The Sixteenth International Symposium on Artificial Life and Robotics 2011 (AROB 16th '11),
B-Con Plaza, Beppu,Oita, Japan, January 27-29, 2011

Improvement of Immunity-Based Diagnosis for a Motherboard

Haruki Shida[1], Takeshi Okamoto[1] and Yoshiteru Ishida[2]

[1] *Department of Information Network and Communication, Kanagawa Institute of Technology,*
1030, Shimo-ogino, Atsugi, Kanagawa 243-0292, Japan
[2] *Department of Knowledge-Based Information Engineering, Toyohashi University of Technology,*
1-1, Tempaku, Toyohashi, Aichi 441-8580, Japan

***Abstract*:** We have utilized immunity-based diagnosis to detect abnormal behavior of components on a motherboard. The immunity-based diagnostic model monitors voltages of some components, CPU temperatures, and fan speeds. After simulating the abnormal behaviors of some components on the motherboard, we assessed the ability of the immunity-based diagnostic model to detect these abnormalities. To improve the diagnostic accuracy of the model, which can be decreased by isolated nodes, we used multiple diagnostic networks to connect isolated nodes to a network or other isolated nodes. This simulation showed that the immunity-based diagnostic model containing multi ple diagnostic networks was an effective method for detecting abnormal behavior of components on the motherboard.

Keywords: Immunity-based system, fault diagnosis, sensor network, motherboard, immune network

I. INTRODUCTION

The prevalence of technology for cloud computing has increased the demand for data centers that provide such cloud computing. Each server in these data centers must therefore be available for data processing and data transmission. To maintain system availability, it is important to detect abnormalities during their early stages, before system failure.

The simplest way of diagnosing abnormalities consists of evaluating each component individually by comparing the output value of its sensor with a predetermined threshold value. However, it is difficult to identify the abnormal component using this method [1]. Another method of diagnosis uses an immunity-based diagnostic model [2-5], which was derived primarily from the concept of an immune network [6]. In this diagnostic model, mutual tests are performed among nodes and the dynamic propagation of active states. This diagnostic model has been used to diagnose node faults in processing plants [7], to the self-monitoring/self-repairing in distributed intrusion detection systems [3], and to sensor-based diagnostics for automobile engines [4].

We previously applied immunity-based diagnosis to the detection of abnormal behaviors of components on a motherboard [8]. After simulating the abnormal behaviors of some components on the motherboard, we evaluated the ability of this model to diagnose abnormalities of components of motherboard sensors in two experiments. In the first experiment, we found that the immunity-based diagnostic model outperformed a stand-alone diagnostic model. In the second experiment, which compared a fully-connected network with a correlation-based network for mutually testing the credibility of sensors, we found that the correlation-based network had greater diagnostic accuracy in all test cases. In addition, we utilized a hybrid model, consisting of the stand-alone and immunity-based diagnostic models, to diagnose nodes connected to the network and isolated from the network. We found, however, that the accuracy of hybrid diagnosis for isolated nodes was dependent on the stand-alone diagnostic model. These isolated nodes could decrease the diagnostic accuracy of the hybrid model. In this paper, we sought to improve diagnostic accuracy of multiple diagnostic networks by connecting the isolated nodes with one of the networks.

II. Embedded Sensors on the Motherboard

Since a motherboard has multiple sensors, including voltage, temperature, and fan speed sensors, abnormalities on the motherboard can be detected by monitoring these sensors. We therefore used sensor output values for diagnosis of the motherboard.

We collected sensor output values on a server from July 27 to September 18. The specifications of the server are shown in Table 1. The average air temperature during that period was 25.3 °C, ranging from 20.1°C to 32.8°C. Data were collected using lm_sensors, a hardware health monitoring package for

Linux that allows information to be obtained from temperature, voltage, and fan speed sensors.

Table 1. Server specifications

Motherboard	Supermicro® X7DVL-I
OS	Debian GUN/Linux 5.0
Kernel	2.6.26-2-amd64
Module	lm-sensors version 3.0.2 with libesensors version 3.0.2
CPU	Intel® Xeon E5410 2.33GHz×2
Power supply	Thermaltake Toughpower 700w
Fan	XFan model: RDM8025B×2 Gantle Typhoon D0925C12B2AP×2 ADDA CFX-120S

After collecting the output values from all 29 sensors on the motherboard, we calculated the correlation coefficients of all sensors. We observed correlations involving 5 sensors (Table 2), and we therefore used these 5 sensors for evaluation.

