Stepwise Composition of Protocol TCP Petri Net Model

Dmitry A. Zaitsev
Odessa National Telecommunication Academy
Kuznechnaya, 1, Odessa, 65029, Ukraine
http://www.geocities.com/zsoftua

Abstract

Proof of the invariance of Petri net model for connection and disconnection phases of TCP protocol was implemented. Decomposition of Petri net model into functional subnets was realized. Calculation of invariants was implemented in the process of stepwise composition, which allows the essential speed-up of computations.

1. Introduction

TCP is the major transport protocol of Internet. Namely via protocol TCP more than two hundreds petabits of public and private information is transferred per day. Therefore, a formal proof of TCP protocol correctness has a key significance for the grounding of modern global networks reliability [6].

Verification of protocols is a traditional field of Petri nets application [5]. At that for a formal proof of protocol correctness, either invariants of Petri net or state space analysis are used. Notice that, state space techniques as well as invariant calculation require an exponential space and time [5,9].

The goal of present work is the proof of Petri net model invariance for connection and disconnection phases of protocol TCP. Specification of protocol besides two phases mentioned defines also the basic phase of information exchange. Investigation of this phase requires extended Petri nets [6] and remains beyond the scope of present paper.

Decomposition is a fundamental way to handle large-scale systems [2]. Known approaches to decomposition of Petri nets [3,4,7,8,12] differ in the classes of subnets in which a given Petri net is decomposed. The most general class was considered in [3]. We study the decomposition into functional subnets [13]. Essential constraints on structure of such subnets provide a considerable speed-up in calculation of invariants [14].

In [13] a polynomial algorithm of decomposition of a given Petri net into minimal functional subnets was represented. In [14] invariants of functional subnets were used for composition of invariants of entire net. It was shown that speed-up of computations obtained is exponential with respect to number of nodes of net. This technique was applied successfully for verification of protocols [15]. In present work, the technique of invariants calculation in the process of stepwise composition of a given Petri net out of its minimal functional subnets is represented.

2. Specifications of protocol TCP

Standard specification of protocol TCP has been represented in year 1981 in RFC 793 [10]. This document had become the result of prolonged discussions reflected, for instance, in RFC with numbers 44, 55, 761. In the process of exploitation, it was made alterations concerned with such items as slow start RFC 1122, quick recovery RFC 2001, repetitive transmission RFC 2988. The improvement of standard is not ceased at present. It is confirmed, for instance, by RFC 3360, 3481, 3562, which propose technique of reliable interaction at connection reset, special rules for wireless lines connections, algorithms of keys exchange for protection of information.

3. Petri net model of protocol TCP

Petri net model of protocol TCP is represented in Fig. 1. Further the notations and definitions introduced in [13,14] will be used.

