An Epistemic Logic Based Framework for Reasoning About Information Hiding

– summary –

Iulian Goriac

Supervisor: Prof. Ferucio Laurenţiu Ţiplea Ph.D.

Introduction

The purpose of our research is the compilation of a fundamental theoretical framework theoretical framework to be used for formally defining the information security concepts.

There are two main sources the theory presented here is based upon. The first is represented by Pfitzmann and Hansen's consolidated proposal that provides formal definitions for the main concepts in information security. The second is a formal multi-agent systems based theory initially used by Halpern and O'Neill for defining anonymity and later used by Tsukada *et. al.* in order to extend the set of formal definitions. The literature that deals with formalising security protocols is significantly broader.

The thesis is divided in three sections. The first one compiles an epistemic logic that extend the one developed by Halpern and O'Neill. The second provides a means of quantifying the definitions for security properties via plausibilistic entropy. The last indexes the

qualitative and quantitative definitions for the formalised security properties.

1 Qualitative Approach

1.1 Entities

The fundamental entities that we use are the multi-agent systems (MAS), the protocols, the runs, and the points that are next to be introduced:

Definition 1.1 (MAS)**.** *An* multi-agent system *is a triple*

$$\mathcal{S} = (Ag, G, Act)$$

with:

$Ag = \{A_1, A_2, \ldots, A_n\}$ *is a non-empty finite set of* agents*, capable of storing and processing information. All the information and agent A has access to at a certain moment is stored in its* local state*, $l_A \in L_A$, where L_A is the set of all the states agent A can have. Occasionally it is useful to consider the* environment*, E, to be a special agent in Ag, in which case all the other agents are* regular agents*;*

$G = L_{A_1} \times L_{A_2} \times \cdots \times L_{A_n}$ *is the set of all the global states of the system. Any $g = (l_{A_1}, l_{A_2}, \ldots, l_{A_n}) \in G$ is a* global state *that tuples all the local states of the agents in Ag at a certain moment;*

$Act = \{a_1, a_2, \ldots\}$ *is a set of* actions*. Actions are initiated by the agents and are defined by the changes they introduce in the global state of the system. Act_A is the set of actions that can be performed by agent A. Obviously $Act_A \subseteq Act$ for all $A \in Ag$.*

Definition 1.2 (protocol)**.** *A* protocol *for agent A in a MAS $\mathcal{S}$ is a function $P_A : L_A \to 2^{Act_A}$ defining the set of actions that an agent can take from any of its local states.*

If such is the case that every local state allows one and only one action to be executed by the agent then the protocol is deterministic.

Definition 1.3 (run)**.** *An* run *is a function $r : T \to G$ defined over a set, T, that we call time over the set of the global states of an agent.*

Definition 1.4 (point)**.** *If r is a run and m an element in T then a* point *is a pair (r, m). Every point corresponds to a global state $r(m) = g \in G$. By $r_x(m) = l_{A_x} \in L_{A_x}$ we refer to the x indexed component of the global state $r(m)$.*

If R is a non-empty set of runs then by $\wp(R)$ we identify the set of all the points in R.

1.1.1 Local State Structure

Our approach is that the local state of an agent is created by *representations* and *determiners*. The representations encode relations about the environment the agent evolves in thua allowing it to reason about its current context. Representation examples could be: "message m was transmitted" or "the authentication was successful". As we will be able to see the representations can be further structured in formulas with various interpretations. Depending on the interpretations an agent assigns to formulas it can take different actions. The determiners are nothing but the rules the agents use that allow the association between the local states of the agents and the actions they initiate.

1.2 An Epistemic Logic

1.2.1 Syntax

The concepts introduced so far allow us to introduce the *syntax* of an epistemic logic over the local state of an agent. The syntax is recursively defined over a set Φ of representations belonging, ultimately, to the system and a set of connectors: negation ($\neg$) and

conjunction ($\wedge$), modal operator for knowledge (K), and also group modal operators everybody knows (E), common knowledge (C) and distributed knowledge (D). For specifying precedence parentheses will be used.

Definition 1.5 (syntax)**.** *If Φ is a set of representations then the set of* formulas *that can be defined over it is recursively defined by using the following rules:*

1. *if $p \in \Phi$ then p is a formula;*
2. *if φ is a formula then (φ) is a formula;*
3. *if φ is a formula then $\neg\varphi$ is a formula;*
4. *if φ and ψ are formulas then $\varphi \wedge \psi$ is a formula;*
5. *if φ is a formula then $K_A[\varphi]$ is a formula;*
6. *if φ is a formula then $E_A[\varphi]$ is a formula;*
7. *if φ is a formula then $C_A[\varphi]$ is a formula;*
8. *if φ is a formula then $D_A[\varphi]$ is a formula.*

$A \in Ag$ is a symbol identifying an agent and $G \in 2^{Ag}$ is a symbol identifying a group of agents.

