NYU·poly
POLYTECHNIC INSTITUTE OF NYU

Security Through Entertainment: Using a Memory Game for Secure Device Pairing

Alexander Gallego, Nitesh Saxena, and Jonathan Voris
agalle01@students.poly.edu, nsaxena@poly.edu, jvoris@isis.poly.edu
Polytechnic Institute of New York University
Department of Computer Science and Engineering

Center for Advanced Technology in Telecommunications
NYSTAR designated Center For Advanced Technology

NYU·poly
POLYTECHNIC INSTITUTE OF NYU

The Problem: Device Pairing

- How can a **secure channel** be **initialized** between two wireless devices when they have:
  - No prior association or shared secret
  - No common source of trust
- Examples of device pairing scenarios:
  - Pairing a Bluetooth cell phone with a headset
  - Connecting a WLAN **laptop** with an **access point**

Center for Advanced Technology in Telecommunications
NYSTAR designated Center For Advanced Technology

NYU·poly
POLYTECHNIC INSTITUTE OF NYU

Previous Work

- **Out of band** channels can be used between devices
  - Created using human perceptible forms of output
    - Audio
    - Visual
    - Tactile
  - Physically authenticable by device owners
- But introduce a **usability burden** for users
  - Pairing tasks may be tedious and time consuming
  - Users may make **errors** while pairing
  - Process is limited by **human factors**
    - Must be slow enough for a human to perceive
    - Security is dependant on an individual's attention span

Center for Advanced Technology in Telecommunications
NYSTAR designated Center For Advanced Technology

NYU·poly
POLYTECHNIC INSTITUTE OF NYU

The "Tom Sawyer" Effect

- "The Adventures of **Tom Sawyer**" by Mark Twain
  - Tom is forced to paint a fence
  - He pretends to enjoy it rather than resent it
  - Friends insist on helping!
- Apply this principle to security tasks
  - Reframe device pairing as a game
  - Introduce entertainment value
- **Competitiveness** between individuals causes them to perform better at certain tasks
  - Such as random number generation and recognition - Halprin and Naor [SOUPS '09]

Center for Advanced Technology in Telecommunications
NYSTAR designated Center For Advanced Technology

NYU·poly
POLYTECHNIC INSTITUTE OF NYU

Alice Says: A Pairing Game

- To leverage the Tom Sawyer Effect, designed a **game** for device pairing
  - Inspired by Hasbro's Simon
- Performed a **usability study** with 20 participants
- Conclusion: **Incentivizing** users with **entertainment** is a promising way to address device pairing and other security issues

Center for Advanced Technology in Telecommunications
NYSTAR designated Center For Advanced Technology

NYU·poly
POLYTECHNIC INSTITUTE OF NYU

Coordination and Bargaining over the Gaussian Interference Channel

Xi Liu

Polytechnic Institute of NYU
Advisor: Prof. Elza Erkip

Center for Advanced Technology in Telecommunications
NYSTAR designated Center For Advanced Technology

Problem: Performance of communication systems is often limited by interference. Interference management methods require cooperation in transmission strategies among users. In practice, *selfish* users may not have an incentive to cooperate.

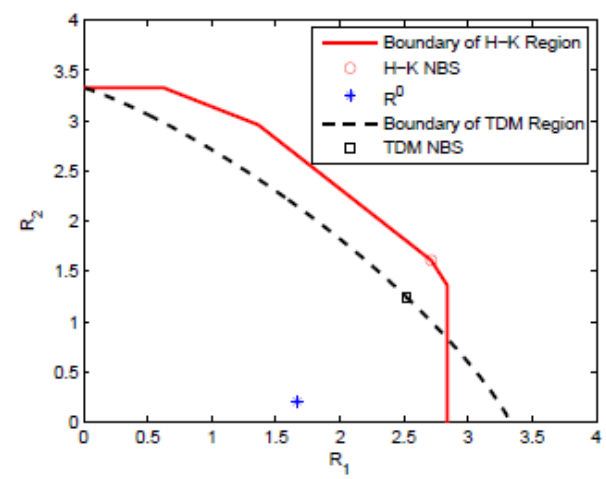
The following problems are treated using tools from game theory and information theory:

- What are the incentive conditions under which users have incentives to cooperate?
- How to determine an operating point for two selfish users if they do cooperate?

Main Result: A two-phase mechanism for coordination is proposed.

- Phase 1: allow users to negotiate for the use of a simple Han-Kobayashi (H-K) type scheme.
- Phase 2: employ the Nash bargaining solution (NBS) from game theory to select a fair operating point.

The H-K NBS is shown to not only provide a fair operating point, but also maintains a good overall performance.



NYU·poly
POLYTECHNIC INSTITUTE OF NYU

CATT
Center for Advanced Technology in Telecommunications

NYSTAR® designated
Center For Advanced Technology

Motivations …

1. **Cache Updates;**

- Update the result caching periodically by issuing batches of queries.

2. **Data Mining;**

- Various internal quality testing by issuing a lot of not-interactive queries;
- In machine learning researchers usually issue queries to mine people's attitude;
- Individual group wants to pull data from a search system, as in the so called "deep web".

3. **Query by Outside Parties;**

- Yahoo! *BOSS* (Build your Own Search Service)
- In May 2009, Yahoo! reported that about 30 million queries per day were issued through *BOSS*.

Ideas …

Improvement for Disk (better caching technique):

(1)Query Reordering:

(2)Clairvoyance:

Since we know all the queries, we can use clairvoyant algorithms for caching lists. It is known that for list caching this is the optimal.

Improvement for CPU:

Modern search engines store the index in main memory. By caching the sub queries we can improve the query processing performance.

Results …

Disk improvement

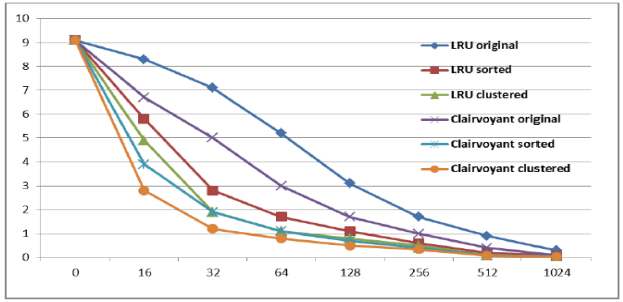


Figure 1: Caching performance using LRU and Clairvoyant, with different query stream reordering, on our 1.16 million query stream. The x-axis is the size of the cache in Millions, and the y-axis is the size of data needs to be transferred from disk in TB.

CPU improvement

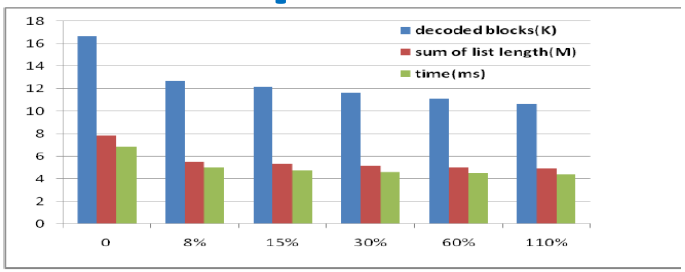


Figure 8: Performance gains with caching pairs (2-term sub-queries) using our greedy algorithm, with different cache size with respect to the inverted index size. Zero means no sub-queries are cached and re-used, 110% means the cache size is even larger than the inverted index size. We average the numbers over our 1.1 million queries.

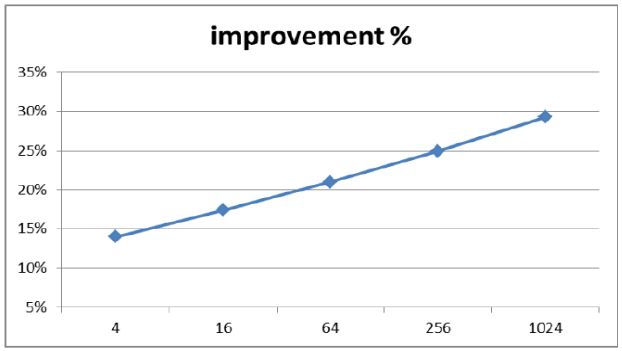
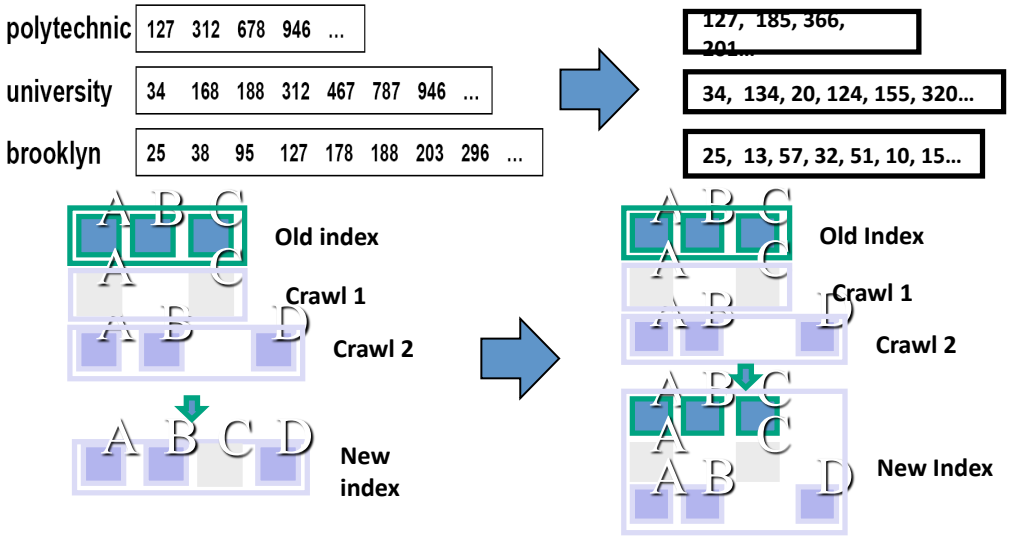


Figure 9: Performance gain with different numbers of queries (in thousands). The benefit is showed as the sum of lists lengths.

