Time-Stamped Claim Logic

João Rasga[1], Cristina Sernadas[1], Erisa Karafili[2], Luca Viganò[3]

[1]Departamento de Matemática, Instituto Superior Técnico and CMAFcIO, ULisboa, Portugal

{joao.rasga,cristina.sernadas}@tecnico.ulisboa.pt

[2]Department of Computing, Imperial College London, UK

e.karafili@imperial.ac.uk

[3]Department of Informatics, King's College London, UK

luca.vigano@kcl.ac.uk

Abstract

The main objective of this paper is to define a logic for reasoning about distributed time-stamped claims. Such a logic is interesting for theoretical reasons, i.e., as a logic *per se*, but also because it has a number of practical applications, in particular when one needs to reason about a huge amount of pieces of evidence collected from different sources, where some of the pieces of evidence may be contradictory and some sources are considered to be more trustworthy than others. We introduce the Time-Stamped Claim Logic including a sound and complete sequent calculus. In order to show how Time-Stamped Claim Logic can be used in practice, we consider a concrete cyber-attribution case study.

Keywords: Time-stamped claim logic, labelled deduction, Gentzen calculus, evidence logic, cyber security.

1 Introduction

The main objective of this paper is to define a logic for reasoning about distributed time-stamped claims. Such a logic is interesting for theoretical reasons, i.e., as a logic *per se*, but also because it has a number of practical applications, most notably the ability to reason about and analyse the evidence left after cyber-attacks, to discover new insights about this evidence, and attribute these attacks.

When reasoning about a cyber-attack, a digital forensics analyst typically collects a large amount of pieces of evidence from different sources [7]. Some of the pieces of evidence may be contradictory [16] and the analyst might consider some sources to be more trustworthy than others. Therefore, inferring conclusions from such evidence requires particular care and time. A similar problem is faced by historians when they are trying to date particular historic events.

The Time-Stamped Claim Logic that we introduce in this paper provides the forensics analyst with a sound and complete calculus for reasoning about the given evidence. More specifically, Time-Stamped Claim Logic is a monotonic propositional logic whose language contains assertions of different kinds: labelled assertions to express statements of agents

about time-stamped claims and relational assertions indexed by propositional symbols that are used to relate agents. In particular, a trust relation with respect to each propositional subject is defined between agents.

We formalize a Gentzen calculus for our logic, which allows one to infer a time-stamped claim whenever (i) there is an agent a that states the claim; (ii) each agent a' that is at least as trustworthy as a with respect to the subject does not state the opposite claim; and (iii) for each agent b stating the opposite claim there is an agent b' at least as trustworthy as b stating the claim. We define a modal and many-valued semantics for our logic, and prove that the calculus is sound and complete with respect to this semantics. In order to show how Time-Stamped Claim Logic can be used in practice, we consider, as a proof of concept, a concrete cyber-attribution case study, inspired by the Ukraine Power Grid Attack that occurred in December 2015.

We proceed as follows. In Section 2, we define the language of Time-Stamped Claim Logic. In Section 3, we formalize a Gentzen calculus for the logic together with a running example. In Section 4, we introduce the semantics, and we then prove the soundness and the completeness of the calculus in Section 5 and Section 6, respectively. In Section 7, we apply Time-Stamped Claim Logic to a realistic case study taken from the cyber-security area. We discuss the most relevant related work in Section 8 and provide some concluding remarks and ideas for future work in Section 9.

2 The Language of Time-Stamped Claim Logic

In this section, we introduce the language of Time-Stamped Claim Logic.

Definition 2.1 *Let P be a non-empty set of propositional symbols and assume fixed non-empty pairwise disjoint sets X_A and X_T of variables, which represent agents names and time points, respectively. The set K_P of* time-stamped propositional claims *is defined as*

$$K_P = \{-(t \cdot p),\ t \cdot p \mid t \in X_T\ and\ p \in P\}$$

■

Definition 2.2 *The* language L_P of assertions *is defined as follows:*

- $K_P \subseteq L_P$;

- $t_1 < t_2 \in L_P$ *whenever* $t_1, t_2 \in X_T$;

- $t_1 \cong t_2 \in L_P$ *whenever* $t_1, t_2 \in X_T$;

- $a_1 \trianglelefteq_p a_2 \in L_P$ *whenever* $a_1, a_2 \in X_A$ *and* $p \in P$;

- $\forall x.\, x \trianglelefteq_p a$ *whenever* $a \in X_A$ *and* $p \in P$;

- $a : \phi \in L_P$ *whenever* $a \in X_A$ *and* $\phi \in K_P$;

- $a : \Box\, \phi \in L_P$ *whenever* $a \in X_A$ *and* $\phi \in K_P$;

- $a :: (\phi_1,\, \ldots,\, \phi_n/\phi)$ *whenever* $a \in X_A$ *and* $\phi, \phi_1, \ldots, \phi_n \in K_P$. ■

Let us briefly discuss the intuitive meaning of these assertions:

- $t \cdot p$ means that p holds at time t.

- $-(t \cdot p)$ means that p does not hold at time t.

- $t_1 < t_2 \in L_P$ establishes that time point t_1 happens before time point t_2.

- $t_1 \cong t_2 \in L_P$ establishes that t_1 and t_2 represent the same time point.

- $a_1 \trianglelefteq_p a_2$ establishes that agent a_2 is at least as trustworthy with respect to p as agent a_1.

- $\forall x.\, x \trianglelefteq_p a$ establishes that a is the most trustworthy agent with respect to statements about p.

- $a : t \cdot p$ states that agent a claims that p holds at time t.

- $a : -(t \cdot p)$ states that agent a claims that p does not hold at time t.

- $a : \boxdot\, t \cdot p$ establishes that there are no agents at least as trustworthy with respect to p as a that state $-(t \cdot p)$. That is, each agent at least as trustworthy with respect to p as a does not claim $-(t \cdot p)$. Similarly, for $a : \boxdot -(t \cdot p)$.

- $a :: (\phi_1,\, \ldots,\, \phi_n/\phi)$ establishes that a states ϕ conditional to statements $\phi_1, \ldots, \phi_n$.

Given the relation of ϕ with respect to the other statements $\phi_1, \ldots, \phi_n$, we will refer to $a :: (\phi_1,\, \ldots,\, \phi_n/\phi)$ as a *derived evidence*. We will instead refer to the previous two assertions $a : \phi$ and $a : \boxdot \phi$ simply as *evidence*. When referring to a general assertion we may use α and β. Observe that the use of the universal quantifier $\forall$ is just a local notation and does not mean that we are dealing with first-order logic.

Let us now illustrate how our logic is used by means of a running example.

Example 2.3 Let us suppose that we want to model a crime situation C that possibly occurred at time t in which there is a potential culprit J and sources $a_1, \ldots, a_6$ providing statements on the case. Let us further suppose that for the source a_1 a person is a culprit provided that the person was at the scene of the crime, is capable of committing the crime and has a motive. Moreover, for source a_5 a person has a motive for committing a crime provided that in the past the person had a serious divergence with the victim. These can be expressed by the assertions

$$a_1 :: (t \cdot \mathrm{inplace}_C^J, t \cdot \mathrm{capable}_C^J, t \cdot \mathrm{motive}_C^J \,/\, t \cdot \mathrm{culprit}_C^J)$$

and

$$a_5 :: (t' \cdot \mathrm{divergence}_C^J, t' < t \,/\, t \cdot \mathrm{motive}_C^J)$$

over $P = \{\mathrm{inplace}_C^J, \mathrm{capable}_C^J, \mathrm{motive}_C^J, \mathrm{culprit}_C^J, \mathrm{divergence}_C^J\}$. Moreover, we can write the assertion

$$\forall x.\, x \trianglelefteq_{\mathrm{motive}_C^J} a_3$$

to express that a_3 is a source recognized to be the most trustworthy with respect to knowing the motive of the potential culprit J. Furthermore, the assumptions

- a_1 is less trustworthy than a_2 with respect to knowing J's motive to commit crime C,

- a_1 claims that J does not have a motive to commit crime C at time t,

- a_2 claims that J has a motive to commit crime C at time t

can be expressed in the Time-Stamped Claim Logic by means of the assertions

- $a_1 \trianglelefteq_{\mathrm{motive}_C^J} a_2$,

- $a_1 : -(t \cdot \mathrm{motive}_C^J)$ and

- $a_2 : t \cdot \mathrm{motive}_C^J$,

respectively. Hence, if a_3 does not have an opinion about whether or not J has a motive to commit crime C at time t, then

- $a_3 : \boxdot\, t \cdot \mathrm{motive}_C^J$ and $a_3 : \boxdot\, -(t \cdot \mathrm{motive}_C^J)$ should hold,

- $a_2 : \boxdot\, t \cdot \mathrm{motive}_C^J$ should hold and $a_2 : \boxdot\, -(t \cdot \mathrm{motive}_C^J)$ should not hold, and

- both $a_1 : \boxdot\, t \cdot \mathrm{motive}_C^J$ and $a_1 : \boxdot\, -(t \cdot \mathrm{motive}_C^J)$ should not hold. ∎

Before we introduce the calculus of our logic, which will allow us to draw conclusions from assertions like the ones in Example 2.3, let us define some useful notation. In this paper, we will write

$$\mathrm{var}_A : \wp L_P \to \wp X_A$$

to denote the map that assigns to each set of assertions the set of elements of X_A that occur in it; *mutatis mutandis* for $\mathrm{var}_T : \wp L_P \to \wp X_T$ and $\mathrm{var}_P : \wp L_P \to \wp P$. We may confuse a singleton set with its unique element. Given $P' \subseteq P$, $X_A' \subseteq X_A$ and $X_T' \subseteq X_T$, we write $L_{P'}^{X_A', X_T'}$ to denote the subset of L_P including all the assertions using only symbols in P' and variables in X_A' and X_T'.

3   The Calculus of Time-Stamped Claim Logic

Let us begin by recalling what is a sequent and an inference rule. Let P be a non-empty set of propositional symbols. A *sequent* over P is a pair (Γ, Δ) and is denoted by

$$\Gamma \to \Delta \,,$$

where Γ and Δ are finite multisets of formulas in L_P. Intuitively, a sequent $\Gamma \to \Delta$ holds whenever an assertion in Δ holds if all the assertions in Γ hold. An *inference rule* over P is of the form

$$\frac{\Gamma_1 \to \Delta_1 \quad \cdots \quad \Gamma_n \to \Delta_n}{\Gamma \to \Delta}\, F$$

where either F is the empty set, and then we present the rule without F, or F is a singleton with a variable in X_A, in which case we present the rule with the variable instead of F. When F is a singleton the variable should be *fresh*, that is, it should not occur in the conclusion of the rule. The sequents $\Gamma_1 \to \Delta_1, \cdots, \Gamma_n \to \Delta_n$ are called the *premises* of the rule and $\Gamma \to \Delta$ the *conclusion* of the rule. A rule with no premises is an *axiom*.

For convenience, below, we will sometimes write

$$--(t \cdot p)$$

to mean $t \cdot p$ and *vice-versa*, in order to avoid the replication of rules NS, NK, SCR, SCL, SKR, and SKL.

Definition 3.1 *The* calculus *over P is composed by the following axioms and inference rules, where we write in parentheses the abbreviated name of the rule:*

- Axiom (Ax)*:*

$$\overline{\beta, \Gamma \to \Delta, \beta}$$

  where β is of the form $a : \phi$, $t_1 < t_2$, $t_1 \cong t_2$ or $a_1 \trianglelefteq_p a_2$

- Cut (Cut)*:*

$$\frac{\beta, \Gamma \to \Delta \qquad \Gamma \to \Delta, \beta}{\Gamma \to \Delta}$$

  where β is of the form $a : \phi$, $t_1 < t_2$, $t_1 \cong t_2$ or $a_1 \trianglelefteq_p a_2$

- Irreflexivity of $<$ (LI)*:*

$$\overline{t < t, \Gamma \to \Delta}$$

- Transitivity of $<$ (LT)*:*

$$\overline{t_1 < t_2, t_2 < t_3, \Gamma \to \Delta, t_1 < t_3}$$

- Connectedness of $<$ (LC)*:*

$$\overline{\Gamma \to \Delta, t_1 < t_2, t_2 < t_1, t_1 \cong t_2}$$

- Reflexivity of $\cong$ (ER)*:*

$$\overline{\Gamma \to \Delta, t \cong t}$$

- Symmetry of $\cong$ (ES)*:*

$$\overline{t_1 \cong t_2, \Gamma \to \Delta, t_2 \cong t_1}$$

- Transitivity of $\cong$ (ET)*:*

$$\overline{t_1 \cong t_2, t_2 \cong t_3, \Gamma \to \Delta, t_1 \cong t_3}$$

- Congruence of $\cong$ for claims and $<$ (EC)*:*

$$\overline{t_1 \cong t_2, [\beta]_{t_2}^{t_1}, \Gamma \to \Delta, \beta}$$

  where $[\beta]_{t_2}^{t_1}$ is a formula obtained from β by replacing t_1 with t_2 and β is either of the form $a : \phi$ or has $<$ as the main constructor,

- Agent preference transitivity (AT):

$$\overline{a_1 \trianglelefteq_p a_2, a_2 \trianglelefteq_p a_3, \Gamma \to \Delta, a_1 \trianglelefteq_p a_3}$$

- Agent preference reflexivity (AR):

$$\overline{\Gamma \to \Delta, a \trianglelefteq_p a}$$

- Agent preference congruence (AC):

$$\overline{a_1 \trianglelefteq_p a_2, a_2 \trianglelefteq_p a_1, [a : \phi]_{a_2}^{a_1}, \Gamma \to \Delta, a : \phi}$$

  where $[a : \phi]_{a_2}^{a_1}$ is a formula obtained from $a : \phi$ by replacing a_1 with a_2

- Agent preference maximum on the right (AMR):

$$\frac{\Gamma \to \Delta, b \trianglelefteq_p a}{\Gamma \to \Delta, \forall x.\, x \trianglelefteq_p a}\; b$$

- Agent preference maximum on the left (AML):

$$\frac{a' \trianglelefteq_p a, \forall x.\, x \trianglelefteq_p a, \Gamma \to \Delta}{\forall x.\, x \trianglelefteq_p a, \Gamma \to \Delta}$$

- Negative statement (NS):

$$\frac{a : -\phi, \Gamma \to \Delta, a : \phi}{a : -\phi, \Gamma \to \Delta}$$

- Negative knowledge (NK):

$$\frac{-\phi, \Gamma \to \Delta, \phi}{-\phi, \Gamma \to \Delta}$$

- Statement confirmation on the right (SCR):

$$\frac{b : -\phi, a \trianglelefteq_{var_P(\phi)} b, \Gamma \to \Delta}{\Gamma \to \Delta, a : \boxdot \phi}\; b$$

- Statement confirmation on the left (SCL):

$$\frac{a : \boxdot \phi, \Gamma \to \Delta, a \trianglelefteq_{var_P(\phi)} a' \qquad a : \boxdot \phi, \Gamma \to \Delta, a' : -\phi}{a : \boxdot \phi, \Gamma \to \Delta}$$

- Extracting knowledge from statement on the right (SKR):

$$\frac{b : -\phi, b : \boxdot -\phi, \Gamma \to \Delta \quad \Gamma \to \Delta, \phi, a : \phi \quad \Gamma \to \Delta, \phi, a : \boxdot \phi}{\Gamma \to \Delta, \phi}\; b$$

- Extracting knowledge on the left (KL):

$$\frac{b : \phi, b : \boxdot \phi, \Gamma \to \Delta}{\phi, \Gamma \to \Delta}\; b$$

- Extracting knowledge from statement on the left (SKL):

$$\frac{\phi, \Gamma \to \Delta, a : -\phi \qquad \phi, \Gamma \to \Delta, a : \boxdot -\phi}{\phi, \Gamma \to \Delta}$$

- Conditional reasoning on the right (CR1):

$$\frac{\phi_1, \ldots, \phi_n, \Gamma \to \Delta, a : \phi}{\Gamma \to \Delta, a :: (\phi_1, \ldots, \phi_n/\phi)}$$

- Conditional reasoning on the left (CR2):

$$\frac{\Gamma \to \Delta, \phi_1 \quad \cdots \quad \Gamma \to \Delta, \phi_n \quad a : \phi, \Gamma \to \Delta}{a :: (\phi_1, \ldots, \phi_n/\phi), \Gamma \to \Delta}$$

∎

Most of the rules are self-explanatory, so let us briefly explain only some of them.