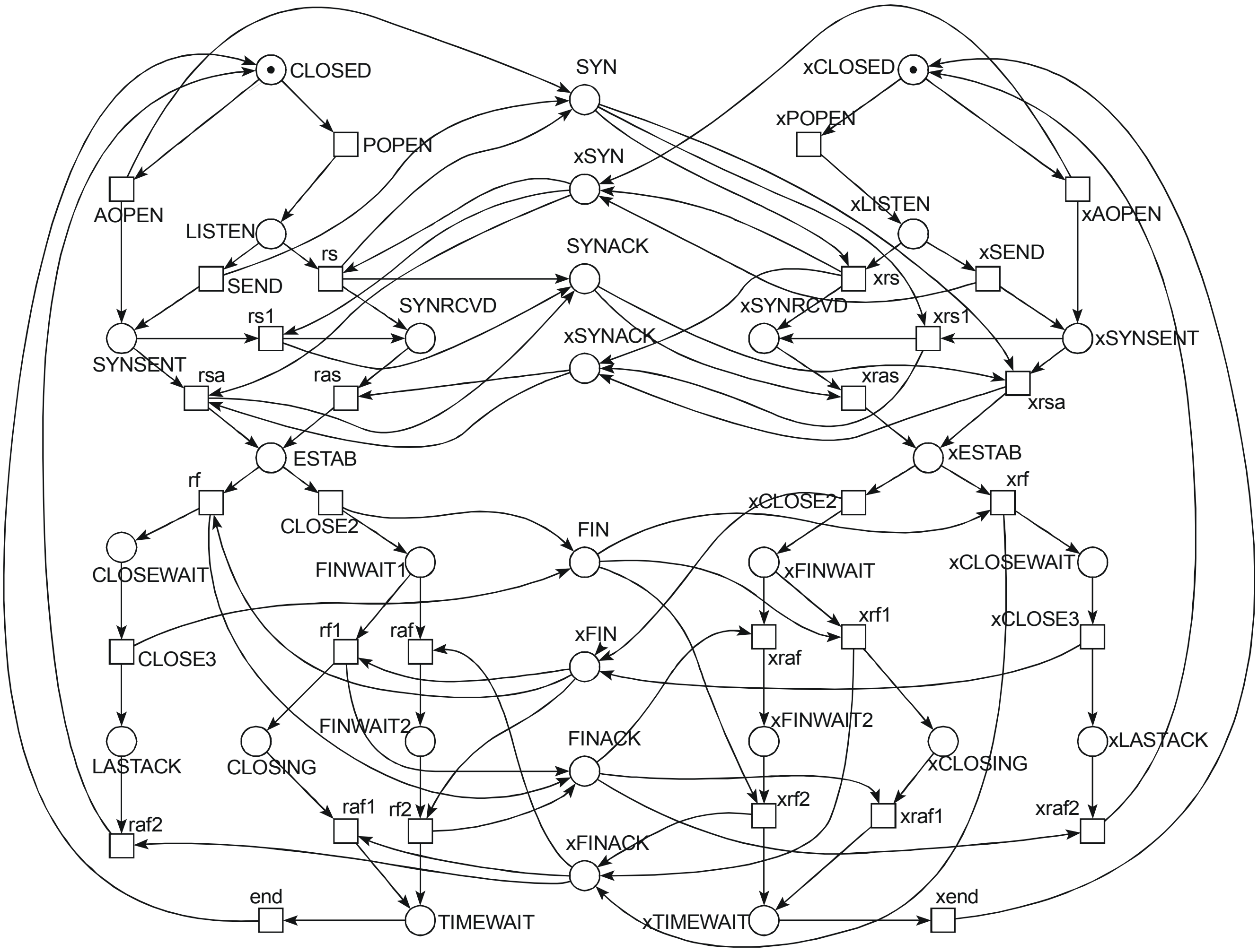


Figure 1. Petri net model of protocol TCP

Model consists of three parts: left interacting system; right interacting system; communication subsystem. Each of interacting systems corresponds exactly to standard state diagram of protocol [10]. Notations of right system contain prefix “x”. States of diagram are represented by places of the same name. At that the additional places corresponding to flags SYN, FIN, ACK of packets’ headers are used. These places constitute the communication subsystem. Flags of packets transmitting by right interacting system have prefix “x”. Notice that, for clearness of model the flag of acknowledgement ACK is represented by separate places corresponding to its receiving either as answer on flag SYN (SYNACK), or as answer on flag FIN (FINACK). Moreover, since model does not contain the descriptions of application level protocols, commands OPEN, CLOSE, SEND are represented merely in notations of corresponding transitions. The names of residuary transitions are chosen as first letters of flags waiting for which are represented in standard state diagram of protocol [10]. Notice that, the source state diagram represented in [10] is defined more exactly accordingly to RFC 896 anticipating congestion avoidance facilities and RFC 1122 studying the slow start problem.

4. Decomposition of model

Let us implement the decomposition of protocol TCP model represented in Fig. 1 into its minimal functional subnets according to algorithm described in [13,14].

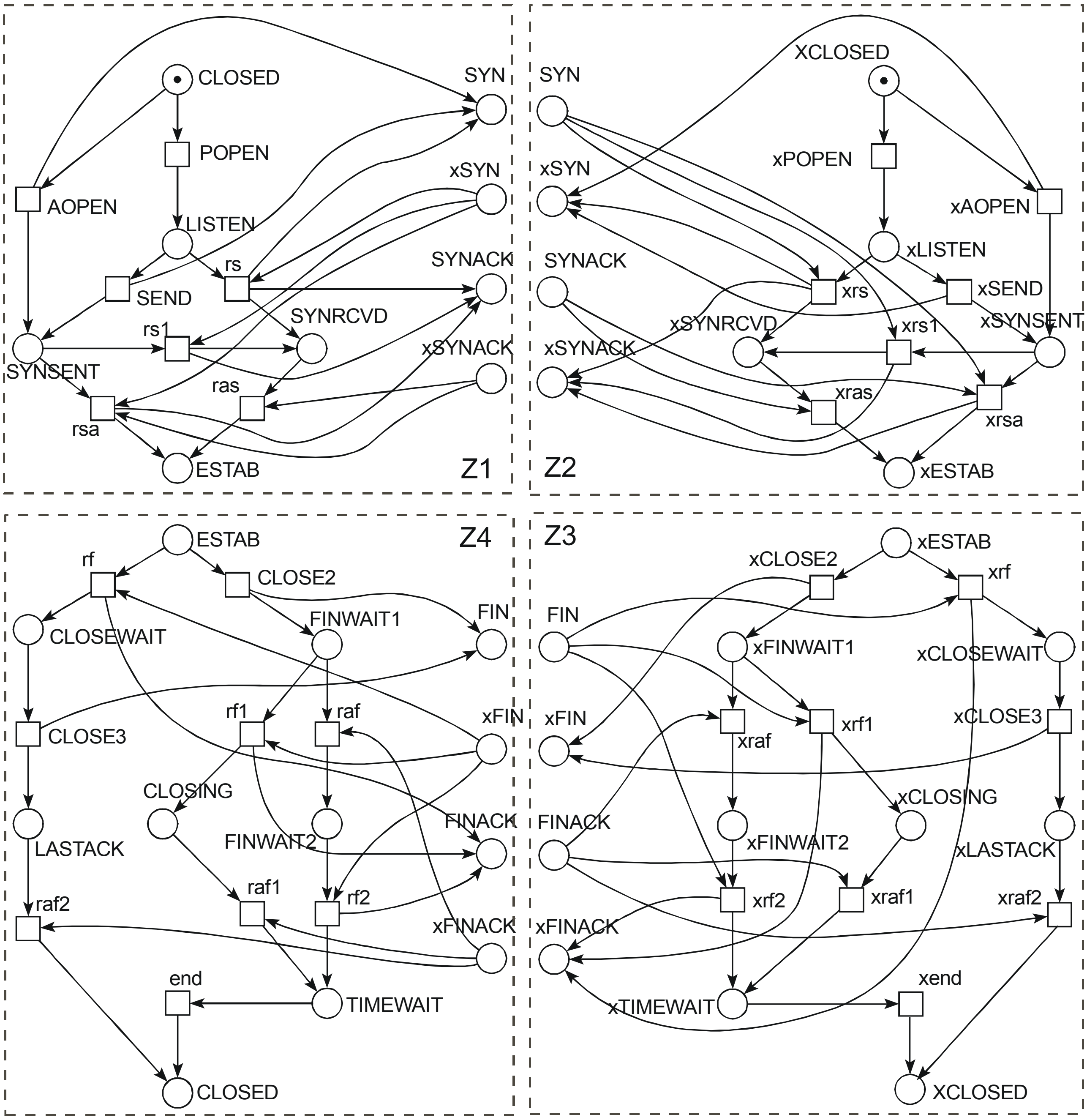
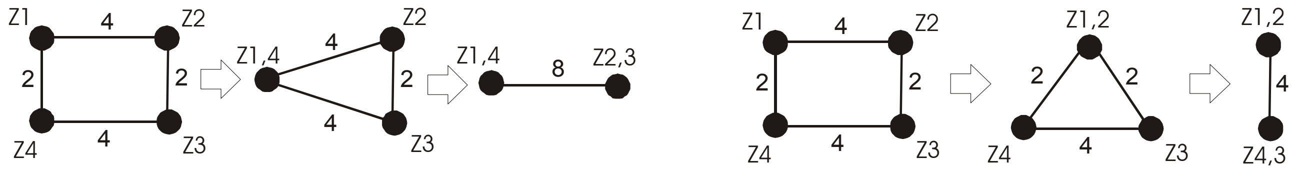


