SCHEME FOR COMPARING RESULTS OF DIVERSE SOFTWARE VERSIONS

Viktor Mashkov and Jaroslav Pokorny
Department of Software Engineering Faculty of Mathematics and Physics, Charles University
Malostranske nam. 25, 11800 Praha 1
Czech Republic

Keywords: Design diversity, software fault-tolerance, adjudicator, system-level diagnosis.

Abstract: The paper presents a scheme for comparing the results produced by diversely designed SW versions in order to select and deliver presumably correct result. It also allows to determine all faulty versions of SW and all faulty comparators. As compared to the majority voting scheme, it requires a lesser number of result comparisons and is able, in most situations, to deliver presumably correct service even if the number of faulty SW versions is greater than the number of correct ones. The scheme is based on system-level diagnosis technique, particularly, on the comparison-based testing model. The proposed scheme can be used for designing fault-tolerant diverse servers and for improving adjudicator in N-version programming technique.

1 INTRODUCTION

The value of redundancy and diversity as a means of tolerating faults in computing systems has long been recognized. For SW faults, non-diverse replication will fail to detect, or recover from, all those failures that do not produce obvious symptoms like crashes, or that occur in identical ways on all the copies of a replicated system, and at each retry of the same operations. For these kinds of failures, diverse redundancy (often referred to as "design diversity") is required (Lyu, 1995).

One of the main mechanisms for building a fault-tolerant server from two or more diverse servers is the adjudicating mechanism responsible for delivering correct service by selecting the one among the multiple services produced by different servers. Adjudicating the results produced by different servers is considered in tight connection with such design issues as synchronization between the servers to guarantee data consistency between them, possible indeterminism of servers, translation of the client queries to be "understood" by different servers (e.g., SQL servers), etc. It must be recognized that the success of a fault-tolerance scheme depends to a great extent upon its adjudicator and unreliability in the adjudicator can have a dramatic impact on the overall system reliability (Lee et al., 1990). One original and effective solution for constructing the simple adjudicator is presented in (Xu, 1991). The author suggests new specific fault tolerance scheme, called t/(n-1)-variant programming, based on the theory of system-level fault diagnosis. It is worth noting that the adjudicator in this scheme intends to detect only the correct variant. We also are going to exploit the theory of system-level fault diagnosis to construct the simple (with minimum number of result comparisons) and, thus, reliable adjudicator. We extend the functionality of adjudicator to detect not only the correct variant but also all the faulty ones, as well as all the faulty comparators. In some cases, adjudicator can select and deliver presumably correct service even if the number of faulty SW variants is greater than the number of fault-free ones.

2 COMPARISON-BASED TESTING MODEL

A diagnosable system S consists of n units denoted by the set $U=\{u_1, u_2,\ldots, u_n\}$. Each unit u_i, $u_i \in U$, is assigned a particular subset of the remaining units in S to compare its own result with result of each unit

Mashkov V. and Pokorny J. (2007).
SCHEME FOR COMPARING RESULTS OF DIVERSE SOFTWARE VERSIONS.
In *Proceedings of the Second International Conference on Software and Data Technologies - SE*, pages 341-344

from this subset. Comparison of results of two units, u_i and u_j, (also termed as test link) is carried out by a comparator, and denoted as ω_{ij}. For each pair of units there can be only one test link. The complete collection of comparators is called comparison assignment $\Omega=\{\omega_{ij}\}$, and is represented by an undirected graph G=(V, E), where each unit $u_i \in U$ is represented by a vertex $v_i \in V$, and each edge $e(v_i, v_j)$ is in E if and only if ω_{ij} is a comparator in the comparison assignment Ω. The outcome produced by comparator ω_{ij} (denoted as r_{ij}) can take the value either 0 or 1 if the results of units u_i and u_j agree or disagree respectively. The outcomes r_{ij} and r_{ji} present the same outcome produced by one comparator, and are always $r_{ij}=r_{ji}$. The collection of all outcomes is called the comparison syndrome, $R=\{r_{ij}\}$. Two classes of faults, independent and related, are taken into account. So, two incorrect results produced by the units can be the same due to the manifestation of related faults.

