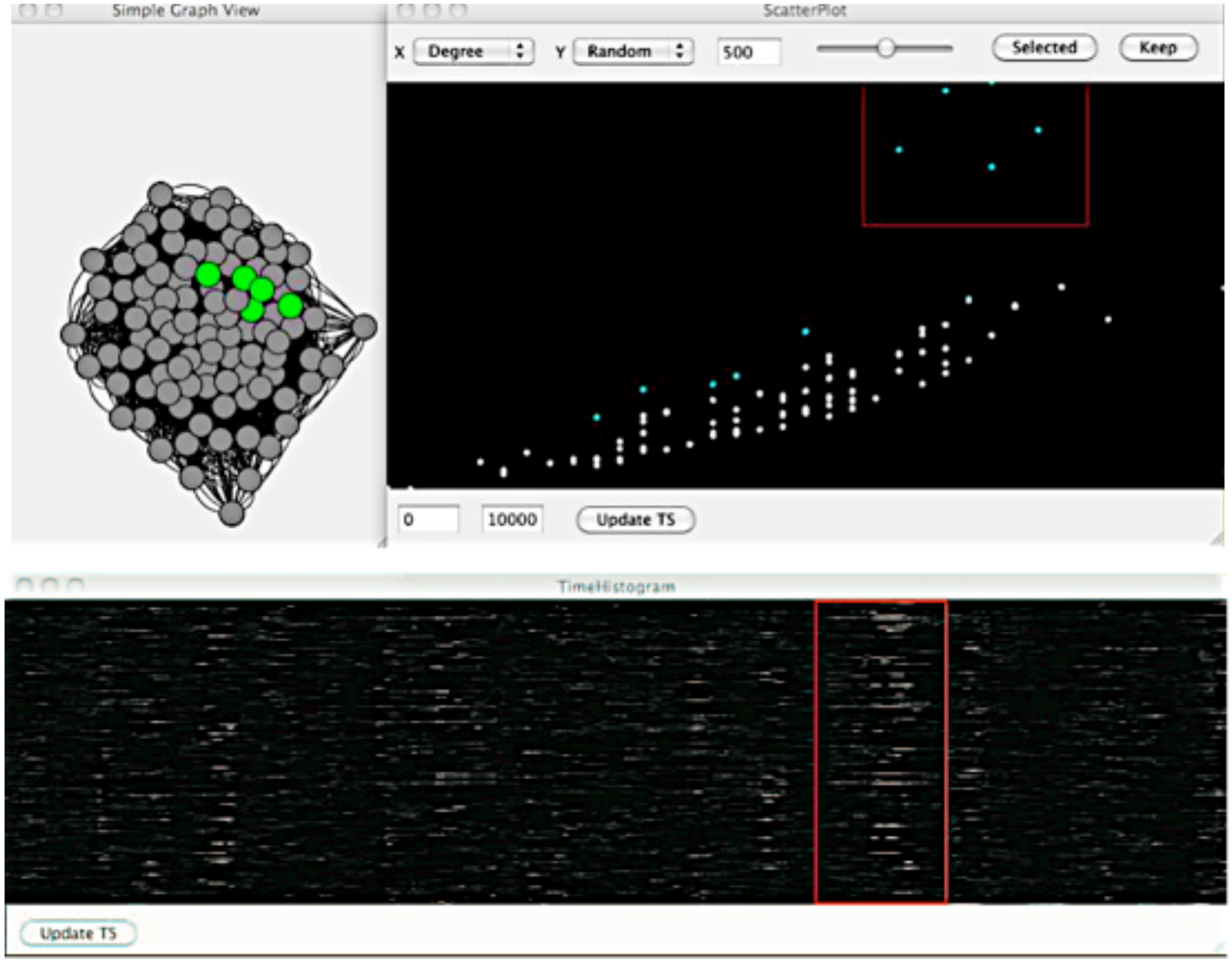
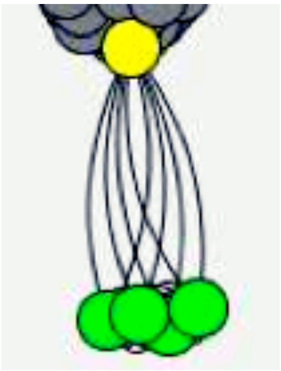


Interactive Detection of Network Anomalies via Coordinated Multiple Views

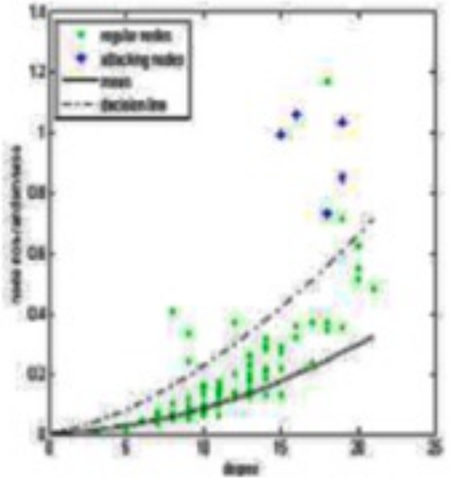
Lane Harrison, Xianlin Hu, Xiaowei Ying, Aidong Lu, Weichao Wang, Xintao Wu
University of North Carolina at Charlotte

Outline

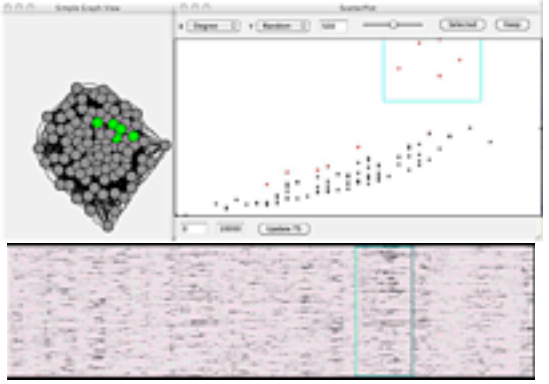
Sybil Attacks



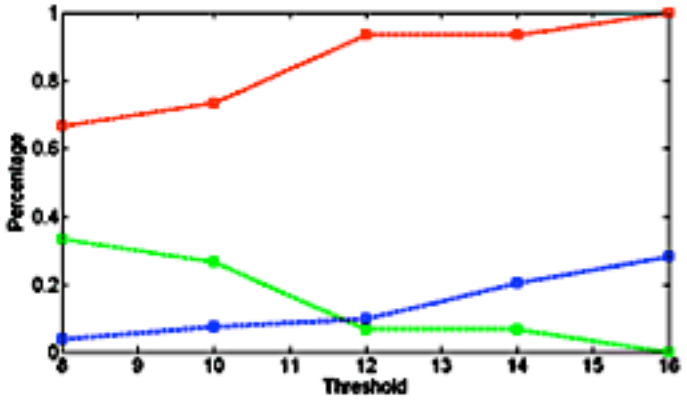
Spectral Analysis



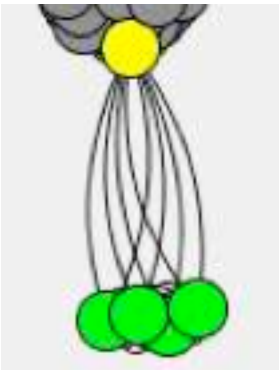
Coordinated Multiple Views



Case Studies



Sybil Attacks

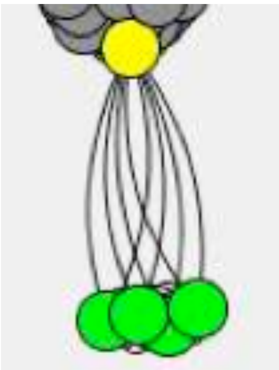


One can have, some claim, as many electronic personas as one has time and energy to create.

