ICDCS 2020

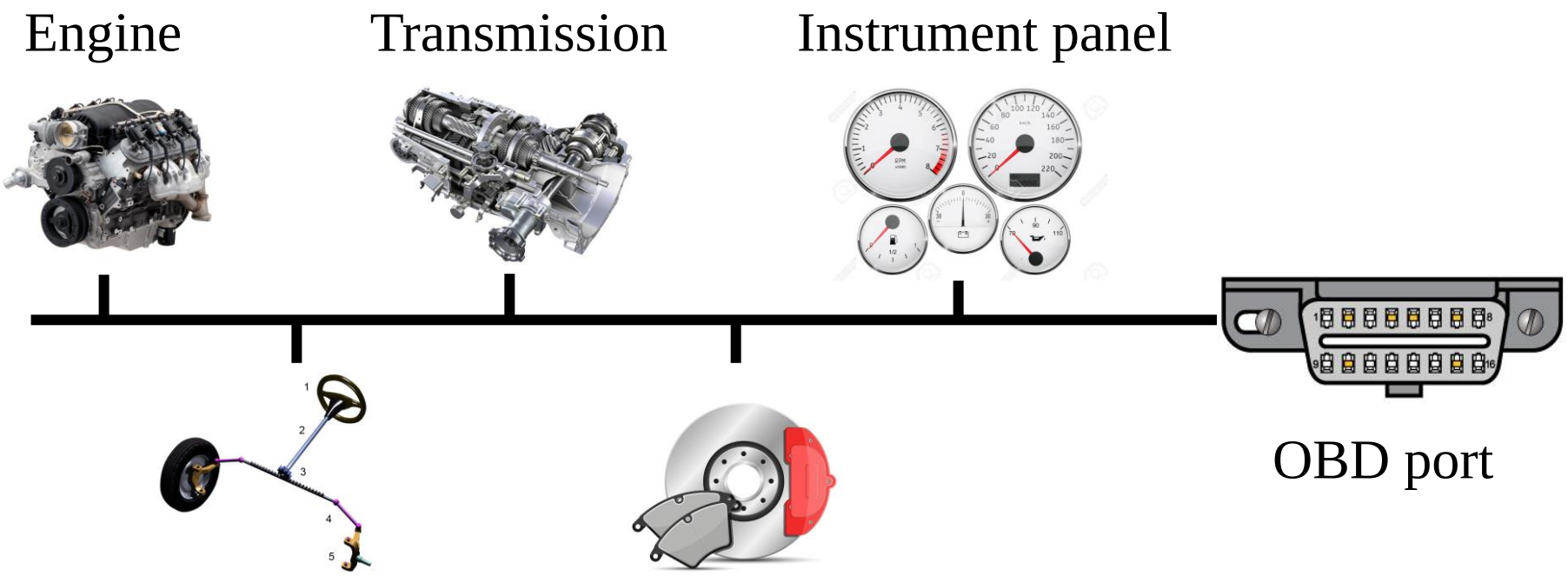
Abnormal Message Detection for CAN Bus Based on Message Transmission Behaviors

Liuwang Kang and Haiying Shen
Department of Computer Science, University of Virginia

Background

CAN bus has several advantages like high communication speed and good fault tolerance

Vehicle subsystems communicate with each other through CAN bus to ensure normal work



Background

- Vehicles are vulnerable to CAN bus attack and their driving safety will be affected greatly

Aug 2, 2016, 10:23am EDT

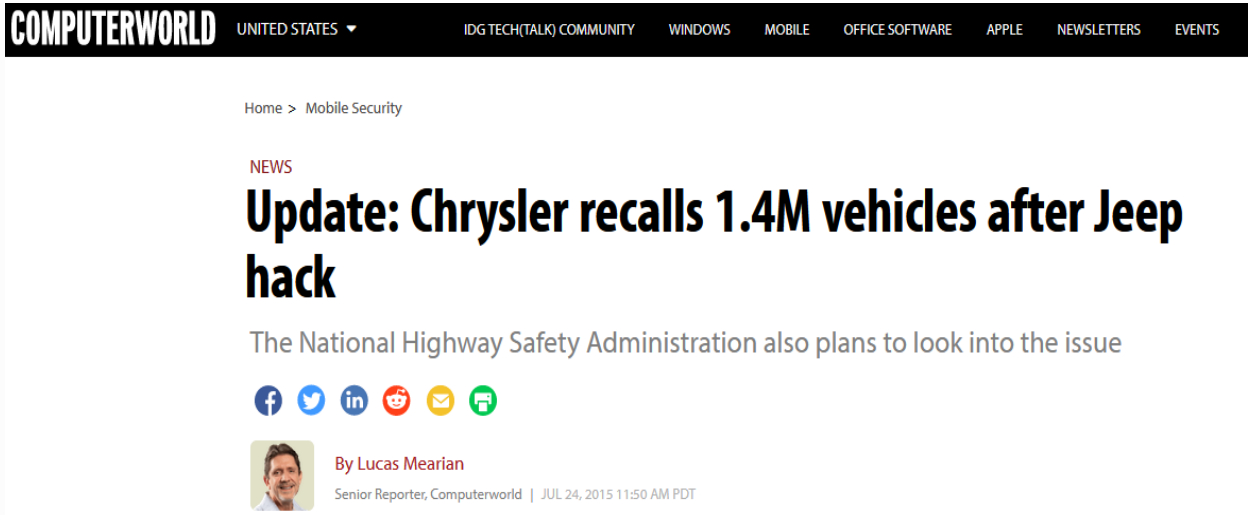
How Jeep Hackers Took Over Steering And Forced Emergency Stop At High Speed

Thomas Brewster Forbes Staff

Cybersecurity

Associate editor at Forbes, covering cybercrime, privacy, security and surveillance.

This article is more than 4 years old.