Figure 2. Decomposition of protocol TCP model

Let us $N=(P,T,F)$ be a given *Petri net*, where $P=\{p_1,p_2,...,p_m\}$ is a finite set of places, $T=\{t_1,t_2,...,t_n\}$ is a finite set of transitions and $P\bigcap T=\varnothing$, a flow relation $F\subseteq P\times T\bigcup T\times P$ defines a set of arcs connecting places and transitions. *Functional subnet* $Z\succ N$ is a triple $Z=(N',X,Y)$, where N' is a subnet of N and N' is connected with the residuary part $N\setminus N'$ of net only via contact places $C=X\cup Y$, moreover input places $X\subseteq P$ have only input arcs from the outside and output arcs to the inside of subnet and output places $Y\subseteq P$ have only input arcs from the inside and output arcs to the outside of subnet and $X\bigcap Y=\varnothing$. *Minimal functional* subnet does not contain any another functional subnet.

In [13] it was proven that functional subnet is induced by the set of its transitions, the set of minimal functional subnets defines the partition of transition set and provide the basis of functional subnets.

It was shown [13,14] that the net of functional subnets is a marked graph, so decomposition may be represented by directed or undirected graph. *Graph of decomposition* of Petri net N is a triple $G=(V,E,W)$, where vertexes v of set V corresponds to minimal functional subnets: $v \leftrightarrow Z, Z \succ N$; edges $E \subseteq [V]^2$ connect subnets having common contact places: $v_1 v_2 \in E \Leftrightarrow$ $\exists p \in C : ({}^{\bullet}p = Z^1 \wedge p^{\bullet} = Z^2) \vee ({}^{\bullet}p = Z^2 \wedge p^{\bullet} = Z^1)$; weight function $W : E \to \mathrm{N}$ maps edge to the number of contact places, where N is a set of natural numbers.



a) Z1+Z4; Z2+Z3; Z1,4+Z2,3

b) Z1+Z2; Z4+Z3; Z1,2+Z4,3

Figure 3. Stepwise composition of protocol TCP model

Application of decomposition algorithm [13,14] to protocol TCP model (Fig. 1) leads to the obtaining of set $\{Z1, Z2, Z3, Z4\}$, consisting of four minimal functional subnets represented in Fig. 2. Notice that, by virtue of symmetry of systems' interaction processes the pairs of subnets $Z1$ and $Z2$ as well as $Z4$ and $Z3$ are isomorphic. Therefore, it is required to investigate the properties only for two of enumerated four subnets.

Various manners of minimal functional subnets composition allow the decomposition of the source model into left and right interacting systems $Zleft$ and $Zright$, and the decomposition into net establishing the connection Zup and disconnecting net $Zdown$, where $Zleft = Z1 + Z4$, $Zright = Z2 + Z3$, $Zup = Z1 + Z2$, $Zdown = Z4 + Z3$.

5. Stepwise calculation of invariants

Invariants [2,5] are a powerful tool for investigation of structural properties of Petri nets. They allow the determination of boundness, safeness, and necessary conditions of liveness and absence of deadlocks. These properties are significant for real-life systems behavior analysis, especially, for telecommunication protocols [5].

Let's remind, that Petri net invariant is a nonnegative integer solution $\overline{x}$ of system

$$\overline{x} \cdot A = 0, \tag{1}$$

where A is the incidence matrix of Petri net for place invariants (p-invariants) or transposed incidence matrix for transition invariants (t-invariants).

In [5] it was shown that a correct telecommunication protocol has to be invariant one. Known methods of invariants calculation [9] have exponential complexity that makes its application difficult for investigation of real-life objects' models numbering thousands of elements. Model of protocol TCP (Fig. 1) allow the convincing illustration of this fact. However, net contains only 30 places and 28 transitions, the calculation of basis invariants for natural generators by known tool Tina [1] had not been completed in 24 hours.

According to theorem 2 proved in [14] Petri net N is invariant if and only if all its minimal functional subnets are invariant and a common nonzero invariant of contact places exists. Therefore, to calculate invariants of Petri net we should to calculate invariants of its minimal functional subnets and then to find common invariants of contact places. It was shown that results are valid also for an arbitrary subset of functional subnets defining a partition of the set of Petri net's transitions.

