Validating Models of Adversary Behaviors

Dr. Jun Zhuang
Associate Professor
Department of Industrial and Systems Engineering
University at Buffalo
Email: jzhuang@buffalo.edu;
Web: http://www.eng.buffalo.edu/~jzhuang/

Presentation to
13th Workshop on Advanced Development for Security Applications (ADSA13)
October 28-29, 2015

NATIONAL CONSORTIUM FOR THE
STUDY OF TERRORISM AND RESPONSES TO TERRORISM

Summary

- Big Picture
  - Knife; shoe/cartridge/underwear bombs
  - Aviation vs. train/shopping mall/stadium/marathon…
- Validating Models of Adversary Behaviors
  - Should models be validated? YES!
  - Can models be validated? Sometimes…
  - How would models be validated?
    - Based on real scenario;
    - With/without data
    - Thought Experiments, Expert opinion, Interviews
    - Validation Exercises, Simulation, Case Studies

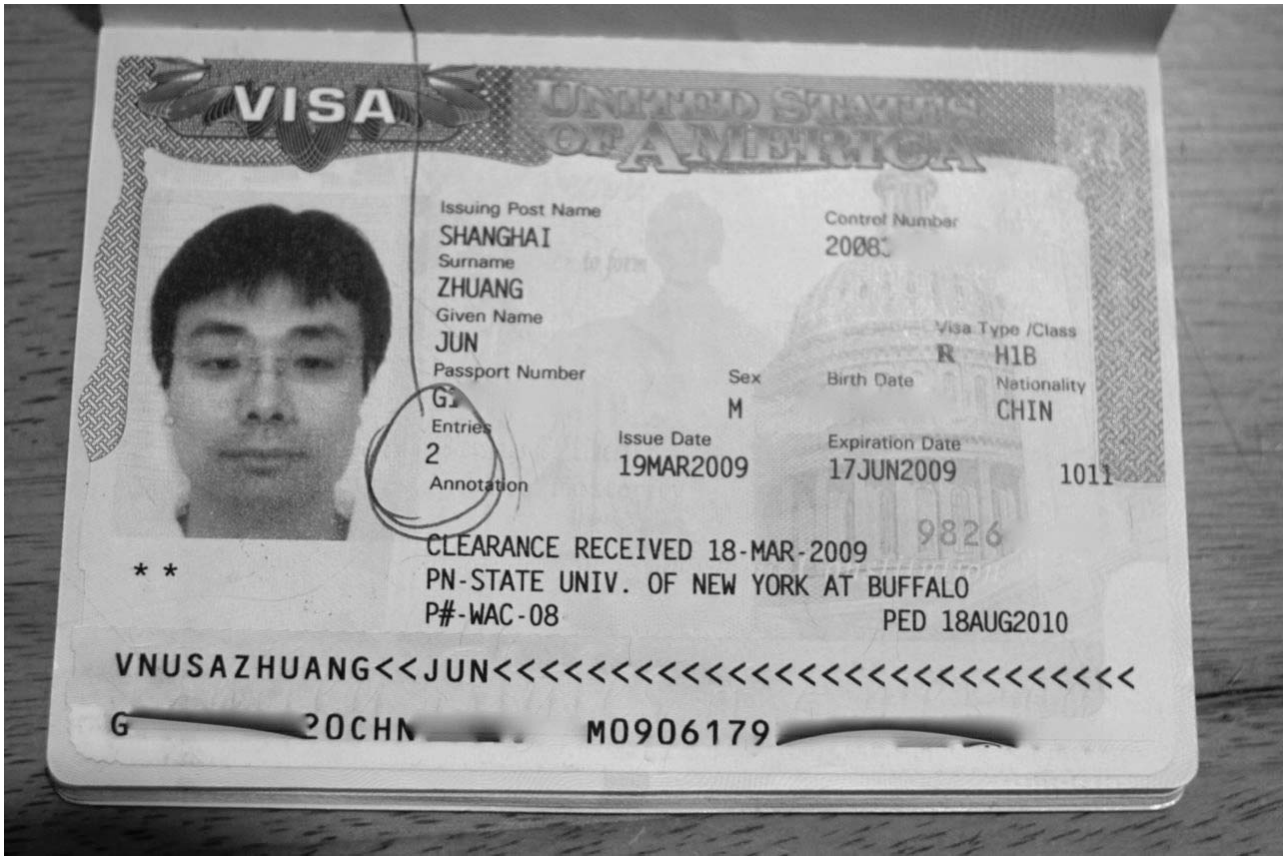
- Balancing Congestion and Security in the Presence of Strategic Applicants with Private Information

Robust Security Screening Games

- My own experience in December 12, 2008 -- March 22, 2009.

Robust Security Screening Games

- My own experience in December 12, 2008 -- March 22, 2009.