Improved Index Compression Techniques for Versioned Document Collections

Jinru He, Junyuan Zeng, Torsten Suel , Polytechnic Institute Of NYU



Background – Inverted Index

An inverted index consists of inverted lists.

One inverted list per distinct term in collection.

Each inverted list is a sequence of postings

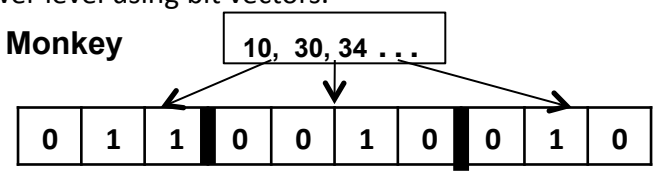
Inverted lists are sorted by DocID and compressed

Issues in Versioned Document

- Index representation and compression
- Index traversal techniques
- Support for temporal range queries
- Aggregate query processing
- (e.g. stable top-k by Leong et al 2010)

Two-level Indexes by Altingovde et al 2008

- Top level index the union of all versions
- Lower level using bit vectors.



- The length of each bit vector is the number of versions in the document.
- For bit vector of term **t**, if t appears in ***i***th version, the ***i***th position of bitmap is set to 1 otherwise, it is set to 0

	Wikipedia	Ireland Dataset
# documents	2,401,799	1,059,670
Versions/Doc	35.54	15.78
Total Postings	5.82 Billion	3.42 Billion

NYU·poly POLYTECHNIC INSTITUTE OF NYU

CATT Center for Advanced Technology in Telecommunications

NYSTAR® designated Center For Advanced Technology

Improved Index Compression Techniques for Versioned Document Collections

Our Solutions

Bitwise Approach:

1.Model Approach:

Given the information of known versions in a document, we derive models to predict what it is like in the next versions.

2. Featured Approach:

Exploit features, machine learning tools to do prediction

Practical Approach:

- Transforming DIFF and MSA into two-level methods
- Bit vector reordering based on amount of change
- Hybrid of DIFF and MSA

	Wiki	Ireland
Previous Result	140	304
Model upper bound	92	254
Model lower bound	88	249
Feature-Based	77.5	209

Our combinatorial approach:

Wikipedia: up to 50% times smaller.

Ireland: up to 30% smaller

	Wiki			Ireland		
	docID	freq	total	docID	freq	total
HUFF	N/A	N/A	336	N/A	N/A	645
2R-DIFF-IPC	214	86	300	564	215	779
2R-DIFF-PFD	242	98	340	623	240	863
2R-MSA-IPC	197	41	238	597	154	751
2R-MSA-PFD	212	51	263	658	170	828
2R-HUFF	210	64	274	568	236	804
2R-HUFF combined	N/A	N/A	235	N/A	N/A	619

Table 2. Compression Size in MB for Wikipedia and Ireland Dataset by applying different proposed methods

Query Processing

- Bit vectors corresponding to the result docIDs are fetched
- AND the bit vector
- **First level index is small, many bit vectors can be skipped to speed up the second level query processing!**

	speed (ms/query)			index size (MB)			decoded
	IPC	PFD	Mix	IPC	PFD	Mix	postings
Sorted	4.28	0.97	-	570	583	-	245
2-DIFF	1.34	0.66	0.68	253	310	269	34
2R-DIFF	1.51	0.83	0.85	176	234	193	34
2-MSA	1.68	0.99	1.01	233	284	243	28
2R-MSA	1.68	0.99	1.01	179	236	195	28
2-Hybrid	1.59	0.88	0.9	166	223	182	30

Table 3. Query processing on Wikipedia on all methods

Our practical approach:

Wikipedia: up to 30% times smaller.

Ireland: up to 5% smaller

Actually, we can do it even faster than previous work!

NYU·poly POLYTECHNIC INSTITUTE OF NYU

CATT Center for Advanced Technology in Telecommunications

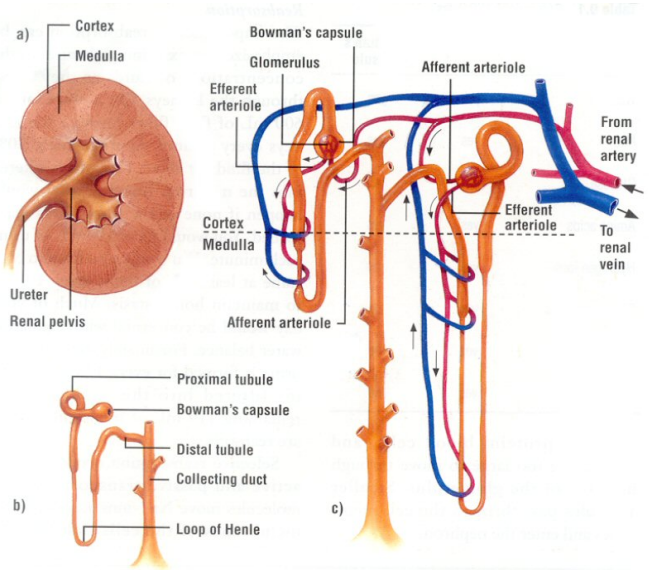
NYSTAR® designated Center For Advanced Technology

Optimal Control Mechanism Involving the Human Kidney

Students: Yu Jiang, Srinivasa Chemudupati, Jan Morup Jorgensen
Advisers: Zhong-Ping Jiang, Charles. C. Peskin
Control and Telecommunication Research Laboratory, NYU-POLY

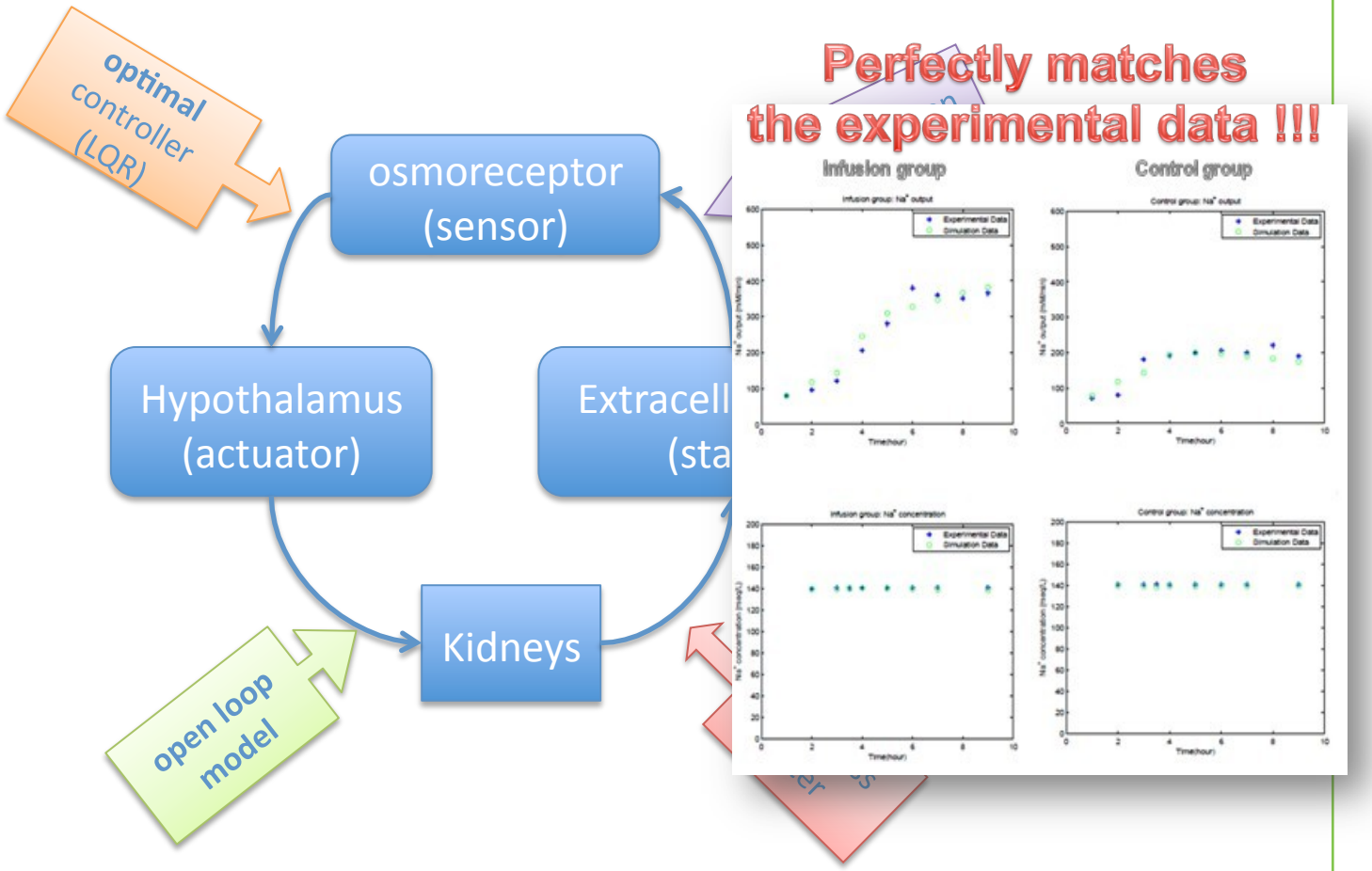
"Hence if too much salt is used for food, the pulse hardens ..."