Let's the general solution for invariant of functional subnet Z^j is represented in the form

$$\overline{x}^j = \overline{z}^j \cdot G^j, \tag{2}$$

where $\overline{z}^j$ is an arbitrary vector of nonnegative integer numbers and G^j is a matrix of basis solutions. Then the system of equations for calculation of common invariants of contact places has the form

$$\left\{ \overline{z}^i \cdot G_p^i - \overline{z}^j \cdot G_p^j = 0, \quad p \in C, \right. \tag{3}$$

where C is the set of contact places and $i.j$ are the numbers of functional subnets incident with place

$p \in C$ and G_p^j is the column of matrix G^j corresponding to place p.

Thus, variables $\bar{z}^j$ become non-free now. Notice that, system (3) has the same form as the source system (1). Consequently, for its solution we may apply early pointed methods. Let's assume that $\bar{z} = \bar{y} \cdot R$, where R is a matrix of basis solutions of system (3) and $\bar{y}$ contains arbitrary nonnegative integer numbers. Then the general solution of system (1) according to (2) may be represented as

$$\bar{x} = \bar{y} \cdot H \,,\; H = R \cdot G \,. \qquad (4)$$

In the cases the number of contact places exceeds considerably the number of places of the largest subnet it is advisable to implement a stepwise composition. We solve the system (3) for a subset of contact places and then continue the process. In such a way, we provide the solution of a sequence of systems with lesser dimension. Under the exponential complexity of system's solution, we obtain an additional speed-up of computations.

Let us consider the graph of decomposition (Fig. 3). The simplest is a pairwise or edge composition at which the pair of adjacent subnets is composed. It corresponds to operation of contracting [11] of adjacent vertexes. In spite of standard contracting [11], we consider the weights of edges equaling to number of contact places, which define the number of equations in system.

At the composition of adjacent subnets Z^i and Z^j we replace the pair of these vertexes by the single vertex $Z^{i,j}$ and assign $G^{i,j} := H^{i,j}$.

This process was applied at intuitive level [15] and then formalized [16] in terms of graph theory [11]. In [15] the sequence shown in Fig. 3 a) was implemented. Maximal number of equations equals to 8 in spite of 12 for simultaneous composition.

In essence, the present paper provides the case study of stepwise composition for protocol TCP model according to optimal sequence represented in Fig. 3 b). It guarantees the maximal number of equations equaling to 4.

6. Invariance of model

Let us enumerate places according to Table 1 for calculation of invariants. Basis invariants of subnets $Z1$ and $Z4$ are calculated with the aid of tool Tina [1]. Invariants for isomorphic subnet $Z2$ and $Z3$ are constructed out of invariants obtained.

Table 1. Places of net

#	Name	#	Name	#	Name
1	CLOSED	11	TIMEWAIT	21	XLISTEN
2	LISTEN	12	SYN	22	XSYNSENT
3	SYNSENT	13	XSYN	23	XSYNRCVD
4	SYNRCVD	14	SYNACK	24	XESTAB
5	ESTAB	15	xSYNACK	25	XCLOSEWAIT
6	CLOSEWAIT	16	FIN	26	xFINWAIT1
7	FINWAIT1	17	XFIN	27	XLASTACK
8	LASTACK	18	FINACK	28	XCLOSING
9	CLOSING	19	xFINACK	29	xFINWAIT2
10	FINWAIT2	20	xCLOSED	30	XTIMEWAIT

We implement the sequence of stepwise composition represented in Fig. 3 b).

6.1. Composition: Z1+Z2

With respect to numeration of places defined by Table 1 the invariants of subnets $Z1$ and $Z2$ may be represented as:

$$(x_1, x_2, x_3, x_4, x_5, x_{12}, x_{13}, x_{14}, x_{15}) = \\ (z_1^1, z_2^1, z_3^1, z_4^1, z_5^1, z_6^1) \cdot G^1,$$

$$(x_{20}, x_{21}, x_{22}, x_{23}, x_{24}, x_{13}, x_{12}, x_{15}, x_{14}) = \\ (z_1^2, z_2^2, z_3^2, z_4^2, z_5^2, z_6^2) \cdot G^2,$$

where the matrixes have the form

$$G^1 = G^2 = \begin{vmatrix} 1&1&1&1&1&0&0&0&0 \\ 1&1&1&0&0&0&0&1&0 \\ 0&0&0&1&1&0&1&0&0 \\ 1&1&0&0&0&1&0&0&0 \\ 0&0&0&0&1&0&0&0&1 \\ 0&0&0&0&0&0&1&1&0 \end{vmatrix},$$

Notice that, components of vectors $\bar{x}^j$ corresponding to subnets $Z1$ and $Z2$ are written in explicit form. They define the indexation of columns of matrixes constructed. Indexes of rows correspond to components of vectors
$\bar{z}^1 = (z_1^1, z_2^1, z_3^1, z_4^1, z_5^1, z_6^1)$, $\bar{z}^2 = (z_1^2, z_2^2, z_3^2, z_4^2, z_5^2, z_6^2)$.

