NS-2 MODULE FOR IEEE 802.22 STANDARD

Galanopoulos Kon/nos

Spatharakis Fotios

Supervisor: Giannis F. Marias

THE IEEE 802.22 STANDARD AND THE MODULE DEVELOPED FOR NS2. ATTACK SCENARIOS SIMULATED IN NS2

Presentation Contents

1. About IEEE 802.22
2. Developing the 802.22 module for NS2
3. Attack scenarios simulation

1. About IEEE 802.22
2. Developing the 802.22 module for NS2
3. Attack scenarios simulated

ABOUT IEEE 802.22

Why IEEE started developing the 802.22 Standard(1/2)

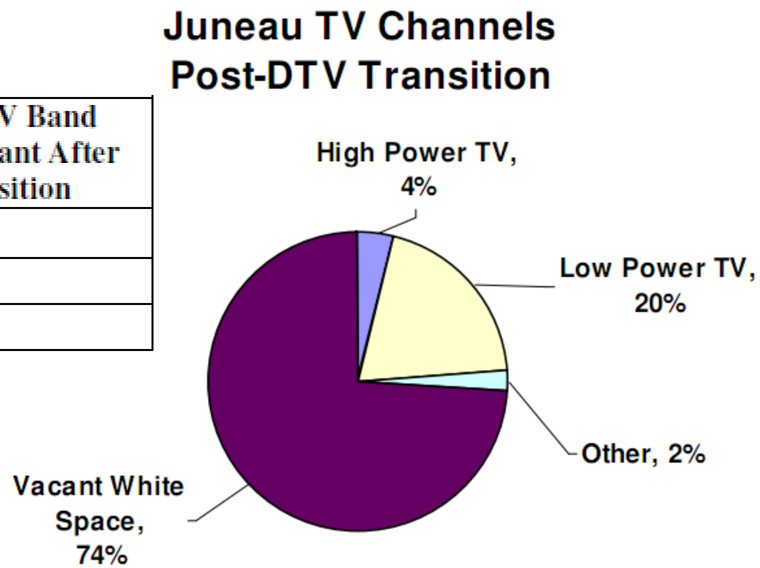
- **May 2004**: According to a Notice of Proposed Rule Making unlicensed radios are allowed to operate in TV bands as long as they don't interfere with TV services.
- So in **November of 2004,** a novel wireless air interface for WRAN (Wireless Regional Area Networks) started being developed using spectrum allocated for TV services.
- **Why use TV bands?**
  - Due to their propagation characteristics
    - It is possible to cover extensive areas in LOS and NLOS conditions at lower power levels.
  - **In suburban and rural areas there is a lot of "whitespace" in this spectrum**

Why IEEE started developing the 802.22 Standard(2/2)

- By using this protocol, suburban and rural areas can be provided with broadband/high speed internet access. This can be also used in developing countries, where these whitespaces are larger.
- Amount of whitespace will be great after the completion of DTV transition

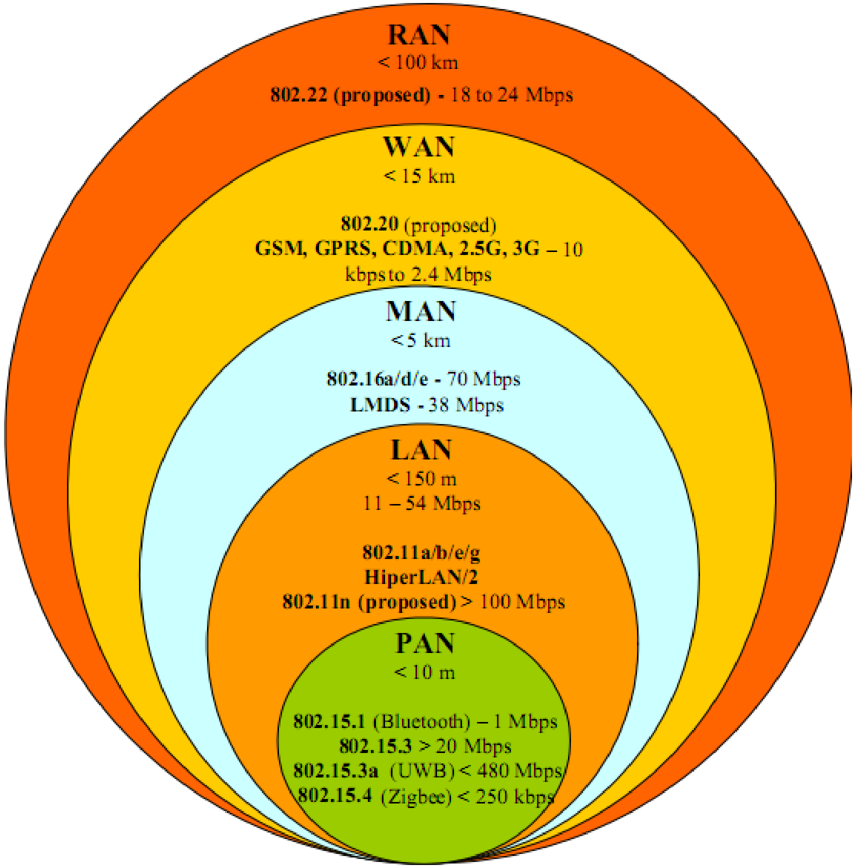
Market	No. of Vacant Channels Between Chs. 2-51 After DTV Transition	Percent of TV Band Spectrum Vacant After DTV Transition
Fargo, North Dakota	41	82%
Dallas-Ft. Worth, Texas	20	40%
San Francisco, California	19	37%

Source: New America Foundation and Free Press. Measuring the TV "White Space" Available for Unlicensed Wireless Broadband. 2007



