Security of Vehicular Networks

03/11/2022

Outline

- Background

- Current solution areas surveyed

- Some interesting works in this areas and their limitations

- Next steps: propose improvements/new solutions to the identified issues

The Era of Connected Vehicles

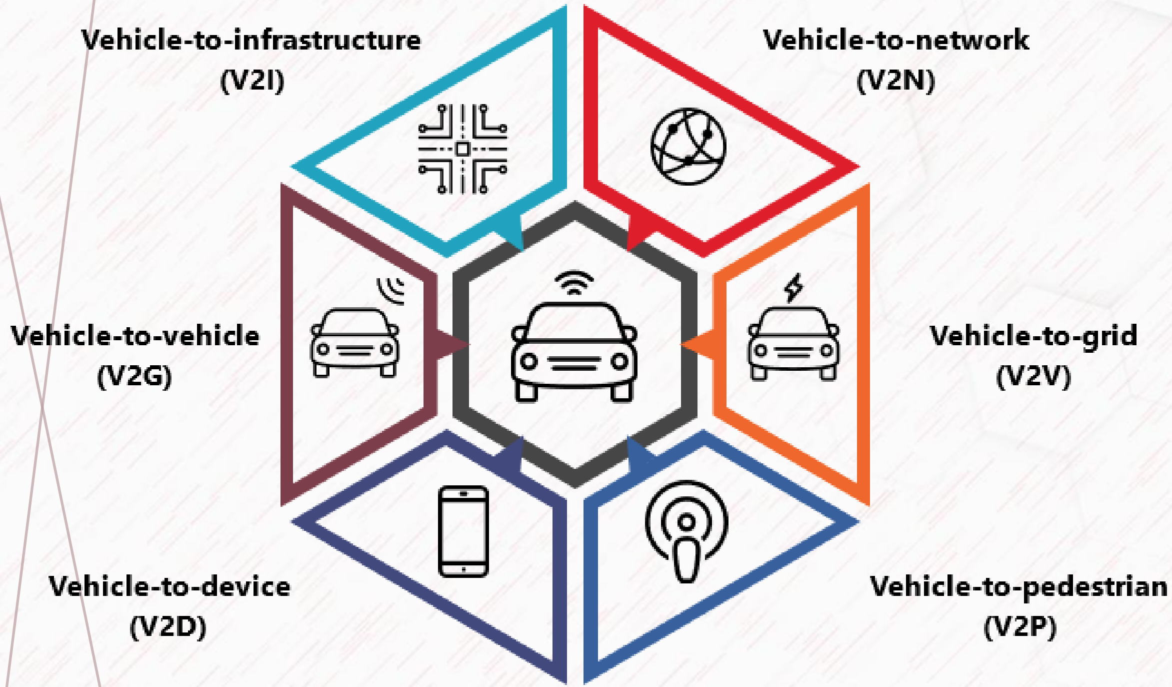
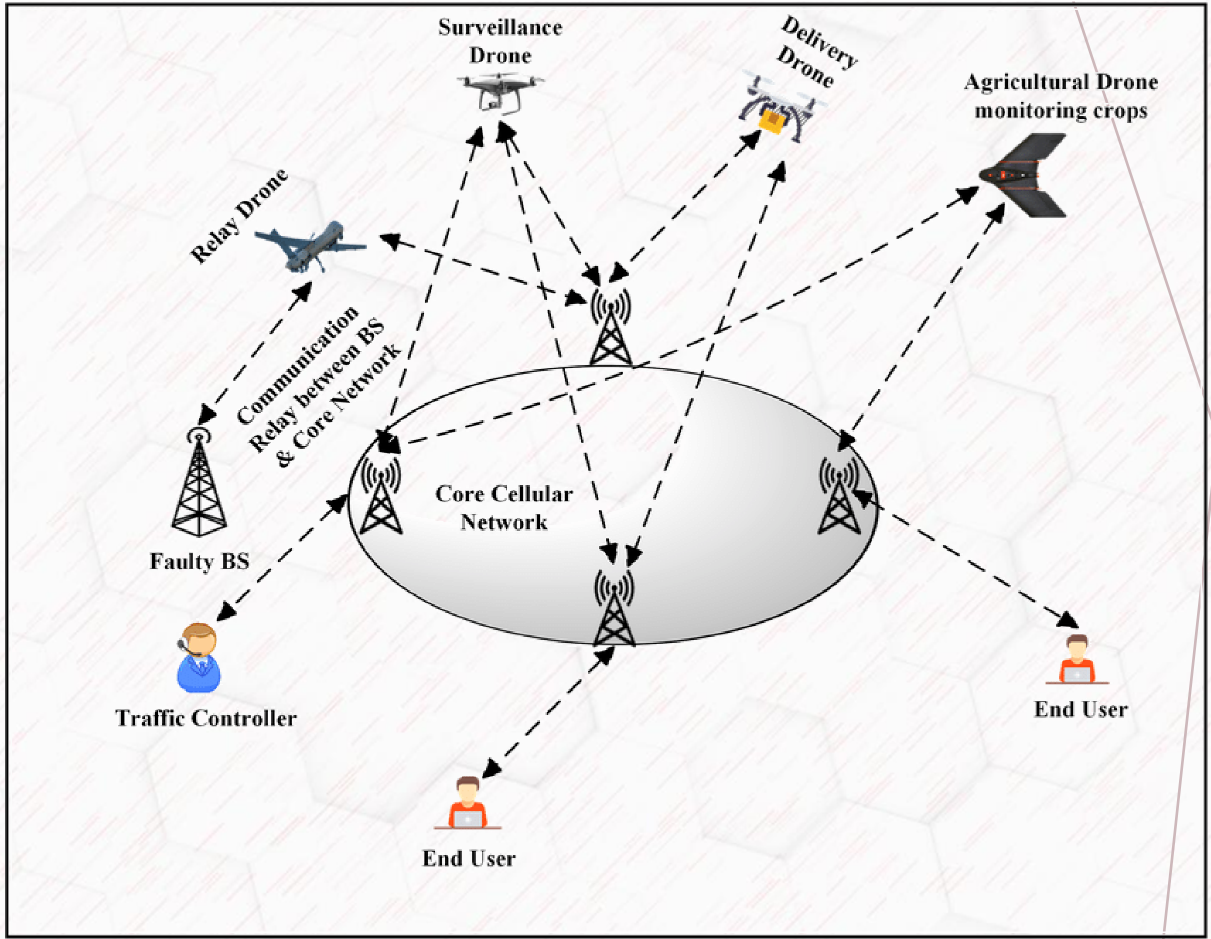