As distinct from t/(n-1)- diagnosability (Friedman, 1975), we intend to identify all correct and all incorrect results produced by the units (i.e., perform the system diagnosis). Our approach to system diagnosis is based on the consistency examination of multiple unit sets.

3 CONSISTENT SETS AND SYSTEM DIAGNOSIS

For our purposes, we will now introduce several definitions, assumptions and simple lemmas. In order not to overload the paper with the details, the proofs of lemmas are omitted.

Definition 1. For a system S and a comparison syndrome R, a subset $Y \subset U$ is a consistent set if and only if:

1) $u_i \in Y$ and $u_j \in Y$ if $r_{ij}=0$;
2) $u_i \in Y$ and $u_j \in U-Y$ if $r_{ij}=1$;
3) $u_i \in Y$ and $u_j \in Y$ if $\exists P(v_i, v_j)$, $P=\{e(v_i, v_l), e(v_l, v_p),\ldots, e(v_k, v_j)\}$, $u_i, u_l, u_p,\ldots, u_k, u_j \in Y$ and $r_{il}=r_{lp}=\ldots=r_{kj}=0$.

Following the widely accepted approach according to which the result produced by the majority of units are trusted (e.g., NVP), we make the following assumptions.

Assumption 1. If the number of faulty units doesn't exceed t, then the consistent set Y, for which $|Y| \geq t+1$, is a set of fault-free units. We named such consistent set as consistent fault-free set, Y_{FF}.

Definition 2. Two consistent sets, Y_i and Y_j, are in contradiction with each other when

$$Y_i \leftrightarrow Y_j : \exists r_{ij}=1,\ u_i \in Y,\ u_j \in Y,\ i,j \in \overline{1,N}.$$

Lemma 1. Given any syndrome, and if the number of faulty units doesn't exceed t, then all fault-free units are either in Y_{FF} or in consistent sets which satisfy the following two conditions:

1) they are not in contradiction with each other;
2) their total number of units is greater than t.

Assumption 2. The state of the unit can be correctly diagnosed if and only if there is a test link between this unit and at least one fault-free unit.

With the account of the above assumptions, we will now introduce the following lemma.

Lemma 2. A system S composed of N units is t-diagnosable if and only if, given any syndrome, each unit u_i, $u_i \in U$, i=1, 2,.., N, has $|z(u_i)| \geq t+1$ test links with other units, provided that the number of faulty units in S doesn't exceed t, where $z(u_i)=\{u_j: \omega_{ij} \in \Omega\}$.

The credibility of system diagnosis result will be greater when all fault-free units are in Y_{FF} , since it is evident that probability of the hypothesis that t+1 or more faulty units produce the same incorrect result is lesser than probability of the hypothesis that these faulty units produce any incorrect results. In view of this, we examine how many test links are needed in order that all fault-free units be in Y_{FF}. The sought number of test links depends, to a great extent, on the number of units in system, N, and on the comparison assignment.

4 COMPARISON ASSIGNMENT

From the assumption that majority of units are trusted it follows that for correct system diagnosis the number of fault-free units, $|C|$, must be greater than the number of faulty units, $|F|$. Let t be the number of faulty units, $|F|=t$. Then N-t>t or N>2t or $N \geq 2t+1$, which is the same result as the one of the PMC model (Preparata et al., 1967). Since even numbers N do not increase the value t as compared to odd numbers, the further consideration is only related to the odd numbers N. We consider the worst situation when the number of faulty units is equal to t, and all faulty units produce the same incorrect result. From Lemma 2, it follows that for a system S to be t-diagnosable it is sufficient that each system's unit has t+1 test links with other units. Such comparison assignment is called basic. Since each test link engages two units, the minimal number of test links providing system t-diagnosability, T_{min}, is equal to $T_{min} = \lceil N(t+1)/2 \rceil$. At the first stage, we examine whether T_{min} is sufficient in order that all

