Response to the comments of the Paper

Symbolic Verification of Current-state Opacity of Discrete Event Systems Using Petri Nets
(Paper ID: SMCA-20-12-2603)

Yifan Dong, Zhiwu Li, and Naiqi Wu

Editor-In-Chief

Dear Dr Zhiwu Li:

Based on the referee reports and the Associate Editors recommendation with which I concur, I regret to inform you that your paper, in its current form, cannot be accepted for publication in the Transactions. Your paper does have merit and you are welcome to revise the manuscript keeping in mind the reviewer comments and to resubmit your paper as a new submission.

When submitting the revised version, please include a detailed statement containing the Authors' Responses to a Reviewer's Comments to address each reviewer's comments. If the authors do not agree with a comment, clearly explain the reason in the Authors' Responses.

Thank you for submitting to the IEEE Transactions on Systems, Man and Cybernetics and we hope to be able to review your paper again.

Sincerely,

Robert Kozma, Fellow IEEE, Fellow INNS

Editor-In-Chief, IEEE Transactions on Systems, Man, and Cybernetics - Systems

Dear Editor-in-Chief Robert Kozma:

Thank you for your careful reading and giving us the opportunity to submit a revised manuscript entitled 'Symbolic Verification of Current-state Opacity of Discrete Event Systems Using Petri Nets'. We appreciate the time and efforts that the editor and reviewers have devoted on our manuscript. The insightful comments with high quality are immensely helpful and enable us to greatly improve the quality and presentation of our paper. We have addressed all comments and suggestions provided by the editor and reviewers in the revised version of our manuscript.

Here is a detailed point-by-point response to the reviewers' comments and concerns. Our answers and the changes in the revised paper are marked in blue. Please kindly note that the reference numbers in the response letter are associated with the bibliography of the letter itself only, and the figures in this letter are numbered independently.

We hope that the revised manuscript will meet the demanding requirements of IEEE Transactions on Systems, Man, and Cybernetics: Systems, and we are happy to consider further revisions. We thank you for your continued interest in our research and look forward to hearing from you at your earliest convenience.

Editor Comments for Authors:

This paper receives mixed review reports.

Recommending: Reject with major revision and encouragement to resubmit

We thank the editor for giving us an opportunity to revise the paper. We have fully considered all the comments and suggestions from the reviewers and addressed the pertinent problems in our original paper.

Reviewer's comments for authors:

Reviewer 1:

What are the contributions of the paper:

This paper addresses the verification of current-state opacity of a discrete event system modeled with Petri nets. The results obtained in this manuscript is interesting. Especially, the reduced computational complexity under MDD for verification is considerable. And the manuscript is well-written.

We thank the reviewer for his/her appreciation of our work.

What are the additional ways in which the paper could be improved:

- Lots of definitions are presented and take up quite spaces.

Response: We thank you for raising this point. In our work, we focus on the MDD-based framework for the verification of current-state opacity, where a formal definition of an MDD under graph theory is mandatory (compared with the work in [1, 2], the observer for the verification of current-state opacity is structured as an automaton). Based on the definition of an MDD, it is necessary to define some concepts such as isomorphism, reduction and paths. These definitions can formally explain the relationships between MDDs and Petri nets.

We agree with the reviewer that there are many definitions that take up quite spaces. However, without the definitions in Section 3, it could be hard to describe the MDD-based framework in a formal way. In fact, every definition in Section 3 is logically necessary. For economy of space, we abnegate some materials that could be cited from other publications (Please see the first paragraph of Section 3 on Page 3 of our revised manuscript, where we explain the reasons for omitting the algorithms in this section). The works in [3, 4] that describe those algorithms are cited in the revised manuscript (Please see the paragraph just before Proposition 2 on Page 6 and the second paragraph on Page 8).

- What's the difference/relationships between Definition 11 and Algorithm 1, 3? Since they are both focus on the union/intersection of MDD. Can Algorithm 1, 3 be omitted if Definition 11 is well defined for the union/intersection of MDD? In Definition 11, the E_i are not explicitly given.

Response: We thank the reviewer for raising this important point. For their relationship, Algorithms 1 and 3 describe the operational details of union and intersection, respectively, which are used in Section 4. Indeed, Algorithms 1, 2 and 3 in the original manuscript are proposed in [3, 4]. We delete the three algorithms for economy of space (Please see Algorithms 1, 2 and 5 of the revised paper on Pages 9–11).

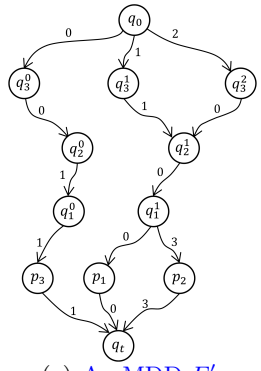
In Definition 11, we have explicitly and recursively defined Q_i and child vertexes of $q_i \in Q_i$, i.e., $q_{i-1} \in Q_{i-1}$. The notation $E_i \subseteq Q_i \times Q_{i-1}$ implies that an edge can connect a vertex in Q_i and one of its child vertexes in Q_{i-1}. Therefore, it is unnecessary to explicitly define E_i again.

