



Motivation

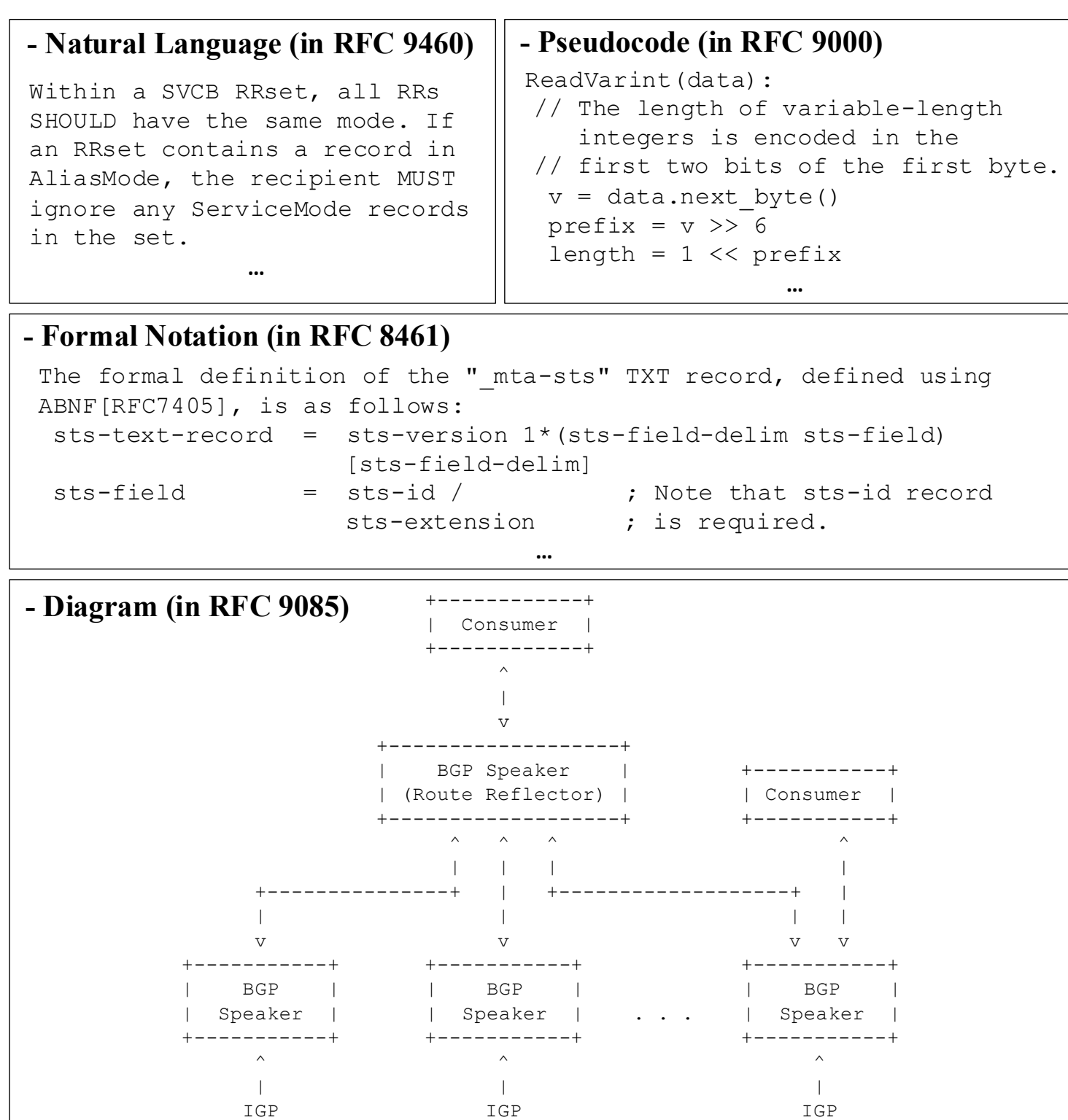
- Internet Protocol specifications are prone to ambiguities, undermining their interoperability and implementation correctness.
- LLMs can automatically analyze specifications by reading heterogeneous formats, combining information from different sources, and applying common networking knowledge.

