Analysis of Non-Deducibility in Water Distribution System Using Security Process Algebra

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

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

Abstract. Cyber-physical systems (CPSs) are integrations of computation and physical processes. A considerable difficulty to model CPSs is how to represent the interactions between the cyber and physical level. Now researchers are confronted with the difficulty in the analysis and verification of information confidentiality in CPSs because of 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 by preserving that of small systems based on security process algebra (SPA) is proposed. This paper analyzes the non-deducibility security property and the sequence 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; Security Process Algebra; Non-Deducibility; 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]. A considerable difficulty to analyze security model in CPSs is the representation of interactions between physical and cyber level.

One better approach to computer security is to control both the direct and indirect information by applying some information flow rules [3], which are called information flow security models, one of the models is non-deducibility model.

In 1986, non-deducibility [4] property was first proposed by Sutherland. Researchers also did a lot of works in recent years, such as [1] [7]. However, there is little SPA-based research on ND composition and its application in CPSs.

This paper has analyzed the non-deducibility security property in water

distribution system, which is a typical application of CPSs. Furthermore, this paper has given the conditions in which the property will be preserved after sequence composition, and provided the proof. The main contribution is to provide a formal method and foundation for studying information confidentiality and security in CPSs.

The rest paper is organized as follows:

Section 2 introduces some basic definitions of SPA. In section 3, the ND property of the water distribution system is analyzed. Section 4 elaborates on the application of the sequence composition to ND security model in water distribution system.

2 Basic definitions

2.1 Security process algebra

In the following, systems will be specified using SPA. The syntax of SPA is based on the following elements:

0 A set $/ = \{a,b,\bullet\bullet\}$ of input actions, a set $o =$ $\bullet\bullet.\}$ of output actions; $r = ruo$ is called the set of visible actions, ranged over by a .

o A function $\bullet : \quad$, such that $aelaE0$ and $,T,EoN=a1$

0 Two sets Act_H and Act_L of high and low level actions which are closed with regard to function • (Act_i, = Act_H , $Act_L = Act_L$). Furthermore, they form a covering of r and they are disjoint.

® A set $Act = £ u \{r\}$ of actions (z is the internal and invisible action), ranged over by p .

0 A set K of constants, ranged over by Z.

The syntax of SPA agents is defined as follows:

$$E := 0 \mid p.E \mid E + E \mid E \mid E \backslash\backslash L \mid E[f] \mid Z$$

where L c r and $f : Act \to Act$ is such that $f(a) = f(a)$ and $f(r) = z$. For every constant Z there must be the corresponding definition: z . Moreover, every E must be guarded on constants.

The only difference from calculus of communication system (CCS) is the restriction operator \\. Intuitively, E\\L can execute all the actions E is able to do, provided that they do not belong to **L. In** CCS the corresponding operator \ requires that the actions do not belong to L u L .

In addition, we define two auxiliary operators because they are useful in characterizing security models in an algebraic style.

$E[f]$ where $f(x) = \begin{cases} x & \text{if } x \in L \\ \end{cases}$ $E\backslash L = E\backslash\backslash L \cup I$

where, $E)_I L$ requires that that actions of E do not belong to $L \cup I$ and E/L turns all the actions in L into internal actions r .

2.1 Operational semantics

Let be the set of SPA agents, ranged over by E or F. Let $L(E)$ denotes the set of the actions occurring syntactically in E. The set of high level agents is defined as $\stackrel{def}{=} 1E\,e\quad G(E)E\,Act_H\{r\}$ and low level one is $^{L\,def} = \{E \mathbf{E} \mathbf{I}\, G(E)\mathrm{E}\, ACt_L\, V\{r\}\}$, respectively, and $S_H \cup L$.

$Act, -*)$ is the operational semantics of SPA, where the states are the terms of the algebra and the transitions relation —)c x $Act\,x$ is defined by structural induction as the least relation generated by the axioms and inference rules shown in Fig.2 (part).

The ND property is based on some notion of low view and equivalence relation. The low view of a transition sequence is nothing but the subsequence where high level transitions are discarded and two agents are equivalent if they have the same execution traces.

Definition 2 The expression $E\,E'$ is an abbreviation for $,(\,)^*_E\, f,;(4)^*_E,$, where (±,; denotes a sequence of r transitions. Let $a = eve,._E$ be a sequence of actions, then $_{EqE'}$ if and only if there exists e such that$E^{6'}$.

We say that E' is reachable from $E\,if3.\,ELL\text{-}$, denoted by $E\,E'$.

Definition 3 For any $E\,e$, the set T(E) of traces associated with E is defined as follows: T(E)= ca $_{\cdot}13E'\,EL\,EI$. We say that E and F are trace equivalence if and only if T(E) =T(F), which is denoted by $E\,F\,F$.

2.3 The definition of sequence composition

Sequence composition [7] is formed by connecting two systems S_i and S2, and passing some of S1 's output events to S2's input events. In this method larger and larger cascade systems can be constructed.

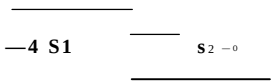

Fig. 1. Sequence composition

3 Model and analysis of water distribution system

3.1 The definition ND security model

If information flows from high level users to low level users when the low level users

observe something which is connected with high level user activity, then confidential information of system can be deduce by an observer.