- In Fig. 1, if we add $q_1^1 \xrightarrow{3} p_2 \xrightarrow{3} q_t$, and adjust $q_1^1 \xrightarrow{0} q_t$ as $q_1^1 \xrightarrow{0} p_1 \xrightarrow{0} q_t$. For $q_1^0 \xrightarrow{1} q_t$ is replaced with $q_1^0 \xrightarrow{1} p_3 \xrightarrow{1} q_t$. In Fig. 4 (a), adjust $q_1^1 \xrightarrow{0} q_t$ as $q_1^1 \xrightarrow{0} p_1 \xrightarrow{0} q_t$, adjust $q_1^0 \xrightarrow{1} q_t$ as $q_1^0 \xrightarrow{1} p_2 \xrightarrow{1} q_t$. Then, in the union of Fig. 1 and Fig. 4(a), i.e., Fig. 4 (b), $q_1^1 \xrightarrow{0} (q_t, q_t)$

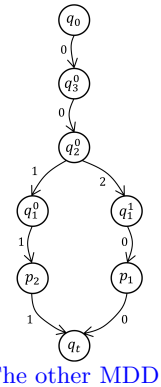
becomes $q_1^1 \xrightarrow{0} p_1 \xrightarrow{0} (q_t, q_t)$ and $q_1^1 \xrightarrow{3} p_2 \xrightarrow{3} (q_t, q_t)$ is added. Then from (q_0, q_0) to (q_t, q_t) in Fig. 4 (b), one has a label sequence 0 0 2 3 3, which does not exist in Fig. 1 and Fig. 4(a), which means that Proposition 2 is doubtful. Further, it makes a worry about the main contribution of this paper.

Response: Thank you for bringing this point to our attention. Indeed, our main contribution is not to improve the efficiency of operations about MDDs. Instead, we mainly focus on the construction of MDD-based observers and verifiers by using these manipulations. Although Proposition 2 is not our main contribution, it is a key to associate the operations of MDDs with the marking sets of Petri nets. Here we explain the confusion from the reviewer about Proposition 2.

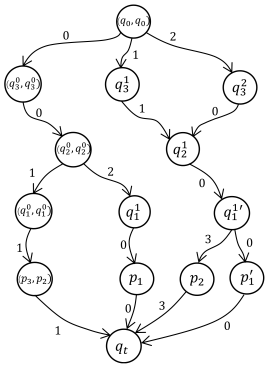
In this response letter, Fig. 1 shows the union of two MDDs considering the reviewer's additional paths. By Definition 11, the child vertexes (with the same name) of non-terminal vertexes from the two different MDDs are "independent". For example, both q_2^1 in Fig. 1(a) and q_2^0 in Fig. 1(b) contain the child vertex q_1^1. However, in the union of two MDDs, they are different, i.e., q_1^1 and $q_1^{1'}$, as shown in Fig. 1(c). Then, the path added to the MDD in Fig. 1(c) should be "$q_1^{1'} \xrightarrow{3} p_2 \xrightarrow{3} (q_t, q_t)$" instead of "$q_1^1 \xrightarrow{3} p_2 \xrightarrow{3} (q_t, q_t)$". Therefore, the label sequence 0 0 2 3 3 does not exist in Fig. 1(c) and it is normal that this label sequence does not exist in Fig. 1 and Fig. 4(a). Note that the MDD shown in Fig. 1(c) is not quasi-reduced since there exist duplicated vertexes, where $F(p_1)$ and $F(p_1')$ are isomorphic by Definition 4. Fig. 1(d) is a quasi-reduced MDD computed by the algorithm proposed in [3], where the vertexes p_1 and p_1' are merged.



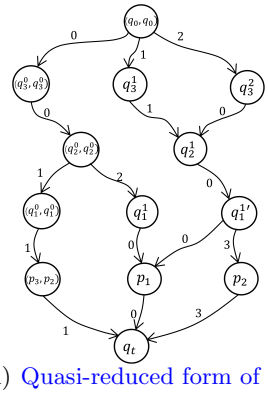
(a) An MDD F'.



(b) The other MDD F''.



(c) The MDD F that is the union of F' and F''.



(d) Quasi-reduced form of F.

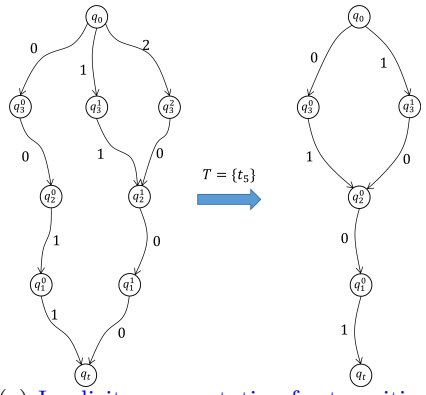
Figure 1: Union of two MDDs.

- Could the authors give a more intuitively illustration for why MDD can reduce the computational complexity?

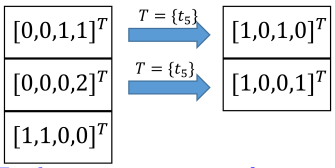
Response: We thank the reviewer for bringing this point to our attention. Indeed, we have explained why the MDD-based approaches are intuitively effective (Please see the 6th paragraph of the introductory section on Pages 1 and 2). For economy of space, we do not show an intuitive example in the paper, but we can explain it graphically in the response letter.

