Anti-jamming Timing Channels for Wireless Networks

Wenyuan Xu
Department of Computer Science and Engineering
University of South Carolina

Professor Wade Trappe and Yanyong Zhang
WINLAB

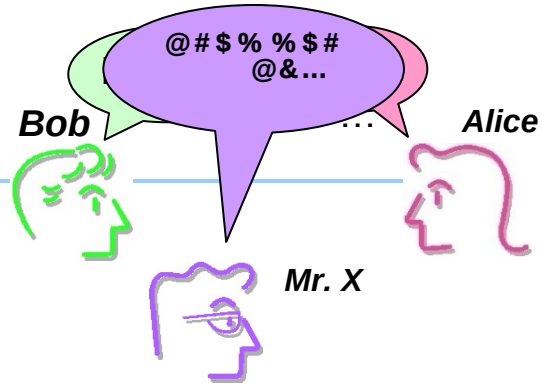
IAB, Dec. 3th, 2007

UNIVERSITY OF SOUTH CAROLINA

Roadmap

- Introduction and motivation
- Jamming / radio interference
  - Observations
- Timing channel
  - Two party prototype
  - Multiple senders
- Ongoing work & Conclusions

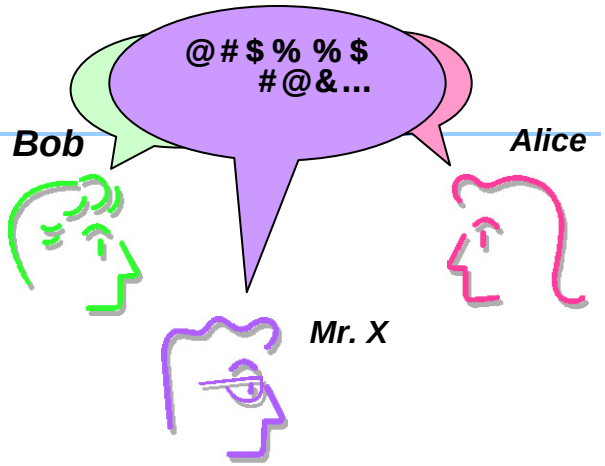
Jamming or Interference



- *Jamming:*
  - *Behavior that prevents other nodes from using the channel to communicate by interfering with the physical transmission and reception of wireless communications*
- *Unintentional jamming:*
  - Co-existing devices: 802.11b/g interferes with cordless phone, Bluetooth, Microwave oven...
  - Equipment accidentally emits a signal on an frequency band that does not belong to it.

- *Intentional jamming:*
  - A transmitter, tuned to the same frequency as the receiving equipment, can override any signal with enough power

Defense Strategies



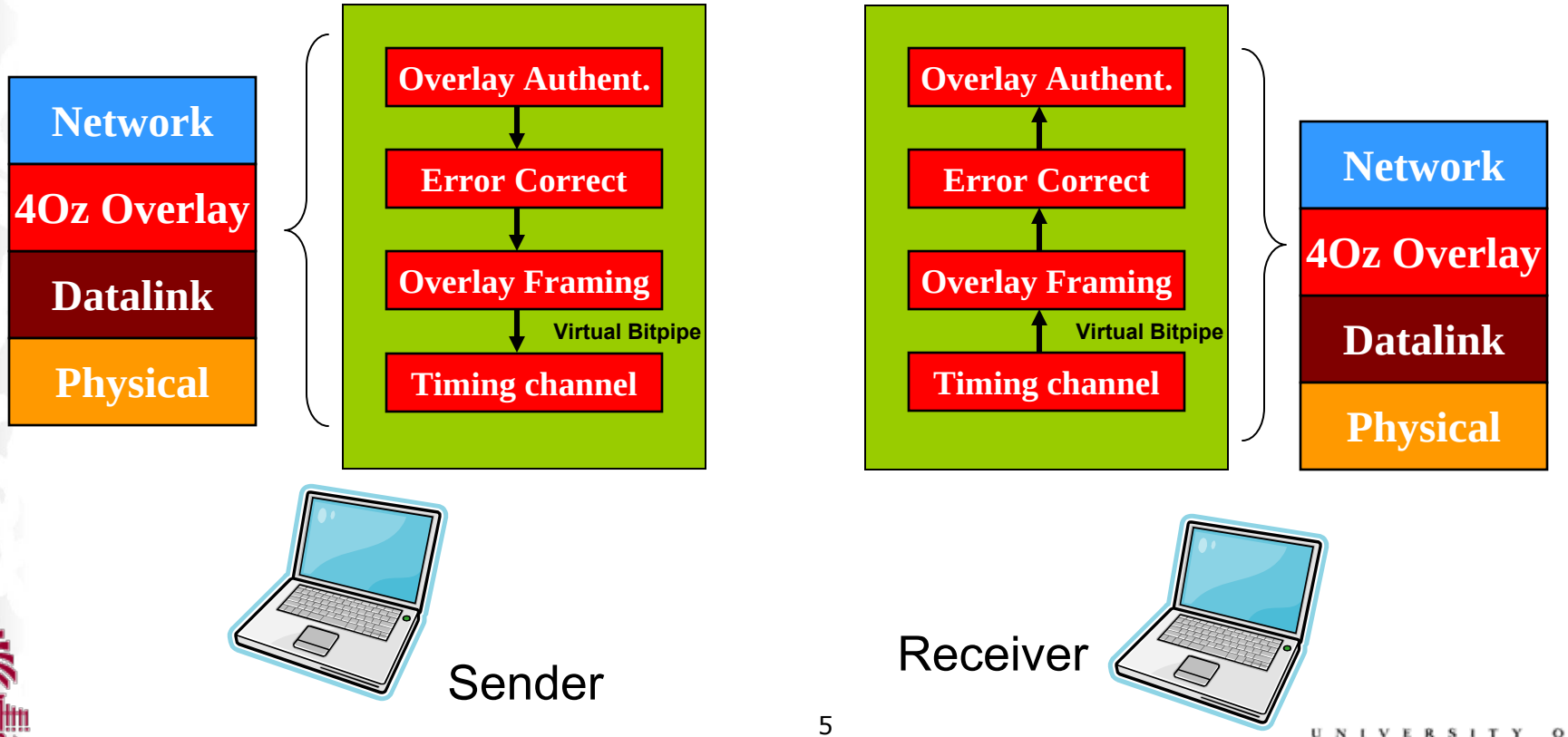
- *Goal:*
  - Convey information between Bob and Alice in the presence of Mr. X, the interferer.
  - Using existing wireless platforms (CSMA)

