Computing and Informatics, Vol. 33, 2014, 61–78

View metadata, citation and similar papers at core.ac.uk
brought to you by CORE
provided by Computing and Informatics (E-Journal - Institute of Informatics,...

TOWARDS THE KNOWLEDGE IN COALGEBRAIC MODEL OF IDS

Daniel Mihályi, Valerie Novitzká

Department of Computers and Informatics
Technical University of Košice
Letná 9
042 00 Košice, Slovakia
e-mail: {Daniel.Mihalyi, Valerie.Novitzka}@tuke.sk

Abstract. In the last decades linear logic became a useful logical system for various usage in computer science. Its ability to handle resources and its competence to describe dynamics of processes predetermine it for describing behavior of programs and program systems. Linear logic can be apprehended as a multiplicative and additive extension of usual logic. We show the possibilities how these fragments can be enriched to describe behavior and to achieve knowledge on an example of simplified Intrusion Detection System (IDS). We construct Kripke model over a coalgebra of modal linear logic for pursuing observable behavior of IDS. Using the same Kripke frame we show how knowledge and belief in the terms of epistemic linear logic can be achieved.

Keywords: Coalgebra, epistemic logic, linear logic, Kripke model

Mathematics Subject Classification 2010: 18B05, 03B42, 03B43

1 INTRODUCTION

Linear logic [7] belongs to the newer logical systems with many applications in computer science within last two decades. This logic is a generalization of classical logic. It allows to describe dynamics of computer processes and to handle with resources. Girard defined two semantical definitions for this logic: by phase spaces (following Tarskian semantics) and coherent semantics (following Heyting semantics). The linear logic includes new logical connectives that are generalized ones of classical logic. Traditionally these connectives are divided into two groups:

- multiplicative connectives and
- additive connectives.

Multiplicative connectives include multiplicative conjunction $\otimes$, multiplicative disjunction $\invamp$ with neutral elements (constants) $1, \bot$. Additive connectives include additive conjunction $\&$ and additive disjunction $\oplus$ with neutral elements $\top$ and 0.

Following semantical aspects we can consider the multiplicative fragment as *intensional* one (Heyting semantical tradition) and additive fragment as *extensional* one (Tarski semantical tradition) [6]. Traditionally, the semantics of the extensional fragment expresses *denotation* (truth) of a given formula whereas the semantics of the intensional fragment expresses *sense* (idea) of a given formula. According to the previous ideas we can generalize classical logic into two distinct fragments of linear logic: intensional or extensional, as we need for our purposes.

The application field of linear logic amplifies if we extend it with modal operators. The aim of our paper is to demonstrate how these two fragments of linear logic can serve for different goals. The multiplicative (intensional) fragment extended with modal operators [21, 31] can serve for describing observable behavior of programs. The additive (extensional) fragment extended with epistemic operators [9, 20, 16] can be useful for acquiring knowledge and belief of some events in program execution.

In our paper we illustrate how these two fragments can be used for different purposes in computer science on an example of Intrusion Detection System (IDS) [1, 38, 41].

There are several works using logical methods in intrusion detection based on linear temporal logic. In [28] linear temporal logic Eagle extended with primitive modalities next, previous and concatenation is used for specifying intrusion patterns as temporal formulae. This approach is deployed in [19] incorporating knowledge into various kinds of agents in the new architecture of IDS. In [40] an intrusion detection algorithm is presented that is based on model checking. The authors use interval temporal logic enabling to describe concurrent attacks. The research in the area of modelling IDS based on various extensions of linear temporal logic has produced several prototype tools among which Orchids [29] based on model checking is most elaborated. We see the main advantage of linear logic used in our approach in its resource-oriented features. Linear logic has integrated time-space calculus at disposal, where every proof of formulae considered as space-resource can be transferred into a polarized proof tree depicting particular, possibly branched time lines [10]. We are convinced that resource-oriented character of linear logic designates it for usage in computing science.

Within investigating program systems we are interested not only in their construction, but also in their observable behavior. Observable behavior can be modelled by coalgebras in categorical terms [12, 35, 34] using coalgebraic modal logic [18, 30]. Relationship between coalgebras and modal logic was formulated in [3]. In Section 2 we define the intensional fragment of coalgebraic modal linear logic for IDS and we construct its model. We follow our results published in [24], where IDS is modelled as a coalgebra over appropriate polynomial endofunctor. The basic idea is that a coalgebra can be considered as a general form of Kripke semantics for modal logic.

Within behavioral observation some events can repeat and they can provide some interesting knowledge about program systems. Following the results in [39] we assume that objective knowledge implies rational belief. *Knowledge* and *belief* are fundamental notions of epistemic logic [2, 4, 5, 22]. In our approach we investigate the possibilities of obtaining objective knowledge and rational belief for simplified model of IDS following our results in [26]. Incoming packets form infinite streams and some of them can contain some intrusion attempts. These attempts can be recognized through characteristic symptoms. A determined combination of these symptoms gives us a knowledge about some kind of incoming intrusion. Moreover, if it comes from the same IP address and repeatedly, then we are sure that it is a real intrusion attempt and we can make our decision about competent reaction. We use extensional fragment of epistemic linear logic for describing objective knowledge and rational belief as a suitable logical system for reasoning about intrusion attempts. Repeating of the intrusion attempts can be described by the exponential operator !.