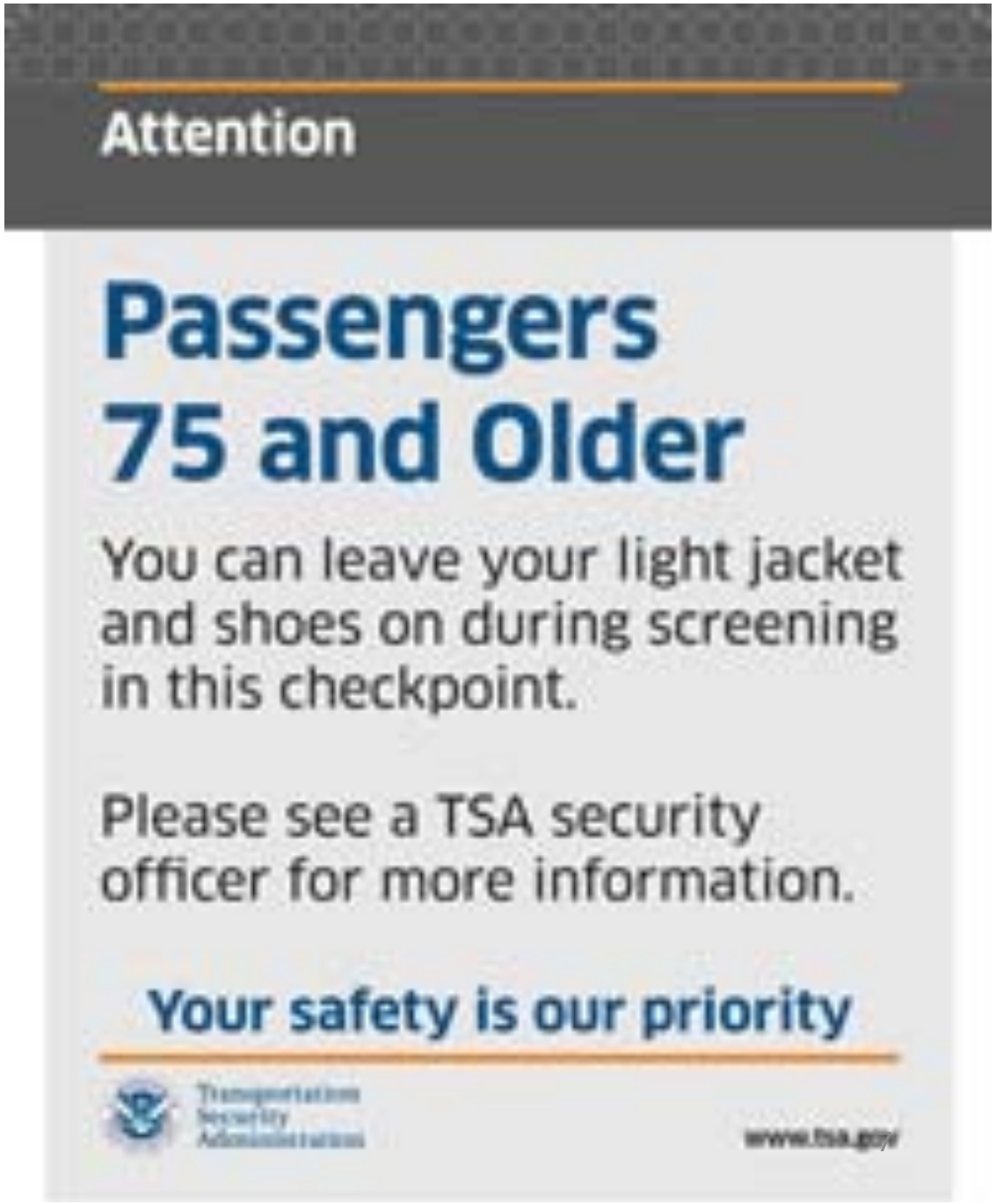
- Wang, X. and J. Zhuang. "Balancing Congestion and Security in the Presence of Strategic Applicants with Private Information, *European Journal of Operational Research*, 212(1): 100-111, 2011.
- Zhuang, J. (PI) "Robust Approval Process in the Face of Strategic Adversaries and Normal Applicants," supported by National Science Foundation, 08/15/2012-07/31/2016, $295,958.

Debates about Airport Screening

- Pat-down, Advanced Imaging Technology
- How to improve passenger experiences

Progress on Risk-based Screening (RBS)

Progress on Risk-based Screening (RBS)





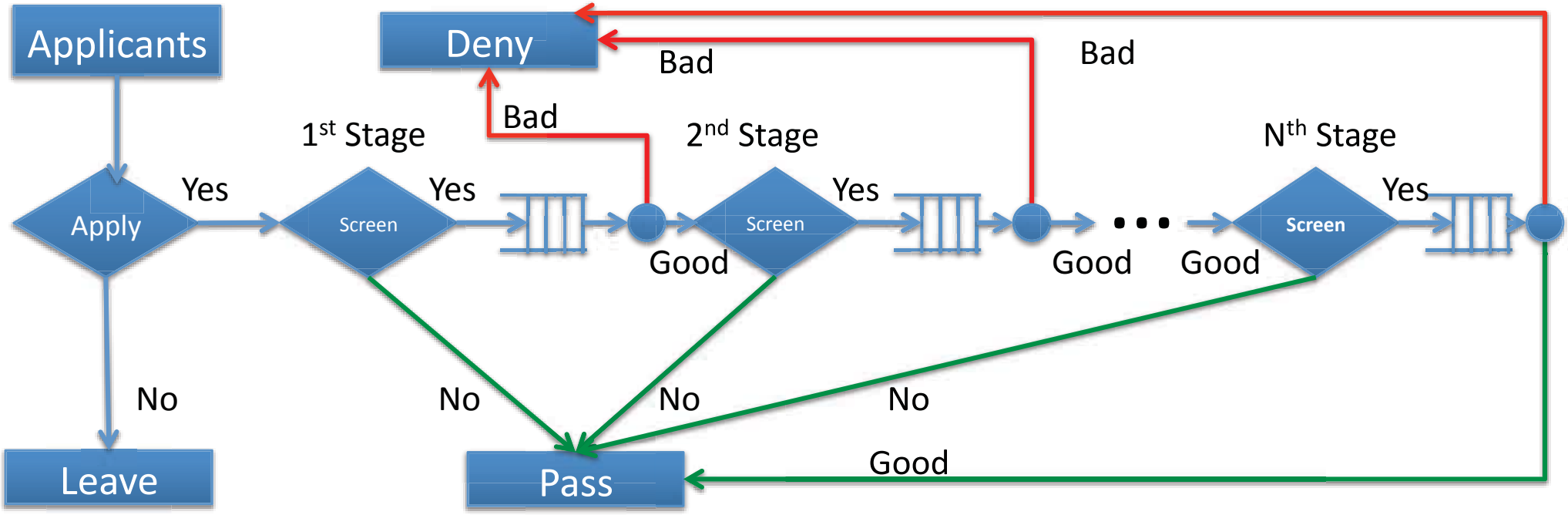
- Security screenings play an important role in many fields:
  - Airport security screening
  - Visa issuance
  - Cargo inspection
- What are the trade-offs?
  - In-depth examination of applicants reduces security risk
  - In-depth examination can entail high congestion which can deter normal applications
  - This may in turn conflict with the approver's interests
- Key Contribution: Considering strategic normal applicants

