

# AI aided Lightweight Authentication for Internet of Vehicles (IoV)

Dr. Haitham Cruickshank

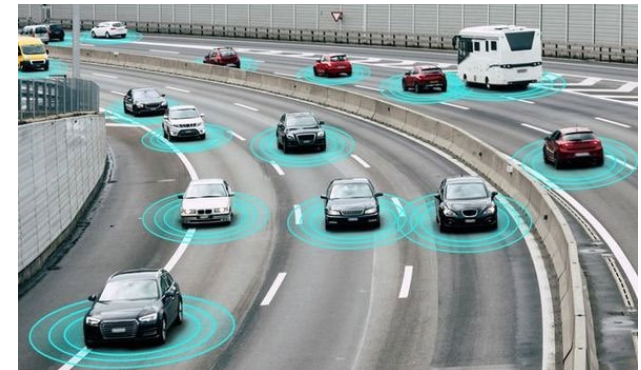
04/10/2022



- Introduction and security challenges of IoV
- TESLA for Light weight authentication
- AI aided Key Management for IoV Networks
- AI aided Intrusion Detection System in IoV
- Conclusions

# Introduction

- An estimate of 24,530 killed or seriously injured casualties in the year 2021.
- Internet of Vehicles (IoV) helps in improving road safety and enhance traffic management.
- Vehicles exchange safety messages to keep drivers aware of the road status (such ETSI define CAM and DENM).
- IoV provides range of applications e.g. safety, comfort
- **IoV is a very challenging IoT Vertical in terms of security and network performance provisioning.**



