Parallel Composition Analysis of Non-interference in Cyber-physical Systems

Jingming Wang*

School of Computer and Information Engineering, Chuzhou University, Anhui 239012, China
Corresponding information : Phone:+86-0550-3512336. Fax:+86-0550-3512336. Email:wjmtime@chzu.edu.cn.

***Abstract* — At present, a rather big challenge to model cyber-physical systems is to stand for the interactions between physical level and cyber level. Researchers are faced with the trouble in the analysis of information security property of noninterference in cyber-physical systems because of the physical components and behavior appended to cyber components and systems. A new method is put forward with Petri net for working out this problem effectively by composing the complicated and large systems with simple and small systems. Meanwhile, it accomplishes the noninterference information flow security property. In this paper, this method is used to analyze the information security property of noninterference and its parallel composition in cyber-physical systems. This research provides a new formal method to explore information security property of noninterference and a sufficiency and necessary condition of parallel composition of noninterference of information security model in cyber-physical systems.**

Keywords* — *Cyber-physical Systems; Petri Net; Information Flow Security; Parallel composition;

I. INTRODUCTION

The systems design has developed increasingly in the direction of cyber-physical systems in recent years, and cyber-physical systems are the integrations of physical and computation components and processes [1-2]. Now, researchers are faced with the trouble in the analysis of information flow security property of noninterference in cyber-physical systems because of the physical components and behavior appended to cyber components and systems. A rather big challenge to model cyber-physical systems is to stand for the interactions between physical level and cyber level.

Access control security models only can figure out direct data confidentiality and information flow security. A better way of information flow security model is to apply some rules of information flow to control the direct and indirect information flow, which is called information flow security models, such as noninterference information security model which is discussed in this paper.

Non-interference information security model was first put forward by Meseguer and Goguen [3-4]. Nevertheless, there is very little research about the parallel composition of noninterference information security model in cyber-physical systems in recent years. This paper not only has defined the noninterference information security model that is based on Petri net, but also has analyzed the model in pipeline flow system. And a sufficiency and necessary condition is provided by which the non-interference information security property of cyber-physical systems will be preserved after parallel composition.

II. BASIC DEFINITIONS

A. Petri Net

Petri net can be efficiently used as a formal tool with rigorous semantics to model and analyze the information flow security properties of system models [5-7].

Definition 1 A tuple $N=(S,T,F)$ is a net, where

(1) S and T are the places sets and transitions sets, and $S\cap T=\varnothing$

(2) $F\subseteq(2^S\times T\times 2^S)$ is the flow relation set

Definition 2 Let $N=(S,T,F)$ be a net. Marking is a multiset over the set S. Given a marking m and a place s, the tokens number of place s is denoted by $m(s)$.

A pair (N,m_0) is a net system, where N is a net and m_0 is a marking of N, in general which is called initial marking. With some misuse of notation, the Petri net system can be denoted by (S,T,F,m_0).

B. Operations on Petri Net

The goal of this paper is to analyze multilevel cyber-physical systems, and different levels of actions can be performed in the systems. For instance, the interaction of cyber-physical systems with high-level actions stands for the interaction with high-level users, and the interaction of cyber-physical systems with low-level actions stands for the interaction with low-level users. This paper is to verify the truth whether the interplay between the high-level user and the high part can affect a low-level user's view or not in cyber-physical systems.

Accordingly, the Petri net transitions set is divided into two disjointed subsets: the high-level transitions set denoted by H and the low-level transitions set denoted by L, the net system is denoted by (S,L,H,F,m_0) which is mentioned above.

Definition 3 Let $N=(S,H\cup L,F,m_0)$, the operations of net system transition sequence are defined as follows [8]:

$$\begin{cases}\varepsilon/H=\varepsilon \\ \delta t/H=\begin{cases}(\delta/H)t & t\in L\\ \delta/H & t\in H\end{cases}\end{cases} \qquad \begin{cases}\varepsilon/L=\varepsilon \\ \delta t/L=\begin{cases}(\delta/L)t & t\in H\\ \delta/L & t\in L\end{cases}\end{cases}$$

In general, if a system is not a determined system , then the result statement can not be unique after the firing of one transition in the net system $N=(S,H\cup L,F,m_0)$. Result statement set is denoted by $next(m_0,\sigma)$, where $\sigma\in TS(N)$. However, the result statement is unique if the systems are determined systems, we use $step(m_0,\sigma)$ denote the result statement.

