


Reliability Model and Analysis for Triple-model with Triple-input Machine Learning System

Qiang Wen and Fumio Machida
Department of Computer Science
University of Tsukuba

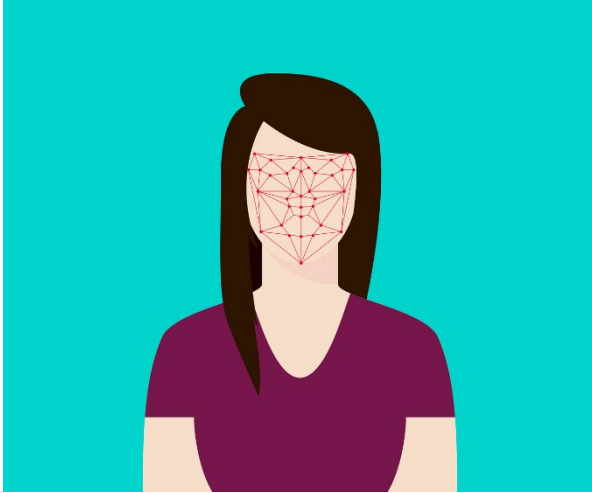
IEEE 5th Conference on Dependability and Secure Computing (IEEE DSC 2022)



Outline

- Introduction
- Background
- Related Work
- Reliability Model
- Numerical Analysis
- Conclusion

Introduction-Machine Learning

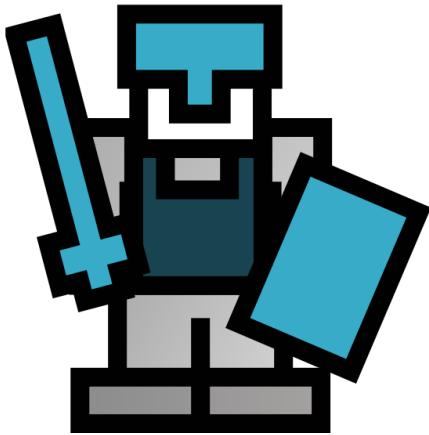


◆ Machine learning (ML)

- Components of many intelligent software systems

◆ ML-based intelligent software

- Speech and image recognition
- Strategy games
- Robot applications



Introduction-Reliability Issues

- ◆ Outputs of machine learning models
 - Uncertain and sensitive to the input data
 - Undesirable consequences

- ◆ ML components
 - Algorithms
 - Training data sets

Introduction-Reliability Issues

- ◆ Approaches to ML-based system reliability improvement
 - Data validations
 - Lack of generalization
 - Safety monitors
 - Lack of flexibility
 - ✓ Redundant architecture

Outline

- Introduction
- **Background**
- Related Work
- Reliability Model
- Numerical Analysis
- Conclusion

Background- Safety-critical ML System

- ◆ Safety-critical ML system
 - Extremely-accurate ML models
 - Impractical to guarantee 100% accuracy for real-world samples
 - Error outputs from ML models are inevitable