# IoV Security Challenges and requirements

## Security:

- Authentication
- Availability
- Integrity
- Access control

## Efficiency:

- Real time guarantee
- Robust security mechanism

## Accountability:

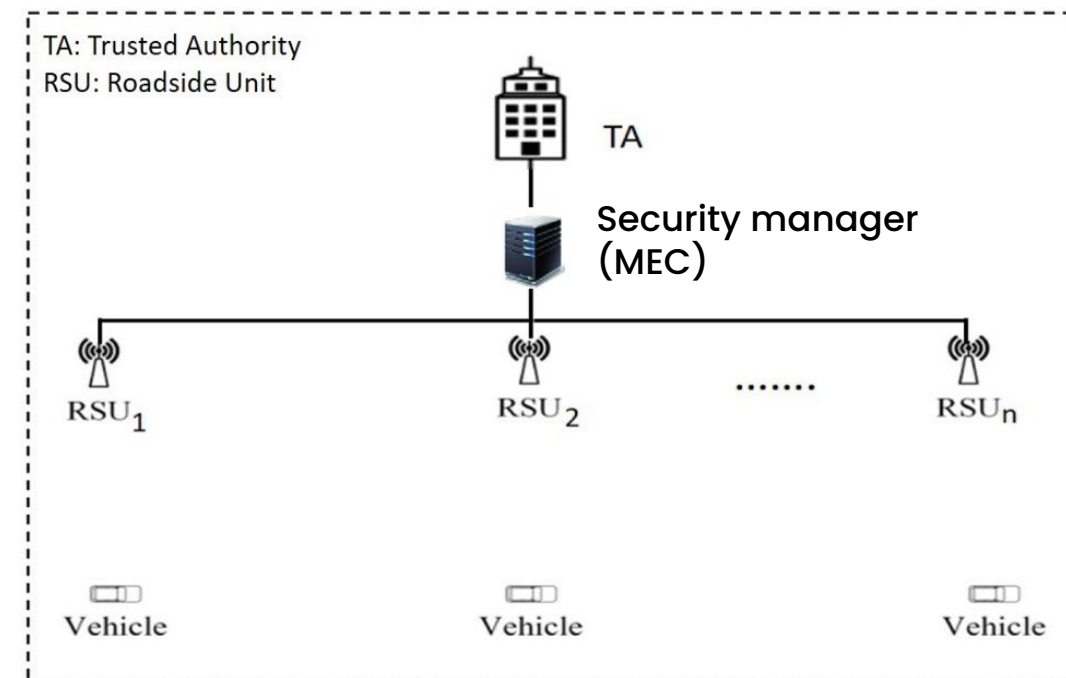
- Government enforcement authorities

**Scalability: Large number of vehicles**  
**Dynamicity: High speeds**



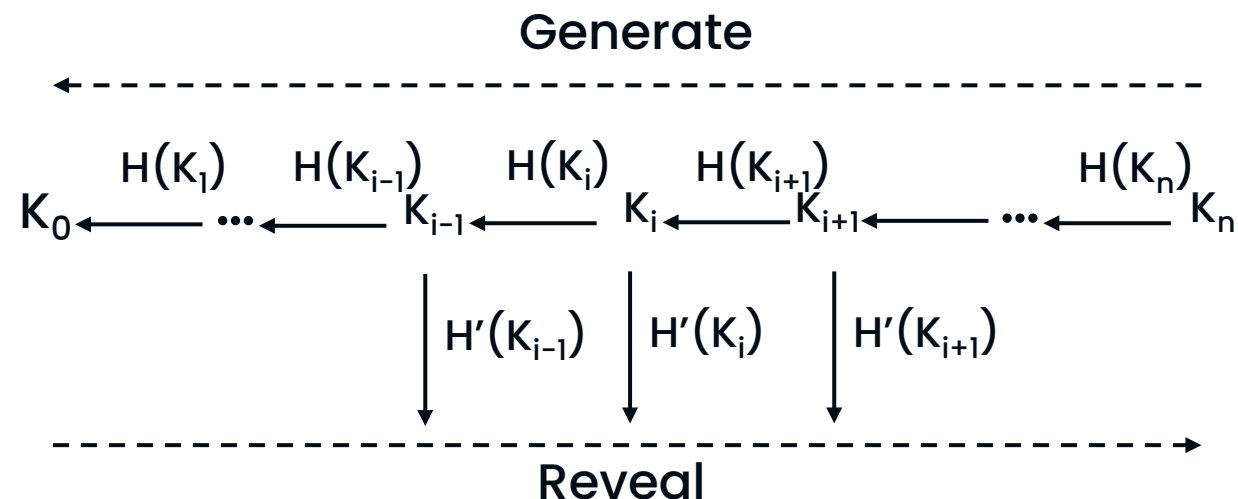
# AI based Key Management architecture: Co-located MEC and SM

- Machine Learning (ML) background:
  - Machine Learning (ML) plays an important role in enhancing network security.