IEEE 802.22 Characteristics

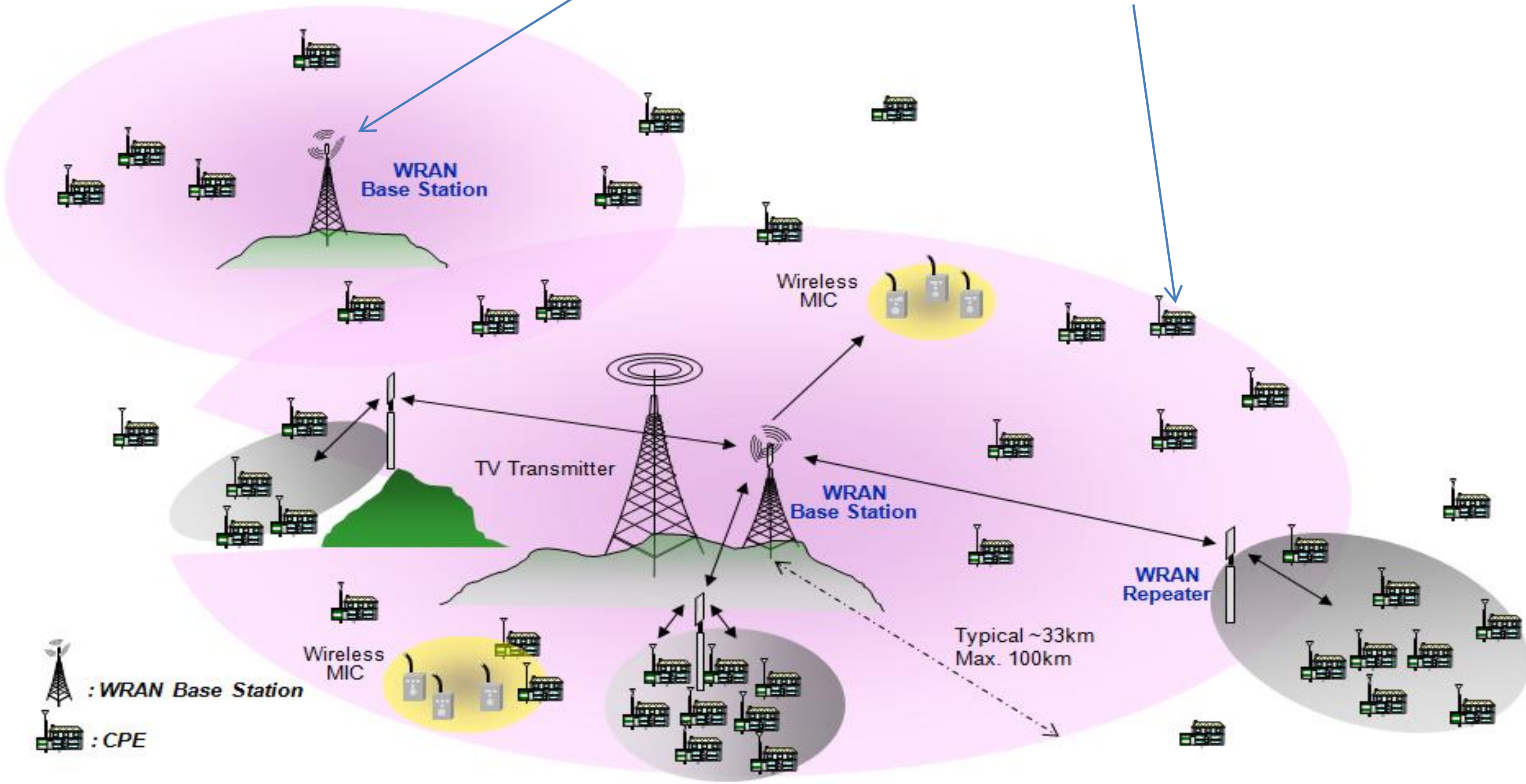
- Service Coverage: 33km– Up to 100km if power is not an issue.
- Use of TV channels of 6-8MHz bandwidth which provide a data rate of at least 18Mbps
- Main issue: Lack of interference with primary users.
  - That's why there are quiet periods, when sensing takes place.
- OFDMA modulation with channel bonding and multiple modulation schemes according to distance.
- MAC is based on 802.16 MAC



802.22 Entities

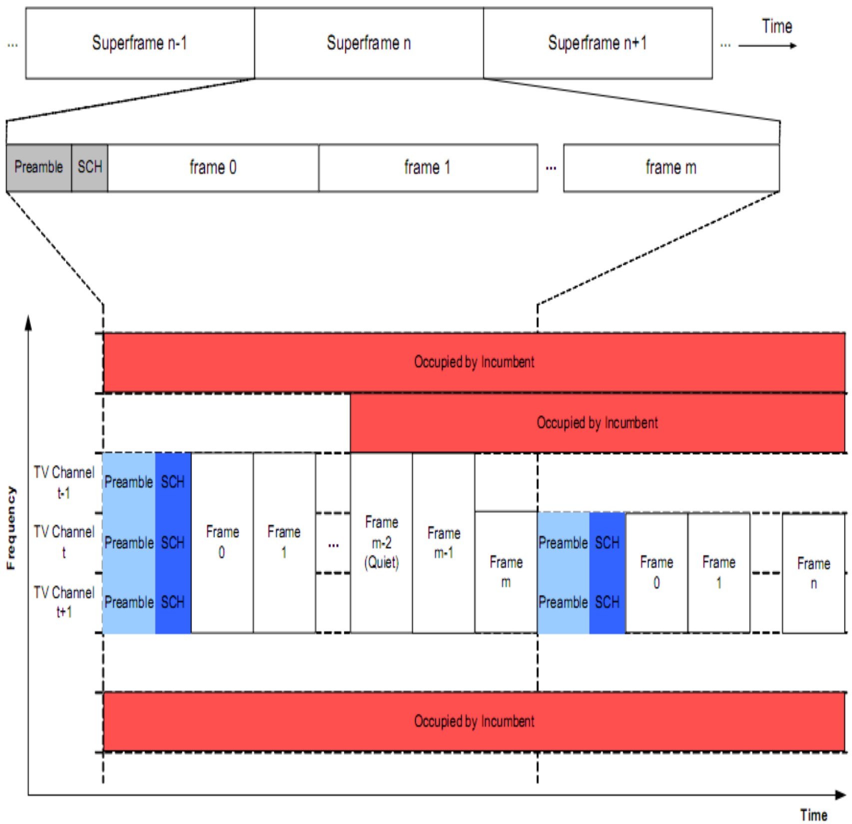
Controls all transmit parameters and network characteristics

