STUDIA UNIV. BABEŞ–BOLYAI, INFORMATICA, Volume **LXII**, Number 2, 2017
DOI: 10.24193/subbi.2017.2.03

LOGICAL TIME AND SPACE OF THE NETWORK INTRUSION

DANIEL MIHÁLYI, JÁN PERHÁČ, AND PATRIK BÁLINT

Abstract. Nowadays, one of the biggest threats for modern computer networks are the cyber attacks. One of the possible ways how to increase the level of computer networks security is a deployment of a network intrusion detection system. This paper deals with the behavior of the network intrusion detection system during specific network intrusion. We formally describe this network intrusion by the modal linear logic formula. Based on this formula, logical space and logical time is expressed from the attacker, and the network environment point of view in the usage of the Ludics theory.

1. Introduction

Just as people communicate with each other, so do the computers. This communication takes place within computer networks. As computer users, people encounter the term 'computer network' on a daily basis. Computer security threats are relentlessly inventive. These threats constantly evolve the possibilities how to find new ways to annoy, steal, or harm the user's data. Intrusion Detection System (IDS) [6] is one of the ways how to protect computer network from security threats. IDS is a device or software application that monitors a network or computer systems for malicious activities or policy violations. Each detected activity or violation is typically reported either to an administrator or collected centrally. A sequence of such causal activities can be described by a resource-oriented logical system properly.

In our approach, we use Linear Logic, which is a suitable logical system for usage in the field of computer science. This Logic [1] [2], is a substructural logic proposed as a refinement of classical and intuitionistic logic. Linear Logic brings new possibilities how to reason about formulæ in the resource oriented

Received by the editors: October 15, 2017.

2010 *Mathematics Subject Classification.* 18C10, 68M10.

1998 *CR Categories and Descriptors.* I.2.7 [**Mathematical Logic and Formal Languages**]: Formal Languages – *Language models*.

Key words and phrases. Linear Logic, DDoS Attack, SYN Flood, Ludics, Logical Space, Logical Time.

form. It means that a formula can be considered as a action or a resource that is performed in control manner. For example, the linear implication is causal which means that after performing it, the assumption is consumed.

In our previous work, we have created the network laboratory and described IDS's behavior during a ARP spoofing attack by linear logic formula [10]. From the coalgebraic point of view, we have described behavior of a IDS step by step through the coalgebra for a polynomial endofunctor in [8]. Then we have translated real network intrusion signatures based to coalgebraic one [9]. In this paper, we present usage of the Modal Linear Logic, which is a suitable logic to describe the behavior of state-oriented dynamic of an executed program system. The whole process of performing network attack and catching a network intrusion by a IDS is specified by behavioral the resource oriented logical formula. Then, we apply a logical time and a logical space from the Ludics theory [3], which was proposed by the J. Y. Girard [1]. In terms of this theory, we can consider a behavioral formula as a polarized game between an attacker and a network environment.

2. Modal linear logic

For the exact description of intrusion detection system's behavior, we have introduced our new logical system. We have proposed the Modal Linear Logic for IDS, which results from generalization of the linear logic's multiplicative fragment and the coalgebraic logic [2] [7]. Compared to the other logical systems, the significant feature of linear logic is resource-oriented approach of dealing with formulæ [1], which creates a strong expressive power for describing the real processes [2], e.g. causality, pleonasm or parallelism and many more [5]. These, together with a modal operators of the coalgebraic modal logic, create an appropriate formalism for describing a behavior of state-oriented program systems such as IDS.

2.1. Syntax of Modal linear logic.

We formulate the syntax of Modal linear logic in [5], by the following production rule in the Backus-Naur form:

$$\varphi ::= a_n \mid 1 \mid \bot \mid \varphi \otimes \psi \mid \varphi \invamp \psi \mid \varphi \multimap \psi \mid \varphi^{\bot} \mid \Box\varphi \mid \Diamond\varphi,$$

where:

- a_n represents the elementary formulæ, where $n = \{1,2 ...\}$,
- $\varphi \otimes \psi$ with its neutral element 1 is the multiplicative conjunction, which describes the process of performing of both actions simultaneously,
- $\varphi \invamp \psi$ with its neutral element $\bot$ is the multiplicative disjunction, which expresses the commutativity of duality between available and

consumed resources by performing either the action φ or the action ψ,
- $\varphi \multimap \psi$ is the linear implication, which expresses that the (re)action ψ is the causal consequence of the action φ and after performing this implication, the resource φ became consumed ($\varphi^\perp$),
- $\varphi^\perp$ is the linear negation, which expresses duality between action (φ) and reaction ($\varphi^\perp$), in the other words, an available and a consumed resource, respectively,
- $\Box\varphi$ is the modal operator expressing necessity of the action φ,
- $\Diamond\varphi$ is the modal operator expressing possibility of the action φ.

2.2. **The proof system.** The proof system of Modal linear logic is defined in the Gentzen's double side sequent calculus. The building block of this calculus is a sequent, which has the following form:

$$\Gamma \vdash \Delta, \tag{1}$$

where Γ, Δ represent (finite) sets of formula(e).

The inference rules have following

$$\frac{assumption(s)}{conclusion}(rule\ name), \tag{2}$$

where the *assumption*(s) and the *conclusion* are sequents. There is a special type of rules without assumption, called *axioms.*

They are defined as follows:

- The identity rule:
$$\frac{}{\varphi \vdash \varphi}(id)$$
- The structural rules are a cut rule and exchange rules:
$$\frac{\Gamma \vdash \varphi \qquad \Delta, \varphi \vdash \psi}{\Gamma, \Delta \vdash \psi}(cut)$$
$$\frac{\Gamma, \varphi, \psi \vdash \Delta}{\Gamma, \psi, \varphi \vdash \Delta}(exl) \qquad \frac{\Gamma \vdash \varphi, \psi, \Delta}{\Gamma \vdash \psi, \varphi, \Delta}(exr)$$
- The logical rules deal with logical connectives:
$$\frac{\Gamma \vdash \Delta}{\Gamma, 1 \vdash \Delta}(1_l) \qquad \frac{}{\vdash 1}(1_r) \qquad \frac{}{\perp \vdash}(\perp_l) \qquad \frac{}{\Gamma \vdash \perp, \Delta}(\perp_r)$$
$$\frac{\Gamma, \varphi, \psi \vdash \Delta}{\Gamma, \varphi \otimes \psi \vdash \Delta}(\otimes_l) \qquad \frac{\Gamma \vdash \varphi, \Delta \qquad \Phi \vdash \psi, \Sigma}{\Gamma, \Phi \vdash \varphi \otimes \psi, \Delta, \Sigma}(\otimes_r)$$