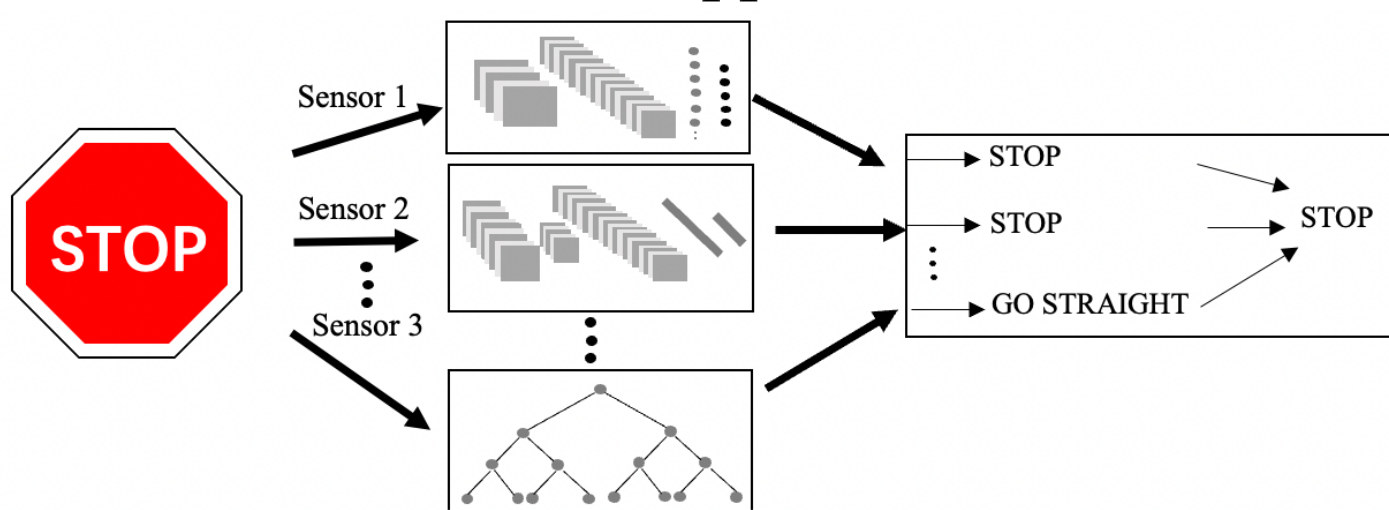
Background- N-version ML Architecture

◆ N-version ML Architecture

- Based on N-version programming.
- Use multiple inputs and multiple ML models in a system

◆ Effects

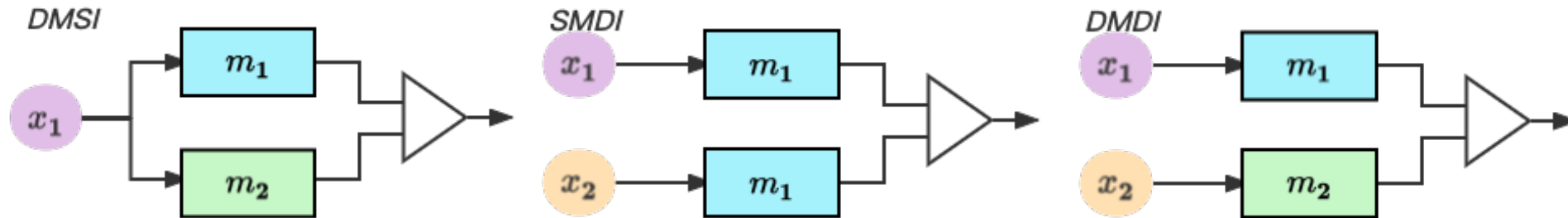
- Get accurate result even if errors happen in some of the ML models



Background- Two-version Architecture

◆ Systems with different reliabilities

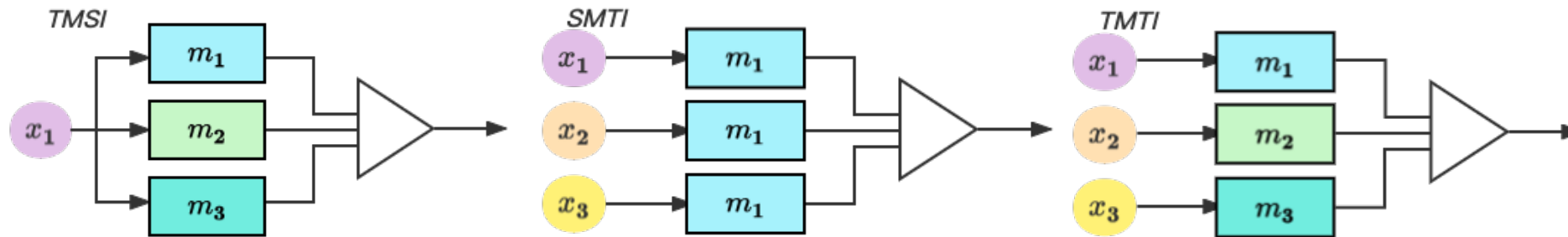
- Double model with single input system (DMSI)
- Single model with double input system (SMDI)
- Double model with double input system (DMDI)



- In a two-version architecture, when both running models output error, the whole system fails.