The rule (NS) states that the claims of an agent are not contradictory, in the sense that an agent cannot claim ϕ and $-\phi$. Observe that we do not have the right counterpart of (NS) that introduces $-$ in the right hand side.

The rule (SCR) states that it is possible to conclude $a : \boxdot \phi$ when there is no agent at least as trustworthy as a that claims $-\phi$.

On the other hand, rule (SKR) states that in order to conclude ϕ, it is enough to show that there is an agent a stating ϕ that is not contradicted by an agent at least as trustworthy as a and that each agent b stating the opposite claim is contradicted by an agent at least as trustworthy as b.

Definition 3.2 *The formula in the conclusion of a rule to which the rule is targeted is said to be the* principal formula *of the rule. The formulas in the premises of the rule that are not present in the conclusion, are said to be* side formulas *of the rule.* ∎

For instance, in rule (CR2) the principal formula is $a :: (\phi_1, \ldots, \phi_n/\phi)$ and the side formulas are $\phi_1, \ldots, \phi_n, a : \phi$.

Definition 3.3 *We say that a sequent $\Gamma \to \Delta$ is a* theorem, *written*

$$\vdash \Gamma \to \Delta \,,$$

if there is a finite sequence of sequents

$$\Gamma_1 \to \Delta_1 \cdots \Gamma_n \to \Delta_n$$

such that:

- $\Gamma_1 \to \Delta_1$ *is* $\Gamma \to \Delta$,

- *for each i,*

    - $\Gamma_i \to \Delta_i$ *is either an axiom or the conclusion of a rule where each premise is a sequent $\Gamma_j \to \Delta_j$ in the sequence with $j > i$,*

– *if $i \neq 1$ then $\Gamma_i \rightarrow \Delta_i$ is a premise of a rule with conclusion $\Gamma_j \rightarrow \Delta_j$ with $j < i$ and the other premises of the rule occur in the sequence in a position later than j.*

In this case, the sequence is said to be a derivation for $\Gamma \rightarrow \Delta$ and $\Gamma \rightarrow \Delta$ is said to be derivable. ∎

Observe that in a Gentzen calculus derivations are constructed in a top-down way starting with the initial sequent at the top. Then the derivation proceeds by unfolding the different constructors appearing in the sequent by applying the rules backwards. For the sake of readability, in the derivations that we give below we underline the principal formula(s) of the rule/axiom that is applied.

The notion of derivable can be brought to the realm of formulas.

Definition 3.4 *For $\Psi \cup \{\alpha\} \subseteq L_P$, we say that α is* derivable *from Ψ, denoted by*

$$\Psi \vdash \alpha \,,$$

whenever there is a finite set $\Gamma \subseteq \Psi$ such that $\vdash \Gamma \rightarrow \alpha$. ∎

We now analyze some meta-properties of our logic. We start by establishing weakening on the left and on the right.

Proposition 3.5 (Weakening) *Let Γ, Δ be finite multisets of formulas in L_P. Then, if*

$$\Gamma_1 \rightarrow \Delta_1 \quad \Gamma_2 \rightarrow \Delta_2 \quad \cdots \quad \Gamma_n \rightarrow \Delta_n$$

is a derivation, then there is a derivation

$$\Gamma, \Gamma_1 \rightarrow \Delta_1, \Delta \quad \Gamma, \Gamma_2' \rightarrow \Delta_2', \Delta \quad \cdots \quad \Gamma, \Gamma_n' \rightarrow \Delta_n', \Delta$$

using the same rules by the same order over the same formulas modulo a renaming of fresh variables.

Proof: We start by renaming the fresh variables used in the given derivation to variables not appearing in $\Gamma \cup \Delta$. Then, the result follows by a straightforward induction. QED

The following meta-theorem proves that evidence claimed by less trustworthy agents is not important.

Proposition 3.6 (Transitivity of Evidence) *Let $a : \phi, \forall x.x \trianglelefteq_{var_P(\phi)} a, \Gamma \rightarrow \Delta, \phi$ be a sequent over P. Then,*

$$\vdash a : \phi, \forall x.x \trianglelefteq_{var_P(\phi)} a, \Gamma \rightarrow \Delta, \phi.$$

Proof: As shown in Figure 1, we have that

$$\vdash a : \phi, \forall x.x \trianglelefteq_{\mathrm{var}_P(\phi)} a \rightarrow \phi.$$

Then, the thesis follows by Proposition 3.5. QED

8

1	$a : \phi, \forall x. \trianglelefteq_{\mathrm{var}_P(\phi)} a \to \underline{\phi}$	SKR:2,3,4
2	$b : -\phi, \underline{b : \Box - \phi}, a : \phi, \forall x. \trianglelefteq_{\mathrm{var}_P(\phi)} a \to$	SCL:5,6
3	$\underline{a : \phi}, \forall x. \trianglelefteq_{\mathrm{var}_P(\phi)} a \to \phi, \underline{a : \phi}$	Ax
4	$a : \phi, \forall x. \trianglelefteq_{\mathrm{var}_P(\phi)} a \to \phi, \underline{a : \Box\,\phi}$	SCR:8
5	$b : -\phi, b : \Box - \phi, a : \phi, \underline{\forall x. \trianglelefteq_{\mathrm{var}_P(\phi)} a} \to b \trianglelefteq_{\mathrm{var}_P(\phi)} a$	AML:7
6	$b : -\phi, b : \Box - \phi, \underline{a : \phi}, \forall x. \trianglelefteq_{\mathrm{var}_P(\phi)} a \to \underline{a : \phi}$	Ax
7	$\underline{b \trianglelefteq_{\mathrm{var}_P(\phi)} a}, b : -\phi, b : \Box - \phi, a : \phi, \forall x. \trianglelefteq_{\mathrm{var}_P(\phi)} a \to \underline{b \trianglelefteq_{\mathrm{var}_P(\phi)} a}$	Ax
8	$b : -\phi, a \trianglelefteq_{\mathrm{var}_P(\phi)} b, a : \phi, \underline{\forall x. \trianglelefteq_{\mathrm{var}_P(\phi)} a} \to \phi$	AML:9
9	$b \trianglelefteq_{\mathrm{var}_P(\phi)} a, \underline{b : -\phi}, a \trianglelefteq_{\mathrm{var}_P(\phi)} b, a : \phi, \forall x. \trianglelefteq_{\mathrm{var}_P(\phi)} a \to \phi$	NS:10
10	$\underline{b \trianglelefteq_{\mathrm{var}_P(\phi)} a}, b : -\phi, \underline{a \trianglelefteq_{\mathrm{var}_P(\phi)} b}, \underline{a : \phi}, \forall x. \trianglelefteq_{\mathrm{var}_P(\phi)} a \to \phi, \underline{b : \phi}$	AC

Figure 1: Derivation of $a : \phi, \forall x. \trianglelefteq_{\mathrm{var}_P(\phi)} a \to \phi$

Taking into account Proposition 3.5, given a derivation $\mathcal{D}$, we denote by

$$\mathcal{D}[\Gamma \to \Delta]$$

the derivation obtained from $\mathcal{D}$ by adding Γ on the left hand side and Δ to the right hand side of each sequent in $\mathcal{D}$ modulo an appropriate renaming of fresh variables in $\mathcal{D}$.

We now show that derived agent evidence is transitive.

Proposition 3.7 *Let us assume that*

$$a_1 : \phi_1 \vdash a_2 : \phi_2 \quad and \quad a_2 : \phi_2 \vdash a_3 : \phi_3,$$

then we can conclude the following:

$$a_1 : \phi_1 \vdash a_3 : \phi_3.$$

Proof: Let $\mathcal{D}_1$ and $\mathcal{D}_2$ be derivations for

$$\vdash a_1 : \phi_1 \to a_2 : \phi_2 \quad and \quad \vdash a_2 : \phi_2 \to a_3 : \phi_3,$$

respectively. The derivation in Figure 2 shows that $\vdash a_1 : \phi_1 \to a_3 : \phi_3$ where m is the length of $\mathcal{D}_2[a_1 : \phi_1 \to]$. QED

Finally, we show that the logic is monotonic.

Proposition 3.8 *Let $\Psi \cup \{\alpha\} \subseteq L_P$ be such that $\Psi \vdash \alpha$. Then*

$$\Psi' \vdash \alpha$$

for every $\Psi' \supseteq \Psi$.

$$\begin{array}{ll} 1 & a_1 : \phi_1 \to a_3 : \phi_3 \qquad\qquad\qquad \text{Cut:2,m} \\[6pt] 2 & a_2 : \phi_2, a_1 : \phi_1 \to a_3 : \phi_3 \\[6pt] & \qquad\qquad\qquad \mathcal{D}_2[a_1 : \phi_1 \to] \\[6pt] \text{m} & a_1 : \phi_1 \to a_3 : \phi_3, a_2 : \phi_2 \\[6pt] & \qquad\qquad\qquad \mathcal{D}_1[\to a_3 : \phi_3] \end{array}$$

Figure 2: Derivation of $a_1 : \phi_1 \to a_3 : \phi_3$

Proof: Let $\Psi' \supseteq \Psi$ and $\Gamma \subseteq \Psi$ be a finite set such that $\vdash \Gamma \to \alpha$. Since $\Gamma \subseteq \Psi'$ then, by definition, $\Psi' \vdash \alpha$. QED

Example 3.9 Let us return to the crime situation described in Example 2.3. Let P be the set composed by the following propositional symbols: inplace_C^J, capable_C^J, motive_C^J, culprit_C^J, divergence_C^J, $\text{guilty}_{C'}^J$ and $\text{similar}_{C'}^C$. Let Γ be the set containing the assertions

- $\psi_1 = a_1 :: (t \cdot \text{inplace}_C^J, t \cdot \text{capable}_C^J, t \cdot \text{motive}_C^J \ / \ t \cdot \text{culprit}_C^J)$

- $\psi_2 = a_2 :: (t \cdot \text{motive}_C^J \ / \ t \cdot \text{culprit}_C^J)$

- $\psi_3 = a_3 :: (-(t \cdot \text{capable}_C^J)/ -(t \cdot \text{culprit}_C^J))$

- $\psi_4 = a_4 :: (t'' \cdot \text{guilty}_{C'}^J, t \cdot \text{similar}_{C'}^C, t'' < t \ / \ t \cdot \text{capable}_C^J)$

- $\psi_5 = a_5 :: (t' \cdot \text{divergence}_C^J, t' < t \ / \ t \cdot \text{motive}_C^J)$

- $\psi_6 = a_6 : t' \cdot \text{divergence}_C^J$

- $\psi_7 = t' < t$

- $\delta_1 = \forall x. \, x \trianglelefteq_{\text{motive}_C^J} a_5$

- $\delta_2 = \forall x. \, x \trianglelefteq_{\text{divergence}_C^J} a_6$

and let Δ be the singleton set with the assertion $a_2 : t \cdot \text{culprit}_C^J$. The derivation in Figure 3 establishes that $\Gamma \to \Delta$ is derivable. ∎

We will show the use of Time-Stamped Claim Logic on a more complex case study in Section 7.

4 The Semantics of Time-Stamped Claim Logic

In this section, we define the semantics of Time-Stamped Claim Logic. In the following sections, we will then prove the soundness and completeness of the sequent calculus with respect to this semantics. We start by introducing the notion of interpretation structure, which has a modal and many-valued flavour.

1	$\psi_1, \underline{\psi_2}, \ldots, \psi_7, \delta_1, \delta_2 \to a_2 : t \cdot \text{culprit}_C^J$	CR2:2,3
2	$\psi_1, \psi_3, \ldots, \underline{\psi_5}, \psi_6, \psi_7, \delta_1, \delta_2 \to a_2 : t \cdot \text{culprit}_C^J, t \cdot \text{motive}_C^J$	CR2:4,5,6
3	$\underline{a_2 : t \cdot \text{culprit}_C^J}, \psi_1, \psi_3, \ldots, \psi_7, \delta_1, \delta_2 \to \underline{a_2 : t \cdot \text{culprit}_C^J}$	Ax
4	$\psi_1, \psi_3, \psi_4, \psi_6, \psi_7, \delta_1, \delta_2 \to a_2 : t \cdot \text{culprit}_C^J, t \cdot \text{motive}_C^J, \underline{t' \cdot \text{divergence}_C^J}$	SKR:7,8,9
5	$a_5 : t \cdot \text{motive}_C^J, \psi_1, \psi_3, \psi_4, \psi_6, \psi_7, \delta_1, \delta_2 \to a_2 : t \cdot \text{culprit}_C^J, \underline{t \cdot \text{motive}_C^J}$	(Prop. 3.6)
6	$\psi_1, \psi_3, \psi_4, \underline{\psi_6}, \psi_7, \delta_1, \delta_2 \to a_2 : t \cdot \text{culprit}_C^J, t \cdot \text{motive}_C^J, \underline{t' < t}$	Ax
7	$b : -(t' \cdot \text{divergence}_C^J), \underline{b : \boxdot -(t' \cdot \text{divergence}_C^J)}, \psi_1, \psi_3, \psi_4, \psi_6, \psi_7, \delta_1, \delta_2$ $\to a_2 : t \cdot \text{culprit}_C^J, \underline{t \cdot \text{motive}_C^J}$	SCL:13,14
8	$\psi_1, \psi_3, \psi_4, \psi_6, \underline{\psi_7}, \delta_1, \delta_2 \to a_2 : t \cdot \text{culprit}_C^J, t \cdot \text{motive}_C^J, t' \cdot \text{divergence}_C^J,$ $\underline{a_6 : t' \cdot \text{divergence}_C^J}$	Ax
9	$\psi_1, \psi_3, \psi_4, \psi_6, \psi_7, \delta_1, \delta_2 \to a_2 :: t \cdot \text{culprit}_C^J, t \cdot \text{motive}_C^J, t' \cdot \text{divergence}_C^J,$ $\underline{a_6 : \boxdot t' \cdot \text{divergence}_C^J}$	SCR:10
10	$\underline{b : -(t' \cdot \text{divergence}_C^J)}, a_6 : \trianglelefteq_{\text{divergence}_C^J} b, \psi_1, \psi_3, \psi_4, \psi_6, \psi_7, \delta_1, \delta_2$ $\to a_2 : t \cdot \text{culprit}_C^J, t \cdot \text{motive}_C^J, t' \cdot \text{divergence}_C^J$	NS:11
11	$b : -(t' \cdot \text{divergence}_C^J), a_6 : \trianglelefteq_{\text{divergence}_C^J} b, \psi_1, \psi_3, \psi_4, \psi_6, \psi_7, \delta_1, \underline{\delta_2} \to$ $a_2 : t \cdot \text{culprit}_C^J, t \cdot \text{motive}_C^J, t' \cdot \text{divergence}_C^J, b : t' \cdot \text{divergence}_C^J$	AML:12
12	$\underline{b \trianglelefteq_{\text{divergence}_C^J} a_6}, b : -(t' \cdot \text{divergence}_C^J), \underline{a_6 : \trianglelefteq_{\text{divergence}_C^J} b},$ $\psi_1, \psi_3, \psi_4, \underline{\psi_6}, \psi_7, \delta_1, \delta_2 \to a_2 : t \cdot \text{culprit}_C^J, t \cdot \text{motive}_C^J,$ $t' \cdot \text{divergence}_C^J, \underline{b : t' \cdot \text{divergence}_C^J}$	AC
13	$b : -(t' \cdot \text{divergence}_C^J), b : \boxdot -(t' \cdot \text{divergence}_C^J), \psi_1, \psi_3, \psi_4, \psi_6, \psi_7, \delta_1, \underline{\delta_2}$ $\to a_2 : t \cdot \text{culprit}_C^J, t \cdot \text{motive}_C^J, b \trianglelefteq_{\text{divergence}_C^J} a_6$	AML:15
14	$b : -(t' \cdot \text{divergence}_C^J), b : \boxdot -(t' \cdot \text{divergence}_C^J), \psi_1, \psi_3, \psi_4, \underline{\psi_6}, \psi_7, \delta_1, \delta_2$ $\to a_2 : t \cdot \text{culprit}_C^J, t \cdot \text{motive}_C^J, \underline{a_6 : t' \cdot \text{divergence}_C^J}$	Ax
15	$\underline{b \trianglelefteq_{\text{divergence}_C^J} a_6}, b : -(t' \cdot \text{divergence}_C^J), b : \boxdot -(t' \cdot \text{divergence}_C^J),$ $\psi_1, \psi_3, \psi_4, \psi_6, \delta_1, \delta_2 \to a_2 : t \cdot \text{culprit}_C^J, t \cdot \text{motive}_C^J, \underline{b \trianglelefteq_{\text{divergence}_C^J} a_6}$	Ax

