Understanding Sanction under Variable Observability in a Secure, Collaborative Environment

Hongying Du, Bennett Narron, Nirav Ajmeri,
Emily Berglund, Jon Doyle, Munindar P. Singh

Department of Computer Science
North Carolina State University

April 21, 2015

Outline

Research Goal

- Understanding how norm-related factors – sanction type and observability – influence a system that pursues security
  - An academic scenario used in our experiment is a proxy of a typical industry scenario

Hard Problem in Security

- Policy-governed secure collaboration

Background (1)

Norm. A directed relationship between two participants within an organizational context

- Failure to comply with normative expectations – *Sanction*

Resilience. The ability to "recover and restore the system to the original state or, if need be, some acceptable state that is different but still safe"

Security.

- Safety: the system does not enter a bad state
- Liveness: users are able to perform their business tasks

Background (2)

Observability. The ability to discover norm violations in terms of time, sooner or later

- *Immediate* – detects norm violations instantaneously
- *Delayed* – requires time to discover norm violations

Sanction Types. We are interested in

- *Individual Sanction* – sanctions agents who violate norms
- *Group Sanction* – sanctions all the agents in an organization

Research Questions

RQ 1. Can one predict resilience of system as a function of different sanction and observability types?

RQ 2. Do any trade-offs exist among sanction, observability, and security?

Why Agent-Based Simulation?

- Problems computationally hard
- Outside of our ability to address using a game-theoretic approach
- Simulation helps us foresee outcomes / problems
- Designed and implemented an exploratory multiagent simulation

Outline

The System: CARLOS

A university graduate research lab and its constituent student researchers, represented by agents

- A *Lab*, or an organization
- A set of *Student Agents*, each representing a graduate research assistant who controls a PC in the lab
- *Carlos*, who is responsible for sanctions, with a kind of observability

Student Agents

Types of Tasks

- *Research Task* – Resilience, Liveness
- *Security Task* – Norm, Safety

Tasks' Attributes

- *Duration*
- *Deadline*

Student Agent's Attributes

- *Agent Health* represents a student agent's health and corresponds to the research tasks assigned to the agent
- *PC Health* represents the PC's health and corresponds to the security tasks assigned to the agent
- *Preference*
- *Research Motivation*
- *Security Compliance*

Change of Attributes

According to Task Completion Status

Task Completion Status	Agent Health	PC Health	Research Motivation
Research task finished	Increase	No Effect	No Effect
Research task not finished	Decrease	No Effect	Increase
Security task finished	No Effect	Increase	No Effect
Security task not finished	No Effect	Decrease	No Effect

Norms in Academic Setting

- Security protocols to ensure the security of the whole network
- Research tasks are required to be done.

Hypotheses in Academic Setting

H1. Delayed observability results in greater motivation of the agents to perform research-related tasks than immediate observability

H2. Group sanction yields greater compliance to security norms than individual sanction

Outline

Evaluation

- Assumptions
- Different network sizes
  - Small (100 agents)
  - Medium (500 agents)
  - Large (1000 agents)
- Observability: Immediate or Delayed
- Sanction: Individual or Group
- 100 simulations for each network size

Metrics

- *System Research Motivation*
  - Median of average of research motivation values of all agents at each tick
- *System Security Compliance*
- *System Load*: Median load
  - Load – Ratio of the number of agents actively performing a research task over the number of agents who have research tasks their queues
- *Resilience*
  - Measurement: average time it takes for the system to recover to an acceptable state after falling into a bad state
  - Smaller values – more resilient

Results

100 Agents over 100 Simulations

O – Observability, S – Sanction type, M – System research motivation, C – System security compliance, L – System load, R – Resilience

O	S	M	C	L	R	Research Tasks	Security Tasks		
						% complete	% complete	Violation	Sanction
Immediate	Individual	0.4	0.64	0.74	1.83	78%	84%	2297	2297
Immediate	Group	0.51	1	0.81	1.5	77%	86%	1961	142*
Delayed	Individual	0.4	0.64	0.74	1.24	78%	84%	2318	2318
Delayed	Group	0.51	1	0.8	1.14	78%	87%	1887	142*

* – Number of group sanctions. Null values for resilience in the tables mean there is no simulation in the 100 simulations where load is observed rising from 0.4 to 0.7. For resilience with non-null values, it is possible that some of the resilience values in 100 simulations are null, and resilience is the average of all the non-null resilience values.