2 COALGEBRAIC MODAL LINEAR LOGIC FOR IDS

Typically, coalgebraic approach uses a modal logic with two modal operators ($\Box$ for necessity and $\Diamond$ for possibility) [18, 27]. In our approach we work with modal linear logic fragment because of the causality of its linear implication. We define the syntax of our intensional modal linear fragment by extended BNF form

$$\varphi ::= a_i | \varphi_1 \multimap \varphi_2 | \varphi_1 \otimes \varphi_2 | \varphi_1 \invamp \varphi_2 | \mathbf{1} | \bot | \Box\varphi | \Diamond\varphi | \nabla\Phi \qquad (1)$$

where

- a_i are atomic propositions,
- $\varphi_1 \multimap \varphi_2$ means linear implication; it ensures that the action φ_2 follows after the action φ_1,
- $\varphi_1 \otimes \varphi_2$ is intensional conjunction expressing that the actions φ_1 and φ_2 are both performed,
- $\varphi_1 \invamp \varphi_2$ is intensional disjunction expressing if φ_1 is not performed then φ_2 is performed and vice versa,
- $\mathbf{1}$ is the neutral element of the intensional conjunction,
- $\bot$ is the neutral element of the intensional disjunction,
- $\Box\varphi$ means application of the necessity operator to the formula φ,

- $\Diamond\varphi$ means application of the possibility operator to the formula φ,
- ∇ is a new modal operator introduced in [8] named *(coalgebraic) cover modality.* This operator ∇ takes a finite sequence $\Phi = \{\varphi_1, \varphi_2, \ldots, \varphi_n\}$ of formulae and returns a single formula $\nabla\Phi$.

  For our fragment of modal linear logic we define $\nabla\Phi$ as

$$\nabla\Phi \equiv \Box(\bigparr \Phi) \otimes \bigotimes \Diamond\Phi \tag{2}$$

where $\bigparr$ denotes

$$\bigparr \Phi \equiv \varphi_1 \parr \varphi_2 \parr \ldots \tag{3}$$

and

$$\Diamond\Phi = \{\Diamond\varphi | \varphi \in \Phi\}. \tag{4}$$

Then following [37] the symbol $\bigotimes$ denotes (possibly infinite) conjunction of formulae and

$$\bigotimes \Diamond\Phi \equiv \Diamond\varphi_1 \otimes \Diamond\varphi_2 \otimes \ldots \tag{5}$$

Modalities of necessity $\Box$ and possibility $\Diamond$ can be defined in the terms of operator ∇ and they satisfy the following equivalences

$$\begin{aligned} \Diamond\Phi &\equiv \nabla\{\Phi, 1\} \\ \Box\Phi &\equiv \nabla\varepsilon \parr \nabla\Phi \end{aligned} \tag{6}$$

where ε is empty sequence of formulae.

We illustrate coalgebraic modal linear logic on the example of IDS. We consider only three types of possible intrusions, A, B and C. If a packet does not contain any intrusion attempt we denote it by X. Because we need some identification of a sender, let O be its IP address. We construct the category $\mathcal{P}acket$ of incoming packets as follows:

- the objects are significant packet fragments for identification of intrusion attempts,

$$p = (A + B + C + X) \times O \tag{7}$$

  where $+$ and $\times$ denote coproduct and product of objects, respectively,
- the morphisms are mappings *next* between objects

$$next : p_i \rightarrow p_{i+1} \tag{8}$$

  for $i \in \mathbb{N}$.

It is clear that the category $\mathcal{P}acket$ has special sets as objects.

We construct the coalgebra over the category $\mathcal{P}acket$. A coalgebra [15] is considered as a structure for keeping track of states by observable properties. Formally, a coalgebra is a pair

$$(U, c) \tag{9}$$

where U is a state space, $c : U \to T(U)$ is a coalgebraic specification and T is a polynomial endofunctor. Let $\mathcal{C}$ be a category and X, Y be its arbitrary objects. A polynomial endofunctor $T : \mathcal{C} \to \mathcal{C}$ on the the category $\mathcal{C}$ is a functor constructed by using finite amount of following functorial operations: products in the form $X \times Y$, coproducts in the form $X + Y$ and exponents in the form X^Y [11, 17].

The state space for IDS is a stream of packets denoted by ρ_p. Now we define a polynomial endofunctor $T : \mathcal{P}acket \to \mathcal{P}acket$ on this category as follows:

$$T(p) = X \times p \quad and \quad T(next(p)) = X \times next(p). \tag{10}$$

Then coalgebraic specification for the polynomial endofunctor T is a tuple

$$\langle hd, tl \rangle : \rho_p \to T\rho_p \tag{11}$$

where hd and tl are obvious operations returning a head or a tail of a given stream. Following our results in [24] we modelled IDS system as a coalgebra (T-model)

$$(\rho_p, \langle hd, tl \rangle). \tag{12}$$

Contemporary experiences in system behavior have shown the importance of selection of an appropriate modal logical language as a specification language for various transition systems. Formulae of this language are used to logical reasoning over states of dynamic system that are captured by the coalgebra of corresponding polynomial (powerset) endofunctor. We formulated coalgebraic logic based on multimodal language suitable for the behavioral description of infinite, non trivial heterogenous data structures, i.e. packets at the coalgebra as intrusion detection system in [23, 25].