Figure 3: Derivation of $\psi_1, \ldots, \psi_7, \delta_1, \delta_2 \to a_2 : t \cdot \text{culprit}_C^J$

Definition 4.1 *An* interpretation structure *over a non-empty set P of propositional symbols is a tuple*

$$I = (D_A, D_T, <^I, \cong^I, \{\trianglelefteq_p^I\}_{p \in P}, V^+, V^-)$$

such that

- D_A *and D_T are non-empty sets,*

- $<^I$ *is an irreflexive, transitive and connected relation over D_T,*

- $\cong^I$ *is an equivalence relation over D_T such that, assuming that $t_1 \cong^I t_2$,*

  - *if $t_1 <^I t_3$ then $t_2 <^I t_3$,*
  - *if $t_3 <^I t_1$ then $t_3 <^I t_2$,*

- $\trianglelefteq^I_p$ is a transitive and reflexive binary relation over D_A for each $p \in P$,

- $V^+, V^- \subseteq P \times D_A \times D_T$ such that

$$V^+ \cap V^- = \emptyset$$

   and for every $p \in P$, $d \in D_A$ and $n, n' \in D_T$,

  - $(p, d, n) \in V^+$ if and only if $(p, d, n') \in V^+$ whenever $n \cong^I n'$,
  - $(p, d, n) \in V^-$ if and only if $(p, d, n') \in V^-$ whenever $n \cong^I n'$,
  - $(p, d, n) \in V^+$ if and only if $(p, d', n) \in V^+$ whenever $d \trianglelefteq^I_p d'$ and $d' \trianglelefteq^I_p d$,
  - $(p, d, n) \in V^-$ if and only if $(p, d', n) \in V^-$ whenever $d \trianglelefteq^I_p d'$ and $d' \trianglelefteq^I_p d$.

In an interpretation structure, $(p, d, n) \in V^+$ means that agent d claims that p holds at time n, $(p, d, n) \in V^-$ means that agent d claims that p does not hold at time n and $(p, d, n) \notin V^+ \cup V^-$ means that agent d does not have an opinion about whether or not p holds at time n.

An *assignment* ρ over I is a pair (ρ_A, ρ_T) such that $\rho_A : X_A \to D_A$ and $\rho_T : X_T \to D_T$ are maps. Moreover, we say that assignments ρ and ρ' are *equivalent up to* $b \in X_A$, written

$$\rho \equiv^A_b \rho',$$

whenever $\rho'_T = \rho_T$ and $\rho'_A(a) = \rho_A(a)$ for every $a \in X_A \setminus \{b\}$.

Given an interpretation structure I over P and an assignment ρ over I, satisfaction of an assertion α by I and ρ, denoted by

$$I\rho \Vdash \alpha,$$

is defined as follows

- $I\rho \Vdash t_1 < t_2$ whenever $\rho_T(t_1) <^I \rho_T(t_2)$,

- $I\rho \Vdash t_1 \cong t_2$ whenever $\rho_T(t_1) \cong^I \rho_T(t_2)$,

- $I\rho \Vdash a_1 \trianglelefteq_p a_2$ whenever $\rho_A(a_1) \trianglelefteq^I_p \rho_A(a_2)$,

- $I\rho \Vdash \forall x. x \trianglelefteq_p a$ whenever $d \trianglelefteq^I_p \rho_A(a)$ for every $d \in D_A$,

- $I\rho \Vdash a : \phi$ whenever $(p, \rho_A(a), \rho_T(t)) \in \begin{cases} V^+ & \text{if } \phi \text{ is } t \cdot p \\ V^- & \text{if } \phi \text{ is } -(t \cdot p), \end{cases}$

- $I\rho \Vdash a : \Box \phi$ whenever, for each assignment ρ' and $b \in X_A$ such that $\rho' \equiv^A_b \rho$, if $I\rho' \Vdash a \trianglelefteq_{var_P(\phi)} b$ then $I\rho' \nVdash b : -\phi$,

- $I\rho \Vdash \phi$ whenever

  - for each assignment ρ' and $b \in X_A$ with $\rho' \equiv^A_b \rho$, if $I\rho' \Vdash b : -\phi$ then $I\rho' \nVdash b : \Box -\phi$,

  - there are assignment ρ' and $a \in X_A$ with $\rho' \equiv^A_a \rho$, $I\rho' \Vdash a : \phi$ and $I\rho' \Vdash a : \Box \phi$,

- $I\rho \Vdash a :: (\phi_1, \ldots, \phi_n/\phi)$ whenever if $I\rho \Vdash \phi_i$ for $i = 1, \ldots, n$ then $I\rho \Vdash a : \phi$. $\blacksquare$

Observe that a time-stamped claim ϕ holds whenever (i) there is an agent a that states the claim ϕ; (ii) each agent a' that is at least as trustworthy as a with respect to the subject does not state the opposite claim $-\phi$; and (iii) for each agent b stating the opposite claim $-\phi$, there is an agent b' at least as trustworthy as b stating the claim ϕ.

Observe also that the following is possible:

$$I\rho \not\Vdash a : \phi \quad \text{and} \quad I\rho \not\Vdash a : -\phi.$$

To simplify the presentation, given a set $\Gamma \subseteq L_P$, we will write

$$I\rho \Vdash \Gamma$$

whenever $I\rho \Vdash \gamma$ for each $\gamma \in \Gamma$.

Definition 4.2 *Given $\Psi \subseteq L_P$ and $\alpha \in L_P$, we say that Ψ entails α, denoted by*

$$\Psi \vDash \alpha \,,$$

whenever for every interpretation structure I and assignment ρ over I, we have

$$I\rho \Vdash \alpha \quad \text{if} \quad I\rho \Vdash \Psi \,.$$

$\blacksquare$

5   Soundness

In this section, we prove that the theorems derived using the calculus of Time-Stamped Claim Logic introduced in Section 3 are valid according to the semantics introduced in Section 4. We start by providing some relevant semantic notions related to sequents.

Definition 5.1 *We say that an interpretation structure I and an assignment ρ satisfy a sequent $\Gamma \to \Delta$, denoted by*

$$I\rho \Vdash \Gamma \to \Delta \,,$$

whenever $I\rho \Vdash \delta$ for some $\delta \in \Delta$ if $I\rho \Vdash \Gamma$. We say that a sequent $\Gamma \to \Delta$ is valid, denoted by

$$\vDash \Gamma \to \Delta \,,$$

whenever it is satisfied by every interpretation structure I and assignment ρ. We say that I and ρ satisfy a rule with the fresh variable b,

$$\frac{\Gamma_1 \to \Delta_1 \quad \cdots \quad \Gamma_n \to \Delta_n}{\Gamma \to \Delta} \, b \,,$$

whenever $I\rho \Vdash \Gamma \to \Delta$ if $I\rho' \Vdash \Gamma_i \to \Delta_i$ for $i = 1, \ldots, n$ for every ρ' such that $\rho' \equiv_b^A \rho$. We say that I and ρ satisfy a rule without a fresh variable,

$$\frac{\Gamma_1 \to \Delta_1 \quad \cdots \quad \Gamma_n \to \Delta_n}{\Gamma \to \Delta} \,,$$

whenever $I\rho \Vdash \Gamma \to \Delta$ if $I\rho \Vdash \Gamma_i \to \Delta_i$ for $i = 1, \ldots, n$. Finally, we say that a rule is sound whenever it is satisfied by every interpretation structure and assignment. $\blacksquare$

The proof of the following proposition is in Appendix A.

Proposition 5.2 *The rules of the sequent calculus are sound.*

The soundness of the rules can be used to show the soundness of deductive consequences.

Proposition 5.3 *Let $\Gamma \to \Delta$ be a sequent over P. Then $\vDash \Gamma \to \Delta$ whenever $\vdash \Gamma \to \Delta$.*

Proof: The proof is by induction on the length of a derivation $\Gamma_1 \to \Delta_1 \cdots \Gamma_n \to \Delta_n$ of $\Gamma \to \Delta$. The base case follows straightforwardly by Proposition 5.2.

For the step case, let us assume that $\Gamma_1 \to \Delta_1$ follows from rule u of the calculus applied to sequents $\Gamma_{i_j} \to \Delta_{i_j}$ for $j = 1, \dots, k$. Then $\vdash \Gamma_{i_j} \to \Delta_{i_j}$ for $j = 1, \dots, k$. Hence, by the induction hypothesis, $\vDash \Gamma_{i_j} \to \Delta_{i_j}$ for $j = 1, \dots, k$. Let I be an interpretation structure, ρ an assignment and ρ' an assignment equivalent modulo the fresh variable of u to ρ. Then $I\rho' \Vdash \Gamma_{i_j} \to \Delta_{i_j}$ for $j = 1, \dots, k$ since $\vDash \Gamma_{i_j} \to \Delta_{i_j}$ for $j = 1, \dots, k$. Taking into account that u is sound, by Proposition 5.2, we conclude that $I\rho \Vdash \Gamma_1 \to \Delta_1$. $\hspace{2em}$ QED

Capitalizing on the soundness at the sequent level, we can establish soundness at the level of assertions.

Proposition 5.4 *Let $\Psi \subseteq L_P$ and $\alpha \in L_P$. Then $\Psi \vDash \alpha$ whenever $\Psi \vdash \alpha$.*

Proof: Let us assume that $\Psi \vdash \alpha$. Then there is a finite set $\Gamma \subseteq \Psi$ such that $\vdash \Gamma \to \alpha$. Thus, by Proposition 5.3, $\vDash \Gamma \to \alpha$. Let I be an interpretation structure and ρ an assignment such that $I\rho \Vdash \Psi$. Therefore, $I\rho \Vdash \Gamma$ and so $I\rho \Vdash \alpha$. $\hspace{2em}$ QED

6 Completeness

In this section, we show that Time-Stamped Claim Logic is complete using a Hintikka style technique. We consider Hintikka pairs instead of just Hintikka sets since the logic does not have a classical negation over all assertions.

Definition 6.1 *A Hintikka pair over $P' \subseteq P$, $X'_A \subseteq X_A$ and $X'_T \subseteq X_T$ is a pair (Ψ_L, Ψ_R) of sets of assertions in $L_{P'}^{X'_A, X'_T}$ such that:*

- *either $\beta \notin \Psi_L$ or $\beta \notin \Psi_R$ for each $\beta \in L_{P'}^{X'_A, X'_T}$ of the form $a : \phi$, $t_1 < t_2$, $t_1 \cong t_2$ and $a_1 \trianglelefteq_p a_2$,*

- *either $\beta \in \Psi_L$ or $\beta \in \Psi_R$ for each $\beta \in L_{P'}^{X'_A, X'_T}$ of the form $a : \phi$, $t_1 < t_2$, $t_1 \cong t_2$ and $a_1 \trianglelefteq_p a_2$,*

- *$t < t \notin \Psi_L$,*

- *if $t_1 < t_2, t_2 < t_3 \in \Psi_L$ then $t_1 < t_3 \notin \Psi_R$,*

- *if $t_1 \cong t_2, t_2 \cong t_3 \in \Psi_L$ then $t_1 \cong t_3 \notin \Psi_R$,*

- *if $a_1 \trianglelefteq_p a_2, a_2 \trianglelefteq_p a_3 \in \Psi_L$ then $a_1 \trianglelefteq_p a_3 \notin \Psi_R$,*

- *$t \cong t \notin \Psi_R$,*

- $a_1 \trianglelefteq_p a_1 \notin \Psi_R$,

- either $t_1 < t_2 \notin \Psi_R$ or $t_2 < t_1 \notin \Psi_R$ or $t_1 \cong t_2 \notin \Psi_R$,

- if $t_1 \cong t_2 \in \Psi_L$ then $t_2 \cong t_1 \notin \Psi_R$,

- if $t_1 \cong t_2, [\beta]_{t_2}^{t_1} \in \Psi_L$ then $\beta \notin \Psi_R$, where β is either of the form $a : \phi$ or has $<$ as the main constructor,

- if $a_1 \trianglelefteq_p a_2, a_2 \trianglelefteq_p a_1, [a : \phi]_{a_2}^{a_1} \in \Psi_L$ then $a : \phi \notin \Psi_R$,

- if $\forall x. x \trianglelefteq_p a \in \Psi_R$ then there is $a' \in X_A'$ such that $a' \trianglelefteq_p a \in \Psi_R$,

- if $\forall x. x \trianglelefteq_p a \in \Psi_L$ then $a_1 \trianglelefteq_p a \in \Psi_L$ for each $a_1 \in X_A'$,

- if $a : \phi \in \Psi_L$ then $a : -\phi \in \Psi_R$,

- if $a : \boxdot \phi \in \Psi_R$ then there is $a' \in X_A'$ such that $a \trianglelefteq_{var(\phi)} a', a' : -\phi \in \Psi_L$,

- if $a : \boxdot \phi \in \Psi_L$ then, for each $a' \in X_A'$ either $a \trianglelefteq_{var(\phi)} a' \in \Psi_R$ or $a' : -\phi \in \Psi_R$,

- if $\phi \in \Psi_R$ then either there exists $a' \in X_A'$ such that $a' : -\phi, a' : \boxdot -\phi \in \Psi_L$ or for each $a \in X_A'$ either $a : \phi \in \Psi_R$ or $a : \boxdot \phi \in \Psi_R$,

- if $\phi \in \Psi_L$ then there is $a' \in X_A'$ such that $a' : \phi, a' : \boxdot \phi \in \Psi_L$ and for each $a \in X_A'$ either $a : -\phi \in \Psi_R$ or $a : \boxdot -\phi \in \Psi_R$,

- if $a :: (\phi_1, \ldots, \phi_n/\phi) \in \Psi_R$ then if $\phi_1, \ldots, \phi_n \in \Psi_L$ then $a : \phi \in \Psi_R$,

- if $a :: (\phi_1, \ldots, \phi_n/\phi) \in \Psi_L$ then either $\phi_i \in \Psi_R$ for some $i = 1, \ldots, n$ or $a : \phi \in \Psi_L$. ∎

We now show that for each Hintikka pair there are an interpretation structure and an assignment satisfying all the assertions in the first component of the pair and not satisfying each assertion in the second component.

