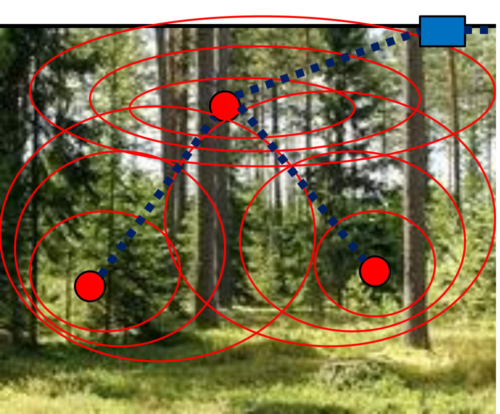
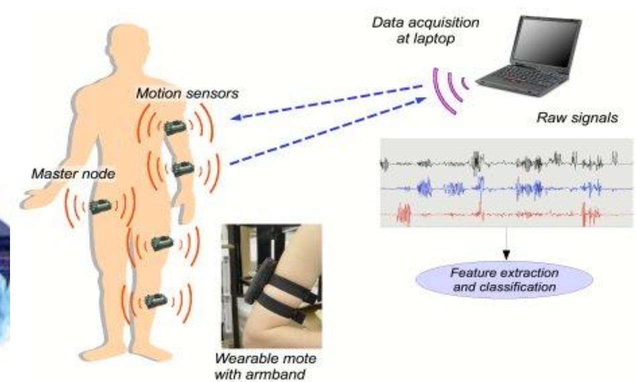
Wireless Sensor Networks: fundamentals, applications, challenges

Vladimir Shakhov

Wireless Sensor Network

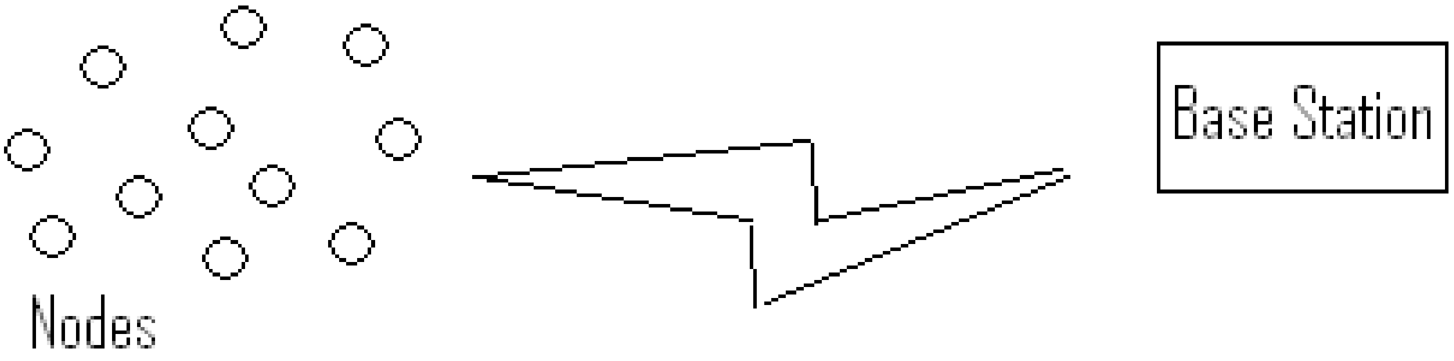
*"A **wireless sensor network** (WSN) is a wireless network consisting of spatially distributed autonomous devices using sensors to cooperatively monitor physical or environmental conditions, such as temperature, sound, vibration, pressure, motion or pollutants, at different locations."*





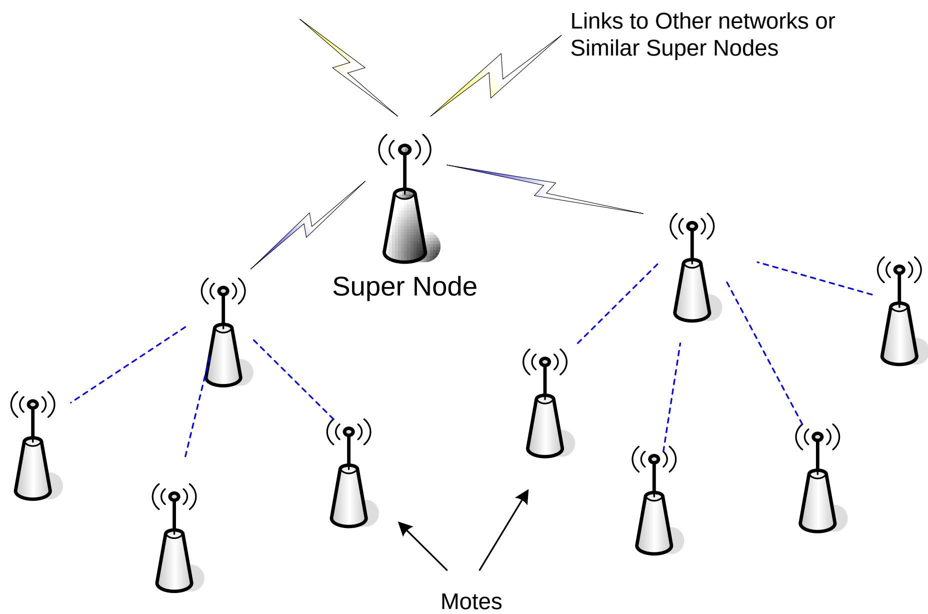
WSN

- A Wireless Sensor Network (WSN) consists of base stations and a number of wireless sensors (nodes).

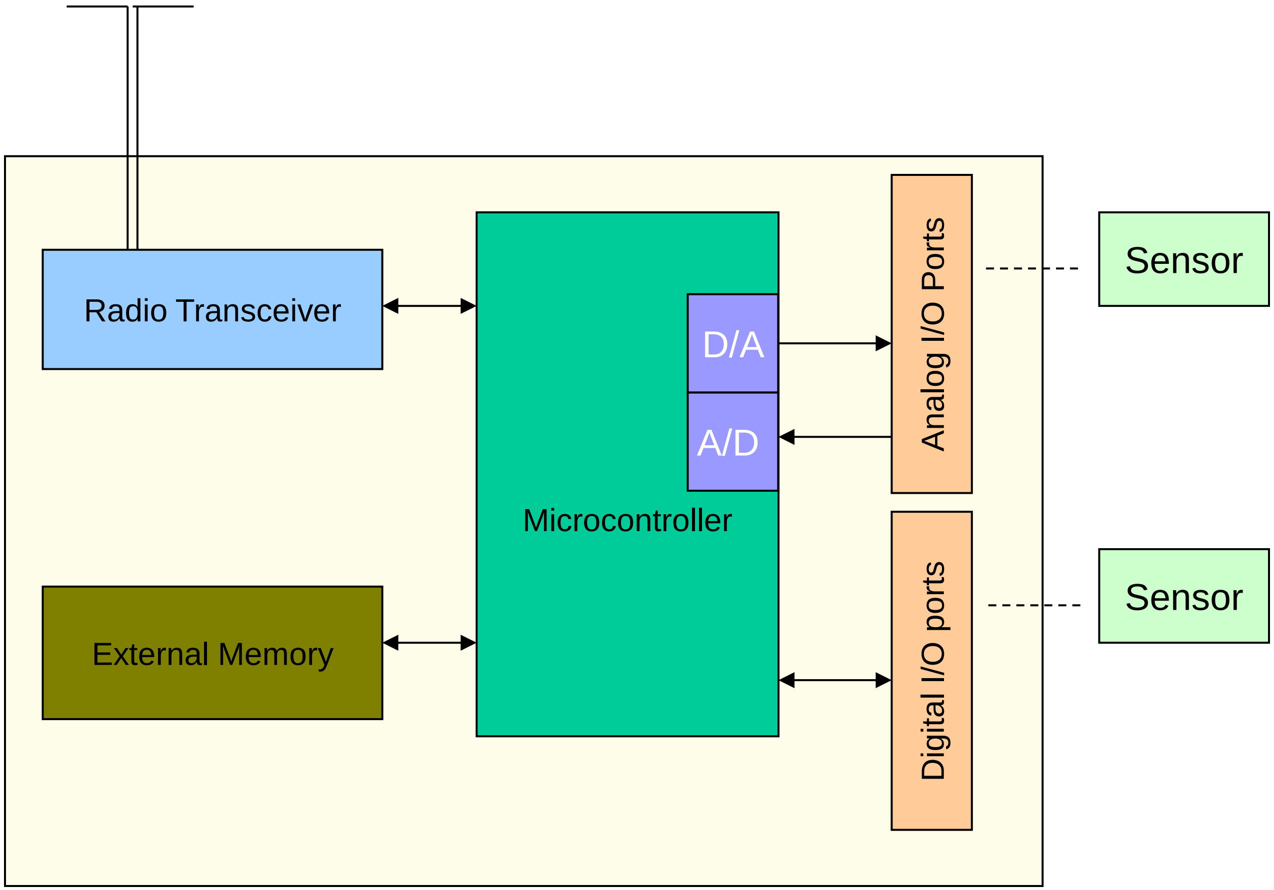


Wireless Sensor Networks

- Formed by hundreds or thousands of motes that communicate with each other and pass data along from one to another