COMPUTERWORLD UNITED STATES IDG TECH(TALK) COMMUNITY WINDOWS MOBILE OFFICE SOFTWARE APPLE NEWSLETTERS EVENTS

Home > Mobile Security

NEWS

Update: Chrysler recalls 1.4M vehicles after Jeep hack

The National Highway Safety Administration also plans to look into the issue

By Lucas Mearian

Senior Reporter, Computerworld | JUL 24, 2015 11:50 AM PDT

Accurately detecting abnormal messages becomes necessary

Related Work

- Some methods [PIV'11, IMCET'18, SSD'19] try to offer cryptographic message authentication to ensure CAN bus security

➢Cryptographic message authentication usually causes high latency and reduces message communication speed

- Other methods [PST'18, CISR'17, PLOS'16] try to detect abnormal messages by analyzing time interval or frequency based on ML and statistical based technologies

➢Vehicle driving conditions (acceleration, key start, key on) affect CAN bus message's time interval and frequency

Challenges

Propose a message transmission behavior-based detection system (MetraDS) to detect abnormal messages considering varying vehicle driving conditions

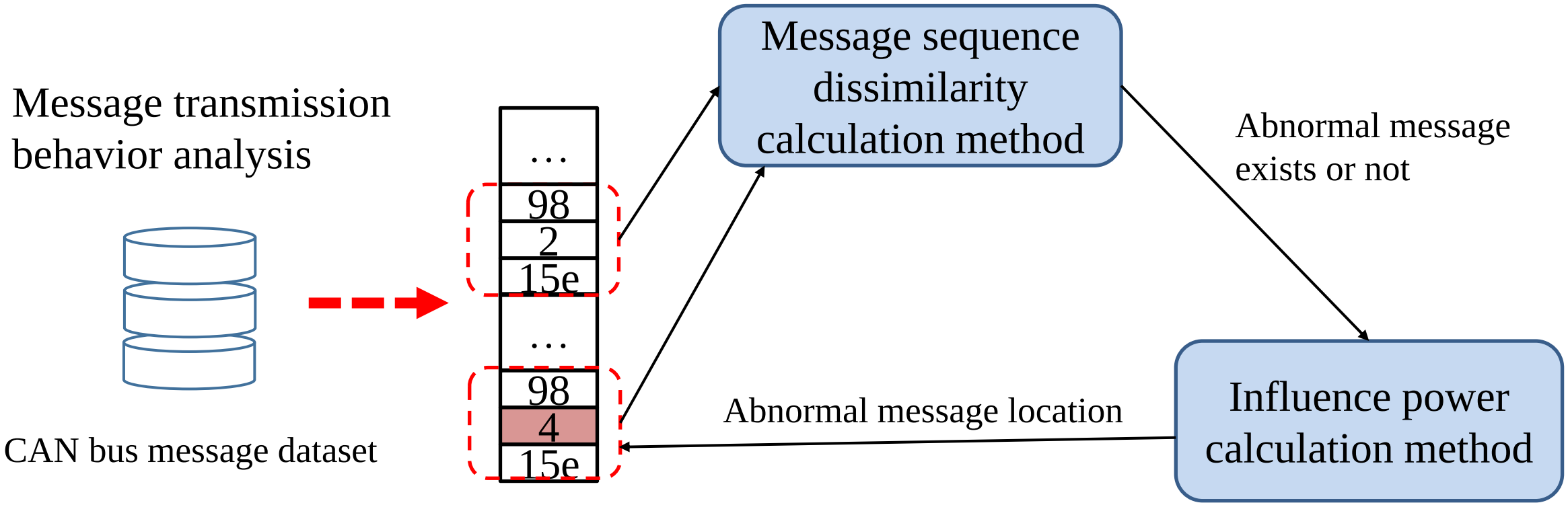
Challenge 1: How to choose message transmission behaviors for detecting messages under varying vehicle driving conditions?

- Message time interval or frequency changes greatly under varying vehicle driving conditions

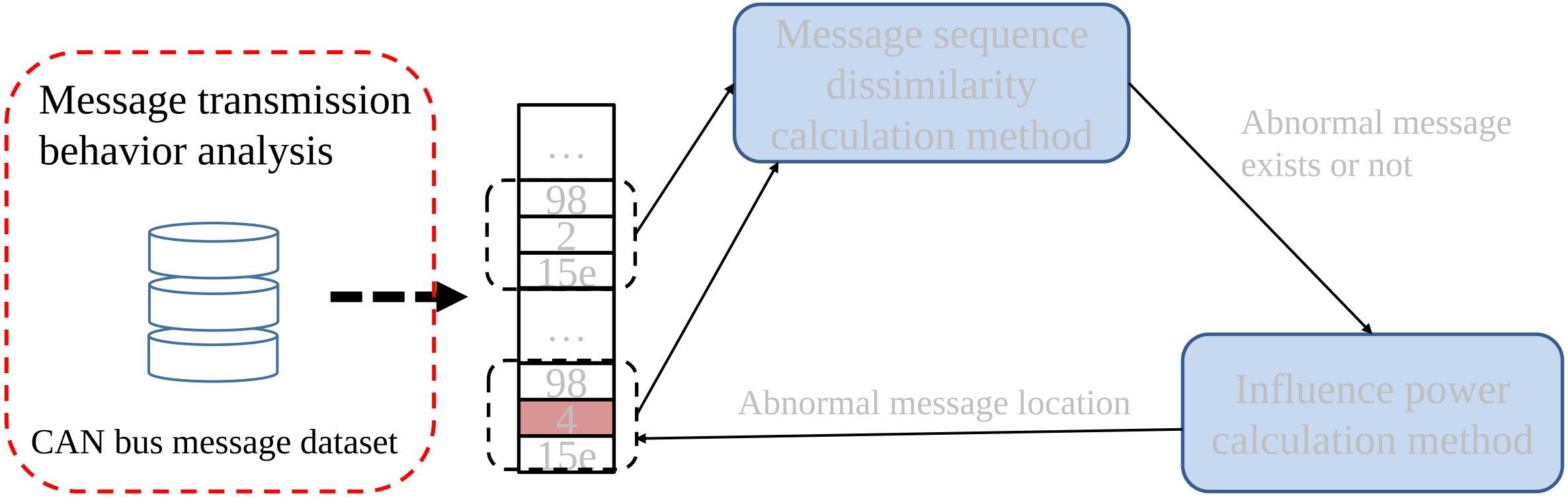
Challenge 2: How to detect abnormal messages with message transmission behaviors?

- Abnormal messages affect time intervals or frequencies of subsequent messages

Abnormal Message Detection System (MetraDS)



Abnormal Message Detection System (MetraDS)



CAN Bus Message Transmission Behavior Analysis

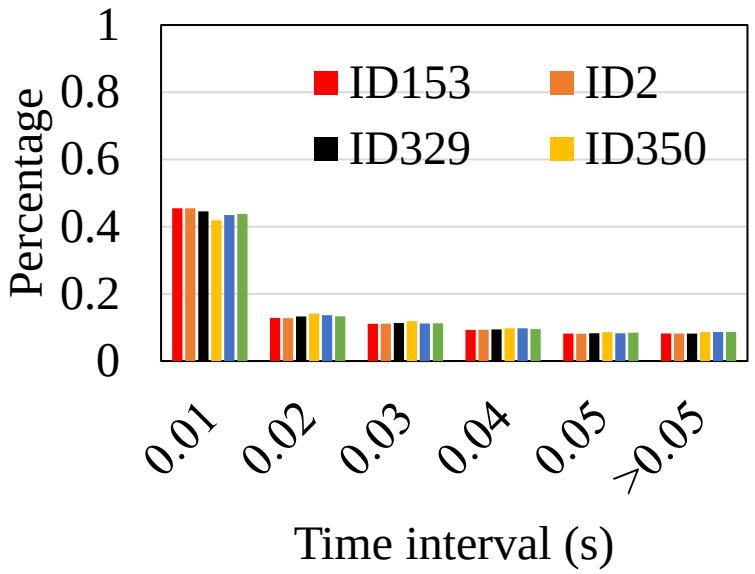
Conduct statistical analysis on a CAN Bus message dataset (2,369,868 normal messages and 2,244,041 abnormal messages) under varying vehicle driving conditions

