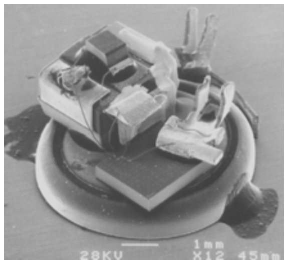



# Wireless Sensor Network Denial of Sleep Attack

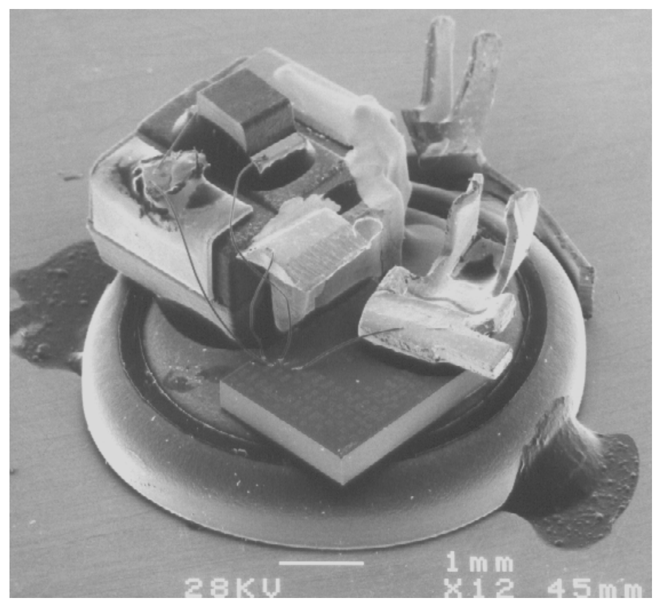
Presentation by Michael I Brownfield

**Paper Authors**
Major Michael Brownfield
Mr. Yatharth Gupta
Dr. Nathanial J. Davis IV (Head, Department of Electrical and Computer Engineering, Air Force Institute of Technology)

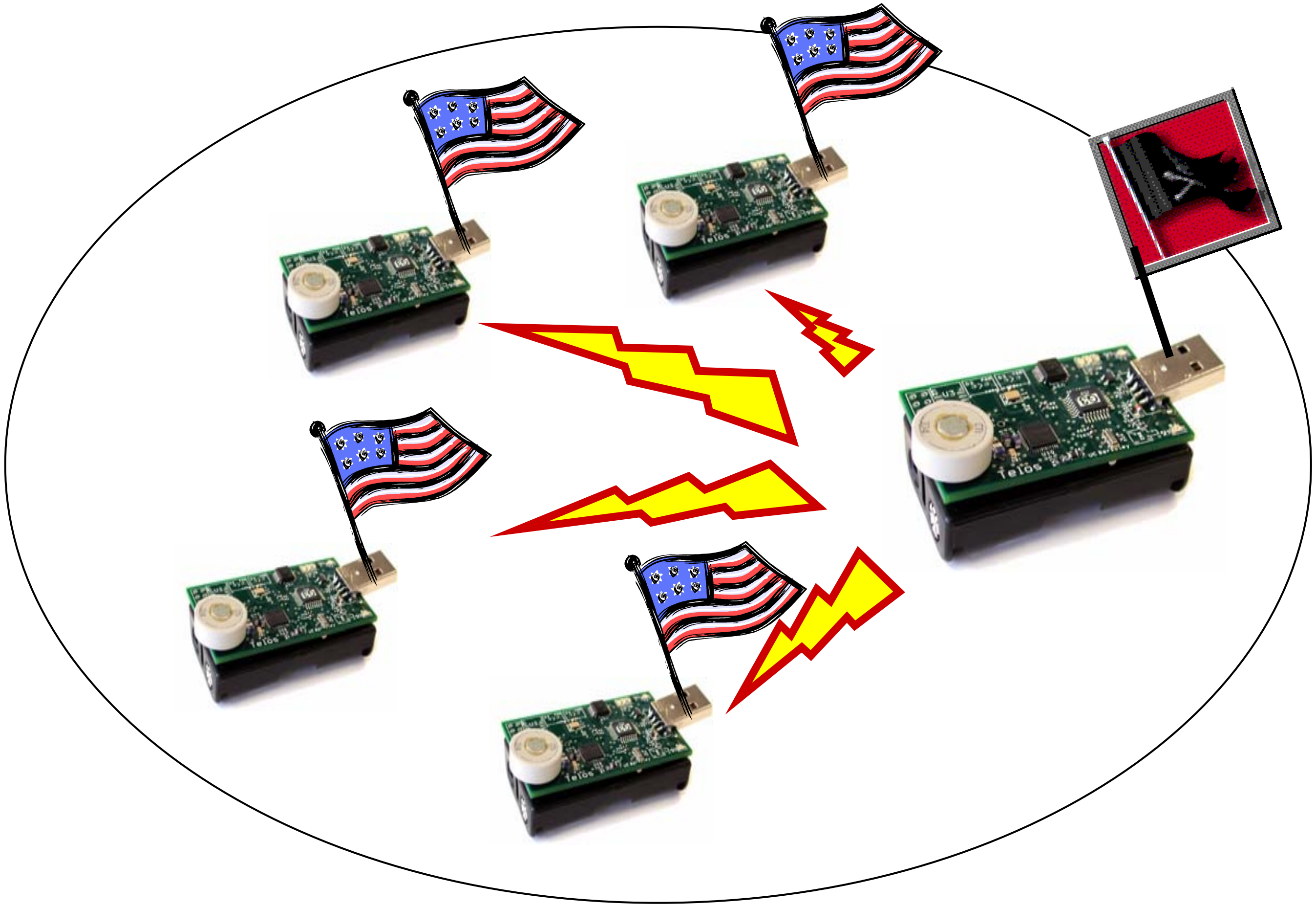
# Motivation


FORTUNE

1. **SMART DUST KICKS UP A STORM**
   **Tiny wireless sensors start monitoring the nation's food, workplaces, and welfare (02/2004).**

