



Understanding Risk – Performance Trade-off at Point of Entry Systems

Bojan Cukic
West Virginia University

DHS University Summit, March 2009 ©

**National Center for
Border Security and Immigration**

Research Lead: The University of Arizona



Systems Approach: Port of Entry

Acceptance, modality, quality?

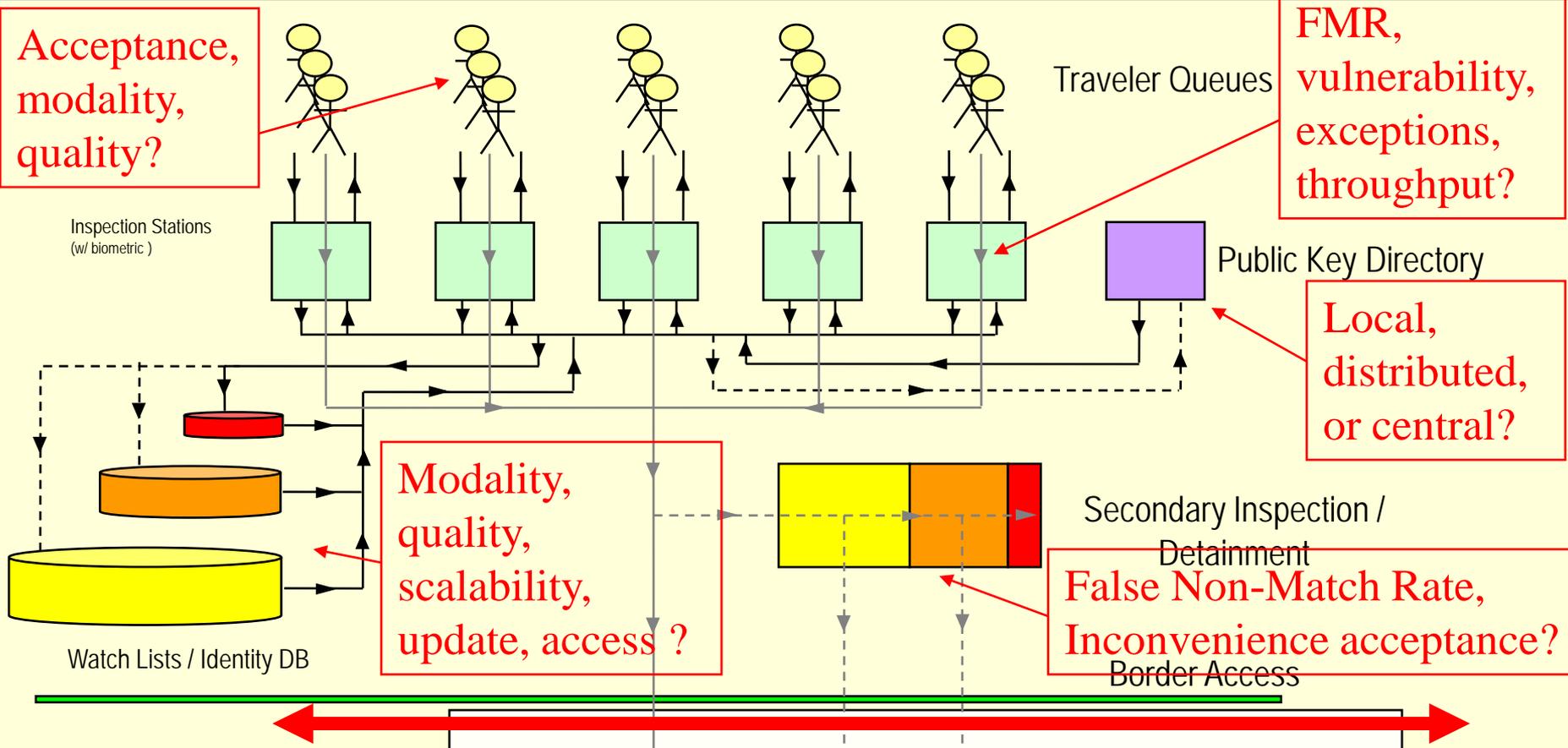
Modality, FMR, vulnerability, exceptions, throughput?

Local, distributed, or central?

Modality, quality, scalability, update, access ?

False Non-Match Rate, Inconvenience acceptance?

False Match Rate



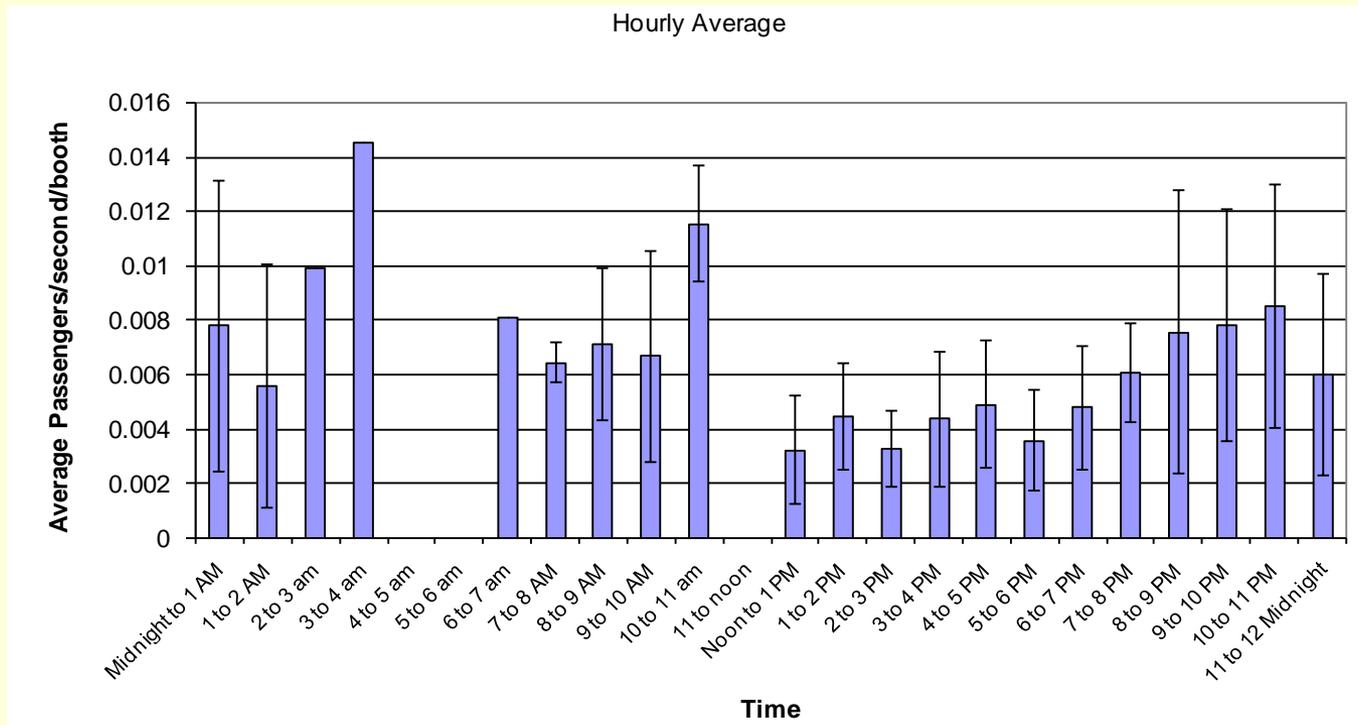
Legend

- > =Required Signal
- - -> =Optional Signal
- > = Movement
- - -> =Optional Movement



