ARTIFACT EVALUATED usenix ASSOCIATION AVAILABLE

ARTIFACT EVALUATED usenix ASSOCIATION FUNCTIONAL

CellularLint: A Systematic Approach to Identify Inconsistent Behavior in Cellular Network Specifications

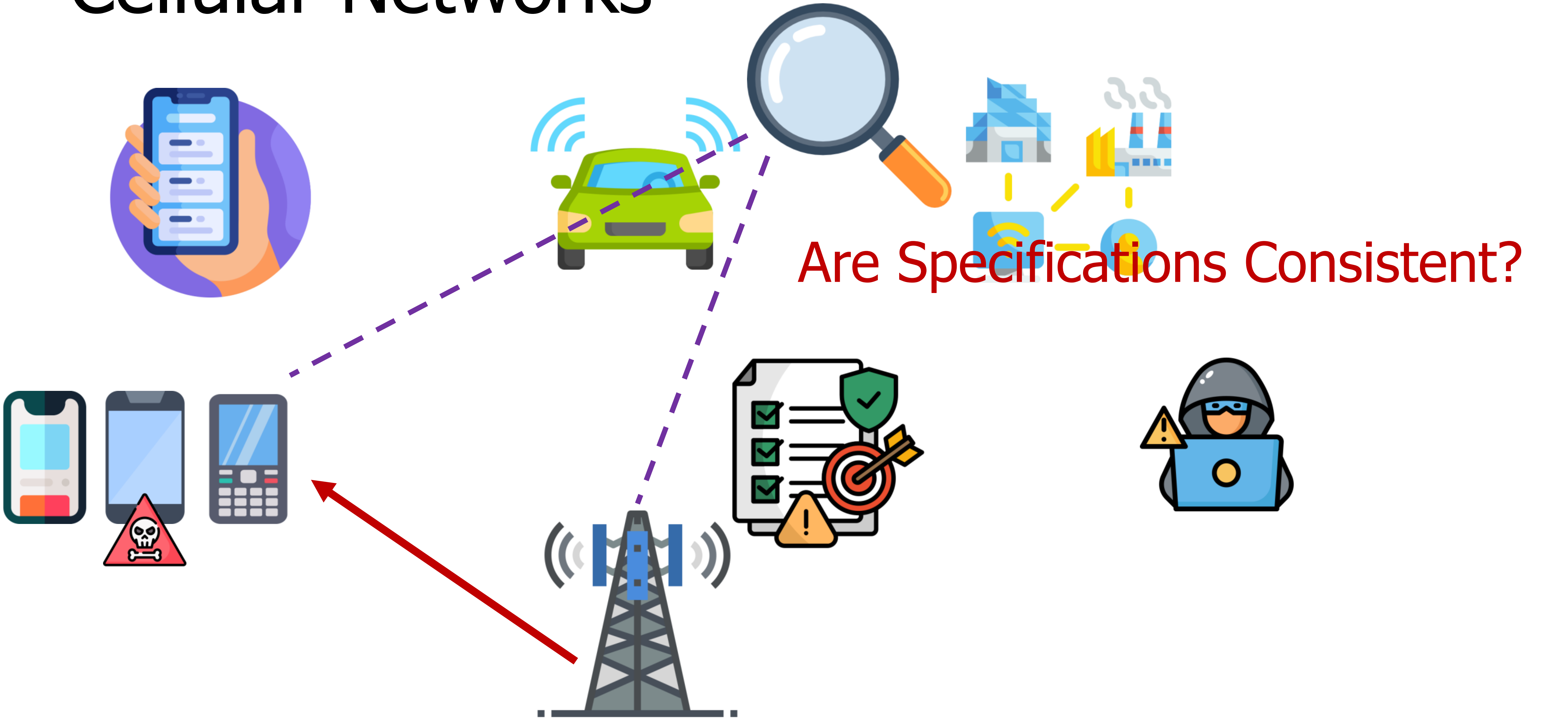
Mirza Masfiqur Rahman*, Imtiaz Karim* & Elisa Bertino

usenix THE ADVANCED COMPUTING SYSTEMS ASSOCIATION

SCAN ME

*Equal contributions

Cellular Networks



Are Specifications Consistent?

Are Specifications Consistent?

Whenever an ATTACH REJECT message with the EMM cause #14 "EPS services not allowed in this PLMN" is received by the UE ··· Additionally the attach attempt counter shall be reset when the UE is in substate EMMDEREGISTERED.ATTEMPTING-TOATTACH.

#14 (EPS services not allowed in this PLMN); The UE shall set the EPS update status to EU3 ROAMING NOT ALLOWED ··· the UE shall reset the attach attempt counter and enter the state EMMDEREGISTERED.PLMN-SEARCH.

The Problem

Is it possible to develop a framework to identify inconsistencies and associate them w/ differential design choices?

