Dissertation Type: research-type project

DEPARTMENT OF COMPUTER SCIENCE

Simulating Privacy Awareness in a Multiagent System

Lik Wong

A dissertation submitted to the University of Bristol in accordance with the requirements of the degree of Bachelor of Science in the Faculty of Engineering.

Thursday 20th May, 2021

Declaration

This dissertation is submitted to the University of Bristol in accordance with the requirements of the degree of BSc in the Faculty of Engineering. It has not been submitted for any other degree or diploma of any examining body. Except where specifically acknowledged, it is all the work of the Author.

Lik Wong, Thursday 20$^{\text{th}}$ May, 2021

Contents

Abstract

In this paper, we aim to construct socially intelligent personal agents (SIPAs) through implementing the intuition of privacy. Our proposed method finds a balance between seeking out one owns self interest, and other's preferences. Given that our model is based upon the multi-armed bandit problem, we will employ the epsilon-decreasing algorithm for our SIPAs to learn the preferences of other stakeholders. To confirm our theories, a simulation of a photo-sharing social media is implemented with user data seeded from our survey. Comparing our SIPA model with other baseline models in various metrics, we conclude that our model, although showing signs of respecting privacy, is not optimal.

Chapter 1

Introduction

Agent-based systems or multi-agent systems (MASs) has gained much traction over the recent years. Compared to traditional centralised methods [42], its autonomous nature allows it to perform various tasks like at much greater speeds and efficiencies. Not only so, according to Parasumanna Gokulan and Srinivasan [21], the benefits of MASs also include (but not limited to) an increase of robustness and reliability due to the graceful degradation of agents when they fail, scalability and flexibility, re-usability and reduced costs. Furthermore, the possibilities are endless with MASs. Oprea [18] reported that it is applicable in numerous and distinct areas such as ambient intelligence, grid computing, resource management, education and bioinformatics just to name a few.

As the development of agents continue to grow and sophisticate, more and more systems with autonomous agents that act proactively are integrated into our daily lives. Hybrid social systems of humans and agents coexisting together have become increasingly common [34]. Thus, demand for a more robust type of autonomy has also emerged. Enter *socially intelligent personal agents* (SIPAs), agents that not only demonstrate some aspect of human-style social intelligence [6, 7], but more specifically, are able to identify and look out for its primary and other stakeholders [3, 1, 2].

However, how do we define *human-style social intelligence*? Persson et al. [22] argued that instead of modelling what "real" intelligence is, we should, by using folk-theory as a basis, rather focus on what users think social intelligence is. Adapting this constructivist approach, we propose implementing the idea of privacy to SIPAs.

As a motivating example, social medias or social networking services (SNSs) have undeniably become a part of our everyday lives. In fact, over the majority of the population of the world are actively using SNSs [13]. Posting and sharing photos within a social media has become an ingrained action for many users, to the extent where just on Facebook alone there are more than 300 million photos posted daily [33]. However, with that many photos being shared, how many of these users know exactly what they are posting online? More accurately, how many of them know what type of information is being shown to everyone when a photo is shared and what are the privacy implications of it?

To define the terms of privacy, more often than not, when the word *privacy* is used online, people tend to allude the term to their personal information being seen, intercepted or sold to unwanted parties as coined by Solove [31]. Nonetheless, in the case with sharing photos online, even if no malicious party gets to see it, there is still a plethora of information that users may disclose unwittingly to their social circle. For example, when Ben posts a photo of him and his friends getting lunch, information such as his current location, time of event and companions are all shared publicly. We, therefore, adopt the 7 types of privacy defined by Friedewald et al. [9] to categorise these information captured in a photo. To concretely describe the previous scenario, by posting that photo to the public, Ben exposes his privacy of *behaviour and action*, *location and space*, and *association* to everyone. This may seem trivial at first glance, however, not everyone has the privacy awareness to notice these implications when posting photos or they simply do not care enough about their privacy. Moreover, when a photo with multiple individuals is posted, privacy of the whole group is also compromised indirectly. There's no guarantee that every person in a photo is content with information about them being shared when their companions post a photo. In particular, when Ben shares that photo of him having lunch with Alice publicly, Alice might not be happy as she is more privacy conscious and she opted for not posting that photo. Furthermore, once a photo is posted on a SNS, there is no method for someone other than the person who uploaded the photo to remove that photo. Figure 1.1 illustrates this scenario.

In reality, there are many methods to rectify this predicament, Alice could simply ask Ben to not

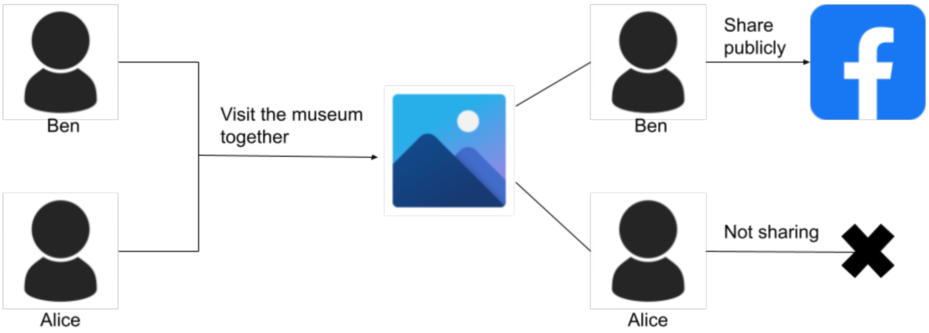

Figure 1.1: Example scenario

share that photo before he posts it. Alternatively, if Ben has had similar previous encounters with Alice, he would have learned Alice's attitude towards privacy based on her reaction after a photo is posted and change his action accordingly. Although this is may seem trivial for us humans, it is not the case for agents.

Research Questions

Consequently, our research questions: (1.) how can we construct SIPAs that can demonstrate privacy-awareness? More specifically, (2.) how do we teach them to look out for other stakeholder's interest? Additionally, (3.) how do we seek a balance between individual and other's interests in a way such that we still provide a pleasant social experience for everyone?

To concretely define *privacy-awareness* for our scenario, a SIPA have to be aware of what their user is posting online and the possible consequences that come from it to not only the primary user, but to other parties as well.

Contributions

Thus we propose a SIPA model that initially learns the preferences of other users by keeping track of past interactions, then by adjusting their future actions accordingly, it maximises the experience of everyone. Furthermore, to evaluate the effectiveness of our model, a MAS simulation of a simple social media solely for photo-sharing is also implemented, where we compare our model with other baseline models.

Novelty

Our approach is novel in that other work related to privacy, or in a more general case, ethics in AI is dominated by the individual decision making process, where the *trolley problem* often gets the spotlight [14]. Whereas our approach focuses on society as a whole, specifically, how actions by an individual contribute to the well-being of a collective group.

Organization

The structure of the paper is as follows: chapter 2 describes the methodology to simulate the idea of privacy and learning process in SIPAs, chapter 3 goes over the implementation of the simulation in detail, chapter 4 presents the results of our method through the simulation by comparing it with two other baseline models in various metrics, and finally, chapter 5 discusses threat of validity and concludes with future direction.

Chapter 2

Proposed Method

We utilise a *value sensitive design* approach of Friedman et al. [10] as a basis for our model. Where each "value" represents how important a person views something, this can include anything such as music, sports, food, a loved one or anything in between. Additionally, according to Dechesne et al. [8], different people have different preferences to these values. In the case for SIPAs, values provide a simple and direct way of expressing a user's preferences which could be modelled to maximise [32].

Before we can discuss the decision making process of our SIPAs, we must first define the rules of how agents communicate.

2.1 Norms

Agents in a MAS typically communicate with each other using Singh's [29, 30] concept of *norms*. Analogous to norms in real life, they govern what is acceptable or expected from members of a society. A norm can be formally defined as a tuple of four values:

$$\mathrm{N}(\mathit{Subject}, \mathit{Object}, \mathit{Antecedent}, \mathit{Consequent})$$

Where it involves a relationship or rule that is directed from the subject to the object, also an antecedent (conditions which the norm comes into force), and a consequent (whether the norm is satisfied or violated). This approach provides a clear and concise method of representing the nature and accountability of an action. Adapting norms as the grounding method of communication for our SIPAs, we employ three main types of norms similar to the Arnor model of Ajmeri et al. [3]: *commitment*, *prohibition* and *sanction*. Moreover, we draw a similar approach to the work of Ajmeri et al. [2] and Kayal et al. [12], combining the concepts of values and norms together, we can have norms that are centered around values of a SIPA's user.