Sensor (Mote)

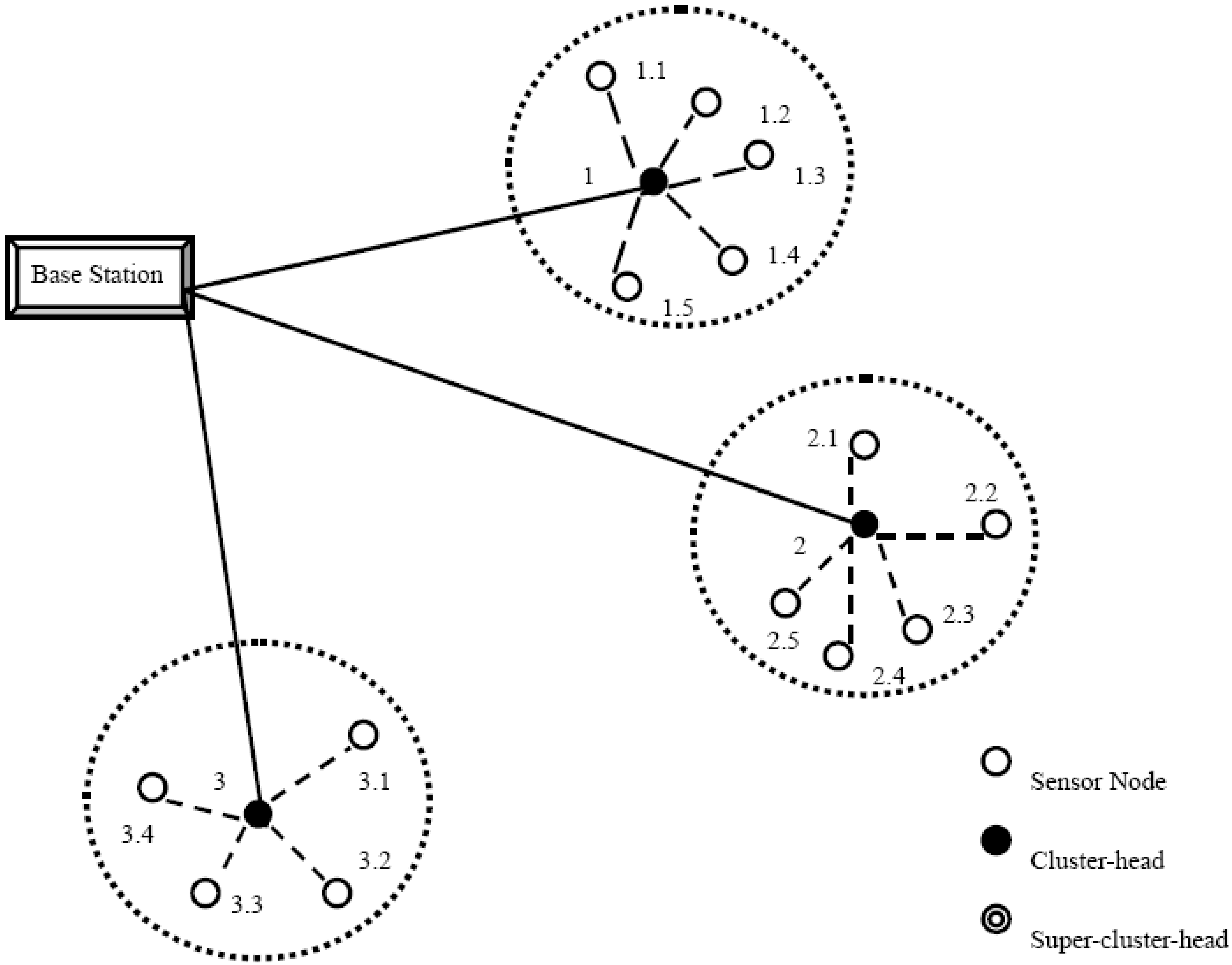


Radio Transceiver
D/A
A/D
Microcontroller
Analog I/O Ports
Sensor
External Memory
Digital I/O ports
Sensor

Problems

- A cost of sensor components is a **critical** consideration in the design of practical sensor networks.
- A cost of sensor network increases with sensor battery power.
- By this reason a battery power is usually a scare component in wireless devices. On the other hand, sensor lifetime depends on battery lifetime.

Clustering Hierarchy



- Duty cycling:
  - An important mechanism for reducing energy consumption in wireless sensor networks
  - Switch nodes between awake and sleeping states
  - Measure the ratio of the time a node is awake to the total time
  - Synchronous and asynchronous

MAC

- Asynchronous duty-cycling:
  - Nodes are battery powered and wireless
  - Each node decides its own wakeup schedule, wakes up asynchronously

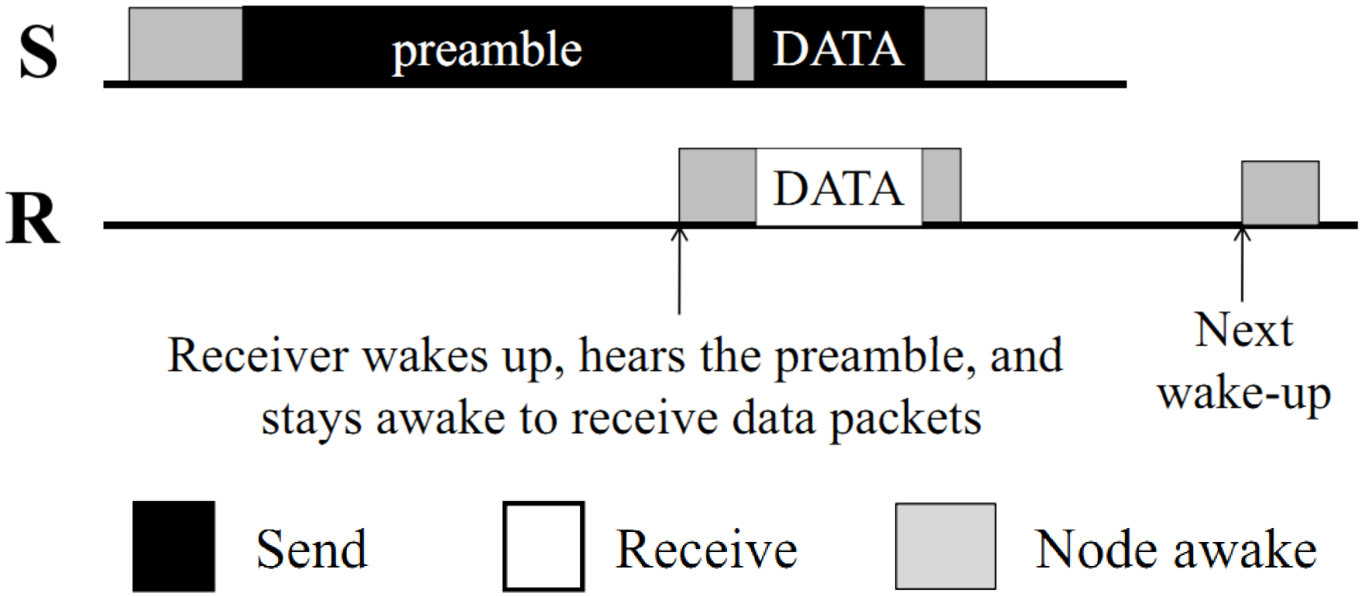
- Asynchronous duty-cycling is widely used because:
  - Reduces energy consumption
  - Requires no clock synchronization

