Analysis of Noninterference in Water Distribution System Using Petri Net

Huiqun YU[I], Chunxia Leng[i], Jingming WANG[1, 2], Guilin CHEN[2]

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

yhq@ecust.edu.cn, cxleng@ecust.edu.cn, wjmtime@chzu.edu.cn, glchen@chzu.edu.cn

Abstract. Cyber-physical systems (CPSs) are one of the most important system design areas. A considerable challenge to model theses systems is how to represent the interactions between the cyber level and the physical level. Now researchers are confronted with the difficulty in the analysis and verification of information confidentiality in the complex CPSs owing to physical observable behavior and physical components appended to cyber systems. A technique for solving this problem effectively by using some simple or small systems to compose the complex systems while achieving the confidentiality of the composite system based on Petri net is proposed. This paper has analyzed the noninterference security property and the cascade composition in water distribution system based on the technique. This study is to provide a formal method and foundation for exploring the confidentiality and information security in cyber-physical systems composition.

Keywords: Cyber-Physical Systems; Information Flow Security; Petri Net; Noninterference Model; Water Distribution System

1 Introduction

In recent years, the design of systems has developed in the area of CPSs [1]. CPSs are integrations of computation and physical processes [2]. Now researchers are confronted with the analysis and verification of confidentiality of complex CPSs owing to physical observable behavior and physical components appended to cyber systems. A considerable difficulty to analyze security model is the representation of interactions between physical level and cyber level.

Access control security modes are unsatisfactory since they are only to solve direct information flow. One better approach to computer security is to control both the direct and indirect information by applying some information flow rules [6], which are called information flow security models.

Noninterference model was first proposed by Meseguer and Goguen [3-4]. A lot

Corresponding author: Huiqun Yu, Ph.D., Professor, 130 Meilong Road, Shanghai 200237, China. Email: yhq@ecust.edu.cn.

of works about this property were done [5-11]. However, there is little research for cyber-physical systems on noninterference composition. This paper has defined the noninterference model based on Petri net and has analyzed the property in water distribution system, and which will be preserved after cascade 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 $S \cap T = 0$

(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 in and a places , $m(s)$ denotes the tokens number of places .

A pair (N, m_o) is a net system, where N is a net and m_o is a marking of N, which is called initial marking in general. With abuse of notation, (S,T,F,m_o) 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 $(S,L,H,F,m0)$ to denote the net system mentioned above.

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

$$e/H = e$$

$$\{$$

$$e \mid L = e$$

$$gtIH = (5 \; I \; H)t \; t \in L$$

$$gtIL =$$

$$5/H \; teH \qquad \{(g \; I \; L)t \; t \; c \; H$$

$$g \; I \; L \quad t \; e \; L$$

For a non-determined system the result statement will not be unique after the firing of a transition of a net system $N=(S,HuL,F,m0)$. We call it result statement set

denoted by $next(m_0, a), o\text{-}ETS(N)$. However, for determined systems the result statement is unique, denoted by *step(mo,o-)* .

Definition 4 Net system $N=(S,HuL,F,m0), mE[mo), View_L(m) = \{(s,m(s))$ 3t E $L,Q,Q'E2^s,(Q,t,Q^1)EF As EQ\}$.

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 $N=(S,HuL,F,m0)$, two statements are low-level equal, , m_2 E $[m_o)$, $m_l\ ^L m_2$ *iff* $View_L(m_i) = View_L(m_2)$

Definition 6 To a net system $N=(S,HuL,F,m0)$, two results statement sets are low-level equal, if and only if: $V A,Bc[m_o),A\ L\ B,ff3m,$ EA,m_2 EB, *s.t.* $View_L(m_i)=View_L(m_2)$

3 Model the noninterference property in water distribution system

3.1 The definition of noninterference model

If low level users observe that information flows from high level users to low level users, then confidentiality of system can be deduce by the low level observer.

The original definition 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 a , there is always a trace a with no same high level input actions. Furthermore, a and a' are low view trace equivalent. NNI is defined as follows based on Petri net.

Definition 6 $E\ e\ NNI <=> (E \setminus Act_H) / Act_H\ L\ E\ I\ Act_H$

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 water distribution system

Water distribution 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.

Fig.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:

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

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

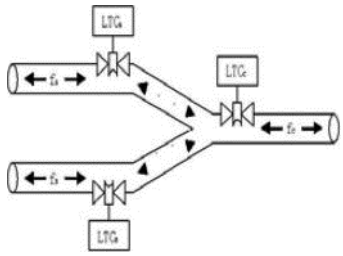

Fig.1 . Pipeline network with three sub-networks controlled by LTCs

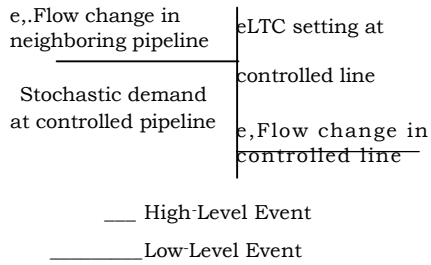

Fig.2. Information flow in the water distribution system

3.3 Analysis of NNI in water distribution system

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

Theorem 1 The water flow in the pipeline system is NNI secure.

