CENTER FOR ADVANCED TECHNOLOGY IN TELECOMMUNICATIONS

NYSTAR® designated Center For Advanced Technology

Identifying Wi-Fi Interference by End-Users

Richard Meng, Xiang Ying Qian, Kyung-Hwa Kim, Henning Schulzrinne
Dept. of CS and EE, Columbia University in the City of New York

NYU·poly
POLYTECHNIC INSTITUTE OF NYU

Motivation & Background

- Identifying causes of WLAN performance degradation is nontrivial
- Most access points (IEEE 802.11b / IEEE 802.11g) are deployed in the 2.4GHz wireless band, which causes network interference
- Most significant interference sources:

Non-WiFi interference

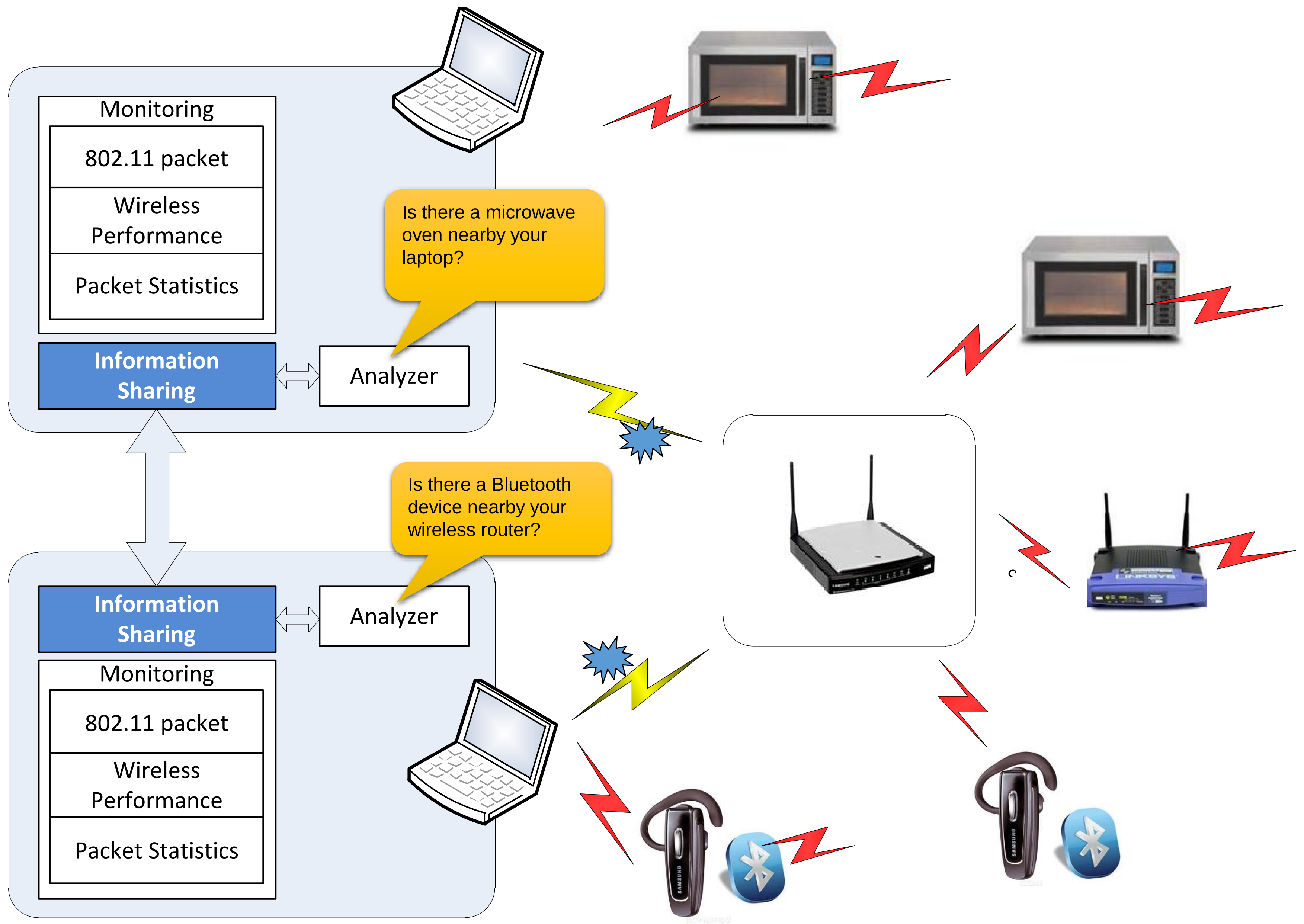
Goal

- Difficult for end-users to identify the devices that cause Wi-Fi interference
- Existing solution:
  - Spectrum Analysis
    - Additional hardware is required (e.g., Wi-Spy)