MAC

- Asynchronous duty cycling MAC protocols can be categorized into:
  - Sender-initiated
    - B-MAC, X-MAC, WiseMAC
  - Receiver-initiated
    - RI-MAC

MAC

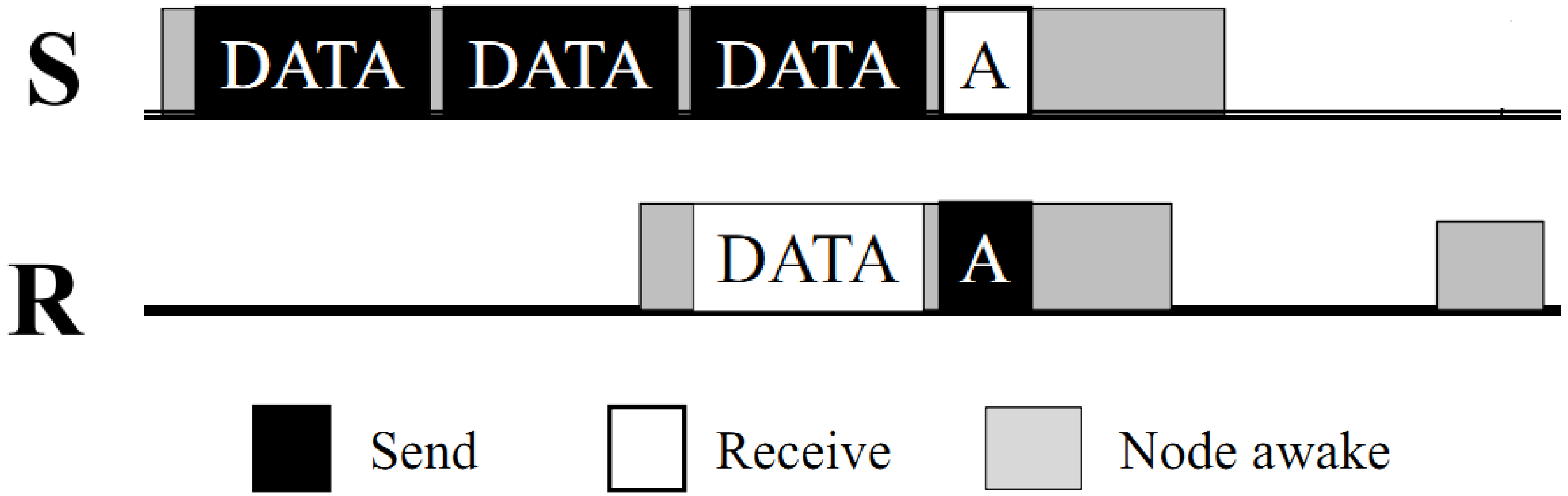
- B-MAC[1]:
  - Sender sends a preamble longer than the receiver wake-up interval to notify receiver the pending transmission



[1] Joseph Polastre, Jason Hill, and David Culler. Versatile low power media access for wireless sensor networks. In SenSys ’04, pages 95–107, 2004.

MAC

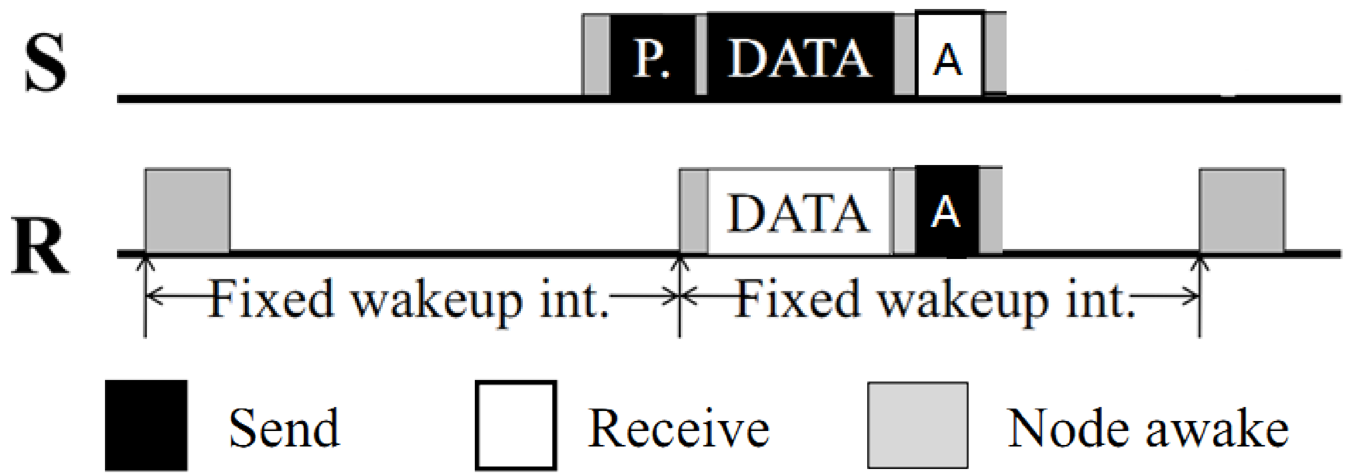
- X-MAC[2] :
  - Sender preamble is replaced by shorter data packets
  - Receiver sends an ACK after receiving a data packet



[2] Michael Buettner, Gary V. Yee, Eric Anderson, and Richard Han. X-MAC: A short preamble MAC protocol for duty-cycled wireless sensor networks. In SenSys 2006, pages 307–320, November 2006

MAC

- WiseMAC[3]:
  - Shorten the long preamble
- Take advantage of fixed node wake-up interval to enable sender to predict the receiver wake-up times



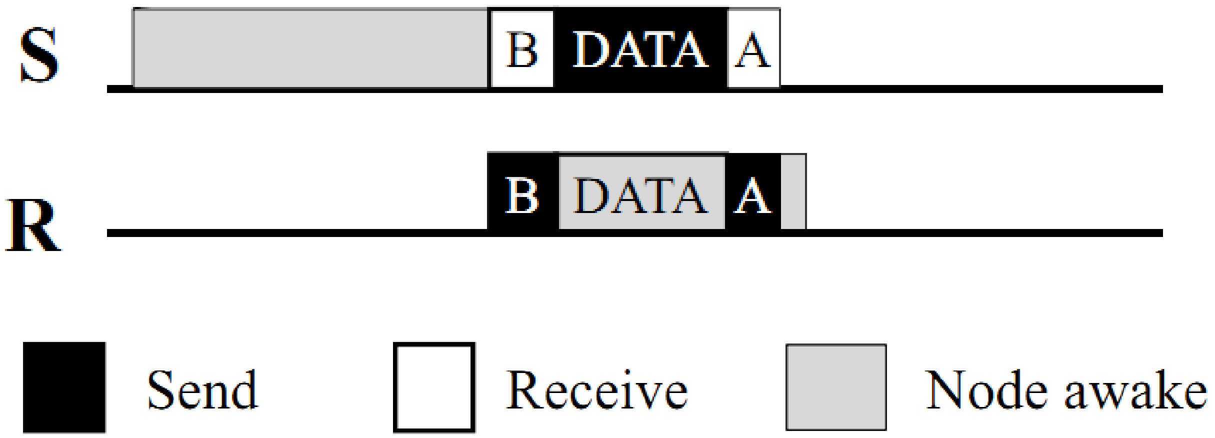
[3]Amre El-Hoiydi and Jean-Dominique Decotignie. WiseMAC: An ultra low power MAC protocol for multi-hop wireless sensor networks. In ALGOSENSORS 2004, pages 18–31, July 2004.