Performs sensing of primary users under BS instructions

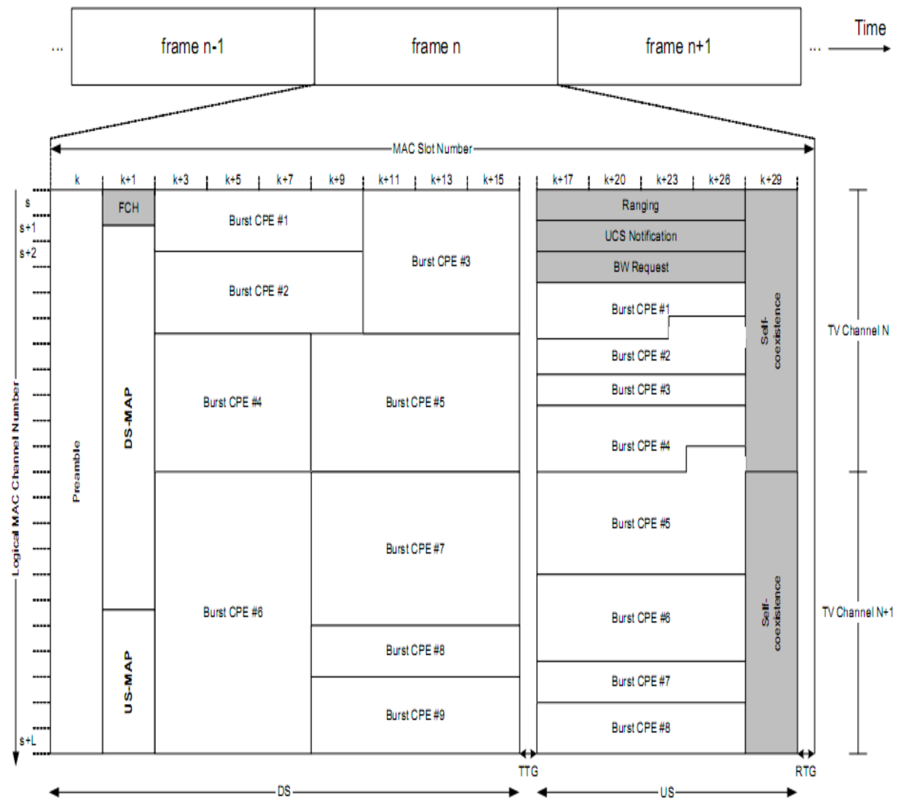


802.22 Superframe and frame structure

Superframe

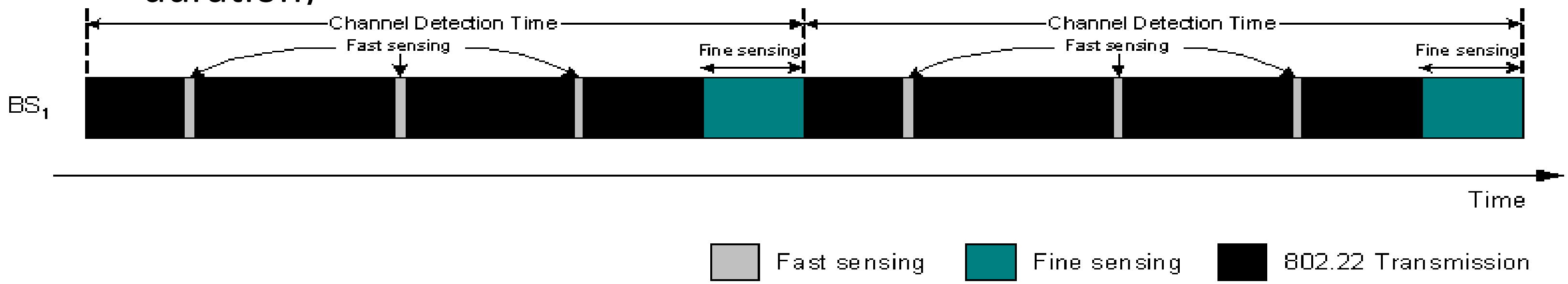


Frame



Quiet Period Management for Sensing

- Sensing is a two-stage process
  - Stage 1: Fast sensing (1 ms duration)
  - Stage 2: **Only if needed**, perform fine sensing (more detailed sensing – 25 ms duration)



- Fast sensing is performed in-band only
- If something is detected during the fast sensing stage, BS determines the begin of the fine sensing stage
- If a particular signature of a transmitted signal is detected during fine sensing, a BS performs an out-of-band sensing (detects an empty channel to continue transmission)

1. About IEEE 802.22
2. Developing the 802.22 module for NS2
3. Attack scenarios simulation

DEVELOPING THE 802.22 MODULE FOR NS2

Development process for 802.22 module for ns-2

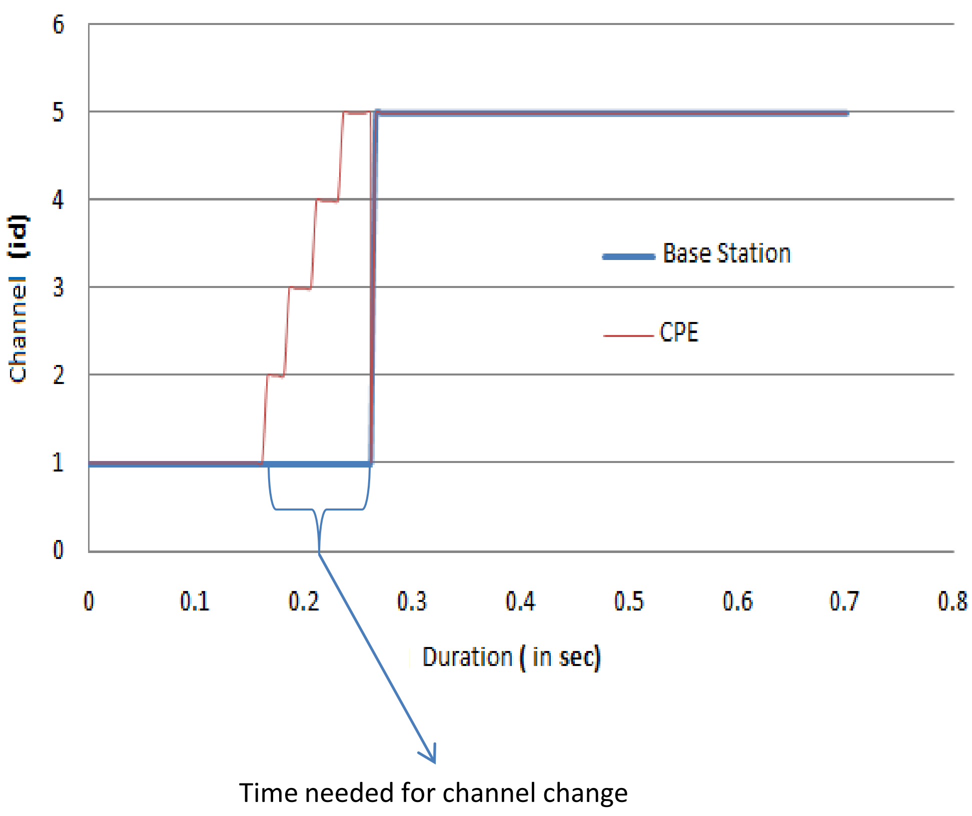
- **There is no module published/known for ns-2 for 802.22**
- There are a lot of similarities between 802.16 and 802.22
  - Develop the 802.22 module by extending an existing and simplified 802.16 module.
- We also studied two more 802.11 modules:
  - The one enhanced in ns2-34 in order to understand the development process and one developed by NIST.

Module functionality

- OFDMA parameters according to 802.22
- MAC level of 802.22
- Three types of sensing:
  – Simple sensing (Algorithm A)
  – In-frame sensing (Algorithm B)
  – Adaptive sensing (Algorithm C)
- Inter-cell channel sharing
- Synchronization

