Performance-Reliability Tradeoff Analysis for Multithreaded Applications

Isil Oz*, Haluk Rahmi Topcuoglu†, Mahmut Kandemir‡, Oguz Tosun*

*Computer Engineering Department, Bogazici University, 34342, Istanbul, Turkey
†Computer Engineering Department, Marmara University, 34722, Istanbul, Turkey
‡Dept. of Computer Science and Engineering, Pennsylvania State University, University Park, PA 16802, USA

Abstract—Modern architectures become more susceptible to transient errors with the scale down of circuits. This makes reliability an increasingly critical concern in computer systems. In general, there is a tradeoff between system reliability and performance of multithreaded applications running on multicore architectures. In this paper, we conduct a performance-reliability analysis for different parallel versions of three data-intensive applications including FFT, Jacobi Kernel, and Water Simulation. We measure the performance of these programs by counting execution clock cycles, while the system reliability is measured by Thread Vulnerability Factor (TVF) which is a recently-proposed metric. TVF measures the vulnerability of a thread to hardware faults at a high level. We carry out experiments by executing parallel implementations on multicore architectures and collect data about the performance and vulnerability. Our experimental evaluation indicates that the choice is clear for FFT application and Jacobi Kernel. Transpose algorithm for FFT application results in less than 5% performance loss while the vulnerability increases by 20% compared to binary-exchange algorithm. Unrolled Jacobi code reduces execution time up to 50% with no significant change on vulnerability values. However, the tradeoff is more interesting for Water Simulation where squared version reduces the vulnerability values significantly by worsening the performance with similar rates compared to faster but more vulnerable spatial version.

Index Terms—Multi-Core Architectures and Support, Reliable Parallel and Distributed Algorithms

I. INTRODUCTION

As technology scales and transistor sizes in modern architectures continuously decrease, transient error rates increase. Soft errors are a kind of transient errors that result from a fault in a single-bit and their rates keep increasing with current design trends [1]. Recent research addressed the soft error problem from both hardware and software perspectives [2], [3], [4], which indicate that the reliability is an important concern in computer architecture.

Chip multiprocessors (CMPs), which have been viewed as the most promising option for the next generation computing platforms, are more error prone due to their smaller transistor sizes and more aggressive power modes [5], [6]. While prior research on CMPs explored performance and power related issues, reliability problem has relatively taken less attention.

Although many performance metrics for multicore architectures have been suggested in the literature [7], [8], there is a lack of metric that quantifies the reliability of parallel architectures. Program Vulnerability Factor (PVF) measures the vulnerability of a program to the hardware faults [9], but it is a metric only for single-threaded applications. A recent study [10] has proposed Thread Vulnerability Factor (TVF) which defines the vulnerability for multithreaded applications running on multicore architectures. TVF measures the vulnerability of a thread (which is one of the threads of a multithreaded application) to transient hardware faults by considering the codes of the threads that communicate with that thread as well as the code of the thread itself.

Our main goal in this work is to present a performance-reliability analysis to provide the characteristics of different multithreaded applications with alternative design choices. We consider three data-intensive programs including Fast Fourier Transform (FFT), Jacobian Calculation, and Water Simulation in our evaluation. While we evaluate two different parallel implementations of FFT algorithm, two different algorithms of the water simulation benchmark are selected. We also apply loop transformations to the standard parallel Jacobi implementation. While we use execution cycles as performance metric, TVF metric is employed to quantify vulnerability. Our analysis compares different implementations of the same program by considering performance and reliability aspects.

Our major contributions can be summarized as follows:

- We perform a performance-reliability analysis of different multithreaded applications running on multicore architectures. We evaluate TVF values and gather execution clock cycles of a set of parallel programs with different versions. Specifically, we demonstrate the performance and vulnerability behavior of two different parallel implementations of FFT algorithm, two different algorithms of water simulation and four versions of Jacobian calculation each of which has an application of a loop transformation.
• We present the performance and vulnerability values of parallel programs and discuss the effect of design choices on the system performance and reliability by comparing different implementations. We observe that the choice is clear for FFT algorithm which has different vulnerability values with almost equal performance, and for Jacobian calculation which, in contrast, has no significant difference in vulnerability values but distinct performance characteristics. However, the choice is not clear for water simulation which demonstrates a performance-reliability tradeoff with higher performance but higher vulnerability as well.