Challenges of Using LLMs

- Lengthy specification documents
- Multi-document reasoning
- Limited domain knowledge
- Prone to hallucination

Key Contributions

- First systematic study of logical ambiguities in Internet Protocol specifications (RFCs)
- First framework for automatically detecting ambiguities in RFCs

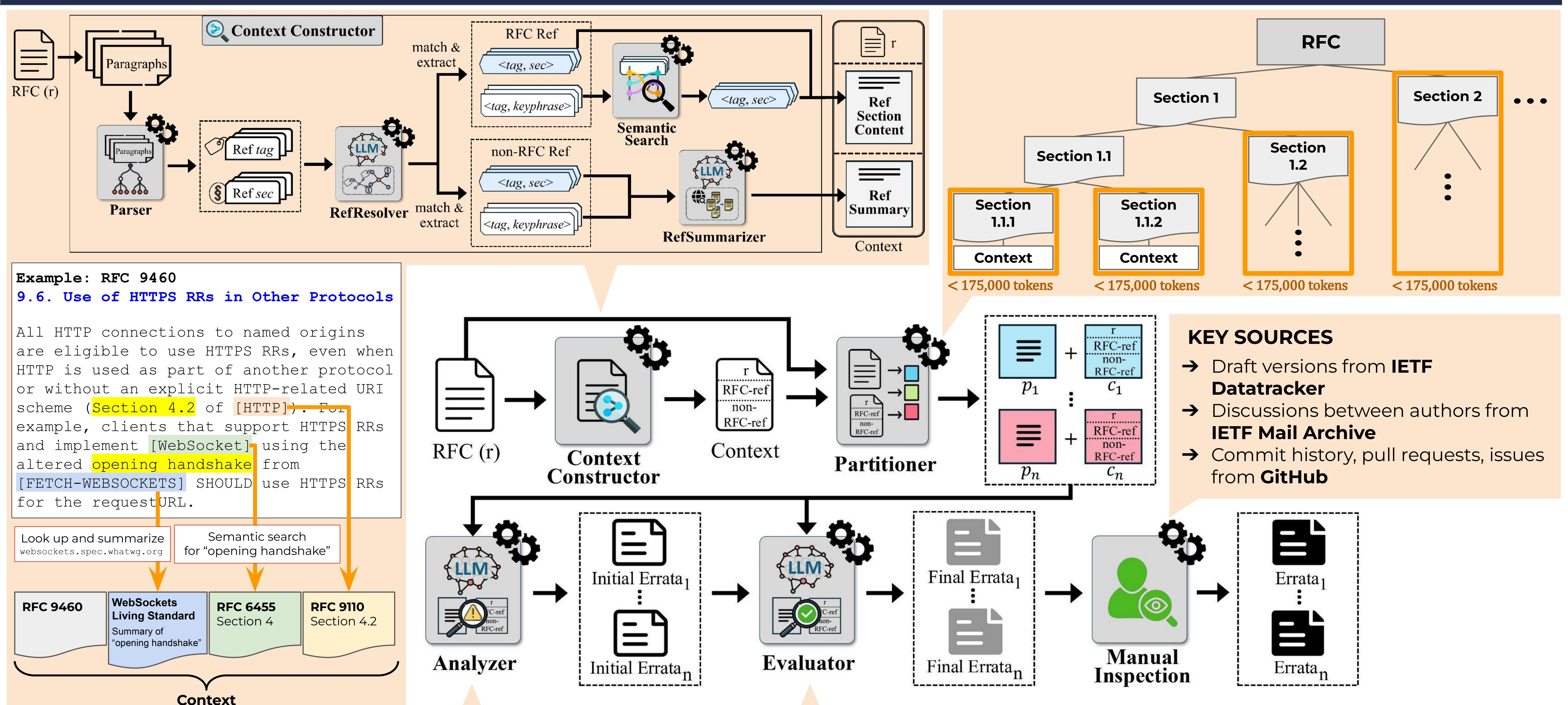


Study

Manual classification of 273 verified technical errata reports from Standards Track RFCs published between January 2014 and January 2025

Main Category (Total Count)	Sub-Category	Count
Inconsistency (202)	I-1 Direct inconsistency within or across specifications	119
	I-2 Indirect inconsistency within or across specifications	70
	I-3 Inconsistency with commonly accepted knowledge	13
Under-specification (37)	U-1 Direct under-specification due to undefined terms	7
	U-2 Direct under-specification due to incomplete constraints	15
	U-3 Indirect under-specification within or across specifications	10
	U-4 Under-specification due to incorrect or missing references	5
Others (34)	Editorial errors	15
	IANA considerations	13
	Suggestions or proposals	6

Approach



The LLM is asked to detect ambiguities in the given section with the **context** and **insights from our study**.

