Internet stvari za električna vozila

Doc.dr Oliver Popović
AUB, Faculty for Traffic, Communication and Logistic, Budva

Bezbednosni izazovi kod primene VANET mreža

Izazovi, pretnje i rešenja za bezbednu komunikaciju u saobraćajnim mrežama

"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

Uvod u VANET mreže

- Vehicular Ad-Hoc Networks (VANET) su vrsta bežičnih mreža namenjenih komunikaciji između vozila i saobraćajne infrastrukture.
- Funkcionišu bez centralizovane kontrole, omogućavajući vozilima da razmenjuju informacije u realnom vremenu.
- Koriste se za unapređenje bezbednosti u saobraćaju, obaveštavanje o uslovima na putevima i optimizaciju saobraćaja.

Uvod u VANET mreže

Primeri primene:

- Upozorenje na sudar.
- Informisanje o vremenskim uslovima i blokadama.
- Navigacija u realnom vremenu.

Ključne karakteristike VANET mreža

- Visoka mobilnost: Vozila se kreću velikim brzinama, što utiče na stabilnost veza.
- Dinamična topologija: Mrežna struktura se stalno menja zbog kretanja vozila.
- Decentralizacija: Mreža funkcioniše bez centralnog servera, što je istovremeno prednost i izazov.
- Kratkotrajne veze: Zbog velike brzine, komunikacija između vozila može trajati samo nekoliko sekundi.
- Nizak kapacitet veze: Mreža mora biti otporna na kašnjenja i gubitke podataka.

Prednosti primene VANET mreža u saobraćaju

- Unapređenje bezbednosti: Razmena informacija između vozila smanjuje rizik od nesreća.
- Efikasniji protok saobraćaja: Optimizacija kretanja vozila kroz dinamičko prilagođavanje semafora i obilaženje gužvi.
- Pravovremeno informisanje: Obaveštavanje vozača o uslovima na putu i potencijalnim opasnostima.
- Podrška za autonomna vozila: Integracija VANET mreža pomaže u koordinaciji autonomnih automobila.

Primeri upotrebe VANET mreža

V2V komunikacija:

- Upozorenje na nesreće i naglo kočenje.
- Koordinacija pri promeni traka i skretanju.

V2I komunikacija:

- Dinamička kontrola semafora za smanjenje gužvi.
- Upozorenja na radove na putu ili zatvorene trake.

V2X komunikacija:

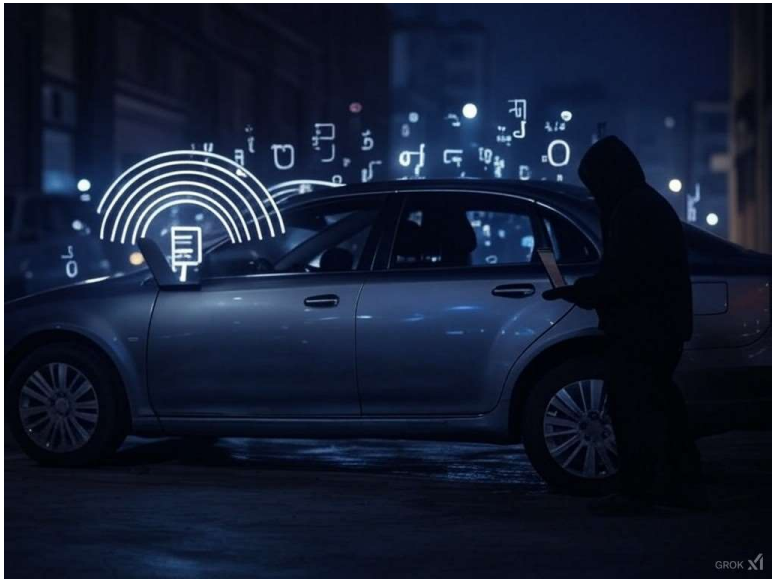
- Komunikacija sa pešacima, biciklistima i pametnim uređajima.