fault-free units be in Y_{FF}. For this we inspect the minimal possible number of test links between fault-free units, R, given T_{min}. The sought number R can be determined as $R=\lceil (q-k)/2 \rceil$, where k- is the maximum number of test links between units from the sets F and C; q- is the total number of test links of all fault-free units. For $|F|=t$ and $|C|=t+1$, $k=t(t+1)$ and $q=(t+1)^2$. Then $R=\lceil (t+1)/2 \rceil$. Consider the corresponding subgraph $G(C_u)$ of graph G(V,E). Vertices of $G(C_u)$ correspond to the fault-free units and edges correspond to the test links among units of C. The $G(C_u)$ is connected if its number of edges is greater than t(t-1)/2. Thus, in order that all fault-free units be in Y_{FF} it is necessary that $R > t(t-1)/2$ or $2t+1 > t^2$. This inequality is met for t<3 (i.e., for N<7). For N≥7 the T_{min} is not sufficient in order that all fault-free units be always in Y_{FF}. At the second stage, we examine for N≥7 how many additional test links are needed in order that all fault-free units be in Y_{FF}. We consider the worst case when faulty units don't have mutual test links. It means that the corresponding subgraph $G(C_u)$ may have the maximum $\pi=\lfloor (N-t)/2 \rfloor$ components, each of which consists either of two vertices for N=3+4a, a=0,1,2,…, or of two vertices except the one consisting of three vertices for N=5+4a, a=0,1,2,… In order to connect these π components, (π-1) additional edges are necessary.

The Table 1 presents the numbers of test links needed for system t-diagnosability for three cases:
Case1: basic comparison assignment, T_{min};
Case 2: comparison assignment providing that all fault-free units be in Y_{FF};
Case 3: comparison assignment based on pairwise comparison needed for majority voting.

Table 1: Number of test links needed for system diagnosis.

N	Case 1	Case 2	Case 3
3	3	3	3
5	8	8	10
7	14	15	21
9	23	24	36
11	33	35	55
13	46	48	78
15	60	63	105
17	77	80	136

The total number of result comparisons needed for system diagnosis (cases 1 and 2) is lesser than the one needed for majority voting (case 3) since system diagnosis doesn't require pairwise comparison of all units' results. The diagnosis algorithm presented below is designed for the systems with comparison assignment providing that all fault-free units be in Y_{FF}.

Algorithm 1. (Given any syndrome $R=\{r_{ij}\}$)
Step 1: set $L_{ui}=\varnothing$, i=1,2..,N;
Step 2: For i=1 to N
For j=1 to N
if $r_{ij}=0$ then $L_{ui}= L_{ui} \cup \{u_j\}$;
Step 3: s=1; i=1;
Step 4: if i=t+2 then STOP ("Number of faulty units >t");
Step 5: $L_{ui}^s= L_{ui}$;
Step 6: For j=1 to N
if $u_j \in L_{ui}^s$ then $L_{ui}^{s+1}= L_{ui}^s \cup L_{ui}$;
Step 7: if $L_{ui}^{s+1} - L_{ui}^s=\varnothing$ then proceed with next Step ;
otherwise $L_{ui}^s= L_{ui}^{s+1}$ and GOTO Step 6 ;
Step 8: if $|L_{ui}^{s+1}|<t+1$ then i=i+1 and GOTO Step 4 ;
otherwise STOP ("$Y_{FF} = L_{ui}^{s+1}$") ;

The comparison-based model also allows to detect the faulty comparators (i.e., incorrect outcomes of result comparisons). The correct result of diagnosing is guaranteed when the total number of faulty units and faulty comparators doesn't exceed t. The detection of faulty comparators is based on checking the outcomes of result comparisons which should be consistent with the result of system diagnosis. It means that the outcomes of comparing the results of fault-free units must be "0", and the outcomes of comparing the results produced by fault-free units and faulty units must be "1". When the outcome different from those is found, it means that the corresponding comparator is faulty.

The approach to system diagnosis based on the examination of consistent sets can also be used to deliver presumably correct service in most situations when the total number of faulty units and faulty comparators exceeds t. It is obvious that the service in these cases will have lesser credibility as compared to the cases when total number of faulty units in the system doesn't exceed t. However, it is possible to set lower bound on the credibility of system diagnosis result which would be acceptable for some practical applications. When the credibility of system diagnosis result is above this bound, the service can be delivered to the client. The credibility of system diagnosis result can be determined by way of computing the probabilities of hypotheses that different consistent sets are the sets of fault-free units.

