Ottawa Wireless Research Alliance (OWRA) Seminar

Intrusion Detection and Radio Frequency Fingerprinting in Mobile and Wireless Networks

Speaker: Michel Barbeau, Prof.
Contributors: Jeyanthi Hall, Ph. Cand., Evangelos Kranakis, Prof.

School of Computer Science, Carleton University
Network Group, Digital Security Group

In this talk:

- What are intrusion, intrusion prevention and intrusion detection?
- Anomaly detection system architecture
- Radio Frequency Fingerprinting (RFF)
- Work in progress

What is an intrusion?

- An unauthorized visitor!
- A misbehaving visitor!

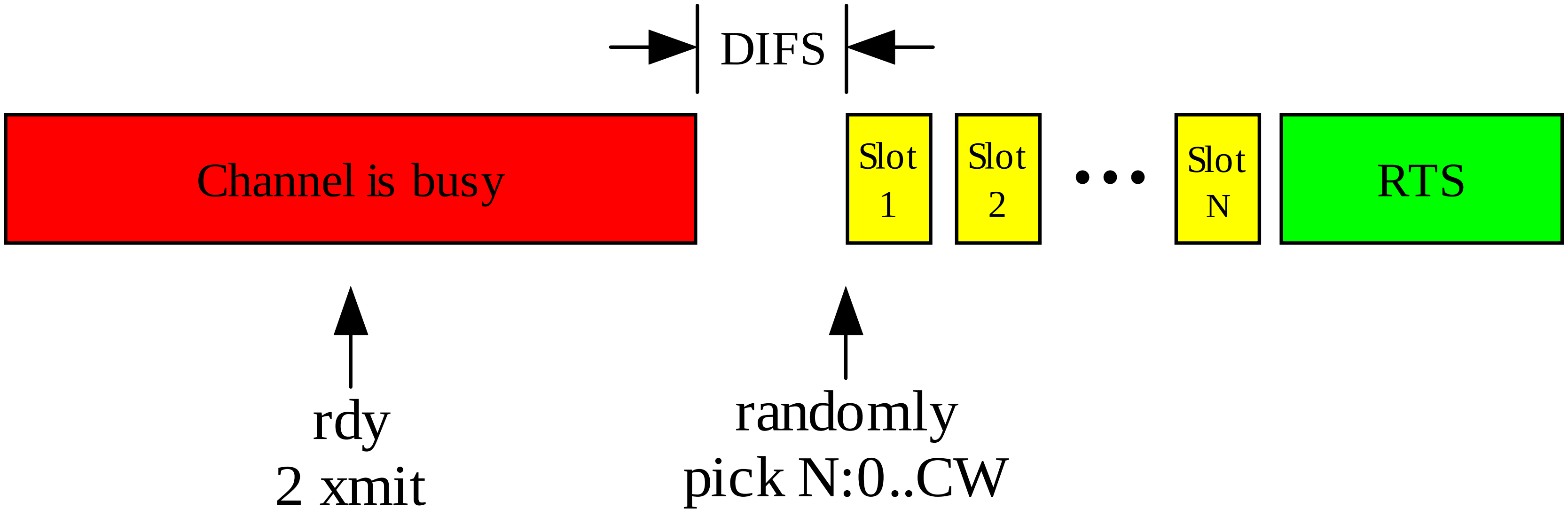
Intrusion prevention

- Authentication, encryption and firewall
- Intruders, however, exploit security weaknesses
  - Absence of access control
  - Buffer overflow
  - Eavesdropping
  - Identity malleability
  - Physical/MAC/Network layer misbehavior

Intrusion detection HOWTO

- Misuse detection
  - Recognizes application of well known patterns of attacks (signatures)
  - Drawback: Fails to find new kinds of attacks!
- Anomaly detection
  - Recognizes deviation from normal behavior
    - Routing misbehavior detection [Just, Kranakis & Wan ’03], [Zhang & Lee ’00]
    - MAC layer misbehavior detection [Kyasanur & Vaidya ’02]
    - Identity theft detection [Hall, Barbeau & Kranakis ’03]
  - Drawback: Higher rate of false positives!