II. BACKGROUND AND RELATED WORK

Since the reliability becomes an important concern in modern architectures, it is crucial to define suitable metrics to evaluate the reliability of the system.

Architectural Vulnerability Factor (AVF) has been defined as the probability that a fault in a processor will induce an error in the program output [11]. In the AVF analysis, the bits in the hardware structure (called as ACE bits) which have visible effect in the program output have been distinguished from the bits (called as un-ACE bits) which may affect the program flow or performance, but have no effect in the final output. ACE bits have been used in calculating the AVF of the hardware structure.

Although AVF is well-defined and useful metric, it is difficult to evaluate the vulnerability of a program to a hardware fault since it is a hardware-based metric. To define the vulnerability of a software to transient errors, Program Vulnerability Factor (PVF) has been proposed [9]. This metric measures the vulnerability of a program to the hardware faults in a microarchitecture independent way and provides the relative vulnerability of the programs to be able to make decisions about the reliability of these programs. While calculating the PVF, microarchitectural resources that are hardware dependent are not considered only architectural resources are taken account by the software’s view.

While PVF is a software-based metric, it is only useful for single-thread applications. In a recent work, Thread Vulnerability Factor (TVF) has been proposed as a reliability metric for multithreaded applications on CMP architectures [10]. TVF measures the vulnerability of a thread to transient hardware faults by considering the thread itself and the threads that communicate with that thread via memory operations. TVF has two components including LVF and RVF, the former holds the vulnerability caused by the code of the target thread while the latter represents the vulnerability induced by the communication between the target thread and the other threads in the application.

In our performance-reliability analysis, we use the TVF metric to evaluate the relative vulnerability of multithreaded applications. TVF can be calculated as follows:

\[ TVF(T_i) = [w_L \times LVF(T_i)] + [w_R \times RVF(T_i)], \]

where \( LVF(T_i) \) is the local vulnerability factor for thread \( i \) and \( RVF(T_i) \) is the remote vulnerability factor for thread \( i \) which iterates over all threads that sends data to thread \( i \). \( w_L \) and \( w_R \) are weight values for local and remote vulnerability factors respectively.

TVF is evaluated for three hardware components including register file, ALU unit, and memory (cache). The local vulnerability factor (LVF) term is calculated in a similar fashion to PVF [9], where the vulnerability values of the resources in the thread are combined and normalized by considering their vulnerable intervals. The remote vulnerability factor (RVF) term represents the vulnerability impact of the threads that interact with the target thread in a multithreaded application. RVF of thread \( i \) can be calculated as follows:

\[ RVF(T_i) = \frac{\sum rVF(T_i, T_j)}{RV}, \]

where \( rVF(T_i, T_j) \) represents the remote vulnerability factor for thread \( i \) induced by thread \( j \) which sends data to thread \( i \). \( RVF(T_i) \) iterates over all threads that sends data to thread \( i \). This is because these threads can pass a corrupted value to thread \( i \). The \( RV \) parameter represents the total number of remote memory accesses on thread \( i \).

Figure 1 represents a data sharing between three threads in a multithreaded application, where TVF value of each thread can be calculated as follows:

\[ TVF(T_1) = LVF(T_1) = LVF(A + B). \]

\[ TVF(T_2) = \left[ w_L \times LVF(T_2) \right] + \left[ w_R \times RVF(T_2) \right] \]
\[ = \left[ w_L \times LVF(T_1) \right] + \left[ w_R \times \left( RVF(T_2, T_1) + RVF(T_2, T_3) \right) \right] \]
\[ = \left[ w_L \times LVF(C + D + E) \right] + \left[ w_R \times \left( \frac{LVF(A) + LVF(F)}{2} \right) \right]. \]

\[ TVF(T_3) = LVF(T_3) = LVF(F + G). \]