Background- Three-version Architecture

- ◆ Triple model with single input system (TMSI)
- ◆ Single model with triple input system (SMTI)
- ◆ Triple model with triple input system (TMTI)



- In a three-version architecture, the system fails when error output occurs to more than two of the running ML models. (Majority voting rule)

Outline

- Introduction
- Background
- **Related Work**
- Reliability Model
- Numerical Analysis
- Conclusion

Related Work-Reliability Improvement

- ◆ Reliability improvement of ML models
 - ML testing technique
 - Adversarial learning
- ◆ Reliability improvement of ML systems
 - Multi-version ML approaches
 - Single input
 - Two-version architectures

Related Work-Reliability Improvement

- ◆ Our research
 - Reliability of three-version ML architectures
 - Diversity metrics
 - Potential reliability improvements
 - TMTI architecture

Outline

- Introduction
- Background
- Related Work
- **Reliability Model**
- Numerical Analysis
- Conclusion

Reliability Model-Parameter Definition

- ◆ f_k : The probability that the ML model m_k outputs error.
- ◆ S : The total sample space of inputs.
- ◆ E_k : ($E_k \subseteq S$) The set of input data that leads to output error by ML model m_k .

$$f_k = \frac{|E_k|}{|S|}$$

Reliability Model-Model Diversity

- ◆ Model diversity- Intersection of errors
 - Intersection of errors $\alpha_{i,j} \in [0,1]$

$$\alpha_{i,j} = \frac{|E_i \cap E_j|}{\min\{|E_i|, |E_j|\}}$$

Reliability Model-Input Diversity

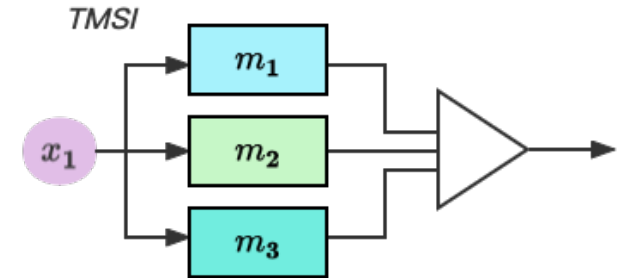
- ◆ Input diversity- Conjunction of errors
 - x_i and x_j : the inputs to ML models from different data sources (e.g., sensors).
 - Conjunction of errors $\beta_{k,i|j} \in [0,1]$

$$\beta_{k,i|j} = Pr[x_i \in E_k | x_j \in E_k]$$

Reliability Model-Reliability of TMSI

◆ TMSI Error cases

Situation(fail)	1	2	3	4
Output error	m_1, m_2	m_1, m_3	m_2, m_3	m_1, m_2, m_3



◆ TMSI failure probability

$$f_{3,1}(m_1, m_2, m_3; x_1)$$

$$= \alpha_{1,2} \cdot f_1 + \alpha_{1,3} \cdot f_1 + \alpha_{2,3} \cdot f_2 - 2\alpha_{1,2} \cdot \alpha_{1,3} \cdot f_1 \quad (\text{We assume } |E_1| \leq |E_2| \leq |E_3|)$$

$$f_{2,1}(m_1, m_2; x_1) = Pr[x_1 \in E_1, x_1 \in E_2] = \alpha_{1,2} \cdot f_1 \quad (\text{DMSI failure probability})$$

$$f_{3,1}(m_1, m_2, m_3; x_1) = f_{2,1}(m_1, m_2; x_1) + f_{2,1}(m_1, m_3; x_1) + f_{2,1}(m_2, m_3; x_1) - 2\alpha_{1,2} \cdot \alpha_{1,3} \cdot f_1$$

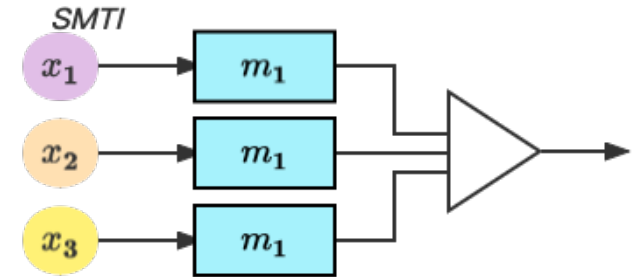
◆ Reliability of TMSI:

$$R_{3,1}(m_1, m_2, m_3; x_1) = 1 - f_{3,1}(m_1, m_2, m_3; x_1)$$

Reliability Model-Reliability of SMTI

◆ SMTI Error cases

Situation(fail)	1	2	3	4
Error	x_1, x_2	x_1, x_3	x_2, x_3	x_1, x_2, x_3



◆ SMTI failure probability

$$f_{1,3}(m_1; x_1, x_2, x_3)$$

$$= \beta_{1,2|1} \cdot f_1 + \beta_{1,3|1} \cdot f_1 + \beta_{1,3|2} \cdot f_2 - 2\beta_{1,2|1} \cdot \beta_{1,3|1} \cdot f_1 \quad (\text{We assume } |E_1| \leq |E_2| \leq |E_3|)$$

$$f_{1,2}(m_1; x_1, x_2) = Pr[x_1 \in E_1, x_2 \in E_1] = \beta_{1,2|1} \cdot f_1 \quad (\text{SMDI failure probability})$$

$$f_{1,3}(m_1; x_1, x_2, x_3) = f_{1,2}(m_1; x_1, x_2) + f_{1,2}(m_1; x_1, x_3) + f_{1,2}(m_1; x_2, x_3) - 2\beta_{1,2|1} \cdot \beta_{1,3|1} \cdot f_1$$

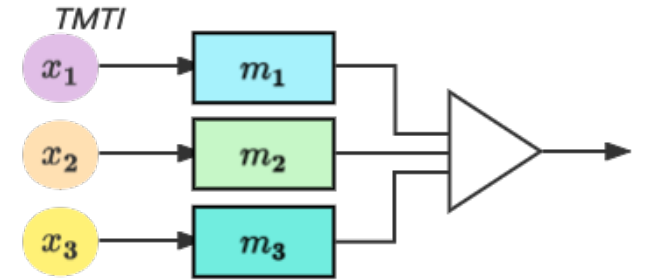
◆ Reliability of SMTI:

$$R_{1,3}(m_1; x_1, x_2, x_3) = 1 - f_{1,3}(m_1; x_1, x_2, x_3)$$

Reliability Model-Reliability of TMTI

◆ TMTI Error cases

Situation(fail)	1	2	3	4
Fail	m_1, m_2	m_1, m_3	m_2, m_3	m_1, m_2, m_3



◆ TMTI failure probability

$$f_{2,2}(m_1, m_2; x_1, x_2) = [\beta_{1,2|1} \cdot \alpha_{1,2} + (1 - \beta_{1,2|1}) \cdot (f_2 - \alpha_{1,2} \cdot f_1) / (1 - f_1)] \cdot f_1 \quad (\text{DMDI failure probability})$$

$$f_{3,3}(m_1, m_2, m_3; x_1, x_2, x_3) = f_{2,2}(m_1, m_2; x_1, x_2) + f_{2,2}(m_1, m_3; x_1, x_3) + f_{2,2}(m_2, m_3; x_2, x_3) - 2f_{2,2}(m_1, m_2; x_1, x_2) \cdot f_{2,2}(m_1, m_3; x_1, x_3) / f_1$$

(We assume $|E_1| \leq |E_2| \leq |E_3|$)

◆ Reliability of TMTI:

$$R_{3,3}(m_1, m_2, m_3; x_1, x_2, x_3) = 1 - f_{3,3}(m_1, m_2, m_3; x_1, x_2, x_3)$$

Outline

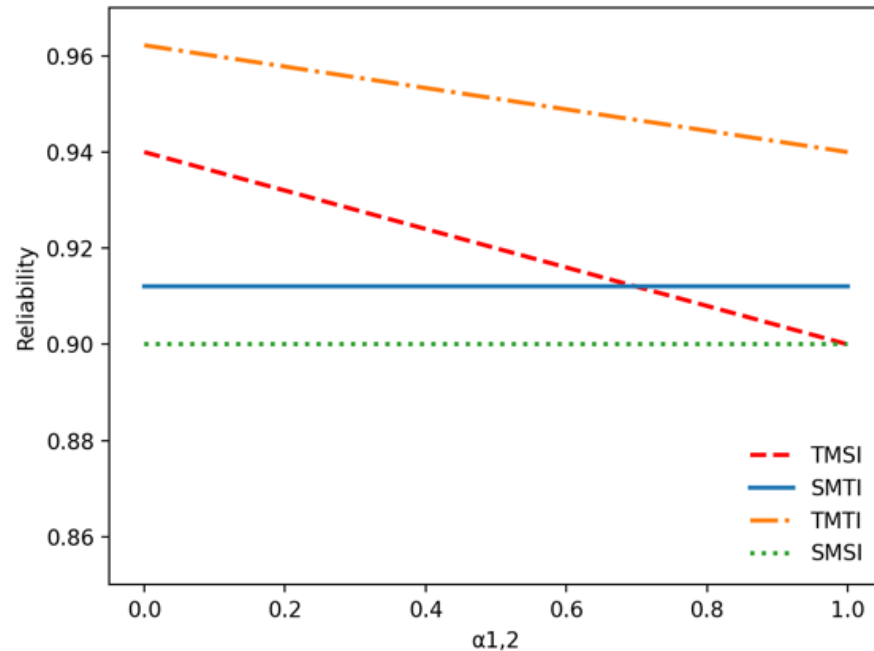
- Introduction
- Background
- Related Work
- Reliability Model
- **Numerical Analysis**
- Conclusion