The proof of the following proposition can be found in Appendix A.

Proposition 6.2 *Let $H = (\Psi_L, \Psi_R)$ be a Hintikka pair over P', X_A' and X_T'. Then there are an interpretation structure I_H over P' and an assignment ρ over I_H such that $I_H \rho \Vdash \psi$ for each $\psi \in \Psi_L$ and $I_H \rho \nVdash \psi$ for each $\psi \in \Psi_R$.*

The main objective now is to show that if a sequent is not derivable then there is an interpretation structure that falsifies it. For this purpose, we must introduce the concept of (deductive) expansion of a sequent. An expansion follows the same conditions and steps of a derivation but is more general. In fact, in an expansion the terminal sequents may not be axioms or there are sequents expanded over and over.

Definition 6.3 *An* expansion *of a sequent $\Gamma \to \Delta$ is a (finite or infinite) sequence of sequents $\Gamma_1 \to \Delta_1 \cdots$ such that:*

- *$\Gamma_1 \to \Delta_1$ is $\Gamma \to \Delta$;*

- *for each $i \neq 1$, $\Gamma_i \to \Delta_i$ is a premise of a rule with conclusion $\Gamma_j \to \Delta_j$ with $j < i$ and all the other premises of the rule occur in the sequence in a position later than j.* ∎

Observe that every derivation is an expansion but not vice versa. From an expansion fulfilling conditions described below, we will define an interpretation structure that falsifies the first sequent in the expansion. We need first to introduce the concept of branch. A branch is a path of the derivation starting in the initial sequent.

Definition 6.4 *A* branch *of an expansion of a sequent* $\Gamma \to \Delta$ *is a subsequence of the expansion starting with* $\Gamma \to \Delta$ *where each element other than the first is a premise of a rule applied in the expansion to a sequent appearing immediately before in the branch. Furthermore, for each sequent in the branch which is the conclusion of a rule used in the expansion, a premise of the rule is the next sequent of the branch.* ∎

For simplicity, we present a branch as a sequence $\Gamma'_1 \to \Delta'_1 \; \Gamma'_2 \to \Delta'_2 \; \cdots$ instead of using the numbering of each sequent of the branch in the expansion. Observe that a branch is always rooted in the sense that it starts with the first element of the expansion.

The following concept of analytical branch captures the idea that the rules applied respect the context that we have in the sense that the symbols used are present explicitly or implicitly in the formulas of the branch. Furthermore, a rule is only applied whenever it brings added information.

Definition 6.5 *We say that a finite branch* $\Gamma'_1 \to \Delta'_1 \cdots \Gamma'_n \to \Delta'_n$ *of an expansion* $\Gamma_1 \to \Delta_1 \; \cdots$ *is* analytical *whenever for each* $j = 2, \ldots, n$, *if* $\Gamma'_j \to \Delta'_j$ *is a premise of a rule* u, *then*

1. *either there is a side formula in the left hand side of a premise of* u *in the expansion which does not occur in* $\bigcup_{i=1}^{j-1} \Gamma'_i$ *not involving fresh variables or there is a side formula in the right hand side of a premise of* u *in the expansion which does not occur in* $\bigcup_{i=1}^{j-1} \Delta'_i$ *not involving fresh variables;*

2. *the time, the propositional and the non fresh agent variables of* $(\Gamma'_j \setminus \Gamma'_{j-1}) \cup (\Delta'_j \setminus \Delta'_{j-1})$ *are in* $\bigcup_{i=1}^{j-1} \Gamma'_i \cup \Delta'_i$;

3. *if* u *has a fresh agent variable in* $(\Gamma'_j \setminus \Gamma'_{j-1}) \cup (\Delta'_j \setminus \Delta'_{j-1})$ *then such a variable is not in* $\Gamma'_{j-1} \cup \Delta'_{j-1}$.

An analytical branch $\Gamma'_1 \to \Delta'_1 \cdots \Gamma'_n \to \Delta'_n$ *is* exhausted *whenever each branch that results from applying a rule to* $\Gamma'_n \to \Delta'_n$ *is not analytical in the augmented expansion. An analytical exhausted branch is* closed *whenever the last sequent is an axiom. Otherwise, it is said to be* open. *An expansion is* open *when it has an open analytical exhausted branch.* ∎

The proof of the following proposition is in Appendix A.

Proposition 6.6 *Let* $\Gamma'_1 \to \Delta'_1 \cdots \Gamma'_n \to \Delta'_n$ *be an open analytical exhausted branch of an expansion* $\Gamma_1 \to \Delta_1 \; \cdots$. *Then*

$$\left(\bigcup_{i=1}^{n} \Gamma'_i, \bigcup_{i=1}^{n} \Delta'_i \right)$$

is a Hintikka pair over $var_P(\bigcup_{i=1}^{n} \Gamma'_i \cup \Delta'_i)$, $var_A(\bigcup_{i=1}^{n} \Gamma'_i \cup \Delta'_i)$ *and* $var_T(\bigcup_{i=1}^{n} \Gamma'_i \cup \Delta'_i)$.

Proposition 6.7 *If a sequent is not a theorem, then it has an expansion with an open analytical exhausted branch.*

Proof: It is straightforward to see that every sequent has an expansion where all branches are analytical and exhausted. Furthermore, if all the branches in that expansion are not open, then the expansion is a derivation. QED

Capitalizing on the previous results in this section, we are able to establish the completeness result at the level of sequents.

Proposition 6.8 *If a sequent is valid, then it is a theorem.*

Proof: Let us assume that the sequent $\Gamma \to \Delta$ is not a theorem. Then, by Proposition 6.7, it has an expansion with an open analytical exhausted branch $\Gamma'_1 \to \Delta'_1 \cdots \Gamma'_n \to \Delta'_n$. So, by Proposition 6.6, there is a Hintikka pair $H = (\Psi_L, \Psi_R)$ over $\mathrm{var}_P(\bigcup_{i=1}^n \Gamma'_i \cup \Delta'_i)$, $\mathrm{var}_A(\bigcup_{i=1}^n \Gamma'_i \cup \Delta'_i)$ and $\mathrm{var}_T(\bigcup_{i=1}^n \Gamma'_i \cup \Delta'_i)$ such that $\Gamma \subseteq \Psi_L$ and $\Delta \subseteq \Psi_R$. Hence, by Proposition 6.2, there are an interpretation structure I_H over $\mathrm{var}_P(\bigcup_{i=1}^n \Gamma'_i \cup \Delta'_i)$ and an assignment ρ over I_H such that $I_H \rho \Vdash \Gamma$ and $I_H \rho \nVdash \delta$ for each $\delta \in \Delta$. Let I be an interpretation structure over P such that I_H is the reduct of I to $\mathrm{var}_P(\bigcup_{i=1}^n \Gamma'_i \cup \Delta'_i)$. Observe that ρ is also an assignment over I. Hence, $I \rho \Vdash \Gamma$ and $I \rho \nVdash \delta$ for each $\delta \in \Delta$. Therefore, $I \rho \nVdash \Gamma \to \Delta$ and so $\Gamma \to \Delta$ is not valid. QED

Finally, we can show that Time-Stamped Claim Logic is complete.

Proposition 6.9 *Let $\Gamma \subseteq L_P$ be a finite set and $\alpha \in L_P$. Then $\Gamma \vdash \alpha$ whenever $\Gamma \vDash \alpha$.*

Proof: Let us assume that $\Gamma \vDash \alpha$. Then $\vDash \Gamma \to \alpha$. Thus, by Proposition 6.8, $\vdash \Gamma \to \alpha$ and so $\Gamma \vdash \alpha$. QED

7 A Concrete Case Study in Cyber-Attack Attribution

In order to show how Time-Stamped Claim Logic works on a large example, we consider a concrete case study inspired by the Ukraine Power Grid Attack that occurred in December 2015 [11]. For the sake of simplicity, we removed the references to the real actors involved in the attack and substituted them with generic ones. A good part of the provided evidence will be similar to the one found for this attack — we just carried out some simplifications for the sake of understandability.

7.1 The Set-Up

We will denote the analysed attack with PGA and its victim with U. We have 5 agents/sources that provide information about this attack: SC_1 and SC_2 are different security companies; SD is the security department of an impartial country; Ag is a well-known international news agency; and Bl is an analyst that writes blog posts related to cyber-attacks. Furthermore, A is a country, and HG denotes a famous group of hackers. For what concerns time, t is a general instant of time that can spread from Spring 2015 to (including) December 2015.

$$\begin{array}{lll}
1 & \psi_1, \underline{\psi_2}, \delta_2 \rightarrow \text{SC}_2 : -(t \cdot \text{econLoss}_{\text{U}}^{\text{PGA}}) & \text{CR2:2,3} \\
2 & \underline{\psi_1}, \underline{\delta_2} \rightarrow \text{SC}_2 : -(t \cdot \text{econLoss}_{\text{U}}^{\text{PGA}}), \underline{t \cdot \text{limitedDamage}_{\text{U}}^{\text{PGA}}} & \text{(Proposition 3.6)} \\
3 & \underline{\text{SC}_2 : -(t \cdot \text{econLoss}_{\text{U}}^{\text{PGA}})}, \psi_1, \delta_2 \rightarrow \underline{\text{SC}_2 : -(t \cdot \text{econLoss}_{\text{U}}^{\text{PGA}})} & \text{Ax}
\end{array}$$

Figure 4: Derivation of $\psi_1, \psi_2, \delta_2 \rightarrow \text{SC}_2 : -(t \cdot \text{econLoss}_{\text{U}}^{\text{PGA}})$

7.2 The Evidence

In the following, we list the evidence provided by the analyst. We start with the given evidence and later provide the given derived evidence. SC_1 states that the IPs from where the attack was originated are geolocated in A (geoSourceIP):

$$\text{SC}_1 : t \cdot \text{geoSourceIP}_{\text{PGA}}^{\text{A}}$$

The agents SC_1 and SC_2 both state that the used malware (usedMalware) in this attack (PGA) was a version of the BlackEnergy malware (BE3):

$$\text{SC}_1 : t \cdot \text{usedMalware}_{\text{PGA}}^{\text{BE3}} \qquad \text{SC}_2 : t \cdot \text{usedMalware}_{\text{PGA}}^{\text{BE3}}$$

The provided information holds as different attackers can use different malware or pieces of software for the same attack.

Source SC_2 states that KillDisk was used during the attack, as SC_2 found traces of the KillDisk malware when analysing the infected system, and SD states that BE3 is similar to its previous version BE2:

$$\text{SC}_2 : t \cdot \text{usedMalware}_{\text{PGA}}^{\text{KillDisk}} \qquad \text{SD} : t \cdot \text{similar}_{\text{BE2}}^{\text{BE3}}$$

Furthermore, at SD's website is stated that BE2 is used mainly (usedBy) by a group of hackers denoted by HG:
$$\text{SD} : t \cdot \text{usedBy}_{\text{HG}}^{\text{BE2}}$$

The evidence related to the negative consequences of the attack PGA is provided by source SC_2, which states that the damages of PGA to the victim (U) were limited (limitedDamage):

$$\text{SC}_2 : t \cdot \text{limitedDamage}_{\text{U}}^{\text{PGA}}$$

The news agency, Ag, states that there was a political conflict (polConflict) between the victim U and country A in that period:

$$\text{Ag} : t \cdot \text{polConflict}_{\text{U}}^{\text{A}}$$

Furthermore, Bl states that HG does not operate in country A and does not have relations with country A:

$$\text{Bl} : -(t \cdot \text{operate}_{\text{HG}}^{\text{A}}) \qquad \text{Bl} : -(t \cdot \text{relation}_{\text{HG}}^{\text{A}})$$

1 $\psi_1, \underline{\psi_2}, \delta_1, \delta_2 \rightarrow -(t \cdot \text{econLoss}_\text{U}^\text{PGA})$	CR2:2,3
2 $\underline{\psi_1}, \delta_1, \underline{\delta_2} \rightarrow -(t \cdot \text{econLoss}_\text{U}^\text{PGA}), t \cdot \underline{\text{limitedDamage}_\text{U}^\text{PGA}}$	(Proposition 3.6)
3 $\underline{\text{SC}_2 : -(t \cdot \text{econLoss}_\text{U}^\text{PGA})}, \psi_1, \underline{\delta_1}, \delta_2 \rightarrow \underline{-(t \cdot \text{econLoss}_\text{U}^\text{PGA})}$	(Proposition 3.6)

Figure 5: Derivation of $\psi_1, \psi_2, \delta_1, \delta_2 \rightarrow -(t \cdot \text{econLoss}_\text{U}^\text{PGA})$

Let us now introduce the given derived evidence for this cyber-attack. The sources provide discordant derived evidence with respect to the motives of the attack, whether the attack had or not economical motives. In particular, SC_2 states that the attacker did not have economical motives (econMotives) to perform the attack as there were not considerable economical losses (econLoss) since the damages caused by the attack to the victim were limited (limitedDamage):

$$\text{SC}_2 :: (t \cdot \text{limitedDamage}_\text{U}^\text{PGA} / -(t \cdot \text{econLoss}_\text{U}^\text{PGA}))$$
$$\text{SC}_2 :: (-(t \cdot \text{econLoss}_\text{U}^\text{PGA}) / -(t \cdot \text{econMotives}_\text{U}^\text{PGA}))$$

A discordance arises for the possible culprit of the attack. SC_1 states that the group of hackers HG is a possible culprit, as malware BE3 was used during PGA, and BE3 is similar to malware BE2 that is used by HG, whereas source Bl states that the possible culprit of the attack is not the hackers group HG, as there was a political conflict in that period between A and the victim U, the source IPs of the attack were geolocated in country A, but the hackers group HG does not operate in A and does not have any relation with A:

$$\text{SC}_1 :: (t \cdot \text{usedMalware}_\text{PGA}^\text{BE3}, t \cdot \text{similar}_\text{BE2}^\text{BE3}, t \cdot \text{usedBy}_\text{HG}^\text{BE2} / t \cdot \text{possibleCulprit}_\text{HG}^\text{PGA})$$
$$\text{Bl} :: (t \cdot \text{polConflict}_\text{U}^\text{A}, t \cdot \text{geoSourceIP}_\text{PGA}^\text{A}, -(t \cdot \text{operate}_\text{HG}^\text{A}),$$
$$-(t \cdot \text{relation}_\text{HG}^\text{A}) / -t \cdot \text{possibleCulprit}_\text{HG}^\text{PGA})$$

Let us now introduce the *relations of trust* the analyst has with respect to the sources that provided the above evidence. In particular, for the analyst, SC_1 is at least as trustworthy as Bl about HG being the possible culprit of PGA:

$$\text{Bl} \trianglelefteq_{\text{possibleCulprit}_\text{HG}^\text{PGA}} \text{SC}_1$$

Moreover, SC_2 is the most trusted agent about the economical losses, the economical motives, the limited damages and the used malware; Ag is the most trusted about identifying political conflicts between entities; SD is the most trusted about the similarities between malware BE3 and malware BE2, and that malware BE2 was used by the group of hackers HG; SC_1 is the most trusted about geolocating the source IPs of an attack, and Bl is the most trusted regarding the statement that HG does not operate in A and does not have relation

with A:

$$\forall x.\, x \trianglelefteq_{\text{polConflict}_{\text{U}}^{\text{A}}} \text{Ag} \qquad\qquad \forall x.\, x \trianglelefteq_{\text{similar}_{\text{BE2}}^{\text{BE3}}} \text{SD}$$

$$\forall x.\, x \trianglelefteq_{\text{econLoss}_{\text{U}}^{\text{PGA}}} \text{SC}_2 \qquad\qquad \forall x.\, x \trianglelefteq_{\text{usedBy}_{\text{HG}}^{\text{BE2}}} \text{SD}$$

$$\forall x.\, x \trianglelefteq_{\text{econMotives}_{\text{U}}^{\text{PGA}}} \text{SC}_2 \qquad\qquad \forall x.\, x \trianglelefteq_{\text{usedMalware}_{\text{PGA}}^{\text{BE3}}} \text{SC}_2$$

$$\forall x.\, x \trianglelefteq_{\text{limitedDamage}_{\text{U}}^{\text{PGA}}} \text{SC}_2 \qquad\qquad \forall x.\, x \trianglelefteq_{\text{geoSourceIP}_{\text{PGA}}^{\text{A}}} \text{SC}_1$$

$$\forall x.\, x \trianglelefteq_{\text{operate}_{\text{HG}}^{\text{A}}} \text{Bl} \qquad\qquad \forall x.\, x \trianglelefteq_{\text{relation}_{\text{HG}}^{\text{A}}} \text{Bl}$$

7.3 The Conclusions of the Analyst

In the following, we show how the analyst can use Time-Stamped Claim Logic to draw some interesting conclusions from the collected evidence.

