Informational Analysis of Formalized Biological Systems *

Damas P. Gruska

Institute of Informatics, Comenius University,
Mlynska dolina, 842 48 Bratislava, Slovakia,
gruska@fmph.uniba.sk.

Abstract. Formalism for analysis of systems of various nature (hardware, software, biological etc.) specified by process algebras is proposed. Biologically motivated it combines several information flow based security notions and approaches. It allows us to formalize such properties of biological systems as diagnosability, detection ability and a presence of, for example, biological intruders and pathological changes. Resulting properties can be viewed as complementary to security ones. Moreover, we present a quantification of these properties by means of information theory.

1 Introduction

There are several different approaches how to model biological systems. Either special biologically motivated formalisms can be exploited (for example, Neural networks, P Systems, Calculus of Looping Sequences etc.) or formalisms originally developed for specifying and modeling hardware or software systems can be exploited. Once we have a model of biological system we can study it, investigate its behavior and compare behavior of the system with behavior of the formal model and in this way we can also improve or correct our model. Moreover, there are additional connections between biology and informatics. Inspirations and motivations from one area can be useful and fruitful in another area and vice versa. Among them a relationship of security of computational systems and such properties of biological systems as immunity, resistance, diagnosability play an important role. The aim of this paper is to propose a formalism for analysis of biological systems specified by process algebras which enables us to define such properties as detection ability, diagnosability of presence of various biological intruders as viruses or pathological changes. These properties can be viewed as complementary ones to security properties. Hence, we obtain also rather general security properties which generalize several traditional ones.

The presented approach combines several ideas emerged from security theory as well as from modeling of biological systems. As regards security, we exploit an idea of an absence of information flow between public and private system's behaviour (see [GM82]). This concept has been many times exploited in various

* Work supported by the grant VEGA 1/0688/10.

CONCURRENCY, SPECIFICATION AND PROGRAMMING
M. Szczuka et al. (eds.): Proceedings of the international workshop CS&P 2011
September 28-30, Pułtusk, Poland, pp. 169-181

formalism. In security property called Non-Deductibility on Composition (NDC) it is assumed that system's actions are divided to private and public ones. An information flow between these two kinds of actions is expressed in the following way: a system has NDC property if for every high level user A (i.e. the one capable to perform only private i.e. high level actions), the low level view of the behaviour (seeing only public i.e. low level actions) of P is not modified (in terms of weak trace equivalence) by the presence of A. In our approach we exploit an idea of intruders taken form NDC. Moreover we will consider several intruders which are differently nested inside a system (as it was done in [GMM10,Gru03]). This approach seems to be more suitable for investigation of biological systems. The information flow will be formalized by opacity (see [BKMR06]). Opacity again seems to be more suitable for biological systems since it can capture more complex information flow then just the flow between occurrences of private and public actions. Opacity has been also exploited for analyses of biological systems. By means of opacity a diagnosability (as a complementary concept to security) for P Systems (see [BGMM10]) has been defined. Note that opacity was already exploited for definitions of security properties for process algebras (see [Gru07]). Combining the above mentioned approaches we propose the formalism for analyses of biological systems which are specified by means of process algebras. We define properties as *Diagnosable intruders, Strongly Diagnosable intruders, Diagnosability for processes, Strong diagnosability for processes, Intruders detectable by weak bisimulation, Intruders detectable by weak bisimulation* and *Strong intruders detectable by a predicate*. As a side affect we obtain very general and strong security properties as complements of these properties. Here we present a quantification of these properties by means of information theory (see [Gru09] for quantification of security properties for timed process algebras). In this way we can express how much information can be obtained about intruders by system's observations. By comparison of this information with experimental statistical data on system's behaviour we can improve the original formal model of the system.

2 Context Process Algebra

In this section we define our working formalism - contexts process algebra (CPA). It is based on Milner's CCS (see [Mil89]) which is extended by placeholders to specify processes contexts. To define the language CPA, we first assume a set of atomic action symbols A not containing symbols τ, and such that for every $a \in A$ there exists $\overline{a} \in A$ and $\overline{\overline{a}} = a$. We define $Act = A \cup \{\tau\}$. We assume that $a, b, \ldots$ range over A and $x, y, \ldots$ range over Act. Assume the signature $\Sigma = \bigcup_{n\in\{0,1,2\}} \Sigma_n$, where

$$\begin{aligned}
\Sigma_0 &= \{Nil\} \\
\Sigma_1 &= \{x. \mid x \in Act\} \cup \{[S] \mid S \text{ is a relabeling function}\} \\
&\quad \cup \{\backslash M \mid M \subseteq A\} \\
\Sigma_2 &= \{|, +\}
\end{aligned}$$

with the agreement to write unary action operators in prefix form, the unary operators $[S], \backslash M$ in postfix form, and the rest of operators in infix form. Relabeling functions, $S : Act \to Act$ are such that $\overline{S(a)} = S(\bar{a})$ for $a \in A$, and $S(\tau) = \tau$.

The set of CPA terms over the signature Σ is defined by the following BNF notation:

$$P \ ::= \ X \ \mid \ \mathcal{A} \ \mid \ op(P_1, P_2, \ldots P_n) \ \mid \ \mu X P$$

where $X \in Var$, Var is a set of process variables, $\mathcal{A} \in PH$, PH is a set of process placeholders, $P, P_1, \ldots P_n$ are CPA terms, $\mu X-$ is the binding construct, $op \in \Sigma$. The set of CPA processes consists of closed CPA terms. The set of CCS processes consists of CPA processes without placeholders.

