

DAL-SMC: Distributed Statistical Model Checking with Abstraction and Learning

Kaiqiang Jiang, Yi Ao, Ping Huang, Hui Zan, Dehui Du*

Shanghai Key Laboratory of Trustworthy Computing, School of Computer Science and Software Engineering,
East China Normal University, Shanghai, 200062, China
Email: dhdu@sei.ecnu.edu.cn

Abstract—The core idea of Statistical Model Checking (SMC) is to decide whether the stochastic model satisfies a given property or to evaluate its probability of satisfaction by combining statistical techniques with Monte-Carlo simulation on model traces. However, SMC still encounters performance bottleneck due to the consumption of the extremely large number of traces, each of which itself could be extremely time-consuming. To solve these problems, we have proposed an optimized SMC approach called AL-SMC to reduce the number of traces in our previous work. In order to reduce the time consumption for generating a single trace further, we propose a general framework for distributed SMC based on master/slaves architecture without introducing bias. A series of algorithms are introduced to show that bayesian interval estimation (BIE) algorithm and AL-SMC are easily parallelizable on our general framework. Besides, we propose parameter optimization approach with a genetic algorithm to reduce the statistical error of distributed AL-SMC (DAL-SMC). We also implemented DAL-SMC algorithms in our ModanaOnline platform to support the automatic process. To illustrate the feasibility of our approach, three benchmarks are presented to compare the number of simulation traces, time consumption and statistical error between DAL-SMC and classic SMC algorithms. The experiment results show that the time consumption of our toolset is effectively reduced and the accuracy is ensured within an acceptable error bound.

Keywords—Statistical model checking, Statistical abstraction, Learning, Distributed technology, Bayesian interval estimation algorithm

I. INTRODUCTION

Statistical Model Checking techniques (SMC) [1]–[3] can be seen as a trade-off between testing and formal verification. Recently, SMC has been an alternative to standard model-checking in order to avoid the state-space explosion problem, especially for verifying Cyber-physical Systems (CPSs) [4]. The core idea of SMC is to decide whether the stochastic model satisfies a given property or to evaluate its probability of satisfaction by combining statistical techniques with Monte-Carlo simulation on model traces. Nowadays, SMC is getting increasing industrial attentions and there are many model checkers which supports SMC techniques to analyze the stochastic model more effectively (e.g., Uppaal-SMC [5], Prism [6]).

CPS focus on the coupling of cyber part viewed as distributed computation units and physical part covering the environment affecting the running of the system. The modeling

of stochastic behaviors for CPS might be highly cumbersome [7] and the analysis of these models demands extremely high confidence [8]. SMC still encounters the performance bottleneck for verifying CPS. There are two factors having a direct influence on the performance of SMC, one is the number of simulation traces, the other is the length of a single trace. In this paper, we focus on these two factors to improve the efficiency of SMC. Figure 1 is the technology roadmap of our approach. A statistical model checker contains three components: *simulator*, *SMC algorithm* and *model checker*. The *simulator* generates simulation traces which are fed to the *model checker*. With model checking technology, it verifies whether the trace satisfies the property, and returns observations. The *SMC algorithm* collects observations obtained from a *model checker* and computes the probability with statistical testing. To reduce the number of simulation traces, we have proposed abstraction and learning technique with *SMC algorithm* called AL-SMC [9]. With many experiments, we find that AL-SMC effectively reduces the number of traces, and improves the performance of SMC. As observed in [10], SMC can be distributed based on master/slave architecture where several slave computers are used to generate simulation traces. Inspired by their work, we apply distributed technology on *simulator* to reduce the time consumption for generating a single trace. Further, we propose the distributed Bayesian Interval Estimation (BIE) algorithm [11]. In this paper, we combine distributed technology with AL-SMC technique, which is called distributed AL-SMC (DAL-SMC). DAL-SMC reduces both the number of simulation traces and the time consumption for generating a single trace.

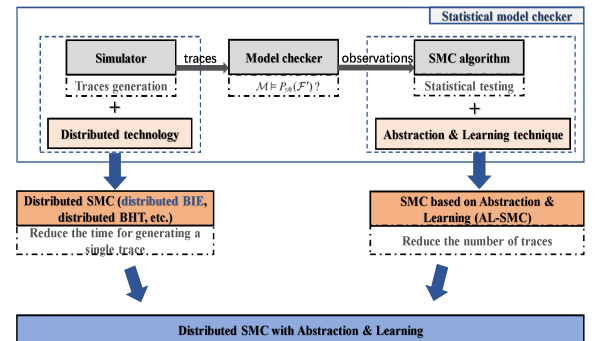


Fig. 1. Technology roadmap.

The main contributions of this paper include:

*Corresponding Author

- We propose a novel verification framework, which applies distributed technology to improve the efficiency of SMC.
- We propose the distributed BIE and DAL-SMC algorithms based on the framework. The parameter optimization method is introduced to reduce the statistical error of DAL-SMC. This work is an extension of our previous work [9].
- The distributed BIE and DAL-SMC algorithms are implemented in our ModanaOnline platform [12] (<http://github.com/ECNU-MODANA/Modana-Online>) to support the automatic process.
- Several experiments are conducted to demonstrate that our approach effectively reduces the time consumption within an acceptable error bound.

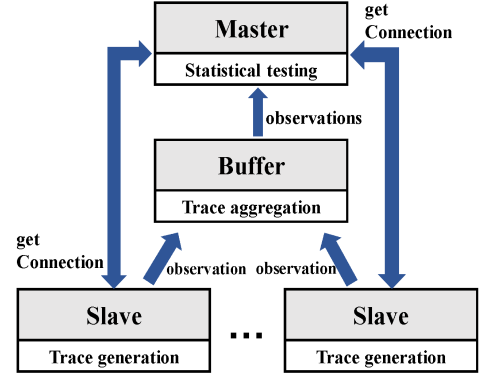
The remainder of this paper is organized as follows. In Section 2, we present the framework of our approach, and several core algorithms of distributed BIE and DAL-SMC in details. Parameter optimization method of DAL-SMC is also presented. Section 3 provides the algorithm analysis of DAL-SMC. Section 4 presents the implementation of our approach in ModanaOnline platform. Several experiments are conducted with three benchmarks. The experimental results show that our DAL-SMC is efficient and feasible. The related work is discussed in Section 5. Finally, conclusions and directions of future research are presented in Section 6.

II. DISTRIBUTED BAYESIAN INTERVAL ESTIMATION AND DAL-SMC

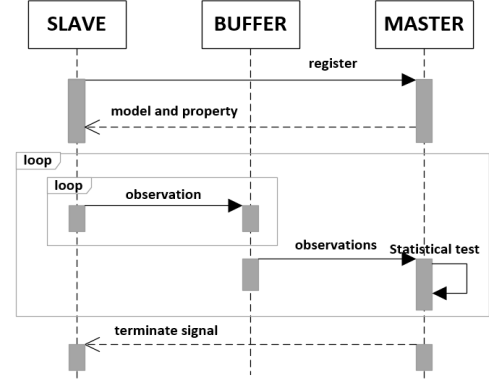
In this section, we first introduce the general framework of distributed SMC based on master/slaves architecture. Next, we apply the framework to BIE algorithm and present the core algorithms of distributed BIE. With the help of distributed BIE, the time for generating a single trace is reduced. Besides, in order to reduce the number of traces generated by distributed BIE, we propose the DAL-SMC technique and present the core algorithms of DAL-SMC, which is an improvement of distributed BIE. However, we found that DAL-SMC has large statistical error compared with distributed BIE. To solve this problem, we propose the parameter optimization with genetic algorithm to reduce the statistical error of DAL-SMC.