  - ML can be used for several tasks, such as intrusion detection, anti-malware
  - Automating security tasks by using ML can help in reducing overheads on a network.
- Top layer consists of Trusted Authority (TA), which responsible for generating vehicles' credentials.
- Mid layer consists of Security Manager (SM) and Road Side Units (RSUs)
- A SM is responsible for managing vehicles and RSU in its region.
- Lower layer consists of vehicles.



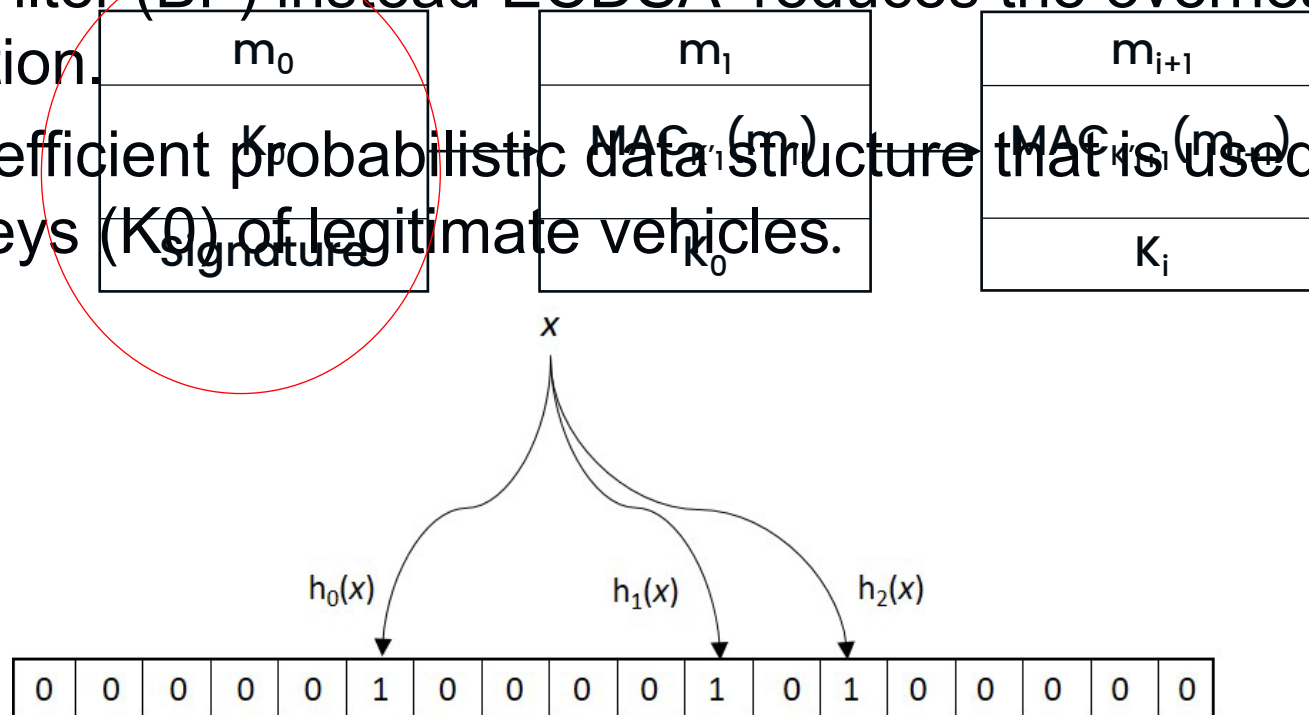
# Light weight source authentication: TESLA