---- An Ancient Chinese Medicine Book, 2698–2598 BC.



NYU·poly
POLYTECHNIC INSTITUTE OF NEW YORK UNIVERSITY

Closed-Loop Control System



NEW YORK UNIVERSITY

NYU·poly
POLYTECHNIC INSTITUTE OF NEW YORK UNIVERSITY

Leading invention, innovation and entrepreneurship

Allocation of Distributed Generations (DG) in a Power Network

Students: Po-Chen Chen, Qincheng Zhu
Advisers: Profs. Z. P. Jiang, F. De Leon, D. Czarkowski
Control and Telecommunications Research Laboratory, NYU Poly

Project Objectives

I. Develop possible scenarios to distribute DGs into a network.
II. Consider both sizing and placement of DGs.
III. Study the impact of DGs to the utility network.
IV. Key Tools: Markov Chain Monte Carlo method and Gibbs sampling algorithm.

Batch Query Processing for Web Search Engines

Shuai Ding

Joint work with

Josh Attenberg, Ricardo Baeza-Yates, Torsten Suel

Power Network of Our Study

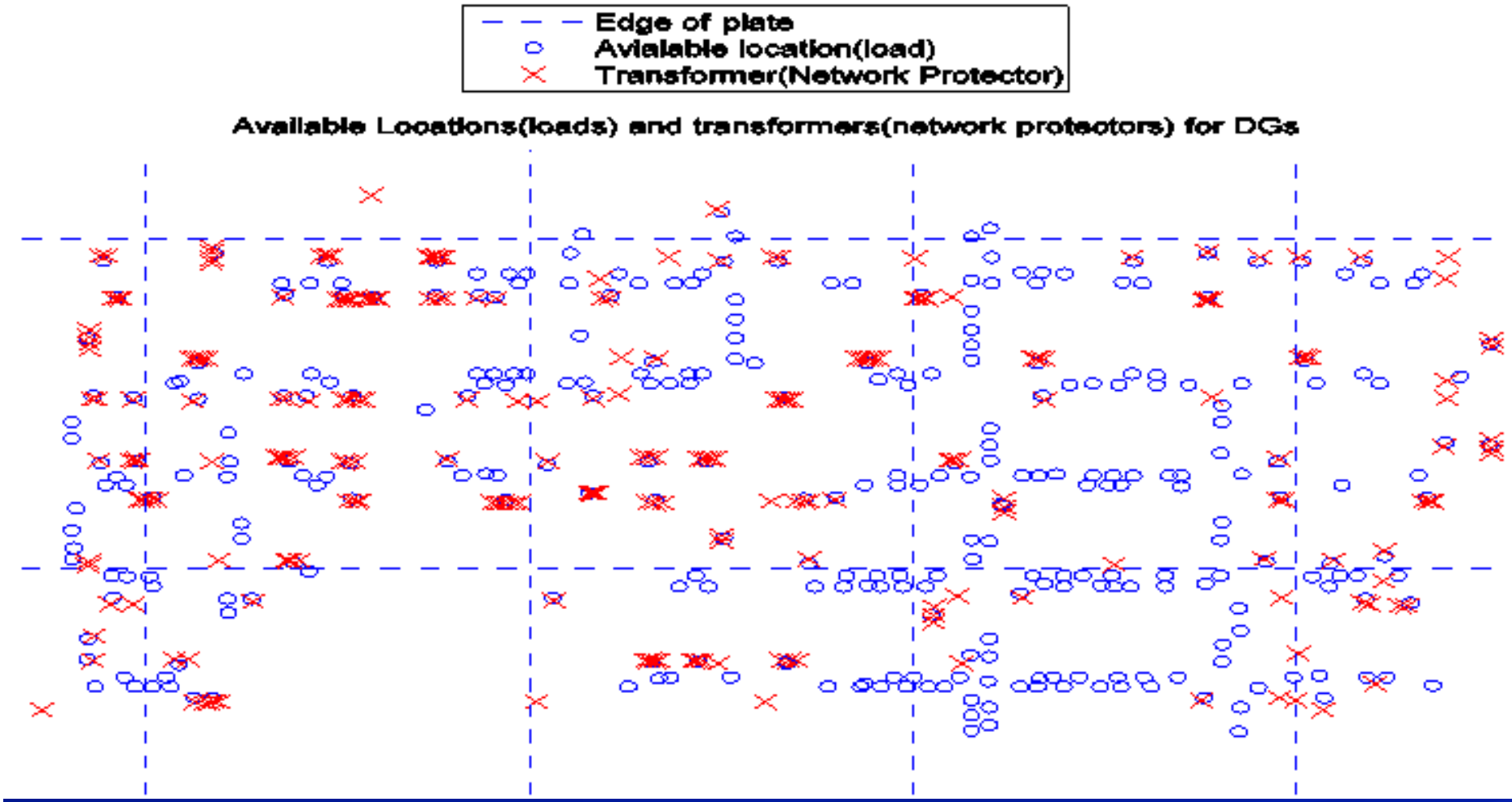


Figure : All available locations (loads) and transformers with network protectors

EMTP Results and Their Analysis

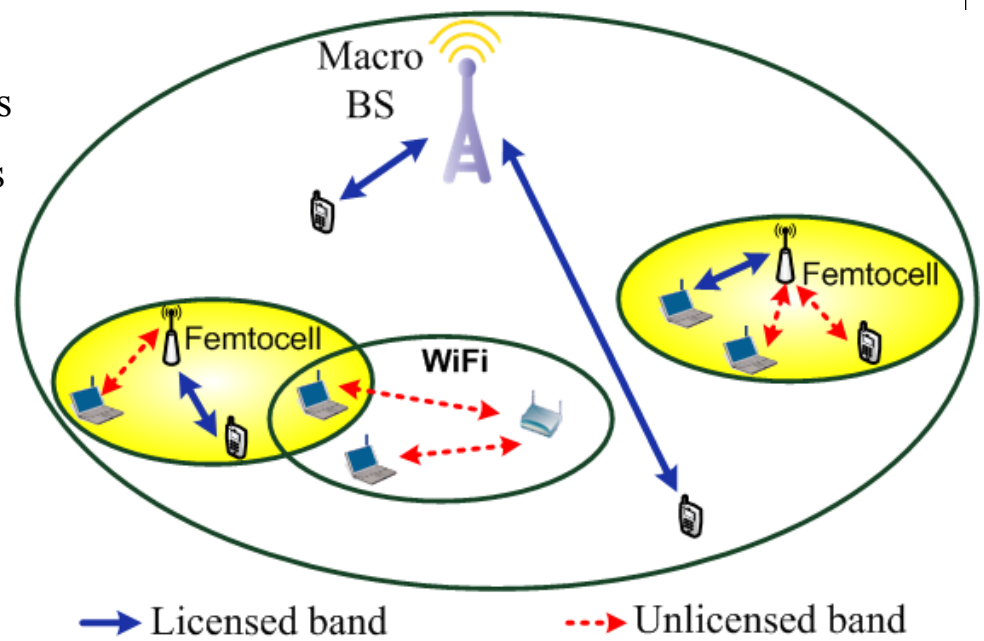
	Voltage of Loads in p.u.			NETWORK PROTECTOR OPEN		DG PROTECTION OPEN	
	Peak value over ±5% limited valuation	Max. Value	Min. VALUE	#	% of total	#	% of total
20% - Light	0	1.041	0.997	0	0.00%	0	0.00%
30% - Light	0	1.020	0.999	0	0.00%	0	0.00%
40% - Light	0	1.021	1.0021	0	0.00%	1	0.45%

Figure : EMTP results

A Framework for Femtocells to Access Both Licensed & Unlicensed Bands

Feilu Liu and Elza Erkip

- Cellular operators are offloading data traffic from licensed spectrum to unlicensed bands
  - E.g., AT&T owns 23,000+ WiFi hotspots
- Femtocells are being deployed to increase cellular capacity
- Femtocells can be a perfect platform to access both licensed & unlicensed bands, and offload traffic from licensed to unlicensed bands in a *smart* way.
  - Interference level in licensed bands
  - Channel usage in unlicensed bands
- We propose that femtocells opportunistically access unlicensed bands on top of licensed cellular bands.



