UNIVERZA V LJUBLJANI
FAKULTETA ZA RAČUNALNIŠTVO IN INFORMATIKO

Darko Gliha

APLIKACIJSKA VARNOST V OMREŽJIH VOZIL

DIPLOMSKO DELO
VISOKOŠOLSKEGA STROKOVNEGA ŠTUDIJA

Mentor: doc. dr. Mojca Ciglarič

Ljubljana, 2011

Univerza
v Ljubljani

Fakulteta za računalništvo
in informatiko

Tržaška 25
1000 Ljubljana, Slovenija
telefon: 01 476 84 11
faks: 01 426 46 47
www.fri.uni-lj.si
e-mail: dekanat@fri.uni-lj.si

Št. naloge: 00118/2011
Datum: 05.04.2011

Univerza v Ljubljani, Fakulteta za računalništvo in informatiko izdaja naslednjo nalogo:

Kandidat: **DARKO GLIHA**

Naslov: **APLIKACIJSKA VARNOST V OMREŽJIH VOZIL**
APPLICATION SECURITY IN VEHICULAR NETWORKS

Vrsta naloge: Diplomsko delo visokošolskega strokovnega študija prve stopnje

Tematika naloge:

Naredite pregled žičnih, brezžičnih in mobilnih tehnologij, ki se uporabljajo za komunikacijo v omrežjih vozil. Nato analizirajte aplikacije, za katere je najbolj verjetno, da se bodo uporabljale v tovrstnih omrežjih. Preučite njihove varnostne izzive in zahteve. Komentirajte, kakšne posledice imajo lahko kopromisi glede razpoložljivosti, zaupnosti, integritete sporočil ipd. Možne napade klasificirajte glede na aplikacije in vrste napadalcev ter opišite anatomijo in posledice izbranih vrst napadov. Delo zaključite s pregledom možnih načinov obrambe in varovanja omrežij vozil.

Mentor:
M. Ciglarič
doc. dr. Mojca Ciglarič

Dekan:
prof. dr. Nikolaj Zimic

Fakulteta za računalništvo in informatiko • UNIVERZA V LJUBLJANI • 2

I Z J A V A O A V T O R S T V U

diplomskega dela

Spodaj podpisani **Darko Gliha**,

z vpisno številko **63970048**,

sem avtor diplomskega dela z naslovom:

Aplikacijska varnost v omrežjih vozil

S svojim podpisom zagotavljam, da:

- sem diplomsko delo izdelal samostojno pod mentorstvom (naziv, ime in priimek)

  doc. dr. Mojce Ciglarič

- so elektronska oblika diplomskega dela, naslov (slov., angl.), povzetek (slov., angl.) ter ključne besede (slov., angl.) identični s tiskano obliko diplomskega dela

- soglašam z javno objavo elektronske oblike diplomskega dela v zbirki »Dela FRI«.

V Ljubljani, dne 1.6.2011 Podpis avtorja:

ZAHVALA

Zahvaljujem se mentorici doc. dr. Mojci Ciglarič za njeno pomoč pri izbiri teme in za strokovno pomoč ter nasvete pri izvedbi diplomske naloge.

Posebna zahvala gre moji družini za moralno podporo pri dokončanju študija.

KAZALO VSEBINE

SEZNAM UPORABLJENIH KRATIC

CAN Controller area network	Upravljalec žičnega avtomobilskega omrežja
HSUPA High Speed Uplink Packet Access	Hitri prenos paketnih podatkov v smeri od uporabnika
IEEE Institute of Electrical and Electronics Engineers	Inštitut inženirjev elektrotehnike in elektronike
IP Internet Protocol	Internetni protokol
ITS Intelligent Transport System	Inteligentni transportni sistem
MAC Media Access Controll	Nadzor dostopa do medija
MANET Mobile Ad-hoc Network	Mobilno ad-hoc omrežje
MBWA Mobile Broadband Wireless Access	Mobilni širokopasovni brezžični dostop
OBU On Board Unit	Naprava v vozilu
OSI Open Systems Interconnection	Referenčni model za implementacijo komunikacijskih standardov
RSU Road Side Unit	Obcestna naprava
TDMA Time Division Multiple Access	Časovna razdelitev večkratnega dostopa
UMTS Universal Mobile Telecommunications System	Univerzalni mobilni telekomunikacijski sistem
V2I Vehicle to Infrastructure	Komunikacija vozila z omrežjem
V2V Vehicle to Vehicle	Komunikacija med vozili
VANET Vehicular Ad-hoc Network	Ad-hoc omrežje vozil
VSAT Very Small Aperture Terminal	Zelo majhna naprava v vozilu
WEP Wired Equivalent Privacy	Zasebnost kot v žičnem omrežju
Wi-Fi	Blagovna znamka združenja Wi-Fi
WiMAX Worldwide Interoperability for Microwave Access	Brezžični širokopasovni prenos podatkov
WPA Wi-Fi Protected Access	Zaščiten brezžični dostop

POVZETEK

Potrebe po informacijah se iz leta v leto povečujejo. Zato je ključno, da informacijo dobimo takoj, ko jo potrebujemo. V tej diplomski nalogi sem se usmeril na področje omrežja vozil. Omrežja vozil so v osnovi podobna vsem ostalim fiksnim omrežjem, z njimi si delijo precej komponent, imajo pa tudi nekatere bistvene razlike. Med te razlike štejemo predvsem različne senzorje, ki jih najdemo v vozilih ter način dostopa do omrežja, ki se povečini dogaja med vožnjo pri višjih hitrostih.

Na začetku diplomske naloge bom predstavil različne tehnologije, ki skrbijo za delovanje takega omrežja in tudi različne možne postavitve takšnega omrežja. V osrednjem delu se bom nato posvetil aplikacijam, zaradi katerih se takšna omrežja sploh razvijajo. Tu bom predstavil različne skupine aplikacij.

Naslednje poglavje diplomske naloge bom namenil ključnemu vidiku v omrežju vozil, to je varnost. Predstavil bom različne varnostne izzive in zahteve iz vidika načrtovanja takega omrežja, kot tudi varnostne zahteve iz vidika aplikacij.

Na koncu diplomske naloge bom predstavil še različne možne napade na omrežja vozil in aplikacije, ki jih v teh omrežjih uporabljamo. V tem poglavju bom tudi predstavil različne možne tipe napadalcev. Diplomsko delo bom zaključil z nekaj ukrepi, ki bi jih lahko sprejeli za višjo raven varnosti in zaščito pred napadalci.

Ključne besede: omrežje vozil, napadi, aplikacije v omrežju vozil

ABSTRACT

Information needs are increasing from year to year. It is therefore crucial that we obtain information as soon as the need arises. The focus of my thesis shall concentrate on the area of vehicular networks. Vehicular networks are essentially similar to all other fixed networks: they share some components, but also have some significant differences. The main differences include various sensors, which are found in vehicles and the way nodes connect to the network, which mainly occurs when travelling at higher speeds.

In the first part of this work I will list various technologies which enable functioning of such networks, as well as their different possible layouts. In the central part, I will focus on applications that drive such networks to evolve. Here I will also present a variety of such applications.

I will then dedicate the following chapter of this thesis to security, a key aspect of the vehicular network. I will present a range of security challenges and requirements in terms of network planning, as well as safety requirements with regards to applications.

Finally, I will present the different possible attacks on vehicular networks and applications used in this type of network, and define attacker types. The work concludes with advice on countermeasures that could be taken to ensure higher level of security and more resilience against attackers.

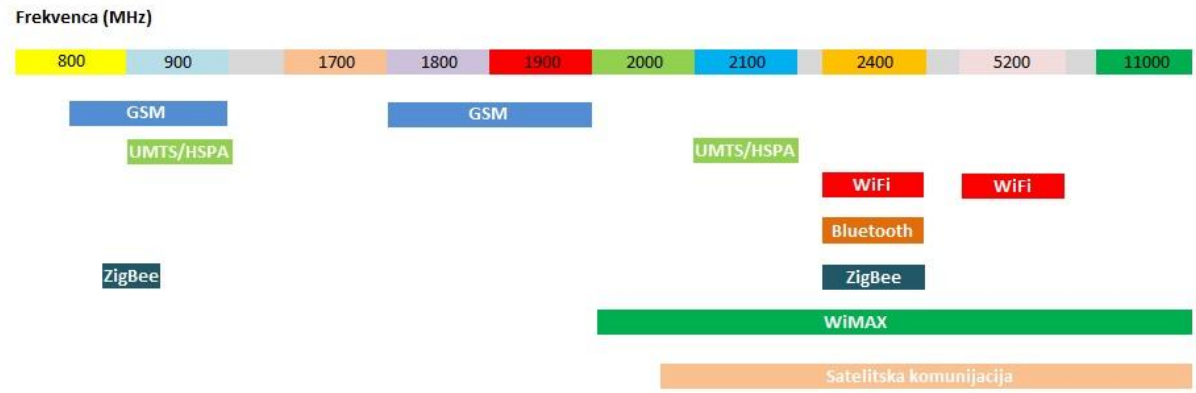
Key words: vehicular network, attacks, applications in vehicular network

1. PREGLED TEHNOLOGIJ ZA OMREŽJA VOZIL

Aplikacije v vozilih bodo gonilna sila pri razvoju in implementaciji omrežja za komuniciranje vozil. Z njimi bomo lahko nadzirali delovanje vozila, okolice, kot tudi sprejemali koristne informacije iz okolice. S tem bomo lahko zagotovili varnost potnikov ter večje udobje med potovanjem. Za delovanje omrežja bodo ključne brezžične tehnologije, ki jih danes že poznamo ter tudi tiste, ki so še v razvoju. V nadaljevanju poglavja bom predstavil tehnologije, ki so potrebne, da postavimo omrežje vozil.