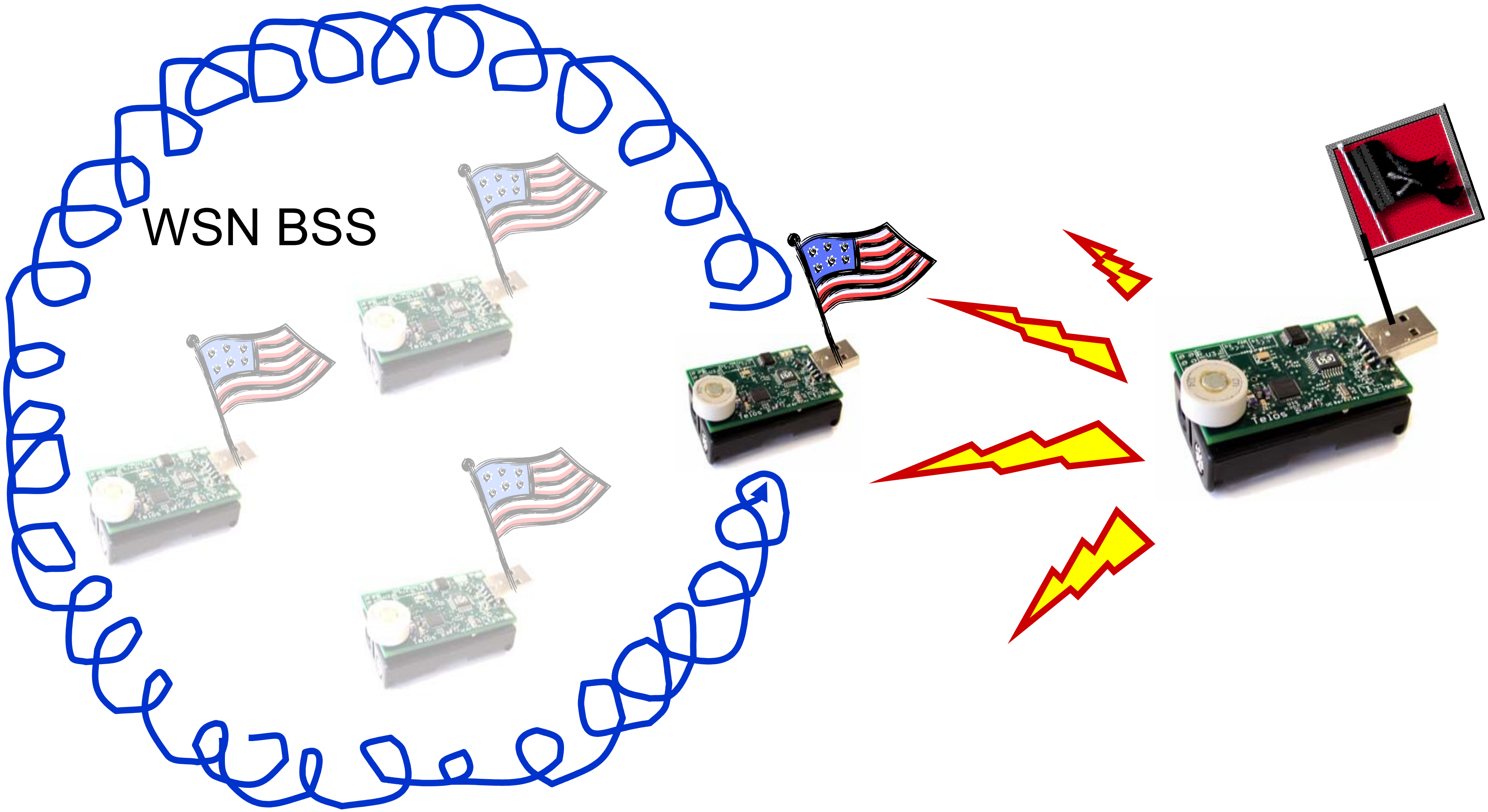


# Even More Motivation



Wireless Sensor BSS

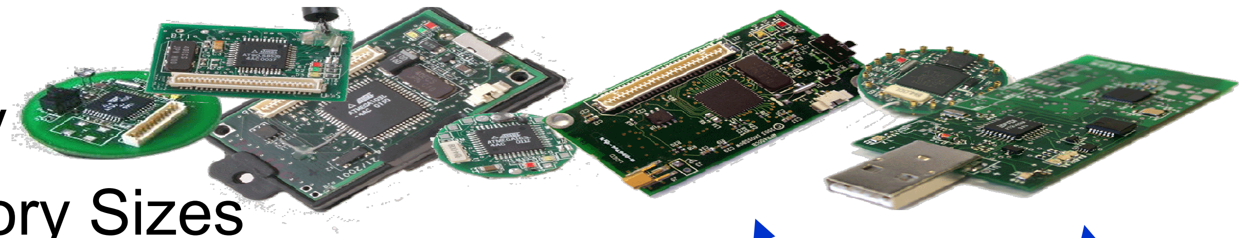
# Yes, Even More Motivation



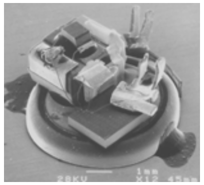
# Agenda

- Wireless Network Challenges
- Related Security Work
  - Software Solutions
  - Hardware Solutions
- MAC Layer Sources of Energy Loss
- Comparison Wireless Sensor Network Protocols
- Gateway MAC
- Protocol Analysis
- Conclusion

# Sensor MAC Protocol Challenges



- Energy Efficiency
- RAM/ROM Memory Sizes
- Embedded Processor Capabilities
- Channel Utilization Efficiency
  - Throughput
  - Delay
  - Fairness
- Self-Configuration
- Network Scalability

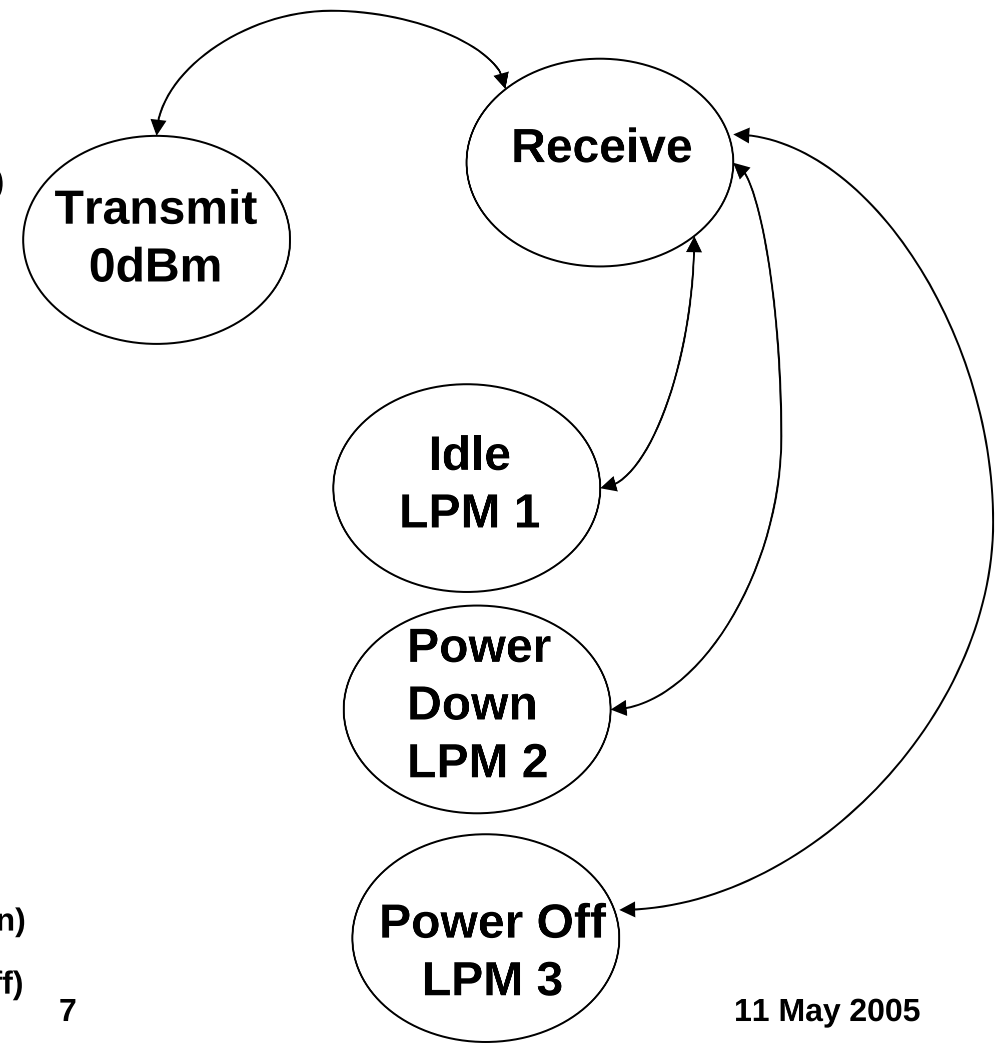


| Platform | Smartdust | Mica2 | TelosA |
|---|---|---|---|
| µ-controller | 8-bit | 16-bit | 16-bit |
| MCU RAM | 512 B | 4 kB | 2 kB |
| EEPROM | 512 B | 128 kB | 60 kB |
| Radio | 916 MHz | 868 MHz | 2.4 GHz |
| Data Rate | 10 kbps | 76.8 kbps | 250 kbps |

VIRGINIA POLYTECHNIC INSTITUTE AND STATE UNIVERSITY

# Sensor Motes Believe it Or Not!

| Radio Current | Platform Current |
|---|---|
| 19.7mA | 20 mA (Radio On, MCU On) |
| 17.4 mA | |
| 426 µA | |
| 20 µA | |
| 1 µA | 420 µa (MCU On)<br>2.4 µA (MCU Off) |



# WSN Software Security Solutions

- Tiny Sec
  - Fully Implemented with only 10% energy, latency, and BW overhead
  - Proves hardware assistance is unnecessary
  - Provides message authentication, integrity, and confidentiality w/out hardware acceleration

| Dest (2) | AM (1) | Len (1) | Src (2) | Ctr (2) | **Data (0..29)** | MAC (4) |
|---|---|---|---|---|---|---|

+5

TinySec-AE packet format

| Dest (2) | AM (1) | Len (1) | Data (0..29) | MAC (4) |
|---|---|---|---|---|

+1

TinySec-Authentication packet format

| Dest (2) | AM (1) | Len (1) | Grp (1) | Data (0..29) | CRC (2) |
|---|---|---|---|---|---|