Let us consider the labeled Petri net in Example 2 of our submitted manuscript and explain why MDDs can reduce the computational complexity. As for the representation of a set of markings ($\{[0,0,1,1]^T, [0,0,0,2]^T, [1,1,0,0]^T\}$), these markings are implicitly represented as the labels of edges in the MDD shown in Fig. 2(a) (the left part), where some values are shared (markings $[0,0,1,1]^T$ and $[0,0,0,2]^T$ share the same numbers of tokens in places p_1 and p_2). However, the explicit representation of a set of markings means that each state is stored independently (shown in Fig. 2(b), the left part). Therefore, the implicit representation for a set of markings requires less memory than the explicit one.

We now assume that transition t_5 fires. Under the implicit technique, where the matrix diagram (shown in Fig. 3(b) of the submitted paper) is decided by $\{t_5\}$, a set of reachable markings are generated concurrently with the operation of relational product (shown in Fig. 2(a)). Besides, since the implicit technique requires less memory for a set of states, the space and time requirements for the computation of a set of reachable states are reduced accordingly. However, for the explicit method shown in Fig. 2(b), the reachable states are generated one by one, and these states are stored inefficiently.



(a) Implicit representation for transition relations.



(b) Explicit representation for transition relations.

Figure 2: Graphical explanation for the efficiency of MDDs.

- What's the main difference between MDD and matrix diagram?

Response: We thank the reviewer for bringing this question to our attention. We expose the differences between MDDs and matrix diagrams from the perspective of definitions and functions (Please see the paragraph on Page 6 just before Definition 11).

MDDs contain a set of labels, and each edge in MDDs is associated with a label under the labeling function. Compared with MDDs, an edge in matrix diagrams is associated with a label pair. Besides, MDDs are used for the storage of states and the representation of MDD-based structures, while matrix diagrams represent the transition relations of Petri nets.

- Can the authors give an example in details to show how to obtain the matrix diagram/MDD from a Petri net? Though there exist the notion of matrix diagrams for transition relations of Petri nets is proposed in [27,28], a brief illustration is expected.

Response: Thank you for this comment. To address this concern, we have added more details to show how to obtain the MDDs and matrix diagrams in Examples 1 and 2, respectively (Please see Pages 5 and 6 of the revised manuscript in Examples 1 and 2). Please note that in Example 2, we detail the procedure of generating a matrix diagram with a single transition t_5. If the set $\hat{T}$ is not a singleton, the corresponding matrix diagram can be constructed under the algorithms proposed in [5]. For economy of space, we do not repeat how to formally generate a matrix diagram in an excessive detail. Instead, we mainly explain the relationships between transition relations of Petri nets and matrix diagrams.

- Could the result can be extended to unbounded Petri nets?

Response: This is a very good question. We would like to thank the reviewer for pointing out this interesting work. In fact, the study on unbounded Petri nets involves the concept of decidability, which is not in the scope of our research. We just discuss the unbounded assumption in the response letter. Bryans *et al.* [6] prove that the verification of current-state opacity is a decidable problem if a labeled Petri net is bounded. In our work, we mainly focus on a decidable problem that could output a definite (yes/no) answer, i.e., verify whether a system is current-state opaque or not. It implies that the Petri nets are required to be bounded. With the bounded assumption for labeled Petri nets, the number of reachable markings is finite, and the proposed MDD-based observers and verifiers could be constructed for the verification purpose. In the future, we will try to use MDDs to represent a coverability graph of an unbounded Petri net and to check the possibility of the extension of the proposed method. Also, we may associate MDD-based structures on other interesting works regarding unbounded Petri nets in the future.

Reviewer 2:

What are the contributions of the paper:

The article proposes symbolic verification of current-state opacity of discrete event systems using Petri nets. The topic of modelling and verification of opacity in Petri nets is not new – both concerning the current state or the initial state. There are various approaches in the literature, the most known and cited are from a few years ago. The most recent research results are however missing in the manuscript. In the submitted manuscript, in order to better deal with large models, multi-valued decision diagrams are used, what is in my opinion the real contribution of the paper and should be more highlighted.

Response: We appreciate the comments of this reviewer. All the issues are addressed in the revised manuscript. The related literature has been reviewed and our main contributions are highlighted.

What are the additional ways in which the paper could be improved:

- The contributions should be more highlighted.

Response: We thank the reviewer for pointing this out. As requested, we highlight our contributions by splitting them into three items (Please see the introductory section on Page 2 of the revised paper).

- The most recent publications regarding opacity in Petri nets should be added and described.

Response: Thank you for this comment. We review the works in [7, 8, 9] that are recently published for the new types of opacity. Besides, we review the techniques in [10, 11, 12] that are published recently for the verification of state-based opacity, which are closely related to our research (Please see the first and fifth paragraphs of the introductory section in the revised manuscript on Page 1).

- The authors write that in the introduction that "the reachable states of Petri nets are generated in a brute-force way and stored in different and independent memory location [21], [22]. The explicit representation for a reachability set would impose a serious restriction on Petri nets with a large number of states". This is generally true, but the authors give here a reference to a paper that deals with safe Petri nets. In safe Petri nets, a place may contain only one token at a moment (or zero), so it is not surprising that the reachable states are then generated in a brute-force way.

Response: We thank the reviewer for bringing this point to our attention. We agree with that Ref. [22] (in the original paper) deals with safe Petri nets. We have deleted this reference in the revised paper and added other related references (Please see the 6th paragraph of the introductory section on Page 2).