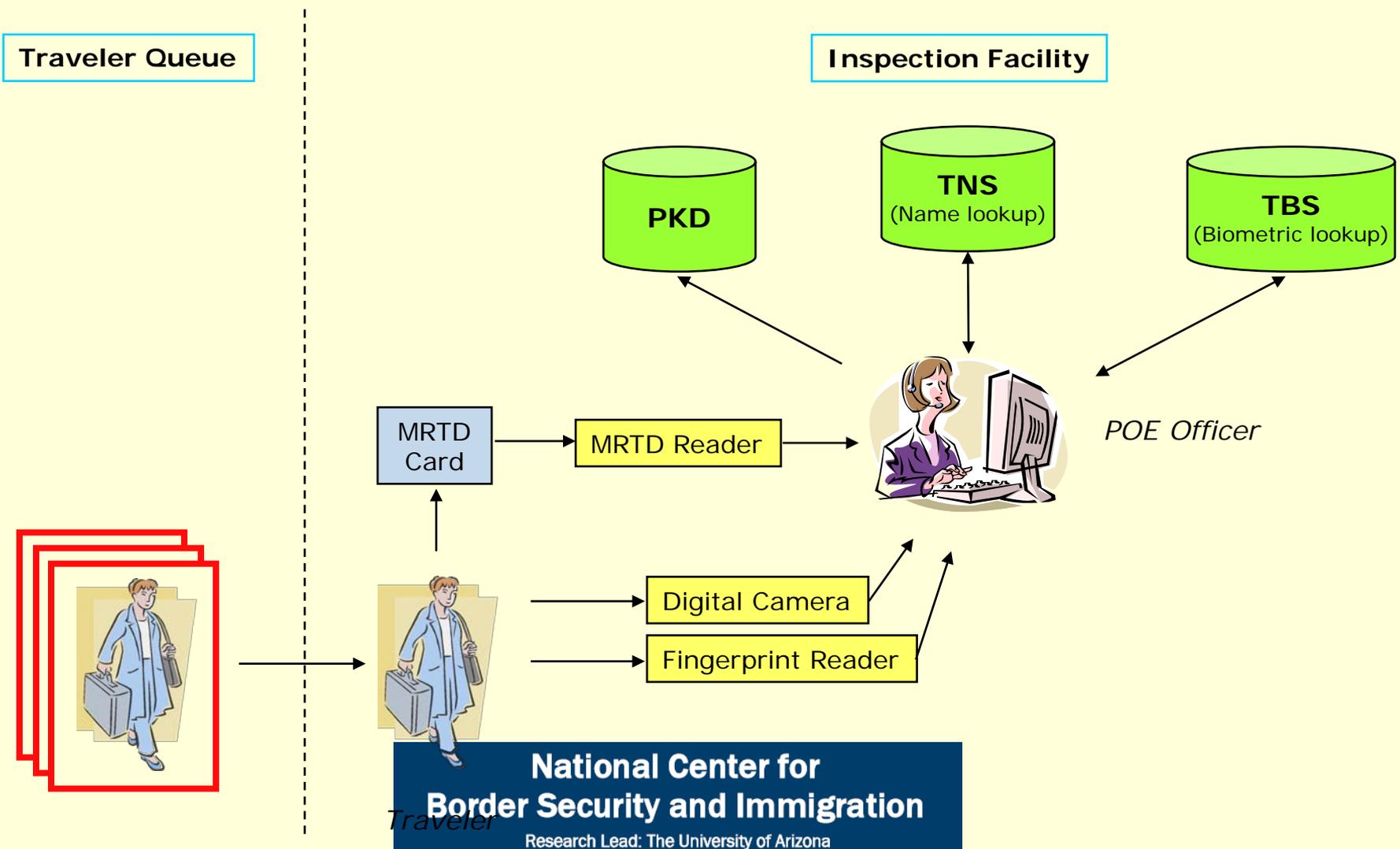
Travelers arrival

- Arrival information from December 2007 in one of the terminals at the Dulles International Airport



