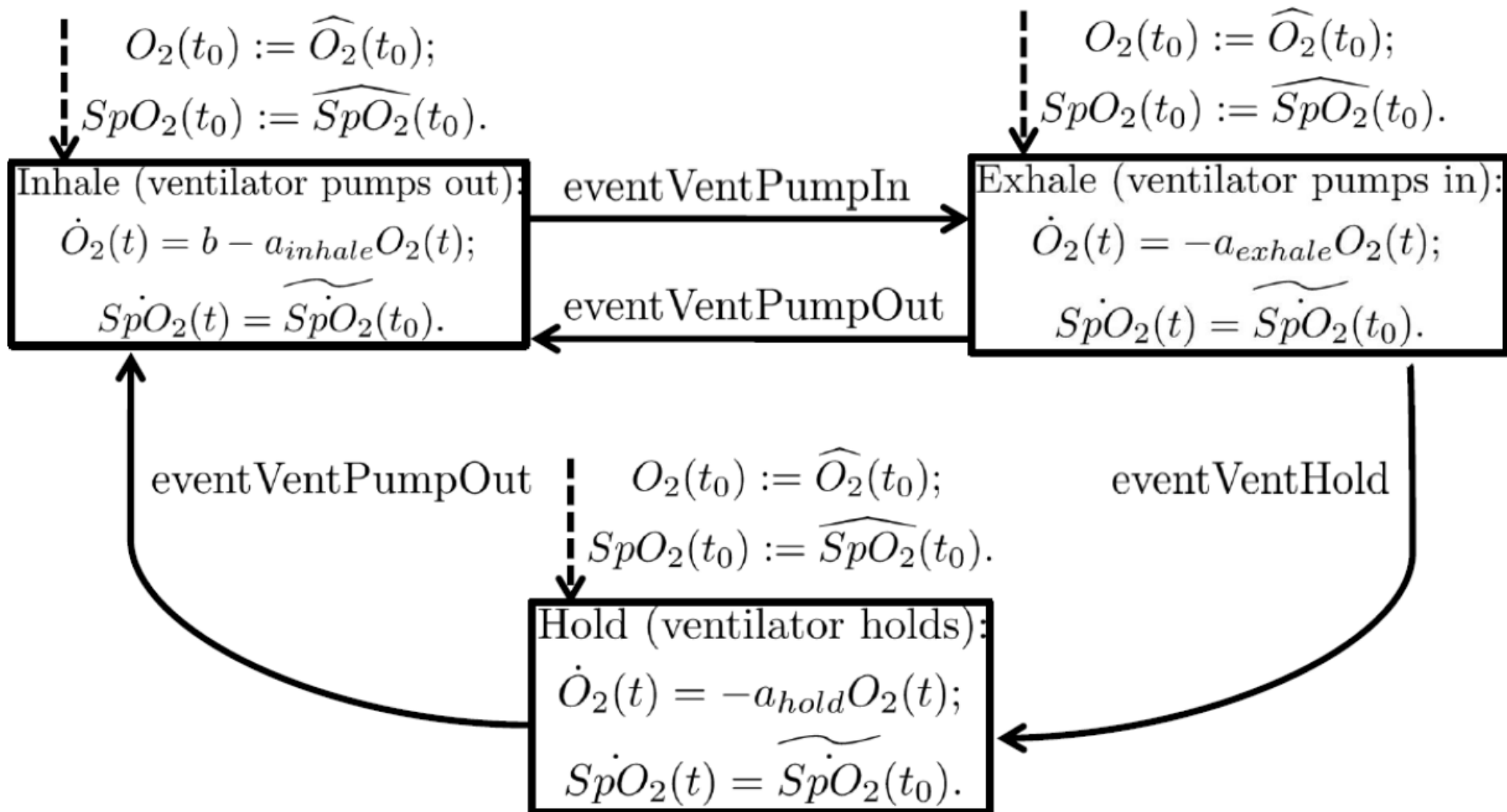
Online → Fixes Many Parameters

Short-Run → Shrink State Space

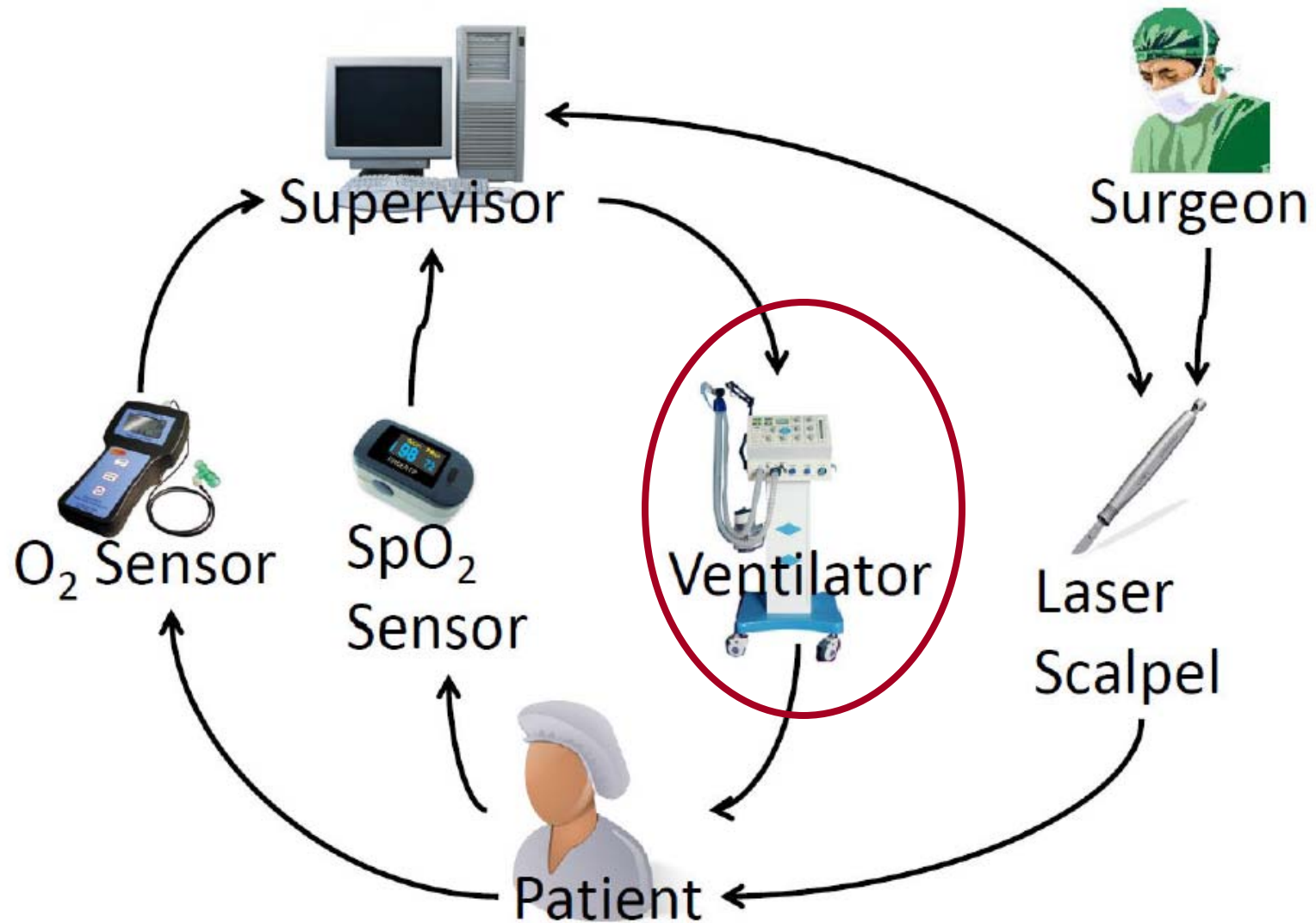
✔✘ Let's model the patient again, now online and short-run, with period  $T$ .



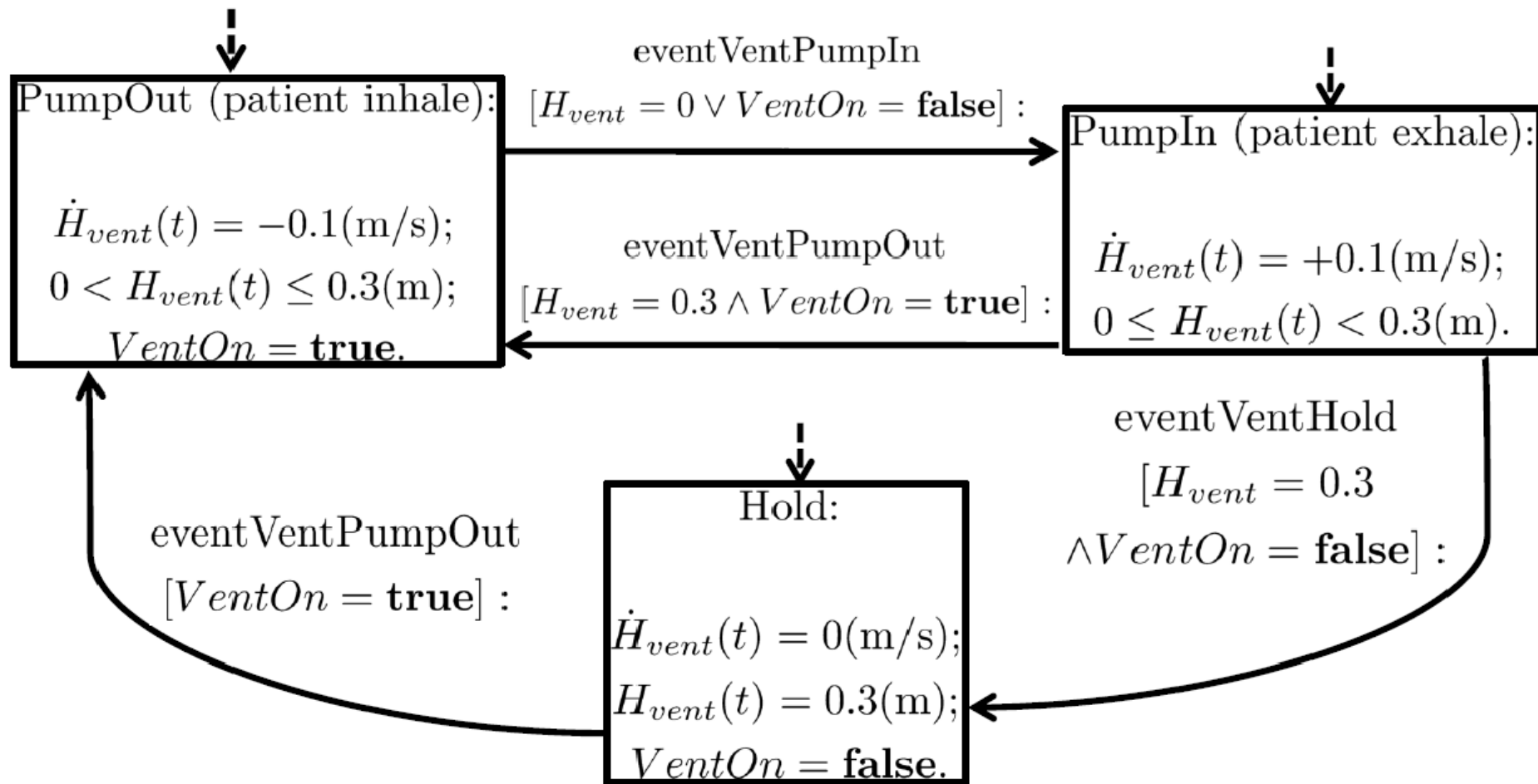
✔✘ Let's model the patient again, now online and short-run, with period  $T$ .



✓✗ The online short-run model for ventilator.

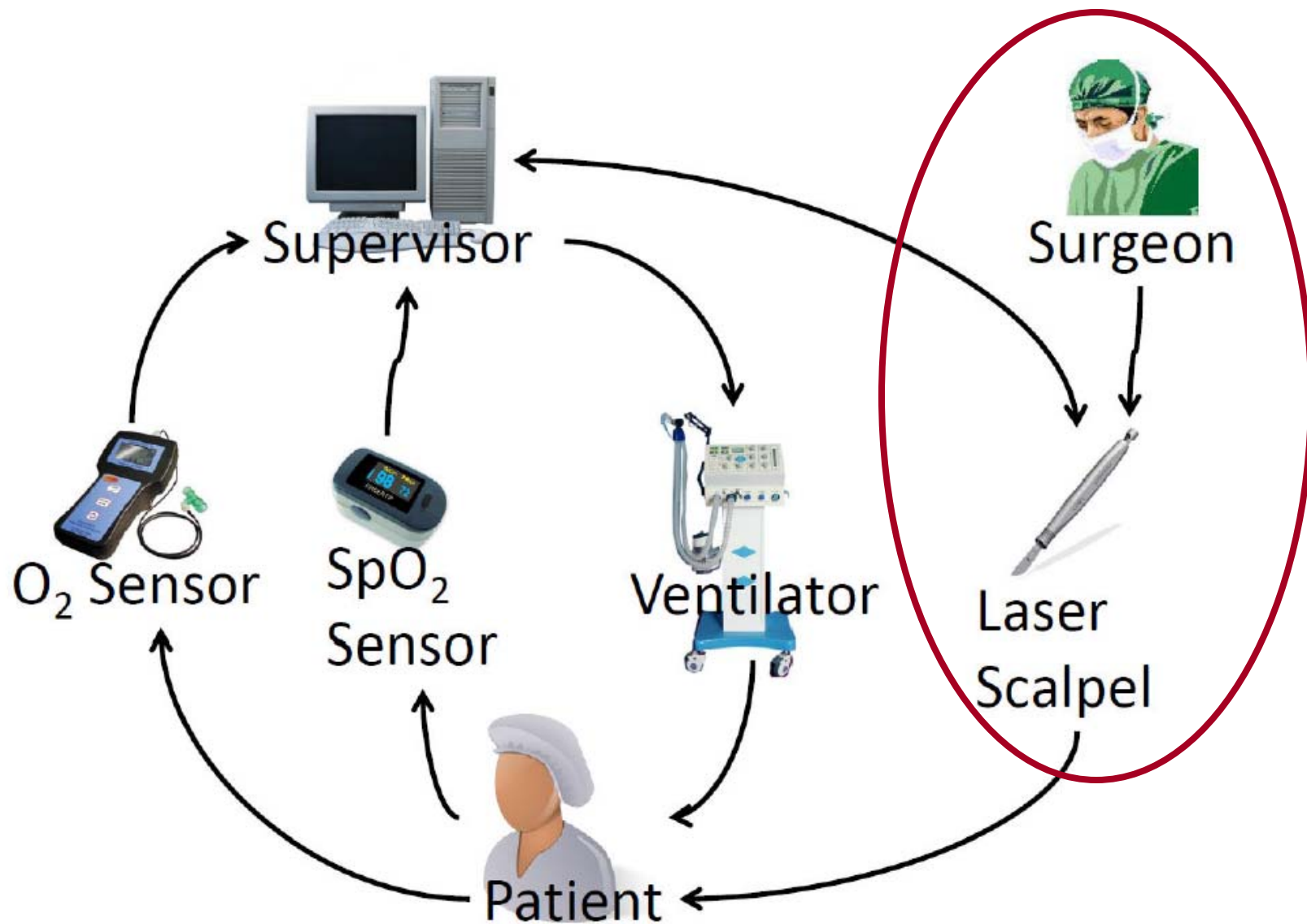


✔✘ The online short-run model for ventilator.