Outline

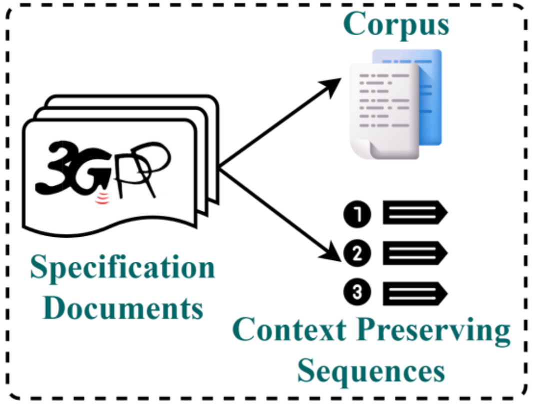
Problem

Approach

Results

Testing

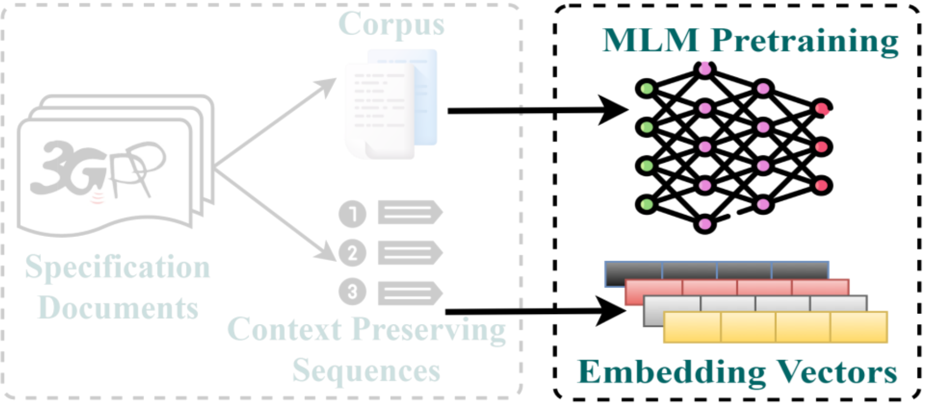
Our Approach



Challenges

LLMs are not domain specific.

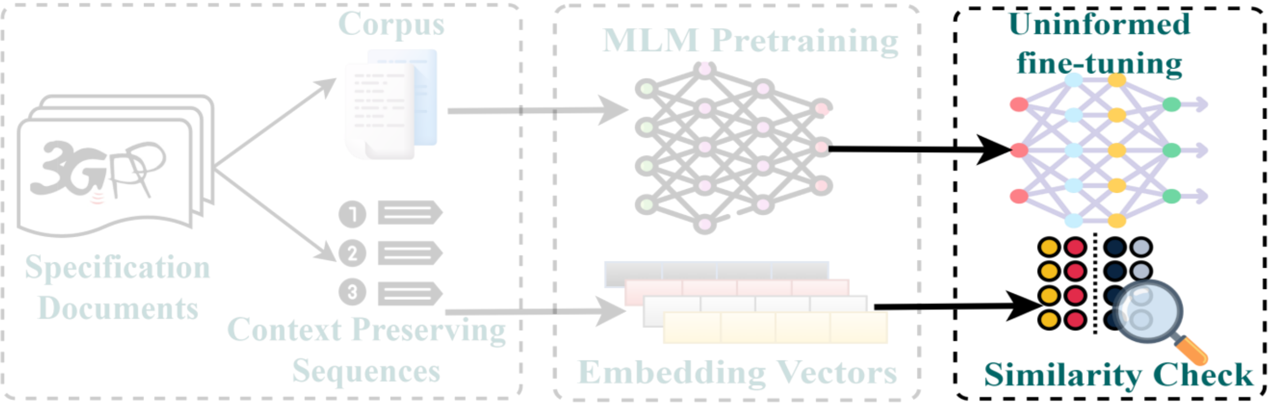
Our Approach



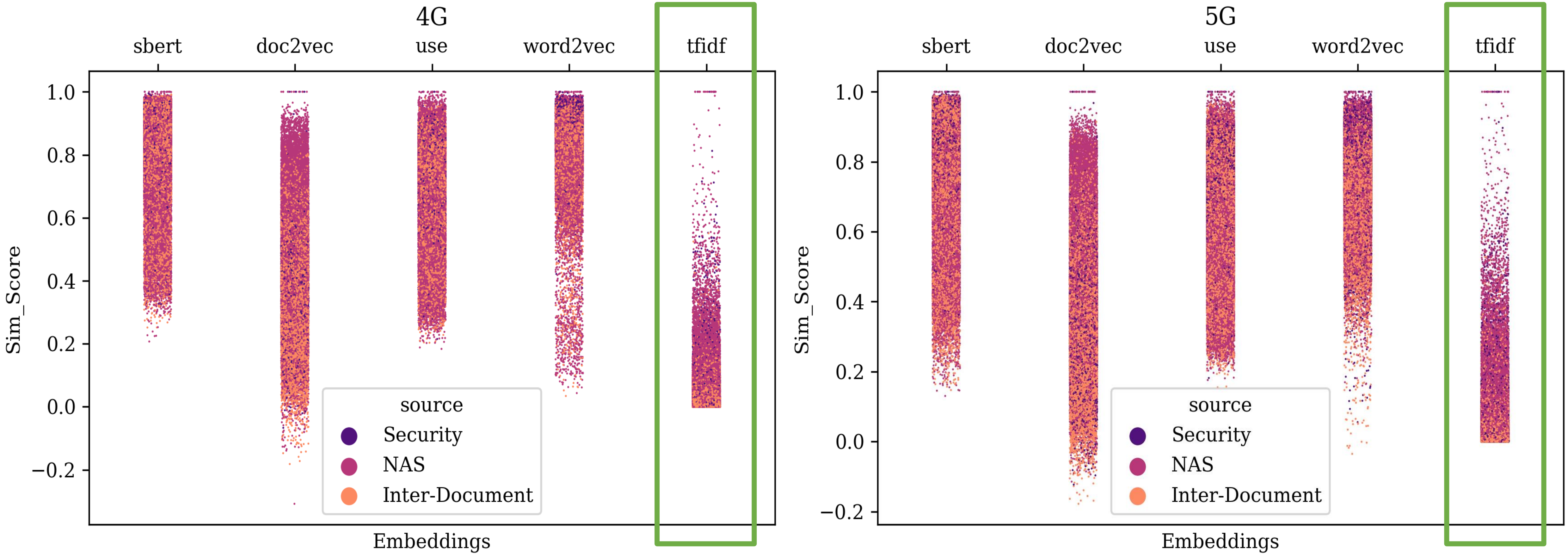
Challenges

- LLMs are not domain specific.
- How do we know where to look for inconsistent pairs?
- Formulation: How can LLMs detect inconsistencies?