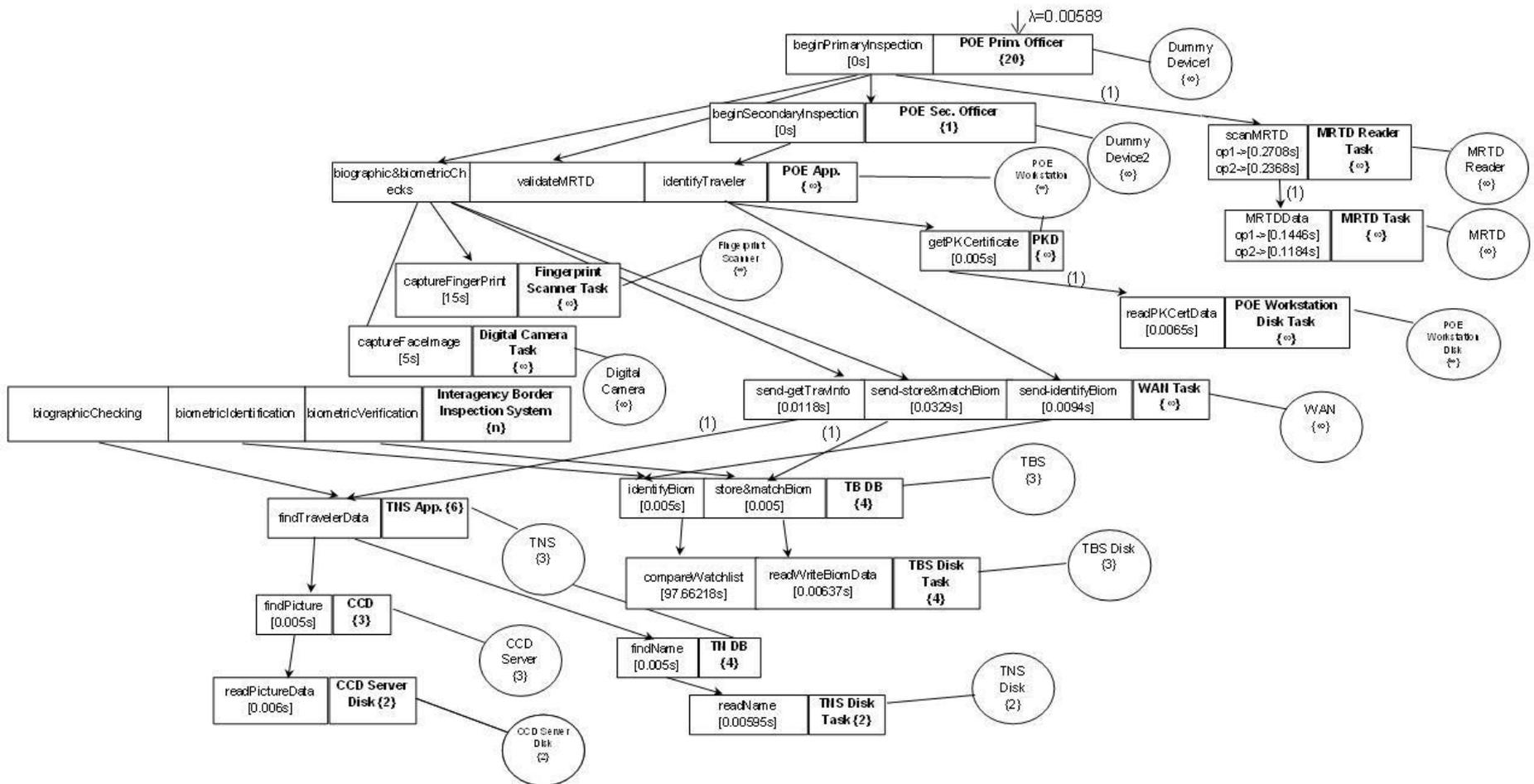


An Airport Inspection System



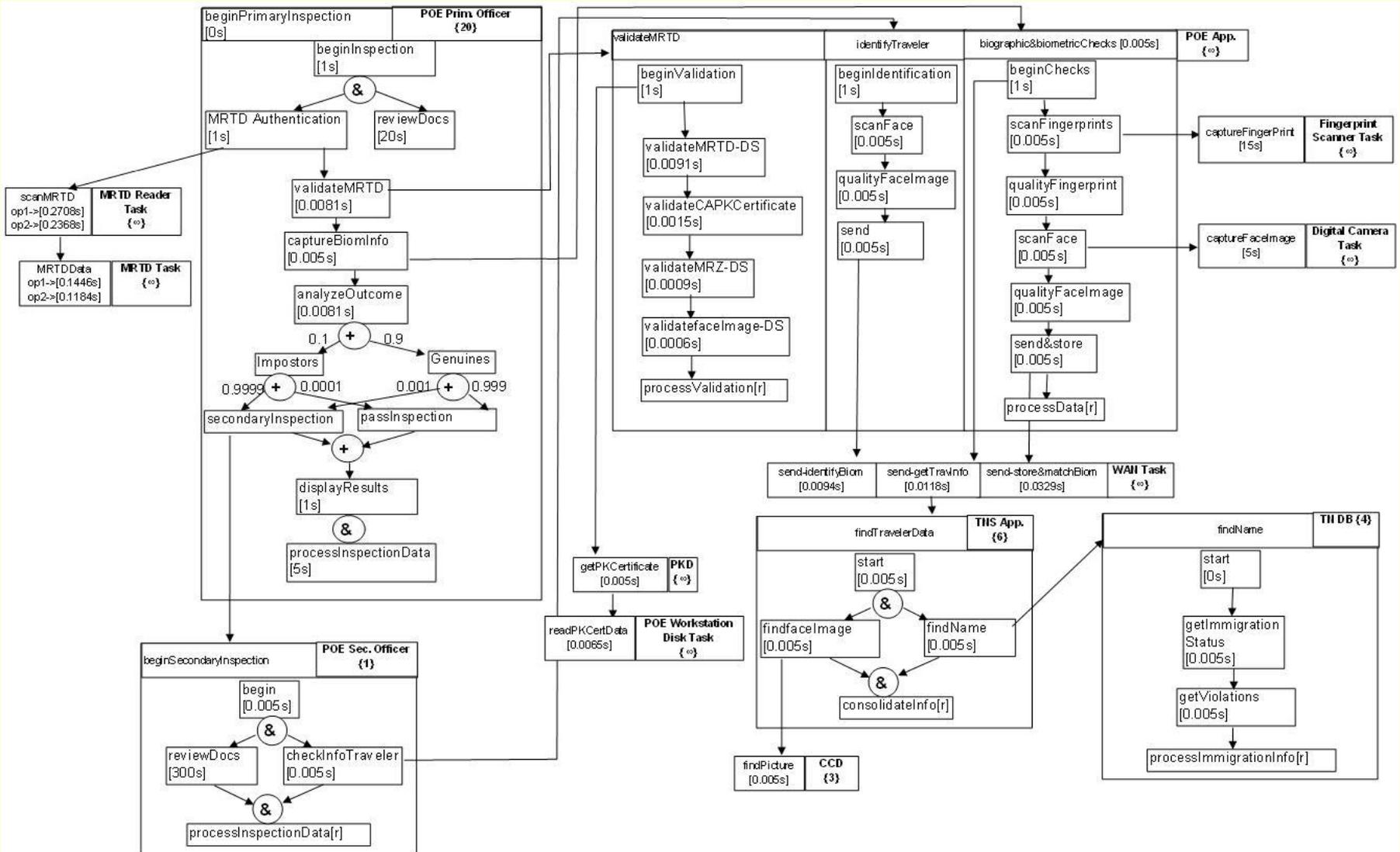


Layered Queuing Network Model





Layered Queueing Network Model



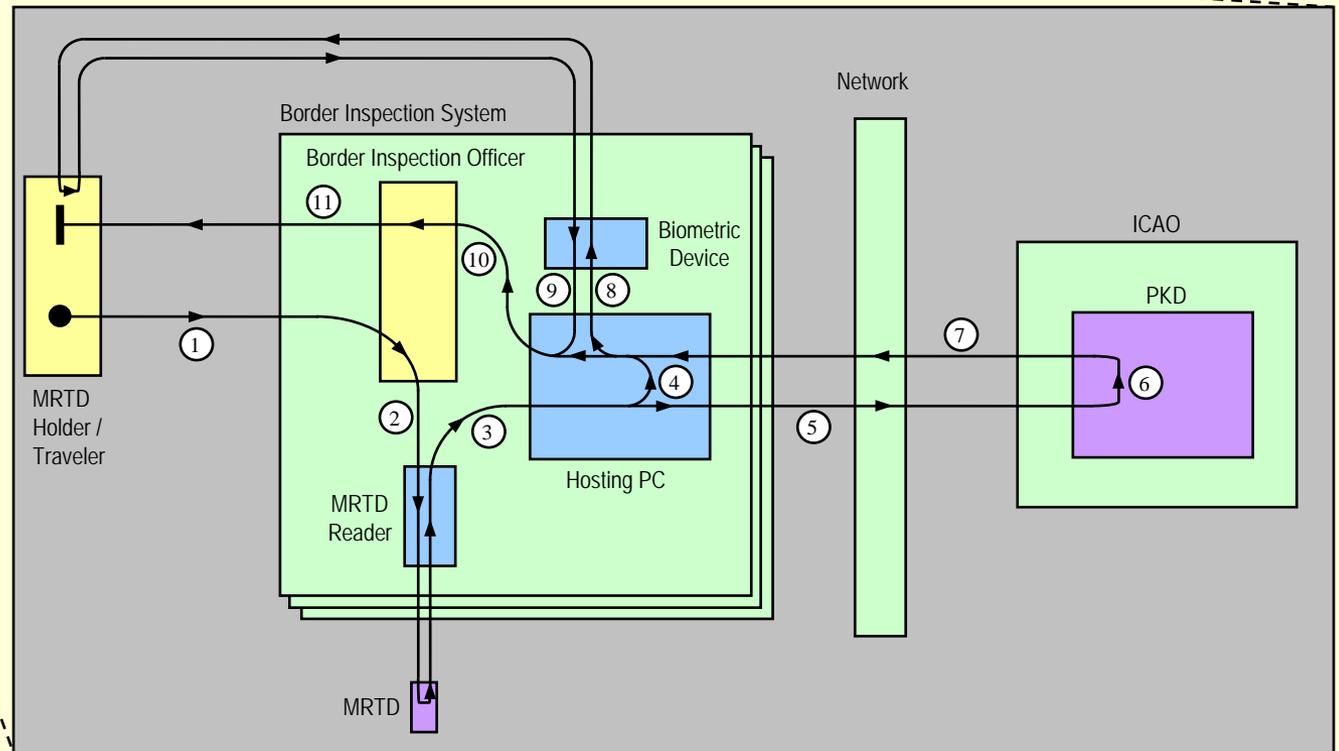
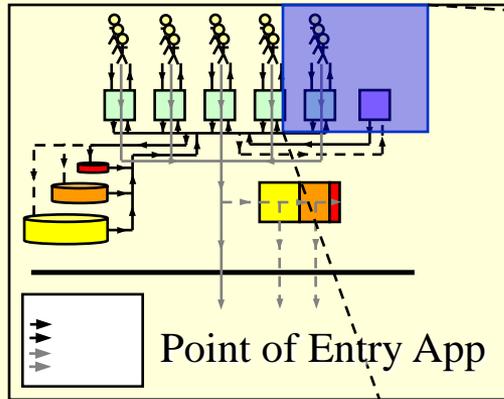


Performance Analysis: An Example

- **Complex system requirements and design tradeoffs.**
 - Point-of-entry applications, digital passports.
 - *How to optimally organize access to national public keys.*
 - Acronyms
 - ICAO-International Civil Aviation Organization
 - MRTD-Machine Readable Travel Document
 - PKD-Public Key Directory, CA – Certificate Authority
- **Goals**
 - Identify possible architectural designs for implementation of PKI subsystem at points-of-entry.
 - **Suggest “best” solution based on performance and security modeling early in the development lifecycle.**