Novelty of This Research

- It allows strategic decisions by all types of potential applicants
- Potential applicants could adapt their behavior according to a disclosed security policy; e.g.,
  - Smugglers may choose the weakest port to enter
  - Leisure travelers may choose not to travel because of congestion, hassle, inconvenience
  - Foreign students may no longer apply to U.S. schools because of the long waiting period for visas
- Very few research has simultaneously considered both the good and bad applicants' strategic behavior and congestion in determining the optimal screening policy

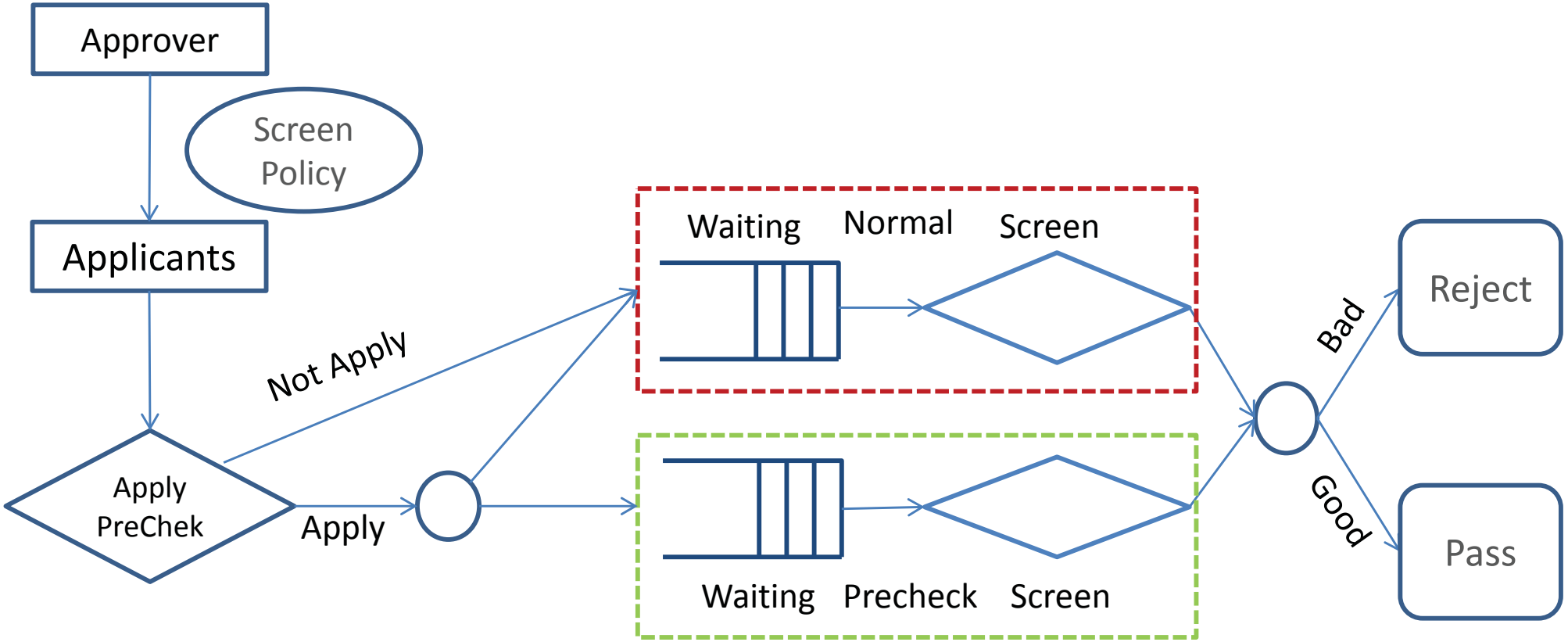
An Overview of the *N*-stage Model with Errors