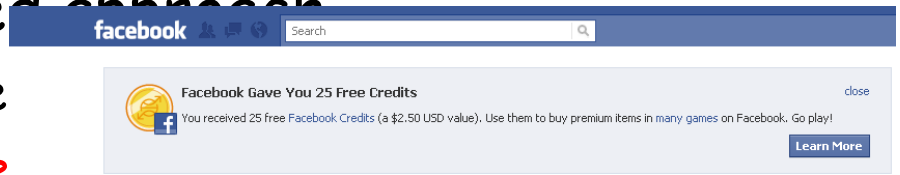
Bayesian-inference Based Recommendation in Online Social Networks

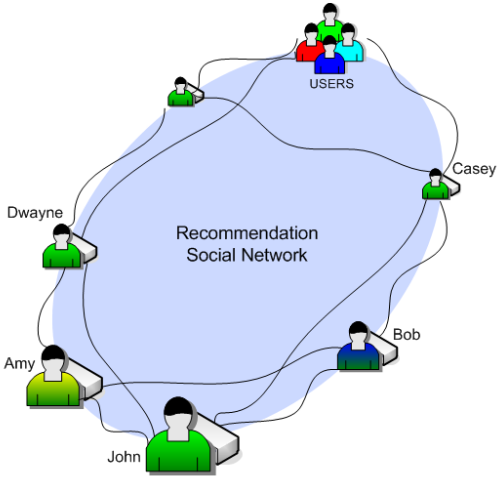
Xiwang Yang, Yang Guo*, and Yong Liu

* Technicolor (Thomson)

Bayesian Recommendation in OSN

- CF-based approach
  - people
  (dis)agre
- Exploitin
  - measur
  by condi
  - predic
  friend
    - add
  - set pri
    - add
- Evaluati
  - beat M
  dataset.





s

and indirect

ers

w users

MAE on Epinions

- Distributed Protocol Design, Prototype in Facebook

NYU·poly
POLYTECHNIC INSTITUTE OF NYU

Optimal Distributed Voltage Control in Smart Grid

Student: Li Yu, Mingyu Li
Advisor: Dariusz Czarkowski

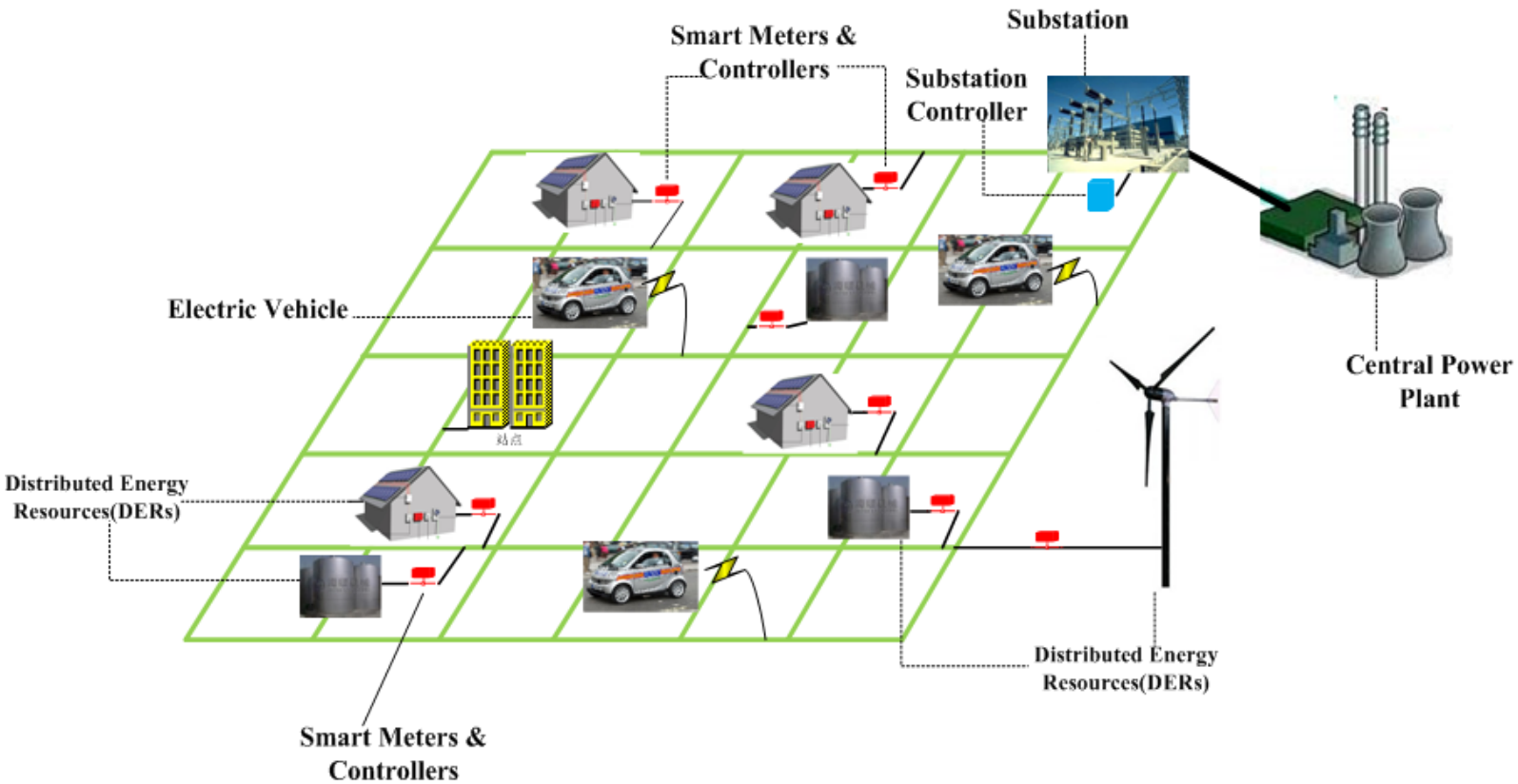
Center for Advanced Technology in Telecommunications
NYSTAR designated Center For Advanced Technology

NEW YORK UNIVERSITY

NYU·poly

POLYTECHNIC INSTITUTE OF NYU

Smart Grid with Smart Controllers and Distributed Energy Sources

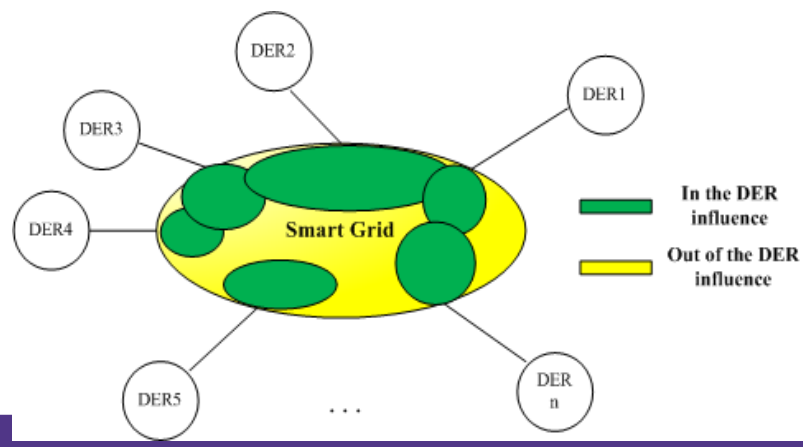


Technology in Telecommunications

NYSTAR designated Center For Advanced Technology

Control Algorithm

$$S = \begin{bmatrix} s_{11} & s_{12} & s_{13} & s_{14} & s_{15} & s_{16} & s_{17} & s_{18} & \cdots & s_{1n} \\ s_{21} & s_{22} & s_{23} & s_{24} & s_{25} & s_{26} & s_{27} & s_{28} & \cdots & s_{2n} \\ s_{31} & s_{32} & s_{33} & s_{34} & s_{35} & s_{36} & s_{37} & s_{38} & \cdots & s_{3n} \\ s_{41} & s_{42} & s_{43} & s_{44} & s_{45} & s_{46} & s_{47} & s_{48} & \cdots & s_{4n} \\ s_{51} & s_{52} & s_{53} & s_{54} & s_{55} & s_{56} & s_{57} & s_{58} & \cdots & s_{5n} \\ s_{61} & s_{62} & s_{63} & s_{64} & s_{65} & s_{66} & s_{67} & s_{68} & \cdots & s_{6n} \\ s_{71} & s_{72} & s_{73} & s_{74} & s_{75} & s_{76} & s_{77} & s_{78} & \cdots & s_{7n} \\ s_{81} & s_{82} & s_{83} & s_{84} & s_{85} & s_{86} & s_{87} & s_{88} & \cdots & s_{8n} \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ s_{m1} & s_{m2} & s_{m3} & s_{m4} & s_{m5} & s_{m6} & s_{m7} & s_{m8} & \cdots & s_{mn} \end{bmatrix} \Rightarrow \tilde{S} = \begin{bmatrix} s_{a1} & s_{c2} & & & & & & & \cdots & \\ s_{b1} & s_{d2} & & & & & & & \cdots & \\ & & s_{e3} & s_{f4} & s_{g5} & & & & \cdots & \\ & & s_{h3} & s_{i4} & s_{j5} & & & & \cdots & \\ & & s_{k3} & & s_{l5} & & & & \cdots & \\ & & & & & s_{m6} & s_{p7} & & \cdots & \\ & & & & & s_{n6} & s_{q7} & & \cdots & \\ & & & & & s_{o6} & s_{r7} & s_{s8} & \cdots & \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ & & & & & & & & \cdots & s_{xn} \end{bmatrix}$$