- Possible Strategies:
  - Channel Surfing -> interference-free channels available
  - Spatial retreat -> mobile wireless nodes
  - Power control -> increase transmission power

- What can you do if:
  - No interference-free channels are available.
  - Mobility is not an option.
  - You cannot over-power the jammer
  - You have a *short emergency* packet to send

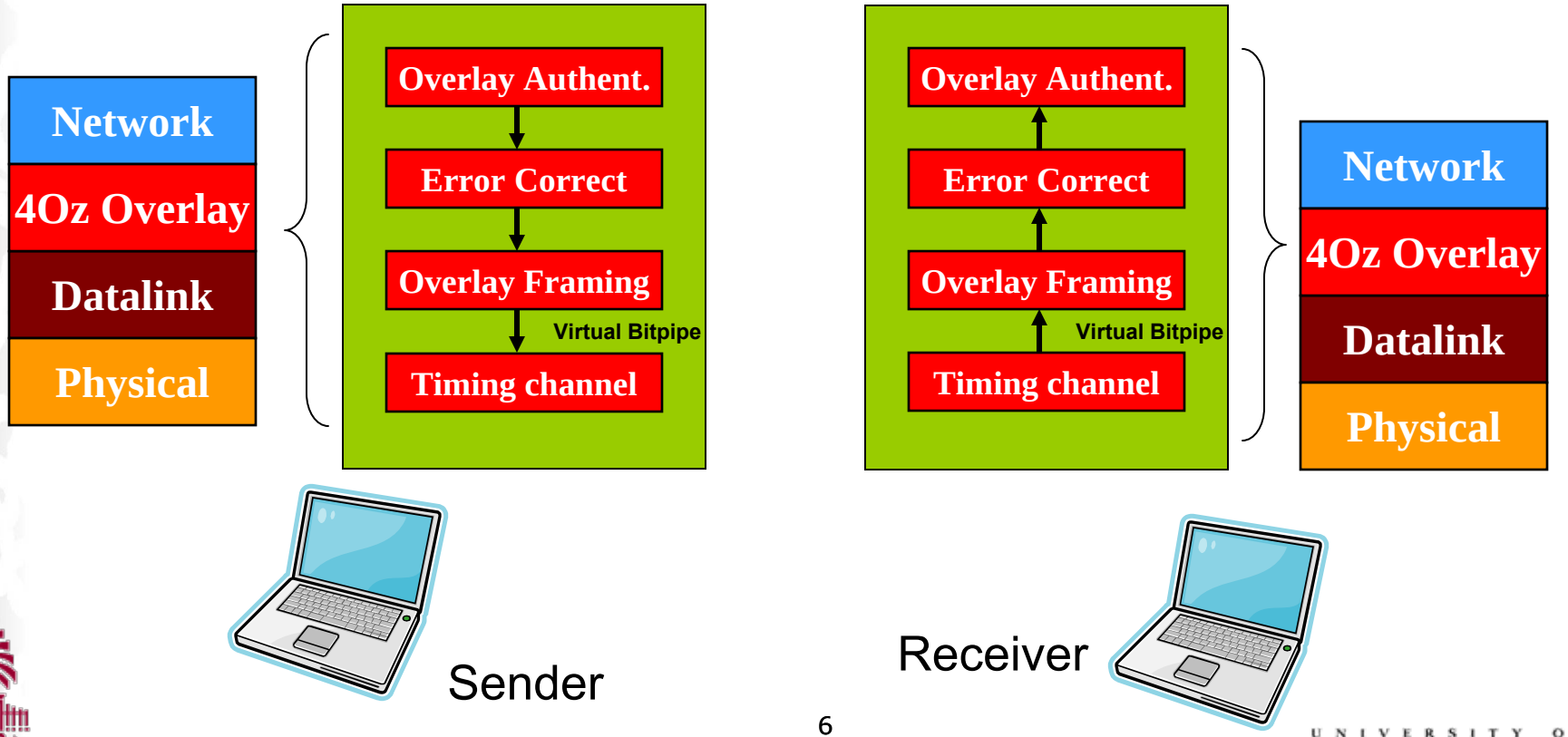
Timing Channel

- Idea:
  - Alice and Bob: Alice did not know exactly what Bob was saying, but she knew that Bob said something by looking at *his lip movements*.
  - Wireless network: exploit the fact that there was an attempted, incoming packet to convey information.



