International Journal of Security and Its Applications
Vol.8, No.3 (2014), pp. 185-192
http://dx.doi.org/10.14257/ijsia.2014.8.3.20

Sequence Composition Analysis of Noninterference in Cyber-Physical System with Petri Net

Jingming Wang[1, 2], Huiqun Yu[1*] and Chunxia Leng[1]

[1]*Department of Computer Science and Engineering, East China University of Science and Technology, Shanghai 200237, China*
[2]*School of Computer and Information Engineering, Chuzhou University, Anhui 239012, China*
wjmtime@chzu.edu.cn, yhq@ecust.edu.cn, cxleng@ecust.edu.cn

Abstract

Now a considerable challenge to model cyber-physical systems (CPSs) is to represent the cyber and physical level's interactions. Owing to physical behavior and components appended to cyber systems, researchers meet with the difficulty in the analysis and verification of noninterference information security model in CPSs. A method is proposed with Petri net for solving this problem effectively by composing the complex systems with small systems while achieving the noninterference information flow security property. This paper analyzes the noninterference security property and the sequence composition in cyber-physical systems using the method. This study provides a formal method and foundation for exploring information flow security property and its composition in cyber-physical systems.

KeyWords: *Cyber-Physical Systems; Information Flow Security; Petri Net; Noninterference Model*

1. Introduction

In recent years, the design of systems has developed in the direction of cyber-physical system [1]. CPSs are integrations of computation and physical processes [2]. Now Owing to physical behavior and components appended to cyber systems, researchers meet with the difficulty in the analysis and verification of noninterference information security model in CPSs. A considerable challenge to model cyber-physical systems (CPSs) is to represent the cyber and physical level's interactions.

Access control security models only can to solve direct information flow. One better approach to information flow security is to control both the direct and indirect information flow by applying some information flow rules [6], which are called information flow security models, such as noninterference security model discussed in this paper.

Noninterference model was first proposed by Meseguer and Goguen [3-4] and a lot of works about this model were done [5-11]. However, there is little research about the sequence composition of noninterference in cyber-physical systems. This paper has defined the noninterference security model based on Petri net and has analyzed the property in pipeline network system and the noninterference security model will be

* Corresponding author:Huiqun Yu, Ph.D. Professor. Department of Computer Science and Engineering, East China University of Science and Technology. 130 Meilong Road, Shanghai 200237, China. Phone:+86-21-64253546 Fax:+86-21-6425 2984. Email:yhq@ecust.edu.cn.

ISSN: 1738-9976 IJSIA

preserved after sequence composition.

2. Basic Definitions

2.1. Petri Net

As a formal tool with rigorous semantics, Petri net can be efficiently used to model and verify the security properties of system models [4-7].

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

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

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

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

A pair (N,m_0) is a net system, where N is a net and m_0 is a marking of N, which is called initial marking in general. With abuse of notation, (S,T,F,m_0) is used to denote the Petri net system.

2.2. Operations on Petri Net

This paper aims to analyze multilevel systems that can perform different levels of actions. For example, the interaction of the system with high-level actions represents the interaction with high level users and the interaction of the system with low-level actions represents the interaction with low level users. This paper is to verify if the interplay between the high-level user and the high part of the system can affect a low-level user's view of the system.

Thereby, the set of transitions of Petri net is partitioned into two disjointed subsets: the set of high level transitions denoted by H and the set of low level transitions denoted by L, we use (S,L,H,F,m_0) to denote the net system mentioned above.

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

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

For a non-determined system the result statement will not be unique after the firing of a transition of a net system $N=(S,H\cup L,F,m_0)$. We call it result statement set denoted by $next(m_0,\sigma),\ \sigma\in TS(N).$ However, for determined systems the result statement is unique, denoted by $step(m_0,\sigma)$.

Definition 4 Net system $N=(S,H\cup L,F,m_0)$, $m\in[m_0\rangle$, $View_L(m)=\{(s,m(s))\mid\exists t\in L,Q,Q'\in 2^{S},(Q,t,Q')\in F\wedge s\in Q\}$.

Two statements of Petri net are low-level equal if the tokens of all places are same from a low-level user's view.