1.2.2 Semantics

Definition 1.6 (interpreted system)**.** *An* interpreted system *is a tuple $\mathcal{I} = (\mathcal{S}, \mathcal{P}, R, \pi)$ with $\mathcal{S}$, $\mathcal{P}$ and R having the previously defined meanings and π is a point dependent interpretation associating truth values to all the representations $p \in \Phi$ in the system: $(\pi(r, m))(p) \in \{true, false\}$.*

Definition 1.7 (truth values for formulas)**.** *Given the interpreted system $\mathcal{I}$ and G a group of agents, the truth value of a formula φ in point (r, m) is recursively defined in the following way:*

1. $(\mathcal{I}, r, m) \models p$ iff $(\pi(r, m))(p) = true$
2. $(\mathcal{I}, r, m) \models \neg\varphi$ iff $(\mathcal{I}, r, m) \not\models \varphi$
3. $(\mathcal{I}, r, m) \models \varphi \wedge \psi$ iff $(\mathcal{I}, r, m) \models \varphi$ and $(\mathcal{I}, r, m) \models \psi$
4. $(\mathcal{I}, r, m) \models K_A[\varphi]$
   iff $(\mathcal{I}, r', m') \models \varphi$ for all $(r', m') \in \mathcal{K}_A(r, m)$
5. $(\mathcal{I}, r, m) \models E_G[\varphi]$
   iff $(\mathcal{I}, r', m') \models \varphi$ for all $(r', m') \in \bigcup_{A \in G} \mathcal{K}_A(r, m)$
6. $(\mathcal{I}, r, m) \models C_G[\varphi]$ iff $(\mathcal{I}, r, m) \models E_G[E_G[\cdots E_G[\varphi] \cdots]]$
7. $(\mathcal{I}, r, m) \models D_G[\varphi]$
   iff $(\mathcal{I}, r', m') \models \varphi$ for all $(r', m') \in \bigcap_{A \in G} \mathcal{K}_A(r, m)$

The meaning of the $\mathcal{K}_A(r, m)$ notation is that of specifying a set of states accessible to the agent starting from a certain local state. Even more, our approach is based on the fact that over the local states of an agent an equivalence relation can be defined, whose nature will be discussed later in the chapter.

1.2.3 Local State Structure *(cont.)*

The first thing to be discussed is the nature of the π-interpretations. We are considering two types of π-interpretations: κ ad β. The κ-interpretations are decided at the system level and their truth value is absolute. They correspond to the *validity* of the representations. The β-interpretations are truth values chosen by the agents for the representations in theis local states. β-interpretations correspond to the agent related *truth* of the interpretations.

The evolution of the agents and, implicitly, of the system they define exclusively depends on the actions they take. Without a causal relation between the local state of an agent and its behaviour there

will be no point in studying the local state. Therefore, our premiss is that the representations the agents have are essential in our approach.

As previously discussed, the representations can be grouped to build formulas to which the agents can assign truth values. We consider that the agent interpreted formulas are used by the agents in selecting the actions they take.

Essentially, an action a is defined by the set of changes that it introduces in the representations of the system between two points. For simplicity, we will consider that only agents can initiate actions and that any action is associated to an agent.

Definition 1.8 (action determination)**.** *Given an action a and a formula φ, we use $\theta(\varphi, a)$ to note that the set of changes introduced by a* may be operated *between two points $p_1 = (r, m_1)$ and $p_2 = (r, m_2)$ of the same execution if and only if the formula φ is evaluated by an agent to be true in point p_1. $\theta(\varphi, a)$ is a* determiner *of action a.*

A dichotomic classification of the actions divides them in *internal* and *external*.

Definition 1.9 (external and internal actions)**.** *An action is* internal *if it changes the local state of the agent that initiated it and* external *if it changes the local state of at least another agent. By state change we understand any modification that appears in the structure of the representations of an agent or the interpretations it associates to these representations.*

Pragmatic-wise, the main factor that differentiates the two types of actions is the *cost*. Thus, it is considered that internal actions have a significantly lower (negligible even) compared to the external actions. To adopt an efficient behaviour, the agent will prefer operating internally until obtaining a formula to be used for acting externally.

Depending on the type of associated interpretation and the type of action the formulas can be categorised as: beliefs, knowledge, hy-

potheses, convictions, and certainties. Thus *beliefs* are β-interpreted formulas based on which the agent decides to act while knowledge are κ-interpreted formulas. The *hypotheses* are formulas an agent bases its strictly internal actions while *convictions* are formulas used to determine external actions. Finally the *certainties* are beliefs for β and κ interpretations are identical and therefore, every time the agent acts on them the expected result is guaranteed.

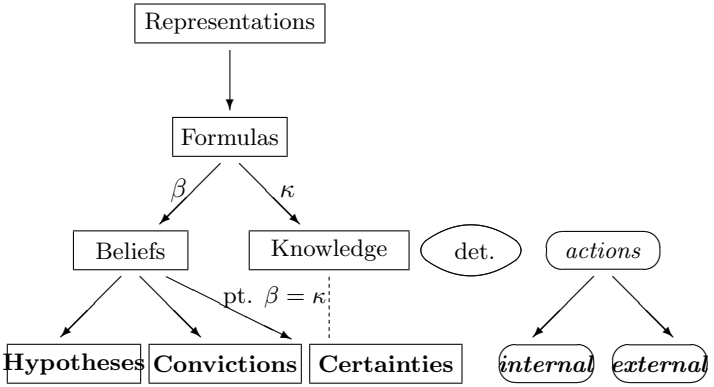


Figure 1: The structure of the local state of an agent

By this approach we suggest a way of dealing with the logical omniscience problem in modelling cryptographic protocols. If the cost associated to inference is not taken into consideration then we can consider that an agent has instantaneous access to all the logically deduced consequences based on its local state. This approach is not realistic since many cryptographic primitives are based exactly on the cost of computation. By introducing definitions for bounded equivalence between local states our approach allows the modelling of this aspect.