Definition 4 Net system $N=(S,H\cup L,F,m_0)$, $m\in[m_0\rangle$,

$$View_L(m)=\{(s,m(s))\mid \exists t\in L,Q,Q'\in 2^S,(Q,t,Q')\in F\wedge s\in Q\}.$$

If the tokens of all places are same from the view of the low-level users, we say that the two statements of Petri net system are low-level equal.

Definition 5 Two statements of Petri net system $N=(S,H\cup L,F,m_0)$ are low-level equal, if and only if:

$$\forall m_1,m_2\in[m_0\rangle, m_1\overset{L}{\square} m_2 \text{ iff } View_L(m_1)=View_L(m_2)$$

Definition 6 Two results statement sets of Petri net system $N=(S,H\cup L,F,m_0)$ are low level equal if and only if:

$$\forall A,B\subseteq[m_0\rangle, A\overset{L}{\square} B, \text{ iff } \exists m_1\in A,m_2\in B, s.t.\ View_L(m_1)=View_L(m_2)$$

III. MODEL NONINTERFERENCE MODEL IN PIPELINE CYBER-PHYSICAL SYSTEM

A. The Definition of Nondeterministic Noninterference Model

In general, the low-level observers can infer the confidentiality of information flow of a system when they observe that information moves from high-level users to low-level users. The initial definition of non-interference model is defined to solve the information flow security of deterministic systems. At present, the non-interference model is extended to solve the information flow security in nondeterministic system.

We defined the generalization as follows. The low-level is not interfered by the high level if and only if for any trace , and the trace with no same high level input actions to the trace . In addition, and are low view trace equivalent. Based on Petri net, the nondeterministic non-interference information flow security model is defined as follows.

Definition 6 $E\in NNI \Leftrightarrow (E\setminus_I Act_H)/Act_H \overset{L}{\square} E/Act_H$

In the definition 6, the function of the operation of \ has something in common with the operation in process algebra[9-10]. Act_H stands for the high level actions set, the symbol of I stands for the input actions set.

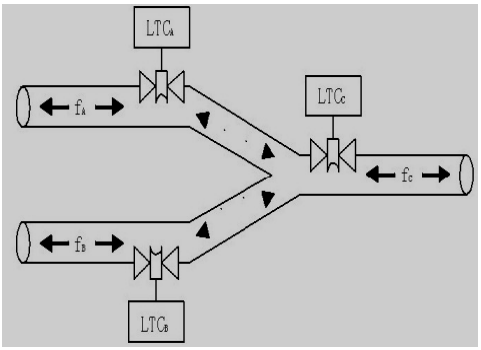

Fig.1 Pipeline network controlled by LTCs

B. Abstract Pipeline Cyber-Physical System

As one of typical cyber-physical systems, pipeline network cyber-physical system offers abundant physical and computational components and their interactivity [5]. Flow control systems in the pipeline network cyber-

physical system control the state of water or other liquid in the pipeline. LTCs carry out two commands of lower or raise the flow.

From Fig.(1) we can see that a water distribution system network with three LTCs. Three LTCs control the sub-networks A, B, and C respectively. Three LTCs of the water distribution system network are in different geographical location and are separated in long distances. The lower or raise flow commands will have impact on adjacent sub-networks inevitably, leading to observable actions at location A and B in the network flow pipes, and the following invariant holds[5]:

$$Vc = Va + Vb \quad (1)$$

Where Va , Vb and Vc stands for the volumes or changes of flow of the pipeline controlled at A, B, and C respectively.

Fig.(2) represented the transitions in the pipeline network cyber-physical system by h_a , h_c and l_b , and $\bar{h}_a$, $\bar{h}_c$ and $\bar{l}_b$ stands for their corresponding output transitions. h_a (h_c) stands for a high level action that can make change of the flow at A (C) , which can make change at h_c (h_a) because of the coordination between A and C . B possibly experiences a physical flow change at A and C by the way of the low-level output $\bar{l}_b$. The pipeline network cyber-physical system is modelled in Fig.(2) with Petri net.