Numerical analysis-Research Questions

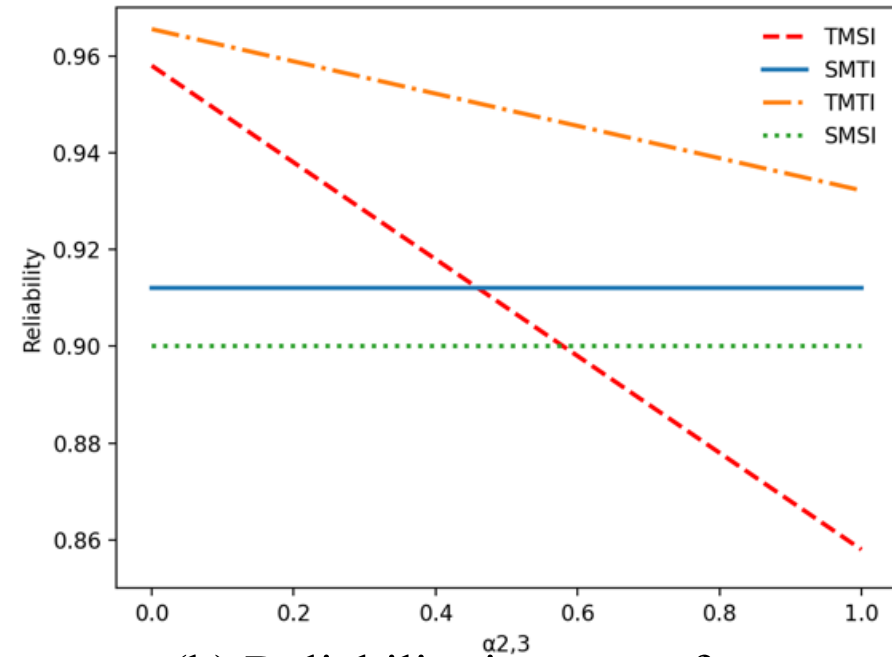
- ◆ How does the model diversity affect the reliabilities of three-version architecture systems? (Q1)
- ◆ How does the input diversity affect the reliabilities of three-version architecture systems? (Q2)
- ◆ Do three-version architectures achieve higher reliabilities than two-version architectures? (Q3)
- ◆ How does the variance of diversity metrics impact the reliability of TMTI? (Q4)

Numerical analysis-Q1

◆ Reliability impacts of model diversity



(a) Reliability impacts of $\alpha_{1,2}$



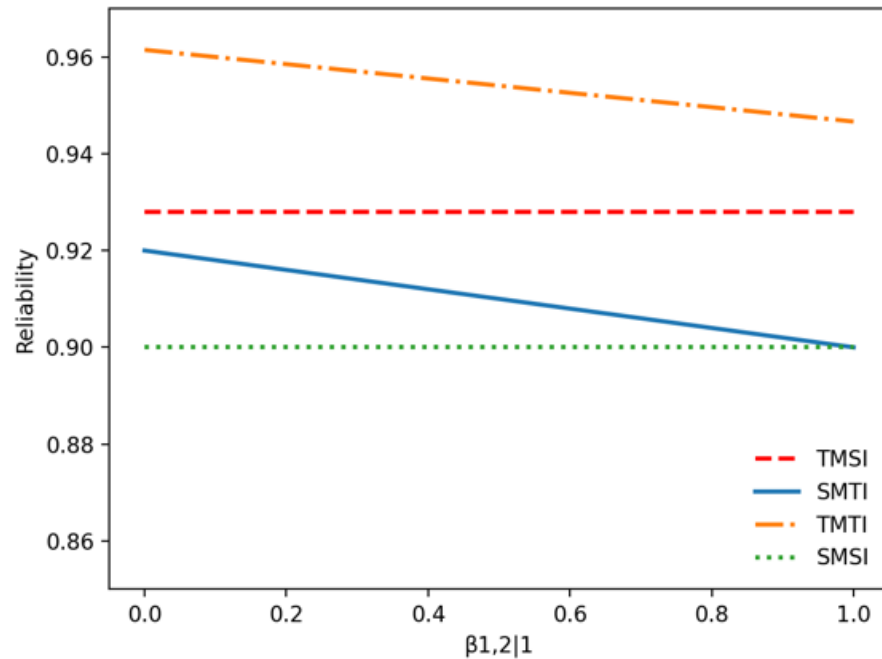
(b) Reliability impacts of $\alpha_{2,3}$