Standard TinyOS packet format

# CC2420 WSN Mote Transceiver Hardware Security Solutions

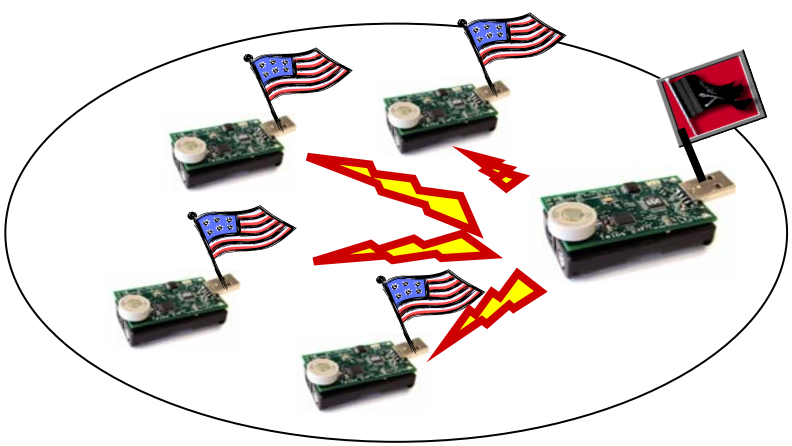
## AES-128 Hardware Encryption with 4 Security Modes

1. Disabled
2. Cipher block chaining – Message Authentication Code (CBC-MAC) authentication
3. Counter (CTR) encryption / decryption
4. Counter with CBC-MAC (CCM) authentication and encryption / decryption

# Link Layer Denial of Service ATTACKS!

- Link Layer Collision Attack
  - Attacker sends a signal at same time and frequency as legitimate traffic

- Link Layer Exhaustion Attack
  - Manipulate the MAC protocol to force nodes to stay awake (repeated RTS messages)



# MAC Layer Sources of Energy Loss

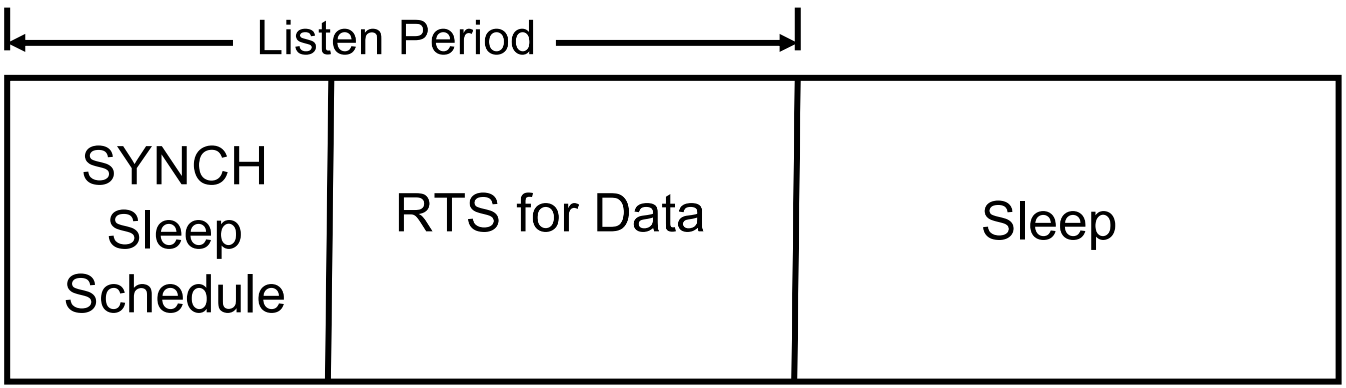
- Idle Listening
- Frame Collisions
  - Propagation Delay
  - Hidden Terminal
  - Capture Effect
- Overhearing
- Protocol / Control Packet Overhead
  - Control Packets (RTS, CTS, ACK)
  - Management Packets (Association requests, Beacon
  - MAC Header transmission , Interframe Spacing
  - Contention Backoff

# Current WSN MAC Approaches

- Slotted CSMA:
  - Sensor MAC (S-MAC) implemented
  - Timeout MAC (T-MAC) implemented
  - Berkeley-MAC (B-MAC) implemented
- TDMA
  - Traffic-Adaptive MAC (TRAMA)
  - Low-Energy Adaptive Clustering Heirarchy (LEACH)
  - Power Aware Clustered TDMA (PACT)
  - Bit-Map Assisted (BMA)
  - Proposed Gateway MAC (G-MAC)