Network Sizes

- The size of the network has no quantifiable affect on all the metrics except resilience
- For resilience, it is hard to compare since we have null resilience values for medium and large networks

Observability Types

- Observability has no influence on system research motivation, system security compliance and system load.
- **H1** Delayed observability results in greater motivation of the agents to perform research-related tasks than immediate observability – **Not Supported**

Table: Delayed Observability vs. Immediate Observability

Individual Sanction	Violations	$>$
Group Sanction	Sanctions	$=$
	Violations	$<$

Sanction Types

Group sanction motivates agents to comply with security policies by sanctioning the whole group whenever any single agent defects, thus leading to

- More completed security tasks (2% - 4%)
- Less norm violations than in individual sanction

H2 Group sanction yields greater compliance to security norms than individual sanction. – **Supported**

Outline

Threats to Validity

- Homogeneous agent behavioral characteristics
- Arbitrarily assigned sanction consequences
- Change of dependent variables according to common sense

Conclusions

- Group sanction motivates agents to comply with security policies; more cost-effective than individual sanction
- Agent-based simulation approach helps policy makers with decisions

Future Work

- A human-subject study or a survey, using concepts from fields including anthropology, sociology, and psychology, among others
- Inter-agent messaging
- Propagating actions such as informal sanction among agents
- Cost of sanctions
- Norm sanctioning capability of the administrator
- Combination of individual sanction and group sanction
- A formal mathematical representation of our model

Thank you

Simulation Settings (1)

Variables with Normal Distribution

Variable	Value
μ of Preference	0.5
σ of Preference	0.3
Upper Limit of Preference	0.8
Lower Limit of Preference	0.4
μ of Research Motivation	0.7
σ of Research Motivation	0.15
Lower Limit of Research Motivation	0.4
μ of Security Compliance	0.7
σ of Security Compliance	0.15
Lower Limit of Security Compliance	0.4
μ of Research Task Duration	5
σ of Research Task Duration	3
Lower Limit of Research Task Duration	1

Simulation Settings (2)

Experiment Parameters

Experiment Parameter	Value
Coefficient for Research Task Duration	1.3
Naturally Decrease Rate of PC Health	0.1
Increase Rate of Agent Health	0.25
Decrease Rate of Agent Health	0.25
Increase Rate of PC Health	0.25
Decrease Rate of PC Health	0.25
Increase Rate of Research Motivation	0.25