A commitment is when a subject is committed to an object to bring about the consequent if the antecedent is true. An instance of a commitment would be if a friend of Bob is hanging out with Bob, they may be committed to publicly share a photo of them together. This can be represented as: $\mathrm{C}(\mathit{Friend}, \mathit{Bob}, \mathit{location} = \mathit{same}, \mathit{action} = \mathit{public})$.

Next, a prohibition means a subjected is prohibited by the object from performing the consequent if the antecedent holds. Returning to a previous example, when Alice and Bob was having lunch together, Bob was prohibited from sharing the photo of their lunch. Using the norm structure:
$\mathrm{P}(\mathit{Bob}, \mathit{Alice}, \mathit{location} = \mathit{lunch}, \mathit{action} = \mathit{public} \vee \mathit{friends})$.

Finally, a sanction acts as the response or consequence of another norm being satisfied or violated. According to Nardin et al. [16], a response from the object to the subject can range from negative, neutral to positive. Again, using the last example, if Bob ignored the prohibition and posted a photo of them publicly, Alice reacts by being unhappy. This can be represented as:
$\mathrm{S}(\mathit{Bob}, \mathit{Alice}, \mathit{action} = \mathit{public}, \mathit{action} = \mathit{unhappy})$.

Although there are two more types of norms mentioned by Singh, namely *authorisation* and *power*, we will not be covering them as the concept of authority is beyond the scope of what we are trying to achieve with our model. Note that norm compliance is not mandatory in our model, a SIPA should learn of the norms through positive/negative sanctions. However, Ajmeri et al. [1] suggested that it is up to SIPAs to robustly reason when to conform or violate norms in particular settings.

2.2 Learning

Referring back to our research question, in order to tackle the problem of SIPAs looking out for other stakeholder's interests, given the values of its user, SIPAs will have to make decisions that may conflict with the norms imposed by other users while attempting to maximise the experience of its own user. In which case, SIPAs should choose their actions based on the satisfaction of experience of its user and other stakeholders. To illustrate, a SIPA should choose selfish actions that solely aim to benefit its user when he or she is having a poor experience. Furthermore, in the other case where a user is having a pleasant experience, its SIPA should look to improve the experience of other users.

Nonetheless, how does a SIPA know *how* to improve the experience of other users? It must first learn the norms of other stakeholders through positive or negative sanctions that comes from complying or violating commitments. Ajmeri et al. [1] presented the Poros model where SIPAs kept a history of past interactions with others, doing so allowed its SIPAs to track norms that may be previously unknown to them and any respective sanctions that they receive. We adopt a similar approach in our model in which each SIPA has their own history, however, we differ from Poros with the method of learning.

One perspective is to view this model as a *multi-armed bandit problem* [11, 4] from reinforcement learning. As the name suggests, given you are presented with multiple slot machines in a casino and a limited amount of money, you want to maximise your winnings (reward). However, you are uncertain which machine to play as you are sceptical of each machine having a different probability of winning. Thus, to find out this probability you would play each a machine a certain number of times (*explore*) before reaching the conclusion of playing the machine with the highest rate of winning (*exploit*). How is this applicable to our model? To elaborate, an agent is placed into an environment where given a possible set of actions, has to choose one that maximises reward. Nevertheless, the caveat of this problem lies in the uncertainty of the outcome of each action. An agent has to learn through trial and error (*explore*), to discover which action yields the most reward (*exploit*). Applying this to our model, our SIPAs learn the commitments and prohibitions through testing all possible actions in different scenarios with different SIPAs. Additionally, by having sanctions as the reward of a multi-armed bandit problem, we can have SIPAs electing for actions that yields the highest positive sanction after the exploration phase. In other words, our SIPAs will choose actions that complies with norms of other stakeholders after figuring out said norms.

Having our model based as a multi-armed bandit problem, we adopt ϵ-greedy algorithm [35] as a method to outline the process as described above. Pseudo-code for this algorithm is summarised in Algorithm 2.1. The best current action is the one with the highest corresponding reward estimate. Estimates of the reward gained for each action a before time t, is determined by an action-value estimate, $Q_t(a)$, where it is the mean reward received (R is the reward for selecting action a at a specific time step, and $N(t)_a$ is the number of times the action was selected) for selecting action a as shown in Equation 2.1 [28]. To increase the efficiency of the model, instead of leaving the exploration phase of the algorithm spread out across the number of time-steps with a fixed ϵ, we make a slight altercation to another version of the algorithm: ϵ-decreasing [4]. This version starts with a high ϵ value to ensure all agents explore their actions initially. Afterwards, as time passes, this probability drops exponentially, resulting in agents exploiting the best actions only.

$$Q_t(a) = \frac{R_1 + R_2 + ... + R_{N(t)_a}}{N(t)_a} \tag{2.1}$$

```
Parameters: ε, a fixed probability, t, number of steps
i = 0
while i < t do
    p = random(0, 1)
    if p < ε then
        pick random action a
    else
        pick a with highest action-value estimate
    end
    i = i + 1
end
```

Algorithm 2.1: ϵ-Greedy Algorithm

2.3 Decision Making

Cointe et al. [5] argued that a SIPA should be able to evaluate norms, context and values of its user to decide upon an action that balances all of them. Furthermore, SIPAs should demonstrate traits of *prioritarianism* [23], meaning extra care and attention should be given to the worse-off individuals. This line of thought provides a *just* society defined by Rawls [25] where there is a relatively low difference between the best-case and worst-case scenario. Ajmeri et al. [2] presented the Elessar model where this difference is considered as a significant metric over norm compliance due to how it represents how just a system is. Now that we have covered the all the components to our model, we will summarise and provide a detailed description of the decision making process of the model. In Figure 2.1, we present a conceptual model for *social experience*.

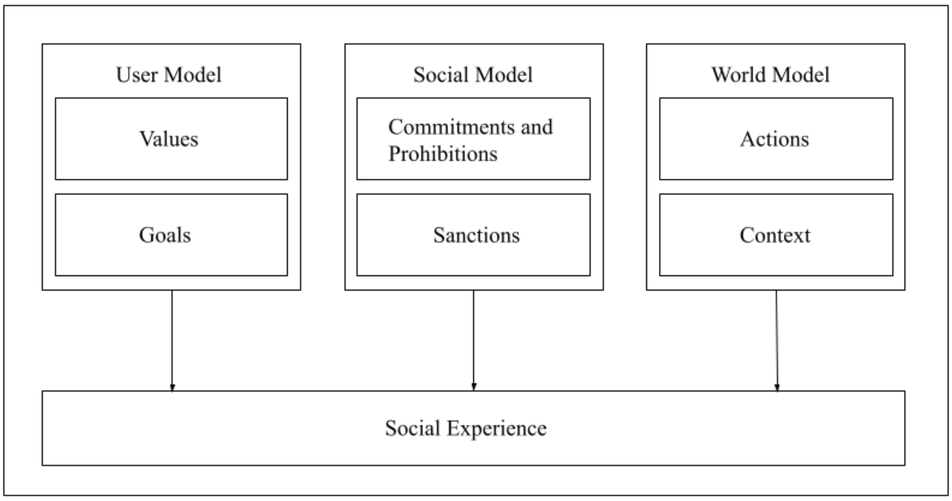

Figure 2.1: Social Experience Conceptual Model inspired by Ajmeri et al. [2, 1, 3]

Social experience, as the primary objective SIPAs should maximise, are made up of multiple factors from different models. At every time step, a SIPA has one or more stakeholders. Users in the model, acting as the main stakeholder a SIPA considers, have *goals* that are motivated by their *values*. To bring about said goals, an *action* is chosen by his/her SIPA while taking other factors in the *social* and *world* model like *context* and *norms* into consideration. Factors of the world model, are the environment in which a SIPA is located (context), and the given set of possible actions to select from where both context and action promotes/demotes certain user values. Moreover, in the social model, a SIPA generate norms to motivate other SIPAs to comply with the user's preferences. SIPAs then records the norms of other stakeholders, *commitments* and *prohibitions*, and any resulting *sanctions* from satisfying or violating them. An aggregation of all of these factors constructs the social experience of a user [32], where this value will be visible to all SIPAs as a metric of how *happy* a user is.