Our Approach



Embedding Choice Affects the Search Space



TF-IDF Embedding

TF: measures importance of a word/term *t* in a document/text sequence *d*

$$tf(t,d) = \frac{f_{t,d}}{\sum_{t' \in d} f_{t',d}}$$

$f_{t,d}$: frequency of *t* in *d*

TF-IDF Embedding

TF: measures importance of a word/term *t* in a document/text sequence *d*

$$tf(t,d) = \frac{f_{t,d}}{\sum_{t' \in d} f_{t',d}}$$

$f_{t,d}$: frequency of *t* in *d*

IDF: measures proportion of documents in the corpus *D* that contain the term t

Corpus, $D : \{d_1, d_2, \dots\}$

$$idf(t,D) = -\log P(t|D) = \log \frac{n}{\sum \mathbb{1}_{(d \in D : t \in d)}}$$

TF-IDF Embedding

TF: measures importance of a word/term t in a document/text sequence d

$$tf(t,d) = \frac{f_{t,d}}{\sum_{t' \in d} f_{t',d}}$$

$f_{t,d}$: frequency of t in d

IDF: measures proportion of documents in the corpus D that contain the term t

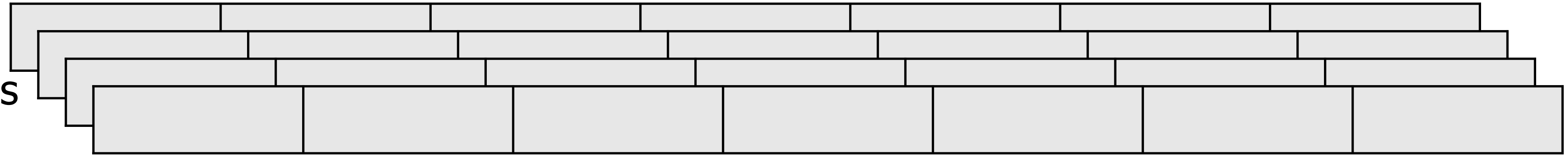
Corpus, $D : \{d_1, d_2, \ldots\}$

$$idf(t,D) = -\log P(t|D) = \log \frac{n}{\sum \mathbb{1}_{(d \in D : t \in d)}}$$

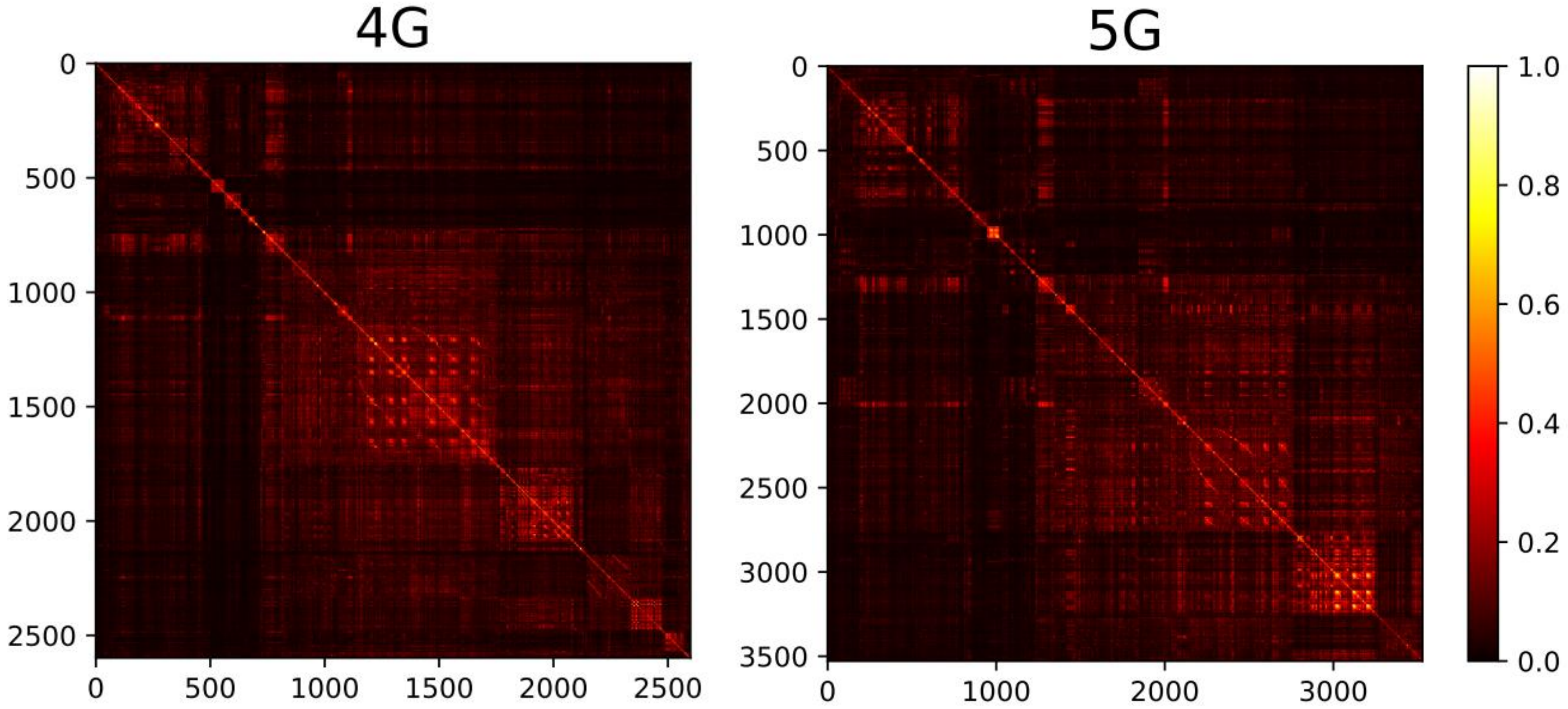
TF-IDF: importance of a term in a document relative to whole corpus