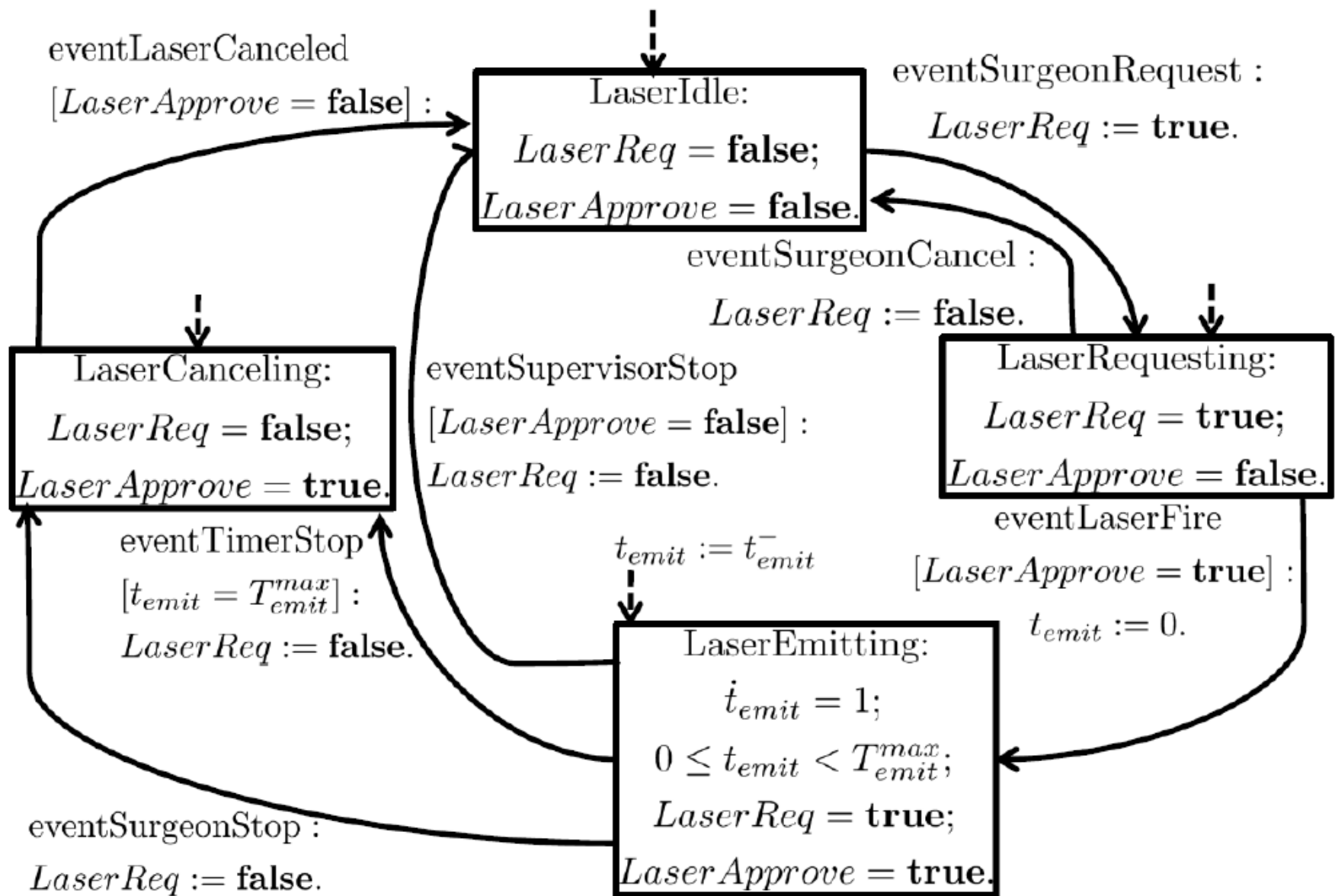




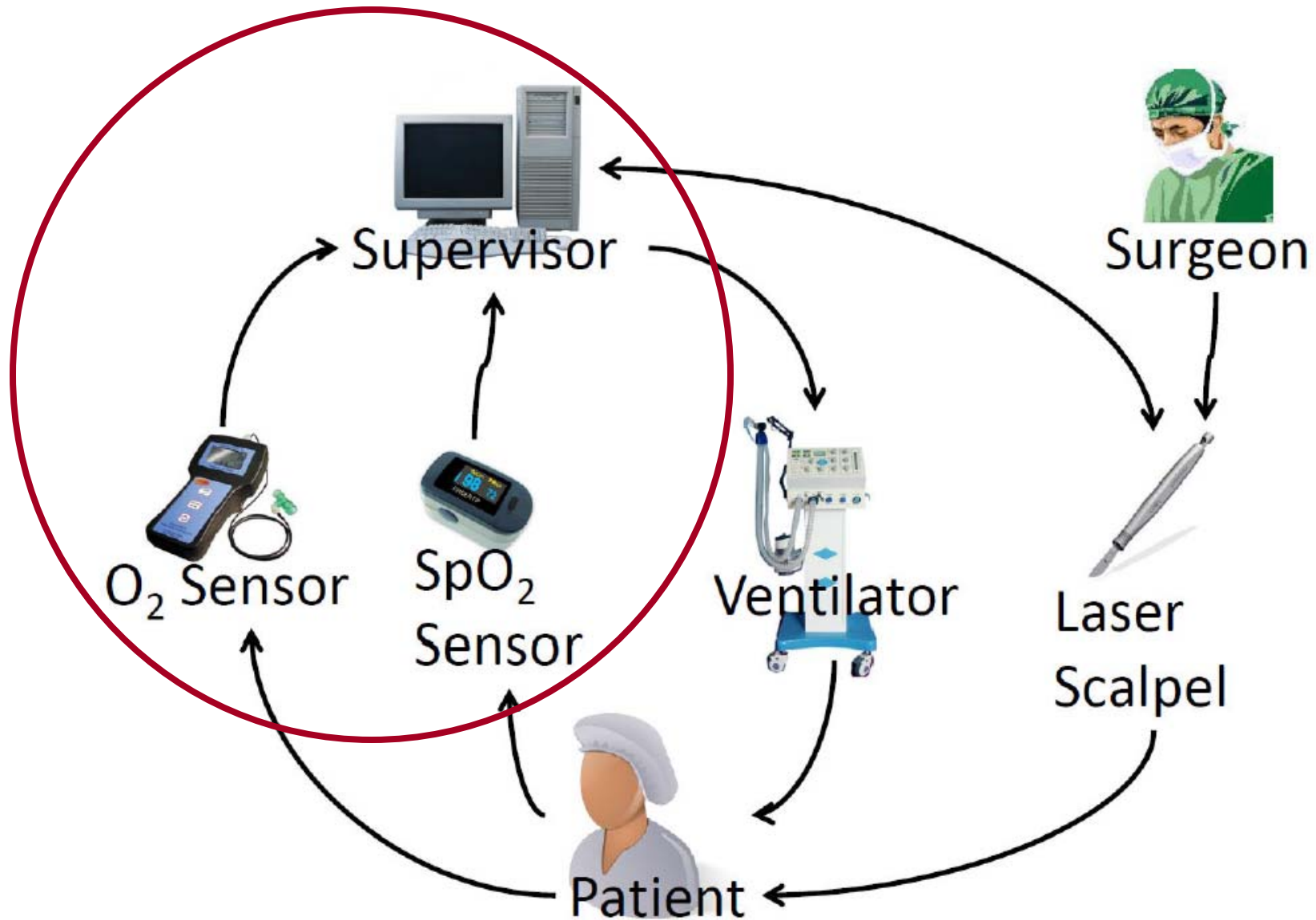
✓✗ The online short-run model for laser-scalpel.



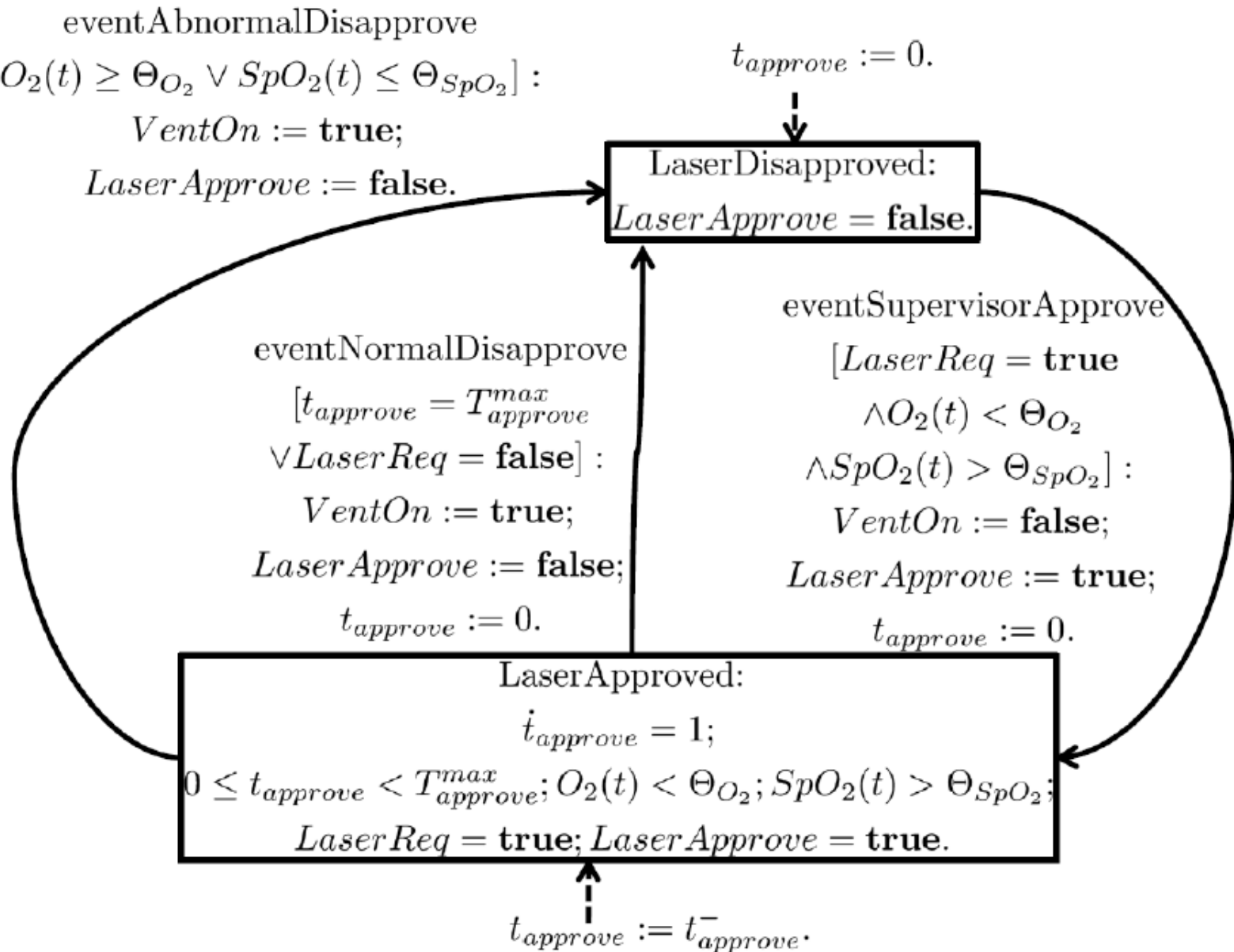
# ✓✗ The online short-run model for laser-scalpel.



✓✗ The online short-run model for supervisor.



# The online short-run model for supervisor.



✔✘ Question: Can the hybrid systems model checking finish (terminate) within period  $T$  ?



✔✘ Question: Can the hybrid systems model checking finish (terminate) within period  $T$  ?

Hybrid Systems Model Checking → undecidable

✓✗ Question: Can the hybrid systems model checking finish (terminate) within period  $T$  ?

Hybrid Systems Model Checking  $\rightarrow$  undecidable



Linear Hybrid Automaton (LHA) model checking  $\rightarrow$  undecidable

✓✗ Question: Can the hybrid systems model checking finish (terminate) within period  $T$  ?

Hybrid Systems Model Checking  $\rightarrow$  undecidable

Linear Hybrid Automaton (LHA) model checking  $\rightarrow$  undecidable

Strongly Non-Zeno LHA time-bounded reachability model checking  $\rightarrow$  decidable

  Question: Can the hybrid systems model checking finish (terminate) within period  $T$  ?

Hybrid Systems Model Checking  $\rightarrow$  undecidable

Linear Hybrid Automaton (LHA) model checking  $\rightarrow$  undecidable

Strongly Non-Zeno LHA time-bounded reachability model checking  $\rightarrow$  decidable

SNZ-LHA is powerful enough to describe laser tracheotomy scenario, a representative MDPnP application.

# ✔✘ Evaluation Setup



## Evaluation Setup

Emulated Oxymeter and O2 sensor using NIH  
PhysioNet real-world patient vital sign traces.