In 1986, ND [4] property was first proposed by Sutherland. ND is originally defined as follows: given two functions fl and 12, a state transition sequences set E and a particular state sequence with a known output on fl (), then information will flow from fl() to f2() , if and only if, (3 $_{cre}$E)(a f2^{1} (6),(f_2(6)#) .

Theoreml Information will not flow from fl to 1'2 if there does not exist any unique output produced by function fl.

Proof. The negation of the equation describes the requirement.

1

-1{(30- E f_2 (-Z-) # *2),* E : *(U)* = *(cr),(f2(o-)# .ff-)1= (3a* E E)(3w.: f_2 (a.) w *2),* E : (a) = (o-) (f_2 (a) W -w)

=CV.T€EXV"Ef2^{1} *(z)*#a),·-{ecrEZ:A(c)=.4*(')*(f2((r)#"2")}=CVa€EXV·E*f2*$^{/}$(-^{1}9#A),^{3}cEE:··{ii (c)=.4(c)(f2(^{0}")#'^{2}))

= E V f2 1*(-Z-)* # *2), 3a* E : *fl (a) = f_i(a)* $_{A}$ (f_2 (a) = *-z-)*

Definition 4 Formally, a net system is ND secure if and only if

$$(\Pi_i \mathrm{lE})1\ Act_{,,}z_{,,,,,,}(11,1E)1\ Act_{,,}$$

Where, *Act* $_{HO}$ represents the set of high level outputs, $_{may}$ represents the test equivalence, ande_{l} , $_{u2}$ represent all high level processes.

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. 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:

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

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

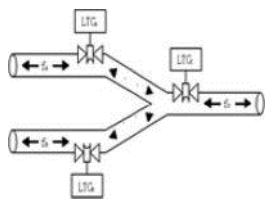

Fig.2. Pipeline network with three sub-networks controlled by LTCs

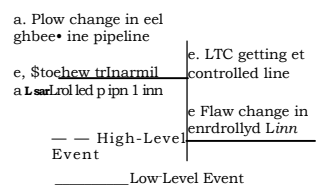

Fig.3. Information flow in the water distribution system

3.3 Analysis of ND **in water distribution system** Theorem

1 The water distribution net system is ND 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: e_4. 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, e_2, e_3, e_ie_4, e_2e_4, e_3e_4, $e_ie_4e_3$, $e_ie_3e_4$, e_l e_2e_4, $e_2e_3e_4$, $e_2e_4e_3$, $e_2e_ie_4$, $e_ie_2e_4e_3$, $e_2e_ie_4e_3$, e2eie3e4 ...} where ... represents interleavings of listed traces in the system.

It is obvious that the system has only one high level event. For any valid trace a^-, there always exists a valid trace a', such that there is no any high-level input event in 0- . Furthermore, c and are low-view trace equivalent. Therefore, the water distribution system is ND secure.

4 Analysis of sequence composition in water distribution system

Theorem 2 A system composed with ND secure subsystems like water distribution system by sequence composition is also ND secure.

Proof. The proof will be done by induction on the number of subsystems.
Base case:
One subsystem is ND secure. This follows directly from the premise of the theorem.
Induction hypothesis:
A system composed of k ND secure subsystems is also ND 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 ND, proving the composed system is ND secure is equal to prove there exists a trace of the composed system for any trace o^- of the composed system, such that $T(6 / Act_H) = T(6 "I Act_H)$.

We will construct a valid trace 6 ^ with the following two steps.

First step, construct the valid trace a' such that:

(1) $a 'I Act_2 =$, such that $T(cr I (Act_{lH} v Act_2))$ $T(cr, I (Act_{,H} u Act_2))$. (2) $Act_i = a / Act,$

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

(3) $a "I Act_1 = a_2,$ such that $T(o^- 'I (Act, u Act_{2H})) _{fr} T(o^-_2 / Act_{2H})$. (4) $a "I Act_2 = a 'I Act_2$

Condition (3) is guaranteed because the second component is ND 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. So, a system composed with ND secure subsystems is also ND secure.

5 Conclusions

In this paper, SPA provides a rigorous formal method for CPSs security model specification and is shown to be applicable to abstract water distribution flow network system. Sequence composition of ND in water distribution system is elaborated on SPA. The results allow a system designer to connect small subsystems verified to be ND secure to form a ND secure cyber-physical system. We believe that the present study provides a formal method and 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, April 2009, pp. 169-183.
2. E. Lee. Cyber Physical Systems: Design Challenges. University of California, Berkeley Technical Report No. UCB/EECS-2008-8, 2008.
34. R. Focardi, R. Gorrieri. The compositional security checker: A tool for the verification of information flow security properties. IEEE Transactions on Software Engineering, 1997, 27: 550-571.
4. D. Sutherland. A model of information. In Proceeding of the 9th National Computer. Security Conference, Baltimore, MD, September 1986, pp. 175-183.
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 Infrastructu- re Protection .2010, 3, 157-173.
6. 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.
7. 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.