$$tf\_idf = tf(t,d).\, idf(t,D)$$

Similarity over Embedding vectors



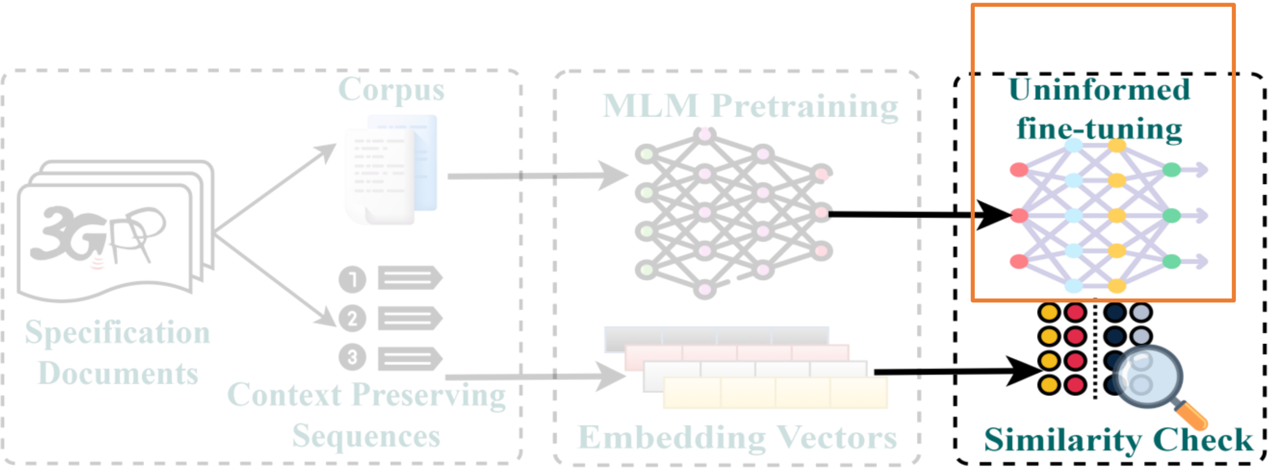
Search Space Contraction through Similarity Matrix



Brighter represents higher similarity → important sequence pair

Our Approach

Solve the NLI task first!



Challenges

- LLMs are not domain specific.
- How do we know where to look for inconsistent pairs?
- Formulation: How can LLMs detect inconsistencies?
- No ground truth for supervised training

Annotation

✓$T_1 = T_2$: T_1 is consistent with T_2

✓$T_1 \neq T_2$: T_1 is inconsistent with T_2

✓$T_1 \otimes T_2$: T_1 is not related to T_2

✓$T_1 \longrightarrow T_2$: T_1 is related to T_2. T_1 happens before T_2

✓$T_1 \longleftarrow T_2$: T_1 is related to T_2. T_2 happens before T_1

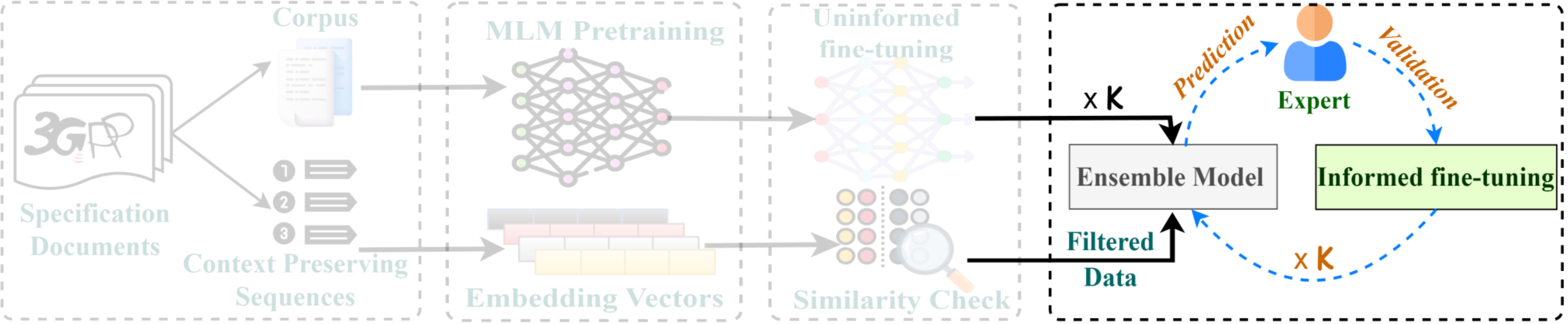
✓$T_1 \sqsubset T_2$: T_1 is related to T_2. T_1 contains more/detailed information than T_2

✓$T_1 \sqsupset T_2$: T_1 is related to T_2. T_2 contains more/detailed information than T_1

