Verification and Simulation: Detection and Mitigation of Clock Deviation.
Proposed new Title: Detection and Mitigation of Clock Deviation in the Verification & Validation of Drone-aided Lifting Operations

Reply to the Editor and Reviewers' Comments
Computer Standards & Interfaces

Manuscript Id.: CSI-D-24-00227R1

We express our gratitude to the reviewers and the Editor-in-Chief of Computer Standards & Interfaces for their valuable comments and constructive suggestions during the first round of review. Their input has significantly contributed to the enhancement of our manuscript. In this revised version, we have addressed the various comments and provided detailed responses to the inquiries the Editor and Reviewers raised. Following the structure of the received email for revision, we have provided comprehensive answers to each question and comment. The modifications made to the updated manuscript are highlighted in blue.

Authors Proposed Enhancement

Enhancement 1: To improve reader interest and better reflect the paper's content, we suggest revising the title to: *Detection and Mitigation of Clock Deviation in the Verification & Validation of Drone-aided Lifting Operations.*

Enhancement 2: We have added line numbers to the revised manuscript for easy reference to the specific changes made.

Enhancement 3: The abstract has been updated to better reflect the paper's key findings.

Enhancement 4: The literature review has been expanded to include recent research that clarifies the Verification and Validation.

Comments from Reviewer #1

Comment 1: This paper, titled "Verification and Simulation: Detection and Mitigation of Clock Deviation," reports a simulation-based verification of a simple system in which clock deviation may be observed. The target system is made, and events are generated by using OMNet++ simulator. In addition, two probabilistic models: direct generation and the model based on the events generated by OMNet++, are generated by using PRISM. Four propertis related to clock deviation are shown, and proved by a probabilistic decision tree method.
A program verification package based on a formal method in is now commonly used. The size of the targets of verification is growing to that of real-world programs. This paper is classified as a case study along this line. This is highly evaluated.

Answer: We sincerely appreciate the positive feedback and valuable comments provided, which greatly improved our contribution. Concerning the updated version, we firmly believe that we have effectively addressed the various concerns, as evidenced by the implemented changes.

Comment 2: Some points to be clarified before publication. I would like to evaluate this paper from two points.

Comment 3: Size and complexity of a verification target. If FiGO itself is complicated enough, applying it to only two entities drastically reduces the complexity. It is no longer "gossip."

Answer: Indeed, the formal verification causes a high state space explosion due to the number of phases described in the model. In our case, the model is described in OMNeT to generate traces that are input to the learning process; and then to generate a decision tree for the reduced model in PRISM.

Comment 4: As the second point, a given gateway is used for synchronization. This does not resolve the problem of synchronization. It does not seem that the communication lag is not considered. Furthermore, the chances of clock deviation is estimated low. More general considerations are mandatory.

Answer: Thank you for your feedback. We appreciate you raising these important points regarding synchronization in our work.

We acknowledge that using a single gateway for synchronization might not be ideal for all scenarios, particularly in large or complex networks. In our current work, we focus on a specific use case where a single gateway is suitable due to the configuration of the network. However, we recognize the need for exploring alternative synchronization methods like IRIG time codes in future work. The best method for clock synchronization will depend on the specific application. Factors to consider include the required accuracy, the network environment, and the cost. In our use case;

the person involved in the project tries to find out the low-cost approach to assist engineers in resolving such problems using formal methods.

Communication lag is a critical factor in synchronization, and we agree it should be addressed. In our current work, we took steps towards considering communication lag by estimating the non-exploitable time during model checking within the simulation scenario. This estimation focuses on the number of messages sent by drones and collected by the gateway. Using the simulator, we assess how synchronization impacts communication delays, resulting in a delay range of [0.3; 21.3] seconds. The developed OMNeT++ code now incorporates the computation of communication lag. To enhance realism, we plan to incorporate more precise communication delays in future work. We aim to achieve this by utilizing electronic tools for delay measurement or more advanced simulation techniques. An update was made to the document in lines 565-568.