- Ambiguity types to find
- Strategies to detect different ambiguity types
- Examples of each ambiguity type

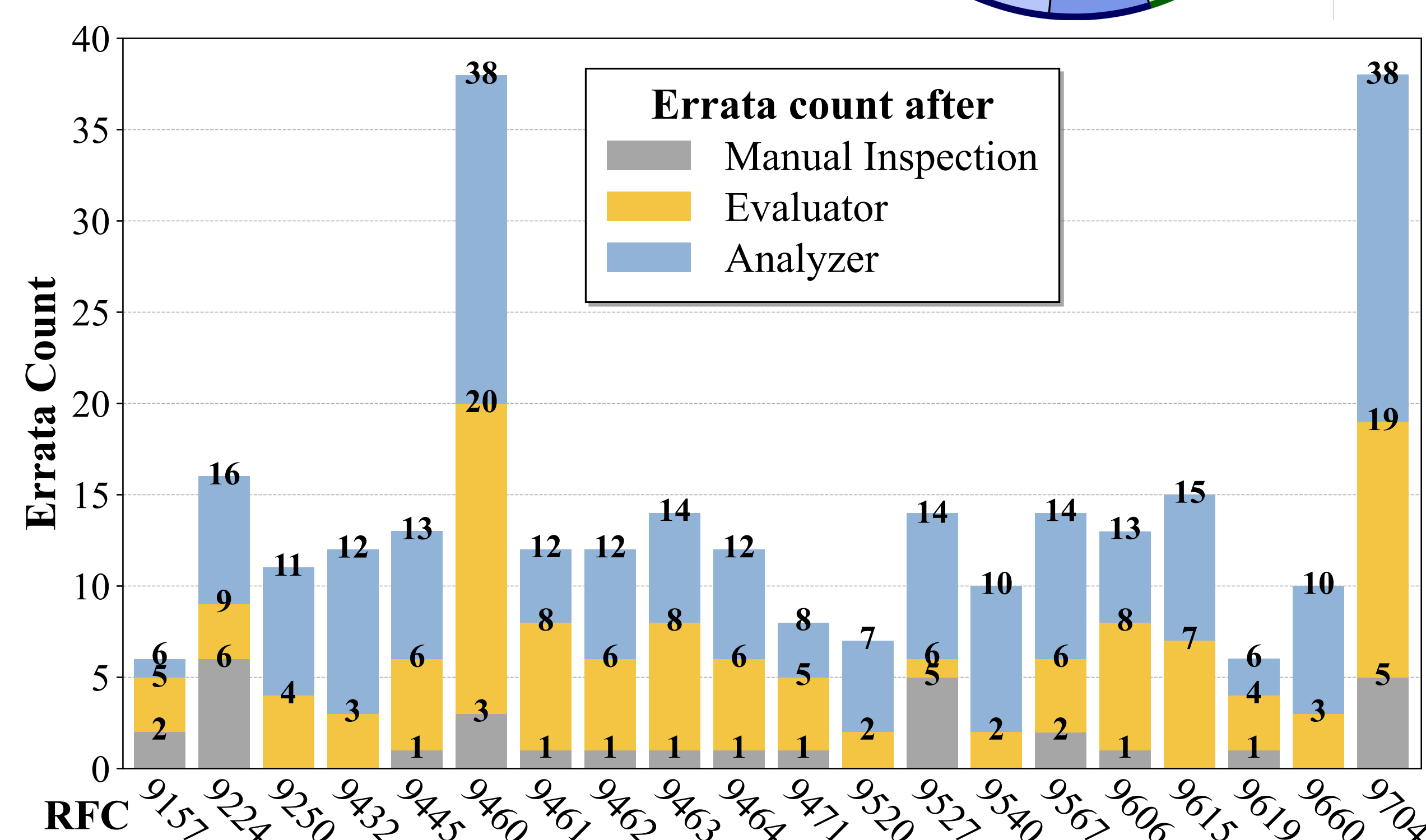
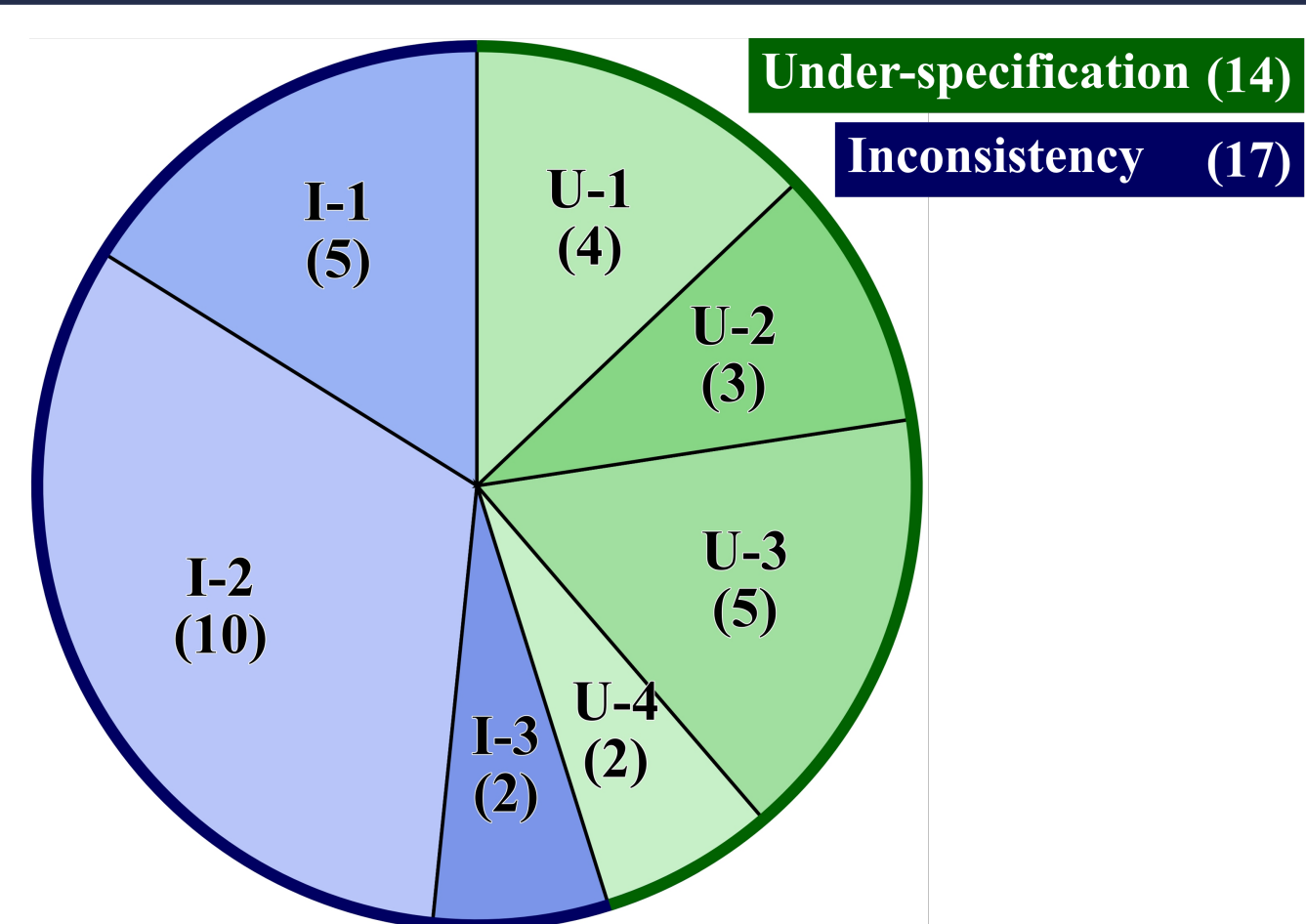
LLM-as-a-Judge