Observation 1. The higher model diversity (the smaller value of intersection of errors) leads to the higher reliability of TMTI and TMSI.

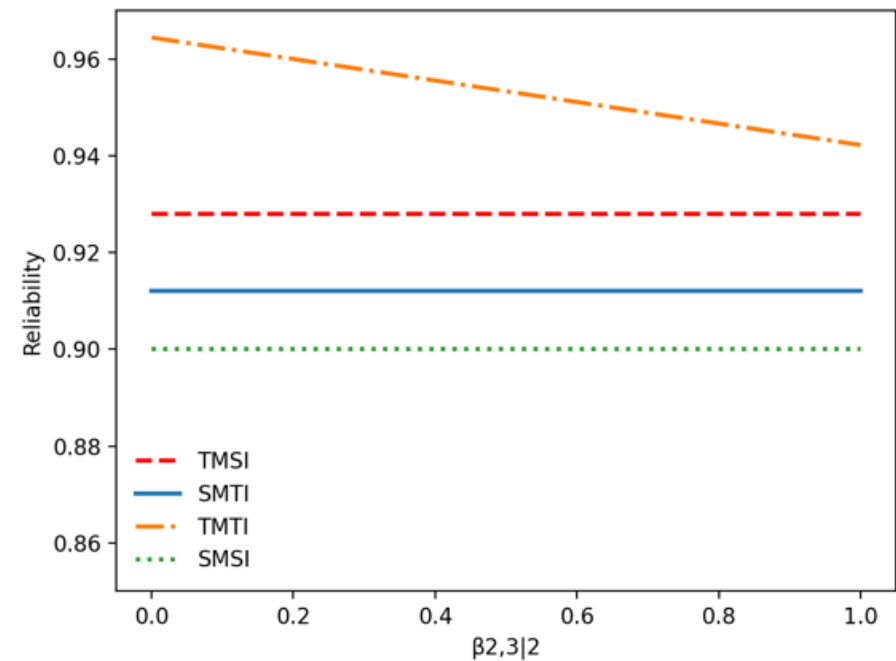
Observation 2. The reliability of TMSI can be worse than even a single model when the intersection of errors is high.

Numerical analysis-Q2

◆ Reliability impacts of input diversity



(a) Reliability impacts of $\beta_{1,2|1}$



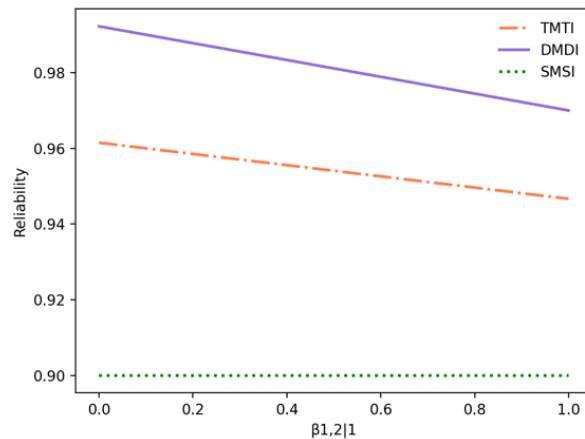
(b) Reliability impacts of $\beta_{2,3|2}$

Observation 3. The higher input diversity (the smaller value of conjunction of errors) results in the higher reliability of TMTI, when other parameters are fixed.