Program: ERASMUS-EDU-2022-CBHE-STRAND-2
Project number: 101082860

Funded by the European Union

Bezbednosni izazovi u VANET mrežama

- Ranljivost podataka: Zbog bežične komunikacije, podaci su podložni presretanju i manipulaciji.
- Ograničenja resursa: Vozila imaju ograničenu procesorsku snagu i memoriju za složene sigurnosne protokole.
- Pitanje poverenja: Kako osigurati da podaci dolaze od pouzdanih izvora?
- Brzina napada: Napadi se dešavaju brzo zbog kratkih vremenskih intervala u mreži.



Napadi na poverljivost podataka

- **Prisluškivanje**:
- Napadač presreće podatke između vozila, poput lokacija i poruka upozorenja.

- **Krađa identiteta**:
- Zlonamerna osoba može preuzeti identitet vozila i slati lažne informacije.

- **Uticaj na privatnost**:
- Mogućnost praćenja kretanja vozila i vozača.

Program: ERASMUS-EDU-2022-CBHE-STRAND-2
Project number: 101082860

Funded by
the European Union

Napadi na integritet podataka

•**Lažne poruke**: Napadači mogu poslati lažne informacije, poput lažnog upozorenja na nesreću, što može izazvati konfuziju.

•**Manipulacija podacima**: Izmena podataka o saobraćajnim uslovima može dovesti do pogrešnih odluka vozača ili sistema.

•**Uticaj na koordinaciju vozila**: Pogrešni podaci mogu uzrokovati sudare i zagušenja.

Napadi na dostupnost

•Denial-of-Service (DoS) napadi: Preopterećuju mrežu velikim brojem lažnih zahteva, što blokira komunikaciju između vozila.

•Distributed Denial-of-Service (DDoS) napadi: Koordinisani napadi sa više izvora, čineći mrežu neupotrebljivom.

•Uticaj na saobraćaj: DoS napadi mogu izazvati kašnjenja, smanjenje bezbednosti i povećanje gužvi.

Napadi zasnovani na identitetu

•Sybil napadi: Napadač kreira više lažnih identiteta kako bi preuzeo kontrolu nad mrežom.

•Lažno predstavljanje: Napadač koristi identitet legitimnog vozila da bi poslao lažne podatke.

•Uticaj: Sybil napadi mogu ometati sistem navigacije i donošenje odluka u mreži.

Izazovi sa autentikacijom i autorizacijom

•Autentifikacija: Kako osigurati da komunikacija dolazi od pravog izvora?

•Autorizacija: Ko ima pravo pristupa određenim podacima ili funkcijama?

•Problemi: Kompleksni sistemi za autentifikaciju mogu usporiti komunikaciju, što je kritično u VANET mrežama.

Kriptoanaliza u VANET mrežama

•Slabosti šifrovanja: Neodgovarajući ili zastareli algoritmi mogu omogućiti napadačima da dešifruju podatke.

•Napadi na ključeve: Krađa ili kompromitovanje kriptografskih ključeva ugrožava bezbednost sistema.

•Balans performansi i bezbednosti: Kompleksniji algoritmi mogu usporiti komunikaciju, što je neprihvatljivo u realnom vremenu.

Zaštita privatnosti vozača

•Praćenje lokacije: Napadači mogu pratiti kretanje vozila i analizirati navike vozača.

•Neovlašćena identifikacija: Privatni podaci vozača mogu biti otkriveni trećim stranama.

•Rešenja: Korisiti metode anonimizacije i enkripcije.

Uloga veštačke inteligencije u prevenciji napada

•Detekcija anomalija: AI može prepoznati neobične obrasce u mrežnom saobraćaju i označiti ih kao potencijalne pretnje.

•Prediktivna analiza: Predviđanje napada na osnovu istorijskih podataka.

•Autonomni odgovor: AI sistemi mogu automatski reagovati na pretnje i prilagoditi mrežne parametre.

Zaključak

•VANET mreže imaju ogroman potencijal za unapređenje bezbednosti i efikasnosti u saobraćaju.

•Bezbednosni izazovi: I dalje postoje značajni problemi koji moraju biti rešeni, naročito u oblasti zaštite podataka i autentifikacije.

•Pogled u budućnost: Sa napretkom tehnologije, očekuje se veća integracija VANET mreža u svakodnevni saobraćaj.