Let P be a CPA process with (all) placeholders $\mathcal{A}_1, \ldots, \mathcal{A}_n$. We will indicate this by $P[\mathcal{A}_1, \ldots, \mathcal{A}_n]$. CCS process obtained from from $P[\mathcal{A}_1, \ldots, \mathcal{A}_n]$ by replacing placeholders $\mathcal{A}_i$ by CCS processes A_i will be indicated by $P[\mathcal{A}_1/A_1, \ldots, \mathcal{A}_n/A_n]$. Note that Nil will be often omitted from processes descriptions and hence, for example, instead of $a.b.Nil$ we will write just $a.b$. A structural operational semantics for CPA terms is given by means of labeled transition systems basicly the same as the one for CCS (see [Mil89]).

For $s = x_1.x_2.\ldots.x_n, x_i \in Act$ we write $P \xrightarrow{s}$ instead of $P \xrightarrow{x_1} \xrightarrow{x_2} \ldots \xrightarrow{x_n}$ and we say that s is a trace of P. The set of all traces of P will be denoted by $Tr(P)$. By ϵ we will denote the empty sequence of actions, by $Succ(P)$ we will denote the set of all successors of P and $Sort(P) = \{x | P \xrightarrow{s.x}$ for some $s \in Act^\star$ and $x \neq \tau\}$. If the set $Succ(P)$ is finite we say that P is finite state. In the later we will use the weak trace equivalence (denoted $\approx_w$) and bisimulation (denoted $\sim$) (see [Mil89]).

Let us have a system described by CCS process P. Suppose that there are places in the system where an intruder or intruders can be put. We indicate those places by placeholders and the resulting CPA process will be called its opening. The opening of process can be defined on syntactical or semantical level. For simplicity we will use the later one.

Definition 1. *Let P be a CCS process. Opening of P is any CPA process $Q[\mathcal{A}_1, \ldots, \mathcal{A}_n]$ such that $P \sim Q[\mathcal{A}_1/Nil, \ldots, \mathcal{A}_n/Nil]$.*

3 Diagnosable intruders

The first inspiration for our work is the security property Non-Deducibility on Composition (NDC for short, see in [FGM03]). Suppose that all actions are divided in two groups, namely public (low level) actions L and private (high level) actions H i.e. $A = L \cup H, L \cap H = \emptyset$. Then process P has property NDC if for every high level user A, the low level view of the behaviour of P is not modified (in terms of weak trace equivalence) by the presence of A. The idea of NDC can be formulated in such a way that it is required that $(P|A)\backslash H \approx_w P\backslash H$ for every $A, Sort(A) \subseteq H \cup \{\tau\}$. Hence, in the case of NDC, only one attacker

is considered and it communicates with the system on the top most level (non-nested attacker) and the system with and without the attacker are compared on level of weak traces (see Fig 1). Our formalism of context process algebra allows us to model several intruders which can be nested arbitrary inside the system . In style of NDC we could define nested non-deducibility (see Fig. 2).

Definition 2. *Let for CCS process P. We say that P has a property Nested Non-Deducibility (NND, for short) if $P \setminus H \approx_w P'[\mathcal{A}_1/A_1, \ldots, \mathcal{A}_n/A_n] \setminus H$ for every opening $P'[\mathcal{A}_1, \ldots, \mathcal{A}_n]$ of process P and every $A_i, Sort(A_i) \subseteq H \cup \{\tau\}, 1 \leq i \leq n$.*

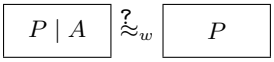

Fig. 1. Non-nested attacker

Example 1. In general we have $NND \subseteq NDC$ since clearly NDC is a special case of NND property. Let $P = l_1.Nil + (h.l_2.Nil) \setminus H$ It is easy to check that $P \in NDC$ but $P \notin NND$. Hence we have that $NND \subset NDC$.

Security property NND would be appropriate in case that an attacker can place several auxiliary processes inside the system in such a way that they can cause some information flow between private and public actions. But since for biological systems division of actions to two static groups (one type of actions cannot be observed and another one is always observed) is not appropriate. Hence instead of Non-Deducibility on Composition we will exploit more general concept opacity (see [BKMR06]). First we define observation function $\mathcal{O}$ on sequences from $Act^\star$ as function $\mathcal{O} : Act^\star \to \Theta^\star$ where Θ be a set of elements called observables. An observation function expresses what an observer - eavesdropper can see from a system behaviour and we will alternatively use both the terms (observation - observer) with the same meaning.

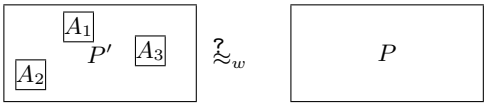

Fig. 2. Nested attacker

Now suppose that we have some security property. This might be an execution of one or more classified actions, an execution of actions in a particular classified order which should be kept hidden, etc. Suppose that this property is expressed by predicate ϕ over process traces. We would like to know whether an observer can deduce the validity of the property ϕ just by observing sequences of actions from $Act^\star$ performed by given process. The observer cannot deduce the validity of ϕ for P if for every trace w of P such that $\phi(w)$ holds, there exists trace w' such that $\neg\phi(w')$ and the traces cannot be distinguished by an observer (see Fig. 3). We formalize this concept by opacity.