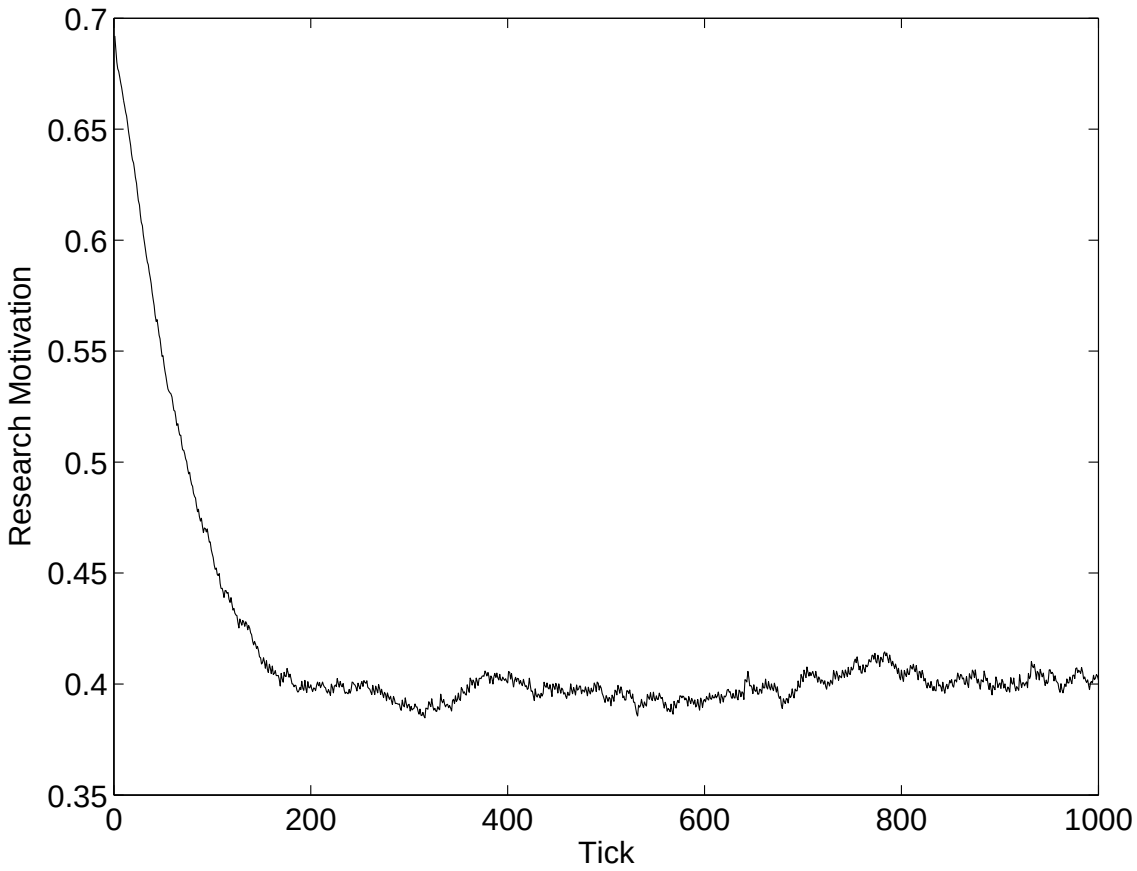
Results for 500 Agents over 100 Simulations

O	S	M	C	L	R	Research Tasks	Security Tasks		
						% complete	% complete	Violation	Sanction
Immediate	Individual	0.4	0.64	0.75	null	78%	84%	11487	11487
Immediate	Group	0.51	1	0.81	1.6	77%	86%	9784	142*
Delayed	Individual	0.4	0.64	0.74	null	78%	83%	12253	12164
Delayed	Group	0.5	1	0.8	1.01	78%	86%	9732	141*

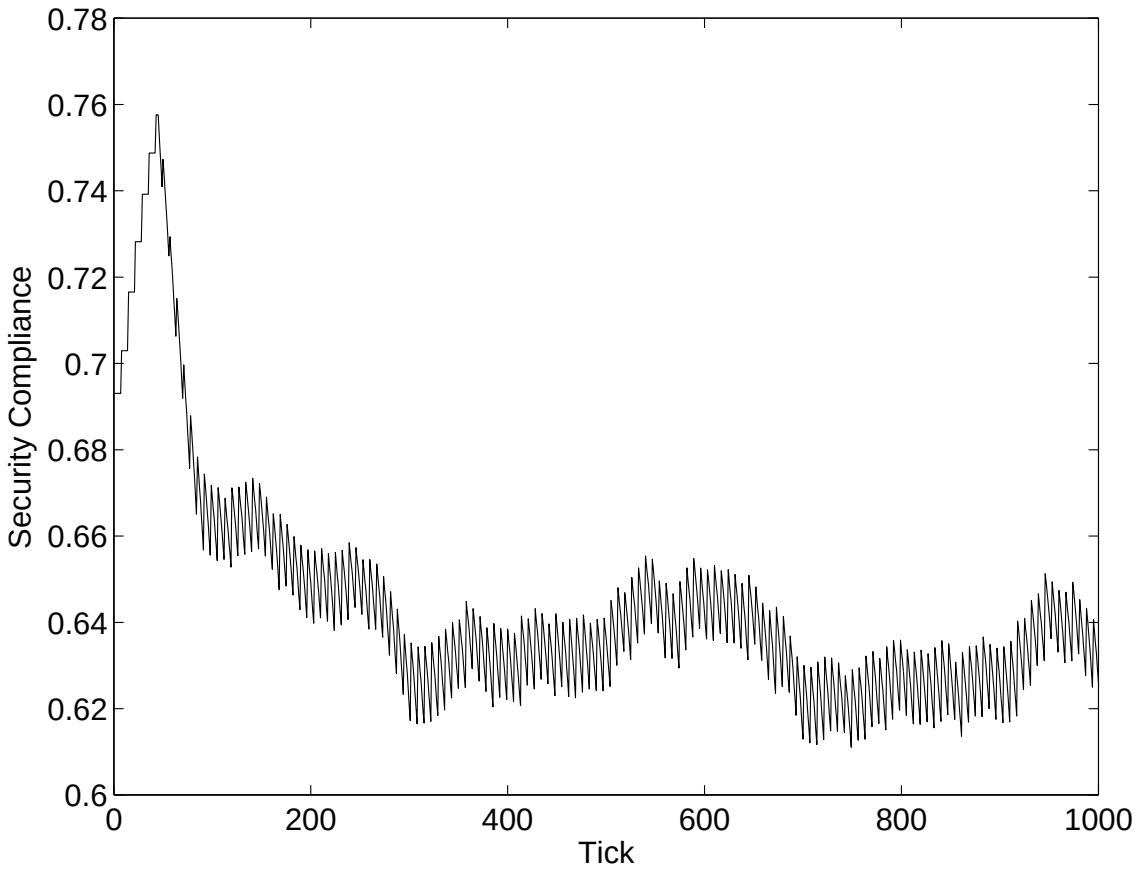
Results for 1000 Agents over 100 Simulations

