# Detection of Transient in Radio Frequency Fingerprinting Using Signal Phase

Jeyanthi Hall

Ph.D. Candidate - Carleton University

Michel Barbeau and Evangelos Kranakis

(MITACS, NSERC, CITO and DREO)

# Problem

- Authentication Protocols in Bluetooth and 802.11b
  - authenticate **devices** at link-layer using **shared secret key**
  - exhibit significant vulnerabilities

# Potential Solutions

- Authentication (user) using higher-layers e.g. VPNs (network-layer)
  - drawback: does NOT address device authentication
- Biometrics
  - user authentication (fingerprint, iris, voice)
  - **device authentication (fingerprint of transceiver) -** Non-malleability of Identity

# Potential Applications of RFF

- Authentication of wireless devices
  - More robust access control (Access Points)
- Intrusion Detection Systems
- Other applications

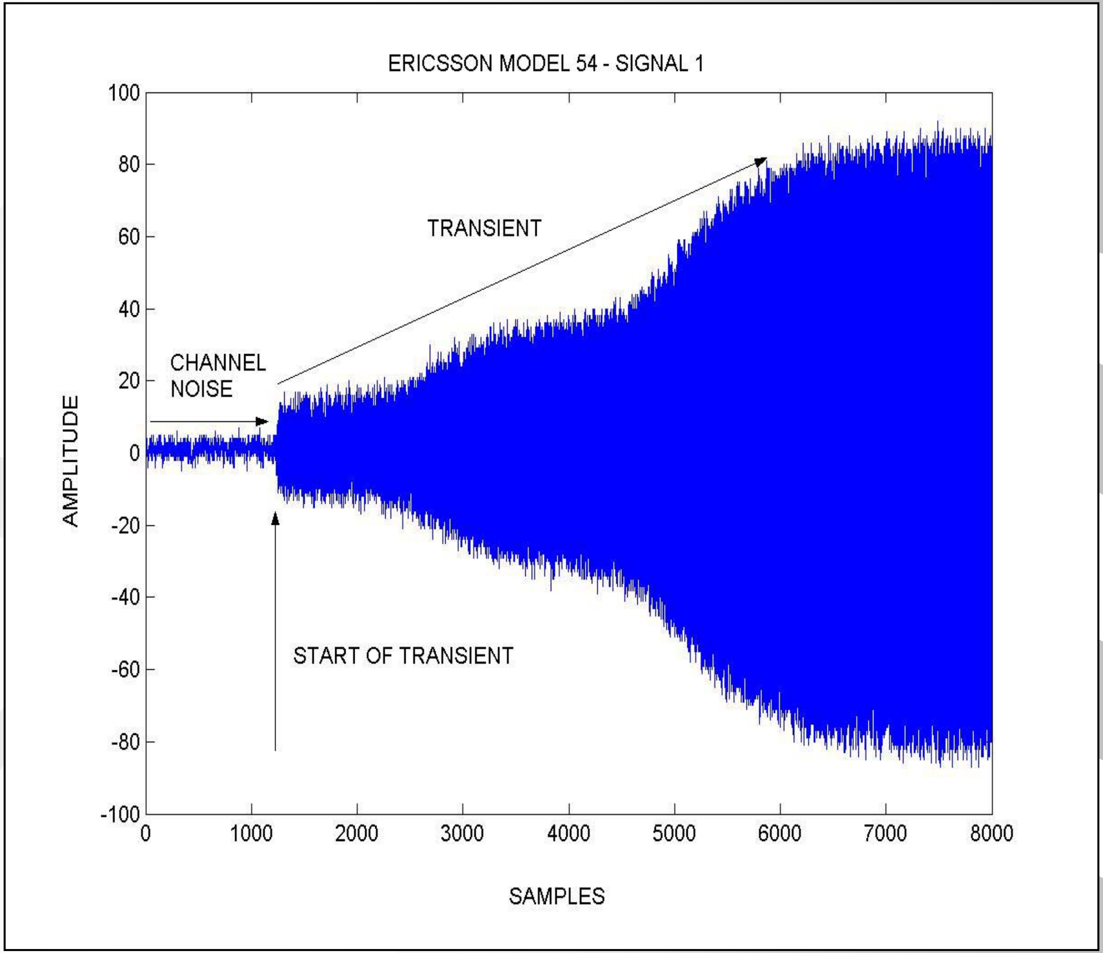
# Presentation Outline

- Radio Frequency Fingerprinting Process
- Current Phase: Detection of Transient
  - 2 current techniques using amplitude characteristics (time domain)
  - **new technique** using phase characteristics (frequency domain)
- Conclusion
- Next Phase