Red: Contradiction Green: Entailment Blue: Neutral

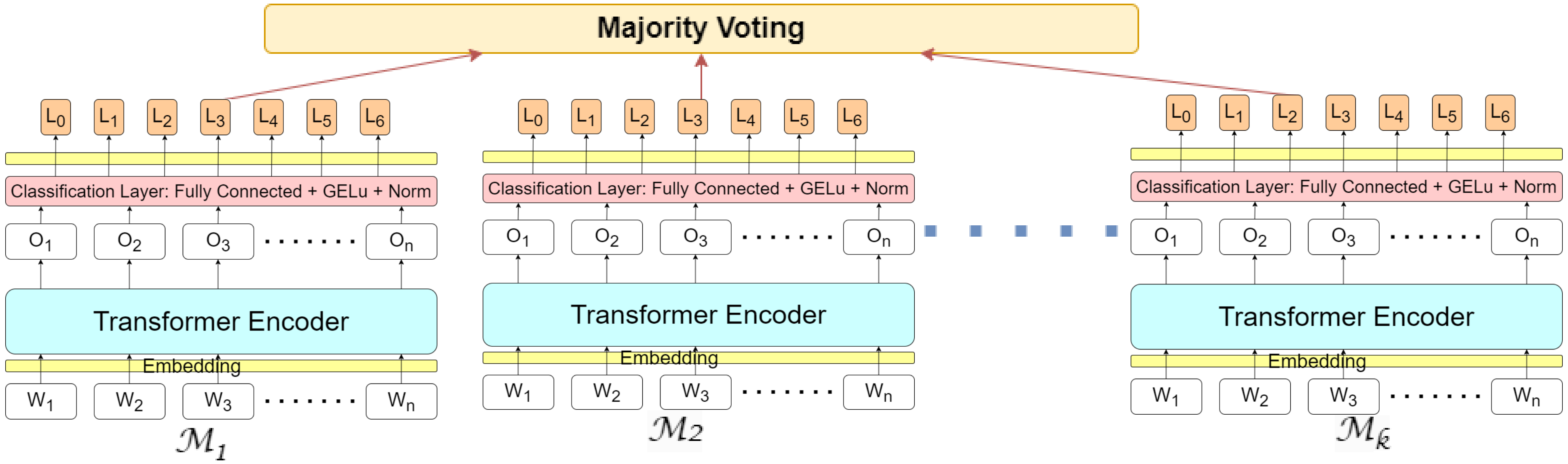
Labels for NLI task

Our Approach

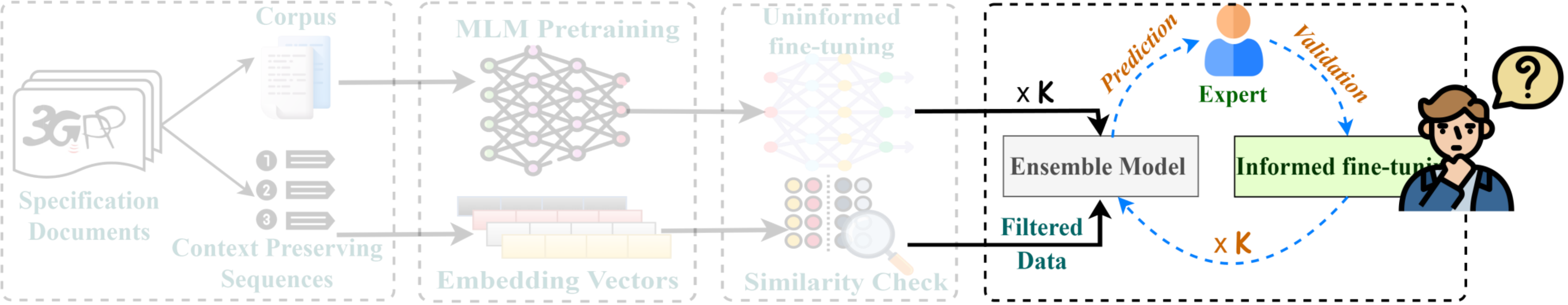


EnCell: Ensemble Transformer Approach

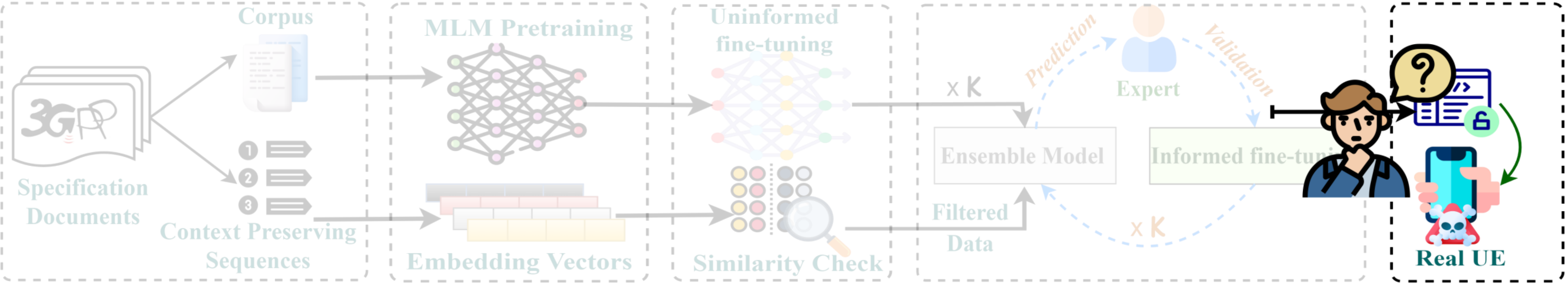
Decision based on best k models


Majority Voting
L$_0$ L$_1$ L$_2$ L$_3$ L$_4$ L$_5$ L$_6$
Classification Layer: Fully Connected + GELu + Norm
O$_1$ O$_2$ O$_3$ .... O$_n$
Transformer Encoder
Embedding
W$_1$ W$_2$ W$_3$ .... W$_n$
$\mathcal{M}_1$
$\mathcal{M}_2$
$\mathcal{M}_k$