$$\frac{\Gamma \vdash \varphi, \Delta \quad \Phi, \psi \vdash \Sigma}{\Gamma, \Phi, \varphi \multimap \psi \vdash \Delta, \Sigma}(\multimap_l) \qquad \frac{\Gamma, \varphi \vdash \psi, \Delta}{\Gamma \vdash \varphi \multimap \psi, \Delta}(\multimap_r)$$

$$\frac{\Gamma, \varphi \vdash \Delta \quad \Phi, \psi \vdash \Sigma}{\Gamma, \Phi, \varphi \parr \psi \vdash \Delta, \Sigma}(\parr l) \qquad \frac{\Gamma \vdash \varphi, \psi, \Delta}{\Gamma \vdash \varphi \parr \psi, \Delta}(\parr r)$$

$$\frac{\Gamma \vdash \varphi, \Delta}{\Gamma, \varphi^{\perp} \vdash \Delta}(()^{\perp}_l) \qquad \frac{\Gamma, \varphi \vdash \Delta}{\Gamma \vdash \varphi^{\perp}, \Delta}(()^{\perp}_r)$$

$$\frac{\Gamma \vdash \varphi, \Delta}{\Gamma \vdash \Box\varphi, \Delta}(\Box r) \qquad \frac{\Gamma, \varphi \vdash \Delta}{\Gamma, \Box\varphi \vdash \Delta}(\Box l)$$

$$\frac{\Gamma \vdash \varphi, \Delta}{\Gamma \vdash \Diamond\varphi, \Delta}(\Diamond r) \qquad \frac{\Gamma, \varphi \vdash \Delta}{\Gamma, \Diamond\varphi \vdash \Delta}(\Diamond l)$$

The proof of a formula is proof tree, constructed from the root (the bottom of the tree) up to the leaves. The proof tree leaves have to be axioms, which implies that Gentzen's style proof tree is constructed correctly. When all leaves are axioms, the formula is proven.

3. Motivation Example

In this section, we briefly introduce basic notions of the used methods related to the detection of a network intrusion by the intrusion detection system, and an informal description of the particular attack, that we demonstrate in the motivation example bellow.

IDS is a security system that monitors the computer system's activities and its network traffic, and analyzes that traffic for possible hostile attacks originating from outside of an organization, and also for a system misuse or attacks originating from inside of an organization. It provides the three significant functions: monitoring, detecting, and responding [4] to unauthorized activities by company insiders and outsider intrusions. IDS uses policies to define certain events that if detected, will issue an alert.

Our motivation example is based on the execution of a Distributed Denial of Service (DDOS) type of attack, which is "extended" Denial of Service (DOS) attack type. The point of the DOS is flooding a target (e.g. server) by requesting attempts to overload it. In case of a DDOS, the attack is performed from more hosts at the same target(s) at the same time. Nowadays there are plethora of DDOS attacks. We have chosen the Syn Flood attack. This attack exploits the Transmission Control Protocol's (TCP) "three way handshake", during a client attempt to connect with a server. The server first passively listens at a port for possible connections. To establish a connection, the client sends a **SYN** to the server. The **SYN** contains various information, but what is important, it contains IP address of the client. The server allocate resources for possible connection for the IP address for a some time *(half-open connection)*. Then the server responses by sending the SYN-ACK, to which the client response with **ACK**. After that a connection is established. The SYN Flood attack exploits the first step of this process. It sends multiple requests (**SYN**) for connections to the server, but with spoofed IP addresses. This can result into the server's overload, which cause its malfunction.

To demonstrate the SYN Flood attack, we have created the laboratory environment (as shown in Figure 1), where we can see the Attacker's machine, its Terminals, the Victim's machine (with a localhost running) and the Router. Attacker uses five terminals to flood the Victim's web server services.

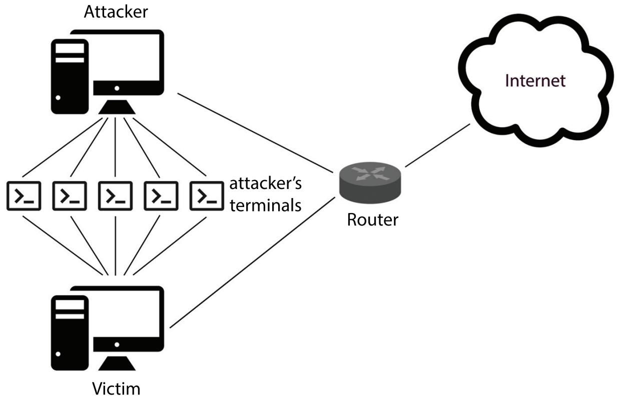


Figure 1. Laboratory network environment.

In our case, it is necessary to do the following steps to perform chosen attack:

1. examination of the Local Area Network (LAN) topology (address space, network mask, default gateway etc.), e.g. by the tool *nmap*,
2. perform a check for open ports on clients (potential victims) connected to the LAN by port scan,
3. execution of the Syn Flood attack at chosen client, from the 5 terminals simultaneously.

3.1. **Formula in Modal Linear Logic.** Now, we can describe the formula (see Figure 3) of the network intrusion by Modal Linear Logic for IDS (section 2):

$$(3)\ (((N \multimap S_1) \multimap \Diamond U_M)\otimes(((((H_1\otimes H_2)\otimes H_3)\otimes H_4)\otimes H_5) \multimap S_2)) \multimap \Box U_N,$$

where:

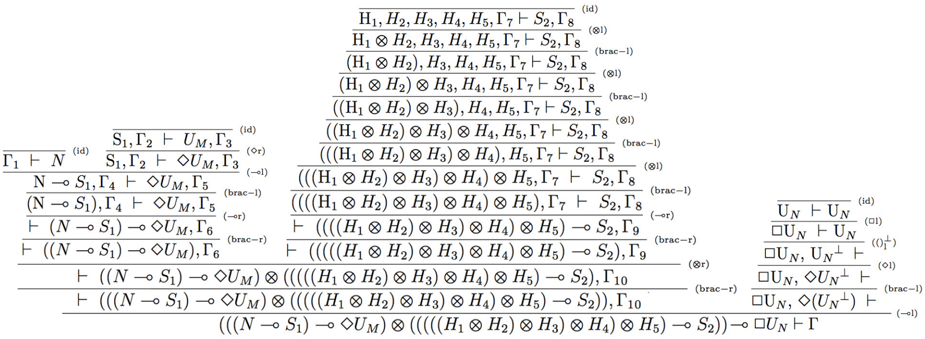
- N represents a vertical port scan of the victim's host port,
- S_1 is a reaction of IDS to vertical scanning of the victim's host ports by creating a log about a potential attack,
- $\Diamond U_M$ represents possible network intrusion,
- elements H_1 ... H_5 represent executing the SYN Flood attack from Attacker's five terminals to the Victim's machine,
- S_2 is a reaction to the SYN Flood attack from the Attacker's terminals,
- $\Box U_N$ represents the necessity of successful network attack.