MAC

- B-MAC, X-MAC, and WiseMAC:
  - B-MAC and X-MAC have large sender duty cycle
  - The fixed wakeup interval of WiseMAC can often causes collisions
  - No efficient retransmission mechanism

MAC

- RI-MAC[4]:
  - Receiver-initiated MAC protocol
  - Sender still has large duty cycle



[4]Yanjun Sun, Omer Gurewitz, and David B. Johnson. RI-MAC: A receiver initiated asynchronous duty cycle MAC protocol for dynamic traffic loads in wireless sensor networks. In SenSys 2008.

Applications

IoT

- Internet of Things (IoT) provides tremendous opportunity for societies around the world.

- Cisco CEO John Chambers predicted the Internet of Things would be a $19 trillion market over the next several years.

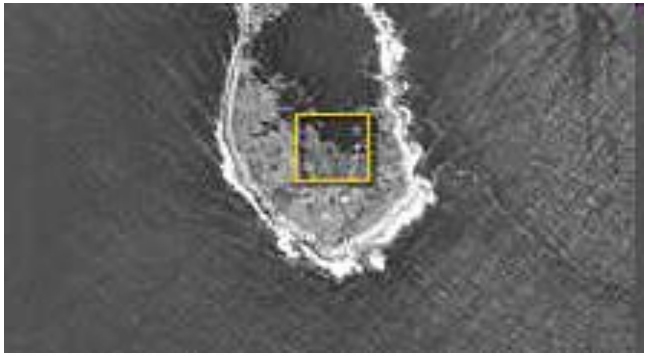
- 50 billion connected devices by 2020

WSN Applications

- Environmental/Habitat monitoring
- Acoustic detection
- Seismic Detection
- Military surveillance
- Inventory tracking
- Medical monitoring
- Smart spaces
- Process Monitoring

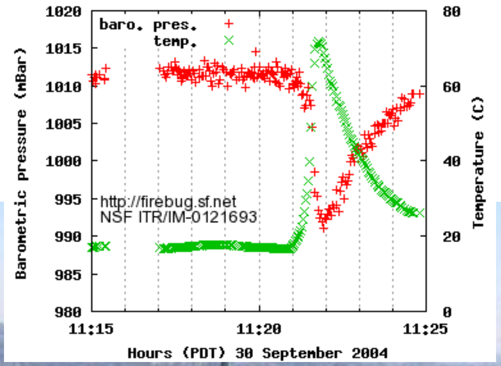
- **etc**

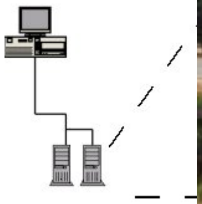
Habitat Monitoring on Great Duck Island



- http://www.greatduckisland.net/
- Intel Research Laboratory at Berkeley initiated a collaboration with the College of the Atlantic in Bar Harbor and the University of California at Berkeley to deploy wireless sensor networks on Great Duck Island, Maine (in 2002)
- Monitor the microclimates in and around nesting burrows used by the Leach's Storm Petrel
- Goal : habitat monitoring kit for researchers worldwide

FireBug





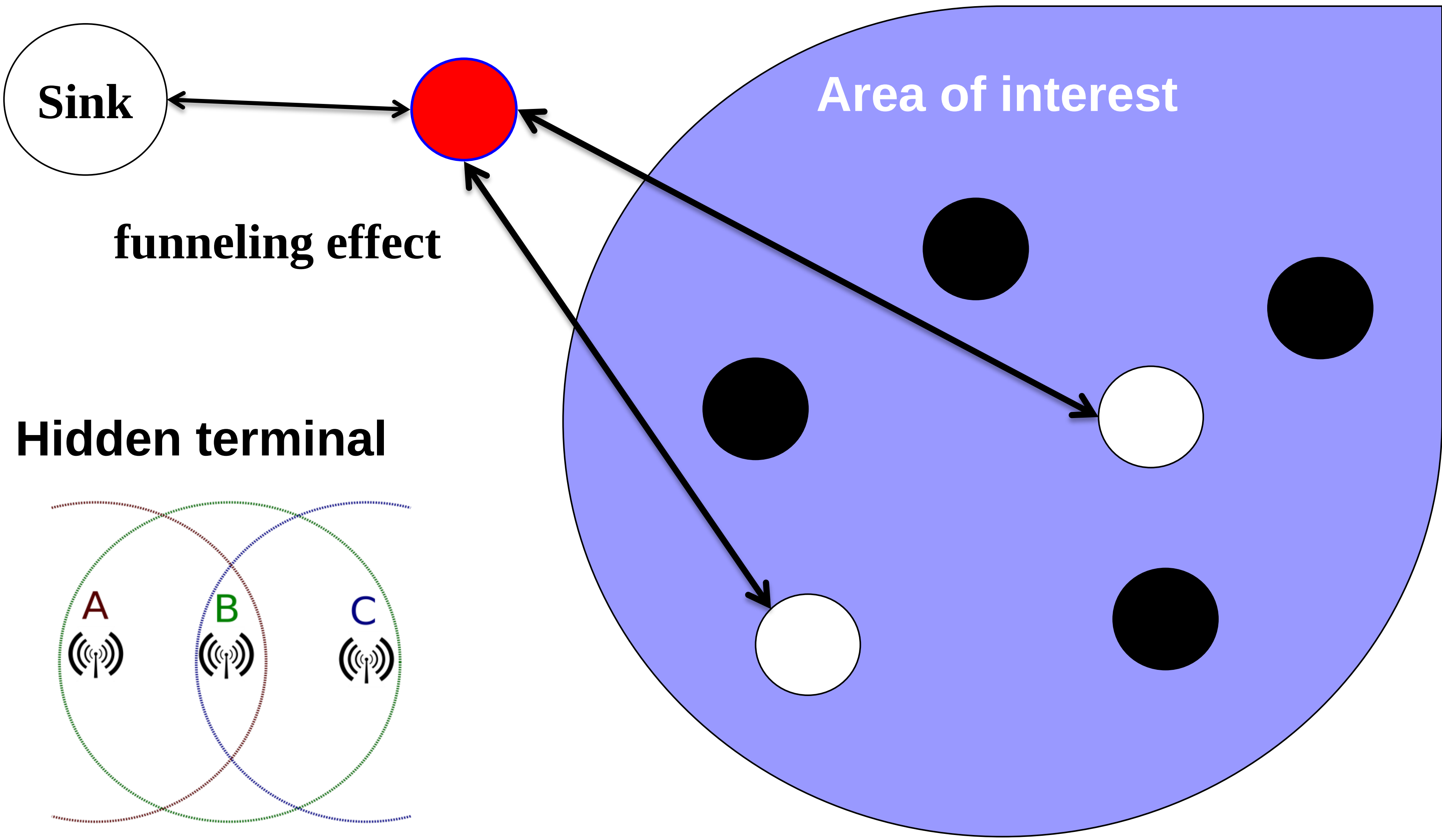
- Wildfire Instrumentation System Using Networked Sensors
- Allows predictive analysis of evolving fire behavior
- Firebugs: GPS-enabled, wireless thermal sensor motes based on TinyOS that self-organize into networks for collecting real time data in wild fire environments
- Software architecture: Several interacting layers (Sensors, Processing of sensor data, Command center)
- A project by University of California, Berkeley CA.