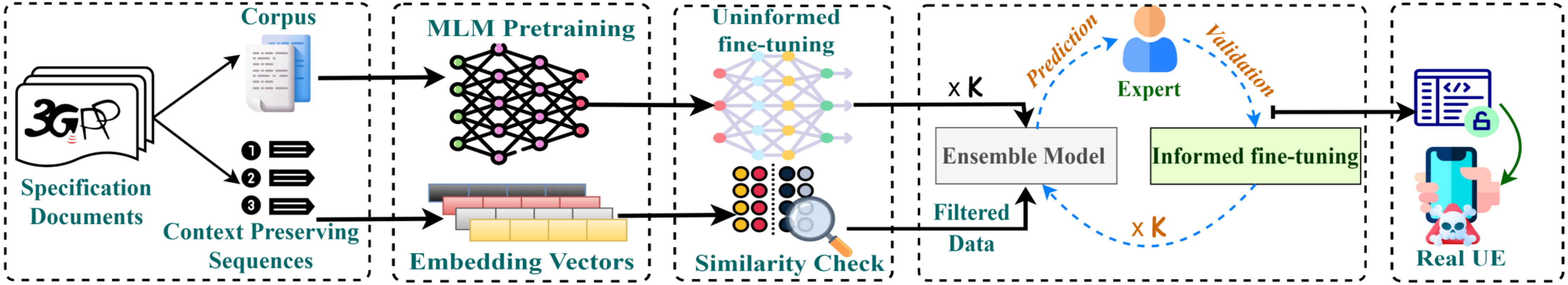
Our Approach



Our Approach



Approach: Summary



Outline

Problem

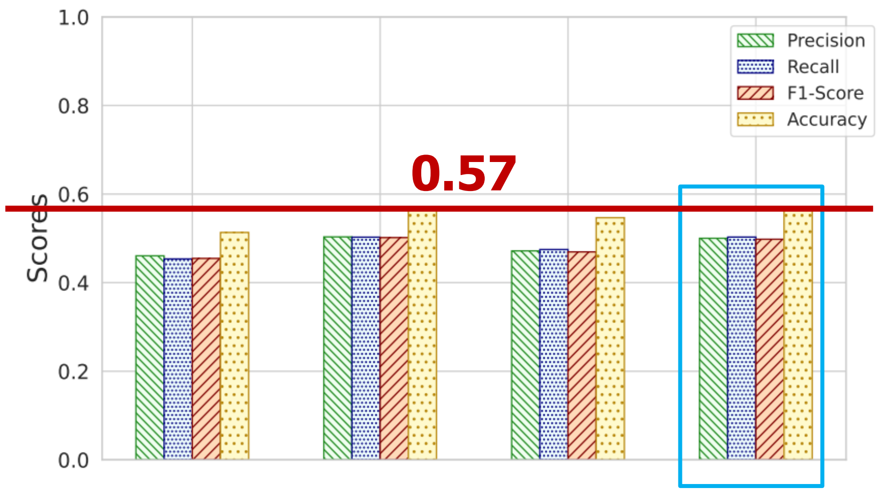
Approach

Results

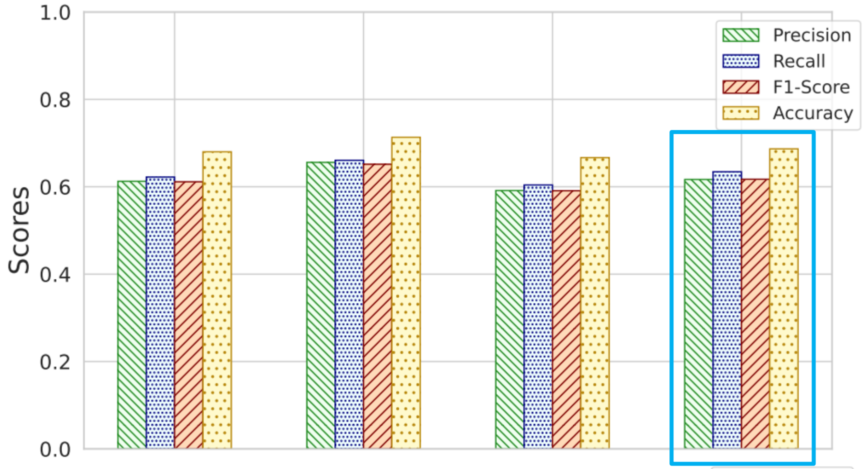
Testing

Model Performance

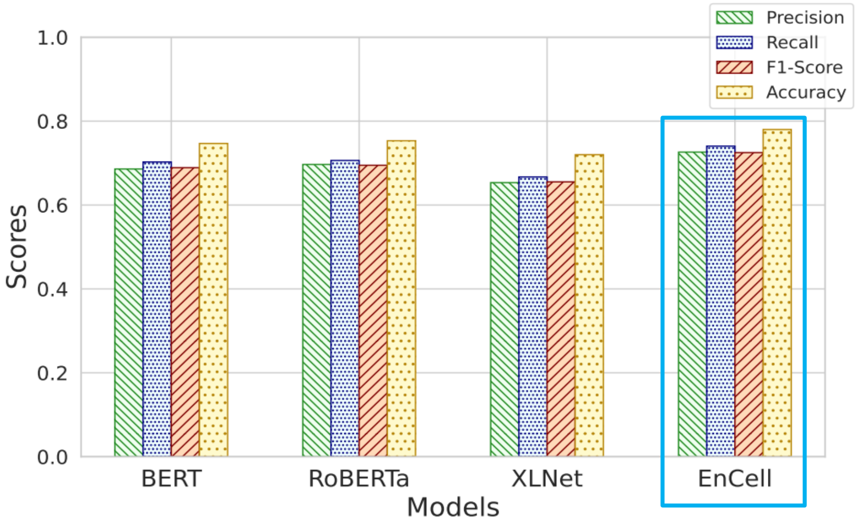
Phase 0



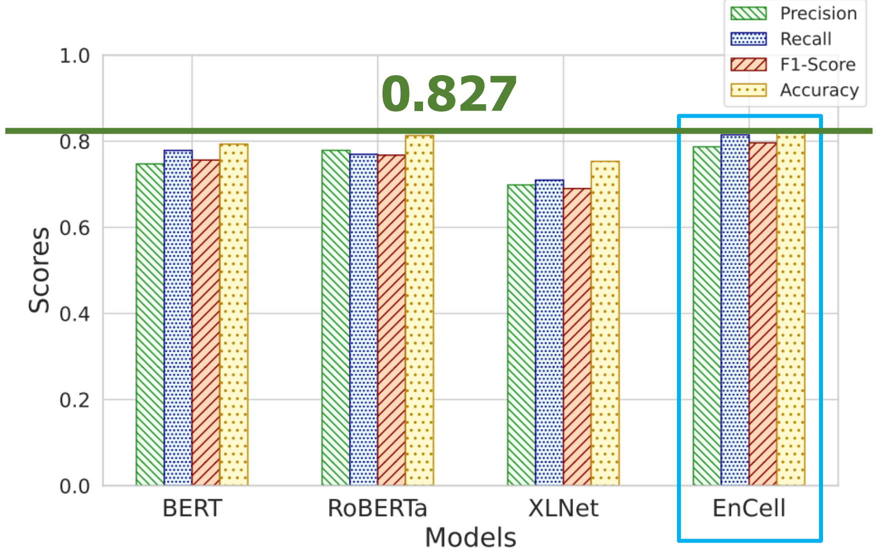
Phase 1



Phase 2



Phase 3



Inconsistency Breakdown

4G

Integrity & Ciphering	26
Security Context Handling	2
Bearer Context	1
GUTI Related	41
State Transition	
Counters	
Misc	3

5G

3	Security Key Generation & Handling
3	Integrity & Ciphering
7	Timers
2	State Transition
	g
	Handling
3	GUTI Related
5	QoS Rules
30	PDU Session Establishment