- The Timed Efficient Stream Loss-tolerant Authentication (TESLA) protocol is used to provide broadcast authentication for V2V communications.
- TESLA is purely based on symmetric cryptographic functions (MAC).
- Despite using MAC functions, TESLA achieves asymmetric properties by delayed disclosure of keys by the sender.
- Each vehicle generates its TESLA keys using one way hash function.



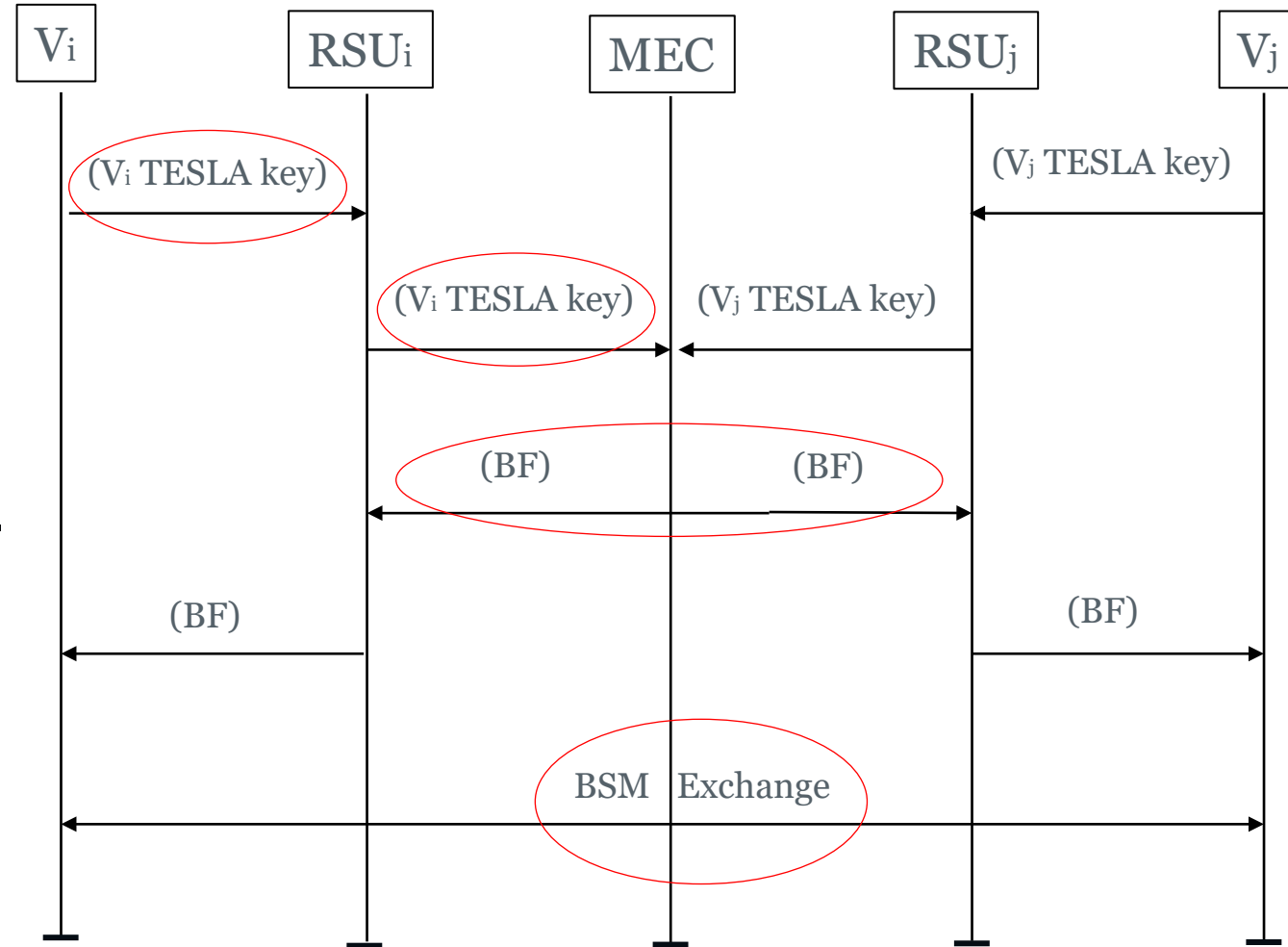
# TESLA and Bloom Filter for lightweight authentication- 1