# Sensor MAC (S-MAC) Approach

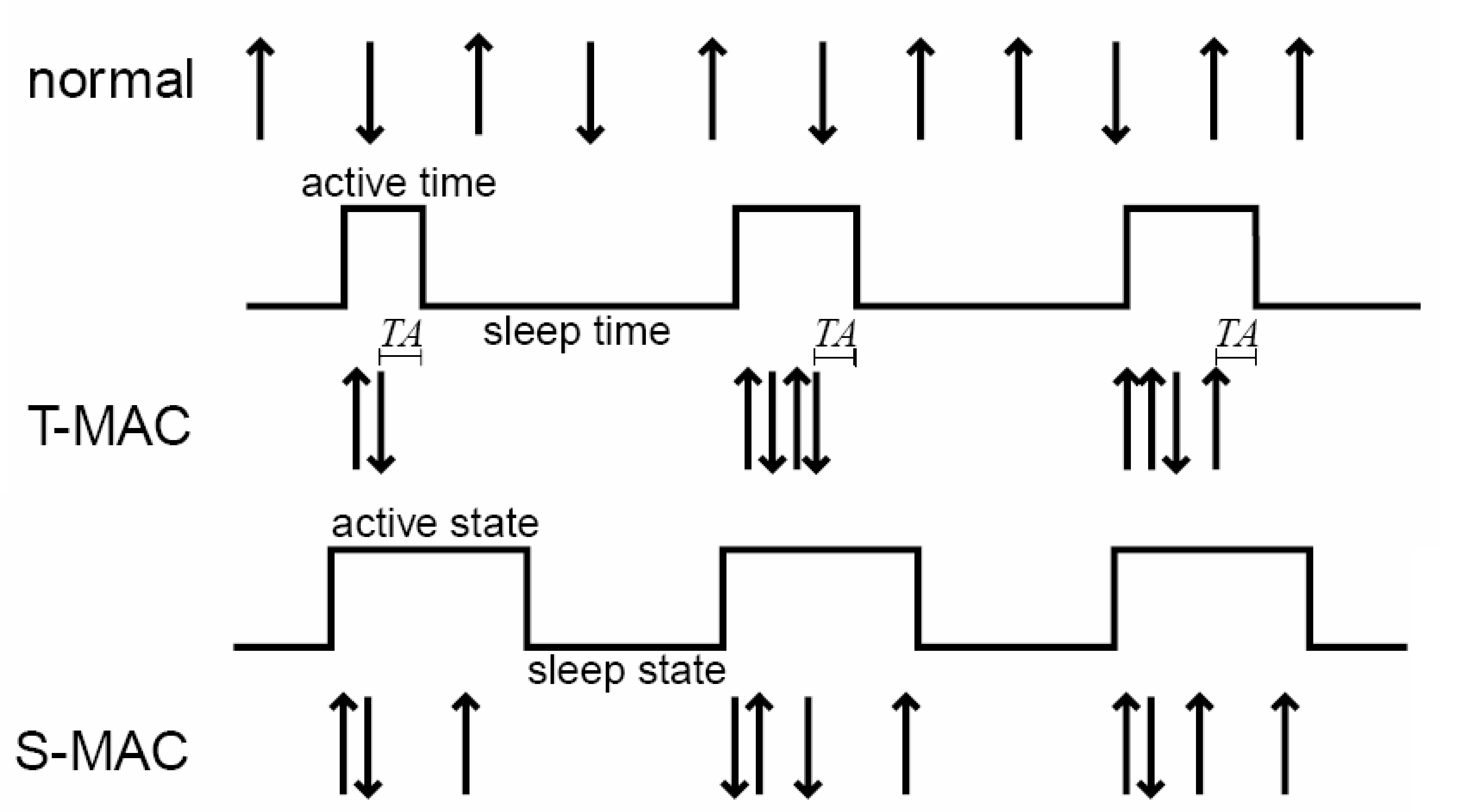
- Reduce energy through sleeping



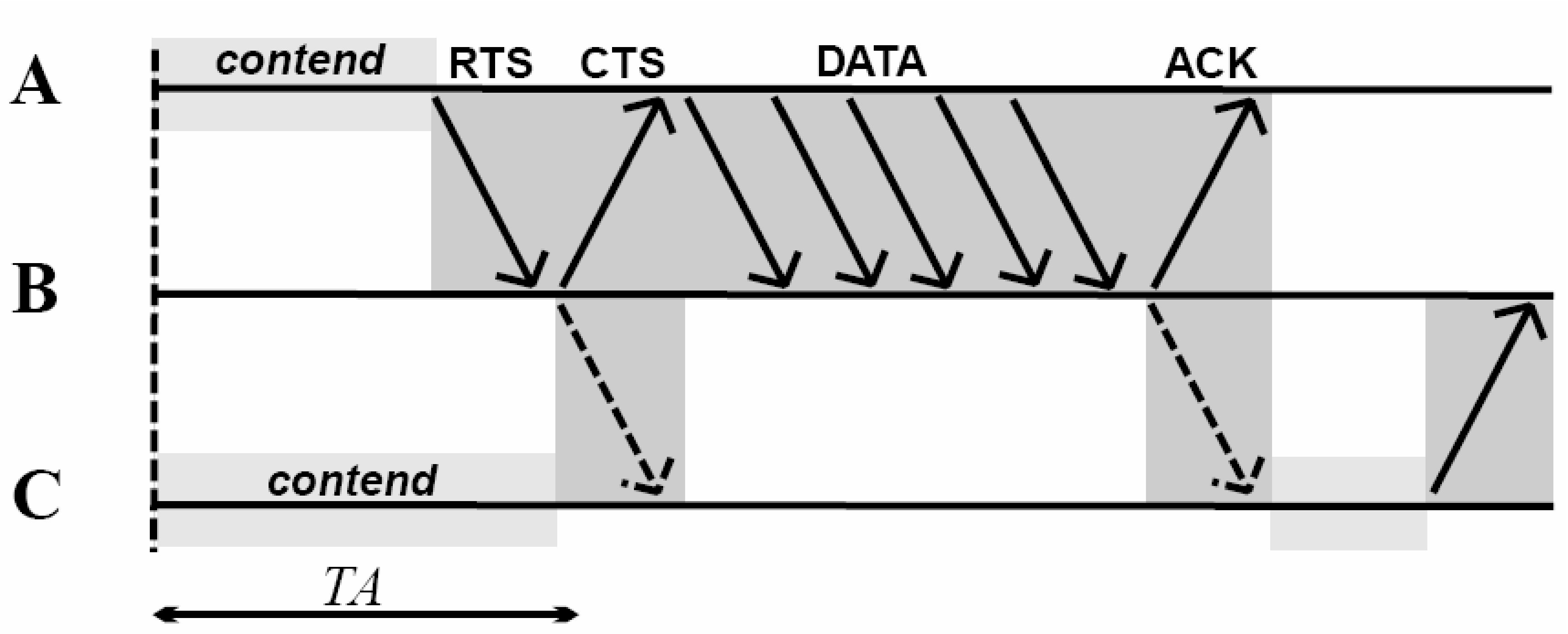

- Reduce energy by synchronizing sleep schedules in clusters

# Idle Listening
# Slotted Approaches

- Reduce energy through sleeping *after* timeout



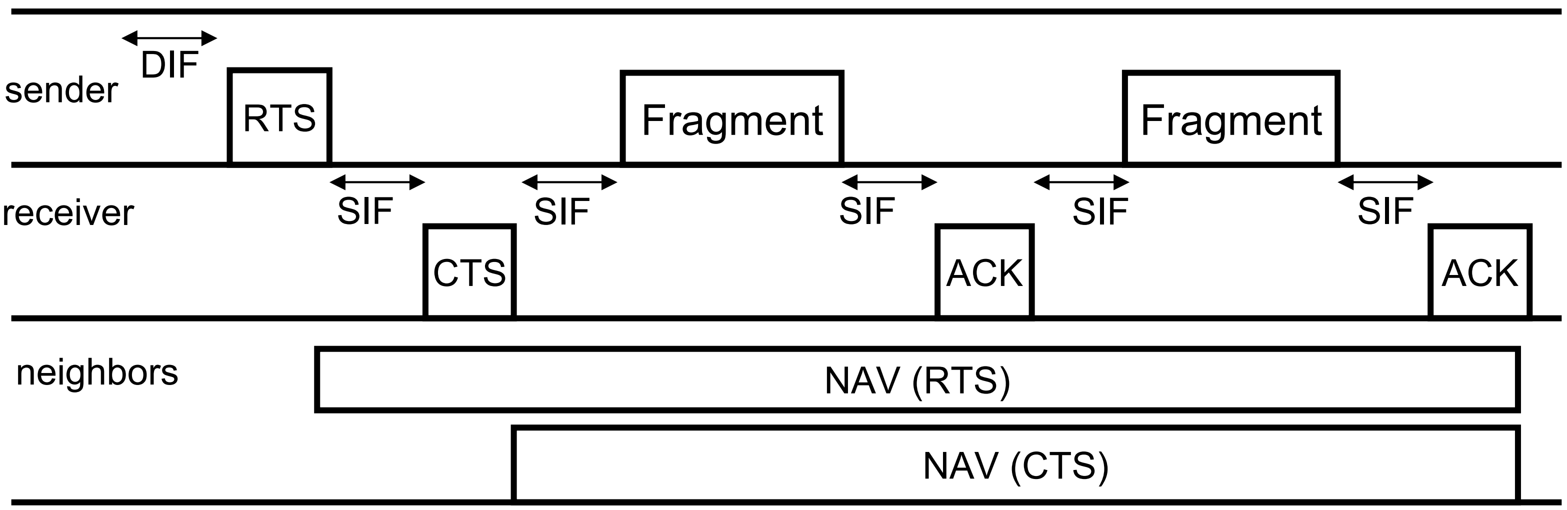
# T-MAC Adaptive Timeout (TA)




$$TA = 1.5 * (T_{contention\_interval} + T_{RTS\_interval} + T_{SIFS})$$

# Frame Collisions / Overhearing Avoidance

- Frame Collisions: RTS-CTS-Data-ACK
- Overhearing Avoidance: In-channel signaling to sleep during other transmissions



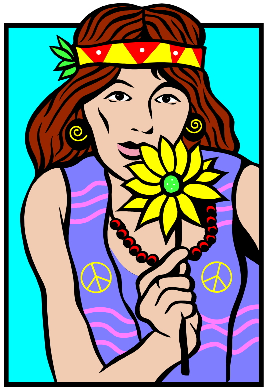
# Berkeley MAC (B-MAC)

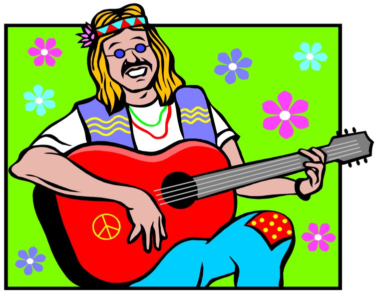
## (Contention-based)

Versatile Low Power Media Access for Wireless Sensor Networks

Joseph Polastre, Jason Hill and David Culler

Sensys November 2004





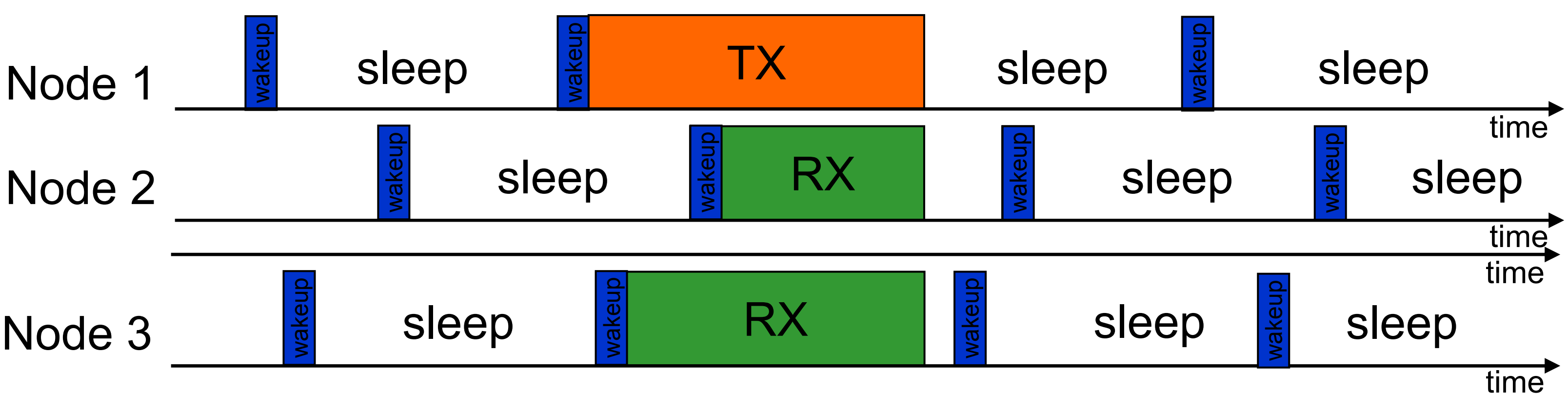
VIRGINIA POLYTECHNIC INSTITUTE AND STATE UNIVERSITY

# B-MAC GOALS

- Low Power operation
- Effective collision avoidance
- Simple and predictable
- Small code size and RAM usage
- Tolerable to changing RF/networking conditions
- Scalable to large numbers of nodes