Figure 1: Vehicle-to-everything (V2X) technology



Common Attacks on Connected Vehicle Network

- Man-in-the-Middle
- Eavesdropping
- Blackhole
- Sybil

Attacks on Integrity

- Spoofing
- Replay
- Traffic analysis

Attacks on Confidentiality

- Man-in-the-Middle
- Jamming
- Physical attacks
- DOS/DDOS

Attacks on Availability

- Malware
- Membership inference attacks

Attacks on Privacy

Common techniques to defend against these attacks

	Categories	Attacks mitigated
Authentication	**Cryptography-based methods** Hash based Identity based Group/Batch Signature Blockchain based **Context-based methods** Physical layer characteristics Multi-factor authentication Environment based	Spoofing Sybil Masquerading
Intrusion/Misbehavior Detection	**Signature-based detection** Rules based Entropy based Machine learning (ML) based **Anomaly-based detection** Machine learning based ML & Honeypot **Sensor fusion approach** **Hybrid-based methods**	Malware Spoofing Message falsification

Common techniques to defend against these attacks

	Categories	Attacks mitigated
Privacy Preservation and Secured Data Sharing	**Trust/Reputation system** Rule based Blockchain based **Machine learning based** Federated learning **Privacy preserving computation** Homomorphic encryption Differential privacy **Encrypted ML models with fog computing**	Malware Data leakage ML adversarial attacks