## Evaluation Setup

Emulated Oxymeter and O2 sensor using NIH PhysioNet real-world patient vital sign traces.

Sampling/Model-Checking Period:  $T = 3$  second.

## Evaluation Setup

Emulated Oxymeter and O2 sensor using NIH PhysioNet real-world patient vital sign traces.

Sampling/Model-Checking Period:  $T = 3$  second.

Hand written online model generator + PHAVer hybrid systems model checker

## Evaluation Setup

Emulated Oxymeter and O2 sensor using NIH PhysioNet real-world patient vital sign traces.

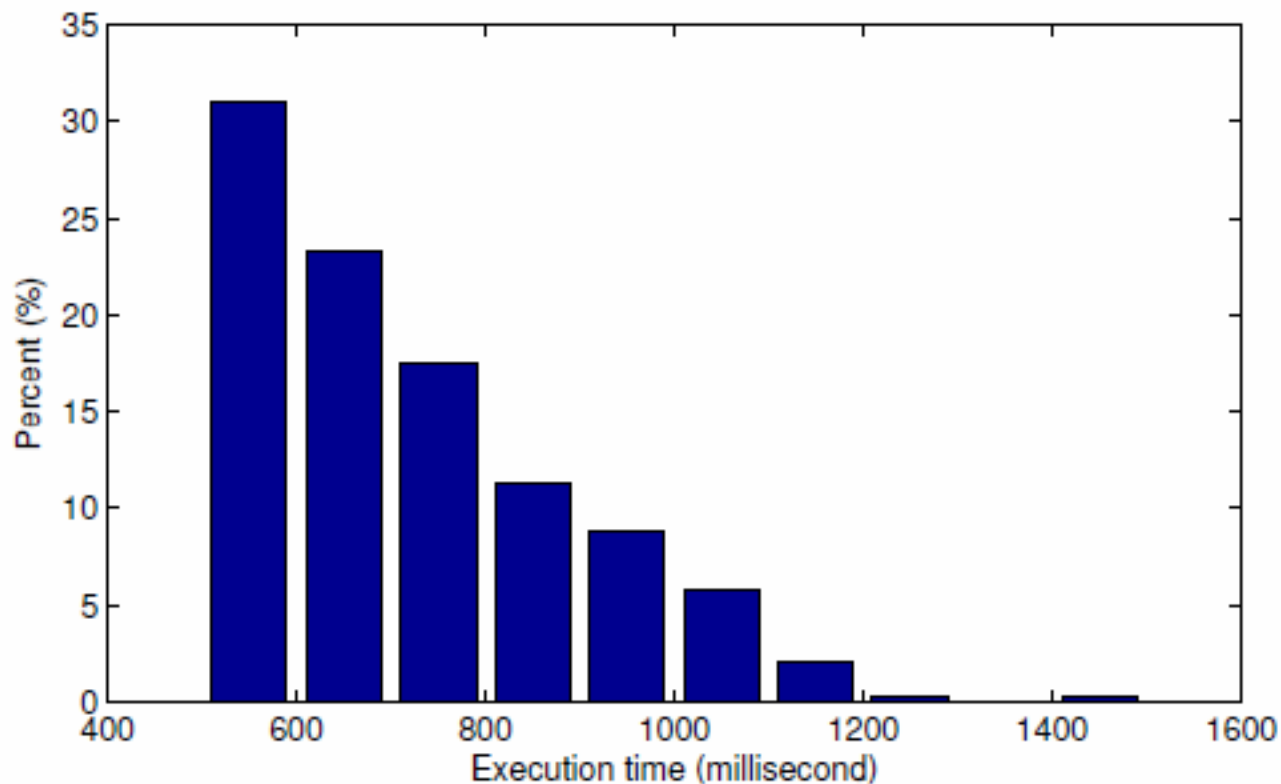
Sampling/Model-Checking Period:  $T = 3$  second.

Hand written online model generator + PHAVer hybrid systems model checker

Lenovo Thinkpad X201 + Intel Core i5  
+ 2.9G Mem + 32-bit Ubuntu 10.10

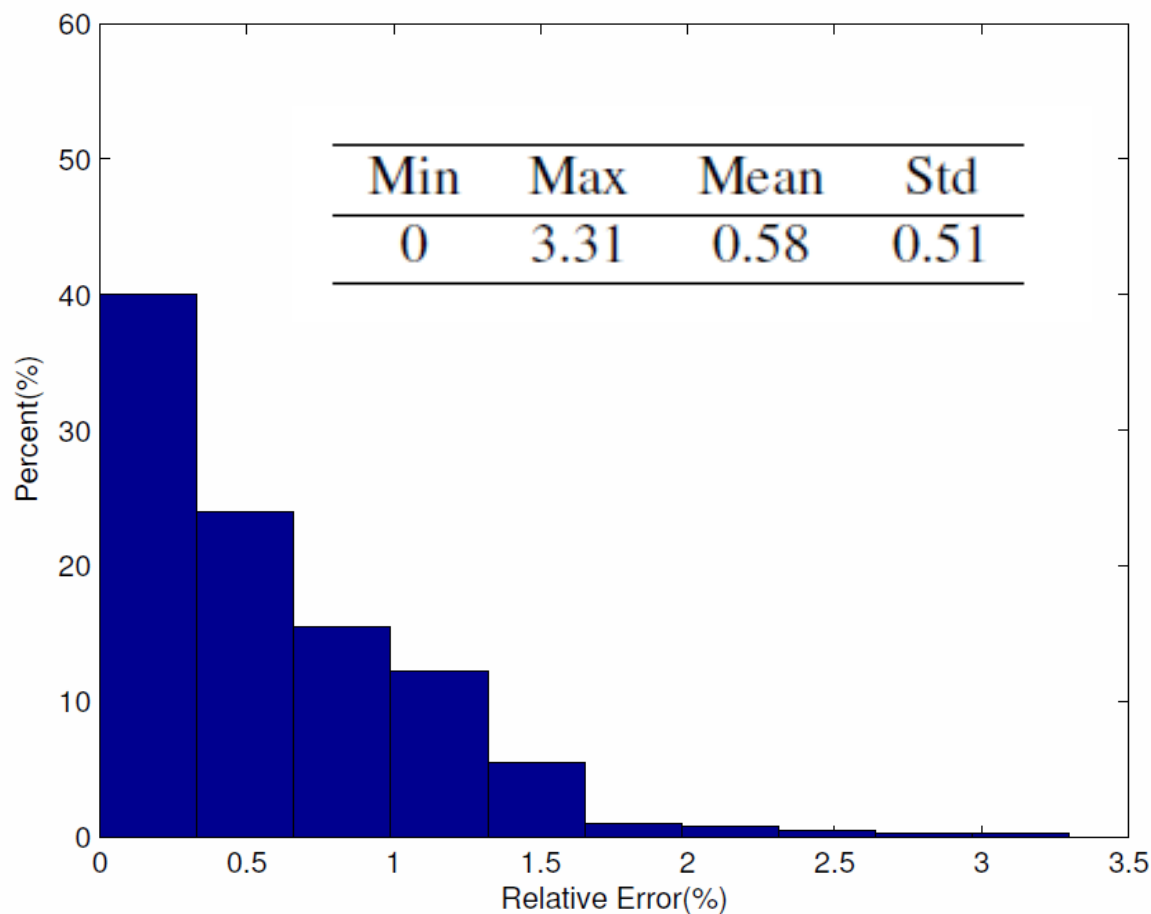
✔✘ Statistics of execution (modeling + checking) time cost: real-time feasible (with pipelining).

Min	Max	Mean	Std
0.571	1.445	0.727	0.163



# Statistics of online SpO<sub>2</sub> prediction accuracy

$$ERR_{SpO_2}(t_0 + T) = \frac{|\widehat{SpO_2}(t_0 + T) - \widetilde{SpO_2}(t_0 + T)|}{\widehat{SpO_2}(t_0 + T)}$$





## Related Work

Runtime Verification [finkbeiner02]

Online discrete systems model checking  
[qi09][easwaran06]

Other hybrid systems model checkers  
[robby03][bartocci08]

# Contents



Demand



Modeling and Verification



**Dependable Medical Wireless Networking**

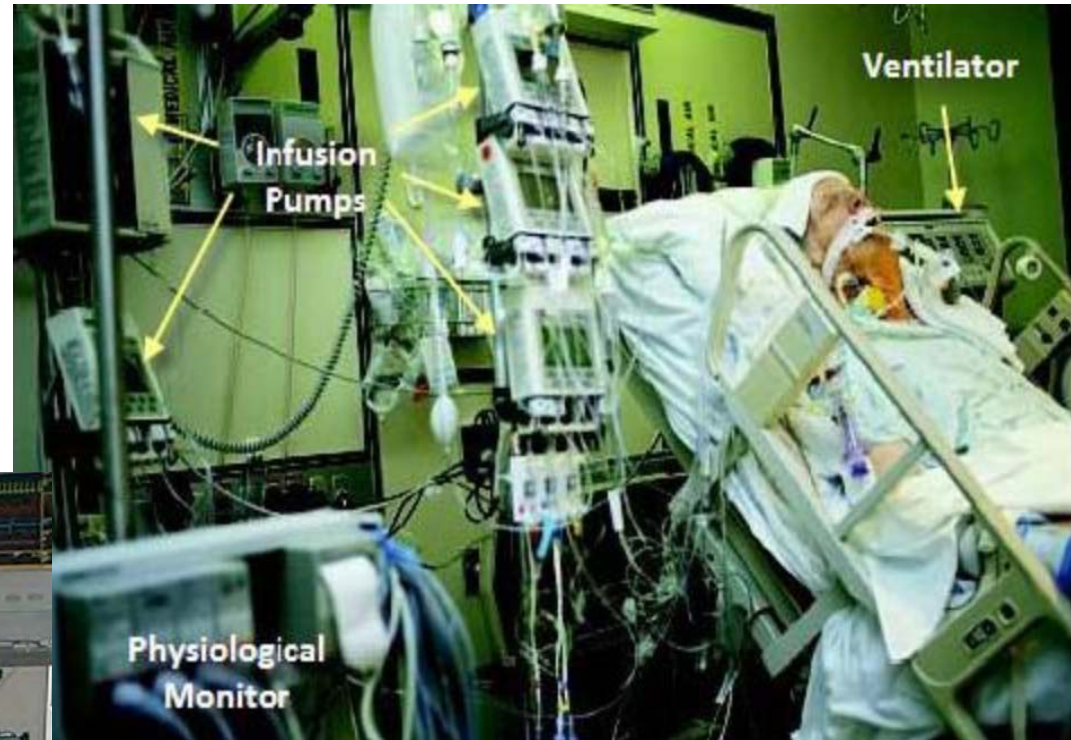


Vision



WBAN based medical parameter monitoring overcomes the many drawbacks of wired monitoring.

- Tying patient to bed 24x7
- Small movement → electrode fall off
- Risk of tripping over wires



## •Wired Monitoring

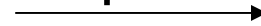
•(photos from <http://www.mdpnp.org> )



# Advantages of WBAN based medical parameter monitoring



uplink



downlink



Electrodes  
/ client

Monitor /  
Base station





# Medical WBAN Features

## Low duty cycle

Typical sampling rate  $< 300\text{Hz}$  [physionet]

Wakeup on demand

Low data rate  $\sim 500\text{Kbps}$  [ieee15.6]

Low transmit power  $< 1\text{mW}$  [ieee15.6]

Disparate Delay requirements

Electro-Cardio Graph (ECG):  $< 500\text{ms}$  [chevrollier05]

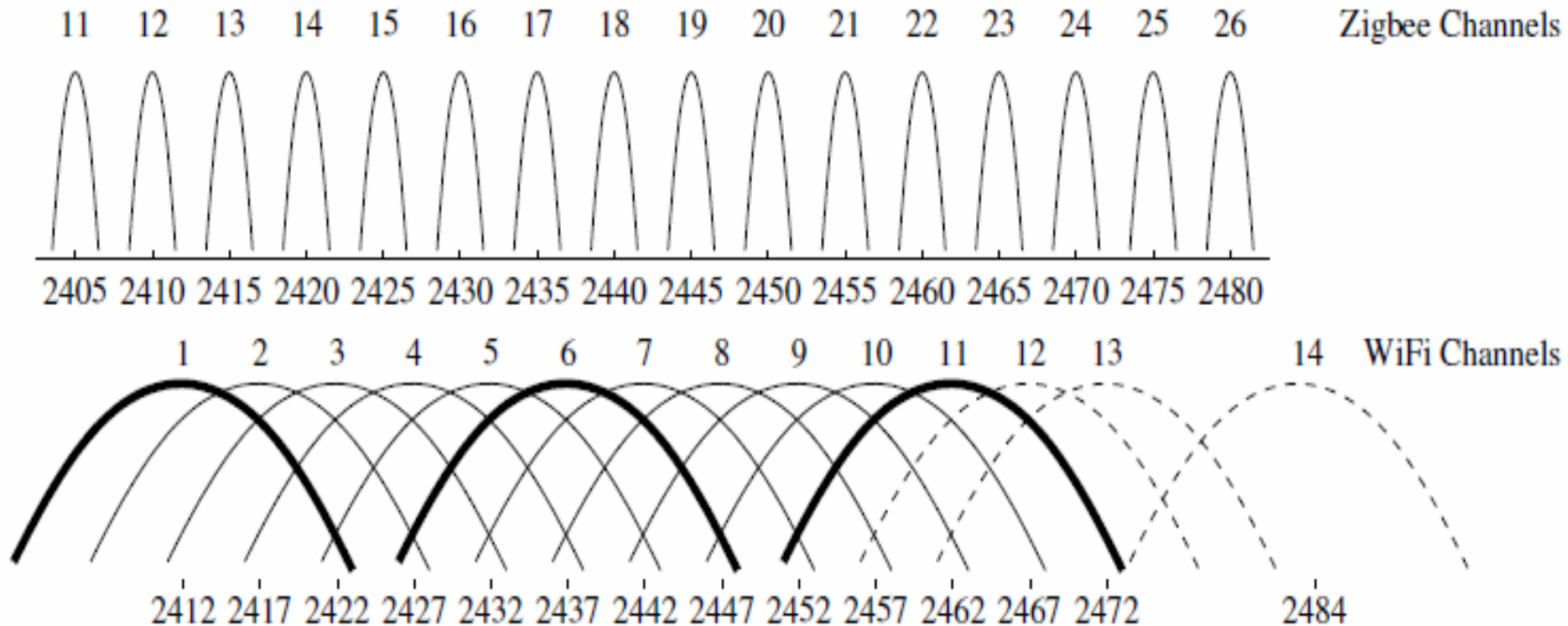
Body temperature monitoring: several seconds  
[chipara10]

