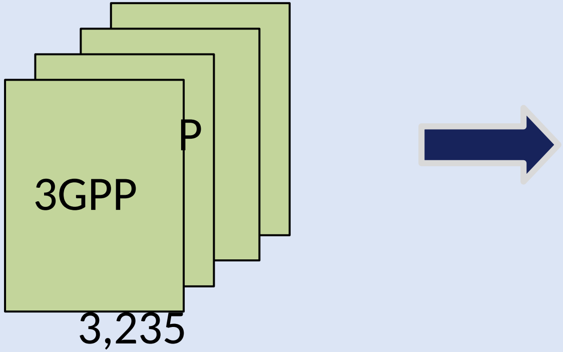
5GPT: 5G Vulnerability Detection by Combining Zero-shot capabilities of GPT-4 with Domain-specific Strategies

Asif Shahriar, Syed Jarullah Hisham, K.M. Asifur Rahman, Ruhan Islam,
Md. Shohrab Hossain, Ren-Hung Hwang, Ying-Dar Lin

IEEE Transactions on Information Forensics & Security (IEEE TIFS), 2025

Presented by: Asif Shahriar

Challenges in Cellular Protocol Vulnerability Discovery



3GPP

P

3,235

Vulnerability Detection Methods

- Formal verification
- ML and NLP models
- Fuzz Testing
- White-box methods

Overall Gap Analysis

Manual Analysis

Time consuming, prone to human error, and miss subtle vulnerabilities

Domain Expertise

Most of the works require significant domain knowledge

NLP Limitations

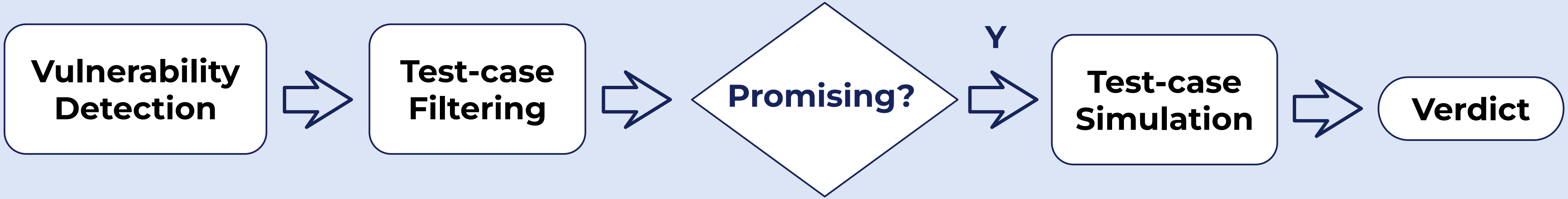
NLP methods struggle to understand the technical jargons and ambiguities

Motivations for Using LLMs

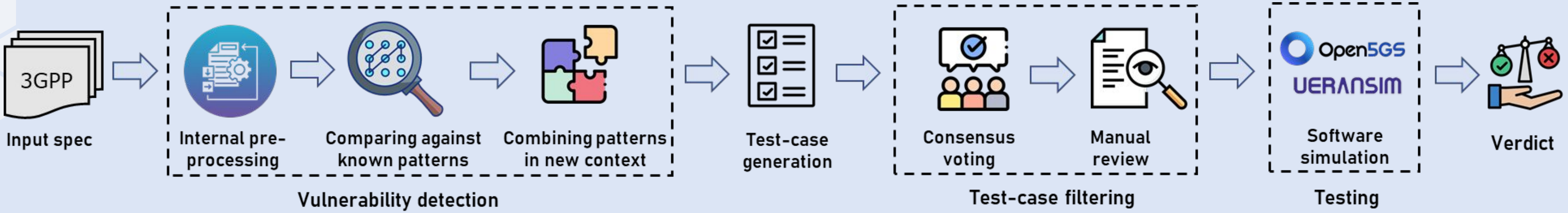
- Deep contextual understanding capability
- Minimal training requirement
- Flexibility & adaptability
- **Prompt engineering**

