Identity Deception and Game Deterrence via Signaling Games

William Casey
Carnegie Mellon University
wcasey@cert.org

Parisa Memarmoshrefi
University of Göttingen
memarmoshrefi@cs.uni-goettingen.de

Ansgar Kellner
University of Göttingen
kellner@cs.uni-goettingen.de

Jose Andre Morales
Carnegie Mellon University
jose@josemorales.org

Bud Mishra
New York University
mishra@nyu.edu

ABSTRACT

Maintenance and verification of persistent identities is an important problem in the area of networking. Particularly, their critical roles in Wireless Ad-hoc networks (WANETs) have become even more prominent as they begin to be deployed in several application domains. In these contexts, Sybil attacks, making use of replicated deceptive identities, represent a major challenge for the designers of these networks. Inspired by biological models of ant colonies and their dynamics studied via information asymmetric signaling games, we propose an architecture that can withstand Sybil attacks, similar to ants, using complex chemical signaling systems and associated physical actions, naturally 'authenticate' colony members. Here, we present a biomimetic authentication protocol with mechanisms similar to the physical processes of chemical diffusion, and formalize approaches to tame the deceptive use of identities; we dub the resulting game an "identity management signaling game". To consider network system of nodes, pursuing non-cooperative and deceptive strategies, we develop an evolutionary game system allowing cooperative nodes to mutate deceptive strategies. We empirically study the dynamics using simulation experiments to select the parameters which affect the overall behaviors. Through experimentation we consider how an *incentive package* in the form of a shared database can impact system behavior.

Categories and Subject Descriptors

Networks [**Security and privacy**]: Mobile and wireless security

Keywords

signaling games; WANET; identity management; Sybil attack; bio-inspired approach

1. INTRODUCTION

Identity management is a challenging, yet critical, problem in networks, particularly in WANET-applications, which are being increasingly used in many risk-sensitive areas. Consider, for instance, the application of a WANET for emergency response during a natural disaster or for medical monitoring – applications involving life-and-death. Thus, it is important that these systems are able to offer an assurance that nodes in the network behave in a trustworthy manner. Furthermore, since deception, underlying security attacks, are cheap and easy in cyber systems, it is possible to overwhelm WANETs with Sybil attacks – attacks that either pilfers or fabricates identities using low overhead computation. Sybil nodes, by undermining a root of trust tied to an identity, enabling untrustworthy actions thereby degrading system quality assurance. The challenge is to create an identity management system, capable of distinguishing the trustworthy from the trusted.

We present a solution to the problem that is motivated by biological systems where the identity of an organism as a member of a super-organism (colony) is an important factor in emergence and persistence of cooperation. An oftencited example is the one involving ant colonies, where the identity of an organism by colony (including even specific roles within the colony) are critical to the "strategic" interactions among the players, as in a classical noncooperative game where one usually assumes rationality and its common knowledge. To set the stage, we first describe the "game" played by the ants, using the *Cuticular Hydrocarbon (CHC)* profile and the physical processes (i.e., diffusion) involved. Inspired by these seemingly simple systems, we construct an authentication protocol for nodes of a WANET and develop an "identity management signaling game," which describes the dynamics similar to those possible with deceptive uses of identity. Our signaling game includes a challenge operation that potentially increases the cost of deceptive signaling. Moreover, because of our constrained communication model, it acts to improve the decision making of other colony members, who may also encounter the same deceptive signaling strategy.

To specialize the game to a network of communicating nodes, we construct an evolutionary game system, on a torus which is capable of exploring strategies with mutations. In addition the game system will allows us to apply a wide variety of optimization concepts to agents based on their proper-

.

BICT 2015, December 03-05, New York City, United States

DOI 10.4108/eai.3-12-2015.2262519

ties (i.e., deceptive vs. honest) to understand how property based benefits may affect dynamics. We computationally simulate the game to generate empirical data and use it to explore what (hyper)parameters impact the bulk behavioral properties in the network. The game system employs a biomimetic constrained authentication protocol, which starts as initialized for all nodes to be cooperative, and as time progresses, allows nodes to mutate their strategies to explore the use of deceptive strategies. In the simulation model we carefully consider how agents may use information to update and optimize their strategies, while focusing on one critical factor, namely, how these updates may differ for the honest vs. deceptive agents.

We introduce the concept of a *cooperative group benefit package* in the form of a shared database (comprising cooperative strategies and their performance measures) allowing agents to apply "boosting" for strategic updates and compare this to a system of individualistic optimizing agents where the same benefit package applies to all strategies whether they are cooperative or not. Unsurprisingly our experiments indicate that systems of individualistic optimizing agents feature a swift 'race to the bottom' with wide scale adaptation of identity deception and low overall value for the network. Somewhat surprising to us was how the *cooperative group benefit package* appears to be instrumental in enhancing overall levels of cooperative behavior. Furthermore, the benefit, in the form of a database of strategic performance for cooperative strategies, can be known to the deceptive agents to provide an incentive to act honestly, just as our experiments indicated how in these scenarios deceptive mutants face trouble finding a suitable niche and must come clean to survive.

2. RELATED WORK

2.1 Identity Management in WANETs

Wireless Ad-hoc Networks consists of spatially distributed autonomous devices (network nodes) that can exchange data wirelessly. The nodes do not rely on an existing infrastructure, but can form an on-demand network without any manual configuration. WANETs are used in a variety of application areas and are likely to play an important role in the upcoming Internet of Things (IoT) application areas such as smart cities, environmental monitoring, health care monitoring, industrial monitoring etc.[17, 5, 18, 14]

The multi-hop nature of WANETs constrains these networks by the requirement of the nodes' cooperative behavior that must ensure that only legitimate nodes can participate in the network, thus avoiding attacks such as information leakage and the spreading of disinformation in the network. Particularly, the use of Sybil nodes in the network, i.e. the creation of fake identities to influence the networks' behavior or decision processes, can be a serious source of unrepairable damage to the network[6, 9].

To distinguish cooperative from non-cooperative participants of a WANET, an authentication protocol must be used that is capable of ensuring the uniqueness of identities and a one-to-one mapping of an identity to the corresponding network node. The identity management for WANETs involves each individual node as a decision maker, since each node must take specific actions towards other nodes in the network depending on their behavior and strategies. To setup the proposed authentication protocol, unique context-based credentials for each node are required, which can be behavioral and/or physical. While the identity for behavioral-based credentials is based on a node's (claimant's) pattern of behavior, physical-based credentials make use of a unique physical characteristic of the claimant's identity.

In this work an identity management framework is presented based on physical-constraints and behavioral-based characteristics of each node that is participating in the network.