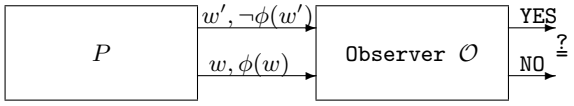

Fig. 3. Opacity observer

Definition 3 (Opacity). *Given process P, a predicate ϕ over $Act^\star$ is opaque w.r.t. the observation function $\mathcal{O}$ if for every sequence w, $w \in Tr(P)$ such that $\phi(w)$ holds and $\mathcal{O}(w) \neq \epsilon$, there exists a sequence $w', w' \in Tr(P)$ such that $\neg\phi(w')$ holds and $\mathcal{O}(w) = \mathcal{O}(w')$. The set of processes for which the predicate ϕ is opaque with respect to $\mathcal{O}$ will be denoted by $Op^\phi_{\mathcal{O}}$.*

The notion of opacity is rather general. With its help many other security properties can be defined (anonymity, non-interference etc. see [BKMR06]). On the other side, opacity is undecidable even for the simplest possible observation function, namely for the constant one, and for finite state processes (see [Gru04]).

Now we are ready to to define diagnosability of intruders as a complementary property to opacity. We start with some notation. For CCS process P we will write $\Phi(P)$ iff there exists $w, w \in Tr(P)$ such that $\Phi(w)$ and we write $\Phi^o(P)$ iff there exists $w, w \in Tr(P)$ such that $\Phi(w)$ and $\mathcal{O}(w) = o$.

Definition 4 (Diagnosable intruders). *Given CPA process $P[\mathcal{A}_1, \ldots, \mathcal{A}_n]$ and a set $V, V = \{A_1, \ldots, A_n\}$ of CCS processes called intruders. We say that the intruders V are* diagnosable *by a predicate ϕ over $Act^\star$ and by the observation function $\mathcal{O}$ for $P[\mathcal{A}_1, \ldots, \mathcal{A}_n]$ if $\phi(P[\mathcal{A}_1/A_1, \ldots, \mathcal{A}_n/A_n])$ and $P[\mathcal{A}_1/A_1, \ldots, \mathcal{A}_n/A_n] \notin Op^\phi_{\mathcal{O}}$. We will denote this by $P[\mathcal{A}_1, \ldots, \mathcal{A}_n] \in DI^{\phi,\mathcal{O}}_V$.*

Example 2. Let us consider CPA process $P = ((h.l_1.Nil + l_2.Nil)|\mathcal{A}) \setminus \{h\}$, $\mathcal{O}(l_1) = \mathcal{O}(l_2) = l$, $\mathcal{O}(h) = \mathcal{O}(\tau) = \epsilon$ and $\phi(s)$ holds if s contains l_2. Then $P \notin DI^{\phi,\mathcal{O}}_{\bar{h}.Nil}$ and $P \in DI^{\phi,\mathcal{O}}_{h.Nil}$.

Opacity, as it is defined in Definition 3, is frequently criticized from the both side - as a qualitative property it might happen that sometimes it is too weak or that in other cases it can be too strong. The same holds for diagnosability of intruders as it is clear from in the following example.

Example 3. Let us consider process $P^n = \sum_{i=1}^{2^k} h_i.(\sum_{j=1,j\neq n}^{2^k} l_j.\bar{l}_{refused} + l_n.\bar{l}_{accepted})$ and CPA process $P = (P^n|\mathcal{A}) \setminus \{h_1, \ldots, h_{2^k}\}$. $\mathcal{O}(\tau) = \epsilon$, $\mathcal{O}(x) = x$ for other actions, and predicate ϕ_i such that $\phi_i(s)$ holds iff s contains action $l_{accepted}$. Let $A_i = \bar{h}_i.Nil$. Then $P \notin DI^{\phi,\mathcal{O}}_{A_i}$ iff $i = n$. In other word detectable are only such intruders which "know" secrete password h_n if we consider process P_n as a simple access control process. If k is large number, i.e. there are many possible passwords, then the probability that action $l_{accepted}$ is performed is very low i.e. probability to diagnose an intruder knowing the password $(h_n.Nil)$ is also very low.

To overcame an insufficiency of (qualitative) diagnosability illustrated in the previous examples we will define quantitative measure of it.

4 Quantification of diagnosability

To define quantification of diagnosability we need some preparatory work. First we recall some basic concepts of information theory. To express quantity of information flow we will exploit Shannon information theory (see [Sh48]). Let X be a discrete random variable and let x ranges over the set of values which X may take. By $p(x)$ we will denote probability that X takes the value x. Self-information (or surprisal) is a measure of the information content associated with the outcome of the random variable X. It is defined as $\mathcal{H}(x) = \log_b \frac{1}{p(x)}$. We put $\mathcal{H}(x) = \infty$ if $p(x) = 0$. The information entropy (also called self-information or a measure of uncertainty) of the variable X is denoted $\mathcal{H}(X)$ and is defined as $\mathcal{H}(X) = \sum_x p(x).\log_b \frac{1}{p(x)}$. We define $p(x).\log_b \frac{1}{p(x)} = 0$ if $p(x) = 0$. We will work with the base b of $\log_b$ equal to 2 and hence the unit of the information entropy will be one bit. Sometimes we will write $\mathcal{H}(p_1, \ldots, p_n)$ instead of $\mathcal{H}(X)$ if probabilities of values of X are $p_1, \ldots, p_n$. Given two random variables X and Y, the mutual information between them, written $\mathcal{I}(X;Y)$, is defined as $\mathcal{I}(X;Y) = \sum_x \sum_y p(x,y).\log \frac{p(x,y)}{p(x).p(y)}$. Conditional entropy of X given knowledge of Y is defined as$\mathcal{H}(X|Y) = \sum_y p(y).\mathcal{H}(X|Y = y)$, and conditional mutual information between X and Y given knowledge of Z is defined as $\mathcal{I}(X;Y|Z) = \mathcal{H}(Y|Z) - \mathcal{H}(Y|X,Z)$.