The formula (3) can be interpreted as follows.

- *"Vertical port scan executed by the attacker (N)*
- *implies ($\multimap$)*
- *an action of the IDS by creating a log (S_1),*
- *and that implies $\multimap$*
- *a possible network intrusion ($\Diamond$ U_M),*
- *and ($\otimes$)*
- *performing the SYN Flood attack from the attacker's five terminals ($H_1\otimes, \ldots, \otimes H_5$),*
- *implies ($\multimap$)*
- *an action of IDS by creating a log (S_2),*
- *and that all implies ($\multimap$)*
- *the necessity of the network intrusion. ($\Box U_N$)"*

Next step is to create a proof tree in Linear Logic proof system, which is constructed from the root to leaves, as shown in Figure 2. All leaves have to be identities. The whole proof tree represents a process of the SYN Flood attack from the Attacker's point of view. The contexts in the proof tree are defined in Figure (3). Every deduction step in the proof tree above (Figure 2) is realized by using an appropriate rule (defined in the Section 2.2) of the linear Gentzen's calculus.

3.2. **De Morgan's form.** The original formula (3) demonstrate a process of the attack from the attacker's point of view. To show the same process from the network environment, it is necessary to transform it to the orthogonal one. It can be done by application of the De Morgan's laws Table 1. By applying



$\mathrm{H}_1, H_2, H_3, H_4, H_5, \Gamma_7 \vdash S_2, \Gamma_8$ (id)
$\mathrm{H}_1 \otimes H_2, H_3, H_4, H_5, \Gamma_7 \vdash S_2, \Gamma_8$ (⊗l)
$(\mathrm{H}_1 \otimes H_2), H_3, H_4, H_5, \Gamma_7 \vdash S_2, \Gamma_8$ (brac−l)
$(\mathrm{H}_1 \otimes H_2) \otimes H_3, H_4, H_5, \Gamma_7 \vdash S_2, \Gamma_8$ (⊗l)
$((\mathrm{H}_1 \otimes H_2) \otimes H_3), H_4, H_5, \Gamma_7 \vdash S_2, \Gamma_8$ (brac−l)
$((\mathrm{H}_1 \otimes H_2) \otimes H_3) \otimes H_4, H_5, \Gamma_7 \vdash S_2, \Gamma_8$ (⊗l)
$(((\mathrm{H}_1 \otimes H_2) \otimes H_3) \otimes H_4), H_5, \Gamma_7 \vdash S_2, \Gamma_8$ (brac−l)
$(((\mathrm{H}_1 \otimes H_2) \otimes H_3) \otimes H_4) \otimes H_5, \Gamma_7 \vdash S_2, \Gamma_8$ (⊗l)
$((((\mathrm{H}_1 \otimes H_2) \otimes H_3) \otimes H_4) \otimes H_5), \Gamma_7 \vdash S_2, \Gamma_8$ (brac−l)
$\vdash ((((H_1 \otimes H_2) \otimes H_3) \otimes H_4) \otimes H_5) \multimap S_2, \Gamma_9$ (⊸r)
$\vdash (((((H_1 \otimes H_2) \otimes H_3) \otimes H_4) \otimes H_5) \multimap S_2), \Gamma_9$ (brac−r)
$\Gamma_1 \vdash N$ (id)
$\mathrm{S}_1, \Gamma_2 \vdash U_M, \Gamma_3$ (id)
$\mathrm{S}_1, \Gamma_2 \vdash \Diamond U_M, \Gamma_3$ (◇r)
$\mathrm{N} \multimap S_1, \Gamma_4 \vdash \Diamond U_M, \Gamma_5$ (⊸l)
$(\mathrm{N} \multimap S_1), \Gamma_4 \vdash \Diamond U_M, \Gamma_5$ (brac−l)
$\vdash (N \multimap S_1) \multimap \Diamond U_M, \Gamma_6$ (⊸r)
$\vdash ((N \multimap S_1) \multimap \Diamond U_M), \Gamma_6$ (brac−r)
$\vdash ((N \multimap S_1) \multimap \Diamond U_M) \otimes (((((H_1 \otimes H_2) \otimes H_3) \otimes H_4) \otimes H_5) \multimap S_2), \Gamma_{10}$ (⊗r)
$\vdash (((N \multimap S_1) \multimap \Diamond U_M) \otimes (((((H_1 \otimes H_2) \otimes H_3) \otimes H_4) \otimes H_5) \multimap S_2)), \Gamma_{10}$ (brac−r)
$\mathrm{U}_N \vdash \mathrm{U}_N$ (id)
$\Box\mathrm{U}_N \vdash \mathrm{U}_N$ (□l)
$\Box\mathrm{U}_N, \mathrm{U}_N{}^\perp \vdash$ $(()_1^\perp)$
$\Box\mathrm{U}_N, \Diamond U_N{}^\perp \vdash$ (◇l)
$\Box\mathrm{U}_N, \Diamond(U_N{}^\perp) \vdash$ (brac−l)
$(((N \multimap S_1) \multimap \Diamond U_M) \otimes (((((H_1 \otimes H_2) \otimes H_3) \otimes H_4) \otimes H_5) \multimap S_2)) \multimap \Box U_N \vdash \Gamma$ (⊸l)

Figure 2. Proof tree in Linear Logic.