A. Framework of distributed SMC

SMC encounters the performance bottleneck in that the high confidence required by an answer may demand large number of traces, each of which itself may be time-consuming. Fortunately, we find that statistical methods which use independent traces are trivially parallelizable. Therefore, we can solve this problem by parallel computation based on master/slaves architecture (Figure 2(a)): multiple slave processes register their abilities to generate traces. The master process is used to collect traces and perform the statistical test. When using distributed sampling with sequential test, the number of simulation traces is unknown in advance. Therefore, it is important to avoid introducing bias when collecting the traces generated by the slave processes. To solve this problem, we adopt the method proposed in [13] which aggregates traces by batches and a buffer.



(a) Distributed architecture for trace generations



(b) Communication protocol

Fig. 2. Framework of distributed SMC.

For Unified Temporal Stochastic Logic (UTSL) model checking [1], each observation involves the generation of a trajectory prefix through the discrete event simulation and the verification of a path formula over the generated trajectory prefix. Figure 2(b) illustrates the communication protocol of distributed acceptance sampling: (i) Multiple slave processes register their abilities with the master process. The master process sends the model and property to the slaves. (ii) The slave processes generate observations and send them to the buffer which is used to aggregate observations, and then the buffer send observations to the master. (iii) The master process executes statistical test. Until the statistical test terminates, it sends terminate signal to the slaves. The framework of distributed SMC is general and flexible. Based on the framework, we present our distributed BIE algorithm in the next subsection. Actually, you can adopt the framework to any other SMC algorithm, not just limits to BIE.

B. Distributed bayesian interval estimation

We can compute an interval estimate of $p = Prob(M \models \phi)$ with BIE which is a faster statistical model checking algorithm based on estimation. ϕ is a Probabilistic Bounded Linear Temporal Logic (PBLTL) formula [14]. M is a Stochastic Hybrid Automata (SHA) model [15]. BIE algorithm (Algorithm 1) iteratively generates trace, verifies whether it satisfies ϕ , and then calls statistical test algorithm (Algorithm 2) to compute the estimate probability p' , interval (t_0, t_1) of width 2δ and posterior probability γ . Until $\gamma \geq c$, the algorithm terminates

Algorithm 1: Bayesian estimation algorithm

Input: BLTL property ϕ , half-interval size $\delta \in (0, 1/2)$, interval coverage coefficient $c \in (1/2, 1)$, Prior Beta distribution with parameters α, β for the (unknown) probability p that the system satisfies ϕ
Output: An interval (t_0, t_1) of width 2δ with posterior probability at least c , estimate p' for the true probability p
 $x = 0; n = 0;$
repeat
 $\sigma = \text{draw a simulation of the model};$
 if $\sigma \models \phi;$
 then
 $x = x + 1;$
 end
 $n = n + 1;$
 $t_0, t_1, p', \gamma = \text{CallAlgorithm2}(\delta, \alpha, \beta, x, n);$
until $\gamma \geq c;$

Algorithm 2: Statistical test algorithm

Input: half-interval size δ , α , β , positive trace number x , total trace number n
Output: An interval (t_0, t_1) of width 2δ , estimate probability p' , posterior probability γ
 $p' = (x + \alpha) / (n + \alpha + \beta);$
 $(t_0, t_1) = (p' - \delta, p' + \delta);$
if $t_1 > 1;$
 then
 $(t_0, t_1) = (1 - 2\delta, 1);$
 else
 if $t_0 > 0;$
 then
 $(t_0, t_1) = (0, 2\delta);$
 end
 end
 end
 $\gamma = \int_{t_0}^{t_1} f(u | x_1, \dots, x_n) du;$

and returns t_0, t_1 and p' , otherwise it generates another trace and repeats.

Based on the BIE algorithm, we implement distributed BIE algorithm with the help of our distributed SMC framework. Algorithm 3 is the slave algorithm of distributed BIE. B is the size of batch which aggregates the outcomes x to reduce communication. The algorithm iteratively generates trace and verifies whether it satisfies ϕ . Until $runs == B$, the algorithm terminates and returns the number of positive traces $sats$, otherwise it generates another trace and repeats.

Algorithm 4 is the master algorithm of distributed BIE. K is the size of buffer which is used to improve concurrency since the slaves can do K runs ahead of the slowest slave, and N is the number of slaves. The main steps of master algorithm are as follows: (i)The slave processes register their abilities with the master. The master sends model and property to the slaves. (ii)The master algorithm chooses a slave process randomly, and then it updates batch and buffer only if the buffer size of the slave is smaller than K . (iii)If the buffers of all slaves are not

Algorithm 3: Slave algorithm of distributed BIE

Input: BLTL property ϕ , model M , batch size B
Output: The number of positive traces $sats$
 $sats = 0, runs = 0;$
repeat
 $\sigma := \text{getSimulationTrace}(M);$
 if $\sigma \models \phi;$
 then
 $sats ++;$
 end
 $runs ++;$
until $runs == B;$

Algorithm 4: Master algorithm of distributed BIE

Input: BLTL property ϕ , model M , half-interval size $\delta \in (0, 1/2)$, interval coverage coefficient $c \in (1/2, 1)$, Prior Beta distribution with parameters α, β for the (unknown) probability p that the system satisfies ϕ , buffer size K , batch size B , the number of nodes N
Output: An interval (t_0, t_1) of width 2δ with posterior probability at least c , estimate p' for the true probability p
 $x = 0; n = 0;$
 $\text{batch}[0 \dots N-1][0 \dots K-1], \text{buffer}[0 \dots K-1], \text{slave}[0 \dots N-1];$
for $\text{slave}[i] \in \text{slave}[0 \dots N]$ **do**
 $\text{getConnection}(\text{slave}[i]);$
 $\text{sendModelandProperty}(M, \phi, \text{slave}[i]);$
end
repeat
 $\text{node} = \text{random}(0, N-1);$
 if $\text{buffer}[\text{node}] < K;$
 then
 $\text{batch}[\text{node}][\text{buffer}[\text{node}]] =$
 $\text{CallAlgorithm3}(\text{node});$
 $\text{buffer}[\text{node}] ++;$
 end
 if $\text{forall}(i < N) \text{buffer}[i] > 0;$
 then
 for $i < N$ **do**
 $x += \text{batch}[i][0];$
 $n += B;$
 $\text{buffer}[i] --;$
 $\text{batch}[i][\text{buffer}[i]] = 0;$
 end
 end
 $t_0, t_1, p', \gamma = \text{CallAlgorithm2}(\delta, \alpha, \beta, x, n);$
until $\gamma \geq c;$

empty, the algorithm updates the value of n and x . (iv)Call algorithm 2 to compute the estimate probability p' , interval (t_0, t_1) of width 2δ and posterior probability γ . Until $\gamma \geq c$, the algorithm terminates and returns t_0, t_1 and p' , otherwise it repeats step (ii), (iii) and (iv).