The Flow Chart

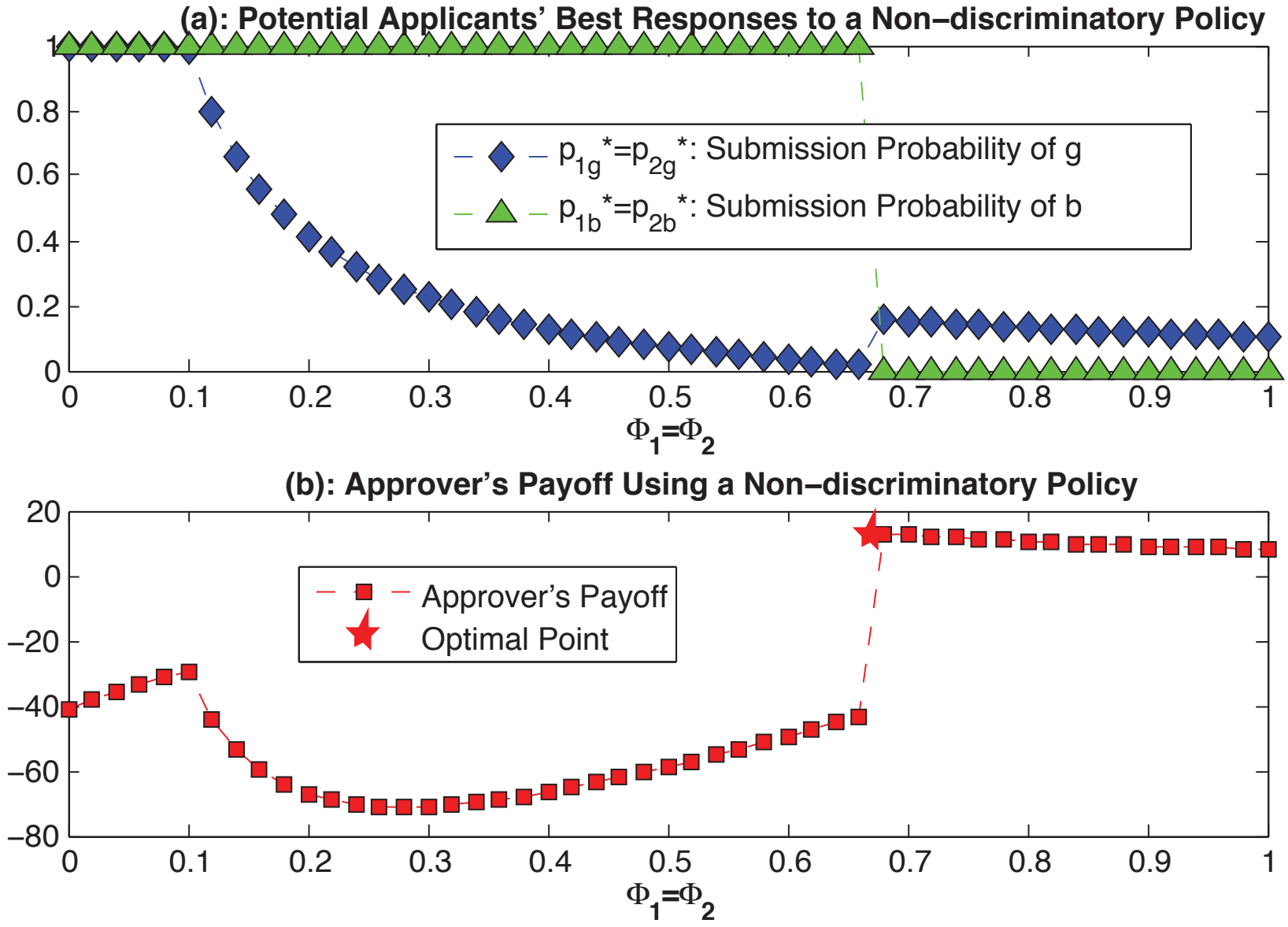


- Applicants:
  - Unobservable attributes: good/bad
  - Observable attributes: age, nationality, gender, education, travel pattern, etc.
- Approver decides the screening probabilities based on applicants' observable attributes