Let's construct the system of equations with the form (2) for contact places:

$$\begin{cases} p_{12}: & z_4^1 - z_3^2 - z_6^2 = 0, \\ p_{13}: & z_4^2 - z_3^1 - z_6^1 = 0, \\ p_{14}: & z_2^1 + z_6^1 - z_5^2 = 0, \\ p_{15}: & z_2^2 + z_6^2 - z_5^1 = 0. \end{cases}$$

Notice that, in composition of subnets $Z1$ and $Z2$ are used such contact places as p_{12}, p_{13}, p_{14}, p_{15}. The general solution of system has the form

$$(z_1^1, z_2^1, z_3^1, z_4^1, z_5^1, z_6^1, z_1^2, z_2^2, z_3^2, z_4^2, z_5^2, z_6^2) = \bar{y} \cdot R^{1,2},$$

$$R^{1,2} = \begin{vmatrix} 0&0&0&0&0&0&1&0&0&0&0&0 \\ 1&0&0&0&0&0&0&0&0&0&0&0 \\ 0&0&0&1&0&0&0&0&1&0&0&0 \\ 0&0&1&0&0&0&0&0&0&1&0&0 \\ 0&0&0&0&0&1&0&0&0&1&1&0 \\ 0&1&0&0&0&0&0&0&0&0&1&0 \\ 0&0&0&1&1&0&0&0&0&0&0&1 \\ 0&0&0&0&1&0&0&1&0&0&0&0 \end{vmatrix}.$$

For calculation of basis invariants of net $Z1{,}2$ according to (4), we construct the joint matrix $G^{1,2}$ out of invariants of subnets G^1 and G^2:

$$G^{1,2} = \begin{vmatrix} 1&1&1&1&1&0&0&0&0&0&0&0&0&0 \\ 1&1&1&0&0&0&0&1&0&0&0&0&0&0 \\ 0&0&0&1&1&0&1&0&0&0&0&0&0&0 \\ 1&1&0&0&0&1&0&0&0&0&0&0&0&0 \\ 0&0&0&0&1&0&0&0&1&0&0&0&0&0 \\ 0&0&0&0&0&0&1&1&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0&0&1&1&1&1&1 \\ 0&0&0&0&0&0&0&0&0&1&1&1&0&0 \\ 0&0&0&0&0&0&0&0&0&0&0&0&1&1 \\ 0&0&0&0&0&0&0&0&0&1&1&0&0&0 \\ 0&0&0&0&0&0&0&0&0&0&0&0&0&1 \\ 0&0&0&0&0&0&0&0&0&0&0&0&0&0 \end{vmatrix}.$$

The indexation of columns corresponds to vector

$$(x_1, x_2, x_3, x_4, x_5, x_{12}, x_{13}, x_{14}, x_{15}, x_{20}, x_{21}, x_{22}, x_{23}, x_{24}).$$

Invariants of contact places are calculated according to matrix for subnet $Z1$.

Matrix of basis solutions $H^{1,2} = R^{1,2} \cdot G^{1,2}$ has the form

$$H^{1,2} = \begin{vmatrix} 0&0&0&0&0&0&0&0&0&1&1&1&1&1 \\ 1&1&1&1&1&0&0&0&0&0&0&0&0&0 \\ 1&1&0&0&0&1&0&0&0&0&0&0&1&1 \\ 0&0&0&1&1&0&1&0&0&1&1&0&0&0 \\ 0&0&0&0&0&0&1&1&0&1&1&0&0&1 \\ 1&1&1&0&0&0&0&1&0&0&0&0&0&1 \\ 1&1&0&0&1&1&0&0&1&0&0&0&0&0 \\ 0&0&0&0&1&0&0&0&1&1&1&1&0&0 \end{vmatrix}.$$

6.2. Composition: Z4+Z3

The invariants of subnets $Z4$ and $Z3$ may be represented as

$$(x_1, x_5, x_6, x_7, x_8, x_9, x_{10}, x_{11}, x_{16}, x_{17}, x_{18}, x_{19}) = (z_1^4, z_2^4, z_3^4, z_4^4, z_5^4, z_6^4) \cdot G^4,$$

$$(x_{20}, x_{24}, x_{25}, x_{26}, x_{27}, x_{28}, x_{29}, x_{30}, x_{17}, x_{16}, x_{19}, x_{18}) = (z_1^3, z_2^3, z_3^3, z_4^3, z_5^3, z_6^3) \cdot G^3,$$

where the matrixes have the form

$$G^4 = G^3 = \begin{vmatrix} 1&1&1&1&1&1&1&1&0&0&0&0 \\ 1&0&1&0&1&1&0&1&0&1&0&0 \\ 0&1&0&1&0&0&1&0&0&0&1&0 \\ 1&0&0&0&0&0&1&1&0&0&0&1 \\ 0&1&1&0&0&0&0&0&1&0&0&0 \\ 0&0&0&0&0&0&0&0&0&1&1&0 \end{vmatrix}.$$

System of equations for contact places has the form:

$$\begin{cases} p_{16}: & z_5^4 - z_2^3 - z_6^2 = 0, \\ p_{17}: & z_5^3 - z_2^4 - z_6^2 = 0, \\ p_{18}: & z_3^4 + z_6^4 - z_4^3 = 0, \\ p_{19}: & z_3^3 + z_6^3 - z_4^4 = 0. \end{cases}$$

The general solution of system may be represented as

$$(z_1^4, z_2^4, z_3^4, z_4^4, z_5^4, z_6^4, z_1^3, z_2^3, z_3^3, z_4^3, z_5^3, z_6^3) = \bar{y} \cdot R^{4,3},$$

$$R^{4,3} = \begin{vmatrix} 0&0&0&0&0&0&1&0&0&0&0&0 \\ 1&0&0&0&0&0&0&0&0&0&0&0 \\ 0&0&0&0&1&0&0&1&0&0&0&0 \\ 0&1&0&0&0&0&0&0&0&0&1&0 \\ 0&0&0&0&0&1&0&0&0&1&1&0 \\ 0&0&1&0&0&0&0&0&0&1&0&0 \\ 0&0&0&1&1&0&0&0&0&0&0&1 \\ 0&0&0&1&0&0&0&0&1&0&0&0 \end{vmatrix}.$$