Center for Advanced Technology in Telecommunications

NYSTAR designated Center For Advanced Technology

NYU POLY WiMAX 4G PROJECT

ABHIJEET MATE

HECTOR MORENO

SANJAY GOYAL

KILLOL MUNSHI

DEEPIKA LAMBA

PROFESSOR THANASIS KORAKIS

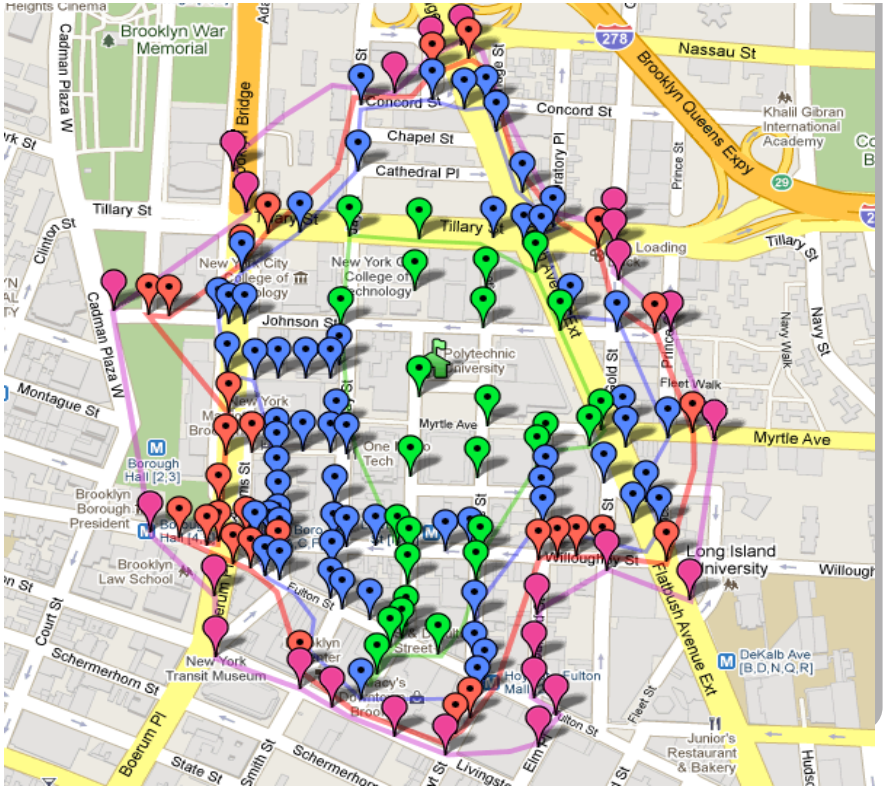
POLYTECHNIC INSTITUTE OF NYU

- A WiMAX 4G network have been installed at NYU:poly
- The efforts are funded by a GENI grant
- The network is based on a NEC Base Station with partial of the MAC functionality implemented in open source software
- It supports applications for mobile devices over high speed connectivity

The IDU, the server, the antenna and the ODU

- Testing of the network has been done using WiMAX clients such as laptops, AWB dongles and HTC EVO phones
- Measurements show good coverage in the grater area of Downtown Brooklyn
- Today we will show a demo on real time conference call that involves mobility