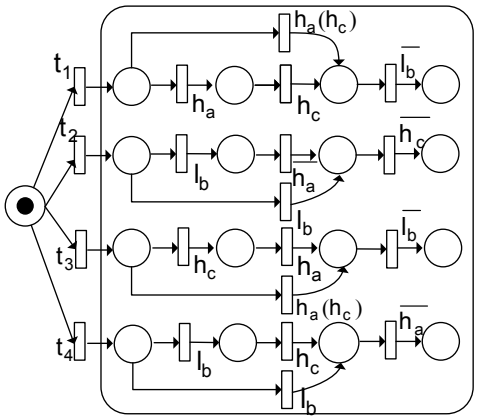

Fig.2 Pipeline system model

C. Analysis of noninterference in pipeline cyber-physical system

The pipeline network cyber-physical system is typical a nondeterministic system. And the system shows that Fig.(1) is made up of interacting LTCs. And the flow of interacting LTCs is dominated by Eq. (1). The pipeline network distribution system and their interconnectivity is nondeterministic non-interference secure.

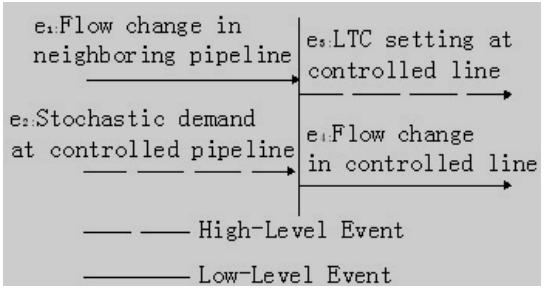

Fig.3 Information flow in the pipeline distribution system

Theorem 1 The pipeline network cyber-physical system is nondeterministic non-interference secure.

Fig.(3) shows the proof, the vital events in the pipeline network cyber-physical system are flow change in the adjacent pipeline, LTC setting at the controlled line, stochastic demand at the controlled pipeline, and flow change in the controlled line. These events are expressed by $e_1 : e_2 : e_3 : e_4$. And e_1 , e_2 , e_3 and e_4 is a low-level input event and a high-level input event and a high-level output event and a low-level output event

respectively. The set of valid traces of the pipeline network system are $\{\{\}, e_1, e_2, e_3, e_1e_4, e_2e_4, e_1e_2e_4, e_2e_3e_4, e_2e_4e_3, e_3e_4, e_1e_4e_3, e_1e_3e_4, e_2e_1e_4, e_1e_2e_4e_3, e_2e_1e_4e_3, e_2e_1e_3e_4 \ldots\}$, where … stands for interleaving of the above listed traces in the pipeline network system[5].

Obviously, there always exists a valid trace σ' for any valid trace σ , such that there is not any same high-level input actions between σ and σ' . Moreover, σ are low-view trace equivalent to σ' . In other words, $(E \setminus_I Act_H) / Act_H \overset{L}{\square} E / Act_H$, E denotes the pipeline network cyber-physical system. Therefore, the system is noninterference secure.

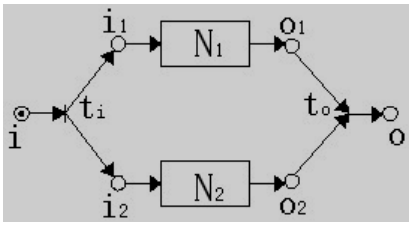

Fig.1 Parallel composition

IV. ANALYSIS PARALLEL COMPOSI-TIONS IN PIPELINE NETWORK SYSTEM

Definition 7 Let $N_1=(S_1,H_1\cup L_1,F_1,m_{01})$, $N_2=(S_2,H_2\cup L_2,F_2,m_{02})$ be two Petri net systems, such that $S_1\cap S_2=\varnothing$ and $(H_1\cup L_1)\cap(H_2\cup L_2)=\varnothing$. For $N=(S,H\cup L,F,m_0)$, if

(1) $S = S_1 \cup S_2 \cup \{i, o\}$

(2) $T = T_1 \cup T_2 \cup \{t_i, t_o\}$, $\{t_i, t_o\} \subseteq \mathrm{L}$

(3) $F = F1 \cup F2 \cup \{(i, t_i), (t_i, i_1), (o_1, t_o), (t_2, o), (t_i, i_2), (o_2, t_o)\}$

Then N is the parallel composition of N_1 and N_2 , we use $N=N_1\|N_2$ to denote the parallel composition. Fig.(4) demonstrates the parallel composition[11].

