PELMOB

Funded by the European Union

Internet of things for electric vehicles

Assistant Professor Oliver Popović
AUB, Faculty for Traffic, Communication and Logistic, Budva

Security challenges at VANET network

Challenges, threats and solutions for secure communication in traffic networks

"Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union. Neither the European Union nor the granting authority can be."

Partnership for Promotion and Popularization of Electrical Mobility through Transformation and Modernization of WB HEIs Study Programs/ PELMOB
Call: ERASMUS-EDU-2022-CBHE-STRAND-2
Project Number: 101082860

Introduction to VANET networks

- Vehicular Ad-Hoc Networks (VANET) are a type of wireless networks intended for communication between vehicles and traffic infrastructure.
- They function without centralized control, allowing vehicles to exchange information in real time.
- They are used to improve traffic safety, inform about road conditions and optimize traffic.

Introduction to VANET networks

Application examples:

- Collision warning.
- Information about weather conditions and blockades.
- Real-time navigation.

Key characteristics of VANET networks

- High mobility: Vehicles move at high speeds, which affects the stability of connections.
- Dynamic topology: The network structure is constantly changing due to the movement of vehicles.
- Decentralization: The network operates without a central server, which is both an advantage and a challenge.
- Short-term connections: Due to the high speed, communication between vehicles can last only a few seconds.
- Low connection capacity: The network must be resilient to delays and data loss.

Advantages applications of VANET networks in traffic

- Improving safety: The exchange of information between vehicles reduces the risk of accidents.

- More efficient traffic flow: Optimizing vehicle movement through dynamic adjustment of traffic lights and bypassing traffic jams.

- Timely information: Informing the driver about road conditions and potential hazards.

- Support for autonomous vehicles: The integration of VANET networks helps coordinate autonomous cars.

Examples of using VANET networks

V2V communication:

- Warning of accidents and sudden braking.
- Coordination when changing lanes and turning.

V2I communication:

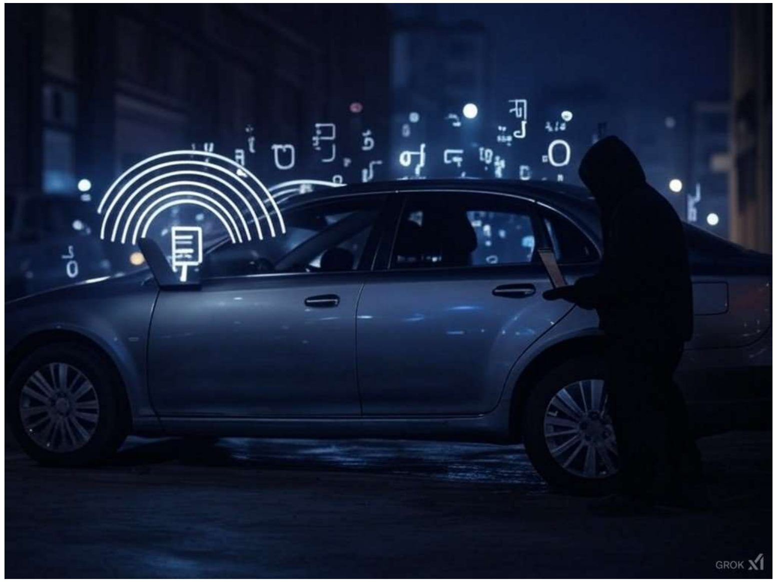
- Dynamic control of traffic lights to reduce congestion.
- Warnings of roadworks or lane closures.

V2X communication:

- Communication with pedestrians, cyclists and smart devices.

Security challenges in VANET networks

- Data Vulnerability: Due to wireless communication, data is susceptible to interception and manipulation.
- Resource constraints: Vehicles have limited processing power and memory for complex security protocols.
- The question of trust: How to ensure that data comes from reliable sources?
- Attack speed: Attacks happen quickly because of the short time intervals in the network.



Attacks on confidentiality data

- **Eavesdropping** :
- Attacker intercepts data between vehicles, such as location and message warnings.

- **Theft identity** :
- Malicious person can take over identity vehicles and send fake informations.

- **Influence on privacy** :
- Possibility monitoring movements of vehicles and driver.

Attacks on integrity data

•**Fake messages**: Attackers can send fake information, such as fake warnings on accident, which can cause confusion .

•**Manipulation data**: Change of traffic data conditions can lead to wrong conclusions in decisions of driver or system.

•**Influence on vehicles coordination**: Wrong data can cause collisions and congestions.

Attacks on availability

- Denial-of-Service (DoS) attacks: Overwhelming network by numberous fake requests blocks communication between vehicles.

- Distributed Denial-of-Service (DDoS) attacks: Coordinated attacks with more sources, making network unusable.

- Influence on traffic : DoS attacks can cause delays, impact on security and increase network traffic.

Attacks identity-based

- Sybil attacks : Attacker creates more fake identity in order to take over control over network.

- False Presentation: Attacker benefits identity legitimate vehicles to send fake data .

- Impact: Sybil attacks can interfere system navigation and bringing decision in the network.

Challenges with authentication and authorization

- Authentication: How to ensure that communication comes from the real one source ?

- Authorization: Who has right access certain data or functions?

- Problems: Complex authentication systems can slow down communication, which is critical in VANET networks.

Cryptoanalysis in VANET networks

- Weaknesses encryption: Inappropriate or outdated algorithms can enable attackers to decrypt data.

- Attacks on keys: Theft or compromising cryptographic keys threatens security system.

- Balance performance and security: More complex algorithms can slow down communication, which is unacceptable in real-time applications.

Protection privacy driver

•Monitoring Locations : Attackers can follow the movement of vehicles and analyze habits of a driver .

•Unauthorized Identification : Private data of the driver can be discovered to third parties.

•Solutions : Use methods for anonymization and encryption .

Role artificial intelligence in prevention attacks

- Detection anomaly : AI can recognize unusual forms in the network traffic and mark them as potential threats .

- Predictive analysis : Prediction attacks on basis historical data .

- Autonomous answer : AI systems I can automatically react on threats and adapt network parameters .

Conclusion

•VANET networks they have huge potential for improvement security and efficiency in traffic .

•Security Challenges : Still going on there are significant problems that must be to be resolved , especially in the area of protection data and authentication .

•Looking to the future : With technology advancements it is expected to be higher integration of VANET networks into traffic.