Table 2. Sensors used for evaluation and range of s ensor output values

Sensor	Component	Range	Mean	Standard deviation
CPU1	CPU temperature	11.00-48.00(℃)	18.68	4.55
Core2	Core2 temperature	35.00-72.00(℃)	42.79	4.45
VcoreA	CoreA voltage	1.11-1.19(V)	1.121	0.007
Vbat	Internal battery voltage	3.23-3.26(V)	3.237	0.009
Fan5	Fan speed	1012-1044(RPM)	1034	5.021

III. Immunity-Based Diagnostic Model

The immunity-based diagnostic model has the feature of a dynamic network, in which diagnoses are performed by mutually testing nodes (i.e., sensors) and by dynamically propagating their active states. In this paper, the targets of the immunity-based diagnosis are components with a sensor embedded on a motherboard. Each sensor can test linked sensors and can be tested by linked sensors. Each sensor is assigned a state variable R_i indicating its credibility.

The initial value of credibility $R_i(0)$ is 1. The aim of diagnosis is to decrease the credibility of all abnormal sensors. That is, according to this model, if the credibility of a sensor is below a threshold value, that sensor is considered abnormal.

When the value of credibility R_i is between 0 and 1, the model is called a gray model, reflecting the ambiguous nature of credibility. The gray model can be expressed by the equation:

$$\frac{dr_i(t)}{dt} = \sum_j T_{ji}^{+} R_j(t) - r_i(t), \quad (1)$$

Where

$$R_i = \frac{1}{1+\exp(-r_i(t))}, \quad (2)$$

$$T_{ij}^{+} = \begin{cases} T_{ij} + T_{ji} - 1, & \text{if one of evaluation from i to j or j to i exists,} \\ 0, & \text{if neither evaluation from i to j nor j to i exists,} \end{cases} \quad (3)$$

$$T_{ij} = \begin{cases} 1, & \text{if a balance formula between sensors } i \text{ and } j \text{ is satisfied,} \\ -1, & \text{if a balance formula between sensors } i \text{ and } j \text{ is not satisfied,} \\ 0, & \text{if there is no balance formula between sensors } i \text{ and } j. \end{cases} \quad (4)$$

In the right-hand side of Equation (1), the first term is the sum of evaluations from other nodes for node i. The second term is an inhibition term that maintains ambiguous states of credibility. In this model, equilibrium points satisfy the equation r_i (t) $=\sum_j T_{ji}^{+} R_j(t)$. Thus R_i monotonically reflects the value of $\sum_j T_{ji}^{+} R_j(t)$. If $\sum_j T_{ji}^{+} R_j(t)$ is close to 0, then R_i is close to 0.5. The balance formulas were determined by calculating the relationships of the output values of the sensors (Table 3).

Table 3. Balance formulas between sensors

Sensor	Balance formula
CPU1-Core2	|CPU1-Core2| ≤ 26
CPU1-VCoreA	|CPU1-VCoreA×25| ≤ 20
CPU1-Vbat	|CPU1-Vbat×9| ≤ 18
CPU1-Fan5	|CPU1-Fan5/34| ≤ 18
Core2-VCoreA	|Core2-VcoreA×45.5| ≤ 28
Core2-Vbat	|Core2-Vbat×16| ≤ 20
Core2-Fan5	|Core2-Fan5/19| ≤ 21
VCoreA-Vbat	|VCoreA-Vbat/2.8| ≤ 0.05
VCoreA-Fan5	|VCoreA-Fan5/893| ≤ 0.07
Vbat-Fan5	|Vbat-Fan5/316| ≤ 0.07

IV. Evaluation of the immunity-based diagnosis for motherboard sensors

We evaluated the immunity-based diagnostic model for motherboard sensors by a simulation, using the four test cases shown in Table 4.

Test cases 1 and 2 assumed that the speeds of Fan5 were far outside the range shown in Table 2. A significant decrease in Fan speed (test case 1) would therefore cause the CPU temperature to rise, with the overheated CPU causing the server to crash. Conversely, a significant increase in Fan speed (test case 2) would waste power and decrease the life span of the Fan. Therefore, test cases 1 and 2 represent abnormal conditions.

Test cases 3 and 4 assumed that the output values of the sensors were slightly out of the range shown in Table 2. Test case 3 assumed that the speed of Fan5 was

slightly higher than that shown in Table 2, but that Fan5 was not abnormal. Test case 4 assumed that the temperature of CPU1 was slightly higher than that shown in Table 2, but that CPU1 was not abnormal. Temperatures outside the range are not always abnormal, because these temperatures depend on room temperature. Therefore, test cases 3 and 4 represent normal conditions.