Proposed Authentication Techniques in the Literature

Paper	Category	Main idea	Evaluation Methods	Limitations
Delegating Authentication to Edge: A Decentralized Authentication Architecture for Vehicular Networks	Cryptography based	Proposed a PKI-free protocol to mitigate the long authentication delay and single point-of-failure in the Vehicular Ad Hoc Network (VANETs). The decentralized architecture enables the authentication server to delegate its authentication capabilities to the edge node (Road Side Units).	The proposed protocol was implemented in Java and simulated on a PC.	❑ Huge computational costs ❑ Extra communication overhead with the decentralized approach.
FBIA: A Fog-Based Identity Authentication Scheme for Privacy Preservation in Internet of Vehicles		The FBIA scheme uses elliptic curve cryptography and random forest algorithm from deep learning to form the two layers for authentication. The first layer is the security authentication layer for vehicles from outside the fog, whereas the second layer is the security surveillance layer for the remaining vehicles.	The proposed system was simulated in SUMO.	

Proposed Authentication Techniques in the Literature

Paper	Category	Main idea	Evaluation Methods	Limitations
LIDAR: Lidar Information based Dynamic V2V Authentication for Roadside Infrastructure-less Vehicular Networks	Context Based	The proposed protocol authenticate vehicles locally using the lidar sensors in the vehicle without involvement of a trusted authority and infrastructures. The proposed scheme prevents against possible man-in-the-middle attacks.	They simulated the proposed protocol in auto-pilot mode using CARLA, an autonomous urban driving simulator.	❑ Single point of failure ❑ Lacks robustness and are not scalable ❑ The proposed schemes does not provide non-repudiation. That is, there is no traceability mechanism to trace and find intruders in the network.
Vision-Based Two-Factor Authentication & Localization Scheme for Autonomous Vehicles		The scheme leverages the vehicles' light sources and cameras to establish an "Optical Camera Communication (OCC)" channel providing an auxiliary channel between vehicles to visually authenticate and localize the transmitter of messages that are sent over Radio Frequency (RF) channels.	The details of the evaluation was not clearly provided.	

Lidar Information based Dynamic V2V Authentication for Roadside Infrastructure-less Vehicular Networks