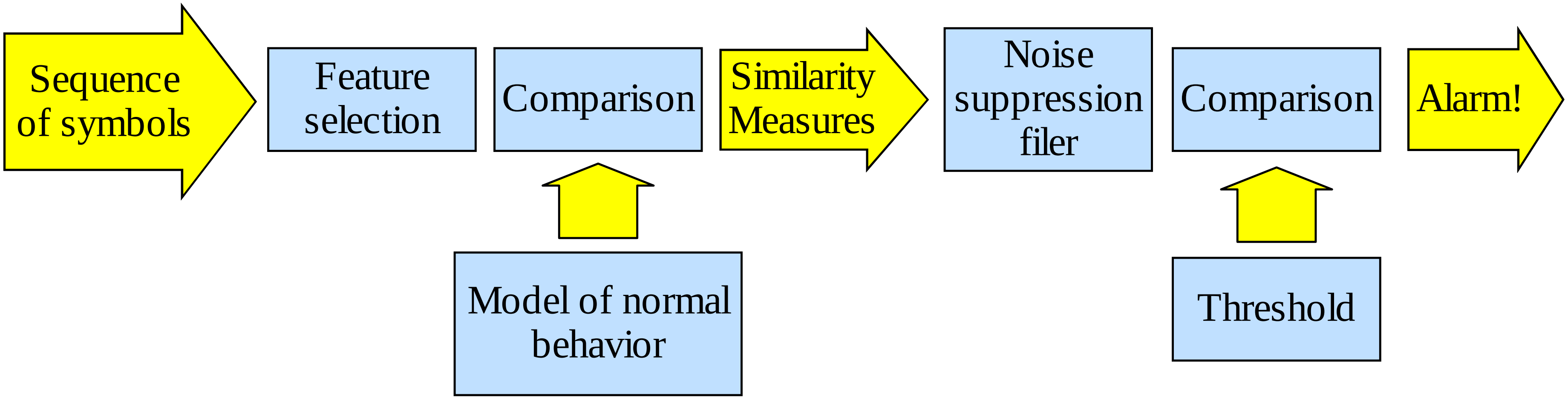
802.11 selfish HOWTO



- xmitting with high prob. in 1st slots
- using a smaller DIFS
- …

Anomaly detection system architecture

Lane and Brodley '99