# RFF Process

- Step 1

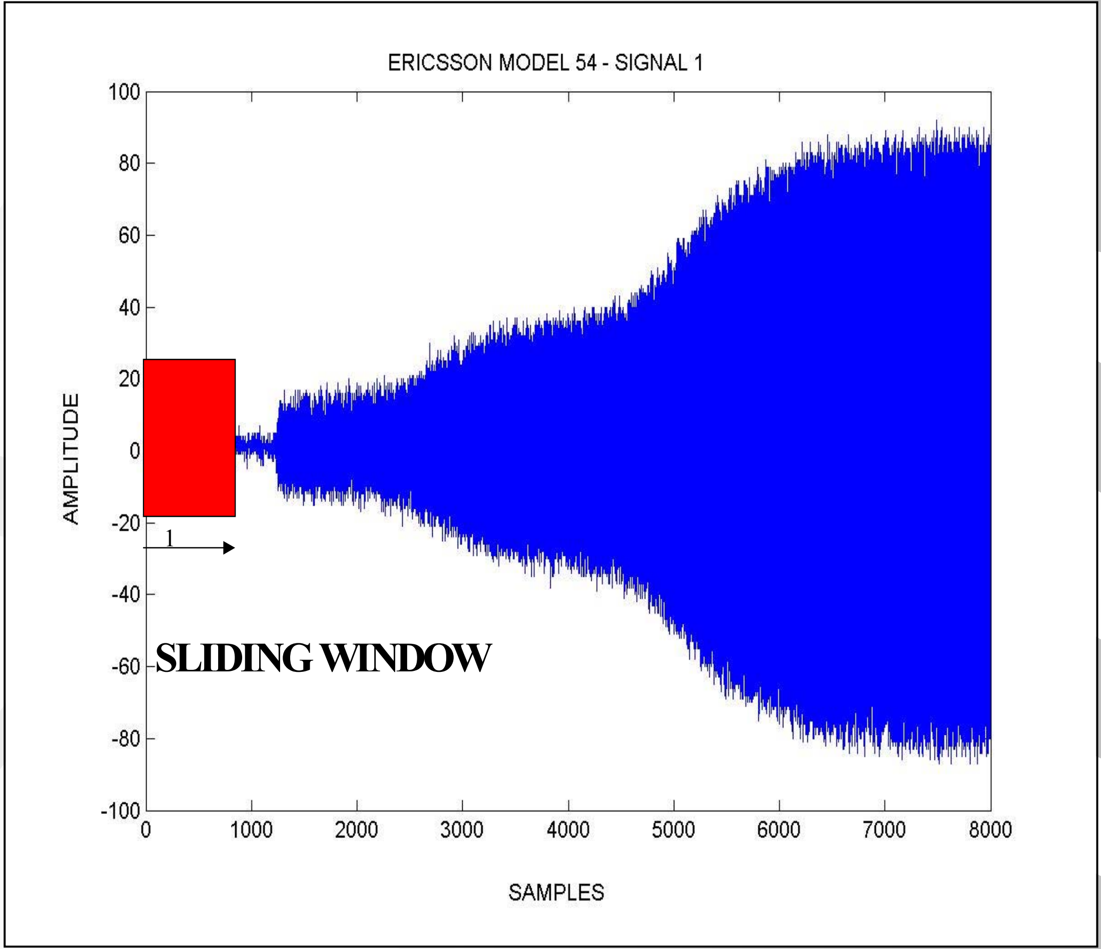
  Extract Features from Signal



# RFF Process

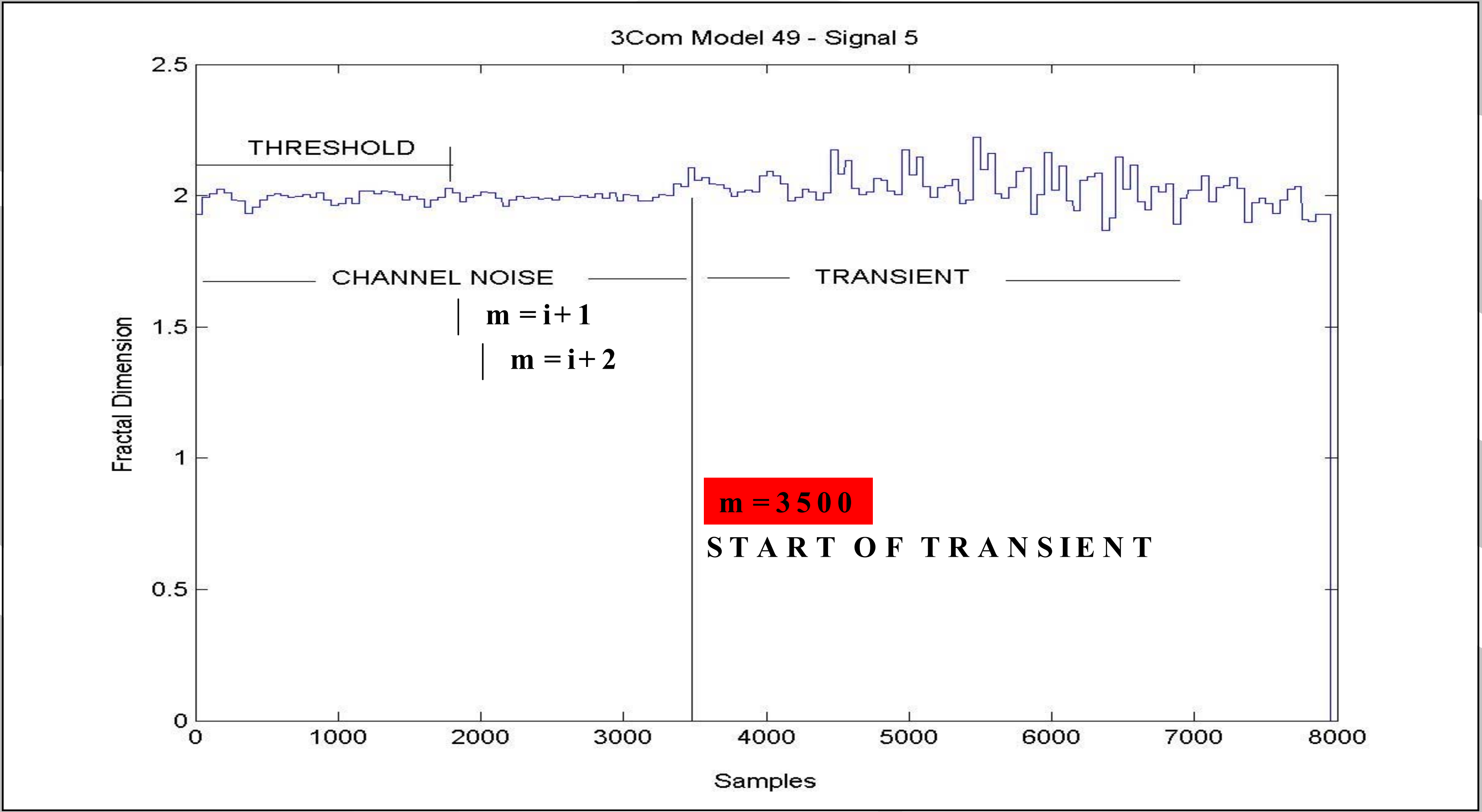
- Step 2

  Detect Start of Transient (pre-processing) stage