Table 4. Test cases

Case	Sensor output value					State
	CPU1	Core2	VcoreA	Vbat	Fan5	
1	70	65	1.12	3.23	200	Abnormal
2	9	35	1.12	3.23	2000	Abnormal
3	14	35	1.12	3.23	1050	Normal
4	50	60	1.12	3.23	1020	Normal

1. Correlation-based network

We previously described the construction of a correlation-based network [8], using the correlation coefficients shown in Figure 1. In the model presented here, we removed a weakly correlated network from a fully-connected network, forming a correlation-based network, because these connections may be unreliable for mutually testing the credibility of their sensors. Table 5 shows the results of correlation-based networks. Each value is a sensor credibility, i.e., R_i of Equation (2).

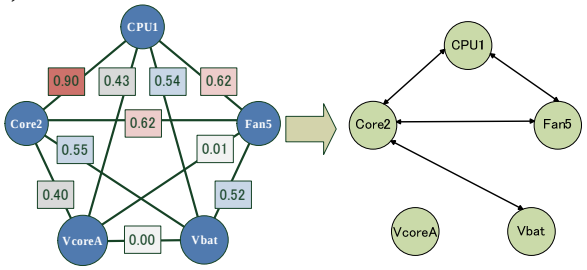

Fig. 1. Correlation-based network

Table 5. Results of a correlation-based network

Test case	Credibility					Decision	Accuracy
	CPU1	Core2	VcoreA	Vbat	Fan5		
1	0.87	0.97	0.50	0.87	0.00	X	O
2	0.87	0.97	0.50	0.87	0.00	X	O
3	0.98	0.99	0.50	0.88	0.98	O	O
4	0.67	0.95	0.50	0.87	0.67	O	O

In Table 5, we assumed that a component on the motherboard was abnormal if its credibility was less than 0.1. A diagnostic decision of "O" indicates an absence of abnormality, whereas a diagnostic decision of "X" indicates an abnormality. An accuracy of "O" indicates a correct decision, whereas an accuracy of "X" indicates an incorrect decision.

The diagnostic model correctly identified the abnormal Fan5 in test cases 1 and 2, and did not falsely identify abnormalities in test cases 3 and 4. However, this diagnostic model could not correctly diagnose the isolated sensor, because the credibility of the isolated VcoreA sensor was always 0.50.

2. Multiple diagnostic networks

We hypothesized that utilizing multiple diagnostic networks, in which isolated nodes are connected to a network or another isolated node, would approve diagnostic accuracy.

All combinations of the multiple networks used for immunity-based diagnosis are shown in Figure 2. Each evaluation was based on the four test cases shown in Table 4. The diagnostic accuracy of all multiple networks is shown in Table 6.

In Table 6, a diagnostic accuracy of "P" indicates that the diagnostic model could not identify the abnormal component, although it detected multiple abnormalities.

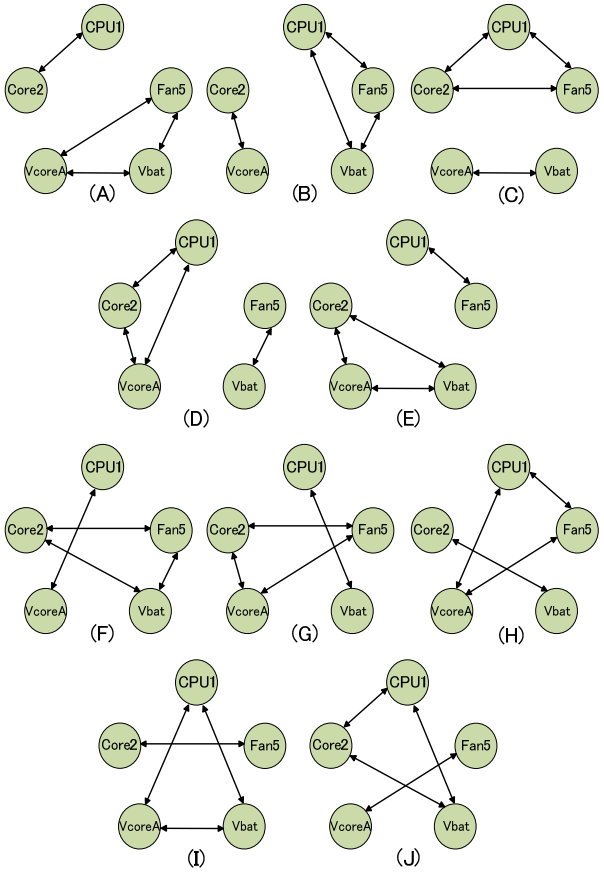

Fig. 2 Multiple diagnostic networks

Table 6. Diagnostic accuracy of multiple networks

Test case	(A)	(B)	(C)	(D)	(E)	(F)	(G)	(H)	(I)	(J)
1	O	X	O	X	X	O	O	X	P	X
2	O	X	O	X	X	O	O	O	X	X
3	O	O	O	O	O	O	O	X	O	O
4	O	X	O	O	O	O	O	O	X	O