Single-Hop centralized WBAN is the preferred architecture

Emerging standard: ZigBee WBAN with centralized polling



# WiFi Co-Channel Interference is a major threat to WBAN [wang11]



Zigbee channels vs. 802.11b WiFi channels  
[liang10]





# WiFi Co-Channel Interference is a major threat to WBANs

## Power asymmetry [huang10]

Typical WiFi power  $\approx 30\text{mW}$

Typical Zigbee (Bluetooth, IEEE 802.15.6 etc.) power  $\leq 1\text{mW}$

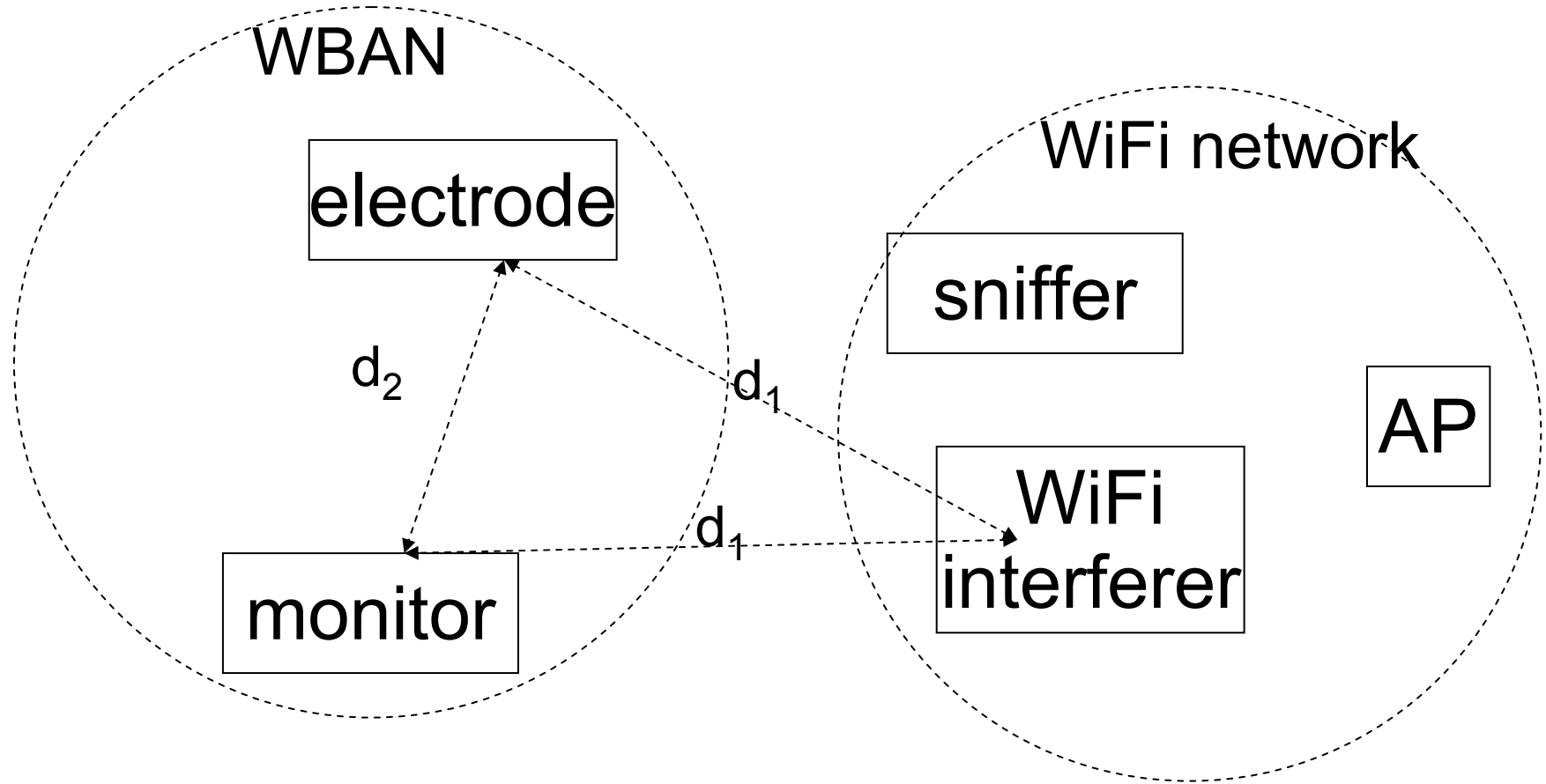
## MAC asymmetry [huang10][gummadi07]

Many WiFi device use *Carrier Sense* (CS) based *Clear Channel Assessment* (CCA). Such WiFi devices do not back off to Zigbee.

Many Zigbee uses *Energy Detection* (ED) CCA to assess the channel. Zigbee backs off to WiFi.

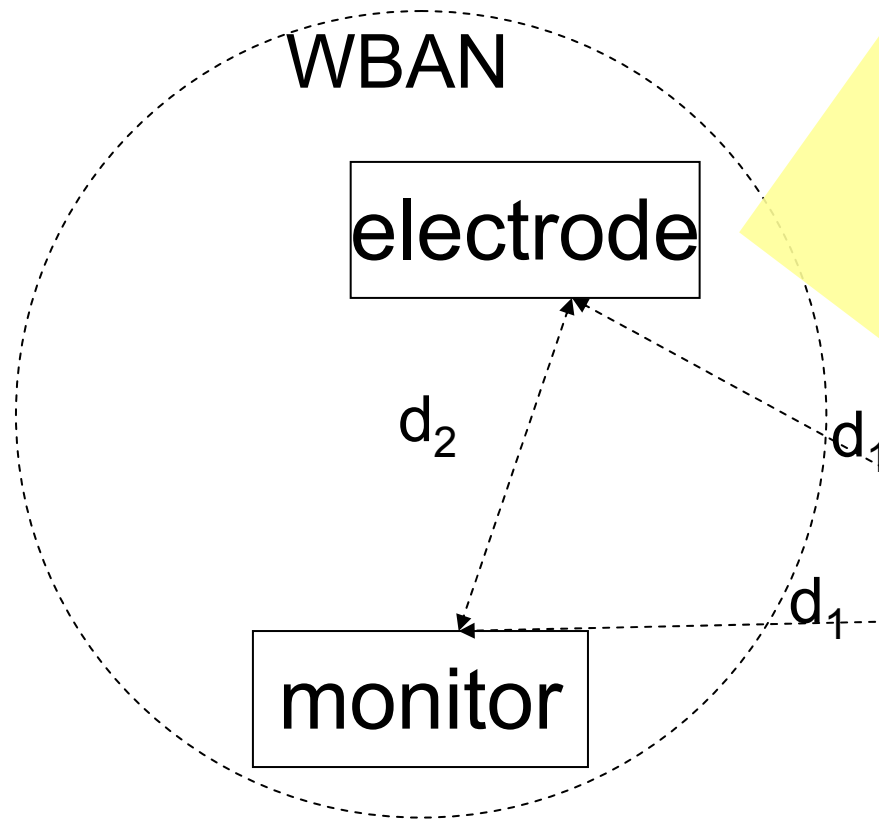


# Our experiment confirms the threat of WiFi to WBANs





# Our experiment confirms the threat of WiFi to WBANs



## WBAN

monitor: Base station  
polling period: 100ms

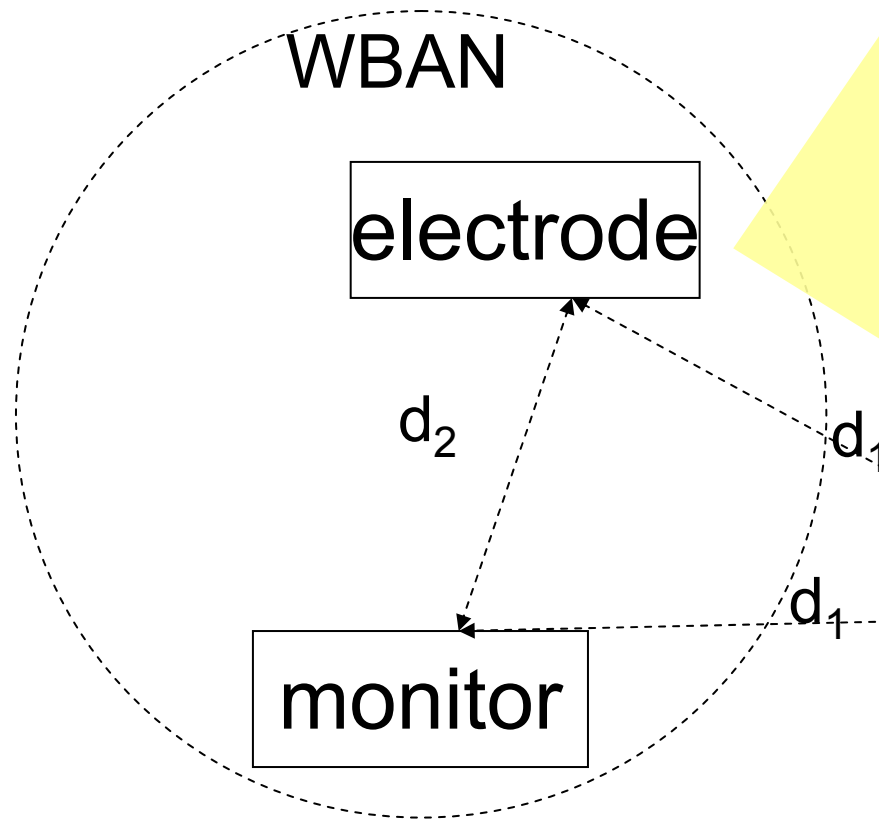
electrode: Client  
250 samples / sec  
(4ms / sample)

25 samples / **chunk**  
(100ms / chunk)

3 chunks / packet, i.e., each  
chunk is retransmitted 3  
times  
(costs  $\leq 4$ ms to send a  
packet)



# Our experiment confirms the threat of WiFi to WBANs



## WBAN

monitor: Base station  
polling period: 100ms

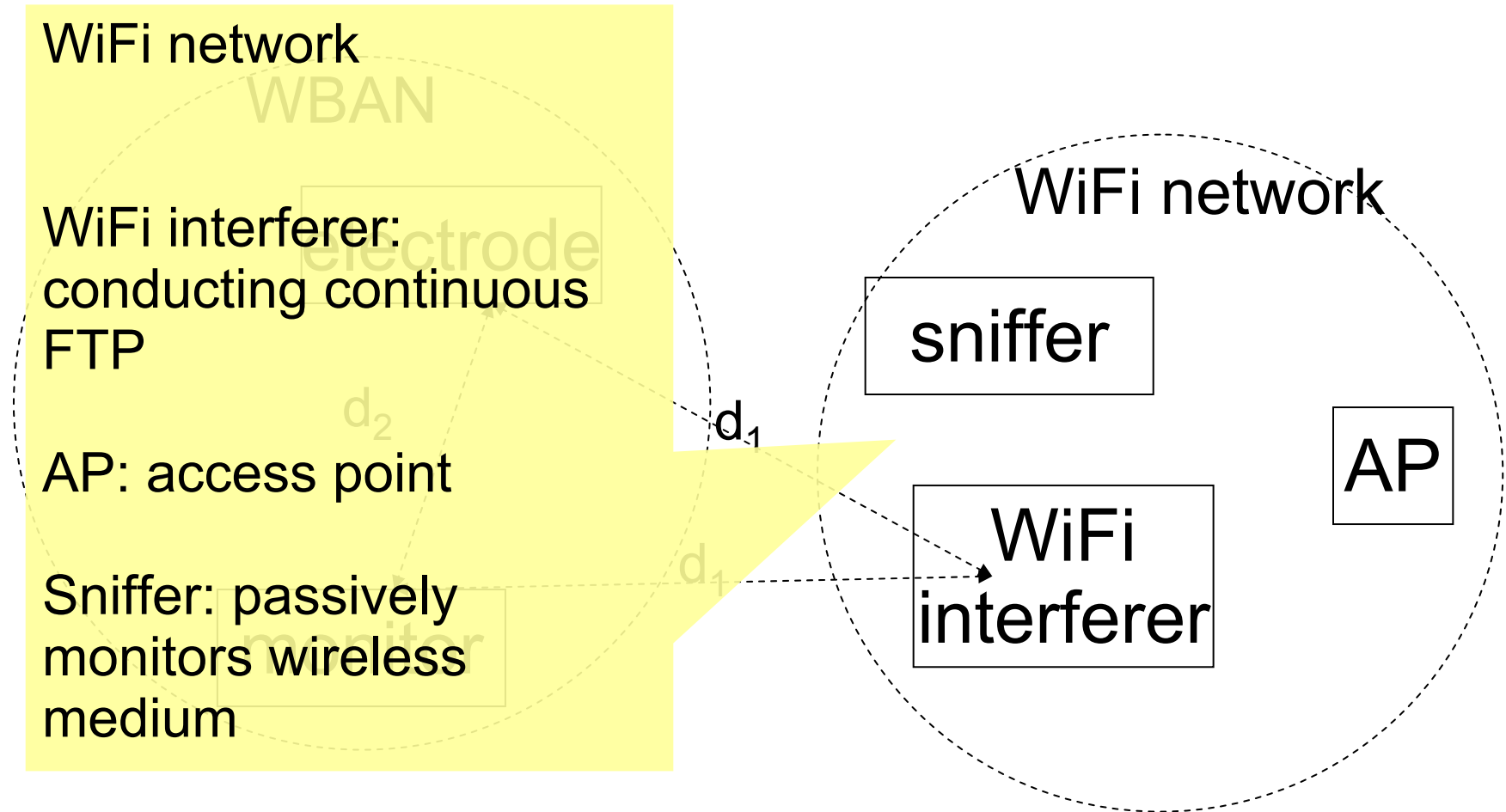
electrode: Client  
250 samples / sec  
(4ms / sample)