A Simplified Framework for Expedited Security Screening

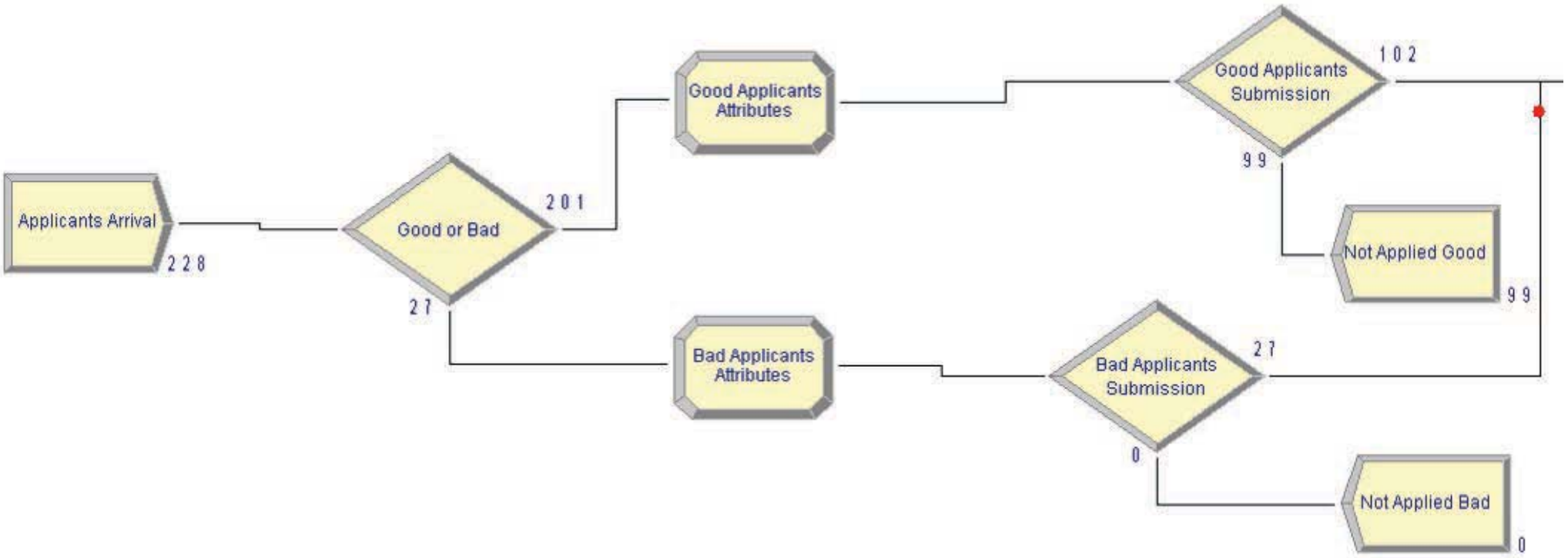


Preliminary Results for balancing Congestion and Security

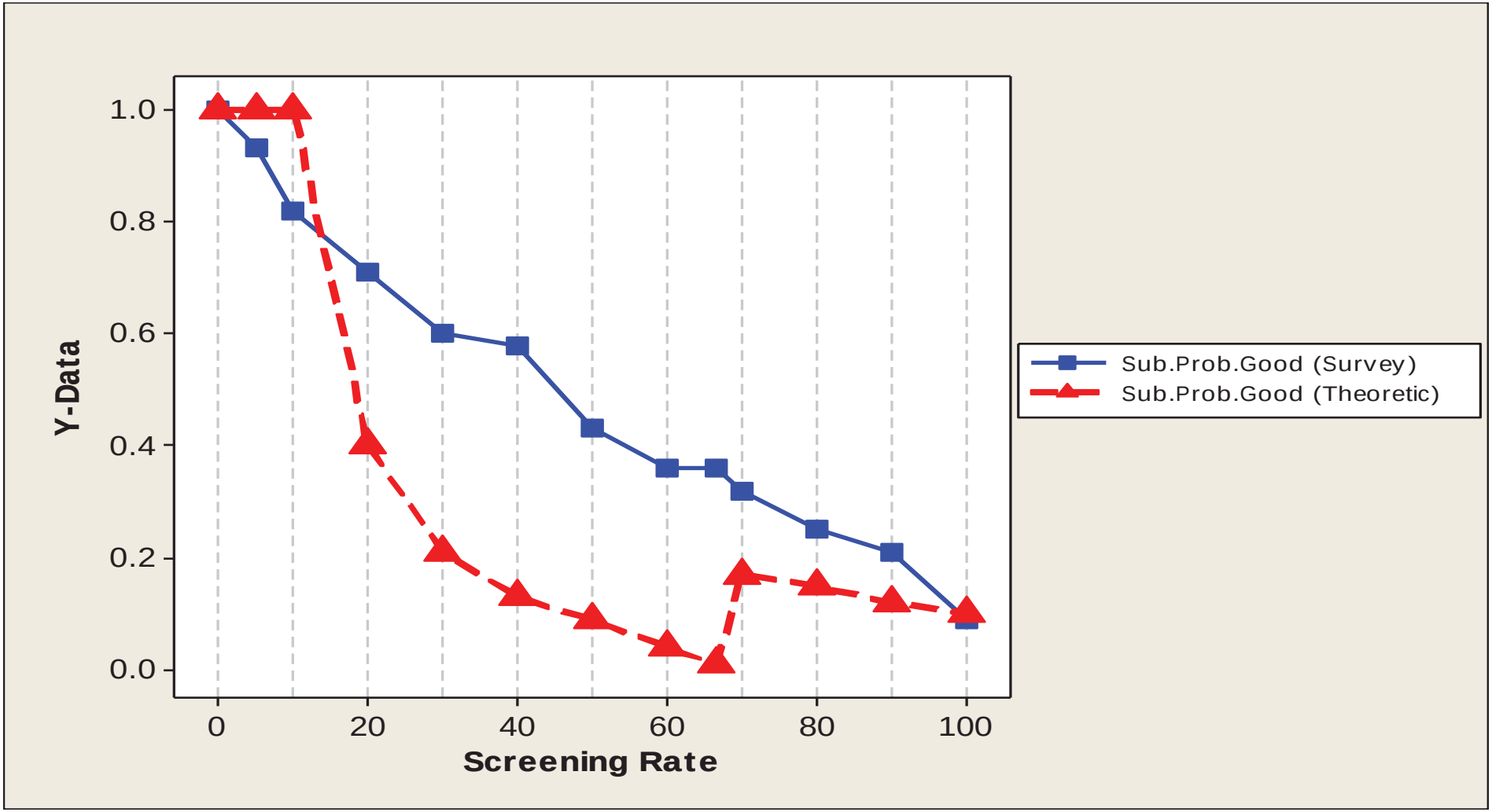


Reference: Wang, X. and J. Zhuang. "Balancing Congestion and Security in the Presence of Strategic Applicants with Private Information, *European Journal of Operational Research*, 212(1): 100-111, 2011.