Tehnologije dostopa do omrežja vozil lahko razdelimo na štiri sklope:

- žične tehnologije za uporabo v vozilih,
- brezžične tehnologije za uporabo v vozilih,
- brezžične tehnologije za dostop do infrastrukture,
- mobilna omrežja.



Slika 1 – Frekvenčni spekter tehnologij

1.1. Žične tehnologije za uporabo v vozilih

1.1.1. Controller area network

CAN (ali CAN-bus) je standard, ki omogoča komunikacijo individualnih sistemov in senzorjev med seboj, brez uporabe centralnega računalnika. Razvoj standarda je leta 1983 pričelo podjetje Bosch, v uporabo pa je prišel leta 1987, ko sta prve kontrolne čipe predstavila Intel in Philips. Leta 1991 je podjetje Bosch predstavilo novo različico standarda CAN 2.0. Čeprav je bil CAN sprva namenjen uporabi v vozilih, se danes uporablja tudi v letalih, industrijskih ter medicinskih napravah. Zaradi patenta, ki ga ima podjetje, morajo za uporabo le-tega proizvajalci naprav, ki delujejo na tem standardu, plačevati licenčnino.

Princip delovanja je preprost. Vsako priključeno vozlišče lahko pošilja in sprejema sporočila, vendar ne istočasno. Sporočilo vsebuje ID, ki ponazarja prioriteto sporočila, dodano pa mu je še do osem podatkovnih bajtov. Tipično so na vodilo priključeni različni senzorji, ki pa niso priključeni direktno na vodilo, pač pa preko krmilnika CAN.

Če je vodilo prosto, lahko z oddajanjem sporočila prične katerokoli vozlišče. Če z oddajanjem sporočila pričneta hkrati dve vozlišči, bo prevladalo sporočilo vozlišča, ki ima višjo številko ID. S tem se bo oddalo le najbolj pomembno sporočilo.

Vsako vozlišče potrebuje:

- Gostiteljski procesor
  Gostiteljski procesor se odloči, kaj prejeto sporočilo pomeni, hkrati pa skrbi še za sporočila, katera želi sam oddati. Nanj so lahko priključeni različni senzorji, kontrolne enote in razna sprožila.
- Krmilnik CAN
  Pri prejemanju sporočila se le-ta iz vodila prenese na krmilnik CAN, ko je sporočilo popolno, pa je na voljo vsem gostiteljskim procesorjem. Pri pošiljanju gostiteljski procesor sporočilo zapiše v krmilnik CAN, le-ta pa nato poskrbi za prenos sporočila do vmesnika.
- Oddajnik/Sprejemnik
  Če je le možno, je zahteva, da je oddajnik/sprejemnik integriran v krmilnik CAN. Pri sprejemanju poskrbi za pretvorbo signalov iz vmesnika v obliko, ki je razumljiva krmilniku CAN. Pri pošiljanju pretvori signal krmilnika CAN v obliko, ki je primerna za prenos po vodilu.

Hitrosti do 1 Mbit/s so možne pri omrežju dolžine do 40 m, zmanjšanje hitrosti pa omogoča uporabo tudi na daljše razdalje. CAN protokol je standardiziran in je opisan v standardu ISO 11898-1.

CAN sam po sebi ne omogoča varnostnih mehanizmov, pričakuje se, da bodo uporabljene aplikacije same poskrbele za potrebne varnostne mehanizme (npr. poskrbele za dokazovanje pristnosti). Če se varnostni vidik prezre, lahko to privede do različnih napadov, vendar pa mora napadalec najprej pridobiti fizični dostop do vodila, šele nato lahko zlonamerno kodo prenese na samo vodilo.

1.2. Brezžične tehnologije za uporabo v vozilih

1.2.1. Bluetooth

Bluetooth je varna brezžična tehnologija, ki omogoča povezovanje različnih naprav v varno osebno mobilno omrežje. Specifikacija je bila prvič predstavljena leta 1994 s strani podjetja Ericsson. Leta 1998 je delo nadaljevala skupina več podjetij, ki so ustanovile posebno skupino, imenovano SIG (Bluetooth special interest group), ki danes šteje preko 13.000 članov. Bluetooth deluje v frekvenčnem pasu 2,4 GHz. Obstaja več različic specifikacije:

- 1.0 in 1.0B – omogoča hitrosti do 1 Mbit/s
- 1.1 - omogoča hitrosti do 1 Mbit/s
- 1.2 – omogoča hitrosti do 1 Mbit/s
- 2.0 EDR – omogoča hitrosti do 3 Mbit/s
- 2.1 EDR - omogoča hitrosti do 3 Mbit/s
- 3.0 HS – omogoča hitrosti do 24 Mbit/s
- 4.0 – omogoča hitrosti do 24 Mbit/s

Glavna slabost bluetootha je dejstvo, da za povezavo v omrežje potrebujemo precej časa, saj je potrebno naprave pred uporabo spariti. Dobra lastnost je, da se naprave, ko so v dosegu omrežja, nanj samodejno povežejo.

Obstajajo trije razredi, ki pogojujejo največjo razdaljo, na kateri delujejo naprave::

- razred 1 – omogoča oddaljenost do 100 m in moč oddajanja do 100 mW
- razred 2 – omogoča oddaljenost do 10 m in moč oddajanja do 2,5 mW
- razred 3 – omogoča oddaljenost do enega metra in moč oddajanja do 1 mW

V teoriji naprava razreda 1 omogoča razdalje do 100 m, vendar so različne praktične rešitve pokazale, da je težava že s komuniciranjem dveh naprav, kjer je ena nameščena na začetek avtomobila, druga pa na konec. Bluetooth ni najbolj primeren za komuniciranje vozila z omrežjem, bolj je uporaben pri povezovanju različnih naprav v samem vozilu.

Bluetooth omogoča več varnostnih mehanizmov, proizvajalci opreme se sami odločijo, katerega izmed njih bodo uporabili. V skorajda vseh primerih se odločijo za uporabo sistema s parjenjem naprav, saj le-ta omogoča prenos podatkov med povezanimi napravami brez dodatnega potrjevanja. Če želi povezavo vzpostaviti neavtorizirana naprava, mora uporabnik le-to vedno potrditi, hkrati pa tudi določiti, ali bo novo napravo dodal med avtorizirane naprave ali ne. Zaradi varnosti lahko tudi skrijemo vidnost naprave, pri tem se lahko avtorizirane naprave še vedno povežejo med seboj. Slednje je zaradi varnosti smiselno uporabiti tudi v vozilih.

1.2.2. ZigBee

ZigBee je brezžična tehnologija, razvita kot odprtokodni standard, ki se opira na standard IEEE 802.15.4-2003. Protokol so ratificirali člani organizacije ZigBee Alliance, v kateri je združenih preko 300 različnih podjetij. Razvit je bil zaradi zahteve po nižjih stroških izdelave naprav ter čim manjši porabi energije. ZigBee deluje v treh frekvenčnih pasovih in sicer v 2,4 GHz (16 kanalov), ki je namenjen svetovni uporabi, 915 MHz (12 kanalov), ki se uporablja v Ameriki ter 868 MHz (en kanal), ki se uporablja v Evropi. Hitrost prenosa je do 250 kbit/s (do 40 kbit/s pri 915 MHz in do 20 kbit/s pri 868 MHz), razdalja prenosa je do 75 m pri osnovni specifikaciji in do 1500 m pri specifikaciji ZigBee Pro.