2	Counters
5	Misc

Total :157

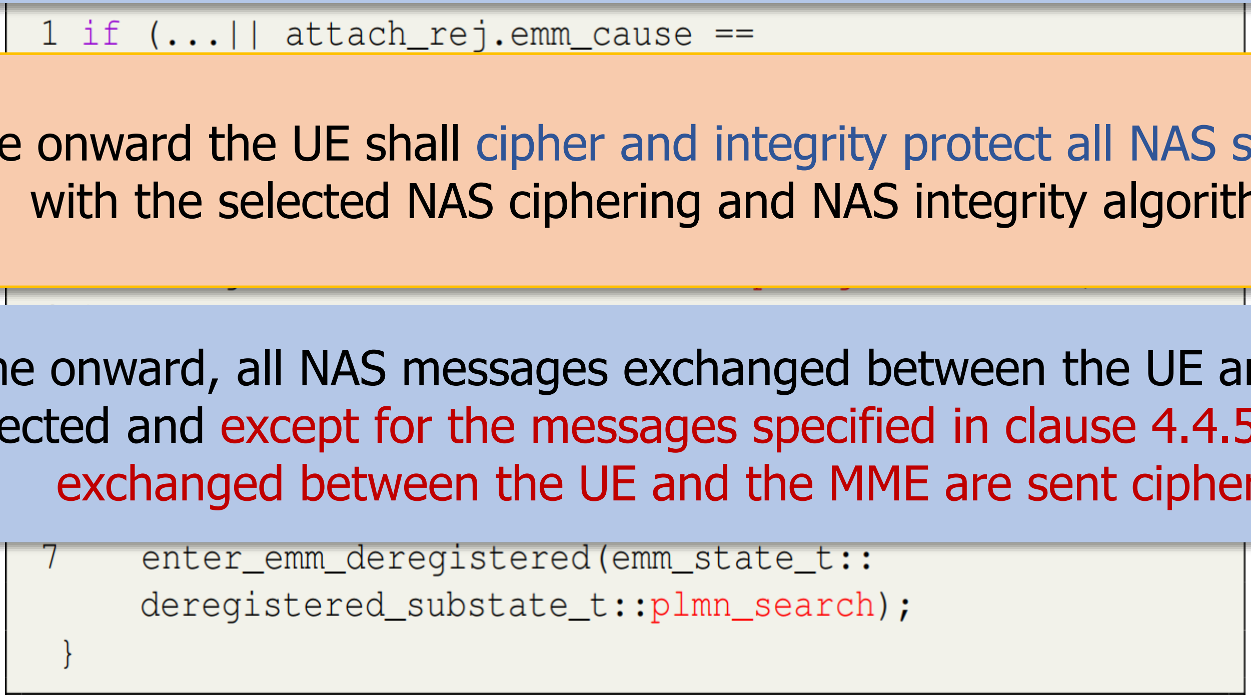
Findings

Whenever an ATTACH REJECT message with the EMM cause #14 "EPS services not allowed in this PLMN" is received by the UE ⋯ Additionally the attach attempt counter shall be reset when the UE is in substate EMMDEREGISTERED.ATTEMPTING-TOATTACH.

#14 (EPS services not allowed in this PLMN); The UE shall set the EPS update status to EU3 ROAMING NOT ALLOWED ⋯ the UE shall reset the attach attempt counter and enter the state EMMDEREGISTERED.PLMN-SEARCH.

From this time onward the UE shall cipher and integrity protect all NAS signalling messages with the selected NAS ciphering and NAS integrity algorithms.