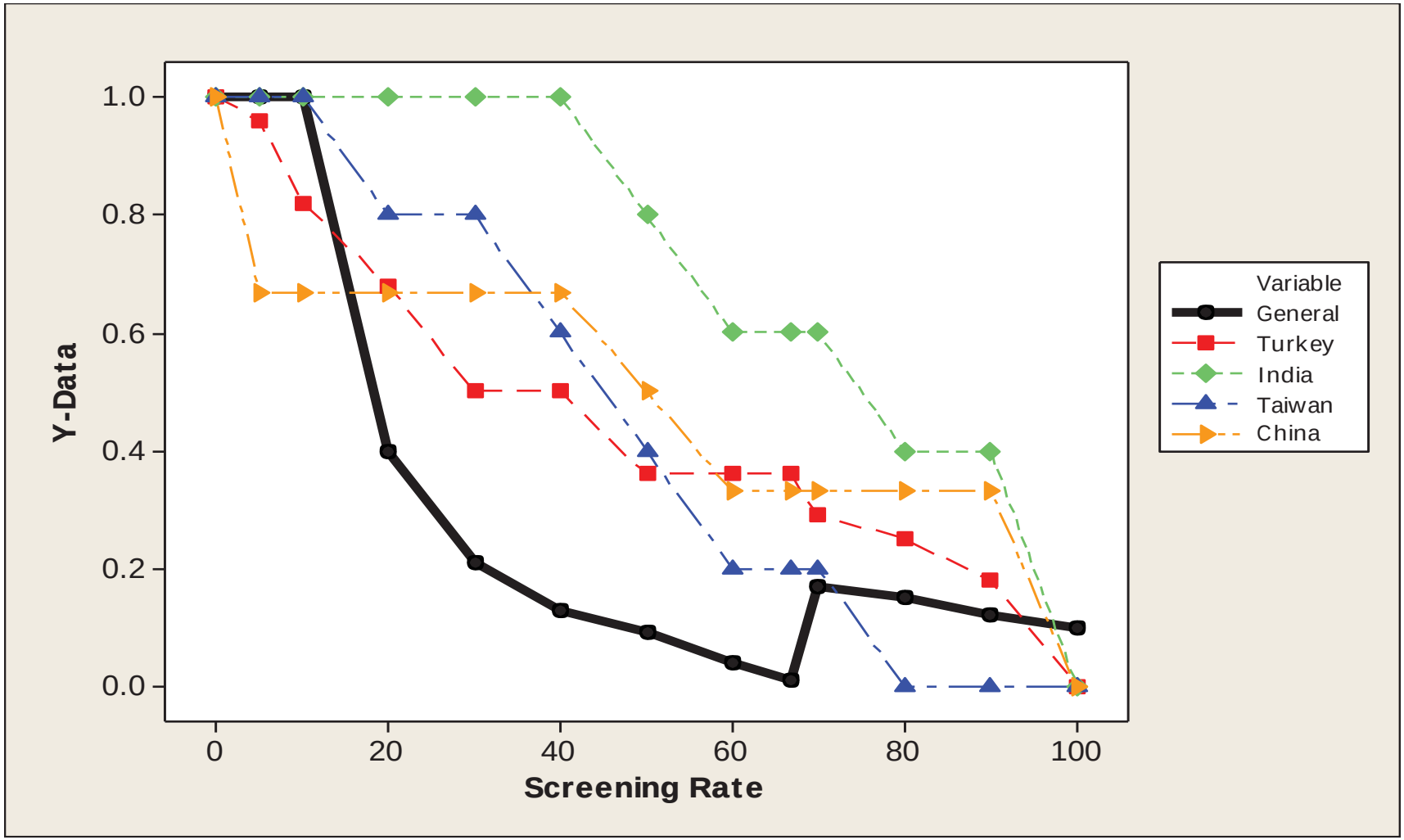
A Sample Simulation



Comparison with Survey Results

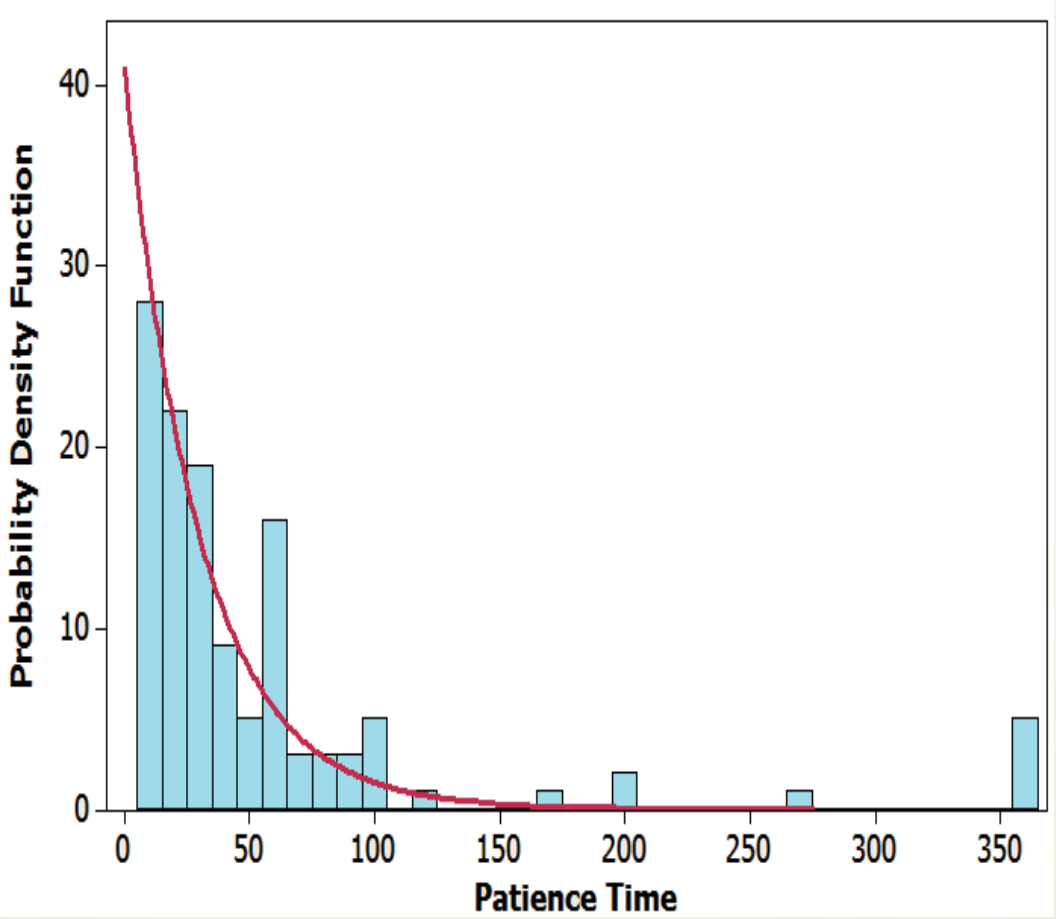


Sorted by Nationality



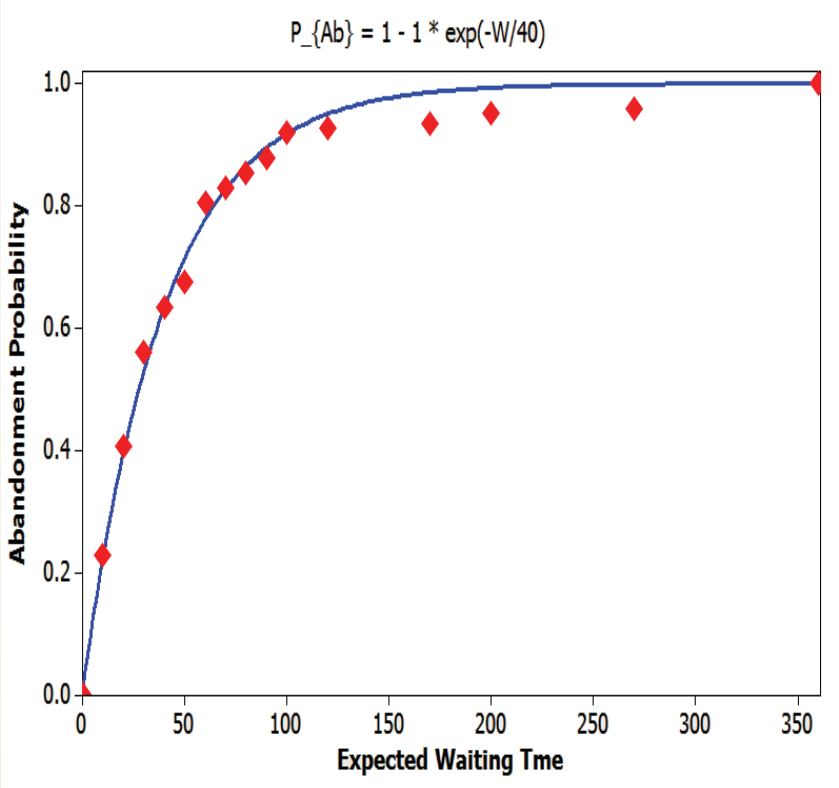
Patience Time

- Survey results showed that, patience time follows exponential distribution.



Modeling Abandonment

- According to survey results, there is a non-linear relation between waiting time and abandonment probability.

