Cyber Security via Minority Games with Epistatic Signaling (Extended Abstract)

W. Casey, L. Metcalf, J. Morales, J. Spring, R. Weaver, E. Wright, and B. Mishra

Courant Institute, NYU, New York
Software Engineering Institute, CMU, Pittsburgh
mishra@nyu.edu
casey@cert.sei.edu
http://cs.nyu.edu/mishra/

Abstract. We propose a game theoretic framework to study strategic interactions among Humans and Things, assumed to be interconnected by a social-technological network, such as Internet of Humans and Things. Often a pair of agents in the network interacts in order for an informed sender agent to signal an uninformed receiver agent to take an action so as to benefit each of the players from the sender's private information, the signal exchanged and the receiver's revealed (and unrevealed) action. In general, the two agents' utilities may not be aligned and may encourage deceptive behavior. For example, a sender, aware of his own private "state of ignorance," may seek useful information from a receiver who owns powerful computational resources to search a large corpora of webpages; the sender does so by sending a signal to the receiver in the-form of a key-word. Obvious examples of deceptiveness here ranges from attempts to hide one's intentions to putting out the keywords on an Ad-Exhange for real-time bidding. A rather troublesome situation occurs when deceptions are employed in order to breach the security of the system, thus making the entire social-technological network unreliable. Earlier, we proposed a signaling-game-theoretic framework to alleviate this problem and demonstrated its usefulness through extensive simulation. This paper reviews the original game architecture and further enhances it by making signals to possess more complex structures (epistatic signals), and the parameters of the utility functions to be dependent on the past strategy profiles (e.g., the distribution of players employing various kinds of vulnerability and threat predictions). The resulting game, a Minority Game with Epistatic Signaling, is empirically studied through extensive computer simulation and leads to certain surprising conclusions.

1 Games and Cyber Conflicts

At the center of many dynamic online strategic interactions (e.g., in social-technological networks) are simple information-asymmetric games. Each interaction among agents, exchanging digital messages or *Apps*, presents a chance that either party may employ deception and gain advantages over the other. Take for example the *flash-light App* for smart-phones which was also discovered to open a *GPS-tracking* backdoor to gain private information by tracking the device's physical location (discovery reported in Kassner [December 11, 2013]). While the producer (e.g. *sender*) of the *flash-light App* may advertise (e.g. *signal*) that the application is designed to provide a flashlight feature (for smart phones) the *sender* creates the deceptive impression of respecting the user's privacy as implied by the app's benign sounding name: 'flash-light App.' Typical user's expectations of privacy would proscribe the surveillance capabilities (physically tracking the user's device via *GPS-tracking*) and not foresee encroachment by an app that is *prima facie* simple, benign, and desirable. In this case (and others like it) a typical consumer (e.g. *receiver*) would recognize that they had been deceived upon discovery of the *App's* true scope of capabilities which include the *GPS-tracking* and subsequent to the discovery of the deceptive attack the *receivers* may label the *sender* as a miscreant and tarnish their reputation with a negative ranking and comments sprinkled with such labels as 'backdoor,' 'Trojan,' or 'Malware.' The encounter, concluded before the discovery of the attack, has its costs and benefits as the cost to the *receiver* is the loss of privacy and the benefit to the *sender* is the ability to gain strategic informational advantages with unanticipated usages.

In considering signal games for cyber security we envision the possibility that security properties such as *non-surveillance* may be implemented via a social-technological recommendation-verification system. Furthermore, the currency of such a system would be M-coins certificates backing the proofs concerning the behavior of *Apps*.

Lacking proofs or certifications that the application behavior complies with reasonable security properties the *receiver* is left with the options to either trust the *sender* or attempt to challenge them. Such challenges may seek their own or otherwise trusted proofs or certificates to let the receiver decide whether the *sender* is being deceptive.

To consider how such a social-technological recommendation-verification system could address the many distinct attacks that a (e.g. *sender*) could deceptively ensnare a consumer (e.g. *receiver*), we consider the extension of Signaling Games to include diverse attack vectors and term this extension **Epistatic Signaling Games**. After defining epistatic signaling games we present experiments designed to understand their dynamics empirically and how such a system could operate in practice.

2 Minority Games with Epistatic Signaling

2.1 Epistatic Signaling.

At the core of epistatic signaling games are the outcomes of *receiver* challenges against *sender* attacks which will result in *detection events* (or otherwise). In epistatic signaling games, we assume that there are K distinct attacks, $A = \{a_1, a_2, \dots a_K\}$ and that the *sending* agent may employ any subset of these when encountering a consumer *receiver* agent. Therefore the sender in principle may send $2^K - 1$ different combinations of attacks as well as the clean or benign signal which can be modeled as the empty subset $\emptyset \subset A$. Therefore the subsets of A represent sender options for an agent. Likewise the *receiver* may in principle identify, prove or certify each/any attack the *sender* has access to. Letting c_i be the check against attack a_i the sender's options are subsets of $C = \{c_1, c_2, \dots c_K\}$ with the empty set $\emptyset \subset C$ also indicating the option of receiving messages with no challenge which may be interpreted as either a trusting or insouciant option.