As covered in the previous section, our SIPAs initially explores different actions with different stakeholders to learn their norms before exploiting the most rewarding action using ϵ-decreasing algorithm. Reflecting how in the real world, you have to try different actions to probe a reaction from the other party. When you find out which action nets the most consistent positive reaction, you tend to stick to that action afterwards. However, after the explore phase, SIPAs are not required to select the most rewarding action in terms of complying with norms, it is merely an additional option to select depending on context and the social experience of its other stakeholders. For example, if there are no stakeholders other than the primary user, a SIPA should always select the action that rewards the user's values and goals without regarding anything learnt from the explore phase. Following Rawls' principles, in each interaction, SIPAs will check and rank the happiness of all users, including its own, that are involved. Based on this result, if the primary user of the SIPA is not having a satisfactory experience, the SIPA should elect for picking a selfish action that only considers his/her values and context. On the contrary, SIPAs should look out for other users' experience by opting for an action that complies with the norms of the unhappy individuals, even if it means the SIPA's own user suffers a lower happiness. Nonetheless, picking an alternative action that results in increasing the happiness of other users at the cost of another should not result in a huge disparity of happiness. SIPAs have to reason whether or not choosing an alternative action where the increase of collective social experience will outweigh the cost of their own user's experience (*regret* in reinforcement learning). A simple flowchart of this decision making process at every time step is shown in Figure 2.2.

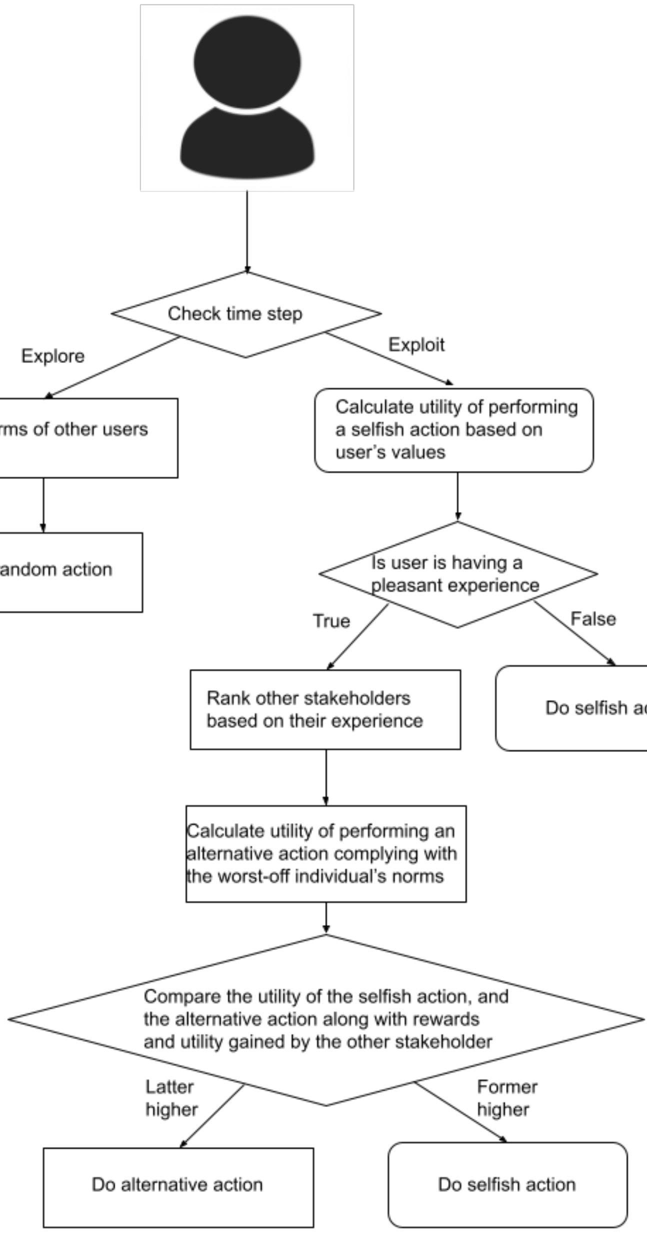

Figure 2.2: Decision Flowchart

Chapter 3

Simulation Design

To simulate a photo-sharing social media MAS with simulated users and their own SIPA from our model, we use Mesa [36], a Python framework for building, analysing and visualising agent-based models.

3.1 Survey

In order to keep the simulation as close to real life as possible and to preserve robustness, a survey for finding out privacy attitudes was conducted. The survey is split into two parts, the first determines the demographic and behaviors on social media of the respondent. The second part presents a number of hypothetical scenarios to the respondent, where they have to decide whether or not they want to post a photo of that scenario publicly, to only friends or not post at all. Using this information, we can deduce the personality type and privacy-awareness level of a respondent. Additionally, the responses from the second part of the survey acts as the grounding values a scenario promotes/demotes in the simulation. A total of 22 responses were recorded where 94.5% of them are between the age of 18 and 34, with a gender split of 15 male to 6 female (one respondent prefer not to disclose their gender). The findings of our survey will be presented in the next section where we define the setup of the simulation.

3.2 Simulation Setup

Given that our SIPAs are guiding users of a social media, they have to possess certain attributes or values that mirror us humans when making judgements with uploading photos. Applicable values include: pleasure, recognition, privacy and security. Our first two values derives from Oeldorf-Hirsch and Sundar's [17] factors of motivation for online photo sharing, people share their photos on social media based on a large number of reasons which could be summarised into these 4 factors. The first value, pleasure, reflects the first and third factor, *Seeking and Showcasing Experiences* and *Social Connection* where individuals have a need to share and keep up with those around them, be it family or friends, for the sake of building and maintaining these relationships. Additionally, the second value, recognition, refers to factor 4, *Reaching Out*. Although at first glance, this factor is similar to the previous two, the focus is on having a person's photo reach a wider audience beyond their social circle. Privacy represents how conscious a person is to their information being shown online. For instance, if a person has a high privacy value, they will be less willing to share their photo's online. Finally, security refers to the degree of awareness a person has to sharing sensitive information that might carry a security risk. Each user has a value from 0 (not caring at all) to 1 (very important) for each value that makes up their personality.

Although theoretically, a photo can convey any and all of the 7 types of privacy. In our scenario, however, we will only be tackling privacy of *behaviour and action*, *location and space*, and *association* as most photos being shared on social media tend to be in this category. For instance, it is more common to see photos of your friends going to the beach together rather than them taking pictures of that expose their personal information such as their birth certificate (*privacy of person*).

From our survey, following the results of Ajmeri et al. [2], we are able to identify the personality types of the respondents and categorise them into three groups based on their privacy attitude: *cautious*, *conscientious* and *casual*. Where cautious individuals are uncomfortable and unwilling to share their personal information online. Conscientious users although being comfortable with posting some of their information, still shows consideration on each individual case with the type of information being shown.

And finally casual users who are unconcerned with the idea of privacy. The values of these users are presented in Table 3.1. Further, adopting the same distribution of the type of users in the survey from the question in Figure 3.1, we use 45.5% (never) cautious, 36.3% (once a month and once a week) conscientious and 18.2% (few times a week and daily) casual as our population.

Privacy Attitude	Pleasure	Recognition	Privacy	Security
Cautious	0.1	0.2	1	0.7
Conscientious	0.4	0.6	0.5	0.6
Casual	1	0.7	0	0.3

Table 3.1: Privacy Attitude Values

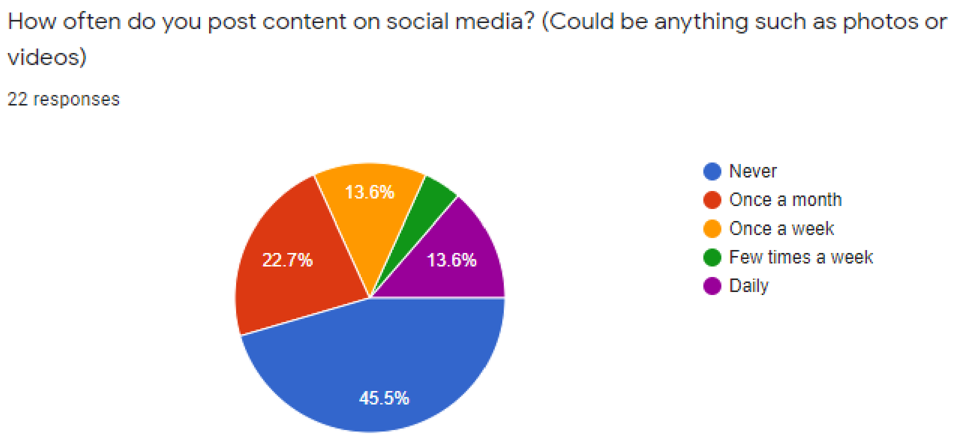

Figure 3.1: Question and Responses for Obtaining Population

In this MAS simulation, users move around places (serving as the context), virtual scenarios that users visit either alone or with companions, and take photo of their current situation. Afterwards, their SIPA decides whether it should share that photo with the general public, friends or no-one (actions). Moreover, for the sake of simplicity, a single action is performed by each agent on a daily basis (measure of time in the simulation).