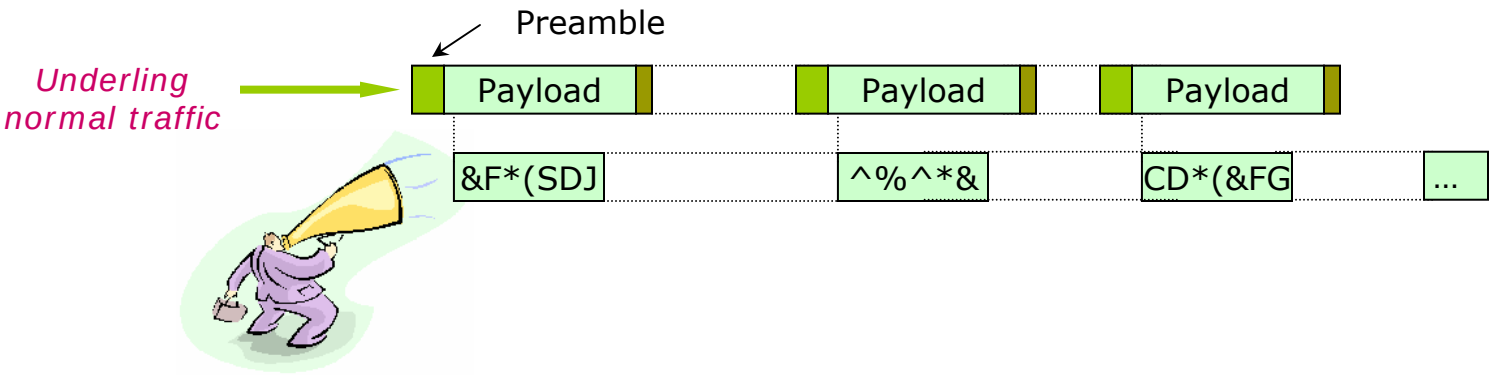
Timing Channel

- Sub-problems:
  - Can you detect a packet in spite of the radio interference?
  - Can you modulate the events of incoming packet?
  - Can you implement such a strategy in a real system?



Can you detect a packet in spite of the failed packet reception?