Interference avoidance

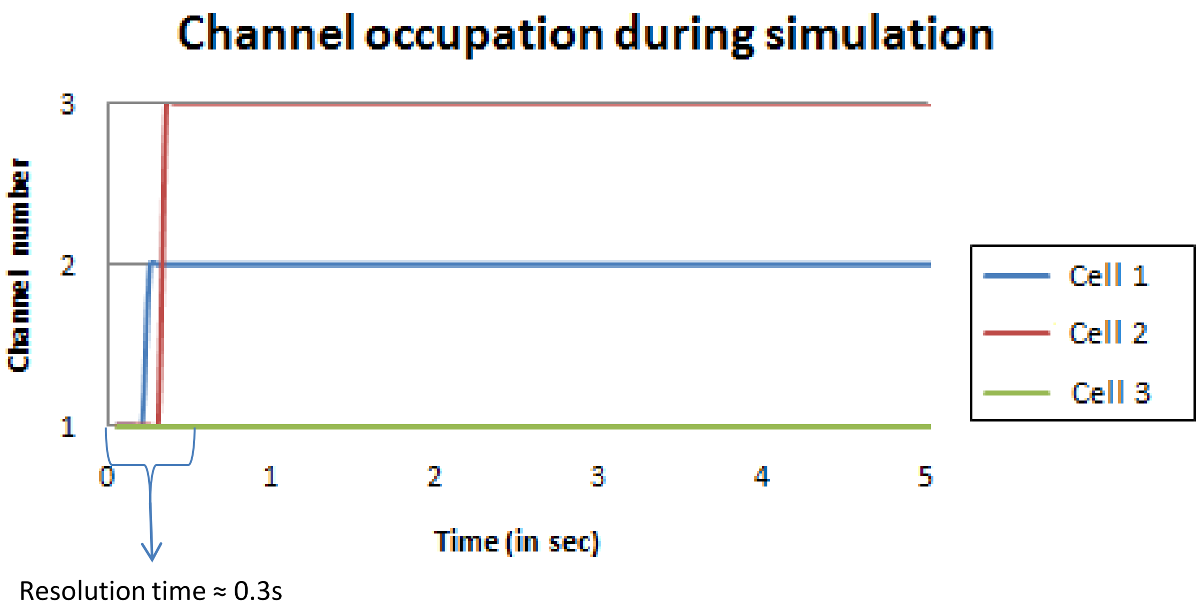
- Cell initiates channel scanning process in order to switch to a vacant channel
  - BS send SCANREQ message to a CPE which will search the spectrum serially.
  - CPE informs the cell about the presence of an unused channel to switch to.



Interference avoidance among multiple cells

- Providing that:
  - There are enough unused channels
  - There are multiple cells using the same channel in a specific area

  each cell switches to an unused channel.
- Cells must be coordinated about the channel change process.



Overhead of fast sensing in network's transmission data rate (1/3)

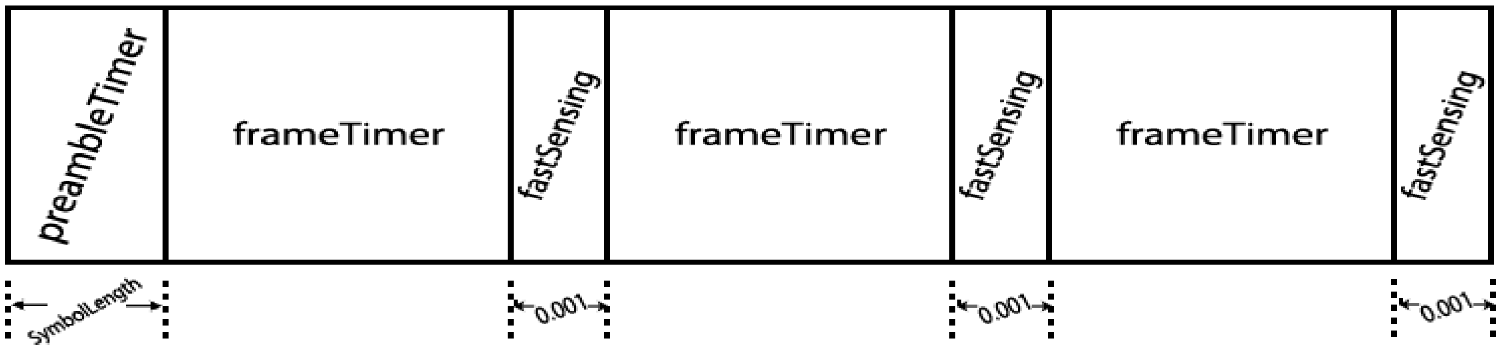
- Considering:
  - T_{sense} : duration of fast sensing
  - T_{frame}: duration of frame

  Then transmission efficiency can be computed as:

$$a = \frac{T_{frame}}{T_{frame} + T_{sense}}$$

Overhead of fast sensing in network's transmission data rate (2/3)

- However multiple fast senses can also be performed in each frame
- Frame is split to multiple parts

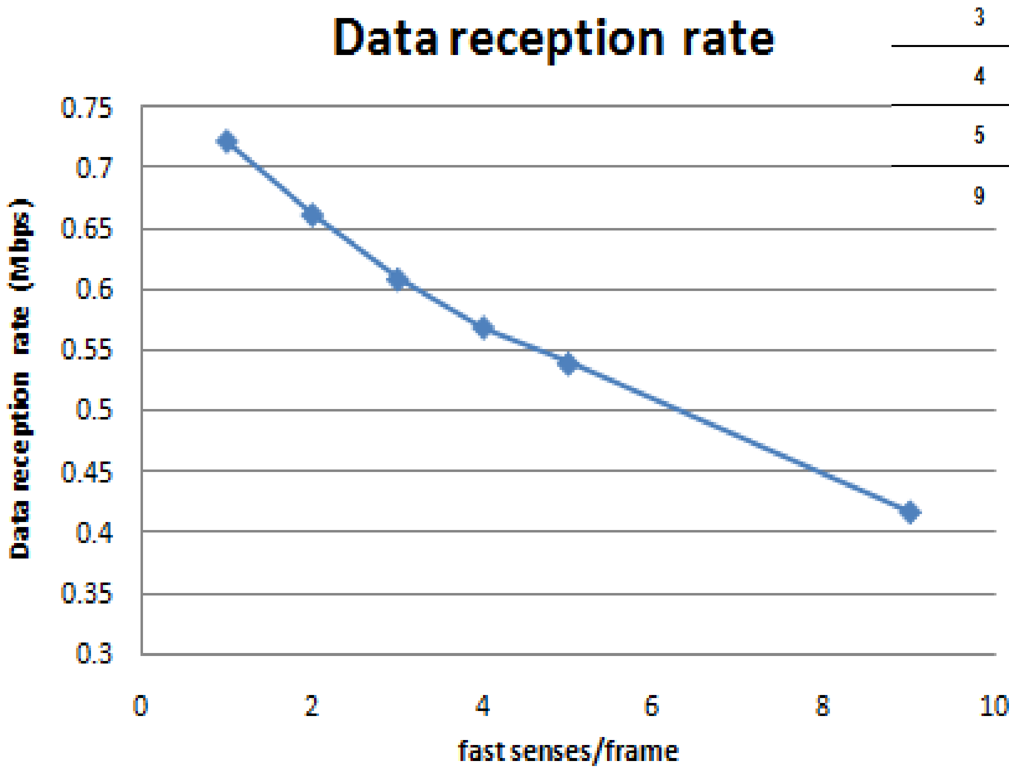


- Transmission efficiency (considering k senses/frame)

$$a = \frac{T_{FRAME}}{T_{FRAME} + k\,T_{SENSE}}$$

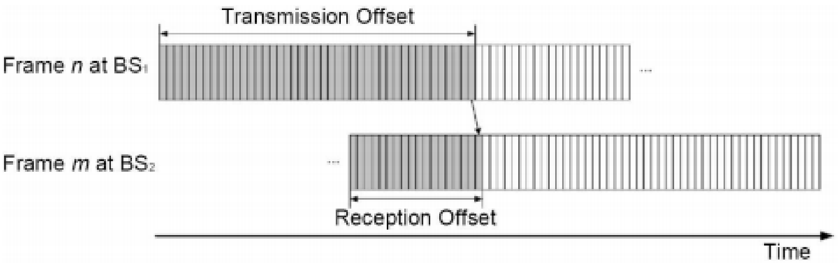
Overhead of fast sensing in network's transmission data rate (3/3)

senses/frame	Theoritical Efficiency	Experimental efficiency
1	0.9090909	0.9106364
2	0.8333333	0.8343505
3	0.7692308	0.7672188
4	0.7142858	0.7175240
5	0.6666667	0.6800349
9	0.5263158	0.5270270



