WHY MOBILE TO MOBILE MALWARE WON'T CAUSE A STORM

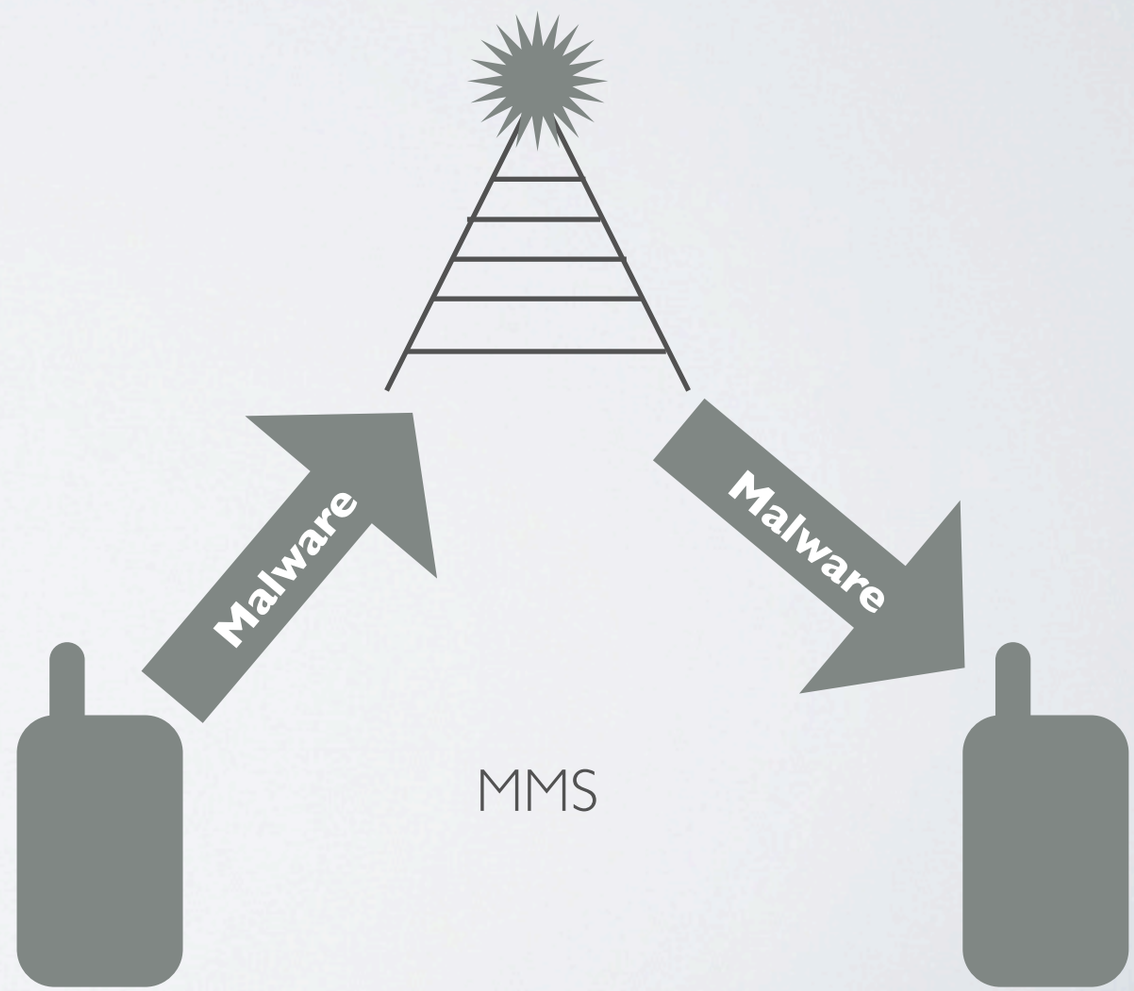
Nathaniel Husted
Steven Myers

Indiana University

INDIANA UNIVERSITY
BLOOMINGTON

MOBILE TO MOBILE MALWARE

- Bluetooth (Mabir/Cabir/Commwarrior) Vs. MMS (Mabir/Commwarrior)
- Symbian OS -- Dominant Market Share
- Feature Phones -- Dominant Phone Style



INDIANA UNIVERSITY
BLOOMINGTON

ROADMAP

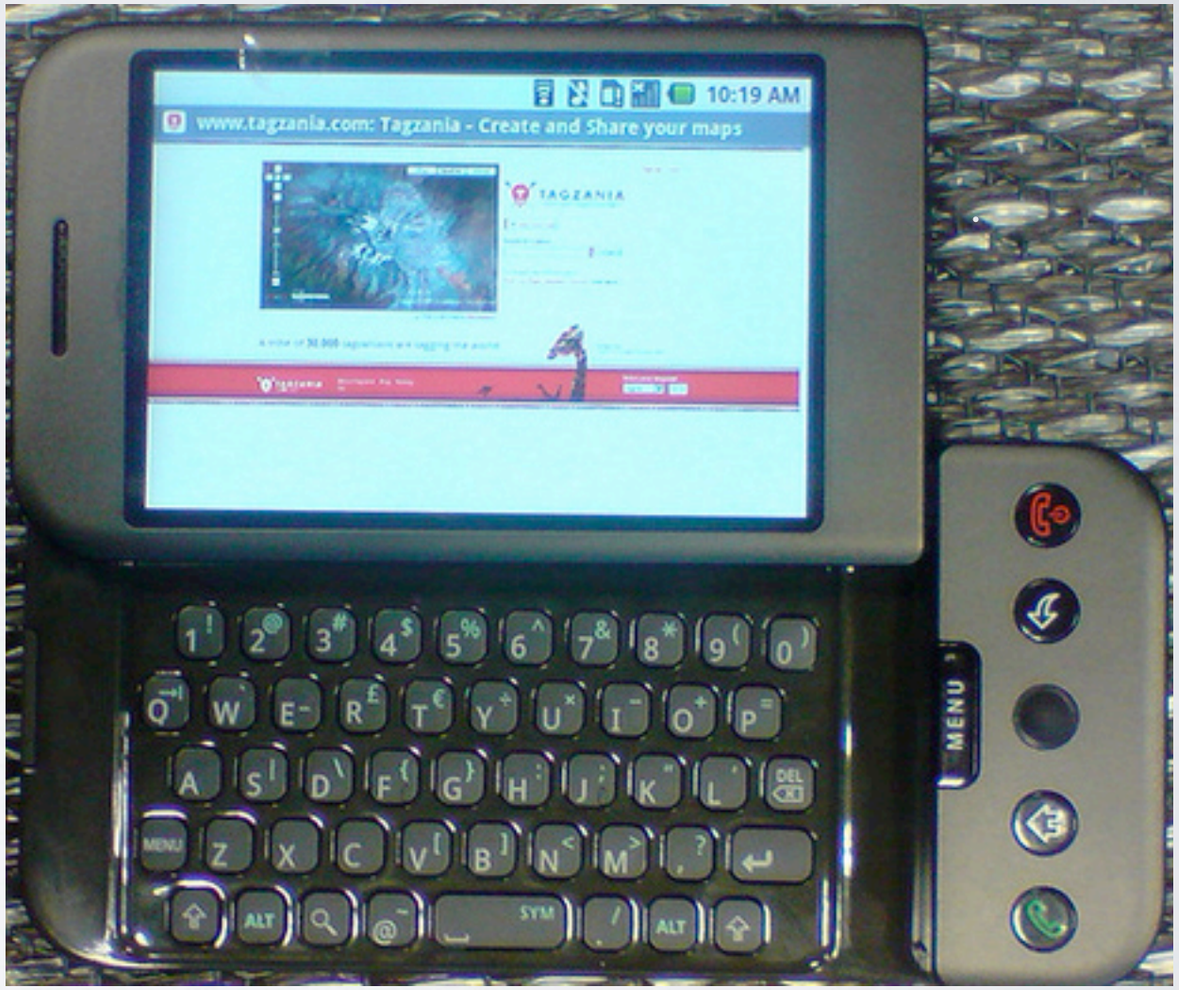
1. Related Work
2. Feature phones to smartphones: expanded threat surface
3. Requirements for studying malware spread
4. Interesting variables
5. Results
6. Conclusion