C. Distributed AL-SMC

BIE algorithm has its shortcoming, because it needs more traces when it verifies the property whose probability is

close to 0.5 [11]. We have proposed AL-SMC technique to solve this problem in our recent work [9]. The framework of AL-SMC is shown in Figure 3. AL-SMC includes three main steps: (i) Sample traces are drawn from the model and input into the abstraction process to obtain abstract traces. The abstraction process includes three steps: **property-based projection**, **PCA-based dimension reduction** [16] and **key states extraction**. (ii) **Building and optimization of Prefix Frequency Tree (PFT)** applies the learning technique [17] to construct optimized PFT with abstract traces. By means of PFT, the original probability space is divided into several **sub-spaces**. (iii) **Probability evaluation via multi-BIE** invokes multiple BIE algorithms to evaluate the probabilities of sub-spaces in parallel. The detail of AL-SMC can be found in [9].

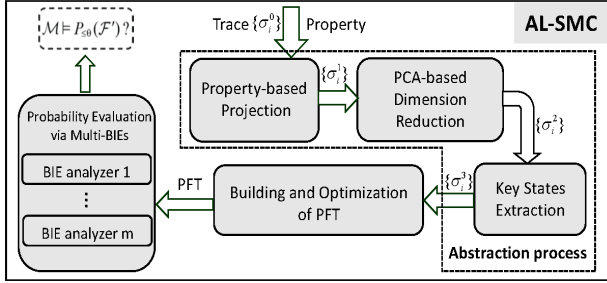


Fig. 3. The framework of AL-SMC.

AL-SMC reduces the number of simulation traces compared with BIE algorithm, especially the verification result is close to 0.5. Therefore, the number of traces and the time consumption for generating a single trace will be effectively reduced if we apply the distributed SMC framework into AL-SMC. Fortunately, we find that AL-SMC can be parallelized with our distributed SMC framework. Therefore, we propose DAL-SMC, whose core algorithms are shown in Algorithm 5 and Algorithm 6.

Algorithm 5 is the master algorithm of DAL-SMC, where SN is the number of sample traces in abstraction process. The master algorithm contains the following steps: (i) The master process generates a set of sample traces $\sigma[0 \dots SN - 1]$ which are fed to abstraction process to obtain a set of abstract traces $\sigma'[0 \dots SN - 1]$. And then, the optimized PFT is constructed with $\sigma'[0 \dots SN - 1]$. (ii) The slave processes get connection with the master. The master process sends model, property and PFT to the slaves. (iii) The algorithm chooses a slave randomly, and then updates $batch[i][j]$ only if the buffer size of this slave is smaller than K . (iv) If the buffers of all slaves are not empty, the algorithm evaluates the probability and obtains $p'[j]$ and $\gamma[j]$ of each sub-space. If $\gamma[j] > c$, the evaluation of j th sub-space is terminated. (v) Until the evaluation of all sub-spaces are terminated, the algorithm estimates the probability of the whole space with $p' := \sum_{i=0}^{S-1} p[i]$, otherwise it repeats step (iii), (iv) and (v).

Algorithm 6 is the slave algorithm of DAL-SMC. T is the optimized PFT which is constructed in master algorithm. d is the number of leaf nodes in optimized PFT tree, i.e., the number of sub-spaces. $sats[i]$ is the number of satisfying traces in i th sub-space. The slave process iteratively generates trace σ which is the input of abstraction process to obtain the abstract

Algorithm 5: Master algorithm of DAL-SMC

Input: BLTL property ϕ , model M , half-interval size $\delta \in (0, 1/2)$, interval coverage coefficient $c \in (1/2, 1)$, Prior Beta distribution with parameters α, β for the (unknown) probability p that the system satisfies ϕ , buffer size K , batch size B , the number of nodes N , the number of sample traces SN

Output: Prefix frequency tree T , estimate p' for the true probability p

```

 $\sigma[0 \dots SN - 1] = \text{getSampleTraces}(M);$ 
 $\sigma'[0 \dots SN - 1] = \text{abstractTraces}(\sigma[0 \dots SN - 1]);$ 
 $T = \text{ConstructPFT}(\sigma'[0 \dots SN - 1]);$ 
 $d = \text{getSubSpacesNum}(T);$ 

```

for $slave[i] \in slave[0 \dots N]$ **do**

```

     $\text{getConnection}(slave[i]);$ 
     $\text{sendModelAndPropertyAndPFT}(M, \phi, T, slave[i]);$ 

```

end

```

 $x[0 \dots d-1], n;$ 

```

```

 $batch[0 \dots N-1][0 \dots K-1][0 \dots d-1], buffer[0 \dots K-1],$ 
 $slave[0 \dots N-1];$ 

```

repeat

```

     $node = \text{random}(0, N-1);$ 

```

```

    if  $buffer[node] < K$  ;

```

then

```

         $batch[node][buffer[node]][0 \dots d-1] =$ 

```

```

        CallAlgorithm6( $node$ );

```

```

         $buffer[node]++;$ 

```

end

```

    if  $\text{forall}(i < N) buffer[i] > 0$  ;

```

then

```

        for  $i < N$  do

```

```

             $x[0 \dots d-1] += batch[i][0][0 \dots d-1];$ 

```

```

             $n += B;$ 

```

```

             $buffer[i]--;$ 

```

```

             $batch[i][buffer[i]] = \Phi;$ 

```

end

end

```

     $ter[0 \dots d-1] = \text{false};$ 

```

```

     $j = \text{findUnTerminateBIE}(ter[0 \dots d-1]);$ 

```

```

     $p'[j], \gamma[j] = \text{CallAlgorithm2}(\delta, \alpha, \beta, x[j], n);$ 

```

```

    if  $\gamma[j] > c$ ;

```

then

```

             $ter[j] = \text{true};$ 

```

end

```

until  $\text{forall}(ter[i] \in ter[0 \dots d-1]) == \text{true};$ 

```

```

 $p' = \sum_{i=0}^{d-1} p'[i];$ 

```

trace σ' . If σ' satisfies ϕ , the algorithm finds a sub-space with σ' and T . Until $runs == B$, the algorithm terminates and returns $sats[0 \dots S - 1]$, otherwise, it generates another trace and repeats.

DAL-SMC is more efficient than distributed BIE with the help of abstraction and learning techniques, and the advantages of DAL-SMC are obvious. Firstly, the slave process of DAL-SMC generates less traces, particularly in verifying the property whose probability is close to 0.5. Secondly, the master of DAL-SMC evaluates the probability with multiple BIEs,

Algorithm 6: Salve algorithm of DAL-SMC

Input: BLTL property ϕ , model M , batch size B , prefix frequency tree T , the number of sub-spaces d

Output: The number of positive traces in sub-spaces $sats[0\dots d-1]$

$sats[0\dots d-1], runs = 0;$

repeat

$\sigma = \text{getSimulationTrace}(M);$

$\sigma' = \text{abstractTrace}(\sigma);$

if $\sigma \models \phi;$

then

$i = \text{findSubSpace}(\sigma', T);$

$sats[i] ++;$

end

$runs ++;$

until $runs == B;$

thus the statistic process is faster than that of distributed BIE algorithm. However, DAL-SMC has bigger statistical error due to the usage of multi-BIE in statistic process. In the remainder of the paper, we focus on the performance analysis of DAL-SMC. In the next subsection, we will introduce our parameter optimization method to reduce the statistical error of DAL-SMC.