The consecutive application of coalgebraic specification produces an infinite sequence of the coalgebraic formulae

$$\begin{array}{r} (\mathbf{1}) \\ (p_1, \mathbf{1}) \\ (p_1, (p_2, \mathbf{1})) \\ (p_1, (p_2, (p_3, \mathbf{1}))) \\ \ldots \\ (p_1, (p_2, (p_3, (\ldots, (\ldots, \mathbf{1}) \ldots)))) \end{array} \tag{13}$$

where the first row $(\mathbf{1})$ denotes the empty sequence, the initial state of the system. The second row arises after the first application of coalgebraic specification and it corresponds with the coalgebraic linear formula $(p_1 \otimes \mathbf{1})$. It describes the system where the first packet has arrived. The following rows describe iterative application of coalgebraic specification up to possible infinite sequence. The last row corresponds with the following coalgebraic linear formula

$$\bigotimes \{(p_1, (p_2, (p_3, (\ldots, (\ldots, \mathbf{1}) \ldots))))\}. \tag{14}$$

In the following text let $Prop$ be a set of propositions.

As a model of our intensional fragment of modal linear logic we define appropriate Kripke model of possible worlds. Kripke model consists of a Kripke frame

$$(W, \leq, w_0) \tag{15}$$

together with a satisfaction relation $\models_i$ forming a tuple

$$(W, \leq, \models_i, w_0) \tag{16}$$

where

- W is a set of possible worlds,
- $\leq$ is an accessibility relation $\leq \subseteq W \times W$,
- $\models_i$ is a intensional satisfaction relation

$$\models_i : W \times Prop \to \{\mathbf{1}, \bot\} \tag{17}$$

  where $\mathbf{1}$ means satisfaction and $\bot$ means non satisfaction,
- w_0 is a designated world.

We read the notation $w_1 \leq w_2$ as follows: A possible world w_2 is reachable (accessible) from w_1. According to the philosophy of possible world semantics: "what is reachable is possible" [42].

A coalgebra can be seen as a general form of Kripke semantics for modal logic [39]. An interpretation of a formula in a coalgebra is given by predicate lifting [32], i.e. a natural transformation

$$\lambda : \mathcal{P}^- \Rightarrow \mathcal{P}^- \circ T \tag{18}$$

where $\mathcal{P}^-$ is a contravariant powerset functor $\mathcal{P}^- : Set \to Set$ between sets (Figure 1).

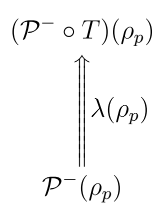

Figure 1. Predicate lifting

$\lambda(\rho_p)$ is a class of morphisms defined by

$$\lambda(\rho_p) : \mathcal{P}^-(\rho_p) \to (\mathcal{P}^- \circ T)(\rho_p). \tag{19}$$

This predicate lifting produces $\mathcal{P}$-model over $\mathcal{T}$-model as follows:

$$\begin{array}{lll} \mathcal{P}\text{-model} & ((\lambda(\rho_p), & \langle hd, tl\rangle : \rho_p \to T\rho_p) \\ & \Uparrow \lambda & \\ T\text{-model} & ((\rho_p), & \langle hd, tl\rangle : \rho_p \to T\rho_p) \end{array}$$

i.e.

- every packet $p \in \rho_p$ lifts to a (designated) world $w \in W$,

$$\begin{array}{ccccc} w_i & w_i & w_i & w_i & \dots \\ \Uparrow \lambda & \Uparrow \lambda & \Uparrow \lambda & \Uparrow \lambda & \dots \\ p_1 & p_2 & p_3 & p_4 & \dots \end{array}$$

  where $i = 1, 2, \dots, n$

- every morphism *next* lifts to the accessibility relation $\leq$.

Now we have Kripke frame $(W, \leq)$.

We define the interpretation of formulae in our $\mathcal{P}$-model

$$(\lambda(\rho_p), \langle hd, tl\rangle : \rho_p \to T\rho_p) \tag{20}$$

as follows:

- for every formula φ we define its semantics as a set $[\![\varphi]\!] \subset \rho_p$ simply by induction on the structure of φ,
- for modal operator $\Box$ we define the satisfaction as a composition

$$[\![\Box\varphi]\!] = \mathcal{P}^{-}(\langle hd, tl\rangle : \rho_p \to T\rho_p) \circ \lambda([\![\varphi]\!]). \tag{21}$$

The operator of possibility $\Diamond$ is dual to the operator of necessity $\Box$.

It is clear that in IDS the set W of possible worlds corresponds to a stream of packets ρ_p.

- Every world $w \in W$ corresponds to a packet $p \in \rho_p$,
- the reachability relation

$$\leq \subseteq W \times W \tag{22}$$

  gives a $\mathcal{P}$-coalgebra

$$(W, \langle hd, tl\rangle : \rho_p \to T\rho_p\rangle) \tag{23}$$

  where

$$(\langle hd, tl\rangle : \rho_p \to T\rho_p)_{\leq}(w) = \{w' \in W | (w, w') \in \leq\}. \tag{24}$$

3 EPISTEMIC LINEAR LOGIC FOR IDS

Epistemic logic is characterised as a logic of objective knowledge and rational belief. Our aim is to show how we can achieve knowledge and belief about intrusion attempts using Kripke model. We use extensional fragment of linear logic and we define the syntax of our epistemic linear logic as follows:

$$\varphi ::= a_i | \varphi_1 \& \varphi_2 | \varphi_1 \oplus \varphi_2 | \mathbf{0} | \top | !\varphi | \varphi^{\perp} | K_x\varphi | B_x\varphi \tag{25}$$

where

- a_i are atomic propositions (i.e. pieces of knowledge),
- $\varphi_1 \& \varphi_2$ is the extensional conjunction of two formulas φ_1,φ_2,
- $\varphi_1 \oplus \varphi_2$ is the extensional disjunction of two formulas φ_1,φ_2,
- $\top$ is the neutral element of the extensional conjunction,
- $\mathbf{0}$ is the neutral element of the extensional disjunction,
- $!\varphi$ is empiric modal linear operator expressing pleonasm property of formula,
- $\varphi^{\perp}$ is linear negation,
- $K_x\varphi$ denotes that a rational agent c knows that φ,
- $B_x\varphi$ denotes that a rational agent c believes that φ.