$$
\begin{aligned}
&\Gamma = \{N^\perp, S_1^\perp, \Diamond(U_M^\perp), H_1^\perp, H_2^\perp, H_3^\perp, H_4^\perp, H_5^\perp, S_2^\perp, \Box(U_N^\perp)\}\\
&\Gamma_1 = \{N^\perp\}\\
&\Gamma_2 = \{S_1^\perp\}\\
&\Gamma_3 = \{U_M^\perp\}\\
&\Gamma_4 = \{N^\perp, S_1^\perp\}\\
&\Gamma_5 = \{\Diamond(U_M^\perp)\}\\
&\Gamma_6 = \{N^\perp, S_1^\perp, \Diamond(U_M^\perp\}\\
&\Gamma_7 = \{H_1^\perp, H_2^\perp, H_3^\perp, H_4^\perp, H_5^\perp\}\\
&\Gamma_8 = \{S_2^\perp\}\\
&\Gamma_9 = \{H_1^\perp, H_2^\perp, H_3^\perp, H_4^\perp, H_5^\perp, S_2^\perp\}\\
&\Gamma_{10} = \{N^\perp, S_1^\perp, \Diamond(U_M^\perp), H_1^\perp, H_2^\perp, H_3^\perp, H_4^\perp, H_5^\perp, S_2^\perp\}
\end{aligned}
$$

Figure 3. Contexts for the proof tree (2)

them, we can obtain dual view between the two participants: in our case, the attacker and the environment.

Table 1. De Morgan's rules

$1^\perp$	$\equiv_{dm1}$	$\perp$
$\perp^\perp$	$\equiv_{dm2}$	1
$(\varphi^\perp)^\perp$	$\equiv_{dm3}$	φ
$(\varphi \otimes \psi)^\perp$	$\equiv_{dm4}$	$\varphi^\perp \parr \psi^\perp$
$(\varphi \parr \psi)^\perp$	$\equiv_{dm5}$	$\varphi^\perp \otimes \psi^\perp$
$(\varphi \otimes \psi)$	$\equiv_{dm6}$	$(\varphi^\perp \parr \psi^\perp)^\perp$
$\varphi \multimap \psi$	$\equiv_{dm7}$	$\varphi^\perp \parr \psi$
$\varphi \parr \psi$	$\equiv_{dm8}$	$(\varphi^\perp \otimes \psi^\perp)^\perp$
$(\Diamond\ \varphi)^\perp$	$\equiv_{dm9}$	$\Diamond\ (\varphi)^\perp$
$(\Box\ \varphi)^\perp$	$\equiv_{dm10}$	$\Box\ (\varphi)^\perp$

To achieve this, we must use the following De Morgan rules (see Table 1 above) to the original formula (3).

$$(((\underline{N \multimap S_1}) \multimap \Diamond U_M) \otimes (((((H_1 \otimes H_2) \otimes H_3) \otimes H_4) \otimes H_5) \multimap S_2)) \multimap \Box U_N \equiv_{dm7}$$

$$\equiv_{dm7} ((\underline{(\mathrm{N}^{\perp} \parr S_1) \multimap \Diamond U_M}) \otimes (((((H_1 \otimes H_2) \otimes H_3) \otimes H_4) \otimes H_5) \multimap S_2)) \multimap \Box U_N \equiv_{dm7}$$

$$\equiv_{dm7} (((\mathrm{N}^{\perp} \parr S_1)^{\perp} \parr \Diamond U_M) \otimes (\underline{(((((H_1 \otimes H_2) \otimes H_3) \otimes H_4) \otimes H_5) \multimap S_2)}) \multimap \Box U_N \equiv_{dm7}$$

$$\equiv_{dm7} (\underline{((\mathrm{N}^{\perp} \parr S_1)^{\perp} \parr \Diamond U_M) \otimes (((((H_1 \otimes H_2) \otimes H_3) \otimes H_4) \otimes H_5)^{\perp} \parr S_2)) \multimap \Box U_N} \equiv_{dm7}$$

$$\equiv_{dm7} ((\underline{(\mathrm{N}^{\perp} \parr S_1)}^{\perp} \parr \Diamond U_M) \otimes (((((H_1 \otimes H_2) \otimes H_3) \otimes H_4) \otimes H_5)^{\perp} \parr S_2))^{\perp} \parr \Box U_N \equiv_{dm5}$$

$$\equiv_{dm5} (((((\mathrm{N}\underline{^{\perp})^{\perp}} \otimes S_1^{\perp})^{\perp})^{\perp} \parr \Diamond U_M) \otimes (((((H_1 \otimes H_2) \otimes H_3) \otimes H_4) \otimes H_5)^{\perp} \parr S_2))^{\perp} \parr \Box U_N \equiv_{dm3}$$

$$\equiv_{dm5} ((((\mathrm{N} \otimes S_1^{\perp})\underline{^{\perp})^{\perp}} \parr \Diamond U_M) \otimes (((((H_1 \otimes H_2) \otimes H_3) \otimes H_4) \otimes H_5)^{\perp} \parr S_2))^{\perp} \parr \Box U_N \equiv_{dm3}$$

$$\equiv_{dm3} ((\underline{(\mathrm{N} \otimes S_1^{\perp}) \parr \Diamond U_M}) \otimes (((((H_1 \otimes H_2) \otimes H_3) \otimes H_4) \otimes H_5)^{\perp} \parr S_2))^{\perp} \parr \Box U_N \equiv_{dm8}$$

$$\equiv_{dm8} (((\mathrm{N} \otimes S_1^{\perp})^{\perp} \otimes (\Diamond U_M)^{\perp})^{\perp} \otimes ((((\underline{(H_1 \otimes H_2)} \otimes H_3) \otimes H_4) \otimes H_5)^{\perp} \parr S_2))^{\perp} \parr \Box U_N \equiv_{dm6}$$

$$\equiv_{dm6} (((\mathrm{N} \otimes S_1^{\perp})^{\perp} \otimes (\Diamond U_M)^{\perp})^{\perp} \otimes ((((\underline{(H_1^{\perp} \parr H_2^{\perp})^{\perp} \otimes H_3}) \otimes H_4) \otimes H_5)^{\perp} \parr S_2))^{\perp} \parr \Box U_N \equiv_{dm6}$$

$$\equiv_{dm6} (((\mathrm{N} \otimes S_1^{\perp})^{\perp} \otimes (\Diamond U_M)^{\perp})^{\perp} \otimes ((((((H_1^{\perp} \parr H_2^{\perp})\underline{^{\perp})^{\perp}} \parr H_3^{\perp})^{\perp} \otimes H_4) \otimes H_5)^{\perp} \parr S_2))^{\perp} \parr \Box U_N \equiv_{dm3}$$