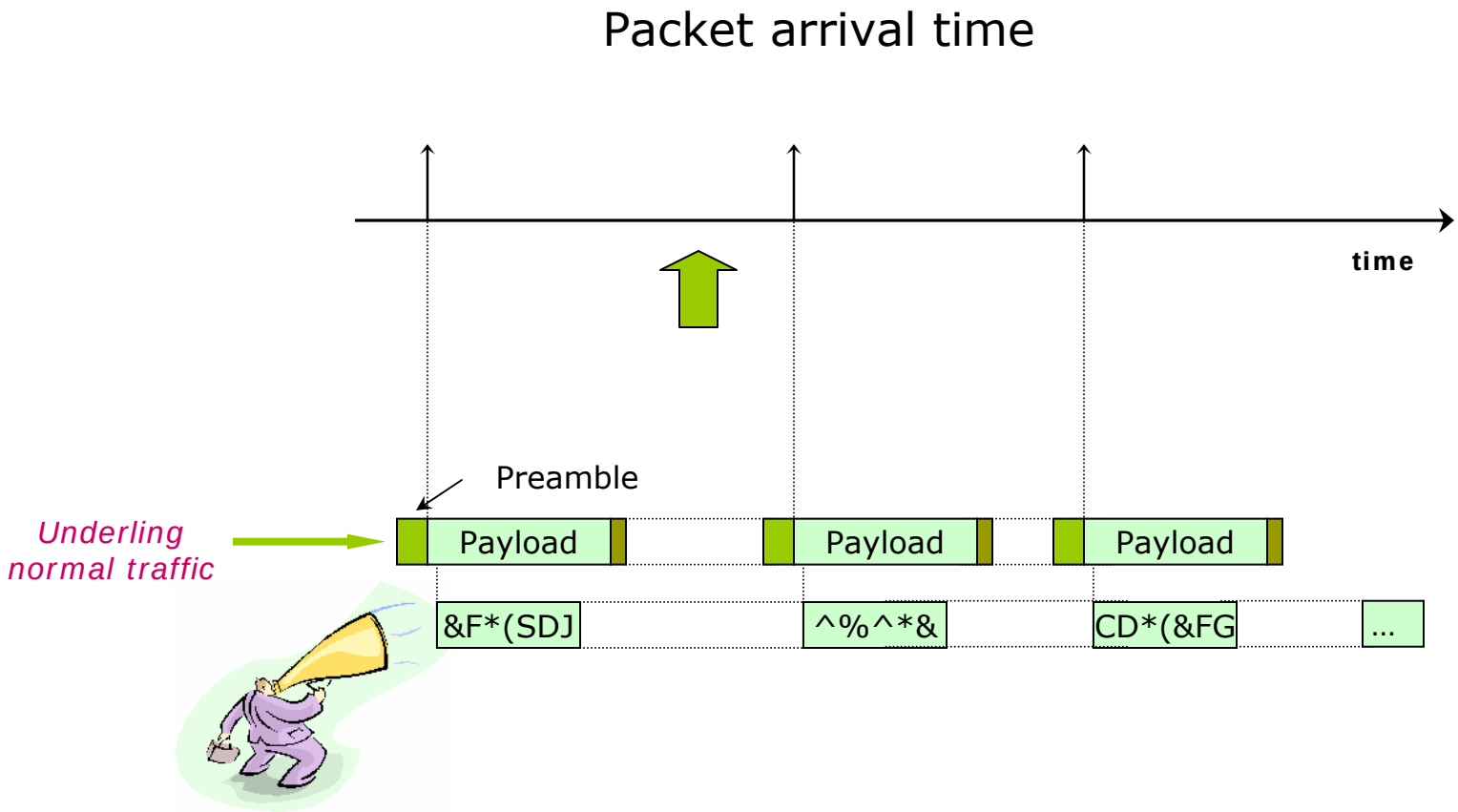
Malicious Jammer



- Reactive jammer:
  - Stays quiet when the channel is idle, but starts jamming as soon as it senses activity on the channel.
- Observation
  - CANNOT decode packets correctly
  - Preamble CAN be detected correctly by the receiver

d_{jr} (feet)	1	2	3	4	6	8
PDR(%)	0.10	0.70	0.15	98.65	100	99.85
DR(%)	99.80	99.80	99.60	99.95	99.65	99.95

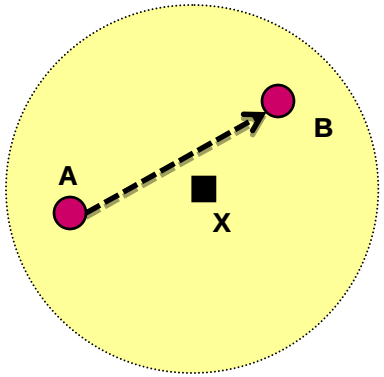
Packet Arrival Times



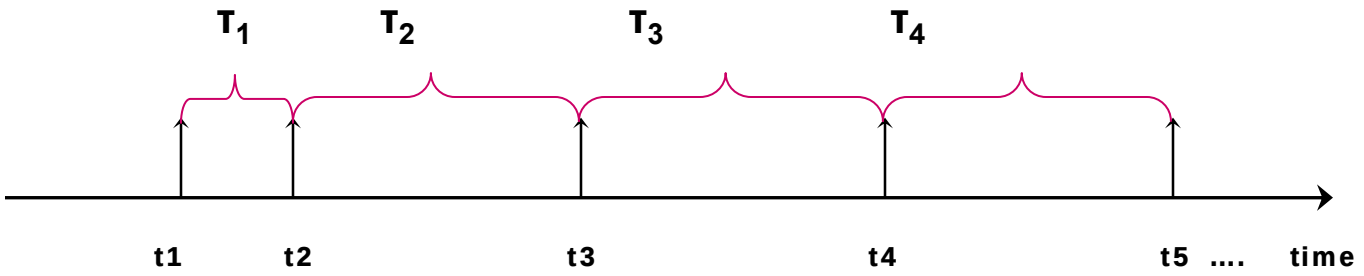
How to modulate inter-arrival time?

Two Party Prototype

- Two party scenario
  - A: Sender
  - B: Receiver
  - X: Interferer

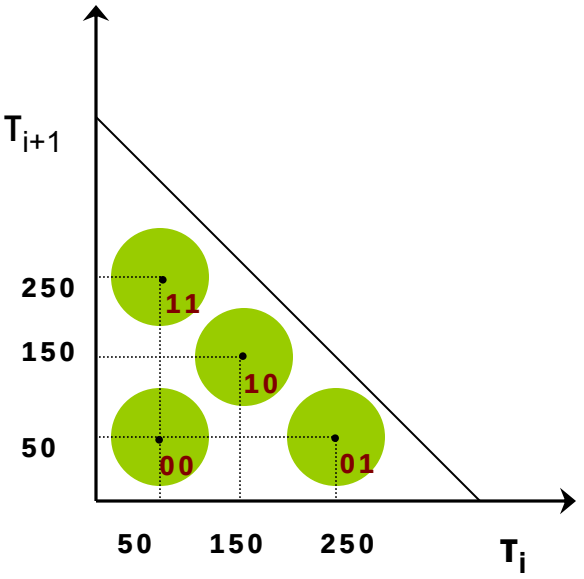


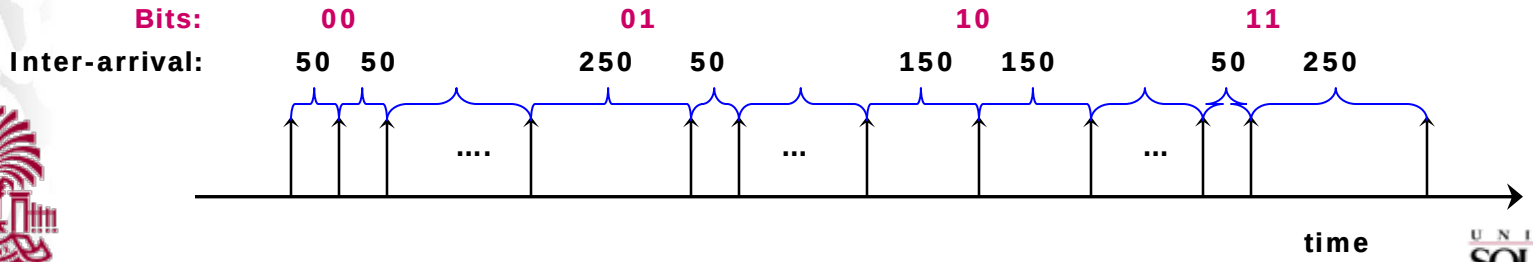
- What B observes:
  - t_i: the arrival time of the i^{th} packet
  - τ_i: the inter-arrival time, $\tau_i = t_{i+1} - t_i$