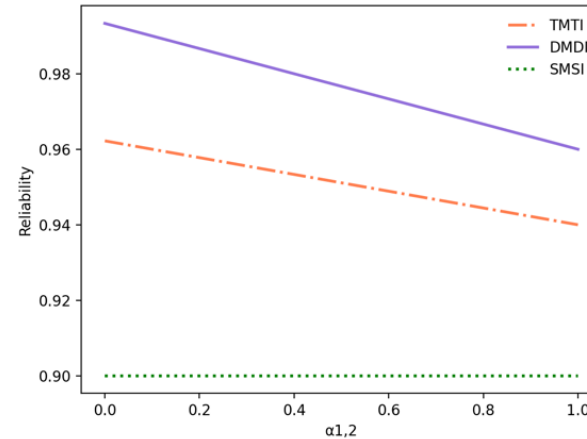
Numerical analysis-Q3

◆ Three-version vs. two-version architectures

$$\alpha_{1,3} = \alpha_{2,3} = 0.3, \\ \beta_{1,3|1} = \beta_{1,3|2} = \beta_{2,3|2} = 0.4.$$

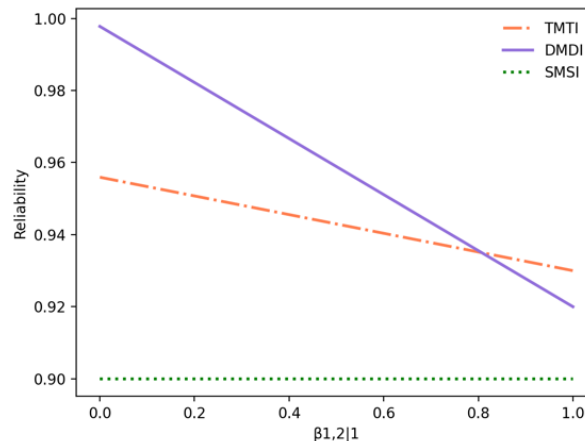


(a) Reliability impacts of $\beta_{1,2|1}$

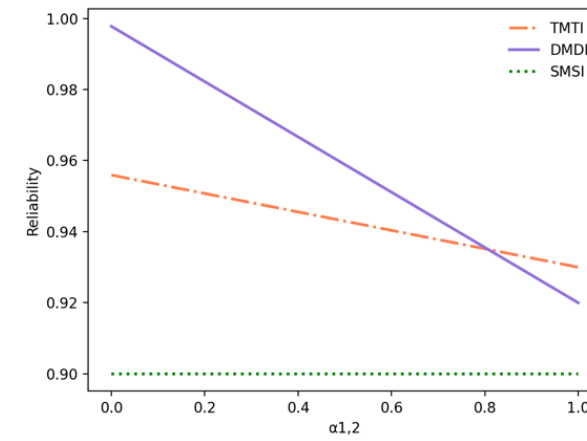


(b) Reliability impacts of $\alpha_{1,2}$

$$\alpha_{1,3} = 0.8 \text{ and } \alpha_{2,3} = 0.1, \\ \beta_{1,3|1} = \beta_{1,3|2} = \beta_{2,3|2} = 0.4.$$