In the situations when there are more than t faulty units, we suggest attempting to find the consistent set of size t, and if there is only one such consistent set (i.e., this consistent set is the greatest one), it can be considered as a set of presumably

fault-free units. This statement is based on the fact that *a posteriori* probability that the units of the greatest consistent set are fault-free satisfies the measure ε (used in majority voting techniques) when comparing this hypothesis with all the other ones. There is only one exception when there exist t units, which are not in this greatest consistent set, and they don't have mutual test links. If t units don't have mutual test links, then the probability $P(R/H_t)$ of obtaining syndrome R under the situation when these t units are considered as fault-free (hypothesis H_t), is not negligible, and the measure ε may not be satisfied. Therefore, the diagnostic algorithm for the situation when there are more than t faulty units in the system, is designed so that it tries to find the greatest consistent set of size t (Steps 1÷4), and to check that there are no t presumably faulty units that don't have mutual test links (Steps 5÷8).

Algorithm 2. (Given syndrome R and consistent sets $Y_1, Y_2, .., Y_\tau$).

Step 1 : i=1 ; α=0 ;
Step 2 : if i=τ+1 then GOTO Step 4;
Step 3: if $|Y_i|$=t then D=U-Y_i; C=Y_i; α=α+1; i=i+1;
and GOTO Step 2;
otherwise i=i+1 and GOTO Step 2;
Step 4: if α=1 then proceed with next Step;
otherwise STOP ("there is no the greatest consistent set of size t");
Step 5: k=1;
Step 6: if k=N+1 then STOP ("C is the set of fault-free units");
Step 7: if $u_k \in D$ then D=D-{u_k} and proceed with next Step;
otherwise k=k+1 and GOTO Step 6;
Step 8: For i=1 to N
For j=1 to N
if $u_i \in D$ and $u_j \in D$ and ω_{ij}=1 then k=k+1 and GOTO Step 6;
otherwise STOP ("there is no acceptable system diagnosis result");

5 CONCLUSIONS

Design diversity used for achieving fault tolerance needs comparing of results produced by different SW variants (servers). For many servers (e.g., SQL servers) the comparison procedure is non-trivial and usually requires complex operations. In view of this, the comparators cannot be considered as absolutely reliable, and it is important to reduce the total number of comparators in the adjudication mechanisms. One of the practical approaches allowing to simplify the adjudicator relies on the system-level fault diagnosis technique. The novelty of this research is that the system-level fault diagnosis is used for broader purpose, namely, not only for detecting the fault-free unit, but also for detecting all faulty units and comparators. In many situations, it also allows to deliver service which can be considered as correct (with acceptable probability) when the total number of faulty units and comparators exceeds the measure of diagnosability, t. We consider the consistent sets of units which are derived from the obtained syndrome as a core element of system diagnosis. Based on the examination of possible consistent sets, we have designed the comparison assignment which is simpler as compared to the one required for majority voting (Kuncheva, 2003). We have also developed the simple diagnosis algorithm for the system with the designed comparison assignment. The proposed comparison assignment providing system diagnosis can be used for designing simple and reliable adjudicator of fault-tolerant diverse servers or for improving adjudicator in N-version programming scheme.

ACKNOWLEDGEMENTS

This research was supported in part by the National program of research (Information society project 1ET100300419).

REFERENCES

Friedman, A., 1975. A new measure of digital system diagnosis. *Proc. Int. Symp. Fault-tolerant computing*, Paris, France, pp. 167-170.

Kuncheva, L., Whitaker, J., Shipp, C., 2003. Limits on the majority vote accuracy in classifier fusion, *Pattern analysis and applications No. 6*, pp. 22-31.

Lee, P., Anderson, T., 1990. *Fault tolerance: Principles and practice*, Prentice-Hall, 2nd edition.

Lyu, M., 1995. *Software fault tolerance, trends in software series.* Wiley.

Preparata, F., Metze, G., Chien, R., 1967. On the connection assignment problem of diagnosable systems. *IEEE Trans. Electron. Comput., Vol. EC-16*, pp. 848-854.

Xu, J., 1991. The t/(t-1)-diagnosability and its applications to fault tolerance. *Technical report series No. 340*, University of Newcastle upon Tyne.