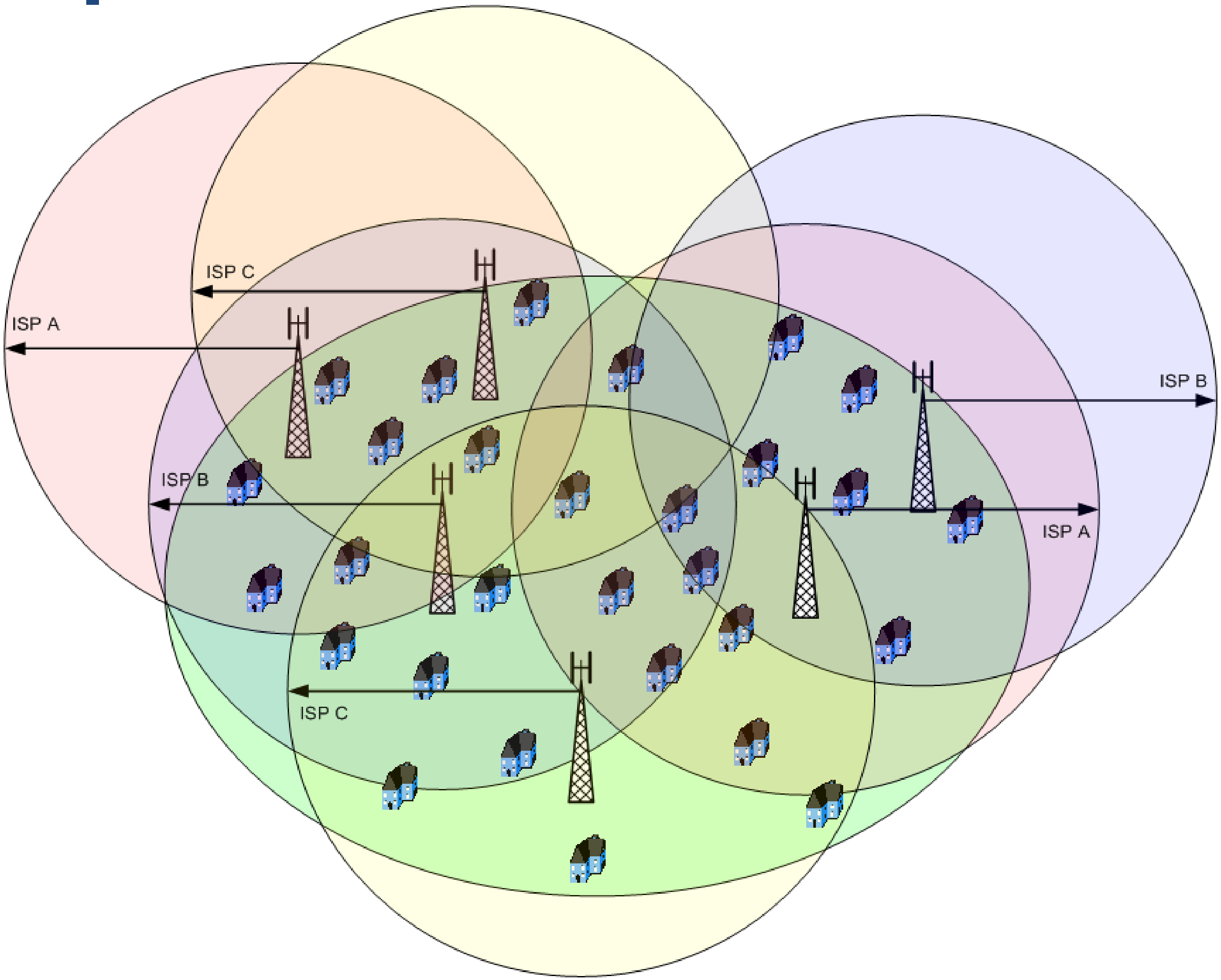
802.22 Inter-Cell Synchronization

- Synchronization of QPs for better detection of primary users with inter-cell beacons
  - E.g. two overlapping BSs, BS_1 and BS_2. BS_1 sends an inter-cell beacon to BS_2. BS_2 tries to slides frames with the following rule:
    - If (FDC – O_{T_x} + O_{R_v} ≤ ceil (FDC/2)), slide frames right by FDC – O_{T_x} + O_{R_v}
    - Else slide frames left by (O_{T_x} - O_{R_v}).
    - FDC: Frame Duration Code (time duration)



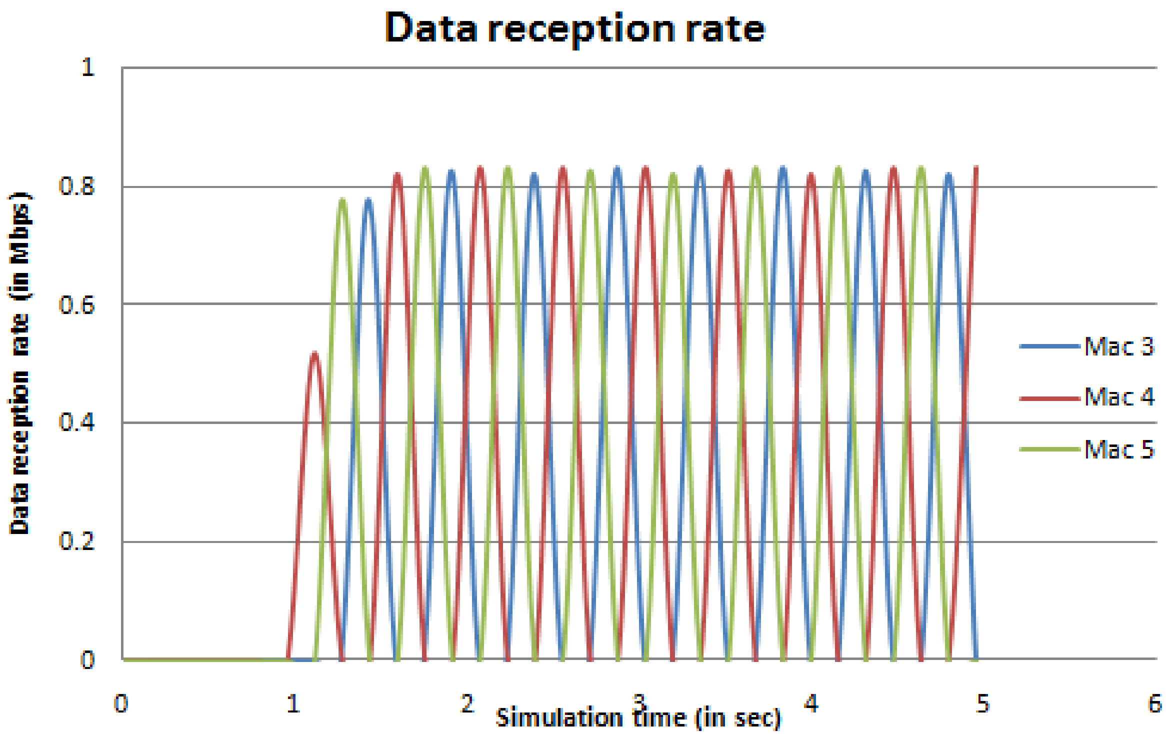
Source: Bian, K. and Park, J. 2008. Security vulnerabilities in IEEE 802.22.

