Luke Osterritter
losterritter@cmu.edu

Dr. Kathleen Carley
kathleen.carley@cs.cmu.edu

Carnegie Mellon University
www.casos.cs.cmu.edu

Modeling Social Interventions for Insider Threat

Motivation

What is “Insider Threat”?

“a **current or former employee**, contractor, or business who has or had authorized access to an organization’s network, system, or data and **intentionally exceeded or misused** that access in a manner that negatively affected the confidentiality, integrity, or availability of the organization’s information or information systems” – CERT Guide to Insider Threat

Insider Threat has a **low base rate** of occurrence and is **difficult to detect**.

Doing experiments regarding the interplay of people and organizations on a meaningful scale could prove difficult or impossible: approaching the study of insider threat as a **modeling problem** is ideal.

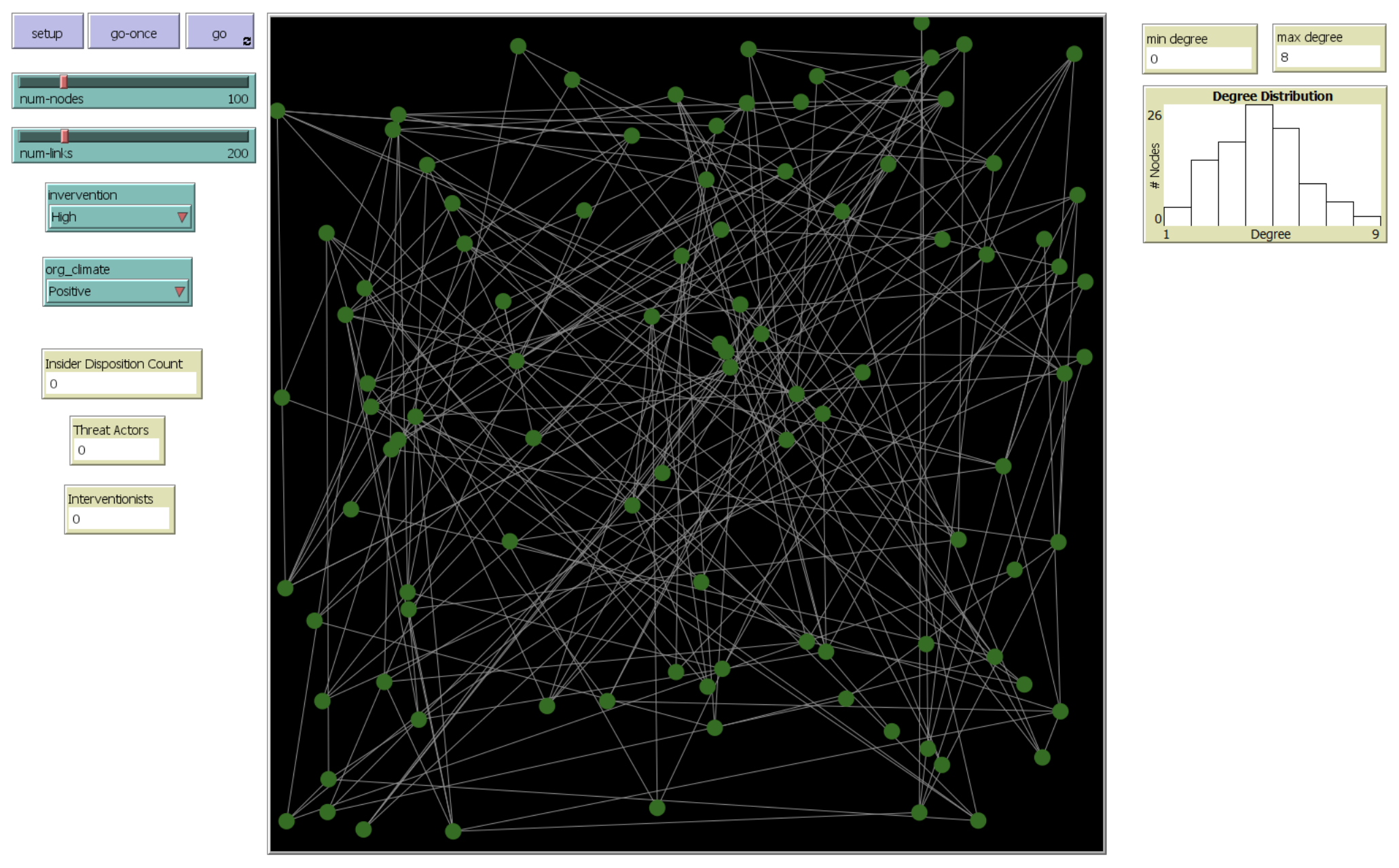
Can we use modeling to explore and demonstrate possible social interventions to prevent or lessen incidence of insider threat?