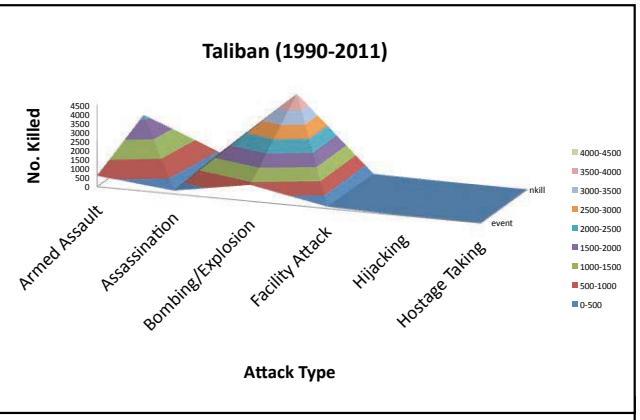


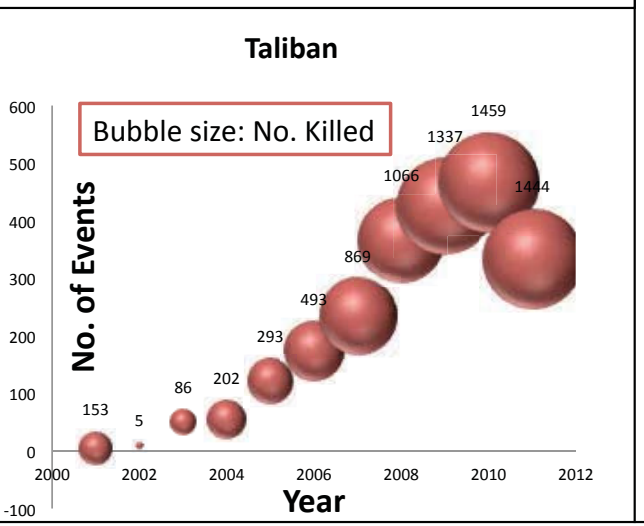
- Red dots represent abandonment probability at corresponding waiting time.
- Blue line shows, non-linear regression model. SSE of the model is 0.0105.
- We obtained following model by regression analysis:

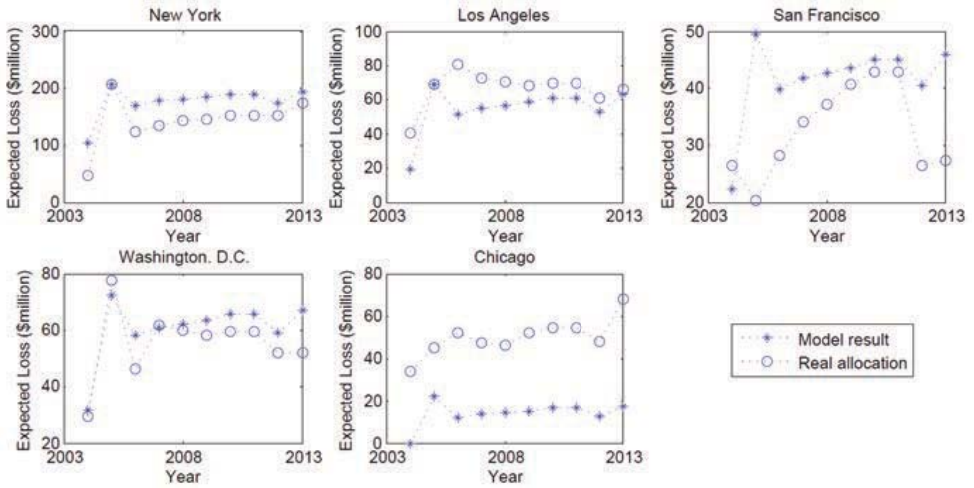
$$P_{Ab}^{nonlin} = 1 - e^{\frac{-W}{\tau}}$$