To calculate TVF of a thread, the vulnerability of each thread on which that thread is dependent should be considered to capture the effect of these threads on the vulnerability of the thread investigated. Since \( T_1 \) is not dependent on other threads, its TVF is calculated using only its instructions. However, the portion of \( T_1 \) should also be considered to obtain TVF of \( T_2 \). Since \( T_2 \) reads data written by \( T_1 \) at the end of the code fragment shown as \( A \), the vulnerability of \( A \) affects the vulnerability of \( T_2 \). Similarly, the code portion \( F \) of \( T_3 \) affects the vulnerability of \( T_1 \) as well. To calculate TVF of \( T_3 \), only the code segment of the thread itself is considered as in \( T_1 \) since there is no remote thread.
III. EXPERIMENTAL SETUP

In this section, we present the details of our benchmark applications considered in our experimental evaluation, which is followed by a brief information about our simulation platform.

A. Benchmark Applications

To evaluate performance and reliability behaviors of multi-threaded applications, we select three data-intensive applications: Fast Fourier Transform, Jacobi, and Water Simulation. Note that FFT and Jacobi are used in both high end and low end computing.

1) Fast Fourier Transform: Fast Fourier Transform (FFT) is an algorithm to compute Discrete Fourier Transform (DFT), which is a mathematical transform requiring complex number calculations and used in various applications including time series, partial differential equations, and digital signal processing [12]. There are several forms of FFT algorithm; in this work, our focus is on one-dimensional, unordered, radix-2 FFT. The pattern of combination of input array elements used in this calculation is represented by a butterfly network. In a parallel algorithm, it is important to assign input elements into threads by considering the communication cost which affects both performance and reliability. We consider two parallel algorithms defined in [13]: binary-exchange and transpose algorithms. These two algorithms have different thread communication pattern.

In the binary-exchange algorithm, the array elements which are denoted as their binary representations are mapped to cores such that elements with indices having the same \( d = \log p \) most significant bits are mapped into the same core where \( p \) is the number of cores in the system. The elements that belong to different cores are combined during first \( d \) iterations, while the elements that belong to the same cores are combined in the remaining iterations. The communication between the cores only exists along these first \( d \) iterations.

The transpose algorithm which involves a matrix transposition operation requires smaller amount of communication among cores. The input array with size \( n \) is arranged in an \( \sqrt{n} \times \sqrt{n} \) two dimensional array in row major order where FFT calculation can be performed by applying FFT over the rows and then applying FFT over the columns. These array elements are mapped to \( p \) cores such that each core stores \( \sqrt{n}/p \) rows.

FFT over the rows requires no communication among the cores. After transposition, FFT over the rows (old columns) is computed to complete FFT operation. The communication between the cores is needed for only transposition operation. The input array in our calculations has \( 2^{18} \) double numbers.

2) Jacobi Kernel: Stencil computation represents a common kernel for engineering applications including multimedia processing, quantum dynamics, and electromagnetics [14]. The performance optimization of computations has been extensively studied and several code transformations have been developed to improve data locality in the calculations [15], [16], [17].

To illustrate the effect of the loop transformations, we consider 2-dimensional Jacobi code which updates the contents of grid elements by using neighbor elements in two consecutive loop iterations. Our parallel implementation is simply parallelization of two loops in the calculation.

The loop transformations used in our performance-reliability analysis are loop unrolling which reduces the loop overhead with smaller number of iterations, loop fusion which replaces multiple loops with a single one, and loop interchange which exchanges the order of two iteration variables. We consider 512x512 grid size for Jacobi computations in our experiments.

3) Water Simulation: The Water Simulation is N-body molecular dynamics application which simulates forces and potential energy of water molecules. The method of molecular dynamics is widely used to analyze the atomic structures in materials science, biochemistry, and biophysics [18].