Preventive Maintenance on an Oil Tanker in the North Sea: The BP Experiment

- Collaboration of Intel & BP
- Use of sensor networks to support preventive maintenance on board an oil tanker in the North Sea.
- A sensor network deployment onboard the ship
- System gathered data reliably and recovered from errors when they occurred.
- The project was recognized by InfoWorld as one of the top 100 IT projects in 2004

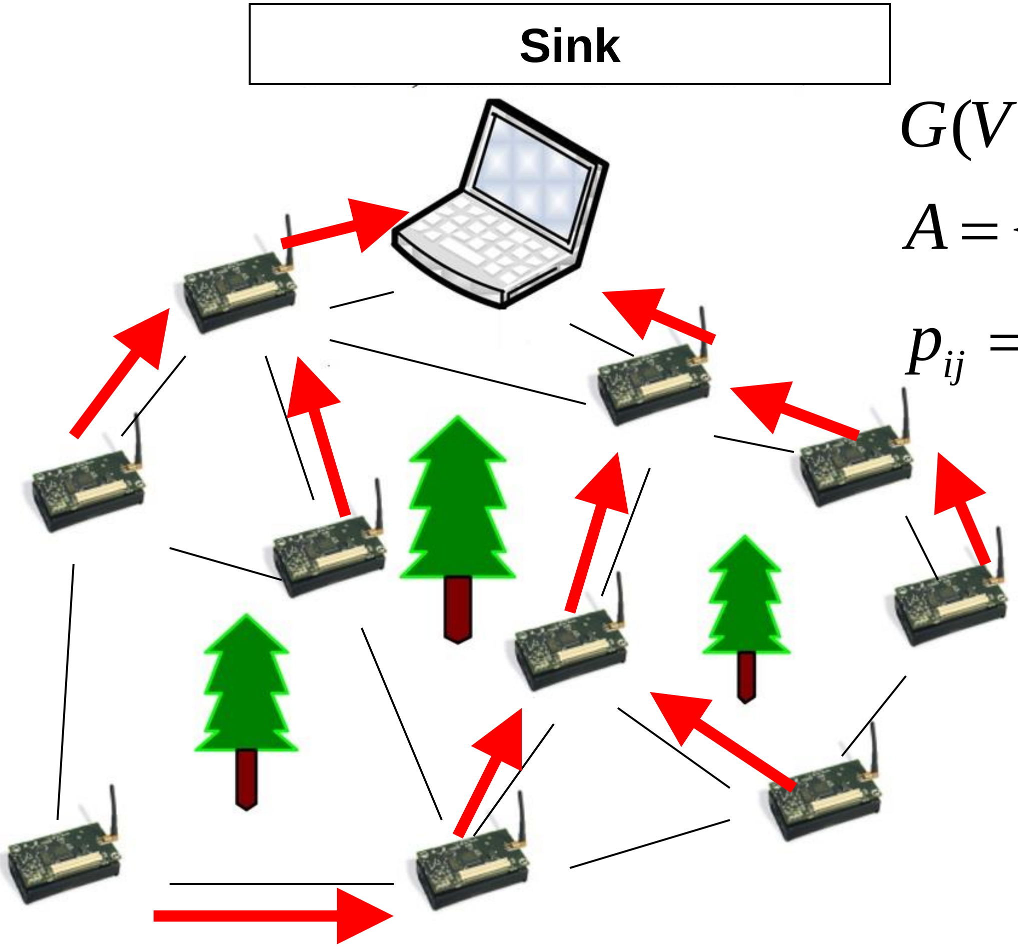
Challenges

Problem


Sink
Area of interest
funneling effect
Hidden terminal
A
B
C

Task

Energy efficient Tree for Traffic Aggregation



$$G(V,E), |V| = n$$

$$A = \{(i,j) : i,j \in V, (i,j) \vee (j,i) \in E\}$$

$$p_{ij} = p_{ji} = \alpha\, d_{ij}^{\beta}$$

$$\mathbf{P} = (P_1, \ldots, P_n)$$

x_{ij} flow ~ *(i,j)*

Task

$$\min \sum_{i \in V} P_i$$

$$\mathbf{x} \in \Psi(G, \mathbf{b}),$$

$$x_{ij} \le (|D|-1) y_{ij}, (i, j) \in A,$$

$$p_{i\pi_i(j)} y_{ij} \le P_i, (i, j) \in A,$$

$$\mathbf{y} \in \{0,1\}^{|A|}$$

$$\Psi(G, \mathbf{b}) = \left\{ \mathrm{x} \in \mathrm{R}_+^{|A|} : \sum_{\substack{j \in V \\ (i,j) \in A}} x_{ij} - \sum_{\substack{j \in V \\ (j,i) \in A}} x_{ij} = b_i, i \in V \right\}$$

$$\forall i \in V, \pi_i : \{1, \ldots, n-1\} \to V \setminus \{i\}$$

QoS

M/G/n/n, M/M/n

$\min x$ $B(\rho - x, n) \le \alpha$	$\min \sum_{i=1}^{k} n_i$ $\delta_i B(\rho_i, n_i) = \delta_j B(\rho_j, n_j)$
$\min_{x,\mathbf{n}} B(x, \mathbf{n})$ $\sum_{i=1}^{k} s_i n_i \le S$ $x \ge L$	$\min_{\mathbf{n}} \alpha B(x, \mathbf{n}) + \beta C(x, \mathbf{n})$ $s_x x - \sum_i s_i n_i \ge R$

QoS

$$B(\rho, n) = \frac{\rho^n}{n!} \Big/ \sum_{i=0}^{n} \frac{\rho^i}{i!}$$

Theorem $\forall\, A > 0,$ if $\rho \geq n + A$

then $1 - \frac{n}{\rho} < B(\rho, n) < 1 - \frac{n}{\rho} + \frac{1}{A}.$

Proposition

$$B(\rho, n) \approx 1 - \frac{n}{\rho}, \;\; n \approx \rho(1 - B(\rho, n)), \quad \rho \approx \frac{n}{1 - B(\rho, n)}.$$

QoS

Definition

$$j \in \mathbf{N},\ \hat{B}(\rho, j, n_0) = \begin{cases} b^*(n_0), & j = n_0, \\ \dfrac{\rho\hat{B}(\rho, j-1)}{j + \rho\hat{B}(\rho, j-1)}, & j > n_0. \end{cases}$$

Theorem $\forall\ \varepsilon > 0, \quad |B(\rho, n_0, n_0) - b^*| \le \varepsilon$

Hence

$$\forall n > n_0\ , |B(\rho, n) - \hat{B}(\rho, n)| \le c^{\alpha}\varepsilon,\ \ 0 < c < 1, \alpha > 1.$$

Fast Method

$$B(0,\rho)=1,\quad m=0;$$

$$B(m,\rho)=\frac{\rho B(m-1,\rho)}{m+\rho B(m-1,\rho)},m\geq 1.$$

V. Iversen. TELETRAFFIC ENGINEERING and NETWORK PLANNING. Technical University of Denmark, 2012

ITU-D SG2/Question_16

Fast Method

m=k, B=b*

m=k+1, B=f(B)

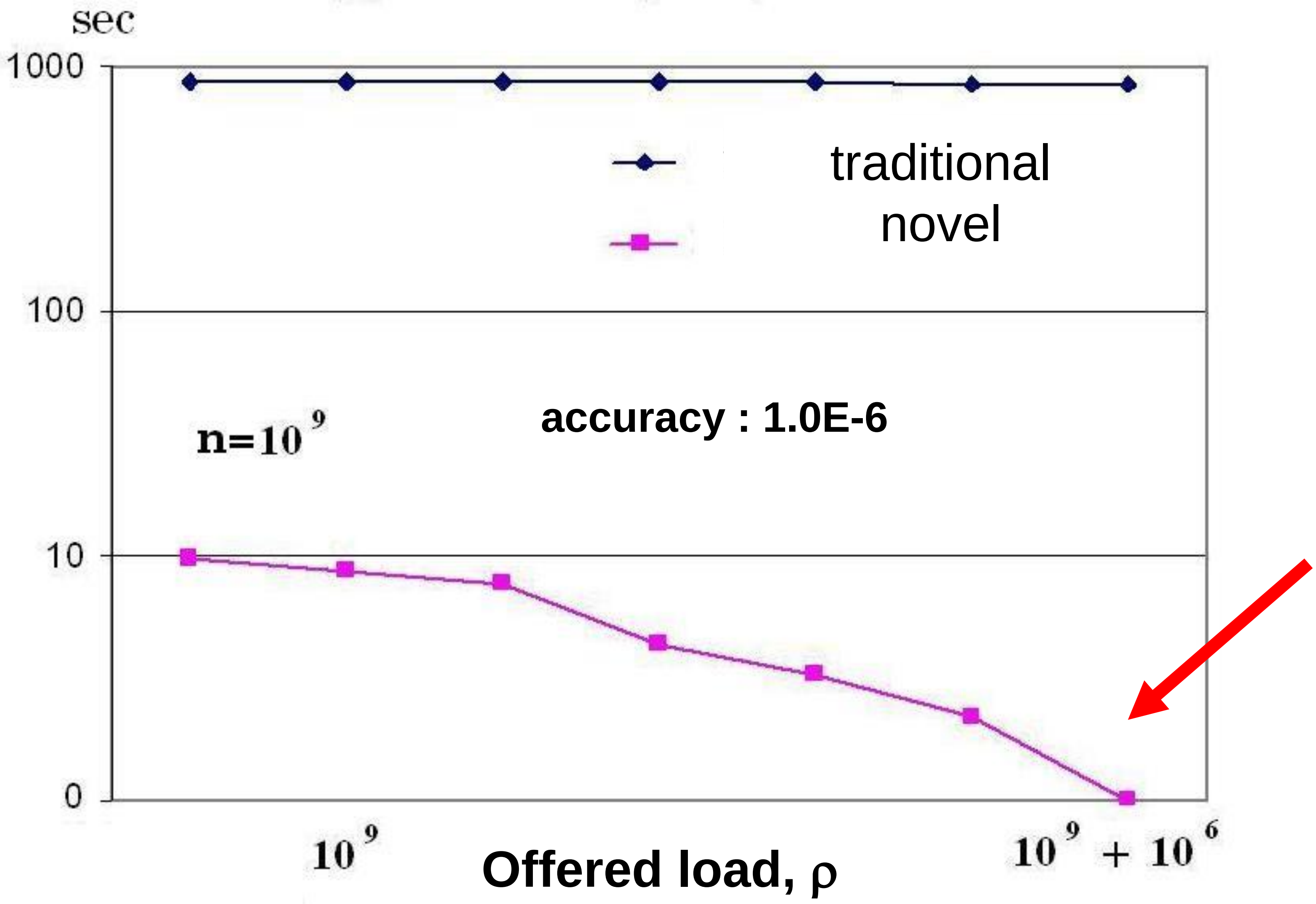
...