Zaradi nizkih stroškov je protokol primeren za uporabo v nadzornih aplikacijah in brezžičnih napravah, majhna poraba energije pa mu omogoča daljše delovanje s fizično manjšimi baterijami. Velika prednost pred ostalimi tehnologijami je sposobnost aktivacije iz spanja v

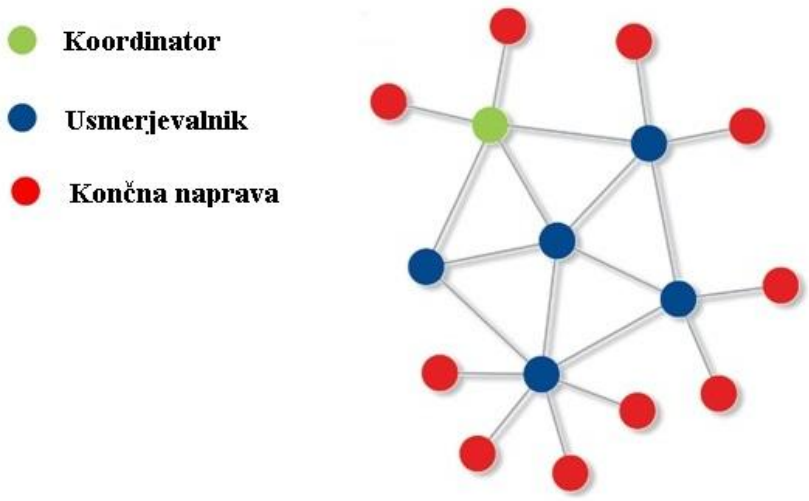
manj kot 30 ms (za primer: bluetooth potrebuje za to več kot 3 s). To posledično tudi omogoča manjšo porabo energije. ZigBee omogoča tudi popolno omrežno povezljivost.

ZigBee zveza je izdala več različnih specifikacij, ki proizvajalcem naprav omogočajo lažjo implementacijo v potrošniške izdelke. Specifikacije so:

- ZigBee avtomatizacija zgradb,
- ZigBee daljinsko upravljanje,
- ZigBee pametna energija,
- ZigBee zdravstvo,
- ZigBee avtomatizacija doma,
- ZigBee vnosne naprave,
- ZigBee storitve na drobno,
- ZigBee telekomunikacijske storitve,
- ZigBee 3D.

V vsakem omrežju ZigBee imamo lahko do 65.000 naprav. Poznamo tri vrste naprav:

- Koordinator
  Koordinator je najbolj napredna naprava, saj mora znati vzpostaviti omrežje, hraniti podatke o omrežju, dodajati naprave in usmerjati podatke. V omrežju je samo en koordinator.
- Usmerjevalnik
  Usmerjevalnik ravno tako omogoča usmerjanje prometa, nanj priklopimo končno napravo ali drug usmerjevalnik.
- Končna naprava
  Končna naprava se poveže na usmerjevalnik ali koordinator, nanjo pa priključimo različne naprave, kot so npr. senzorji ali releji.



Slika 2 – Primer povezovanja ZigBee naprav

1.3. Brezžične tehnologije za dostop do infrastrukture

1.3.1. Satelitska komunikacija

Satelitska komunikacija v osnovi omogoča enosmerno komuniciranje. Je zelo razširjena tehnologija, saj lahko s samo nekaj sateliti pokrijemo praktično celotno površino zemlje. Poznana je iz uporabe GPS sistema, manj znano pa je, da omogoča tudi dvosmerno komuniciranje. To nam omogoča majhna prenosna naprava VSAT. V primeru oddajanja naprave signal prejme satelit, nato pa ga posreduje zemeljski postaji. Če poteka komunikacija med dvema napravama VSAT signal potuje preko zemeljskih postaj, šele nato pa se pošlje do satelita. Hitrosti prenosa so pri tej vrsti komunikacije med 64 in 128 kbit/s pri prenosu k satelitu, ter do 438 kbit/s pri prenosu k uporabniku. Večina satelitov deluje na frekvenci višji od 2 GHz, za delovanje pa med oddajnikom in sprejemnikom ne sme biti ovir.

Čeprav je satelitska komunikacija prisotna povsod, pa je zaradi nizkih hitrosti prenosa in visokih odzivnih časov skorajda nikoli ne uporabimo za dvosmerno komunikacijo. Bolj je primerna za enosmerni prenos podatkov.

1.3.2. IEEE 802.11 Wi-Fi

IEEE 802.11 je skupek standardov, ki opredeljujejo lokalno brezžično omrežje za komunikacijo naprav med seboj. Njegove korenine segajo 25 let nazaj, ko je Ameriški svet za telekomunikacije sprejel sklep o prepovedi dostopa do razpoložljivih radijskih frekvenc. Danes poznamo več podstandardov, ki so se razvili tekom let:

- 1997 – osnovni 802.11-1997,
- 1999 – 802.11a in 802.11b,
- 2003 – 802.11g,
- 2009 – 802.11n.

Najbolj znan predstavnik je standard 802.11b. Deluje na frekvenci 2.4 GHz in omogoča najvišjo hitrost 11 Mbit/s. Standard 802.11g, ki je bil predstavljen kasneje, omogoča že precej višje hitrosti in sicer do 54 Mbit/s, deluje pa ravno tako na frekvenci 2,4 GHz. Manj uporabljen standard 802.11a pa je s strani uporabe v vozilih precej uporaben. V osnovi je podoben standardu 802.11g, omogoča hitrosti do 54 Mbit/s, vendar deluje na precej višji frekvenci 5,2 GHz. To pomeni, da je podvržen manj motnjam okolice, saj le redke uporabniške naprave uporabljajo ta spekter. Zadnji večji popravek je standard 802.11n, ki za delovanje uporablja »multiple input multiple output« (MIMO) tehnologijo, kar omogoča hitrosti do 150 Mbit/s in delovanje na frekvenci 2,4 in 5 GHz.

Vse različice protokola 802.11 uporabljajo prilagajanje hitrosti prenosa, kjer je hitrost pogojena s kvaliteto signala. Tako bi v primeru vožnje mimo dostopne točke le-ta moč signala povečala na najvišjo vrednost, dokler je vozilo v njenem dosegu. Ko bi vozilo zapustilo območje pokritosti te dostopne točke, pa bi se moč oddajanja ustrezno znižala. S poznavanjem dosega bi lahko dostopne točke hitreje menjale hitrosti prenosa, kar bi posledično omogočilo večje število prenesenih podatkov.

1.3.3. IEEE 802.16 WiMax

Standard 802.16 WiMax je zasnovan kot fiksno širokopasovno brezžično omrežje. Za delovanje večinoma uporablja frekvenčni razpon od 5 do 6 GHz, čeprav standard dovoljuje uporabo med 2 in 11 GHz. Njegov glavni namen je ponujati višje hitrosti prenosa na večje razdalje, do 50 km. Deluje lahko na različnih terenih. V teoriji omogoča hitrosti prenosa do 72 Mbit/s, vendar to velja le za naprave, ki so blizu dostopnih točk. Z oddaljevanjem od dostopne točke se hitrost ustrezno zmanjšuje. Ime WiMax so določili pri leta 2001 ustanovljenem WiMax Forumu, v okviru katerega deluje preko 420 podjetij, ki se ukvarjajo z razvojem in testiranjem sistemov, ki uporabljajo standard 802.16. V uporabi sta predvsem dve podimeni:

- 802.16-2004 (ali 802.16d) je poimenovan Fixed WiMax,
- 802.16e-2005 (ali 802.16e) je poimenovan Mobile WiMax.

Ker Fixed Wimax ne omogoča nikakršne podpore za mobilnost, so standardizirali Mobile WiMax, ki mobilnost podpira in dovoljuje uporabo do hitrosti 160 km/h. Mobile WiMax ima največ komercialnega interesa, saj se ga po svetu najbolj uporablja.

1.3.4. 802.20 MBWA

Leta 2002 je IEEE pričela s procesom standardizacije za mobilni širokopasovni brezžični dostop. Cilj je bil omogočiti IP brezžični vmesnik, ki bi deloval na frekvenci pod 3,5 GHz in pri hitrostih vozil do 250 km/h, ob tem pa vseeno omogočal hitrosti večje od 1 Mbit/s na uporabnika. Najvišja teoretična hitrost prenosa MBWA je preko 80 Mbit/s. Prvotni namen je bila zamenjava mobilnega sistema, ki je IP promet pošiljal preko sistema, narejenega za govor in ki ni omogočal višjih hitrosti. Tudi druge tehnologije, kot je npr. WiMax, prvotno niso bile narejene za uporabo v vozilih. Vseeno so cilji tehnologij Mobile WiMax in MBWA dokaj podobni. Standard je bil dokončno potrjen junija 2008.