2.2 Biological Background

Motivated by the autonomously self-organizing nature of WANETs, biologically-inspired algorithms, such as ant colony optimization (ACO), appear well-suited. They have already been applied successfully in different network contexts such as data routing and distribution[**?**, 11]. Furthermore, based on the interesting phenomena of ants' behaviors, ant colony inspired security mechanisms can be derived[12]. In nature, each ant has a *Cuticular Hydrocarbon (CHC)* profile in which diverse information about the ant itself and its environment can be encoded[13, 4]. For example, as described in the original ACO algorithm, ants make use of pheromone to reinforce good paths between the nest and a food source and communicate via chemical substances to inform nest mates about these good paths. In addition to the use of pheromones for marking routes, auxiliary information is stored in an ant's CHC profile such as diet, genetics, and common nesting materials. As a result, ants from the same colony that share a certain diet have a similar CHC profile which enables them to identify the non-nest members. This latter idea will be seized in this work and transferred from the domain of biology to its application in device-to-device networks to identify foreign, illegitimate nodes in the network – in particular, Sybil nodes. While in previous works ants are normally defined as packages that are exchanged between network nodes, in this work a new point of view is considered in which an ant is defined as network node. For that reason, throughout this work the ant organism of a biological system and the communication network entity are used interchangeably. The exchanged messages between the nodes play the role of (chemical) communication signals between ants.

In the remainder of the paper we consider a more general notion of the CHC profile as *keying materials* when they are used as a mechanism for sharing identity information and will be subject to a diffusion process or more generally they will be subject to constraints inherent to diffusion including finite quantities, exchanges, decay rates, and creation rates.

2.3 Signaling Games

Games describe scenarios where a collection of agents interact strategically to select options to produce a utility optimizing outcome. An interesting subclass of games arises when agents have partial information concerning the options and utilities of other entities. Here we consider an important partial information game focused on identity deceptions, which we do by building upon prior empirical studies that elucidated dynamics of cyber security via signaling games ([2], [3]).

A *signaling game* describes a game between two players (agents) with incomplete information: a sender S and a receiver R. The sender is aware of their own type T (assigned by nature: cooperative or deceptive) and sends messages to

a receiver R. The receiver R, unaware of the sender's type, uses the received message to select an action leading to different payoffs depending on the outcomes of type, signal, and action. Classical signaling ([16] and [10]) introduced in language evolution and economics has been widely used in biology and computer science (see [15], [7], [8], [1], and [2]).

The signaling game scenario accounts for the possibility that a sender exploits their information-asymmetric advantage by sending signals that are "deceptive" and that elicit actions (of the receiver) that may not be beneficial. Signaling games provide a formal framework for considering the effects of deception in games; in particular, a zero-sum equity transferred from receiver to sender can emphasize a conflict between the agent utilities, which can motivate a deceptive signal as a strategy. Generally, deceptive games played among the agents in social-technological systems may describe agents exchanging various signals and forming decisions (of actions to take) with equities at risk.

3. PHYSICAL CONSTRAINTS

In communication networks, an identity management system is one of the important pillars of security provision. At its foundation, authentication and identity verification are absolutely fundamental. Authentication is the process which an entity (claimant) proves the possession of a certain identity property to another party (verifier). Based on the verification of the received proof, the verifier can take an authentication decision. Certificates issued by a central authority (CA) are commonly used in current implementations of identity management. From a biological point of view each ant posses a physical – i.e. not copyable –, but ephemeral (PE) profile as a subset of the CHC profile, which is used for the identification of an ant as part of a colony. To transfer the idea from the biology to the computer science domain, we make use of the idea of cryptocurrencies that can satisfy both criteria: on the one hand, crypto coins cannot be copied and on the other hand, a time stamp can be used to limit its temporal validity as crypto coins. In the context of this work we refer to modified crypto coins as *keying material*. Similar to biological ant colonies in which the queen of a colony plays an important role, we promote one of the network nodes to the position of queen having the special capability of generating new keying material and distributing it among the nodes in the network. In real ant colonies each organism is capable of affecting the environment by depositing scents, substances, and pheromones that experience diffusion and evaporation over time. Other colony members, who inhabit the same locations or encounter their peers directly, are affected as their own CHC profile may mix with ongoing diffusion processes. This diffusion-based process naturally contributes to a rich chemical signaling that can be used to verify an organism's status as nest mate vs. non-nest mate by verifying physically resident markers on organisms during encounters. Each time two ants of the same colony encounter each other keying material may be exchanged to support their membership to the same colony. If too little or no keying material is received, countermeasures can be initiated.

These basic mechanisms including physical constraints, diffusion and similarity enable us to design a biologically inspired, scalable authentication approach for WANETs, which are prone to Sybil attacks. We suggest a device capable of imposing constraints similar to that of the rich chemical signaling language in ant colonies, and use it to design mechanisms for signaling games. Because physical materials are used to establish signals of similarity, a strategically deceptive agent faces certain dilemmas and challenges. For example, when an agent wishes to fabricate an identity they will be burdened to either collect more materials or weaken their own signal of 'colony member' in order to support the fabricated identity's claim to 'colony member'. Using this mechanism we hope to explore this inherent risk/reward trade off for deceptive actions and identify parameters where it becomes particularly non-strategic to sustain deception campaigns.

3.1 Agent Based Diffusion Model

Particle diffusion, the underlying physical process for chemical concentrations, is central to a chemical signaling process leveraged in biological system for determining nest-mates (i.e., authentication). We develop an agent based diffusion model and build upon this to form authentication signaling games which feature various payoff outcomes and diffusion controls for agents. The interaction of agents, including the decisions and movement of agents, reinforce various gradients and concentrations of the chemical signaling providing a means for the formation of complex identity signaling strategies. We outline the physical of diffusion allowing agents to move and affect the transport of materials. The physical process informs our suggested bio-inspired authentication systems which incorporates a protocol constraining the communication to also include a diffusion process for keying material. In our experimental studies we further simplify and constrain a system but still observe a complex signaling system where agents may explore strategies for identity usage.

Our model will start with the standard second order partial differential equation for diffusion on a domain $x \in \Omega$:

$$\frac{\partial}{\partial t}\phi(t,x) = D(t,x)\Delta\phi(t,x),$$

whose classical and weak solutions with various boundary conditions (e.g., Dirichlet, Neumann, mixed) are well known. Moreover numerical solutions such as the methods finite differences, which discretize time and space, can be used to create *explicit* numerical schemes:

$$\Phi_{i,j+1} = \left(1 - \frac{\delta t}{(\delta x)^2}|\mathcal{N}_i|\right)\Phi_{i,j} + \left(\sum_{k\in\mathcal{N}_i}\frac{\delta t}{(\delta x)^2}\Phi_{k,j}\right)$$

where $\Phi_{i,j}$ is the approximate solution at discrete spatial position i and discrete time $t_0 + (\delta t)j$. The set $\mathcal{N}_i$ are the neighboring discrete spatial positions of position i. Further the Lax equivalence theorem applied to well poised problems provides an upper bound for $\frac{\delta t}{(\delta x)^2}$ for *convergence* or assurance that the solution of the discrete equation approaches the analytic solution in the limit as $(\delta t, \delta x) \to (0,0)$.