D. Parameter optimization of DAL-SMC

In order to reduce the statistical error of DAL-SMC, we introduce two parameter optimization methods: r **optimization** is used to divide the probability space more evenly, and δ **prediction** is used to predict half-interval size of the BIE algorithm used in each sub-space.

r **optimization:** For DAL-SMC, we divide the probability space into several sub-spaces by building and optimizing the PFT. Note that the number of sub-spaces is determined by the leaf nodes of optimized PFT. Therefore, we need input the reduction degree r of PFT into the optimization algorithm to generate optimized PFT. However, the value of r is difficult to predict. On one hand, if the value of r is too large, we will obtain a large number of sub-spaces and the error of the algorithm will be enlarged. On the other hand, if the value of r is too small, we will obtain few sub-spaces and the efficiency of the algorithm will be reduced. To solve the problem, we obtain the optimized value of r with genetic algorithm [18].

$$r_k = M - \sum_{i=1}^k \sum_{j=1}^k |T_i - T_j| \quad (1)$$

Suppose k is the population quantity in genetic algorithm, i.e., the number of sub-spaces of each generation. T_i is the number of satisfying traces in i th sub-space. In order to obtain the optimal r , we need to divide the probability space more evenly and ensure a moderate number of sub-spaces. Therefore, we adopt formula 1 as evaluation function and $k \geq 6$ and $k \leq 10$ as constraint function of genetic algorithm. M is a large positive number, if we divide the probability space more evenly, the value of $\sum_{i=1}^k \sum_{j=1}^k |T_i - T_j|$ is smaller. Thus, we obtain the optimal r which helps to get the maximum M .

TABLE I. THE TIME AND SPACE COMPLEXITY OF DAL-SMC.

Algorithm phase	Time	Space
Trace abstraction	$O(mn) + O(\min(k^3, n^3))$	$O(k^2)$
PFT construction	$O(mn) + O(d \log d)$	$O(\log d)$
Probability evaluation	$O(B * (\log d + i))$	$O(1)$

δ **prediction:** Through building and optimizing of PFT, we obtain several sub-spaces. Then we execute BIE algorithm for each sub-space, each BIE algorithm has its half-interval size and interval coverage coefficient. In algorithm 6, we suppose all BIE algorithms have the same δ and c . However, the probabilities of some sub-spaces may have a big difference. For instance, we suppose the half-interval sizes of all BIE algorithms are 0.1, but there may be a sub-space whose probability is less than 0.1, thus the half-interval size of this BIE algorithm is unreasonable. It will lead to a large statistical error. To solve this problem, we use the leaf nodes of PFT to predict the half-interval size of m th BIE algorithm as shown in formula 2. Note that k is the number of sub-spaces, T_m is the number of satisfying traces in m -th sub-space, and N_i is the number of total traces in i -th sub-space. η is half-interval rate, the η is bigger, the probability is more precise. By means of formula 2, the half-interval size of each BIE is more accurate.

$$\delta_m = T_m / \sum_{i=1}^k N_i / \eta \quad (2)$$

III. ALGORITHM ANALYSIS OF DAL-SMC

A. Time and space complexity

We analyse the time and space complexity of DAL-SMC as shown in Table I.

(i) The time and space complexity of abstraction process are $O(mn) + O(\min(k^3, n^3))$ and $O(k^2)$ respectively, where m denotes the length of the trace, n denotes the number of sampling traces and k denotes the dimension of each trace.

(ii) The time and space complexity of PFT construction are respectively $O(mn) + O(d \log d)$ and $O(\log d)$, where d denotes the number of leaf nodes in PFT.

(iii) Suppose the iterations of BIE algorithm is B , the time complexity of each statistical test iteration is $O(i)$, and the time of searching leaf node is $\log d$. Therefore, the time complexity of probability evaluation is $O(B * (\log d + i))$.

B. Error bound

Models in step i and ii of Algorithm 5 are probabilistically equivalent in terms of a certain property. Therefore, the statistical error is only generated in probability evaluation. We use multiple BIEs to evaluate the probability in DAL-SMC, therefore the error is enlarged compared with distributed BIE. Suppose the half-interval size of each BIE is δ and the number of BIEs is M , thus the error of multi-BIE is less than $\delta * M$. Besides, we use δ prediction method in section 2.4 to reduce the statistical error. Consequently, the error (ξ) of DAL-SMC with parameter optimization satisfies the formula 3.

$$|\xi| \leq \sum_{m=1}^M (T_m / \sum_{i=1}^k N_i / \eta) \quad (3)$$

IV. IMPLEMENTATION AND BENCHMARK EXPERIMENTS

The distributed SMC framework has been implemented in our ModanaOnline platform which is an online platform for modeling and analysis CPS. We have implemented the core algorithms of distributed BIE and DAL-SMC in this platform. To illustrate the feasibility of our approach, we explore some experiments with three benchmarks: train-gate [?], energy-aware building [19] and robots path planning [20].

A. DAL-SMC implementation

In our previous work, we have implemented Modana platform which is an integrated modeling and verification environment for CPS [12]. Recently, we implement the on-line version of Modana, called ModanaOnline, in which the distributed BIE and DAL-SMC are implemented. ModanaOnline is a web project, whose back end is implemented in Java based on SpringMVC, Spring and Mybatis. The front end is implemented in JavaScript based on AngularJS which supports information transmission of distributed framework with web service. Figure 4 is the user interface of DAL-SMC in ModanaOnline. Users can import the model files(such as uppaal [?] and prism [6]) and the property to verify the model. Besides, there are several parameters v, t, s, n, η, c should be customized, in which v, t, s are used in abstraction and leaning phase, n, η, c are used in probability evaluation phase where,

(i) v denotes the number of sample traces in abstract process, t denotes the threshold in PCA-based dimension reduction and s denotes the number of extracted states during the key states extraction.

(ii) n denotes the number of slaves, η denotes the half-interval rate in Section 2.4, and c denotes the interval coverage coefficient of BIE algorithm.

Users can verify the property with DAL-SMC and generate a bar graph as shown in Figure 4. It shows the distribution of traces more obviously with the bar graph.

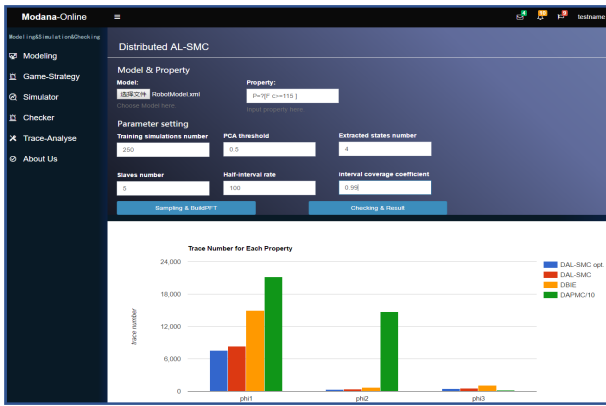


Fig. 4. The user interface of DAL-SMC.