Places	Pleasure	Recognition	Privacy	Security
Going to the beach	2	2	-1	-1
Visiting a museum	1.5	1.5	0	0
Meeting in a company	0	-1	1.5	1.5
Family member undergoing surgery	-2	-2	2	1.5
Failing an exam	-1	0	1	1
Winning a competition	2	2	-2	-2
Attending a funeral	-2	-1	1.5	2
Surfing in a typhoon	-1.5	0	1	2
Getting a speed Ticket	-1	-2	1.5	2

Table 3.2: Values Promoted for Each Place

Share with	Pleasure	Recognition	Privacy	Security
No-one	0	0	2	2
Friends	2	1	0.5	1
Public	1	2	0	0

Table 3.3: Values Promoted for Each Action

However, values are not only limited to users, every place and action promotes different values. Tables 3.2 and 3.3 illustrates the values promoted for each place and action. Note that value for places range from -2 to 2 and value for actions range from 0 to 2. The values specified in Table 3.2 utilises the mean answers from the second part of the survey where the same scenarios were presented to users. The scenarios or places are designed to cover a range of situations that prompt a different reaction for each user. For instance, pleasant experiences such as going to the beach or visiting a museum should invoke users to share their context. Whereas private or sensitive matters such as attending a funeral or meeting in a company creates an uncomfortable situation for users to share.

An agent evaluates the best individual action (selfish) to take by computing the social experience value, or happiness value, for each action. Firstly, we multiply the user's own values, the place's promote/demote value and the action's promote/demote value together. We then proceed by summing all the values up, so that all values are taken into account. Maximising this happiness is the goal of users. As shown by the Equation 3.1 below:

$$\begin{aligned} selfishHappiness =& (agentPleasure \times placePleasure \times actionPleasure) + \\ & (agentRecognition \times placeRecognition \times actionRecognition) + \\ & (agentPrivacy \times placePrivacy \times actionPrivacy) + \\ & (agentSecurity \times placeSecurity \times actionSecurity) \end{aligned} \tag{3.1}$$

If a SIPA has elected for being selfish, it makes the decision by performing the action with the highest selfish happiness value. Table 3.4 shows an example of how everything is calculated when an agent goes to the beach alone. As we can see in this instance, this particular agent will choose sharing their photo publicly as their action.

User & Place					Action					
	Pleasure	Recognition	Privacy	Security		Pleasure	Recognition	Privacy	Security	Happiness
User	0.4	0.8	0.7	0.1	No-one	0	0	-1.4	-0.2	-1.6
Place	2	2	-1	-1	Friends	1.6	1.6	-0.35	-0.1	2.75
Result	**0.8**	**1.6**	**-0.7**	**-0.1**	**Public**	0.8	3.2	0	0	**4**

Table 3.4: Example Day: Going to the Beach Alone

3.3 Social Network

Every social media has some form of social network for its users, for example, in Facebook you add others as your friend and in Instagram has a follower/following system. We will be utilising a friends list system similar to Facebook's for its ease of implementation. In order to construct a robust and random social network (friends in social media), we will use the Watts-Strogatz Model [40], a model for randomly generating undirected *Small World Graphs*. Graphs of this nature possess numerous properties that mirror social networks, one of which being small world graphs have *six degrees of separation*, meaning that on average, every person is 6 or fewer social connections away from each other. As a matter of fact, previous work such as by Wohlgemuth and Matache [41] has modelled networks of individual users of Facebook as small world graphs.

The Watts-Strogatz model has three parameters: number of nodes, number of connections per node and randomness. Shown in Figure 3.2 are examples of small world graphs with increasing randomness. In our case, a friend list is constructed as a small world graph with each node representing a user, and each connection to another node represents that they are friends. For experimental purposes, we can alter all three of these parameters to see how it affects our simulation.

3.4 Social Model

The next step, with components of user (values and goals) and world (context and action) model implemented, we continue on to the social model of commitments, prohibitions and sanctions.

Whenever a user visits a place with another user that is in their friend list, they become *companions* (other stakeholders). For the sake of simplicity, whenever a SIPA decides to perform an action, that SIPA receives a positive sanction if another SIPA chose the same action. This acts as a simple method of rewarding SIPAs for complying with the norms of other SIPAs. Conversely, this also works for negative

Figure 3.2: Example of Small World Graphs [40]

sanctions when a SIPA selects a different action from another SIPA (violating commitments). Equation 3.2 illustrates the total *rewards* a SIPA receives for performing an action, where c is the number of companions and s represents sanction from a companion. Rewards contribute directly to the social experience, or $S(A)$ of a SIPA. This is expressed in Equation 3.3, serving as the primary value of utility SIPAs should maximise.

$$Rewards = \sum_{i=0}^{c} s_i \tag{3.2}$$

$$S(A) = selfishHappiness + Rewards \tag{3.3}$$

Although maximising social experience is the main objective for SIPAs, they should also follow Rawls' [25] principle of fairness. More specifically, SIPAs should select an alternative action that complies with the norms of users that are suffering in terms of social experience if they can afford to do so. For instance, in an interaction with Ben and Alice, Ben initially decides to share a photo of them publicly as it suits his values of pleasure and recognition. However, by doing so, it leaves Alice with a low happiness even if she elects for not sharing that photo as Ben has violated his commitment to her. Ben's SIPA notices Alice's unhappiness and will suggest an alternative action that complies with Alice's norms if the utility of the alternative action and the social experience of Alice gained is greater than the lost of Ben's. This process, Rawls Check, is expressed in Algorithm 3.1. Conforming to his definition of a fair society, we attempt to improve the experience of worse-off users, in our case, users that are suffering a social experience below average. By using this approach, we seek to achieve a high mean social experience while improving the minimum utility.

Parameters: $S(A_1(a_{self}))$, primary user social experience of initial selfish action,
$S(A_1(a_\epsilon))$, primary user social experience of alternative action,
$S(A_2)$, companion social experience,
$S_+(A_2)$, the increase of companion social experience for selecting alternative action

threshold = average social experience of all users
if $S(A_2) < threshold$ **then**
  if $S(A_1(a_\epsilon)) + S_+(A_2) > S(A_1(a_{self}))$ **then**
    do a_ϵ
  else
    do a_{self}
  end
else
  do a_{self}
end

Algorithm 3.1: Rawls Check

Chapter 4

Results and Evaluation

In order to evaluate the effectiveness of our model in terms of our research question, we will conduct a few experiments on the simulation we implemented. We will first present the setting of the experiments, then proceed to the results. Due to the similarities in the implemented model, we will adopt a evaluation method close to Ajmeri et al. [2].

4.1 Model Comparison

If we are to test our proposed SIPA model fairly, we will require other baseline decision making models for comparison. Namely: *random*, *selfish* and *majority*.

- Random. Agents in this model will randomly pick actions, regardless of values, context or norms.
- Selfish agents solely seek to maximise their primary user's values and goals based on context.
- Majority. In each interaction, these agents and their companions vote for which action they wish to do. The action with the majority of votes will chosen as the action everyone in the group shall do. In other words, norm compliance is forced upon all members of the group, disregarding the minority's values and goals. Ulusoy and Yolum's [39] decision making model utilises majority voting in the case of conflicting norms. Additionally, although used in a different scenario, Qiu and Phang [24] presented that majority voting as a strategy has been used commonly in political MAS decision making models.

Theoretically, our SIPA model should combines the positive elements of the selfish and majority model while reasoning when to adapt to improve the experience of other stakeholders.

4.2 Metrics

Measuring how effective our SIPAs are, we employ the following metrics. Note that these metrics are recorded at each time step.