RELATED WORK

- [CARETONNI07] - Analytical model...
- [SU06] - Analytical model...
- [WANG09] - Empirical data but without fine positioning...
- [CHANNAKESHAVA09] - Activity based data but no transmission during mobility...

FEATURE PHONES TO SMARTPHONES

- **Bluetooth to WiFi**
- Larger threat surface
  - More features
  - More complex software
  - Always on Internet



Google Developer Phone
http://www.flickr.com/photos/tagzania/3119293948

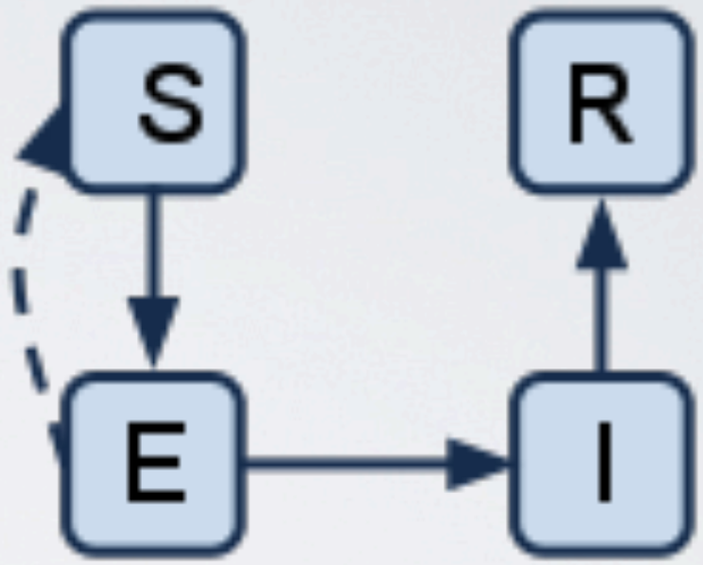
- Potential: Jailbroken iPhone's with default SSH credentials

FEATURE PHONES TO SMARTPHONES

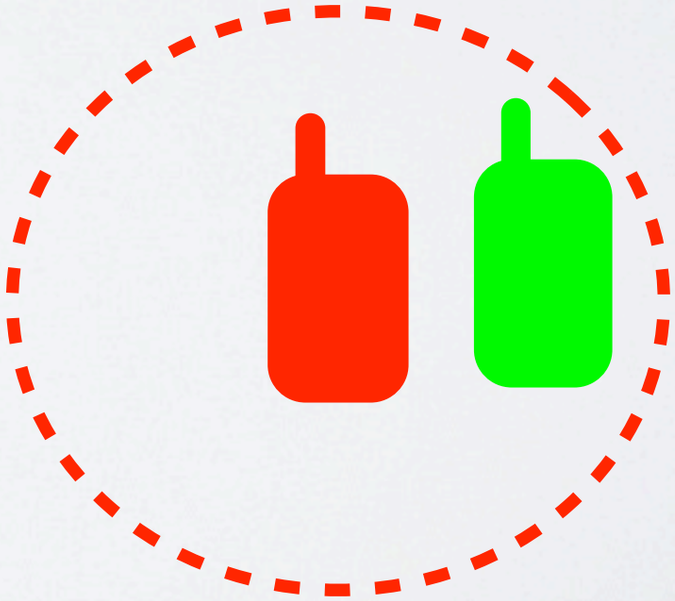
- **Bluetooth to WiFi**
  - WiFi devices, when on, are always visible, Bluetooth devices must be discoverable to be visible
  - WiFi management traffic is transparent
  - WiFi has greater range than common Bluetooth devices
  - WiFi has higher speeds
  - We assume WiFi is always on

LOOKING AT MALWARE SPREAD

1. Epidemiological Model
    - S-E-I-R Model
        - Susceptible
        - Exposed
        - Infected
        - Recovered



5...



Exposure Example

INDIANA UNIVERSITY BLOOMINGTON

LOOKING AT MALWARE SPREAD

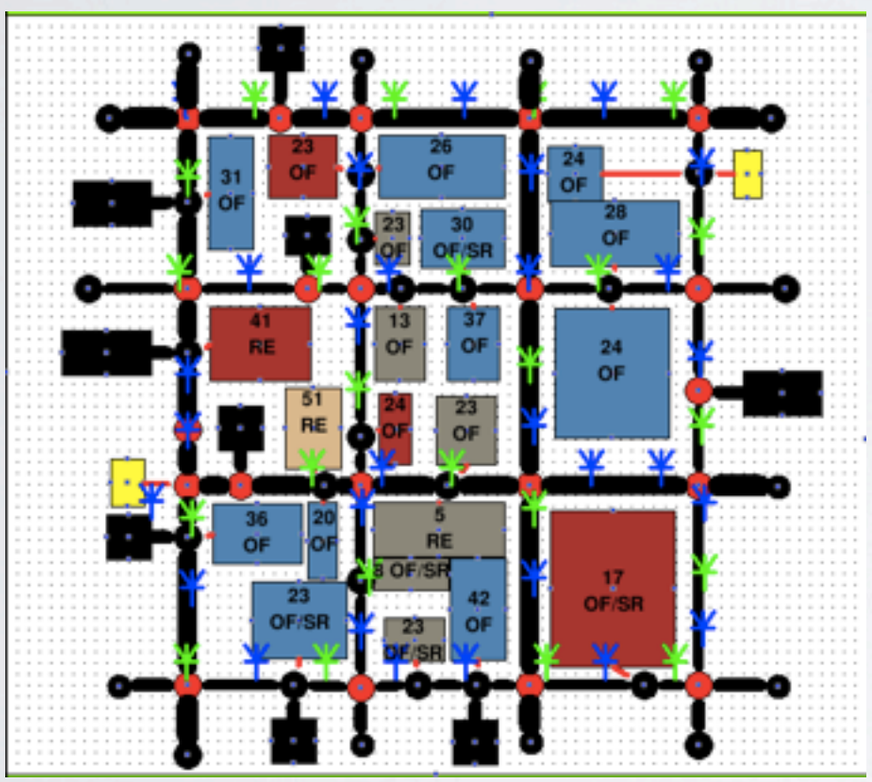
2. Realistic Mobility Model - UdelModels