WiMAX clients of the Poly network



The coverage range of the Poly WiMAX network

A Demo of ParkNet System using WiMAX GENI Network of NYU Poly

TONG JIN

SANJIT KAUL

BIN ZAN

ABHIJEET MATE

HECTOR MORENO

SANJAY GOYAL

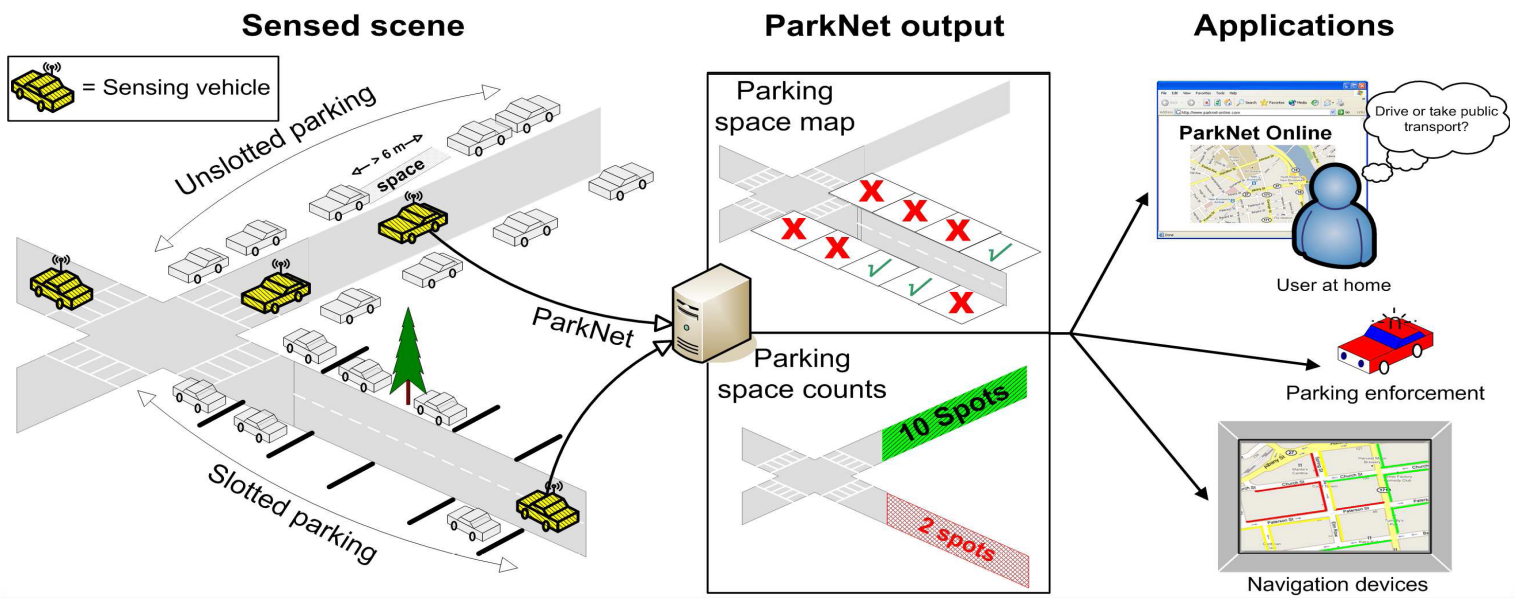
KILLOL MUNSHI

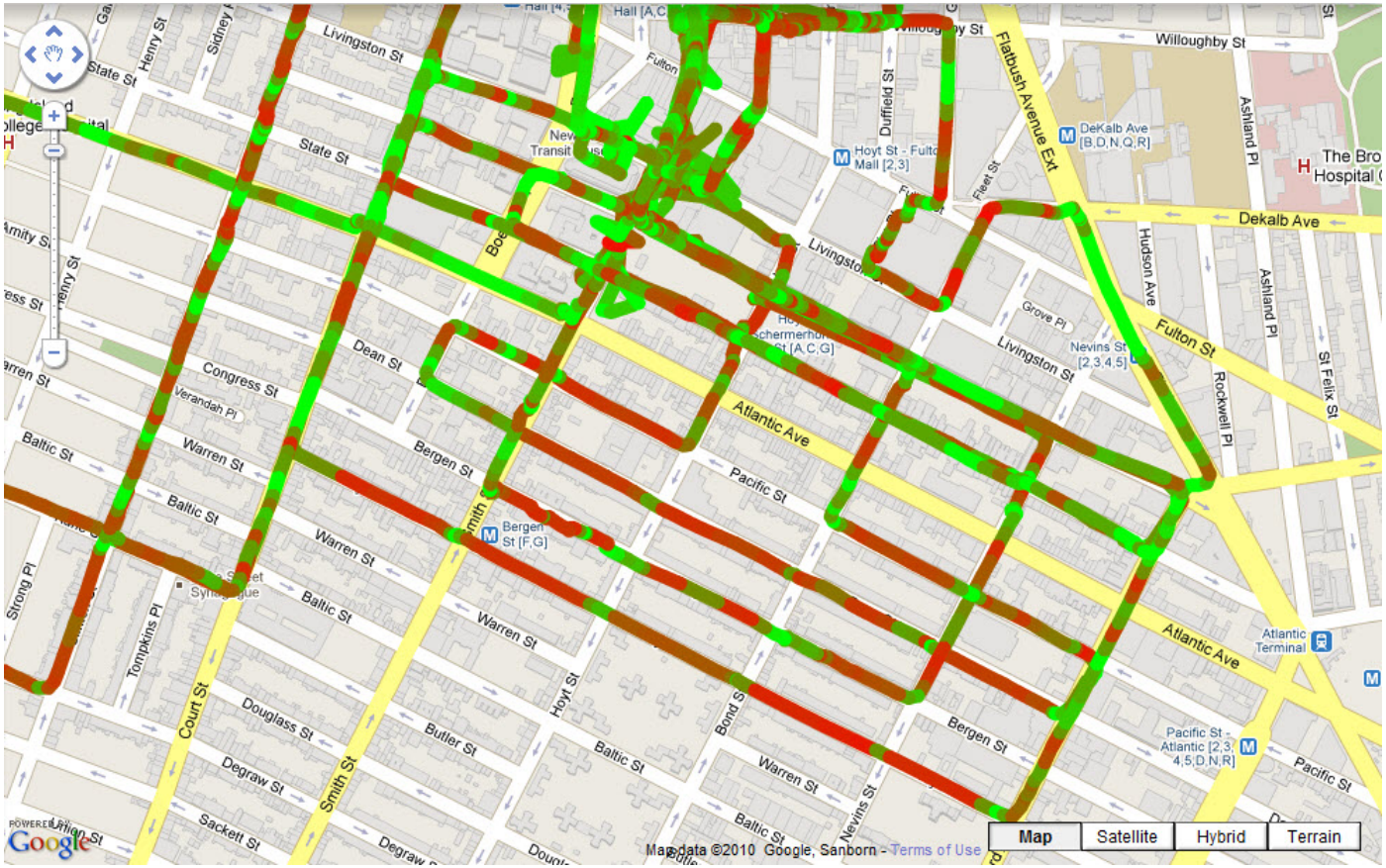
DEEPIKA LAMBA

PROFESSOR MARCO GRUTESER
RUTGERS UNIVERSITY

PROFESSOR THANASIS KORAKIS
POLYTECHNIC INSTITUTE OF NYU

- Demonstration of the synergy of the WiMAX GENI network at NYU Poly with the ParkNet mobile system
- A joint GENI demo between NYU:Poly, Rutgers, NICTA
- 8 cars equipped with ultrasound sensor and GPS receivers drove around Brooklyn, collecting information about available parking spots.
- The data is forwarded though the 4G WiMAX network of NYU:Poly to a central server which builds a real time map of parking availability though a real time application.
- Different routes were covered by the vehicles, the data was successfully presented in real-time
- Recorder videos of real-time traces on a Brooklyn map will be presented in this demo





Real-time map of parking availability in downtown Brooklyn.

Sip Filter Hardware Implementation

Jianping Quan

Nallammai Sekar

Ramesh Karri

11/08/10

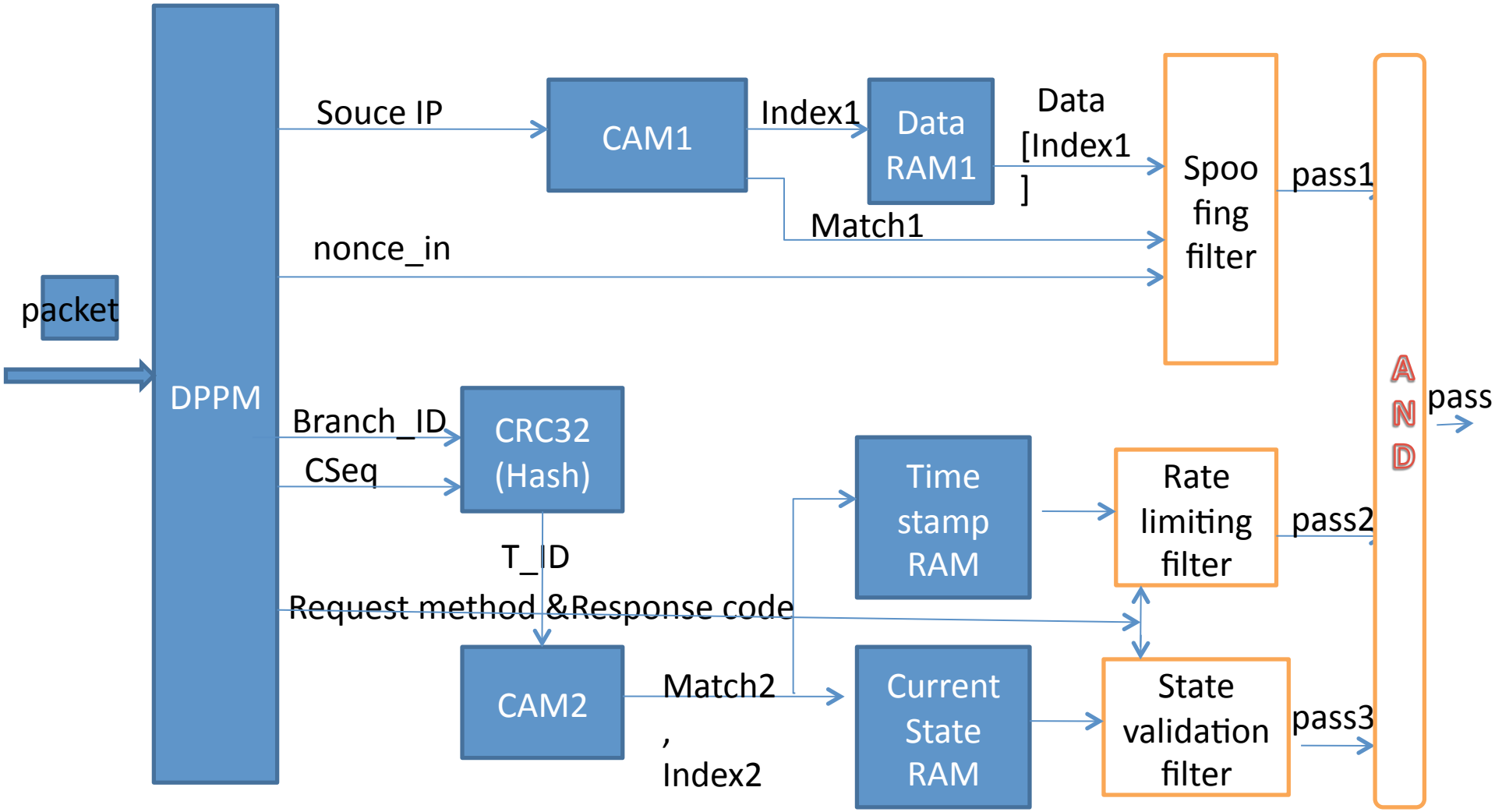
Session Initiation Protocol (SIP)

- Application-layer signaling protocol
- Text -based protocol like HTTP
- Runs on static port 5060
- Used to create and terminate sessions and to negotiate media stream parameters
    - Type of media
    - Transport protocol used
    - Port numbers for media transfer
  - Defined using session description protocol (SDP)
  - SDP is transported along with the SIP packet

Motivation

- New security vulnerabilities at the application layer
  - SIP over UDP – spoof SIP requests
    - Registration/Call Hijacking
    - Session teardown
    - Request and Response flooding
  - SIP packet format - Plain text
    - Easy to modify and intercept
- Layer-3 filters are not sufficient
  - Arbor Networks, Cisco (formerly Riverhead Networks), TopLayer, Mazu networks, Juniper etc
- Key differentiator: Application layer (Layer 7) filtering
  - Prototype demonstration: Columbia-Verizon
  - Carrier class implementation: NYU-Poly Verizon and Cisco

Basic Data Flow



- CAM1 and CAM2 are both 32-bit by 4k;
- RAM1 is about 26bytes by 4k; Time stamp RAM is 35-bit by 4k; Current state RAM is 3-bit by 4k.