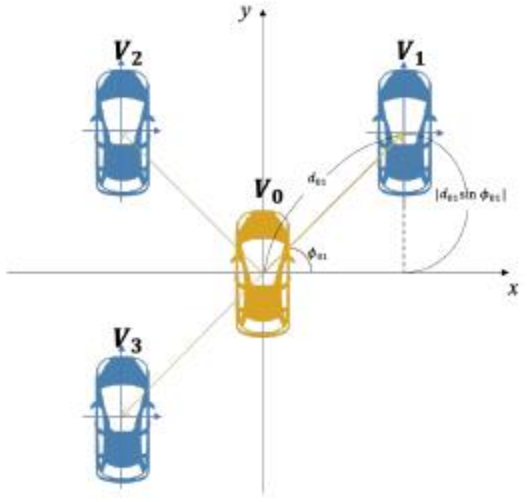


Fig. 2. V_0's view

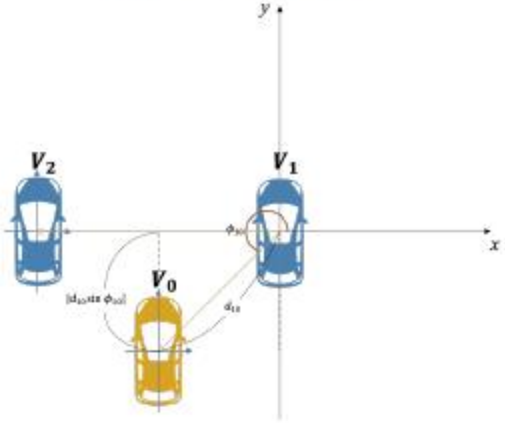


Fig. 3. V_1's view

Overview of system model

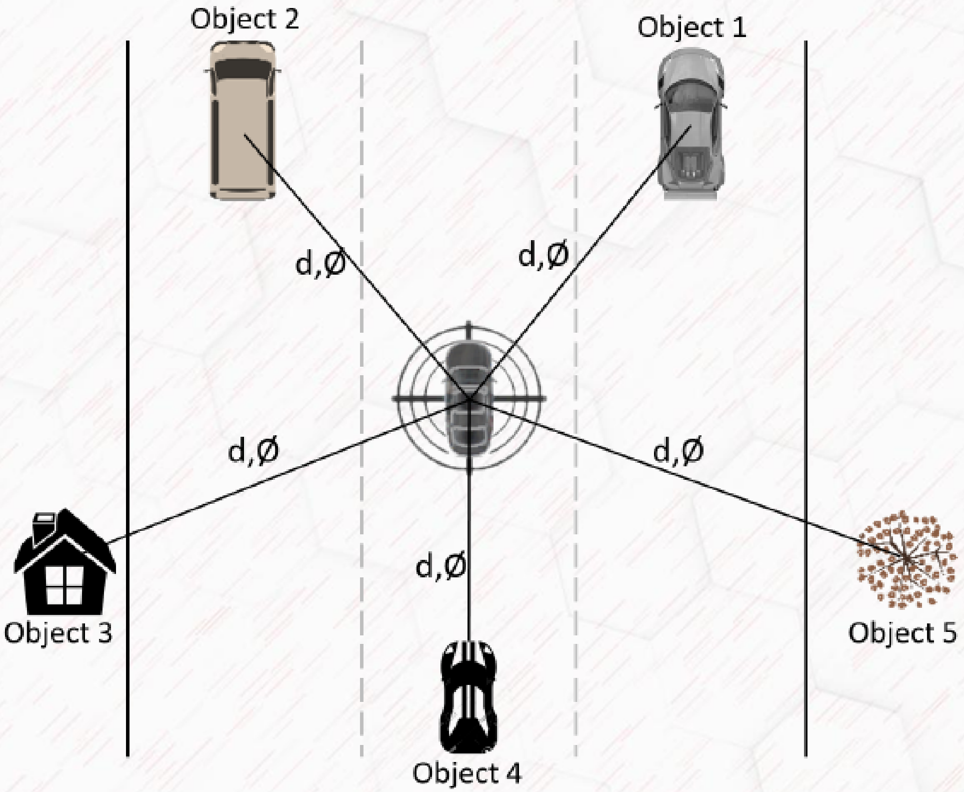


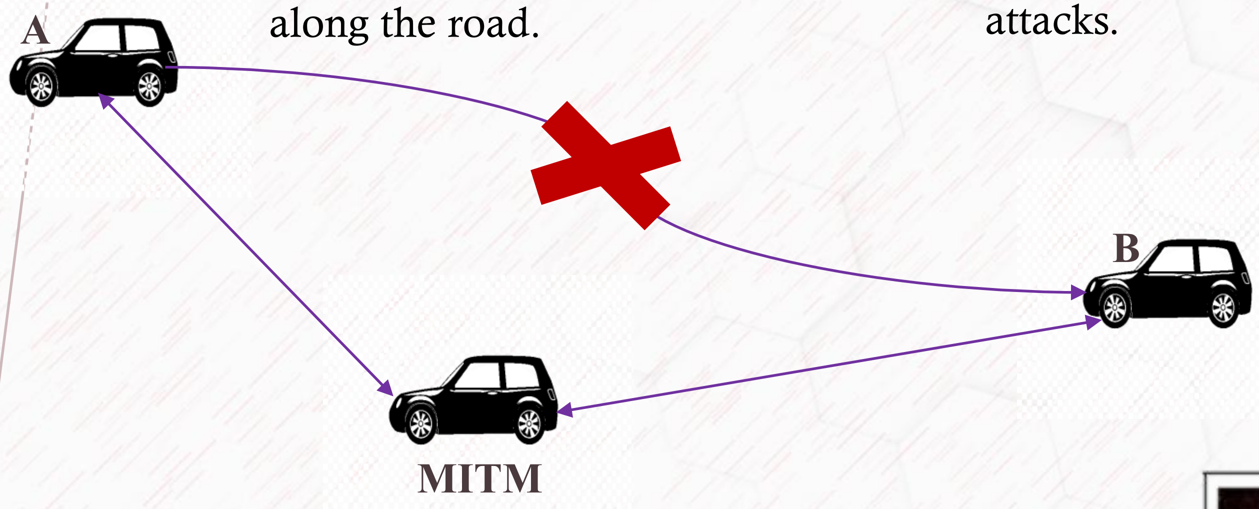
Figure 1: Overview of the System Model

- The locality information of vehicle is used for authentication.
- The scheme utilizes the existing sensors on vehicles and the locality information of vehicles are identified by comparing the similarity of the locality information of the surroundings generated by sensor data.
- The vehicle computes the distance (d) and angle (Ø) towards the surrounding objects and exchange this information over the DSRC wireless channel to authenticate with other vehicles.

Lidar Information based Dynamic V2V Authentication for Roadside Infrastructure-less Vehicular Networks

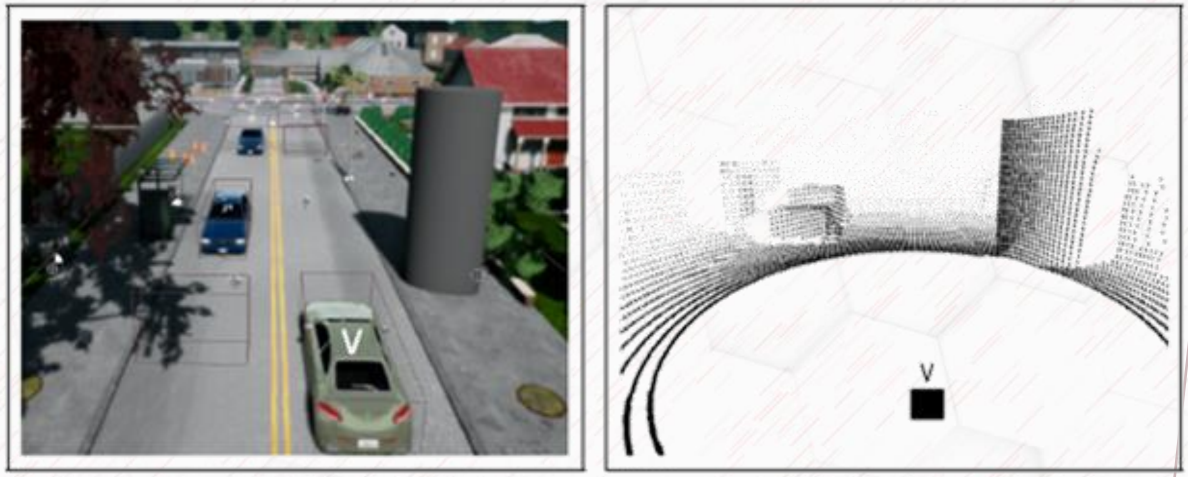
- The attack threat model is attacks co-located with the legitimate entities i.e., the neighboring vehicles traveling along the road.

- Focus is on attackers impersonating legitimate entities by launching man-in-the middle (MITM) attacks.



- The proposed system was simulated in auto-pilot mode using CARLA, an autonomous urban driving simulator.

- The objects and environment settings are configured using Unreal Engine 4.18.



(a) Target vehicle

(b) Front view of lidar image

Open Challenges in Authentication

- Due to low latency demands, short lifetime and low computational capacity requirements of vehicular communications, the major bottleneck still with the existing techniques is that of lowering the authentication time using lightweight algorithms without compromising the quality of security.

- Scalable and distributed authentication and secure message dissemination protocols.