4.1 Surprisal and uncertainty of security properties

To exploit information theory we need a way how to express probability of some observations. We will denote a multiset of finite traces of P by $MTr(P)$. For example, the trace $a.b$ is contained in $MTr(a.bNil + a.b.c.Nil)$ two times. There exist a few techniques how to define this multiset, originally developed for probabilistic process algebras (but here we will assume that all sequences have the same probability). For example, in [SL95] a technique of schedulers are used to resolve the nondeterminism and in [GSS95] all transitions are indexed and hence pathes can be distinguished by different indexes. In the former case, every scheduler defines (schedules) a particular computation path and hence two different schedulers determine different pathes, in the later case, the index records which transition was chosen in the case of several possibilities. The set of indexes for process P consists of sequences $i_1 \ldots i_k$ where $i_j \in \{0,1,2\} \cup \{0,1,2\} \times \{0,1,2\}$. An index records how a computation path of P could be derived, i.e. it records which process was chosen in case of nondeterminism. If there is only one possible successor then transitions are indexed by 1 (i.e. corresponding $i_l = 1$) If transition $P \xrightarrow{x} P'$ is indexed by k (i.e. corresponding $i_l = k$) then transition $P + Q \xrightarrow{x} P'$ is indexed by $k.1$ and transition $Q + P \xrightarrow{x} P'$ is indexed by $k.2$. If transitions $P \xrightarrow{x} P'$ and $Q \xrightarrow{x} Q'$ are indexed by k and

l, respectively, then transitions of $P|Q$ have indexes from $\{(k,0),(0,l),(k,l)\}$ depending on which transition rule for the parallel composition was applied. Every index defines at most one trace and the set of all indexes defines the multisets of traces $MTr(P)$. First we express quantification of an amount of information flow by means of the simplest concepts and later we develop more elaborated ones. Let $\mathcal{O}$ be an observation function and ϕ be a predicate over traces. Let $o \in Act^\star$. We denote $MTr(P)^{\mathcal{O}=o} = \{s | s \in MTr(P), \mathcal{O}(s) = o\}$ and $MTr(P)_\phi^{\mathcal{O}=o} = \{s | s \in MTr(P), \phi(s) \wedge (\mathcal{O}(s) = o)\}$. We define

$$p(MTr(P)_\phi^o) = |MTr(P)_\phi^{\mathcal{O}=o}|/|MTr(P)^{\mathcal{O}=o}|.$$

Definition 5. *Given CPA process $P[\mathcal{A}_1,\ldots,\mathcal{A}_n]$ and a set $V, V = \{A_1,\ldots,A_n\}$ of CCS processes called intruders. We define surprisal $\mathcal{H}(P[V]_\phi^{\mathcal{O}=o})$ of ϕ for process P, intruders V and observation $o, o \neq \epsilon$ as*

$$\mathcal{H}(P[V]_\phi^{\mathcal{O}=o}) = \log \frac{1}{p(MTr(P[\mathcal{A}_1/A_1,\ldots,\mathcal{A}_n/A_n])_\phi^{\mathcal{O}=o})}.$$

Example 4. 3 Let us consider CPA process P^n from Example 3 and $V = \sum_{i=1}^{2^k} \bar{h}_i.Nil$ and $o = l_{accepted}$. Then $\mathcal{H}(P[V]_\phi^{\mathcal{O}=o}) = k$.

As it is stated in the following theorem there is a correspondence between a value of $\mathcal{H}(P[V]_\phi^{\mathcal{O}=o})$ and predicate opacity and so surprisal can be seen as a quantification of opacity.

Theorem 1. *$P[\mathcal{A}_1,\ldots,\mathcal{A}_n] \in DI_V^{\phi,\mathcal{O}}$ iff $\mathcal{H}(P[V]_\phi^{\mathcal{O}=o}) = 0$ for every o such that $\mathcal{O}(o) \neq \epsilon$ and $\phi^o(P[\mathcal{A}_1/A_1,\ldots,\mathcal{A}_n/A_n])$ where $V = \{A_1,\ldots,A_n\}$.*

Proof. Let $P[\mathcal{A}_1,\ldots,\mathcal{A}_n] \in DI_V^{\phi,\mathcal{O}}$ and let $w \in Tr(P[\mathcal{A}_1,\ldots,\mathcal{A}_n])$ such that $\phi(w)$ and $\mathcal{O}(w) = o, o \neq \epsilon$. Then there does not exist w', $w' \in Tr(P[\mathcal{A}_1/A_1,\ldots,\mathcal{A}_n/A_n])$ such that $\neg\phi(w')$ and $\mathcal{O}(w) = \mathcal{O}(w')$. From this we have $p(MTr(P[\mathcal{A}_1/A_1,\ldots,\mathcal{A}_n/A_n])_\phi^{\mathcal{O}=o}) = 1$ i.e. $\mathcal{H}(P[V]_\phi^{\mathcal{O}=o}) = 0$.

Let $\mathcal{H}(P[V]_\phi^{\mathcal{O}=o}) = 0$ for every o such that $\mathcal{O}(o) \neq \epsilon$ and let $w \in Tr(P)$ such that $\phi(w)$ and $\mathcal{O}(w) = o$. Since $\mathcal{H}(P[V]_\phi^{\mathcal{O}=o}) = 0$ we have that $p(MTr(P[\mathcal{A}_1,\ldots,\mathcal{A}_n])_\phi^{\mathcal{O}=o}) = 1$ i.e. there does not exist w', $w' \in Tr(P[\mathcal{A}_1,\ldots,\mathcal{A}_n])$ such that $\neg\phi(w')$ and $\mathcal{O}(w) = \mathcal{O}(w')$ i.e. $P[\mathcal{A}_1/A_1,\ldots,\mathcal{A}_n/A_n] \in DI_V^{\phi,\mathcal{O}}$. □

So if $\mathcal{H}(P[V]_\phi^{\mathcal{O}=o}) = 0$ then from observation o we have certainty that for corresponding trace(s) of P predicate ϕ holds. If $\mathcal{H}(P[V]_\phi^{\mathcal{O}=o}) \geq 1$ then it is equally or more probable that ϕ does not hold than it holds.