25 samples / **chunk**  
(100ms / chunk)

3 chunks / packet, i.e., each  
chunk is retransmitted 3  
times  
(costs  $\leq 4$ ms to send a  
packet)

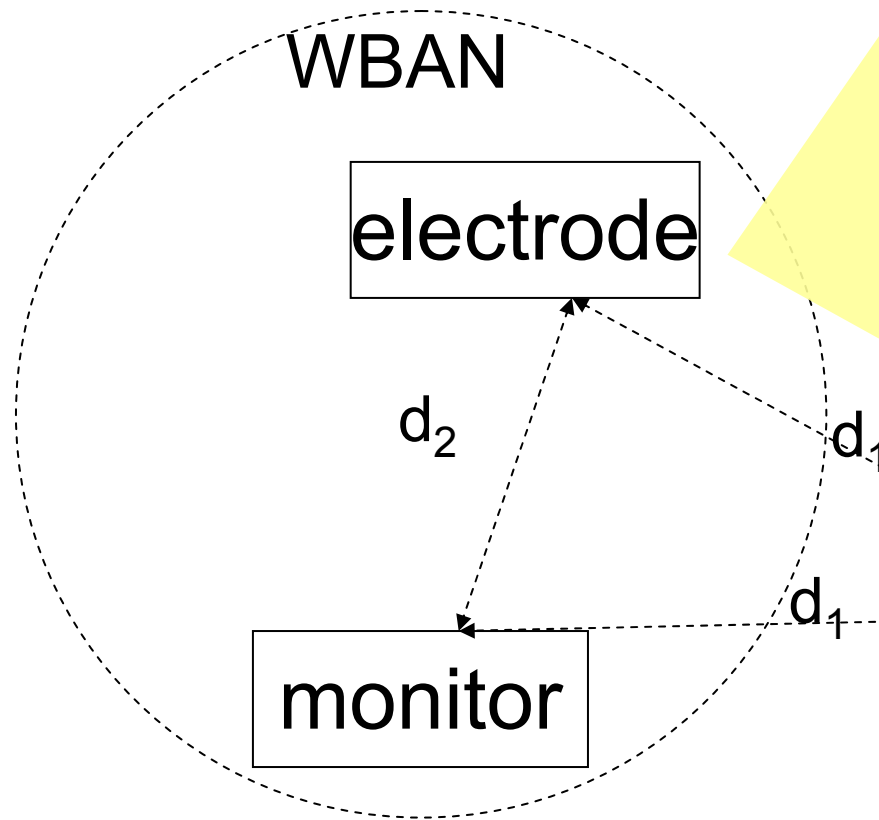


# Our experiment confirms the threat of WiFi to WBANs





# Our experiment confirms the threat of WiFi to WBANs



## WBAN

monitor: Base station  
polling period: 100ms

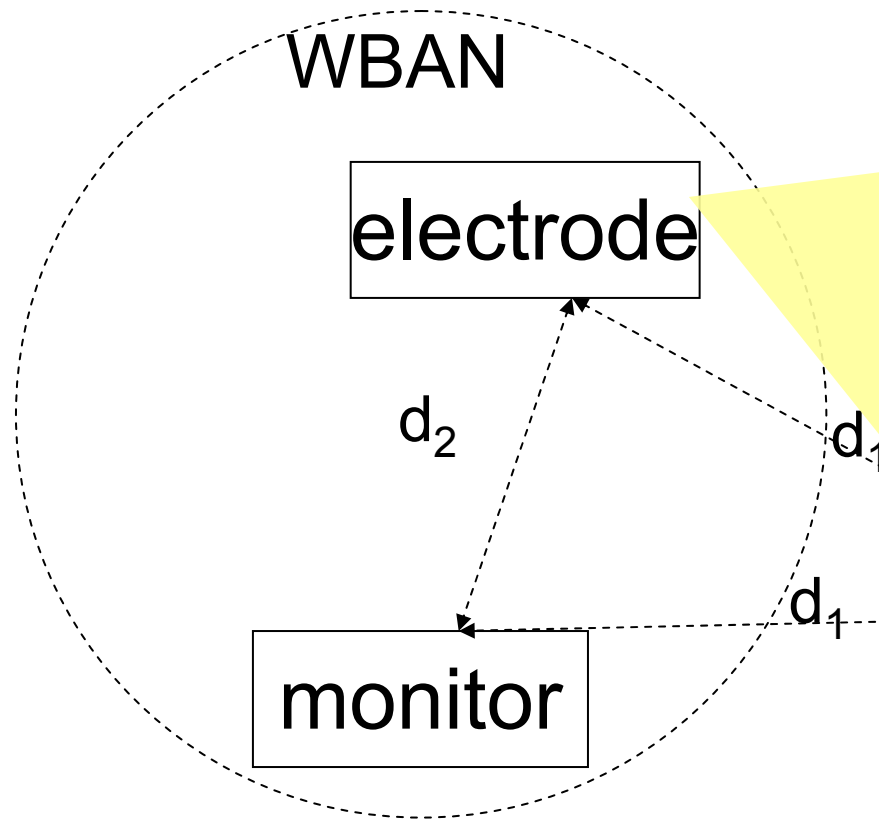
electrode: Client  
250 samples / sec  
25 samples / chunk  
3 chunks / packet, i.e., each  
chunk is retransmitted 3  
times

**Failure:** a chunk fails all of its retransmissions.





# Our experiment confirms the threat of WiFi to WBANs



Failure: a chunk fails all  $Nre = 3$  retransmissions.

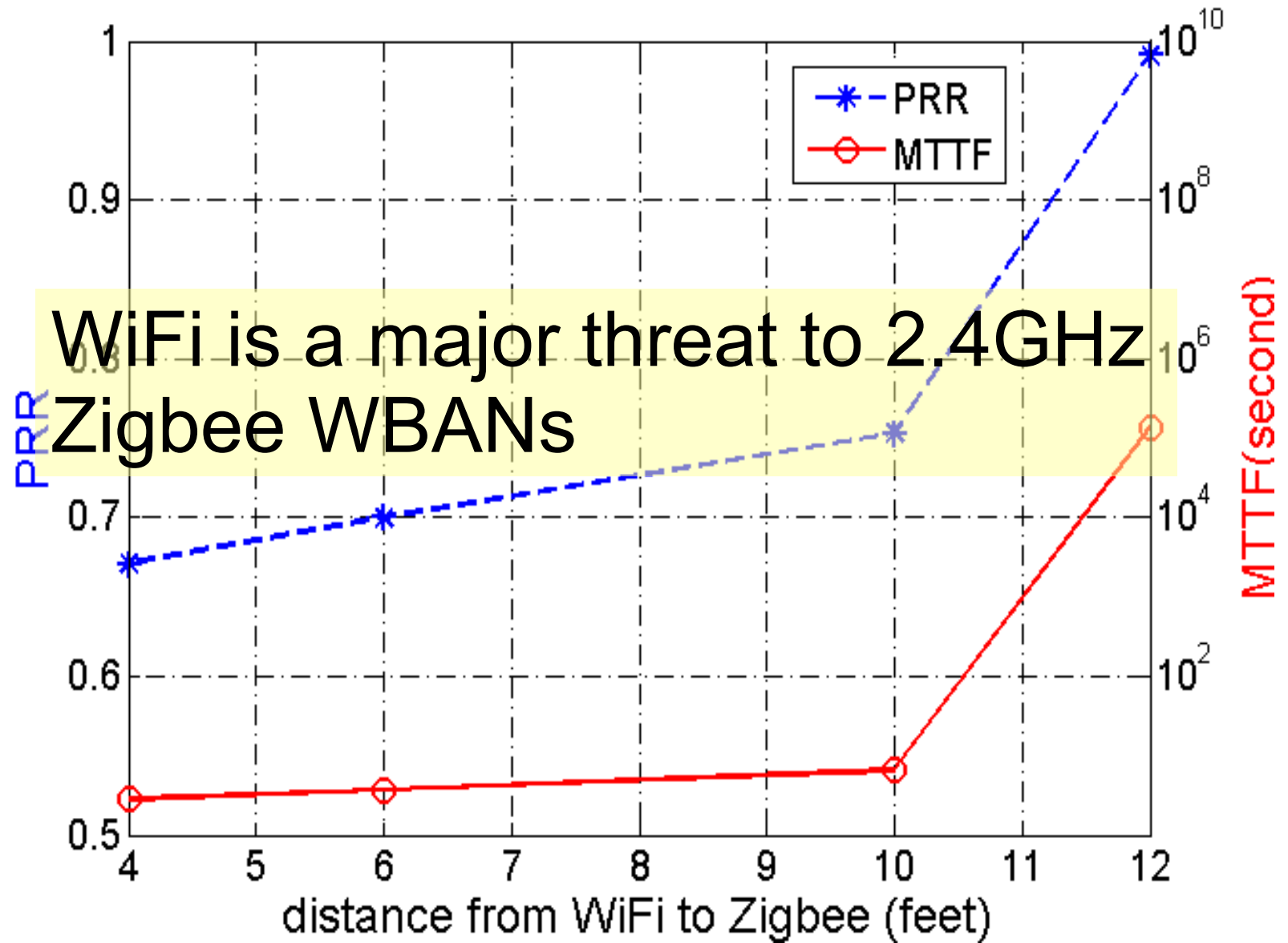
Mean Time To Failure (MTTF)

Packet Reception Rate (PRR)

$$MTTF = \frac{T_{polling}}{(1 - PRR)^{Nre}}$$

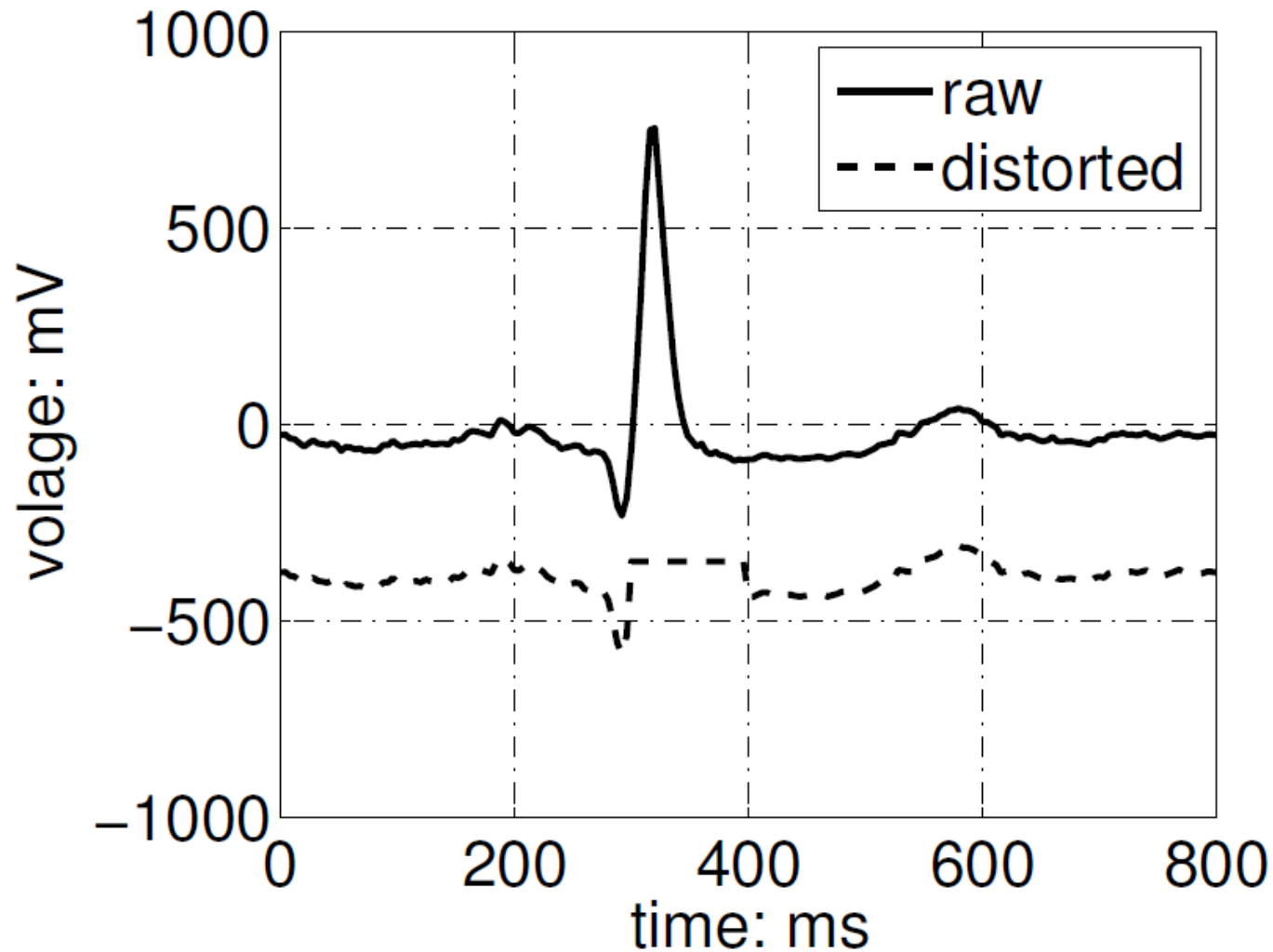


# Zigbee WBAN performance under WiFi interference





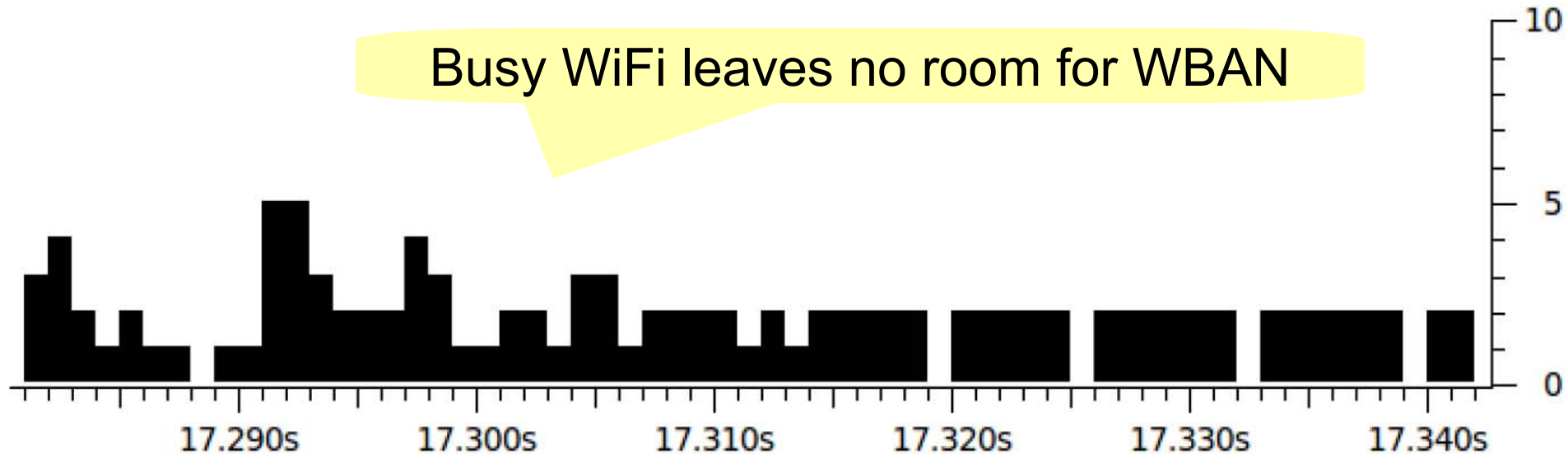
# Zigbee WBAN performance under WiFi interference