Assume an infinite stream of packets ρ_p as the following sequence

$$(p_i, p_{i+1}, \ldots, p_n, \ldots, p_{n+299}, p_{n+300}, p_{n+301}, \ldots). \tag{26}$$

This sequence can be elaborated stepwise:

$$\begin{array}{ll}
\mapsto (A \times O, X \times O, \ldots, A \times O, \ldots, A \times O, B \times O, C \times O, \ldots) & \mapsto \\
\mapsto (X \times O, \ldots, A \times O, \ldots, A \times O, B \times O, C \times O, \ldots) & \mapsto^{*} \\
\mapsto^{*} (A \times O, \ldots, A \times O, B \times O, C \times O, \ldots) & \mapsto^{300} \\
\mapsto^{300} (B \times O, C \times O, \ldots) & \mapsto \\
\mapsto (C \times O, \ldots) & \mapsto \\
\mapsto \ldots &
\end{array} \tag{27}$$

In this stream

- $p_j, j \in \mathbb{N}$ are treated packet fragments,
- A is an intrusion attempt *COMMUNITY SIP*,
- B is an intrusion attempt *SNMP AgentX/tcp, request*
- C is an intrusion attempt *SNMP request tcp.*

Using Kripke frame from (20) we show how knowledge and belief about some intrusion attempt can be achieved from the stream of packets. The extensional satisfaction relation for our epistemic linear logic is defined as

$$\models_e : W \times Prop \to \{\top, \mathbf{0}\} \tag{28}$$

where $\top$ means satisfaction and **0** means non satisfaction.

Before we define how to acquire a knowledge and belief from the symptoms in incomming stream of packets, we have to define Kripke semantics for epistemic operators K of knowledge and B of belief. We come out from approach published in [13] and [14].

In the following, let x be an agent.

A formula $K_x\varphi$ is satisfied in a world w if and only if φ is satisfied in all worlds w' accessible from w, $w \leq w'$

$$w \models_e K_x\varphi \qquad \textbf{iff} \qquad \text{for every} \qquad w', w \leq w', \qquad w' \models_e \varphi. \tag{29}$$

In the definition of the semantics of the operator B we use the basic idea of epistemic logic: a "knowledge implies a belief", i.e. a formula $B_x\varphi$ is satisfied in a world w if $K_x\varphi$ is satisfied in this world. If we formalize this idea in the form of implication, it does not embrace the case when a formula $B_x\varphi$ is not satisfied in a world w. Therefore we use equivalence in the form

$$w \models_e K_x\varphi \qquad \textbf{iff} \qquad w \models_e B_x\varphi. \tag{30}$$

However, this definition states that both epistemic operators K and B have the same semantics. We make this definition more meaningful if we require repeated knowledge of φ using exponential operator "!", i.e. $!K_x\varphi$

$$w \models_e !K_x\varphi \qquad \textbf{iff} \qquad w \models_e B_x\varphi. \tag{31}$$

We explore the following cases. It is not enough to obtain a knowledge $K_x\varphi$ to acquire a belief about an intrusion attempt. Our definition requires repeated knowledge. By contraries, if $B_x\varphi$ is satisfied in a world w, then $!K_x\varphi$ has to be satisfied in this world. In other words, a belief in an intrusion attempt is equivalent with repeatedly obtained knowledge about this attempt. If $B_x\varphi$ is not satisfied in a world w then $!K_x\varphi$ is not satisfied in this world. In other words, if an agent x is not convinced of an intrusion attempt then either it has obtained a knowledge only once or has not obtained any knowledge about intrusion attempt.

Type A	*Type B*	*Type C*

(COMMUNITY SIP)
`Protocol == ip`
`Port == 5060`
`count == 300`
`seconds == 60`
	(SNMP AgentX/tcp request)
	`Protocol == tcp`
	`Port == 705`
	`classtype == attempt-recon`
		(SNMP request tcp)
		`Protocol == tcp`
		`Port == 161`
		`flow == stateless`

Table 1. Particular types of network intrusions

Let $AP = \{a_1, a_2, a_3, a_4, b_1, b_2, b_3, c_1, c_2, c_3, \ldots\}$ be a set of atomic propositions. Every atomic proposition denotes one symptom of possible intrusion attempt.

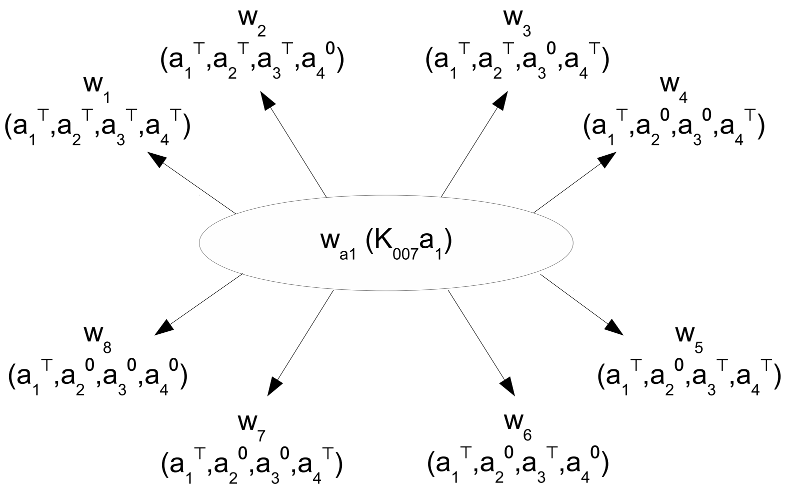

Figure 2. Achieving knowledge

In our example of IDS we consider only one (rational) agent 007. This agent can be a part of communication interface between human and computer system.