For calculation of basis invariants of net $Z4{,}3$ according to (4), we construct the joint matrix $G^{4,3}$ out of invariants of subnets G^4 and G^3:

$$G^{4,3} = \begin{vmatrix} 1&1&1&1&1&1&1&1&0&0&0&0&0&0&0&0&0&0&0&0 \\ 1&0&1&0&1&1&0&1&0&1&0&0&0&0&0&0&0&0&0&0 \\ 0&1&0&1&0&0&1&0&0&0&1&0&0&0&0&0&0&0&0&0 \\ 1&0&0&0&0&0&1&1&0&0&0&1&0&0&0&0&0&0&0&0 \\ 0&1&1&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0&0&1&1&0&0&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0&0&0&0&0&1&1&1&1&1&1&1&1 \\ 0&0&0&0&0&0&0&0&0&0&0&0&1&0&1&0&1&1&0&1 \\ 0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&1&0&0&1&0 \\ 0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&1&1 \\ 0&0&0&0&0&0&0&0&0&0&0&0&0&1&1&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0 \end{vmatrix}.$$

The indexation of columns corresponds to vector

$$(x_1, x_5, x_6, x_7, x_8, x_9, x_{10}, x_{11}, x_{16}, x_{17}, x_{18}, x_{19}, x_{20}, x_{24}, x_{25}, x_{26}, x_{27}, x_{28}, x_{29}, x_{30}).$$

Matrix of basis solutions $H^{4,3} = R^{4,3} \cdot G^{4,3}$ has the form

$$H^{4,3} = \begin{vmatrix} 0&0&0&0&0&0&0&0&0&0&0&0&1&1&1&1&1&1&1&1 \\ 1&1&1&1&1&1&1&1&0&0&0&0&0&0&0&0&0&0&0&0 \\ 0&1&1&0&0&0&0&0&1&0&0&0&1&0&1&0&1&1&0&1 \\ 1&0&1&0&1&1&0&1&0&1&0&0&0&1&1&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0&0&1&1&0&1&1&1&0&0&0&1&1 \\ 0&1&0&1&0&0&1&0&0&0&1&0&1&0&0&0&0&0&1&1 \\ 1&1&1&0&0&0&1&1&1&0&0&1&0&0&0&0&0&0&0&0 \\ 1&0&0&0&0&0&1&1&0&0&0&1&0&1&0&1&0&0&1&0 \end{vmatrix}.$$

6.3. Composition: Z1,2 +Z4,3

System of equations for contact places has the form:

$$\begin{cases} p_1: & z_2^{4,3}+z_4^{4,3}+z_7^{4,3}+z_8^{4,3}-z_2^{1,2}-z_3^{1,2}-z_6^{1,2}-z_7^{1,2}=0, \\ p_5: & z_2^{1,2}+z_4^{1,2}+z_7^{1,2}+z_8^{1,2}-z_2^{4,3}-z_3^{4,3}-z_6^{4,3}-z_7^{4,3}=0, \\ p_{20}: & z_1^{4,3}+z_3^{4,3}+z_5^{4,3}+z_6^{4,3}-z_1^{1,2}-z_4^{1,2}-z_5^{1,2}-z_8^{1,2}=0, \\ p_{24}: & z_1^{1,2}+z_3^{1,2}+z_5^{1,2}+z_6^{1,2}-z_1^{4,3}-z_4^{4,3}-z_5^{4,3}-z_8^{4,3}=0. \end{cases}$$

This system has 48 basis solutions constituting matrix R:

$$R=\begin{vmatrix}
0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&1\\
0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&1\\
0&0&0&0&0&0&1&0&0&0&0&0&0&0&1&0\\
0&1&0&0&0&0&0&0&0&0&0&0&0&0&1&0\\
0&0&0&0&0&1&0&0&0&0&0&1&0&0&0&0\\
0&0&1&0&0&0&0&0&0&0&0&1&0&0&0&0\\
0&0&0&0&0&0&1&0&0&1&0&0&0&0&0&0\\
0&1&0&0&0&0&0&0&0&1&0&0&0&0&0&0\\
0&0&0&0&0&0&0&1&0&0&0&0&0&1&0&0\\
0&0&0&1&0&0&0&0&0&0&0&0&0&1&0&0\\
0&0&0&0&1&0&0&0&0&0&0&0&1&0&0&0\\
1&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0\\
0&0&0&0&0&0&0&1&0&0&1&0&0&0&0&0\\
0&0&0&1&0&0&0&0&0&0&1&0&0&0&0&0\\
0&0&0&0&1&0&0&0&1&0&0&0&0&0&0&0\\
1&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0\\
0&0&0&0&1&0&1&0&0&0&0&0&0&1&0&1\\
0&1&0&0&1&0&0&0&0&0&0&0&0&1&0&1\\
0&0&0&0&1&0&1&0&0&0&0&1&0&1&0&0\\
0&1&0&0&1&0&0&0&0&0&0&1&0&1&0&0\\
1&0&0&0&0&0&1&0&0&0&0&0&0&1&0&1\\
1&1&0&0&0&0&0&0&0&0&0&0&0&1&0&1\\
1&0&0&0&0&0&1&0&0&0&0&1&0&1&0&0\\
1&1&0&0&0&0&0&0&0&0&0&1&0&1&0&0\\
0&0&0&0&1&0&1&0&0&0&1&0&0&0&0&1\\
0&1&0&0&1&0&0&0&0&0&1&0&0&0&0&1\\
0&0&0&0&1&0&1&0&0&0&1&1&0&0&0&0\\
0&1&0&0&1&0&0&0&0&0&1&1&0&0&0&0\\
1&0&0&0&0&0&1&0&0&0&1&0&0&0&0&1\\
1&1&0&0&0&0&0&0&0&0&1&0&0&0&0&1\\
1&0&0&0&0&0&1&0&0&0&1&1&0&0&0&0\\
1&1&0&0&0&0&0&0&0&0&1&1&0&0&0&0\\
0&0&0&0&0&1&0&1&0&0&0&0&1&0&1&0\\
0&0&0&1&0&1&0&0&0&0&0&0&1&0&1&0\\
0&0&0&0&0&1&0&1&1&0&0&0&0&0&1&0\\
0&0&0&1&0&1&0&0&1&0&0&0&0&0&1&0\\
0&0&1&0&0&0&0&1&0&0&0&0&1&0&1&0\\
0&0&1&1&0&0&0&0&0&0&0&0&1&0&1&0\\
0&0&1&0&0&0&0&1&1&0&0&0&0&0&1&0\\
0&0&1&1&0&0&0&0&1&0&0&0&0&0&1&0\\
0&0&0&0&0&1&0&1&0&1&0&0&1&0&0&0\\
0&0&0&1&0&1&0&0&0&1&0&0&1&0&0&0\\
0&0&0&0&0&1&0&1&1&1&0&0&0&0&0&0\\
0&0&0&1&0&1&0&0&1&1&0&0&0&0&0&0\\
0&0&1&0&0&0&0&1&0&1&0&0&1&0&0&0\\
0&0&1&1&0&0&0&0&0&1&0&0&1&0&0&0\\
0&0&1&0&0&0&0&1&1&1&0&0&0&0&0&0\\
0&0&1&1&0&0&0&0&1&1&0&0&0&0&0&0
\end{vmatrix}$$

Let us construct the joint matrix G out of invariants of subnets $G^{1,2}=H^{1,2}$ and $G^{4,3}=H^{4,3}$:

$$G=\begin{vmatrix}
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&1&1&1&1&0&0&0&0&0&0\\
1&1&1&1&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
1&1&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&1&1&0&0&0&0&0&0\\
0&0&0&1&1&0&0&0&0&0&0&0&1&0&0&0&0&0&0&1&1&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&1&1&0&0&0&0&0&1&1&0&0&1&0&0&0&0&0&0\\
1&1&1&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0\\
1&1&0&0&1&0&0&0&0&0&0&1&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&1&0&0&0&0&0&0&0&0&0&1&0&0&0&0&1&1&1&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&1&1&1&1&1\\
0&0&0&0&0&1&1&1&1&1&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&1&0&1&1&0&1\\
0&0&0&0&0&1&0&1&1&0&1&0&0&0&0&0&1&0&0&0&0&0&0&0&1&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&1&0&0&0&0&0&0&1&0&0&0&1&1\\
0&0&0&0&0&0&1&0&0&1&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&1&1\\
0&0&0&0&0&1&0&0&0&1&1&0&0&0&0&1&0&0&1&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&1&1&0&0&0&0&0&0&0&1&0&0&0&0&0&0&1&0&0&1&0
\end{vmatrix}$$

Matrix of basis solutions $H^{4,3}=R^{4,3}\cdot G^{4,3}$ after the erasing of nonminimal solutions has the form:

$$H=\begin{vmatrix}
1&1&1&0&0&0&0&0&0&1&1&0&0&1&0&0&0&0&1&0&0&0&0&1&0&1&0&0&1&0\\
1&1&0&0&0&0&0&0&0&1&1&1&0&0&0&0&0&0&1&0&0&0&1&1&0&1&0&0&1&0\\
1&1&0&0&1&1&0&0&0&1&1&1&0&0&1&1&0&0&1&0&0&0&0&0&0&0&0&0&0&0\\
1&1&1&1&1&1&0&0&0&1&1&0&0&0&0&1&0&0&1&0&0&0&0&0&0&0&0&0&0&0\\
1&1&1&0&0&1&0&1&1&0&1&0&0&1&0&0&1&0&0&0&0&0&0&1&1&0&0&0&0&0\\
1&1&0&0&0&1&0&1&1&0&1&1&0&0&0&0&1&0&0&0&0&0&1&1&1&0&0&0&0&0\\
1&1&0&0&1&1&1&1&1&1&1&1&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
1&1&1&1&1&1&1&1&1&1&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&1&0&1&0&0&1&0&0&0&0&1&0&0&1&0&1&1&1&0&0&0&0&0&0&1&1\\
0&0&0&1&1&0&1&0&0&1&0&0&1&0&0&0&0&1&0&1&1&0&0&0&0&0&0&0&1&1\\
0&0&0&0&0&0&0&0&0&0&0&0&1&1&0&0&1&1&0&1&1&0&0&1&1&0&0&0&1&1\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&1&0&1&1&1&1&1&1&0&0&0&1&1\\
0&0&0&0&1&1&0&0&0&0&0&0&0&0&1&1&0&0&0&1&1&1&0&0&1&0&1&1&0&1\\
0&0&0&1&1&1&0&0&0&0&0&0&1&0&0&1&0&0&0&1&1&0&0&0&1&0&1&1&0&1\\
0&0&0&0&0&0&0&0&0&0&0&0&1&1&0&0&0&0&0&1&1&0&0&1&1&1&1&1&1&1\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&1&1&1&1&1&1&1&1&1&1\\
1&1&0&0&1&0&1&0&0&2&1&1&1&1&1&0&0&1&1&1&1&0&0&1&0&1&0&0&2&1\\
1&1&1&1&1&0&1&0&0&2&1&0&0&0&0&0&0&1&1&1&1&1&1&1&0&1&0&0&2&1\\
1&1&0&0&1&2&0&1&1&0&1&1&1&1&1&1&1&0&0&1&1&0&0&1&2&0&1&1&0&1\\
1&1&1&1&1&2&0&1&1&0&1&0&0&0&0&1&1&0&0&1&1&1&1&1&2&0&1&1&0&1\\
1&1&1&0&1&1&0&0&0&1&1&0&0&1&1&1&1&1&1&1&1&1&0&1&1&0&0&0&1&1\\
1&1&0&1&1&1&0&0&0&1&1&1&1&0&0&1&1&1&1&1&1&0&1&1&1&0&0&0&1&1\\
1&1&1&0&1&1&1&1&1&1&1&0&0&1&1&0&0&0&0&1&1&1&0&1&1&1&1&1&1&1\\
1&1&0&1&1&1&1&1&1&1&1&1&1&0&0&0&0&0&0&1&1&0&1&1&1&1&1&1&1&1
\end{vmatrix}$$