The SPLASH-2 benchmark suite [19] has two parallel pthread versions of water simulation application: Water-n squared and Water-spatial. Water-squared is an improved version of the original Water program in SPLASH [20] and computes force and potentials in \( O(n^2) \). The computation is performed over a number of time steps by using a predictor-correction method. It improves the original version by using a locking strategy in the updates which stores a local copy of the particle accelerations as it calculates and sends to the shared copy at the end. Water-spatial is a more efficient method and uses an \( O(n) \) algorithm. It divides the molecules into a grid of cells (processors) and employs spatial locality to calculate inter-molecular forces by considering only molecules in nearby cells. Our experiments for water simulation are conducted for Water-n squared and Water-spatial programs by considering 512 water molecules and default parameters provided by the SPLASH-2 benchmark.

B. Simulation Platform

To evaluate performance and reliability of the multi-threaded applications by measuring their execution times and thread vulnerability factors respectively, we use the Simics toolset [21]. Main characteristics of the simulated multicore are given in Table I.

IV. RESULTS AND DISCUSSION

We measure execution clock cycles and calculate TVF of each thread in target applications with respect to L1 caches,
The parameters of the simulated multicore architecture are shown in Table I.

Table I

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>L1 data cache</td>
<td>16K/core</td>
</tr>
<tr>
<td>L1 cache latency</td>
<td>2-way cache</td>
</tr>
<tr>
<td>L1 cache latency</td>
<td>1 cycle</td>
</tr>
<tr>
<td>L2 shared cache size</td>
<td>4MB 4-way cache</td>
</tr>
<tr>
<td>L2 cache latency</td>
<td>10 cycles</td>
</tr>
<tr>
<td>Memory latency</td>
<td>200 cycles</td>
</tr>
</tbody>
</table>

Table II presents the vulnerability and execution time values of our benchmark applications for two, four, eight, and sixteen-thread (one thread per core) execution scenarios.

One can see from the FFT results that two parallel algorithms have different TVF values. As mentioned in Section III, the binary-exchange algorithm has more communication whereas the transpose algorithm does not have much thread communication after transpose operation. However, the transpose algorithm spends its execution cycles to transposition which requires more local resource usage. The effect of this distinct characteristics of the algorithms can be observed on the local vulnerability values as well as on the remote vulnerability values. LVF values for transpose algorithm which requires more computation are larger than LVF values for binary-exchange, especially for register resources (e.g., binary-exchange 1.27, transpose 1.56 for the 4-core case, binary-exchange 2.53, transpose 3.13 for the 8-core case). Since these parallel algorithms have different thread communication patterns, RVF values which result from communication of threads in a multithreaded application differ for these algorithms as well. The binary-exchange algorithm which requires thread communication for more iterations has larger RVF (especially for memory resource) values than the transpose algorithm which has thread communication only for one phase (before transposition) of the algorithm (e.g., binary-exchange 0.87, transpose 0.75 for the 8-core case and binary-exchange 1.64, transpose 1.43 for the 16-core case). On the other hand, the execution time values are not so distinct while binary-exchange performs well for all core cases.

The results of the Jacobi kernel reveal that loop fusion and loop unrolling improves the performance of the code by eliminating loop overhead. On the other hand, loop interchange has no significant effect on the execution time. While the fusion increases the vulnerability values (for both local and remote) which results in a tradeoff between performance and reliability, the loop unrolling, which has the largest performance gain, does not affect the vulnerability if compared with the original version. The unrolled version has similar vulnerability results, the values are even the same for some cases (1.00, 2.00, 4.03 for memory resources in the 2-core, 4-core and 8-core executions respectively).

The execution time values of the water simulation application are significantly different for two parallel versions. The difference becomes more clear as the core count rises due to the communication overhead of the nsquared algorithm. Although there is more communication overhead in the nsquared algorithm, RVF values that result from remote read operations are larger in the spatial algorithm. Since cache miss rates are smaller for nsquared version due to the lack of spatial locality, LVF values with respect to memory (cache) resources are smaller as well. Therefore, RVF values calculated by using local vulnerability become larger for the spatial version which demonstrates that the faster spatial algorithm is more vulnerable to soft errors with larger vulnerability values (e.g., nsquared 0.58, spatial 0.64 for the 2-core case and nsquared 1.01, spatial 1.20 for the 4-core case).