Consider the following assertions:

$$\psi_1 = \text{SC}_2 : t \cdot \text{limitedDamage}_{\text{U}}^{\text{PGA}}$$
$$\psi_2 = \text{SC}_2 :: (t \cdot \text{limitedDamage}_{\text{U}}^{\text{PGA}} / -(t \cdot \text{econLoss}_{\text{U}}^{\text{PGA}}))$$
$$\psi_3 = \text{SC}_2 :: (-(t \cdot \text{econLoss}_{\text{U}}^{\text{PGA}}) / -(t \cdot \text{econMotives}_{\text{U}}^{\text{PGA}}))$$
$$\delta_1 = \forall x.\, x \trianglelefteq_{\text{econLoss}_{\text{U}}^{\text{PGA}}} \text{SC}_2$$
$$\delta_2 = \forall x.\, x \trianglelefteq_{\text{limitedDamage}_{\text{U}}^{\text{PGA}}} \text{SC}_2$$
$$\delta_3 = \forall x.\, x \trianglelefteq_{\text{econMotives}_{\text{U}}^{\text{PGA}}} \text{SC}_2$$

Observe that

$$\vdash \psi_1, \delta_2 \to t \cdot \text{limitedDamage}_{\text{U}}^{\text{PGA}}$$

holds by Proposition 3.6.

We can now show that

$$\text{SC}_2 : -(t \cdot \text{econLoss}_{\text{U}}^{\text{PGA}})$$

is derived from ψ_1, ψ_2 and δ_2 as can be seen in Figure 4. The derivation in Figure 5 infers

$$-(t \cdot \text{econLoss}_{\text{U}}^{\text{PGA}})$$

from ψ_1, ψ_2, δ_1 and δ_2. From ψ_1, ψ_2, ψ_3, δ_1 and δ_2, we can also derive

$$\text{SC}_2 : -(t \cdot \text{econMotives}_{\text{U}}^{\text{PGA}})$$

as can be seen in Figure 6. From ψ_1, ψ_2, ψ_3, δ_1, δ_2 and δ_3 we can derive

$$-(t \cdot \text{econMotives}_{\text{U}}^{\text{PGA}})$$

as can be seen in Figure 7. From

$$\psi_4 = \text{SC}_1 :: (t \cdot \text{usedMalware}_{\text{PGA}}^{\text{BE3}}, t \cdot \text{similar}_{\text{BE2}}^{\text{BE3}}, t \cdot \text{usedBy}_{\text{HG}}^{\text{BE2}} / t \cdot \text{possibleCulprit}_{\text{HG}}^{\text{PGA}})$$
$$\psi_5 = \text{SC}_2 : t \cdot \text{usedMalware}_{\text{PGA}}^{\text{BE3}}$$
$$\psi_6 = \text{SD} : t \cdot \text{similar}_{\text{BE2}}^{\text{BE3}}$$
$$\psi_7 = \text{SD} : t \cdot \text{usedBy}_{\text{HG}}^{\text{BE2}}$$
$$\delta_4 = \forall x.\, x \trianglelefteq_{\text{similar}_{\text{BE2}}^{\text{BE3}}} \text{SD}$$
$$\delta_5 = \forall x.\, x \trianglelefteq_{\text{usedBy}_{\text{HG}}^{\text{BE2}}} \text{SD}$$
$$\delta_6 = \forall x.\, x \trianglelefteq_{\text{usedMalware}_{\text{PGA}}^{\text{BE3}}} \text{SC}_2$$

$$\begin{array}{lll}
1 & \psi_1, \psi_2, \underline{\psi_3}, \delta_1, \delta_2 \rightarrow \mathrm{SC}_2 : -(t \cdot \mathrm{econMotives}_{\mathrm{U}}^{\mathrm{PGA}}) & \mathrm{CR2:2,3} \\[4pt]
2 & \underline{\psi_1}, \underline{\psi_2}, \underline{\delta_1}, \underline{\delta_2} \rightarrow \underline{-(t \cdot \mathrm{econLoss}_{\mathrm{U}}^{\mathrm{PGA}})}, \mathrm{SC}_2 : -(t \cdot \mathrm{econMotives}_{\mathrm{U}}^{\mathrm{PGA}}) & (\mathrm{Fig.\ 5,\ Prop.\ 3.5}) \\[4pt]
3 & \underline{\mathrm{SC}_2 : -(t \cdot \mathrm{econMotives}_{\mathrm{U}}^{\mathrm{PGA}})}, \psi_1, \psi_2, \delta_1, \delta_2 \rightarrow \\[4pt]
& \qquad\qquad\qquad \underline{\mathrm{SC}_2 : -(t \cdot \mathrm{econMotives}_{\mathrm{U}}^{\mathrm{PGA}})} & \mathrm{Ax}
\end{array}$$

Figure 6: Derivation of $\psi_1, \psi_2, \psi_3, \delta_1, \delta_2 \rightarrow \mathrm{SC}_2 : -(t \cdot \mathrm{econMotives}_{\mathrm{U}}^{\mathrm{PGA}})$

$$\begin{array}{lll}
1 & \psi_1, \underline{\psi_2}, \psi_3, \delta_1, \delta_2, \delta_3 \rightarrow -(t \cdot \mathrm{econMotives}_{\mathrm{U}}^{\mathrm{PGA}}) & \mathrm{CR2:2,3} \\[4pt]
2 & \underline{\psi_1}, \underline{\psi_2}, \underline{\delta_1}, \underline{\delta_2}, \delta_3 \rightarrow -(t \cdot \mathrm{econMotives}_{\mathrm{U}}^{\mathrm{PGA}}), \underline{-(t \cdot \mathrm{econLoss}_{\mathrm{U}}^{\mathrm{PGA}})} & (\mathrm{Fig.\ 5,\ Prop.\ 3.5}) \\[4pt]
3 & \underline{\mathrm{SC}_2 : -(t \cdot \mathrm{econMotives}_{\mathrm{U}}^{\mathrm{PGA}})}, \psi_1, \psi_2, \delta_1, \delta_2, \underline{\delta_3} \rightarrow \underline{-(t \cdot \mathrm{econMotives}_{\mathrm{U}}^{\mathrm{PGA}})} & (\mathrm{Proposition\ 3.6})
\end{array}$$

Figure 7: Derivation of $\psi_1, \psi_2, \psi_3, \delta_1, \delta_2, \delta_3 \rightarrow -(t \cdot \mathrm{econMotives}_{\mathrm{U}}^{\mathrm{PGA}})$

we can conclude

$$\mathrm{SC}_1 : t \cdot \mathrm{possibleCulprit}_{\mathrm{HG}}^{\mathrm{PGA}}$$

as can be seen in Figure 8. Finally, it is not difficult to conclude

$$\mathrm{Bl} : -(t \cdot \mathrm{possibleCulprit}_{\mathrm{HG}}^{\mathrm{PGA}})$$

from

$\mathrm{Bl} :: (t \cdot \mathrm{polConflict}_{\mathrm{U}}^{\mathrm{A}}, t \cdot \mathrm{geoSourceIP}_{\mathrm{PGA}}^{\mathrm{A}}, -(t \cdot \mathrm{operate}_{\mathrm{HG}}^{\mathrm{A}}), -(t \cdot \mathrm{relation}_{\mathrm{HG}}^{\mathrm{A}})/-t \cdot \mathrm{possibleCulprit}_{\mathrm{HG}}^{\mathrm{PGA}})$

$\mathrm{SC}_1 : t \cdot \mathrm{geoSourceIP}_{\mathrm{PGA}}^{\mathrm{A}}$

$\mathrm{Ag} : t \cdot \mathrm{polConflict}_{\mathrm{U}}^{\mathrm{A}}$

$\mathrm{Bl} : -(t \cdot \mathrm{operate}_{\mathrm{HG}}^{\mathrm{A}})$

$\mathrm{Bl} : -(t \cdot \mathrm{relation}_{\mathrm{HG}}^{\mathrm{A}})$

$\forall x.\, x \trianglelefteq_{\mathrm{geoSourceIP}_{\mathrm{PGA}}^{\mathrm{A}}} \mathrm{SC}_1$

$\forall x.\, x \trianglelefteq_{\mathrm{polConflict}_{\mathrm{U}}^{\mathrm{A}}} \mathrm{Ag}$

$\forall x.\, x \trianglelefteq_{\mathrm{operate}_{\mathrm{HG}}^{\mathrm{A}}} \mathrm{Bl}$

$\forall x.\, x \trianglelefteq_{\mathrm{relation}_{\mathrm{HG}}^{\mathrm{A}}} \mathrm{Bl}$

and some of the above results. However, thanks to the trust relation

$$\mathrm{Bl} \trianglelefteq_{\mathrm{possibleCulprit}_{\mathrm{HG}}^{\mathrm{PGA}}} \mathrm{SC}_1 \,,$$

which says that for the analyst, SC_1 is at least as trustworthy as Bl for what concerns the possible culprit of the attack, the analyst's final result will discard Bl's statement, and the analyst will conclude that the possible culprit of the attack is HG.

7.4 Summary

In this case study, one of the forensics analyst's conclusions is that a *possible culprit* of the attack is the *group of hackers* denoted by HG. This conclusion was derived using the analyst's

1	$\underline{\psi_4}, \psi_5, \psi_6, \psi_7, \delta_4, \delta_5, \delta_6 \rightarrow \mathrm{SC}_1 : t \cdot \mathrm{possibleCulprit}_{\mathrm{HG}}^{\mathrm{PGA}}$	CR2:2–5
2	$\psi_5, \psi_6, \psi_7, \delta_4, \delta_5, \delta_6 \rightarrow \mathrm{SC}_1 : t \cdot \mathrm{possibleCulprit}_{\mathrm{HG}}^{\mathrm{PGA}}, \underline{t \cdot \mathrm{usedMalware}_{\mathrm{PGA}}^{\mathrm{BE3}}}$	(Proposition 3.6)
3	$\psi_5, \psi_6, \psi_7, \delta_4, \delta_5, \delta_6 \rightarrow \mathrm{SC}_1 : t \cdot \mathrm{possibleCulprit}_{\mathrm{HG}}^{\mathrm{PGA}}, \underline{t \cdot \mathrm{similar}_{\mathrm{BE2}}^{\mathrm{BE3}}}$	(Proposition 3.6)
4	$\psi_5, \psi_6, \psi_7, \delta_4, \delta_5, \delta_6 \rightarrow \mathrm{SC}_1 : t \cdot \mathrm{possibleCulprit}_{\mathrm{HG}}^{\mathrm{PGA}}, \underline{t \cdot \mathrm{usedBy}_{\mathrm{HG}}^{\mathrm{BE2}}}$	(Proposition 3.6)
5	$\underline{\mathrm{SC}_1 : t \cdot \mathrm{possibleCulprit}_{\mathrm{HG}}^{\mathrm{PGA}}}, \psi_5, \psi_6, \psi_7, \delta_4, \delta_5, \delta_6 \rightarrow \underline{\mathrm{SC}_1 : t \cdot \mathrm{possibleCulprit}_{\mathrm{HG}}^{\mathrm{PGA}}}$	Ax

Figure 8: Derivation of $\psi_4, \psi_5, \psi_6, \psi_7, \delta_4, \delta_5, \delta_6 \rightarrow \mathrm{SC}_1 : t \cdot \mathrm{possibleCulprit}_{\mathrm{HG}}^{\mathrm{PGA}}$

relation of trust, where for the analyst, the security company SC_1 is at least as trustworthy as Bl. Given the set of evidence collected, our Time-Stamped Claim Logic allows the analyst to filter the conflicting evidence by using his relations of trust. This reduces the number of evidence that the analyst needs to consider during the analysis phase. Furthermore, the set of evidence that the analyst obtains in this way is consistent, as all the conflicting pieces of evidence are removed (assuming that the analyst has provided all the required trust relations).

Our Time-Stamped Claim Logic provides a sound and complete calculus for reasoning about the evidence at hand. In other words, the logic uses the evidence and the derivation of evidence of trusted sources together with the analyst's relations of trust to reason with the inconstancies and provide to the analyst only evidence that is trustworthy (from his point of view). Furthermore, the logic is able to provide to the analyst *new evidence* derived using the given set of evidence. The derived evidence can be general evidence that is always true or statements made by the sources and that the analyst trusts.

8 Related Work

In this section, we discuss the logics and approaches that are most closely related to our Time-Stamped Claim Logic.

We begin by pointing out that there are a number of recent works on reasoning about claims from different logical points of view, namely *Justification Logics* (see [4, 13, 8]), which capitalizes on the *Logic of Proofs* (see [3]), *Modal Evidence Logic* (see [28, 27, 6]) and a logical account of *Formal Argumentation* (see [9]). A recent work presents a paraconsistent logic able to reason about the preservation of evidence and of truth (see [10]).

In *Justification Logics* [4, 13, 8] propositional formulas are labelled with justification terms built from variables and constants using several operations. The semantics is provided by Kripke structures enriched with an evidence function that associates a set of worlds to each propositional formula and justification term. Justifications in this logic are seen as the strongest form of evidence providing a direct proof of the truth of an assertion.