Letting $\frac{\delta t}{(\delta x)^2} = \epsilon$ be sufficiently small our discrete equation becomes:

$$\Phi_{\cdot,j+1} = L\Phi_{\cdot,j}$$

with L a bi-stochastic matrix whose entries describe symmetric material flux:

$$L_{ij} = \begin{cases} 1 - \epsilon|\mathcal{N}_i| \text{ if } i = j, \\ \epsilon \text{ if } j \in \mathcal{N}_i \\ 0 \text{ o.w.} \end{cases}$$

To generalize this to a setting of spatially arranged communicating nodes exchanging keying material we let e_{ij} be the amount of keying material which is transferred from node i to node j (assumed to be small ϵ). Therefore the diffusion in our system is defined by matrix L with:

$$L_{ij} = \begin{cases} 1 - \sum_{j \in \mathcal{N}_i} e_{ij} \text{ if } i = j, \\ e_{ij} \text{ o.w.} \end{cases}$$

4. IDENTITY SIGNALING GAMES

The simplest signaling game involving identity will focus on the possibility that during an encounter S, a sender node, may utilize a strategic deception by claiming either a fabricated identity or a malicious attempt to impersonate another node's identity. We will consider two natural types of nodes $\mathcal{T}_C$ and $\mathcal{T}_D$ to indicate respectively a *cooperative node* which employs no deceptions (preserving the desired system wide properties of identity management), and a *deceptive node* which directly employs a deception. In either case the node will, during an interaction, communicate a signal to a receiver node R including a status of c to indicate it is *cooperative* with respect to system security and a status of d to indicate *anomalous behavior* or *compromised status*. A receiver node R, given the signal of a sender node S but unaware of the sender node's true natural type, must select an action to take based on the information provided including S's disclosed status. One option for the receiver is to simply trust the sender node, denoted as t, alternatively the receiver node may pose a challenge action, denoted as a, which creates an attempt to reveal sender's nature and leads to costly outcomes for deception. While any individual challenge may not reveal completely the nature of a sender, repeated challenges will eventually expose Sybil identities due to the physical constraint of keying material imposed on the exchange.

We sketch the outcomes of an encounter scenario with an extensive-form game tree illustrated in figure 1. Starting in the center, the sender S has type $\mathcal{T}_C$ (cooperative) or $\mathcal{T}_D$ (deceptive). Next, the sender selects a signal c (cooperative) or d (otherwise); the receiver selects an action t (trust) or a (challenge).

We explore the essential outcomes and structure a challenge game with payoffs affecting both the utility and diffusion, these outcomes are summarized in table 1.

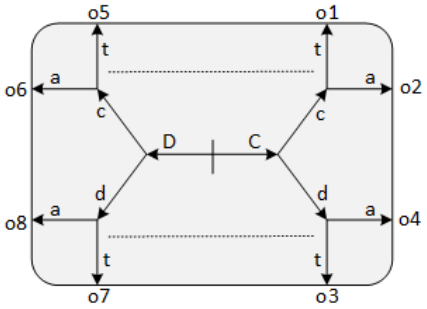


Figure 1: Interaction outcomes in node based identity signaling game.

4.1 Game Outcomes

In figure 1, the outcomes may be interpreted in the following ways: Outcome o_1 describes a sender S that is cooperative by nature and offers a nominal proof of identity to the receiver R. The receiver R, having received the nominal proof of identity trusts S and acts upon the information provided by S, for example relaying the communicated message. The receiver having selected a trusting option may also take an additional step to promote the colonies' decision toward acceptance of S, for example by reciprocating a nominal amount of keying materials. This exchange being symmetrical helps to strengthen a 'colony identity.'

Outcome o_2 describes a scenario similar to o_1 except the receiver R, having received the nominal proof of identity, challenges S to provide a more rigorous proof of identity. In this case, lacking a more rigorous proof of identity, the receiver may disregard the communicated message and implement controls (i.e., preventing diffusion) to affect the colonies' decision making in future games played against the sender S. In this case, given the cooperative nature of the sender, the challenge is unnecessarily punitive and adds costs to maintaining a trusted network.

Outcome o_3 describes a sender S that is cooperative by nature but is not willing or able to offer a nominal proof of identity to the receiver R. The receiver R nonetheless trusts S and may also take an additional step to promote the colonies' decision making toward acceptance of S, for example by offering colony keying materials. In this case the exchange is altruistic but helps to recover a trustworthy node in distress.

Outcome o_4 describes a sender S that is cooperative by nature but is not willing or able to offer a nominal proof of identity to the receiver R. The receiver R challenges S to provide a more rigorous proof of identity. In this case, given the cooperative nature of the distressed sender, the challenge adds costs to maintaining a trusted network.

On the other hand, the outcome o_7 describes a sender S that is deceptive and not willing or able to offer a nominal proof of identity to the receiver R. The receiver R nonetheless trusts S and acts upon the information provided and also promote the colonies' decision making toward acceptance of S. In this case the exchange being one-sided, and altruistic, only serves the interest of a deceptive Sybil node.

Outcome o_8 describes a sender S that is deceptive and not willing or able to offer a nominal proof of identity. The receiver R challenges S to provide a more rigorous proof of identity and prevents diffusion. In this case, given the deceptive nature of the sender, the challenge and actions of the receiver help to protect the trustworthiness of the colony.

Signaling games usually involve information constraints on the receiver, notice that without awareness of the sender's nature the receiver cannot distinguish outcome o_1 from o_6, nor can they distinguish o_3 from o_8. By selecting the checking action, the receiver with additional resource cost may distinguish outcomes o_2 from o_6, as well as distinguish outcomes o_4 from o_8. From the point of view of maintaining a trustworthy network, we summarize outcomes $\{o_1, o_3\}$ as naturally supporting the network, while $\{o_5, o_7\}$ are the most destructive to the network, outcomes $\{o_2, o_4\}$ add cost of challenging trustworthy nodes, and $\{o_6, o_7\}$ enhance the trust within a network by revealing risks.