$$\equiv_{dm3} (((\mathrm{N} \otimes S_1^{\perp})^{\perp} \otimes (\Diamond U_M)^{\perp})^{\perp} \otimes (((\underline{((H_1^{\perp} \parr H_2^{\perp}) \parr H_3^{\perp})^{\perp} \otimes H_4}) \otimes H_5)^{\perp} \parr S_2))^{\perp} \parr \Box U_N \equiv_{dm6}$$

$$\equiv_{dm6} (((\mathrm{N} \otimes S_1^{\perp})^{\perp} \otimes (\Diamond U_M)^{\perp})^{\perp} \otimes (((((((H_1^{\perp} \parr H_2^{\perp}) \parr H_3^{\perp})\underline{^{\perp})^{\perp}} \parr H_4^{\perp})^{\perp} \otimes H_5)^{\perp} \parr S_2))^{\perp} \parr \Box U_N \equiv_{dm3}$$

$$\equiv_{dm3} (((\mathrm{N} \otimes S_1^{\perp})^{\perp} \otimes (\Diamond U_M)^{\perp})^{\perp} \otimes ((\underline{((((H_1^{\perp} \parr H_2^{\perp}) \parr H_3^{\perp}) \parr H_4^{\perp})^{\perp} \otimes H_5})^{\perp} \parr S_2))^{\perp} \parr \Box U_N \equiv_{dm6}$$

$$\equiv_{dm6} (((\mathrm{N} \otimes S_1^{\perp})^{\perp} \otimes (\Diamond U_M)^{\perp})^{\perp} \otimes (((((((H_1^{\perp} \parr H_2^{\perp}) \parr H_3^{\perp}) \parr H_4^{\perp})\underline{^{\perp})^{\perp}} \parr H_5^{\perp})^{\perp})^{\perp} \parr S_2))^{\perp} \parr \Box U_N \equiv_{dm3}$$

$$\equiv_{dm3} (((\mathrm{N} \otimes S_1^{\perp})^{\perp} \otimes (\Diamond U_M)^{\perp})^{\perp} \otimes ((((((H_1^{\perp} \parr H_2^{\perp}) \parr H_3^{\perp}) \parr H_4^{\perp}) \parr H_5^{\perp})\underline{^{\perp})^{\perp}} \parr S_2))^{\perp} \parr \Box U_N \equiv_{dm3}$$

$$\equiv_{dm3} (\underline{((\mathrm{N} \otimes S_1^{\perp})^{\perp} \otimes (\Diamond U_M)^{\perp})^{\perp} \otimes (((((H_1^{\perp} \parr H_2^{\perp}) \parr H_3^{\perp}) \parr H_4^{\perp}) \parr H_5^{\perp}) \parr S_2)})^{\perp} \parr \Box U_N \equiv_{dm4}$$

$$\equiv_{dm4} ((((\mathrm{N} \otimes S_1^{\perp})^{\perp} \otimes (\Diamond U_M)^{\perp})\underline{^{\perp})^{\perp}} \parr (((((H_1^{\perp} \parr H_2^{\perp}) \parr H_3^{\perp}) \parr H_4^{\perp}) \parr H_5^{\perp}) \parr S_2)^{\perp}) \parr \Box U_N \equiv_{dm3}$$

$$\equiv_{dm3} (\underline{((\mathrm{N} \otimes S_1^{\perp})^{\perp} \otimes (\Diamond U_M)^{\perp}) \parr (((((H_1^{\perp} \parr H_2^{\perp}) \parr H_3^{\perp}) \parr H_4^{\perp}) \parr H_5^{\perp}) \parr S_2)^{\perp}) \parr \Box U_N} \equiv_{dm8}$$

$$\equiv_{dm8} ((((\mathrm{N} \otimes S_1^{\perp})^{\perp} \otimes \underline{(\Diamond U_M)^{\perp}}) \parr (((((H_1^{\perp} \parr H_2^{\perp}) \parr H_3^{\perp}) \parr H_4^{\perp}) \parr H_5^{\perp}) \parr S_2)^{\perp})^{\perp} \otimes (\Box U_N)^{\perp})^{\perp} \equiv_{dm9}$$

$$\equiv_{dm9} ((((\mathrm{N} \otimes S_1^{\perp})^{\perp} \otimes \Box (U_M)^{\perp}) \parr (((((H_1^{\perp} \parr H_2^{\perp}) \parr H_3^{\perp}) \parr H_4^{\perp}) \parr H_5^{\perp}) \parr S_2)^{\perp})^{\perp} \otimes \underline{(\Box U_N)^{\perp}})^{\perp} \equiv_{dm10}$$

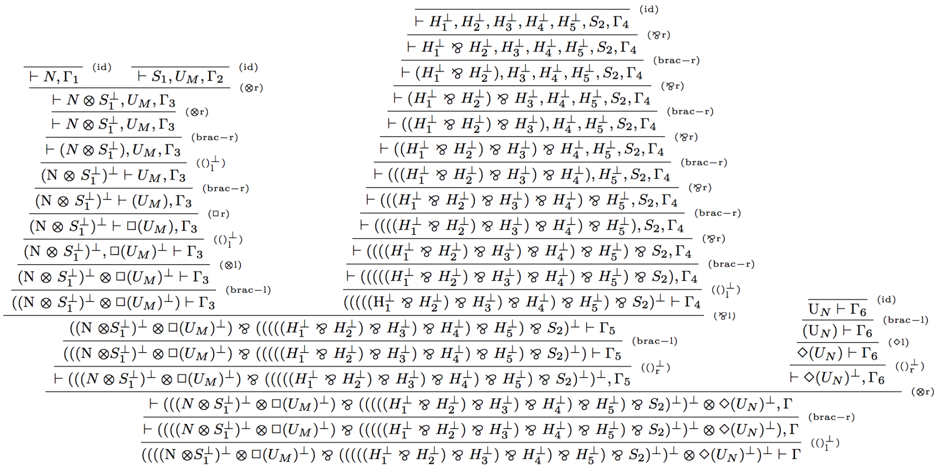
$$\equiv_{dm10} ((((\mathrm{N} \otimes S_1^{\perp})^{\perp} \otimes \Box (U_M)^{\perp}) \parr (((((H_1^{\perp} \parr H_2^{\perp}) \parr H_3^{\perp}) \parr H_4^{\perp}) \parr H_5^{\perp}) \parr S_2)^{\perp})^{\perp} \otimes \Diamond (U_N)^{\perp})^{\perp}$$

FIGURE 4. De Morganized formula.