Defined by J. R. Douceur, 2002

Fundamental problem in P2P networks

Shirley Ardell Mason (**Sybil**)



Sybil Attack Threats

Voting Systems

Reputation Systems

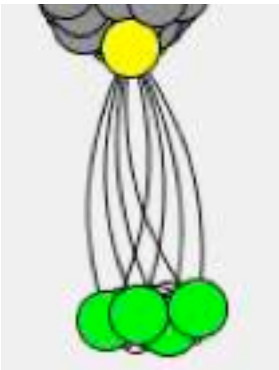
Misbehavior Detection

Routing

Distributed Storage

Resource Allocation

Newsome et al



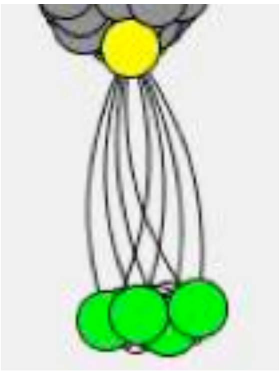
Sybil Attack Types

Direct vs. Indirect

Fabrication vs. Impersonation

Simultaneous vs. Non-Simultaneous

Newsome et al



Sybil Defense

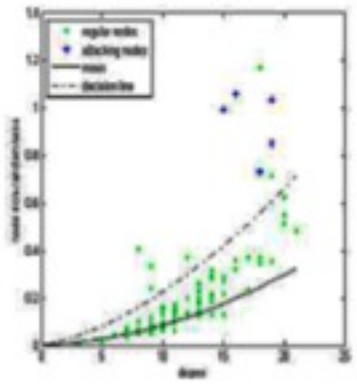
Device Resource Testing

Radio Signal Testing

Location Testing

Random Key Pre-distribution

Topological Methods

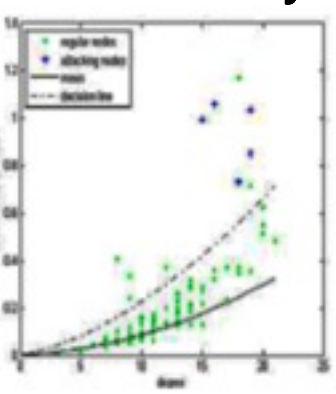


Spectral Analysis

Part of Graph Theory

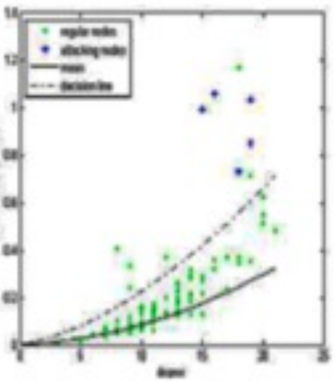
Assigns metrics to topological features of nodes in a network

Many other metrics remain unexplored in visualization



Spectral Decomposition

A as an nxn matrix	$A = (a_{ij})_{nxn}$
	$\downarrow$
Decomposition	$\sum_{i=1}^{n} \lambda_i \boldsymbol{x}_i \boldsymbol{x}_i^T$
	$\downarrow$
Non-Randomness	$R_i = \sum_{j=1}^{k} \lambda_j x_{ji}^2$



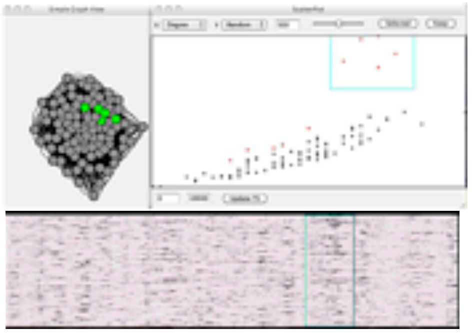
Putting it together

Sybil nodes, under most cases, have similar neighbors over time.

Non-randomness values for these nodes are high.

This alone is not enough to achieve detection with certainty.