Since, for instance, the sum of all the rows has all the natural components, model of protocol is p-invariant and, consequently, it is bounded and safe net.

In the same way, using dual net and decomposition [14], it may be shown that model is t-invariant also. It means that net is persistent and constitutes the necessary conditions for its liveness.

Notice that, expenses of time for invariants calculation via stepwise composition of functional subnets completely corresponds to exponential estimations of acceleration represented in [14]. The total time for construction of basis invariants of places did not exceed 10 seconds on computer Pentium.

7. Conclusion

The primary result of present work is the proof of invariance of protocol TCP Petri net model. Invariance is the necessary condition of protocols' correctness. Application of decomposition of model into functional subnets and stepwise composition provided the essential speed-up of invariants calculation process.

This technique may be applied successfully at hardware and software design.

References

[1] Berthomieu B., Ribet O.-P., Vernadat F. "The tool TINA - construction of abstract state space for Petri nets and Time Petri nets". *International Journal of Production Research,* Vol. 42, no. 4, 2004.

[2] Cortadella J., Kishinevsky M., Kondratyev A., Lavagno L., Yakovlev A. *Logic synthesis of asynchronous controllers and interfaces.* Springer-Verlag, 2002, 273 p.

[3] Christensen S., Petrucci L. "Modular analysis of Petri nets". *The Computer Journal,* 43(3), 2000, pp. 224-242.

[4] Desel J. “On abstraction of nets”. *Advances in Petri Nets,* LNCS 524, 1991, pp. 78-92.

[5] Girault C., Valk R.: *Petri nets for systems engineering*. Springer-Verlag, 2003, 607 p.

[6] Han B., Billington J. “Experience using Colored Petri Nets to model TCP connection management procedures”, *Proceedings of Fifth Workshop and Tutorial on Practical Use of Coloured Petri Nets and CPN Tools*, Aarhus, Denmark, October 8-11, 2004, pp.57-76.

[7] Haddad S., Klai K., Ilie J.-M. “An incremental verification technique using decomposition of Petri nets”, *Proceedings of the second IEEE International Conference on Systems, Man and Cybernetics*, October 6-9, 2002, Hammamet, Tunisia, vol. 2.

[8] Juan E.Y.T., Tsai J.J.P., Murata T. “Compositional verification of concurrent systems using Petri net based condensation rules”, *ACM Trans. on Programming Languages and Systems*, Vol. 20, No. 5, 1998, pp. 917-979.

[9] Kryviy S.L. “Methods of solution and criteria of compatibility of systems of linear Diophantine equations over the set of natural numbers”, *Cybernetics and Systems Analysis,* no. 4, 1999, pp. 12-36.

[10] Postel, J., Editor, "Transmission Control Protocol," *STD 7, RFC 793,* September 1981.

[11] Tutte W.T. *Graph Theory*, Addison-Wesley, 1984.

[12] Valmari A. “Composition and abstraction”. *Modelling and verification of parellel processes*, LNCS 2067, 2001, pp. 58-99.

[13] Zaitsev D.A. “Decomposition of Petri Nets”, *Cybernetics and Systems Analysis*, Vol. 43, No. 5, 2004.

[14] Zaitsev D.A. “Decomposition-based calculation of Petri net invariants”, *Proceedings of Token based computing Workshop of the 25-th International conference on application and theory of Petri nets*, Bologna, Italy, June 21-25, 2004, pp. 79-83.

[15] Zaitsev D.A. “Verification of protocol TCP via decomposition of Petri net model into functional subnets”, *Proceedings of the Poster session of 12th Annual Meeting of the IEEE / ACM International Symposium on Modeling, Analysis, and Simulation of Computer and Telecommunication Systems,* October 5-7,2004, Volendam, Netherlands, pp. 73-75.

[16] Zaitsev D.A. “Stepwise Composition of Functional Subnets”, *Proceedings of Odessa National Telecommunication Academy*, no. 3, 2004. In Russ.

Published: Proceedings of the Design, Analysis, and Simulation of Distributed Systems Symposium, April 2-8, 2005, San Diego, USA, p. 72-78.