# BMAC Design Approach

- Minimalistic (BMAC)
  - Small core functionality: media access control
  - RTS/CTS, ACKs, etc are considered higher layer functionality (services) that Applications can turn on and off



# Denial of Sleep Threat Analysis

- S-MAC

$$T_{network\,lifetime} = T_{sensor\,lifetime} = \frac{C_{battery(mAhr)}}{(D)\left(I_{active(mA)}\right) + (1 - D)\left(I_{sleep(mA)}\right)}$$

- T-MAC and B-MAC

$$T_{network\,lifetime} = T_{sensor\,lifetime} = \frac{C_{battery(mAhr)}}{I_{active(mA)}}$$

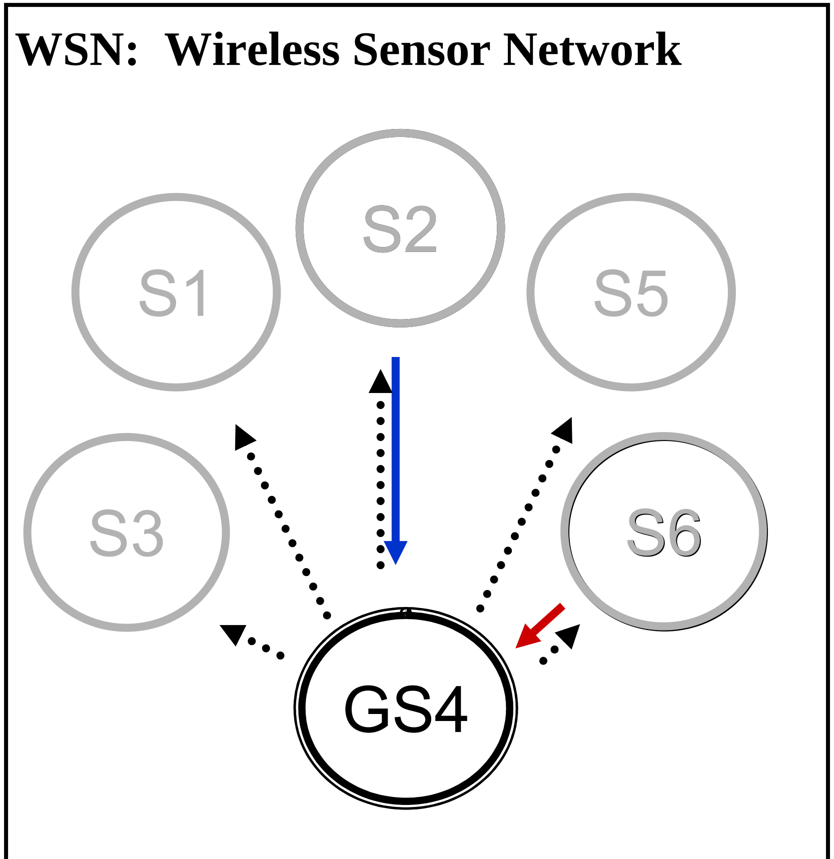
- Proposed Gateway MAC

$$T_{network\,lifetime} = T_{sensor\,lifetime} = \frac{n_{nodes} * C_{battery(mAhr)}}{\left(I_{active(mA)}\right)}$$

# Gateway MAC (G-MAC) Design Goals

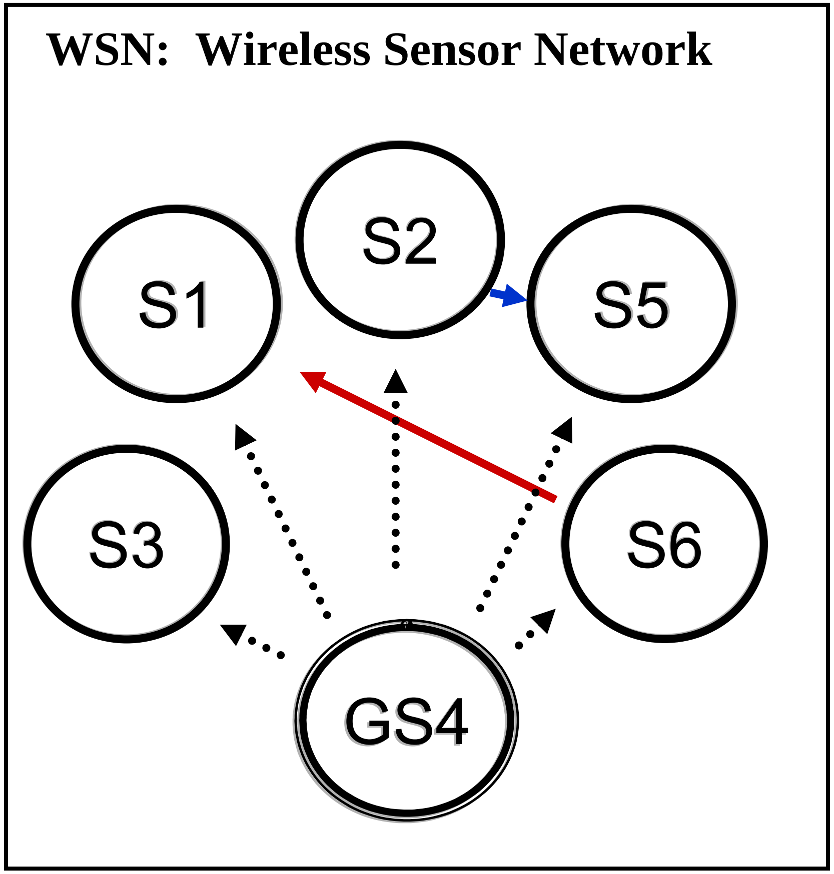
- Flexible and Scalable
  - Allocate Transmission Slots for Active Communication
  - *Distribute Clusterhead/Gateway Duties*
- Energy-efficient
  - *Eliminate Network-wide Idle Listening*
  - Create Traffic Rhythm for Increased Sleep Duration
- Secure
  - *Gateway Sentry*
  - *Embedded AES-128*
- Dynamic
  - Self-configure, Self-recover