Proposed Intrusion Detection Techniques in the Literature

Paper	Category	Main idea	Evaluation Methods	Limitations
Collaborative Intrusion Detection for VANETs: A Deep Learning-Based Distributed SDN Approach	Signature based detection	They utilize deep learning with generative adversarial networks and distributed SDN to design a collaborative intrusion detection system (CIDS) for VANETs, which enables multiple SDN controllers to jointly train a global intrusion detection model for the entire network without directly exchanging their sub-network flows.	The proposed protocol was implemented in python and simulated on a PC. They used the KDD99 dataset and the refined version, NSL-KDD99 for the experimental evaluation. They evaluated the scheme with metrics such as precision, accuracy, F1-Score, recall, and AUC.	• Classification performance of these methods is usually low in zero-day (previously unknown) attack scenarios.
Novel Deep Learning-Enabled LSTM Autoencoder Architecture for Discovering Anomalous Events From Intelligent Transportation Systems	Anomaly based	The authors proposed an IDS to discover suspicious network activity of In-Vehicles Networks (IVN), vehicles to vehicles (V2V) communications and vehicles to infrastructure (V2I) networks using deep learning architecture-based Long-Short Term Memory (LSTM) autoencoder algorithm designed to recognize intrusive events from the central network gateways of AVs.	The proposed IDS is evaluated using two benchmark datasets, i.e., the car hacking dataset for in-vehicle communications and the UNSWNB15 dataset for external network communications.	The proposed scheme is computationally expensive due to high model complexity even though the proposed scheme can achieve high accuracy.

Proposed Intrusion Detection Techniques in the Literature

Paper	Category	Main idea	Evaluation Methods	Limitations
MTH-IDS: A Multi-Tiered Hybrid Intrusion Detection System for Internet of Vehicles	Hybrid	A multi-tiered hybrid IDS that incorporates a signature-based IDS and an anomaly-based IDS is proposed to detect both known and unknown attacks on vehicular networks.	They evaluated the performance and overall efficiency of the proposed model on two state-of-the-art datasets, CAN-intrusion-dataset and CICIDS2017, and discusses its feasibility in real-world IoV devices.	• High false positive rate in the anomaly detection stage since being reliant on the signatures of attacks in the training step, the IDS might not be effective to distinguish zero day attacks. • High computational cost and detection delays.
Real-Time Sensor Anomaly Detection and Identification in Automated Vehicles	Sensor Fusion	They proposed a generic framework combining a deep learning technique, i.e., CNN, and Kalman filtering with a χ^2 detector, and investigate their ability to detect and identify various types of anomalous behavior in real-time.	They evaluated the proposed scheme using dataset from SPMD which contains data captured by different sensors over a period of two years.	The data driven approach is unable to identify the sensor(s) under attack.

Open Challenges in Intrusion Detection

- Zero-day attacks detection with low FPR.
- Real world deployment and testing.
- Dire requirement of a specialized dataset containing pattern of most of the attacks of VANET.
- Requirement of lightweight and resource friendly IDS.
- Framework to predict attacks beforehand.
- No updating or online learning mechanism.
- Deployment location in VANET.

Proposed Privacy and Secured Data Sharing Techniques

Paper	Category	Main idea	Evaluation Methods	Limitations
Privacy Preserving Misbehavior Detection in IoV using Federated Machine Learning	Machine learning based	The author proposed a federated learning scheme where personal information of a vehicle resides locally on the vehicle and performs ML training without sending data to the central node. The vehicles only send their updated and trained local model to the central node for learning of an aggregated smarter model. The centrally trained model not only detects but also identifies the position of an attack.	They used Precision, Recall and Accuracy to evaluate the misbehavior detection scheme with Veremi simulated dataset which contains message logs of GPS data of the vehicle and BSM data received from other vehicles communicated through DSRC.	Performing ML training locally on the vehicle can be energy expensive
Edge-Assisted Privacy-Preserving Raw Data Sharing Framework for Connected Autonomous	Encrypted Machine Learning models	They proposed an edge-assisted privacy-preserving raw data sharing framework that leverage the additive secret sharing technique to encrypt raw data into two ciphertexts and construct two classes of secure functions. The functions are then used to implement a privacy-preserving convolutional neural network (P-CNN) and two edge servers are deployed to cooperatively execute P-CNN to extract features from two ciphertexts to obtain the same object detection results as the original CNN.	KITTI data set containing 3000 training samples and 750 test samples was used to train and test the P-CNN model.	The scheme is not scalable due to the huge computational overhead involved with the proposed P-CNN model.