1.2.4 Local State Equivalence

If we think of all the points of an MAS we realise that we cannot always bijectively map the global states of the system to every local state. It is possible, for instance, that an agent A had the same local state in two or more different global states. Since A only has access to its local state it will be impossible to differentiate between the aforementioned local states thus considering both of them to be possible. The two states will be *indistinguishable* for agent A.

Definition 1.10 (indistinguishability [10])**.** *Given $\mathcal{S}$ an MAS with a protocol $\mathcal{P}$, a set of runs R, an agent A and a point (r, m), the set of all the points in $\wp(R)$ that A thinks that are possible in (r, m) is*

$$\mathcal{K}_A(r, m) = \{(r', m') \in \wp(R) \mid r_A(m) = r'_A(m')\}$$

an be referred to as the agent information set*.*
Two points are indistinguishable *for agent A if they both belong to the same agent information set $\mathcal{K}_A(r, m)$. We will also use $(r, m) \sim_A (r', m')$ to symbolise this.*

In the current form, the equality is not unambiguously defined. In the following we present two approaches for defining the equivalence of the local states and also dome implications.

Definition 1.11 (extrospective equivalence)**.** *Given $\mathcal{S}$ an MAS with a protocol $\mathcal{P}$, two local states $l_1, l_2 \in L_A$ belonging to the same agent A are* extrospectively equivalent*, $l_1 \equiv_{ext} l_2$, if the following two properties are satisfied:*

- $P_A(l_1) = P_A(l_2)$*;*
- *if l'_1 and l'_2 are reached from l_1 and l_2 respectively by taking identical sequences of external actions then $P_A(l'_1) = P_A(l'_2)$.*

$P_A(l)$ is limited to external actions only.

Observaie: We call this equivalence *extrospective* because it takes into consideration only the agent's behaviour that is 'visible' by another agent – only the actions that are capable of changing some other agent's state. Intuitively, if two local states lead to identical sequences of actions the the two states are equivalent.

Definition 1.12 (introspective equivalence)**.** *Given $\mathcal{S}$ an MAS with a set of runs R, we say that two local states $l_1, l_2 \in L_A$ belonging to the same agent A are* introspectively equivalent*, $l_1 \equiv_{int} l_2$, if the following two properties are satisfied:*

- $(\forall\, \varphi)\ \varphi \in det(l_1) \Leftrightarrow \varphi \in det(l_2)$*;*
- $(\forall \varphi)\ l_1 \models \varphi$ iff $l_2 \models \varphi$*.*

Only β-interpretations are considered in this definition. $det(l)$ identifies the set of determiners (Definition 1.8) contained in the local state l.

Observaie: We call this equivalence *introspective* because it only takes into consideration the information available to the agent. Usually only the agent itself has access to this kind of information.

Theorem 1.1. *For deterministic agents that only use valid interpretations ($\beta = \kappa$) introspective equivalence implies extrospective equivalence.*

A first problem to be analysed is that of proving state equivalence. Even when using exclusively valid interpretations ($\beta = \kappa$) the extrospective equivalence is difficult to prove. A generic approach would be that of profiling agent behaviour and evaluating the agents based on these profiles (it tries to insert the password for 10 times – it is probably an unauthorised access). Because introspective equivalence implies the extrospective equivalence in this particular case, the architect of a security protocol could try to extensively check all the situations that can appear in a system by logical inference.

The following issues are related to the identification of all the variables that can be considered and, also, to the costs of the computation (that can exponentially grow with the size of the system). To tackle the problem of the computational complexity we suggested the employment of cost bounded definitions of the two types of equivalence. Thus the extrospective equivalence can be defined taking into consideration finite sequences of actions in order to decide the equivalence of states while introspective equivalence (or rather the non-equivalence) can be decided by a limited number of inferential steps. Probabilities can be used in finding appropriate limits.

1.2.5 Reasoning

The following result shows that the epistemic logic that we use is compatible with a KDT45 inferential system that also has the conjunctivity property:

Proposition 1.1. *In a $\beta = \kappa$-interpreted system $\mathcal{I}$ the K modal operator has the following properties:*

C: $(\mathcal{I}, r, m) \models K_A[\varphi] \wedge K_A[\psi]$ iff $(\mathcal{I}, r, m) \models K_A[\varphi \wedge \psi]$;

K: $(\mathcal{I}, r, m) \models K_A[\varphi] \wedge K_A[\varphi \Rightarrow \psi]$ then $(\mathcal{I}, r, m) \models K_A[\psi]$;

D: $(\mathcal{I}, r, m) \models \neg K_A[\varphi \wedge \neg\varphi]$;

T: $(\mathcal{I}, r, m) \models K_A[\varphi]$ then $(\mathcal{I}, r, m) \models \varphi$;

4: $(\mathcal{I}, r, m) \models K_A[\varphi]$ then $(\mathcal{I}, r, m) \models K_A[K_A[\varphi]]$;

5: $(\mathcal{I}, r, m) \models \neg K_A[\varphi]$ then $(\mathcal{I}, r, m) \models K_A[\neg K_A[\varphi]]$.