Proof. As shown in Fig.2, 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_l: e_2:e_3: ez_t. And e_l 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_l, e2, e3, eie4, e2e4, e3e4, e1e4e3, e1e3e4, e1e2e4, e2e3e4, $e_2e_4e_3$, $e_2e_ie_4$, eie2e4e3, e2e1e4e3, e2e1e3e4 ...} where ... represents interleavings of listed traces in the system.

It is obvious that for any valid trace 0- , there always exists a valid trace *0.* , such that there is no same high-level input actions between *c* and 0- . Furthermore,

a and *CT* are low-view trace equivalent. That is to say, *(E \ Act H) / Act„* = *E / Act,* the water distribution system denoted by E. So, the system is NNI secure.

4 Analysis the composition for water distribution system

Feedback free or Cascade composition [11] is formed by connecting two systems S_i and S2, and some of S 1's output events become S2's input events. The formal definition of feedback composition is as follows.

Definition 7 Let N_i =(s_i LA_I ,Fi ,mo1) , N_2=(s_2,H_2(.)1,2,F_2,01_{02}) be two Petri net systems, such that Si nS2 =0 and (H_i)*n(H 2uL2)=0.* For *N=(S,HuL,F,m0),* if

(1) *S= Sl* u S2 (2) H=H_1uH_2 , *L=L1uL2o{t}* (3) *F=F1uF2o{(O1,t),(t,i2)}*

We say *N* is the sequence composition of N_1 and N_2 , denoted by *N=N1.N2* . Fig. 3 demonstrates the composition.

Theorem 2 A system composed with NNI secure subsystems like water distribution system by feedback free composition is also NNI secure.

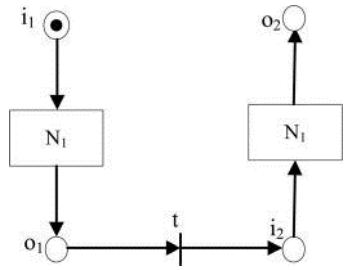

Fig.3. Cascade composition

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

Base case:

One subsystem is NNI secure. This follows directly from the premise of the theorem.

Induction hypothesis:

system composed of k NNI secure subsystems by cascade composition is NNI secure.

Induction step:

Consider a system comprised of k+1 subsystems. Without loss of generality, consider the first subsystem to be composed of the k previously composed system and the second subsystem to be the new system that is added to the system. Let Act_i be the set of events for the first subsystem and Act_2 be the set of events for the second subsystem.

By the definition of NNI, proving the composed system is NNI secure is equal to prove there exists a trace a '. of the composed system for any trace *a* of the composed

system, such that *T (vI Act$_H$) L T (cr "I Act$_H$)* A *cr "I (Act$_L$ u (Act$_H$ n I))* = 0.

We will construct a valid trace *a "* with the following two steps.

First step, construct the valid trace *o"* such that:

'I Act$_2$ = a$_1$, such that *T(o- I (Act$_{iH}$ u Act$_2$))^{L} o- T(o- $_1$ / (Act$_{1H}$ u Act$_2$)) A o- / (Act$_{IL}$ v (Act$_{IH}$* n *I)) = 0.* (1) (2)0- v Act$_1$ = a I *Act$_1$*

Condition (1) is guaranteed by the induction hypothesis of the first subsystem is NNI secure. Condition (2) ensures that all the events in the second subsystem are left unchanged. This condition is satisfied because 0- could not affect any events in Act_2. Second step, construct the trace *c"* such that:

(3) *ct* "I *Act$_1$* = cr$_2$, such that *T(o- 'I (Act$_s$ u Act$_{2H}$))L T(o-$_2$ I Act$_{2H}$) A o-$_2$ / (Act$_{2H}$ n I)) = 0.* **(4)** *a "1 Act$_2$ = 6'l Act$_2$*

Condition (3) is guaranteed because the second component is non-interference secure. Condition (4) ensures that all other events are unchanged. This construction may change the output events of the second subsystem, but because the composition involves no feedback, it will have no effect on the input or output events of the first subsystem. Therefore, by induction, a system composed with NNI secure subsystems is also NNI secure by cascade composition.

5 Conclusions

In this paper, Petri net provides a rigorous formal method for CPSs security model specification and is shown to be applicable to abstract water distribution flow network system. The results allow a system designer to connect certain small subsystems verified to be NNI secure to form a NNI secure cyber-physical system. We believe that the present study provides a formal method and the foundation for exploring confidentiality and information security in CPSs.

6 Acknowledgements

The work was supported by the NSF of China under grants No. 60773094, 60473055 and 61173048, Shanghai Shuguang Program under grant No. 07SG32, and the NSF of high education of Anhui province, China under Grant No. KJ2011Z279, and the NSF of Chuzhou University, Anhui, China under Grant No.2010kj008Z.

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. Analysis of information flow security in cyber-physical systems. 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. A. Zakinthinos. On The Composition of Security Properties. Ph.D. dissertation, University of Toronto, Toronto. Ontario. 1996.