Methodology

Methodology Overview



Zero-shot Approach



Input spec

Internal pre-processing

Comparing against known patterns

Combining patterns in new context

Vulnerability detection

Test-case generation

Consensus voting

Manual review

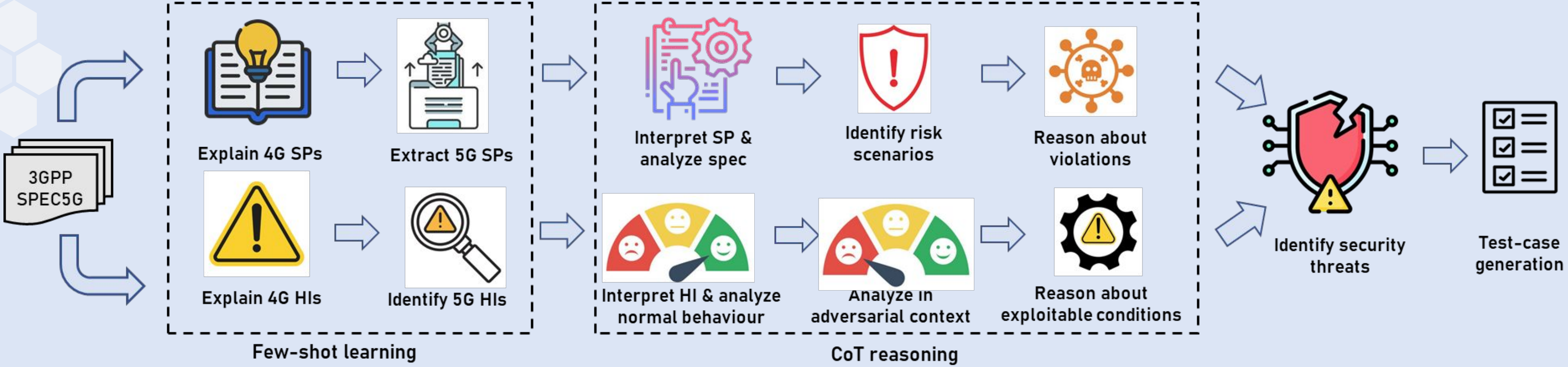
Test-case filtering

Software simulation

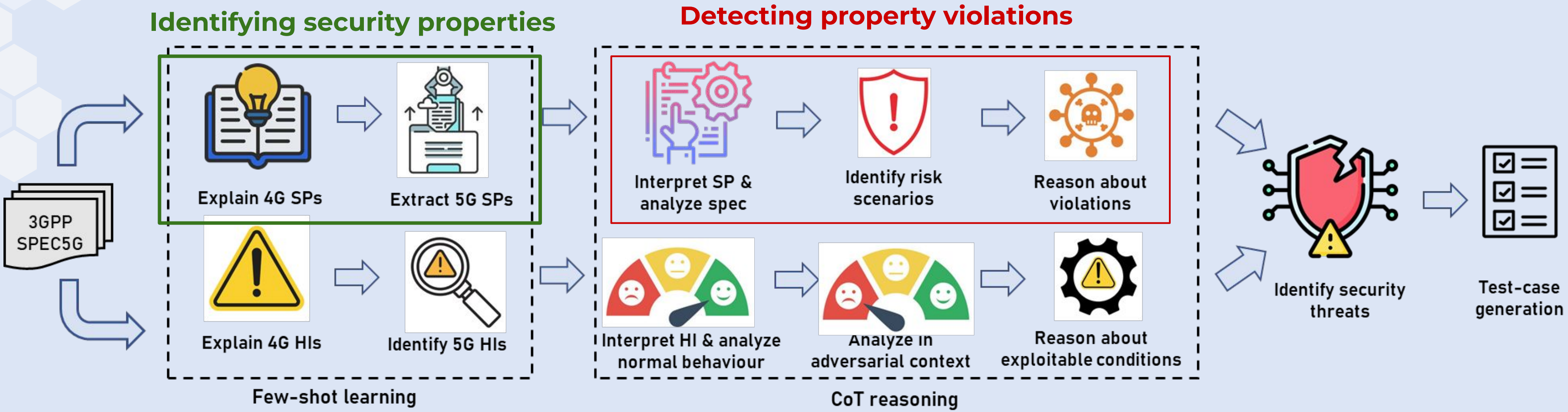
Testing

Verdict

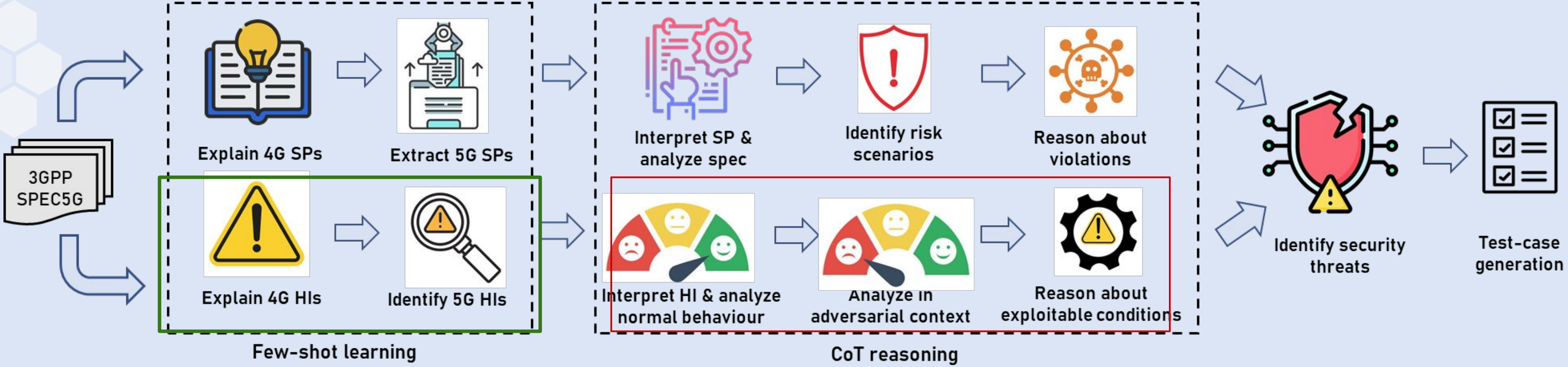
Domain-aware Approach



Detecting Security Violation


Identifying security properties
Detecting property violations
3GPP SPEC5G
Explain 4G SPs
Extract 5G SPs
Explain 4G HIs
Identify 5G HIs
Few-shot learning
Interpret SP & analyze spec
Identify risk scenarios
Reason about violations
Interpret HI & analyze normal behaviour
Analyze in adversarial context
Reason about exploitable conditions
CoT reasoning
Identify security threats
Test-case generation