Theorem 4 Let $N_1=(S_1,H_1\cup L_1,F_1,m_{01})$ and $N_2=(S_2,H_2\cup L_2,F_2,m_{02})$ be two Petri net systems which are nondeterministic noninterference secure. Then $N=N1\|N2$ is nondeterministic noninterference secure if and only if $\forall(s_1',t_1')\in{}^{\cdot}o_1,(s_2',t_2')\in{}^{\cdot}o_2$, if $t_1'\in H$ then $\exists(s_1'',t_1'')\in{}^{\cdot}o_1$ and if $t_2'\in H$ then $\exists(s_2'',t_2'')\in{}^{\cdot}o_1$. Fig.(5) demonstrates the sufficient and necessary conditions for parallel composition .

Proof.

(1) Sufficiency: N is nondeterministic non-interference secure

Assuming $(s_1',t_1')\in{}^{\cdot}o_1, t_1'\in H_1$ and do not exist $(s'',t'')\in{}^{\cdot}o_1$. We consider the transition list $\sigma=t_i\sigma_1t_1't_o\in TS(N)$, where $\sigma_1\in TS(N_1)$. N is not nondeterministic noninterference secure since there is not the corresponding σ'' , such that $next(m_0,\sigma)\overset{L}{\square}next(m_0,\sigma')$. Likewise, the proof is given by the $\sigma=t_i\sigma_2t_2't_o\in TS(N)$, if $\sigma_2\in TS(N_2)$. N is not nondeterministic noninterference secure. So the assumption does not hold.

(2)Necessary: $\forall(s_1',t_1')\in{}^{\cdot}o_1,(s_2',t_2')\in{}^{\cdot}o_2$, if $t_1'\in H$ then $\exists(s_1'',t_1'')\in{}^{\cdot}o_1$ and if $t_2'\in H$ then $\exists(s_2'',t_2'')\in{}^{\cdot}o_1$

Let $\forall\sigma\in TS(N)$, if $\sigma\in TS(N_1)$, there will be a transition sequence σ' , such that $next(m_0,\sigma)\overset{L}{\square}next(m_0,\sigma')$ because N_1 is nondeterministic noninterference secure. Similarly, we can give the proof that if $\sigma\in TS(N_2)$. If $\sigma\notin TS(N_1)$ and $\sigma\notin TS(N_2)$, we suppose $\sigma=t_i\sigma_1t't_o$, where $\sigma_1\in TS(N_1)$. If $t'\in L$, it is obvious that N is nondeterministic noninterference secure. If $t'\in H_1$, according to the assumption, $\exists(s'',t'')\in{}^{\cdot}o_1$, such that $next(m_0,\sigma)\overset{L}{\square}next(m_0,\sigma')$, where $\sigma=t_i\sigma_1t't_o$ and $\sigma=t_i\sigma_1t''t_o$. Since N is sequence composite by place i and o , it is non-deterministic non-interference secure[10]. Therefore, N satisfies non-deterministic non-interference secure.