ICAO MRTD PKD



**National Center for
Border Security and Immigration**

Research Lead: The University of Arizona



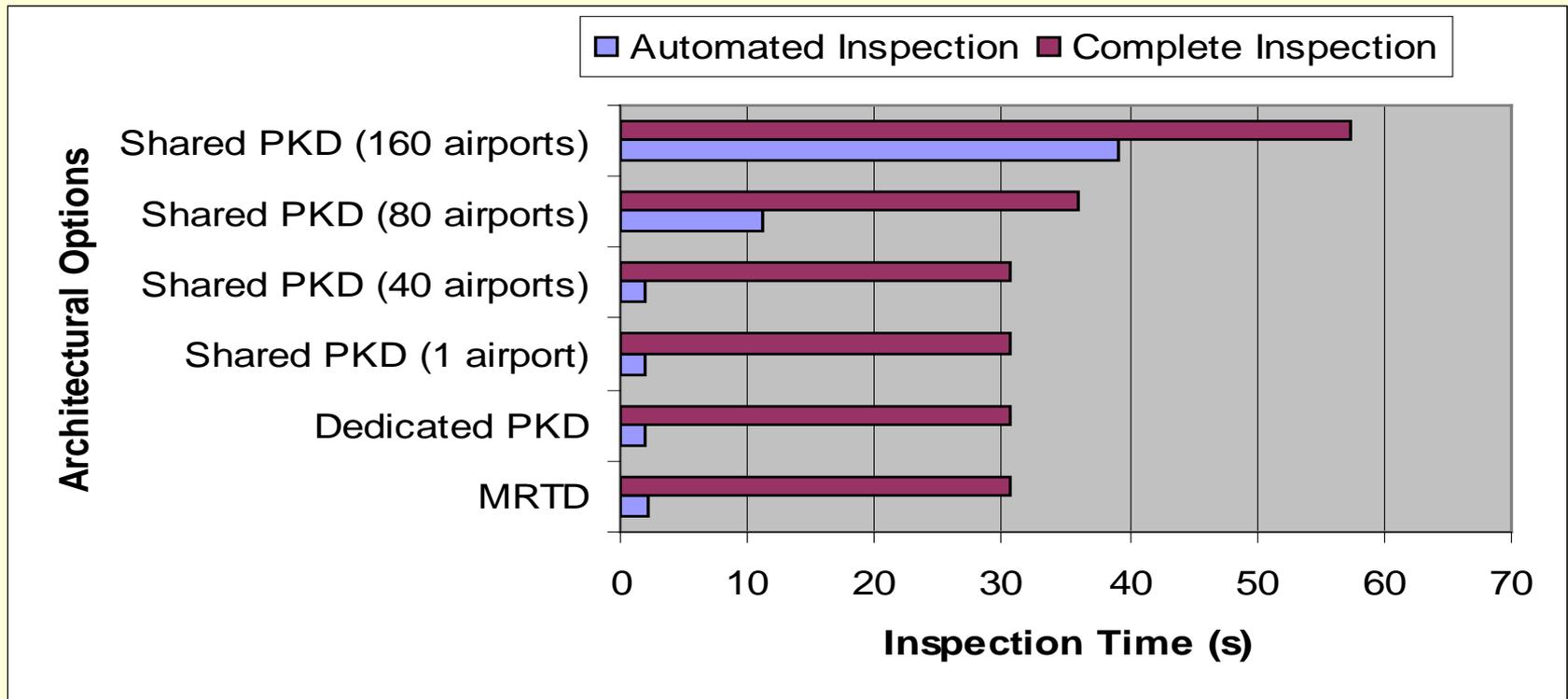
Architectural Differences

- **One Key Distribution Access Point**
 - The simplest distribution scheme, single centralized copy of the PKD.
 - Network delay a function of networking infrastructure and CA PKD request response time.
- **Localized PKDs**
 - A “middle-ground” architecture.
 - A local copy of the PKD at each port of entry (POE).
 - The network delay greatly reduced.
 - Decisions must be made on when and how to update the CA PKD.
- **Border Inspection Site Replicated PKD**
 - The most involved PKD distribution scheme for participating countries.
 - Complex design decisions regarding update/synchronization schemes, times, and frequencies.
 - In theory, this scheme eliminates network traffic delays (except for the updates).



Performance Results

Primary Inspection Time





Performance Results

Response Time and Resource Utilization

80 Airports					
PKD #	Inspection Time (s)	Waiting Time (m)	PKD DB Utilization	PKD Proc. Utilization	PKD Disk Utilization
1	36.09	30	0.9995	0.2769	0.7226
2	30.67	26	0.7406	0.2052	0.5354
3	30.67	26	0.4942	0.1369	0.3573
4	30.67	26	0.3707	0.1027	0.2680
5	30.67	26	0.2965	0.0822	0.2144

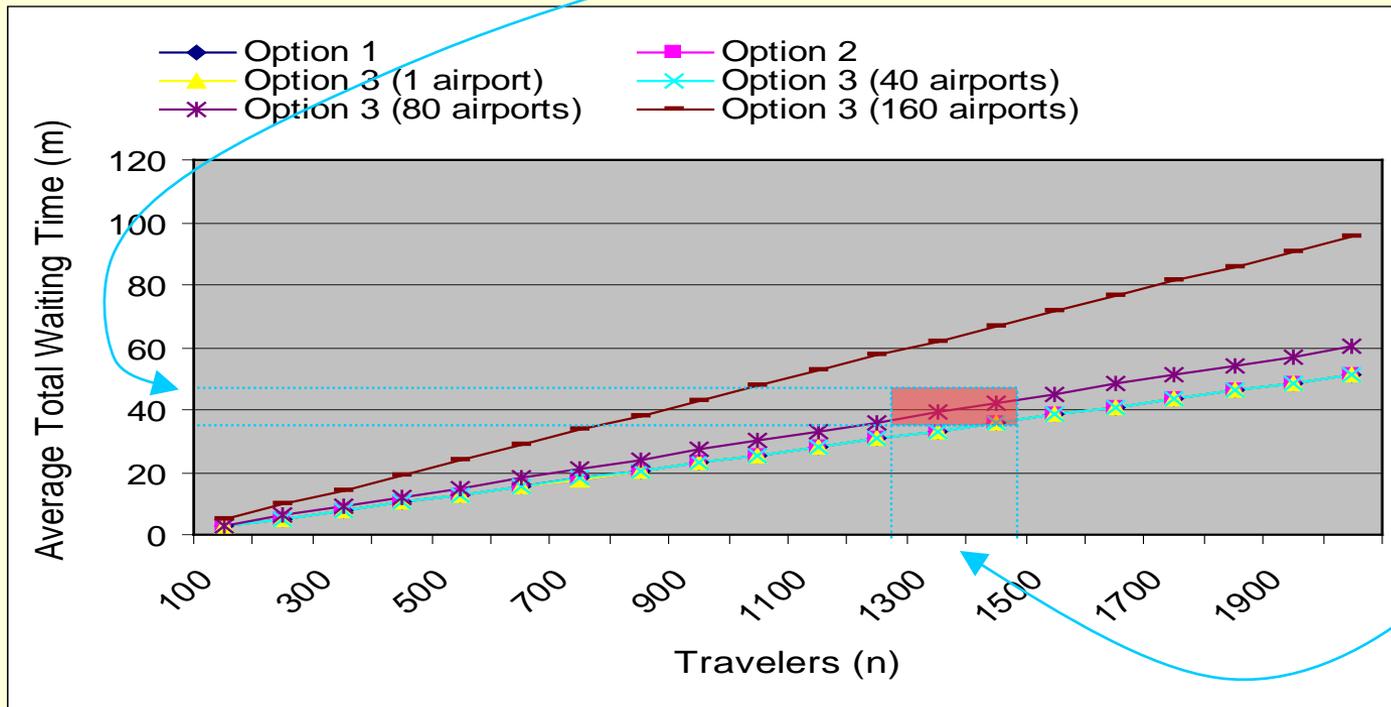
160 Airports					
PKD #	Inspection Time (s)	Waiting Time (m)	PKD DB Utilization	PKD Proc. Utilization	PKD Disk Utilization
1	57.28	48	0.9999	0.2770	0.7229
2	35.98	30	0.9999	0.2770	0.7230
3	30.73	26	0.9746	0.2700	0.7046
4	30.67	26	0.7381	0.2045	0.5336
5	30.67	26	0.5907	0.1636	0.4270