Importance of self-coexistence



Channel sharing simulation (1/2)

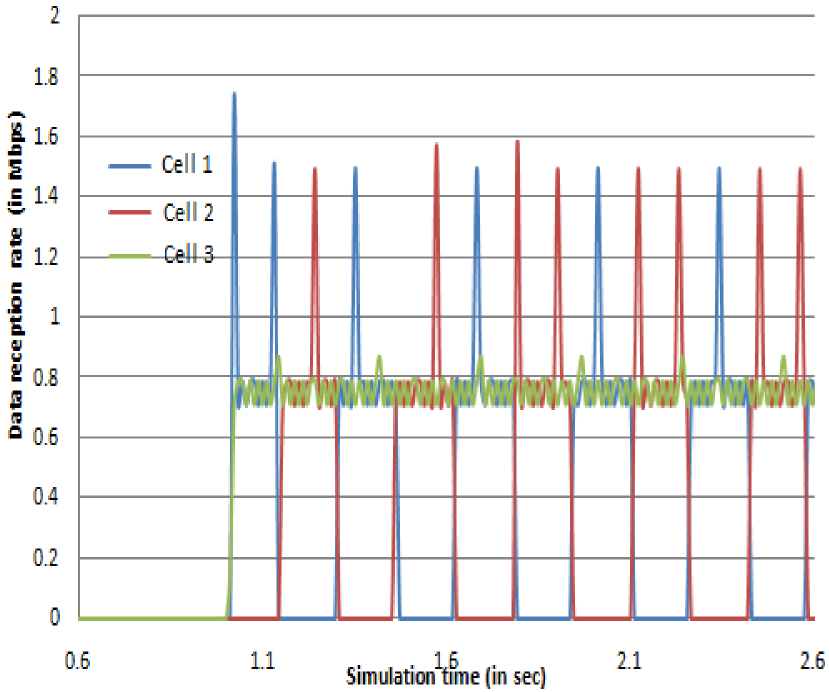
- If all available channels are used and overlapping cells cause low SIR to each other.
- In this case, synchronized cells can decide to share the same channel.
- Simulation scenario: Three cells in the same channel

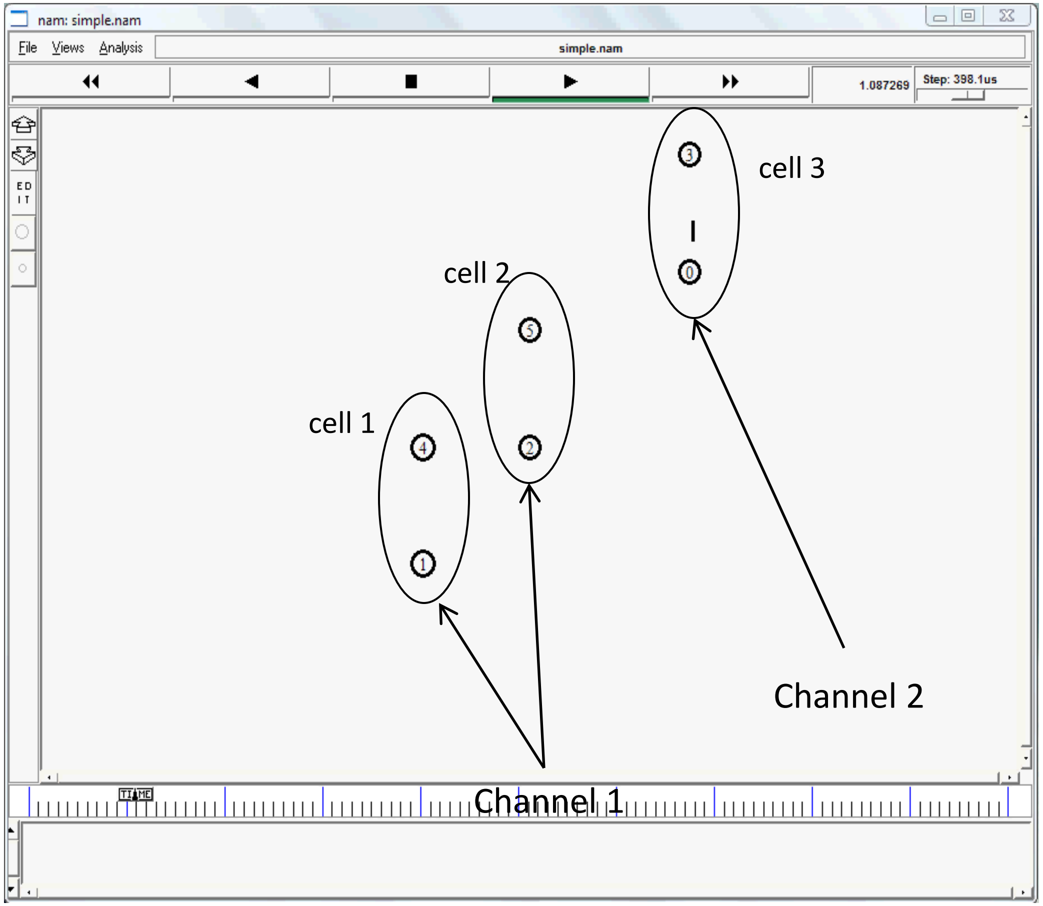


Channel sharing simulation (2/2)

If CPE finds out that there are no channels available, it changes back to original one and triggers the channel sharing process

Channel 1: 2 cells (channel sharing)
Channel 2: 1 cell (exclusive use)