1.4. Mobilna omrežja

1.4.1. GSM/GPRS/EDGE

GSM je svetovno najbolj razširjen mobilni standard, saj se ocenjuje, da ga uporablja kar 80 odstotkov mobilnega trga. Smatra se za drugo generacijo mobilnega omrežja. Začetki uporabe segajo v leto 1991, deluje pa na frekvenci 900 in 1800 MHz. Redko se uporablja tudi frekvenca 850 in 1900 MHz. Prenos poteka digitalno, poleg govora pa omogoča tudi prenos podatkov. Za prenos podatkov poskrbi standard GPRS, ki deluje s hitrostjo med 56 in 114 kbit/s, odvisno od števila uporabljenih kanalov. Večje hitrosti so možne z uporabo tehnologije EDGE, ki je bila prvič predstavljena leta 2003. Temelji na enakem principu kot GPRS, vendar uporablja izboljšane metode kodiranja in pošiljanja in zato omogoča višje hitrosti podatkov kot GPRS. Hitrost je odvisna od števila uporabljenih kanalov pri multipleksiranju (uporablja se TDMA multipleksiranje) in je lahko največ do 473,6 kbit/s pri uporabljenih osmih kanalih. EDGE ne potrebuje novega omrežja, pač pa le nadgradnjo obstoječih baznih postaj.

GSM tehnologija je primerna zaradi nizke frekvence delovanja, saj omogoča večjo pokritost s signalom. Vseeno pa aplikacije, ki prenašajo večje število podatkov, za GSM niso primerne, zato je za njih potrebno poseči po omrežju tretje generacije kot sta UMTS in HSPA.

1.4.2. UMTS/HSPA

UMTS je omrežje tretje generacije, ki za svoje delovanje potrebuje novo opremo in nove frekvence. Tipično se v Evropi uporablja frekvenčni spekter 2100 MHz. UMTS ni zamenjava za starejše standarde, pač pa le njihova nadgradnja. Operaterjem so na voljo trije različni standardi, najširše pa je uporabljen standard W-CDMA. Ta omogoča, da vsi uporabniki enega operaterja oddajajo na isti frekvenci, vendar ima vsak uporabnik različno razprševalno kodo. W-CDMA je precejšen porabnik frekvenčnega spektra, saj za delovanje uporablja široke dvojne 5 MHz kanale. Ključnega pomena je tudi prilagajanje oddajne moči, saj s tem dosežemo, da naprave bližje bazni postaji oddajajo z manjšo močjo. Tudi sama bazna postaja prilagaja moč glede na potrebe odjemalcev. Hitrosti, ki jih UMTS trenutno omogoča, so 384 kbit/s. Višje hitrosti omogoča tehnologija HSPA, točneje HSDPA in HSUPA.

HSDPA omogoča hitrejši prenos podatkov k uporabniku. V teoriji podpira HSDPA hitrosti do 14,4 Mbit/s, v praksi pa so hitrosti odvisne od omrežja operaterja in so trenutno nekje na 7,2 Mbit/s. Za nadgradnjo UMTS omrežja je dovolj le posodobitev programske opreme, zato je bilo na to tehnologijo nadgrajenih že preko 90 % vseh UMTS omrežij. HSUPA omogoča hitrejši prenos podatkov od uporabnika. V teoriji podpira HSUPA hitrosti do 5,76 Mbit/s, vendar mobilni operaterji trenutno uporabljajo le hitrost do nekje 1,4 Mbit/s.

Lani se je začela uporabljati tudi evropska direktiva o mobilni telefoniji, ki frekvenčni spekter okrog 900 MHz sprošča tudi za druge tehnologije. Ta spekter bi lahko operaterji uporabili za UMTS/HSPA, saj omogoča večji doseg glede na frekvenčni spekter 2100 MHz, ki je navadno uporabljena v gosto poseljenem območju. Z uporabo frekvence 900 MHz bi lahko dosegli večje območje, tudi uporabo v hribovitem področju, ki je tipično za našo državo.

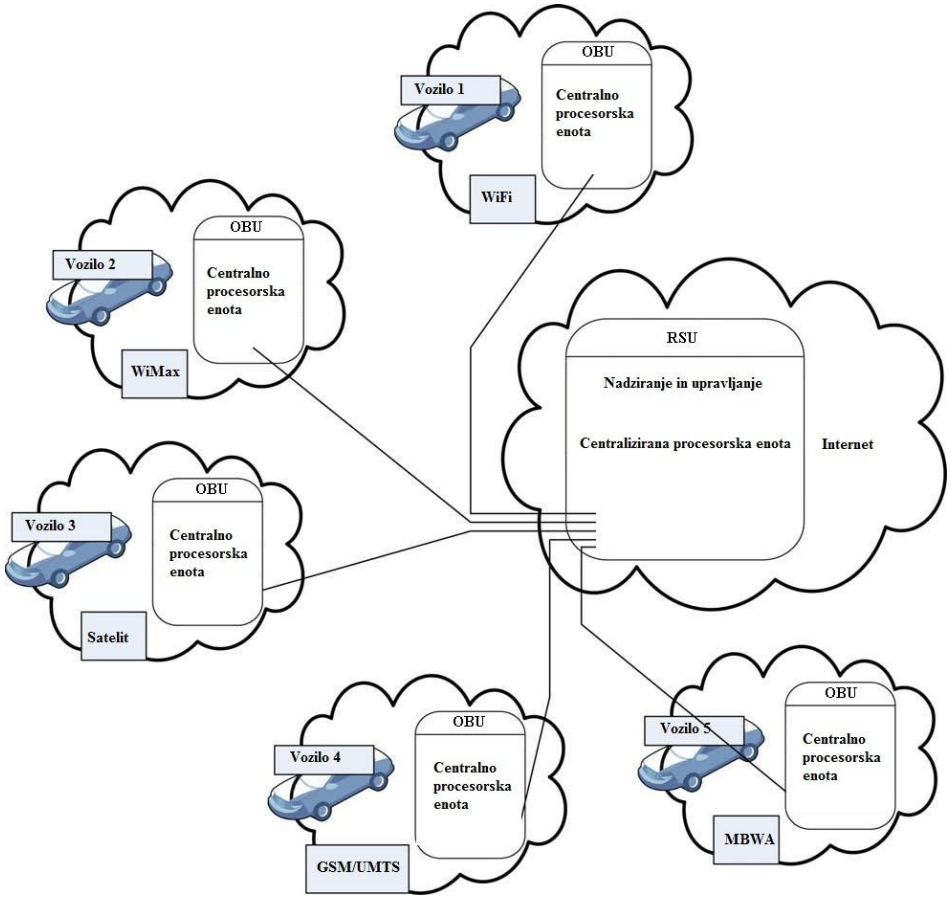
1.5. Pregled predstavljenih tehnologij

Karakteristike / Uporabljena tehnologija	Frekvenčni pas delovanja	Hitrost prenosa podatkov	Doseg	Osnovni namen
CAN	/	do 1 Mb/s	40 m +	avtomobilsko omrežje
Bluetooth	2,4 GHz	do 24 Mb/s	do 100 m	osebno omrežje
ZigBee	2,4 GHz 915/868 MHz	do 250 kb/s	do 75 m	osebno omrežje
Satelitska komunikacija	nad 2 GHz	do 438 kb/s	praktično neomejen	prenos slike in zvoka
Wi-Fi	2,4/5,2 GHz	150 Mb/s +	100 m +	fiksni internet
WiMax	2 – 11 GHz	do 72 Mb/s	do 50 km	mobilni internet
MBWA	pod 3,5 GHz	do 80 Mb/s	15 km +	mobilni internet
GSM/GPRS/EDGE	850/900/1800/1900 MHz	470 kb/s	1000 m +	mobilni internet
UMTS/HSPA	900/2100 MHz	14 Mb/s	1000 m +	mobilni internet

Tabela 1 – Pregled osnovnih specifikacij tehnologij omrežja

2. PREDSTAVITEV OMREŽJA VOZIL

Načrtovanje in implementacija kateregakoli omrežja naj kar se da uporablja že znane in preizkušene tehnologije. S tem se izognemo visokim stroškom postavitve opreme, hkrati pa je postavitev hitra in učinkovita. Vseeno pa morajo načrtovalci imeti v mislih bodoče nadgradnje in izboljšave.