- Message time interval analysis
- Message frequency analysis
- Message sequence dissimilarity analysis
- Influence of abnormal messages on subsequent messages

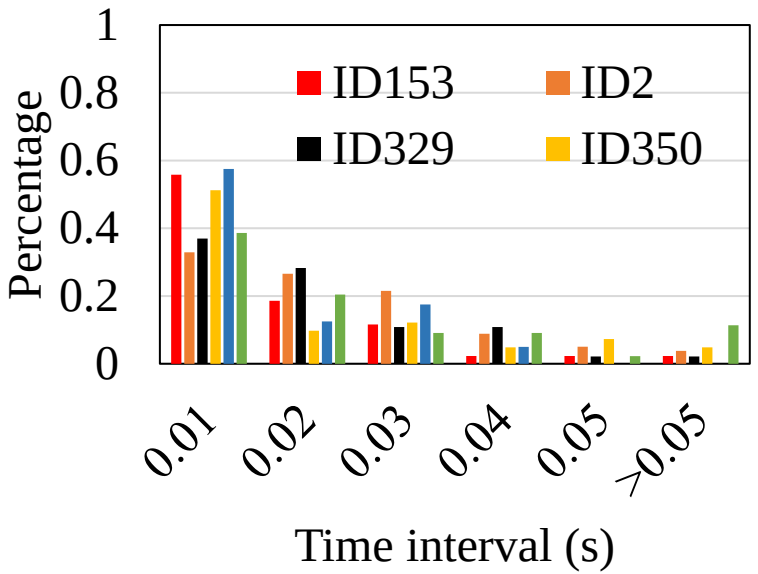
CAN Bus Message Transmission Behavior Analysis

Message time interval analysis results

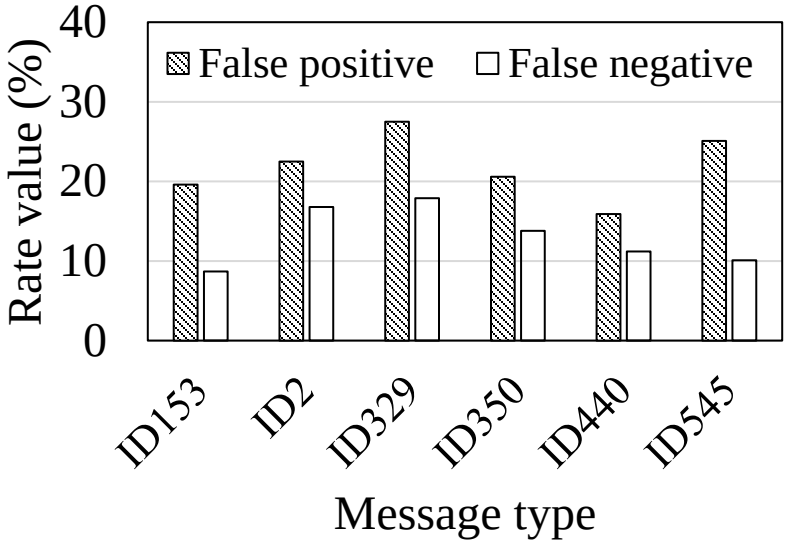
- Each normal message has different time intervals under varying vehicle driving conditions
- Time interval distributions of a normal message change when it becomes abnormal



Time intervals of normal messages



Time intervals of abnormal messages

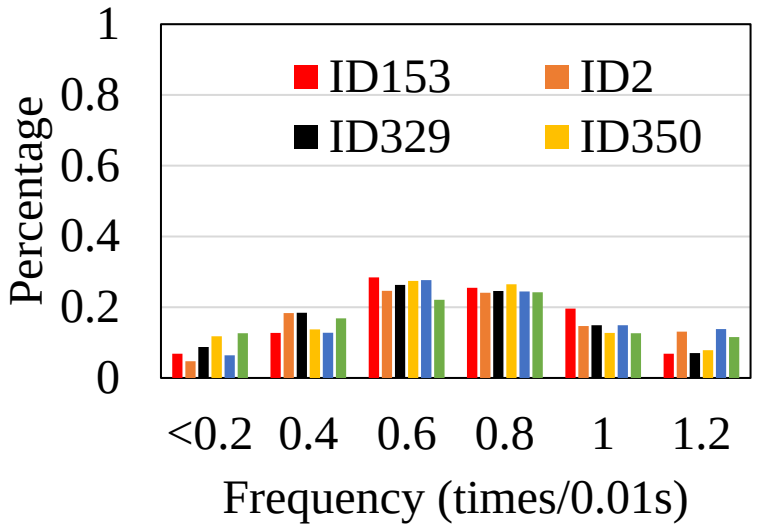


Time interval-based detection result

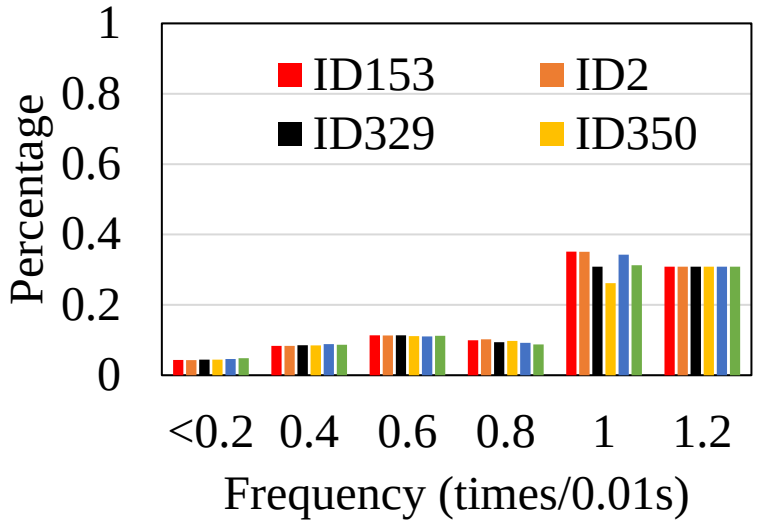
CAN Bus Message Transmission Behavior Analysis