In the Figure (4), we have translated the formula (3) in Modal linear logic *(from the attacker point of view)* to the De Morganized one *(from the network environment point of view)*. In every step of the formula translation, we underline the appropriate part, where a particular De Morgan's law was applied. Later, we construct a polarized proof tree (see Figure 5), where the root of tree is De Morganized formula and every derivation step is realized by using an appropriate rule applied to obtain a new proof instance.

3.3. **Logical space and logical time.** To successfully express the logical space and time, it is necessary to identify changes in the polarity within the proof tree. Logical connectives are divided into the two groups depending on their polarity. The positive connectives are $\otimes$, 1, $\Box$ and the connectives $\parr$, $\bot$, $\Diamond$, are the negative ones.

The polarity of formula depends on its outermost connective [11]. Change of polarity within the proof tree instance of a linear formula characterizes an incrementation of time. The steps of a proof with the same polarity can be enclosed into a cluster [11]. The actions in a cluster can be performed simultaneously. Application of the negation rule is causing a leaping of an appropriate formula or its subformula between left and right side of the turnstile. It occurs when a new cluster of the same polarity passes. To achieve this, a polarized proof tree must be created with the root of De Morganized formula as shown in the Figure (4). At the end all the leaves of the proof tree have to be identities.



$\vdash N, \Gamma_1$ (id)
$\vdash S_1, U_M, \Gamma_2$ (id)
(⊗r)
$\vdash N \otimes S_1^\perp, U_M, \Gamma_3$
(⊗r)
$\vdash N \otimes S_1^\perp, U_M, \Gamma_3$
(brac−r)
$\vdash (N \otimes S_1^\perp), U_M, \Gamma_3$
$(()_1^\perp)$
$(\mathrm{N} \otimes S_1^\perp)^\perp \vdash U_M, \Gamma_3$
(brac−r)
$(\mathrm{N} \otimes S_1^\perp)^\perp \vdash (U_M), \Gamma_3$
(□r)
$(\mathrm{N} \otimes S_1^\perp)^\perp \vdash \Box(U_M), \Gamma_3$
$(()_1^\perp)$
$(\mathrm{N} \otimes S_1^\perp)^\perp, \Box(U_M)^\perp \vdash \Gamma_3$
(⊗l)
$(\mathrm{N} \otimes S_1^\perp)^\perp \otimes \Box(U_M)^\perp \vdash \Gamma_3$
(brac−l)
$((\mathrm{N} \otimes S_1^\perp)^\perp \otimes \Box(U_M)^\perp) \vdash \Gamma_3$
(id)
$\vdash H_1^\perp, H_2^\perp, H_3^\perp, H_4^\perp, H_5^\perp, S_2, \Gamma_4$
(⅋r)
$\vdash H_1^\perp \parr H_2^\perp, H_3^\perp, H_4^\perp, H_5^\perp, S_2, \Gamma_4$
(brac−r)
$\vdash (H_1^\perp \parr H_2^\perp), H_3^\perp, H_4^\perp, H_5^\perp, S_2, \Gamma_4$
(⅋r)
$\vdash (H_1^\perp \parr H_2^\perp) \parr H_3^\perp, H_4^\perp, H_5^\perp, S_2, \Gamma_4$
(brac−r)
$\vdash ((H_1^\perp \parr H_2^\perp) \parr H_3^\perp), H_4^\perp, H_5^\perp, S_2, \Gamma_4$
(⅋r)
$\vdash ((H_1^\perp \parr H_2^\perp) \parr H_3^\perp) \parr H_4^\perp, H_5^\perp, S_2, \Gamma_4$
(brac−r)
$\vdash (((H_1^\perp \parr H_2^\perp) \parr H_3^\perp) \parr H_4^\perp), H_5^\perp, S_2, \Gamma_4$
(⅋r)
$\vdash (((H_1^\perp \parr H_2^\perp) \parr H_3^\perp) \parr H_4^\perp) \parr H_5^\perp, S_2, \Gamma_4$
(brac−r)
$\vdash ((((H_1^\perp \parr H_2^\perp) \parr H_3^\perp) \parr H_4^\perp) \parr H_5^\perp), S_2, \Gamma_4$
(⅋r)
$\vdash ((((H_1^\perp \parr H_2^\perp) \parr H_3^\perp) \parr H_4^\perp) \parr H_5^\perp) \parr S_2, \Gamma_4$
(brac−r)
$\vdash (((((H_1^\perp \parr H_2^\perp) \parr H_3^\perp) \parr H_4^\perp) \parr H_5^\perp) \parr S_2), \Gamma_4$
$(()_1^\perp)$
$(((((\mathrm{H}_1^\perp \parr H_2^\perp) \parr H_3^\perp) \parr H_4^\perp) \parr H_5^\perp) \parr S_2)^\perp \vdash \Gamma_4$
(⅋l)
$((\mathrm{N} \otimes S_1^\perp)^\perp \otimes \Box(U_M)^\perp) \parr (((((H_1^\perp \parr H_2^\perp) \parr H_3^\perp) \parr H_4^\perp) \parr H_5^\perp) \parr S_2)^\perp \vdash \Gamma_5$
(brac−l)
$(((\mathrm{N} \otimes S_1^\perp)^\perp \otimes \Box(U_M)^\perp) \parr (((((H_1^\perp \parr H_2^\perp) \parr H_3^\perp) \parr H_4^\perp) \parr H_5^\perp) \parr S_2)^\perp) \vdash \Gamma_5$
$(()_r^\perp)$
$\vdash (((N \otimes S_1^\perp)^\perp \otimes \Box(U_M)^\perp) \parr (((((H_1^\perp \parr H_2^\perp) \parr H_3^\perp) \parr H_4^\perp) \parr H_5^\perp) \parr S_2)^\perp)^\perp, \Gamma_5$
(id)
$\mathrm{U}_N \vdash \Gamma_6$
(brac−l)
$(\mathrm{U}_N) \vdash \Gamma_6$
(◇l)
$\Diamond(U_N) \vdash \Gamma_6$
$(()_r^\perp)$
$\vdash \Diamond(U_N)^\perp, \Gamma_6$
(⊗r)
$\vdash (((N \otimes S_1^\perp)^\perp \otimes \Box(U_M)^\perp) \parr (((((H_1^\perp \parr H_2^\perp) \parr H_3^\perp) \parr H_4^\perp) \parr H_5^\perp) \parr S_2)^\perp)^\perp \otimes \Diamond(U_N)^\perp, \Gamma$
(brac−r)
$\vdash ((((N \otimes S_1^\perp)^\perp \otimes \Box(U_M)^\perp) \parr (((((H_1^\perp \parr H_2^\perp) \parr H_3^\perp) \parr H_4^\perp) \parr H_5^\perp) \parr S_2)^\perp)^\perp \otimes \Diamond(U_N)^\perp), \Gamma$
$(()_1^\perp)$
$((((\mathrm{N} \otimes S_1^\perp)^\perp \otimes \Box(U_M)^\perp) \parr (((((H_1^\perp \parr H_2^\perp) \parr H_3^\perp) \parr H_4^\perp) \parr H_5^\perp) \parr S_2)^\perp)^\perp \otimes \Diamond(U_N)^\perp)^\perp \vdash \Gamma$