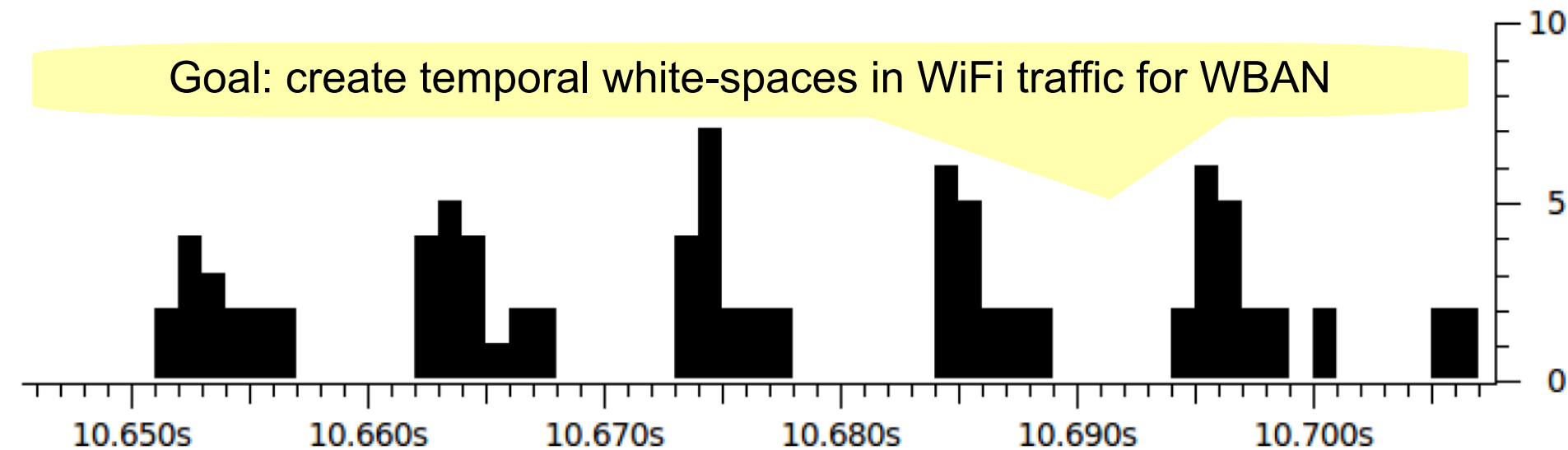


“Engineer” temporal white-spaces between WiFi transmissions to allow WBAN transmissions

Busy WiFi leaves no room for WBAN

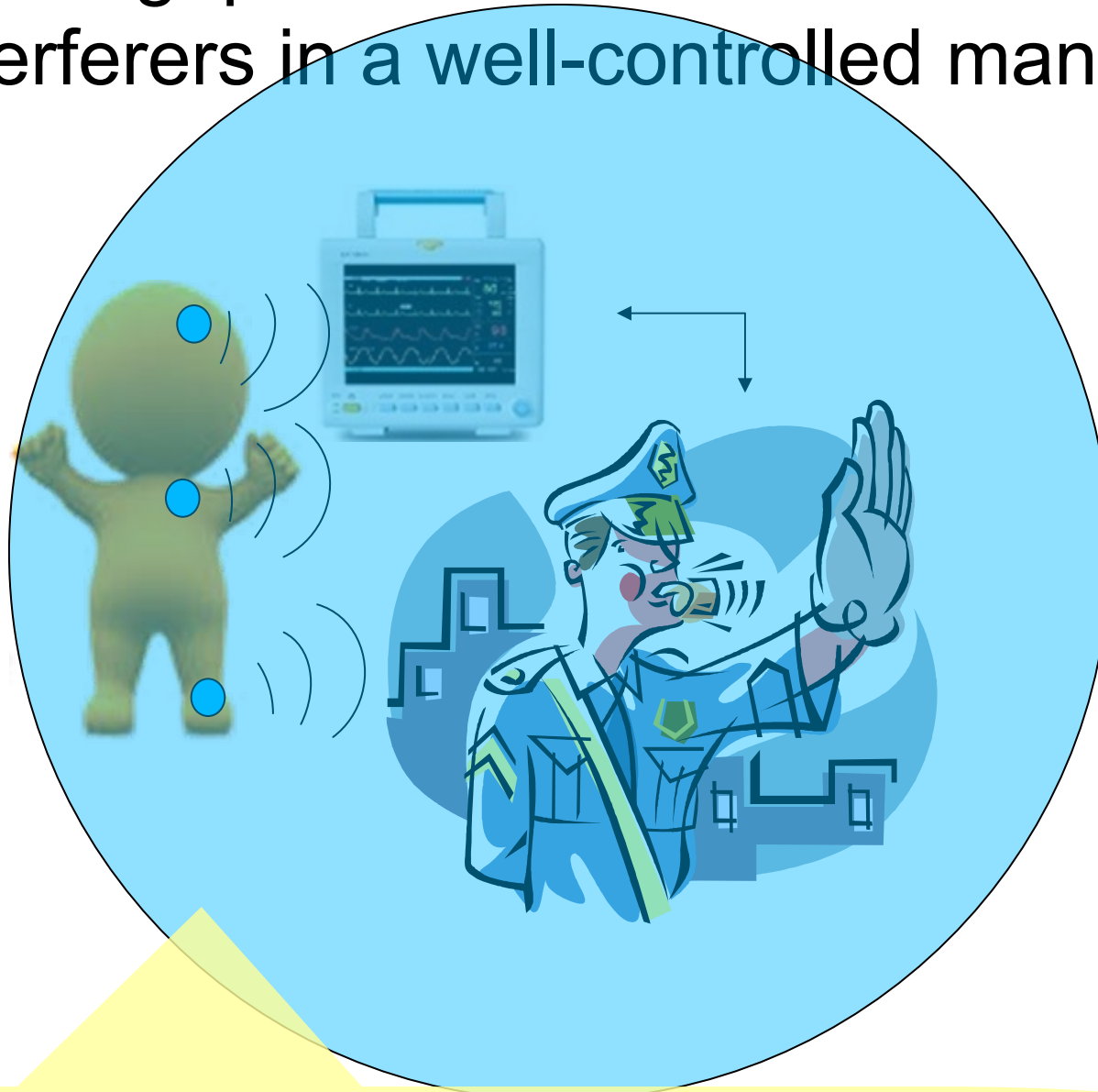


Goal: create temporal white-spaces in WiFi traffic for WBAN





Policing: prohibit the transmissions of WiFi interferers in a well-controlled manner



Shield WBAN transmissions in space and time



# Two mechanisms

Utilizing the carrier sensing mechanisms in WiFi

Fake-PHY-Hdr

DSSS-Nulling

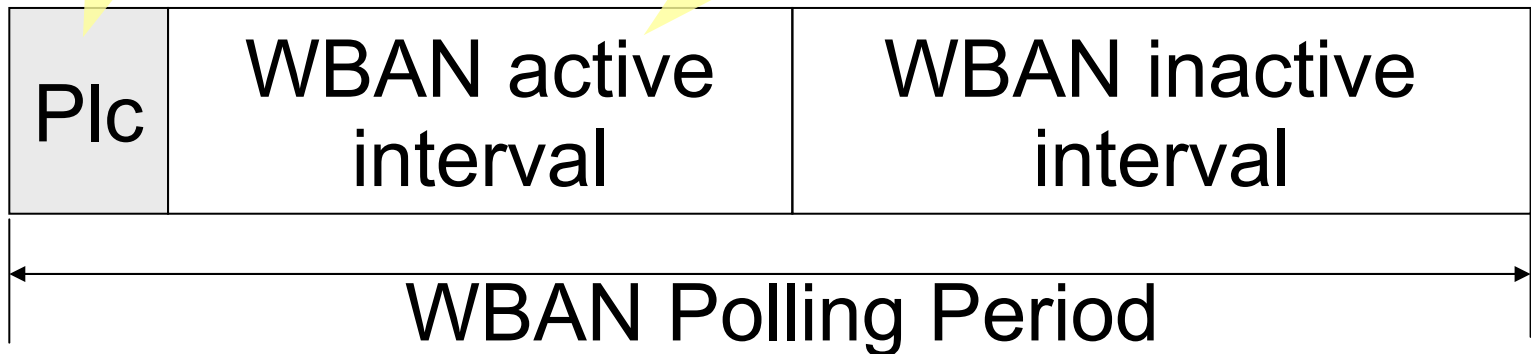




# Fake-PHY-Hdr: temporal scheme

Fake-PHY-Hdr *policing signal* (Plc):  
claims a (**fake**) WiFi packet with duration  
= WBAN active interval

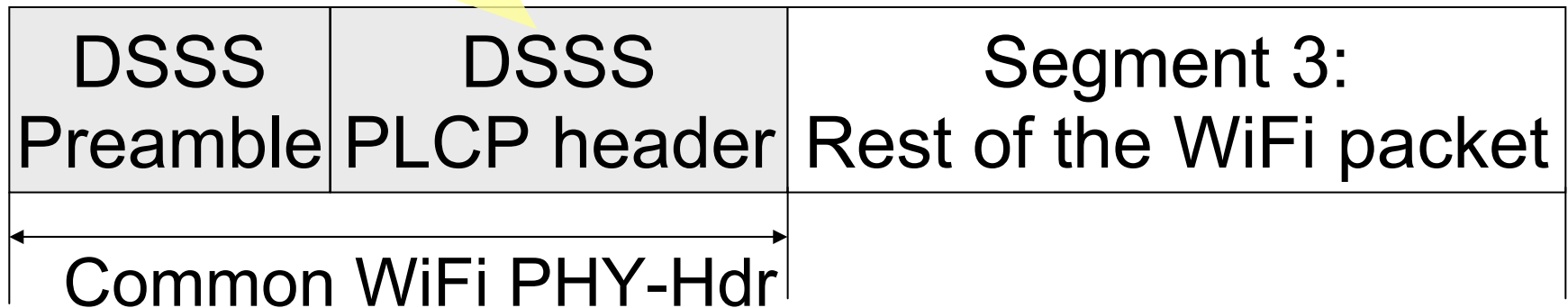
Includes:  
Downlink beacon  
Uplink data





802.11b/g/n recognize the following PHY-Hdr.