CMV

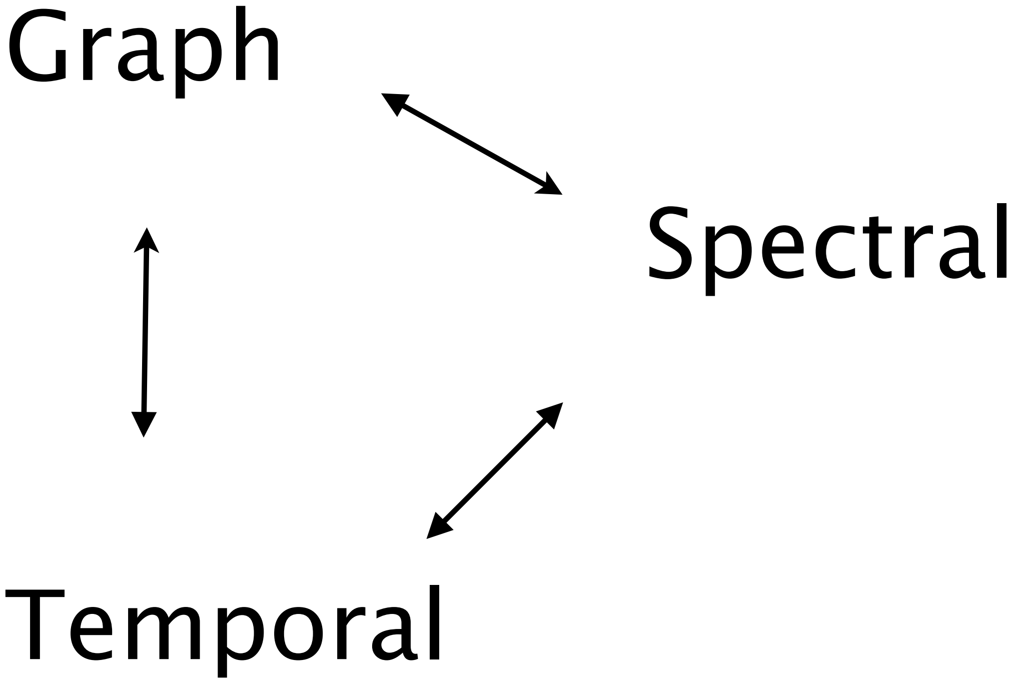


Coordinated Multiple Views

Auto-detection amplification

Iterative exploration

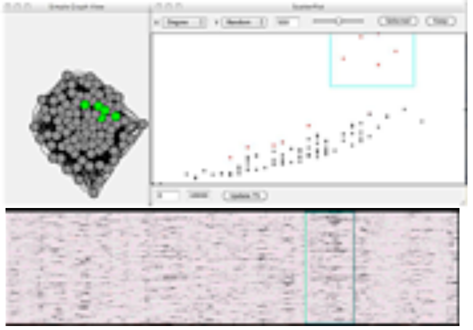
Simulated wireless network data used



Graph

Spectral

Temporal

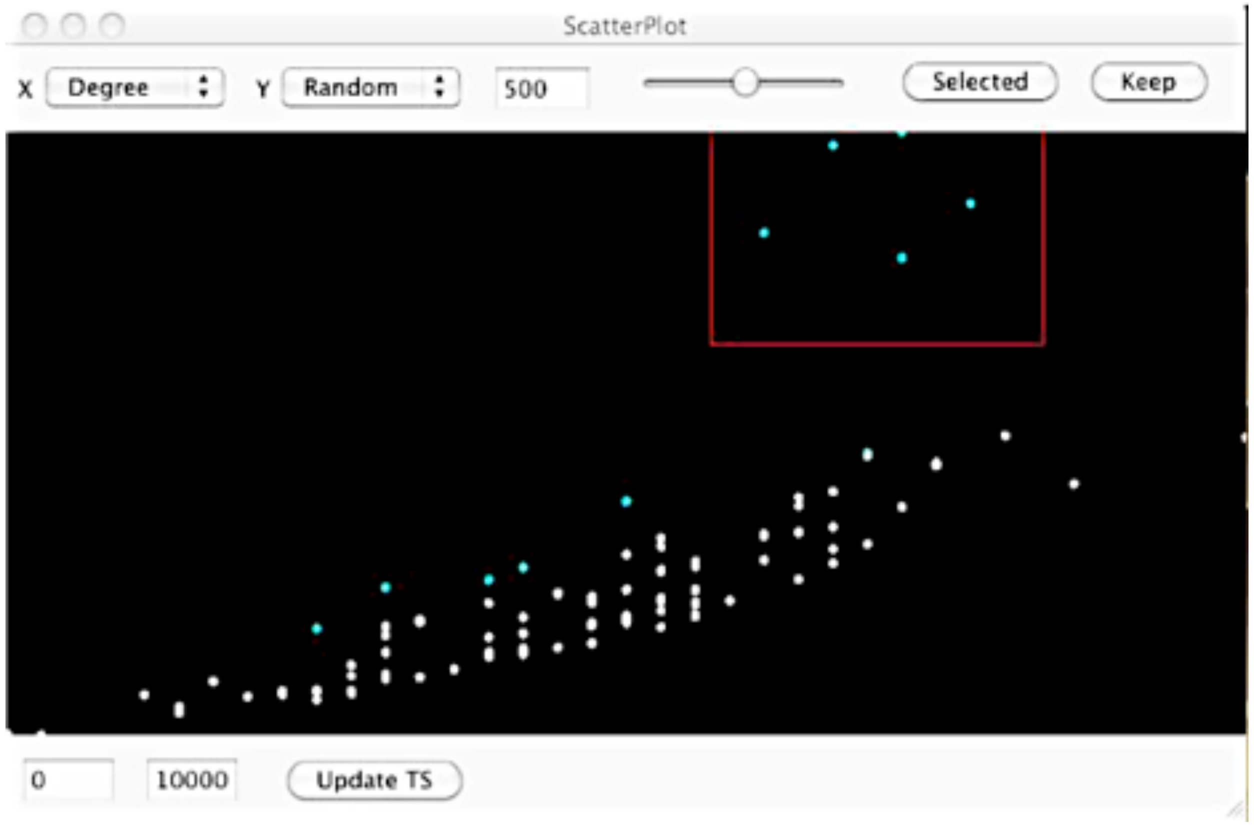


Spectral - Scatterplot

Display Degree/Random or EigV1/EigV2

Selections are shown in the graph space

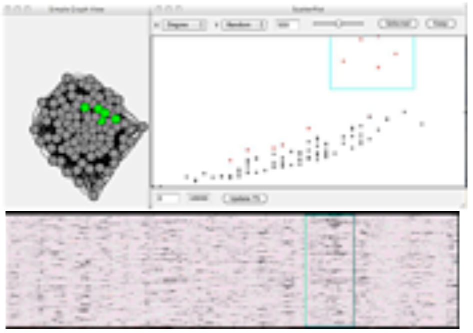
Spatially consistent position of outliers



X Degree Y Random 500

0 10000

CMV

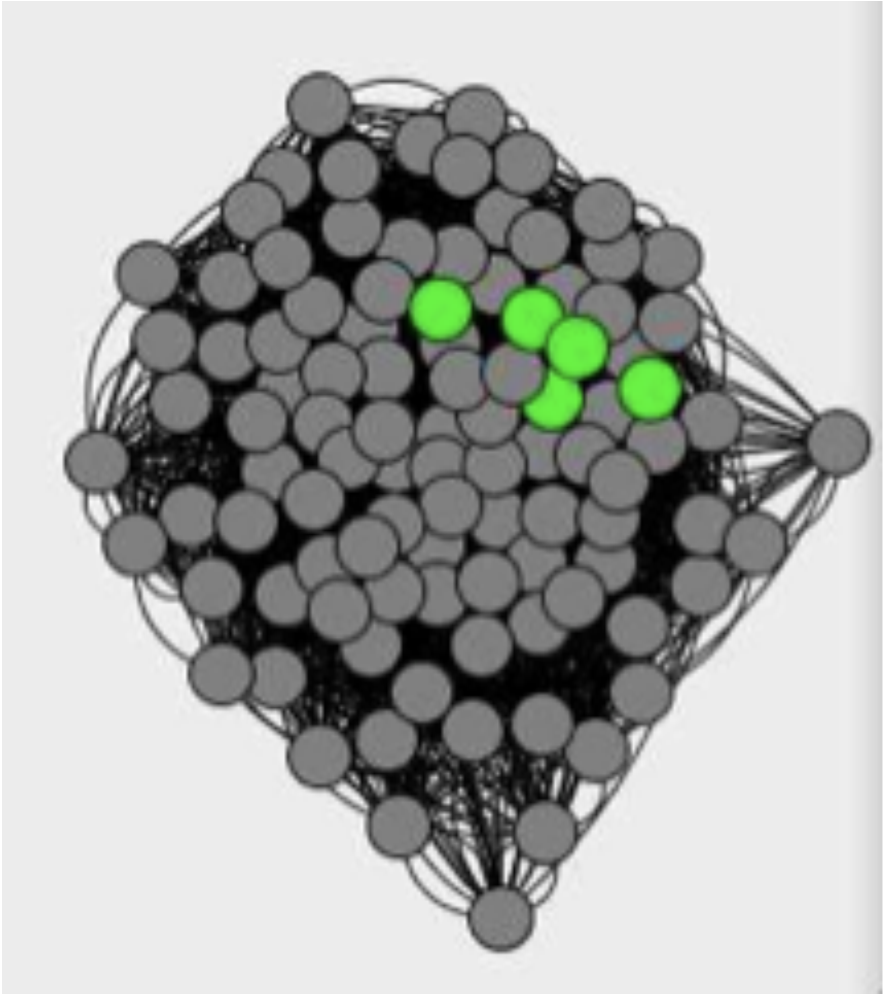


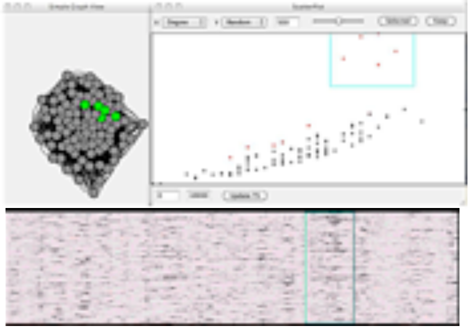
Graph - Node-Link

Connectivity relationships and subgraphs

Better suited for interactions (vs. matrix visualizations)