2 Quantitative Approach

2.1 Plausibility Spaces

Plausibility spaces are a generalised approach for representing uncertainty.

Definition 2.1 (plausibility spaces and measures)**.** *A* plausibility space *is a tripe* $(\Omega, \mathcal{F}, \nu)$ *with:*

- Ω *– the set of all possible outcomes;*
- $\mathcal{F}$ *is a (sigma-)algebra over* Ω*;*
- ν *is a* plausibility measure *matching to every element in* $\mathcal{F}$ *a value from* D *(a partially ordered set by* $\leq$ *relation and containing to special elements* $\top$ *and* $\bot$ *with* $\bot \leq d \leq \top$*,* $\forall d \in D$*) —* ν *has the following properties:*
  1. $\nu(\emptyset) = \bot$*;*
  2. $\nu(\Omega) = \top$*;*
  3. *if* $F_1, F_2 \in \mathcal{F}$ *with* $F_1 \subseteq F_2$ *then* $\nu(F_1) \leq \nu(F_2)$*.*

2.2 Plausibilistic Entropy

What we are interested in is the identification of a global measure for the degree of uncertainty in a plausibilistic space. To do this we modelled both the concept of *entropy* introduced by Shannon for probabilistic settings and the way this concept was built.

Shannon entropy is defined to be a function $H(p_1, p_2, \ldots, p_n)$ with the following properties:

1. H is continuous in p_i.
2. If all the p_i are equal, $p_i = \frac{1}{n}$, then H is a monotonic increasing function of n. With equally likely events there is more choice, or uncertainty, when there are more possible events.

3. If a choice [can] be broken down into two successive choices, the original H should be the weighted sum of the individual values of H.

Finally, a theorem is proven showing that the only H satisfying the three above assumptions is of the form:

$$H = -K \sum_{i=1}^{n} p_i \log(p_i)$$

where K is a positive constant.

We started elaboration of plausibilistic entropy formula with a set of properties the new concept should satisfy:

1. any two plausibility structures must be comparable regardless of their dimensions or complexities;

2. if all the n elements of a plausibility space (short of $\top$ and $\bot$) have the same plausibility then the entropy should be a monotonic increasing function of n;

3. The entropy of a plausibility structure represents the amount of uncertainty in that structure, the more variants at any level the greater the entropy.

The process of elaborating the formula was supported by three particular cases shown in Figure 2. For each pair we considered the preferable structure for an agent having to make a decision. The righthand side was always selected:

A. because of the smaller number of choices;

B. the number of choices must be considered relative to the layer and not to the entire structure;

C. the number of choices is not strictly related to the size of the structure.

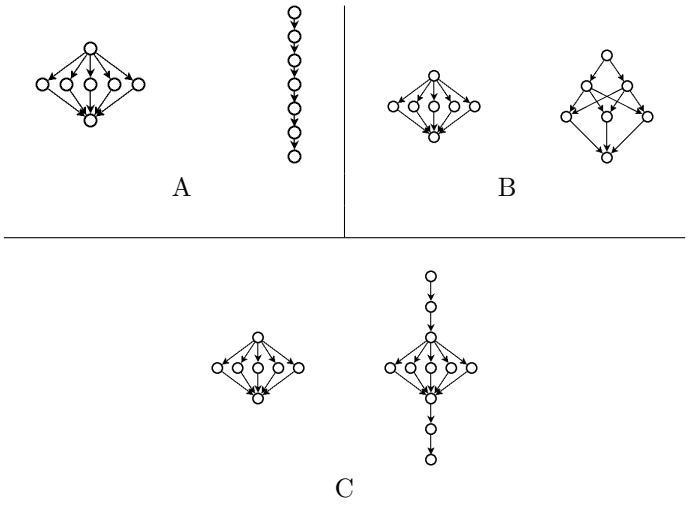


Figure 2: For each pair of structures, which would be preferable for an agent that has to make a decision?