- Average Social Experience. The mean social experience or happiness across all agents. The higher the better.
- Maximum Social Experience. The highest social experience an individual agent possesses in the simulation. The higher the better.
- Minimum Social Experience. The opposite of the previous metric, the lowest social experience an individual agent has in the simulation. The higher the better.
- Average Reward. The mean reward (sanctions) an agent receives from selecting norm-compliant actions. Although stated previously that norm complience does not provide a clear metric in terms of how fair a society is, it is still significant if agents are caring about sanctions at all. The higher the better.
- Below Average Social Experience. The number of agents in the simulation that has a social experience value lower than the average social experience. Mainly implemented for examining the effectiveness of our SIPA's Rawls Check. The lower the better.

4.3 Experiment Setup

We will be running a one-tailed paired t-test for each metric with all the decision making models (including our SIPA model). Our null hypotheses claims that our proposed SIPA model will not outperform the baseline models in every metric. On the contrary, our alternative hypotheses claim otherwise. As listed below:

Null hypotheses

- $H_{0(average)}$, our SIPA model does not outperform other models in average social experience.
- $H_{0(max)}$, our SIPA model does not outperform other models in maximum individual social experience.
- $H_{0(min)}$, our SIPA model does not outperform other models in minimum individual social experience.
- $H_{0(reward)}$, our SIPA model does not outperform other models in average reward.
- $H_{0(belowAverage)}$, our SIPA model does not outperform other models in number of below average social experience agents.

Alternative hypotheses

- $H_{1(average)}$, our SIPA model outperform other models in average social experience.
- $H_{1(max)}$, our SIPA model outperform other models in maximum individual social experience.
- $H_{1(min)}$, our SIPA model outperform other models in minimum individual social experience.
- $H_{1(reward)}$, our SIPA model outperform other models in average reward.
- $H_{1(belowAverage)}$, our SIPA model outperform other models in number of below average social experience agents.

Furthermore, our experiments have 20 (we are aware of this value being low, reason for this will be explained in a later section) agents per run with 200 time steps. Thus, settings for the Watts-Strogatz model are 20 nodes, 8 connections and 0.3 rewiring probability.

4.4 Experiment: Seeded Users

We conduct our first experiment using the proportion of privacy types of users specified in Section 3.2. With 45.5% cautious, 36.3% conscientious and 18.2% casual as the population, we ran our SIPA model along with other baseline models in the simulation five times and take the mean value of every metric at each time step to obtain an accurate result and eliminate randomness. Our findings are visualised through plotting the results of the simulation in a line graph, with each plot representing a metric to confirm our hypotheses. Figures 4.4, 4.2, 4.3, 4.4 and 4.5 below presents our plots.

Note that the explore phase of our SIPA model can be seen clearly throughout the plots. During this phase, our SIPAs chooses random actions to learn of their stakeholder's norms, therefore, the results are potentially worse than the random model. Initial observations on Figures 4.2 and 4.3 shows the explore phase of ϵ-decreasing algorithm rather distinctively. With maximum and minimum social experience even lower than the random model, it showcases our SIPAs testing out all their actions with stakeholders. After around the 50th time step, the probability of exploiting increases tremendously, therefore leading to the jump in certain results. As such, we will omit the first 50 time steps for all models in the t-tests to provide a clearer result. The t-tests done for comparing our SIPA model with other baseline models in $H_{average}$, H_{max}, H_{min}, H_{reward} and $H_{belowAverage}$ are shown in Table 4.1.