- The last column in Tables 2 and 3 is not needed, as it contains the same value. It could be just summarized in the text.

Response: We agree with the reviewer that the last columns of Tables 2 and 3 could be summarized in the text. As requested, we delete the last columns of Tables 2, 3, and 4, and summarize them in the text (Please see Tables 2, 3, and 4 on Pages 12 and 13, and two paragraphs just before Table 2 and after Table 3 on Page 12, respectively).

- Some figure are too small and the used font is too small (e.g. Fig. 3, Fig. 4, Fig. 9) – it is hard to read the text.

Response: Thank you for raising this point. As requested, we have enlarged the used fonts and Figs. 1, 3, and 4 to ensure that the notations in them are clear (Please see Pages 4, 5, and 7, respectively). Due to the limited space (13 pages limitation in SMCA journal), the enlarged Fig. 9 in the original submitted paper is presented on the web https://github.com/dongyifan199/MDD-on-LPN (Please see the second paragraph of Section 5 on Page 12).

- In some references the year is missing (e.g. [17], [19]).

Response: We thank the reviewer for raising this error. We have corrected them in the revised manuscript (Please see references [14] and [16] on Page 13 of the revised manuscript).

- English language should be checked by a native speaker. There are several gramma errors in the manuscript (even in the abstract, e.g. "the symbolic approach is practically efficient than traditional techniques" – when comparing with other solutions – it should be rather "more efficient"; or at the end of the paper "in Table 2" not "in Tables 2"). Try also to be more consistent – in some places there is "proof" and in the others "Proof".

Response: We thank the reviewer for pointing out these errors. We apologize for the negligence and have corrected all the errors in the revised paper (Please see the penultimate line in the abstract, the first line of the second paragraph just after Table 2 on Page 12, and the word "Proof" of Proposition 1, Theorems 1 and 2 on Pages 4, 9 and 11, respectively).

Reviewer 3:

What are the contributions of the paper:

What are the contributions of the paper: This paper proposed a symbolic technique for verifying current-state opacity for a system modeled with labeled Petri nets.

Response: We appreciate the comments of this reviewer.

What are the additional ways in which the paper could be improved:

- In fact, the application of MDD to represent the states of Petri nets was already proposed some years ago. But the paper does not mention this in the related work. Please consider it and compare with these existing work.

Response: Thank you for this comment. Although there are many applications about MDDs on Petri nets such as model checking and reachability analysis, only the application of MDDs to state space generation of Petri nets is related to our research. As requested, we add some recent works about MDDs on Petri nets for state space generation. We cite the works in [13, 14], where the impact of variable ordering is discussed (Please see the second paragraph of Section 1 on Page 2). Other works about the basic operations of MDDs in [3, 4] are also reviewed (Please see the fifth paragraph in the introductory section on Page 2). As outlined in the introductory section, we have clarified that our main contribution is the construction of an MDD-based observer and verifier for the verification of current-state opacity (Please see the first item of the contribution on Page 2). In other words, state generation using MDDs is only a slight part of our work, and we mainly touch upon the problem of current-state opacity verification in labeled Petri nets.

An excessive comparison of existing state generation methods would pose a threat to our research priorities. Besides, the performance of advanced techniques for state space generation relies on the structure of models, and those methods may behave differently on diverse models. Since the improvement of MDD structures for state space generation is not our priority, we uniformly employ the classical breadth-first iterative strategy for the state generation during the construction of the MDD-based observer. Under this consideration, our numerical experiments, whose purpose is to improve the efficiency of the current-state opacity verification compared with the works in [1, 2], are not affected by other extra factors, such as the different strategies of state space generation (Please see the third and fourth paragraphs of the introductory section on Page 2 of the revised paper). In summary, a more computationally efficient state space representation technique (if existing) than the proposed one will definitely lead to a more efficient opacity verification procedure.

Other issues:

- "construct a reachability graph initially, and then convert it into a deterministic finite automaton" Why should it be converted into an automaton? I think the usual way is to perform modeling checking on a reachability graph.

Response: Thank you for bringing this point to our attention. In fact, due to the state explosion problem of large-sized systems, it is hard to directly perform modeling checking on a reachability graph. By the definition of current-state opacity of labeled Petri nets, a critical process for verifying current-state opacity is the computation of state estimations for all observations w, i.e., $\mathcal{C}(w)$.

The converted automaton from a reachability graph is constructed to compute state estimations for all observations of a system, which is intuitive and expedient for the verification purpose. We have also added a sentence "The construction of an observer for the state estimation is a classical technique for the verification of current-state opacity." (here the observer is an automaton) to summarize the usual process for the current-state opacity verification (Please see the first sentence in the 6th paragraph of Section 1). The works in [1, 2] have demonstrated this classical process as well.

- Necessary references about Petri nets are missing on Page 3.

Response: We thank the reviewer for bringing this point to our attention. As requested, we have reviewed some necessary references about Petri nets (Please see the first paragraph of Section 2 on Page 2).

- Table IV, besides the number of states, it is better to give also performance comparison.

Response: We thank the reviewer for bringing this point to our attention. Indeed, in Table 4, we have shown the CPU seconds for the verification of current-state opacity compared with the works in [1, 2]. We have added a description that the comparative indicators are the same as those in Tables 2 and 3 (Please see the fourth sentence in the paragraph just after Table 3 on Page 12 of our revised paper).