Reviewers are right; the likelihood of clock deviation may be underestimated depending on the specific scenario. In our work, we assumed a lower degree of clock deviation based on the parameters collected from the referenced paper [7,8]. It's important to highlight that our model is fully parameterizable, allowing users to manually set drift values without the need for additional coding.

We completely agree that more general considerations for synchronization are necessary. Our work currently focuses on the use case by portraying the tools that can enable verification and validation from an engineering perspective. In future work, we plan to expand our research to include considerations like drifting frequency due to other environmental variations.

Comment 5: the list of properties given in this paper in terms of appropriateness to express the clock deviation. Actually, as the authors admit, property 1 depends on the liveness, or fairness in scheduling. Usually, fairness is expressed in a form of formula, and the property "scheduling is fair → property 1 is satisfied."
Property 2 in a natural language is not of the form "property." That in the form of formula makes sense, however, it is not clear if "Desynchronized" is an atomic property or can be broken down.

Answer: We agree that fairness in scheduling can influence the satisfaction of Property 1. But it has not been addressed in our paper as the fairness can be expressed in the form of "unfair"$\rightarrow P \geq 1[F(D1H == D2H)]$ where "unfair"= !(D1H = D2H)

Property 2 is formulated as a reward structure as part of the PCTL property structure. To address the reviewer's point, we emphasize the specific structure of this property in lines 16-20 of listing 3. The rewards content has been portrayed to explain its structure in PRISM in lines 480-482.

Comment 6: Property 4 lacks some fundamental assumption. In general, the property that clock deviation is within a given range is never trivial. Some assumptions are necessary, but they are not explained. This property is not for clock deviation, but just used for justification of the target program. Generally, clock deviation is dependent on its environment, which means that both positive and negative directions must be considered. It is dubious that the authors have considered these cases.

Answer: Thank you for your valuable feedback on Property 4. We appreciate you raising these important points concerning clock deviation and its assumptions.

We acknowledge that the explanation of Property 4 may lack clarity regarding its underlying assumptions. In our work, we employ machine learning to generate a rule set that facilitates reasoning about the system's behavior, specifically focusing on the synchronization of drones' values not the output of the synchronization of their values. Unlike neural networks, decision tree learning generates a set of rules that can be directly interpreted to identify classes within the data produced by the simulation.

Comment 7: I also admit the effectiveness of probabilistic model checking for events generated by a simulator in terms of efficiency, but the authors must also note that it is not a verification in its most rigid meaning. The gap must be discussed and reflected in the paper.
Overall, the authors must reconsider the problem setting in terms of the size and complexity. Properties must be also reconsidered so that appropriate assumptions are expressed in the properties.

Answer: We completely agree that Probabilistic model checking, while efficient for analyzing event streams from simulators, differs from verification in its strictest sense. There is an inherent gap due to the statistical nature of Probabilistic model checking results.

Our paper addresses a gap between verification and validation in drone lifting operations with restricted components. We propose a simple, yet effective algorithm specifically tuned to address clock synchronization issues. To handle model complexity, we learn rules that reflect the behavior of the cluster (drones and cranes). Furthermore, the cluster can be replicated to demonstrate the efficiency of the synchronization algorithm and highlight the gap between the verification of the original model and the learned model as clearly demonstrated in Table 1.

Comments from Reviewer #2

Comment 1: In this work authors proposed an approach to model, analyze, and verify clock deviations due to changes in the environmental conditions. The approach exploits the OMNeT++ simulation framework to model the studied system and to derive a Probabilistic Decision Tree (PDT) which is then interpreted and verified through the PRISM language. The proposed approach has been applied to a multi-crane scenario in which a set of drones is helping to coordinate the cranes during the joint lifting of a payload.
The paper is well-written and the overall approach seems sound, however, the motivational aspects and the discussion about related works must be improved. In addition, some introductive aspects are missing or provided in a later stage, making the paper somehow difficult to read.