When the *receiver* challenges the *sender* four possibilities could result:

True-Positive: The effort to seek certification (invested by the *receiver* at the *challenge cost* of G per challenge) results in a *detection event* which determines that the *sender* is a deceptive attacker. Within a social network the detection event may carry a heavy reputational cost for the *sender* which we term *E the cost of getting caught.* For the *receiver* a *reputational benefit* for catching the attacker F may also be conferred and help to balance the *challenge cost* of G. Further the benefit of F is higher when the challenging receiver is in a *minority*, as he shares the benefit with few others.

False-Positive: The *receiver* who claims that a particular sender is a deceptive attacker (when in fact they are not) will not impart the high *cost of getting caught* upon the *sender* because the proof will not be repeatable by other challenging *receivers*. Therefore the net result of a false positive will be a cost incurred by the *receiver* in proportion to the number of challenges (at G per challenge) against the *sender*. Additionally we may argue that the *sender* should incur a direct reputational cost as well; while we do not model this explicitly, the symmetric and repeated game may in fact provide some ability to model these costs by reversing the roles of *sender* and *receiver* and in this context the *false accusation* can be treated as attack (in the next round).

False-Negative: Despite the effort to seek certification (invested by the *receiver* at cost G) the *receiver* may not recognize the deceptive actions of the *sender* and thereby the *sender* achieves an attack at benefit D for each attack achieve (all at the cost of the *receiver*).

True-Negative: Despite any and all effort to seek certification (invested by the *receiver* at cost G per challenge) the *receiver* does not detect any deceptiveness in the actions of the *sender* while the *sender* launches no attacks against the *receiver*.

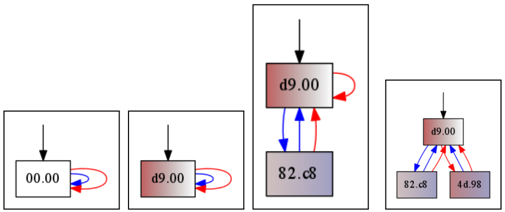
Strategy for Repeated Epistatic Signaling Games. In each encounter the agents may play the role of either *sender* or *receiver*. There are 2^K strategic options available to the *sender* (all the subsets of A) and 2^K strategic options available to the receiver for checking each attack set (all the subsets of C). In a single round of play the challenges of the *receiver* are matched against the attacks of the *sender* to determine how many **detections** are achieved, letting $m, 0 \leq m \leq K$, be the number of detections the penalty for the *sender* will include a cost for getting caught which will be $m \cdot E$, (E being the cost of getting caught). Said differently, the cost for sending more attacks/vulnerabilities scales with the number of detections the *receiver* achieves while the benefits scale with the number of attacks attained.

The symmetric epistatic signaling game will allow the agents of each encounter to play both the roles of *sender* and *receiver*, therefore the strategic options for each agent include a *sending* option and an independent *receiving* option. The symmetric form of the epistatic signal game provides some ability to treat the *false-accusation* as itself an attack which can also be debunked as a challenge but generally treats agents of a population as having equal access to strategic options. Because interactions among agents in cyber space are inherently dependent on prior interactions, strategies for single shot games may not sufficiently model the environment.

However a strategy for repeated games should address how an agent *receiver* should react when the *sender* in an encounter has been detected as a deceptive attacker. Therefore the *detection* event which is the matching of least one of the *receiver* challenges to the associated *sender* attack is an important event because in the absence of detection an attack may not be immediately distinguishable from a benign signal.

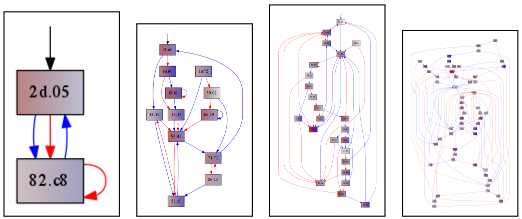
To incorporate the *detection* event into the strategy of an agent, which may play symmetric repeated games, we model each agent as a labeled deterministic finite state automata (DFA), as we did in our earlier work. Labeled DFA provides a means to evolve complex strategic interactions spanning multiple plays of a repeated game among agents. This technique (used in Binmore and Samuelson [1992], van Veelen et al. [2012]) enhances the dynamics possible while simple mutation provides a means for exploration (of a vast strategic space), thus allowing an ensemble of agents to adapt strategies to population dependent fitness landscapes.

Below in figure 1 we show how strategy structures can evolve and in figure 2 illustrate a mutational process for strategies generates diverse strategies over time.



(a) $j = 0$ (b) $j = 1$ (c) $j = 2$ (d) $j = 3$

Fig. 1. In our epistatic signaling game, each agent has ability to signal a subset of 'attacks' as well as a subset of 'checks.' For each agent, strategy is succinctly represented as a deterministic finite state automaton, which evolves over time during a simulation via mutation. As an example we show a sequence of four mutations with $K = 8$ attack and defense possibilities, with each attack and check vector in a state being denoted by a number in hexadecimal notation and a color gradient. Starting with (a) the initial seed strategy employs no attacks and no defenses, the label 00.00 represents the selected attacks (two hexadecimal digits to the left) and selected defenses (two hexadecimal digits to the right), transitions (edges) in the FSA are color coded red will be used if the strategy detects an attack and blue transition will be used otherwise. Next in (b) the sending signal is modified from 00 to $d9$ which encodes (in hexadecimal) the attack set $\{a_1, a_4, a_5, a_7, a_8\}$ as the new attack option. A gradient coloration from red on the left to blue on the right is used indicate the density of attacks and defenses are employed in each state. Next in (c) mutation adds an additional state with random send option $\{a_2, a_8\}$ and receive option $\{c_4, c_7, c_8\}$ encoded as $82.c8$. Finally in (d) an additional state is added having label $4d.98$ and representing attack option $\{a_1, a_3, a_4, a_7\}$ and defense option $\{c_4, c_5, c_8\}$. In particular notice that the options for a newly create state are selected uniformly randomly over the option spaces with 2^K possibilities.