# GMAC Design: Phase 1 Data Collection



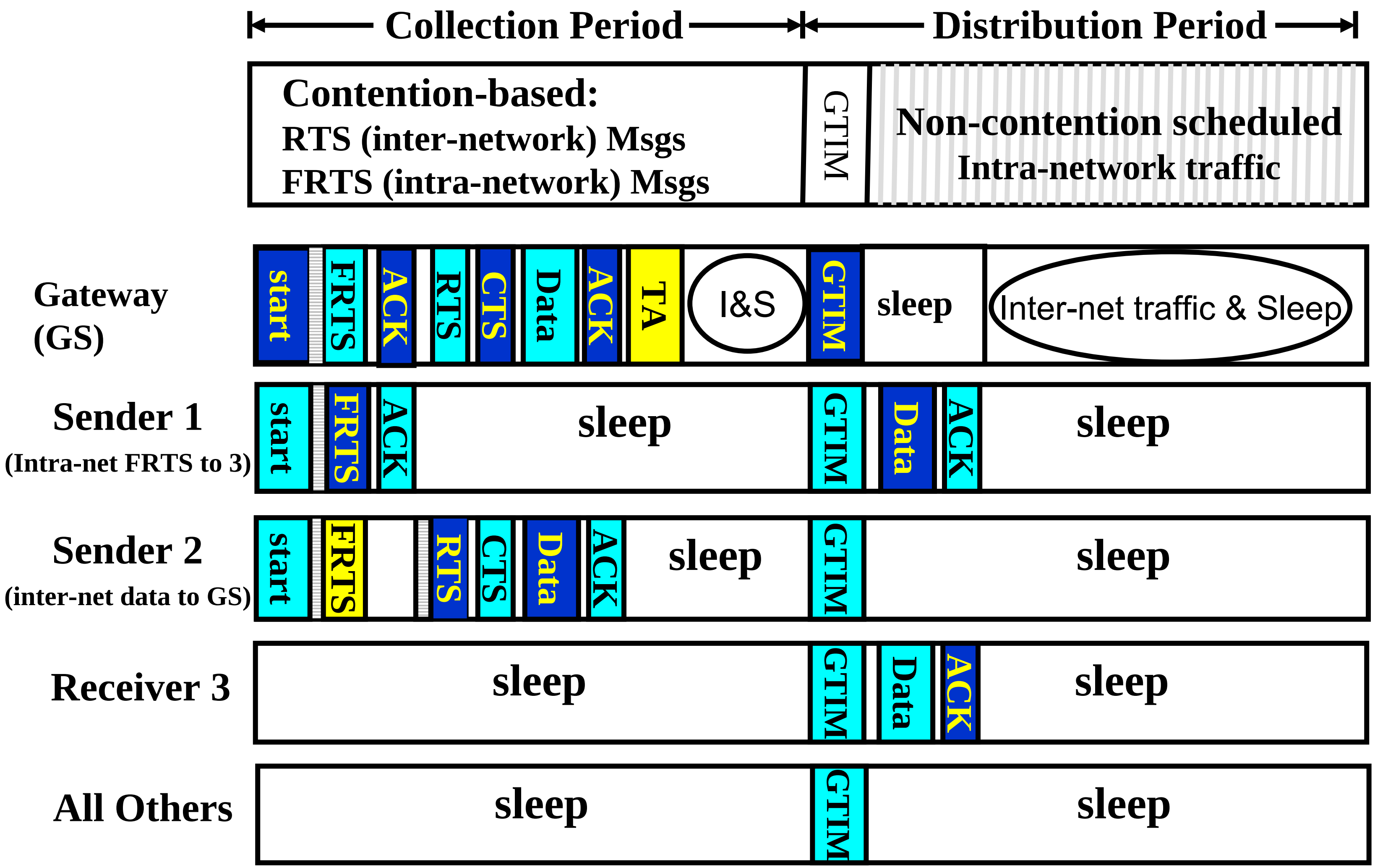

- Collects Intra-Network Traffic:
  - Local Gossip reservations
  - Cluster Association Requests
- Collects Inter-Network Traffic:
  - Converge-cast (out to WDS)
  - Network Routing
    - Tandem routing
    - Terminal

# GMAC Design: Phase 1 Data Distribution

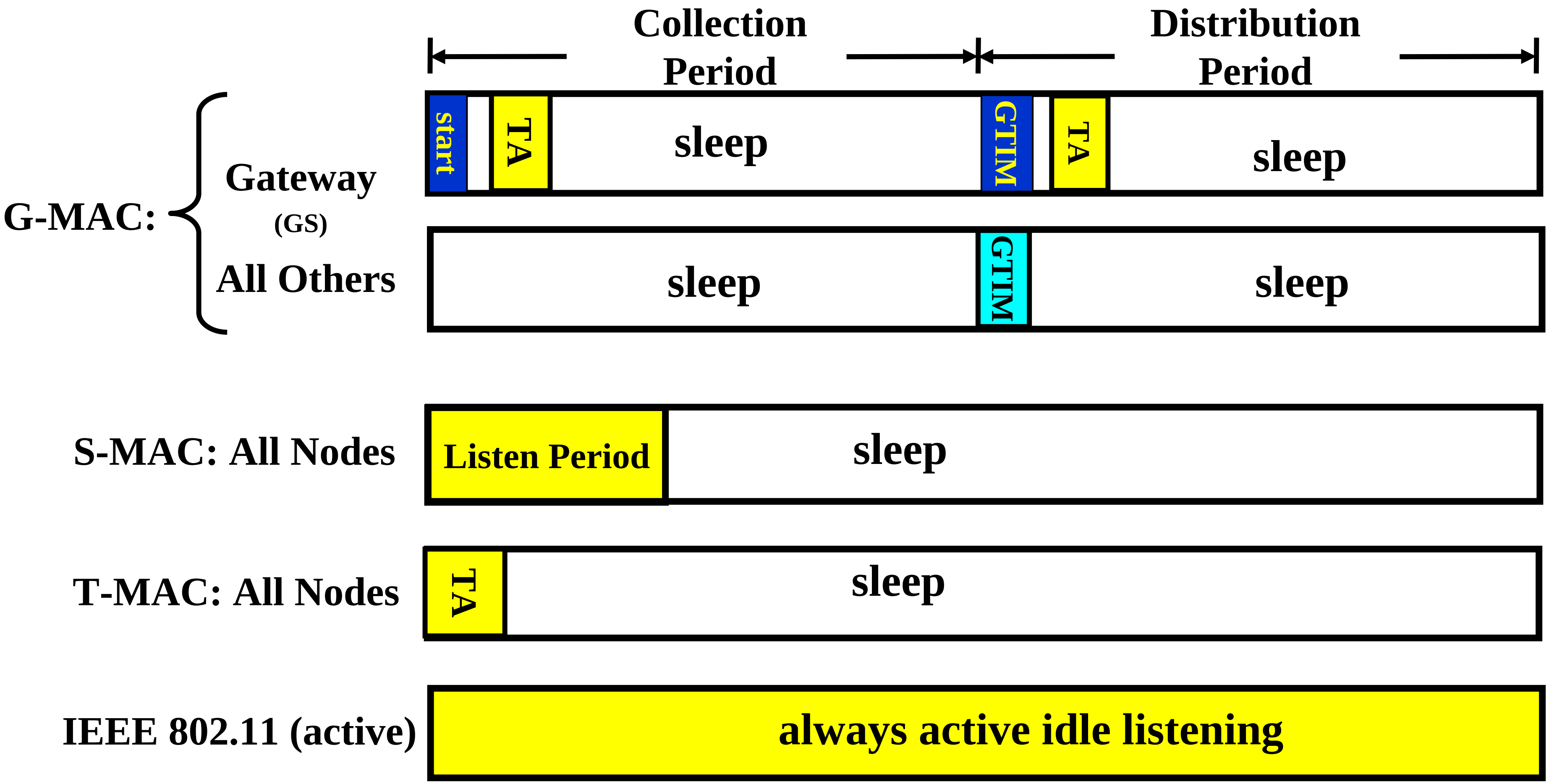



- Gateway Node broadcasts Traffic Indication Map (GTIM)
  - Local Broadcast (dotted lines)
  - Gossip exchanges
  - Cluster Synchronization Beacon