Since LVF values have been counted for RVF calculation (RVF value of one thread is calculated by adding TVF values of threads communicating with the target thread), only RVF values are considered as the reliability metric by ignoring very small LVF values that are not counted for RVF calculation. We also examine the vulnerability values for the resource which has the largest difference between different cases. For instance, RVF values with respect to ALU and register resources are not significantly different for two FFT algorithms (e.g., 2.21% higher in transpose algorithm in the 2-core execution for the ALU resource, 3.18% higher in binary-exchange algorithm in the 4-core execution for the register resource). On the other hand, the change in RVF values with respect to memory (cache) resources is large enough to evaluate reliability measure in tradeoff analysis. To evaluate performance-reliability tradeoff between different versions of our applications, we demonstrate the change (in percentage) for both vulnerability values and execution time of the applications (see Figure 2, Figure 3, and Figure 4). The plots provide the behavior of the applications in terms of both reliability and performance if we choose a specific version.

Figure 2 reveals that if we use the transpose algorithm instead of the binary-exchange algorithm, we should sacrifice approximately 3% performance but gain 20% reliability with lower RVF values in the 2-core case. This observation is valid for any number of cores. We can say that one may prefer the transpose algorithm rather than the binary-exchange algorithm to work with much higher reliability by accepting little amount of performance loss.

There is similar observation for the versions of the Jacobi...
Since the loop unrolling gives the best performance among the other loop transformations, we evaluate the vulnerability and performance change if one prefers loop unrolling instead of other versions. Figure 3 presents the change in both RVF and execution time values for loop unrolling and other code versions (original, fused, and interchanged respectively). The vulnerability values do not differ much for each case. Specifically, the values are smaller than 5% even there is almost no change if we compare the original version with the unrolled one. On the other hand, the performance gain is obvious if the unrolled version is used. For instance, if one employs the unrolled version instead of the interchanged one, about 50% speedup is possible by sacrificing only 5% reliability.

Although the choice is clear for two applications in terms of performance and reliability, water simulation application reveals more interesting results which yield a tradeoff between performance and reliability concerns. Figure 4 demonstrates this tradeoff between two different water simulation algorithms. While spatial has larger performance advantage, nsquared is more reliable with similar rates. For the 8-core execution, one should trade 27% performance gain with 21% reliability loss if he selects spatial algorithm. We cannot easily conclude that one version satisfies both performance and reliability constraints. While the safety-critical systems with higher reliability needs may prefer the nsquared version by sacrificing some performance, the systems for which the performance is the most crucial factor may opt for the spatial version, which has higher performance but is much more vulnerable to hardware errors. However, it is difficult to trade the vulnerability with performance for the systems which do not have evident performance and reliability needs.

V. Conclusion

In this paper, we perform a performance-reliability analysis of different multithreaded applications running on multicore architectures. While the performance of the applications is measured by execution clock cycles, we use Thread Vulnerability Factor metric to evaluate the relative reliability of multithreaded applications. Using these values gathered from experimental evaluation, we conduct a performance-reliability tradeoff analysis which compares the different parallel versions of three applications in terms of reliability as well as performance. Our results indicate that the choice is clear for FFT and Jacobi Kernel. The transpose algorithm for FFT calculation results in less than 5% performance loss while the vulnerability increases by 20% instead of binary-exchange algorithm. One can prefer transpose algorithm for better reliability by sacrificing little performance. The unrolled Jacobi code reduces execution time up to 50% by not effecting vulnerability values. However, the tradeoff is more interesting for Water Simulation application. While nsquared version reduces the vulnerability values significantly, it increases execution time with similar rates compared to spatial version. One should trade performance with reliability to choose one version of the application.