Example of Inter-arrival Time Coding

- Use (τ_i,τ_{i+1}) to code 2-bit symbols
  - Triangular simplex
  - Each circle represents 2 bits
    - (50,50) -> 00
    - (250,50) -> 01
    - (150,150) -> 10
    - (50,250) -> 11
  - Sender *encodes*:
    - 00->(50,50)
    - Send pkts at time 0, 50 & 100
  - Receiver *decodes* (nearest neighbor):
    - Receive packets at 0, 50 and 100
    - Get inter-arrival time pair (τ_i,τ_{i+1})=(50,50)
    - (τ_i,τ_{i+1}) -> Calculate the Euclidean distance

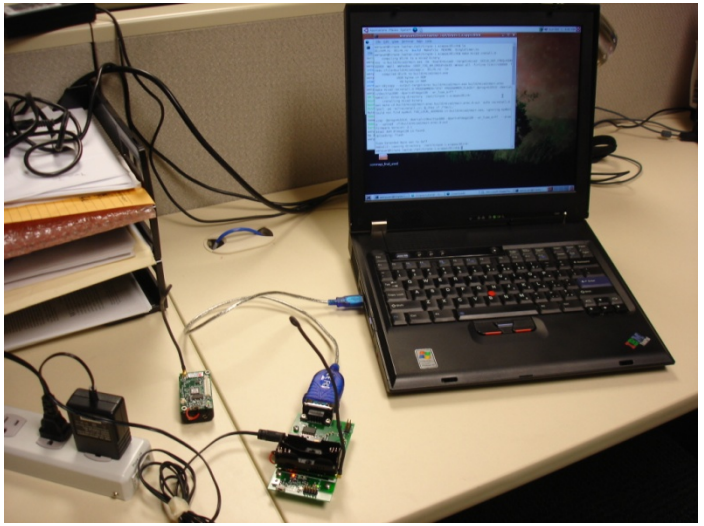




UNIVERSITY OF SOUTH CAROLINA

Experimental Validation

- Mica2 Motes
  - 8-bit CPU at 4MHz,
  - 128KB flash, 4KB RAM
  - 916.7MHz radio
  - OS: TinyOS

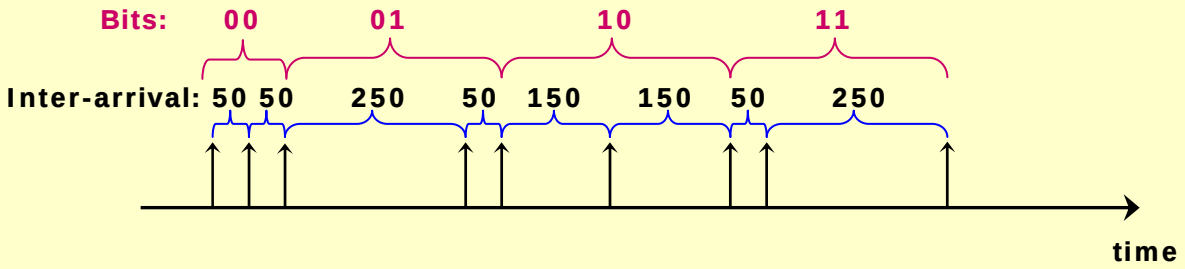


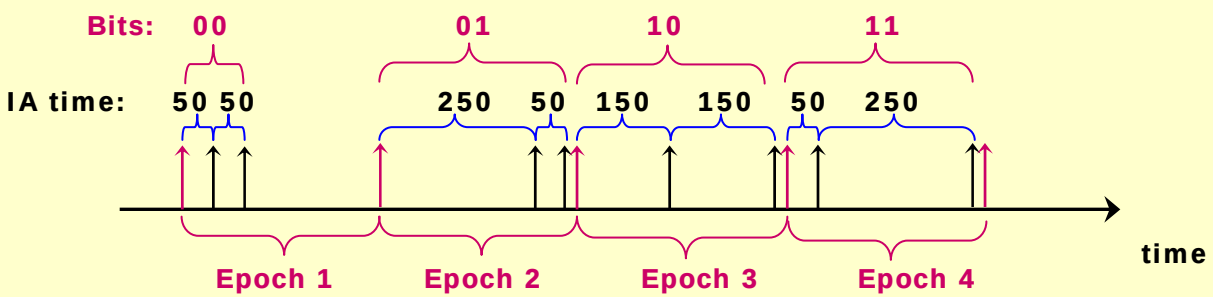
- Three nodes:
  - Sender:
    - Send 00, 01, 10, 11, 00…
  - Receiver
  - Interferer: Reactive jammer