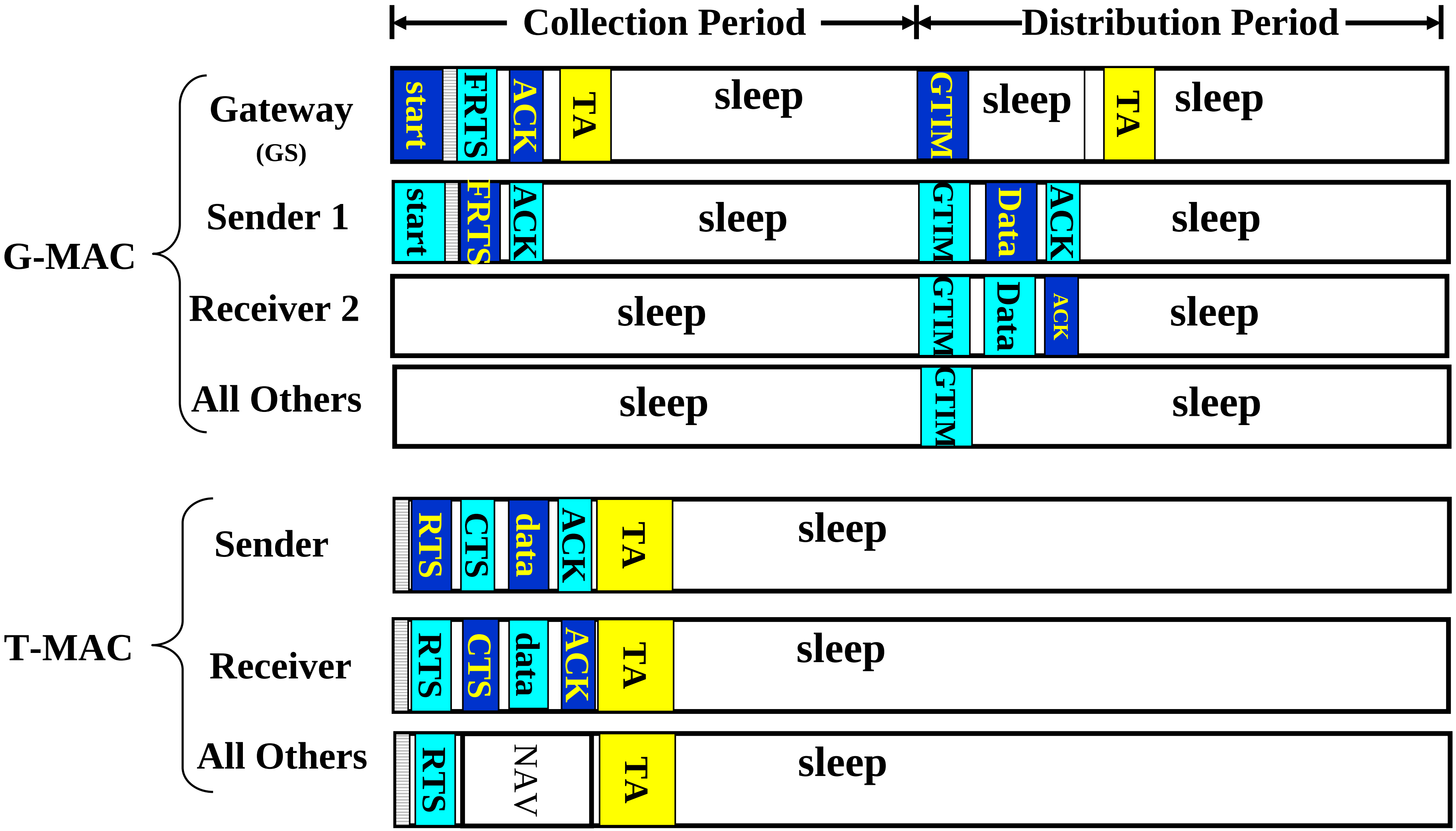
# GMAC Design


Collection Period
Distribution Period
Contention-based:
RTS (inter-network) Msgs
FRTS (intra-network) Msgs
GTIM
Non-contention scheduled
Intra-network traffic
Gateway (GS)
start
FRTS
ACK
RTS
CTS
Data
ACK
TA
I&S
GTIM
sleep
Inter-net traffic & Sleep
Sender 1
(Intra-net FRTS to 3)
start
FRTS
ACK
sleep
GTIM
Data
ACK
sleep
Sender 2
(inter-net data to GS)
start
FRTS
RTS
CTS
Data
ACK
sleep
GTIM
sleep
Receiver 3
sleep
GTIM
Data
ACK
sleep
All Others
sleep
GTIM
sleep

# Protocols in Empty Network

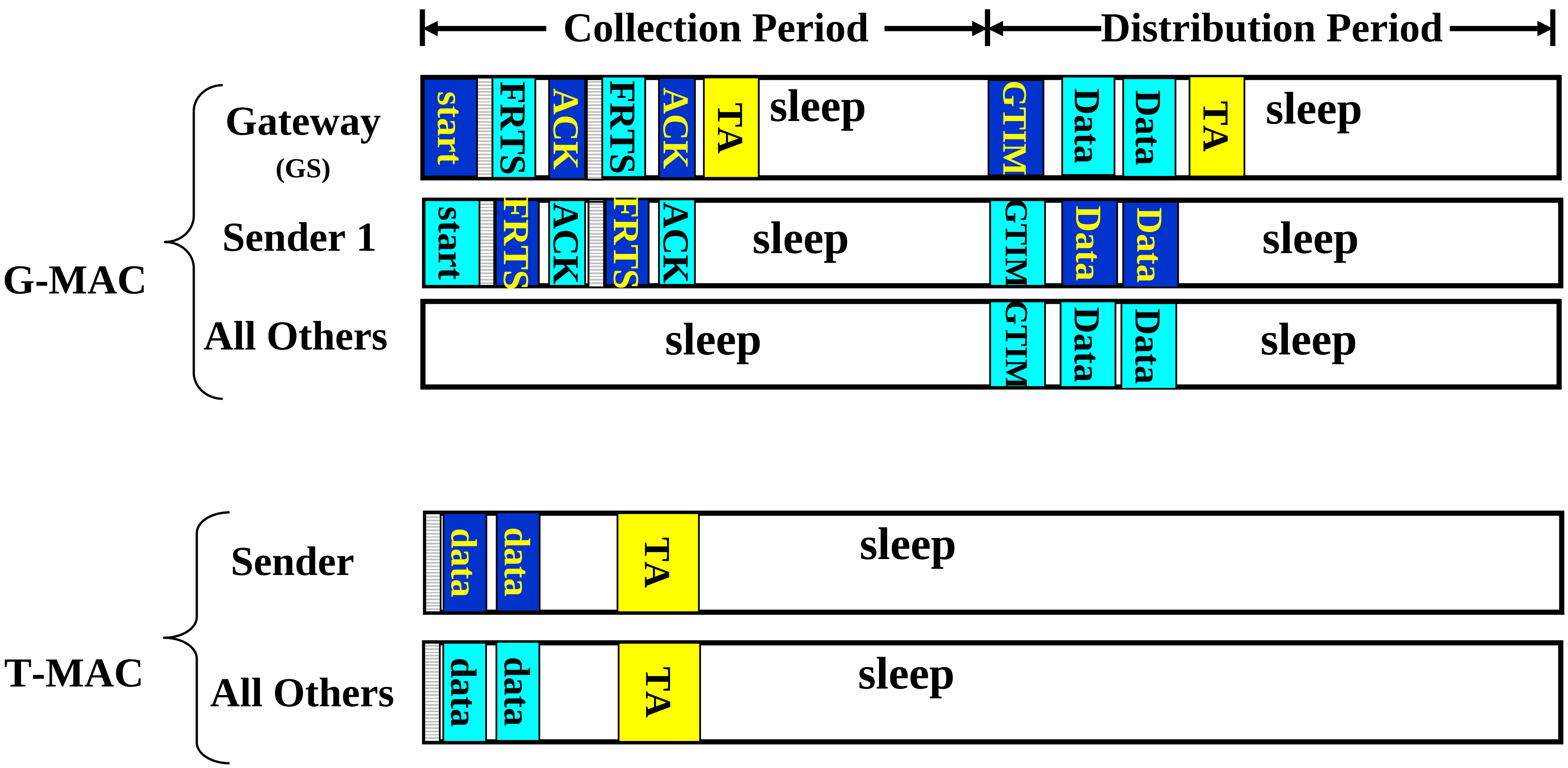


# G-MAC vs T-MAC
# Unicast Message



VIRGINIA POLYTECHNIC INSTITUTE AND STATE UNIVERSITY

# G-MAC vs T-MAC Broadcast Message



# GMAC Point Coordinator/ Gateway Election

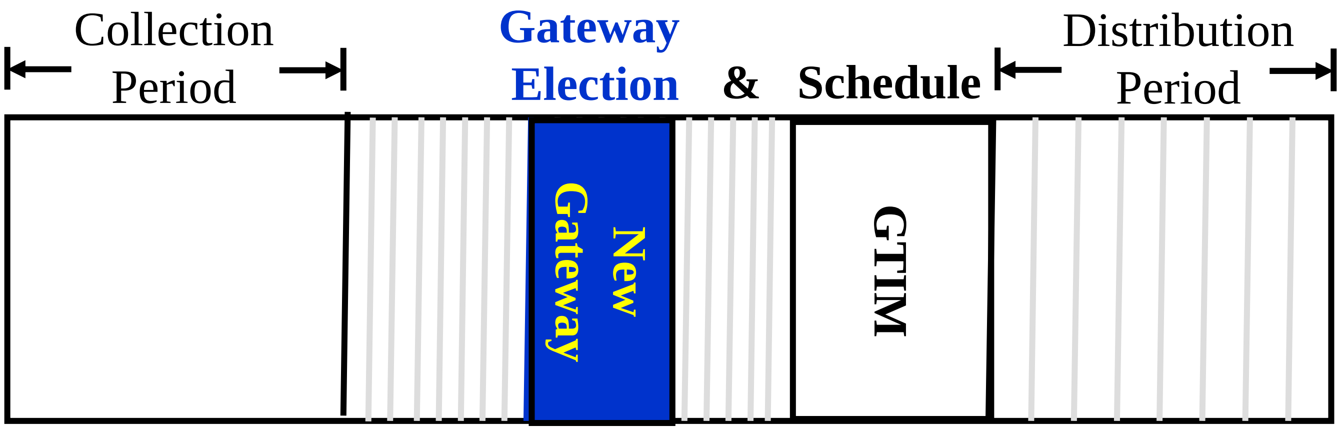
| Battery Pwr Level | | Voltage Range |
|---|---|---|
| 11 | High | 2.6 < Pwr (3.0-3.6) |
| 10 | Med | 2.4 < Pwr ≤ 2.6 |
| 01 | Low | 2.1 < Pwr ≤ 2.4 |
| 00 | Min | Pwr ≤ 2.1 volt |

| Memory Capacity Level | | Percentage Avail. Capacity |
|---|---|---|
| 11 | High | 30% < Mem |
| 10 | Med | 20% < Mem ≤ 30% |
| 01 | Low | 10% < Mem ≤ 20% |
| 00 | Min | Mem ≤ 10% |