- Can the codes to implement the method be publicated for test?

Response: We thank the reviewer for this suggestion. As requested, we have uploaded some executable programs for the test and replication of the proposed experiments (available at https://github.com/dongyifan199/MDD-on-LPN).

- I would like to see a deep discussion about the application of the method in real systems.

Response: We thank the reviewer for pointing this out. We have fully considered the reviewer's suggestions, and replaced the first example with a more realistic model in Section 5, which is a robot manipulation system. Through this realistic system, we explain the practical purpose for verifying whether the real-world system is safe from intruders (Please see the first example in Section 5). In the second test, we consider a parameterized manufacturing system. We describe the meanings of places and transitions in this system to show the practical significance of opacity verification (Please see the second example on Pages 12 and 13 of our revised paper). Due to the limited space (13 pages limitation in SMCA journal), more detailed descriptions about these two systems are presented in https://github.com/dongyifan199/MDD-on-LPN (Please see the second paragraph of Section 5 on Page 12). Through these two realistic

cases, we show that the proposed method is practically more efficient than traditional techniques.

Reviewer 4:

What are the contributions of the paper:

This paper proposes an efficient technique for the verification of current-state opacity of discrete event systems modeled with bounded labeled Petri nets. The main idea is to use symbolic approaches by leveraging on multi-valued decision diagrams rather than an explicit representation of the state space. Preliminary experiments show that for two examples the approach is more scalable with respect to the one proposed in [11].

Response: We appreciate the comments of this reviewer.

What are the additional ways in which the paper could be improved:

- The paper is quite easy to follow and I've no concerns about the technical soundness of this work. Even though authors deal with a problem considered relevant by the research community in discrete event systems, the current proposal has in my opinion some weaknesses and is not ready to be published as an SMCA article.

Response: We thank the reviewer for bringing this point to our attention. All the issues have been addressed in this revised version.

Major issues follow.

- In my opinion, the authors do not provide good arguments to position the paper into the aim/scope of the SMCA journal. Which phases of the systems engineering lifecycle the current proposal is supposed to contribute to? The paper misses connections with real-world experience or at least examples. This is fundamental to allow readers to grasp how the technique can be used as an aid for the specification and the analysis of security-critical systems. At the current stage, the major contribution is given by the theoretical formulation of the proposed technique. This is good in principle, but I feel that SMCA is not the right place for such a contribution, without comprehensive empirical evidence supporting the claims.

Response: We thank the reviewer for the valuable suggestion regarding the real-world application of the proposed technique. In the revised manuscript, we have associated our work to the scope of SMCA journal. We believe that our work is concerned with the system design phase. We add a sentence "Before a system is put into service, we need to check in its design phase the security to avoid the theft or attack of secret information from the intruders." (Please see the second paragraph of the introductory section on Page 1) to clarify that our current proposal focuses on the modeling for the safety verification phase of the systems engineering. In fact, opacity verification methods for security-critical systems modeled with discrete event systems have been proposed by many researchers, and those techniques are significant for the modeling and optimization of systems (Please see the references [3–10] cited in the introductory section of the revised paper).

In Section 5 of our original manuscript, we present some numerical examples without giving their descriptions. We agree with the reviewer that the practical meanings of those systems would be incomprehensible if they are not explained well in realistic cases. Therefore, we replace the first example with a more realistic model, namely the robot manipulation system that is

available at "https://mcc.lip6.fr/pdf/RobotManipulation-form.pdf", and explain the practical purpose for verifying whether the real-world system is opaque (Please see the first example in Section 5). If a system is verified to be not opaque, there exists the potential that the secret information of the system is obtained by the intruder. Under the specification of the protection of a system, it is necessary to check its opacity. In the second test, we consider a parameterized manufacturing system. We describe the meanings of places and transitions in this system to show the practical significance of opacity verification (Please see the second example on Pages 12 and 13). Due to the limited space (13 pages limitation in SMCA journal), more detailed descriptions about these two systems are presented in https://github.com/dongyifan199/MDD-on-LPN (Please see the second paragraph of Section 5 on Page 12).

- As mentioned above, missing empirical evidence supporting the claims of this paper is a major issue. The paper shows two numerical examples in Section 5 that are not enough to understand both advantages and shortcomings of the approach in a real-world setting. I can suggest the authors exemplify the technique with a realistic case study in the domain of security-critical systems and then carry out a systematic empirical evaluation with a number of open-source benchmarks (e.g., those available from the "model checking contest" community: https://mcc.lip6.fr/). The evaluation shall be used to answer clear research questions and point out pros/cons, and threats to validity.

Response: We thank the reviewer for indicating these important references and one of models from https://mcc.lip6.fr/ has now been included in our tests. Besides, for both two real-world systems, we have added more details about those models to explain the practical significance of our studies (Please see Section 5 on Pages 12 and 13 of the revised manuscript). In our work, we are only interested in the verification of current-state opacity using labeled Petri nets and mainly consider its optimization compared with the state-of-the-art methods proposed in [1, 2]. For the problem of opacity verification, we consider the CPU seconds and the variety of systems to evaluate the proposed techniques.