Message frequency analysis results

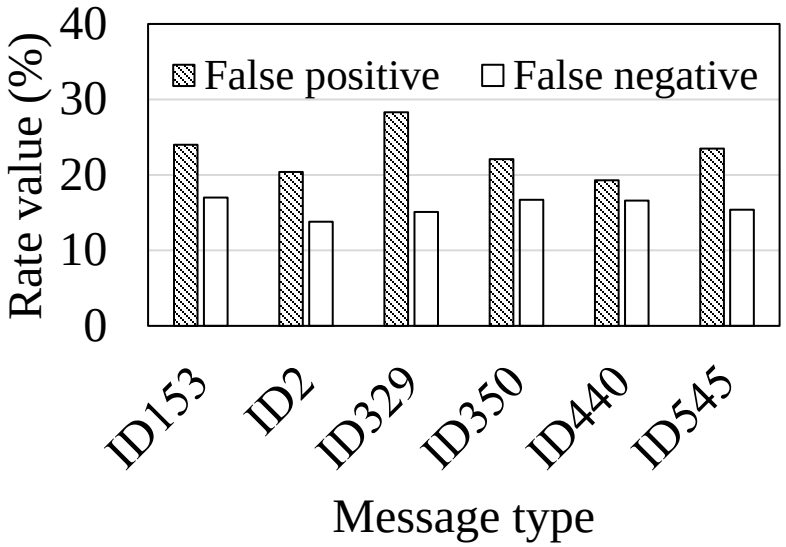
- Each normal message has different frequencies under varying vehicle driving conditions
- Frequency distributions of a normal message change when it becomes abnormal



Frequencies of normal messages



Frequencies of abnormal messages



Frequency-based detection result

CAN Bus Message Transmission Behavior Analysis

Message sequence dissimilarity analysis results

➢Message sequence

- A series of messages from itself to its preceding message
- Example: ID3, ID4, ID1, ID2, ID3, ID4, ID1, ID2, ID3, ID2, ID4,…

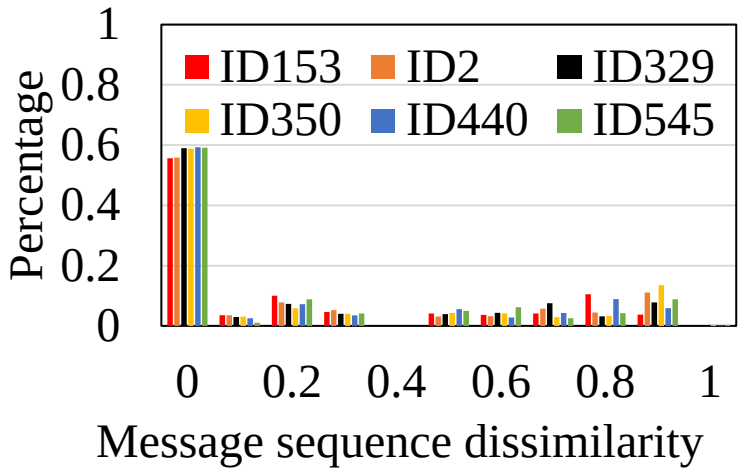
➢Message sequence dissimilarity

- Calculated as Hamming distance between two message sequences
- Example: 2/5=0.4
- (ID1, ID3, ID2, ID1, ID4)
- (ID1, ID2, ID1, ID1, ID4)

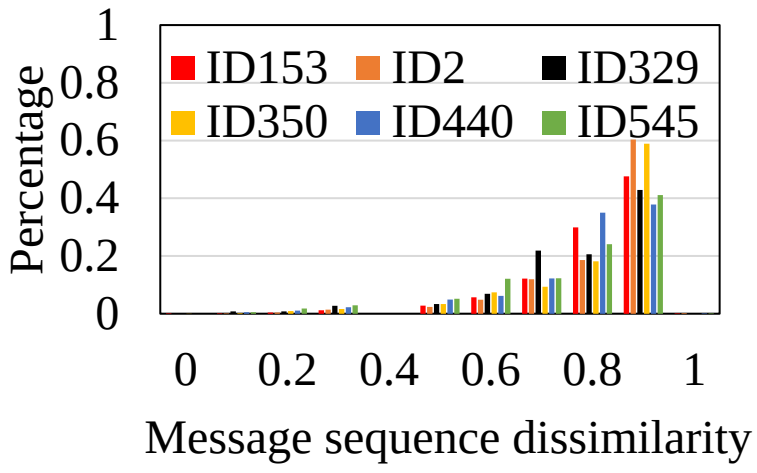
CAN Bus Message Transmission Behavior Analysis

Message sequence dissimilarity analysis results

- Message sequence dissimilarity without abnormal messages keeps around 0 under varying vehicle driving conditions
- Message sequence dissimilarity will increase greatly if message sequence has abnormal messages



Normal message situations



Abnormal message situations

CAN Bus Message Transmission Behavior Analysis

Influence of abnormal messages on subsequent messages

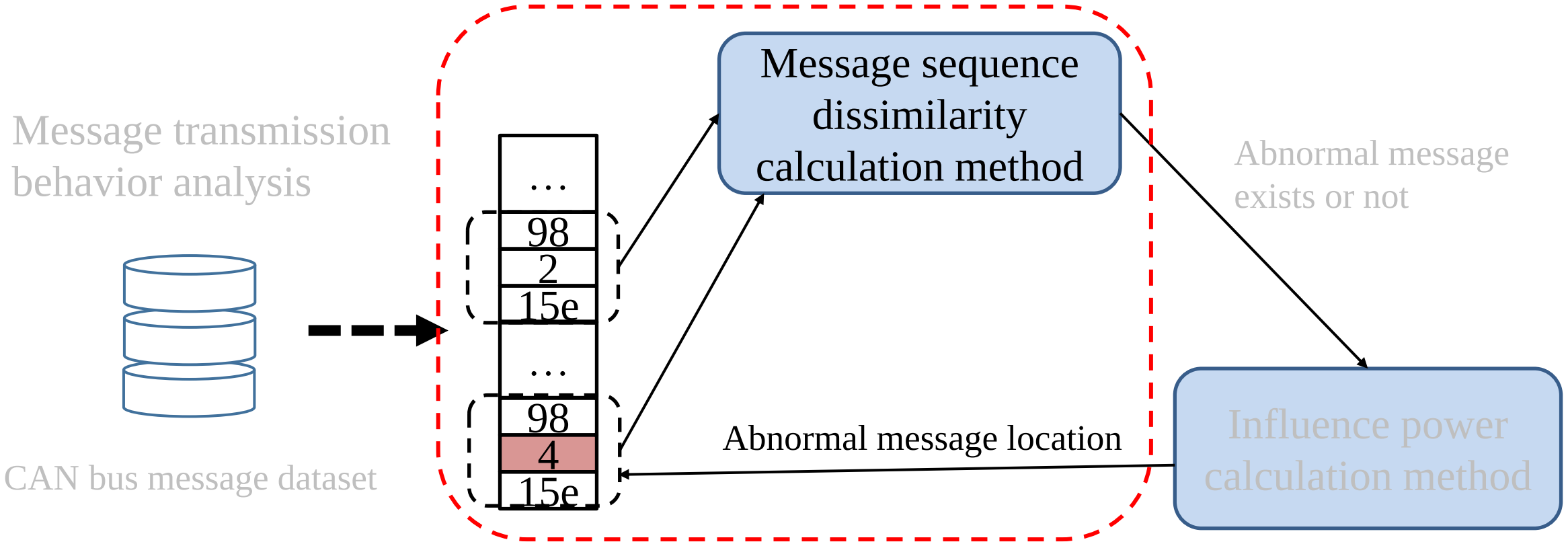
- An abnormal message increases time intervals of its subsequent normal messages in the same message sequence