(a) $j = 10$ (b) $j = 100$ (c) $j = 1000$ (d) $j = 5000$

Fig. 2. Continuing the example of an agent's evolution from Fig 1, we illustrate how mutation of strategy creates diverse strategies. We show steps of (a) 10, (b) 100, (c) 1000, and (d) 5000 of a mutation sequence starting from the simplest single state strategy labeled 00.00. Mutation allows strategies to develop complex transitions based on detection [red transition] or otherwise [blue transition] for application against encountered agents in repeated games.

2.2 Signaling Games in Cyber Security.

In signaling games for cyber security the notion of deception was a primary consideration in the simulations revealing a range of outcomes for system behavior over the space of payoff parameters (Casey et al. [2014]). Epistatic signaling games differs from signal games for cyber security in the following two ways. First in signal games the strategic options for *sender* and *receiver* are limited to single attack and challenge option: namely, such a game is a special case of the general epistatic signaling formulation when $K = 1$. By considering the dynamics of diverse attack and defense portfolios in a population as set systems over 2^A and 2^C we provide more realism such as undetected attacks (e.g. the false-negatives detection events) but we also create the possibility that strategic options for attack and defense can be scored to bias the selection process during mutation events (vs. uniform random selection) and this may be an important consideration in a social-technological recommendation-verification system which a population could employ. When the agents are allowed to select the options in challenging, based on performance rather than obliviously or randomly, has a distinct effect on the overall system behaviors and is empirically studied in this paper through computational experiments, to be described in the simulations section ahead.

The second way in which this approach differs from traditional signaling games is that we simplify the transitions in strategies for repeated games. In this approach we are limiting the agents to two transitions based on if a *detection event* occurred or otherwise. While this constraint may appear to be limiting, it is more realistic, since agents are primarily interested in resolving an attack (e.g. *detection event*); note particularly that in the case of False-Negatives detection events, the user will not have immediate access to what attack succeeded, and identifying all such non-detection outcomes may seem reasonable. There remains the possibility that a *receiver* who achieves a *detection* may select subsequent play options based on the attack resolved (for example a more sophisticated attack may call on a stronger reaction than a weaker one), however for now we keep things simple and impose the constraint that transitions in strategies are binary and determined by whether a *sender* achieves a detection. This constraint could also be achieved in the simulations in (Casey et al. [2014]) by requiring that mutation of strategies maintains certain equivalencies in transition structure, the details involve a discussion of its own and are excluded.

To show the relation between signal games and this approach of epistatic signal games we review briefly the strategic options and payoff of signaling games for cyber security.

The strategic options: In signaling games the *sender* may select the option: to send *cooperatively* C or to send an attack D. Similarly the options for the *receiver* are to accept *trusting* C or to *challenge* D. We encode all options using strings where the first letter is the *sender* option and the second the *receiver* option. Using this encoding the option space for a single round of signaling games is the set $\{CC, CD, DC, DD\}$.

Game Payoff: The payoff matrix for the symmetric signaling game is then defined over the product of row-player options and column player options $\{CC, CD, DC, DD\} \times \{CC, CD, DC, DD\}$. Letting d the benefit of an attack for the sender (assumed to be a zero sum quantity), e the cost of getting caught attacking as sender, f the prize for catching an attacker, and g the cost of challenging a sender as receiver. The contributions to payoff of these quantities for the row player payoff is:

(row, col)	CC	CD	DC	DD
CC	$(0, 0)$	$(0, -g)$	$(-d, d)$	$(-d, d-g)$
CD	$(-g, 0)$	$(-g, -g)$	$(f-g, -e)$	$(f-g, -e-g)$
DC	$(d, -d)$	$(-e, f-g)$	$(0, 0)$	$(-d-e, d+f-g)$
DD	$(d-g, -d)$	$(-e-g, f-g)$	$(d+f-g, -d-e)$	$(-e+f-g, -e+f-g)$

Note that the column-player payoff is the transpose of the row-player payoff (symmetric games).

2.3 Epistatic Signaling Games.

We define the Epsitatic Signal game below as an extension of signal games[1]. We begin by discussing strategic options and game payoffs; to assist in computing payoffs, we introduce a few auxiliary accounting functions. We introduce the auxiliary functions by considering two phases of each symmetric game: The play is in offense when the agent is a *sender* facing a potentially challenging *receiver* and in defense when the agent is a *receiver* facing a possibly deceptive *sender*. Finally we present the payoff function for a row-player and exploit the transpose relation for the column-player payoff.