For processes we have the following compositionality property.

Theorem 2. *Let $V = \{A_1,\ldots,A_n\}$ and $\mathcal{H}(P[V]_\phi^{\mathcal{O}=o}) = e_1$, $\mathcal{H}(Q[V]_\phi^{\mathcal{O}=o}) = e_2$ then*

$$\min\{e_1,e_2\} \leq \mathcal{H}((P+Q)[V]_\phi^{\mathcal{O}=o}) \leq \max\{e_1,e_2\}.$$

Proof. Let $|MTr(P[\mathcal{A}_1/A_1,\ldots,\mathcal{A}_n/A_n])^{\mathcal{O}=o}_{\phi}| = n_1$, $|MTr(P[\mathcal{A}_1/A_1,\ldots,\mathcal{A}_n/A_n])^{\mathcal{O}=o}| = m_1$ and $|MTr(Q[\mathcal{A}_1/A_1,\ldots,\mathcal{A}_n/A_n])^{\mathcal{O}=o}_{\phi}| = n_2$, $|MTr(Q[\mathcal{A}_1/A_1,\ldots,\mathcal{A}_n/A_n])^{o}| = m_2$. Without loss of generality we can assume that $e_1 \leq e_2$ i.e. $n_1/m_1 \leq n_2/m_2$. From that we have $n_1.m_2 \leq n_2.m_1$. We have that $|MTr(P+Q)[\mathcal{A}_1/A_1,\ldots,\mathcal{A}_n/A_n]^{\mathcal{O}=o}_{\phi}| = n_1+n_2$ and $|MTr(P+Q)[\mathcal{A}_1/A_1,\ldots,\mathcal{A}_n/A_n]^{\mathcal{O}=o}| = m_1+m_2$ and so $n_1/m_1 \leq (n_1+n_2)/(m_1+m_2) \leq n_2/m_2$. □

The definition of predicate opacity (see Definition 3) is asymmetric in the sense that if $\phi(w)$ does not hold than it is not required that there exist another trace for which it holds (in general $Op^{\phi}_{\mathcal{O}} \neq Op^{\neg\phi}_{\mathcal{O}}$). This means that opacity says something to an intruder which tries to detect only validity of ϕ (if it is opaque, than validity cannot be detected) but not its non-validity i.e. it says nothing about predicate $\neg\phi$. The same hold for intruder's diagnosability.

To overcome this disadvantage we introduce a measure of uncertainty of ϕ under observation o. The uncertainty expresses an amount of information which can be learned by attacker about predicate ϕ.

Definition 6. *Given CPA process $P[\mathcal{A}_1,\ldots,\mathcal{A}_n]$ and a set $V, V = \{A_1,\ldots,A_n\}$ of CCS processes called intruders (we will write $P[V]$ instead of $P[\mathcal{A}_1/A_1,\ldots,\mathcal{A}_n/A_n]$). We define uncertainty $\mathcal{H}_u(P[V]^{\mathcal{O}=o}_{\phi})$ of ϕ for process P and observation $o, o \neq \epsilon$ as $\mathcal{H}_u(P[V]^{\mathcal{O}=o}_{\phi}) = p(MTr(P[V])^{\mathcal{O}=o}_{\phi}).\log\frac{1}{p(MTr(P[V])^{\mathcal{O}=o}_{\phi})}$ $+(1-p(MTr(P[V])^{\mathcal{O}=o}_{\phi})).\log\frac{1}{1-p(MTr(P[V])^{\mathcal{O}=o}_{\phi})}$.*

The uncertainty expresses how uncertain is predicate ϕ under observation o. The maximal value (equal to 1) means that probabilities that ϕ holds and that ϕ does not hold are equal. The uncertainty has a similar relationship to opacity as the suprisal (see Theorem 1). Also the proof is similar.

Theorem 3. *If $P[\mathcal{A}_1,\ldots,\mathcal{A}_n] \in DI^{\phi,\mathcal{O}}_V$ then $\mathcal{H}_u(P[V]^{\mathcal{O}=o}_{\phi}) = 0$ for every o such that $\mathcal{O}(o) \neq \epsilon$ where $V = \{A_1,\ldots,A_n\}$.*

The inverse implication in Theorem 3 does not hold but we have the following property. Its proof is straightforward.

Theorem 4. *If $\mathcal{H}_u(P[V]^{\mathcal{O}=o}_{\phi}) = 0$ for every o such that $\mathcal{O}(o) \neq \epsilon$ where $V = \{A_1,\ldots,A_n\}$ then $P[\mathcal{A}_1,\ldots,\mathcal{A}_n] \in DI^{\phi,\mathcal{O}}_V$ or $P[\mathcal{A}_1,\ldots,\mathcal{A}_n] \in DI^{\emptyset,\mathcal{O}}_V$.*

5 Variants of diagnosability

Property *Diagnosable intruders* suppose that we know the set V of intruders in advance. This is not always the case and hence we define a property, called *Strongly Diagnosable intruders*, which does not expect any set of intruders in advance.