Slika 3 – Arhitektura preprostega omrežja vozil

Omrežje vozil imenovano VANET je nova oblika omrežja, kjer vozila in bazne postaje oz. dostopne točke komunicirajo med seboj. Večinoma omrežja vsebujejo dve vrsti vozlišč in sicer dostopne točke ob cesti RSU ter dostopne točke v vozilih OBU. Obe vrsti naprav štejemo med naprave za namensko komunikacijo na kratke razdalje DSRC. Naprave DRSC delujejo v frekvenčnem pasu 5,9 GHz s pasovno širino 75 MHz v ZDA in 30 MHz v Evropi, doseg pa tipično znaša 1000 m. Omrežje mora omogočati tako privatno kot javno komunikacijo, vendar mora večjo prioriteto imeti javni promet, preko katerega aplikacije dobivajo informacije iz okolice. Omrežje vozil se tipično razvije pod okriljem inteligentnega transportnega sistema ITS. Ime inteligentni transportni sistem ITS se nanaša na željo dodati informacijo in komunikacijo transportnemu sistemu, torej vozilom in omrežju. S tem želimo izboljšati varnost v prometu, hkrati pa tudi zmanjšati prevozne čase in porabo goriva. ITS se razlikuje glede na vrsto tehnologije, ki jo uporablja, od preprostih sistemov, kot je satelitska

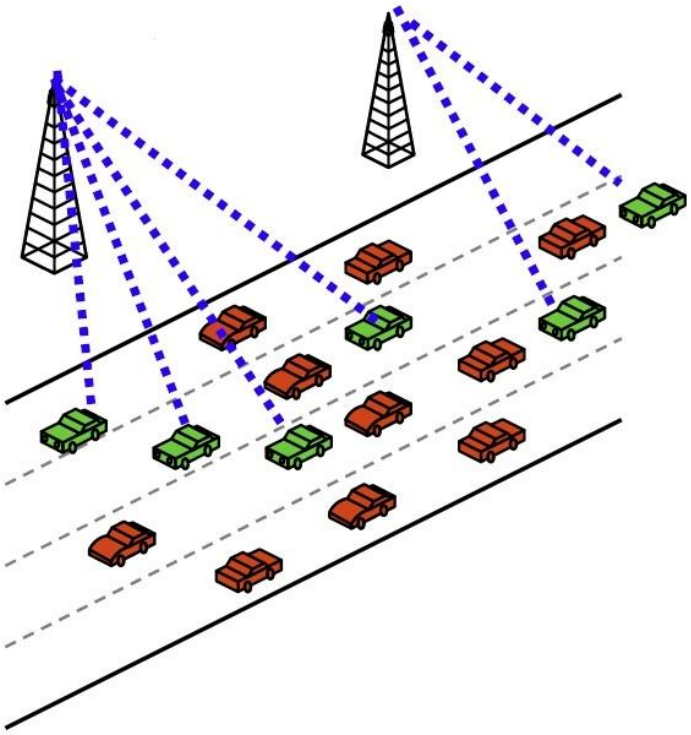
navigacija, signalizacija in hitrostne kamere do bolj specifičnih rešitev kot so informacije ostalih udeležencev v prometu.

Vedno predvidevamo, da ima vozilo, ki je del sistema ITS nameščeno potrebno strojno opremo. Vsako vozilo mora tako vsebovati:[8]

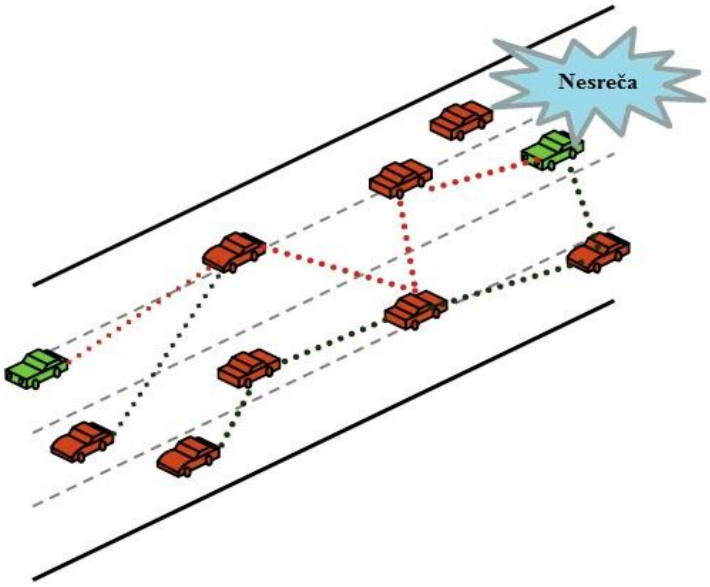
- centralno procesorsko enoto, ki skrbi za delovanje aplikacij in komunikacijskih protokolov,
- brezžični vmesnik, ki skrbi za oddajanje in sprejemanje podatkov,
- sprejemnik GPS, ki poskrbi za določanje natančne lokacije in časa,
- več senzorjev, ki spremljajo različne parametre,
- napravo, ki omogoča voznikov interakcijo s sistemom.

2.1. V2V in V2I omrežja

Poglavitna razlika med omrežjema V2V in V2I je način komuniciranja. Pri omrežju V2V komunicirajo med seboj vozila, pri omrežju V2I pa vozila komunicirajo z infrastrukturo. To pomeni, da s tem definiramo, kako se bodo podatki v omrežju prenašali. Najbolj učinkovita je kombinacija obeh načinov komuniciranja, t.i. V2V2I.

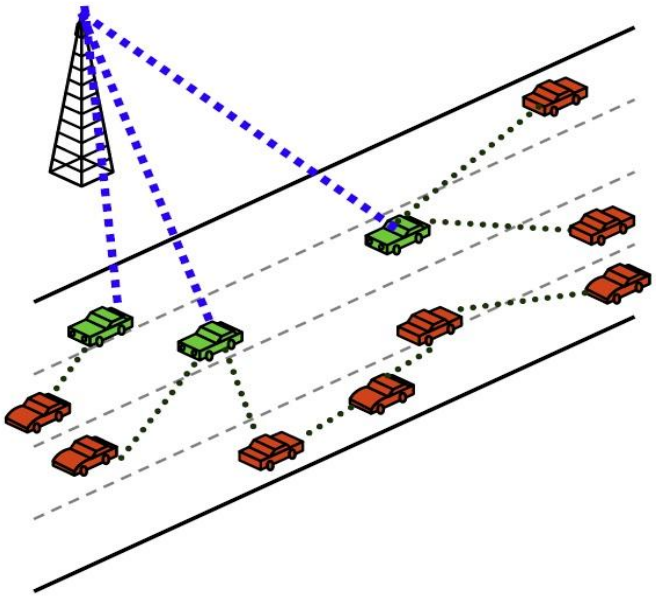


Slika 4 – Prenos podatkov v V2I omrežju

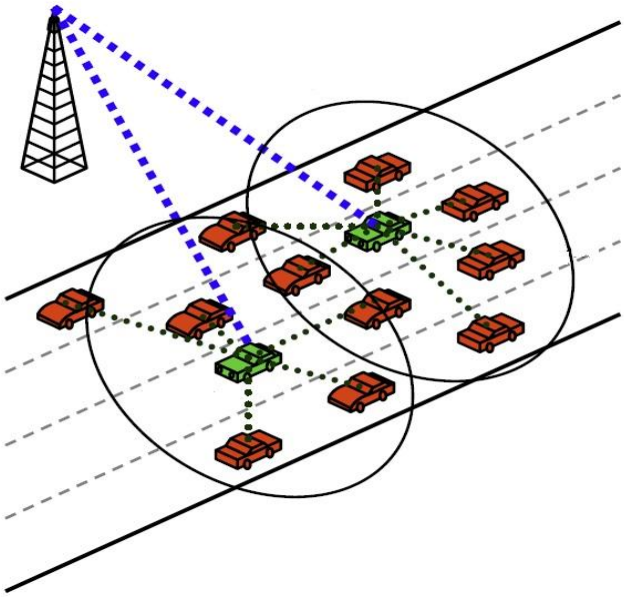


Slika 5 – Prenos podatkov v V2V omrežju

Prenos iz baznih postaj k vozilu je neposredni prenos in se uporablja tam, kjer so vozila v dosegu bazne postaje. Če se vozilo nahaja izven dosega bazne postaje se lahko uporabi t.i. multihop prenos. V tem primeru se informacija prenese iz bazne postaje v vozila, ki so v dosegu, le-ti pa nato poskrbijo za prenos v ostala vozila do končne točke. Možen pa je še prenos informacije iz bazne postaje do izbranega vozila posrednika, ki nato poskrbi za prenos do ostalih vozil v njegovem dosegu.



Slika 6 – Multihop prenos podatkov



Slika 7 –Prenos podatkov do posrednika

2.2. Naslavljanje

Večina aplikacij, ki jih bomo uporabljali potrebuje neke vrste naslavljanje. Ker so omrežja vozil povečini narejena na ad-hoc principu, lahko tu uporabimo enako naslavljanje, kot v fiksnih ad-hoc omrežjih:[8]

- Stalno naslavljanje: Vsako vozlišče ima stalno dodeljen naslov od trenutka, ko se priključi v omrežje. Le-to se uporablja za čas, ko je v omrežju.
- Lokacijsko naslavljanje: Vsako vozlišče se naslavlja glede na lokacijo. Ko se vozilo premika, se spreminja tudi naslov. Uporabimo lahko tudi dodatne atribute za naslavljanje (smer vožnje, tip vozila, identifikator ceste ...).