Message distance	Time interval		Frequency	
	Original value	Increase rate	Original value	Increase rate
1	0.0374	25.67%	0.6470	-22.19%
2	0.0367	22.88%	0.5857	-23.40%
3	0.0379	30.08%	0.5864	-19.56%
4	0.0246	68.29%	0.6735	-22.86%
5	0.0254	16.93%	0.6659	-14.20%
6	0.0276	47.10%	0.6346	-18.81%
7	0.0267	140.8%	0.6094	-7.38%

Challenge 1

How to choose message transmission behaviors for detecting messages under varying vehicle driving conditions?

Abnormal Message Detection System (MetraDS)



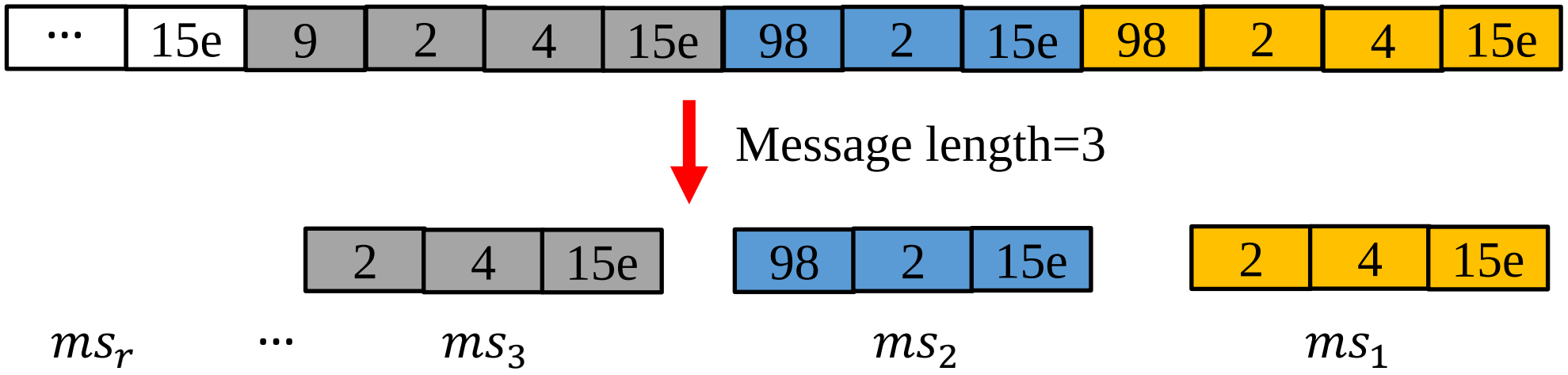
Message Sequence Dissimilarity Calculation Model

Observations from analysis results

A message sequence containing abnormal messages has high dissimilarity with its previous message sequences without abnormal messages

Message sequence dissimilarity calculation

- Step 1: Determine message sequence ms_1 and previous message sequences (ms_2, ms_3, …, ms_r) for a message



Message Sequence Dissimilarity Calculation Model

Message sequence dissimilarity calculation

- Step 2: Calculate Hamming distances between ms_1 and $(ms_2, ms_3, \ldots, ms_r)$

$$\mathrm{H}(ms_1, ms_i) = \frac{N_{min}(ms_1, ms_i)}{N_{total}(ms_1, ms_i)}$$

$N_{min}(ms_1, ms_i)$ – the minimum number of changed messages to ensure $ms_1 = ms_i$

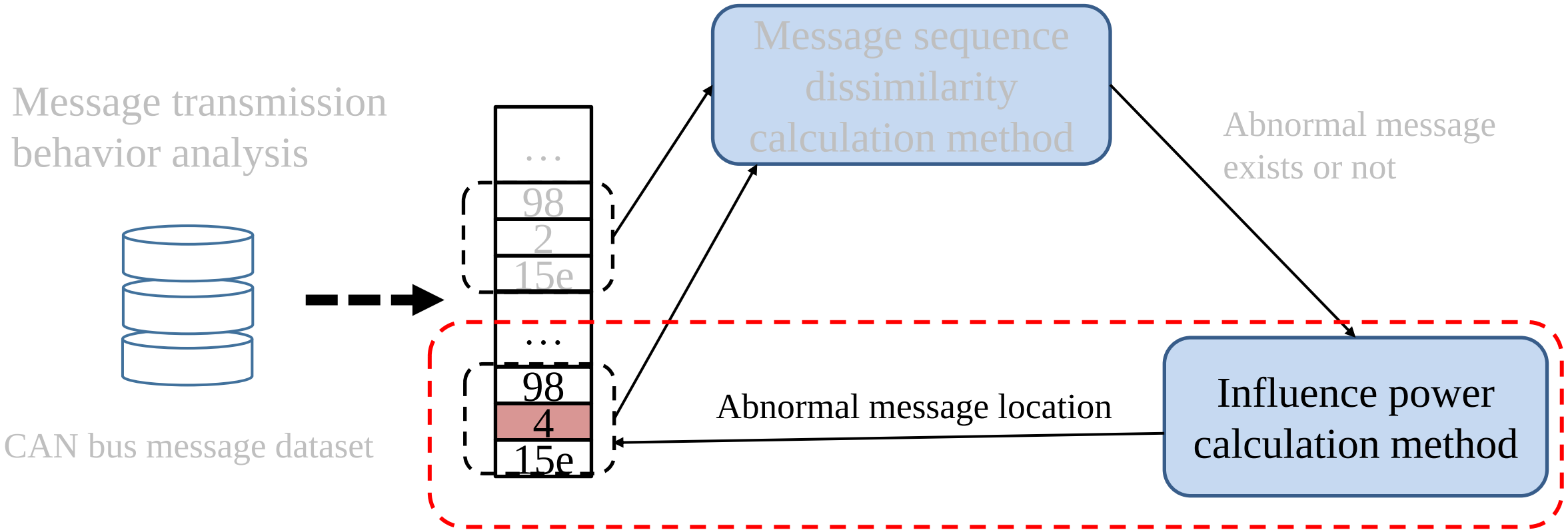
$N_{total}(ms_1, ms_i)$ – the total number of messages in ms_1