- Although TESLA is suitable for V2V communication, it does not provide non-repudiation.
- ECDSA can be used along with TESLA to provide non-repudiation.
- Utilise Bloom Filter (BF) instead ECDSA reduces the overheads and enhances the authentication.
- BF is a space-efficient probabilistic data structure that is used to store the commitment keys ( $K_0$ ) of legitimate vehicles.



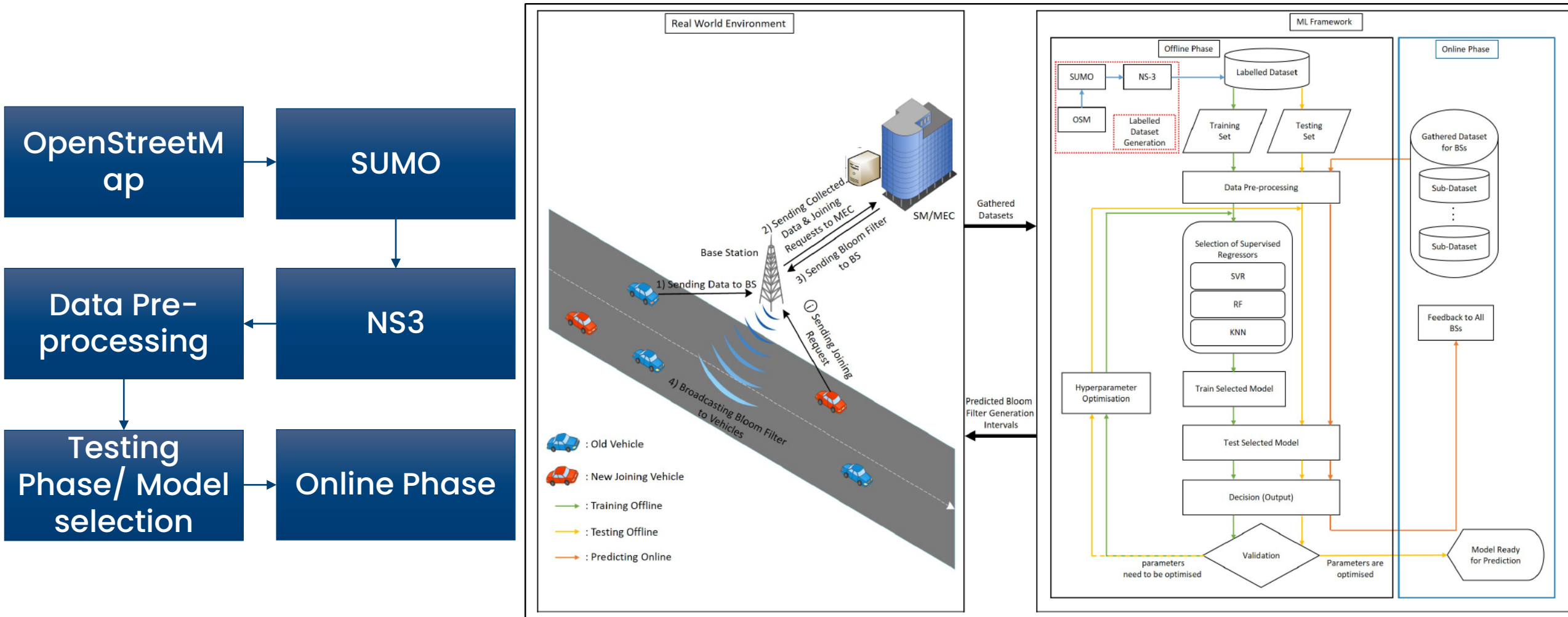
# TESLA and Bloom Filter for lightweight authentication- 2