- Experiment results cannot be replicated. Openness in science is key to fostering scientific progress via reproducibility/replicability. Since one of the main contributions of this paper is supposed to be the presentation of a technique that overcomes state-of-the-art methods, I can suggest making this reproducible through a replication package.

Response: We thank the reviewer for this suggestion. As requested, we have uploaded some executable programs for the test and replication of the proposed experiments (available at https://github.com/dongyifan199/MDD-on-LPN).

Minor issues follow.

- The introduction mixes compelling motivations for improving the scalability of existing approaches. Here I can suggest using a realistic case study (rather than a toy example) to put into place major concepts.

Response: We thank you for this suggestion. In the introductory section, we have stated that the current techniques for the opacity verification are not able to deal with large-sized systems. It motivates us to introduce an efficient method to cope with the opacity verification problems when a system is modeled with labeled Petri nets. Indeed, the scalability of existing approaches (for both the verification of current-state opacity and the state space generation using MDDs) are not discussed in our paper. With the motivation of our work, we focus on the

design of MDD-based structures to improve the efficiency of current-state opacity verification (Please see the fifth paragraph of the introductory section on Page 2).

As for the comments for major issue of our work, we have added a study on realistic cases to explain our major concepts (Please see Section 5 on Pages 12 and 13 of the revised manuscript).

- This work heavily relies on existing approaches, but a state-of-the-art section is missing. At the current stage, it is mixed together with the introduction, which shall instead provide motivations from other perspectives.

Response: We agree with the reviewer that our work mainly relies on the existing work proposed by Tong *et al.* [1, 2]. Indeed, our work is the first attempt to apply the theory of MDDs on labeled Petri nets, and we have explained our new techniques for the solution of the existing work (Please see the second part of Section 4 on Pages 8–11). Based on the existing verification problem, we propose an approach from a new perspective of a mathematical tool, i.e., the MDDs. We employ two realistic examples to show that the proposed approaches perform better than the state-of-the-art approaches, i.e., the BRG-based methods proposed in [1, 2]. As for the works on new concepts of opacity such as K-step opacity and infinite-step opacity, we would like to associate MDD-based structures on them in our future work.

Reviewer 5:

What are the contributions of the paper:

This paper addresses the verification of current-state opacity of a discrete event system modeled with Petri nets, where the secret is defined as a set of states. Given such a system, it is said to be opaque if an intruder who can partially observe system behavior, is never able to verify whether the current state of the system is within the secret states.

The existing methods cannot deal with large-sized systems due to complexity issues mainly due to the exploration of the reachable state space. To address this problem, multi-valued decision diagrams can be used. In this paper, the authors use MDD for representing the large reachability sets of Petri nets with partial observable transitions and propose an approach for the verification of current-state opacity as far as the given net is bounded. Numerical experimental studies are proposed to show that the symbolic approach is practically more efficient than other techniques e.g., basis marking reachability graphs.

Response: We appreciate the comments of this reviewer.

What are the additional ways in which the paper could be improved:

- The topic of the paper (opacity of DES) is of great importance for cyber-security but has been widely investigated this last decade, including numerous nice contributions with Petri nets. The authors made a short review of these results but the state of the art could be enhanced by adding some recent contributions. Also I suggest that the authors have a deeper review of the contributions about the logical analysis of MDD. In particular, the authors are expected to provide more details concerning their contribution on MDD and the position of this contribution with the existing literature. Propositions 2 and 3 are about intersection, union and other logical compositions of MDD. In the paper, these propositions have been presented as two original contributions from the authors. I'm not sure that these results are not trivial extensions of some existing works (see the work of Mateescu et al., 2008 as an example). Clarifications should be added.

Response: We thank this reviewer for the suggestions. In the revised manuscript, we have reviewed more papers that are recently published for the new concepts of opacity [7, 8, 9], and cited the most recent techniques in [10, 11, 12] for the verification of state-based opacity (Please see the first and fifth paragraphs of the introductory section in the revised manuscript on Page 1). We apologize for our ambiguous description of our contributions in the original manuscript. A clearer presentation of our contributions is highlighted in the revised version (Please see the introductory section on Page 2 of the revised paper).

Indeed, our main contribution is not limited to the construction and operations of MDDs. We are primarily interested in the construction of the MDD-based observer and verifier for the verification of current-state opacity, where some basic operations such as union and intersection are used and cited from other studies [3, 4]. Since a specific graph structure is required to record the state estimations of all observations, we define MDDs formally under graph theory (compared with the work in [1, 2], the observer for the verification of current-state opacity is structured as an automaton).

In fact, Proposition 2 is not an extension of some existing works. However, with our formal definition of MDDs, Proposition 2 is significant logically, since it is a key to associate the operations of MDDs with the marking sets of Petri nets. For economy of space, we delete Proposition 3 in our revised paper, since its proof can be derived directly from Definition 12 (Please see the second paragraph on Page 8). To avoid the misleading of the contributions regarding MDDs, we delete Algorithms 1, 2 and 3 in Section 3 of our original manuscript. Some related references about the basic operations of MDDs are cited (Please see Algorithms 1, 2 and 5 of the revised paper on Pages 9–11).

- In my view, there is not much to add about opacity in a pure logical DES perspective (the one considered here by the authors) excepted the issues about complexity. This incites the authors to study MDD based methods. I think that The problem is not well stated: MDD may be a promising solution to reduce the representation of (parts of) the reachability graph and consequently to develop advanced methods that explore such graphs. But the particular advantages for MDD to address opacity problems is not well motivated. In brief, what is not clear for me is why MDD are more promising when used to solve complexity aspects for opacity problems than when used for any other problems that requires an analysis in the reachability set.