- High Spatial Fidelity
- High Temporal Fidelity
- Accurate Population Density

Example UdelModels Simulation
http://www.udelmodels.eecis.udel.edu/

LOOKING AT MALWARE SPREAD

3. Target Geographical Area -- CHICAGO



http://www.udelmodels.eecis.udel.edu/

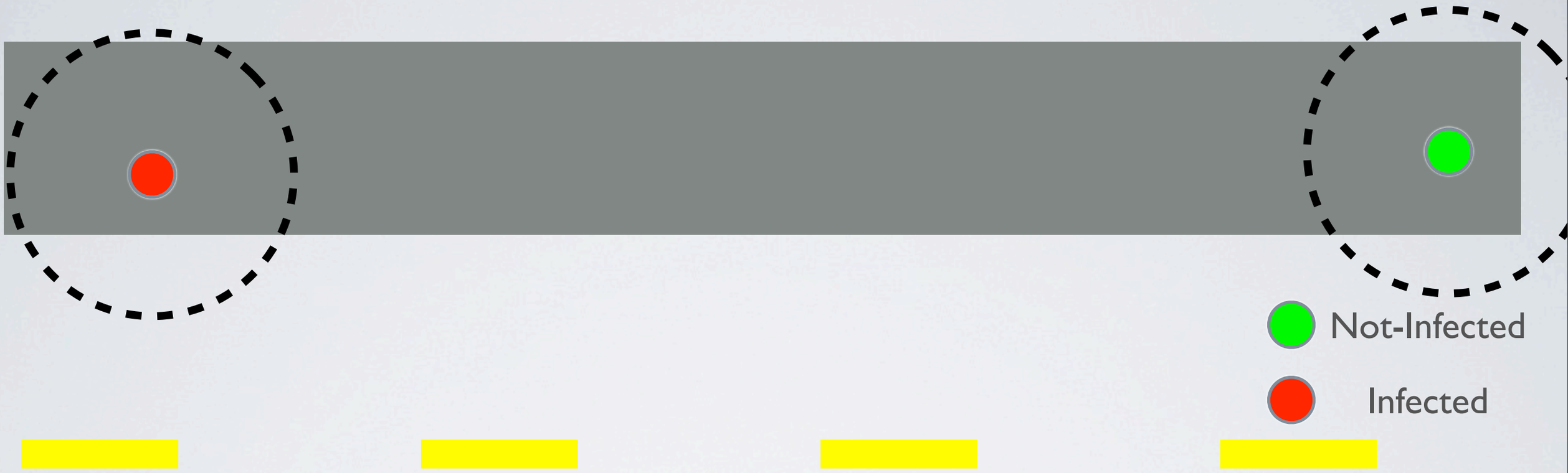
Population
9056
[Landscan]

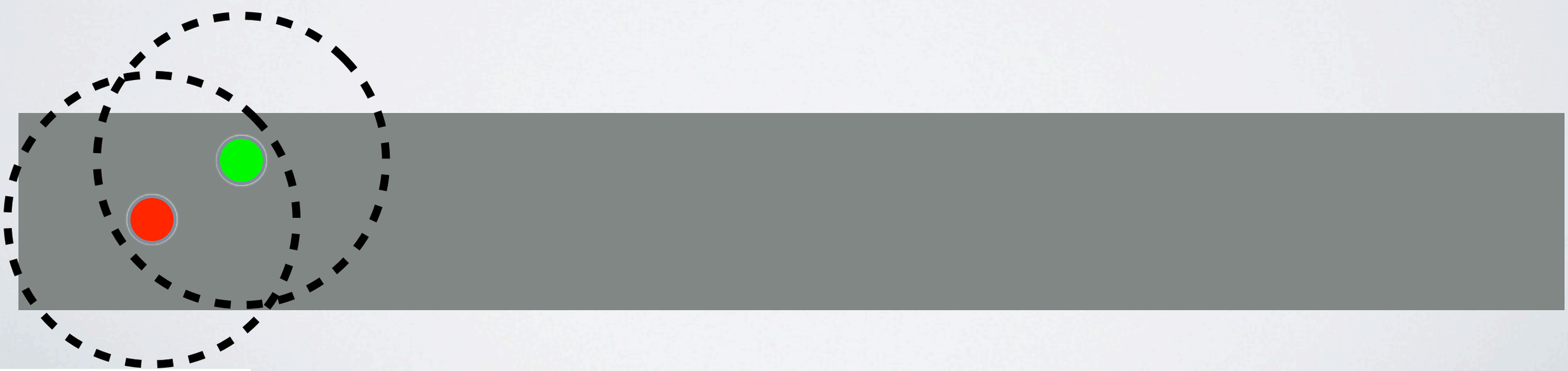
http://seamless.usgs.gov/hro.php

LOOKING AT MALWARE SPREAD

- Infection Style: Parallel Vs. Serial
  - Parallel -- **Many** devices targeted and infected *all at once.*
  - Serial -- **One** device targeted and infected *at one time*.
- Exposure Time - Viral Spread Speed
- Susceptibility - Different phone hardware/software
- Broadcast Radius - 802.11g vs. 802.11n