Answer: We are grateful for the valuable feedback we received, which has significantly improved our work. We appreciate both the positive comments and the constructive criticism that helped us address the raised concerns. This is evident in the revised version, which includes several improvements. We have strengthened the Related Works section by incorporating recent research on clock drift evaluation (lines 156-158 and 171-197) and performing the reorganization. Additionally, we have improved the clarity of the abstract and refined the clock drift definition (lines 55-61). Furthermore, we have expanded the introduction section on formal methods, explaining their necessity (lines 62-67) and clarifying the use case (lines 86-91). Finally, the contribution overview has been enhanced (lines 92-108) to communicate the key advancements of our work.

Comment 2: The introduction provided in Sec.1 must be extended. The motivational aspects of this work are not clear, why is detecting clock inaccuracies so important? What kind of errors could it generate? In this section, the authors also provided a brief state-of-the-art on formal methods, but this is difficult to understand as the role of formal methods within the proposed approach has not been yet introduced.

Answer: Thanks for the feedback. We have strengthened the introduction by adding a concrete example of how clock deviations can impact systems lines 50-53. We have also included a reference to a research paper to support the importance of detecting these inaccuracies. Furthermore, we emphasize the value of formal methods in addressing clock deviation issues in lines 55-61.

Comment 3: Still in Sec.1 the proposed case study has not been introduced nor motivated. Why are you studying clock deviation in this scenario? Why is it a relevant example for your approach? I think that the paper would benefit from a brief description/motivation of the case study at this stage, also because the sentence "cranes in a drone system" is not sufficient to summarize the application.

Answer: The use case has been introduced in section 1 in lines 85-90.

Comment 4: The literature review provided in Sec.2 and Sec.7 is not sufficient. Authors mostly list background approaches and methodologies but there is no motivation nor references to similar works. Authors must provide a discussion/comparison about/against similar works and some motivational insights related the proposed approach. I also suggest to move Sec.7 after the introduction and to merge it with Sec.2 in order to improve the paper readability.

Answer: Thanks for the feedback. We have combined Section 7 and a subsection of Section 2 to create a comprehensive literature review. This consolidated section provides a more comprehensive overview of existing research. A comparative analysis of related works is now included in lines 171-197.

Comment 5: The FiGo protocol described in Sec.4 has never been introduced previously, but this is odd as it seems to me that the proposed framework is designed specifically to validate such algorithm. Authors must introduce FiGo at an early stage and motivate why they decided to focus on this algorithm among others. In addition, I think that a discussion about if or how the proposed approach can be used to model different synchronization algorithms can improve the impact of the paper.

Answer: An explanation of the algorithm used has been added to the introduction (lines 55-61) for better clarity. A discussion on the feasibility of the approach has been added to the Discussion section (lines 666-682).

Comment 6: Description of case study is not clear. Why do cranes need drones for lifting instead of simple position sensors? Why does this operation need clock synchronization instead of a simple synchronization protocol? Also in this case some comments about motivational aspects are needed.

Answer: This use case originates from a European research project aiming to automate the lifting process without human intervention. The project utilizes drones to synchronize the lifting operation between cranes (lines 385-393). Moreover, drones are increasingly optimized for energy consumption throughout their life cycle, while also implementing synchronization to ensure accurate data output as mentioned in lines 80-85.

Comment 7: In Sec.1 the sentence "our contribution can be summarized as follows threefold" seems wrong as there are 4 items listed.

Answer: Thanks. The contribution numbering has been updated in lines 101-111.

Comment 8: Achronyms (such as PA and PDT) are defined several times in the text. Please define them just the first time, then use the abbreviation only.

Answer: Thanks for the comment. We have incorporated the relevant updates into the manuscript.

Comment 9: In Sec.2 perhaps it would be better to explain the PRISM Language before to define the automat since some concepts such as communication and synchronization are explained here.

Answer: Update has been performed over section 2 (Background).

Comment 10: The text from Fig.3 and 4 is too small and difficult to read.

Answer: The font size of figure captions has been increased.

Comment 11: There are 2 references to Alg.1 in the paper.

Answer: The references have been updated to ensure each section of the paper accurately cites the relevant algorithms.