The strategic options: In this approach we dramatically increase the size of the signal space available to the agent in each round, therefore the *sender* and *receiver* will have vastly more options for strategic selection. By letting $A = \{a_1, a_2, \ldots, a_K\}$ be the finite set of attack vectors to include zero-day attacks, vulnerabilities, injections, deceptions, social engineering, etc. and letting $C = \{c_1, c_2, \ldots, c_K\}$ be their associated counters or detectors we increase the options for *sender* to include every element of 2^A and the options for *receiver* to include 2^C. An agent who provides apps may send no attacks but include vulnerabilities (perhaps, unwittingly), therefore we generally model these actions as subsets of A.

Therefore in a single round of the symmetric game the agent has options $\{(A', C') : A' \in 2^A, C' \in 2^C\}$. The first index refers to a subset of A employed by the agent as *sender* and the second index refers to a subset of C employed by the agent as *receiver*. We will let $U = 2^A \times 2^C$ comprise the strategic options for an agent in symmetric epistatic signaling games.

Game Payoff: The form of the payoff matrix for the epistatic signaling game may be considered as an assignment of payoff (for the row-player i against column-player j) over the product space of signals: $U \times U$. Letting the $u_i \in U$ be the strategic option for the row-player and $u_j \in U$ the strategic option for the column-player we denote $u_i = \alpha_i \times \gamma_i$ and $u_j = \alpha_j \times \gamma_j$ with $\alpha_i, \alpha_j, \gamma_i, \gamma_j \in \{1, 2, \ldots, K\}$ to index, in turn, the corresponding attacks employed by row-player, attacks employed by column-player, defenses fielded by row-player, and defenses fielded by column-player.

The payoff matrix for epistatic signaling games takes the form $M(u_i, u_j)$ to quantify the payoff for the row-player when the row-player i employs option u_i and column player j employs option u_j. Further the payoff for the column player is also the transpose of indices that is $M^\top(u_i, u_j) = M(u_j, u_i)$.

Payoff values: To compute $M(u_i, u_j)$ we introduce a few simple auxiliary accounting functions involved in stages of the symmetric game for a single player (the row-player), the stages are the offense stage when row-player is a *sender*) and the defense stage when the row-player is a *receiver*.

Offense: In each round of play the row-player i launches a total number of attacks against the column player j counted as $\textsc{Attacks-Fielded}(i, j) = |\alpha_i|$, while the number of successful attacks by the row player i against the column player j is counted as $\textsc{Attacks-Achieved}(i, j) = |\alpha_i \setminus \gamma_j|$. For each attack launched by the *sender* a fixed cost H is added to the overall cost of the *sender* option. This fixed cost may be associated with the cost to develop/deploy an attack, identify a software vulnerability, develop an exploit, or apply resources to attack. For each attack achieved by the row-player i against the column player j a fixed zero-sum equity of D is transferred to the row-player as a benefit at the expense of the column-player. This zero sum equity is intended to model the value of a digital asset, authorization token, credential, personal identifiable information, or digital currency (e.g. bitcoin or more specifically, M-coin), etc.

[1] With the caveat that transitions in repeated game strategies are simplified to binary outcomes based on detection events.

Defense: In each round of play the row-player i fields a total number of defenses (or checks) against the column-player j, denoted as $\textsc{Defenses-Fielded}(i,j) = |\gamma_i|$, while the number of effective defenses or equivalently *detection events* for the row player i against column player j are counted as $\textsc{Detects}(i,j) = |\gamma_i \cap \alpha_j|$, and finally the false positive challenges for player i agaisnt player j are counted as: $\textsc{Futile-Challenge}(i,j) = |\gamma_i \backslash \alpha_j|$. For each defense fielded by the *receiver* a fixed cost G is applied to the strategic option; this cost can be treated as a cost to develop the detector algorithms and may be amortized and scaled to affordable quantities via a social-technical network where detection methods are deployed. Each detection event will imposes a heavy cost of E on the *sender* and will also confer a benefit of F to the *receiver*. The cost associated with a detection event for the *sender* is designed to model the loss of reputation, loss of security certifications, M-coin tokens, etc. As an example a code project that imparts users with a large vulnerability surface[2] will naturally suffer a reputational loss as multiple receivers prove its deficiencies. Defenses that are fielded but do not result in detections may be considered futile (at least for that round) and will carry a cost burden for the *receiver* thus imposing a natural pressure on agents to be parsimonious with detection and thereby establish an incentive to measure effectiveness of *receiver* options so that the most effective methods for detection can be selected and propagated in a population.

Allowing for strategy mutation allows for dynamic drift in attack and detection efficacy as well as introducing a realistic aspect in that strategy effectiveness is dependent on the context of the population of strategies employed.

Payoff Structure for Epistatic Signal Games: For row-player i selecting option $u_i = \alpha_i \times \gamma_i$ playing against column player j who selects option $u_j = \alpha_j \times \gamma_j$ the row-player payoff is defined as:

$$\begin{aligned} M(u_i, u_j) &= D \cdot \textsc{Attacks-Achieved(i,j)} \\ &- D \cdot \textsc{Attacks-Achieved}(j,i) \\ &+ F \cdot \textsc{Detects}(i,j) \\ &- E \cdot \textsc{Detects}(j,i) \\ &- H \cdot \textsc{Attacks-Fielded}(i,j) \\ &- G \cdot \textsc{Defenses-Fielded}(j,i). \end{aligned}$$

Remarks: The settings of parameters D, E, F, G, H are shown to be critically important for the behavior of a system for evolving populations in [Casey et al. [2014]]. The important distinction for this model (epistatic) is that costs/benefits are allowed to scale (linearly) in the counts of the following: number of attacks, number of defenses, and number of detections. These scale laws naturally place incentives on selecting effective options and afford a means to study many system behavioral outcomes of interest such as system effects for various rates of evolution in attacks vs. defenses. Our motivation for studying this problem is rooted in the following questions: whether a social-technological recommendation-verification system can be effective in providing defenses flexibly, and if so, what mechanisms can achieve these desiderata.