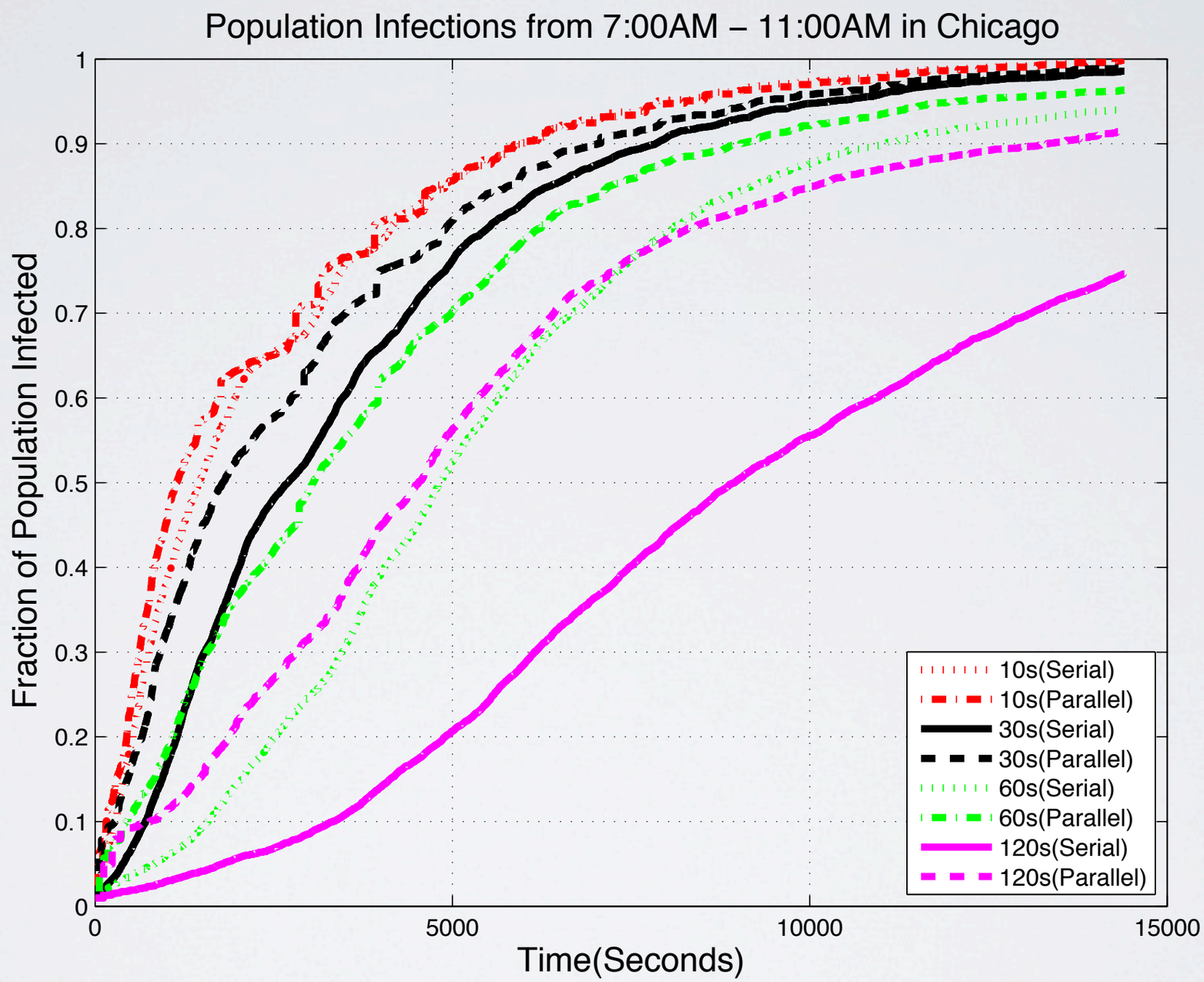
IMPORTANCE OF VIRAL SPREAD SPEED





INDIANA UNIVERSITY
BLOOMINGTON

EXPOSED POPULATIONS



Constants:

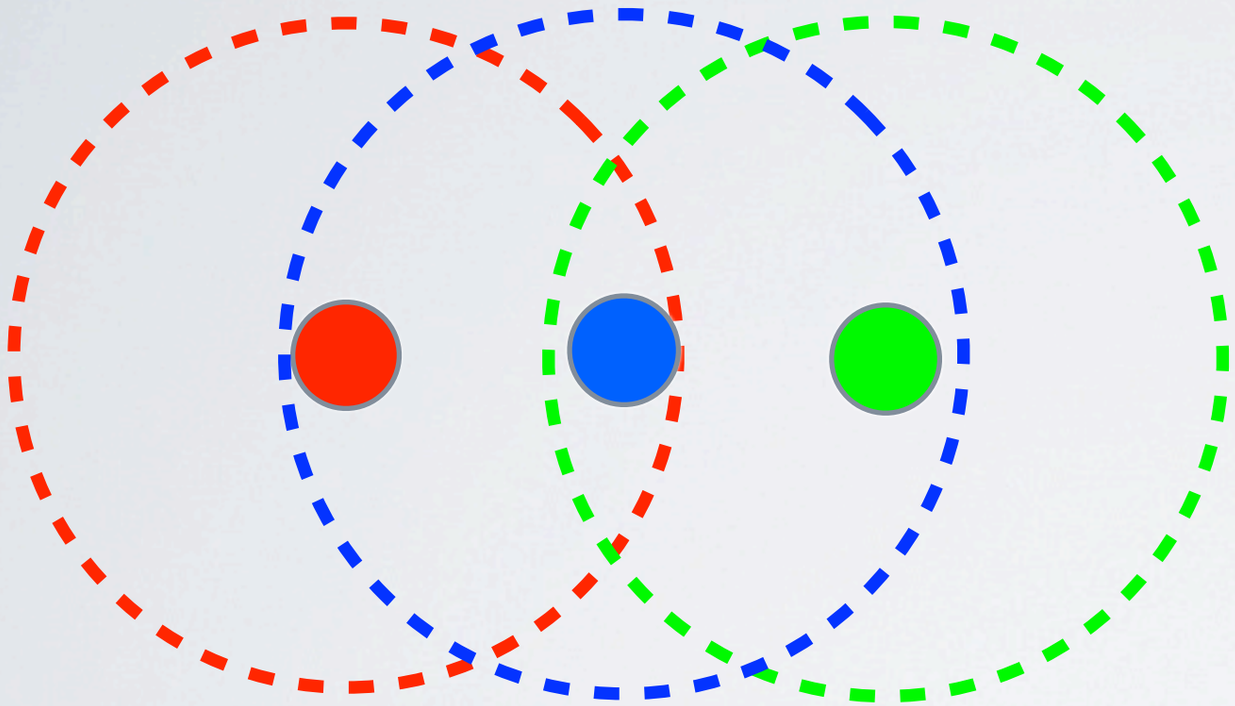
Radius: 15m

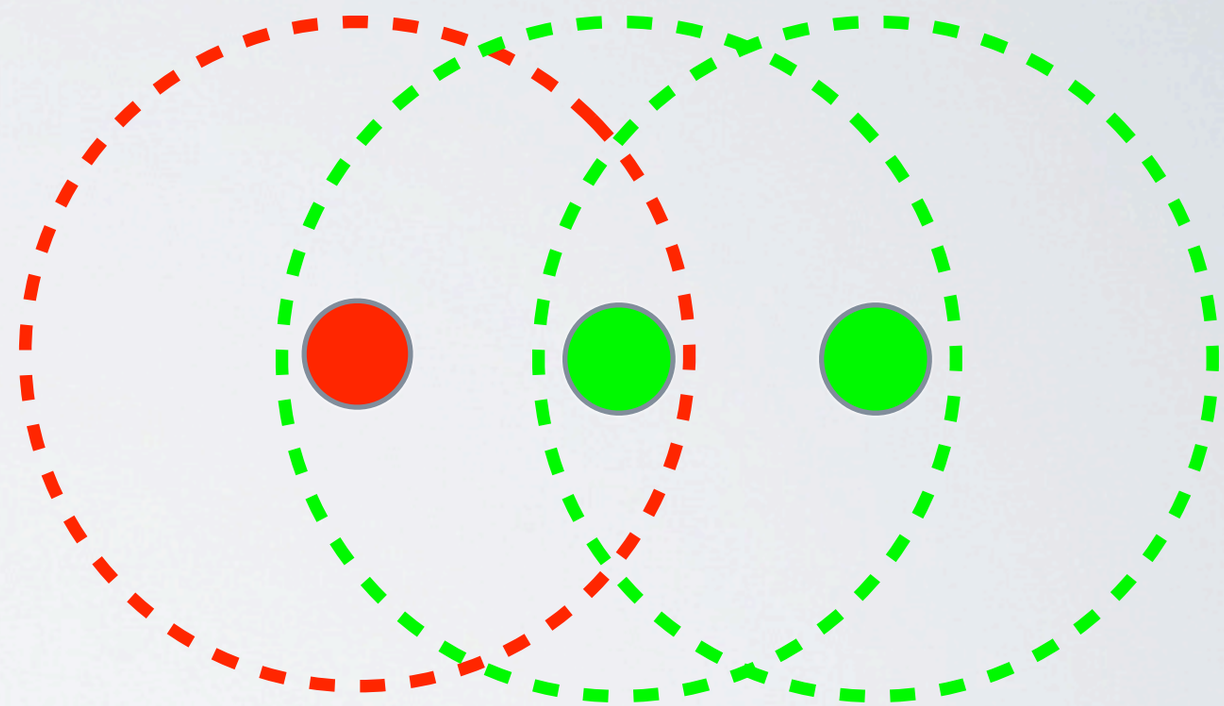
Susceptibility: 100%

Initial Infection: 1%

INDIANA UNIVERSITY
BLOOMINGTON

IMPORTANCE OF SUSCEPTIBILITY



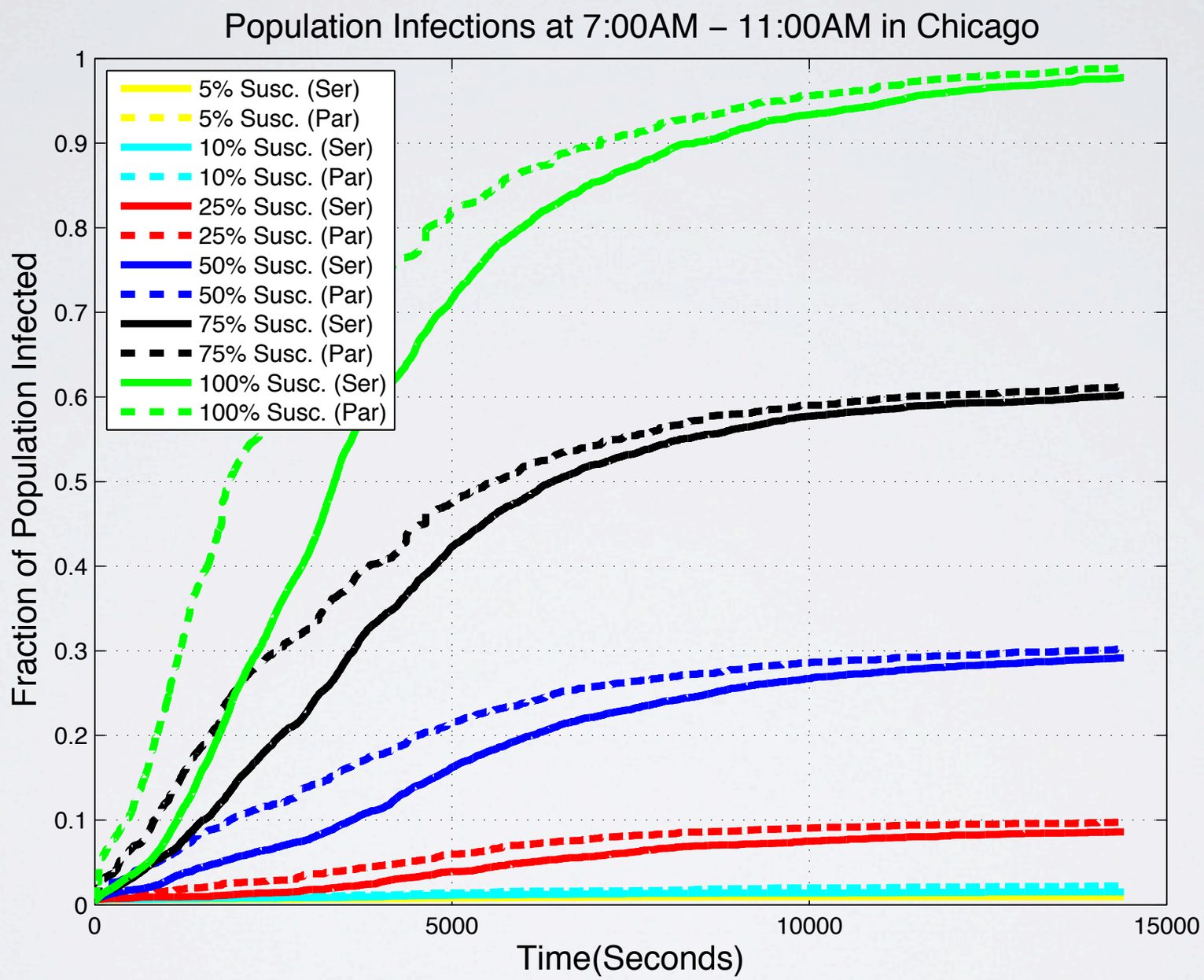


Not-Infected

Infected

Non-Susceptible

SUSCEPTIBLE POPULATIONS



Constants:

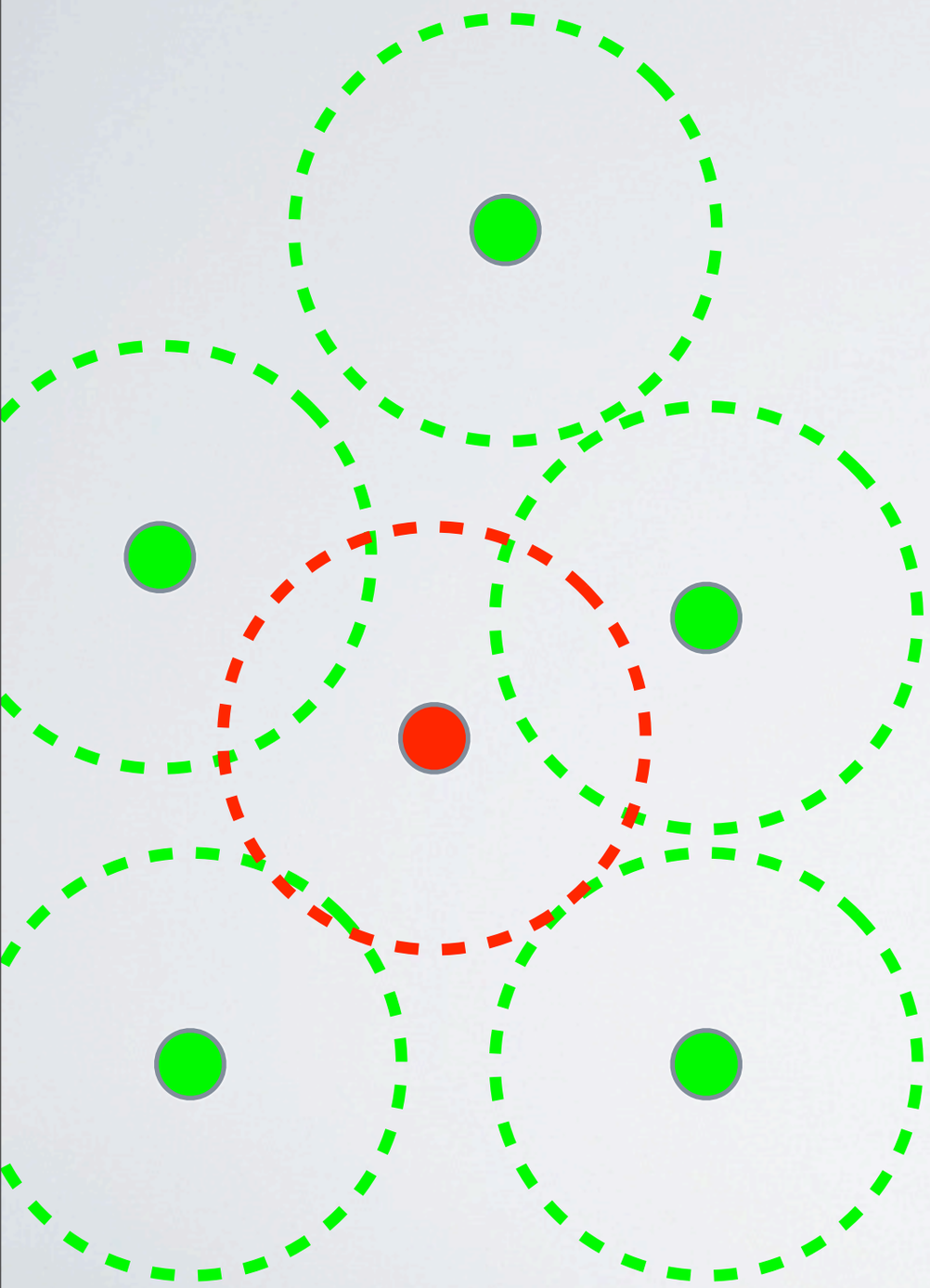
Radius: 15m

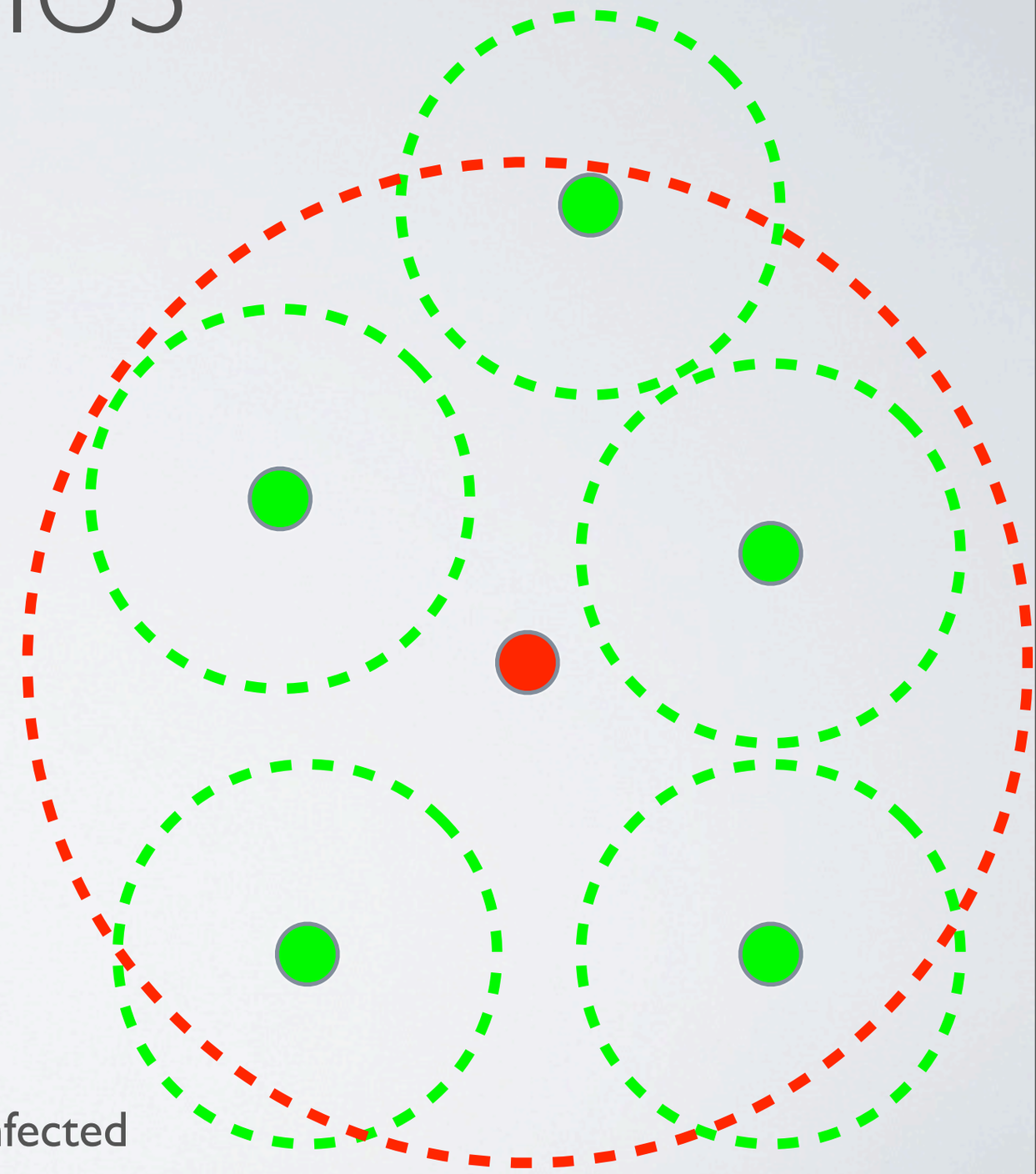
Exposure Time: 30s

Initial Infection: 30 People

INDIANA UNIVERSITY
BLOOMINGTON