Figure 5. Polarized proof tree.

where the contexts are defined as follows:

$$\begin{aligned}
&\Gamma = \{N^\perp, S_1, U_M^\perp, H_1, H_2, H_3, H_4, H_5, S_2^\perp, U_N^\perp\}\\
&\Gamma_1 = \{N^\perp\}\\
&\Gamma_2 = \{S_1^\perp, U_M^\perp\}\\
&\Gamma_3 = \{N^\perp, S_1, U_M^\perp\}\\
&\Gamma_4 = \{H_1, H_2, H_3, H_4, H_5, S_2^\perp\}\\
&\Gamma_5 = \{N^\perp, S_1, U_M^\perp, H_1, H_2, H_3, H_4, H_5, S_2^\perp\}\\
&\Gamma_6 = \{U_N^\perp\}
\end{aligned}$$

Figure 6. Contexts for the polarized proof tree.

In the polarized proof tree Figure (5), we observe the change of polarity. We identify the clusters of polarities determined by the linear negation rule. Where it is applied, a proof step expresses a time incrementation. The actions enclosed in clusters can be performed simultaneously. The time incrementation reflects the fact, that the use of the negation rule causes tilting of the corresponding formula between the right and left sides of the turnstile. The following proof tree Figure (7) is constructed from its clusters. Proof trees with clusters are not only simpler but also indicate the time incrementation. The cluster proof tree (depicted in the Figure (7)), is derived from the polarized proof tree (depicted in the Figure (5)) in such a way, that it contains only those tree forms where the rule of linear negation was used.

$$\dfrac{\dfrac{\dfrac{\dfrac{}{\vdash E,\,\Lambda_3}\,{\scriptstyle(\maltese)}\qquad \dfrac{}{\vdash F,\,\Lambda_4}\,{\scriptstyle(\maltese)}}{\mathrm{C}\vdash\Lambda_1}\,{\scriptstyle(-,\mathrm{C}\vdash,\{\{\mathrm{E}\},\{\mathrm{F}\}\})}\qquad \dfrac{}{\mathrm{D}\vdash\Lambda_2}\,{\scriptstyle(\maltese)}}{\vdash B,\,\Lambda}\,{\scriptstyle(+,\vdash\mathrm{B},\{\{\mathrm{C}\},\{\mathrm{D}\}\})}}{\mathrm{A}\vdash\Lambda}\,{\scriptstyle(-,\mathrm{A}\vdash,\{\mathrm{B}\})}$$

Figure 7. Cluster proof tree.

Appropriate contexts are depicted in the Figure (8).

$$A = ((((\mathrm{N}\otimes S_1^{\perp})^{\perp}\otimes\Box(U_M)^{\perp})\parr(((((H_1^{\perp}\parr H_2^{\perp})\parr H_3^{\perp})\parr H_4^{\perp})\parr H_5^{\perp})\parr S_2)^{\perp})^{\perp}\otimes\Diamond(U_N)^{\perp})^{\perp}$$
$$\mathrm{B} = ((((N\otimes S_1^{\perp})^{\perp}\otimes\Box(U_M)^{\perp})\parr(((((H_1^{\perp}\parr H_2^{\perp})\parr H_3^{\perp})\parr H_4^{\perp})\parr H_5^{\perp})\parr S_2)^{\perp})^{\perp}\otimes\Diamond(U_N)^{\perp})$$
$$\mathrm{C} = (((N\otimes S_1^{\perp})^{\perp}\otimes\Box(U_M)^{\perp})\parr(((((H_1^{\perp}\parr H_2^{\perp})\parr H_3^{\perp})\parr H_4^{\perp})\parr H_5^{\perp})\parr S_2)^{\perp})$$
$$\mathrm{D} = \Diamond(U_N)$$
$$\mathrm{E} = (N\otimes S_1^{\perp}),\ U_M$$
$$\mathrm{F} = (((((H_1^{\perp}\parr H_2^{\perp})\parr H_3^{\perp})\parr H_4^{\perp})\parr H_5^{\perp})\parr S_2)$$

Figure 8. Cluster proof tree contexts.

In the linear logic, we consider a space in terms of locations. Every formula has a location, i.e. its address [11]. Based on that, we remove the content of subformulæ, and we replace it by its locations. Proof trees containing only locations are called designs, where any logical information about the original subformula is substituted by appropriate locative addresses, i.e. loci in the design (Figure 9).

The following rules are used in the process of constructing a proof tree in the time-spatial Ludics theory.

- *Positive rule* is used when the outermost formula has positive polarity,

$$\frac{\ldots, \xi * i, \ldots \ \vdash \Lambda_i, \ldots}{\vdash \Lambda, \xi}(+,\xi,I), \tag{4}$$

  where the ξ is the address of a formula, and for every $i \in I$, and the Λ_i is set of addresses of every immediate subformulas.
- *Negative rule* is used when the outermost formula has negative polarity:

$$\frac{\ldots \ \vdash \Lambda_I, \xi * I, \ldots}{\xi \vdash \Lambda}(-,\xi,N), \tag{5}$$

  where the N is set of ramifications, where for the every $I \in N$ holds, that $\xi * I$.
- The *daemon* rule is used otherwise, mostly in the leaves:

$$\frac{}{\vdash \Lambda, \xi}(\maltese). \tag{6}$$

A location of proved formula in the design is denoted by ξ, where ξ is the location address. If the formula has its immediate subformula ξ_1, their locations are called biases (the bias Λ_1 or the concentrated biases Λ_{11}, Λ_{12} etc.). The structure of space occupied by a formula is uniquely identified by a finite sequence of biases [11].