We found that diagnostic models (A), (C), (F) and (G) made correct decisions, whereas the other diagnostic models made incorrect decisions.

In test cases 1, 2 and 3, each of the diagnostic networks (A), (C), (F) and (G) consisted of 3 sensors including Fan5. In contrast, the other diagnostic networks either consisted of 2 sensors including Fan5 or were weakly correlated networks. In test case 4, all diagnostic networks other than (B) and (I) showed results similar to those of CPU1.

For example, Table 7 shows the successful results of diagnostic network (C), and Table 8 shows the unsuccessful results of diagnostic network (I).

Table 7. Results of diagnostic model (C)

Test case	Credibility					Decision	Accuracy
	CPU1	Core2	VcoreA	Vbat	Fan5		
1	0.640	0.640	0.659	0.659	0.021	X	O
2	0.640	0.640	0.659	0.659	0.021	X	O
3	0.844	0.844	0.659	0.659	0.844	O	O
4	0.385	0.683	0.659	0.659	0.385	O	O

Table 8. Results of diagnostic model (I)

Test case	Credibility					Decision	Accuracy
	CPU1	Core2	VcoreA	Vbat	Fan5		
1	0.021	0.293	0.640	0.640	0.293	X	P
2	0.385	0.293	0.683	0.385	0.293	O	X
3	0.844	0.659	0.844	0.844	0.659	O	O
4	0.021	0.659	0.640	0.640	0.659	X	X

The diagnostic model in Table 7 misidentified the normal CPU1 in test case 1, and misidentified the abnormal Fan5 in test case 2. These results indicate that an immunity-based diagnostic model could not diagnose sensors on a weakly correlated network consisting of 2 sensors.

In test case 4 of Table 8, the diagnostic network misidentified the normal CPU1 due to a weak correlation network, although CPU1 belongs to the diagnostic network consisting of 3 sensors.

This simulation showed that diagnostic accuracy depends on the size of the network and the correlation between nodes.

V. CONCLUSION

We applied immunity-based diagnosis to the detection of abnormal behaviors of components on a motherboard. We simulated the abnormal behaviors of some components on the motherboard, and we evaluated all the combinations of the diagnostic networks. We showed that diagnostic accuracy depends on the size of the network and the correlation between nodes of the network. In addition, we showed that the immunity-based diagnostic model with multiple diagnostic networks was an effective method for detecting abnormal behavior of components on the motherboard.

In future, we will attempt to determine the relationships among diagnostic network topologies and correlation between nodes, and to improve the accuracy of the diagnostic model.

REFERENCES

[1] Tanaka T, Kawazu T, Kanda S (2003), Computer-assisted Diagnostic System Applied with ANFIS. Biomedical Fuzzy System Association 5(1):49-54

[2] Ishida Y (1996), An immune network approach to sensor-based diagnosis by self-organization. Comples Systems Publication 10:73-90

[3] Watanabe Y, Ishida Y (2003), Immunity-based Approaches for Self-monitoring in Distributed Intrusion Detection System. Knowledge-Based Intelligent Information and Engineering Systems (KES'2003) 2774(2):503-510

[4] Ishida Y (2006), Designing an Immunity-Based Sensor Network for Sensor-based diagnosis of Automobile Engines. Lecture Notes Computer Science 4252:146-153

[5] Watanabe Y, Ishida Y (2003), Mutual tests among agents in distributed intrusion detection systems using immunity-based diagnosis. Proc. of AROB 8th '03:682-685

[6] Jerne N K (1973), The immune system. Scientific Amrecian, 229(1):52-60

[7] Ishida Y (2004), Immunity-Based Systems: A Design Perspective. Springer-Verlag

[8] Shida H, Okamoto T, Ishida Y (2010), Evaluation of Immunity-Based Diagnosis for a Motherboard. Knowledge-Based Intelligent Information and Engineering Systems (KES'2010) 6278:628-636