Performance Results

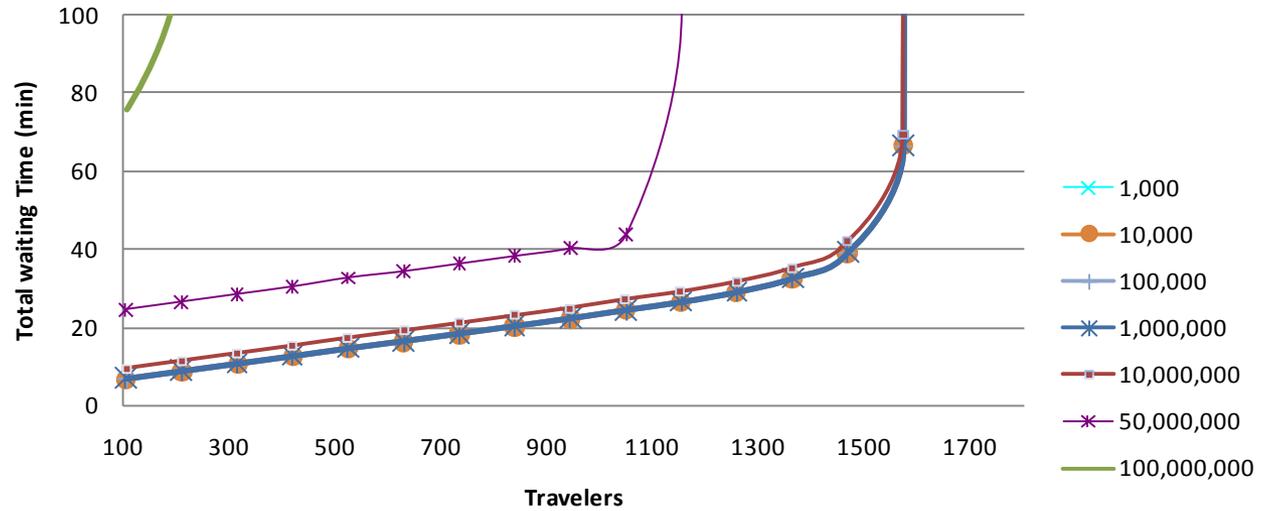
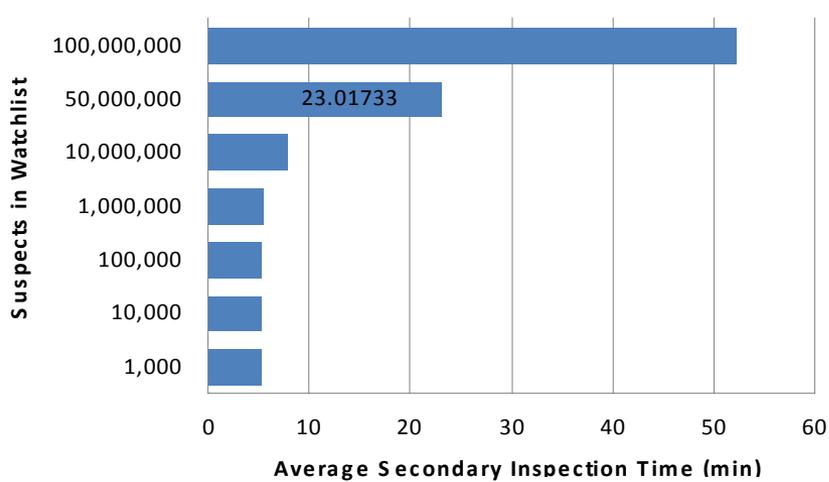
Validation (2)

	Scenario	Primary queue average wait time (min.)	Change in average wait time (min.)	Primary queue maximum length (# people) ⁷⁸	Change in queue length
0	Base Case ("as-is")	30.3 +/-4.6	-	1190+/-94	-
1	US-VISIT (NIV prints & photo)	43.2 +/-5.4	+12.9	1374 +/-108	+184





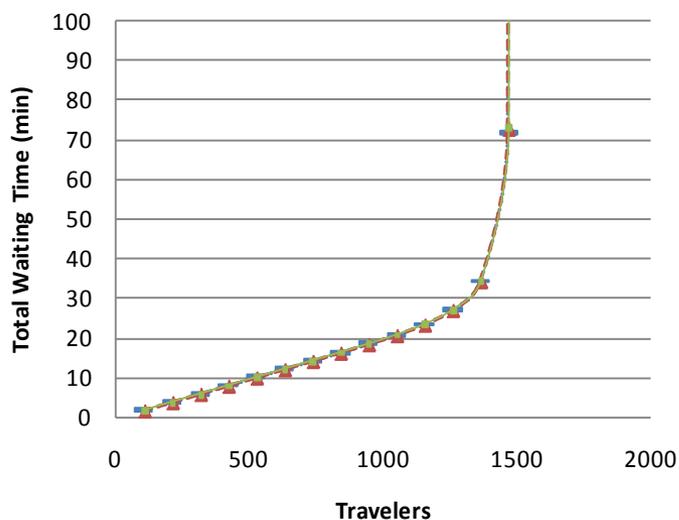
Performance experiments: Watch list size



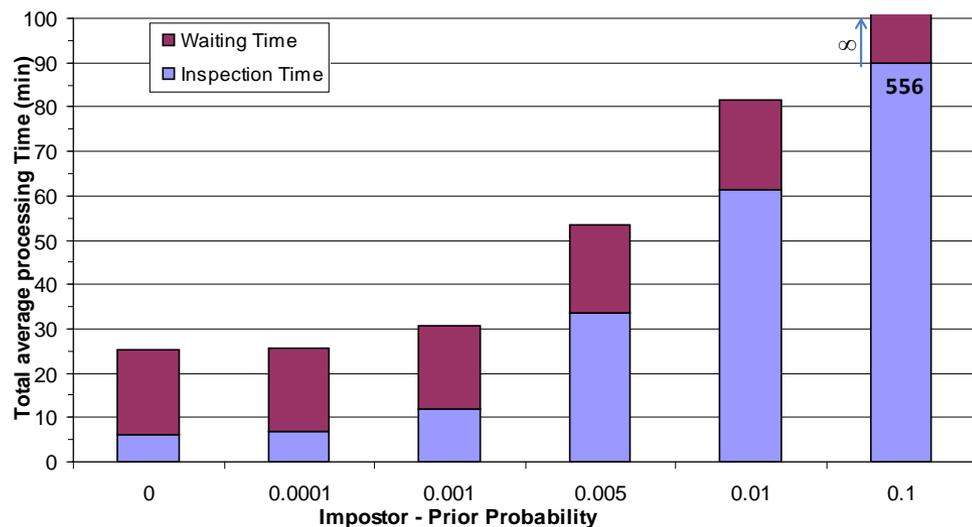
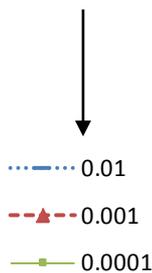


Performance experiments: Biometric system match rates

• Biometric False Match Rates create increased workload at secondary inspection point.