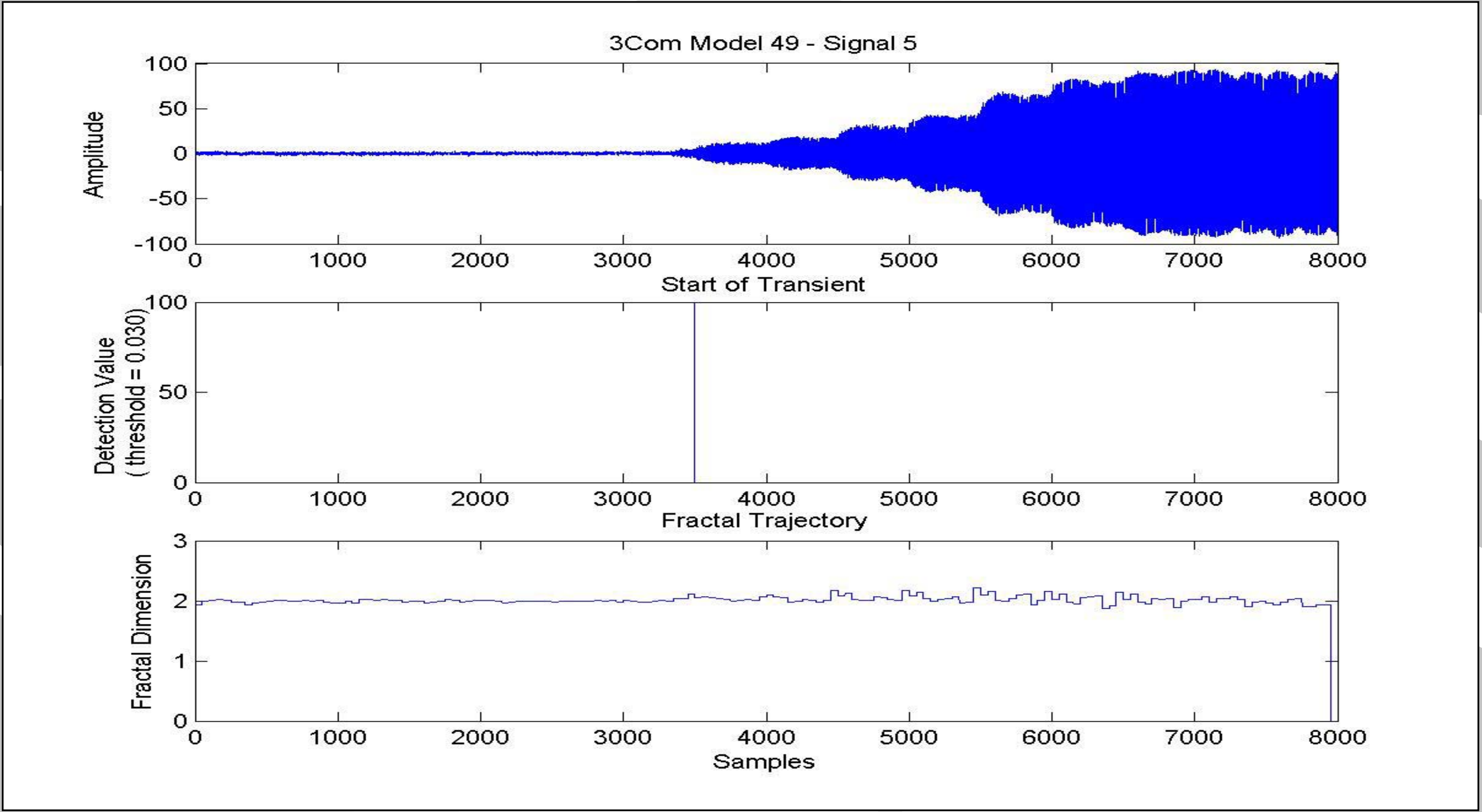
# Threshold Detection

- **D. Shaw and W. Kinsner (1997)**



# Threshold Detection

- **D. Shaw and W. Kinsner (1997)**

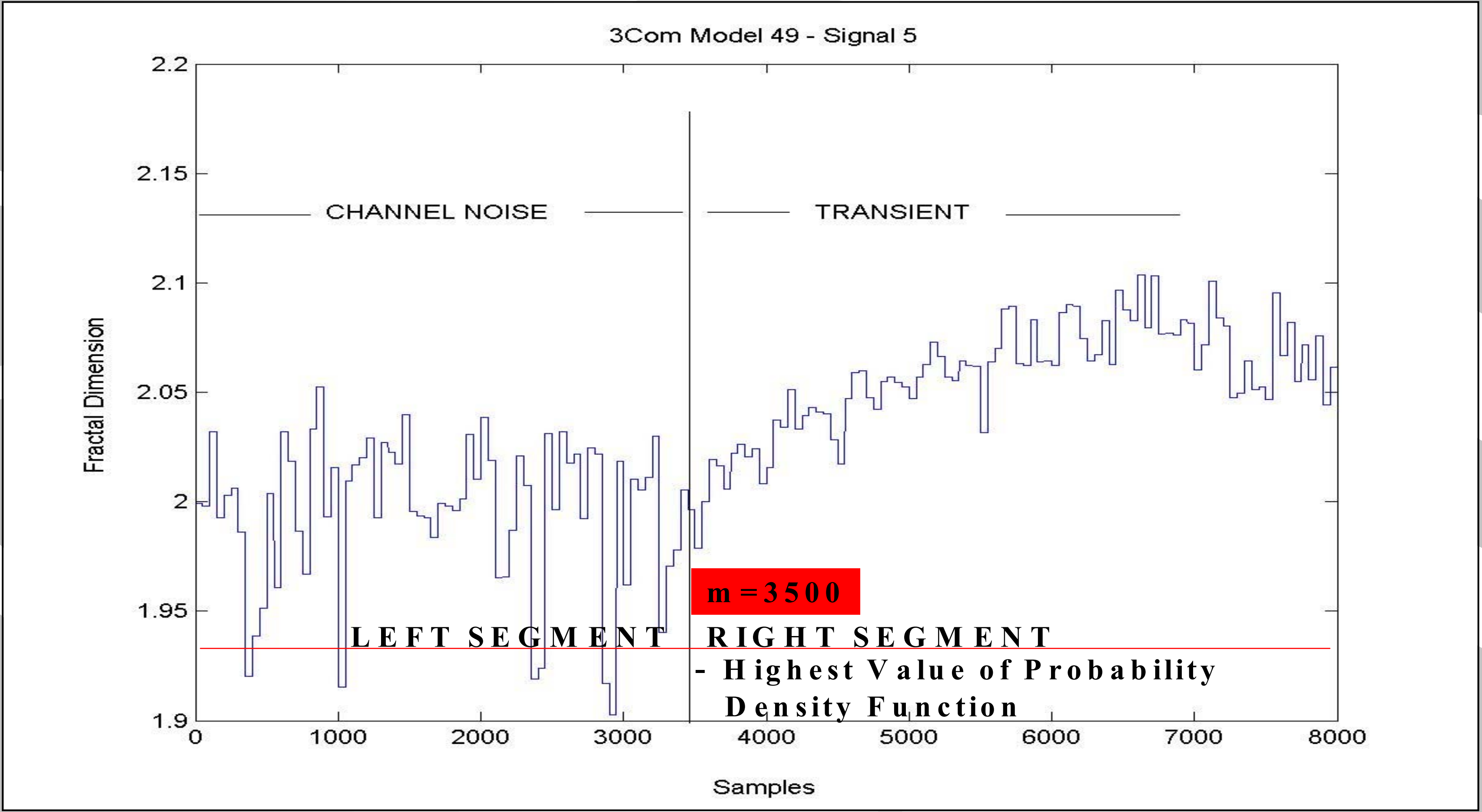


# Threshold Detection

- **Advantages**
  - most efficient (order n)
- **Disadvantages**
  - threshold is difficult to establish (experiments discontinued)
  - **abrupt spikes within noise segment**