O	*S*	*M*	*C*	*L*	*R*	Research Tasks	Security Tasks		
						% complete	% complete	Violation	Sanction
Immediate	Individual	0.4	0.64	0.75	null	78%	84%	22973	22973
Immediate	Group	0.51	1	0.81	1.62	77%	86%	19550	142*
Delayed	Individual	0.4	0.64	0.74	null	78%	82%	25760	25206
Delayed	Group	0.51	1	0.81	1.65	77%	86%	19580	139*

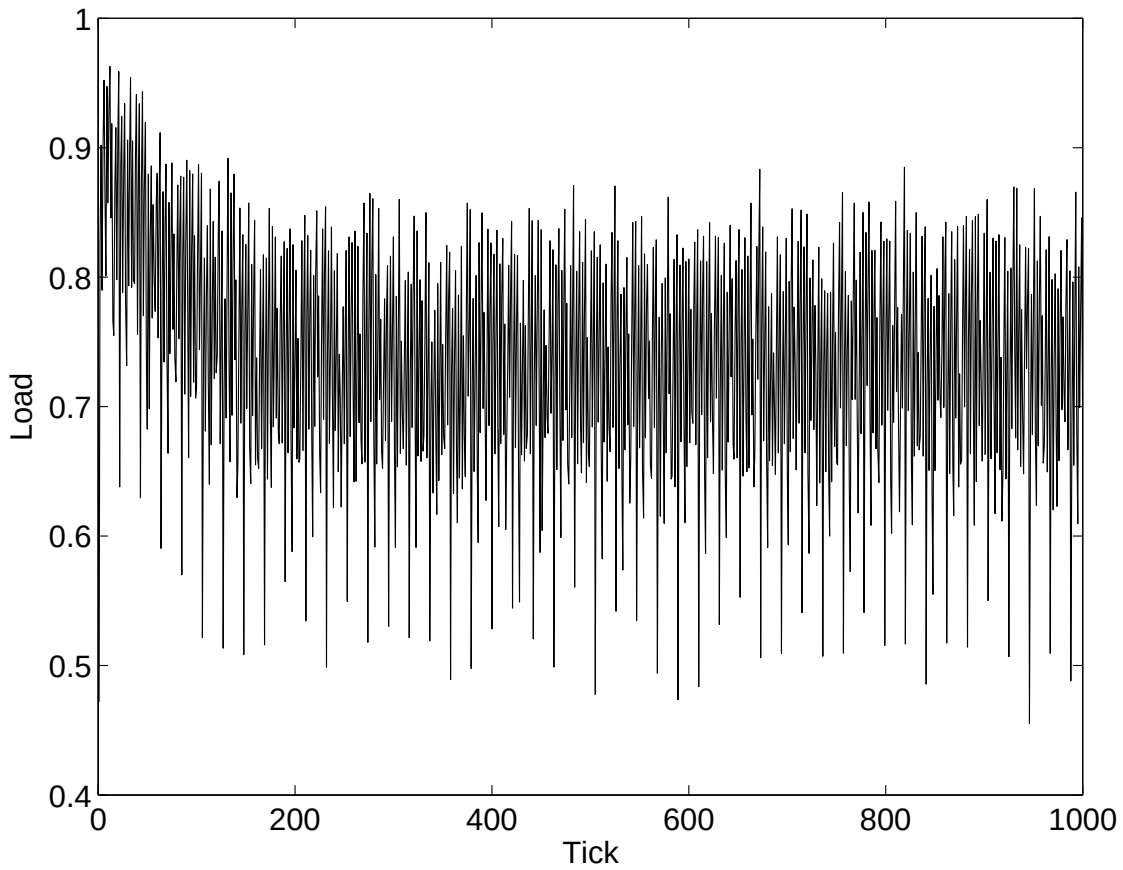
Research Motivation under Immediate Observability and Individual Sanction