After the analysis we came with the following definition:

Definition 2.2 (plausibilistic entropy)**.** *Given D a normalised*[1] *plausibility space/structure the* plausibilistic entropy *of D is the sum of the average amounts of choice per layer divided by the number of elements in D:*

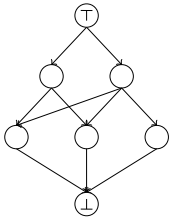
$$\hat{H} = \frac{\sum_{k=0}^{l-2} \left(\frac{\sum_{v \in L_k} d_D^+(v)}{|L_k|} - 1 \right)}{n}$$

where:

l is the number of layers in D ($\top$ and $\bot$ containing layers included);

L_k is the set of elements in layer k;

[1]edges that can be introduced based on transitivity are eliminated



$$
\begin{array}{lcccl}
\hat{h}_0 & = & \frac{(2-1)}{1} & = & 1 \\
\hat{h}_1 & = & \frac{(2-1)+(3-1)}{2} & = & 1.5 \\
\hat{h}_2 & = & \frac{(1-1)+(1-1)+(1-1)}{3} & = & 0 \\
\hat{H} & = & \frac{1+1.5+0}{7} & \sim & 0.375\ldots
\end{array}
$$

Figure 3: A step by step example for calculating the plausibilistic entropy

$d_D^+(v)$ *is the number of edges emerging from* v*;*

n *is* $|D|$*, the number of elements in* D*.*

In this case $|\cdot|$ *represents the number of elements in a set.*

The properties that can be derived directly from this definition are summarised by the following proposition:

Proposition 2.1. *Given a family of all plausibility structures with the same order* n*:*

a. *the total order (or chain) has the minimal plausibilistic entropy* $\hat{H} = 0$*;*

b. *having established a fixed layer structure for* D *– the number of layers and the number of nodes in each layer –*

$(|L_0|, |L_1|, \ldots, |L_{l-1}|)$*, the plausibilistic entropy is minimised when any two consecutive layers are minimally connected and maximised when any two consecutive layers are maximally connected:*

$$\frac{\sum_{k=0}^{l-2} \left(max\left(1, \frac{|L_{k+1}|}{|L_k|}\right) - 1 \right)}{n} \leq \hat{H} \leq 1 - \frac{l}{n};$$

c. *the plausibilistic entropy of the fully connected structures strictly decreases when the number of layers increases;*

d. *the flat structure has the maximum entropy:* $\hat{H}_n = 1 - \frac{3}{n}$*;*

e. *any other structure (neither chain nor flat) has an entropy* $\hat{H} \in (0, \hat{H}_n)$.

Consequently the following result characterises the values plausibilistic entropy can have:

Proposition 2.2. *For any finite structure* D, $\hat{H}(D) \in [0, 1) \bigcap \mathcal{Q}$.

2.3 Plausibilistic Entropy vs. Shannon Entropy

A comparison between the plausibilistic entropy and Shannon entropy is summarised in Figure 4 and Table 1. This will be accompanied by a result stating the structural similarity between the two entropies

Proposition 2.3. *For finite probability spaces increasing the number of layers on a fixed size distribution leads to a decrease in the maximal entropy that can be obtained by that structure.*

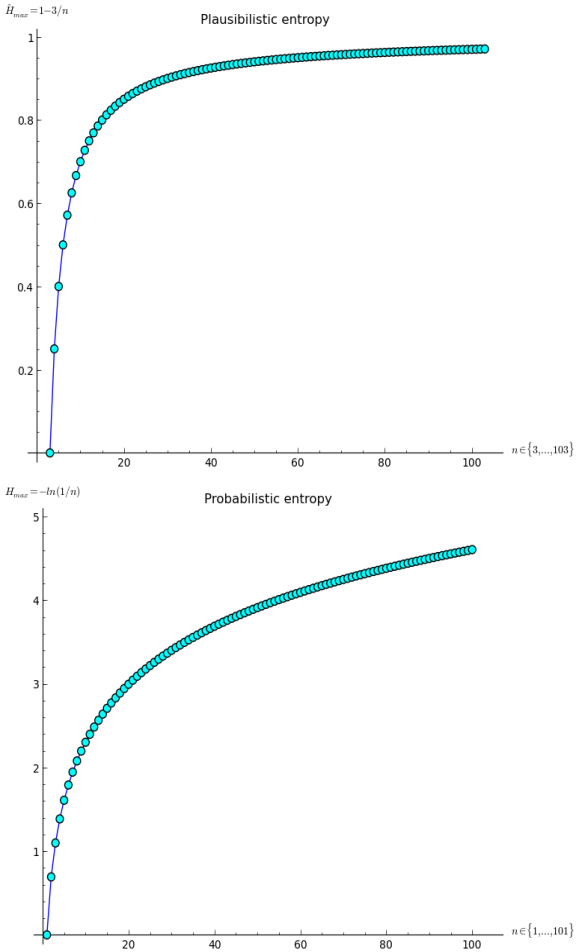


Figure 4: A visual comparison between the maximal entropy variations for a n size structure.

	Plausibilistic entropy	**Probabilistic entropy**
Top element	$\top$	1
Bottom element	$\bot$	0
Properties	$<$	$\mathbb{R}$
Layer definition	a set of all the elements equally distanced from $\top$	a set of all the elements with the same probability
Formula	$\hat{H} = \frac{\sum_{k=0}^{l-2} \left(\frac{\sum_{v \in L_k} d_D^+(v)}{\lvert L_k \rvert} - 1 \right)}{n}$	$H = -K \sum_{i=1}^{n} p_i \log(p_i)$
Domain (discussed here)	finite plausibility structures	discrete probability distributions
Codomain	$[0, 1)$	$[0, +\infty)$
Maximum entropy structure	flat structure	uniform probability distribution
Maximum entropy value	$1 - \frac{3}{n}$	$-log\left(\frac{1}{n}\right)$
Minimum entropy structure	chain structure	$\{1, 0, \ldots, 0\}$
Minimum entropy value	0	0
Structural correlations (fixed size structures)	for fully connected structures entropy strictly decreases if the number of layers increases	the maximal value of the entropy that a structure can obtain decreases when the number of layers increases
Applicability	when obtaining the actual probability values is impossible or too expensive	whenever we have enough information to make educated guesses regarding the probabilities

Table 1: A properties based comparison between entropies.