- Thanks

NYU·poly
POLYTECHNIC INSTITUTE OF NYU

Video Conferencing with Adaptive FEC and Video Rate Allocation

Yen-Fu Ou, Minyi Yang, Yao Wang
Polytechnic Institute of NYU

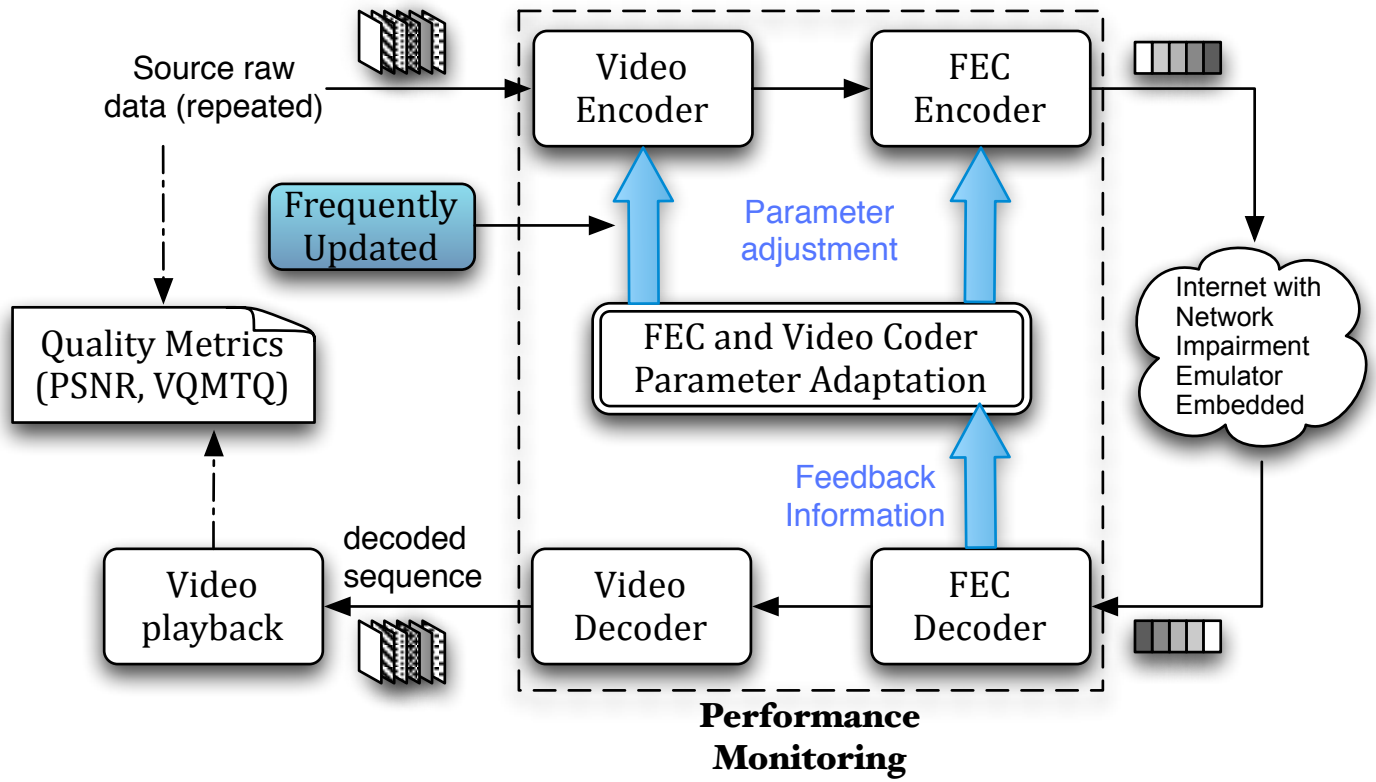
Center for Advanced Technology in Telecommunications
NYSTAR designated Center For Advanced Technology

NEW YORK UNIVERSITY

Motivation

- ARQ induces unacceptable delay for video conferencing
- Application layer FEC is necessary to recover lost packets
- Both the total data rate (R_T) and the allocation between video rate (R_V) and FEC redundancy (α) should be adjusted based on network feedback
- Establish a testbed on which our adaptation algorithm can be validated over real network impairments.