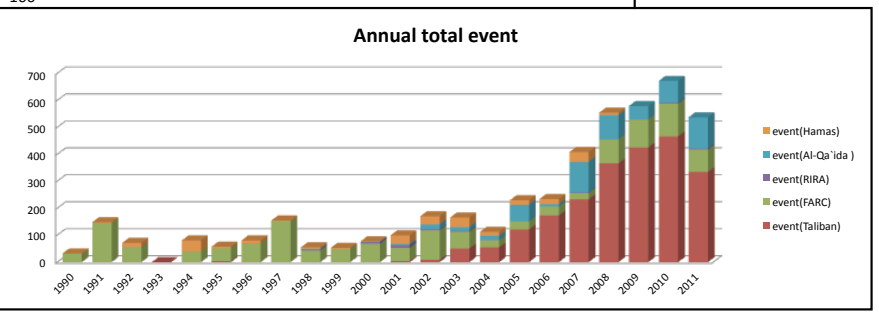
Validating Models of Adversary Behavior

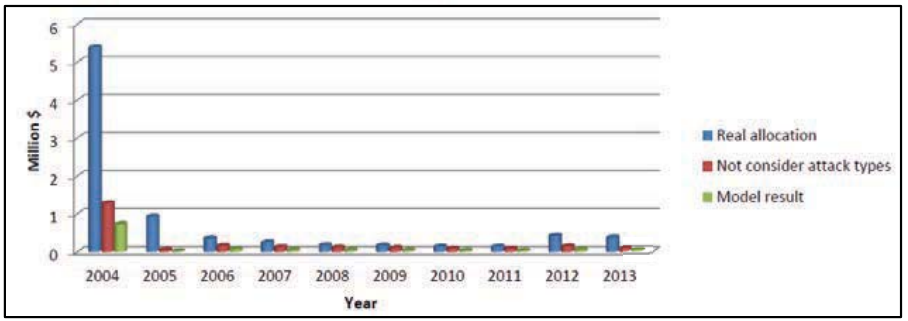
- We are validating a class of multi-period, multi-type, multi-target attacker-defender games
  - Using data from Global Terrorism Database and DHS Urban Area Security Initiative
- Attackers have multiple attack modes:
  - Assassination, armed assault, bombing/explosion, hijacking, hostage taking, etc.
- Compare “optimal” strategy v.s. real allocation?









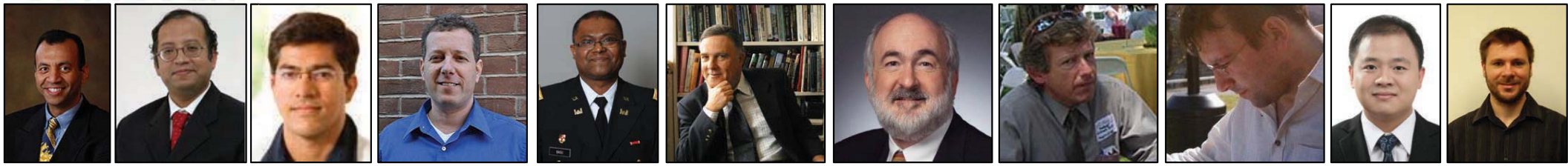


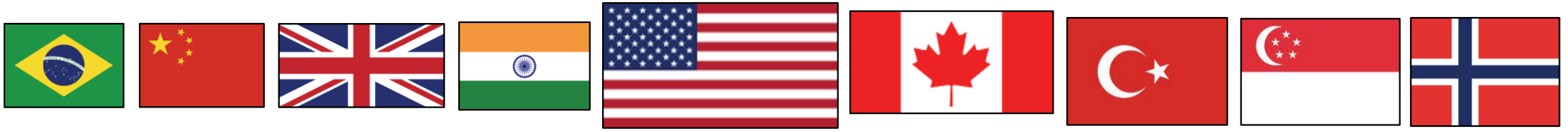
Other Methods for Model Validating

- Thought Experiments
- Simulation
- Validation Exercises
- Case Studies
- Interviews with decision makers (and potentially with “attackers”)
- Experiments:
  - Use student subjects as proxies for terrorists
  - These games would be later replicated with more knowledgeable subjects (e.g., terrorism experts)

- Second Conference on Validating Models of Adversary Behavior, Buffalo/Niagara Falls, NY, Aug 2-5, 2015.
  ttp://www.eng.buffalo.edu/~jzhuang/Conference13/






Thank you for your time!!
Any questions/comments?

Collaborations are welcome!

Contact:

Dr. Jun Zhuang
Associate Professor
Department of Industrial and Systems Engineering
University at Buffalo
Phone: 1-716-645-4707
Email: jzhuang@buffalo.edu;
Web: http://www.eng.buffalo.edu/~jzhuang/

Image Sources

- Slide 6
  - http://i.imgur.com/BQsZXku.jpg
  - http://i.huffpost.com/gen/345432/thumbs/r-AIRPORT-SCREENING-SHOES-large570.jpg
- Slide 7
  - http://www.cristyli.com/?m=201012
- Slide 8
  - http://www.cnn.com/videos/us/2015/04/17/lead-dnt-foreman-tsa-groping.cnn