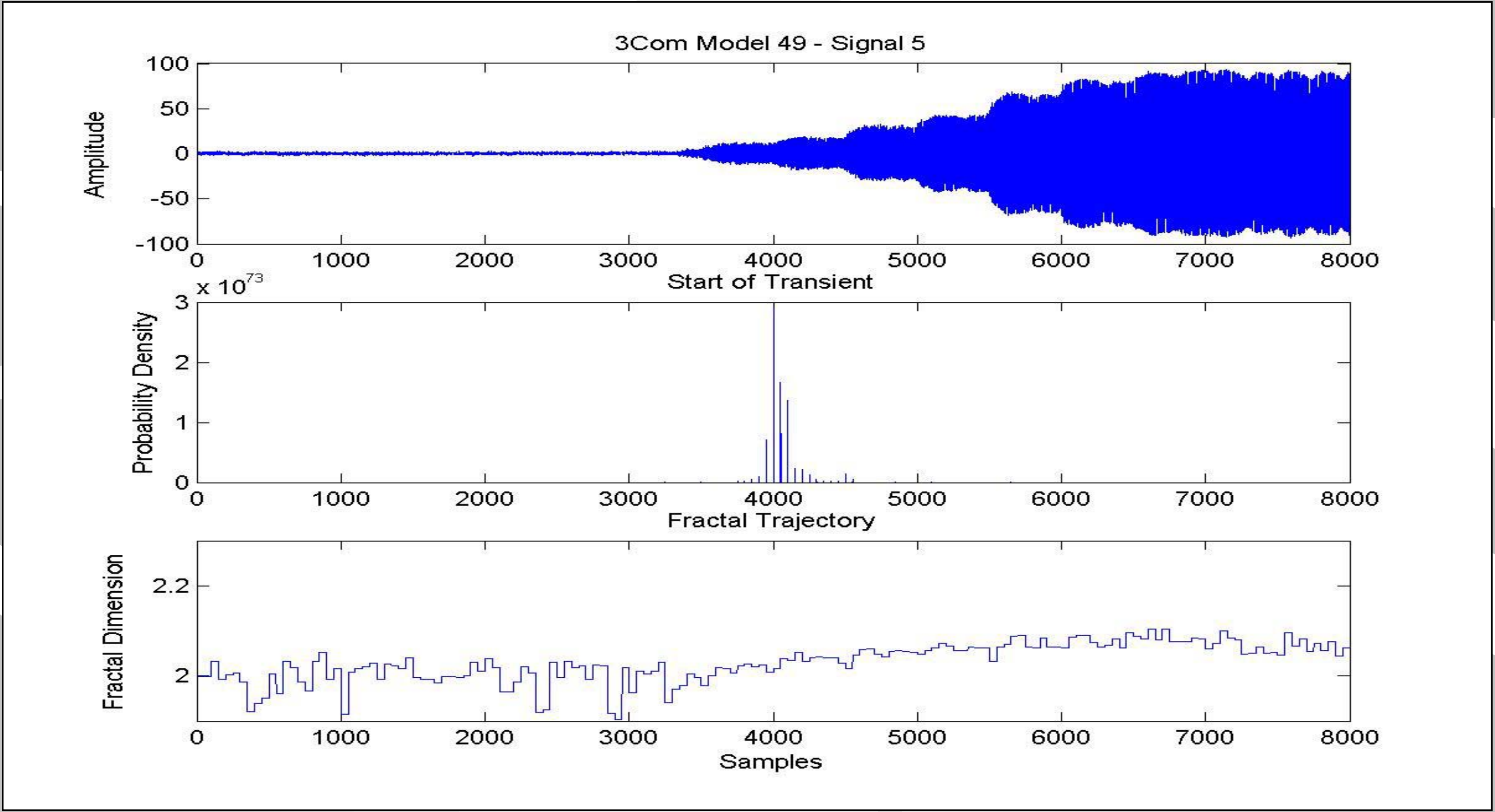
# Bayesian Step Change Detection

- **O. Ureten (1999)**



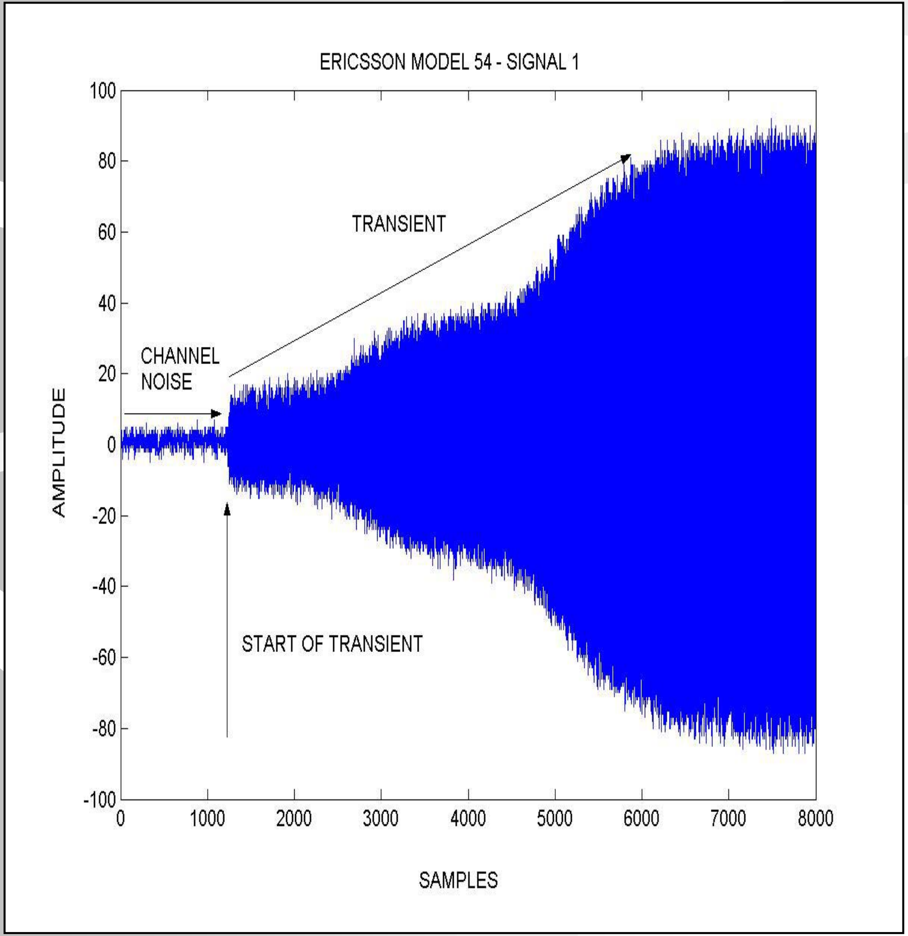
# Bayesian Step Change Detection

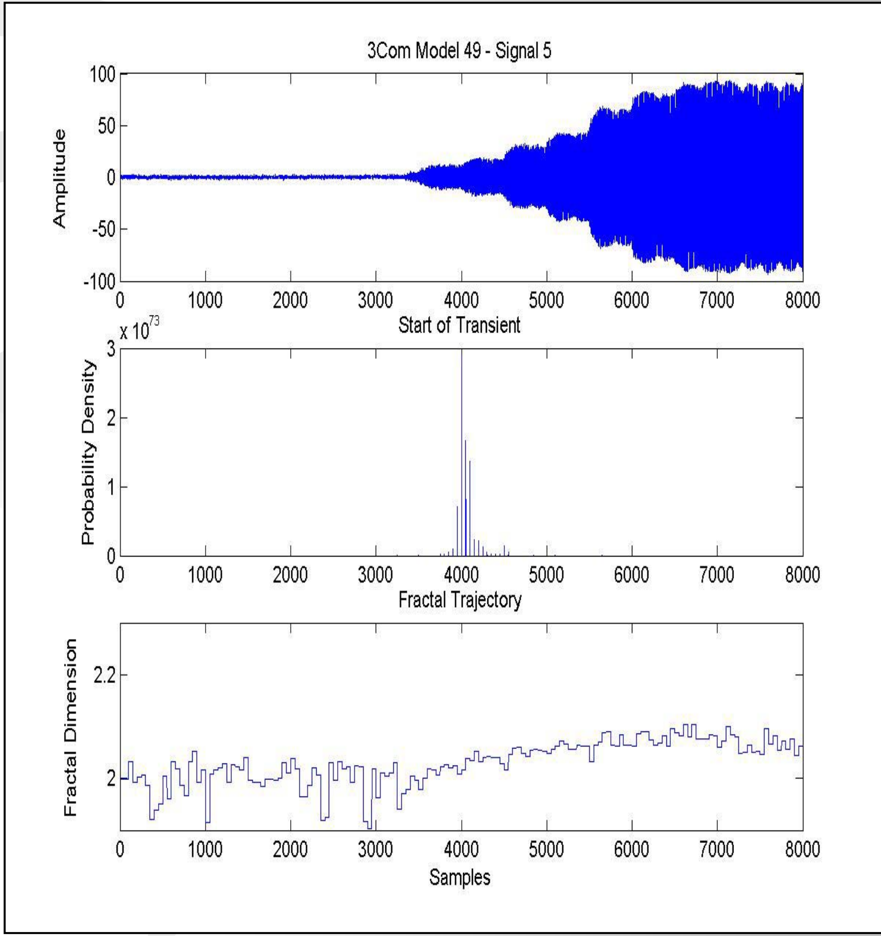
- **O. Ureten (1999)**



# Bayesian Step Change Detection

- **Experimentation**



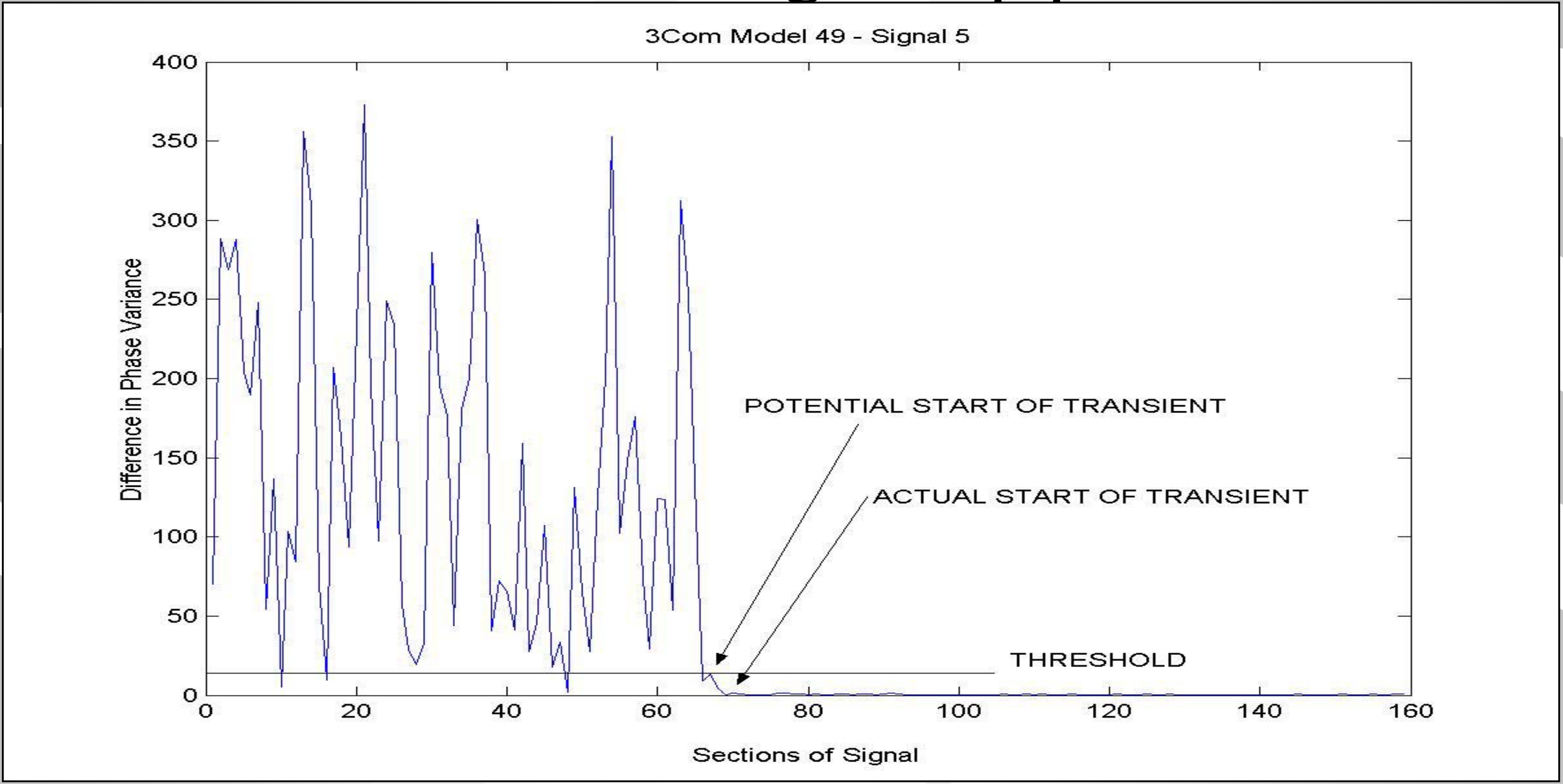


# Bayesian Step Change Detection

- **Advantages**
  - does not require samples to set threshold
  - can be applied to various types of signals
  - success rate of **80-85%**
- **Disadvantages**
  - complexity (order $n^2$)
  - poor detection  (spikes in channel noise and **rate of change is very gradual**)