According to Table 1 we achieve the knowledge about intrusion attempt of Type A from the tuple (a_1, a_2, a_3, a_4) if

- a_1: `Protocol` is equal to `ip`,
- a_2: `Port` is equal to `5060`,
- a_3: `count` is equal to `300`,
- a_4: `seconds` is equal to `60`.

If a symptom a_i is present then we assign the value $\top$ to it. Otherwise we assign the value $\mathbf{0}$ to a_i. All possible situations are shown in Table 2. We see that we will work with sixteen possible worlds.

According to the definition of operator K, Figure 2 shows how the agent 007 achieves the particular piece of knowledge about a_1. Similarly, we can apply this technique on the other symptoms a_2, a_3, a_4.

The intrusion attempt of Type A occurs only if all symptoms a_i have occurred, i.e. there exists a world w_a where

$$w_a \models_e K_{007}a_1 \quad w_a \models_e K_{007}a_2 \quad w_a \models_e K_{007}a_3 \quad w_a \models_e K_{007}a_4. \tag{32}$$

The existence of a world w_a results from our Kripke frame. Therefore the agent 007 has objective knowledge about intrusion attempt of Type A if it has objective knowledge about all symptoms a_i, $i = 1, \ldots, 4$.

Type A	a_1	a_2	a_3	a_4
w_{16}	$\mathbf{0}$	$\mathbf{0}$	$\mathbf{0}$	$\mathbf{0}$
w_{15}	$\mathbf{0}$	$\mathbf{0}$	$\mathbf{0}$	$\top$
w_{14}	$\mathbf{0}$	$\mathbf{0}$	$\top$	$\mathbf{0}$
w_{13}	$\mathbf{0}$	$\mathbf{0}$	$\top$	$\top$
w_{12}	$\mathbf{0}$	$\top$	$\mathbf{0}$	$\mathbf{0}$
w_{11}	$\mathbf{0}$	$\top$	$\mathbf{0}$	$\top$
w_{10}	$\mathbf{0}$	$\top$	$\top$	$\mathbf{0}$
w_9	$\mathbf{0}$	$\top$	$\top$	$\top$
w_8	$\top$	$\mathbf{0}$	$\mathbf{0}$	$\mathbf{0}$
w_7	$\top$	$\mathbf{0}$	$\mathbf{0}$	$\top$
w_6	$\top$	$\mathbf{0}$	$\top$	$\mathbf{0}$
w_5	$\top$	$\mathbf{0}$	$\top$	$\top$
w_4	$\top$	$\top$	$\mathbf{0}$	$\mathbf{0}$
w_3	$\top$	$\top$	$\mathbf{0}$	$\top$
w_2	$\top$	$\top$	$\top$	$\mathbf{0}$
w_1	$\top$	$\top$	$\top$	$\top$

Table 2. Intrusion Type A – *COMMUNITY SIP TCP/IP*

The following formula $K_{007}\chi$ denotes objective knowledge about intrusion attempt of Type A

$$K_{007}\chi \quad \equiv \quad K_{007}a_1 \& K_{007}a_2 \& K_{007}a_3 \& K_{007}a_4 \tag{33}$$

and it is satisfied in w_1, i.e. $w_a = w_1$.

Similarly, for the next intrusion attempt of Type B we consider the following pieces of knowledge about given intrusion attempt from a tuple (b_1, b_2, b_3) if

- b_1: `Protocol` is equal to `tcp`,
- b_2: `Port` is equal to `705`,
- b_3: `classtype` is equal to `attempt-recon`.

If a symptom b_i is present then we assign the value $\top$ to it. Otherwise we assign the value $\mathbf{0}$ to b_i. According to Table 3 we will work with eight possible worlds.

Using the same technique as in the previous case, we can affirm that the agent 007 has the particular piece of knowledge about b_i, $i = 1, \ldots, 3$.

The intrusion attempt of Type B occurs only if all symptoms b_i have occurred, i.e. there exists a world w_b where

$$w_b \models_e K_{007}b_1 \quad w_b \models_e K_{007}b_2 \quad w_b \models_e K_{007}b_3. \tag{34}$$

Therefore the agent 007 has objective knowledge about intrusion attempt of Type B if it has objective knowledge about all symptoms b_i, $i = 1, \ldots, 3$.

Type B	b_1	b_2	b_3
w_{24}	$\mathbf{0}$	$\mathbf{0}$	$\mathbf{0}$
w_{23}	$\mathbf{0}$	$\mathbf{0}$	$\top$
w_{22}	$\mathbf{0}$	$\top$	$\mathbf{0}$
w_{21}	$\mathbf{0}$	$\top$	$\top$
w_{20}	$\top$	$\mathbf{0}$	$\mathbf{0}$
w_{19}	$\top$	$\mathbf{0}$	$\top$
w_{18}	$\top$	$\top$	$\mathbf{0}$
w_{17}	$\top$	$\top$	$\top$

Table 3. Intrusion Type B – *SNMP AgentX/tcp request*

The following formula $K_{007}\varphi$ denotes objective knowledge about intrusion attempt of Type B

$$K_{007}\varphi \quad \equiv \quad K_{007}b_1 \& K_{007}b_2 \& K_{007}b_3 \tag{35}$$

and it is satisfied in w_{17}, i.e. $w_b = w_{17}$.