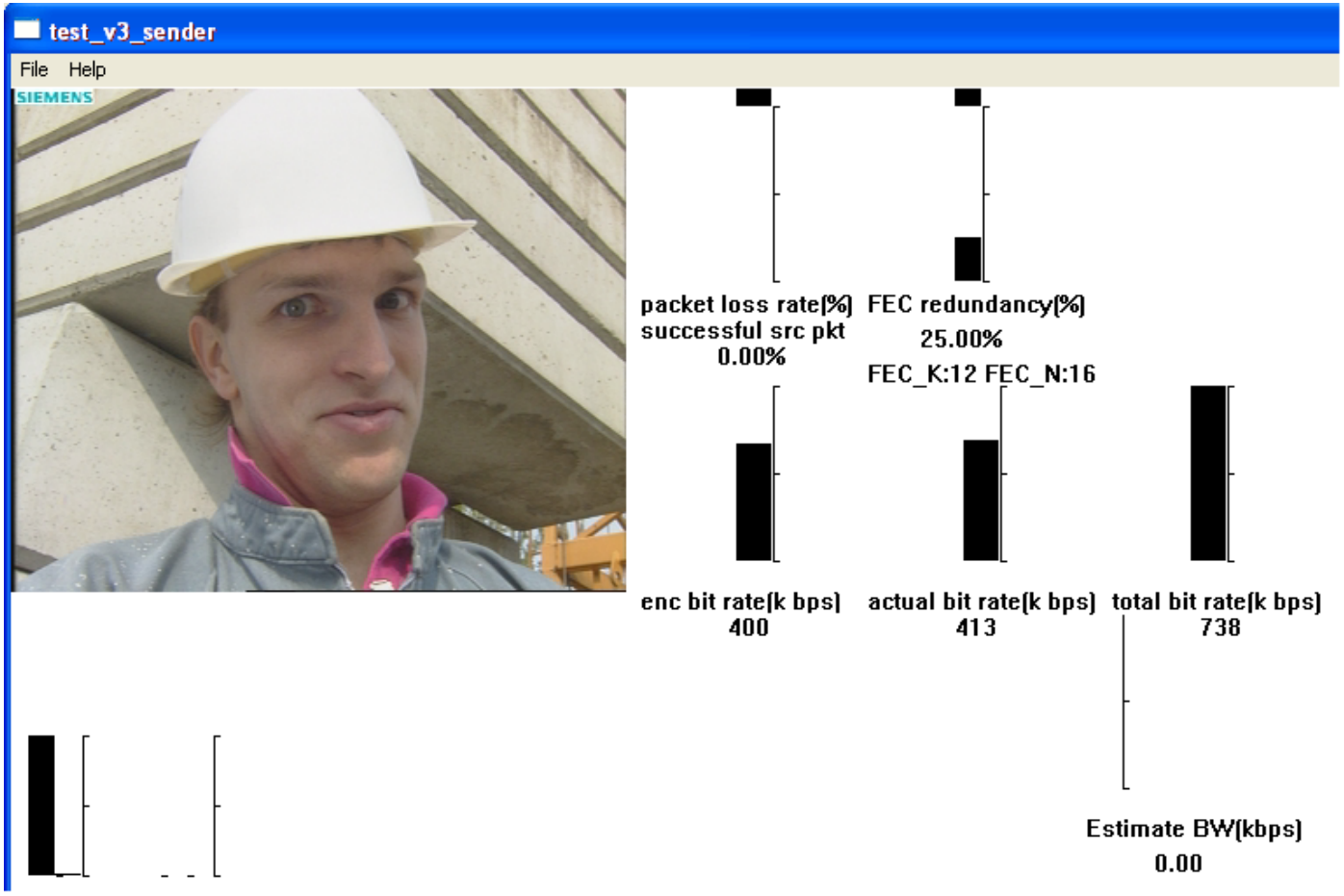
Flow Diagram of Proposed Scheme



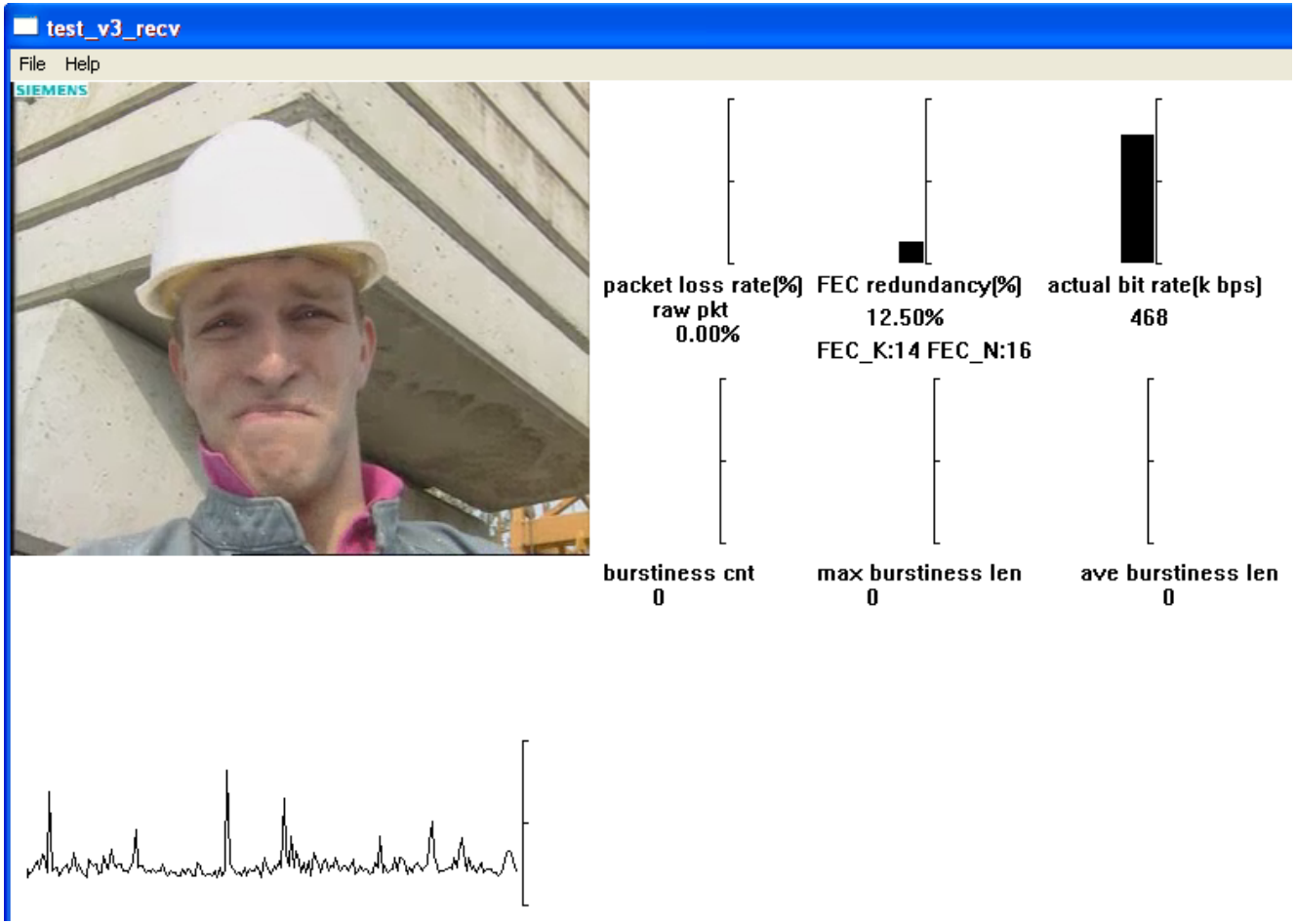
FEC and Video Rate Allocation

- Total data rate (R_T) is adjusted according to the estimated network throughput based on the delay (RTT) and packet loss (P)
- Given R_T, allocation between video and FEC is adapted based on the raw and residual packet loss rate
- Given R_V, we choose the frame rate at which to code the video, based on prior subjective quality test results.
- For More Details, please see our poster and demonstration !!

Sender


test_v3_sender
File Help
SIEMENS
packet loss rate(%)
successful src pkt
0.00%
FEC redundancy(%)
25.00%
FEC_K:12 FEC_N:16
enc bit rate(k bps)
400
actual bit rate(k bps)
413
total bit rate(k bps)
738
Estimate BW(kbps)
0.00

Receiver


test_v3_recv
File Help
SIEMENS
packet loss rate(%)
raw pkt
0.00%
FEC redundancy(%)
12.50%
FEC_K:14 FEC_N:16
actual bit rate(k bps)
468
burstiness cnt
0
max burstiness len
0
ave burstiness len
0

Perceptual Video Quality Assessment on a Mobile Platform Considering both Spatial and Quantization

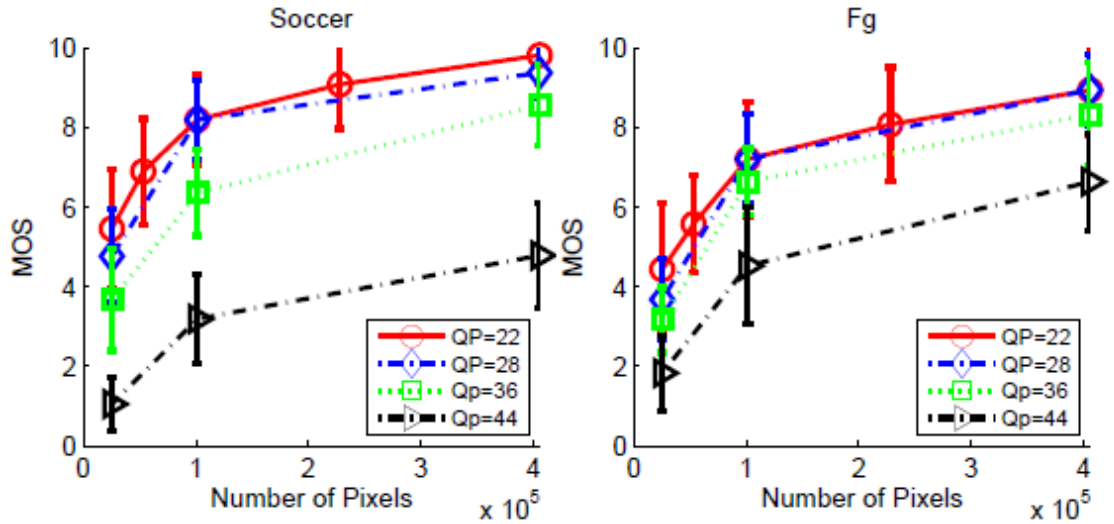
Yuanyi Xue, Yen-Fu Ou, Zhan Ma, Yao Wang
Polytechnic Institute of NYU

- Motivation
  - Video can be coded at different frame size (s), frame rate (t) and quantization stepsize (q) and one should choose s,t,q to maximize the perceptual quality for a given rate constraint;
  - Our prior work investigated the impact of t and q on perceptual quality and rate;
  - This work examines the impact of s and q on perceptual quality.
- Test Protocol
  - 7 sequences, 5 spatial resolutions, 4 QPs.
  - Single stimulus.
  - Developed a subjective test interface using a smartphone platform. (TI Zoom 2 with Android)

Perceptual Video Quality Assessment on a Mobile Platform Considering both Spatial and Quantization

Yuanyi Xue, Yen-Fu Ou, Zhan Ma, Yao Wang
Polytechnic Institute of NYU

- Results



  - MOS vs. Spatial Resolution follows a falling exponential decay
- More Results – See poster

NYU·poly
POLYTECHNIC INSTITUTE OF NYU

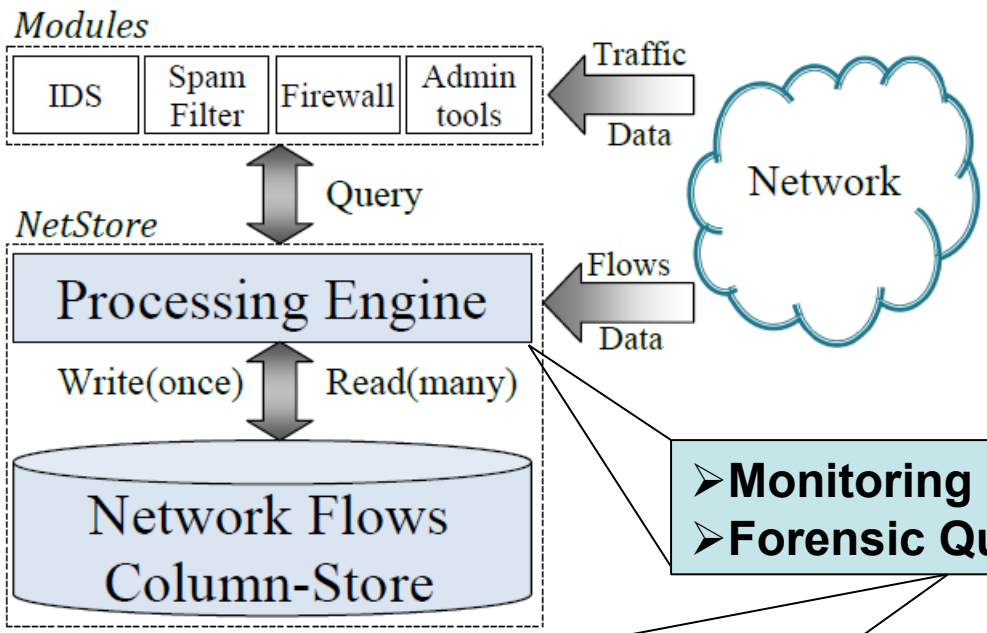
An Efficient Querying Framework For Network Monitoring and Forensics

Paul Giura

PhD Student
Polytechnic Institute of NYU

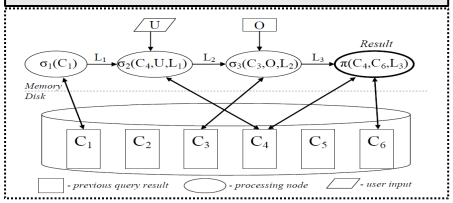
Center for Advanced Technology in Telecommunications

NYSTAR designated Center For Advanced Technology



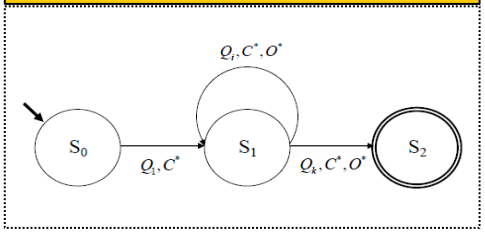
- Monitoring Queries
- Forensic Queries

Simple Queries

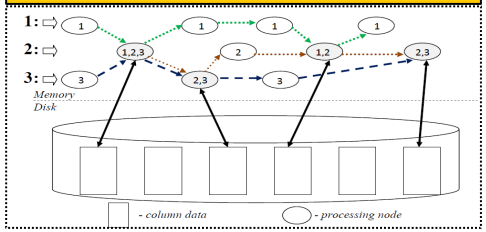


Complex Queries

Sequential



Batch



NYU·poly POLYTECHNIC INSTITUTE OF NYU

CATT Center for Advanced Technology in Telecommunications

NYSTAR® designated Center For Advanced Technology