Definition 7 (Strongly Diagnosable intruders). *Given CPA process* $P[\mathcal{A}_1, \ldots, \mathcal{A}_n]$. *We say that the intruders are* strongly diagnosable *by a predicate* ϕ *over* $Act^\star$ *and by the observation function* $\mathcal{O}$ *for* $P[\mathcal{A}_1, \ldots, \mathcal{A}_n]$ *if there exists a set* $V, V = \{A_1, \ldots, A_n\}$ *of CCS processes such* $\phi(P[\mathcal{A}_1/A_1, \ldots, \mathcal{A}_n/A_n])$ *and* $P[\mathcal{A}_1/A_1, \ldots, \mathcal{A}_n/A_n] \notin Op^\phi_\mathcal{O}$. *We will denote this by* $P[\mathcal{A}_1, \ldots, \mathcal{A}_n] \in SDI^{\phi,\mathcal{O}}$.

A relationship between Strongly Diagnosable intruders and Diagnosable intruders is given by the following theorem.

Theorem 5. $SDI^{\phi,\mathcal{O}} = \bigcup_{V,V=\{A_1,\ldots,A_n\},A_i \in CCS} DI^{\phi,\mathcal{O}}_V$.

Proof. Sketch. Let us suppose that $P[\mathcal{A}_1, \ldots, \mathcal{A}_n] \in SDI^{\phi,\mathcal{O}}$ then there exists a set $V, V = \{A_1, \ldots, A_n\}$ of CCS processes such $\phi(P[\mathcal{A}_1/A_1, \ldots, \mathcal{A}_n/A_n])$ and $P[\mathcal{A}_1/A_1, \ldots, \mathcal{A}_n/A_n] \notin Op^\phi_\mathcal{O}$. From this we have $P[\mathcal{A}_1, \ldots, \mathcal{A}_n] \in DI^{\phi,\mathcal{O}}_V$. The proof of the inverse inclusion is similar. □

Diagnosability of intruders assumes also that we know possible holes (placeholders in our formalism) for the intruders in a system specification (as CPA term) and a set of intruders. This is not always the case and hence we define diagnosability for CCS processes.

Definition 8 (Diagnosability for processes). *Given CCS process* P *and a set* $V, V = \{A_1, \ldots, A_n\}$ *of CCS processes called intruders. We say that the processes* V *are* strongly diagnosable processes *by a predicate* ϕ *over* $Act^\star$ *and by the observation function* $\mathcal{O}$ *if for every opening every* P' *of which is opening of* P *it holds* $P'[\mathcal{A}_1/A_1, \ldots, \mathcal{A}_n/A_n]) \notin Op^\phi_\mathcal{O}$. *We will denote this by* $P[V] \in DP^{\phi,\mathcal{O}}_V$.

A relationship between Diagnosable intruders and Diagnosability for processes is given by the following theorem.

Theorem 6. $P \in DP^{\phi,\mathcal{O}}_V$ *iff* $P'[\mathcal{A}_1/A_1, \ldots, \mathcal{A}_n/A_n] \in DI^{\phi,\mathcal{O}}_V$ *for every opening* P' *of* P.

Proof. The proof follows directly from Definition 1 and 8. □

No we are ready to define the most general of the previous notions, called *Strong diagnosability for processes*, which does not assume that either a possible set of intruders (V) is known in advance nor possible placing of these intruders (placeholders).

Definition 9 (Strong diagnosability for processes). *Given CCS process* P *and the observation function* $\mathcal{O}$. *We say that* P *is strongly diagnosable by a predicate* ϕ *over* $Act^\star$ *if there exists a set* V *such that* V *is strongly diagnosable by* ϕ *and* $\mathcal{O}$. *We will denote this by* $\in SDP^{\phi,\mathcal{O}}$.

Theorem 7. $P \in SDP^{\phi,\mathcal{O}}$ *iff* $P' \in SDI^{\phi,\mathcal{O}}$ *for every opening* P' *of* P.

Proof. The proof follows directly from Definition 1 and 9. □

As it is clear from the above theorems that the above mentioned properties have different strengths as regards diagnosability as well as their complements have different strengths as security properties. Now we will quantify these properties.

Definition 10. *Given CPA process $P[\mathcal{A}_1, \ldots, \mathcal{A}_n]$. We define strong surprisal $\mathcal{H}^s(P[V]_\phi^{\mathcal{O}=o})$ of ϕ for process P as*

$$\mathcal{H}^s(P_\phi^{\mathcal{O}=o}) = \min\{\mathcal{H}(P[V]_\phi^{\mathcal{O}=o}) | V = \{A_1, \ldots, A_n\}, A_i \in CCS\}.$$

From Theorem 1 we know that if $\mathcal{H}^s(P_\phi^{\mathcal{O}=o}) = 0$ then there exist intruders $A_1, \ldots, A_n$ which are diagnosable for $P[\mathcal{A}_1, \ldots, \mathcal{A}_n]$, ϕ and $\mathcal{O}$.

Definition 11. *Given CCS process P and a set $V, V = \{A_1, \ldots, A_n\}$ of CCS processes called intruders. We define process surprisal $\mathcal{H}^p(P[V]_\phi^{\mathcal{O}=o})$ of ϕ for intruders V and observation $o, o \neq \epsilon$ as*

$$\mathcal{H}^p(P[V]_\phi^{\mathcal{O}=o}) = \min\{\mathcal{H}(P'[V]_\phi^{\mathcal{O}=o}) | \text{ where } P' \text{ is an openning of } P\}.$$

Again, if $\mathcal{H}^p(P[V]_\phi^{\mathcal{O}=o}) = 0$ then there exists an opening P' of P such that intruders $V = \{A_1, \ldots, A_n\}$ are diagnosable by ϕ and $\mathcal{O}$.