m=n, B=f(B)

C++ code

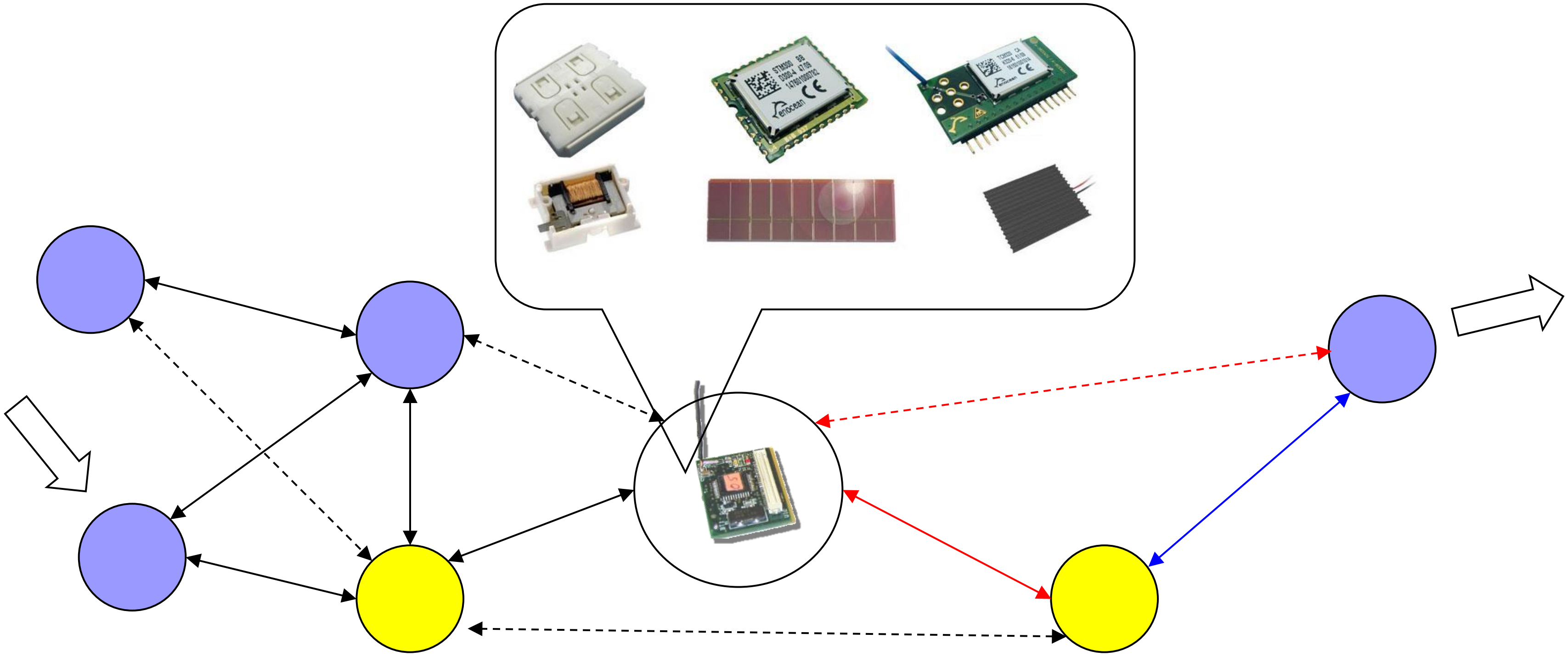
```
template <typename RealType, typename IntType>
  RealType tFastErlang_B(RealType rho, IntType N, RealType accuracy)
  {
        RealType s;
        IntType n0 = (IntType) max (0.0, rho - 1.0/accuracy);
        if (n0 > N) s = 1.0 - N/rho;
        else
        {
              RealType b0 = 1.0 - n0/rho;
              s = 1.0/b0;
              for (int j = n0; j <= N; j++)
              {
                          s = 1+ RealType(j)*s/rho;
              }
              s = 1.0/s;
        }
        return s;
  }
```

Performance Ciomparision



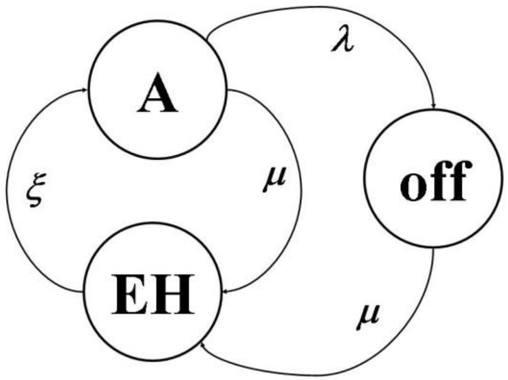
EH-WSNs

$$r = \arg\max_{r \in \Omega_r} R(G(n, m(r), p(r))).$$



EH-WSNs Node Model

$$\lambda \to \infty \Rightarrow \lim \mathrm{P}_{\mathrm{off}} = \left(1+\frac{\eta}{\xi}\right)^{-1}.$$



$$\frac{dP_0(t)}{dt} = -\delta P_0 + \mu P_1 + \lambda P_k,$$

...

$$\frac{dP_i(t)}{dt} = -(\delta+\mu)P_i + \mu P_{i+1} + \delta P_{i-1}, 1 \le i < k,$$

...

$$\frac{dP_i(t)}{dt} = -(\delta+\mu+\lambda)P_i + \mu P_{i+1} + \delta P_{i-1} + \lambda P_{i+k},$$

$$k \le i \le N-k,$$

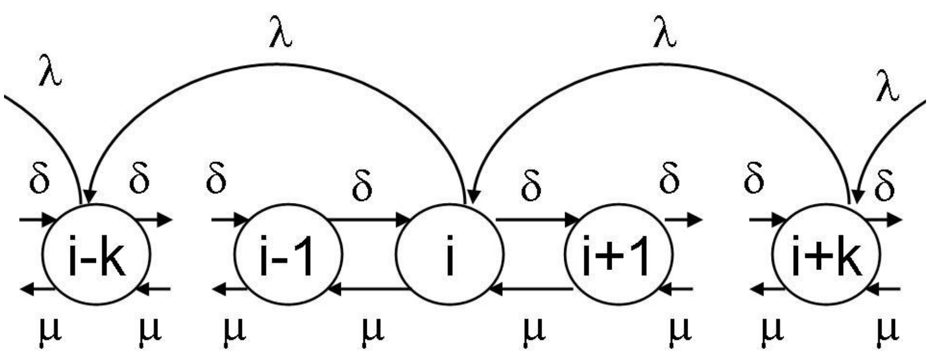
...