- Step 3: Compare Hamming distances with a threshold T_d to determine whether ms_1 has abnormal messages

Challenge 2

How to detect abnormal messages with message transmission behaviors

Abnormal Message Detection System (MetraDS)



Influence Power Calculation Model

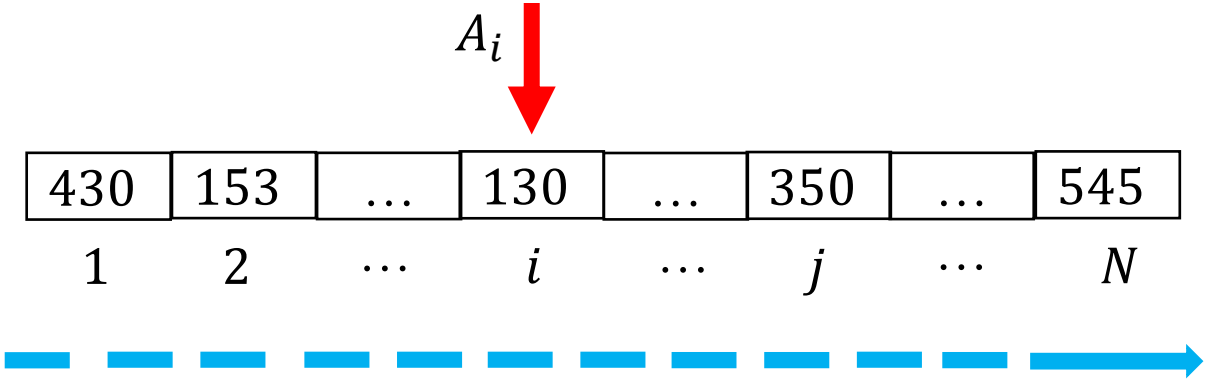
Observations from analysis results

An abnormal message will cause time interval increase and frequency decrease of its subsequent message

Influence power calculation

- Step 1: Calculate frequency increase status A_i of message m_i in message sequence ms_1

$$A_i = \begin{cases} 1 & if\ \Delta f_i > T_{f\,i} \\ 0 & otherwise \end{cases}$$

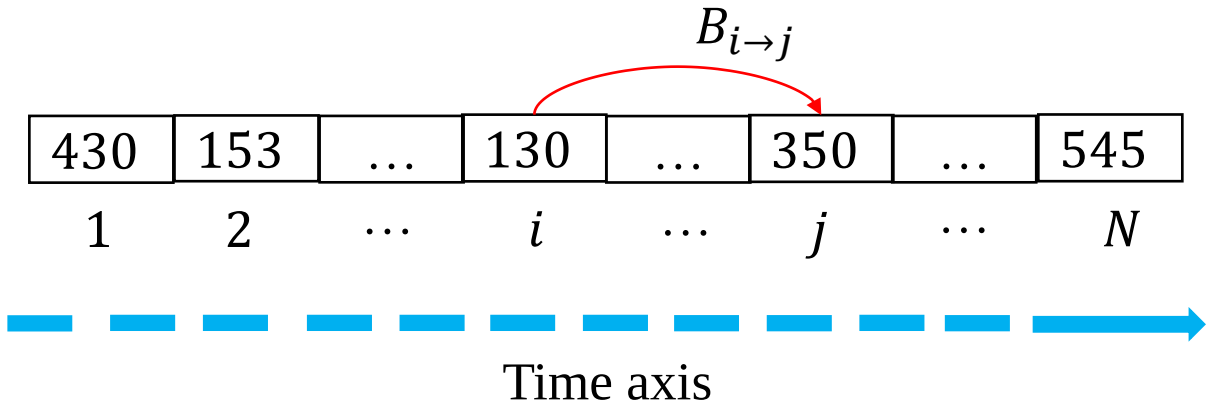


Influence Power Calculation Model

Influence power calculation

- Step 2: Calculate influence $B_{i\to j}$ of message m_i on frequency of subsequent message m_j

$$B_{i\to j} = \begin{cases} 1 & if\ \Delta f_j < -T_{f_j} \\ 0 & otherwise \end{cases}$$



- Step 3: Calculate influence power I_i of message m_i on itself and on subsequent messages in message sequence ms_1

$$I_i = \frac{1}{N-i}\sum_{j=i+1}^{N} A_i B_{i\to j}$$

Performance Evaluation

Experiment settings

- Implement MetraDS by running MATLAB on one laptop (Intel i5 CPU and 16 gigabyte memory)
- CAN bus dataset is collected from three different vehicle types and includes 2,379,392 normal messages and 2,246,341 abnormal messages

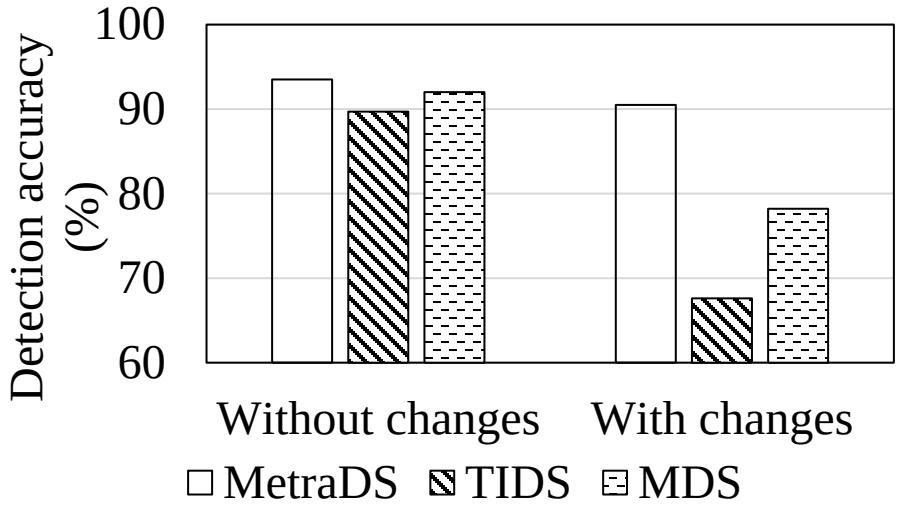
Comparison methods

- Time-interval based detection method (TIDS) [PCISR'17] models normal time interval range of each message to detect a message with time interval outside its normal range as abnormal
- ML based detection method (MDS) [PLOS'16] detects an abnormal message based a neural network with message contents as inputs and message status as output