3 Taxonomy

This chapter includes a set of formal definitions for main concepts in information security. For identifying the concepts we took [14] as reference. The formalisations are based on the theory exposed in the previous chapters. The full list of the properties can be found in Figure 5.

$$
\begin{array}{l}
\textit{Secrecy} \left\{ \begin{array}{l}
\textit{Unlinkability},\ \textit{Untracebility} \\
\textit{Undetectability},\ \textit{Unidentifiability} \\
\textit{Unobservability} \\
\begin{array}{ll}
\textit{Anonymity} & \left\{ \begin{array}{l} \textit{minimal} \\ \textit{group} \\ \textit{role interchangeability} \end{array} \right. \\
\textit{Privacy} &
\end{array}
\end{array} \right. \\
\\
\textit{Authenticity} \left\{ \begin{array}{l}
\textit{Linkability},\ \textit{Traceability} \\
\textit{Detectability},\ \textit{Identifiability} \\
\begin{array}{ll}
\textit{Onymity} & \left\{ \begin{array}{l} \textit{maximal} \\ \textit{group} \\ \textit{role noninterchangeability} \end{array} \right. \\
\textit{Identity} &
\end{array}
\end{array} \right.
\end{array}
$$

Figure 5: Concepts used in information security.

Pfitzmann and Hansen identify eight main concepts that we summarised in Table 2.

Relative to the formalisation of the concepts in Figure 5 we can say the formalisation of the concept of *secrecy* has been performed by Halpern and O'Neill n [10]. The same authors also provided qualitative and quantitative formalisations (based on probability theory) for *minimal anonymity* and *group anonymity* in [9]. Tsukada *et. al.* [20] formally define *role interchangeability* and all properties related to *privacy*, *onymity* and *identity*. The same group of researchers also provide a first definition for *linkability*.

anonymity	*identifiability*
pertains the ability of the attacker to identify the subject within a set of subjects	

unlinkability	*linkability*
pertains the ability of the attacker to relate two items of interest (IOI)	

undetectability	*detectability*
pertains the ability of the attacker to identify the very existence of an IOI	

unobservability	*observability*
combines the ability of an IOI not to be detectable by a involved subjects together with the reciprocal anonymity of the involved subjects	

Table 2: Overview of the main security properties according to [14].

The thesis offers formal qualitative definitions for the other concepts in Figure 5 and a plausibilistic based quantitative definition for *anonymity*. To this set of properties we add that of *traceability* inspired by Chaum in [1]. Here we will add definitions for *(un)linkability*, *(un)traceability* and *anonymity* together with a summary of the relations between them.

3.1 (Un)Linkability

Our premiss is that the relation between IOIs is causal in nature. Thus an agent can be the initial cause of an action (by actually performing it) or indirect (by determining its performance by another agent). Generally, if every time an IOI is manifested another IOI is also manifested a *link* can be established between the two of them. Logical implication is appropriate for expressing such a relation. By analysing the definition for *linkability* in Table 2 a third party is identified that has to be taken into consideration: the attacker who

has to notice the link Therefore the causal relation between two IOIs can be defined at two levels: system and agent.

3.1.1 System Level Linkability

At system level the implication takes into consideration two entities only (any pairing between agent and action). Intuitively, every time an IOI is manifested another IOI is also manifested.

Definition 3.1 (action-to-action linkability)**.** *Action* $a \in Act$ *is* linkable *to action* $a' \in Act$ *in* $\mathcal{I}$ *if*

$$\mathcal{I} \models \exists_{(A \in Ag)}\, \theta(A, a) \Rightarrow \exists_{(A' \in Ag)}\, \theta(A', a').$$

Observaie: There are, in fact, four definitions for this concept, one for every pairing of the two types of IOIs discussed here. To save space however we will limit ourselves to only one exemplification for each case.

3.1.2 Agent Level (Un)Linkability

If we take into consideration the *observer* Definition 3.1 will be updated to:

Definition 3.2 (action-to-action linkability)**.** *Action* a *is* linkable *to action* a' *in* $\mathcal{I}$ *w.r.t. agent* I *if*

$$\mathcal{I} \models K_I[\exists_{(A \in Ag)}\, \theta(A, a)] \Rightarrow K_I[\exists_{(A' \in Ag)}\, \theta(A', a')].$$

Observaie: An intuitive formulation of this relation is that when an agent I knows that an IOI manifested itself then the same agent I knows that a second IOI also manifested itself.