2.3. Vidiki načrtovanja omrežja vozil

Pri načrtovanju oblike omrežja vozil je potrebno imeti v mislih, da omrežje načrtujemo za aplikacije. Zato je potrebno pred načrtovanjem razmisliti o naslednjih izzivih:[9]

- Zakasnitev (Latenca)
  Najpomembnejši faktor pri pošiljanju sporočil je latenca, ki meri čas od trenutka oddaje sporočila do prihoda na cilj. V omrežjih vozil je latenca odvisna od oddaljenosti vozila od »nastanka nevarne situacije«. V klasičnih omrežjih je latenca velikosti nekaj 10 ms, v omrežjih vozil pa lahko ta številka drastično naraste zaradi

števila skokov v omrežju. V najslabših primerih bi lahko na razdalji 1000 m ta znašala tudi 10 s, kar je občutno preveč za varno uporabo aplikacij.

- Poznavanje sosednjih vozil
  V omrežjih vozil je poznavanje sosedov pomembno predvsem iz vidika usmerjanja prometa, kot tudi iz vidika aplikacij. Če npr. poznamo lokacijo vozila pred nami, lahko temu vozilu sporočimo, da mora zaradi nesreče takoj zmanjšati hitrost.
- Pametna izraba omrežja
  Problem v omrežjih vozil je število nepomembnih sporočil, ki jih vozilo sprejme. Navadno so to sporočila, ki se nanašajo na dogodke, ki so daleč izven dosega, ali pa je dogodek na nasprotnem voznem pasu avtoceste. Temu bi se lahko ognili z uporabo lokacije GPS pri aplikacijah.
- Simulacija različnih modelov
  Zaradi težavnega testiranja novih protokolov in modelov v delujočih omrežjih vozil je zelo pomembno, da se le-ti predhodno testirajo v simulatorju. Z njihovo uporabo lahko testiramo različne prometne situacije in kako se na njih odzivajo različne aplikacije. Vseeno pa simulacije ne podajo vedno prave rešitve, saj se te pokažejo šele kasneje, med uporabo aplikacije v prometu .
- Penetracija
  Eno večjih vprašanj pri varnosti v omrežjih vozil je število vozil, ki so opremljeni s tem sistemom. Če je število le-teh premajhno, lahko ogrozimo tudi posredovanje varnostnih sporočil v primeru, da obcestna infrastruktura ni dovolj pogosta.
- Stroški
  O stroških omrežja vozil se do sedaj še ni veliko govorilo. Če pogledamo, da je sistem, ki je vgrajen v vozilo, pravzaprav računalnik z omogočeno mrežno povezljivostjo ter dodanim sprejemnikom GPS, so stroški glede na prednosti pravzaprav zanemarljivi.

2.4. Posebnosti omrežja vozil

Omrežja vozil imajo določene lastnosti, zaradi katerih se razlikujejo od drugih oblik omrežij. Glavna lastnost, ki omrežja vozil loči od fiksnih omrežij, je mobilnost. Lastnosti, ki so unikatne omrežju vozil, so:[8]

- Skoraj neomejen dostop do energije
  Mobilne naprave se vseskozi soočajo s pomanjkanjem električne energije, ki jo potrebujejo za svoje delovanje. Ta težava pa v omrežju vozil ni tako izrazita, saj lahko vozilo samo priskrbi dovolj energije za delovanje komunikacijskih naprav.
- Večje računske sposobnosti
  Vozila si lahko med delovanjem zaradi večje moči omogočijo večjo računsko moč, sporočanje in zmogljivosti zaznavanja. Pri tem jim ni potrebno skrbeti za pomanjkanje energije.

- Predvidljiva mobilnost
  V klasičnih omrežjih je izredno težko napovedovati mobilnost vozlišč. V omrežjih vozil je predvidevanje mobilnosti preprosto, saj so vozila večinoma omejena na cestno infrastrukturo. Le-ta je že dodobra popisana s strani navigacijskih podjetij. Tako lahko bodočo lokacijo vozila predvidimo glede na podatke o povprečni in trenutni hitrosti vozila ter o podatkih o cesti, na kateri se vozilo nahaja.

Da bi omrežja vozil izkoristili do popolnosti, je potrebno upoštevati nekaj zahtevnih značilnosti, med katere spadajo:

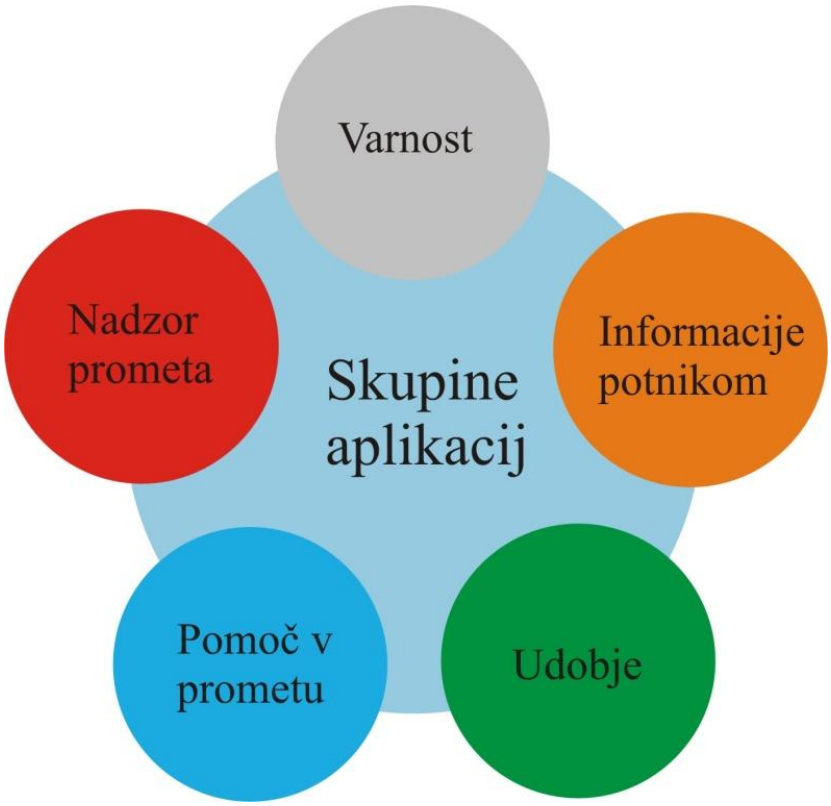
- Potencialno velik obseg
  Omrežja vozil se lahko za razliko od klasičnih omrežij raztegnejo čez celotno cestno infrastrukturo. V takem omrežju bi sodelovalo veliko število udeležencev.
- Visoka mobilnost
  Okolje, v katerem deluje omrežje vozil, je zelo dinamično in vključuje različne načine konfiguracije: zmogljivejši avtomobili lahko na avtocestah dosegajo hitrosti preko 200 km/h. Gostota vozlišč pri manj prometnih cestah je nekje do dve vozili na en km. V mestih je hitrost večinoma nizka, je pa zato gostota ostalih udeležencev precej višja, še posebno v prometnih konicah.
- Delitev omrežja
  Omrežja vozil bodo pogosto razdeljena. Dinamičnost prometa lahko privede do velikih vrzeli v redko poseljenih okoljih in s tem izoliranih skupin vozlišč.
- Topologija omrežja in povezljivost
  Ker se vozila v omrežju vozil premikajo in s tem spreminjajo svojo lokacijo, se topologija omrežja nenehno spreminja. Omrežje bo svoje cilje izpolnilo le, če bo zagotovljena obcestna infrastruktura, ter dovolj vozil, ki bodo opremljeni z brezžičnim sistemom.

3. APLIKACIJE V OMREŽJU VOZIL

V modernih vozilih se nahaja kopica senzorjev, ki skupaj s centralno procesorsko enoto skrbijo za varno delovanje vseh sklopov. Če te informacije povežemo z omrežjem in z drugimi vozili in jim dodamo še nekatere nove, bi lahko dobili sistem, ki bi reševal tudi človeška življenja. Vendar pa za uspešno komercialno uporabo takega omrežja potrebujemo aplikacije.

V omrežjih VANET se trend vrti okoli petih različnih tipov aplikacij in sicer varnost, informacije potnikom, nadzor prometa, pomoč v prometu in udobje pri vožnji. Kdaj bodo te aplikacije dodane v vozila, je težko napovedati, saj je življenjska doba novih modelov med 10 in 15 let, tako da bodo vozila, prodana letos, v uporabi še leta 2026. S tem pridemo do situacije, ko bo potrebno v obstoječa vozila namestiti dodatno opremo, ki bo omogočala komuniciranje z omrežjem.