Limited scalability, but could only visualize outliers

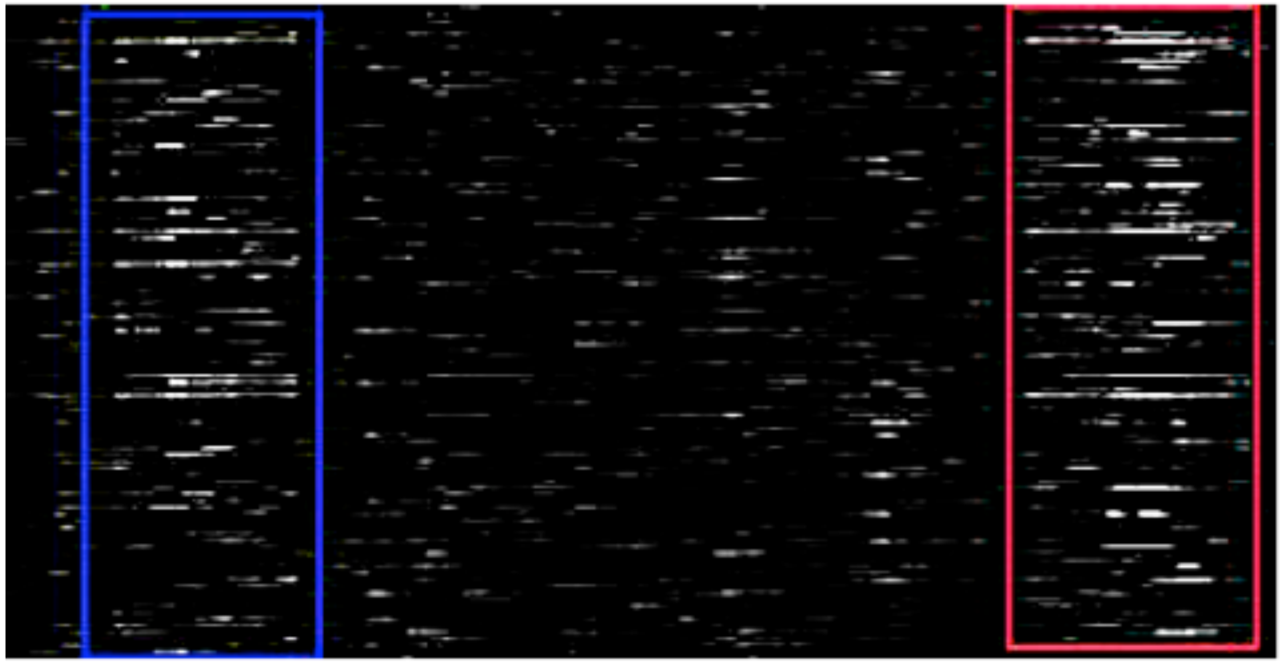


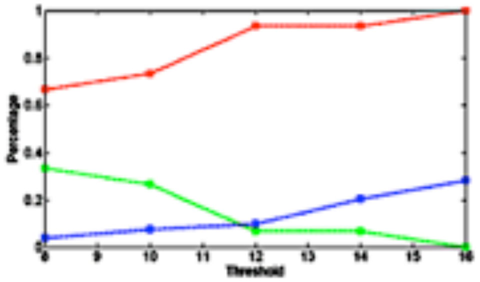


Temporal - Time-Histogram

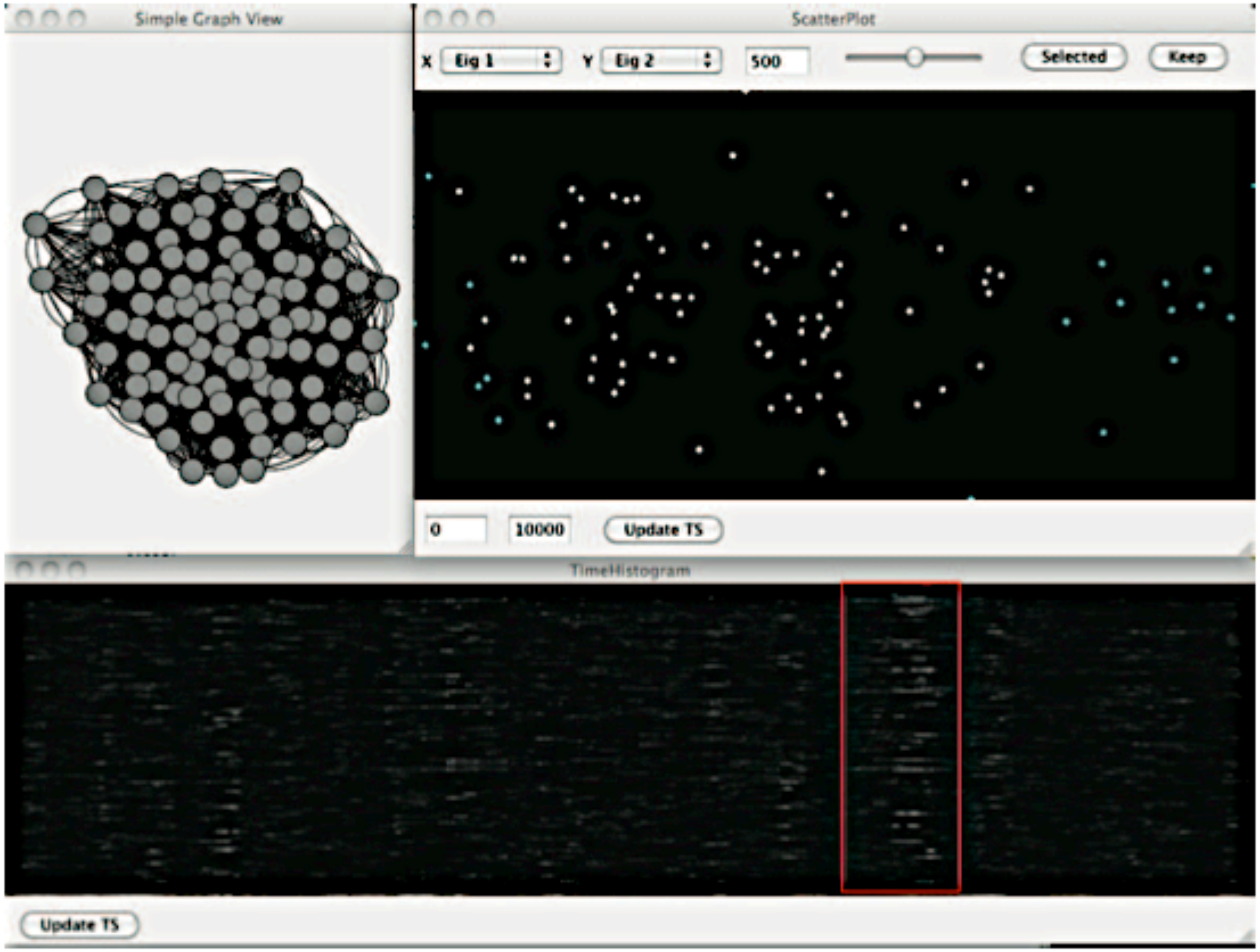
Used to identify suspicious durations

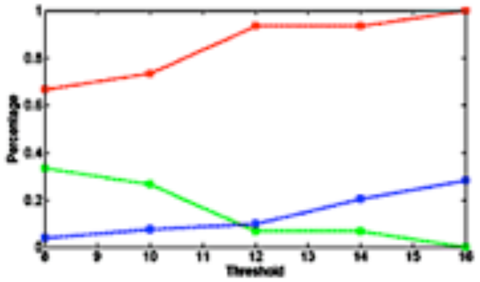
Necessary for detection success