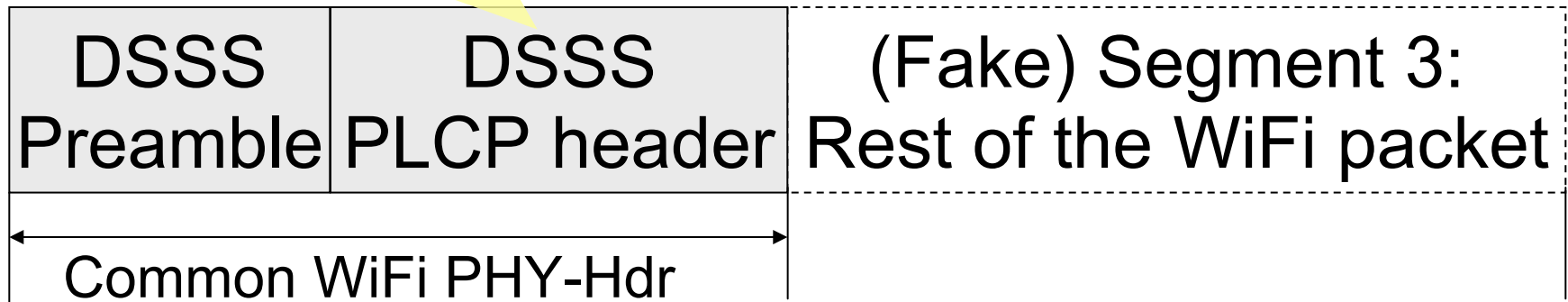
Claims the duration of Segment 3





WiFi devices will back off for the claimed (fake)  
Segment 3

Claims the duration of Segment 3





# DSSS-Nulling: repeated DSSS preamble

DSSS-Nulling policing signal

WBAN active interval

WBAN idle interval

WBAN polling period

Continuously repeated DSSS Preambles

DSSS  
Preamble

DSSS  
Preamble

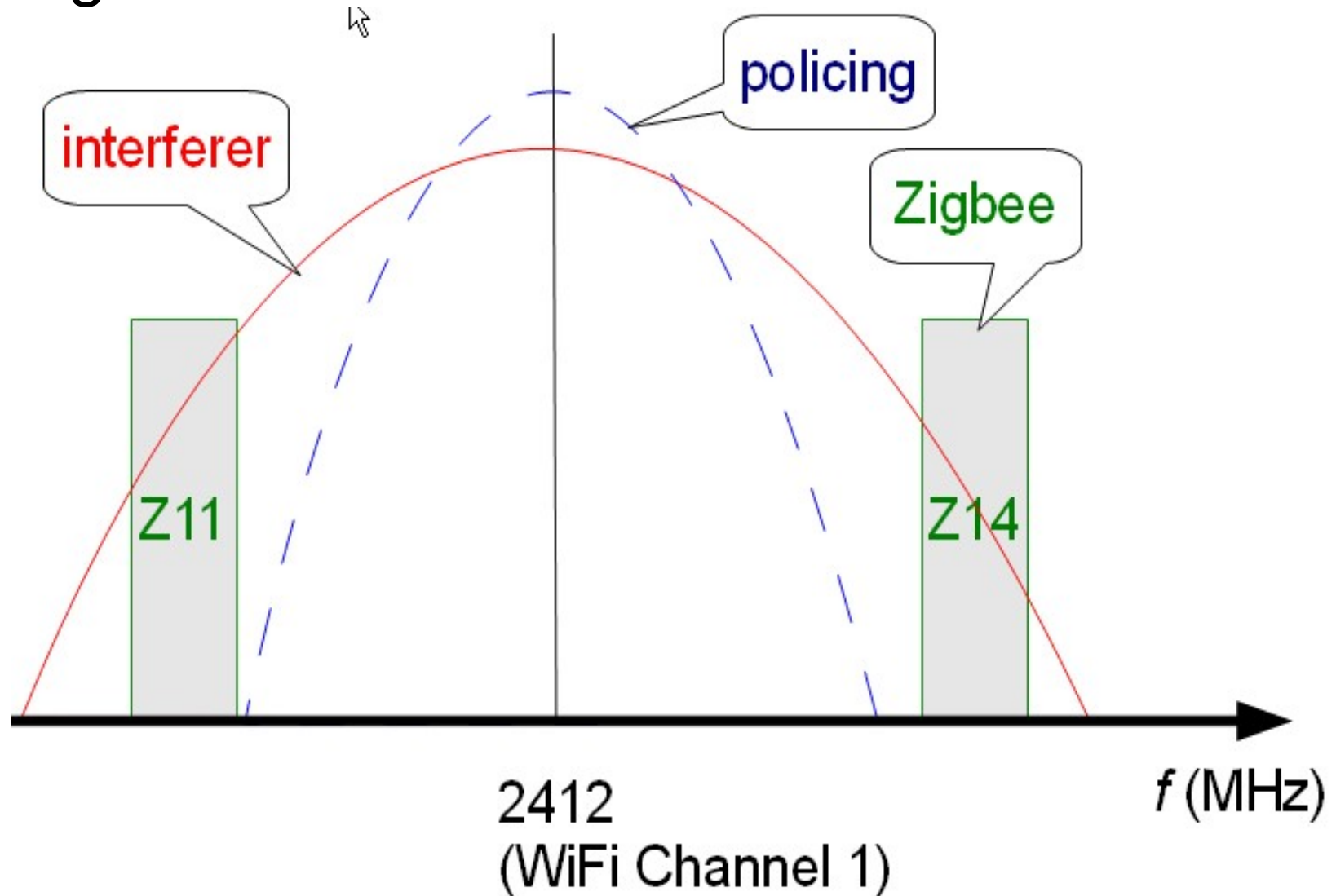
DSSS  
Preamble

■ ■ ■

DSSS  
Preamble



# Band-rejection filtered DSSS-Nulling policing signal



Spectrum illustration of interferer, policing and Zigbee signal



# Implementation details

Hardware platform: Microsoft SORA [tan11]

A Software Defined Radio platform

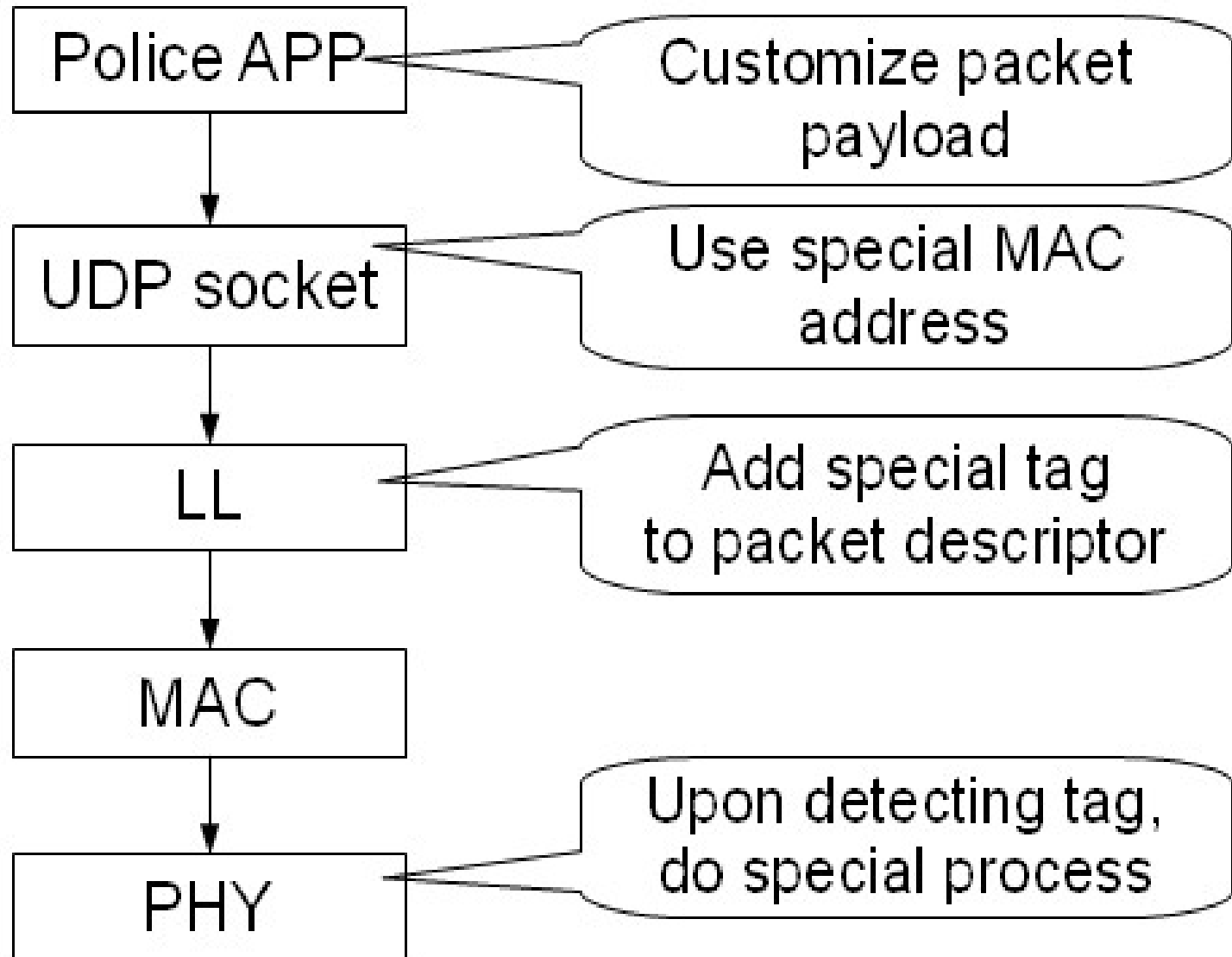
Multi-core based real-time signal processing

Support PCIe bus

open source WiFi driver



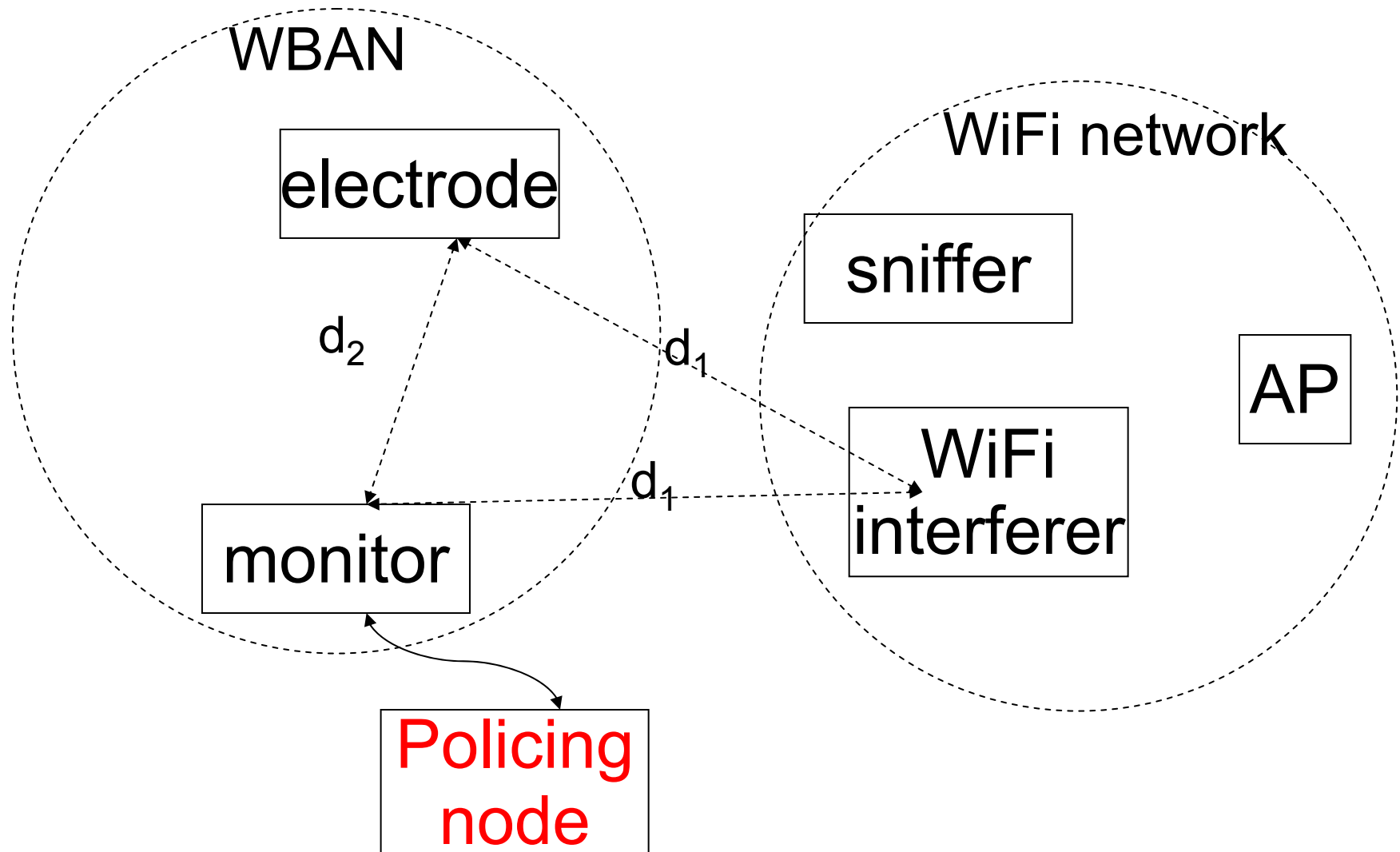
# Transmission of policing frames







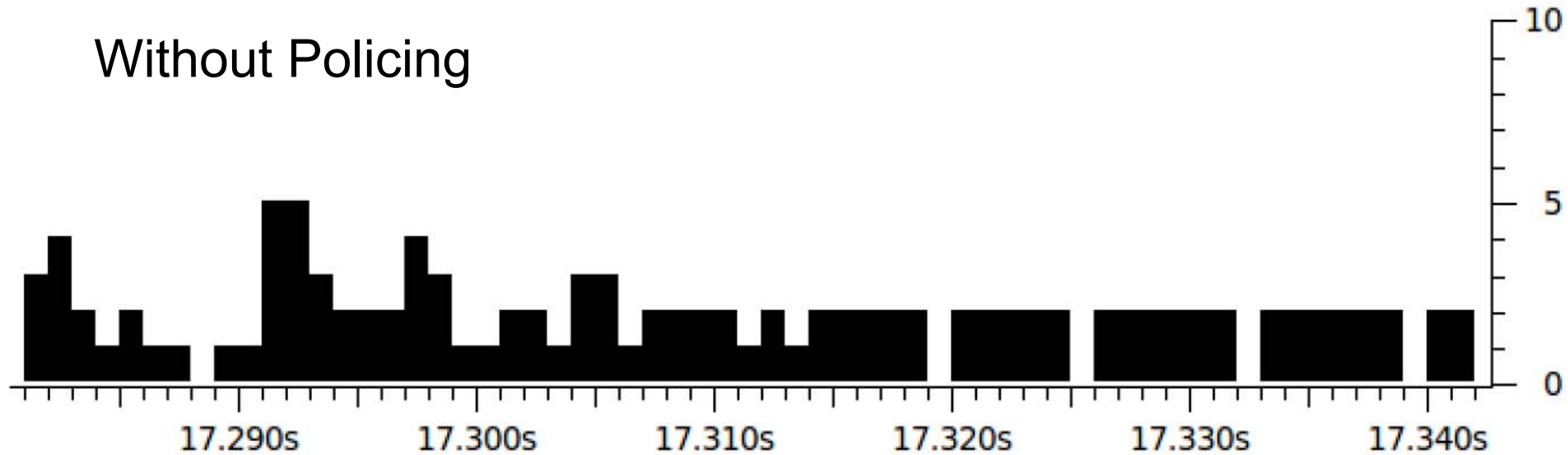
The policing node implements the two policing mechanisms