B. Benchmark experiments

Uppaal-SMC [5] is a new version of UPPAAL which supports SMC and adopts many SMC algorithms (BHT [25], SPRT [24], BIE [11], APMC [?] etc.). In this paper, we model the benchmark with Uppaal-SMC, and then import the model

(.xml) into our platform to verify the properties. Here, we use a simple benchmark to exhibit the distribution of traces in each slave and compare the probability partition between DAL-SMC with parameter optimization (DAL-SMC opt.) and DAL-SMC. Besides, two complex benchmarks are also introduced to compare the efficiency and accuracy among distributed BIE, DAL-SMC, DAL-SMC opt. and distributed APMC (DAPMC) which is a classical quantitative SMC algorithm.

1) *Train-gate*: A number of trains are approaching a gate on which there is only one track, gate controls the trains to avoid collisions, and restarts them when it is possible to make sure that trains will eventually cross the gate. Figure 5(a) is the template of the train. Trains delay according to an exponential distribution and synchronize with the gate. The gate keeps track of the trains with an internal queue data structure as shown in Figure 5(b). We use Formula 4 to evaluate the probability of Train(0) crossing the gate:

$$P_{=?}(F^{\leq 100} \text{Train}(0).Cross) \quad (4)$$

The PBLTL property is used to evaluate the probability

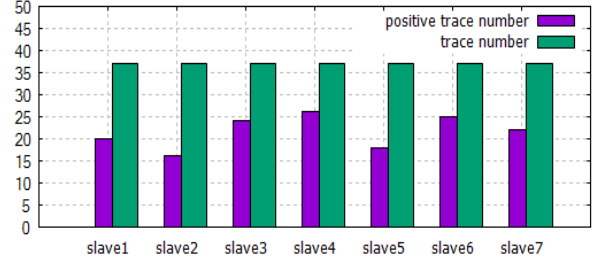


Fig. 6. Trace number of each slave

interval of Train(0) crossing the gate in 100 time units. The evaluation result is in $[0.52707, 0.626969]$ with half-interval size of ± 0.05 and interval coverage coefficient of 95%. We plot the number of traces and satisfying traces of each slave in Figure 6. It shows that the slaves generate the same number of traces, however, the number of satisfying traces are not equal. Besides, in order to compare the probability partition between DAL-SMC and DAL-SMC opt, we plot the probability of each sub-space as shown in Figure 7. Figure 7(a) and Figure 7(b) are the probability of each sub-space in DAL-SMC and DAL-SMC opt. respectively. We find that the probability distribution of DAL-SMC opt. is more evenly than that of DAL-SMC, therefore, the parameter optimization is effective. In the next subsections, we will use two complex CPS benchmarks to compare the performance of distributed BIE, DAL-SMC, DAL-SMC opt. and DAPMC.

2) *Energy-aware building*: Energy-aware buildings play an important role in achieving an energy efficient society. The goal is to evaluate and compare the energy consumption of various control strategies with varying environmental settings. There are five SHA models: *room temperature*, *heater*, *controller*, *weather* and *user profile*. Figure 8 shows the main SHA templates for energy-aware building. In Figure 8(a), the room needs to be heated when the temperature is lower than a threshold. The heater moves between locations "Off" and "On" based on the temperature thresholds $on[r]$ and $off[r]$, where r denotes the number of heated room. The central controller

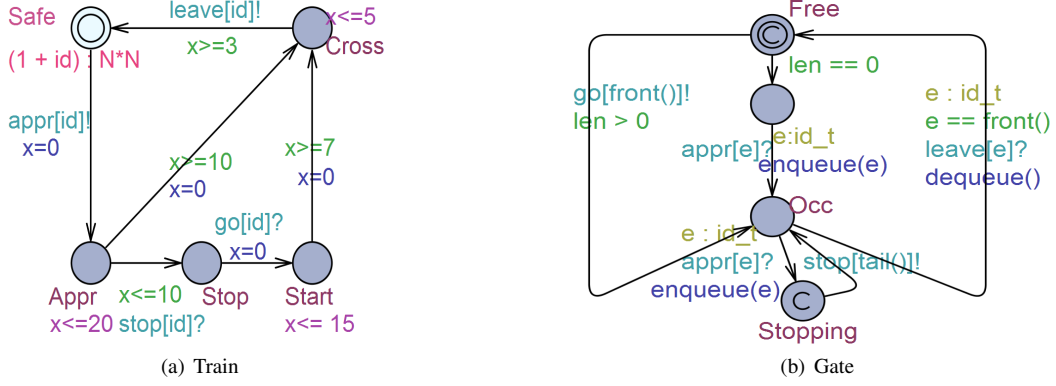


Fig. 5. The SHA templates for train-gate.

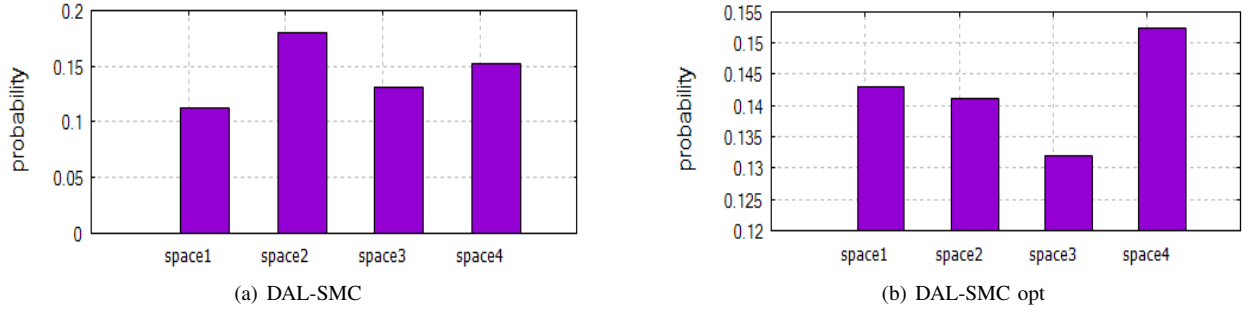


Fig. 7. Probability of each sub-space.

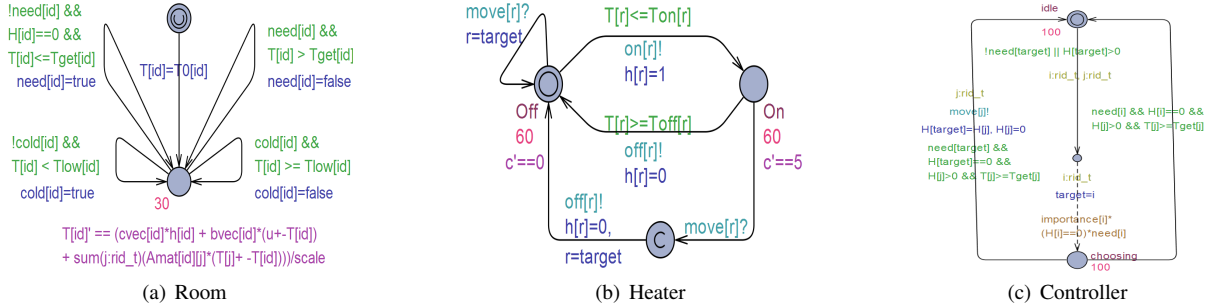


Fig. 8. The main SHA templates for energy-aware building.