- $V_i$  sends its ( $K_0$ ) to nearest RSU.
- MEC includes  $K_0$  in BF.
- A BF is signed and broadcasted to all vehicles.
- Non-repudiation is achieved by verifying the signature of a vehicle.





# AI based Key Management for IoV Networks

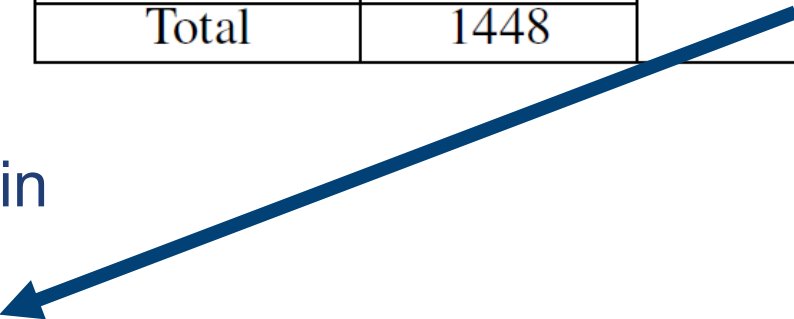


# Selected ML algorithms and features for the AIKEMA Key Management

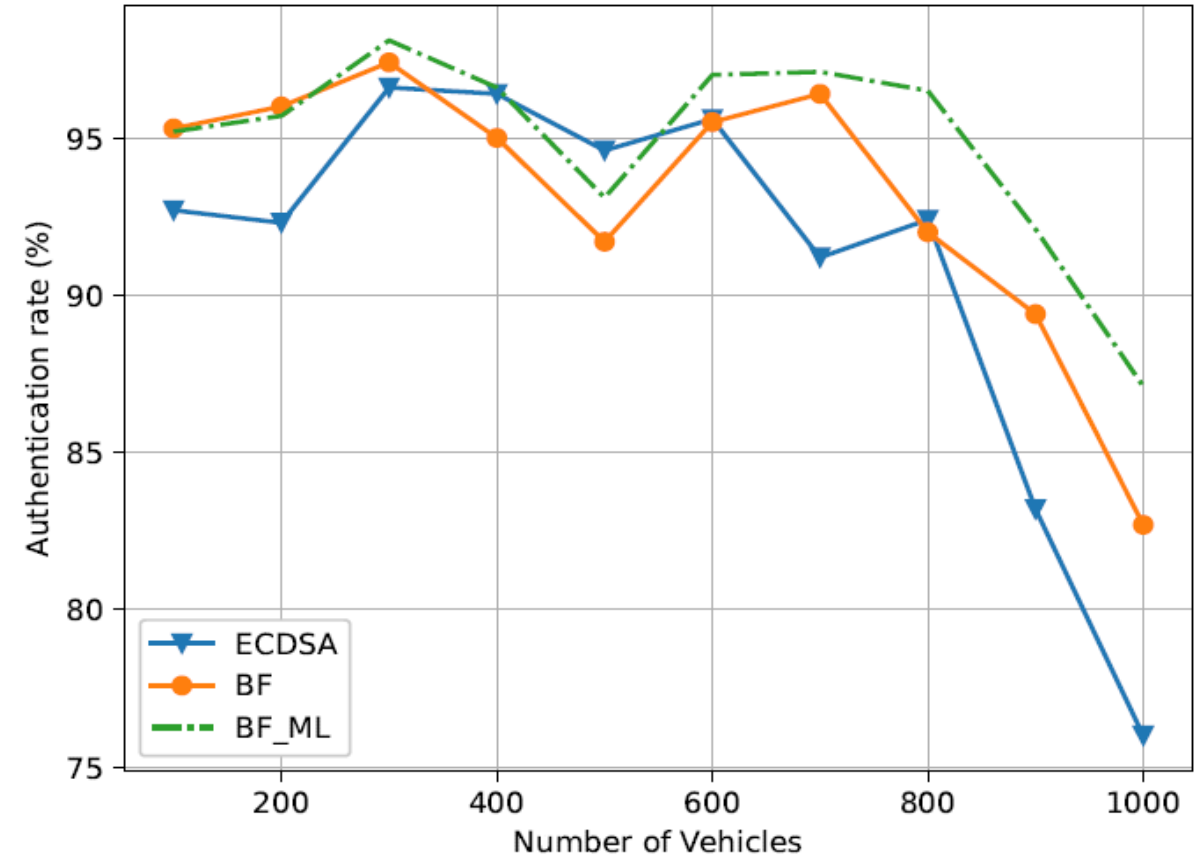
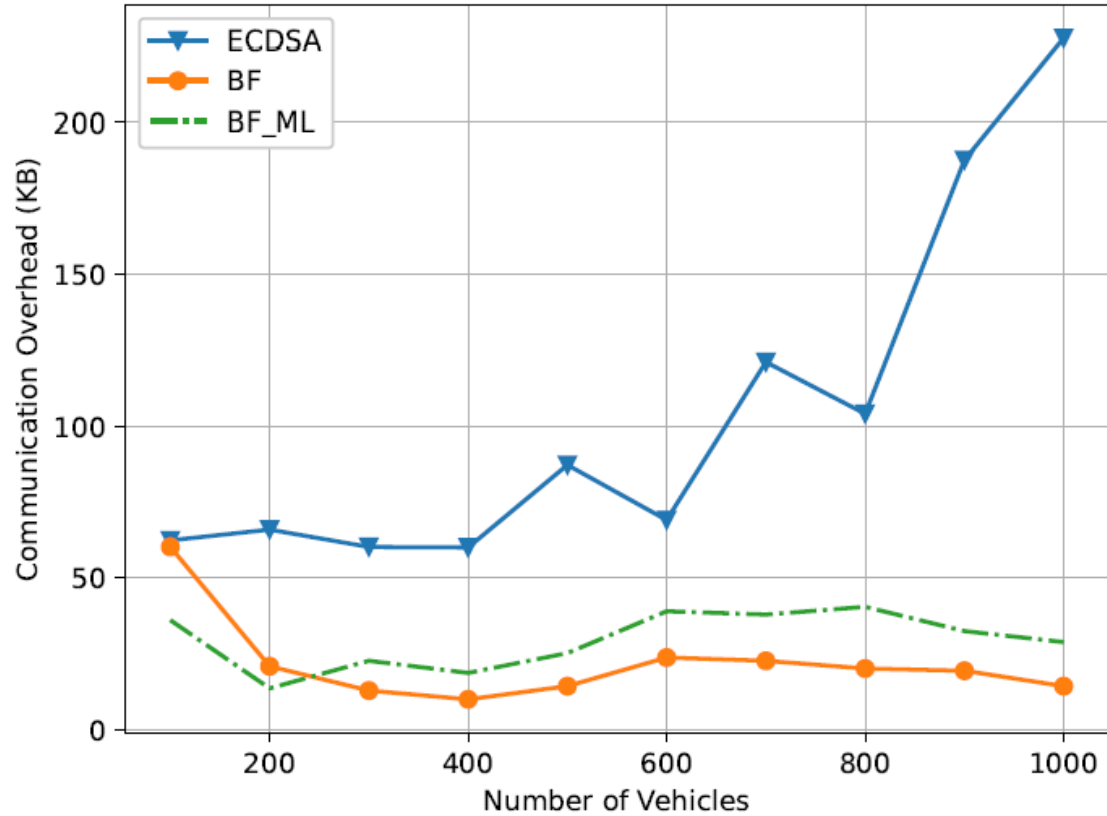
- ML algorithms used:
  1. Random Forest (RF),
  2. Support Vector Regression (SVR)
  3. K-Nearest Neighbour (KNN)
- Selected features:
  1. Number of current vehicles in a domain
  2. Average speed of vehicles
  3. Number of joining vehicles
  4. Joining frequency of vehicles

Dataset Table

Dataset	Instances	Features
London	510	4
Manchester	253	
Guildford	212	
Portsmouth	180	
Derby	293	
Total	1448	