2.4 Minority Signaling Games.

In Signaling Games played in social technological systems, we may consider the possibility of variable costs/payoffs depending on bulk population behavior. In this context, there will be certain

[2] Vulnerabilities may result from technical deficits such as sloppy code writing and leave a user exposed to any attacker.

advantages (e.g., in reputitional gain) by being in the minority as a challenging receiver. These considerations led us to formulate minority signaling games. If early adapters (minorities) have slight preferential advantage there may also be incentives for the population to develop and maintain diverse challenging options. It may also be possible that a population that develops and sustains diversity in strategies may mitigate some of the most wild dynamics observed in signaling games which include drifting oscillation between low to high levels of attacks and checking (either all players deciding to challenge or to be insouciant).

To study this problem we consider introducing non-constant cost/payoff coefficients in the payoff structure a mechanism that will give rise to dynamics similar to the El Farol bar problem. To introduce El Farol bar dynamics into the epistatic signal games we consider allowing the cost parameter G to vary based on bulk population behavior, the simplest adjustment is a step function which increases the cost (by a multiple ζ) when the fraction of outcomes in a population exceed a given fractional threshold τ. We define the set of agents as $U = \{u_1, u_2, \ldots, u_M\}$ and consider all the games occurring during encounters in a given generation. Summing over all encounters during a generation we let $\mathcal{C}$ be a monitor for the fractional amount of checks deployed among all defensive *receiver* options compared to the total possible capacity for checking during the generation (i.e. if all *receiver* options employed every check).

In minority signaling games the general form of the payoff for row-player is a slight modification to equation for $M(u_i, u_j)$ where the coefficient G is modified to be a step function depending on the population quantity $\mathcal{A}$ computed during the games of a generation:

$$G(U) = \begin{cases} G & \text{if } \mathcal{C}(U) \leq \tau \\ \zeta \times G & \text{otherwise} \end{cases} .$$

3 Simulations.

We discuss the simulation results by first outlining the general framework for evolutionary games which will be used throughout as the underlying simulation model for the population of social technical users. Next we outline a set of two experiments for epistatic signaling games, which are designed to provide insights into the nature of system evolution and dynamics. After providing some simulation visualizations of the basic epistatic signaling game, we investigate the following experiments:

- Effect of strong and transparent measures for the challenge options in a population vs. random selection. This experiment seeks to compare the system behavior in each of the following two cases:
  - *receiver* challenge options are selected uniformly randomly over the *receiver* option space (when mutation events occur).
  - *receiver* challenge options are selected based on performance measures proven in the previous generation of games (when mutation events occur). Some fraction ξ of mutations that will affect *receiver* options will be selected uniformly randomly over the entire *receiver* option space.
- Effects of minority games and El Farol dynamics when applied as a step function for *sender* costs. This experiment introduces the population behavior based step function $G(U)$ already defined with fractional behavior quantity $\mathcal{C}$ and threshold τ and explores if this mechanism can diversify *sender* options in a population and lead to effects on system dynamics.

Each of these results is meaningful for prospective engineering of better cyber security in social technical networks. In the first experiment where the effects of strong and transparent measures for challenge options we investigate a possible means to organize a distributed cyber response system related to epistatic signaling games and related to other notions of cellular immune response systems (van den Berg [2009]).

In this experiment the fraction ξ must be positive to prevent fixation effects that would otherwise occur on the *receiver* strategies while the *sender* strategies are allowed to mutate freely. To retain the ability for *receiver* options to adapt defense strategies to novel attack strategies a positive ξ will be required. While the effects of mutation rates and ξ are of practical interest this experiment provides only a start in that direction.

The second experiment address some of the wild dynamics observed in these systems, which include constructs such as *defection invasions*, and *spontaneous cooperation* as well as wild oscillation between them. The experiment is designed to investigate the possible effects of a mechanism, which may incentivize the parsimonious use of defense options, the diversification of defense options, and increase stability in these complex dynamics. Such a mechanism may either be designed as part of a system or otherwise may be discovered as a natural factor.

After outlining the general framework for evolution games we describe the slight augmentation of the framework needed to conduct the experiments. The results obtained from the experimentation are reported in images and exposition of what this may mean for security in social-technical systems.

3.1 Simulation Outline:

We outline the general simulation and provide descriptions of how we can augment or modify each step to achieve the analytic steps outlined above.