Definition 5 To a net system $N=(S,H\cup L,F,m_0)$, two statements are low-level equal, iff: $\forall m_1,m_2\in[m_0\rangle, m_1\overset{L}{\sqcap}m_2$ iff $View_L(m_1)=View_L(m_2)$

Definition 6 To a net system $N=(S,H\cup L,F,m_0)$, two results statement sets are low-level equal, if and only if: $\forall A,B\subseteq[m_0\rangle, A \overset{L}{\square} B, iff\ \exists m_1\in A, m_2\in B, s.t.\ View_L(m_1)=View_L(m_2)$

3. Model the Noninterference Property in Cyber-physical System

3.1. The Definition of Noninterference Model

Generally, if low level users observe that information flows from high level users to low level users, then information confidentiality of system can be deduce by the low level observers. The original definition of noninterference security model is defined for deterministic systems, now the model is extended for nondeterministic systems (NNI).

The generalization is as follows. The high level does not interfere with the low level if and only if for any trace σ, there is always a trace σ' with no same high level input actions. Furthermore, σ and σ' are low view trace equivalent. NNI is defined as follows based on Petri net.

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

Where, the function of the operation of \ is similar to the operation in process algebra [10], Act_h represents the set of high level actions, I represents the set of input actions.

3.2. Abstract Pipeline Cyber-Physical System

Pipeline cyber-physical system, as one of typical cyber-physical systems, provides rich computational and physical processes and their interactivity [5]. Flow control systems (FCSs) in the system automate or control the state of water or other fluid in the pipeline. LTCs execute two commands of raise and lower the flow.

Figure 1 shows a water distribution system network with three LTCs that control the sub-networks A, B, and C respectively, which are geographically separated in large distances. Either of the raise and lower flow commands will affect neighbouring sub-networks necessarily, resulting in observable actions at location A and location B in the network of pipes, and the following invariant holds [5]:

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

Where Va, Vb and Vc represent the changes or volumes of water flow of the pipes controlled at A, B, and C respectively.

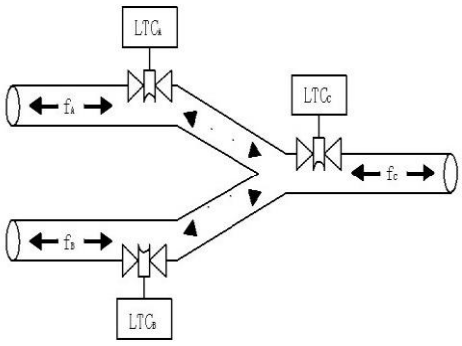

Figure 1. Pipeline Network with Three sub-networks Controlled by LTCs

As shown in Figure 7, the transitions in the system are represented by ^{h}a, ^{h}c and ^{l}b, and $\bar{h}a$, $\bar{h}c$ and $\bar{l}b$ are their corresponding output. Here, ^{h}a (^{h}c) represents a high level

action that changes the flow at A (C), which results in a change at h_c (h_a) due to the coordination between A and C. B possibly experiences a change in physical flow at A and C in the form of a low-level output, $\bar{l}_b$. The gas pipeline system is modelled in Fig. 7 using Petri net.

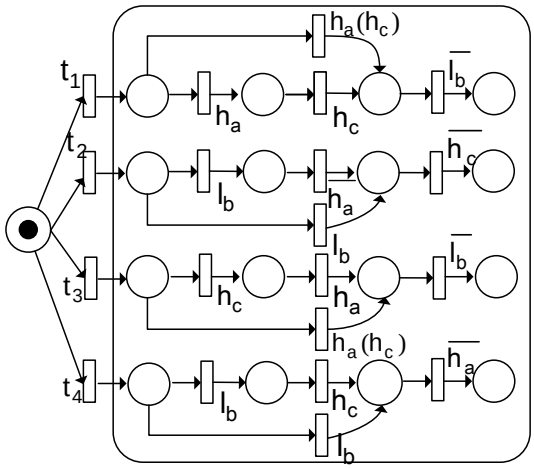

Figure 2. Pipeline System Model based on Petri Net

3.3. Analysis of NNI in Pipeline cyber-physical System

The pipeline cyber-physical system, which is a non-deterministic system, shown in Figure 1 consists of interacting LTCs whose flow is governed by Eq. (1). The pipeline distribution system with FCSs and their interconnectivity is NNI secure.

