

<http://ansinet.com/itj>

ITJ

ISSN 1812-5638

# INFORMATION TECHNOLOGY JOURNAL

**ANSI***net*

Asian Network for Scientific Information  
308 Lasani Town, Sargodha Road, Faisalabad - Pakistan

## Security Infrastructure Verification of Library Information Grid Based on ePr/T net

<sup>1</sup>Xian-Wen Fang, <sup>2</sup>Xiao-Qin Fan and <sup>1</sup>Yan-Ni Zou

<sup>1</sup>Department of Information and Computing Science,  
Anhui University of Science and Technology, Huainan Anhui, 232001, China

<sup>2</sup>School of Computer and Information Technology,  
Shanxi University, Taiyuan Shanxi, 030006, China

---

**Abstract:** Grid Security Infrastructure of Library Information (GSI-LI) is difficult to analyze dynamic traits and behavior relationships by using ordinary modeling tools. In the study, the modeling methods about GSI-LI are presented based on the extend Predication/Transition net (ePr/T net) and then taking advantage of S-invariant properties of the ePr/T net, the model of GSI-LI is validated. The analyzing effect shows the GSI-LI is correct and the verification methods are effective.

**Key words:** The extend predication/transition net, grid security infrastructure of library information, S-invariant, verification

---

### INTRODUCTION

By constituting fully shared resource integration through high-speed Internet with the calculating resources distributed at different places, grid provides a sort of resource capability for high-performance calculation, management and service (Chard *et al.*, 2009). In the grid computing environment, all sorts of resources are dynamically linked to the internet and can be used conveniently by users (Foster *et al.*, 2001). Therefore, the grid computing environment must have the capability to resist the illegal attack and encroachment and guarantee the security of information.

Grid as a new resources management form of next-generation internet, it can provide a secure, reliable and efficient operating environment for on-demand digital library (Thomasr *et al.*, 2007). Because of the grid nodes are located in different regions, these will be key problem that how to safely share data between the resources nodes of the digital library (Yang and Hu, 2005), how to ensure the integrity of sharing data. Grid security includes grid system security, data transmission security, information storage security. Therefore, we must adopt advanced security technology and need to identify data and information which to be sent and to be received online between the two sides, in order to ensure the security, integrity, reliability and transaction non-repudiation of all transmission of information.

The use of Grid Security Infrastructure of Library Information (GSI-LI) to build a digital library platform that enables secure sharing of library resources. All nodes of libraries to the library resource agent (Agent) supplied data resources (Candela and Castellil, 2005) so this will form local management domain, which has regional trading security policy and name of data resources. On this basis, a virtual share trading field is built, a virtual library of resources and global security strategy are provided and the transaction is managed by agent.

The project of digital library information provides safety authentication and safety communication by putting forward GSI-LI. Based on the system of public key encryption, GSI (Foster *et al.*, 2002) adopts X.509 authentication and SSL (Secure sockets layer) communication protocol and expand them in certain degree. The main security technology method includes safety authentication and mutual identification of safety identity, communication encryption, private key protection (Zhang and Wang, 2008), commission and single dot logging on, etc. Grid is prevalent in recent years; there are some literatures to study why, in the attempt to better satisfy the user requirements, develop a service-oriented digital library infrastructure on the grid. The study describes and compares the two systems by focusing, in particular, on that part of the architecture that controls and supplies the necessary features for creating and managing digital libraries, but the security infrastructure of OpenDLib is not be analyzed systemically by model checking. Barbosa *et al.* (2007)

investigated the benefits and drawbacks of a strategy for verification of occurrence graphs that uses computational grids as infrastructure for distribution. This investigation was performed using a tool set for the Petri net formalism and a computational grid for bag-of-tasks applications. Cholia and Porter (2008) analyzed the various vectors of information being published from sites to grid infrastructures and analyze the risks and potential threat models posed by the publication and collection of such data. We also offer some recommendations and best practices for sites and grid infrastructures to manage and protect sensitive data. But there are few people setting foot in GSI's assignment submission and implementation procedure in grid environment using ePr/T net. EPr/T net is a kind of advanced Petri net, it can depict the system's dynamic characteristic concisely from the process angle completely, it has great advantage on describing some important activities and phenomena such as concurrence, conflict and synchronization, etc. The established model not only can achieve the macro-control effect by ePr/T, but also can feed back every detail of the flow with reference to microcosmic aspect. This study applies ePr/T net theory in the description of GSI-LI, it could make this complicated process transparent toward customers, therefore it is very useful for the improvement of grid structure.