The LLM is prompted to evaluate the results of the Analyzer by

- validating the reasoning provided by the Analyzer.
- checking each reported errata against a **checklist-criteria** for plausible errata.
- identifying which category of ambiguities each reported errata belongs to.

Evaluation

- RFCScope discovered 31 previously unreported ambiguities across 14 of the 20 most recent RFCs related to Domain Name System (DNS).
- 8 of these have been confirmed by RFC authors, of which 3 are officially verified as technical errata.



Verified Technical Errata 8426 (rfc-editor.org/errata/eid8426)	I-2
RFC 9619	
Section 1. Introduction	(Spec)
...update the DNS base specification to clarify the allowable values of the QCODE parameter in the specific case of DNS messages with OPCODE = 0.	

Verified Technical Errata 8431 (rfc-editor.org/errata/eid8431)	I-2
RFC 9445	
Section 5. An Example: Applicability to Encrypted DNS Provisioning	(Spec 1)
...replies with an Access-Accept message (possibly after having sent a RADIUS Access-Challenge message...	
Section 7. Table of Attributes	(Spec 2, table)
Table with 5 columns: Access-Request, Access-Accept, Access-Reject, Challenge, Attribute	

Verified Technical Errata 8590 (rfc-editor.org/errata/eid8590)	U-4
RFC 9704	
Section 6.2. Using DNSSEC	(Spec 1)
The client ... performs full DNSSEC validation locally [RFC6698].	
RFC 6698	(Spec 2, ref)
Section 1.2. Securing the Association of a Domain Name with a Server's Certificate	
This document only relates to securely associating certificates for TLS and DTLS with host names; retrieving certificates from DNS for other protocols is handled in other documents.	
Section 1.3. Method for Securing Certificate Associations	
This document does not specify how DNSSEC validation occurs...	