FMR



Impostor prior: 0.01

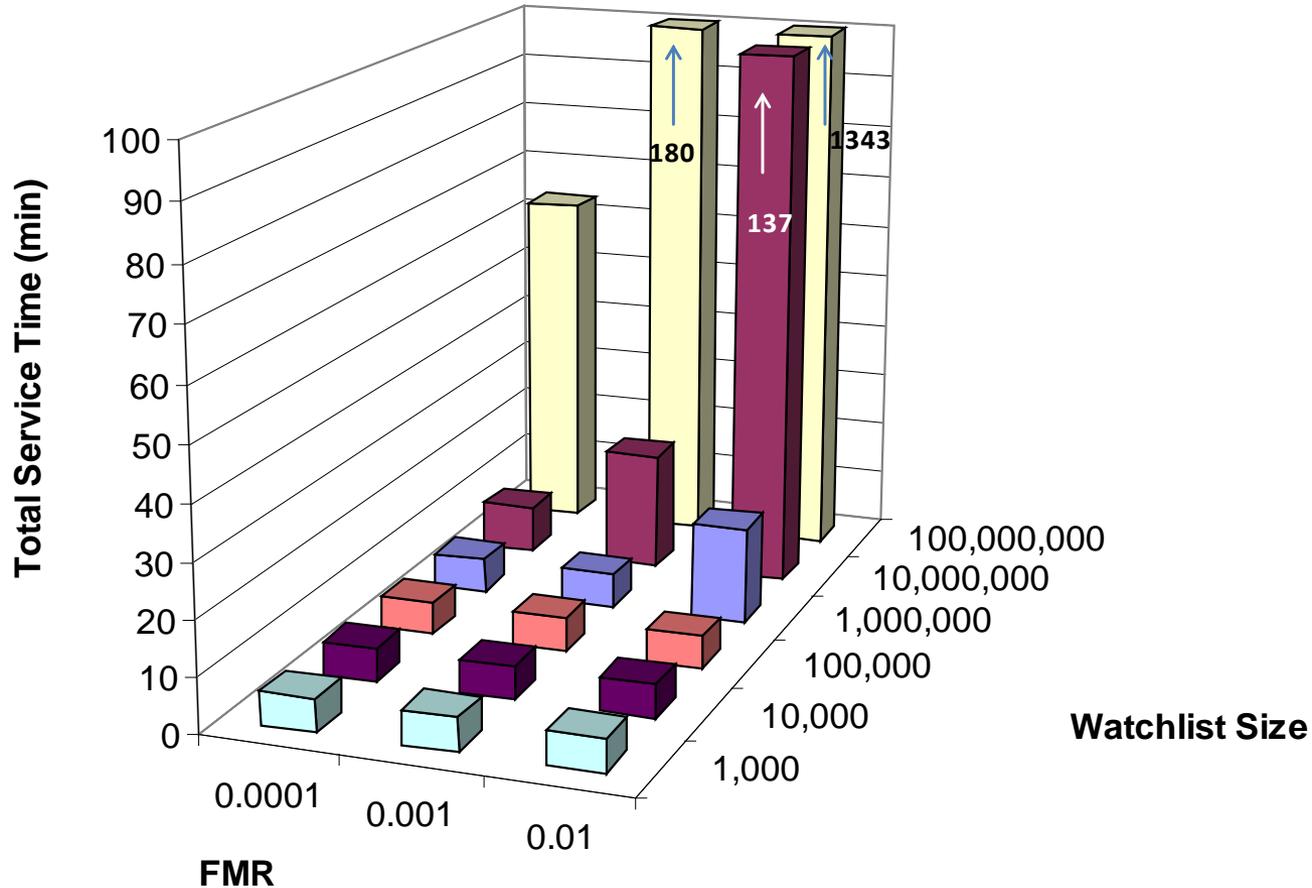
National Center for
Border Security and Immigration

Research Lead: The University of Arizona



Performance experiments

Match rates & watch lists





Systems Approach: Port of Entry

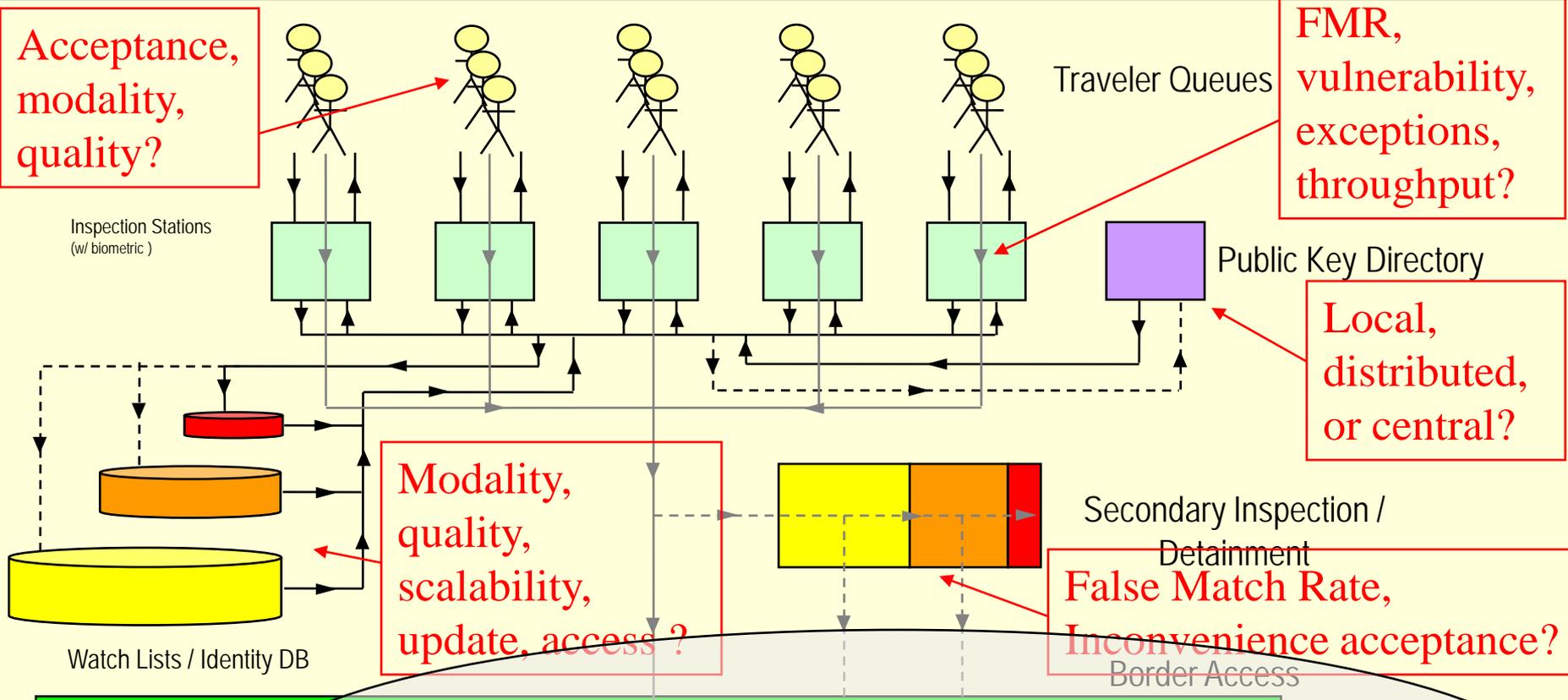
Acceptance, modality, quality?

Modality, FMR, vulnerability, exceptions, throughput?

Local, distributed, or central?

Modality, quality, scalability, update, access?

False Match Rate, Inconvenience acceptance?



Legend

- > = Required Signal
- - -> = Optional Signal
- > = Movement
- - -> = Optional Movement

False Non Match Rate

after Cukic et al.