Shape Parameters: $\langle M, K, N\rangle$: population size, option set size, and number of generations.
System Parameters: $\langle D, E, F, G, H, \delta, \mu, \rangle$: payoff settings, continuation factor, mutation rate.
Initialize: A population U of M users initialized with random strategies.
For each generation:

- **Encounter:** Using the population of strategies (time n) we create pairwise encounters for game play.
- **Play:** For each encounter: repeated games are played using agent strategies. Number of rounds determined by continuation parameter δ. Each player aggregates a vector of outcomes.
- **Aggregate and Evaluate Scores**: Total performance measures are aggregated across strategies and unique options used during the encounters for generation n. Scores and measures are computed using epistatic signaling game payoff matrix, outcome vectors resulting from play, and system parameters.
- **Re-create**: A population of M strategies is recreated (for next generation n+1) by sampling the existing strategies with probability density proportional to performance scores.
- **Mutate**: Players are chosen with rate μ for mutation. Each mutation event may modify the strategic encoding of strategy.

The encounters may be created in a variety of ways including: random pairing, use of an underlying neighborhood graph to describe kinship or geographical relations, or various hybrid notions.

In (van Veelen et al. [2012]) the use of population structure parameters α, δ as introduced and allow the study of mixture of random encounters to structured encounters resolvable up to a single parameter δ. In our experiments we use $\frac{M}{2}$ encounters selected as random encounters only. During the play the continuation parameter δ is used to determine number of rounds by generating a random geometric derivate with δ as continuation parameter. For pairwise agent encounters playing repeated games each will use their strategy (described by a labeled deterministic finite automata, DFA), which is used to compute options and outcomes for each round of play in during the repeated epistatic signal games. The labeled deterministic finite automata are used in the following way (described for the row-player): Starting from the start-state the *sending* and *receiving* signals are determined, if the row-player detects an attack from the column-player then the red transition edge is used to determine the next strategic options for both sending and receiving, if an attack was not detected then the blue transition edge is used to determine the next strategic option for the row-player. In either case in the next round the option including both send and receive are determined. By following this sequence of steps in the strategic automata each agent may aggregate a vector of outcomes (e.g. number of attacks, number of defenses, number of detections, number of time opponent detect their attacks). These aggregate counts are stored for the next step where the strategies are scored.

Mutation of strategy is performed on the generation of M strategies with base rate μ with an expected number of mutants as μM per generation. Given that a strategy is selected for mutation, one of the five mutation types is selected according to a mutational type frequency vector which through out the experiments will be fixed at: $\nu = [0.15, 0.15, 0.1, .3, 0.3]$, next we describe the mutational types:

- *type-i*: mutate the *sender* option.
- *type-ii*: mutate the *receiver* option. The selection distribution is the subject of experiment titled: Effect of strong and transparent measures.
- *type-iii*: mutate an edge (selected uniformly randomly in all experiments).
- *type-iv*: create a new strategy state with randomly selected edges. (Through out these experiments we limit the size of automata to 256).
- *type-v*: remove a strategy state. (Throughout these experiments we limit the size of automata to be one or more states).

In experiment one where we investigate the effects of strong and transparent measures on *receiver* options we also track the number of times each *receiver* option detects an attack. When a mutation event modifies a strategies *sender* option we replace the send option with a random selection with probability $1 - \xi$ and with probability ξ we use a performance scaled density over the options at play in generation n. The first outcome (with probability $1 - \xi$) mitigates the fixation of *receiver* strategies while the second outcome should allow the population to track existing attack vectors in the population more effectively.

In Experiment two where we investigate El Farol dynamics we will augment the aggregate and evaluate step to compute $\mathcal{C}$ and update the evaluation of price per defense using function $G(U_n)$ for generation n. Thus allowing us to draw some conclusions about the use of such a mechanism in epistatic signaling game system.

3.2 Experimental Results.

Using shape parameters $M = 320, K = 8, N = 80,000$ with system parameters $D = 10, E = -100, F = 4, G = -2, H = -2, \mu = 0.03, \delta = 0.5$ and letting our encounter mechanism being random pairs $\alpha = 0.0$ we conduct experiments by generating 100 histories of simulations of the following systems. Throughout the mutation type rates will remain fixed at: $\nu = [0.15, 0.15, 0.1, .3, 0.3]$.

S1 : Epistatic signal games with receiver options mutated uniformly randomly over the option space.
S2 : Epistatic signal games with receiver options scored as a strong and transparent measure in the population $\xi = 0.5$.
S3 : Epistatic signal games with minority step function $G(U)$ with $\tau = 0.4, \zeta = 4.5$.
S4 : Epistatic signal games with receiver options scored as a strong and transparent measure in the population $\xi = 0.5$, and minority step function $G(U)$ with $\tau = 0.4, \zeta = 4.5$.

In figure 3 we illustrate a single history of (**S1**), epistatic signal games, where receiver options are mutated uniformly randomly over the option space.

In figure 4 we illustrate a single history of (**S2**), epistatic signal games where receiver options are scored as a strong and transparent measure for selection in the population ($\xi = 0.5$).