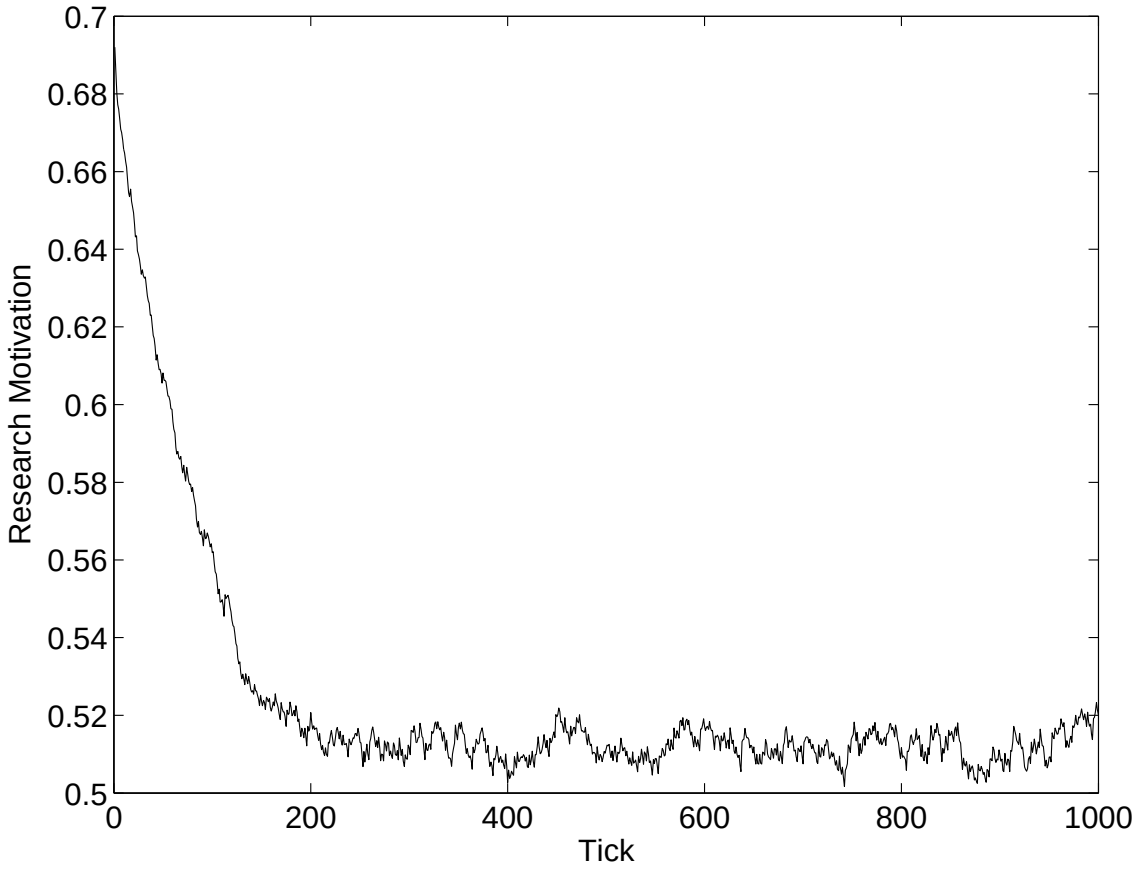
Security Compliance under Immediate Observability and Individual Sanction



