Broadcast LTE Data Reveals Application Type

Arjun Balasingam, Manu Bansal, Rakesh Misra, Rahul Tandra, Aaron Schulman, Sachin Katti
Mobicom 2017, Snowbird, UT

1. Motivation & Problem Statement

- Growth in apps and content being supported by mobile platforms
- Mobile traffic expected to increase 7x by 2021
- More data being pushed through cloud with growth of IoT
- Potential to expose a trail of personal data
- Protocols must be secure to prevent malicious attacks
- In LTE, data is encrypted, but control information is broadcast

We show that it is possible to *infer the type of application being hosted by any LTE session* from only its radio resource allocation patterns.

Contributions:

1. Phone can infer its own app type from just PHY-layer data
2. *Anyone* can identify all apps being served by cell tower

2. PROMINENCE Metric

- Derived from LTE PHY-layer DCIs at PDCCH
- Data at phone's modem exposed by QXDM

Derived Metrics

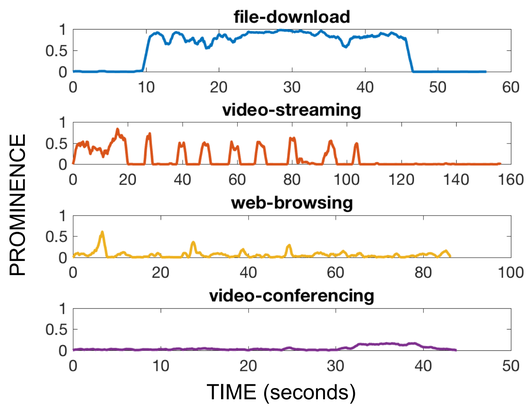
- SCHEDTIME: # of ms where session was scheduled resource blocks (RBs)
- SESSDUR: session duration (in ms)

$$\text{PROMINENCE} = \frac{\text{SCHEDTIME}}{\text{SESSDUR}}$$

- Simple to compute
- Captures traffic arrival patterns
- Abstracts out session-specific factors

3. Design of Application Classifier

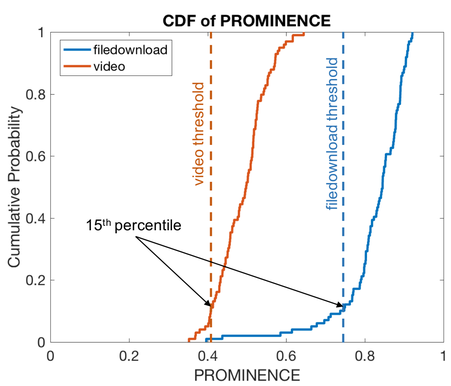
PROMINENCE time series
computed over 1 second moving window



Application	PROMINENCE Signatures
file download	• full buffer flows • 80% of RBs/sec
video streaming	• regular periodicity • segment downloads • idle periods
web browsing	• brief file downloads
video conferencing	• low PROMINENCE • data sent per ms (not as larger segments)

Different classes of apps have *distinct* PROMINENCE signatures.

Features from PROMINENCE



- PROMINENCE is repeatable
- Select PROMINENCE thresholds for heuristic

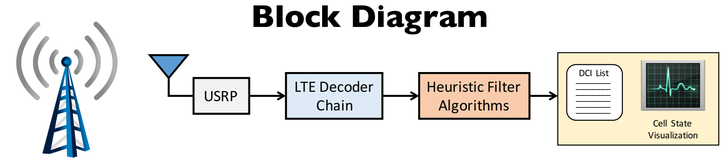
1. PROMINENCE score for session
2. Fraction of 1-second windows with nonzero PROMINENCE

Application	Feature (1)	Feature (2)
file download	high	high
video streaming	low	high
web browsing	low	high
video conferencing	low	low

4. Cell-Wide Application Inference

eNBsniffer: A Cell-Wide View of PHY-layer Resource Allocation

- Off-the-shelf USRP
- Standard MATLAB LTE decoder
- Heuristic filter algorithms
- < 5% false negative error (for favorable RF conditions)
- *Passive* sniffer

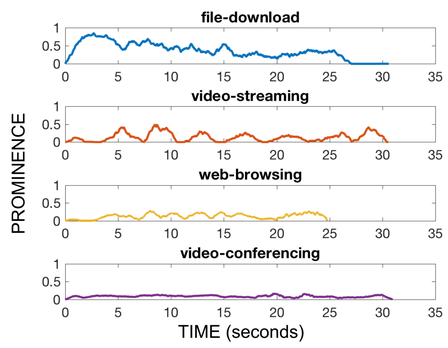


eNBsniffer decodes DCIs for *all* users served by cell tower.

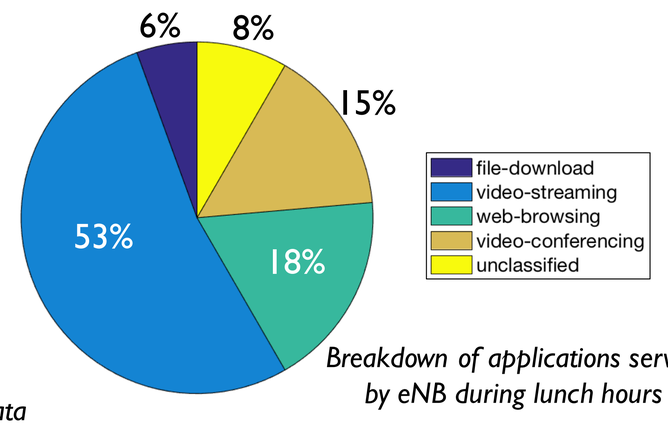
eNBsniffer + Application Classifier

- Apply classifier on data from eNBsniffer
- Tag each user connected to cell with type of application being run on phone

Analysis of Congested Cell in Downtown Palo Alto, CA



PROMINENCE signatures from eNBsniffer data



Breakdown of applications served by eNB during lunch hours

Can infer mobile applications served by cell tower from *broadcast* LTE data.

5. Implications & Future Directions

Heuristic Refinement

- Expand classifier to broader class of apps
- Validate generality on different video clients
- Verify robustness to different schedulers
- Identify hidden patterns in PROMINENCE signatures (with ML)

Privacy Implications

- This work raises several privacy concerns
  - e.g. Hackers could sniff broadcast data and isolate desired applications to attack
- Encourages an open discussion about security of LTE protocols
  - Enhance standards to mask features that can exploited to infer application type