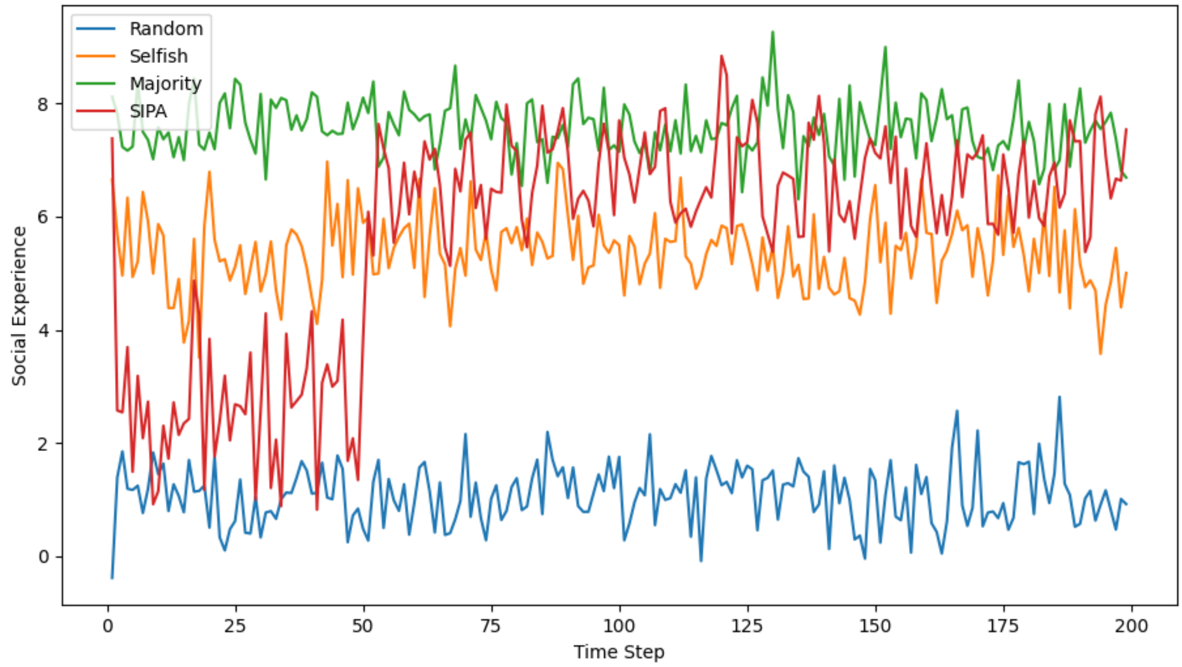

Figure 4.1: Average Social Experience of All Models

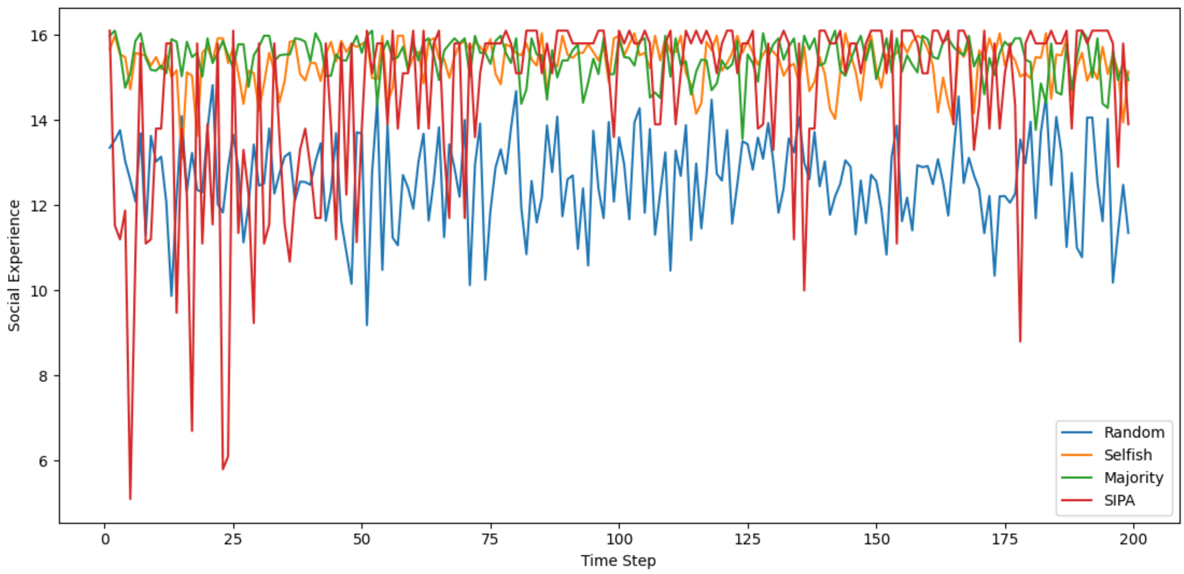

Figure 4.2: Maximum Social Experience of All Models

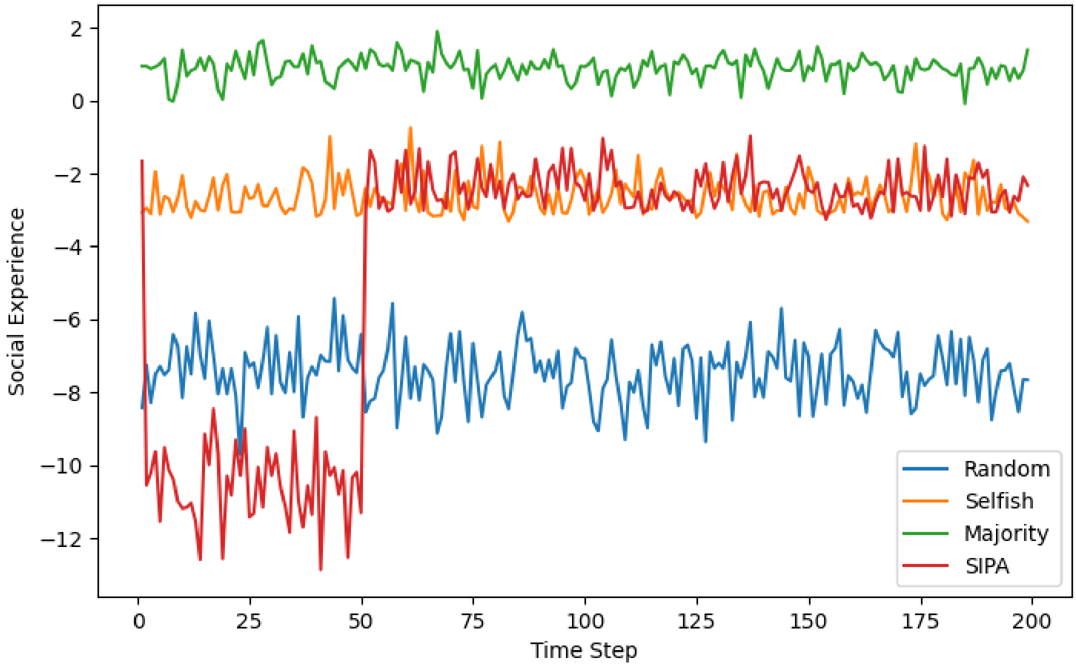

Figure 4.3: Minimum Social Experience of All Models

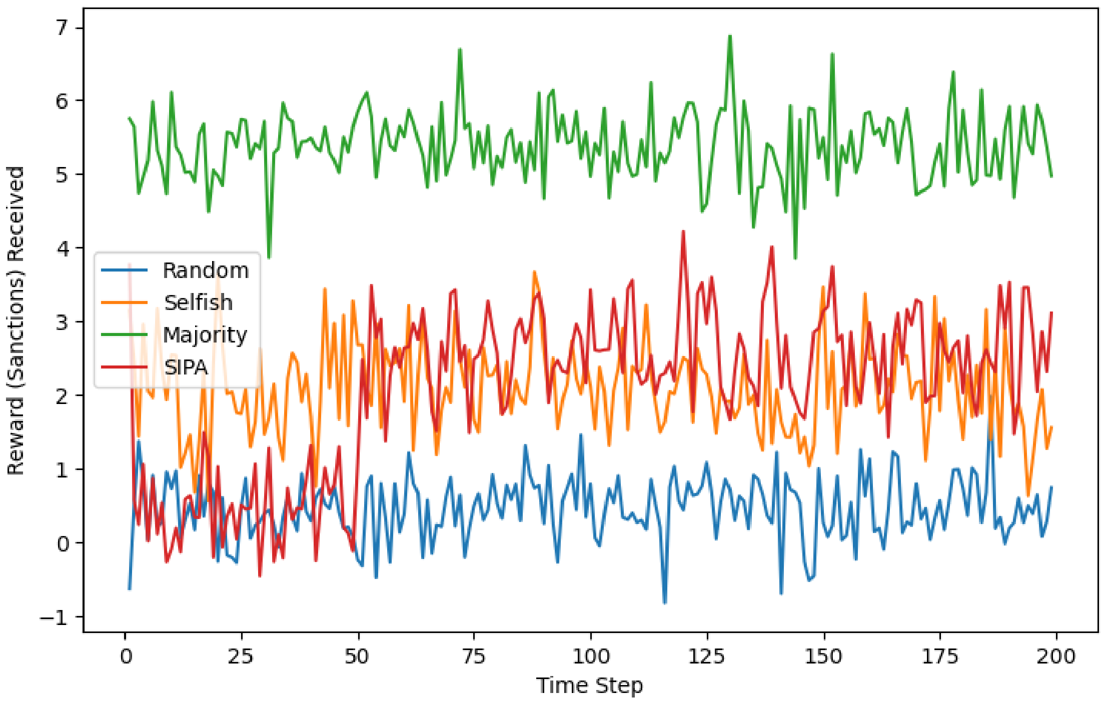

Figure 4.4: Average Reward (Sanction) of All Models

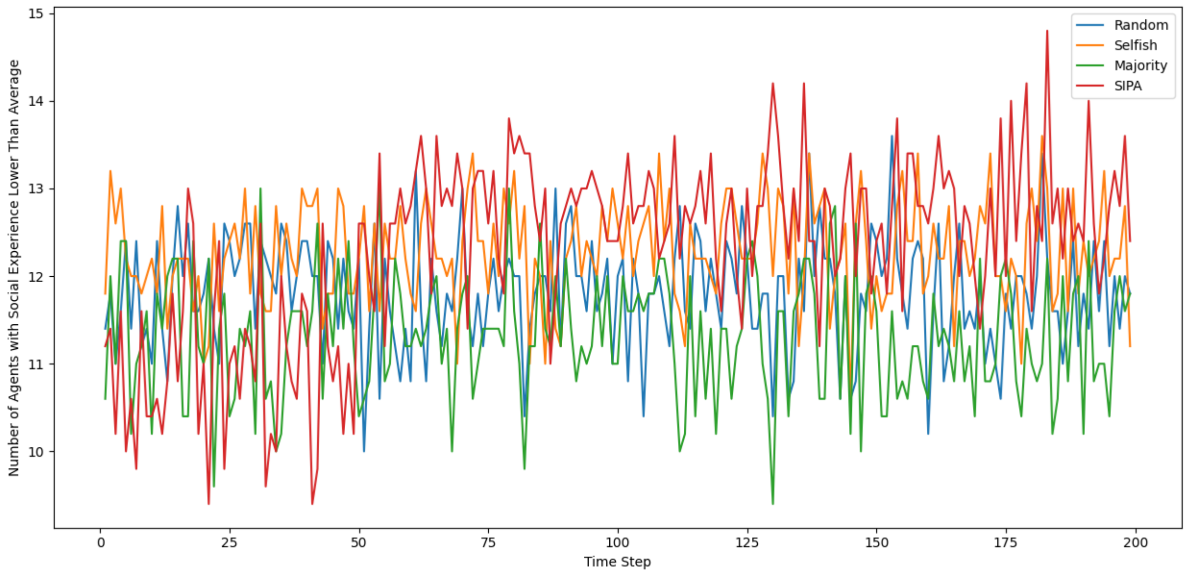

Figure 4.5: Number of Agents Below the Average Social Experience in All Models

Hypotheses	Random	Selfish	Majority
$H_{average}$	1.4×10^{-123}	7.0×10^{-39}	1
H_{max}	4.3×10^{-41}	0.83	0.86
H_{min}	3.1×10^{-112}	0.00049	1
H_{reward}	4.5×10^{-77}	2.3×10^{-14}	1
$H_{belowAverage}$	1	1	1

Table 4.1: p-value of Every T-test Performed on Our SIPA Model

As seen from our results, our SIPA model generally outperforms the random and selfish models but not the majority model. In Table 4.1, the p-value for every metric except H_{max} and $H_{belowAverage}$ for random and selfish models are smaller than 0.01. Nevertheless, our SIPA model did not outperform the majority model in any metrics, therefore, we fail to reject $H_{0(average)}$, $H_{0(max)}$, $H_{0(min)}$, $H_{0(reward)}$ and $H_{0(belowAverage)}$, and can not accept $H_{1(average)}$, $H_{1(max)}$, $H_{1(min)}$, $H_{1(reward)}$ and $H_{1(belowAverage)}$. Relating back to our research questions, even though the t-test indicated that our SIPA model has much room to improve, it still (1.) demonstrated privacy-awareness, (2.) looked out for other stakeholder's norms and (3.) achieved a satisfactory social experience for everyone when compared to the selfish model.