V raziskavi, ki jo je izvedel Arhitecture Development Team so predstavili, da bodo v časovnem obdobju 15 let omrežja vozil zelo razširjena, kar bo še povečalo uporabnost aplikacij. Sodelovanje med vozili bo zmanjšalo vplive okolice in tudi znižalo število nesreč.

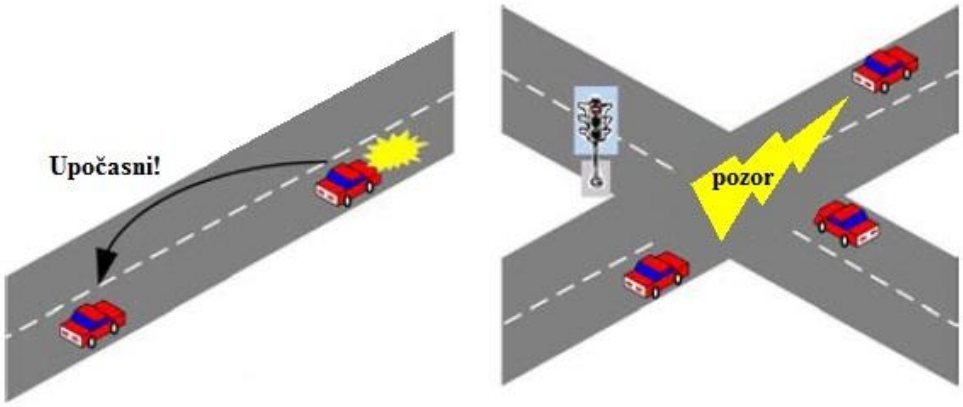


Slika 8 –Skupine aplikacij v omrežju VANET

3.1. Skupine aplikacij

3.1.1. Varnost

Varnost je v vseh pogledih izredno pomembna, varnostne aplikacije so narejene z namenom preprečevanja nesreč. Za dosego tega cilja so že bili predstavljeni sistemi za zaznavanje nesreč. Na avtocestah je največji problem nalet na spredaj počasno vozeče ali ustavljeno vozilo, kar ima lahko katastrofalne posledice. Z uporabo tehnologije za preprečevanje nesreč bi vozila med seboj komunicirala in nesreči bi se izognili. Podobno je tudi v križišču, ko udeleženec prevozi rdečo luč. Če bi uporabljali tehnologijo ITS, bi enoti v vozilu med seboj komunicirali in nesreči bi se izognili.



Slika 9 –Uporaba varnostnih aplikacij

Podoben sistem se lahko uporabi tudi za vse druge tipe prevoza. Če bi sistem zaznal, da se trku ne da izogniti, bi lahko samodejno poskrbel, da bi imel trk kar najmanjši učinek na udeležence (lahko bi samodejno sprožil zračne vreče). Seveda pa obstajajo določene omejitve. Sistem je uporaben le, če voznik dobi informacijo dovolj zgodaj in v realnem času. Ker gre za varnost je smiselno, da jo dobi vsako vozilo, ki se dogodku približuje. Smiselno je še, da informacijo o dogodku dobi le vozilo, ki se le-temu približuje in tisto vozilo, ki se od njega oddaljuje.

Varnostne aplikacije vsebujejo tri faze in sicer informacija, opozorilo in samodejna kontrola. Prva faza nikakor ne sme zmesti voznika med vožnjo, varnostna faza pa mora opozoriti voznika o prihajajoči nevarnosti. Zadnja faza vozniku odvzame kontrolo nad vozilom in samodejno ukrepa v primeru nevarnosti (če npr. voznik reagira prepozno). Od leta 2006 je visoka prioriteta na osmih varnostnih aplikacijah, ki bi po mnenju različnih organizacij pripomogle k izboljšanju varnosti.

Te aplikacije so:

- nadzor nad prometno signalizacijo,
- opozorilo hitrosti v ovinkih,

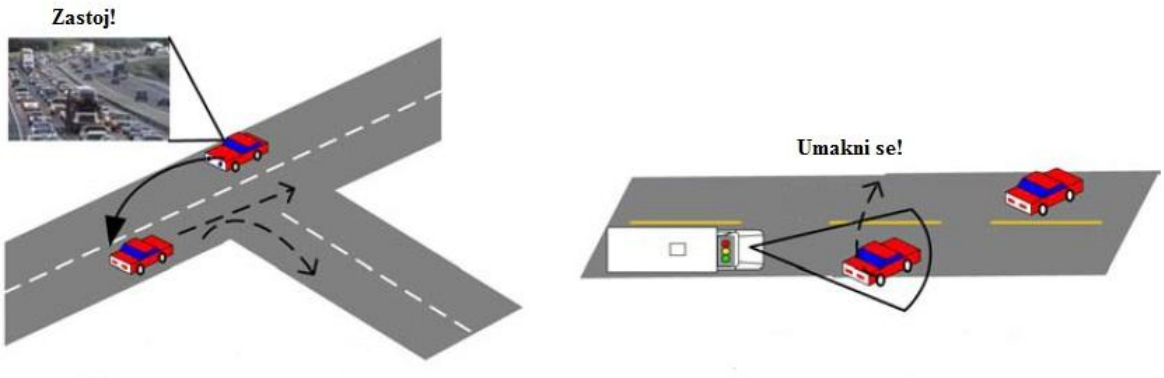
- zasilna zavorna signalizacija,
- zaznavanje trka,
- preprečevanje naleta na spredaj vozeče vozilo,
- pomoč pri zavijanju levo,
- opozorilo ob menjavi pasu,
- opozorilo znaka stop.

Vse omenjene aplikacije morajo delovati v območju od 50 do 300 m, najkrajša zakasnitev od zaznavanja nevarnosti do ukrepanja pa naj ne bi bila večja od 100 ms.

3.1.2. Nadzor prometa

Nadzor prometa je orientiran na izboljšanje prometnega toka, kar doseže z nadzorom pretoka prometa ter zmanjševanjem nesreč zaradi zastojev, s tem pa tudi zmanjšuje čas potovanja. Aplikacije, ki pridejo v poštev, so nadzor prometa, nadzor in upravljanje semaforjev in nadzor nad reševalnimi vozili.

Nadzor prometa lahko poteka v radiju več kilometrov od lokacije vozila. Pri tej aplikaciji vsako vozilo deluje kot senzor za ostala vozila v sistemu. Informacijo lahko uporabi za obveščanje voznika o času do cilja, v zahtevnejših sistemih pa celo ureja promet z nadzorom semaforjev in omejitvami hitrosti. Pri uporabi v reševalnih vozilih lahko le-ti obveščajo ostale udeležence v prometu o nujni vožnji, smiselno pa je imeti tudi nadzor nad semaforji. Slednje je trenutno precej slabo urejeno, saj se delovanje semaforjev nastavi statično, v nekaterih redkih izjemah pa tudi tako, da se signal spremeni, ko vozilo ustavi pred njim. To bi lahko izboljšali z novim sistemom, ki bi posredoval dodatne informacije o dolžini kolone pred semaforjem in približno oceno števila vozil, ki bodo v nekem času še pripeljali do semaforja.



Slika 10 – Primer nadzora prometa in reševalnega vozila

Aplikacije v tem razredu tipično nimajo strogih zahtev po informaciji v realnem času, saj sistem nadzoruje stanje več kilometrov okoli vozila. Seveda pa se ta zahteva viša glede na oddaljenost od pomembnega dogodka.

3.1.3. Pomoč v prometu

Pomočjo v prometu se opira na aplikacije, ki bodo pomagale izboljšati pretočnost na obstoječi cestni infrastrukturi. Če bi na avtocesti formirali kolono vozil, ki bi se premikala z isto hitrostjo pri isti oddaljenosti, bi lahko precej povečali kapaciteto vozil na trenutni cestni infrastrukturi. Tudi pomoč pri prehitevanju in menjavi pasu lahko zmanjša nesreče, ali pa jih celo popolnoma odpravi.