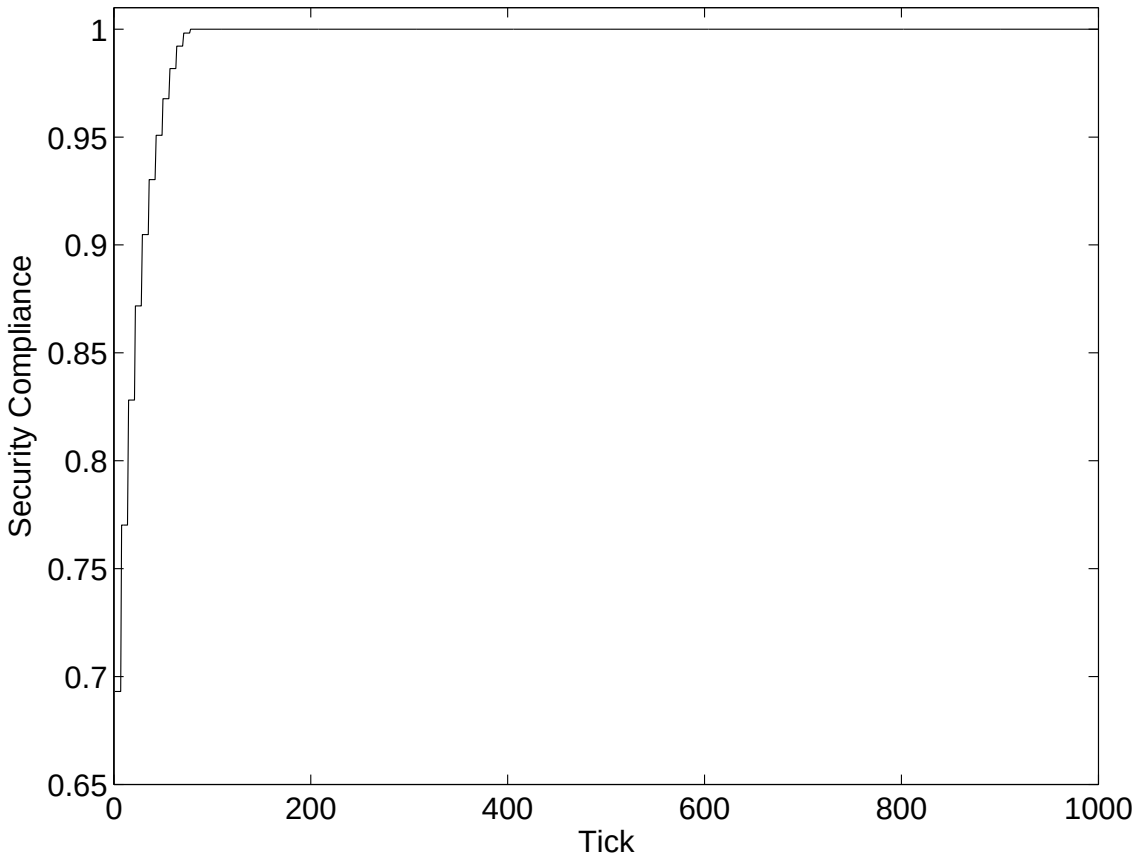
Load under Immediate Observability and Individual Sanction



Research Motivation under Immediate Observability and Group Sanction



Security Compliance under Immediate Observability and Group Sanction



Load under Immediate Observability and Group Sanction