4.5 Evaluation

From the conducted experimented, it is fair to arrive at a conclusion that our SIPA model has a number of major flaws. Although it achieved certain goals as listed in our research question, it did not achieve them to the extent as expected. We shall investigate the reasons and factors that lead to this result in this section.

Firstly, our learning algorithm: ϵ-decreasing, is not greatly suitable for our model. Simply put, this algorithm takes too long to learn of other companion's norms effectively. To illustrate, in our experiment setup, we have 20 agents with 8 friends each. Learning the full scope of norms of each friend requires exploring all available actions in all locations (contexts). Without taking randomness into account, this takes 24 time-steps for each friend, and in our case, at least 192 time steps are needed. The time needed to explore in the algorithm scales exponentially with the number of friends each agent has. Moreover, additional variables such as actions and locations all contribute to the problem. As such, we adopted a low number of agents and number of friends to aid the run time of our SIPA model.

Second, our SIPA model performed the worst during the exploit phase in terms of one significant metric, below average social experience. This is especially surprising as our model employs a Rawls Check covered in Algorithm 3.1 to hope for the opposite result. However, it is likely due to the reasons discussed previously with ϵ-decreasing that led to this result. The fact that our SIPAs are not learning the norms of other stakeholders efficiently means that the alternative action that our Rawls Check motivates does not net the SIPA as much reward as it should. Thus, SIPAs enjoying a high social experience may not necessarily know the best alternative action that fulfills the commitments of its stakeholders, leading to them opting for their original selfish action as it is unlikely a sub-optimal alternative action will outweigh the selfish action.

To confirm these suspicions, further experimentation with different parameters are required. An example of this includes a run of the simulation with a larger time step for our SIPAs to explore. Although this may improve our SIPA model's results, the run time of the simulation will be much longer as well. Next, we can run our simulation with a different, fixed population instead of adopting the population of our survey respondents. For instance, a run with only casual users, or only cautious users may reveal more flaws of our simulation or SIPA model.

Chapter 5

Conclusion

To conclude this paper, we initially set out to create SIPAs that demonstrate privacy-awareness. Or more specifically, SIPAs that care about the social experience of its stakeholders, both primary and others. Through combining concepts and techniques such as norms, ϵ-decreasing algorithm and our proposed Rawls Check, we implemented a SIPA model that learns the norms of its stakeholders by trial-and-error, then uses this knowledge depending on context and experience of its companions. Via simulation with seeded values from our survey, we are able to evaluate our SIPA model with other baseline decision making models.

Although, the results are sub-par when compared with the majority model, to the extent where we fail to reject all of our null hypotheses, our SIPA model still holds value as it did achieve and answer our research questions relative to the selfish baseline model. To elaborate, our SIPAs outperformed the selfish model in almost every metric except maximum social experience with a p-value < 0.01, thus confirming our research questions. Moreover, we arrive at a conjecture that ϵ-decreasing algorithm as a learning process was not the most optimal choice for a decision making model. Perhaps modelling our problem as a multi-armed bandit problem to begin with was a mistake. Additional augmentations and experimentation, such as changing the explore-exploit algorithm or running the simulation with different population types, could have been made to our model, however, due to time constraints, they were not implemented.

5.1 Related Works

Ajmeri et al. [2] proposed the Elessar model, in which SIPAs aggregate values of users and selects ethical actions through VIKTOR, a multicritea decision making method [19]. Although we utilise a similar setup of agents in our model, we differ from Elessar in our decision making methods where we first learn of other stakeholder's norms. Another similar model: Kayal et al.'s [12] model predicts a user's preferences through values and norms, effectively solving norm conflicts automatically.

Tzeng et al. [37] proposed a psychology approach that involves modelling emotions as a result of complying or violating norms, which leads to a higher rate of norm compliance and social experience. Scheve et al. [26] takes a step further and generates emotions for both subject and object in a norm, such as when the object violates a norm, the subject reacts with a strong negative emotion, which then results in another strong negative emotion being invoked on object. Our model does not explicitly employ emotion, however, it is on a simplified and abstract level where it is represented by values.

Ulusoy and Yolum [39] presents their privacy model in a normative approach, where norms are generated based on previous decisions. Plus, conflict in norms are settled using a majority voting decision making model. Ulusoy and Yolum [38] also has another privacy model: PANO, where an auction is held whenever an imagine is shared. This auction allows agents to bid on how private an image is on behalf of a user. While privacy is a major talking point, there are multiple ways to interpret it. We adopt a simplified idea of privacy where we only consider the three types of privacy stated in Section 3.2.

5.2 Future Directions

Given the nature of our project, there are numerous directions to expand our model and simulation. The most obvious one is changing the learning algorithm (ϵ-decreasing) and problem model (multi-armed bandit problem) to improve results. One possibility is to model our problem as a *associative search task* or contextual bandits [35]. This problem model is more suitable as it combines the process of a multi-armed bandit problem with one extra element, an *association* describing the situations which action is best performed. From this abstract understanding, one can assume context as association, therefore, potentially decreasing the learning time needed for its algorithms.

Moreover, the survey conducted could follow the findings of Naeini et al. [15] and questions of Schnorf et al. [27] to more accurately represent user's values and preferences

Another interesting outlook is how the simulation is setup. To offer a more realistic and robust simulation, we could implement (1.) additional features of a social media such as "liking" photos, (2.) elicit non-simplified emotional reactions of users from seeing photos or (3.) a communication protocol where agents reason with one another about their context and norms instead of solely increasing/decreasing social experience. Taking a huge shift in direction, one could also combine image process as a topic into our model and make agents evaluate the privacy implications of real photos as seen in Orekondy et al.'s [20] work.

Bibliography

[1] Nirav Ajmeri, Hui Guo, Pradeep K. Murukannaiah, and Munindar P. Singh. 2018. Robust Norm Emergence by Revealing and Reasoning about Context: Socially Intelligent Agents for Enhancing Privacy. In *Proceedings of the 27th International Joint Conference on Artificial Intelligence (IJCAI)*. IJCAI, Stockholm, 28–34.

[2] Nirav Ajmeri, Hui Guo, Pradeep K. Murukannaiah, and Munindar P. Singh. 2020. Elessar: Ethics in Norm-Aware Agents. In *Proceedings of the 19th International Conference on Autonomous Agents and Multiagent Systems (AAMAS)*. IFAAMAS, Auckland, 16–24.

[3] Nirav Ajmeri, Pradeep K. Murukannaiah, Hui Guo, and Munindar P. Singh. 2017. Arnor: Modeling Social Intelligence via Norms to Engineer Privacy-Aware Personal Agents. In *Proceedings of the 16th International Conference on Autonomous Agents and Multiagent Systems (AAMAS)*. IFAAMAS, São Paulo, 230–238.

[4] Peter Auer, Nicolò Cesa-Bianchi, and Paul Fischer. 2002. Finite-time Analysis of the Multiarmed Bandit Problem. *Machine Learning* 47 (05 2002), 235–256. https://doi.org/10.1023/A:1013689704352

[5] Nicolas Cointe, Grégory Bonnet, and Olivier Boissier. 2016. Ethical Judgment of Agents' Behaviors in Multi-Agent Systems. In *Proceedings of the 2016 International Conference on Autonomous Agents and Multiagent Systems*. IFAAMAS, Singapore, 1106–1114.

[6] Kerstin Dautenhahn. 1998. THE ART OF DESIGNING SOCIALLY INTELLIGENT AGENTS: SCIENCE, FICTION, AND THE HUMAN IN THE LOOP. *Applied Artificial Intelligence* 12, 7-8 (1998), 573–617. https://doi.org/10.1080/088395198117550 arXiv:https://doi.org/10.1080/088395198117550

[7] Kerstin Dautenhahn. 2001. Editorial - Socially Intelligent Agents - the Human in the Loop. *Trans. Sys. Man Cyber. Part A* 31, 5 (Sept. 2001), 345–348. https://doi.org/10.1109/TSMCA.2001.952709

[8] Francien Dechesne, Gennaro Di Tosto, Virginia Dignum, and Frank Dignum. 2013. No Smoking Here: Values, Norms and Culture in Multi-Agent Systems. *Artificial Intelligence and Law* 21, 1 (01 Mar 2013), 79–107.