For the intrusion attempt of Type C we consider the following pieces of knowledge (c_1, c_2, c_3) if

- c_1 : `Protocol` is equal to `tcp`,
- c_2 : `Port` is equal to `161`,
- c_3 : `flow` is equal to `stateless`.

If a symptom c_i is present then we assign the value $\top$ to it. Otherwise we assign the value $\mathbf{0}$ to c_i. According to Table 4 we will also work with eight possible worlds.

Type C	c_1	c_2	c_3
w_{32}	$\mathbf{0}$	$\mathbf{0}$	$\mathbf{0}$
w_{31}	$\mathbf{0}$	$\mathbf{0}$	$\top$
w_{30}	$\mathbf{0}$	$\top$	$\mathbf{0}$
w_{29}	$\mathbf{0}$	$\top$	$\top$
w_{28}	$\top$	$\mathbf{0}$	$\mathbf{0}$
w_{27}	$\top$	$\mathbf{0}$	$\top$
w_{26}	$\top$	$\top$	$\mathbf{0}$
w_{25}	$\top$	$\top$	$\top$

Table 4. Intrusion Type C – *SNMP request tcp*

Again, using the same technique as in the previous case, we can affirm that the agent 007 has the particular piece of knowledge about c_i, $i = 1, \dots, 3$.

The intrusion attempt of Type C occurs only if all symptoms c_i have occurred, i.e. there exists a world w_c such that

$$w_c \models_e K_{007}c_1 \quad w_c \models_e K_{007}c_2 \quad w_c \models_e K_{007}c_3. \tag{36}$$

Therefore the agent 007 has objective knowledge about intrusion attempt of Type C if it has objective knowledge about all symptoms c_i, $i = 1, \dots, 3$.

The following formula $K_{007}\psi$ denotes objective knowledge about intrusion attempt of Type C

$$K_{007}\psi \quad \equiv \quad K_{007}c_1 \& K_{007}c_2 \& K_{007}c_3 \tag{37}$$

and it is satisfied in w_{25}, i.e. $w_c = w_{25}$.

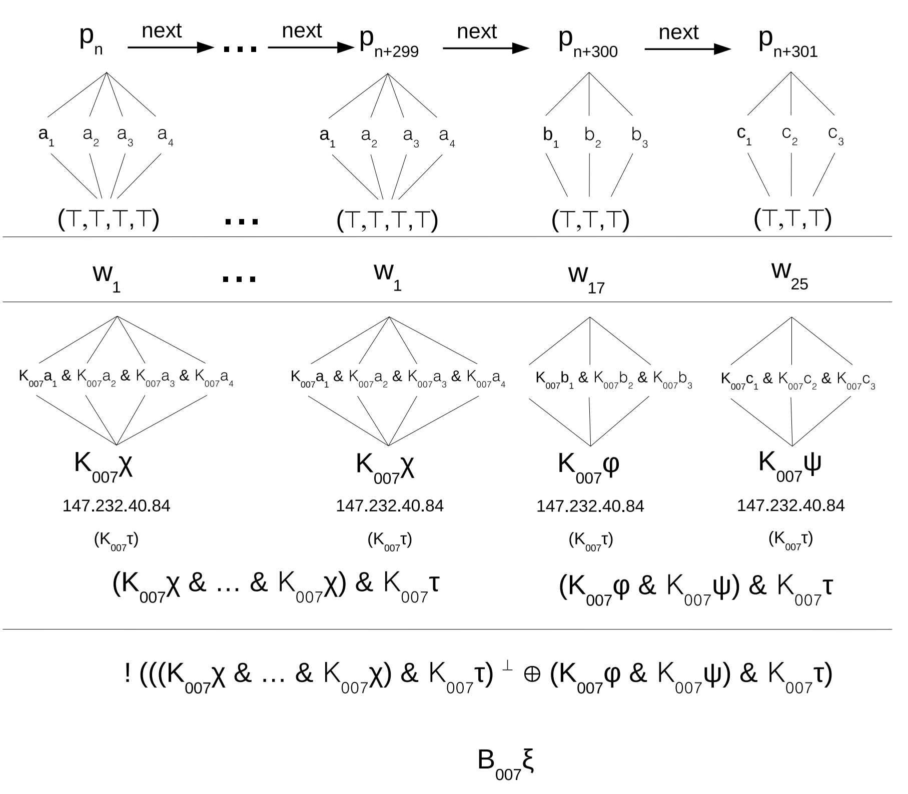

Figure 3. Epistème

We denote by $K_{007}\tau$ the knowledge about sender identification.

In Figure 3 we illustrate how we achieve knowledge and belief about intrusion attempts from a fragment of packet stream in (27).

The formula

$$(\underbrace{K_{007}\chi \& \dots \& K_{007}\chi}_{300}) \& K_{007}\tau \tag{38}$$

describes that an attempt of Type A from the same sender occurred 300 times. The formula

$$(K_{007}\varphi \& K_{007}\psi) \& K_{007}\tau \tag{39}$$

describes the attempts of Type B and Type C from the same sender. Extensional consequence in terms of epistemic linear logic can be written through negation and extensional disjunction. Then the formula

$$K_{007}\xi \equiv ((\underbrace{K_{007}\chi \& \ldots \& K_{007}\chi) \& K_{007}\tau}_{300})^{\perp} \oplus ((K_{007}\varphi \& K_{007}\psi) \& K_{007}\tau) \tag{40}$$

describes the situation, when after repeated attempt of Type A the attempts of Type B and Type C from the same sender follow immediately. This situation is known as *vertical portscan* [36]. There exists a world w_0, our designated world, such that $w_0 \models_e K_{007}\xi$. If this situation repeats, using our semantics of operator B we state that the agent 007 has achieved rational belief about vertical portscan occurrence in the world w_0

$$w_0 \models_e !K_{007}\xi \quad \textbf{iff} \quad w_0 \models_e B_{007}\xi \tag{41}$$

and we can make some protecting actions.