To model these benefits and costs we propose the payoff structure with four parameters associated with game outcomes (table 1). We let A be the zero-sum equity trans-

Payoff (S, R), Transport of substance $(S \to R, S \leftarrow R)$					
Sender S		Receiver R	outcomes		
type	signal	action	label	payoff	$(\rightarrow, \leftarrow)$
$\mathcal{T}_C$	c	*trust*	o_1	(B, B)	(ϵ, ϵ)
		challenge	o_2	$(0, -C)$	$(\epsilon, 0)$
	d	*trust*	o_3	(B, B)	$(0, \epsilon)$
		challenge	o_4	$(0, -C)$	$(0, 0)$
$\mathcal{T}_D$	c	*trust*	o_5	$(A, -A)$	(ϵ, ϵ)
		challenge	o_6	$(-D, -C)$	$(\epsilon, 0)$
	d	*trust*	o_7	$(A, -A)$	$(0, \epsilon)$
		challenge	o_8	$(-D, -C)$	$(0, 0)$

Table 1: Payoff and transport for identity management signal game.

ferred in a Sybil attack, that is a benefit received by the sender at the loss of the trusting receiver. We let B be the benefit enjoyed by both sender and receiver nodes acting cooperatively in message passing. We let C be the cost of challenging a node for additional proof concerning its identity. Finally D is the imputed cost to the sender for being deceptive (identified by a receiver's challenge).

Similar to an ant's claim of colony membership we consider a node's statement of identity as a membership or trustworthiness claim to a particular trusted network. Each colony has its keying material and every node manages a finite but variable amount of material keyed to each colony.

In addition to communicating messages we propose that a network of nodes can also efficiently transfer keying material and that this transfer, subject to and limited by the decision making of nodes, gives rise to diffusion within trusted components of the network and this diffusion itself can also become a useful feature of a network's utility. In particular by reinforcing trust upon existing communication paths the process of diffusion may ease the global costs associated with persistently having to re-identify the adversarial and deceptive use of identities by particular nodes, once a node is marked (by a drifting profile or possibly even a more direct negative attribution) its nominal claims to identity, even when offered, may be rejected as a mismatch by the colony members.

4.2 Diffusion Similarity and Authentication

We will assume that in a domain $D \subset \mathbb{R}^n$ a set of nodes $A = \{a_1, a_2, \cdots, a_n\}$ operate. Each node has position $x_i \in D$ and are able to communicate with any nearby neighbor. In addition we will assume the existence of k distinct networks (colonies) with no natural requirement for separate networks to be cooperative, however each network will have a natural desire to maintain its own liveness, integrity and trustworthiness (i.e., prevent the possibility of degrading Sybil attacks on its nodes).

At each point in time, every node will maintain an amount of keying material from each network, represented by columns in the matrix:

$$W \in \mathbb{R}^{\geq}_{k \times n}.$$

We denote the profile of agent a_i with the i^{th} column of $W(t)$ as W_i. We will consider a_i to be from colony j if W_{ji} is the largest value in column W_i.

Letting $s, r \in \{1, 2, \cdots, n\}$ to denote the sender and receiver we describe the authentication procedure as a sequence of actions leading to a game outcome $\{o_1, \cdots o_8\}$, various payoffs and keying material transport.

The sender a_s wishes to pass a message m to a_r, the protocol is considered in four stages:

Stage 1: Nature determines Sender's type this information is known privately to the sender.

Stage 2: The sender selects a signal $\{c, d\}$, as a nominal proof to their identity (i.e., which colony they belong to). This identity signal is an offer χ (encoded as a vector $\mathbb{R}^k$), either equal to a fixed portion of their profile as $\langle \min(W_{js}, \epsilon) \rangle_{j=1}^k$ or $\bar{0}$ otherwise. The message and portion profile are sent as (m, χ) to the receiver a_r. The sender updates their profile quantities as:

$$W_s \leftarrow W_s - \chi.$$

Stage 3: The receiver obtains (m, χ) from the sender, and has a chance to downgrade χ to χ'. The possible downgrades will modify slightly the transport terms in table 1, and are intended to discount a signal that is not trusted or is out of band (i.e., from another colony). For example, if the receiver is a member of colony j and the sender is not, it will be unlikely that the j^{th} coordinate of χ will be a strong signal. In this case the receiver may naturally consider the message as routed to the wrong colony, and discard it causing destruction of the keying material and loss of message m. Another possible downgrade arises when the sender's portion χ includes a sufficient amount of a warning signal - an experiment involving attributing an alert keying material to a node.

Stage 4: The receiver a_r strategically selects an action from $\{challenge, trust\}$, based on the possibly downgraded signal sent χ' and prior interactions with a_s. If a_r selects *trust* as an option then they will accept the message and provide a fixed portion of their own profile as a counter offer $(\zeta = \langle \min(W_{jr}, \epsilon) \rangle_{j=1}^k)$ to the sender. Profiles are update as:

$$W_r \leftarrow W_r - \zeta + \chi',$$

and

$$W_s \leftarrow W_s + \zeta.$$

If, on the other hand, a_r selects to *challenge* they will not accept the message, not offer any of their own profile as a counter offer and destroy χ.

4.3 Repeated Games and Strategy

A repeated game form is needed to model node utilities (and strategies) that would select options based on revealed information and the previous history of revealed outcomes (with a given identity). To accommodate these considerations we encode the agent strategies for repeated games by using deterministic finite automata (DFA). For each identity encountered the strategy can maintain a token in the automata and use revealed information to advance the token to a next state which prescribes the next strategic play for that opponent. The DFA strategy space offers a vast space of strategies that agents may explore. Evolutionary games that provide a combination of strategic search and exploitation. We are particularly interested in the question of whether an agent is able to find a persistent means to exploit the population with deceptive strategies.

We illustrate a few strategies in figure 2.

A repeated game with r rounds is computed deterministically from a pair of strategies by determining a path of

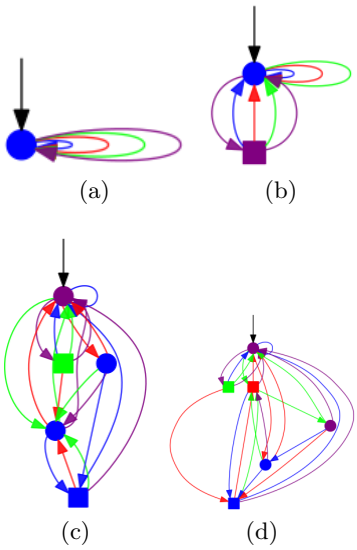


Figure 2: Agent strategies as deterministic finite automata (DFA). States describe a sender's nature, signal selection and a receivers' action.

state	shape and color	sender			receiver
		nature	send	rnd	action
1	circle blue	$\mathcal{T}_C$	c	1	*trust*
2	circle green	$\mathcal{T}_C$	c	1	*challenge*
3	circle purple	$\mathcal{T}_C$	d	1	*trust*
4	circle red	$\mathcal{T}_C$	d	1	*challenge*
5	square blue	$\mathcal{T}_D$	c	$\frac{1}{2}$	*trust*
6	square green	$\mathcal{T}_D$	c	$\frac{1}{2}$	*challenge*
7	square purple	$\mathcal{T}_C$	d	$\frac{1}{2}$	*trust*
8	square red	$\mathcal{T}_C$	d	$\frac{1}{2}$	*challenge*

Table 2: Strategy state coding.

length r within each DFA. To emulate the additional time and risk burden of controlling split personas in deceptive strategies we discount the play counter when a sender implements a deceptive state as only counting for half a round but carrying full payouts. A game sequence with r rounds may involve as many as $2r$ outcomes depending on the number of deceptive plays the sender expresses.