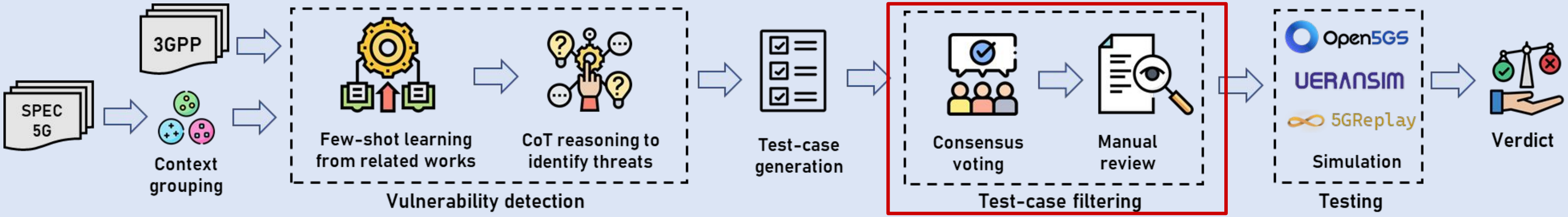
Identifying Hazard Indicators



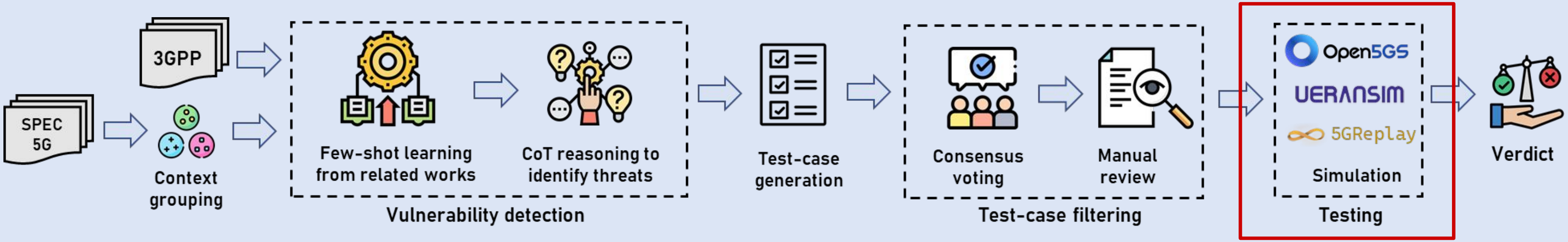
Finding Hazard Indicators

Identifying potential exploitation

Test-case Filtering



Test-case Simulation



SPEC 5G

3GPP

Context grouping

Few-shot learning from related works

CoT reasoning to identify threats

Vulnerability detection

Test-case generation

Consensus voting

Manual review

Test-case filtering

Open5GS

UERANSIM

5GReplay

Simulation

Testing

Verdict

Findings

Summary Findings

47

Potential vulnerabilities identified

27

Novel vulnerabilities

20

Known vulnerabilities

9

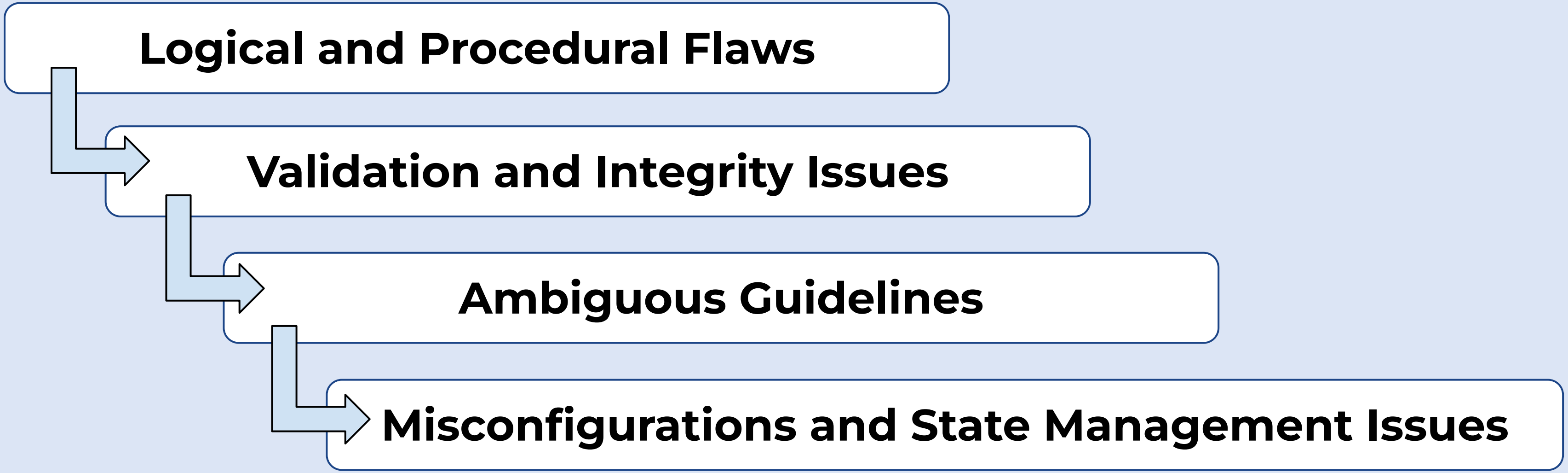
Validated through simulation

Zero-shot Findings

46 Suggestions

24 Potential vulnerabilities

12 Novel



Logical and Procedural Flaws

Validation and Integrity Issues

Ambiguous Guidelines

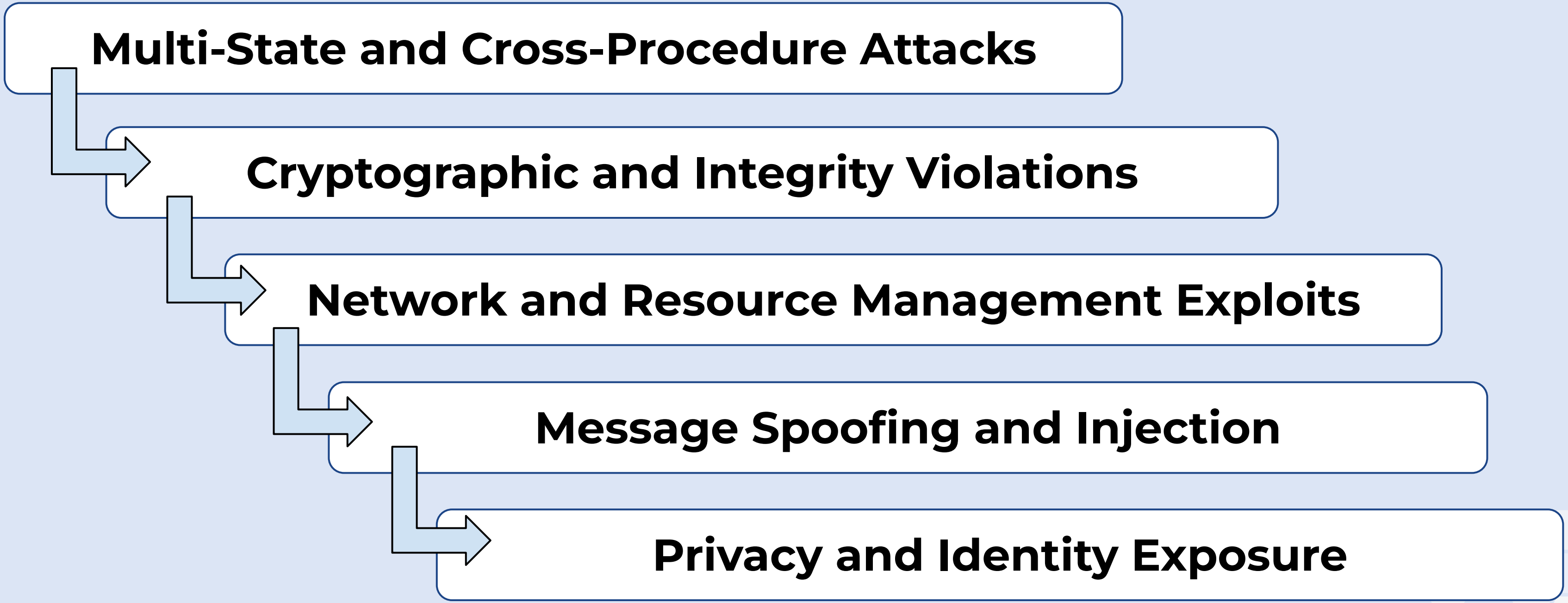
Misconfigurations and State Management Issues

Domain-Aware Findings

34 Suggestions

23 Potential vulnerabilities

15 Novel



Multi-State and Cross-Procedure Attacks

Cryptographic and Integrity Violations

Network and Resource Management Exploits

Message Spoofing and Injection

Privacy and Identity Exposure

Limitations & Future Work

- Inherent simulator limitations
- Risk of losing context due to segmentation
- Not all potential vulnerabilities were tested
- Reliance on manual filtering

Limitations

- Testing all potential vulnerabilities
- Hardware testing
- Automating the filtering process
- Develop mitigation strategies

Future Work

Acknowledgements

Collaborators:

- Dr. Ren-Hung Hwang, *Professor, College of AI, National Yang, Ming Chiao Tung University, Tainan, Taiwan*
- Dr. Ying-Dar Lin, *Professor, Department of Computer Science, National Chiao Tung University, Taipei, Taiwan*

Guidance:

- Dr. Imtiaz Karim, *Assistant Professor, Department of Computer Science, UT-Dallas, BUET-CSE alumni*
- Kazi Samin Mubasshir, *Graduate Research Assistant, Department of Computer Science, Purdue University, BUET-CSE alumni*

Thank You

Q/A