4 CONCLUSIONS

In this paper we present our ideas about achieving knowledge and belief from the observable behavior of program systems. We illustrate our approach on the simplified IDS and we show how the pieces of knowledge can be achieved from some symptoms, how its combination gives us the knowledge about some intrusion detection and how repeating of some knowledge leads to belief about a concrete intrusion attempt. Our approach is based on coalgebraic modelling of system behavior. Instead of obvious correspondence with modal logic we construct Kripke model of extensional fragment of epistemic linear logic suitable for our purposes and we show how we can achieve objective knowledge and rational belief from this model from pieces of knowledge.

Our approach uses only IP protocol version ipv4 and only three possible intrusion attempts. Our idea can be generalized for any type of intrusion attempt and we would like to investigate achieving of knowledge and belief for IP protocol version ipv6, too. In further research we would like to follow our results and extend our approach for distributed intrusion attempts considering groups of agents as rational carriers of knowledge.

Our formal approach can also be implemented for real intrusion attempts with very sophisticated nature and can help us to make correct decisions about competent reactions.

Acknowledgements

This work was supported by the Slovak Research and Development Agency under contract No. APVV-0008-10 "Modelling, simulation and implementation of GPGPU-enabled architectures of high-throughput network security tools".

This work is the result of implementating the project "Center of Information and Communication Technologies for Knowledge Systems" (ITMS project code: 26220120030) supported by the Research & Development Operational Program funded by the ERDF.

REFERENCES

[1] Akyazi, U.—Uyar, S. A.: Distributed Detection of DDoS Attacks during the Intermediate Phase Through Mobile Agents. Computing and Informatics, Vol. 31, 2012, No. 4, pp. 759–778.

[2] Baltag, A.—Coecke, B.—Sadrzadeh, M.: Epistemic Actions as Resources. Journal of Logic and Computation 2007, pp. 555–585.

[3] Barwise, J.—Moss, L.: Vicious Circles. Center of the Study of Language and Information, Standford University 1996.

[4] Benthem, A.: Games in Dynamic-Epistemic Logic. Bulletin of Economic Research, Vol. 53, 2001, No. 4, pp. 219–248.

[5] Cirstea, C.—Sadrzadeh, M.: Coalgebraic Epistemic Update without Change of Model. Conference on Algebra and Coalgebra in Computer Science, Bergen, Norway 2007, pp. 158–172.

[6] Girard, J. Y.—Taylor, P.—Lafont, Y.: Proofs and Types. Cambridge University Press, New York 1989, ISBN 0-521-37181-3.

[7] Girard, J. Y.: Linear logic. Theoretical Computer Science 50, 1987, pp. 1–102.

[8] Bílková, M.—Palmigiano, A.—Venema, Y.: Proof Systems for the Coalgebraic cover modality. Advances in Modal Logic, Vol. 7, 2008, pp. 1–21.

[9] Garg, D.—Bauer, L.—Bowers, K. D.—Pfenning, F.—Reiter, M. K.: A Linear Logic of Authorization and Knowledge. Lecture Notes in Computer Science, Vol. 4189/2006, 2006, pp. 297–312.

[10] Girard, J.-Y.: From Foundations to Ludics. Bulletin of Symbolic Logic, Vol. 9, 2003, No. 2, pp. 131–168.

[11] Goldblatt, R.: A Calculus of Terms for Coalgebras of Polynomial Functors. Electronical Notes of Theoretical Computer Science, Vol. 44, 2001, No. 1.

[12] Gumm, H. P.: Functors for Coalgebras. Algebra Universalis, Vol. 45, 2001, pp. 135–147.

[13] Hintikka, J.: Knowledge and Belief: An Introduction to the Logic of the Two Notions. Cornell University Press 1962.

[14] Hoeck, W.—Verbrugge, R.: Epistemic Logic: A Survey. 2002.

[15] Jacobs B.—Rutten, J.: A Tutorial on (Co)Algebras and (Co)Induction. EATCS Bulletin, Vol. 62, 1997, pp. 222–259.

[16] Kamide, N.: Linear and Affine Logics with Temporal, Spatial and Epistemic Operators. Theoretical Computer Science 353, 2007, Vol. 13, pp. 165–207.

[17] Kock, J.: Notes on Polynomial Functors. Universitat Autònoma de Barcelona, 2007.

[18] Kurz, A.: Coalgebras and Modal Logic. CWI, Amsterdam, Netherlands, 2001.

[19] Das, P.—Niyogi, R.: A Temporal Logic Based Approach to Multiagent Intrusion Detection and Prevention. International Journal of Communication Network & Security, Vol. 1, 2011, No. 1, pp. 53–61.

[20] Marion, M.—Sadrzadeh, M.: Reasoning about Knowledge in Linear Logic: Modalities and Complexity, Logic, Epistemology, and the Unity of Science. Kluwer, 2004.

[21] Martini, S.—Masini, A.: A Modal View of Linear Logic. Journal of Symbolic Logic, Vol. 59, 1994, No. 3, pp. 888–899.