(c) Reliability impacts of $\beta_{1,2|1}$

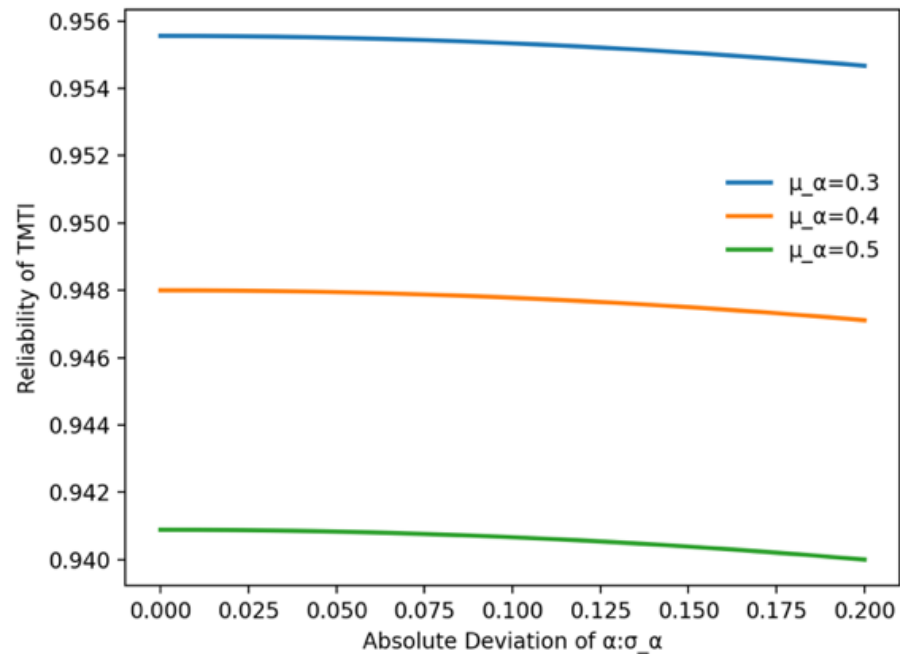


(d) Reliability impacts of $\alpha_{1,2}$

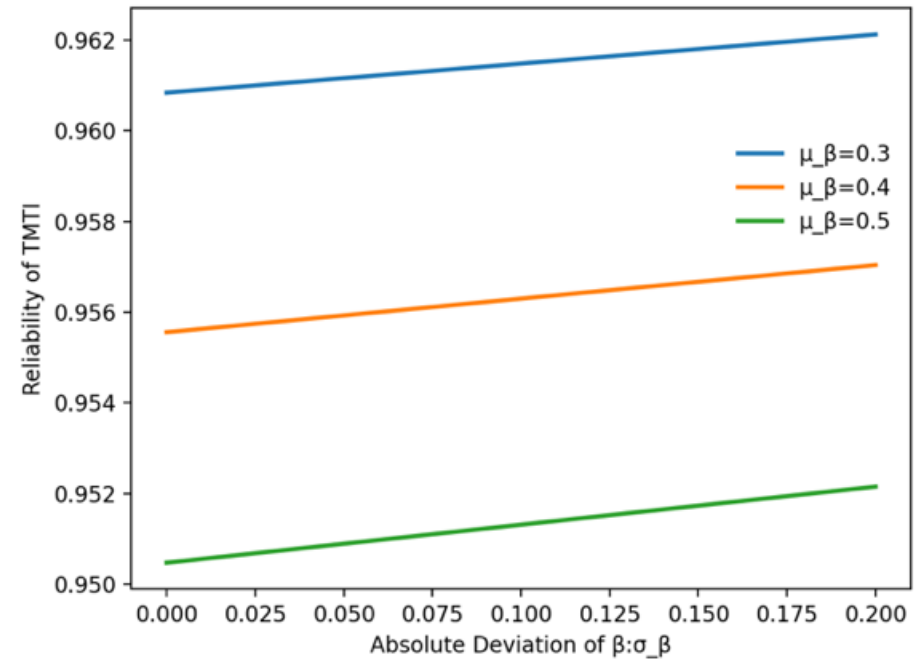
Observation 4. The reliability of DMDI tends to be better than the reliability of TMTI because of the difference of decision logic. However, with more stringent restrictions, the advantage of TMTI can emerge.

Numerical analysis-Q4

◆ Reliability impacts of TMTI



(a) Reliability of TMTI by varying σ_α



(b) Reliability of TMTI by varying σ_β

Observation 5. A larger variance of model diversities negatively impacts the TMTI reliability, while a larger variance of input diversity has opposed impacts.

Outline

- Introduction
- Background
- Related Work
- Reliability Model
- Numerical Analysis
- **Conclusion**

Conclusion

- ◆ Propose reliability models for three-version architectures
 - Diversity metrics
- ◆ Conduct numerical analysis on the proposed model.
- ✓ The reliability of TMTI systems tends to be higher than other three-version systems.
- ✓ The reliability of a DMDI system is generally more reliable than the reliability of a TMTI system.
- ✓ The variance of model diversity negatively impacts on TMTI reliability, while the variance of input diversity has positive impacts.

Conclusion

◆ Future work

- Extend our model to higher versions and compare the reliability of different architectures.
- Analytically identify the conditions where TMTI achieves higher reliability than others.
- Estimate the parameter values of diversity parameters from empirical studies.

THANKS FOR YOUR ATTENTION!