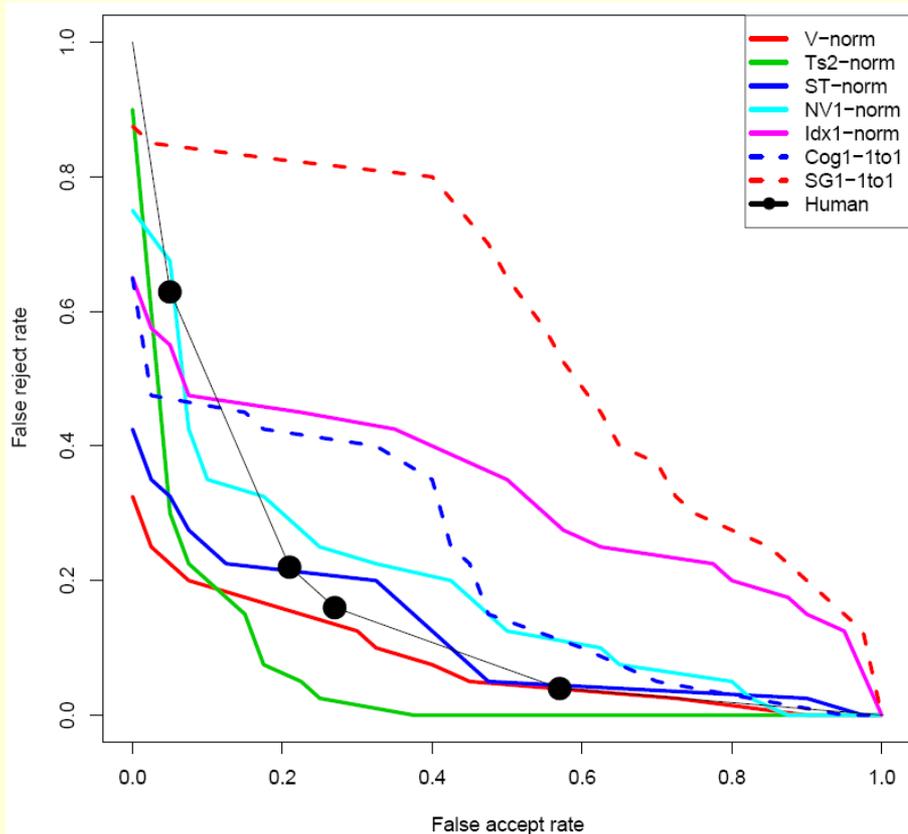
Cost Curve Modeling for Biometric PoE Inspection

- **A methodology for adaptation of biometric system set-up based on expected cost of misclassification**
 - $C(+/-)$ denotes the cost of incorrectly classifying a genuine user (as an impostor)
 - Secondary inspection.
 - $C(-/+)$ denotes the cost of misclassifying an impostor as a genuine user.
 - Security breach.
 - $p(+)$ probability of a user being an impostor.
 - $p(-)$ probability of a user being a genuine.



Face Recognition in Border Inspections

• Face Recognition Vendor Test (FRVT) 2006

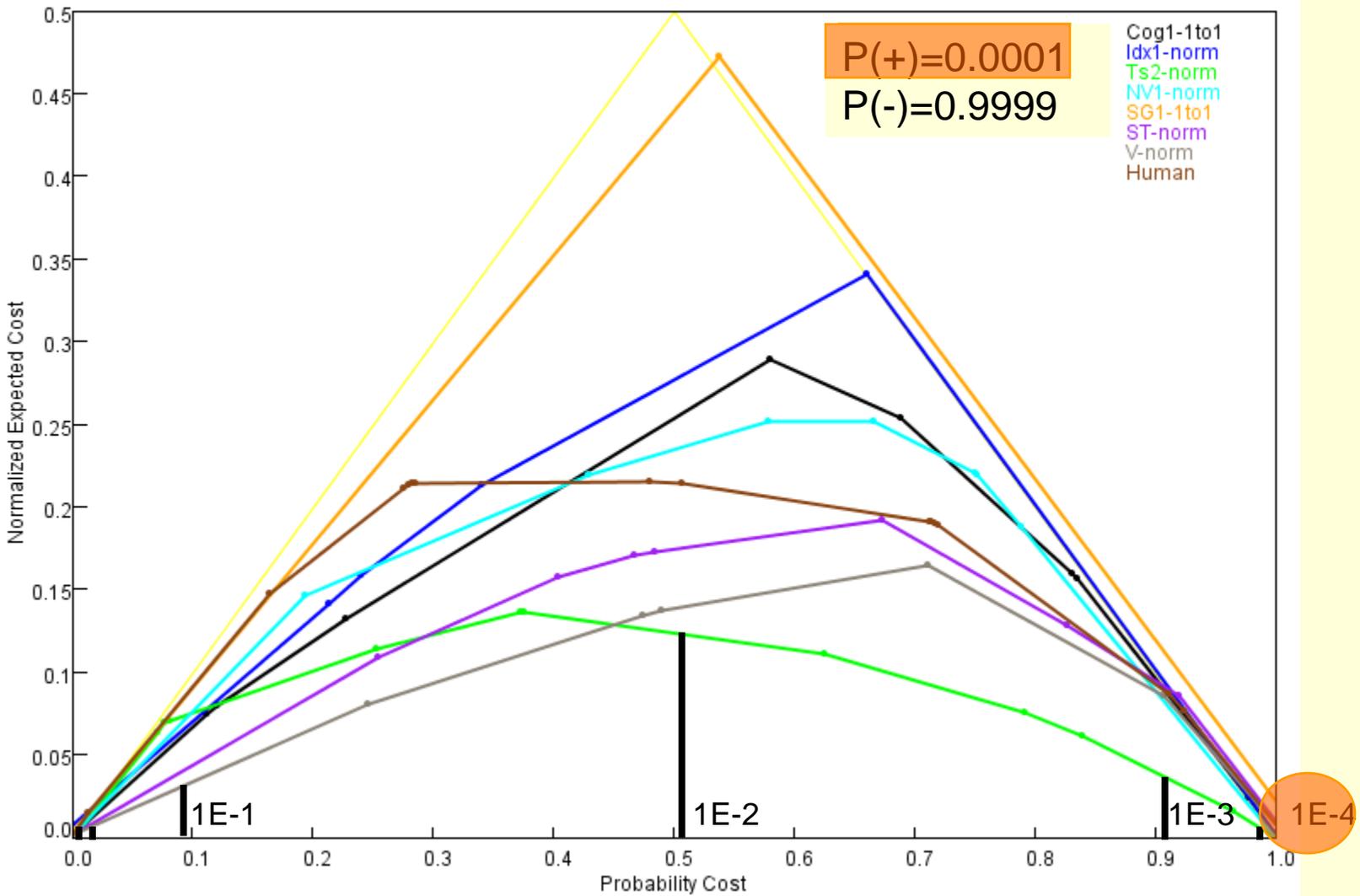


Test which algorithm is better when:

- Impostor arrival rate varies 0.01 – 0.0001
- Misclassification cost ratio, $\mu=C(+|-):C(-|+)$ varies between 0.1 and 0.0001;
- Misclassifying an impostor is 10 – 10,000 times more “expensive” than misclassifying a genuine user.