We enumerate the strategic states in table 2.

The outcomes of a single game depends on the states (i.e., selected options listed in 2) of a sender a_s and receiver a_r. The outcome matrix is:

$$O(a_s, a_r) = \begin{bmatrix} o_1 & o_2 & o_1 & o_2 & o_1 & o_2 & o_1 & o_2 \\ o_1 & o_2 & o_1 & o_2 & o_1 & o_2 & o_1 & o_2 \\ o_3 & o_4 & o_3 & o_4 & o_3 & o_4 & o_3 & o_4 \\ o_3 & o_4 & o_3 & o_4 & o_3 & o_4 & o_3 & o_4 \\ o_5 & o_6 & o_5 & o_6 & o_5 & o_6 & o_5 & o_6 \\ o_5 & o_6 & o_5 & o_6 & o_5 & o_6 & o_5 & o_6 \\ o_7 & o_8 & o_7 & o_8 & o_7 & o_8 & o_7 & o_8 \\ o_7 & o_8 & o_7 & o_8 & o_7 & o_8 & o_7 & o_8 \end{bmatrix}$$

The signaling game, having information asymmetries, will leave the receiver less than fully informed to the outcome, as mentioned before the receiver has no access the sender's nature. The common knowledge revealed from a game play is encoded as integers $\{1, 2, 3, 4\}$ and will depend also on the states (i.e., selected option listed in 2) of a sender s_s and receiver s_r. The common knowledge revealed is provided in matrix form as:

$$I(a_s, a_r) = \begin{bmatrix} 1 & 2 & 1 & 2 & 1 & 2 & 1 & 2 \\ 1 & 2 & 1 & 2 & 1 & 2 & 1 & 2 \\ 3 & 4 & 3 & 4 & 3 & 4 & 3 & 4 \\ 3 & 4 & 3 & 4 & 3 & 4 & 3 & 4 \\ 1 & 2 & 1 & 2 & 1 & 2 & 1 & 2 \\ 1 & 2 & 1 & 2 & 1 & 2 & 1 & 2 \\ 3 & 4 & 3 & 4 & 3 & 4 & 3 & 4 \\ 3 & 4 & 3 & 4 & 3 & 4 & 3 & 4 \end{bmatrix}$$

Letting $c = 0$, we can compute the outcome sequence of a multi stage game between a given sender and receiver playing with C rounds. To compute the outcome sequence of length in $[C, 2C]$ for an encounter, we use the following update function:

Update function:
input: sender and receiver strategy, lower sequence length C.
initalize: Use black arrows to determine start states: s_s and s_r, place token t_r on s_s and t_s on s_r.
loop: until $c > C$:
outcome: PRINT $O(s_s, s_r)$
increment: $c \leftarrow \begin{cases} c+1 \text{ if } s_s \in \{1,2,3,4\} \\ c+\frac{1}{2} \text{ o.w. (overburden)} \end{cases}$
revelation: $q \leftarrow I(s_s, s_r)$
transition: $p = \begin{cases} blue \text{ if } q = 1; green \text{ if } q = 2 \\ purple \text{ if } q = 3; red \text{ if } q = 4 \end{cases}$
shift states: Useing arrow p:
from token t_r to update state s_s
from token t_s to update state s_r
advance: Move t_r to state s_s, and t_s to state s_r.

For each opponent a state token can be maintained, within the strategy graph, to support asynchronous updates in multi-stage games with more than one opponent (i.e., more than one encounter occurring simultaneously).

5. SIMULATIONS

To consider a network systems of nodes with our proposed identity management system we develop an evolutionary game system which evolves agent strategies allowing them to develop and exploit deceptive or Sybil identities in an environment of partially informed identity information. The dynamic system we outline is a stochastic process acting on the distribution of all strategic species for the repeated identity management signaling game. This stochastic process allows the agents to explore, learn and exploit utility concepts within an environment of other non-cooperative strategies. We outline the system by defining some of the system parameters and summarize a general simulation framework, which we use in experiments.

The *shape parameters* describe the size of the simulation in the number of nodes n, the number of networks K, the mathematical domain D (and its discretization parameters), the number of generations simulated I. In our simulations the domain D will be a torus described by DX, DY for measure of width and height and NX, MY describing the number of equally spaced lattice positions dividing DX and DY

respectively[1]. We denote the shape parameters as $\Theta_1 = \langle n, K, D, I\rangle$.

Each generation is a fixed interval of time where agents may implement strategies. During each generation, agents will encounter each other to play repeated games using selected strategies (remaining constant throughout all encounters during the generation). The encounters are generated as a randomized ordered list of sender/receiver pairs over the set of all possible senders and receivers. We refer its distribution as the *encounter distribution*. When two agents encounter, a geometric distribution (with continuation parameter δ) is used to generate a lower bound for the length of outcome sequence as C. This can be thought of as a signaling frequency among agents as number of messages exchanged per generation. With the value C, an outcome sequence is generated using the DFA update function specified earlier. The DFA tokens, which identify the state of play against specific players, clarify that the messages may be communicated asynchronously and the essential games played are between strategies. This decision making process, as a strategy, is capable of learning identity attributes of the profiles it encounters – however lacking variation of profiles or experience with players it should view all opponents as equals. We denote the encounter parameters as $\Theta_2 = \langle \rho, \delta\rangle$, and because they will most closely reflect network architectures in the sense of who talks to who and how much, we refer to them as *network architecture parameters*.

For each encounter the strategies (of agents) play repeated games and the outcomes of these games are payoff and substance transport parameterized by *game parameters*: $\Theta_3 = \langle A, B, C, D, \epsilon\rangle$.