More specifically, Justification Logics are enrichments of classical propositional logic with assertions of the form

$$s : F,$$

where s is a term and F is a propositional formula, meaning that s is a justification for F. The operations allowed on the labels express the possible interactions that justifications may have. The logic we propose differs significantly from Justification Logics since our main

goal is to address distributed time-stamped claims instead of justifications. Reflecting this different goal, the labels in Time-Stamped Claim Logic are an agent and/or a time-stamp. Furthermore, our logic includes explicit constructions for expressing trust relations between agents with respect to relevant evidence. On the other hand, Justification Logics may allow nesting of labels which our logic currently does not support. Both Justification Logics and Time-Stamped Claim Logic allow reasoning about labelled formulas and formulas without labels. However, the relationship between these formulas is made clear at the meta-level in Justification Logics, whereas in the calculus of Time-Stamped Claim Logic this relationship is internalized.

Modal Evidence Logic [28, 27, 6] provides a way to model epistemic agents when dealing with evidence from different sources. It is a multi-modal logic that comprises three modal-like operators: one for representing that an agent has evidence for a formula, another for stating that an agent believes a formula to be true and a last one asserting that a formula is true in every world. An important difference between Modal Evidence Logic and our Time-Stamped Claim Logic is that Modal Evidence Logic is not a labelled logic. Consequently, no explicit reasoning about agents is possible in Modal Evidence Logic contrarily to what happens in our logic. Moreover, in Modal Evidence Logic there is no specific mechanism for dealing with time-stamped claims.

Formal argumentation has been investigated since the early 1990s but it was the landmark work in [12] that started an abstract perspective on argumentation. A logical foundation of formal argumentation was proposed in [9] using classical logic as well as modal logic to characterize different extensions for argumentation. The main difference between that work and Time-Stamped Claim Logic is that the former is related to arguments and the latter is concerned with agent claims. So, naturally, there is an attack relation between arguments in Formal Argumentation, whereas there is a trust relationship between agents with respect to a given subject in Time-Stamped Claim Logic. In both Formal Argumentation and Time-Stamped Claim Logic, there are three possibilities for the valuation of both an argument and a claim. Hence, both have three-valued interpretations. In Formal Argumentation, an argument can be explicitly accepted (truth value *in*), explicitly rejected (truth value *out*) or neither explicitly accepted nor explicitly rejected (truth value *undec*). In our logic, either an agent a claims that p occurred at time t, or an agent a claims that p did not occur at time t or an agent a does not have an opinion about the occurrence of p at time t.

Digital forensics techniques suffer from quantity and complexity problems [7] due to the necessity to handle an enormous amount of pieces of evidence and to the low format of the collected evidence. In this work, we proposed a solution that deals with the quantity problem: Time-Stamped Claim Logic reduces drastically the number of given evidence using the relations of trust of the analyst. Our logic allows the forensics team to decrease the resources spent on the analysis, which is usually a human-based process, and to arrive at a swift conclusion. Filtering the evidence reduces the chances of human error as the analyst needs to deal with a considerably lower number of pieces of evidence during the analysis phase.

The gathered pieces of evidence can be in conflict with each other because they are collected from difference sources and because of the anti-forensics techniques [16, 30] and deception techniques [1, 2] used by the attackers to hide their traces. Digital forensics techniques are able to deal with conflicting information [5, 14, 19, 20], but without taking into account the analyst's relations of trust. Our logic solves the conflicts by using in the derivations only trusted pieces of evidence, thus providing as conclusions only consistent sets of pieces of

evidence.

Filtering the evidence of the attack using Time-Stamped Claim Logic helps the analyst to swiftly identify who has performed the attack with a higher level of confidence. In particular, the results of the filtering process can be used by the analyst during the *attribution phase* [19, 20]: the analyst can then deal only with trusted evidence and has a higher level of confidence for the given result. Using this filtering process reduces the resources and time spent during the attribution phase, which is a crucial aspect of digital forensics investigations.

In [18], Karafili, Cristani and Viganò have proposed another formal solution for filtering the evidence of cyber-attacks. They introduced the *Evidence Logic (EL)*, which is based on an enriched Linear Temporal Logic and represents the evidence (simple and derived), the sources, the reasonings, the instants of time, and the analyst's relations of trust with respect to the sources and the used reasoning. EL and Time-Stamped Claim Logic obviously share some similarities, starting with the objective of providing security analysts with the formal means to reason with the collected set of evidence. There are also some fundamental differences, though. Most notably, EL is based on a monotonic-reasoning procedure that rewrites the pieces of evidence with the use of tableau rules, but the rewriting system and algorithm that govern the inferences lack a completeness proof. There are also differences in the expressive power of the two logics. In particular, EL has a restrictive constraint, where an evidence is either given or derived, whereas Time-Stamped Claim Logic is more expressive, as it permits one to represent the same evidence as given and derived. Time-Stamped Claim Logic permits one to better represent real evidence that can be both given and derived by other evidence. Moreover, Time-Stamped Claim Logic uses in its reasonings only trusted evidence, whereas EL has a more *credulous* nature, where it considers in its reasonings also the simple evidence used by the sources to derive new evidence.

There are differences also at the level of trust relations. The trust relations in EL are binary relations between two different sources, whereas Time-Stamped Claim Logic has also *universal* trust relations, where a certain source is the most trusted for a particular evidence ($\forall x. \, x \trianglelefteq_p a$ and $a : \boxdot \phi$). EL is able to represent the relation $\forall x. \, x \trianglelefteq_p a$ by introducing all the needed binary relations of trust (if there are a finite number of sources), but in case new evidence is added, it needs to add new trust relations as well. However, EL is not able to represent the $a : \boxdot \phi$ relation.

EL represents the *reasonings* followed by the source to derive an evidence, as well as the trust relations between reasonings. The reasonings can be applied by different sources to derive the same conclusion, using the same premises. Time-Stamped Claim Logic does not represent the reasonings or their trust relations, instead, it uses the trust relations between sources. The use of the reasonings and their trust relations in EL permits it to be more generic, whereas the use of trust relations between sources for the derived evidence gives a higher level of specificity to Time-Stamped Claim Logic.

Finally, it is interesting to note that, for all these reasons, EL is not able to handle the case study that we considered in this paper in the same way as Time-Stamped Claim Logic. In order to allow an analyst to derive the same conclusions we obtained here, EL would need to undergo some changes which would come at the cost of losing expressivity.

9 Concluding Remarks and Future Work

We proposed a logic for reasoning about time-stamped claims by presenting a Gentzen calculus and a semantics, and proved soundness and completeness. We also showed how it can be applied concretely to a case study in cyber-security attribution. There are several directions for future work. The first is to provide automated support for our calculus (e.g., by implementing it in a logical framework such as Isabelle or as a tableaux system) in order to avoid having to carry out the derivations by hand. We plan to address the question of whether or not the logic is semantically compact. In future works, we also intend to investigate whether the logic is decidable [24] and whether the logic has Craig interpolation [26]. Moreover, we would like to provide a Kripke-style semantics for time-stamped claims by taking assignments as possible worlds and analyse the modal properties of the underlying operator. Furthermore, it would be interesting to generalize the language of the logic in order to address other general claims as well as to enrich the logic with dynamic features [29]. It also seems natural and worthwhile to incorporate probabilistic primitives and reasoning in the logic [22, 21, 25, 17]. Finally, another interesting future research direction is to investigate the combination of this logic with logics addressing different aspects in order to obtain a logic with a broader applicability [15, 23].

References

[1] M. H. Almeshekah and E. H. Spafford. Planning and integrating deception into computer security defenses. In *NSPW*, pages 127–138. ACM, 2014.

[2] M. H. Almeshekah and E. H. Spafford. Cyber security deception. In S. Jajodia, V. S. Subrahmanian, V. Swarup, and C. Wang, editors, *Cyber Deception: Building the Scientific Foundation*, pages 23–50. Springer, 2016.

[3] S. Artemov. Explicit provability and constructive semantics. *The Bulletin of Symbolic Logic*, 7(1):1–36, 2001.

[4] S. Artemov. The logic of justification. *The Review of Symbolic Logic*, 1(4):477–513, 2008.

[5] B. Aziz. Modelling and refinement of forensic data acquisition specifications. *Digital Investigation*, 11(2):90–101, 2014.

[6] A. Baltag, B. Renne, and S. Smets. The logic of justified belief, explicit knowledge, and conclusive evidence. *Annals of Pure and Applied Logic*, 165(1):49–81, 2014.

[7] N. Beebe. Digital forensic research: The good, the bad and the unaddressed. In *Advances in Digital Forensics V - Fifth IFIP WG 11.9 International Conference on Digital Forensics*, pages 17–36, 2009.

[8] S. Bucheli, R. Kuznets, and T. Studer. Justifications for common knowledge. *Journal of Applied Non-Classical Logics*, 21(1):35–60, 2011.

[9] M. Caminada and D. M. Gabbay. A logical account of formal argumentation. *Studia Logica*, 93(2-3):109–145, 2009.

[10] W. A. Carnielli and A. Rodrigues. An epistemic approach to paraconsistency: a logic of evidence and truth. *Synthese*, in print.

[11] Defense Use Case. Analysis of the cyber attack on the Ukrainian power grid. *Electricity Information Sharing and Analysis Center (E-ISAC)*, 2016.

[12] P. M. Dung. On the acceptability of arguments and its fundamental role in nonmonotonic reasoning, logic programming and n-person games. *Artificial Intelligence*, 77(2):321–357, 1995.

[13] M. Fitting. A quantified logic of evidence. *Annals of Pure and Applied Logic*, 152(1-3):67–83, 2008.

[14] M. Fontani, T. Bianchi, A. De Rosa, A. Piva, and M. Barni. A framework for decision fusion in image forensics based on Dempster-Shafer theory of evidence. *IEEE Transactions on Information Forensics and Security*, 8(4):593–607, 2013.

[15] D. M. Gabbay. Fibring argumentation frames. *Studia Logica*, 93(2-3):231–295, 2009.

[16] R. K. Goutam. The problem of attribution in cyber security. *International Journal of Computer Applications, Foundation of Computer Science*, 131(7):34–36, 2015.

[17] J. Y. Halpern and R. Pucella. A logic for reasoning about evidence. *Journal of Artificial Intelligence Research*, 26:1–34, 2006.

[18] E. Karafili, M. Cristani, and L. Viganò. A formal approach to analyzing cyber-forensics evidence. In *Proceedings of ESORICS 2018, Part I*, pages 281–301, 2018.

[19] E. Karafili, L. Wang, A. C. Kakas, and E. Lupu. Helping forensic analysts to attribute cyber-attacks: An argumentation-based reasoner. In *PRIMA*, volume 11224, pages 510–518. Springer, 2018.

[20] E. Karafili, L. Wang, and E. Lupu. An argumentation-based approach to assist in the investigation and attribution of cyber-attacks. *CoRR*, abs/1904.13173, 2019.

[21] I. Kokkinis, Z. Ognjanović, and T. Studer. Probabilistic justification logic. In *Logical Foundations of Computer Science*, volume 9537 of *Lecture Notes in Computer Science*, pages 174–186. Springer, 2016.

[22] J. Lurie. Probabilistic justification logic. *Philosophies*, 3(1):2, 2018.

[23] J. Rasga, A. Sernadas, C. Sernadas, and L. Viganò. Fibring labelled deduction systems. *Journal of Logic and Computation*, 12(3):443–473, 2002.

[24] J. Rasga, C. Sernadas, and A. Sernadas. A roadmap to decidability. In *The Road to Universal Logic*, pages 423–445. Springer, 2015.

[25] A. Sernadas, J. Rasga, and C. Sernadas. On probability and logic. *Portugaliae Mathematica*, 74(4):267–313, 2017.

[26] C. Sernadas, J. Rasga, and A. Sernadas. Preservation of Craig interpolation by the product of matrix logics. *Journal of Applied Logic*, 11(3):328–349, 2013.

[27] J. van Benthem, D. Fernández-Duque, and E. Pacuit. Evidence logic: a new look at neighborhood structures. In *Advances in Modal Logic*, volume 9, pages 97–118. College Publications, London, 2012.

[28] J. van Benthem and E. Pacuit. Logical dynamics of evidence. In *Logic, Rationality, and Interaction*, volume 6953 of *Lecture Notes in Computer Science*, pages 1–27. Springer, 2011.

[29] H. van Dirmarsch, W. van der Hoek, and B. Kooi. *Dynamic Epistemic Logic*. Springer, 2008.

[30] D. A. Wheeler and G. N. Larsen. Techniques for cyber attack attribution. Technical report, Institute for Defense Analyses Alexandria VA, 2003.

A   Some Proofs of Sections 5 and 6

Proposition 5.2 The rules of the sequent calculus are sound.

Proof: It is quite straightforward to see that the rules Ax, Cut, LI, LT, LC, ER, ES and ET are sound.

(EC) Let us assume that $I\rho \Vdash t_1 \cong t_2$, $I\rho \Vdash [\beta]_{t_2}^{t_1}$ and $I\rho \Vdash \Gamma$, where β is either of the form $a : \phi$ or has $<$ as the main constructor. If $t_1 \notin \mathrm{var}_T(\beta)$ then β is $[\beta]_{t_2}^{t_1}$ and so the thesis follows immediately. Otherwise, the result is immediate by definition of I.

(AT) Let us assume that $I\rho \Vdash a_1 \trianglelefteq_p a_2$, $I\rho \Vdash a_2 \trianglelefteq_p a_3$ and $I\rho \Vdash \Gamma$. The thesis follows immediately by the definition of interpretation structure since $\trianglelefteq_p^I$ is transitive.

(AR) Observe that $I\rho \Vdash a \trianglelefteq_p a$ since $\trianglelefteq_p^I$ is reflexive.

(AC) Let us assume that $I\rho \Vdash a_1 \trianglelefteq_p a_2$, $I\rho \Vdash a_2 \trianglelefteq_p a_1$, $I\rho \Vdash [a : \phi]_{a_2}^{a_1}$ and $I\rho \Vdash \Gamma$. If a is not a_1 then $[a : \phi]_{a_2}^{a_1}$ is $a : \phi$ and so the thesis follows immediately. Otherwise, the result is obtained by the definition of I.

(AMR) Let us assume that $I\rho' \Vdash \Gamma \to \Delta, b \trianglelefteq_p a$ for every ρ' such that $\rho' \equiv_b^A \rho$ and $I\rho \Vdash \Gamma$. Suppose that there is no $\delta \in \Delta$ such that $I\rho \Vdash \delta$. Then $I\rho' \Vdash b \trianglelefteq_p a$ for every ρ' such that $\rho' \equiv_b^A \rho$. Hence, $d \trianglelefteq_p^I \rho_a(a)$ for each $d \in D_A$, and so $I\rho \Vdash \forall x. x \trianglelefteq_p a$.

(AML) Let us assume that $I\rho \Vdash a' \trianglelefteq_p a, \forall x. x \trianglelefteq_p a, \Gamma \to \Delta$, $I\rho \Vdash \forall x. x \trianglelefteq_p a$ and $I\rho \Vdash \Gamma$. Then $d \trianglelefteq_p^I \rho_A(a)$ for every $d \in D_A$. Hence, in particular, $\rho_A(a') \trianglelefteq_p^I \rho_A(a)$ and so $I\rho \Vdash a' \trianglelefteq_p a$. Therefore, by the hypothesis, there is $\delta \in \Delta$ such that $I\rho \Vdash \delta$.

(NS) Let us assume that $I\rho \Vdash a : -\phi, \Gamma \to \Delta, a : \phi$, $I\rho \Vdash \Gamma$ and $I\rho \Vdash a : -\phi$. We just consider

the case that ϕ is $t \cdot p$. Thus $(p, \rho_A(a), \rho_T(t)) \in V^-$. Therefore, $I\rho \not\Vdash a : \phi$ and so, by the hypothesis, there is $\delta \in \Delta$ such that $I\rho \Vdash \delta$.