Response: We appreciate the reviewer a lot. We agree with the reviewer that the statement on motivation about complexity is significant. As requested, we carefully compare the complexity of the observers derived from BRG-based and MDD-based techniques, i.e., $\mathcal{O}(2^{|N_b|})$ and $\mathcal{O}(|Obs_M| \times (\sum_{i=1}^{m} |Q_i'|_{max} \times |Q_i''|_{max}))$, respectively (Please see the first and second paragraphs on Page 11 just after the proof of Theorem 2 in the revised paper).

In fact, our work is the first attempt to apply the theory of MDDs on labeled Petri nets, where transitions are split into several parts by different labels. We have explained the reasons using MDDs for opacity problems in our revised manuscript (Please see the fifth paragraph of the introductory section on Page 2). The advantages of using MDDs can also be represented in the second part of Section 4 on Pages 8–11. Apart from the classical mathematical techniques such as basis reachability graphs and integer linear programming, we introduce the tool of MDDs to cope with opacity verification problems when a system is modeled with labeled Petri nets. Compared with the state-of-the-art method for the verification of current-state opacity, i.e., the BRG-based approach, we show that the proposed MDD-based one is more efficient.

- As far as complexity is considered, my opinion is that the authors should address the question of SPACE and TIME complexity in more exhaustive and formal way. What I mean is that the contribution should address the complexity evaluation in a formal way by expressing complexity as a function of some input parameters. The last section of the paper proposes some numerical examples that seem promising. Nevertheless, such examples should be used for illustration and not for validation purpose.

Response: Thank you for pointing this out. In fact, our work is compared with those proposed in [1, 2]. In many related works about opacity verification problems, researchers regard the CPU seconds as the evaluation criterion of different approaches instead of memories [2, 10, 12]. Therefore, to evaluate the performance of the proposed techniques, we mainly consider the time complexity of the construction for observers in our paper (Please see the first and second paragraphs on Page 11 just after the proof of Theorem 2 in the revised paper). The question of space complexity is discussed in this response letter.

As outlined in the revised manuscript, we formally compare the time complexity of the observers derived from BRG-based and MDD-based techniques, i.e., $\mathcal{O}(2^{|N_b|})$ and $\mathcal{O}(|Obs_M| \times (\sum_{i=1}^{m} |Q'_i|_{max} \times |Q''_i|_{max}))$, respectively. In fact, it is hard to compare the efficiency of those two methods directly, since the input parameters contained in them are different (the BRG-based method contains $|N_b|$ as its parameter, while the MDD-based technique depends on the parameter $|Obs_M|$, and the numbers of nodes in MDDs or matrix diagrams, i.e., $|Q'_i|_{max}$ and $|Q''_i|_{max}$). However, the time complexity for BRG-based observers is exponential. It is intuitive that the MDD-based approaches are more practically efficient if the systems are large-sized.

We now discuss the comparison of space complexity between BRG-based and MDD-based observers. The space complexity of the construction of a BRG-based observer is $\mathcal{O}(2^{|N_b|})$ as well. Since edges would take up the memories of a computer, the space complexity derived from an MDD-based observer is $\mathcal{O}(|Obs_M| \times |D| \times (\sum_{i=1}^{m} |Q'_i|_{max} \times |Q''_i|_{max}))$, where $|D|$ represents the number of labels. Similar to the analysis of time complexity, it is still hard to compare their space complexity, since the input parameters in these two expressions, i.e., the parameter $|N_b|$ contained in $\mathcal{O}(2^{|N_b|})$ and the parameters $|Obs_M|$, $|D|$, $|Q'_i|_{max}$, and $|Q''_i|_{max}$ contained in $\mathcal{O}(|Obs_M| \times |D| \times (\sum_{i=1}^{m} |Q'_i|_{max} \times |Q''_i|_{max}))$, are different. Compared with the exponential complexity of BRG-based methods, it seems that the MDD-based techniques require less memory with large-sized systems.

- The presentation is not nice and there are several points to address in order to enhance the organization of the paper. First of all, the enumeration of numerous definitions in Section II is tedious. Moreover, in some places, the authors mix definitions and examples (e.g., on page 4). Second, the use of MDD with PN must be better explained. This can be obtained by revising Example 1. In particular, the authors should explain how they defined set Q_i and the function δ. Observe that example 1 is really important to understand the utility of MDD. This question should be also addressed in a general way. What are the options and choices when using MDD? This should be discussed.

Response: We agree with the reviewer that there are many definitions and algorithms that take up quite spaces in Section 3. However, without these definitions, it could be hard to describe the MDD-based framework. In fact, every definition in Section 3 is logically necessary. For economy of space, we abnegate some materials that could be cited from other publications

(Please see the first paragraph of Section 3 on Page 3 of the revised manuscript. We explain the reasons for deleting Algorithms 1, 2, and 3 in this section). The works in [3, 4] that describe those algorithms are cited in the revised manuscript (Please see the paragraph just before Proposition 2 on Page 6 and the second paragraph on Page 8).