### BASIC CONCEPTION

Here, we only introduce several conceptions correlating with the study close, other Petri Nets terms in the literature (Murata, 1989).

**Definition 1:** The condition for  $\Sigma = (S, T; F, D, V, A_p, A_r, A_s, M_0)$  to constitute Pr/T net:

- If  $(S, T; F)$  is a directed net, then  $(S, T; F)$  is the  $\Sigma$ 's elementary net
- If  $D$  is a nonempty finite set, then  $D$  is the  $\Sigma$ 's individual set;  $\Omega$  is a given operator set limited in scope of  $D$
- $V$  is a variable set limited in scope of  $D$
- $A_p: S \rightarrow \pi$ ,  $\pi$  is a variable predicate set limited in scope of  $D$ . According to  $s \in S$ , if  $A_s(S)$  is predicate of  $n$  variable, then  $S$  is predicate of  $n$  variable
- $A_r: T \rightarrow f_D$ ,  $f_D$  is  $D$ 's formulary, according to  $t \in T$ ,  $A_r(t)$  can only include static predicate and operator in  $\Omega$
- $A_s: F \rightarrow f_s$ ,  $f_s$  is  $D$ 's symbol set. According to predicate of  $n$  variable  $s \in S$ , if  $(s, t) \in F$  or  $(t, s) \in F$ , then  $A_r(t, s)$  or  $A_s(s, t)$  is symbol sum of  $n$  variable. According to  $t \in T$ , the free variable in formula  $A_r(t)$  (viz., variable

unrestrained by  $\forall$  and  $\exists$ ) must be a free variable on the directed arc where  $t$  is located at the end

- $M_0: S \rightarrow f_s$ , according to predicate of  $n$  variable  $s \in S$ ,  $M_0(s)$  is symbol sum of  $n$  variable

**Definition 2: Murata (1989):** Nonzero  $m = |S|$  dimensional row vector  $V = (V_1, V_2, \dots, V_m)$  is called  $S$ -invariable of Pr/T net, if:

- All the  $V_i (i=1, 2, \dots, m)$  are 0 or 1
- According to any reachable marking  $M$ , it can conclude that:

$$\sum_{i=1}^m V_i \cdot R(M(s_i)) = \sum_{i=1}^m V_i \cdot R(M_0(s_i))$$

viz.,  $V_i \cdot R(M) = V_i \cdot R(M_0)$ , among it,  $M, M_0$  are column vectors.

**Definition 3:** A ePr/T net is a quintuples called  $EPR = (Pr/T; M, R)$ , among it:

- Pr/T is a Predication/Transition net system
- $R$  is a flow of Pr/T, elements in  $R$  are called inhibit arc.  $\text{---}\bullet$ , a section with a small circle in the end is used to describe inhibit arc. If  $(x, y) \in R$ , then  $x$  is  $y$ 's inhibit place

**Definition 4:** The firing rule of transition in a ePr/T net called  $EPR = (S, T, F, M, R)$  is:

- According to  $t \in T$ , if it meets the following two conditions:

- $\forall s(s \in S \wedge (s, t) \in F) \rightarrow M(s) \neq \infty$
- $\forall s(s \in S \wedge (s, t) \in R) \rightarrow M(s) = \infty$

then  $t$  is enabled under the marking  $M$ .

- If  $t$  is enabled, then it could be fired, called  $M' ([t >]$ . If  $M[t > M'$ , then:

$$M'(s) = \begin{cases} M(s) - A_r(s, t) & (s, t) \in F \text{ and } (t, s) \notin F \\ M(s) + A_r(t, s) & (s, t) \notin F \text{ and } (t, s) \in F \\ M(s) & \text{others} \end{cases}$$

**Definition 5:** Murata (1989). The condition that  $|S| \times |T|$  step matrix  $C$  is the incidence matrix of Pr/T net is:  $C$ 's matrix element  $C_{ij}$  is demonstrated by the formula below:

$$C_{ij} = -A_r(S_i, t_j) + A_r(t_j, S_i)$$

Among:

it  $i = 1, 2, \dots, |S|$ ;  $j = 1, 2, \dots, |T|$ ;

and:

if  $S_i \neq t_j$ ,

then:

$A_F(S_i, T_j) = \diamond$ ;

if  $s_i \neq t_j$ ,  $nA_F(t_j, s_i) = \diamond$

**Definition 6:** Murata (1989). If  $V = (v_1, v_2, \dots, v_m)$  is a S-invariable of Pr/T net, then  $v\text{-IC} = \theta_T$ , among it,  $\bullet$  is matrix multiplication,  $\theta_T$  is  $n = |T|$  dimensional zero row vector (IC is an incidence matrix of Pr/T net).

#### THE DESCRIPTION OF ASSIGNMENT SUBMISSION AND IMPLEMENTATION PROCEDURE ABOUT GSI-LI

The description of assignment submission and implementation procedure about GSI-LI as follows:

- Before conducting the globus assignment submission and implementation, customer and service node send petition to safety certification center for obtaining safety certification certificate

- After receiving the petition, safety certification center inspects the customer or service node, if the inspection result is qualified, then it returns the signed safety certification certificate to the petitioner
- Before submitting assignment, customer can create a user agent with time jurisdiction
- After identifying safety mutually between the customer and the remote service node called gatekeeper, user agent submits the assignment to the gatekeeper and the gatekeeper gives task manager the assignment for processing
- If other remote resources are needed in assignment implementation, it must take safety identification between assignment process and resource agent. If remote data or document needed to be accessed in implementation, it is necessary to take safety identification between assignment process and remote resource agent (Limaye *et al.*, 2005), afterwards, give warrant and map local ID, then access document or data

#### MODELING AND ANALYSIS BASED ON EPr/T NET

**Modeling based on ePr/T net:** In this assignment submission, it involves the flow of many kinds of resources and the flowing process is relatively complicated. If singly seeing general depicting graph, we can only find some main flows, whereas some details can not be mastered, in view of the inhomogeneous flowing resources, here we model based on Pr/T net to solve this problem (Fig. 1).

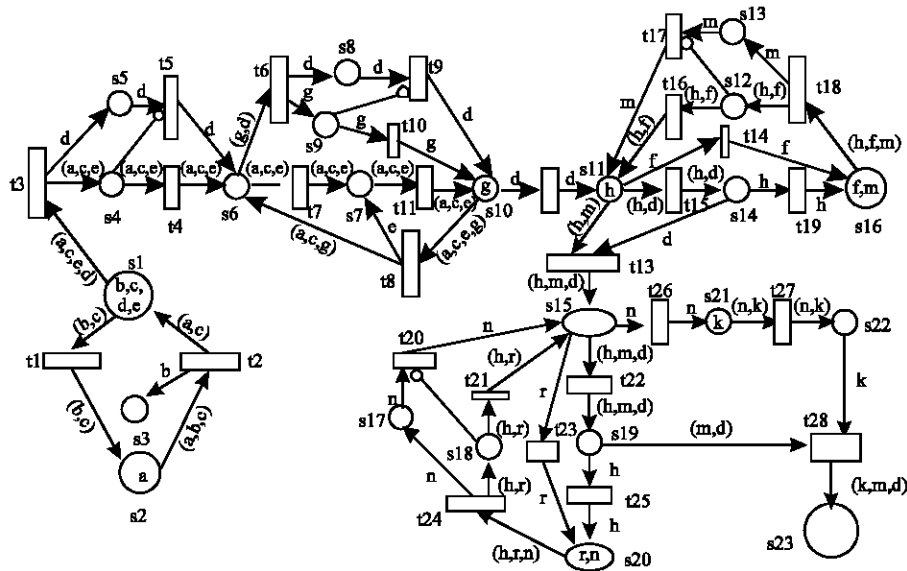


Fig. 1: ePr/t net based on GSI's assignment submission and implementation procedure

Because of too many transitions and places, enumeration is not given here. Connotation and features of the main places and transitions in this process can be concluded as follows:

- **Main places:** s1: user; s2: CA identification center; s6: user agent; s10: gatekeeper; s11: task process; s16: resource agent; s20: remote resource agent; s21: remote data; s23: finished assignment
- **Main transitions:** t1: making a request for signing safety certificate; t2: signing and returning safety certificate; t4: establishing user agent; t5: submitting assignment to user agent; t9: submitting assignment to gatekeeper; t11: user agent asking gatekeeper for identifying its identity; t12: submitting assignment to assignment process; t18: resource agent returning the certificate of assignment process and dispatching resources to process; t28: assignment receiving required data and resource and ending the implementation
- **Representation of every sort of resources:** a: CA public key; b: user private key; c: user's certificate requesting to be signed; d: task; e: agent certificate; f: resource agent certificate; g: gatekeeper certificate; h: certificate for assignment process; m: the required resource; r: certificate for remote resource agent; n: authorized certificate of remote document; k: remote document

From Fig. 1, we can find the flowing procedure of every sort of initial resource and grasp every detail in submitting assignment from the microcosmic angle. At first, t1 is fired, viz., s1 sends C and b to s2, after s2 receives resources, t2 could be fired, viz., CA identification center returns certificate c which has been signed and public key a to the user and saves the private key into s3. The subsequent firing procedure is almost the same, so here it is unnecessary to give the similar narration.

**Model analysis based on S-invariable:** As ePr/T net is different from elementary Petri net, its resources are in different variety, so the reachability can't be analyzed by the matrix equation. Here, S-invariable is adopted to analyze reachability.

The original meaning of S-invariable (Murata, 1989) is to seek for the trace of resources and the reachability of certain state marking could be verified according to the definition of S-invariable. First of all, S-invariable should be calculated and incidence matrix of the ePr/T net could be written out (Table 1).

Table 1: Incidence matrix of the ePr/T net based on GSI-LI's assignment submission and implementation procedure

|                 | t <sub>1</sub> | t <sub>2</sub> | t <sub>3</sub> | t <sub>4</sub> | t <sub>5</sub> | ... | t <sub>28</sub> |
|-----------------|----------------|----------------|----------------|----------------|----------------|-----|-----------------|
| S <sub>1</sub>  | -<b, c>        | <a, c>         | -<a, c, e, d>  | <>             | <>             | ... | <>              |
| S <sub>2</sub>  | <b, c>         | -<a, b, c>     | <>             | <>             | <>             | ... | <>              |
| S <sub>3</sub>  | <>             | <b>            | <>             | <>             | <>             | ... | <>              |
| S <sub>4</sub>  | <>             | <>             | <a, c, e>      | -<a, c, e>     | <>             | ... | <>              |
| ...             | ...            | ...            | ...            | ...            | ...            | ... | ...             |
| S <sub>23</sub> | <>             | <>             | <>             | <>             | <>             | ... | <m, d, k>       |

According to Table 1, if resource categories of every row and column are ignored and the numbers of resources are only paid close attention to, then the following incidence matrix with 23 rows and 28 columns could be written out. The incidence matrix of ePr/t model as:

$$\begin{pmatrix} -2 & 2 & -4 & 0 & 0 & \dots & 0 \\ 2 & -3 & 0 & 0 & 0 & \dots & 0 \\ 0 & 1 & 0 & 0 & 0 & \dots & 0 \\ 0 & 0 & 3 & -3 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & 0 & 0 & 3 \end{pmatrix}$$

According to definition 6, v vector can be calculated, here the numbers of rows and columns of the matrix are with big amount, as majority of element are zero, so the calculation is not very complicated, 23 dimensional row vector  $v = (1, 1, 1, \dots, 1)$  is obtained by calculation, on the basis of  $v \cdot R(M) = v \cdot R(M_0)$ , it can be verified whether v is a S-invariable. The initial marking is  $M_0^T = (<b, c, d, e>, <a>, <>, \dots, <>)$ , if  $M_0[t_1 > M_1 >$ ,  $M_1^T = (<e, d>, <a, b, c>, <>, <>)$ . Through the verification: v satisfies the formula above, viz., v is a S-invariable.

According to the quality of S-invariable, the reachability of any one of state markings could be verified. For the model based on ePr/T net, assignment can be verified whether it is submitted and finished ultimately. If the ultimate state cannot be reached, then the system could be directly inspected, which promotes the work efficiency.