$$\frac{dP_i(t)}{dt} = -(\delta+\mu+\lambda)P_i + \mu P_{i+1} + \delta P_{i-1},$$

$$N-k < i < N,$$

...

$$\frac{dP_N(t)}{dt} = -(\lambda+\mu)P_N + \delta P_{N-1}.$$



Probabilistic Sensing Model

$$y = \eta\,(x, \theta) + e$$

$$\varepsilon(N) = \begin{pmatrix} x_1, \ldots x_n \\ r_1, \ldots, r_n \end{pmatrix} \qquad \sum_{i=1}^{n} r_i = N$$

$$M(\varepsilon(N)) = \sum_{i=1}^{n} \omega(x_i) r_i \left(\nabla \eta\,(x, \theta)\right)^T \nabla \eta\,(x, \theta)$$

$$\hat{\theta} = f(\theta)$$

$$\max M(\varepsilon(N)) \Rightarrow x_{opt} = g(\theta)$$

$$y = \eta\,(x_{\text{opt}}, \theta) = Const$$

D-optimal design

$$\max_{\varepsilon_N} \det M(\varepsilon(N)),$$

$$\sum_{i=1}^{n} r_i \leq N,$$

$$x \in \Omega_x.$$

$$\varepsilon^* = \begin{pmatrix} x_1 \\ N \end{pmatrix}, \; x_1 = \arg\max_{x \in \Omega_x} \left(\omega(x) \left(\frac{\partial \eta(x,\theta)}{\partial \theta} \right)^2 \right);$$

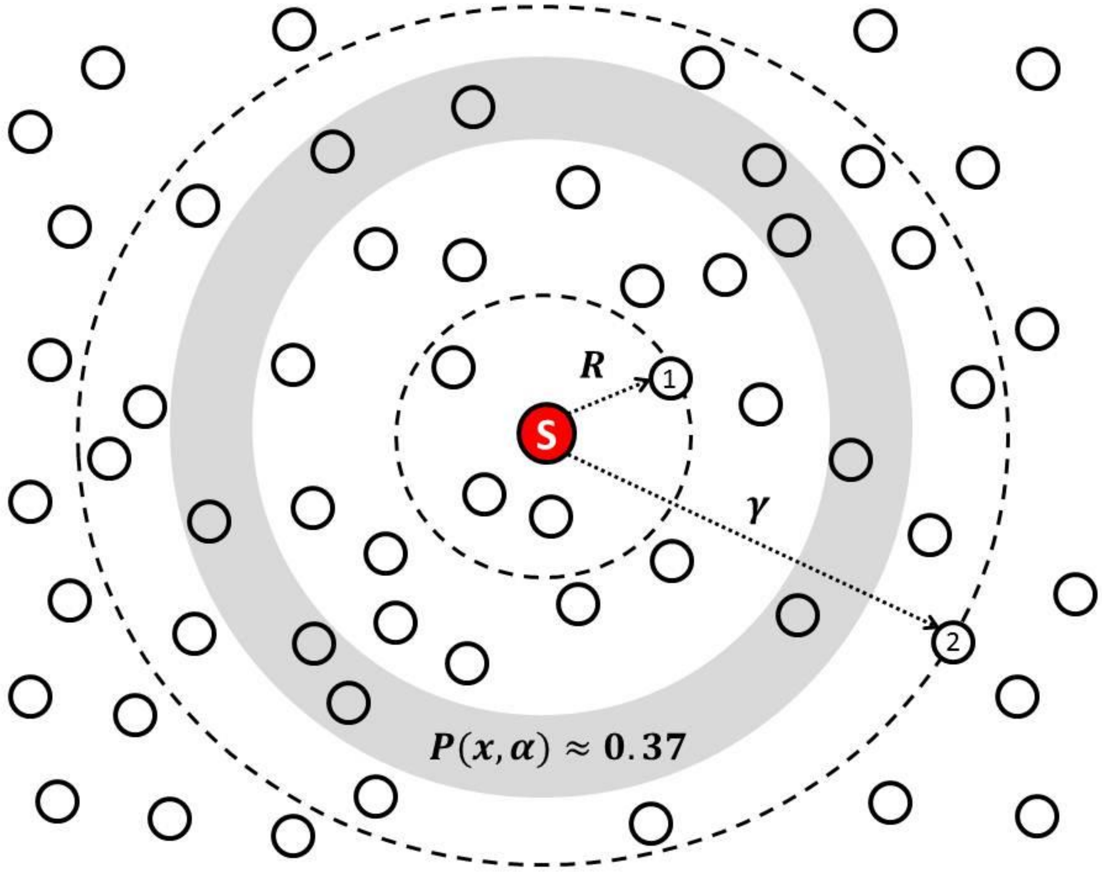
$$\frac{\omega_x^{'}(x)}{\omega(x)} = -\frac{\eta_{\theta x}^{''}}{\eta_{\vartheta}^{'}}$$

$$\left(\eta_{\theta}^{'}(x,\vartheta)\right)^2$$

$$x_1 = \arg\max_{x \in \Omega_x} \left(\left(\frac{\partial \eta(x,\theta)}{\partial \theta} \right)^2 \right)$$

Example

$$\eta(x,\theta) = e^{-\alpha x}$$



Security Challenges

- The emerging Internet of Things has tremendous potential, but also tremendous dangers.
- The world community was seriously concerned about the societal costs of the IoT outweigh its benefits. A few investigations have repeatedly shown that many IoT device manufacturers and service providers are failing to implement common security measures in their products.
- Cyber security experts report that only 10% of enterprises feel confident that they can secure those devices against intrusions, whereas IoT threats will disable home security systems, flood fields, paralysis of traffic, and disrupt hospitals.

The Economist | World politics | Business & finance | Economics | Science & technology | Culture

Cyber-security

The internet of things (to be hacked)

Hooking up gadgets to the web promises huge benefits. But security must not be an afterthought

Jul 12th 2014 | From the print edition

Like 217 | Tweet 594

How the Internet of Things Could Kill You

By Fahmida Y. Rashid JULY 18, 2014 7:30 AM - Source: Tom's Guide US | 5 COMMENTS

Hacking the Fridge: Internet of Things Has Security Vulnerabilities

JESS SCANLON | MORE ARTICLES
JUNE 28, 2014

Philips Hue LED smart lights hacked, home blacked out by security researcher

By Sal Cangeloso on August 15, 2013 at 11:45 am | 7 Comments

BBC WORLD NEWS

'Smart' home devices used as weapons in website attack

CNN tech | business | culture | gadgets | future | startups

The Cybercrime Economy

Internet of fails: What's wrong with connected devices

FBI Warns Public on Dangers of the Internet of Things

TREND MICRO

The Washington Post

Can anyone keep us safe from a weaponized 'Internet of Things?'

By Andrea Peterson October 25, 2016

BUSINESS INSIDER | BI INTELLIGENCE

A major red flag about security could threaten the entire IoT

Andrew Meola
Mar. 3, 2016, 12:12 PM 6,184

The New York Times

POLITICS

A New Era of Internet Attacks Powered by Everyday Devices

By DAVID E. SANGER and NICOLE PERLROTH OCT. 22, 2016

Internet of Things comes back to bite us as hackers spread botnet code

Elizabeth Weise, USATODAY Published 6:44 p.m. ET Oct. 3, 2016 | Updated 8:02 p.m. ET Oct. 3, 2016

BBC WORLD NEWS

How easy is it to hack a home network?

By Mark Ward
Technology correspondent, BBC News

25 February 2016 | Technology

THE WALL STREET JOURNAL.