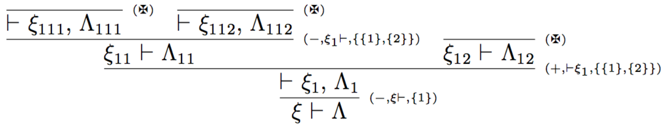

$\vdash \xi_{111}, \Lambda_{111}$
$(\maltese)$
$\vdash \xi_{112}, \Lambda_{112}$
$(\maltese)$
$(-,\xi_1\vdash,\{\{1\},\{2\}\})$
$\xi_{11} \vdash \Lambda_{11}$
$(\maltese)$
$\xi_{12} \vdash \Lambda_{12}$
$(+,\vdash\xi_1,\{\{1\},\{2\}\})$
$\vdash \xi_1, \Lambda_1$
$(-,\xi\vdash,\{1\})$
$\xi \vdash \Lambda$

Figure 9. Design.

Appropriate contexts are depicted below.

$$\begin{aligned}
\Delta &= \xi \\
\Delta_1 &= \xi_1 \\
\Delta_{11} &= \xi_{11} \\
\Delta_{12} &= \xi_{12} \\
\Delta_{111} &= \xi_{111} \\
\Delta_{112} &= \xi_{112}
\end{aligned}$$

Finally, we obtain the design on the network attack as shown in Figure (9) for expressing the locative structure of the network intrusion. Designs are the significant objects of the Ludics theory. The design in the Figure (9) consists of the three time lines of comparable loci with respect to ordering relation $\sqsubseteq$.

(1) $\xi \sqsubseteq \xi_1 \sqsubseteq \xi_{11} \sqsubseteq \xi_{111}$, represents the linear time line of the possibility of the vertical portscan intrusion,
(2) $\xi \sqsubseteq \xi_1 \sqsubseteq \xi_{11} \sqsubseteq \xi_{112}$, represents the linear time line of necessity of the SYN Flood network attack,
(3) $\xi \sqsubseteq \xi_1 \sqsubseteq \xi_{12}$, represents the linear time line of neccessity of network intrusion.

A design can have one or more branches and it expresses two relationships [11]: time and space. The addresses in the same branch of design are comparable addresses and they have time relationship. The addresses in different branches are incomparable, i.e. they have space relationship in order to relation $\sqsubseteq$.

We can also interpret this design as the polarized game, where the linear negation is conductive to move alternation between the proponent (attacker) and the opponent (network environment). From the computer science point of view, we were able to express logical space that represents the computer memory and also logical time, which represents the calculation of computer processor.

4. Conclusion

In this contribution, we show how the resource-oriented logical system can be used to describe real processes in network environment, such as network intrusion. We have expressed IDS's behavior during network intrusion by a formula of Modal Linear Logic. Our method is helpful that proof of such a formula ensures the correctness of component software system design.

The main goal of this paper is to apply the time-spatial calculus from Girard's Ludics theory. Finally, we were able to express logical space that represents the computer memory and also logical time, which represents the calculation time of operation.

In the future, we would like to extend our approach by joining the host-based intrusion detection systems with the network-based one i.e. create a complex security of program systems. Such a combination of the both types of IDSs will secure computer systems even more. The next step in our work, will be extending IDS by applying the resource oriented Belief-Desire-Intention logical system. We plan to create a BDI architecture, that will perform automated IDSs reactions, instead of a system administrator intervention as it is now.

Acknowledgment

This paper was supported by KEGA project ViLMA: Virtual Laboratory for Malware Analysis (079TUKE-04/2017).

This work is a result of international cooperation under the CEEPUS network No.CIII-HU-0019-12-1617.

References

[1] J.-Y. Girard. *Linear Logic*, Theoretical Computer Science 50, Elsevier Science Publishers Ltd. Essex, UK, 1987

[2] J.-Y. Girard. *Linear Logic: its syntax and semantics*, Laboratoire de Mathematiques Descretes, UPR 9016 - CRNS, 1995

[3] J.-Y. Girard. *Locus Solum: From the rules of logic to the logic of rules*, Mathematical Structures in Computer Science, Vol. 11, N. 3, 2001

[4] P. Innella, O. McMillan, T. Digital Integrity, LLC. *An Introduction to IDS*, Symantec Connect, 2001

[5] J. Perháč, D. Mihályi. *Intrusion Detection System Behavior as Resource-Oriented Formula*, Acta Electrotechnica et Informatica, Vol. 15, No. 3, 2015

[6] SANS Institute. *Intrusion Detection Systems: Definition, Need and Challenges", SANS Institute Reading Room*, 2011

[7] J. Perháč, D. Mihályi, V. Novitzká, *Between Syntax and Semantics of Resource Oriented Logic for IDS Behavior Description*, The Publishing Office of Czestochowa University of Technology, Journal of Applied Mathematics and Computational Mechanics, Vol. 15, No. 2, ISSN:2353-0588, 2016

[8] J. Perháč, D. Mihályi, *Coalgebraic modeling of IDS behavior*, 2015 IEEE 13th International Scientific Conference on Informatics, November 18-20, 2015, Poprad, Slovakia, 2015

[9] J. Perháč, D. Mihályi, *Coalgebraic specification of network intrusion signatures*, Studia Universitatis Babes-Bolyai, Informatica, Vol. 61, N. 2 pp. 83-94, 2016

[10] J. Perháč, D. Mihályi, *Intrusion Detection System Behavior as Resource-Oriented Formula*, Acta Electrotechnica et Informatica. Vol. 15, N. 3, 2015, pp. 9-13. ISSN 1335-8243

[11] W. Steingartner, A. Poláková, P. Prazňák, V. Novitzká, *Linear Logic in Computer Science*, Journal of Applied Mathematics and Computational Mechanics, Vol. 14(1), 91-100, 2015

Department of Computers and Informatics, Faculty of Electrical Engineering and Informatics, Technical University of Košice, Letná 9, 042 00 Košice, Slovak Republic,

E-mail address: Daniel.Mihalyi@tuke.sk

E-mail address: Jan.Perhac@tuke.sk

E-mail address: Patrik.Balint@globallogic.com