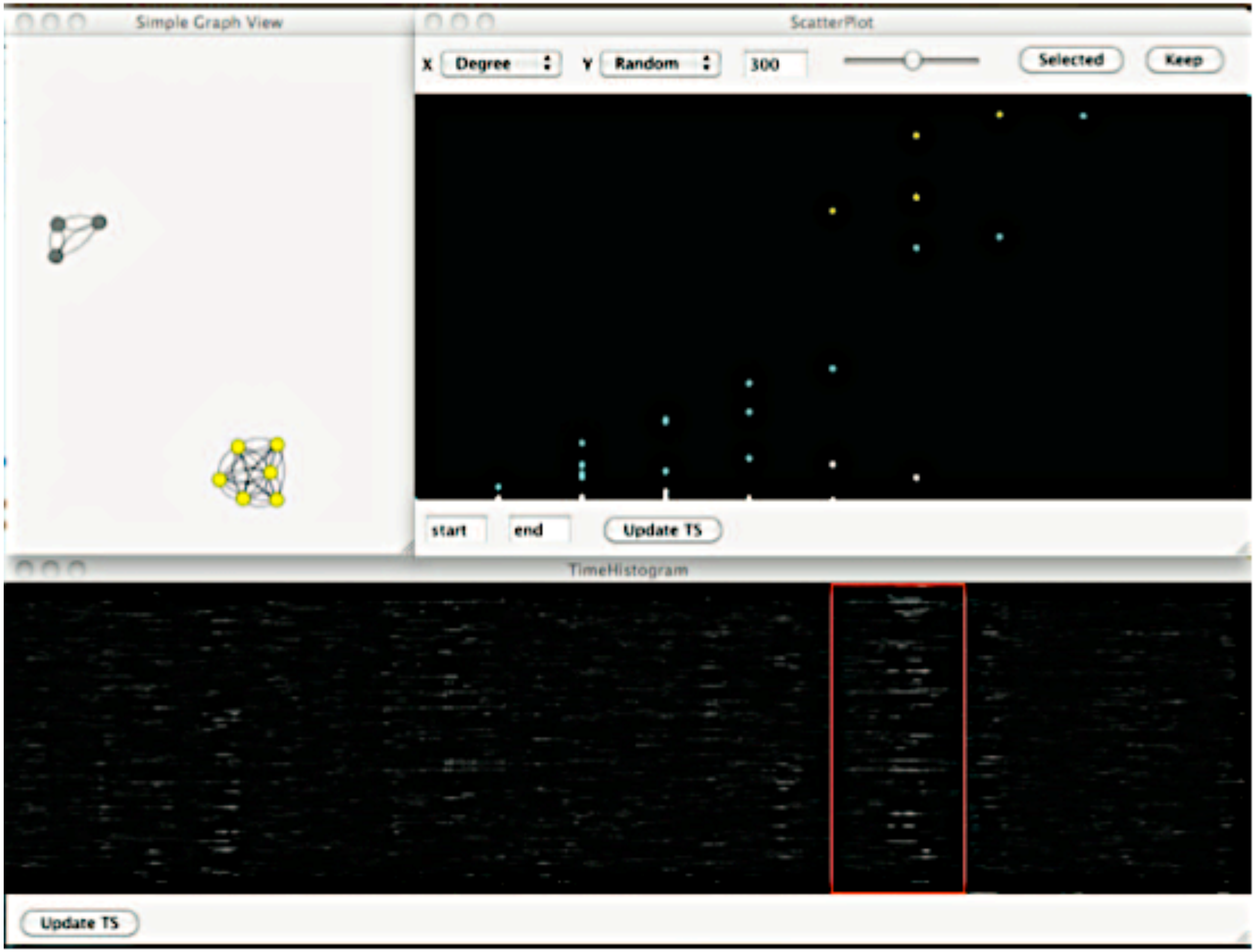


Direct Sybil Attack

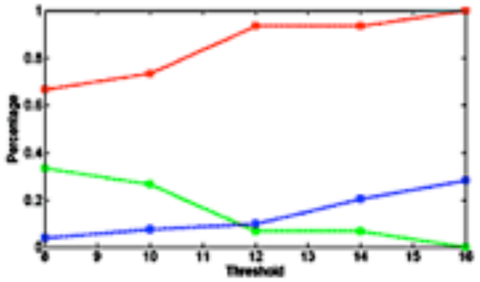




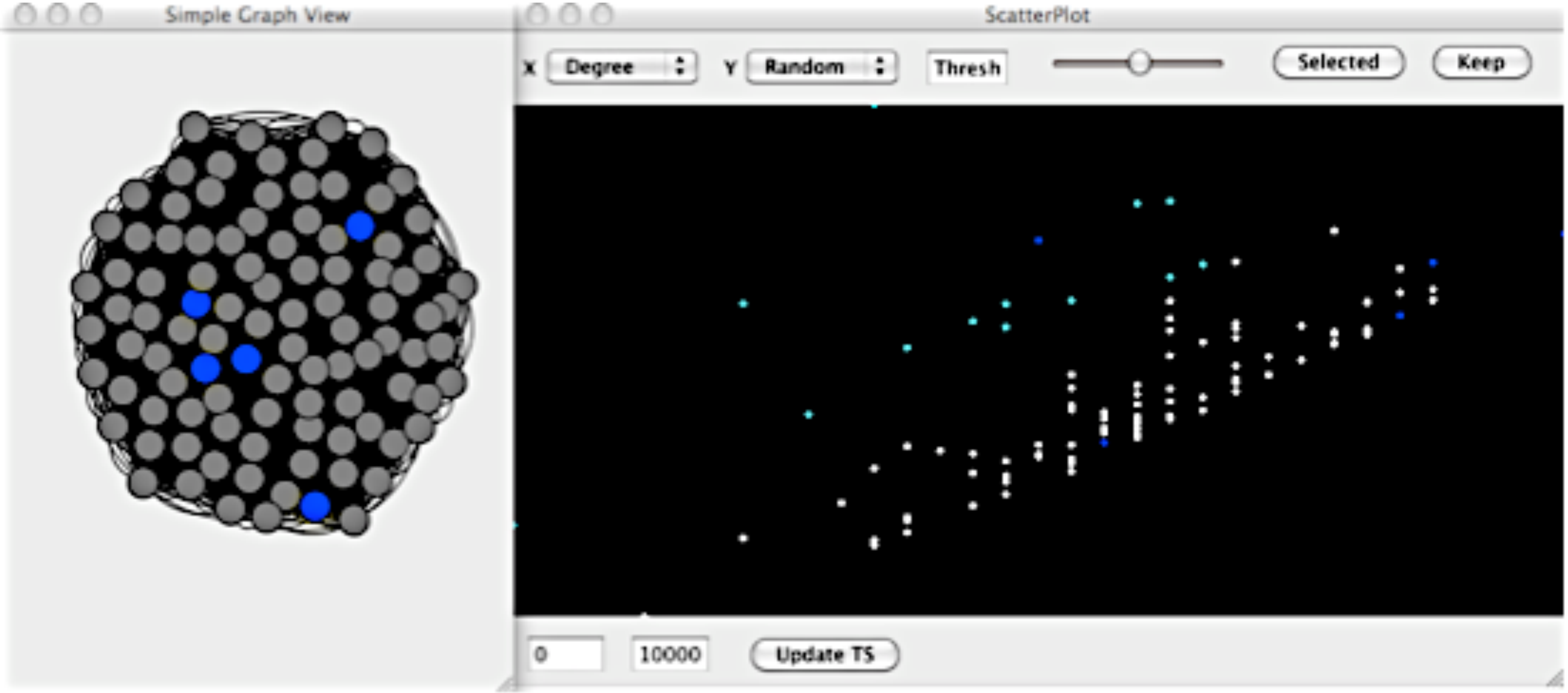
Direct Sybil Attack

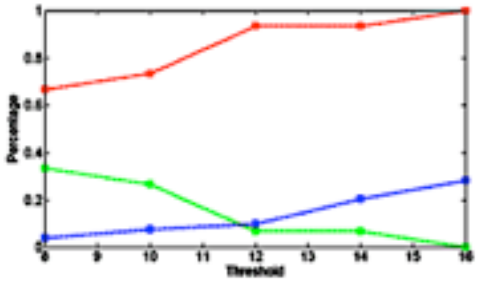


X Degree Y Random 300

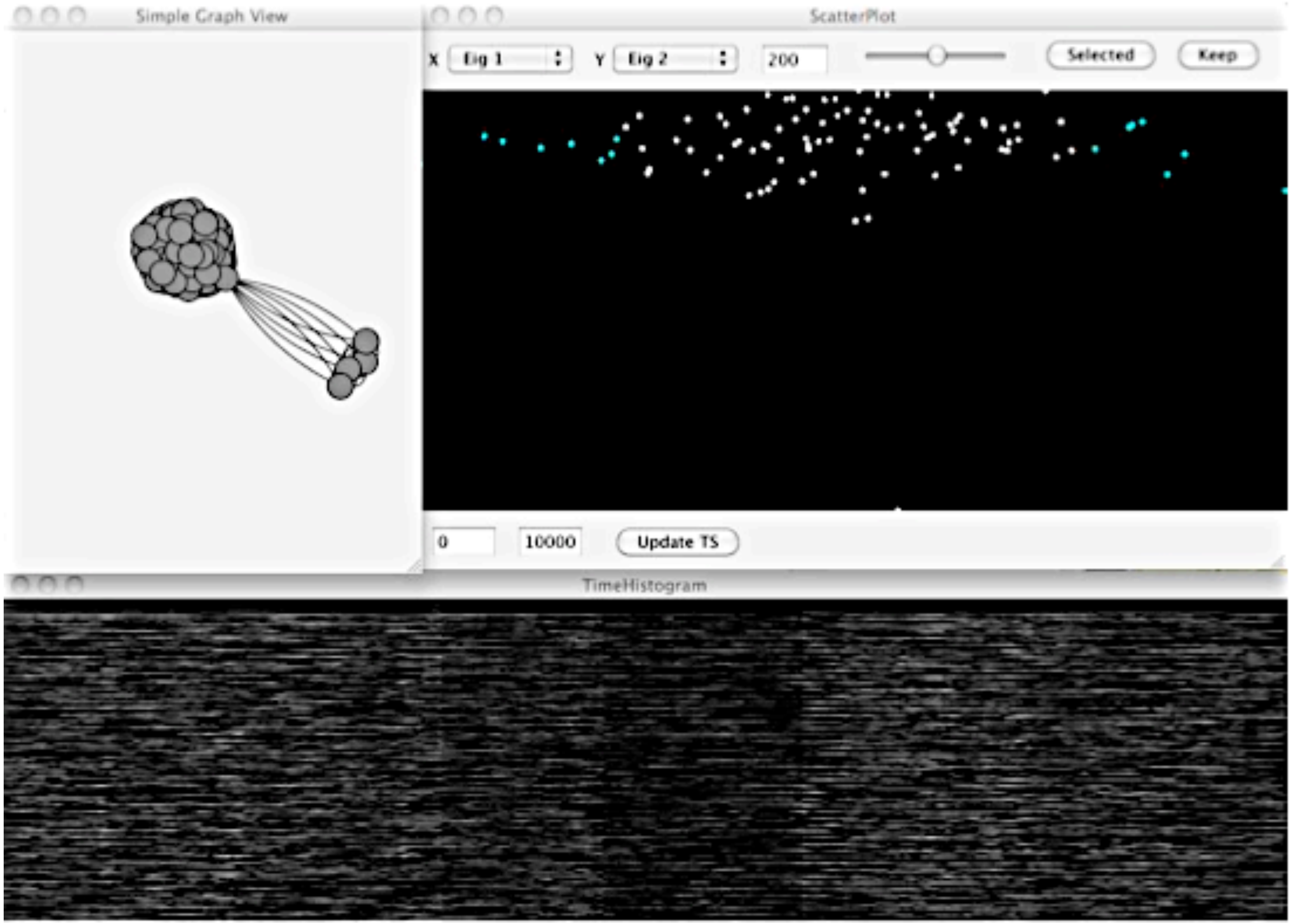


Direct Sybil Attack



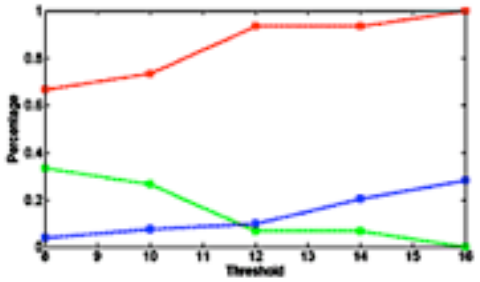