As far as *unlinkability* is concerned, it can be expressed by the simple logical negation of the *linkability* formula:

Definition 3.3 (action-to-action unlinkability)**.** *Action* a *is* unlinkable *to action* a' *in* $\mathcal{I}$ *w.r.t. agent* I *if*

$$\mathcal{I} \models K_I[\exists_{(A \in Ag)}\, \theta(A, a)] \wedge P_I[\forall_{(A' \in Ag)}\, \neg\theta(A', a')].$$

3.2 (Un)Traceability

Traceability was introduced as a weaker form of *linkability*. Thus if the latter indicates a "hard" relation (providing a high degree of certainty) *traceability* rather indicates some degree o possibility. Formally, in order to define *traceability*, we will make use of the $P\varphi = \neg K \neg \varphi$ operator – complementary to the modal operator K.

Definition 3.4 (action-to-action traceability)**.** *Action a is* traceable *to action a' in $\mathcal{I}$ w.r.t. agent I if*

$$\mathcal{I} \models K_I[\exists_{(A \in Ag)}\, \theta(A, a)] \Rightarrow P_I[\exists_{(A' \in Ag)}\, \theta(A', a')].$$

... and by logically negating the above formula we get the definition for *untraceability*:

Definition 3.5 (action-to-action untraceability)**.** *Action a is* untraceable *to action a' in $\mathcal{I}$ w.r.t. agent I if*

$$\mathcal{I} \models K_I[\exists_{(A \in Ag)}\, \theta(A, a)] \wedge K_I[\forall_{(A' \in Ag)}\, \neg\theta(A', a')].$$

Observaie: Unlike *traceability*, *untraceability* is a "hard" concept (high degree of certainty). A similar relation can be identified between the concepts of *unlinkability* and *linkability*.

3.3 Anonymity

In [9] Halpern and O'Neill state that *the basic intuition behind anonymity is that actions should be divorced from the agents who perform them for some set of observers.*

Thus the easiest way of expressing anonymity is to say that an agent A performs an action a and an observer I can assume, based on the available information, that it was not actually A the author of a.

Definition 3.6 (minimal anonymity [20])**.** *An action a performed by an agent A is* minimally anonymous *in $\mathcal{I}$ w.r.t. an agent I if*

$$\mathcal{I} \models \theta(A, a) \Rightarrow P_I[\neg\theta(A, a)].$$

Closer to the meaning of anonymity the way it is introduced in Pfitzmann and Hansen (Table 2) is the group anonymity:

Definition 3.7 (group anonymity [20])**.** *Action a performed by agent A is* anonymous up to anonymity set $G \subseteq Ag \setminus \{I\}$ *in $\mathcal{I}$ w.r.t. agent I if*

$$\mathcal{I} \models \theta(A, a) \Rightarrow \forall_{(A' \in G)} P_I[\theta(A', a)].$$

3.3.1 A Quantitative Plausibilistic Entropy Based Definition Of Anonymity

Given a MAS and a plausibility distribution over the set of runs, by using the Halpern-Tuttle [11] construction, we get a plausibility distribution, $\nu_{A,r,m}$, over $\wp()$ (the set of points in the system), for each and every agent. By using the same line of reasoning from [9, 13] we can attach semantics to plausibility expressions.

If $Pl_A(\varphi)$ will be the plausibility agent A associates to φ in (r, m) it will be possible for us to define a quantitative form of anonymity by requiring that the plausibilistic entropy the agents associates to a set of formulas to have a lower bound α:

Definition 3.8 (plausibilistic group α-anonymity)**.** *Action a, performed by agent A, is* plausibilistically α-anonymous up to anonymity set $G \subseteq Ag \setminus \{I\}$ *in the plausibilistic interpreted system $\mathcal{I}$ w.r.t. agent I if*

$$\mathcal{I} \models \theta(A, a) \Rightarrow \hat{H}\left(\{Pl_I[\theta(A', a)] : A' \in G\}\right) \geq \alpha.$$

Observaie: This form of anonymity takes into consideration all the information an observer has in relation to a certain anonymity context, regardless of the way it structures its information. Since α can take any value in $[0, 1)$ any two degrees of anonymity can be compared – this fact facilitating the decision if a security protocol has to be chosen. Generally, the level of anonymity increases with the number of agents in G yet the anonymity never becomes perfect if the number of agents is finite. Because the plausibilistic

entropy approaches 1 (perfection) only when the number of agents appraoches infinity, this definition supports a this intuition.

Figure 6 summarises some relations between the anonymity related concepts.

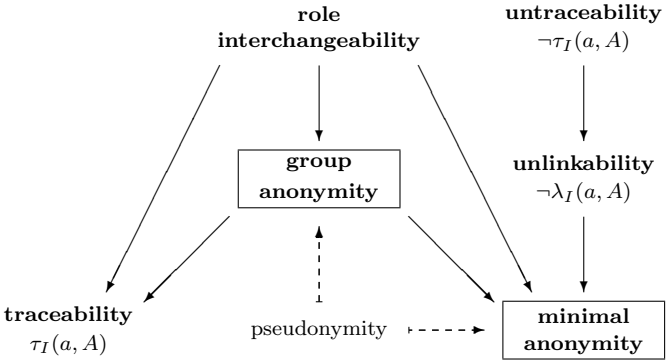


Figure 6: Relations between anonymity related properties.