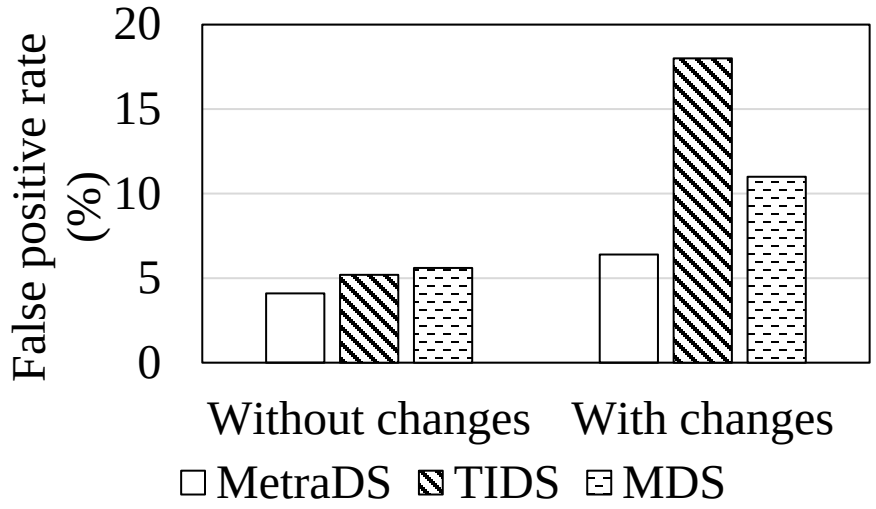
Performance Evaluation

Abnormal message detection accuracy of MetraDS

- Abnormal message detection accuracy of MetraDS keeps almost constant under varying driving conditions
- MetraDS has lower false positive rates under varying driving conditions



Abnormal message detection accuracies

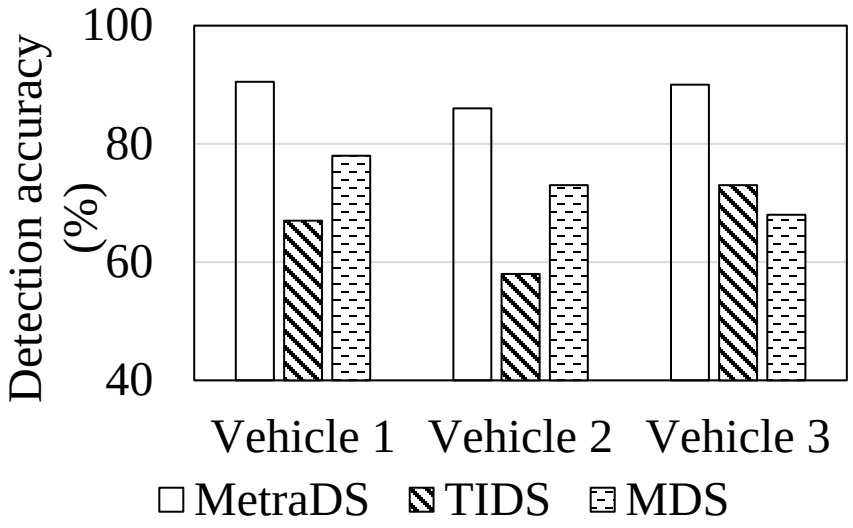


False negative rate comparisons

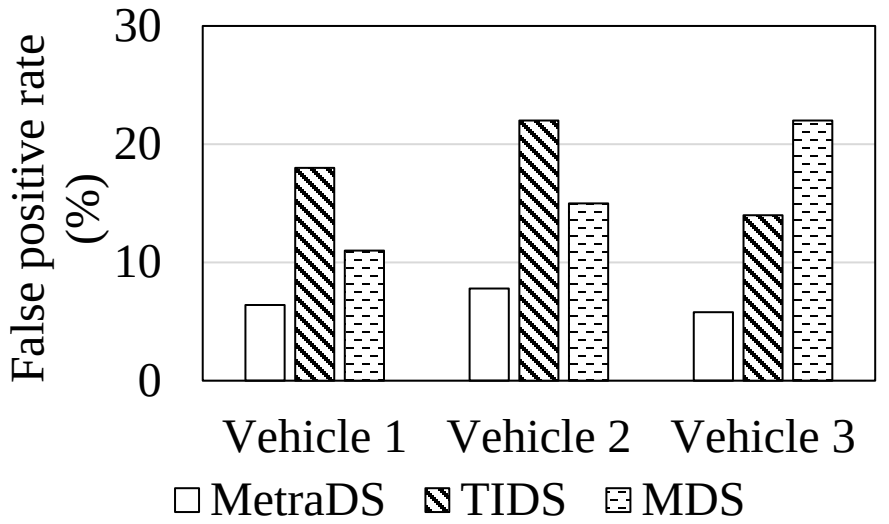
Performance Evaluation

Detection accuracy of MetraDS on different vehicle types

- MetraDS has higher detection accuracies on different vehicle types
- MetraDS has lower false positive rates for different vehicle types and its maximum value reaches 7.8%