- *Challenges:*
  - Jitter
    - *disable carrier sensing and back-off*
    - *code design*
  - Clock skew
  - *How to achieve efficient symbol streaming through the timing channel?*

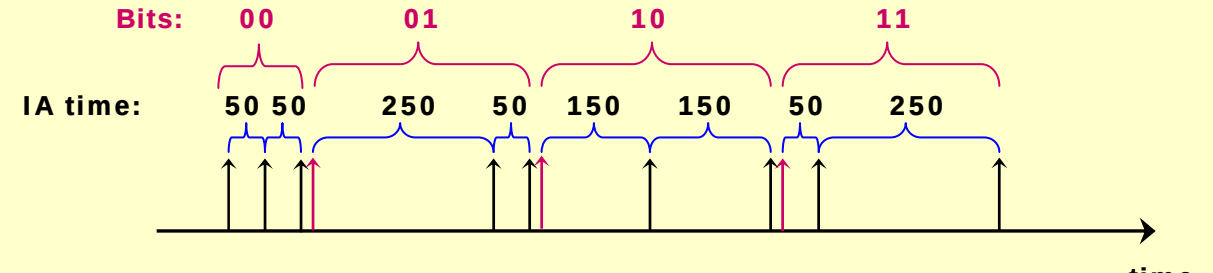
Symbol Streaming Strategies

Back-to-back streaming





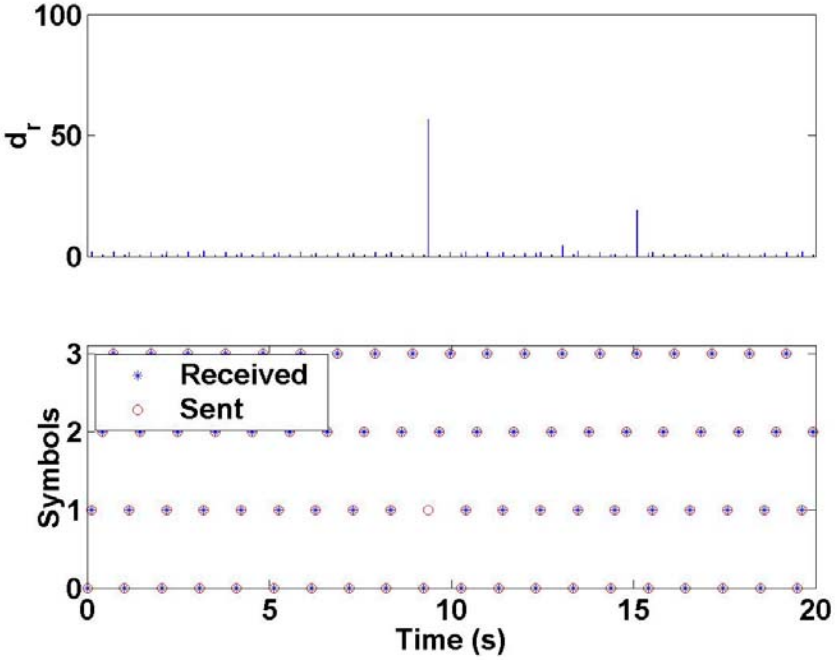
Fixed interval streaming

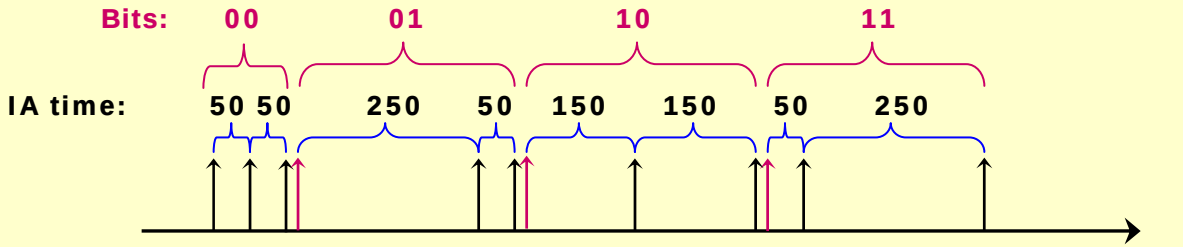


Marker streaming