Conclusion

Summarising the main theoretical contributions brought the following can be pointed out:

- the compilation of an MAS based epistemic logic framework to be used for formally defining the information security related properties;
- the definition of the introspective and extrospective equivalences over the local states of an agent providing thus means of determining it;
- the introduction of the concept of plausibilistic entropy as a very general measure of the degree of uncertainty in a plausibilistic context and comparing it with Shannon entropy;

- the formalisation of the main definitions in information security identified by Pfitzmann and Hansen inside the compiled theoretical framework – both qualitative and quantitative definitions are supported.

There are at least two directions where these results can find applications:

- The first one is related to quantifying the degrees of anonymity the current security protocols provide. For example we can consider the Herbivore protocol introduced by Goel *et. al.* in [3]. This is a DC-networks based protocol that uses anonymity cliques of a certain dimension n. By using the anonymity definition based on plausibilistic entropy we can say that the maximum degree of anonymity associated to $n = 64$ (value is chosen by the authors) is $\frac{63}{66} \sim 0.954...$ thus giving us the possibility to compare it with the degree of anonymity provided by other protocols.

- The second application could be related to the automatic proving of the properties of security protocols. We can take for example the MCMAS tool introduced by Raimondi and Lomuscio in [15, 12]. As an alternative, by using plausibilistic entropy based definitions of various properties we could iterate the states of the MAS and record the maximum and the minimum degree to which a certain property is satisfied.

References

[1] David L. Chaum. Untraceable electronic mail, return addresses, and digital pseudonyms. *Communications of the ACM*, 24(2):84–90, February 1981.

[2] Ronald Fagin, Joseph Y. Halpern, Yoram Moses, and Moshe Y. Vardi. *Reasoning about Knowledge*. The MIT Press, 2004.

[3] Sharad Goel, Mark Robson, Milo Polte, and Emin G. Sirer. Herbivore: A scalable and efficient protocol for anonymous communication. Technical Report 1890, Cornell University, February 2003.

[4] Iulian Goriac. An epistemic logic based framework for reasoning about information hiding. In *Proc. of the 6th International Conference on Availability, Reliability, and Security (ARES'11), Vienna, Austria*, pages 286–293. IEEE, August 2011.

[5] Iulian Goriac. Compiling an epistemic logic for multiagent systems. *International Journal of Intelligent Systems*, 28(7):648–668, July 2013.

[6] Iulian Goriac. Measuring anonymity with plausibilistic entropy. In *Proc. of the 8th International Conference on Availability, Reliability, and Security (ARES'13), Regensburg, Germany*, pages 151–160. IEEE, September 2013.

[7] Iulian Goriac. Plausibilistic entropy and anonymity. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA)*, 5(1):64–83, 3 2014.

[8] Joseph Y. Halpern. *Reasoning about Uncertainty*. The MIT Press, 2005.

[9] Joseph Y. Halpern and Kevin R. O'Neill. Anonymity and information hiding in multiagent systems. *Journal of Computer Security*, 13(3):483–512, May 2005.

[10] Joseph Y. Halpern and Kevin R. O'Neill. Secrecy in multiagent systems. *ACM Transactions on Information and System Security*, 12(1):1–47, October 2008.

[11] Joseph Y. Halpern and Mark R. Tuttle. Knowledge, probability, and adversaries. *Journal of the ACM*, 40(4):917–962, September 1993.

[12] Alessio Lomuscio and Franco Raimondi. Mcmas: A model checker for multi-agent systems. In *Proceedings of TACAS 2006*, pages 450–454. Springer Verlag, 2006.

[13] Kevin Ross O'Neill. *Secrecy and Anonymity in Interactive Systems.* PhD thesis, Cornell University, August 2006.

[14] Andreas Pfitzmann and Marit Hansen. A terminology for talking about privacy by data minimization: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management, 2010. v0.34.

[15] Franco Raimondi and Alessio Lomuscio. Automatic verification of multi-agent systems by model checking via ordered binary decision diagrams. *Journal of Applied Logic*, 5(2):235–251, June 2007.

[16] Claude E. Shannon. A mathematical theory of communication. *Bell System Technical Journal*, 27(3):379–423, July 1948.

[17] Yoav Shoham and Kevin Leyton-Brown. *Multiagent Systems: Algorithmic, Game-Theoretic, and Logical Foundations.* Cambridge University Press, Cambridge, UK, 2009.

[18] Ferucio Laurenţiu Ţiplea, Loredana Vămanu, and Cosmin Vârlan. Complexity of anonymity for security protocols. In *Proc. of the 15th European Symposium on Research in Computer Security (ESORICS'10), Athens, Greece, LNCS*, volume 6345, pages 558–572. Springer Berlin Heidelberg, September 2010.

[19] Ferucio Laurenţiu Ţiplea, Loredana Vămanu, and Cosmin Vârlan. Reasoning about minimal anonymity in security protocols. *Future Generation Computer Systems*, 29(3):828–842, March 2013.

[20] Yasuyuki Tsukada, Ken Mano, Hideki Sakurada, and Yoshinobu Kawabe. Anonymity, privacy, onymity, and identity: A

modal logic approach. *Transactions on Data Privacy*, 3(3):177–198, December 2010.