Definition 12. *Given CCS process P. We define strong process surprisal $\mathcal{H}^{sp}(P_\phi^{\mathcal{O}=o})$ of ϕ for process P and observation $o, o \neq \epsilon$ as*

$$\mathcal{H}^{sp}(P_\phi^{\mathcal{O}=o}) = \min\{\mathcal{H}(P'[V]_\phi^{\mathcal{O}=o}) | V = \{A_1, \ldots A_n\}, A_i \in CCS \text{ and } P' \text{ is an openning of } P\}.$$

If $\mathcal{H}^{sp}(P_\phi^{\mathcal{O}=o}) = 0$ then there exist such an opening P' of P and intruders $V = \{A_1, \ldots, A_n\}$ they they are diagnosable by ϕ and $\mathcal{O}$.

5.1 Mutual information flow

Now we will define a quantified variant of NDC. Let A be a finite subset of $Act^*, A \neq \emptyset$. X_A be a corresponding discrete random variable with range A and uniform probability. Let P be a process and let Y_P be a random variable which ranges over $\bigcup_{s \in A} MTr((P|s) \setminus H))$ with uniform probability (string s is considered as process $s.Nil$).

We define the mutual information between X_A and Y_P as follows (see [Gru09]):

$$\mathcal{F}(A \rightsquigarrow P) = \mathcal{I}(X_A, Y_P).$$

We illustrate mutual information by the following example. Note that if two variables are independent then mutual information is equal to zero.

Example 5. Let $P = h.c.Nil + d.Nil$, $A = \{\epsilon, \bar{h}\}$. We have that $\mathcal{F}(A \rightsquigarrow P) = \mathcal{H}(X_A) + \mathcal{H}(Y_P) - \mathcal{H}(X_A, Y_P) = 1 + 1 - 1,58 = 0{,}42$.

Again mutual information can be viewed as a quantification of NDC as it is stated by the following theorem (see [Gru09]).

Theorem 8. *Let $P \notin NDC$ then there exists A such that $\mathcal{F}(A \rightsquigarrow P) > 0$.*

Also an inverse of the previous theorem holds (see [Gru09]).

Theorem 9. *Let for every A, $A \subset Act^*, A \neq \emptyset$ we have $\mathcal{F}(A \rightsquigarrow P) > 0$ for some P. Then $P \notin NDC$.*

Now we define generalizationo of ideas behind NDC as well of NND (see Definition 2).

Definition 13 (Intruders detectable by weak bisimulation). *Given CPA process $P[\mathcal{A}_1, \ldots, \mathcal{A}_n]$ and a set $V, V = \{A_1, \ldots, A_n\}$ of CCS processes called intruders. We say that the intruders V are* detectable by weak bisimulation *if if $P[\mathcal{A}_1/Nil, \ldots, \mathcal{A}_n/Nil]) \not\approx P[\mathcal{A}_1/A_1, \ldots, \mathcal{A}_n/A_n]$. We will denote this by $P[\mathcal{A}_1, \ldots, \mathcal{A}_n] \in DT_V$.*

Theorem 10. *$P \in NDC$ iff $(P|\mathcal{A}) \setminus H \notin DT_V$ for every V such that $V = \{A | sort(A) \subseteq H \cup \{\tau, t\}\}$.*

Proof. Sketch. If process P has NDC property than an observer can distinguish between an absence and presence of an intruder $A|sort(A) \subseteq H \cup \{\tau, t\}$ i.e. such teh intruder is not detectable. □

Definition 14 (Strong detectable by weak bisimulation). *Given CCS process P and a set $V, V = \{A_1, \ldots, A_n\}$ of CCS processes called intruders. We say that the intruders V are* strongly detectable by weak bisimulation *if for every opening $P'[\mathcal{A}_1, \ldots, \mathcal{A}_n]$ of P it holds $P'[\mathcal{A}_1/Nil, \ldots, \mathcal{A}_n/Nil]) \not\approx P'[\mathcal{A}_1/A_1, \ldots, \mathcal{A}_n/A_n]$. We will denote this by $P \in SDT_V$.*

Theorem 11. *$NND \subset (SDT_V)^c$ for every $V, V = \{A_1, \ldots, A_n\}, Sort(A_i) \subseteq H \cup \{\tau, t\}$, where $(SDT_V)^c$ is the set complement of SDT_V.*

Proof. Sketch. Suppose that $P \in NND$. This means that a presence of nested intruders cannot be detected by an observer i.e. P does not belong to $(SDT_V)^c$ for every $V, V = \{A_1, \ldots, A_n\}, Sort(A_i) \subseteq H \cup \{\tau, t\}$. □

Again, both properties DT_V and SDT_V a can be quantified in style of NDC. But instead of doing so we propose detectability by predicate.

Definition 15 (Intruders detectable by a predicate). *Given CPA process $P[\mathcal{A}_1, \ldots, \mathcal{A}_n]$ and a set $V, V = \{A_1, \ldots, A_n\}$ of CCS processes called intruders. We say that the intruders V are* detectable *by a predicate ϕ over $Act^\star$ and by the observation function $\mathcal{O}$ for $P[\mathcal{A}_1, \ldots, \mathcal{A}_n]$ if $P[\mathcal{A}_1/A_1, \ldots, \mathcal{A}_n/A_n]) \notin Op^\phi_\mathcal{O}$ but $P[\mathcal{A}_1/Nil, \ldots, \mathcal{A}_n/Nil]) \in Op^\phi_\mathcal{O}$. We will denote this by $P[\mathcal{A}_1, \ldots, \mathcal{A}_n] \in DT^{\phi,\mathcal{O}}_V$.*

In general, properties *Intruders detectable by a predicate* and *Intruders detectable by weak bisimulation* correspond to different detectability approaches and represent different observational power as well as different requirement on a property we are looking for.