Sequence of symbols

Feature selection

Comparison

Model of normal behavior

Similarity Measures

Noise suppression filer

Comparison

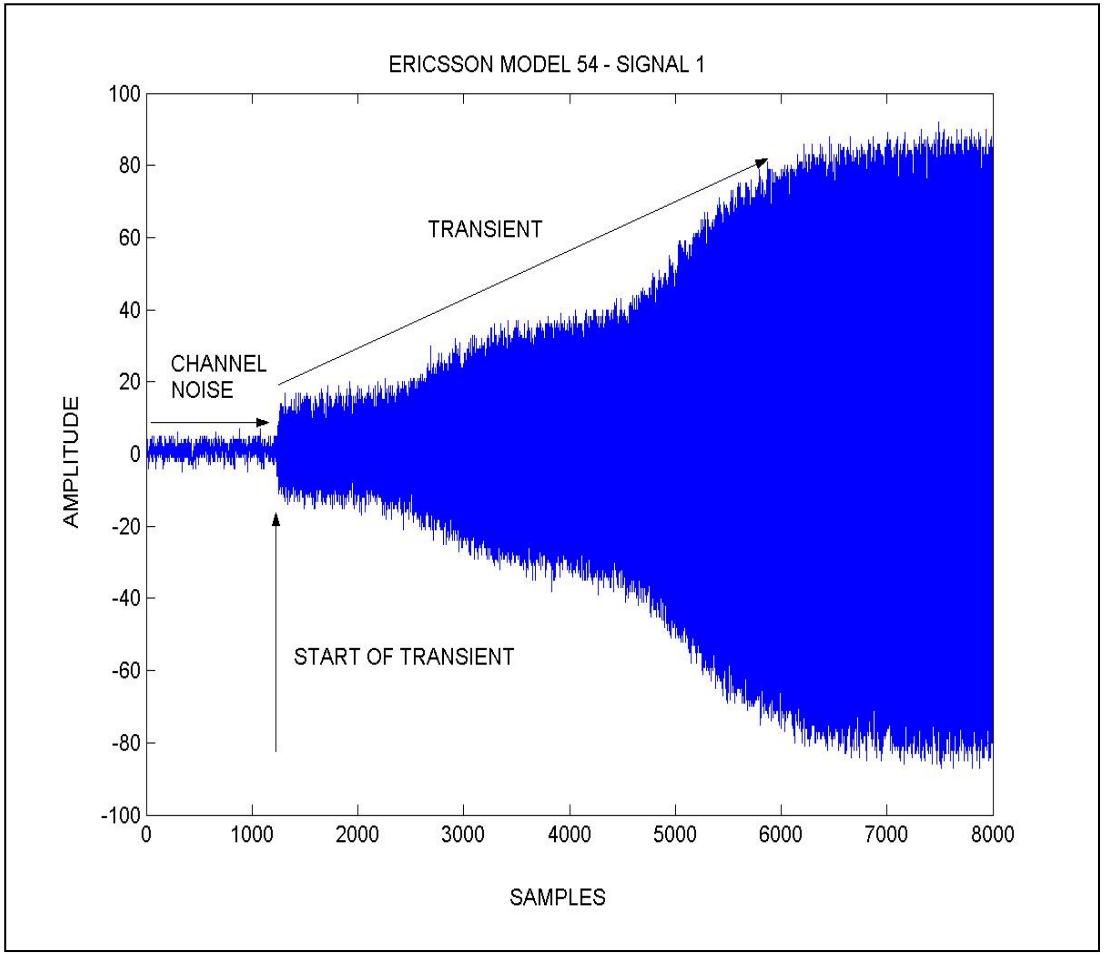
Threshold

Alarm!