Monitors RF activity within a given frequency range (Wi-Spy by *Metageek*, $84, *metageek.net*)

- Our goal is to *identify the source of Wi-Fi interference without any hardware support*.
  - Monitor and analyze the patterns of various parameters related to Wi-Fi performance.
  - Obtain data from other collaborative nodes to see whether others also observe the same interference
  - Train the pattern analyzer with the dataset obtained from different environments and nodes
  - Provide users the best matched devices that are supposed to cause the interference

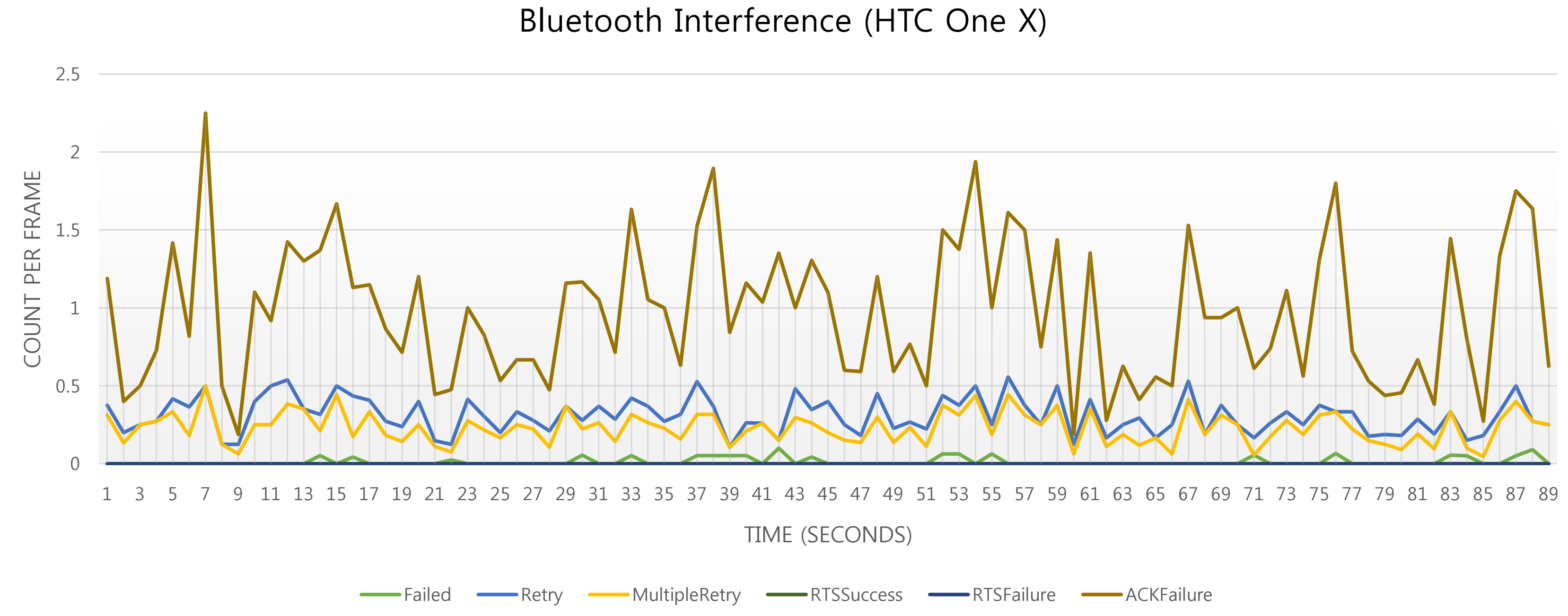
Architecture

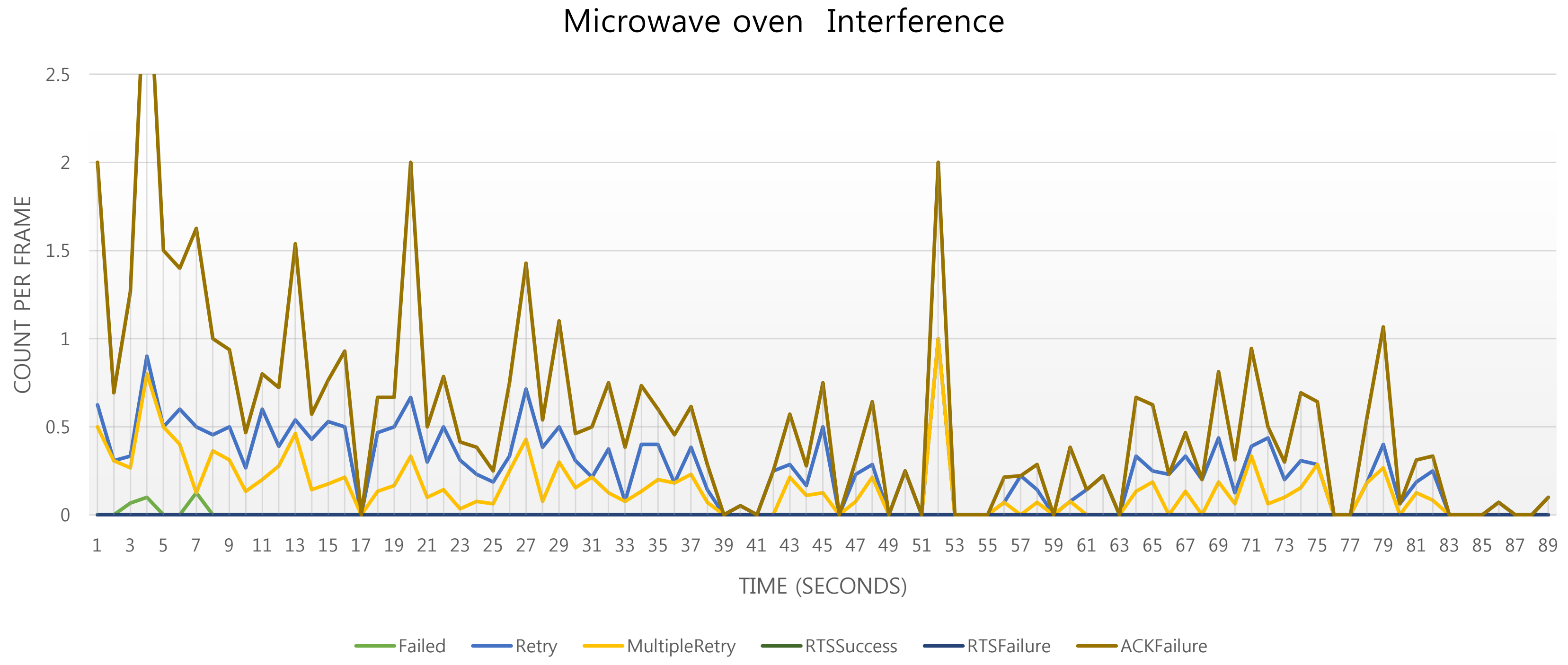


Implementation & Experiment

- Interference measurement
  - Existing waves makes measuring interference difficult
  - We measured network throughput, SNR, 802.11 retry counter, and other variables to infer a characteristic of current interference.
- Implementation
  - On Linux: Analyze the information of Radiotap 802.11 header in the data link frames captured by integrating *Wireshark*, *Jpcap*, and *Alpacka* library.
  - On Windows: Analyze built-in parameters in network systems collected by *Windows Native Wi-Fi API*.
- Experiment setup
  - 802.11g Cisco Linksys AP (Channel 1,6,7)
  - Measurement on laptops
  - Experiment with and without microwave ovens / Bluetooth devices
  - Sharing information using *DYSWIS*[1] framework

Preliminary Measurement





Results & Future work

- In our experiment, Bluetooth devices and microwave ovens showed different patterns (e.g., the magnitude of standard deviation of retry count, percentage of ACK failures, i.e. microwave oven tends to cause more unstable network condition)
- This result enables to identify some interference sources.
  - However, the patterns are difficult to be resolved by human.
- A Machine learning method is needed to achieve more accurate identification of interference sources

References

[1] DYSWIS, Collaborative network fault diagnosis,
Kyung-Hwa Kim, Vishal Singh, Henning Shulzrinne