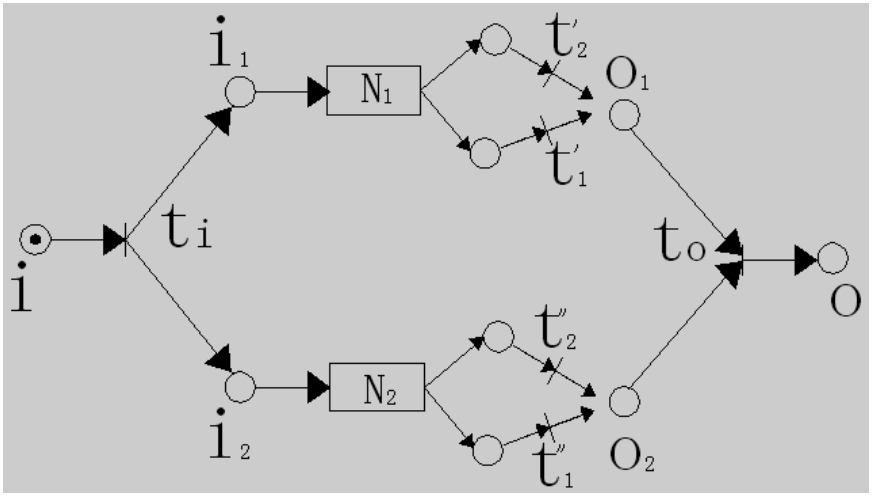

Fig.5 The sufficient and necessary conditions for parallel composition

V. CONCLUSIONS

In this paper, Petri net is a formal tool used for nondeterministic noninterference information flow security model specification in cyber-physical system, and is proved to be applicable to abstract pipeline distribution flow network system. In addition, the method in this paper is given to analyze the nondeterministic noninterference model and its parallel composition in cyber-physical system. Owing to these results, a system designer can connect certain small subsystems confirmed to be nondeterministic noninterference secure to constitute a complicated nondeterministic noninterference secure cyber-physical system.

CONFLICT OF INTEREST

The author confirms that this article content has no conflicts of interest.

ACKNOWLEDGEMENTS

The work was supported by the Natural Science Foundation of Anhui Province, China (Grant No.1508085MF123), and the Key University Science Research Project of Anhui Province, China (Grant No.KJ2015A190).

REFERENCES

[1] T. T. Gamage and B. M. McMillin. "Observing for Changes: Non-Deducibility Based Analysis of Cyber-Physical Systems". In Proceedings of the 3rd International Federation for Information Processing Conference (IFIP WG 11.10). Hanover, NH: Springer Boston, pp. 169–183, April 2009.

[2] E. Lee. "Cyber Physical Systems: Design Challenges. University of California", Berkeley Technical Report No. UCB/EECS-2008-8, 2008.

[3] J. A. Goguen, J. Meseguer. "Security policies and security models". Proc. 1982 IEEE Symposium on Security and Privacy, IEEE Press, pp 11-20, 1982.

[4] J. A. Goguen, J. Meseguer. "Inference control and unwinding". Proc. 1984 IEEE Symposium on Security and Privacy, IEEE Press, pp. 75-86, 1984.

[5] Ravi Akella, Han Tang, Bruce M. McMillin. "Analysis of information flow security in cyber-physical system". International Journal of Critical Infrastructure Protection. 3:157~173, 2010.

[6] Simone Frau, Roberto Gorrieri, Carlo Ferigato. "Petri Net Security Checker: Structural Non-interference at Work". Formal Aspects in Security and Trust, Springer LNCS 5491:210-225, 2009.

[7] N. Busi, R. Gorrieri. "A Survey on NonInterference with Petri Nets". Advanced Course on Petri Nets 2003, Springer LNCS 3098:328-344, 2004.

[8] R. Focardi, R. Gorrieri. "Classification of Security Properties (Part I: Information Flow)"", Foundations of Security Analysis and Design - Tutorial Lectures (R. Focardi and R.Gorrieri, Eds.), Springer LNCS 2171: 331-396, 2001.

[9] Song Chen, Cong-hua Zhou, Shi-guang Ju, Hai-yang Li. "Analysis for the composition of information flow security properties on Petri net". In Proceedings of the 3rd IEEE International Conference on Information Science and Engineering, Hefei, china, Dec, 2010.

[10] R. Focardi, R. Gorrieri. "A Classification of Security Properties". Journal of Computer Security. 3 (1): 5-33, 1995.

[11] Jingming Wang, Huiqun Yu. "Analysis of the Composition of Non-Deducibility in Cyber-Phyiscal Systems". Applied Mathematics & Information Sciences. 8,6, pp. 3137-3143.2014

[12] Jingming Wang, Huiqun Yu. "Sequence compostion analysis of non-interference in cyber-physical system with Petri net". International Journal of Security and its Applications. 8,3, pp. 185-192.2014