Open Challenges in Privacy Preservation

- Lightweight privacy-preserving authentication

- Scalable and robust techniques for secure data sharing in vehicular networks.

Next Steps: Secured Data-centric Misbehavior Detection in Vehicular Networks

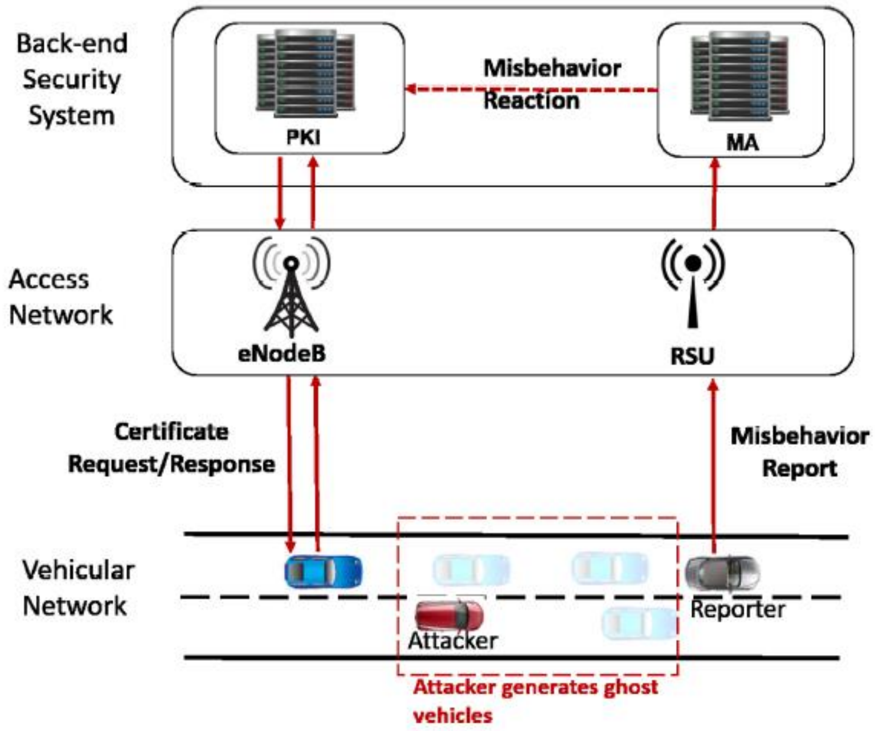
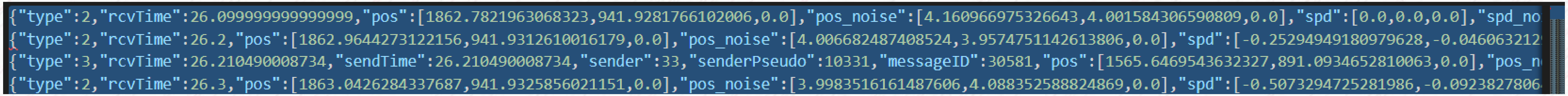


Fig. 1. C-ITS security architecture.



```
{"type":2,"rcvTime":26.099999999999999,"pos":[1862.7821963068323,941.9281766102006,0.0],"pos_noise":[4.160966975326643,4.001584306590809,0.0],"spd":[0.0,0.0,0.0],"spd_no
{"type":2,"rcvTime":26.2,"pos":[1862.9644273122156,941.9312610016179,0.0],"pos_noise":[4.006682487408524,3.9574751142613806,0.0],"spd":[-0.25294949180979628,-0.046063212
{"type":3,"rcvTime":26.210490008734,"sendTime":26.210490008734,"sender":33,"senderPseudo":10331,"messageID":30581,"pos":[1565.6469543632327,891.0934652810063,0.0],"pos_n
{"type":2,"rcvTime":26.3,"pos":[1863.0426284337687,941.9325856021151,0.0],"pos_noise":[3.9983516161487606,4.0883525888824869,0.0],"spd":[-0.5073294725281986,-0.0923827806
```