<table>
<thead>
<tr>
<th></th>
<th>FF</th>
<th>WATER</th>
<th>JACOBIAN</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>binary-exchange</td>
<td>transpose</td>
<td>nsquared</td>
</tr>
<tr>
<td>2 core</td>
<td>ALU</td>
<td>0.61</td>
<td>0.61</td>
</tr>
<tr>
<td></td>
<td>Register</td>
<td>0.62</td>
<td>0.76</td>
</tr>
<tr>
<td></td>
<td>Memory</td>
<td>0.35</td>
<td>0.33</td>
</tr>
<tr>
<td></td>
<td>ALU</td>
<td>0.37</td>
<td>0.38</td>
</tr>
<tr>
<td></td>
<td>Memory</td>
<td>0.29</td>
<td>0.23</td>
</tr>
<tr>
<td>Execution time</td>
<td>32.61</td>
<td>33.35</td>
<td>9.78</td>
</tr>
<tr>
<td>4 core</td>
<td>ALU</td>
<td>1.21</td>
<td>1.22</td>
</tr>
<tr>
<td></td>
<td>Register</td>
<td>1.27</td>
<td>1.56</td>
</tr>
<tr>
<td></td>
<td>Memory</td>
<td>1.00</td>
<td>1.06</td>
</tr>
<tr>
<td></td>
<td>ALU</td>
<td>0.82</td>
<td>0.84</td>
</tr>
<tr>
<td></td>
<td>Register</td>
<td>0.68</td>
<td>0.66</td>
</tr>
<tr>
<td></td>
<td>Memory</td>
<td>0.52</td>
<td>0.41</td>
</tr>
<tr>
<td>Execution time</td>
<td>16.32</td>
<td>16.68</td>
<td>5.46</td>
</tr>
<tr>
<td>8 core</td>
<td>ALU</td>
<td>2.43</td>
<td>2.45</td>
</tr>
<tr>
<td></td>
<td>Register</td>
<td>2.53</td>
<td>3.13</td>
</tr>
<tr>
<td></td>
<td>Memory</td>
<td>2.00</td>
<td>2.12</td>
</tr>
<tr>
<td></td>
<td>ALU</td>
<td>1.66</td>
<td>1.63</td>
</tr>
<tr>
<td></td>
<td>Register</td>
<td>1.16</td>
<td>1.19</td>
</tr>
<tr>
<td></td>
<td>Memory</td>
<td>0.87</td>
<td>0.75</td>
</tr>
<tr>
<td>Execution time</td>
<td>8.17</td>
<td>8.35</td>
<td>3.29</td>
</tr>
<tr>
<td>16 core</td>
<td>ALU</td>
<td>4.87</td>
<td>4.89</td>
</tr>
<tr>
<td></td>
<td>Register</td>
<td>5.14</td>
<td>6.35</td>
</tr>
<tr>
<td></td>
<td>Memory</td>
<td>2.86</td>
<td>4.23</td>
</tr>
<tr>
<td></td>
<td>ALU</td>
<td>3.26</td>
<td>3.25</td>
</tr>
<tr>
<td></td>
<td>Register</td>
<td>2.22</td>
<td>2.18</td>
</tr>
<tr>
<td></td>
<td>Memory</td>
<td>1.64</td>
<td>1.45</td>
</tr>
<tr>
<td>Execution time</td>
<td>4.09</td>
<td>4.18</td>
<td>2.55</td>
</tr>
</tbody>
</table>

**TABLE II**

**TVF VALUES AND EXECUTION TIME OF OUR BENCHMARK APPLICATIONS**
This research was supported by The Scientific and Technological Research Council of Turkey (TUBITAK) with a research grant (Project Number: 108E035).

ACKNOWLEDGMENT

This research was supported by The Scientific and Technological Research Council of Turkey (TUBITAK) with a research grant (Project Number: 108E035).

REFERENCES


Fig. 3. The change in percentage of RVF values and execution time for loop transformations of Jacobi code

Fig. 4. The change in percentage of RVF values and execution time for versions of water simulation