**Critical Resource Level Algorithm**

if Pwr = **Min** or Mem = **Min**
then Resource Level = **3**
elseif Pwr = **Low** or Mem = **Low**
then Resource Level = **2**
elseif Pwr = **Med** or Mem = **Med**
then Resource Level = **1**
Elseif Pwr = **High** or Mem = **High**
then Resource Level = **0**

# GMAC Point Coordinator/ Gateway Election



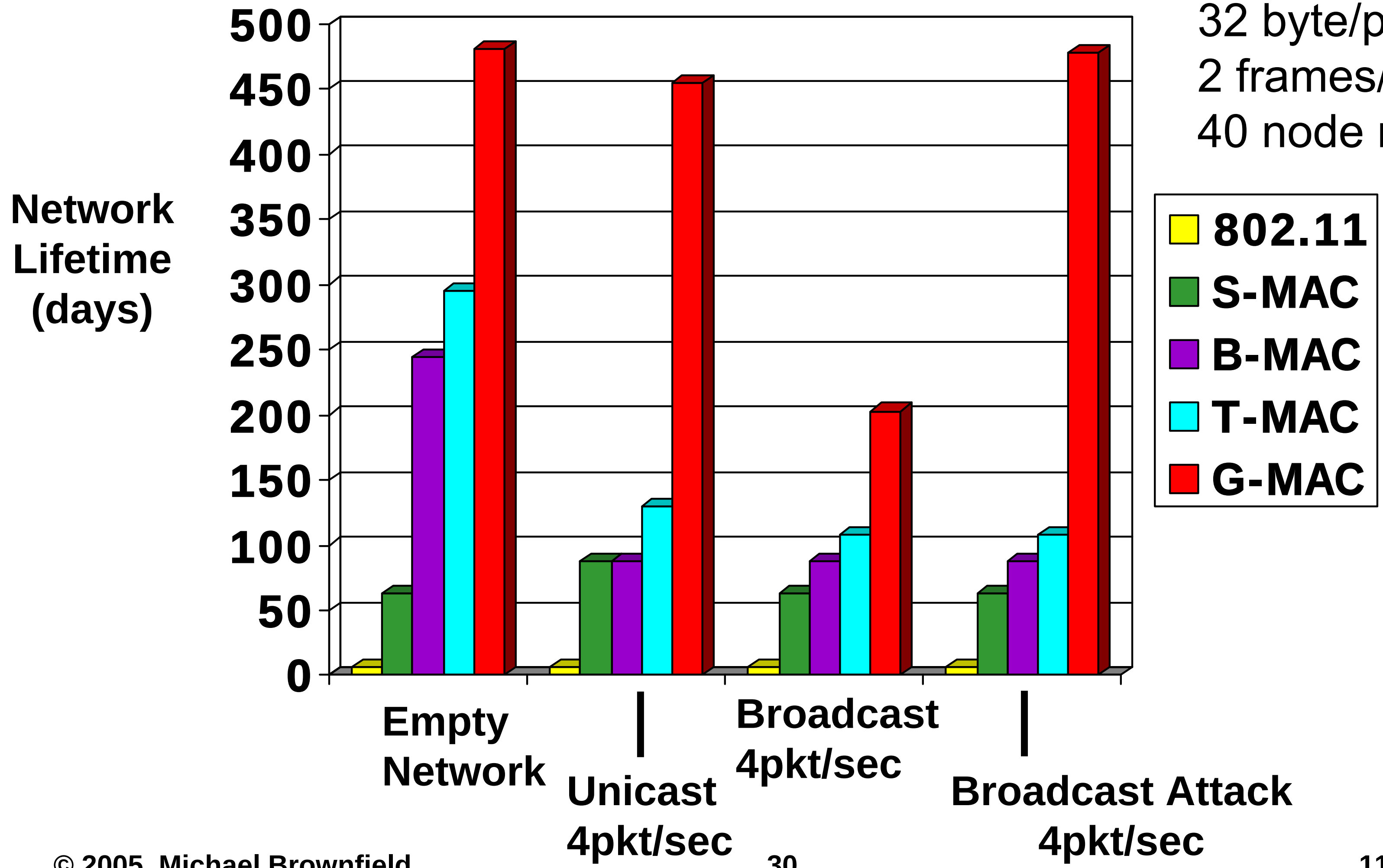

Election Contention Backoff = (16-bit Random Number mod $2^7$) + (RL * 128)

| Resource Level (RL) | Contention Window Random($2^7$) + RL * 128 |
|---|---|
| 0 (Max) | 0 to 127 Slots (16µs to 2ms) |
| 1 | 128 to 255 Slots (2ms to 4ms) |
| 2 | 256 to 511 Slots (4ms to 8ms) |
| 3 (Low) | 512 to 1023 Slots (8ms to 16ms) |

Virginia Tech
VIRGINIA POLYTECHNIC INSTITUTE AND STATE UNIVERSITY

# Preliminary Results: G-MAC

Data Rate 62.6kbps
32 byte/pkt
2 frames/second
40 node network



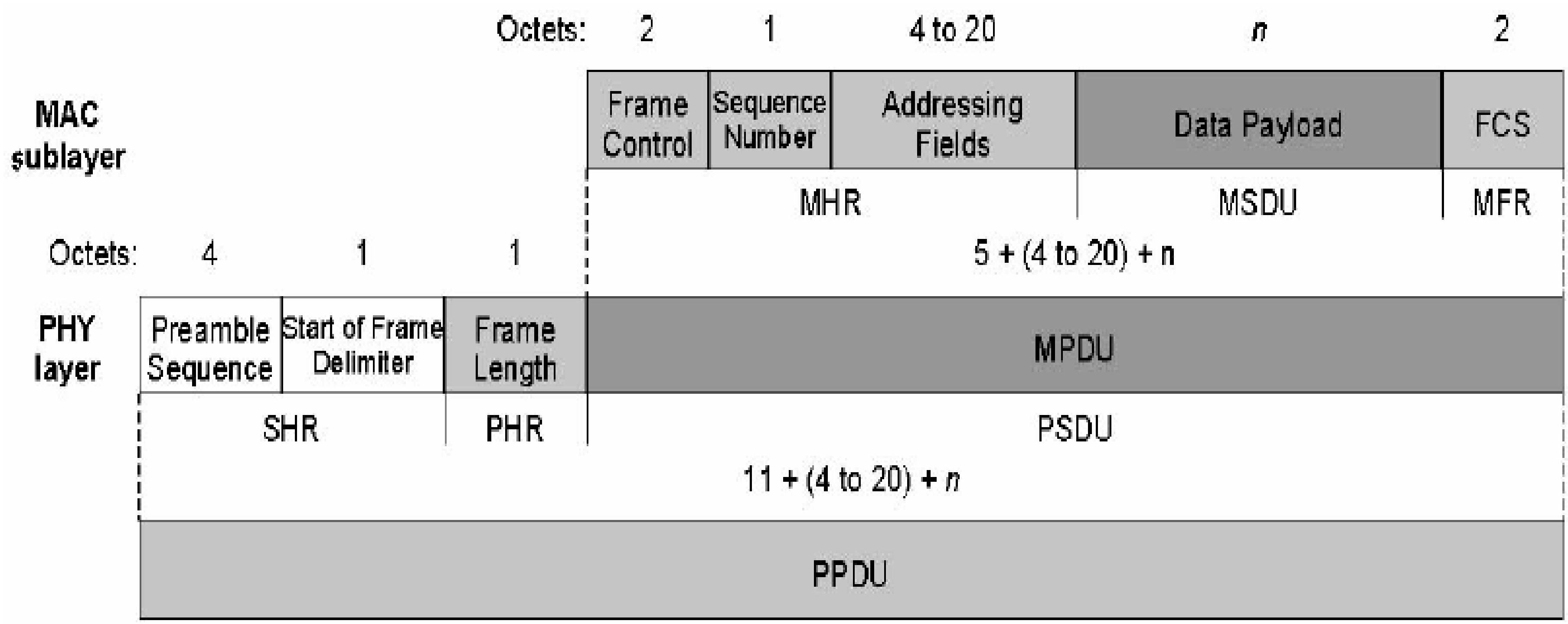
# Denial of Sleep Summary

- WSN networks are vulnerable to Denial of Sleep Attacks
- Design Security Measures at the System Architectural Level (when possible)
- Centralized network coordination functions (Gateway) can reduce the effects of Denial of Sleep Attacks

# Questions

**If we knew what it was we were doing,**
**it would not be called research, would it ?**
**--Albert Einstein**

# 802.15.4 Frame Format



# Symbiotic Network