IMPORTANCE OF BROADCAST RADIUS



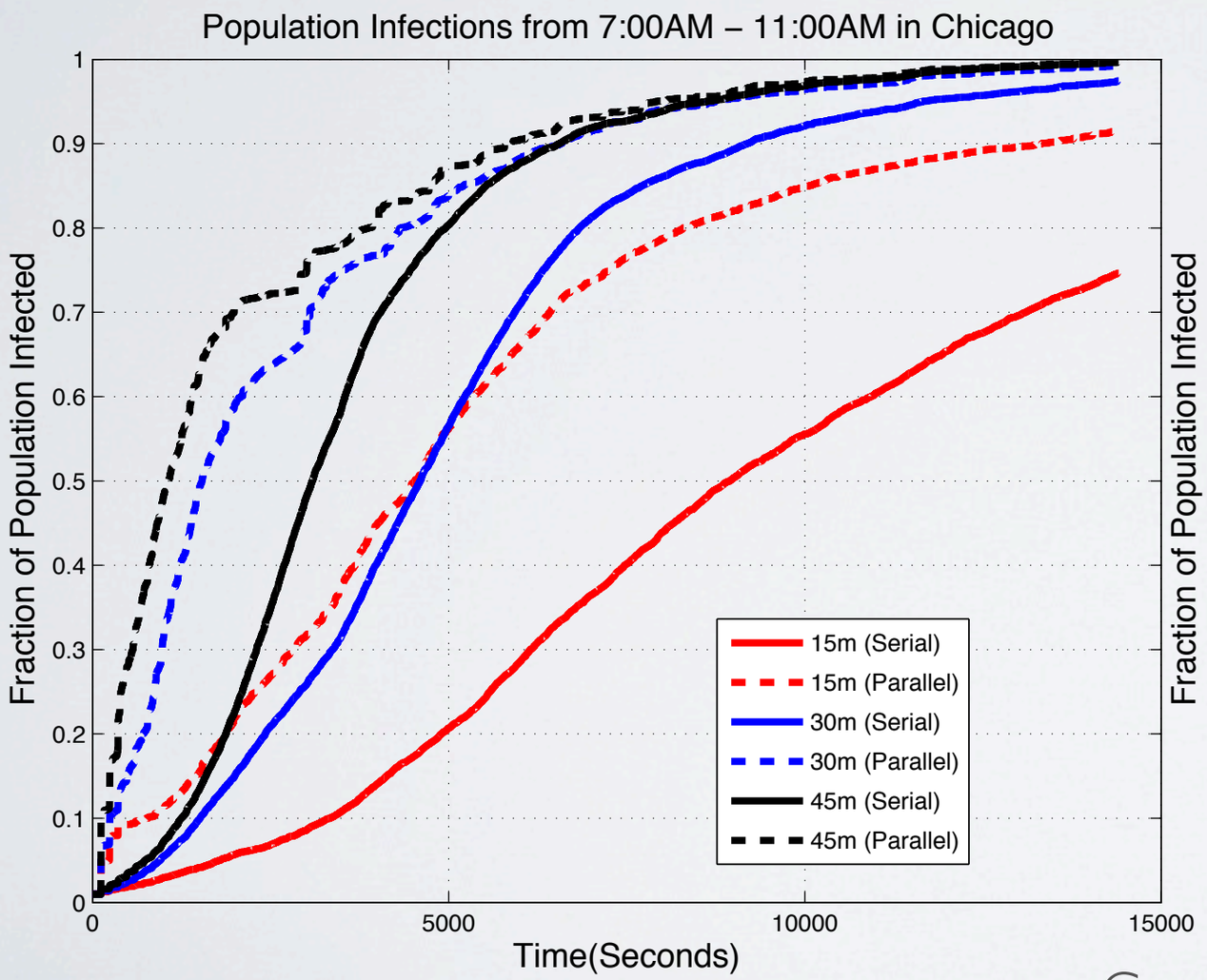


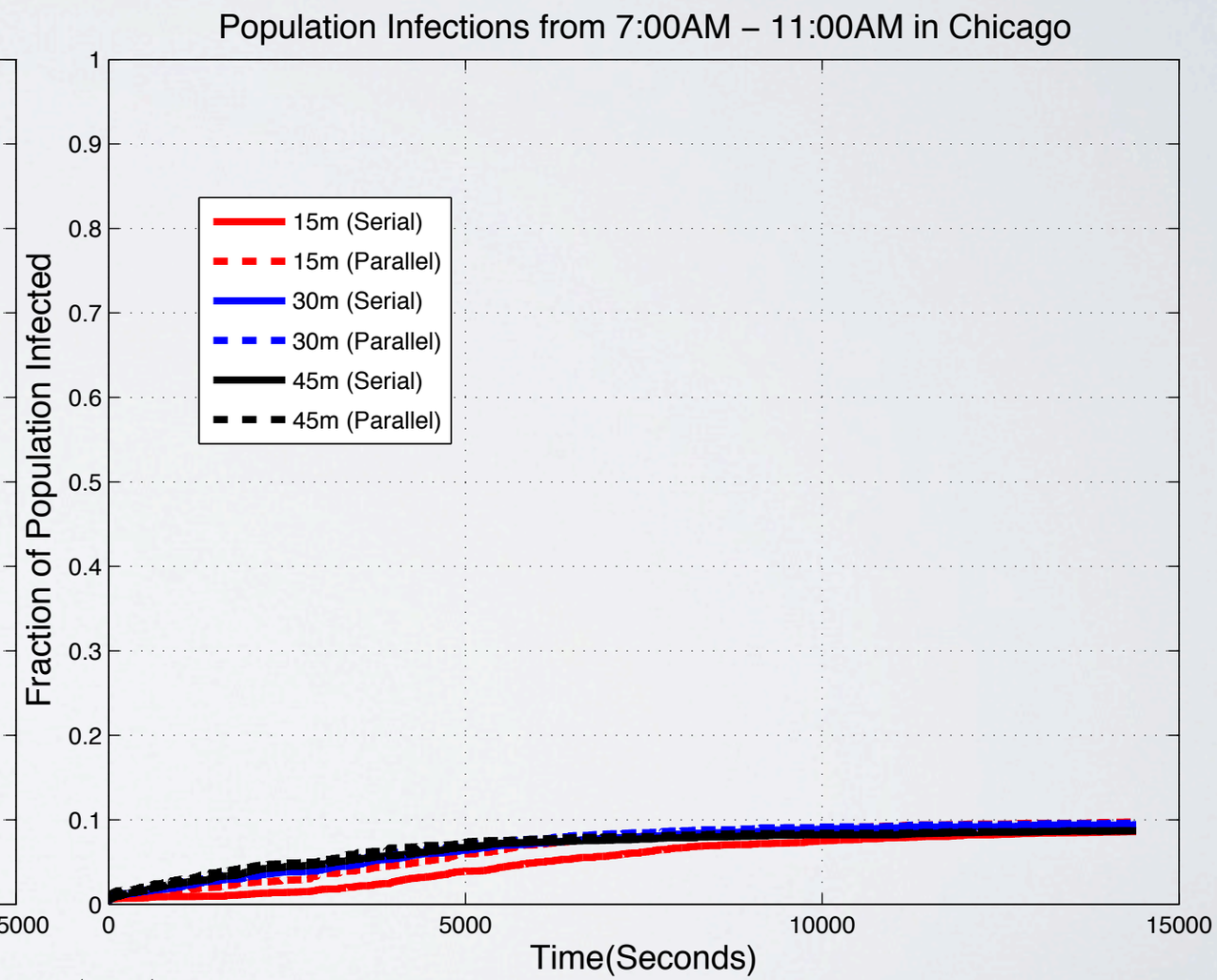
Not-Infected

Infected

INDIANA UNIVERSITY
BLOOMINGTON

BROADCAST RADIUS





Constants:

100% Susceptible

Exposure Time: 30s

Initial Infection: 1%

25% Susceptible

INDIANA UNIVERSITY
BLOOMINGTON

CONCLUSIONS

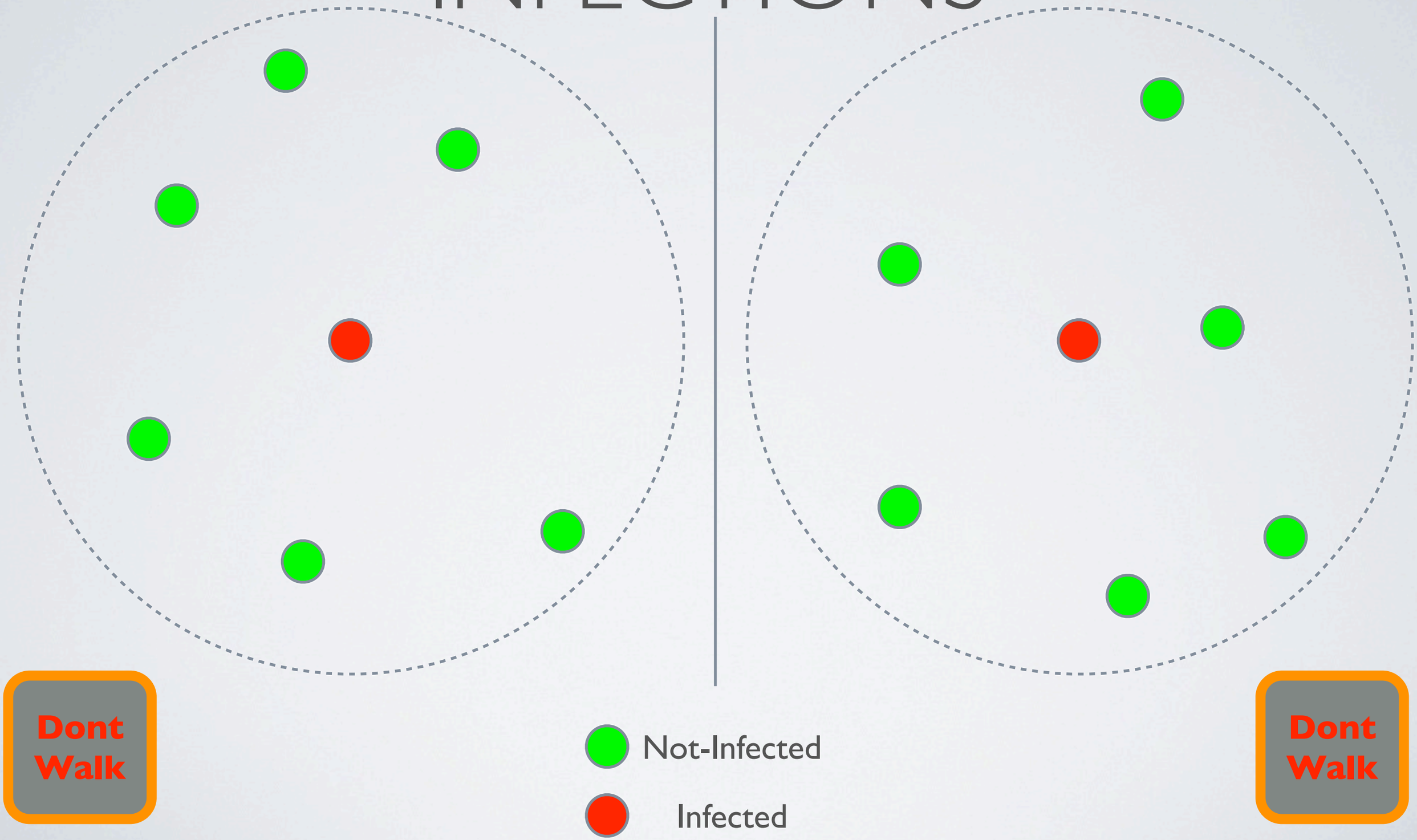
- Current U.S. city resident densities do not lead to epidemics, even with increased range
- Epidemics in the U.S. will only occur with very high (arguably unrealistic) susceptibility rates
- Parallel spread has little effect
- Mobile-to-mobile epidemics are the least of our worries...
  - Privacy violating mobile malware -- Tapsnake
  - SoundComber -- http://www.cs.indiana.edu/~kapadia/soundcomber-news.html
  - Malware targeting mobile banking -- Mitmo

QUESTIONS?

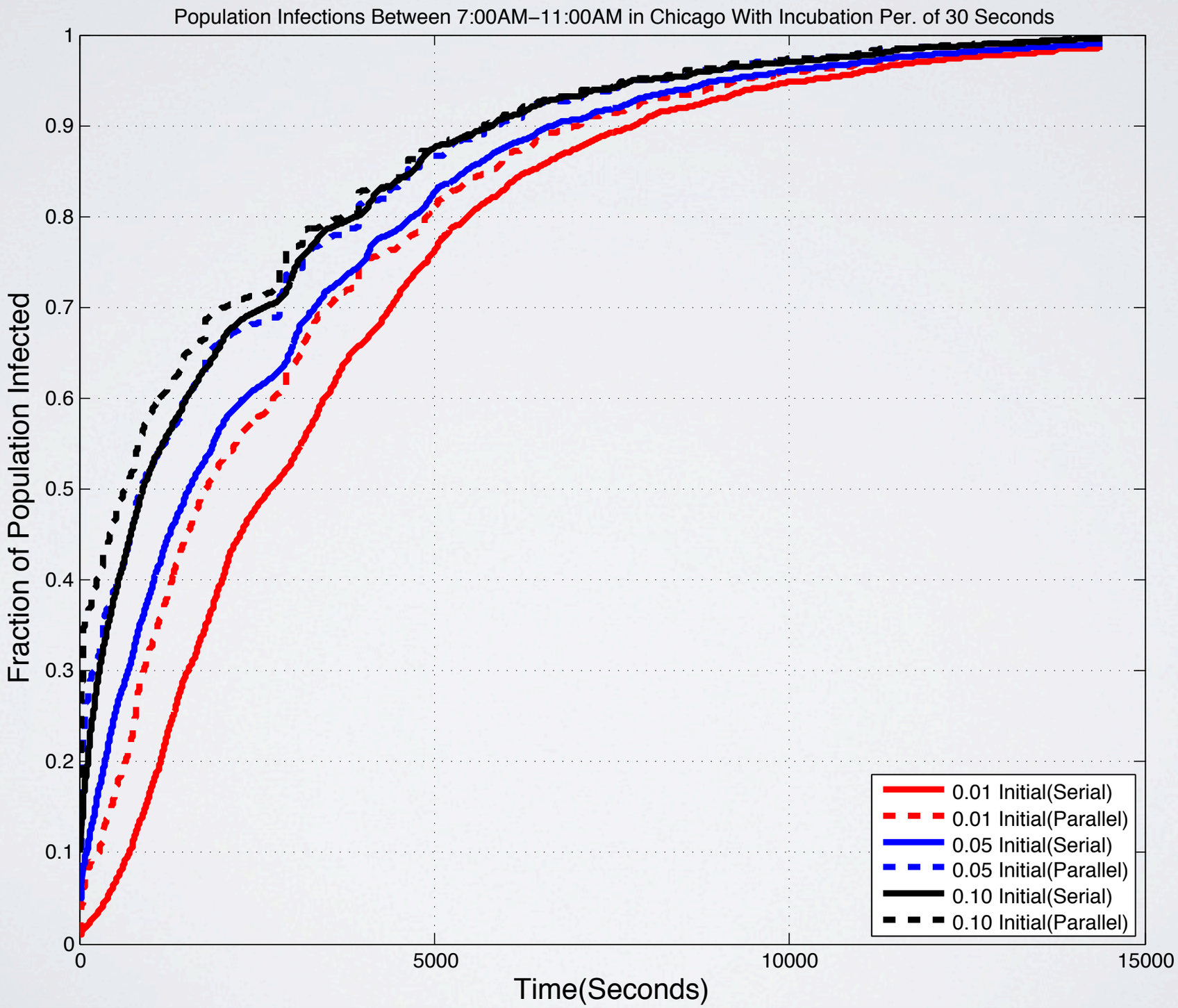
REFERENCES

- [Landscan] http://www.ornl.gov/sci/landscan/(July 2010).
- [CARETONNI07] CARETTONI, L., MERLONI, C., AND ZANERO, S. Studying bluetooth malware propagation: The bluebag project. IEEE Security and Privacy 5, 2 (2007), 17–25.
- [SU06] SU, J., CHAN, K., MIKLAS, A., PO, K., AKHAVAN, A., SAROIU, S., DE LARA, E., AND GOEL, A. A preliminary investigation of worm infections in a bluetooth environment. In Proceedings of the 4th ACMworkshop on Recurring malcode (2006), ACM, p. 16.
- [WANG09] WANG, P., GONZALEZ, M., HIDALGO, C., AND BARABASI, A. Understanding the spreading patterns of mobile phone viruses. Science 324, 5930 (2009), 1071.
- [CHANNAKESHAVA09] CHANNAKESHAVA, K., CHAFEKAR, D., BISSET, K., KUMAR, V., AND MARATHE, M. EpiNet: a simulation framework to study the spread of malware in wireless networks. In Proceedings of the 2nd International Conference on Simulation Tools and Techniques (2009), ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), pp. 1– 10.

SERIAL VS. PARALLEL INFECTIONS



INFECTED POPULATIONS



INDIANA UNIVERSITY
BLOOMINGTON