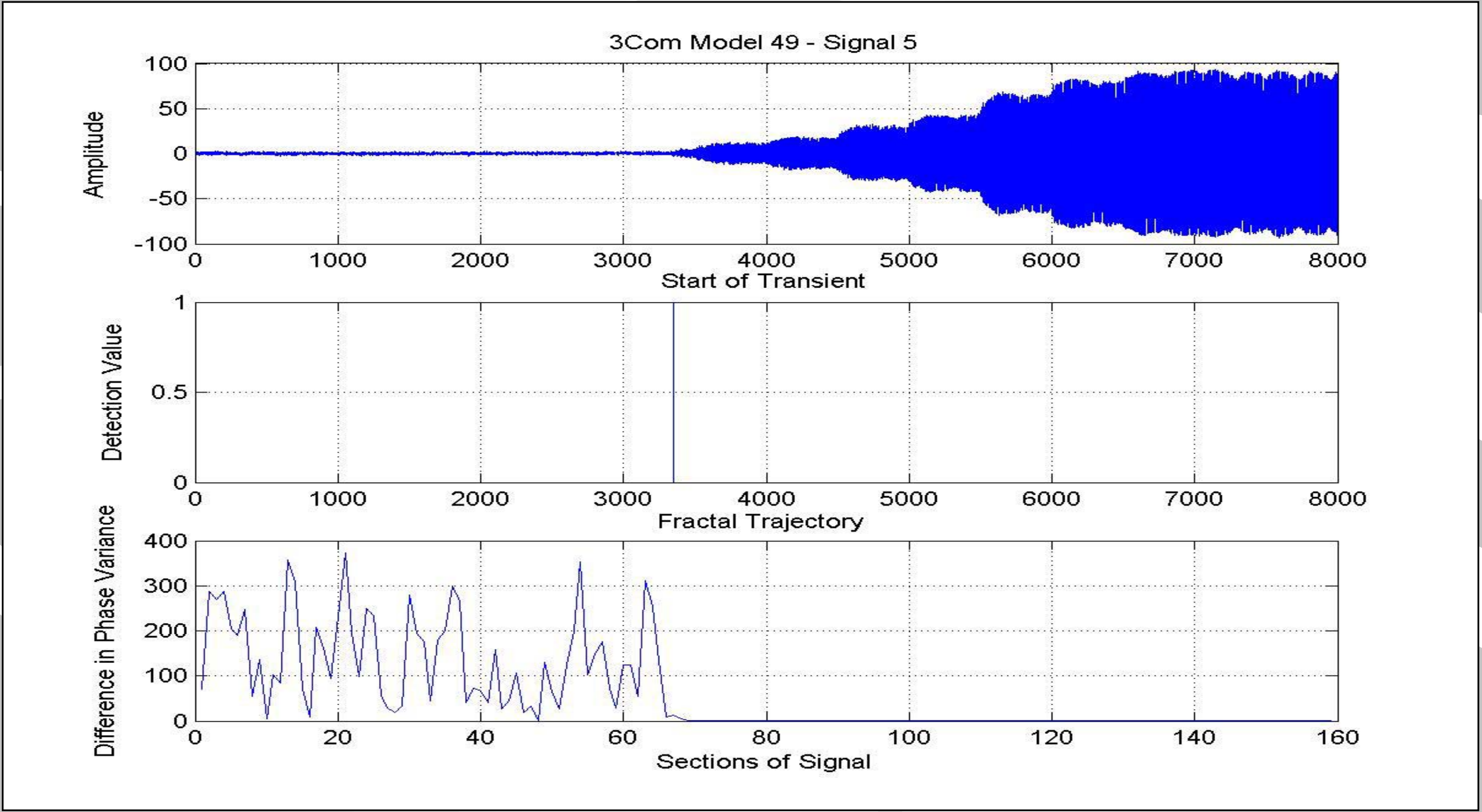
# Transient Detection using Phase

- Hall, Barbeau, Kranakis (2003)
- TD is carried out using 2 step process



# Transient Detection using Phase

- **Experimentation**

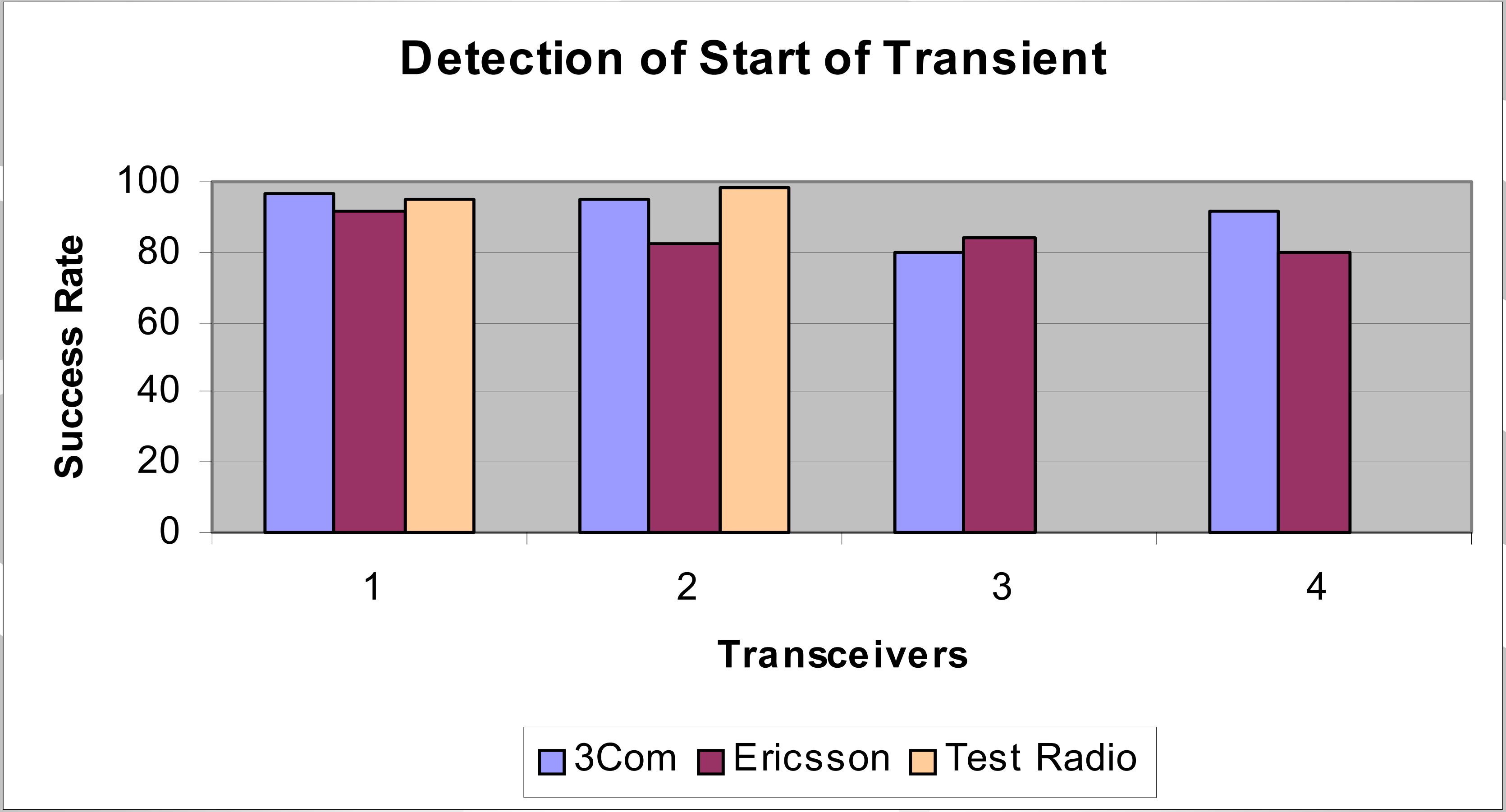


# Transient Detection using Phase

- **Benefits**
  - Threshold can be established with less difficulty
  - same complexity as Threshold (order n)
  - success rate of **85-90%**
- **Work in Progress**
  - establish threshold value using a larger sample size of transceivers
  - adjust algorithm to accommodate QPSK signals e.g 802.11b

# Results

- Success Rate is comparable between models



# Next Phase

- Complete RFF process
  - Step 3: Extract Fingerprint
    - using wavelet analysis
    - defining WT-DNA strand (consistent and **unique**)
  - Step 4: Classify Fingerprint using Probabilistic Neural Network
- Incorporate RFF mechanism into existing authentication protocols

# Thank You Comments/Suggestions are most welcome

jeyanthihall@rogers.com

Special Thanks to 3Com and Ericsson