In our manuscript, we have checked the mixed places with definitions and examples. Indeed, definitions and examples have been distinguished clearly by notations "◊" and "□", respectively. Paragraphs without markings elaborate the meanings of definitions and explain their relationships with Petri nets.

Besides, considering the suggestion that the set Q_i and the function δ should be explained in detail, we have described how they are connected with the markings of Petri nets in Example 1 (Please see Example 1 on Page 5). This question has been explained in a more general way (Please see lines 4–13 of the paragraph just before Example 1 on Page 4).

As for the options and choices of MDDs, we have discussed them from several perspectives in our revised manuscript (Please see the introductory section on Page 2, the third and fourth paragraphs).

- I'm worry about the terminal vertex / vertices in MDD approaches. It is not clear for me if the terminal vertex is necessarily a singleton (as it seems to be in this paper, e.g., Def. 3 and related parts.

Response: We thank the reviewer for raising this point. In general, researchers usually define MDDs with two terminal vertexes that are valued with true and false, and this form of terminal vertexes is conducive to the presentation of operations of MDDs [3, 4]. However, the examples and figures of MDDs shown in these materials have only one terminal vertex valued with true (or 1), since only the top-bottom paths ended with this vertex are related to the markings of MDDs.

As outlined in the contribution part of the introductory section, we focus on the MDD-based framework for the construction of observers and verifiers, where a formal definition of an MDD under graph theory is mandatory, and our concern is not to improve the computational efficiency of the basic operations between two MDDs. The definition of a single terminal vertex in an MDD can be more intuitive to describe MDD-based structures and explain the relationships between MDDs and Petri nets. Besides, it does not affect the utilization of the existed basic operations proposed in [3, 4], where some "irrelevant paths" pointing to the terminal vertex valued with false (or 0) could just be added to match the computation.

Minor comment

- One the notation $F(q)$ is introduced, you have to use it and define $F(q_0)$ in Proposition 1.

Response: Thank you for raising this point. However, we are afraid that $F(q_0)$ does not need to be defined again in Proposition 1. Indeed, by Definition 6, we have defined $F(q)$, where $q \in Q_n$ is a non-terminal vertex. By Definition 2, the rooted vertex q_0 defined in Definition 3 is a non-terminal vertex as well. Therefore, when we use the notation $F(q)$, $F(q_0)$ is implicitly defined.

References

[1] Y. Tong, Z. W. Li, C. Seatzu, and A. Giua, "Verification of current-state opacity using Petri nets," in *Proc. Amer. Control Conf.*, 2015, pp. 1935–1940.

[2] Y. Tong, Z. W. Li, C. Seatzu, and A. Giua, "Verification of state-based opacity using Petri nets," *IEEE Trans. Autom. Control*, vol. 62, no. 6, pp. 2823–2837, 2017.

[3] G. Ciardo, G. Lüttgen, and R. Siminiceanu, "Efficient symbolic state-space construction for asynchronous systems," in *International Conference on Application and Theory of Petri Nets*. Springer, 2000, 103–122.

[4] M. Wan and G. Ciardo, "Symbolic state-space generation of asynchronous systems using extensible decision diagrams," in *International Conference on Current Trends in Theory and Practice of Computer Science*. Springer, 2009, pp. 582–594.

[5] A. S. Miner, "Implicit GSPN reachability set generation using decision diagrams," *Perform. Eval.*, vol. 56, nos. 1-4, pp. 145–165, 2004.

[6] J. W. Bryans, M. Koutny, L. Mazaré, and P. Y. Ryan, "Opacity generalised to transition systems," in *International Workshop on Formal Aspects in Security and Trust*. Springer, 2005, pp. 81–95.

[7] A. Saboori and C. N. Hadjicostis, "Verification of K-step opacity and analysis of its complexity," *IEEE Trans. Autom. Sci. Eng.*, vol. 8, no. 3, pp. 549–559, 2011.

[8] A. Saboori and C. N. Hadjicostis, "Verification of infinite-step opacity and complexity considerations," *IEEE Trans. Autom. Control*, vol. 57, no. 5, pp. 1265–1269, 2011.

[9] X. Yin and S. Lafortune, "A new approach for the verification of infinite-step and K-step opacity using two-way observers," *Automatica*, vol. 80, pp. 162–171, 2017.

[10] X. Y. Cong, M. P. Fanti, A. M. Mangini, and Z. W. Li, "On-line verification of current-state opacity by Petri nets and integer linear programming," *Automatica*, vol. 94, pp. 205–213, 2018.

[11] X. Y. Cong, M. P. Fanti, A. M. Mangini, and Z. W. Li, "On-line verification of initial-state opacity by Petri nets and integer linear programming," *ISA Tran.*, vol. 93, pp. 108–114, 2019.

[12] I. Saadaoui, Z. W. Li, and N. Q. Wu, "Current-state opacity modelling and verification in partially observed Petri nets," *Automatica*, vol. 116, pp. 108907, 2020.

[13] B. Smith and G. Ciardo, "SOUPS: A variable ordering metric for the saturation algorithm," in *Proc. 18th International Conference on Application of Concurrency to System Design*. 2018, pp. 1–10.

[14] E. G. Amparore, S. Donatelli, and G. Ciardo, "Variable order metrics for decision diagrams in system verification," *International Journal on Software Tools for Technology Transfer*. Springer, 2019, pp. 1–22.