Detection accuracies for different vehicle types

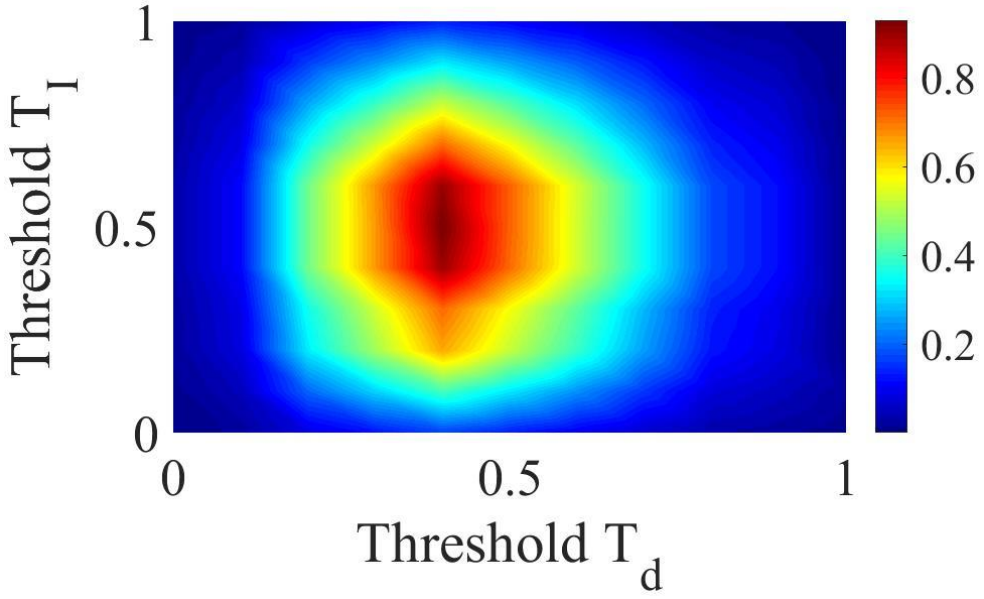


False negative rates for different vehicle types

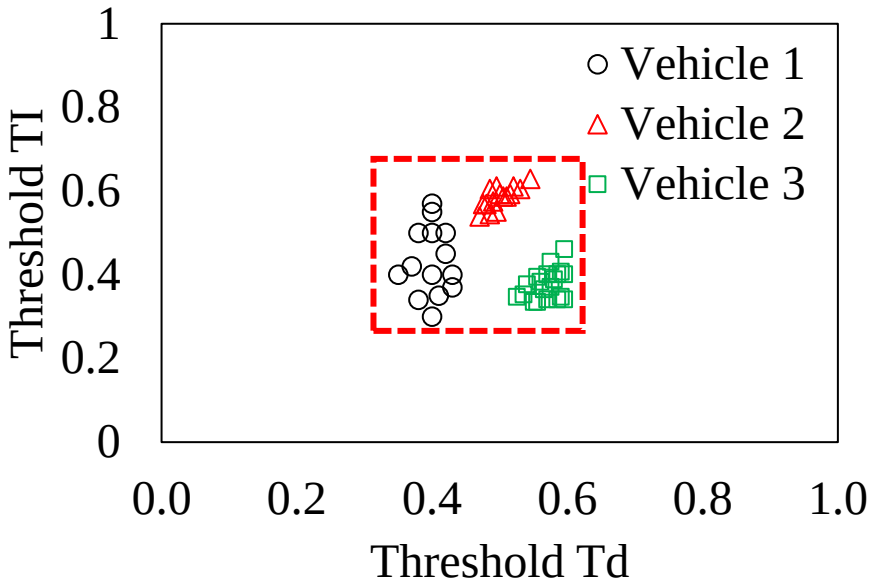
Performance Evaluation

Optimal thresholds of MetraDS

- Detection accuracy increases greatly as threshold T_d is larger than 0.2
- Optimal ranges of thresholds T_d and T_d are in the range [0.3, 0.6] and [0.3, 0.7]



Relationship between detection accuracy and thresholds

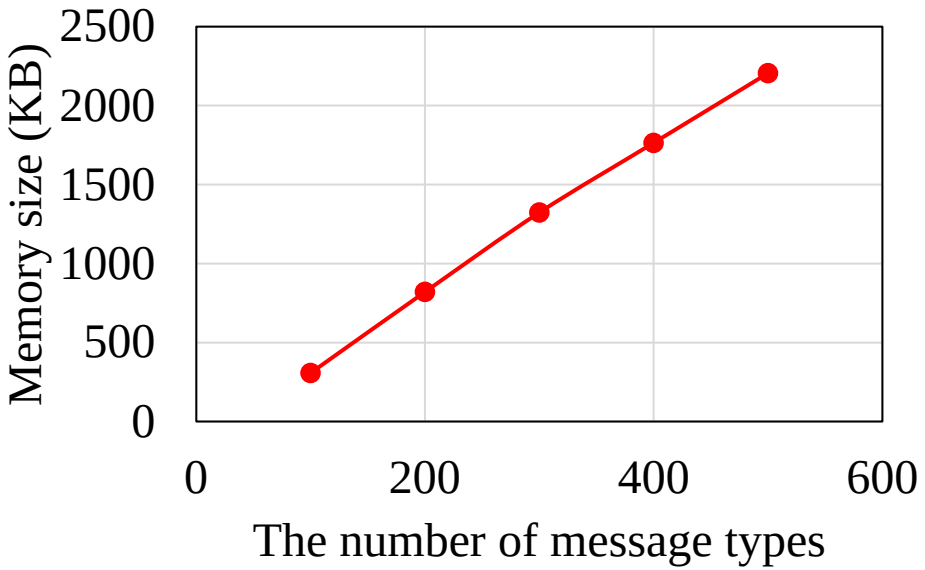


Optimal threshold regions for different vehicle types

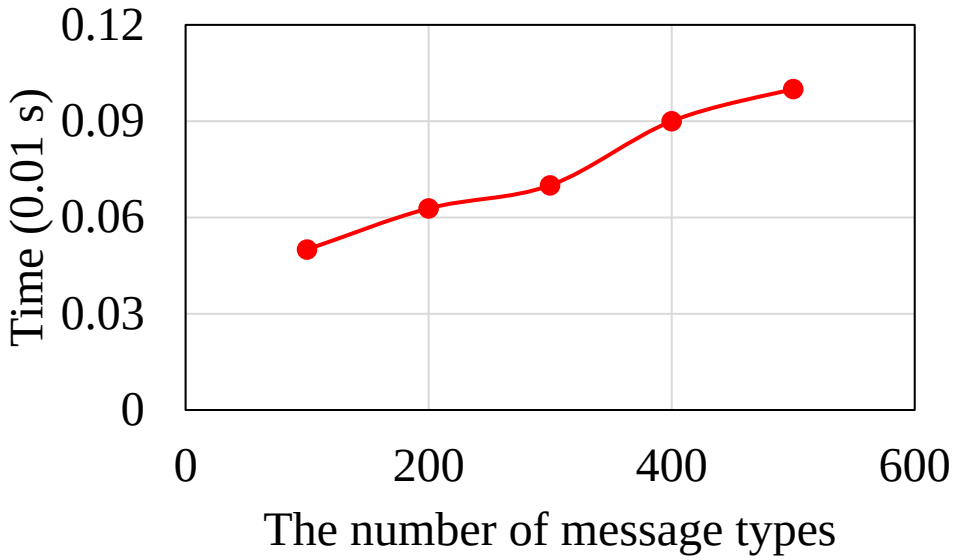
Performance Evaluation

Memory and computation cost

- Memory size of MetraDS becomes larger as the increase of message type numbers
- MetraDS needs more computation time as message type numbers increases



Memory size of MetraDS



The number of message types in one vehicle

Summary

Propose MetraDS to detect abnormal CAN bus messages based on message transmission behaviors

- Did statistical message transmission behavior analysis
- Built an abnormal message detection system based on transmission behavior analysis results
- Used CAN bus message datasets from real vehicles to verify MetraDS

Future work

- Explore other message transmission behaviors (e.g., values in message data field)

Thank you!