[9] Michael Friedewald, Rachel Finn, and David Wright. 2013. *Seven Types of Privacy*. Springer, Netherlands, 3–32. https://doi.org/10.1007/978-94-

[10] Batya Friedman, Peter H. Kahn Jr., and Alan Borning. 2008. Value Sensitive Design and Information Systems. In *The Handbook of Information and Computer Ethics*, Kenneth Einar Himma and Herman T. Tavani (Eds.). John Wiley & Sons, Hoboken, New Jersey, Chapter 4, 69–101.

[11] Michael Katehakis and Veinott Jr. 1987. The Multi- Armed Bandit Problem: Decomposition and Computation. *Math. Oper. Res.* 12 (05 1987), 262–268. https://doi.org/10.1287/moor.12.2.262

[12] Alex Kayal, Willem-Paul Brinkman, Mark A. Neerincx, and M. Birna van Riemsdijk. 2018. Automatic Resolution of Normative Conflicts in Supportive Technology based on user values. *ACM Transactions on Internet Technology (TOIT)* 18, 4, Article 41 (May 2018), 21 pages.

[13] Simon Kemp. 2021. *DIGITAL 2021: GLOBAL OVERVIEW REPORT*. DataReportal. https://datareportal.com/reports/digital-2021-global-overview-report

[14] Pradeep K. Murukannaiah, Nirav Ajmeri, Catholijn M. Jonker, and Munindar P. Singh. 2020. New Foundations of Ethical Multiagent Systems. In *Proceedings of the 19th International Conference on Autonomous Agents and MultiAgent Systems* (Auckland, New Zealand) *(AAMAS '20)*. International Foundation for Autonomous Agents and Multiagent Systems, Richland, SC, 1706–1710.

[15] Pardis Emami Naeini, Sruti Bhagavatula, Hana Habib, Martin Degeling, Lujo Bauer, Lorrie Faith Cranor, and Norman Sadeh. 2017. Privacy Expectations and Preferences in an IoT World. In *Proceedings of the 13th Symposium on Usable Privacy and Security (SOUPS)*. USENIX Association, Santa Clara, 399–412.

[16] Luis G. Nardin, Tina Balke-Visser, Nirav Ajmeri, Anup K. Kalia, Jaime S. Sichman, and Munindar P. Singh. 2016. Classifying sanctions and designing a conceptual sanctioning process model for socio-technical systems. *The Knowledge Engineering Review* 31, 2 (2016), 142–166. https://doi.org/10.1017/S0269888916000023

[17] Anne Oeldorf-Hirsch and S. Shyam Sundar. 2016. Social and Technological Motivations for Online Photo Sharing. *Journal of Broadcasting & Electronic Media* 60, 4 (2016), 624–642. https://doi.org/10.1080/08838151.2016.1234478 arXiv:https://doi.org/10.1080/08838151.2016.1234478

[18] Mihaela Oprea. 2004. Applications of Multi-Agent Systems. In *Information Technology*, Ricardo Reis (Ed.). Springer US, Boston, MA, 239–270.

[19] Serafim Opricovic and Gwo-Hshiung Tzeng. 2004. Compromise solution by MCDM methods: A comparative analysis of VIKOR and TOPSIS. *European Journal of Operational Research* 156, 2 (2004), 445–455.

[20] Tribhuvanesh Orekondy, Bernt Schiele, and Mario Fritz. 2017. Towards a Visual Privacy Advisor: Understanding and Predicting Privacy Risks in Images. In *IEEE International Conference on Computer Vision (ICCV)* (2017-10-29).

[21] Balaji Parasumanna Gokulan and D. Srinivasan. 2010. *An Introduction to Multi-Agent Systems*. Vol. 310. Springer-Verlag Berlin Heidelberg, Berlin, 1–27. https://doi.org/10.1007/978-3-642-14435-6_1

[22] Per Persson, Jarmo Laaksolahti, and Peter Löonnqvist. 2006. *Understanding Social Intelligence*. Vol. 3. Kluwer Academic Publishers, Boston, 21–28. https://doi.org/10.1007/0-306-47373-9_2

[23] Martin Peterson and Sven Ove Hansson. 2005. Equality and Priority. *Utilitas* 17 (11 2005), 299–309. https://doi.org/10.1017/S0953820805001664

[24] Lin Qiu and Riyang Phang. 2020. *Agent-based Modeling in Political Decision Making*. Oxford University Press, Oxford, UK, Chapter 3. https://doi.org/10.1093/acrefore/9780190228637.013.913

[25] John Rawls. 1985. Justice as Fairness: Political not Metaphysical. *Philosophy and Public Affairs* 14, 3 (1985), 223–251.

[26] C. Scheve, D. Moldt, Julia Fix, and R. V. Lüde. 2006. My agents love to conform: Norms and emotion in the micro-macro link. *Computational & Mathematical Organization Theory* 12 (2006), 81–100.

[27] Sebastian Schnorf, Aaron Sedley, Martin Ortlieb, and Allison Woodruff. 2014. A Comparison of Six Sample Providers Regarding Online Privacy Benchmarks. In *Proceedings of the SOUPS Workshop on Privacy Personas and Segmentation*. Menlo Park, 1–7.

[28] Sami Shawl. 2020. *Epsilon-Greedy Algorithm in Reinforcement Learning*. GeeksforGeeks. https://www.geeksforgeeks.org/epsilon-greedy-algorithm-in-reinforcement-learning/

[29] Munindar P. Singh. 1999. An Ontology for Commitments in Multiagent Systems: Toward a Unification of Normative Concepts. *Artificial Intelligence and Law* 7 (1999), 97–113.

[30] Munindar P. Singh. 2014. Norms as a Basis for Governing Sociotechnical Systems. *ACM Trans. Intell. Syst. Technol.* 5, 1, Article 21 (Jan. 2014), 23 pages. https://doi.org/10.1145/2542182.2542203

[31] Daniel J. Solove. 2006. A Taxonomy of Privacy. *University of Pennsylvania Law Review* 154, 3 (2006), 477–564. http://www.jstor.org/stable/40041279

[32] Kaj Sotala. 2016. Defining Human Values for Value Learners. In *Proceedings of the Workshops of the 30th AAAI Conference on Artificial Intelligence: AI, Ethics, and Society*. AAAI Press, Phoenix, 113–123.

[33] Dustin W. Stout. 2021. *Social Media Statistics: Top Social Networks by Popularity*. Dustin Stout. https://dustinstout.com/social-media-statistics/#:~:text=There%20are%20over%20300%20million,billion%20video%20views%20per%20day.

[34] Michael Straeubig. 2017. Let the Machines out. Towards Hybrid Social Systems. In *Proceedings of AISB 2017*. AISB, Bath, UK, 28–31.

[35] Richard S. Sutton and Andrew G. Barto. 1998. *Reinforcement Learning: An Introduction*. A Bradford Book, Cambridge, UK, 31–33.

[36] Project Mesa Team. 2016. *Mesa Overview*. Project Mesa Team. https://mesa.readthedocs.io/en/master/overview.html

[37] Sz-Ting Tzeng, Nirav Ajmeri, and Munindar P. Singh. 2021. Noe: Norms Emergence and Robustness Based on Emotions in Multiagent Systems. arXiv:2104.15034 [cs.AI]

[38] Onuralp Ulusoy and Pınar Yolum. 2018. PANO: Privacy Auctioning for Online Social Networks. In *Proceedings of the 17th International Conference on Autonomous Agents and MultiAgent Systems* (Stockholm, Sweden) *(AAMAS '18)*. International Foundation for Autonomous Agents and Multiagent Systems, Richland, SC, 2103–2105.

[39] Onuralp Ulusoy and Pınar Yolum. 2019. Emergent Privacy Norms for Collaborative Systems. In *Proceedings of the 22nd International Conference on Principles and Practice of Multi-Agent Systems (PRIMA)*. Springer, Torino, 514–522.

[40] Duncan J. Watts and Steven H. Strogatz. 1998. Collective dynamics of 'small-world' networks. *Nature* 393 (1998), 440–442. https://doi.org/10.1038/30918

[41] Jason Wohlgemuth and Mihaela Matache. 2014. Small-World Properties of Facebook Group Networks. *Complex Systems* 23 (09 2014), 197–225. https://doi.org/10.25088/ComplexSystems.23.3.197

[42] Jing Xie and Chen-Ching Liu. 2017. Multi-agent systems and their applications. *Journal of International Council on Electrical Engineering* 7, 1 (2017), 188–197. https://doi.org/10.1080/22348972.2017.1348890 arXiv:https://doi.org/10.1080/22348972.2017.1348890