1. About IEEE 802.22
2. Developing the 802.22 module for NS2
3. Attack scenarios simulation

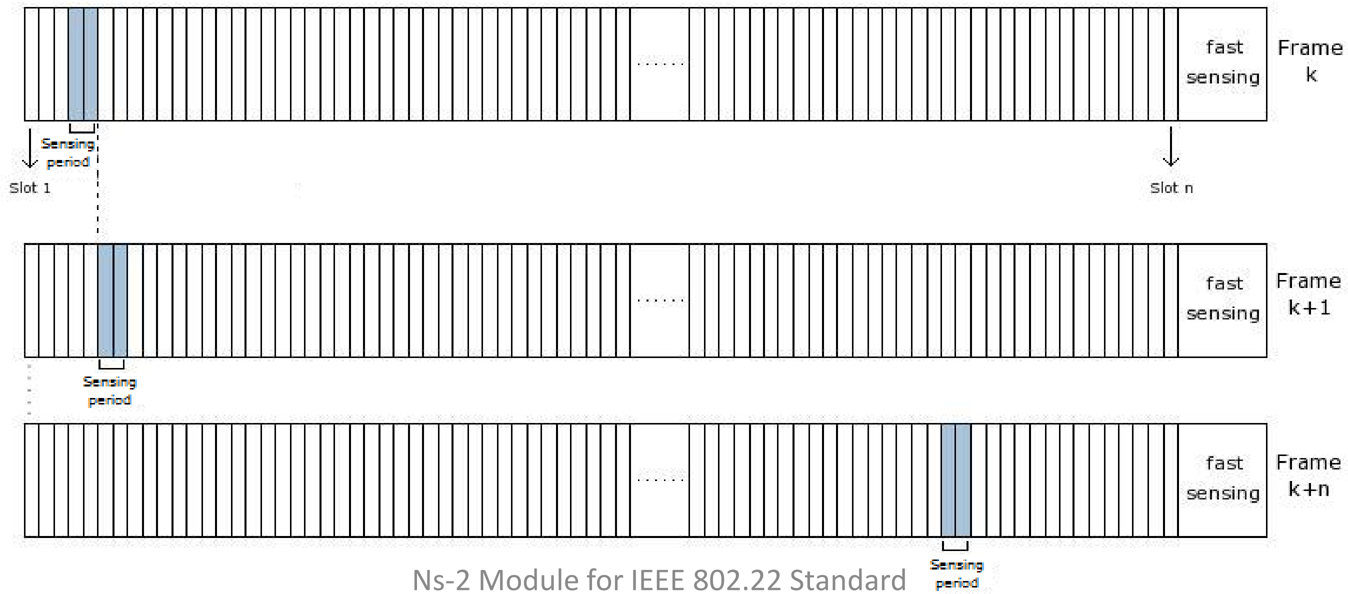
ATTACK SCENARIOS SIMULATION

Sensing vulnerabilities

- 802.22 is not immune to attacks
- An attacker is possible to predict quiet periods and avoid sending spurious packets
- Cell loses data in constant rate without detecting the attack
- Two countermeasures are proposed
  - In-frame sensing
  - Adaptive sensing

In-frame sensing (Algorithm B)

- In case of a collision:
  - Cell stops transmissions for a number of slots without changing the frame length.
  - At these slots all CPEs perform fast sensing
  - If a CPE detects energy then fine sensing is performed.
  - Sensing slots vary in time



Adaptive sensing (Algorithm C)

- In case of a collision:
  - All idle CPEs perform fine sensing at the slots collision occurred
  - Attacker must be detected from all CPEs performing the sensing.
  - After detection cell begins the channel change process.
- Energy consumption is an important factor.
  - Sensing cannot be performed in infinite time
  - Energy loss due to sensing shouldn't override energy loss caused by interference.

Sensing energy cost (1/2)

- Energy loss caused by interference:

$$aP_{RC} + 2(k-1)aP_{RC} = (2k-1)aP_{RC}$$

  - k: interference duration in frames
  - P_{RC}: Reception energy/slot
  - a: # of slots collided
- Energy loss caused by sensing

$$(2\lambda + 1)aP_{RC} + n\lambda(aP_{RC} + P_{RT})$$

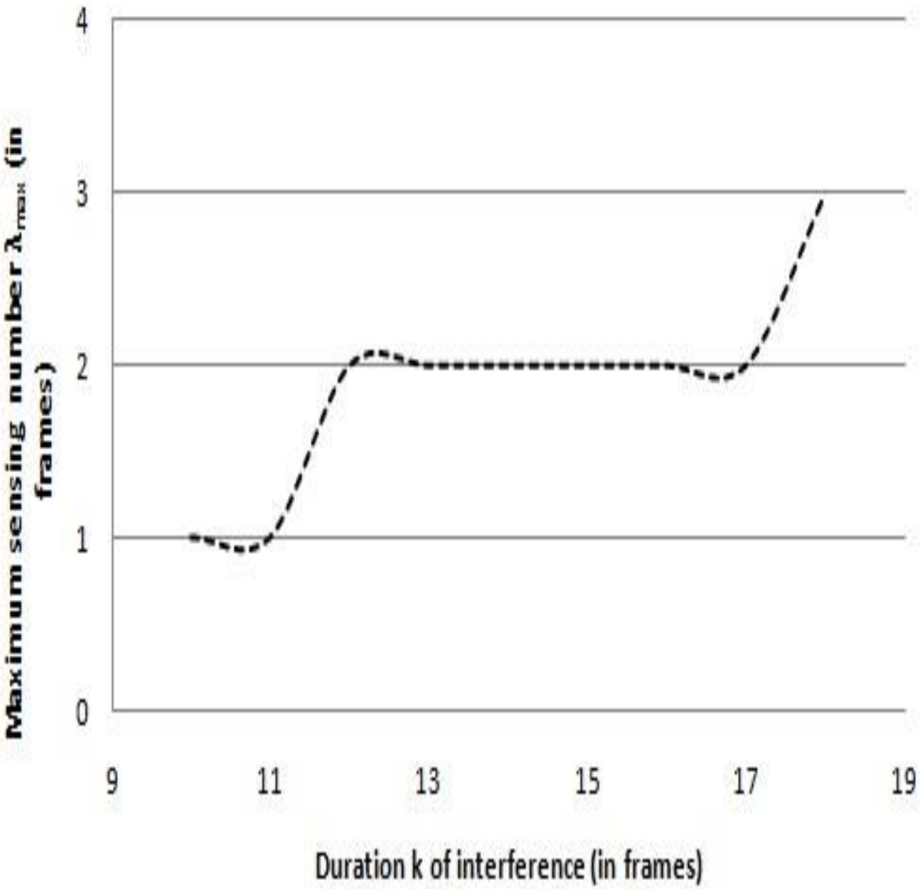
  - λ: frames where sensing takes place
  - P_{RT}: Reporting energy/frame

Sensing energy cost (2/2)

- Sensing should take place up to a level of λ frames:

$$\lambda < \frac{(2k - 2)a}{a(2 + n) + ni}$$

  - n: # of CPEs which perform sensing
- For the graph at the right assume:
  - n = 3 CPEs
  - a = 1 slot/frame
  - i = 2 ($P_{RT} = 2P_{RC}$)