Theorem 12. *There exist CPA processes* $P[\mathcal{A}_1, \ldots, \mathcal{A}_n]$, $P'[\mathcal{A}_1, \ldots, \mathcal{A}_n]$, *a set* $V, V = \{A_1, \ldots, A_n\}$ *of CCS processes, a predicate* ϕ *over* $Act^\star$ *and an observation function* $\mathcal{O}$ *such that* $P[\mathcal{A}_1, \ldots, \mathcal{A}_n] \in DT_V^{\phi,\mathcal{O}}$, $P[\mathcal{A}_1, \ldots, \mathcal{A}_n] \notin DT_V$ *and* $P'[\mathcal{A}_1, \ldots, \mathcal{A}_n] \notin DT_V^{\phi,\mathcal{O}}$, $P'[\mathcal{A}_1, \ldots, \mathcal{A}_n] \in DT_V$.

Proof. Sketch. DT_V property expects different weak trace behaviour of processes with and without intruders. If we take an observational function which does not see τ we can find appropriate processes and an predicate such that for one of them the predicate is more restrictive and for another one less restrictive than weak trace equivalence. □

6 Discussion

For the sake of simplicity we have worked with classical process algebra instead of a probabilistic process algebra (depending on an application one can chose between reactive, generative or stratified probabilistic calculi, see [GSS95]). Using that kind of algebras we could have more adequate tools for expressing probabilities of traces. Instead of that we have used uniform probability distribution but all the concepts and results could be easily translated to a probabilistic calculus. Actually we would have different definitions of $p(MTr(P)^o_\phi)$ which appears in Definition 5 and 6 of surprisal and uncertainty. In the case of mutual information flow ($\mathcal{F}(A \rightsquigarrow P)$) we could associate probabilities also with elements of set A (i.e. X_A could have also other than uniform probability distribution) and with Y_P in $\mathcal{I}(X_A, Y_P)$.

References

[BGMM10] Barbuti R., D.P. Gruska, A. Maggiolo-Schettini and P. Milazzo: A notion of biological diagnosability inspired by the notion of opacity in systems security. Fundamenta Informaticae, Vol. 102, No. 1 (2010), s. 19-34, 2010.

[BKMR06] Bryans J., M. Koutny, L. Mazare and P. Ryan: Opacity Generalised to Transition Systems. In Proceedings of the Formal Aspects in Security and Trust, LNCS 3866, Springer, Berlin, 2006.

[CHM07] Clark D., S. Hunt and P. Malacaria: A Static Analysis for Quantifying the Information Flow in a Simple Imperative Programming Language. The Journal of Computer Security, 15(3). 2007.

[FGM00] Focardi, R., R. Gorrieri, and F. Martinelli: Information flow analysis in a discrete-time process algebra. Proc. 13^{th} Computer Security Foundation Workshop, IEEE Computer Society Press, 2000.

[FGM03] Focardi, R., R. Gorrieri, and F. Martinelli: Real-Time information flow analysis. IEEE Journal on Selected Areas in Communications 21 (2003).

[GSS95] Glabbeek R. J. van, S. A. Smolka and B. Steffen: Reactive, Generative and Stratified Models of Probabilistic Processes Inf. Comput. 121(1): 59-80, 1995.

[GM04] Gorrieri R. and F. Martinelli: A simple framework for real-time cryptographic protocol analysis with compositional proof rules. Science of Computer Programming archive Volume 50, Issue 1-3, 2004.

[GMM10] Gorrieri R., F. Martinelli and I. Matteucci: Specification and Analysis of Information Flow Properties for Distributed Systems. Submitted for publications, 2010.

[Gru10] Diagnosability of nested intruders, Proc. of Bionetics 2010, Springer Verlag, 2010.

[Gru09] Gruska D.P.: Quantifying Security for Timed Process Algebras Fundamenta Informaticae, Vol. 93, No. 1-3, 2009.

[Gru08] Gruska D.P.: Probabilistic information flow security. Fundamenta Informaticae, Vol. 85, No. 1-4, 2008.

[Gru07] Gruska D.P.: Observation Based System Security. Fundamenta Informaticae, vol 79, Numbers 3-4, 2007.

[Gru06a] Gruska D.P.: Information-Flow Security for Restricted Attackers. in Proc. of 8th International Symposium on Systems and Information Security, Sao Jose dos Campos, 2006.

[Gru04] Gruska D.P.: Information Flow in Timing Attacks. Proceedings CS&P'04, 2004.

[Gru03] Gruska D.P. and A. Maggiolo-Schettini: Nested Timing Attacks, in proceedings of FAST'03, Pisa, pp 147-161, 2003.

[GM82] Goguen J.A. and J. Meseguer: Security policies and security models. Proc. of IEEE Symposium on Security and Privacy, 1982.

[L02] Lowe G.: Quantifying information flow". In Proc. IEEE Computer Security Foundations Workshop, 2002.

[Mil89] Milner, R.: *Communication and concurrency.* Prentice-Hall International, New York, 1989.

[SL95] Segala R. and N. Lynch: Probabilistic Simulations for Probabilistic Processes. Nord. J. Comput. 2(2): 250-273, 1995.

[Sh48] Shannon, C. E.: A mathematical theory of communication. Bell System Technical Journal, vol. 27, 1948.