TABLE II. PROPERTIES OF ENERGY-AWARE BUILDING

PID	(δ, c)	Property
ϕ_1	(0.05, 0.99)	$P_{=?}(F^{\leq 48} \text{energy} \geq 210)$
ϕ_2	(0.01, 0.99)	$P_{=?}(F^{\leq 48} \text{discomfort} \geq 15)$
ϕ_3	(0.02, 0.9)	$P_{=?}(F^{\leq 48} \text{discomfort} \leq 15 \wedge \text{energy} \geq 170)$

decides how to move the heater from one room to another room as shown in Figure 8(c).

The experiment has been performed on five slaves on a cluster with Intel Core(TM) i7-4790 (octa-cores at 3.6GHz) interconnected with infiniband. To compare the efficiency and accuracy of the algorithms, three properties are verified, which are listed in Table II. δ and c denotes half-interval size and interval coverage coefficient respectively.

We execute each algorithm many times, and compare them

in three aspects: the number of traces, time consumption and statistical error. In order to analyse the statistical error of algorithm, we verify the property with high interval coverage coefficient and small half-interval size to obtain the probability (P_r). We suppose P_r is the true probability, therefore, the statistical error of each algorithm is $P_r - P_a$, where P_a is the estimation of the true probability. Figure 9 shows the number of traces, time consumption and statistical error of each algorithm.

Figure 9(a) shows the trace number of energy-aware building benchmark generated by each algorithm. We can find that DAPMC algorithm needs 200000 traces to verify property ϕ_2 , however, distributing BIE (DBIE) algorithm only needs 20000 traces. DAL-SMC and DAL-SMC opt. need less traces (about 10000). The time consumption of each algorithm is shown in Figure 9(b). The time consumption for verifying property ϕ_2 with BIE algorithm is 6000 seconds, while it is around

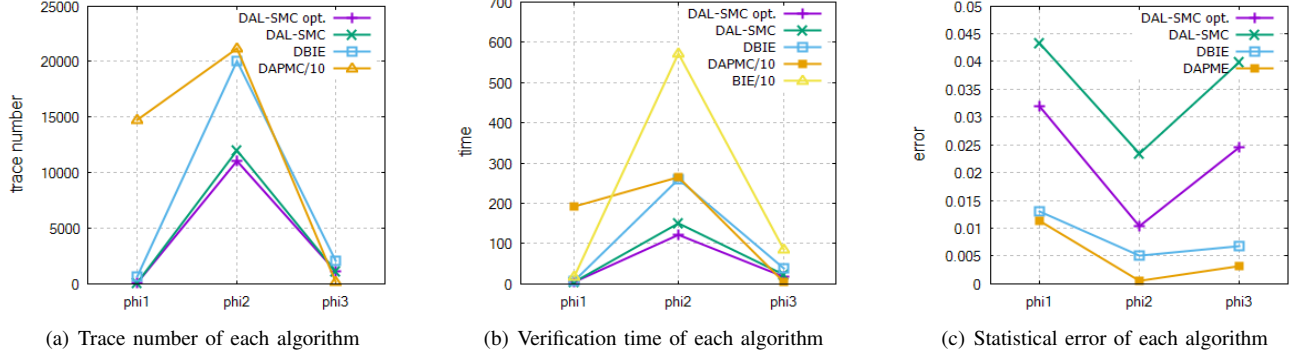


Fig. 9. Algorithms comparison with energy-aware building.

TABLE III. PROPERTIES OF ROBOTS PATH PLANNING

PID	(δ, c)	Property
ϕ_4	(0.01, 0.99)	$P_{=?}(F^{\leq 100} \text{ robot.collision})$
ϕ_5	(0.05, 0.99)	$P_{=?}(F^{\leq 100} \text{ energy} \geq 500)$
ϕ_6	(0.02, 0.9)	$P_{=?}(F^{\leq 100} \text{ robot.collision} \wedge \text{energy} \geq 500)$

250 seconds consumed by distributed BIE. DAL-SMC and DAL-SMC opt. consume less time. Figure 9(c) is the statistical error of each algorithm. The statistical error of DAPMC and distributed BIE are about 0.013 for verifying property ϕ_1 . The statistical error of DAL-SMC and DAL-SMC opt are about 0.045 and 0.032 respectively. The detailed experiment results are listed in Table IV.

3) *Robots path planning*: Robots path planning has attracted public attention these years [21]. The basic goal of a mobile robot is to avoid collision with the moving obstacles, which move irregularly around the environment. As soon as the robot observes the moving obstacle, it will take actions immediately. Different actions consume different energy, so we use some variables to monitor the total energy consumption. Figure 10 shows the main SHA templates for robot path planning.

We also verify three properties ϕ_4 , ϕ_5 , ϕ_6 for this benchmark as shown in Table III. The experiment results are shown in Figure 11.

In order to analyse the performance of SMC algorithms, the detailed data is listed in Table IV. Property ϕ_2 is verified to illustrate the experimental results, we can conclude that:

(i) DAPMC generates the most traces for verifying the property, while distributed BIE needs less traces compared with DAPMC. Furthermore, DAL-SMC reduces the number of traces (about 50%) relative to distributed BIE. In short, DAL-SMC is the most effective algorithm to generate traces.

(ii) The main time consumption of verification is generating traces (more than 90%). DAPMC consumes most time, and DAL-SMC consumes less time compared with distributed BIE profiting from less traces. For the benchmark, we use 40 cores to implement distributed algorithms, and we find that the time consumption of BIE algorithm is nearly 25 times as much as distributed BIE which shows it is effective to improve the performance of SMC with distributed techniques.

(iii) The statistical error of DAPMC and DBIE are similar.

The error of DAL-SMC is bigger than that of DAPMC and DBIE due to use multi-BIE. Besides, we find that the error of DAL-SMC opt. is less than that of DAL-SMC. It shows that the parameter optimization method is effective.

In general, DAL-SMC opt. generates less traces and consumes less time for verification with the help of distributed technology and AL-SMC technique. Meanwhile, the parameter optimization method reduces the statistical error of DAL-SMC to an acceptable range.