To model strategic exploration by agents within the space of all strategies we introduce parameters, μ a base rate of mutation and probability vector $\bar{m} = (m_1, m_2, m_3, m_4)$ which prescribe mutation operations. Mutation operations are: 1) add a state, 2) delete a state (if possible), 3) change a state's option, and 4) change an edges destination

The exploration parameters keeps all strategies 'live,' in the sense that a mutation pathway exists from each strategy to every other strategy with some positive probability, and this is particularly useful for exploring mutants which go from being cooperative to deceptive or vice versa. We denote the exploration parameters with $\Theta_4 = \langle \mu, \bar{m}\rangle$.

Finally we indicate the dynamic quantities of state for agents as variables, for example $s_{i,t}$ may identify the strategy implemented by agent i in generation t. Further each agent will maintain a dynamic profile $\langle W_i\rangle_{i=1}^n$ of keying material. This profile vector will vary within a generation depending on sender offers, receiver downgrades, and counter-offers. The profile vector will identify its strongest claim of identity with its dominant non-zero entry. In addition each agent will maintain a position on the domain $x_i \in D$.

We outline a general simulation framework augmented for focused examination of agents by their properties. For example we will focus our attention on nodes which implement deceptive signaling (i.e., Sybil identities), and attempt to understand how well they may do when they encounter clean strategies that share information concerning best defenses.

[1]In a torus, the boundary of the rectangle DX, DY is *wrapped*, meaning that the points of the plain $(x+nDX, y+mDY)$ are identified with (x, y) for all integers n, m.

Given parameters for shape, network architecture, games, and exploration as: $\Theta_1, \Theta_2, \Theta_3, \Theta_4$. And given a property for nodes labeled P.

Initialize: A population of n nodes are initialized with a basic or random strategy.
Loop: For each generation. Let S_j is the subset of nodes belong to colony j.

- **Distribute keys:** Each node of S_j receives new material keyed to a colony identity.
- **Property Split:** Let $S_j^P \subset S_j$ be a subset of nodes which satisfy a given property e.g. be the subset of nodes which utilize deceptive strategies for sending messages (i.e., a Sybil Identity)
- **Encounter:** Using parameters Θ_2 we generate an ordered list of encounters for game play between sender and receiver nodes.
  - **Play:** For each encounter: repeated games are played by agent strategies using parameters Θ_3. Payoffs are recorded and diffusion executed during games according to the stages specified in authentication procedure.
- **Aggregation**: Strategies are measured in aggregate over all plays of a generation (total payoff).
- **Re-create**: For each colony j, the aggregate measures over S_j are used to re-create a population for the next generation.
- **Mutate**: Players are chosen randomly with rate μ for mutation. Each mutation event may modify the strategic nature of a node but allows the population to explore the strategy space.

The simulation model includes a large class of processes, however in our initial experiments we will present several model simplifications. Note that network architecture parameters Θ_2 are possible to observe or estimate in many network applications and this fact offers the system designer some choices in game parameters Θ_3 that may have desirable effects toward curtailing the use of deception. For example because Sybil states in a sender's strategy employ additional efforts and introduce additional risk (and this is added to our model by counting each deceptive send as only half a round), we select a value of ϵ which is capable of causing Sybil identities, facing sufficient number of challenges significant difficulty in providing nominal proofs of identity.

Simplifications: In our studies and experiments presented here we will restrict the positions of nodes to the discrete lattice positions of a torus D, and hold node positions constant throughout the entire history of simulations. We will place a single node at each lattice position of the torus. This choice introduces an unnecessary relation between the number of nodes and the domain discretization but still suffices to provide many observations of interest such as how will strategies adapt when they are at the colony boundary vs. its interior. We will simulate multiple colonies and each colony will occupy a band in the torus, so for K colonies, colony j will be constructed from nodes found in positions $\{(x, y) : \textsc{Floor}(\frac{x}{DX}K) = j\}$. We will simplify our encounter distribution by using these fixed positions on a torus. During a generation each node will encounter each of its nearest neighbor once as a sender and once as a receiver. In most ad hoc networks the order of communication will include randomizing factors, so we will pseudo randomize the ordering of encounters, and this should prevent strategies

from possibly learning and exploiting features arising from ordering.

Re-create by boosting: During the *Re-create* phase strategic agents may attempt to increase performance (in subsequent generations) by changing a strategy, this reflects a process where agents may learn from experience and information revealed at longer timescale - for example having concluded a generation of games, agents may observe which strategies perform well given the current environment. We typically employ a boosting re-selector that preferentially prefers strategies that do well in the prior environment. We describe the boosting re-selector with a single parameter ξ which we generally set to a value around $\frac{1}{n}$.

Fixing a subset of agents S, at the conclusion of a generation we let v_i be the performance measure for strategy utilized by agents $a_i \in S$. Letting $v_* = \min_{i \in S}\{v_i\}$ and $v^* = \max_{i \in S}\{v_i\}$ we can safely transfer the performance measures to the interval $[0, 1]$ as the limit of linear fractional transformation:

$$V_i^{\xi} = \lim_{\eta \to 0^+} \frac{v_j + (\xi - v_*)}{v^* - (v_* - \eta)}$$

The term η simply prevents division by zero, the term ξ is a *statistical shrinkage* term and is used as a model parameter which helps to distort the clarity of global information available to agents when they reselect a strategy – for example a worst performing strategy may remain live in a next generation of play. We describe the probability that agent $i \in S$ will switch over to using the strategy which agent $j \in S$ previously implemented as:

$$\frac{V_j^{\xi}}{\sum_{k \in S} V_k^{\xi}}$$

The *boosting distribution* for S will therefore reselect a population of $|S|$ strategies as Multinomial $\left(|S|, \langle \frac{V_j^{\xi}}{\sum_{k \in S} V_k^{\xi}} \rangle_{j \in S}\right)$. Overall the boosting distribution acts to guide the set's strategic selection and preferentially selects strategies that perform better in the current environment. We may consider the sets over which the boosting is applied to be a grouping of agents where information sharing occurs: perhaps globally, at the colony level, or limited to an individual. It is also possible that information asymmetric flows may arise and we will be explore this notion in our experiments. In our experiments we specify each performance measure and the re-create selector implemented. The re-create selector will generally be based on performance measures considering factors of payoff from repeated games and properties of an agent's profile where colony loyalty or indicators of deception (imputed from costly checking) may be examined.

6. EXPERIMENTS

In this section we design simulation experiments to investigate the robustness features of a network constructed with our identity management mechanism. The experiments allow agents to naturally explore (via mutation) deceptive utilities (i.e., employing Sybil identities), but ultimately aims to understand their characteristics such as persistence and ability to exploit cooperative networks and at what costs.

In each experiments we shall explore our suggested mechanism for identity management for a system of communicating network nodes (with $n = 800$) divided into two colonies ($K = 2$) with the simplifications previously mentioned. We will further begin the simulations from a start state where all nodes are cooperative and there are no nodes employing (immediately) deceptive or Sybil identities. From these initial conditions mutation will allow nodes to quickly use deceptive strategies and test their efficacy. While these game systems give rise to complex dynamics we will summarize high level network behaviors in summary statistics from the viewpoint of an omniscient oracle.