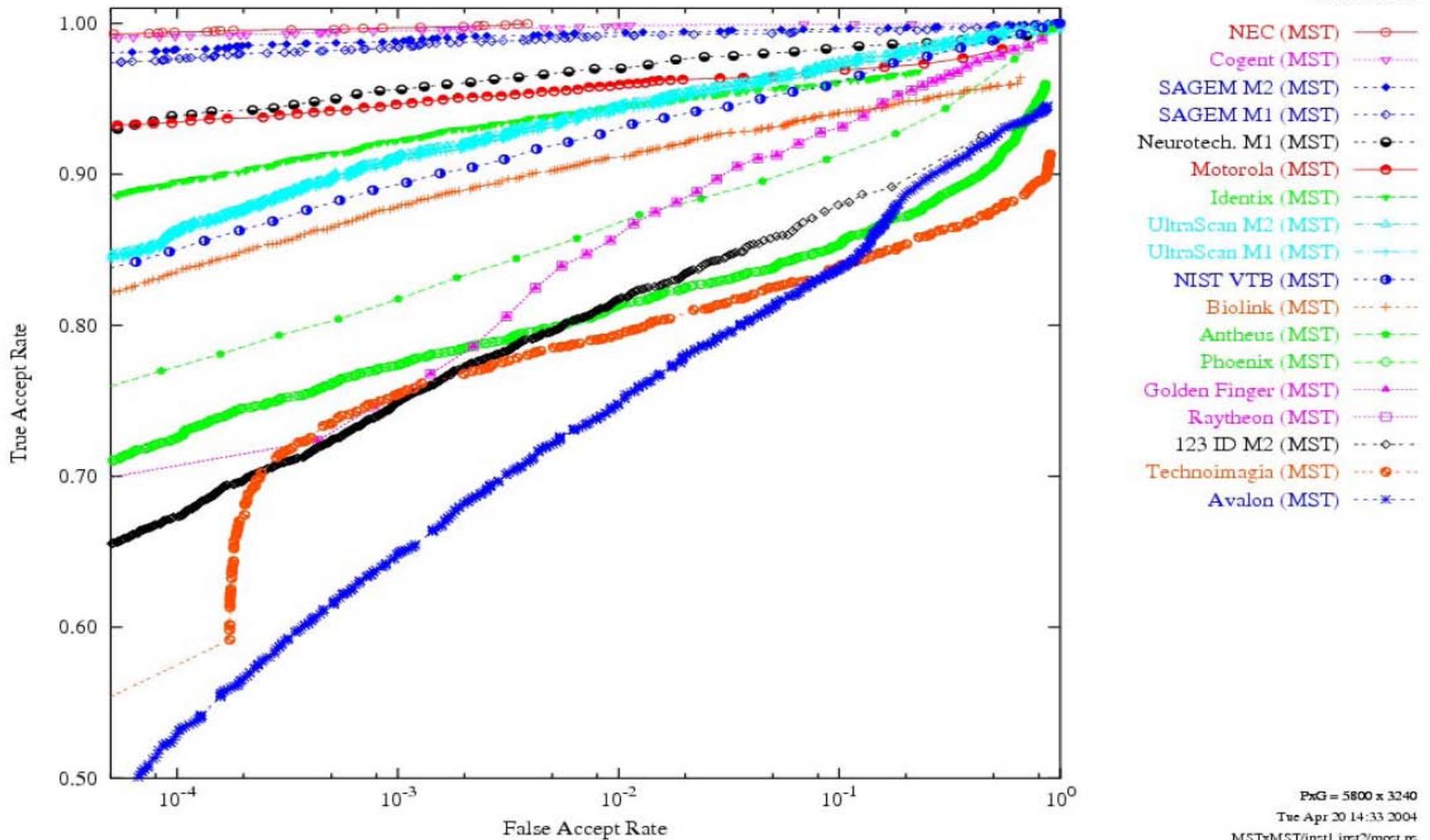


Face recognition cost curves



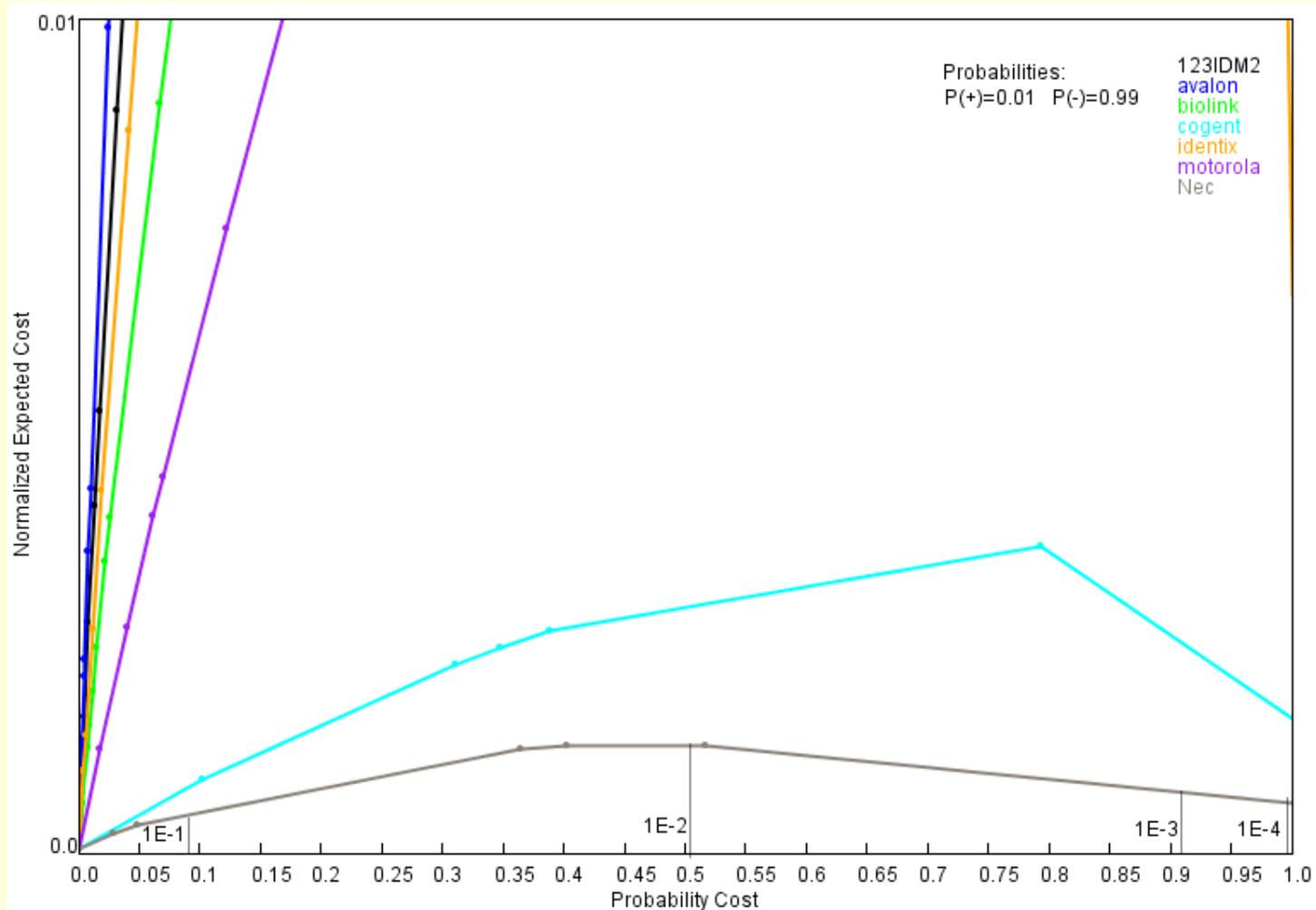


Fingerprint matching algorithms (FpVTE 2003)





Fingerprint – Cost curve





FMR, Risks, Performance

Face Recognition

$P(+)=0.0001$

$\mu=1/100$



Probability Cost, PC(+)	Norm($E[Cost]$)	FMR	FNMR	Total Waiting (min)
0.001	0.3227	0.00152	0.322	infinite
0.1	0.0314	0.00152	0.322	infinite
0.5	0.1235	0.175	0.073	205.5807

Fingerprint recognition

Probability Cost, PC(+)	Norm($E[Cost]$)	FMR	FNMR	Total Waiting (min)
0.001	0.00689	0.00005376	0.0059	25.5008
0.1	0.0004	0.0001834	0.0031	25.06776
0.5	0.0013	0.001276	0.0013	24.79358



Summary

- **“Rapid” screening cannot be considered as a goal by itself.**
 - Related to security risk, system design, data set size, etc.
- **Points of entry need to adapt to the operational environment.**
 - Cost curves demonstrate the strategy for threshold adjustment in deployed biometric systems.
 - Need very few parameters
 - The “arrival rate” for impostors and the misclassification cost ratio.
 - Such design minimizes the overall risk.
- **Current work**
 - Incorporating multimodal biometrics.
 - Deriving system design rules in light of the privacy parameters.