Challenges in wireless networks

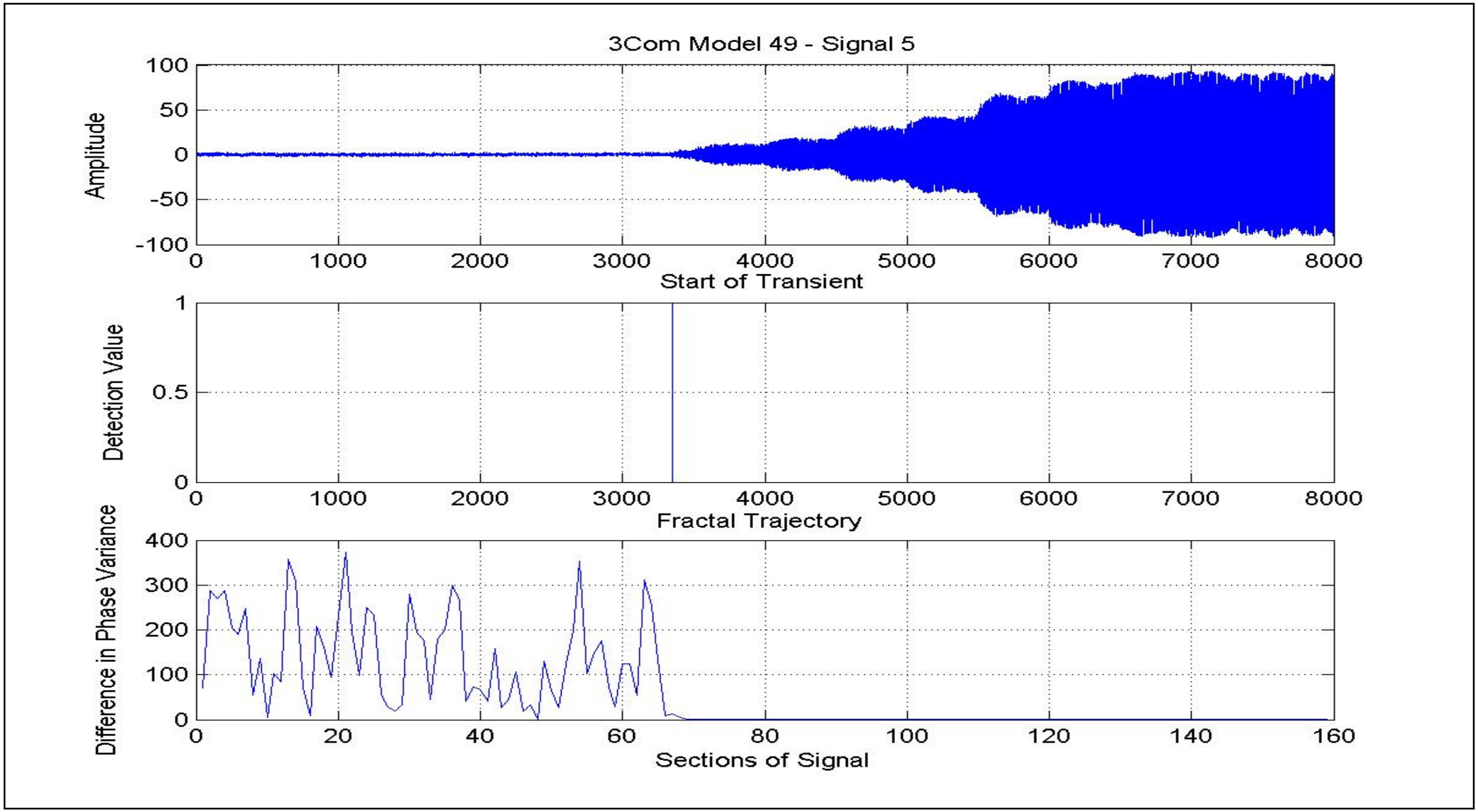
- Malleability of identity
- Sequences of symbols of arbitrary length:
  - Feature selection and comparison
- Modeling normal behavior:
  - Safety and liveness requirements
- Partial observation:
  - RF noise, blockage, interference

Handling malleability of identity : RFF



Transient detection using phase

Hall, Barbeau and Kranakis ‘03



Work in progress

- Radio frequency fingerprinting:
  - Increase sample size of Bluetoorh transceivers
  - Adjust algorithm to accommodate 802.11b
  - Extract and classify fingerprint
- Misbehavior detection using metric temporal logic, handles:
  - Safety and liveness requirements
  - Infinite sequences of symbols

Bibliography

- M. Just, E. Kranakis and T. Wan, Resisting Malicious Packet Dropping in Wireless Ad-Hoc Networks Using Distributed Probing, In: Proceedings of 2nd Annual Conference on Adhoc Networks and Wireless (ADHOCNOW'03), Montreal, 2003.
- P. Kyasanur and N.H. Vaidya, Detection and Handling of MAC Layer Misbehavior in Wireless Networks, Technical Report, Coordinated Science Laboratory, University of Illinois at Urbana-Champaign, August 2002.
- J. Hall, M. Barbeau and E. Kranakis, Detection of Transient in Radio Frequency Fingerprinting Using Phase Characteristics of Signals, In: L. Hesselink (Ed.), Proceedings of the 3rd IASTED International Conference on Wireless and Optical Communications (WOC), ACTA Press, Banff, 2003, pp. 13-18.
- T. Lane and C.E. Brodley, Temporal Learning and Data Reduction for Anomaly Detection, ACM Transactions on Information System Security, Vol. 2, No. 3, Aug. 1999, pp. 295-331.
- Y. Zhang and W. Lee, Intrusion Detection in Wireless Ad-Hoc Networks, Mobile Computing and Networking, 2000, pp. 275-283.