Our experiments are performed as a set of closely related systems varying slightly in controls and pseudo-random generator seed value. We simulate a history and report the observed behavioral statistics.

Major Control – The Cooperative group benefit package Our major control in experiments examines how differing re-creation constraints for cooperative vs deceptive utilities lead to differing qualitative behavior outcomes. To do so, we construct two systems, both will feature competitive pressure for agents to optimizing strategies and explore with mutations.

In the first system agents S_0, agents will select strategies based on performance in previous rounds whether they employ deception or not. In this system each agent boosts individually and identically considering all strategies as in play treating cooperative and deceptive strategies alike, simply to increase performance measures which become the driver for re-selection of strategy.

In the second system of agents S_1, agents will have differing re-selection criteria depending on whether they employ deception or not. The property P will qualify the cooperative strategies. The cooperative nodes will share information collaboratively to address deception (as it may manifest) in a colony population; on the other hand the deceptive strategies will rely on mutation to find effective niches in the environment. Agents may select strategies using a common database of clean strategies and their performance measures, however once an agent implements a deceptive strategy the database is of little use so they are essentially on their own to develop an efficient use. Moreover when a deceptive strategy is performing poorly (for example less than the cooperative group average) then they abandoning a deceptive strategy as being non-productive and come clean by re-selecting strategies from the shared database as the best survival option. We specify this second system as one that constructs a *cooperative group benefit package* in the form of a shared database of strategies and their performances.

Minor Control – The performance measure. In addition to the major control we explore differing performance measures relevant to maintaining a cooperative network of nodes. These experiments explore reselection in both system S_0 and S_1 by using a variety of performance measures for boosting, the consideration for performance will be:

i Aggregate payoffs from games of a generation.

ii Strength of colony identity in the exchanged keying material.

iii Avoidance of an alert keying material.

The aggregate payoffs from games are the typical consideration applied in evolutionary game systems. Applied to S_0 we consider a system $S_{0.1}$ where the node utilities are guided by individual payoff optimization in games alone. When applied to S_1 we consider system $S_{1.1}$ where the information for

re-selection remains focused on clean strategies. The nodes satisfying the property P are trustworthy and will not select a deceptive strategy even when it outperforms trustworthy strategies. We assume that the deceptive nodes would naturally deny reporting their true payoffs as it may jeopardize their private information. While trustworthy nodes do not re-create deceptive strategies they may still explore their application via the mutation. In this system when a deceptive strategy is formed the node will construct information controls to keep its strategy and performance measure as 'private information.'

The second consideration (ii) will focus performance measure on the strength of a colonies identity. From S_0 and S_1 we derive systems $S_{0.2}$ and $S_{1.2}$. Our performance measure will be defined by an inner product with an idealized colony vector. Recalling that the authentication process will prevent diffusion when a receiver employs a *challenge* and further that a deceptive strategy may incur extra rounds, the deception places an agent's profile (strength of a colonies identity) at risk when encountering multiple receivers who are willing to challenge.

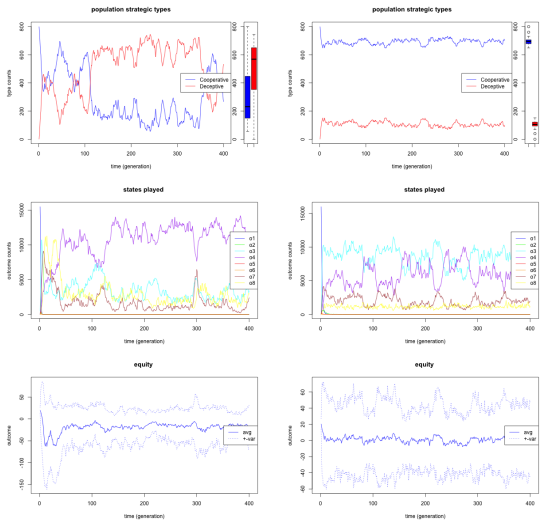
The third consideration (iii) focuses on the strength of a repulsion signal. In order to create this experiment several augmentations are necessary. Similar to W we consider a second channel used by each colony to mark deceptive agents $\tilde{W}$ (a matrix equal in size to W but having keying material indicate possible deceptive behavior). We consider these augmentations to S_0, S_1 as systems $S_{0.3}, S_{1.3}$. Our performance measure will be inverse to an inner product of an agent's column in $\tilde{W}$ with the colonies ideal alert vector. We implement this by using another profile matrix $\tilde{W}$ identical in size to W but initialized to zero during the *distribute keys* stage of the simulation. When a cooperative receiver identifies a case of deception (via a challenge) a fixed amount β is added into the sender's column of $\tilde{W}$ (in the row identified by receiver's colony) as an alert signal imputed by the receiver. The alert signal may be interpretable by any cohort in the receiver's colony as a mark of deceptive type. However, noting prevents deceptive nodes from utilizing the same technique to disrupt the colonies decision system. To account for this adversarial possibility we augment slightly the strategic encoding for receiver strategies to allow a 'false accusation.' This augmentation can be done within the existing strategy codes, and involves re-encoding the receiver's actions as a function of state. We do this by triggering a 'false accusation' if the strategy state is in $\{5, \cdots, 8\}$. A false accusation will count as a full round reflecting the ease at which the operation can be done. This new feature gives rise to an entirely new use of non cooperative behaviors by allowing nodes to attack and degrade the alert system itself.

We set shape parameters to $\langle 800, 2, D, 400\rangle$, with D a torus with $[DX, DY] = [2.0, 1.0], [NX, NY] = [40, 20]$ and encounter parameters $\delta = 0.8$, game parameters to $\langle 4, 0.5, 0.5, 4.0, 0.02\rangle$, and mutation rates are $\mu = 0.2$, with $\bar{m} = [0.12, 0.10, 0.39, 0.39]$.

Below in figure 5 we show simulation traces for systems $S_{0.1}$ and $S_{0.2}$

7. CONCLUSIONS AND FUTURE WORK

This paper presents a bio-inspired systems for identity management and authorization by considering a novel point of view in that the network nodes themselves may be considered the strategically agents interacting with one another.