In this model, the ultimate state  $M^T = (<>, <>, <b>, \dots, <m, d, k>)$ , can be verified that it is reachable according to the methods described above; meanwhile, it also verifies the correctness of the model based on ePr/T net.

## CONCLUSIONS

In the reality, the library information grid is a major project, so the GSI-LI must be designed correctly, Because the mistakes in design are very difficult to trace and it needs to waste a big cost to make up for a loss, the study presents a verification methods of GSI-LI based on

ePr/T net. The net's superiority showing in concurrence, conflict and synchronization, etc. and rigorous mathematical theory used for analyzing the procedure, if simulated by ePr/T net, it is very easy to be analyzed the flowing condition of the resources, moreover, problems can be discovered in time. It is benefit to implement the resources sharing of digital library entirely, to improve the consult efficiency and can guarantee the security, integrity and reliability of information communication.

Based on the theoretical analysis, the innovation and advantage of the study are:

- The description of assignment submission and implementation procedure about GSI-LI are given
- The modeling of GSI-LI is proposed based on the ePr/T net
- Using the S-invariable to analyze the GSI-LI model, the analyzing effect shows the GSI-LI is correct and feasible

In the future, we should study the high efficient resource manage mechanism of digital library grid.

#### **ACKNOWLEDGMENTS**

We would like to thank the support of the National Natural Science Foundation of China under Grant No. 60873144, the excellent young talents project of Anhui province of China (2009SQRS045) and the Humanity and Society Science project of Anhui province of China (2009SK156).

#### **REFERENCES**

- Barbosa, P.E.S., C.L. Rodrigues, J.C.A. Figueiredo and D.D.S. Guerrero, 2007. Distributed verification of occurrence graphs: Investigating the use of computational grids. Proceedings of the 33rd Annual Conference of the IEEE Industrial Electronics Society, Nov. 5-8, Univ. Fed. de Campina Grande, Campina Grande, pp: 82-87.
- Candela, L. and D. Castellil, 2005. Moving digital library service systems to the Grid. *Lecture Notes Comput. Sci.*, 36: 236-259.
- Chard, K., W. Tan, J. Boverhof and I. Foster, 2009. Wrap scientific applications as WSRF grid services using gRAVI. Proceedings of the IEEE International Conference on Web Services, July 06-10, IEEE Computer Society Washington, DC., USA., pp: 83-90.
- Cholia S. and R.J. Porter, 2008. Publication and protection of sensitive site information in a grid infrastructure. Proceedings of the CCGRID 2008-8th IEEE International Symposium on Cluster Computing and the Grid, May 19-22, IEEE Computer Society Washington, DC., USA., pp: 639-644.
- Foster, I., C. Kesselman and S. Tuecke, 2001. The anatomy of the grid: Enabling scalable virtual organizations. *Int. J. High Perform. Comput. Appl.*, 15: 200-222.
- Foster, I., C. Kesselman, J.M. Nick and S. Tuecke, 2002. Grid services for distributed system integration. *Computer*, 35: 37-46.
- Limaye, K., B. Eangsuksun, Y. Liu, Z. Greenwood, S.L. Scott, R. Libby and K. Chanchio, 2005. Reliability-aware resource management for computational grid/cluster environments. Proceedings of the 6th IEEE/ACM International Workshop on Grid Computing, Nov. 13-14, IEEE Computer Society Washington, DC., USA., pp: 211-218.
- Murata, T., 1989. Petri nets, properties, analysis and applications. *Proc. IEEE*, 77: 541-580.
- Thomasr, R., E. Jeanvoine and C. Morin, 2007. GAMoSe: an accurate monitoring service for grid applications. Proceedings of the 6th International Symposium on Parallel and Distributed Computing, July 5-8, Univ. de Rennes, Rennes, pp: 40-40.
- Yang, C.T. and H.C. Ho, 2005. Using data grid technologies to construct a digital library environment. Proceedings of the 3rd International Conference on Information Technology, June 27-30, Tunghai Univ., Taichung, Taiwan, pp: 388-392.
- Zhang, S. and B. Wang, 2008. Research on an extended OCSP protocol for grid. Proceedings of the World Congress on Intelligent Control and Automation, June 25-27, North China Electr. Power Univ., Baoding, pp: 5438-5443.