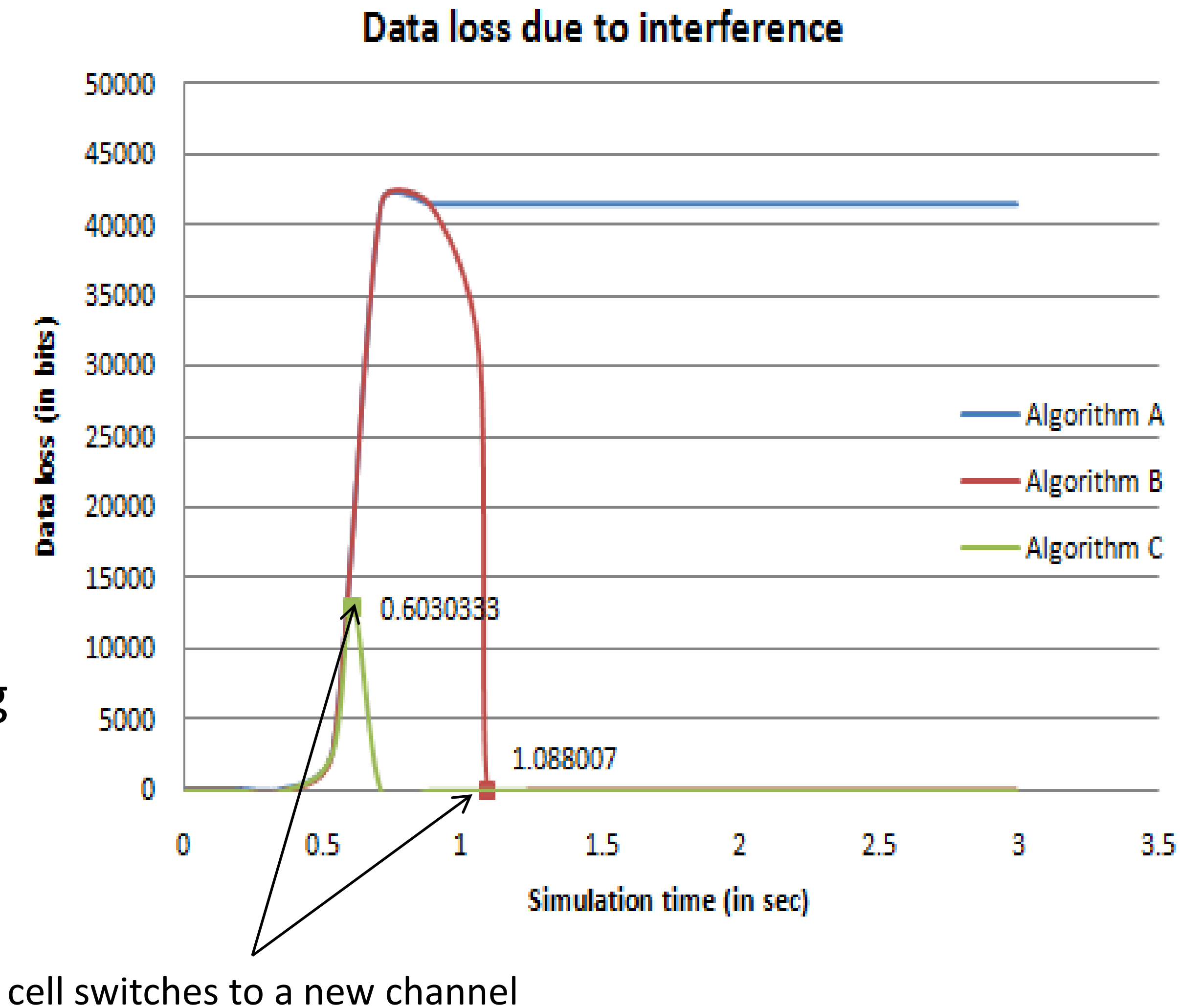
Simulation scenarios (1/2)

- Cell with one BS and 3 CPEs

- Attacker causes interference to the cell by sending packets in 3 contiguous slots

- Attacker avoids sending packets during fast sensing

- Victim: 1 CPE.



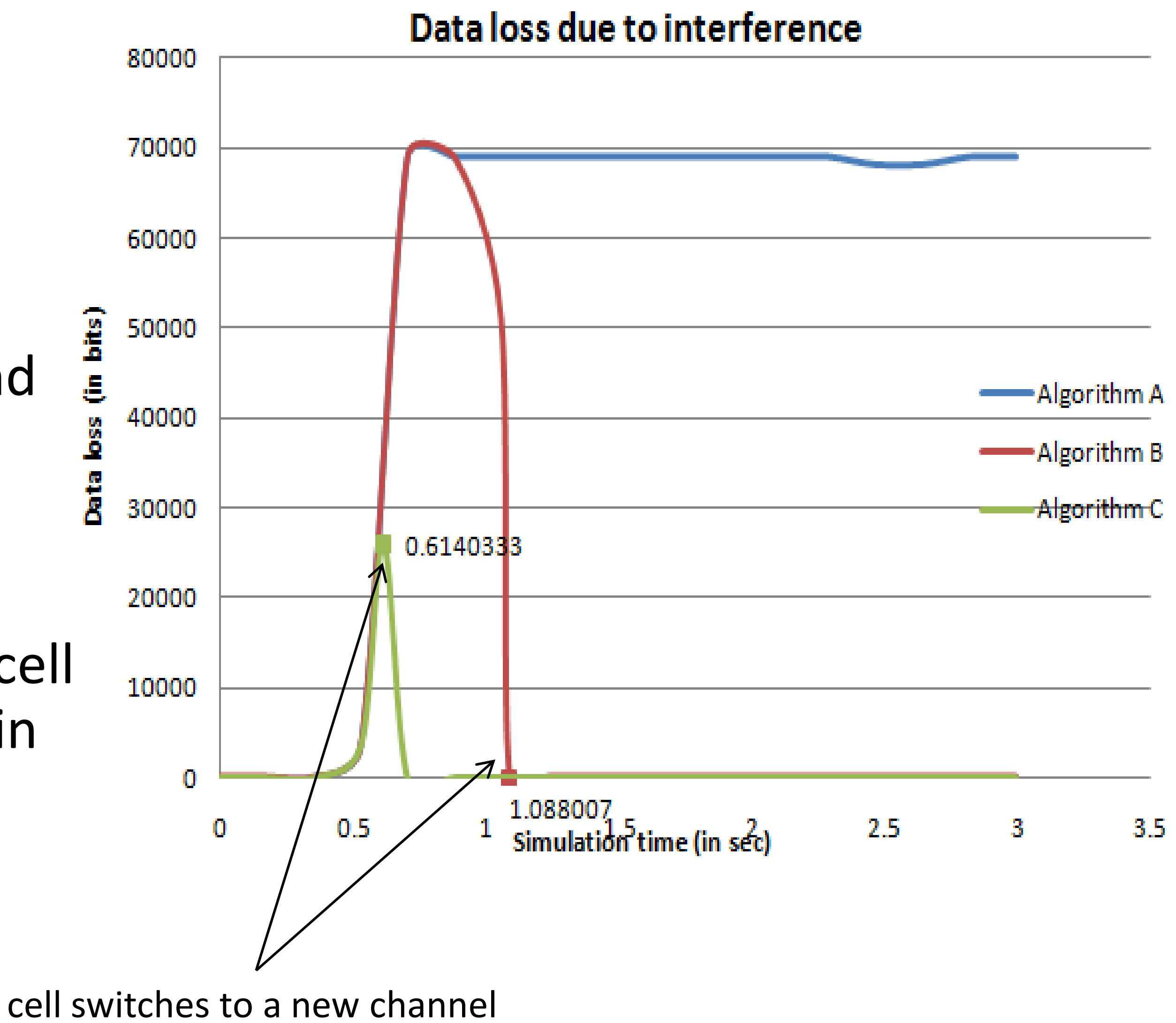
Simulation scenarios (2/2)

- Same concept as before

- Cell with one BS and 3 CPEs

- Attacker causes interference to the cell by sending packets in 5 random slots

- Victim: 2 CPEs.



Future Work

- Enhancements after standardization
- More types of sensing, including trust models
- Improve scheduling mechanisms in order to reward CPEs that perform sensing
- Improve channel sharing scheduling