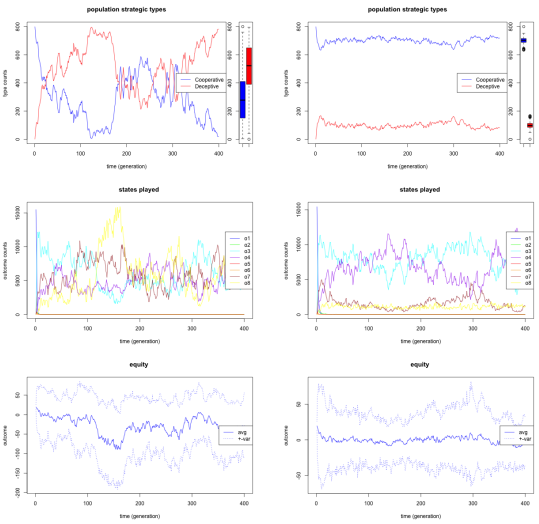
(a) (b)

Figure 3: Simulation traces for system $S_{0.1}$ in (a) and $S_{1.1}$ in (b).

The exchange of messages and keying material between nodes are constrained to act in a similar ways to chemical diffusion, but changes the dynamics by making the signaling potentially costly (with credible threats). This system specified in protocol and games sets the stage for a complex signaling system which formally includes the possibility that deceptive strategies may employ Sybil identities. We develop an agent based diffusion model and build upon this to form authentication-signaling games that feature various payoff outcomes and diffusion controls for agents. We construct a network of non-cooperative nodes and study their strategy optimization by using evolutionary games. The approach leads directly to simulation based optimization and mechanism design, leading to experiments, where it is possible to explore how a cooperative group-benefit-package may deter the early success of deceptive strategies. Our experiments indicate that the cooperative group benefit package strongly deters deception and further considers variations on how performance measures can be considered. Our future work includes further study of identity, and agents identity decisions subject to physical and biological processes constraints. Our next phase of work will incorporate mobile nodes and consideration of self adaptive devices.

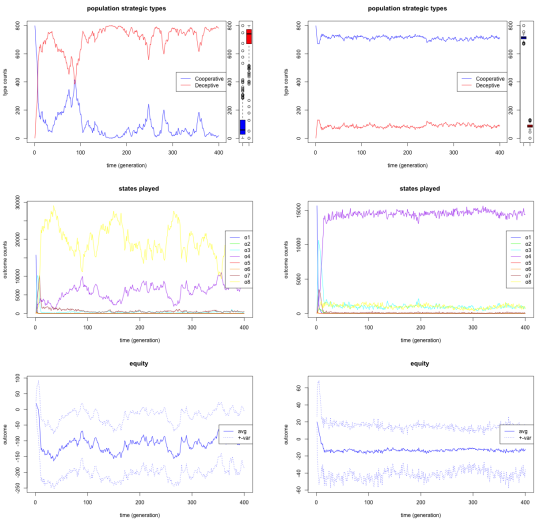
8. ACKNOWLEDGEMENTS

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center. This material has been approved for public release and unlimited distribution. DM-0002919



(a) (b)

Figure 5: Simulation traces for system $S_{0.3}$ in (a) and $S_{1.3}$ in (b).



(a) (b)

Figure 4: Simulation traces for system $S_{0.2}$ in (a) and $S_{1.2}$ in (b).

9. REFERENCES

[1] K. Binmore and L. Samuelson. Evolution and mixed strategies. *Games and Economic Behavior*, 34(2):200–226, 2001.

[2] W. Casey, J. A. Morales, T. Nguyen, J. Spring, R. Weaver, E. Wright, L. Metcalf, and B. Mishra. Cyber security via signaling games: Toward a science of cyber security. In *ICDCIT*, pages 34–42, 2014.

[3] W. Casey, R. Weaver, L. Metcalf, J. A. Morales, E. Wright, and B. Mishra. Cyber security via minority games with epistatic signaling: Invited paper. In *Proceedings of the 8th International Conference on Bioinspired Information and Communications Technologies*, BICT '14, pages 133–140, ICST, Brussels, Belgium, Belgium, 2014. ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering).

[4] H. Chung and S. B. Carroll. Wax, sex and the origin of species: Dual roles of insect cuticular hydrocarbons in adaptation and mating. *BioEssays*, 2015.

[5] L. Da Xu, W. He, and S. Li. Internet of things in industries: A survey. *Industrial Informatics, IEEE Transactions on*, 10(4):2233–2243, 2014.

[6] J. R. Douceur. The sybil attack. In *Peer-to-peer Systems*, pages 251–260. Springer, 2002.

[7] S. M. Huttegger and B. Skyrms. Emergence of information transfer by inductive learning. *Studia Logica*, 89(2):237–256, 2008.

[8] S. M. Huttegger, B. Skyrms, R. Smead, and K. J. Zollman. Evolutionary dynamics of lewis signaling games: signaling systems vs. partial pooling. *Synthese*, 172(1):177–191, 2010.

[9] R. John, J. P. Cherian, and J. J. Kizhakkethottam. A survey of techniques to prevent sybil attacks. In *Soft-Computing and Networks Security (ICSNS), 2015 International Conference on*, pages 1–6. IEEE, 2015.

[10] D. Lewis. *Convention: A philosophical study*. John Wiley & Sons, 2008.

[11] T. L. Lin, Y. S. Chen, and H. Y. Chang. Performance evaluations of an ant colony optimization routing algorithm for wireless sensor networks. In *Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP), 2014 Tenth International Conference on*, pages 690–693. IEEE, 2014.

[12] P. Memarmoshrefi, H. Zhang, and D. Hogrefe. Social insect-based sybil attack detection in mobile ad-hoc networks. In *Proceedings of the 8th International Conference on Bioinspired Information and Communications Technologies*, BICT '14, pages 141–148, ICST, Brussels, Belgium, Belgium, 2014. ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering).

[13] K. R. Sharma, B. L. Enzmann, Y. Schmidt, D. Moore, G. R. Jones, J. Parker, S. L. Berger, D. Reinberg, L. J. Zwiebel, B. Breit, et al. Cuticular hydrocarbon pheromones for social behavior and their coding in the ant antenna. *Cell reports*, 12(8):1261–1271, 2015.

[14] Y. Singh et al. A study on efficient defense mechanism against sybil attack in wsn. *International Journal for Innovative Research in Science and Technology*, 2(1):289–295, 2015.

[15] B. Skyrms. *Signals: Evolution, learning, and information*. Oxford University Press, 2010.

[16] M. Spence. Job market signaling. *The quarterly journal of Economics*, pages 355–374, 1973.

[17] C.-W. Tsai, C.-F. Lai, and A. V. Vasilakos. Future internet of things: open issues and challenges. *Wireless Networks*, 20(8):2201–2217, 2014.

[18] A. Zanella, N. Bui, A. Castellani, L. Vangelista, and M. Zorzi. Internet of things for smart cities. *Internet of Things Journal, IEEE*, 1(1):22–32, 2014.