From this time onward, all NAS messages exchanged between the UE and the MME are sent integrity protected and except for the messages specified in clause 4.4.5, all NAS messages exchanged between the UE and the MME are sent ciphered.



```
if (...|| attach_rej.emm_cause ==
    enter_emm_deregistered(emm_state_t::
    deregistered_substate_t::plmn_search);
}
```

Findings

If the sent NCC value is fresh and belongs to an unused pair of {NCC, NH}, the gNB shall save the pair of {NCC, NH} in the current UE AS security context and shall delete the current AS key Kg_{NB}.

the UE shall take the received NCC value and save it as stored NCC ··· . If the stored NCC value is different from the NCC value associated with the current Kg_{NB}, the UE shall delete the current AS
key Kg_{NB}.

#13 (Roaming not allowed in this tracking area) The UE shall set the 5GS update status to 5U3 ROAMING NOT ALLOWED (and shall store it according to subclause5.1.3.2.2) and shall delete 5GGUTI, last visited registered TAI, TAI list and ngKSI.

#13 (Roaming not allowed in this tracking area) The UE shall set the 5GS update status to 5U3 ROAMING NOT ALLOWED (and shall store it according to subclause5.1.3.2.2) and shall delete the list of equivalent PLMNs (if available).

Outline

Problem

Approach

Results

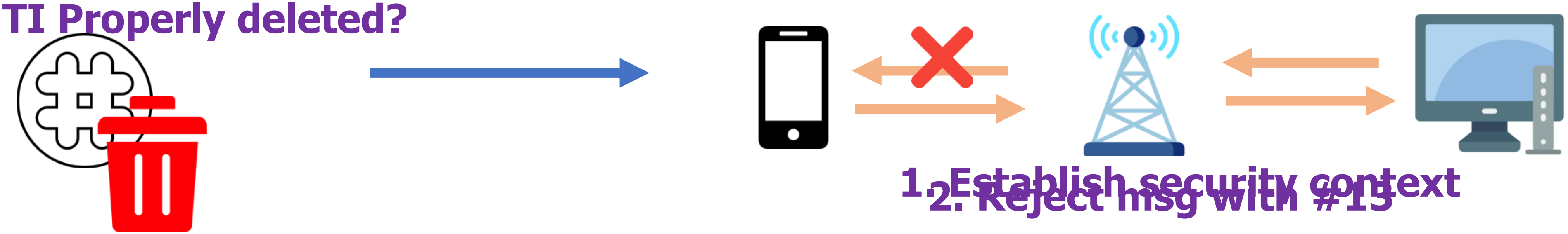
Testing

Inconsistency to Exploit

#13 (Roaming not allowed in this tracking area) The UE shall set the 5GS update status to 5U3 ROAMING NOT ALLOWED (and shall store it according to subclause5.1.3.2.2) and shall **delete 5GGUTI, last visited registered TAI, TAI list and ngKSI.**

#13 (Roaming not allowed in this tracking area) The UE shall set the 5GS update status to 5U3 ROAMING NOT ALLOWED (and shall store it according to subclause5.1.3.2.2) and shall delete the list of equivalent PLMNs (if available).

GUTI Properly deleted?



1. Establish security context

2. Reject msg with #13

	Plain auth_req accepted	Plain iden_req accepted	Plain det_req accepted	Integrity failed msg accepted	Causes connection drop	Att_rej clears context	Serv_rej clears context	Tau_rej clears context	Tau & detach collision
Google Pixel 7a	✓	✗	✗	✗	✓	✓	✗	✗	Tau Progressed
Samsung S20 FE	✗	✗	✗	✗	✓	✓	✗	✗	Tau Progressed
HTC One E9+	✓	✓	✗	✗	✓	✓	✗	✗	Tau Progressed
Huawei Y5	✓	✓	✗	✗	✓	✓	✗	✗	Tau Progressed
Xiaomi 11 Lite	✗	✗	✗	✗	✓	✓	✗	✗	Tau Progressed
Moto Edge 30Pro	✗	✗	✗	✗	✓	✓	✗	✗	Tau Progressed
Oneplus 9 Pro	✗	✗	✗	✗	✓	✓	✗	✗	Tau Progressed
Huawei Honor 8X	✗	✗	✗	✗	✗	✓	✗	✗	Tau Progressed
Apple Iphone 12 Pro	✗	✗	✗	✗	✓	✓	✓	!	!
Google Pixel 3a	✗	✗	✗	✗	✓	✓	✗	✗	Tau Progressed
Samsung Galaxy A04	✗	✗	✗	✗	✓	✓	✗	✗	Tau Progressed
LG Velvet 5G	✓	✓	✗	✗	✓	✓	✗	✗	Tau Progressed
Oneplus 8T	✗	✗	✗	✗	✓	✓	✗	✗	Tau Progressed
Blu C5L Max	✗	✗	✗	✗	✓	✓	✗	✗	Tau Progressed
TCL 30	✗	✗	✗	✗	✓	✓	✗	✗	Tau Progressed
Samsung Galaxy S8+	✗	✗	✗	✗	✓	✓	✗	✗	Tau Progressed
Moto G Play	✗	✗	✗	✗	✓	✓	✗	✗	Tau Progressed

Thank you. In conclusion…

ARTIFACT EVALUATED usenix ASSOCIATION AVAILABLE

ARTIFACT EVALUATED usenix ASSOCIATION FUNCTIONAL

- ➢ We propose a novel context-aware inconsistency detection framework for protocol specifications.

- ➢ We found a total of 157 inconsistent pairs from 6070 shortlisted (~19.2M total possible) sequences.

- ➢ Inconsistencies lead to differing device implementations that we show under four security critical categories.

usenix THE ADVANCED COMPUTING SYSTEMS ASSOCIATION

PURDUE™

SCAN ME