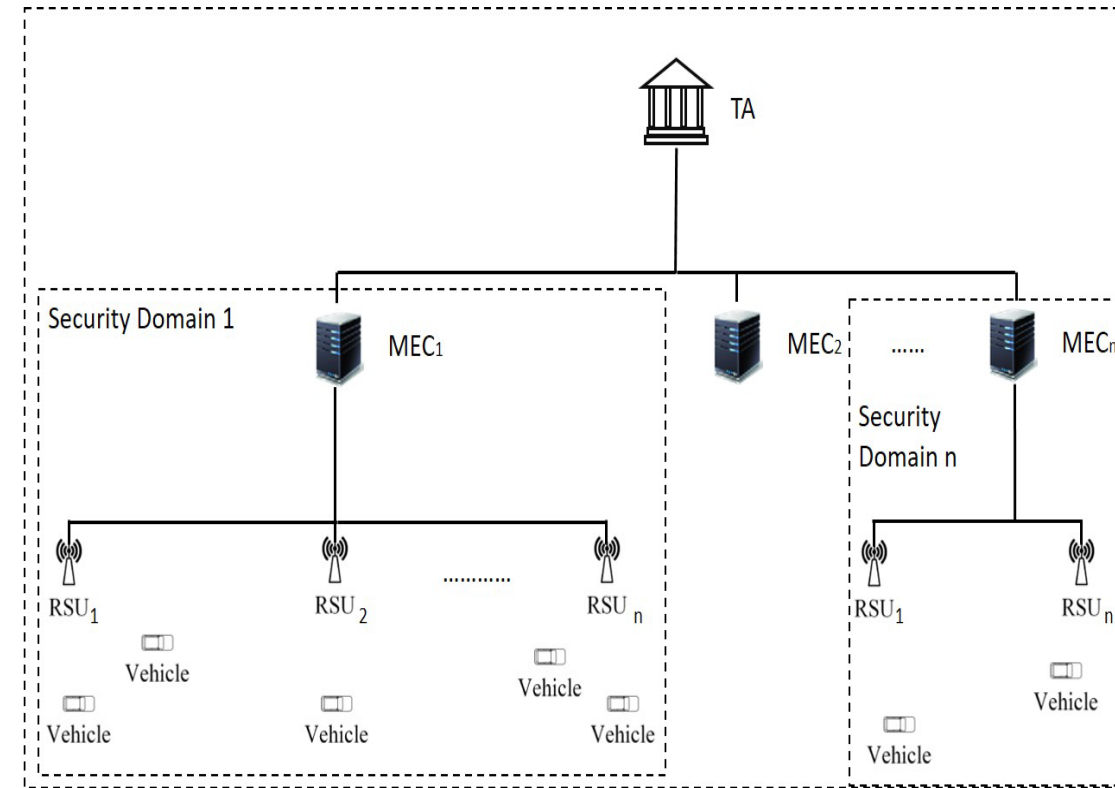


# Comparison of various authentication schemes

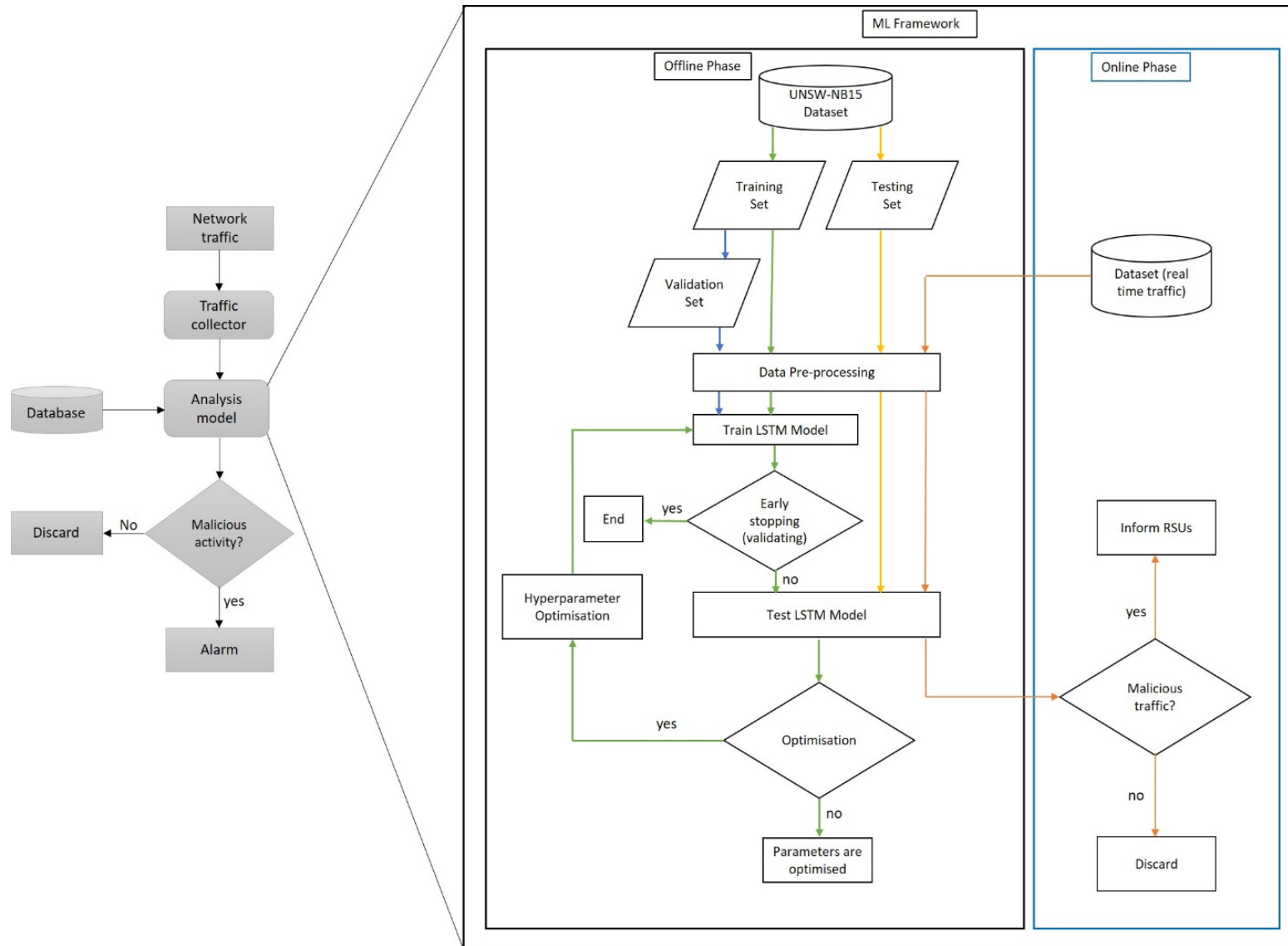


# Intrusion Detection System (IDS)

- IDS is co-located with the SM to detect DoS attacks.
- Long Short Term Memory (LSTM) is used as the underlying algorithm to detect DoS attacks.
- LSTM network architecture consists of 2 LSTM layers and 2 dense layers.
- The dataset used to train and test the LSTM is UNSW-NB15 dataset.



# AI aided IDS Architecture for IoV



# Intrusion Detection System (IDS) – Comparisons 1

Method	Accuracy (%)	Recall (%)	Precision (%)	F1-Measure (%)
Gao [RF]	98.7519	98.9793	94.1937	96.4747
Wang [DBN]	93.54	96.60	92.30	89.02
Nie [CNN]	96.6753	98.4977	95.5981	97.0263
Proposed method	98.3940	99.6118	97.5249	98.5573

RF: Random Forest

DBN: Deep Belief Networks

CNN: Convolutional Neural Network

Proposed method: based on LSTM



# Intrusion Detection System (IDS) – Comparisons 2

Table 1 Confusion matrix on UNSW-NB15 dataset for Gao's IDS

Gao Actual class	Predicted class	
	DoS	Normal
DoS	8270	3994
normal	496	55504

Table 2 Confusion matrix on UNSW-NB15 dataset for proposed method

Proposed method Actual class	Predicted class	
	DoS	Normal
DoS	12216	48
normal	1766	54238

# Conclusions

- Analysis of AI based key management or key agreement in IoV is provided, based on the impact on network performance. This is important for IoV broadcast applications like safety messages (CAM and DENM).
- Design an AI/ML aided Intrusion Detection System (IDS) for DoS. The key management is adaptable in relation to threat levels. So that the security measures are always proportional to the present threat levels.
- For both tasks above the security manager was co-located with MEC
- Future outlook: The use of MEC and future federated AI/ML techniques can playing an important role in fast security synchronization of distributed and heterogeneous IoV security domain.

THANK YOU

# Comparison of various ML schemes