The Model

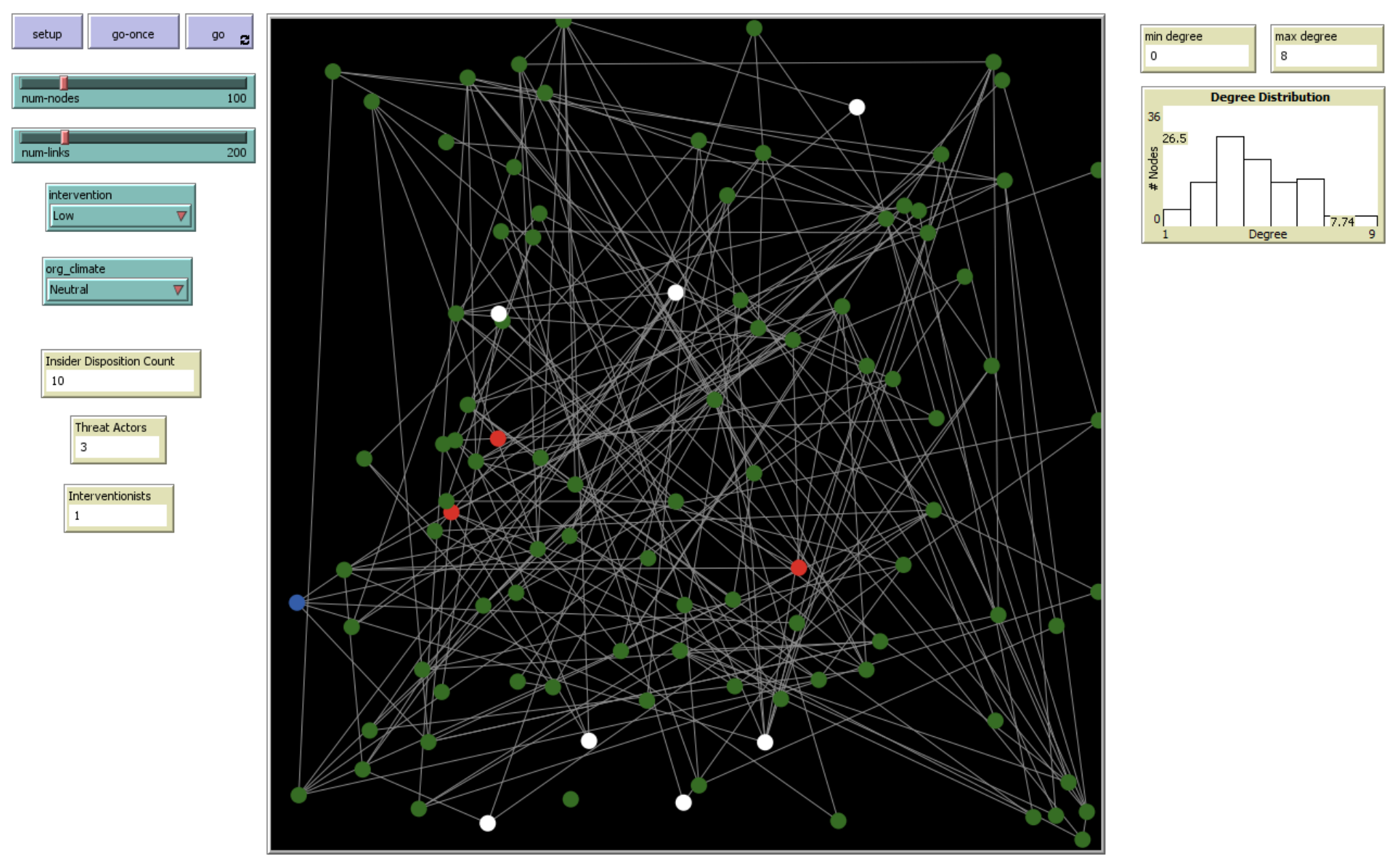
Base Run Details

	Time 1040, 1 run	Time 1040, 20 runs
Intervention level	Off	Off
Organizational climate	Neutral	Neutral
Interventionists	0	0
Agents with disposition above threshold	28	22.65 (avg) 4.09 (stdev)
Active malicious insiders	7	8.8 (avg) 2.82 (stdev)

Model Setup



Results of Base Run



Virtual Experiment Results

Negative Organizational Climate with Low Intervention

	Time 1040, 1 run	Time 1040, 20 runs
Intervention level	Low	Low
Organizational climate	Negative	Negative
Interventionists	1	1
Agents with disposition above threshold	17	15.6 (avg) 3.73 (stdev
Active malicious insiders	9	7.05 (avg) 2.31 (stdev)

Negative Organizational Climate with High Intervention

	Time 1040, 1 run	Time 1040, 20 runs
Intervention level	High	High
Organizational climate	Negative	Negative
Interventionists	3	3
Agents with disposition above threshold	0	2 (avg) 1.55 (stdev)
Active malicious insiders	0	.85 (avg) 0.81(stdev)

Conclusions

- Social interventions can help to reduce or eliminate instances of insider threat which feature social isolation as a precursor.
- Even a low intervention rate can reduce the number of malicious insider occurrences
- Provides a strong proof-of-concept for realizing the the social interplay at work in organizations, the cause and occurrence of malicious insider attacks, and possible intervention strategies.

This work was supported in part by the the Center for Computational Analysis of Social and Organization Systems (CASOS) and the SEI Software Scholars Program. The views and conclusions contained in this document are those of the authors and should not be interpreted as representing official policies, either expressed or implied, of the U.S. government.