(NK) Let us assume that $I\rho \Vdash -\phi, \Gamma \to \Delta, \phi$, $I\rho \Vdash \Gamma$ and $I\rho \Vdash -\phi$. Then there is an assignment ρ' such that $\rho' \equiv_a^A \rho$, $I\rho' \Vdash a : -\phi$ and $I\rho' \Vdash a : \boxdot -\phi$. Thus we can conclude immediately that $I\rho \not\Vdash \phi$. Therefore, by the hypothesis, there is $\delta \in \Delta$ such that $I\rho \Vdash \delta$.

(SCR) Let us assume that $I\rho' \Vdash b : -\phi, a \trianglelefteq_{\operatorname{var}_P(\phi)} b, \Gamma \to \Delta$ for every ρ' such that $\rho' \equiv_b^A \rho$, $I\rho \Vdash \Gamma$ and that there is no $\delta \in \Delta$ such that $I\rho \Vdash \delta$. We now show that $I\rho \Vdash a : \boxdot \phi$. Let σ be such that $\sigma \equiv_b^A \rho$ and $I\sigma \Vdash a \trianglelefteq_{\operatorname{var}_P(\phi)} b$. Observe that $I\sigma \Vdash b : \phi, a \trianglelefteq_{\operatorname{var}_P(\phi)} b, \Gamma \to \Delta$, $I\sigma \Vdash \Gamma$ and there is no $\delta \in \Delta$ such that $I\sigma \Vdash \delta$. Then $I\sigma \not\Vdash b : -\phi$.

(SCL) Let us assume that $I\rho \Vdash a : \boxdot \phi, \Gamma \to \Delta, a \trianglelefteq_{\operatorname{var}_P(\phi)} a'$, $I\rho \Vdash a : \boxdot \phi, \Gamma \to \Delta, a' : -\phi$, $I\rho \Vdash \Gamma$ and $I\rho \Vdash a : \boxdot \phi$. Suppose, by contradiction, that there is no $\delta \in \Delta$ such that $I\rho \Vdash \delta$. Then $I\rho \Vdash a \trianglelefteq_{\operatorname{var}_P(\phi)} a'$ and $I\rho \Vdash a' : -\phi$. These facts contradict the hypothesis that $I\rho \Vdash a : \boxdot \phi$.

(SKR) Let us assume that $I\rho' \Vdash b : -\phi, b : \boxdot -\phi, \Gamma \to \Delta$ for every $\rho' \equiv_b^A \rho$, $I\rho \Vdash \Gamma \to \Delta, \phi, a : \phi$, $I\rho \Vdash \Gamma \to \Delta, \phi, a : \boxdot \phi$ and $I\rho \Vdash \Gamma$. Let us assume, by contradiction, that there is no $\psi \in \Delta \cup \{\phi\}$ such that $I\rho \Vdash \psi$. Then $I\rho \Vdash a : \phi$ and $I\rho \Vdash a : \boxdot \phi$. We now show that $I\rho \Vdash \phi$ leading to a contradiction. Let $\sigma \equiv_b^A \rho$ be such that $I\sigma \Vdash b : -\phi$. Taking ρ' as σ, by hypothesis, $I\sigma \not\Vdash b : \boxdot -\phi$. With respect to the second condition it is enough to take ρ' as ρ.

(KL) Let us assume that $I\rho' \Vdash b : \phi, b : \boxdot \phi, \Gamma \to \Delta$ for every $\rho' \equiv_b^A \rho$, $I\rho \Vdash \Gamma$ and $I\rho \Vdash \phi$. Let us assume, by contradiction, that there is no $\delta \in \Delta$ such that $I\rho \Vdash \delta$. Then, for every $\rho' \equiv_b^A \rho$ either $I\rho' \not\Vdash b : \phi$ or $I\rho' \not\Vdash b : \boxdot \phi$. Since $I\rho \Vdash \phi$ then there is $\sigma' \equiv_a^A \rho$ such that $I\sigma' \Vdash a : \phi$ and $I\sigma' \Vdash a : \boxdot \phi$ which contradicts the facts above.

(SKL) Let us assume that $I\rho \Vdash \phi, \Gamma \to \Delta, a : -\phi$, $I\rho \Vdash \phi, \Gamma \to \Delta, a : \boxdot -\phi$, $\rho \Vdash \Gamma$ and $I\rho \Vdash \phi$. Let us assume, by contradiction, that there is no $\delta \in \Delta$ such that $I\rho \Vdash \delta$. Thus $I\rho \Vdash a : -\phi$ and $I\rho \Vdash a : \boxdot -\phi$ contradicting the fact that $I\rho \Vdash \phi$.

(CR1) Let us assume that $I\rho \Vdash \phi_1, \ldots, \phi_n, \Gamma \to \Delta, a :: \phi$ and $I\rho \Vdash \Gamma$. If there is no $\delta \in \Delta$ such that $I\rho \Vdash \delta$ then $I\rho \Vdash a : \phi$ and so the thesis follows by definition.

(CR2) Let us assume that $I\rho \Vdash \Gamma \to \Delta, \phi_i$ for $i = 1, \ldots, n$, $I\rho \Vdash a : \phi, \Gamma \to \Delta$, $I\rho \Vdash \Gamma$ and $I\rho \Vdash a :: (\phi_1, \ldots, \phi_n/\phi)$. Suppose, by contradiction, that there is no $\delta \in \Delta$ such that $I\rho \Vdash \delta$. Hence, $I\rho \not\Vdash a : \phi$. Moreover, $I\rho \Vdash \phi_i$ for $i = 1, \ldots, n$. So, by hypothesis, $I\rho \Vdash a : \phi$ which is a contradiction. QED

Proposition 6.2 Let $H = (\Psi_L, \Psi_R)$ be a Hintikka pair over P', X'_A and X'_T. Then there are an interpretation structure I_H over P' and an assignment ρ over I_H such that $I_H\rho \Vdash \psi$ for each $\psi \in \Psi_L$ and $I_H\rho \not\Vdash \psi$ for each $\psi \in \Psi_R$.

Proof: Let $H = (\Psi_L, \Psi_R)$ be a Hintikka pair. Consider the interpretation structure I_H over P' defined as follows:

- the domain D_A is X'_A, that is, $\operatorname{var}_A(\Psi_L \cup \Psi_R)$,

- the domain D_T is X'_T, that is, $\operatorname{var}_T(\Psi_L \cup \Psi_R)$,

- $(t_1, t_2) \in <^{I_H}$ iff $t_1 < t_2 \in \Psi_L$,

- $(t_1, t_2) \in \cong^{I_H}$ iff $t_1 \cong t_2 \in \Psi_L$,

- $(a_1, a_2) \in \trianglelefteq_p^{I_H}$ iff $a_1 \trianglelefteq_p a_2 \in \Psi_L$,

- $V^+ = \{(p, a, t) : a : t \cdot p \in \Psi_L\}$,

- $V^- = \{(p, a, t) : a : -(t \cdot p) \in \Psi_L\}$.

Consider also an assignment ρ such that ρ_A and ρ_T are identities. We show that for every $\psi \in L_{P'}^{X'_A, X'_T}$ we have

$$\psi \in \Psi_L \text{ implies } I_H \rho \Vdash \psi \quad \text{and} \quad \psi \in \Psi_R \text{ implies } I_H \rho \nVdash \psi.$$

1. ψ is $t_1 < t_2$.

   (a) Let us assume that $t_1 < t_2 \in \Psi_L$. Then $(t_1, t_2) \in <^{I_H}$ and so $I_H \rho \Vdash t_1 < t_2$.

   (b) Let us assume that $t_1 < t_2 \in \Psi_R$. Then $t_1 < t_2 \notin \Psi_L$. Hence, $(t_1, t_2) \notin <^{I_H}$ and so $I_H \rho \nVdash t_1 < t_2$.

2. ψ is $t_1 \cong t_2$.

   (a) Let us assume that $t_1 \cong t_2 \in \Psi_L$. Then $(t_1, t_2) \in \cong^{I_H}$ and so $I_H \rho \Vdash t_1 \cong t_2$.

   (b) Let us assume that $t_1 \cong t_2 \in \Psi_R$. Then $t_1 \cong t_2 \notin \Psi_L$. Hence, $(t_1, t_2) \notin \cong^{I_H}$ and so $I_H \rho \nVdash t_1 \cong t_2$.

3. ψ is $a_1 \trianglelefteq_p a_2$.

   (a) Let us assume that $a_1 \trianglelefteq_p a_2 \in \Psi_L$. Then $(a_1, a_2) \in \trianglelefteq_p^{I_H}$ and so $I_H \rho \Vdash a_1 \trianglelefteq_p a_2$.

   (b) Let us assume that $a_1 \trianglelefteq_p a_2 \in \Psi_R$. Then $(a_1, a_2) \notin \trianglelefteq_p^{I_H}$ and so $I_H \rho \nVdash a_1 \trianglelefteq_p a_2$.

4. ψ is $\forall x . x \trianglelefteq_p a$.

   (a) Let us assume that $\forall x . x \trianglelefteq_p a \in \Psi_L$. Then for each $a_1 \in X'_A$ we have $a_1 \trianglelefteq_p a \in \Psi_L$. Hence, $I_H \rho \Vdash a_1 \trianglelefteq_p a$ for each $a_1 \in D_A$ and so $I \rho \Vdash \forall x \, x \trianglelefteq_p a$.

   (b) Let us assume that $\forall x . x \trianglelefteq_p a \in \Psi_R$. Then there is $a' \in X'_A$ such that $a' \trianglelefteq_p a \in \Psi_R$. Therefore, $I \rho \nVdash a' \trianglelefteq_p a$ and so $I \rho \nVdash \forall x . x \trianglelefteq_p a$.

5. ψ is $a : t \cdot p$.

   (a) Let us assume that $a : t \cdot p \in \Psi_L$. Then $(p, a, t) \in V^+$ and $I_H \rho \Vdash a : t \cdot p$.

   (b) Let us assume that $a : t \cdot p \in \Psi_R$. Then $(p, a, t) \in V^-$ or $(p, a, t) \notin V^+ \cup V^-$ and so $I_H \rho \nVdash a : t \cdot p$.

6. ψ is $a : -(t \cdot p)$.

   (a) Let us assume that $a : -(t \cdot p) \in \Psi_L$. Then $(p, a, t) \in V^-$. Hence $I_H \rho \Vdash a : -(t \cdot p)$.

   (b) Let us assume that $a : -(t \cdot p) \in \Psi_R$. Then $(p, a, t) \in V^+$ or $(p, a, t) \notin V^+ \cup V^-$ and so $I_H \rho \nVdash a : -(t \cdot p)$.

7. ψ is $a : \boxdot \phi$.

(a) Let us assume that $a : \Box\, \phi \in \Psi_L$. Then, for each $a' \in X'_A$ either $a \trianglelefteq_{\mathrm{var}(\phi)} a' \in \Psi_R$ or $a' : -\phi \in \Psi_R$. Hence, by the induction hypothesis, for each $a' \in X'_A$ either $I_H\rho \not\Vdash a \trianglelefteq_{\mathrm{var}(\phi)} a'$ or $I_H\rho \not\Vdash a' : -\phi$. Thus, for each $a' \in X'_A$ if $I_H\rho \Vdash a \trianglelefteq_{\mathrm{var}(\phi)} a'$ then $I_H\rho \not\Vdash a' : -\phi$. Let ρ' be an assignment such that $\rho' \equiv_b^{A'} \rho$ and $I_H\rho' \Vdash a \trianglelefteq_{\mathrm{var}(\phi)} b$. Thus, $I_H\rho \Vdash a \trianglelefteq_{\mathrm{var}(\phi)} \rho'(b)$ and, therefore, $I_H\rho \not\Vdash \rho'(b) : -\phi$ and so $I_H\rho' \not\Vdash b : -\phi$.

(b) Let us assume that $a : \Box\, \phi \in \Psi_R$. Then there is $a' \in X'_A$ such that $a \trianglelefteq_{\mathrm{var}(\phi)} a', a' : -\phi \in \Psi_L$. So, by the induction hypothesis, there is $a' \in X'_A$ such that $I_H\rho \Vdash a \trianglelefteq_{\mathrm{var}(\phi)} a'$ and $I_H\rho \Vdash a' : -\phi$. Let $\rho' \equiv_b^{A'} \rho$ be such that $\rho'(b) = a'$. Then $I_H\rho' \Vdash a \trianglelefteq_{\mathrm{var}(\phi)} b$ and $I_H\rho' \Vdash b : -\phi$ and, therefore, $I\rho \not\Vdash a : \Box\, \phi$.

8. ψ is $\phi \in K_P$.

(a) Let us assume that $\phi \in \Psi_L$. Then there is $a' \in X'_A$ such that $a' : \phi, a' : \Box\, \phi \in \Psi_L$ and for every $a \in X'_A$ either $a : -\phi \in \Psi_R$ or $a : \Box\, -\phi \in \Psi_R$. Thus, by the induction hypothesis, there is $a' \in X'_A$ such that $I_H\rho \Vdash a' : \phi$ and $I_H\rho \Vdash a' : \Box\, \phi$ and for each $a \in X'_A$ either $I_H\rho \not\Vdash a : -\phi$ or $I_H\rho \not\Vdash a : \Box\, -\phi$. We now show that $I_H\rho \Vdash \phi$. Let $\rho' \equiv_b^{A'} \rho$ be such that $I_H\rho' \Vdash b : -\phi$. Then, $I_H\rho \Vdash \rho'(b) : -\phi$. Hence, $I_H\rho \not\Vdash \rho'(b) : \Box\, -\phi$, by hypothesis. Therefore, $I_H\rho' \not\Vdash b : \Box\, -\phi$. The other condition follows straightforwardly taking into account one of the assumptions.

(b) Let us assume that $\phi \in \Psi_R$. Then either there exists $a' \in X'_A$ such that $a' : -\phi, a' : \Box\, -\phi \in \Psi_L$ or for each $a \in X'_A$ either $a : \phi \in \Psi_R$ or $a : \Box\, \phi \in \Psi_R$. Hence, by the induction hypothesis, either there exists $a' \in X'_A$ such that $I_H\rho \Vdash a' : -\phi$ and $I_H\rho \Vdash a' : \Box\, -\phi$ or for each $a \in X'_A$ either $I_H\rho \not\Vdash a : \phi$ or $I_H\rho \not\Vdash a : \Box\, \phi$. We now show that $I_H\rho \not\Vdash \phi$. Let us assume that for each assignment ρ' such that $\rho' \equiv_b^A \rho$, if $I_H\rho' \Vdash b : -\phi$ then $I_H\rho' \not\Vdash b : \Box\, -\phi$. Then, for each $a \in X'_A$ either $I_H\rho \not\Vdash a : \phi$ or $I_H\rho \not\Vdash a : \Box\, \phi$. Hence, for each ρ' such that $\rho' \equiv_a^A \rho$ and $I_H\rho' \Vdash a : \phi$ we have $I_H\rho' \not\Vdash a : \Box\, \phi$.

9. ψ is $a :: (\phi_1, \ldots, \phi_n/\phi)$.

(a) Let us assume that $a :: (\phi_1, \ldots, \phi_n/\phi) \in \Psi_L$. Then, either $\phi_i \in \Psi_R$ for some $i = 1, \ldots, n$ or $a : \phi \in \Psi_L$. Hence, by the induction hypothesis, either $I_H\rho \not\Vdash \phi_i$ for some $i = 1, \ldots, n$ or $I_H\rho \Vdash a : \phi$. Therefore, $I_H\rho \Vdash a :: (\phi_1, \ldots, \phi_n/\phi)$.