Indirect Sybil Attack

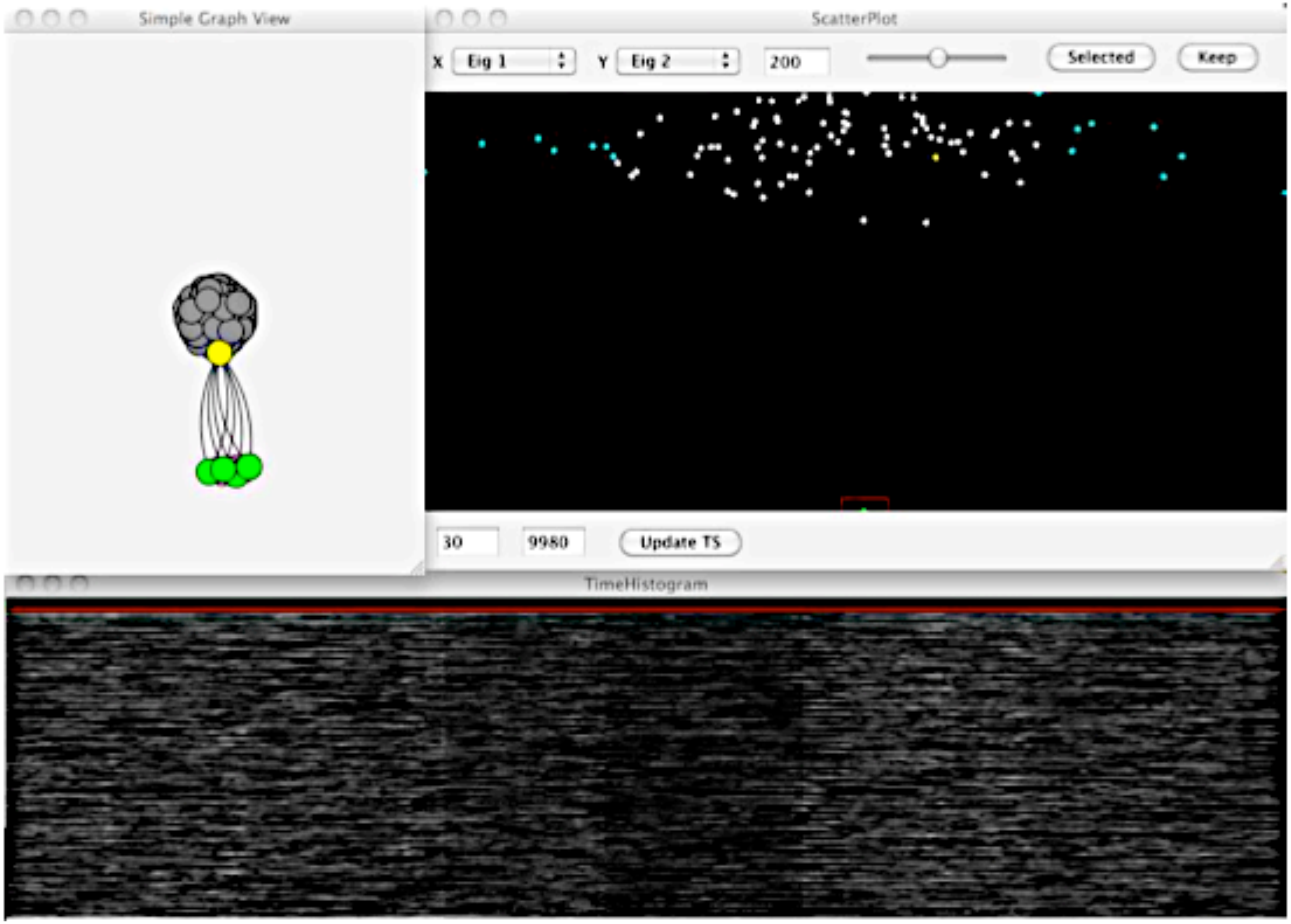


X Eig 1 Y Eig 2 200

0 10000

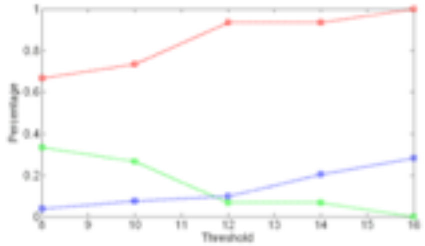


Indirect Sybil Attack

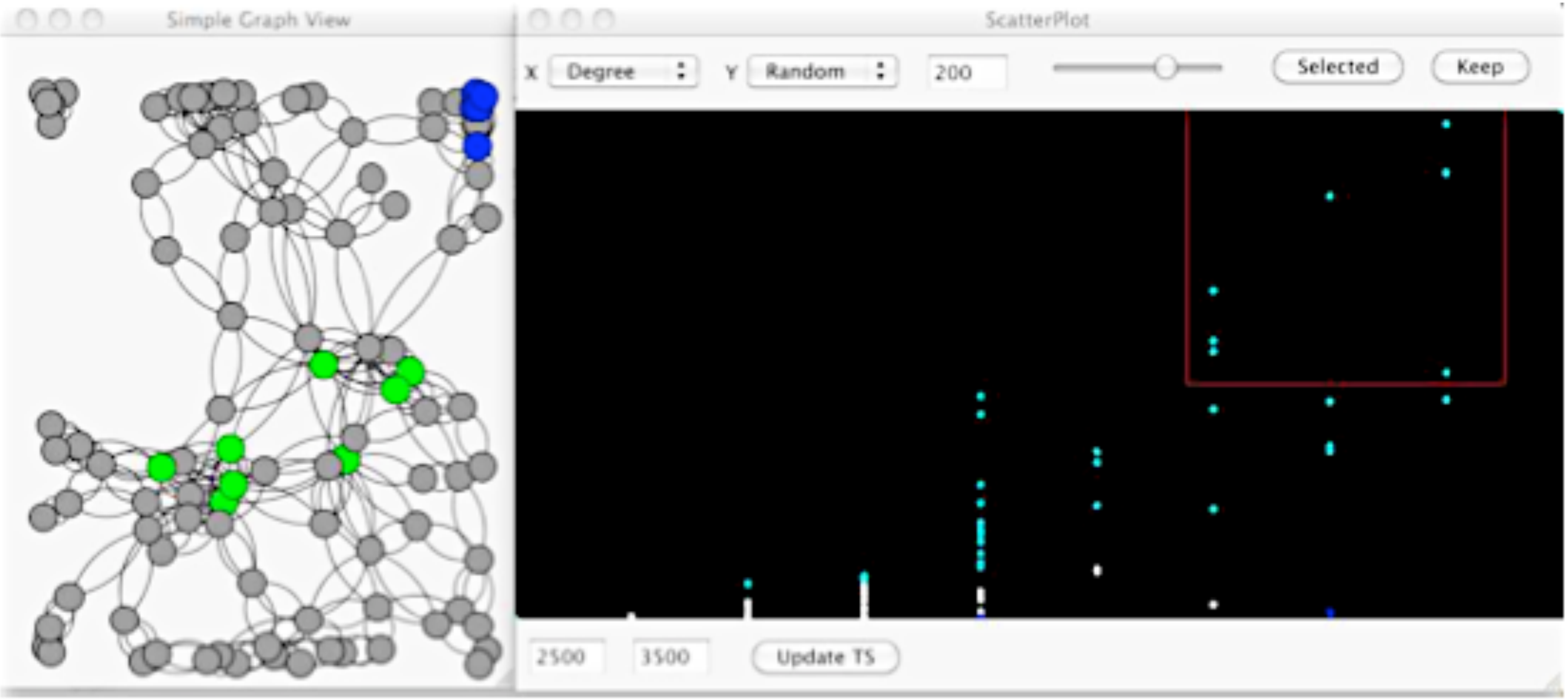


X Eig 1 Y Eig 2 200

30 9980



Indirect Sybil Attack



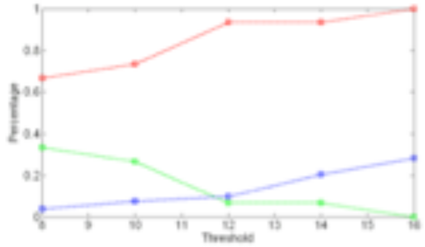