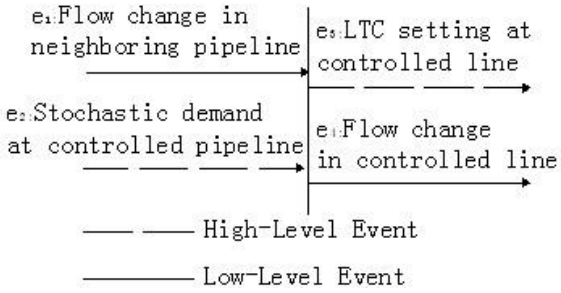

Figure 3. Information Flow in the Pipeline Distribution System

Theorem 1 The pipeline newwork system is NNI secure.

Proof. As shown in Figure 3, the significant events in the pipeline system are flow change in the neighbouring pipeline, stochastic demand at the controlled pipeline, LTC setting at the controlled line, and flow change in the controlled line, which are represented by e_1: e_2:e_3: e_4. And e_1 is a low-level input event, e_2 is a high-level input event, e_3 is a high-level output event, and e_4 is a low-level output event. The set of valid traces of the system are {{}, e_1, e_2, e_3, e_1e_4, e_2e_4, e_3e_4, $e_1e_4e_3$, $e_1e_3e_4$, $e_1e_2e_4$, $e_2e_3e_4$, $e_2e_4e_3$, $e_2e_1e_4$, $e_1e_2e_4e_3$, $e_2e_1e_4e_3$, $e_2e_1e_3e_4$ …} where … represents interleavings of listed traces in the system[5].

It is obvious that for any valid trace σ, there always exists a valid trace σ', such that there is no same high-level input actions between σ and σ'. Furthermore, σ and σ' are low-view trace equivalent. That is to say, $(E \setminus_I Act_H) / Act_H \overset{\Pi}{=} E / Act_H$, the pipeline network system denoted by E. So, the system is NNI secure.

4. Analysis the Sequence Composition of Pipeline Network Distribution System

Sequence composition [11] is formed by connecting two systems S_1 and S_2, and some of S1's output events become S2's input events. The formal definition of feedback composition is as follows.

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) $S = S_1 \cup S_2$

(2) $H=H_1\cup H_2$, $L=L_1\cup L_2\cup\{t\}$

(3) $F=F_1\cup F_2\cup\{(o_1,t),(t,i_2)\}$

We say N is the sequence composition of N_1 and N_2, denoted by $N=N1\square N2$. Figure 3 demonstrates the composition.

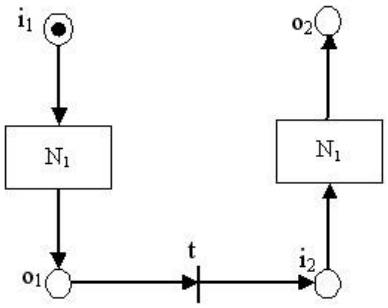

Figure 3. Sequence Composition

Theorem 2 A system composed with nondeterministic noninterference secure subsystems like pipeline distribution system by sequence composition is also nondeterministic noninterference secure.

Proof. The proof of noninterference sequence composition will be done by induction on the number of subsystems.

Base case:

It is obvious that a system combined by only one subsystem is nondeterministic noninterference secure. This follows directly from the premise of the theorem, because every subsystem is nondeterministic noninterference secure.

Induction hypothesis:

We can suppose that system composed of k nondeterministic noninterference secure subsystems by sequence composition is nondeterministic noninterference secure.

Induction step:

Now we can consider a composite system which is comprised of k+1 subsystems. Without loss of generality, we can consider that the first subsystem is composed of the k previously composed system and the second subsystem is the new system that is to be added to the system. Let Act_1 and Act_2 be the sets of events for the first subsystem and the second subsystem respectively.

By the definition of nondeterministic noninterference model, proving the composed system is nondeterministic noninterference secure is equal to prove there exists a

trace σ'' of the composed system for any trace σ of the composed system, such that

$$T(\sigma / Act_H) \overset{L}{\sqsubset} T(\sigma''/ Act_H) \wedge \sigma''/ (Act_L \cup (Act_H \cap I)) = \varnothing.$$

We can construct a valid trace σ'' by two steps.

