Formal analysis and verification of industrial control system security via timed automata

Wang Guoqing[1], Zhuang Lei[1], Liu Taotao[1], Li Shuxia[1], Yang Sijin[1], Lan Julong[2]
[1]School of Information Engineering, Zhengzhou University
[2]China National Digital Switching System Engineering & Technological R&D Center

三等奖

Abstract

The industrial Internet of Things (IIoT) can facilitate industrial upgrading, intelligent manufacturing, and lean production. Industrial control system (ICS) is a vital support mechanism for many key technologies in the IIoT. However, natural defects in the ICS network security mechanism and the susceptibility of the programmable logic controller (PLC) program to malicious attack pose a threat to the safety of national infrastructure equipment. To improve the security of the underlying equipment in ICS, a model checking method based on timed automata is proposed in this work, which can effectively model the control process and accurately simulate the system state when incorporating time factors. Formal analysis of the ICS and PLC is then conducted to formulate malware detection rules which can constrain the normal behavior of the system. The model checking tool UPPAAL is then used to verify the properties by detecting whether there is an exception in the system and determine the behavior of malware through counter-examples. The chemical reaction control system in Tennessee-Eastman process is taken as an example to carry out modeling, characterization, and verification, and can effectively detect multiple patterns of malware and propose relevant security policy recommendations.

Proposed Method

1.Research idea

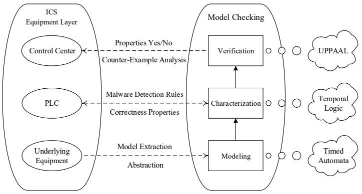

Figure 1. Model checking framework of ICS equipment layer

2. Implementation process

1）Modeling of ICS nased on timed automata

In model checking of ICS, the main concern is the value of variables in the system (including input variables, output variables, and clock variables) and their properties.

ICS state：State σ is defined as a mapping relationship between variables and values in ICS, where

$$\sigma: V \rightarrow D$$

V is the set of variables. D is the set of values. $\sigma(V')$ represents the values of some variables in state σ.

Timed automata：The states are modeled as locations and the state transitions are modeled as edge transitions, in which time can be used to model the control process.

ICS model：ICS model $\xi = (V, C, Ch, L, L_0, S, P, F, I, E)$.

2）Temporal logic representations of properties

Temporal logic is used to describe the state transition sequence in the system and to express time implicitly through semantics.

ICS to be attacked by malware：

Controlling output signal (M1): Malware directly controls part of the output variables, causing abnormal behavior of the equipment itself.

Manufacturing equipment conflict (M2): Malware destroys the security lock, and makes the mutually exclusive process concurrent.

Tampering control logic (M3): Malware changes the logic relationship by tampering with the control logic of PLC.

Denial of service attack (M4): Malware adds a conditional branch to the system.

Design strategies of attack modes：

Threshold, conflict, logic, liveness and availability strategies

3）Verification by model checking tool UPPAAL

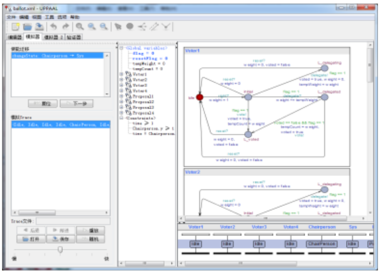

Figure 2. Verification

Experiment

1. Case introduction

Tennessee-Eastman (TE) process is a model for testing continuous process control methods. Based on the abstraction of a real chemical system, it can simulate the impact of different attacks on the system in ICS security research. The TE process consists of five components: a condenser, reactor, gas-liquid separator, stripper, and circulating compressor.

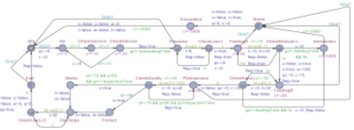

Figure 3. The main model of CRCS (System)

1）Threshold constraints

P1：A[] w==0 or w==100

2）Conflict constraints

P2：A[] !(x and y)

P3：A[] !(u and v)

P4：A[] !((x or y) and (u or v))

P5：A[] y imply w==100

3）Logic constraints

P6：A[] (System.End and !l) imply (!u and !v)

P7：A[] (System.FeedingB and l and m) imply !x

P8：A[] (System.CheckQuality and l and m and h) imply q>=70

P9：A[] u imply q>=90

4）Liveness constraints

P10：E<> s and (u or v)

P11：!s --> !x and !y and !u and (!v or (v and System.c<=5000))

P12：A[] System.Intervention imply gc>=5000

5）Availability constraints

P13：A[] not deadlock

2. Verification Results

Table 1. Model checking verification results in UPPAAL

规约性质	时间/s	内存/KB	验证结果
P1	0.248	31556	满足
P2	0.252	31568	满足
P3	0.282	31556	满足
P4	0.248	31556	满足
P5	0.220	31568	满足
P6	0.280	31568	满足
P7	0.218	31552	满足
P8	0.282	31552	满足
P9	0.992	31560	满足
P10	0.020	31562	满足
P11	0.281	31020	满足
P12	0.284	30252	满足
P13	1.218	31616	满足

3. Counter Example Analysis and System Improvement

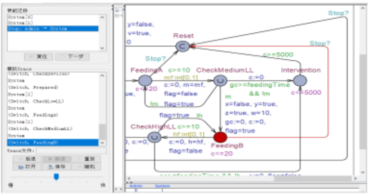

Figure 4. The counterexample of P5 in CRCS with M1

Table 2. Model checking verification results of malware
(S: Satisfied, US: Unsatisfied)

	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11	P12	P13
M1	US	S	S	S	US	S	S	S	S	S	S	S	S
M2	S	US	S	S	S	S	US	S	S	US	US	S	US
M3	S	S	S	S	S	S	S	US	US	S	S	S	S
M4	S	US	US	US	US	US	US	US	US	US	US	US	S

Conclusion

ICS equipment security in the IIoT will usually only analyze the PLC program itself, ignoring the modeling combined with the control process. Based on the above analysis, a method of ICS equipment security model checking based on timed automata was proposed in this work. Timed automata are employed for system modeling, temporal logic is used in property characterization, and UPPAAL is used to verify the system. Contrasting from the general model checking work, according to the security requirements of ICS equipment, the design strategies of five kinds of properties which can restrict normal behavior were emphatically studied, and the anomalies detected were then used to judge malicious attacks.

References

[1] L. Lemaire, J. Vossaert. J. Jansen, "A logic-based framework for the security analysis of industrial control systems," Autom. Control Comput. Sci., vol. 51, no. 2, pp. 114–123, Mar. 2017.

[2] R. Alur and D. L. Dill, "A theory of timed automata," Theor. Comput. Sci., vol. 126, no. 2, pp. 183–235, Apr. 1994.

[3] G. Wang, L. Zhuang, R. Wang, "Modeling and verifying on timed automata based Internet of things gateway security system," J. Commun., vol. 39, no. 3, pp. 63–75, Mar. 2018.

[4] M. T. Khan, D. Serpanos, H. Shrobe, "ARMET: Behavior-based secure and resilient industrial control systems," Proc. IEEE, vol. 106, no. 1, pp. 129–143, Jan. 2018.

[5] S. Kriaa, M. Bouissou, Y. Laarouchi, "A new safety and security risk analysis framework for industrial control systems," J. Risk Reliab., vol. 233, no. 2, pp. 151–174, Apr. 2019.

Contact

Corresponding author：Wang Guoqing
Phone：18530826587
E-mail：iegqwang@163.com