X Degree

Y Random

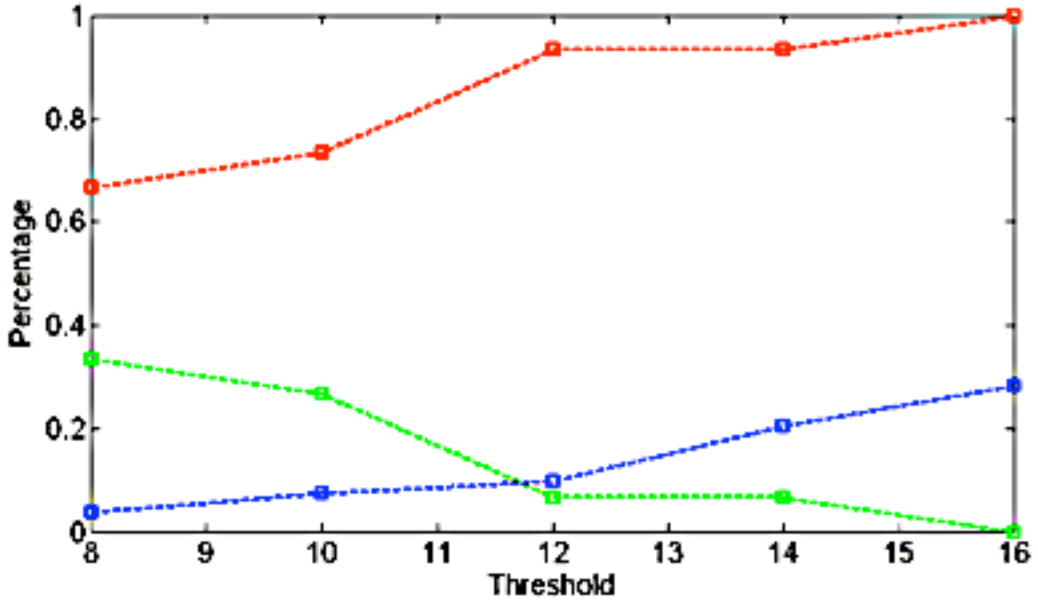
200

2500

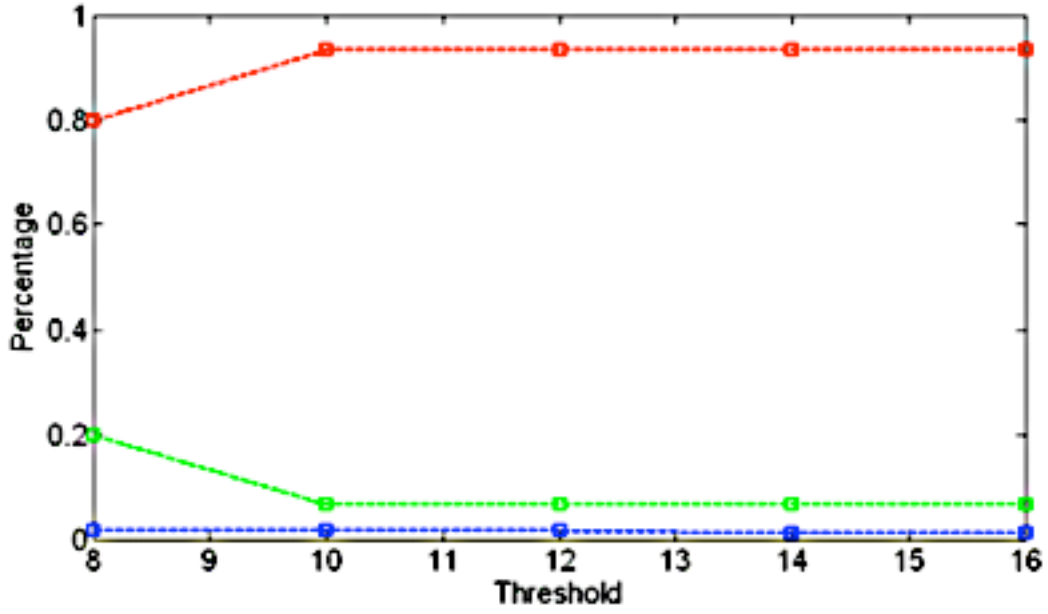
3500



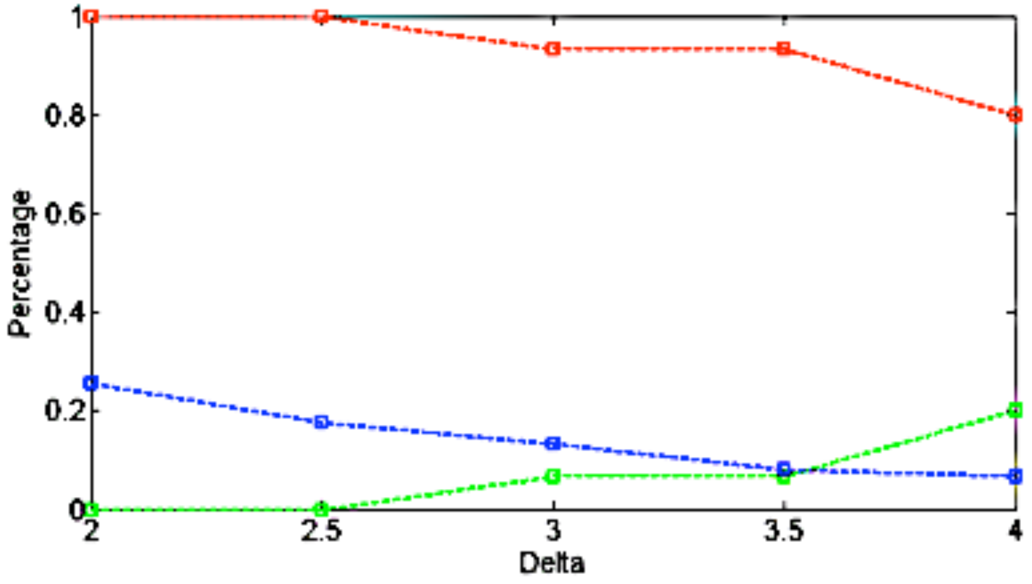
Detection Rate Comparison



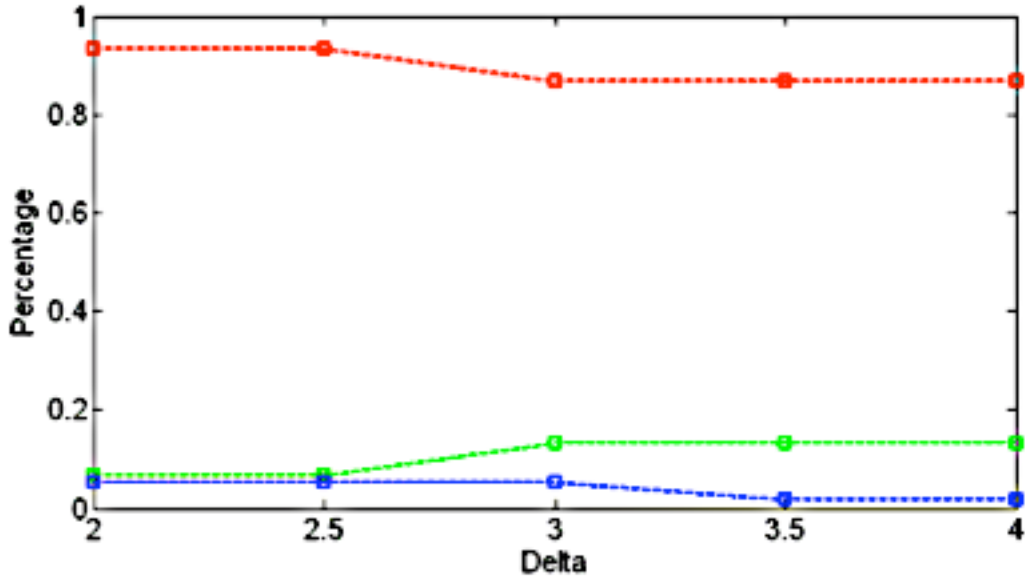
(a) false alarm rate *vs* threshold value



(a) false alarm rate *vs* threshold value



(b) false alarm rate *vs* delta value



(b) false alarm rate *vs* delta value

Conclusion

Detection can be achieved by combining CMV with automated-analysis.

Acknowledgements

- DOE Award No. DE-FG02-06ER25733
- NSF Awards Nos. 0754592, 0831204, and 1047621
- U.S. Department of Homeland Security Award No. 2008-ST-104-000017