UNIVERSITY OF SOUTH CAROLINA

Symbol streaming strategies

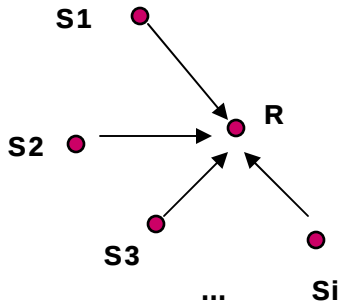


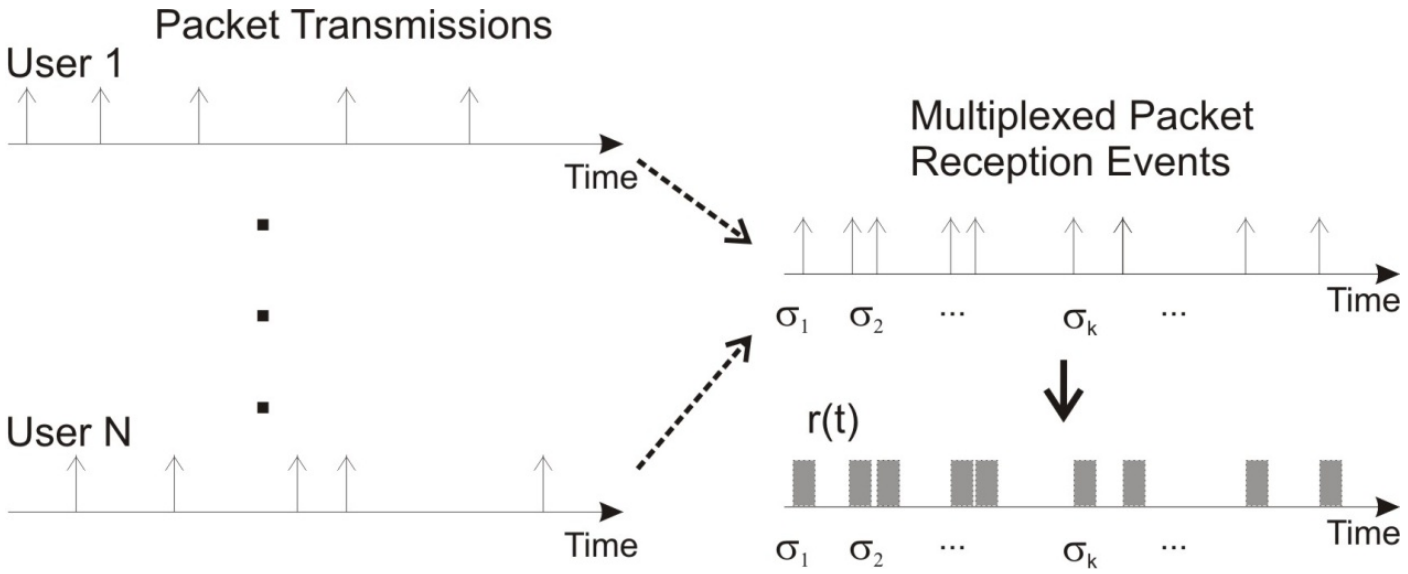


Marker streaming

Multiple Senders

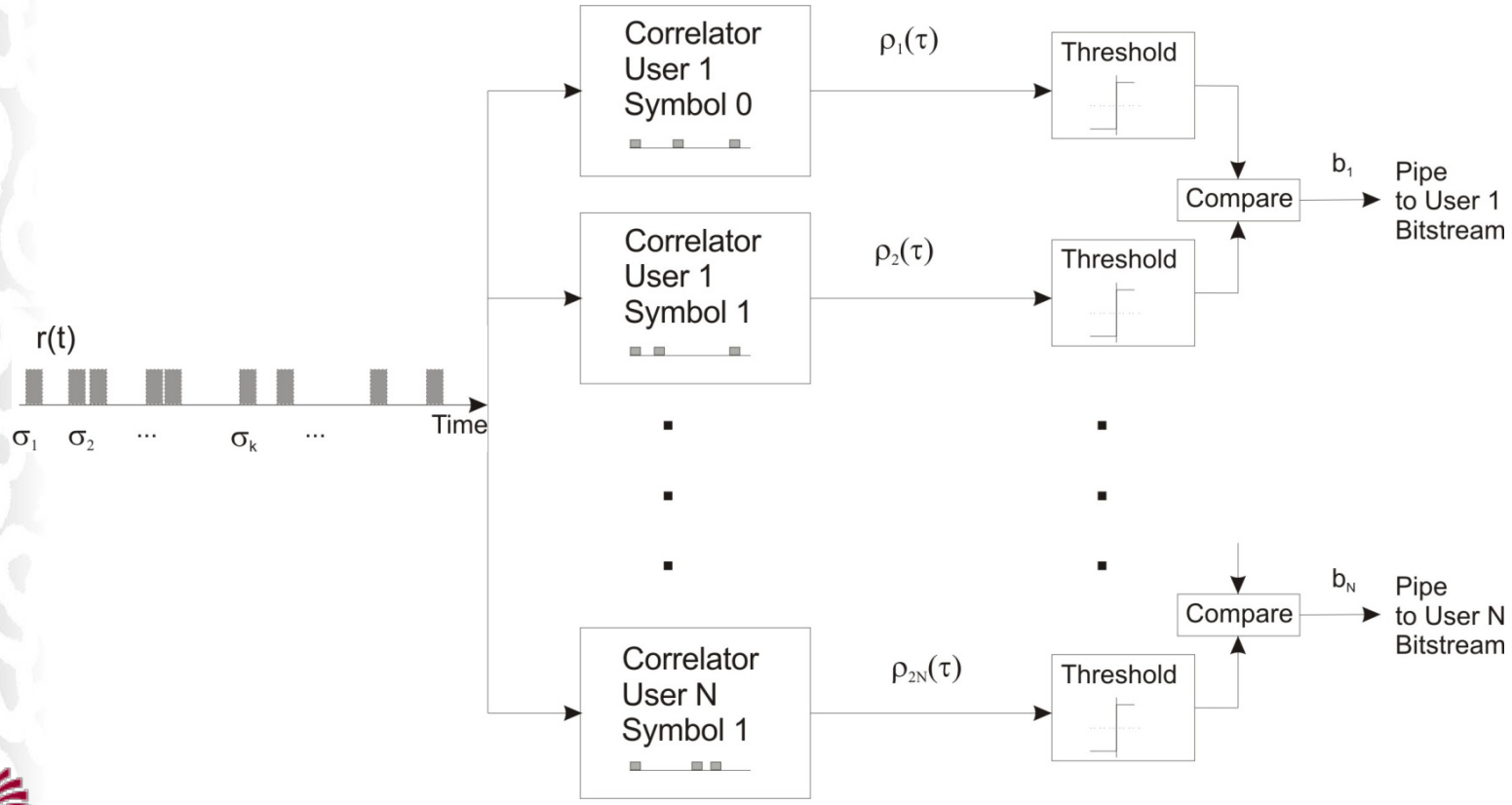
- Challenges:
  - Packets from various receivers interleave with each other
  - Extract individual sender's communications from the mixed packet arrivals at the reciever