(b) Let us assume that $a :: (\phi_1, \ldots, \phi_n/\phi) \in \Psi_R$. Thus, if $\phi_1, \ldots, \phi_n \in \Phi_L$ then $a : \phi \in \Psi_R$. So, by the induction hypothesis, if $I_H\rho \Vdash \phi_1, \cdots, I\rho \Vdash \phi_n$ then $I_H\rho \not\Vdash a : \phi$. Hence, $I_H\rho \not\Vdash a :: (\phi_1, \ldots, \phi_n/\phi)$.

$$\text{QED}$$

Proposition 6.6 Let $\Gamma'_1 \to \Delta'_1 \cdots \Gamma'_n \to \Delta'_n$ be an open analytical exhausted branch of an expansion $\Gamma_1 \to \Delta_1 \; \cdots$. Then

$$\left(\bigcup_{i=1}^n \Gamma'_i, \bigcup_{i=1}^n \Delta'_i \right)$$

is a Hintikka pair over $\mathrm{var}_P(\bigcup_{i=1}^n \Gamma'_i \cup \Delta'_i)$, $\mathrm{var}_A(\bigcup_{i=1}^n \Gamma'_i \cup \Delta'_i)$ and $\mathrm{var}_T(\bigcup_{i=1}^n \Gamma'_i \cup \Delta'_i)$.

Proof: In the following, we denote by Ψ_L and Ψ_R the left-hand and the right-hand side of the pair. We now show that this pair fulfils the conditions to be a Hintikka pair:

1. Either $\beta \notin \Psi_L$ or $\beta \notin \Psi_R$, where β is of the form $a : \phi$, $t_1 < t_2$, $t_1 \cong t_2$ and $a_1 \unlhd_p a_2$ such that $\mathrm{var}_P(\phi) \in \mathrm{var}_P(\bigcup_{i=1}^n \Gamma'_i \cup \Delta'_i)$, $a, a_1, a_2 \in \mathrm{var}_A(\bigcup_{i=1}^n \Gamma'_i \cup \Delta'_i)$ and $\mathrm{var}_T(\phi), t_1, t_2 \in \mathrm{var}_T(\bigcup_{i=1}^n \Gamma'_i \cup \Delta'_i)$. Let us assume by contradiction that $\beta \in \Psi_L$ and $\beta \in \Psi_R$. Hence, there are $1 \le i, j \le n$ such that $\beta \in \Gamma'_i$ and $\beta \in \Delta'_j$. Observe that any rule preserves β. Therefore, $\beta \in \Gamma'_n \cap \Delta'_n$ and so $\Gamma'_n \to \Delta'_n$ is an axiom contradicting the hypothesis that the branch is open.

2. Either $\beta \in \Psi_L$ or $\beta \in \Psi_R$, where β is of the form $a : \phi$, $t_1 < t_2$, $t_1 \cong t_2$ and $a_1 \unlhd_p a_2$ such that $\mathrm{var}_P(\phi) \in \mathrm{var}_P(\bigcup_{i=1}^n \Gamma'_i \cup \Delta'_i)$, $a, a_1, a_2 \in \mathrm{var}_A(\bigcup_{i=1}^n \Gamma'_i \cup \Delta'_i)$ and $\mathrm{var}_T(\phi), t_1, t_2 \in \mathrm{var}_T(\bigcup_{i=1}^n \Gamma'_i \cup \Delta'_i)$. Let us assume, by contradiction, that β is not in $\Psi_L \cup \Psi_R$. Consider the branch $\Gamma'_1 \to \Delta'_1 \cdots \Gamma'_n \to \Delta'_n, \Gamma'_n \to \Delta'_n, \beta$ using the cut rule in the last step. Observe that this branch is still analytical. Indeed, β does not occur in $\bigcup_{i=1}^n \Delta'_i$ and no fresh variables are involved. We get a contradiction since the given branch is analytical and exhausted.

3. $t < t \notin \Psi_L$. Immediate by rule (LI) since the branch is open.

4. If $t_1 < t_2, t_2 < t_3 \in \Psi_L$ then $t_1 < t_3 \notin \Psi_R$ and similarly for $\cong$ and $\unlhd_p$. Suppose that $t_1 < t_2, t_2 < t_3 \in \Psi_L$. Then, if $t_1 < t_3 \in \Psi_R$ we could conclude that the branch was not open using rule (LT).

5. $t \cong t \notin \Psi_R$. Immediate by rule (ER) since the branch is open. Similarly for $\unlhd_p$.

6. Either $t_1 < t_2 \notin \Psi_R$ or $t_2 < t_1 \notin \Psi_R$ or $t_1 \cong t_2 \notin \Psi_R$. Suppose that $t_1 < t_2, t_2 < t_1 \in \Psi_R$. Then, if $t_1 \cong t_2 \in \Psi_R$ we could conclude that the branch was not open using rule (LC).

7. If $t_1 \cong t_2 \in \Psi_L$ then $t_2 \cong t_1 \notin \Psi_R$. Suppose that $t_1 \cong t_2 \in \Psi_L$. Then, if $t_2 \cong t_1 \in \Psi_R$ we could conclude that the branch was not open using rule (ES).

8. If $t_1 \cong t_2, [\beta]_{t_2}^{t_1} \in \Psi_L$ then $\beta \notin \Psi_R$ where β is either of the form $a : \phi$ or has $<$ as the main constructor. Suppose that $t_1 \cong t_2, [\beta]_{t_2}^{t_1} \in \Psi_L$. Then, if $\beta \in \Psi_R$ we could conclude that the branch was not open using rule (EC).

9. If $a_1 \unlhd_p a_2, a_2 \unlhd_p a_1, [a : \phi]_{a_2}^{a_1} \in \Psi_L$ then $a : \phi \notin \Psi_R$. The proof is similar to the one of (6).

10. If $\forall x. x \unlhd_p a \in \Psi_R$ then there is $a' \in \mathrm{var}_A(\bigcup_{i=1}^n \Gamma'_i \cup \Delta'_i)$ such that $a' \unlhd_p a \in \Psi_R$. Let us assume that $\forall x. x \unlhd_p a \in \Psi_R$. Suppose, by contradiction, that for every $a' \in \mathrm{var}_A(\bigcup_{i=1}^n \Gamma'_i \cup \Delta'_i)$, $a' \unlhd_p a \notin \Psi_R$. Then, rule (AMR) was not applied to $\forall x. x \unlhd_p a$ and so $\forall x. x \unlhd_p a \in \Delta'_n$. Consider the branch $\Gamma'_1 \to \Delta'_1 \cdots \Gamma'_n \to \Delta'_n, \Gamma'_n \to (\Delta'_n \setminus \{\forall x. x \unlhd_p a\}), b \unlhd_p a$ using in the last step the rule (AMR) where b is not in $\bigcup_{i=1}^n \Gamma'_i \cup \Delta'_i$. Observe that this branch is still analytical. So, the original branch is not exhausted, which contradicts the hypothesis.

11. If $\forall x. x \unlhd_p a \in \Psi_L$ then $a_1 \unlhd_p a \in \Psi_L$ for each $a_1 \in \mathrm{var}_A(\bigcup_{i=1}^n \Gamma'_i \cup \Delta'_i)$. Let us assume that $\forall x. x \unlhd_p a \in \Psi_L$. Suppose, by contradiction, that there is $a_1 \in \mathrm{var}_A(\bigcup_{i=1}^n \Gamma'_i \cup \Delta'_i)$ such that $a_1 \unlhd_p a \notin \Psi_L$. Observe that $\forall x. x \unlhd_p a$ is in Γ'_n. Consider the branch $\Gamma'_1 \to \Delta'_1 \cdots \Gamma'_n \to \Delta'_n, a_1 \unlhd_p a, \Gamma'_n \to \Delta'_n$ using in the last step the rule (AML). Observe that this branch is still analytical. So, the original branch is not exhausted, which contradicts the hypothesis.

12. If $a : \phi \in \Psi_L$ then $a : -\phi \in \Psi_R$. Suppose that $a : \phi \in \Psi_L$. Let us assume, by contradiction that $a : -\phi \notin \Psi_R$. Consider the branch $\Gamma_1' \to \Delta_1' \cdots \Gamma_n' \to \Delta_n' \, \Gamma_n' \to \Delta_n', a : -\phi$ using in the last step the rule (NS). Observe that this branch is still analytical. Indeed, $a : -\phi$ does not occur in $\bigcup_{i=1}^n \Delta_i'$ and no fresh variables are involved. We get a contradiction since the given branch is analytical and exhausted.

13. If $a : \boxdot \phi \in \Psi_R$ then, there is $a' \in \mathrm{var}_A(\bigcup_{i=1}^n \Gamma_i' \cup \Delta_i')$ such that $a \trianglelefteq_{\mathrm{var}(\phi)} a', a' : -\phi \in \Psi_L$. Let us assume that $a : \boxdot \phi \in \Psi_R$. Suppose, by contradiction, that for every $a' \in \mathrm{var}_A(\bigcup_{i=1}^n \Gamma_i' \cup \Delta_i')$ either $a \trianglelefteq_{\mathrm{var}(\phi)} a' \notin \Psi_L$ or $a' : -\phi \notin \Psi_L$. In both cases, rule (SCR) was not applied to $a : \boxdot \phi$. Then $a : \boxdot \phi$ is in Δ_n'. Consider the branch $\Gamma_1' \to \Delta_1' \cdots \Gamma_n' \to \Delta_n' \, a \trianglelefteq_{\mathrm{var}(\phi)} b, b : -\phi, \Gamma_n' \to (\Delta_n' \setminus \{a : \boxdot \phi\})$ using in the last step the rule (SCR) where b is not in $\bigcup_{i=1}^n \Gamma_i' \cup \Delta_i'$. Observe that this branch is still analytical. So, the original branch is not exhausted, which contradicts the hypothesis.

14. If $a : \boxdot \phi \in \Psi_L$ then, for each $a' \in \mathrm{var}_A(\bigcup_{i=1}^n \Gamma_i' \cup \Delta_i')$ either $a \trianglelefteq_{\mathrm{var}(\phi)} a' \in \Psi_R$ or $a' : -\phi \in \Psi_R$. Let us assume that $a : \boxdot \phi \in \Psi_L$. Suppose, by contradiction, that there is $a' \in \mathrm{var}_A(\bigcup_{i=1}^n \Gamma_i' \cup \Delta_i')$ such that $a \trianglelefteq_{\mathrm{var}(\phi)} a' \notin \Psi_R$ and $a' : -\phi \notin \Psi_R$. Observe that $a : \boxdot \phi$ is in Γ_n'. Consider the branch $\Gamma_1' \to \Delta_1' \cdots \Gamma_n' \to \Delta_n' \, \Gamma_n' \to \Delta_n', a \trianglelefteq_{\mathrm{var}(\phi)} a'$ using in the last step the rule (SCL). Observe that this branch is still analytical. So, the original branch is not exhausted, which contradicts the hypothesis.

15. If $\phi \in \Psi_R$ then either there exists $a' \in \mathrm{var}_A(\bigcup_{i=1}^n \Gamma_i' \cup \Delta_i')$ such that $a' : -\phi, a' : \boxdot -\phi \in \Psi_L$ or for each $a \in \mathrm{var}_A(\bigcup_{i=1}^n \Gamma_i' \cup \Delta_i')$ either $a : \phi \in \Psi_R$ or $a : \boxdot \phi \in \Psi_R$. Suppose that $\phi \in \Psi_R$. Let us assume, by contradiction, that the thesis does not hold. Then, $\phi \in \Delta_n'$ since rule (SKR) was not applied to ϕ in the branch. Consider the branch $\Gamma_1' \to \Delta_1' \cdots \Gamma_n' \to \Delta_n' \, b : -\phi, b : \boxdot -\phi, \Gamma_n' \to \Delta_n'$ using in the last step the rule (SKR) where b is not in $\bigcup_{i=1}^n \Gamma_i' \cup \Delta_i'$. Observe that this branch is still analytical. So, the original branch is not exhausted, which contradicts the hypothesis.

16. If $\phi \in \Psi_L$ then there is $a' \in \mathrm{var}_A(\bigcup_{i=1}^n \Gamma_i' \cup \Delta_i')$ such that $a' : \phi, a' : \boxdot \phi \in \Psi_L$ and for each $a \in \mathrm{var}_A(\bigcup_{i=1}^n \Gamma_i' \cup \Delta_i')$ either $a : -\phi \in \Psi_R$ or $a : \boxdot -\phi \in \Psi_R$. Let us assume that $\phi \in \Psi_L$. Suppose, by contradiction and with no loss of generality, that for every $a' \in \mathrm{var}_A(\bigcup_{i=1}^n \Gamma_i' \cup \Delta_i')$, either $a' : \phi \notin \Psi_L$ or $a' : \boxdot \phi \notin \Psi_L$. Then, rule (KL) was not applied in the branch to ϕ. Hence, ϕ is in Γ_n'. Consider the branch $\Gamma_1' \to \Delta_1' \cdots \Gamma_n' \to \Delta_n' \, b : \phi, b : \boxdot \phi, \Gamma_n' \to \Delta_n'$ using in the last step the rule (KL) where b is not in $\bigcup_{i=1}^n \Gamma_i' \cup \Delta_i'$. Observe that this branch is still analytical. So, the original branch is not exhausted, which contradicts the hypothesis.

17. If $a :: (\phi_1, \ldots, \phi_n/\phi) \in \Psi_R$ then if $\phi_1, \ldots, \phi_n \in \Psi_L$ then $a : \phi \in \Psi_R$. Let us assume that $a :: (\phi_1, \ldots, \phi_n/\phi) \in \Psi_R$ and $\phi_1, \ldots, \phi_n \in \Psi_L$. Let us assume, by contradiction, that $a : \phi \notin \Psi_R$. Then, rule (CR1) was not applied in the branch to $a :: (\phi_1, \ldots, \phi_n/\phi)$. Hence, $a :: (\phi_1, \ldots, \phi_n/\phi)$ is in Δ_n'. Consider the branch $\Gamma_1' \to \Delta_1' \cdots \Gamma_n' \to \Delta_n' \, \phi_1, \ldots, \phi_n, \Gamma_n' \to \Delta_n', a : \phi$ using in the last step the rule (CR1). Observe that this branch is still analytical. So, the original branch is not exhausted, which contradicts the hypothesis.

18. If $a :: (\phi_1, \ldots, \phi_n/\phi) \in \Psi_L$ then either $\phi_i \in \Psi_R$ for some $i = 1, \ldots, n$ or $a : \phi \in \Psi_L$. Suppose that $a :: (\phi_1, \ldots, \phi_n/\phi) \in \Psi_L$. Let us assume, by contradiction, that $\phi_i \notin \Psi_R$ for every $i = 1, \ldots, n$ and $a : \phi \notin \Psi_L$. Then, rule (CR2) was not applied in the

branch to $a :: (\phi_1, \ldots, \phi_n/\phi)$. Hence, $a :: (\phi_1, \ldots, \phi_n/\phi)$ is in Γ'_n. Consider the branch $\Gamma'_1 \to \Delta'_1 \cdots \Gamma'_n \to \Delta'_n \; \Gamma'_n \to \Delta'_n, \phi_1$ using in the last step the rule (CR2). Observe that this branch is still analytical. So, the original branch is not exhausted, which contradicts the hypothesis.

QED