First step, we can construct a valid trace σ', such that:

(1) $\sigma'/ Act_2 = \sigma_1$, such that $T(\sigma / (Act_{1H} \cup Act_2)) \overset{L}{\sqsubset} T(\sigma_1 / (Act_{1H} \cup Act_2)) \wedge \sigma_1 / (Act_{1L} \cup (Act_{1H} \cap I)) = \varnothing.$

(2) $\sigma'/ Act_1 = \sigma / Act_1$

Condition (1) is guaranteed by the induction hypothesis, because the first subsystem is nondeterministic noninterference secure. Condition (2) guarantees that all the events or actions in the second subsystem are left unchanged. This condition is satisfied because σ' could not affect any events in Act_2.

Second step, we can construct the trace σ'', such that:

(3) $\sigma''/ Act_1 = \sigma_2$, such that $T(\sigma'/ (Act_1 \cup Act_{2H})) \overset{L}{\sqsubset} T(\sigma_2 / Act_{2H}) \wedge \sigma_2 / (Act_{2H} \cap I)) = \varnothing.$

(4) $\sigma''/ Act_2 = \sigma'/ Act_2$

Condition (3) is guaranteed because the second component is nondeterministic noninterference secure. Condition (4) guarantees all other events are left unchanged. The output events of the second subsystem maybe changed by this construction method, but because the composition method involves no feedback in the composite system, so it will not have effect about the input/output events of the first subsystem.

Therefore, we can draw the conclusion that a system composed with nondeterministic noninterference secure subsystems is also nondeterministic noninterference secure by the method of sequence composition.

5. Conclusions

In this paper, Petri net is used as a formal tool for nondeterministic noninterference security model specification of cyber-physical system and is shown to be applicable to abstract pipeline distribution flow network system. Furthermore, this paper gives the method to analyze the nondeterministic noninterference model and the conclusion about the sequence composition of nondeterministic noninterference model in cyber-physical system. These results allow a system designer to connect certain small subsystems verified to be nondeterministic noninterference secure to form a complex nondeterministic noninterference secure cyber-physical system.

Acknowledgements

The work is supported in part by the NSF of China under grants No. 61173048, and NSF of Anhui province, China under Grant No. KJ2011ZD06, and NSF of Chuzhou University, Anhui province, China under grant No. 2013RC004 and 2012qd08.

References

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

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

[3] J. A. Goguen and J. Meseguer, "Security policies and security models", Proc. 1982 IEEE Symposium on Security and Privacy, IEEE Press, **(1982)**, pp. 11-20.
[4] J. A. Goguen and J. Meseguer, "Inference control and unwinding", Proc. 1984 IEEE Symposium on Security and Privacy, IEEE Press, **(1984)**, pp. 75-86.
[5] R. Akella, H. Tang and B. M. McMillin, "Analysis of information flow security in cyber-physical system", Analysis of information flow security in cyber-physical systems, International Journal of Critical Infrastructure Protection, vol. 3, **(2010)**, pp. 157-173.
[6] S. Frau, R. Gorrieri and C. Ferigato, "Petri Net Security Checker: Structural Non-interference at Work", Formal Aspects in Security and Trust, Springer LNCS, vol. 5491, **(2009)**, pp. 210-225.
[7] N. Busi and R. Gorrieri, "A Survey on NonInterference with Petri Nets", Advanced Course on Petri Nets 2003, Springer LNCS 3098:328-344, **(2004)**.
[8] R. Focardi and 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] S. Chen, C.-H. Zhou, S.-G. Ju and H.-Y. Li, "Analysis for the composition of information flow security properties on Petri net", Proceedings of the 3rd IEEE International Conference on Information Science and Engineering, Hefei, China, **(2010)** December.
[10] R. Focardi and R. Gorrieri, "A Classification of Security Properties", Journal of Computer Security, vol. 3, no. 1, **(1995)**, pp. 5-33.
[11] A. Zakinthinos, "On the Composition of Security Properties", Ph.D. dissertation, University of Toronto, Toronto, Ontario, **(1996)**.

Corresponding author: Huiqun YU, Ph.D., Professor.
Department of Computer Science and Engineering,
East China University of Science and Technology, Shanghai, China
130 Meilong Road, Shanghai 200237, China
Email:yhq@ecust.edu.cn