Home | World | U.S. | Politics | Economy | Business | Tech | Markets | Opinion | Arts | Life | Real Estate

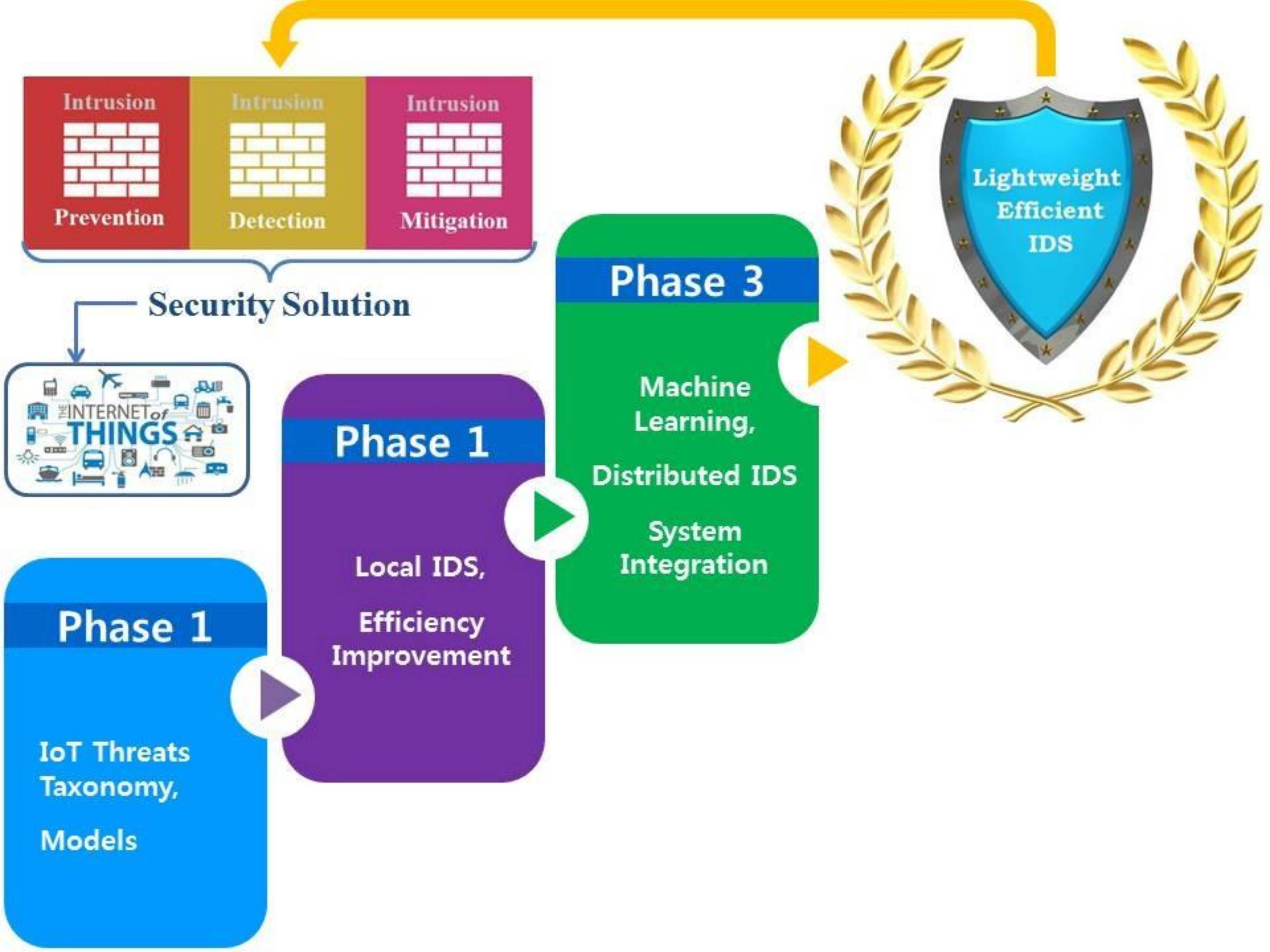
THE EXPERTS

Here's Why the Internet of Things Could Be a Security Nightmare

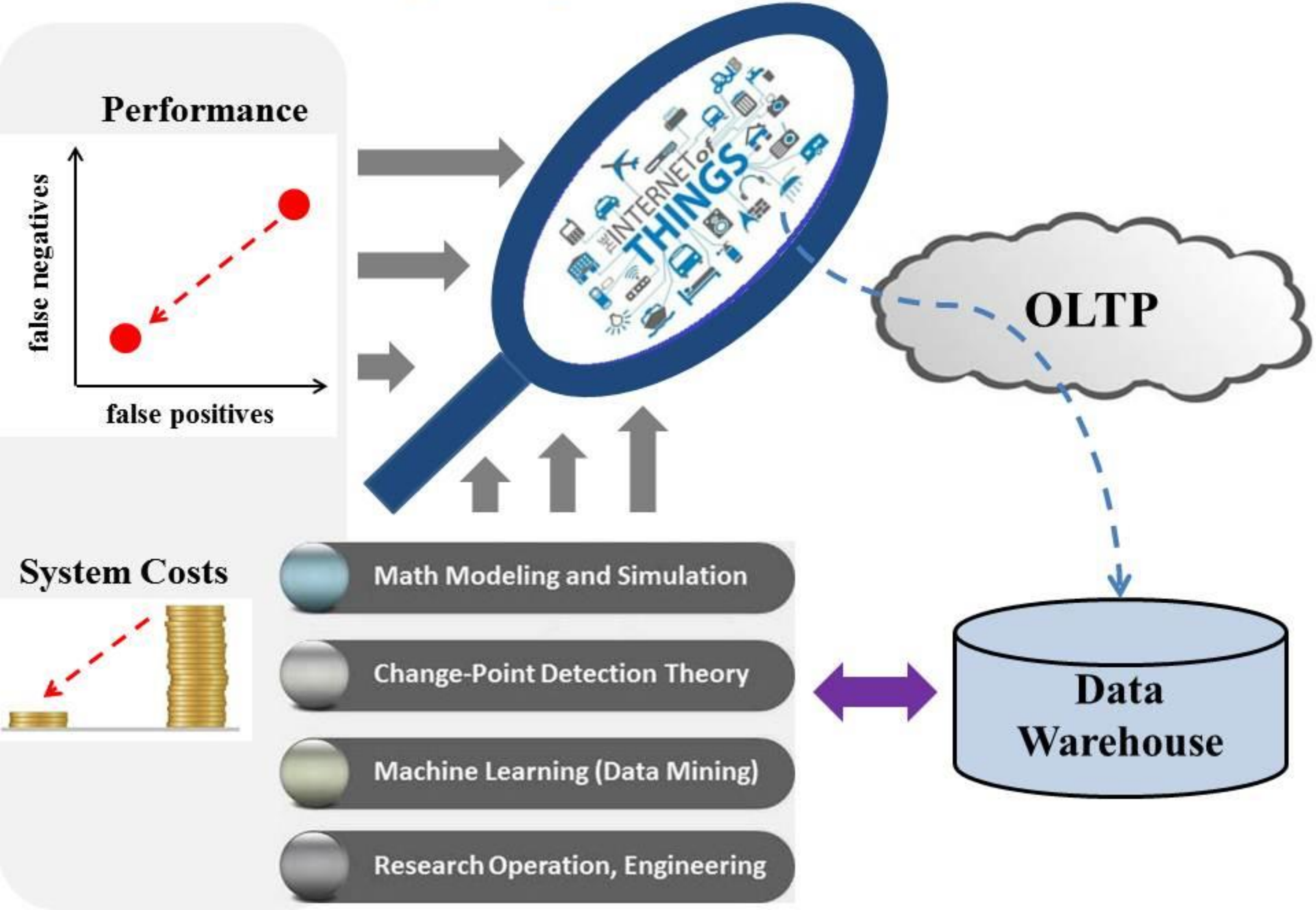
By ROBERT PLANT
Feb 23, 2016 11:00 am ET

Motivation

To unlock the IoT potential it needs to improve the security of IoT applications.


Intrusion
Prevention
Intrusion
Detection
Intrusion
Mitigation
Security Solution
THE INTERNET of THINGS
Lightweight
Efficient
IDS
Phase 3
Machine
Learning,
Distributed IDS
System
Integration
Phase 1
Local IDS,
Efficiency
Improvement
Phase 1
IoT Threats
Taxonomy,
Models

Lightweight anomaly based IDS



Thank you for the attention!

Q&A