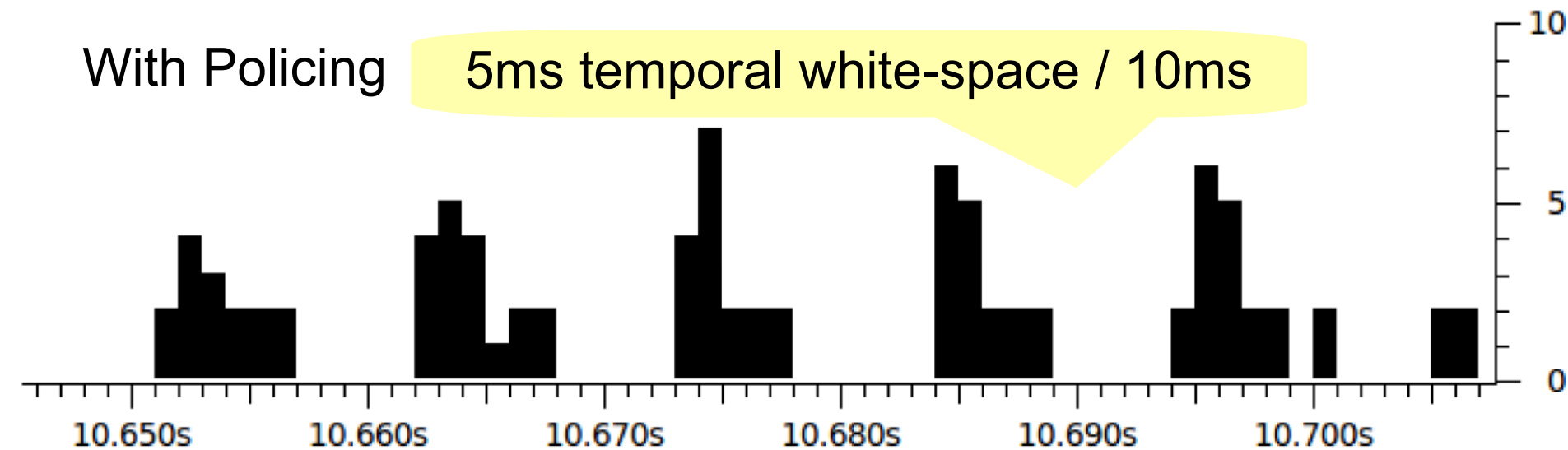
# Temporal whitespaces due to WiCop

Without Policing



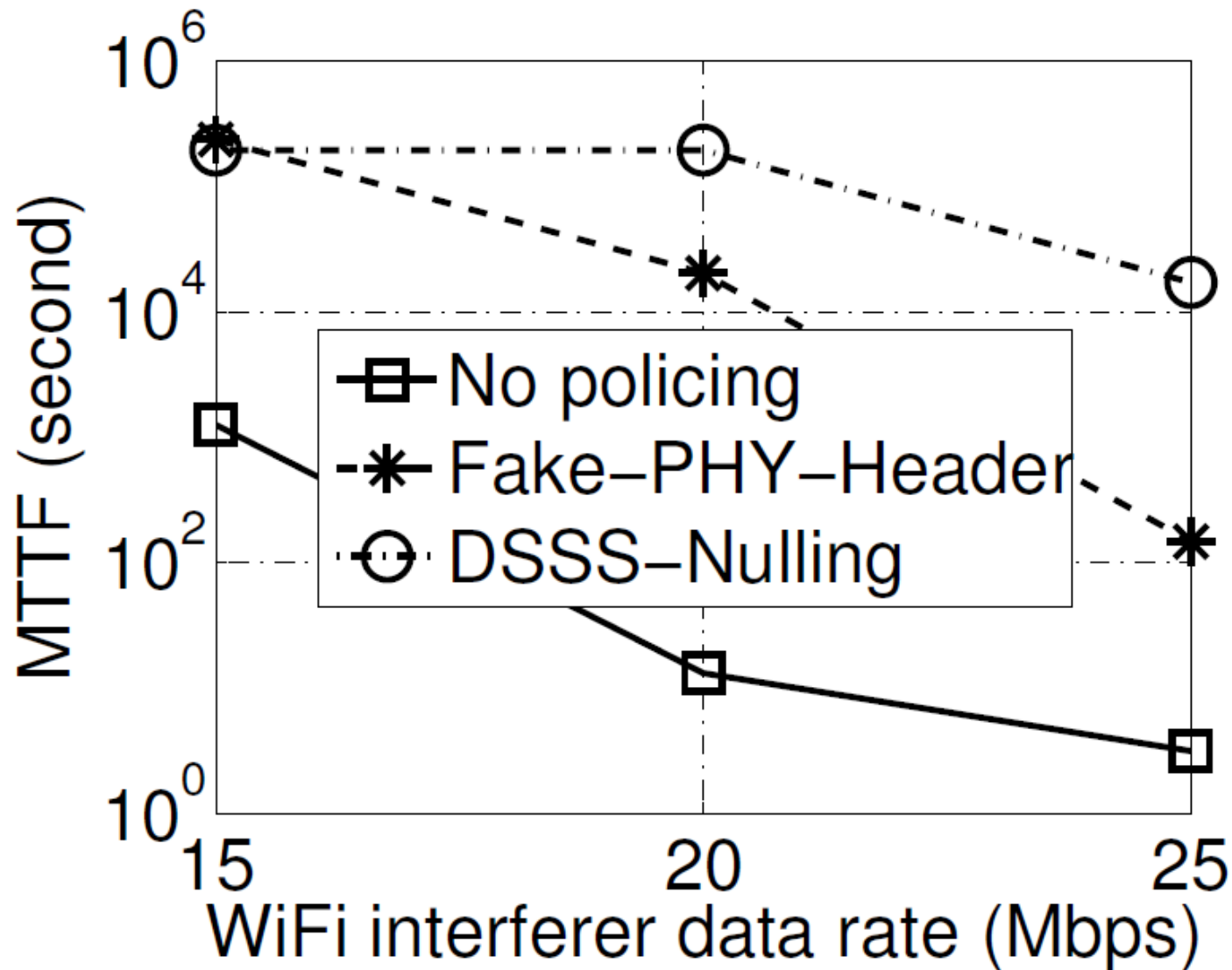
With Policing

5ms temporal white-space / 10ms





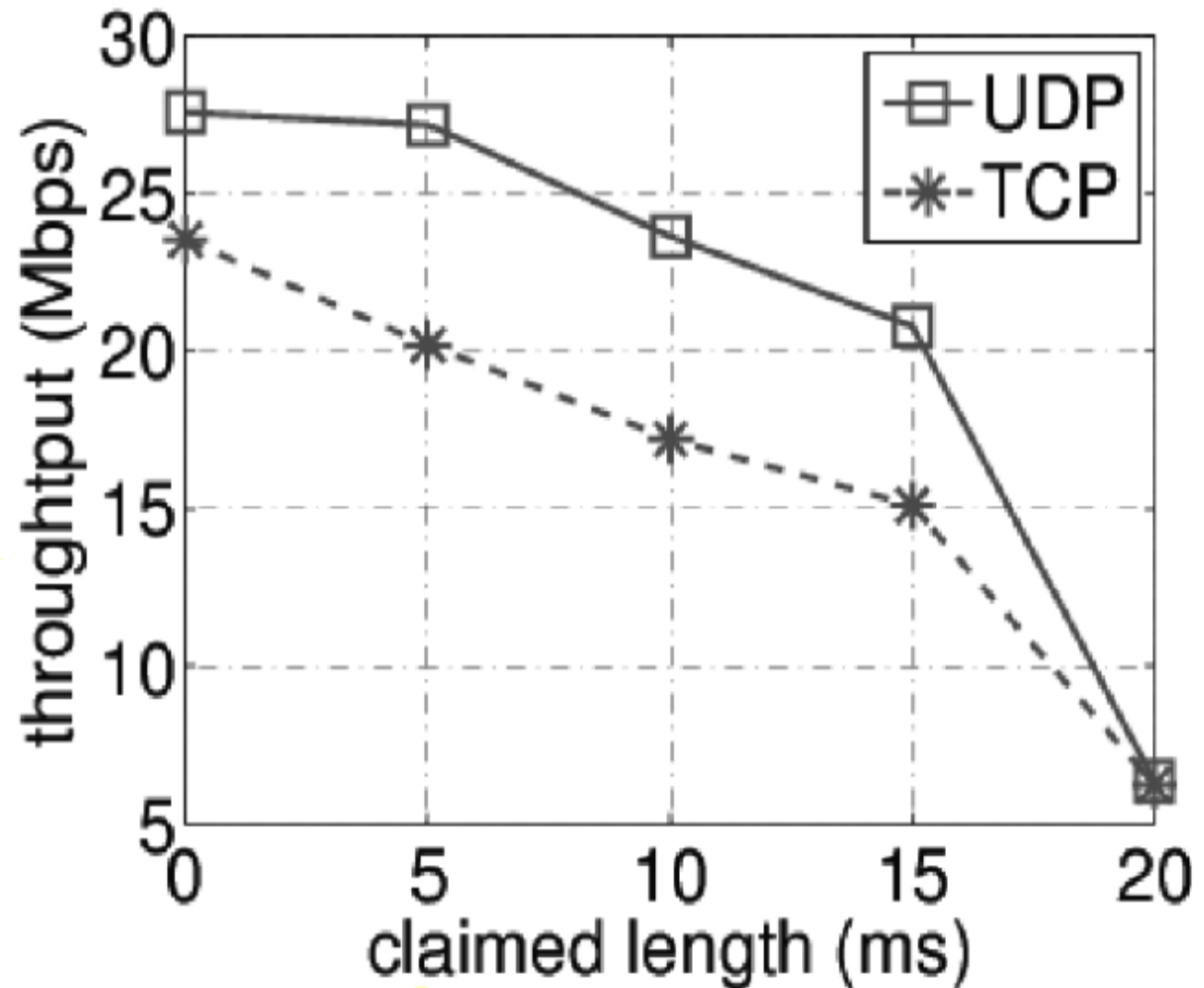
# Mean time to failure





# Moderate Impact on WiFi traffic

WiFi throughput degradation



Use Fake PHY Hdr to claim a white space  
WBAN polling period is 25ms



# Methods protecting Zigbee from WiFi

Exploiting (instead of engineering) temporal white-spaces of WiFi traffic [liang10][huang10]

Exploiting (instead of engineering) spectral white-spaces of WiFi traffic [won05][musaloiu-e08]

Use fake RTS to protect Zigbee [hou09]: pros and cons



# WiFi PHY/MAC security

Continuously transmitting WiFi preamble  
[wullems04].

Fake de-auth packet and fake virtual carrier sense  
[bellardo94].

DIFS waiting jamming and acknowledge corruption  
[thuente06]

Partial band jamming [park03] [mishra06]  
[karhima04]



# Conclusion

WiCop significantly improves WBAN performance

Controlled impact on WiFi

DSSS-Nulling is more effective than Fake-PHY-Hdr  
in improving MTTF, mainly due to repeated  
transmissions of DSSS preamble

Fake-PHY-Hdr incurs much less overhead than  
DSSS-Nulling





# Demo Video

# Contents



Demand



Modeling and Verification



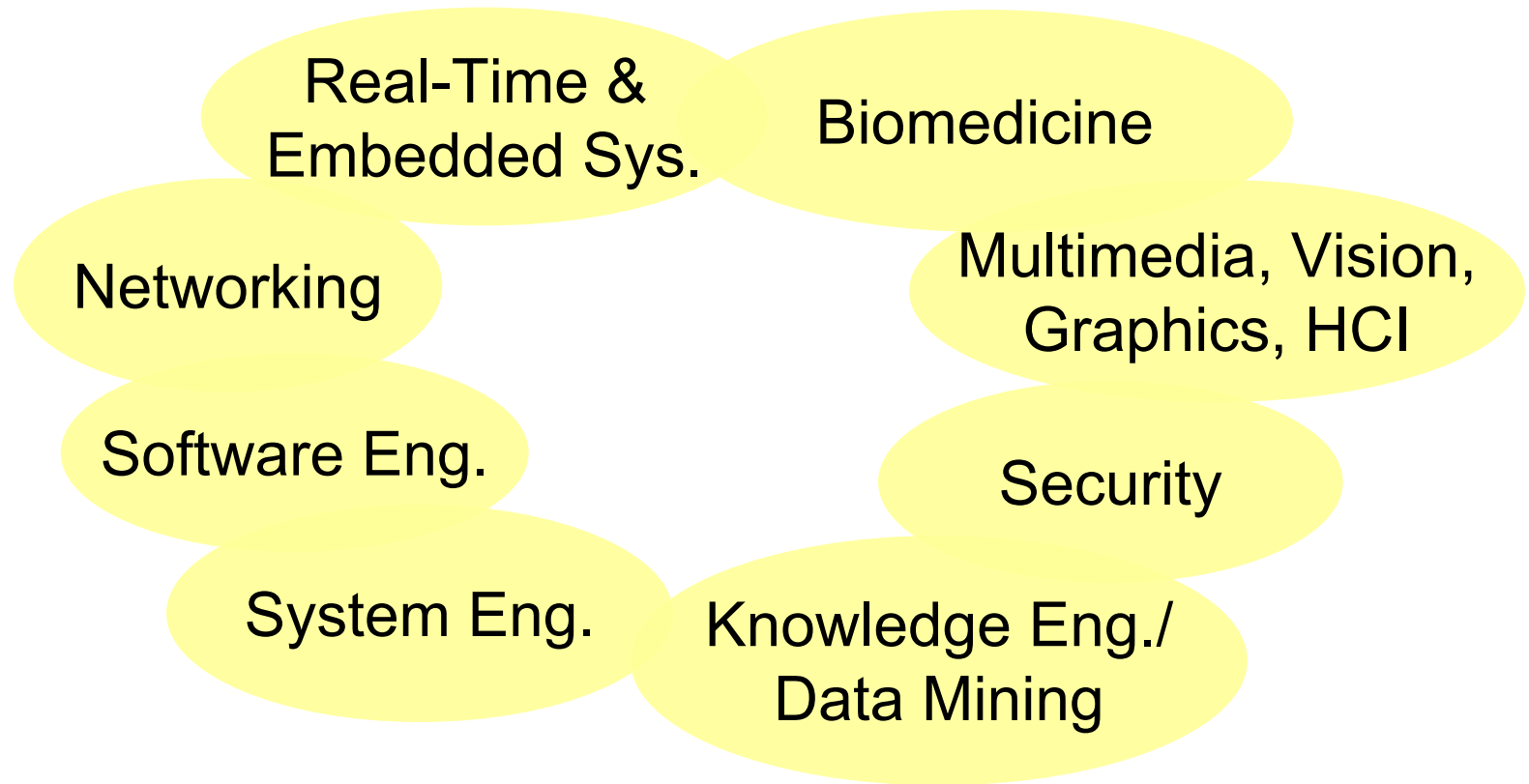
Dependable Medical Wireless Networking



Vision



# Medical MDPnP to Medical Cyber-Physical Systems: A Interdisciplinary Community Effort





# Medical MDPnP to Medical Cyber-Physical Systems: An Interdisciplinary Community Effort