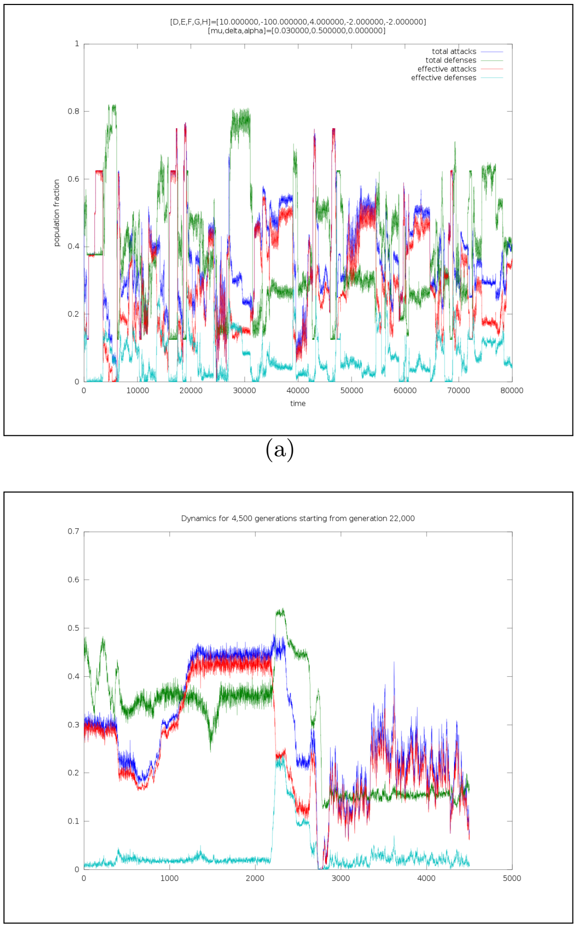
In figure 5 we illustrate a single history of (**S4**) epistatic signal games where receiver options are scored as a strong and transparent measure for selection in the population ($\xi = 0.5$), and minority step function $G(U)$ with $\tau = 0.4, \zeta = 4.5$.

Effects of Experiments. In figure 6 we compare the behavioral of each system using the quantities which measure the fraction of all attacks sent (of the total possible capacity of users to attack) as A, the fraction of attacks that are not detected as $[A]$, the fraction of defenses which detect attacks as $[D]$, and the fraction of defenses fielded (of the total possible capacity of users to field defenses) as D.

The effect of strong and transparent measures for challenge options appears not to decrease the number of attacks but does seem to reduce both the number of defenses fielded, while maintaining an equivalent detection rate. The effects of minority games, which introduce a multiplier cost to G, the cost of fielding defenses seems to also have an equivalent effect to that of imposing strong and transparent measures on the *receiver* options. The combination of using both seems to have compounding effects.

4 Discussion

We have shown a natural role for signaling games in modeling various strategic interactions among agents in a social-technological network such as Internet of Humans and Things. In particular, we have studied the effect of recommendation-verification system augmenting the two-player sender-receiver games, and how it could be implemented using a newly-devised crypto-coin (i.e., M-Coins).



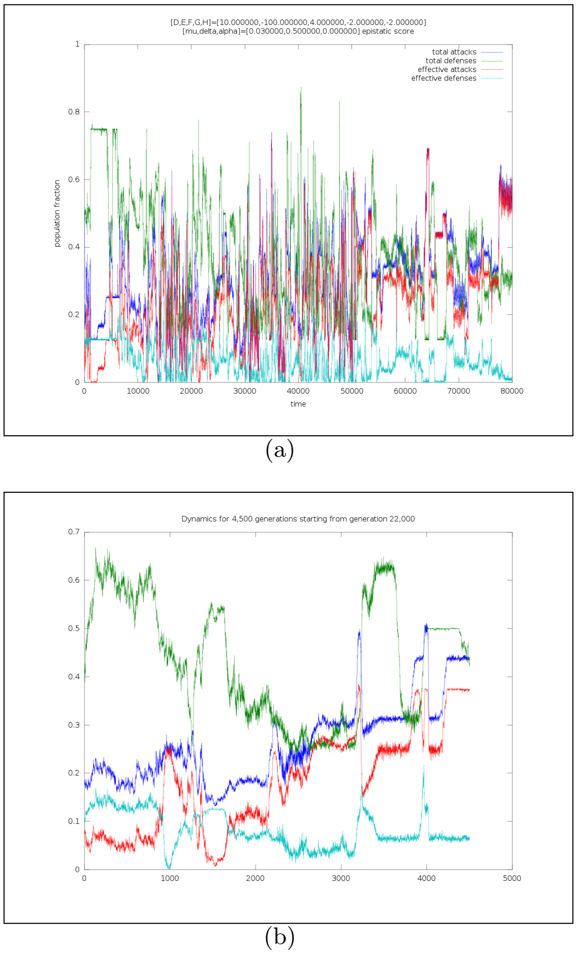
(a)

(b)

Fig. 3. S1: Dynamics of epistatic signal games. (a) Fractional quantities of attacks, effective attacks, defenses, and effective defenses in 80,000 generations. (b) Shows in higher resolution these quantities in 4,500 generations starting from generation offset 22,000 in (a). The quantities plotted are [blue] total attacks, [red] effective attacks, [green] total defenses, and [cyan] effective defenses.

In this paper, we have further advanced the design by introducing a complex form of signaling, called, epistatic signaling and explored the role of minority games in this context. Our simulations have identified some counter-intuitive behaviors, for instance the behavior of the attackers in exploiting the signal complexity as the dimension of the attack and checking vectors grew. In our future work, we plan to explore the natural trade-offs that exist between complexity of signals and levels of deception.