[22] Martini, J.-J. Ch.: Epistemic Logic. Artifical Intelligence Preprint Series, No. 10, 1999.

[23] Mihályi, D.: Duality Between Formal Description of Program Construction and Program Behaviour. Information Sciences and Technologies Bulletin of the ACM Slovakia, Vol. 1, 2010, No. 2, ISSN 1338-1237, pp. 1–5.

[24] Mihályi, D.—Novitzká, V.: A Coalgebra as an Intrusion Detection System. Acta Polytechnica Hungarica, Budapest, Vol. 7, 2010, Issue 2, ISSN 1785-8860, pp. 71–79.

[25] Mihályi, D.—Novitzká, V.: Princípy Duality Medzi Konštruovaním a Správaním Programov. Equilibria, 2010, ISBN 9788089284580.

[26] Mihályi, D.—Novitzká, V.—Ľaľová, M.: Intrusion Detection System Epistème. In: Š. Hudák and V. Novitzká (Eds.): Principles of Knowledge Representation and Reasoning, Proceedings of the 11th event of International Scientific Conference on Informatics, Informatics 2011, Rožňava, November 2011.

[27] Moss, L. S.: Coalgebraic Logic. Annals of Pure and Applied Logic, Vol. 96, 1999, pp. 277–317.

[28] Naldurg, P.—Sen, K.—Thati, P.: A Temporal Logic Based Framework for Intrusion Detection. FORTE, LNCS 3235, Springer, 2004, pp. 359–376.

[29] Olivain, J.—Goubalt-Larrecq, J.: The Orchids Intrusion Detection Tool. In Proceedings of the 17th International Conference on Computer Aided Verificatioon (CAV '05), Edinburgh, July 2005, LNCS 3576, pp. 286–290.

[30] Pattinson, D.: Semantical Principles in the Modal Logic of Coalgebras. In. Proceedings 18th International Symposium on Theoretical Aspects of Computer Science STACS, Springer LNCS Berlin, 2001.

[31] Sadrzadeh, M.: Modal Linear Logic in Higher Order Logic, an Experiment in Coq. In (Basin, D., Burkhart, W., eds.): Theorem Proving in Higher Order Logics, September 2003, Rome, Italy. pp. 75–93.

[32] Santocanale, L.—Venema, Y.: Uniform Interpolation for Monotone Modal Logic. Advances in Modal Logic, 2010, pp. 350–370.

[33] Schröder, L.—Pattinson, D.: Coalgebraic Modal Logic: Forays Beyond Rank 1. IFIP WG 1.3 Meeting, 2008, Sierra Nevada.

[34] Slodičák, V.: Some Useful Structures for Categorical Approach for Program Behavior. Journal of Information and Organizational Sciences, Vol. 35, 2011, No. 1, ISSN 1846-9418, pp. 99–109.

[35] Slodičák, V.—Macko, P.: New Approaches in Functional Programming Using Algebras and Coalgebras. In European Joint Conferrences on Theory and Practice of Software – ETAPS 2011 (March 2011), Workshop on Generative Technologies, Universität des Saarlandes, Saarbrücken, Germany, 2011, ISBN 978-963-284-188-5, pp. 13–23.

[36] Snort Web Site. Availaible on: `http://www.snort.org`.

[37] Venema, Y.: A Modal Logic of Quantification and Substitution. Bulletin of the IGPL, Vol. 2, 1995, pp. 293–309.

[38] Vokorokos, L.—Baláž, A.: Distributed Detection System of Security Intrusions Based on Partially Ordered Events and Patterns, Towards Intelligent Engineering and Information Technology. Studies in Computational Intelligence, Springer, Vol. 243, 2009, pp. 389–403.

[39] Voorbraak, F.: Generalized Kripke Models for Epistemic Logic. Proceedings of Fourth Conference on Theoretical Aspects of Reasoning About Knowledge, Morgan Kaufmann Publishers Inc. San Francisco, CA, USA, 1992, SBN: 1-55860-243-9, pp. 214–228.

[40] Weijun, Z.—Zhongyong, W.—Haibin, Z.: Intrusion Detection Algorithm Based on Model Checking Interval Temporal Logic. China Communications, Vol. 8, 2011, No. 3, pp. 66–72.

[41] Zhao, F.—Jin, H.: Automated Approach to Intrusion Detection in VM-based Dynamic Execution Environment. Computing and Informatics, Vol. 31, 2012, No. 2, pp. 271–297.

[42] Zouhar, M.: Základy Logiky. Proceedings of Fourth Conference on Theoretical aspects of reasoning about knowledge, Veda SAV, Bratislava, 2008, ISBN 978-80-224-1040-3 (in Slovak).

Daniel Mihályi worked as a researcher at the Department of Computers and Informatics of the Faculty of Electrical Engineering and Informatics, Technical University in Košice, Slovakia and later as an Assistant Professor. In 2009 he defended his Ph. D. thesis "Duality of Formal Description of Construction and Program Behavior". The main focus of his research includes application of category theory in informatics and using of resource-based logical systems for formal description of program systems behavior.

Valerie Novitzká works as a Full Professor of Informatics at the Department of Computers and Informatics of the Faculty of Electrical Engineering and Informatics, Technical University in Koice, Slovakia. She defended her Ph. D. thesis "Formal Semantics of Annotated ADA" in Budapest, Hungary in 1989. Her fields of research include non-classical logical systems and their applications in computing science. She also works with type theory, behavioural modeling of large program systems based on categories.