Multiple Senders

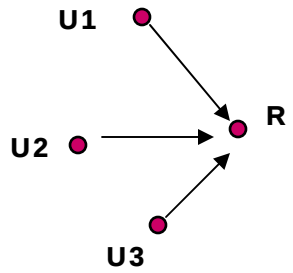
- Idea: design transmission sequences based on optical orthogonal codes (OOC)
  - The cross-correlation between different code words is very small
  - The auto-correlation is high



UNIVERSITY OF SOUTH CAROLINA

Experimental Validation

- Setup-5 MICA2 motes
  - Senders -u1, u2 & u3
  - One receiver R
  - One reactive jammer



- OOC code (37, 3, 1)

- Scenarios:
  - u2 and u3 sent, u1 remain silent
  - u1, u2 & u3 send

- Each user sends out 650 symbols, the receiver tries to decode and calculate the symbol error ratio.

Table1: Codewords

User	Symbol 0	Symbol 1
u1	{0, 1, 11}	{0, 2, 9}
u2	{0, 3, 17}	{0, 4, 12}
u3	{0, 5, 18}	{0, 6, 12}

Table2: The symbol error rate

Scenarios	u1	u2	u3
(u2, u3)	0%	0.64%	0.48%
(u1, u2, u3)	0.15%	0.31%	0.46%

Challenge & Ongoing Work

- Multiple-users:
  - We would like to have OOC's that are not based on a slotted time system
  - General continuous code design is underway
  - Looking for alternative modulation schemes
- Putting it together:
  - Further in the future: integrating into a holistic ad hoc network system where only small portions of network are jammed

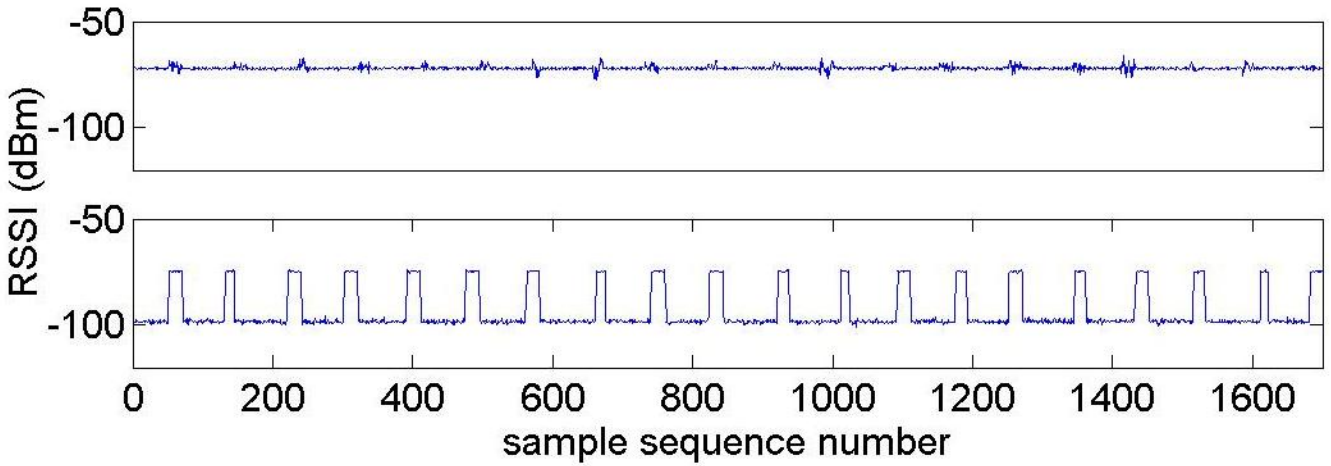
Thank you!

Questions?

UNIVERSITY OF SOUTH CAROLINA

Unintentional Radio Interferer

- Constant Interferer:
  - Continuously emits a radio signal
- Observation:
  - Bob CANNOT decode packets correctly
  - Bob MAY observe the *spikes*, representing the presence of packet on the air….
  - The ability to observe the spike depends on the transmission power levels of the sender and interferer and the sensitivity of the receiver.



Jamming or Radio Interference

- Observation
  - CANNOT decode packets correctly
  - CAN observe the *presence* of a packet
- Information: packet-arrival time → inter-arrival time
- Idea:
  - Using inter-arrival time to build a *timing channel*
  - Modulate inter-arrival time