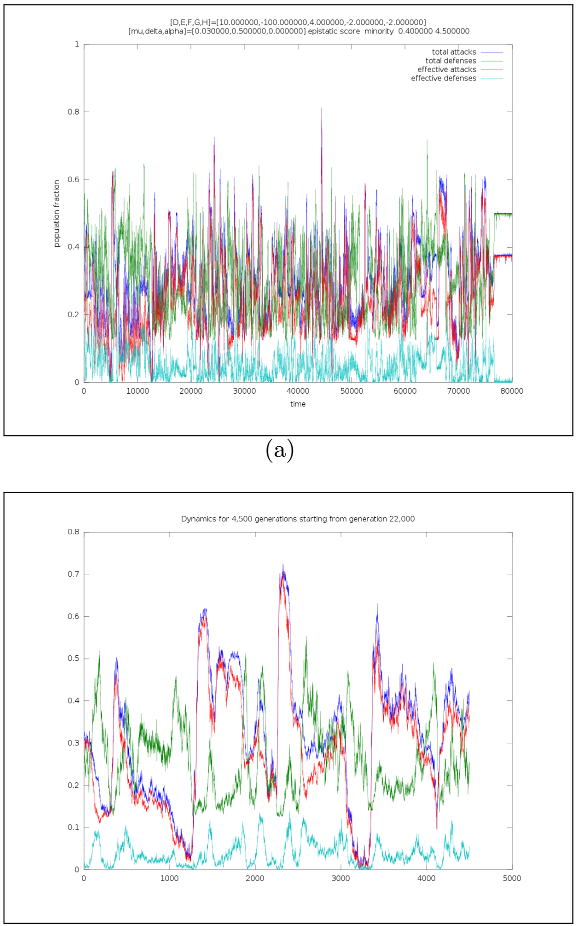
.



(a)

(b)

Fig. 4. S2: Experiment i). Dynamics of epistatic signal games when the mutation for *receiver* options is biased toward strong and transparent performance measures proven in previous rounds against employed attacks. (a) Fractional quantities of attacks, effective attacks, defenses, and effective defenses in 80,000 generations. (b) shows in higher resolution these quantities in 4,500 generations starting from generation offset 22,000 in (a). The quantities plotted are [blue] total attacks, [red] effective attacks, [green] total defenses, and [cyan] effective defenses.



(a)

(b)

Fig. 5. S4: Experiment ii) Dynamics of epistatic signal games when the mutation for *receiver* options is biased toward strong and transparent performance measures and minority step function $G(U)$ is used to determine the cost of applying each defense. (a) Fractional quantities of attacks, effective attacks, defenses, and effective defenses in 80,000 generations. (b) shows in higher resolution these quantities in 4,500 generations starting from generation offset 22,000 in (a). The quantities plotted are [blue] total attacks, [red] effective attacks, [green] total defenses, and [cyan] effective defenses.

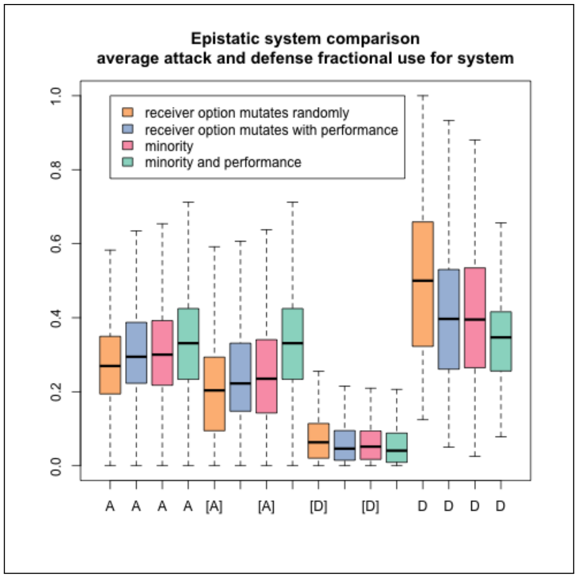


Fig. 6. Dynamics of epistatic signal games in behavioral quantities: A the fraction of attacks sent (of the total possible capacity of users to attack), $[A]$ the fraction of attacks that are not detected, $[D]$ the fraction of defenses which detect attacks, and D the fraction of defenses fielded (of the total possible capacity of users to field defenses).

Bibliography

Kenneth G. Binmore and Larry Samuelson. Evolutionary Stability in Repeated Games Played by Finite Automata. *Journal of Economic Theory*, pages 278–305, 1992.

William Casey, Jose A. Morales, Thomson Nguyen, Jonathan Spring, Rhiannon Weaver, Evan Wright, Leigh Metcalf, and Bud Mishra. Cyber security via signaling games: Toward a science of cyber security. In *ICDCIT*, pages 34–42, 2014.

Michael Kassner. Android flashlight app tracks users via gps, ftc says hold on, December December 11, 2013. URL http://www.techrepublic.com/blog/it-security/why-does-an-android-flashlight-app-need-gps-permission/. [Online; posted December 11, 2013, 9:49 PM PST].

Hugo Antonius van den Berg. Design principles of adaptive cellular immunity for artificial immune systems. *Soft Comput.*, 13(11):1073–1080, 2009. URL http://dblp.uni-trier.de/db/journals/soco/soco13.htmlBerg09.

Matthijs van Veelen, Julián García, David G. Rand, and Martin A. Nowak. Direct reciprocity in structured populations. *Proceedings of the National Academy of Sciences*, 109(25):9929–9934, June 2012. ISSN 1091-6490. doi: 10.1073/pnas.1206694109. URL http://dx.doi.org/10.1073/pnas.1206694109.