V. RELATED WORKS

Statistical Model Checking technique was first proposed by R.Grosu [22]. Some variations [23] [1] [24] [25] [11] [3] based on the basic SMC have been proposed in the past few years. Some related work are summarized as follows:

Basic SMC. SMC refers to a series of simulation-based techniques that can be used to answer two questions: (1)Qualitative: Is the probability of model s satisfying property ϕ greater than or equal to a certain threshold? and (2)Quantitative: What is the probability of model s satisfying property ϕ ? For qualitative SMC, Kim.G.larsen et al. [26] have given an empirical evaluation. BHT and SPRT are more effective than SSP. BHT generates more traces when checking the property whose estimation probability is close to its real probability, so SPRT is faster than BHT for this situation. For other situation, BHT is obviously more efficient than SPRT. For quantitative SMC, Zuliani et al. [11] have compared the number of traces analyzed by APMC and BIE, and they have concluded that BIE excels remarkably in performance. Our approach focuses on the performance of BIE algorithm.

SMC with abstraction and learning. BIE algorithm needs more traces when checking the property whose probability is close to 0.5, while the number of traces is drastically reduced when the probability approaches to 0 or 1 [11]. In our recent work [9], we have partitioned the original probability space Ω into many sub-spaces $\Omega_1, \dots, \Omega_m$, and evaluated the probability of each sub-space in parallel. Therefore, the trace number for evaluating the original probability will be decreased and depends on the maximum number of traces for evaluating sub-spaces theoretically. We find that the number of traces is effectively reduced while ensuring the accuracy of the probability within an acceptable error bound.

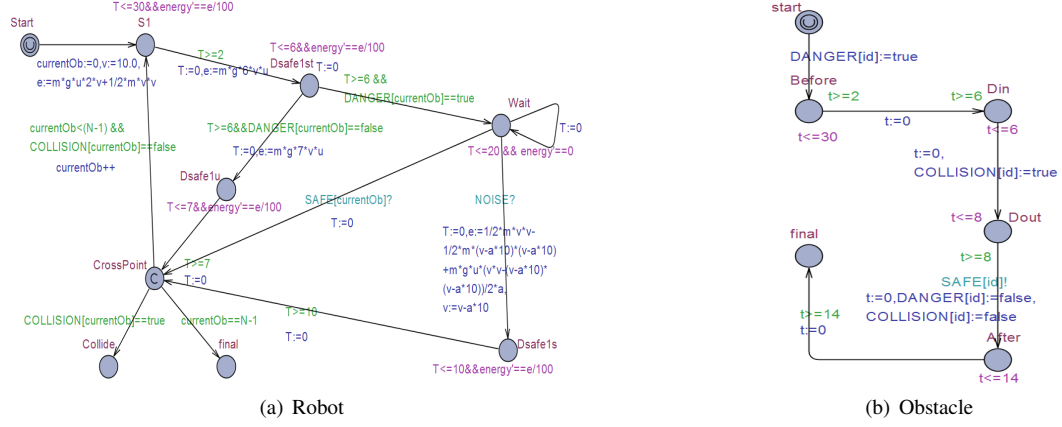


Fig. 10. The main SHA templates for robot path planning.

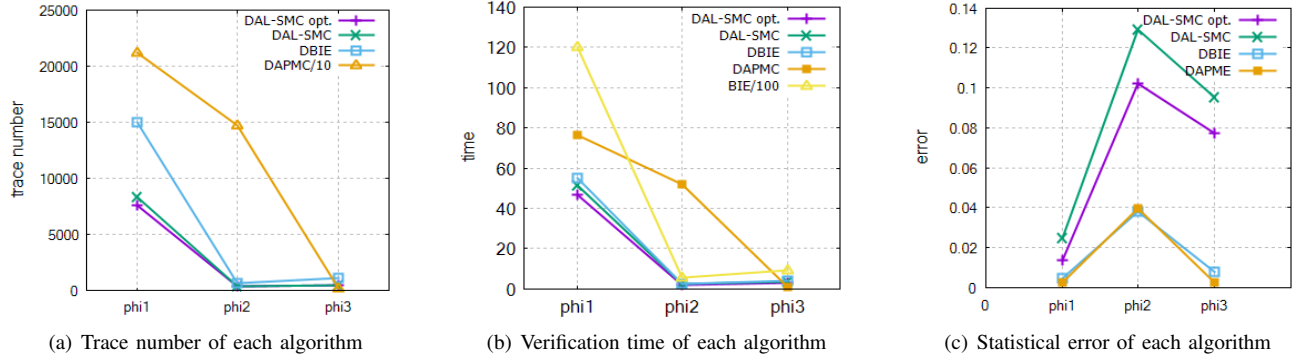


Fig. 11. Algorithms comparison with robots path planning.

TABLE IV. EXPERIMENTAL RESULTS

Algorithm	Property	Trace Number	Time consumption	Statistical Error
DAPMC	$\phi 1(0.05, 0.99)$	147000	1934.31	0.0113
	$\phi 2(0.01, 0.99)$	211932	2649.15	0.0005
	$\phi 3(0.02, 0.9)$	1950	38.05	0.0032
	$\phi 4(0.01, 0.99)$	211930	76.282	0.0024
	$\phi 5(0.05, 0.99)$	147550	52.206	0.0399
	$\phi 6(0.02, 0.9)$	1850	1.159	0.0026
DBIE	$\phi 1(0.05, 0.99)$	600	7.895	0.0131
	$\phi 2(0.01, 0.99)$	20000	259.275	0.0051
	$\phi 3(0.02, 0.9)$	2100	38.057	0.0068
	$\phi 4(0.01, 0.99)$	15000	55.281	0.0049
	$\phi 5(0.05, 0.99)$	702	2.483	0.0382
	$\phi 6(0.02, 0.9)$	1120	4.226	0.0078
DAL-SMC	$\phi 1(0.05, 0.99)$	103	5.685	0.0433
	$\phi 2(0.01, 0.99)$	12000	151.785	0.0235
	$\phi 3(0.02, 0.9)$	1137	22.841	0.0399
	$\phi 4(0.01, 0.99)$	8318	41.68	0.0246
	$\phi 5(0.05, 0.99)$	384	2.32	0.1295
	$\phi 6(0.02, 0.9)$	520	3.601	0.0751
DAL-SMC opt.	$\phi 1(0.05, 0.99)$	95.79	4.65	0.0319
	$\phi 2(0.01, 0.99)$	11040	121.425	0.0103
	$\phi 3(0.02, 0.9)$	1091	18.73	0.0246
	$\phi 4(0.01, 0.99)$	7569	36.512	0.0138
	$\phi 5(0.05, 0.99)$	349	1.81	0.102
	$\phi 6(0.02, 0.9)$	494	3.171	0.0575
BIE	$\phi 1(0.05, 0.99)$	590	175.44	0.0121
	$\phi 2(0.01, 0.99)$	19586	5730.67	0.0047
	$\phi 3(0.02, 0.9)$	2040	845.73	0.0063
	$\phi 4(0.01, 0.99)$	15400	1202.467	0.0044
	$\phi 5(0.05, 0.99)$	762	55.221	0.0352
	$\phi 6(0.02, 0.9)$	1150	91.98	0.0069

Distributed SMC. As observed in [10], SMC algorithms can be distributed with master/slave architecture where multiple slave processes are used to generate traces. When working with an estimation algorithm, the number of traces for verifying the property is known in advance and can be equally distributed between the slaves. When working with the sequential algorithms, the situation gets more complicated, so we need to avoid introducing bias when collecting the traces generated by the slave processes. To solve this problem, H. L. S. Younes proposed a method in [1] where the bias is avoided by committing, *a priori*, to the order in which observations will be taken into account. Peter Bulychev et al. generalized the above method with batches and buffer [13]. Batches aggregate the outcomes for reducing communication and the buffer is used to improve concurrency since the nodes are more loosely synchronized. They also implemented the distributed Hypothesis testing algorithm without introducing bias. The algorithm effectively reduce the time consumption for generating a single trace. Our work is different from the existing work, we use abstraction and learning technique (AL-SMC) to reduce the number of simulation traces, and adopt distributed technology with AL-SMC to reduce both the number of traces and time consumption for generating a single traces.

VI. CONCLUSIONS AND FUTURE WORK

In this paper, we focus on improving the performance of SMC with distributed technology. When we analyse the complex CPSs with SMC, huge-sized models and high confidence of probability estimation require a great number of traces. It is extremely time-consuming. To solve this problem, we present a distributed framework for SMC without introducing bias, and propose distributed BIE and DAL-SMC algorithms based on the framework. The framework is implemented in ModanaO online platform which is an online platform for modelling and analysis of CPSs. Besides, the parameter optimization methods are proposed to reduce error and improve efficiency of DAL-SMC. Finally, to illustrate the feasibility of our approach, three benchmarks are presented. The experiment results show that the DAL-SMC is more efficient than other SMC algorithms. Besides, The parameter optimization method reduces statistical error effectively.

As part of future work, in addition to focusing on the efficiency of our implementation, we plan to apply our framework to more complex systems. Furthermore, we will improve our tool to make it more extendable.

REFERENCES

- [1] H. Younes and L. S. Kan, "Planning and verification for stochastic processes with asynchronous events," in *Nineteenth National Conference on Artificial Intelligence, Sixteenth Conference on Innovative Applications of Artificial Intelligence, July 25-29, 2004, San Jose, California, Usa*, 2004, pp. 1001–1002.
- [2] K. Sen, M. Viswanathan, and G. Agha, *Statistical Model Checking of Black-Box Probabilistic Systems*. Springer Berlin Heidelberg, 2004.
- [3] T. Héroult, R. Lassaigne, F. Magniette, and S. Peyronnet, "Approximate probabilistic model checking," in *Verification, Model Checking, and Abstract Interpretation*. Springer, 2004, pp. 73–84.
- [4] H. Yoo and T. Shon, "Challenges and research directions for heterogeneous cyber physical system based on iec 61850: Vulnerabilities, security requirements, and security architecture," *Future Generation Computer Systems*, vol. 61, pp. 128–136, 2016.
- [5] P. Bulychev, A. David, K. G. Larsen, and M. Mikučionis, "Uppaal-smc: Statistical model checking for priced timed automata," *Electronic Proceedings in Theoretical Computer Science*, vol. 85, 2012.
- [6] M. Kwiatkowska, G. Norman, and D. Parker, "Prism: Probabilistic symbolic model checker," *Lecture Notes in Computer Science*, vol. 2324, pp. 200–204, 2002.
- [7] A. Basu, S. Bensalem, M. Bozga, B. Caillaud, B. Delahaye, and A. Legay, "Statistical abstraction and model-checking of large heterogeneous systems," in *Formal Techniques for Distributed Systems*. Springer, 2010, pp. 32–46.
- [8] J. L. Dehui Du, Bei Cheng, "Statistical model checking for rare-event in safety-critical system," *Journal of Software*, no. 2, pp. 305–320, 2015.
- [9] K. J. Dehui Du, Ping Huang, "Al-smc: Optimizing statistical model checking by automatic abstraction and learning," *International Journal of Software and Informatics*, vol. 10, p. 4:0, 2016.
- [10] H. L. Younes, "Ymer: A statistical model checker," in *Computer Aided Verification*. Springer, 2005, pp. 429–433.
- [11] P. Zuliani, A. Platzer, and E. M. Clarke, "Bayesian statistical model checking with application to stateflow/simulink verification," *Formal Methods in System Design*, vol. 43, no. 2, pp. 338–367, 2013.
- [12] B. Cheng, X. Wang, J. Liu, and D. Du, "Modana: An integrated framework for modeling and analysis of energy-aware cpss," in *IEEE Computer Software and Applications Conference*, 2015, pp. 127–136.
- [13] P. Bulychev, A. David, K. G. Larsen, A. Legay, M. Mikučionis, and D. B. Poulsen, "Checking and distributing statistical model checking," *Lecture Notes in Computer Science*, vol. 7226, pp. 449–463, 2012.
- [14] C. Baier, J.-P. Katoen et al., *Principles of model checking*. MIT press Cambridge, 2008, vol. 26202649.
- [15] A. David, K. G. Larsen, A. Legay, and D. B. Poulsen, "Statistical model checking of dynamic networks of stochastic hybrid automata," *Francisco Javier Fuente Fernandez*, vol. 66, pp. 91–104, 2014.
- [16] G. H. Duntzman, *Principal components analysis*. Sage, 1989, vol. 69.
- [17] R. C. Carrasco and J. Oncina, "Learning stochastic regular grammars by means of a state merging method," in *Grammatical Inference and Applications*. Springer, 1994, pp. 139–152.
- [18] S. N. Sivanandam and S. N. Deepa, *Introduction to genetic algorithms*. Springer, 2008.
- [19] A. David, D. Du, K. G. Larsen, M. Mikučionis, and A. Skou, "An evaluation framework for energy aware buildings using statistical model checking," *Science China information sciences*, vol. 55, no. 12, pp. 2694–2707, 2012.
- [20] J. Miura and Y. Shirai, "Modeling motion uncertainty of moving obstacles for robot motion planning," in *IEEE International Conference on Robotics and Automation, 2000. Proceedings. ICRA, 2000*, pp. 2258–2263 vol.3.
- [21] M. Lahijanian, J. Wasniewski, S. B. Andersson, and C. Belta, "Motion planning and control from temporal logic specifications with probabilistic satisfaction guarantees," in *Proc. 2010 IEEE International Conference on Robotics and Automation*, 2010, pp. 3227–3232.
- [22] R. Grosu and S. A. Smolka, "Monte carlo model checking," in *International Conference on Tools and Algorithms for the Construction and Analysis of Systems*. Springer, 2005, pp. 271–286.
- [23] A. Legay, B. Delahaye, and S. Bensalem, "Statistical model checking: An overview," in *Runtime Verification*. Springer, 2010, pp. 122–135.
- [24] H. L. Younes and R. G. Simmons, "Statistical probabilistic model checking with a focus on time-bounded properties," *Information and Computation*, vol. 204, no. 9, pp. 1368–1409, 2006.
- [25] S. K. Jha, E. M. Clarke, C. J. Langmead, A. Legay, A. Platzer, and P. Zuliani, "A bayesian approach to model checking biological systems," in *Computational Methods in Systems Biology*. Springer, 2009, pp. 218–234.
- [26] Y. Kim, M. Kim, and T.-H. Kim, "Statistical model checking for safety critical hybrid systems: An empirical evaluation," in *Hardware and Software: Verification and Testing*. Springer, 2012, pp. 162–177.