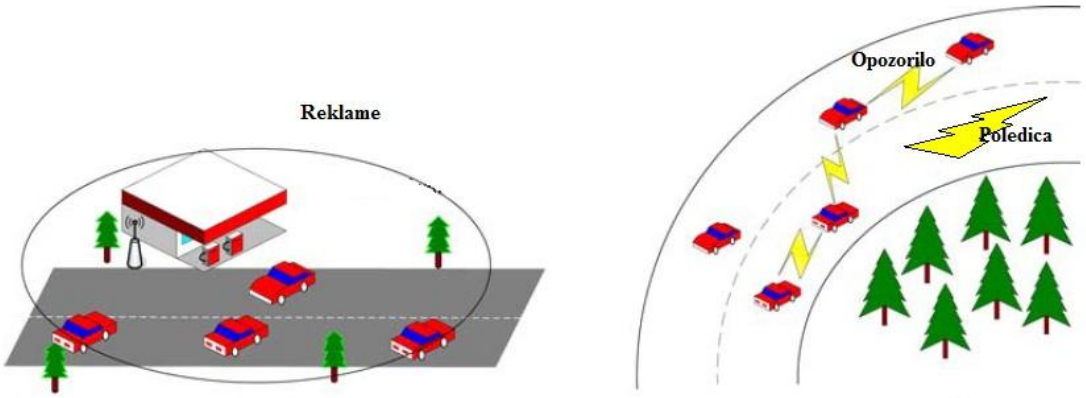
Slika 11 – Primer vožnje s konstantno hitrostjo in menjava pasu

Seveda te aplikacije potrebujejo konstantne informacije v realnem času. Če so pravilno narejene in umeščene v omrežje, omogočajo varno vožnjo in so dober korak k pametnim avtocestam.

3.1.4. Informacije potnikom

Informacije potnikom so aplikacije, ki posredujejo karte, splošna sporočila in lokalne informacije, ki so pomembne v nekem časovnem obdobju. Te sporočila so večinoma informacije o ponudbi in cestna opozorila.

Informacije lokalnega pomena, kot so bencinske postaje, parkirna mesta in delovni čas trgovin in muzejev, si lahko uporabnik prenese iz omrežja ali pa iz ostalih vozil, ki so na tem območju doma. Na zaslon v vozilu se lahko posredujejo tudi reklame prehrambne industrije. Zelo pomembna so tudi cestna obvestila, med katere spadajo obvestila o razlitem olju, nizkih mostovih, vodi in luknjah na cesti. Ta se lahko v vozilo prenesejo samodejno, ali pa to storijo pooblaščene osebe. Potrebno se je zavedati, da so te informacije le lokalnega pomena, zato jih je potrebno posredovati le vozilom, ki se temu dogodku približujejo. Doseg tu nima velikega pomena, kot tudi ne prejem informacij v realnem času. Informacije se pošiljajo vsem vozilom okoli interesne točke.

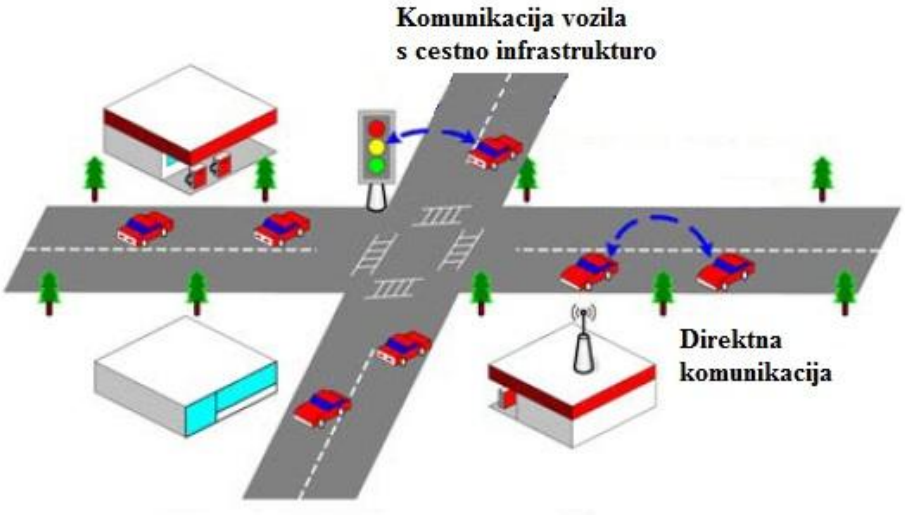


Slika 12 – Primer reklamnih in cestnih obvestil

3.1.5. Udobje

Glavni namen aplikacij za udobje je udobno potovanje. To vrsto aplikacij poganja želja po komunikaciji potnikov z drugimi vozili ali po dostopu do interneta in javnega telefonskega omrežja. Med dvema voziloma, ki potujeta skupaj, bi tako lahko tekla govorna in pisna komunikacija. Možnost je tudi komunikacije med policisti in vozniki, če bi prvi želeli ustaviti voznika in opraviti kontrolo.

Zelo uporabna je možnost komuniciranja vozila z dostopnimi točkami, saj nam to odpira popolnoma nov spekter aplikacij, od elektronske pošte in predvajanja video vsebin, do spletnega brskanja in klicev. Za udobje lahko skrbijo tudi aplikacije o ceni cestnin, mostnin, saj bi se te zbirale samodejno. Danes že obstaja nekaj zametkov takega sistema, predvsem na servisih in prodajalnah vozil višjega cenovnega razreda. V teh vozilih že lahko gledamo video, poslušamo glasbo ali novice, ki jih v sistem vnesejo ali med čakanjem na servis, ali pa si jih naloži uporabnik sam.



Slika 13 – Primer udobne komunikacije na različni lokaciji

3.2. Razdelitev aplikacij glede na vrsto komunikacije

Aplikacije lahko razdelimo tudi glede na tip komunikacije. Tako poznamo aplikacije, ki se uporabljajo pri komunikaciji med vozili in aplikacije, ki se uporabljajo pri komunikaciji z infrastrukturo.[2]

Nekaj možnih aplikacij V2V:

- približevanje reševalnega vozila,
- opozorilo nevarne točke,
- opozorilo trka,
- prilagajanje potovalne hitrosti,
- opozorilo naleta,
- opozorilo o združitvi pasov,
- opozorilo o menjavi pasu,
- zaznavanje trkov,
- stanje na cesti,
- opozorilo o vožnji v napačno smer,
- elektronski nadzor zasilne zavorne luči.

Nekaj možnih aplikacij V2I:

- opozorilo hitrosti v ovinkih,
- opozorilo trka na avtocesti ali železnici,
- pomoč pri zavijanju levo,
- opozorilo višine predora ali podvoza,
- informacija o stanju na cesti,
- opozorilo o prevoženem znaku stop,
- opozorilo o prevoženi rdeči luči,
- opozorilo o delovišču,
- opozorilo o prehodu za pešce.

3.3. Pregled skupin aplikacij glede na vrsto tehnologije

Za svoje delovanje potrebujejo različne skupine aplikacij različne tehnologije, ki sem jih predstavil v prvem poglavju. V naslednji tabeli bom predstavil pregled vseh skupin aplikacij glede na tehnologijo, ki jo za svoje delovanje lahko uporabljajo.

Skupina aplikacij / Uporabljena tehnologija	Varnost	Nadzor prometa	Informacije potnikom	Pomoč v prometu	Udobje
CAN	✓			✓	
Bluetooth	✓		✓		✓
ZigBee	✓		✓		✓
Satelitska komunikacija	✓	✓	✓	✓	✓
IEEE 802.11	✓	✓	✓	✓	✓
WiMax	✓	✓	✓	✓	✓
MBWA	✓	✓	✓	✓	✓
GSM/GPRS/EDGE	✓	✓	✓	✓	✓
UMTS/HSPA	✓	✓	✓	✓	✓

Tabela 2 – Pregled tehnologij, ki jih uporabljajo skupine aplikacij

Smiselno je, da imajo varnostne aplikacije dostop do vseh uporabljenih tehnologij. S tem si zagotovimo, da lahko v skrajnem primeru prevzamejo nadzor nad vozilom in npr. v primeru trka pred vozilom aktivirajo samodejno zaviranje v sili. Dostop do fizičnega vodila v vozilu lahko dovolimo še aplikacijam za pomoč v prometu, saj nam določene aplikacije lahko omogočijo konstantno hitrost in oddaljenost do spredaj vozečega vozila. Za vse ostale skupine aplikacij pa nadzor do fizičnega vodila ni bistvenega pomena. Vse skupine aplikacij uporabljajo tehnologije, ki tvorijo infrastrukturo. Manjša osebna omrežja, ki se tvorijo v vozilu, pa bodo uporabljale predvsem aplikacije za udobje in informacije potnikom.

4. VARNOST OMREŽJA VOZIL

Čeprav je varnost pomemben vidik omrežja vozil, se temu ni posvečalo veliko pozornosti. Pravzaprav je bil problem varnosti preložen za kasnejše obdobje raziskav, tako s strani razvijalcev kot industrije. Ker pa se komercialna uporaba teh omrežij vse bolj bliža, bo za njihov uspeh in varno uporabo potrebno izdelati varnostne rešitve, ki bodo zadovoljile uporabnike, proizvajalce avtomobilov in omrežnih ponudnikov, konec koncev pa tudi vlade. Potrebno bo zagotoviti, da informacij, ki bi kakorkoli vplivale na kritične dogodke, ne bo moč spreminjati. Ravno tako je potrebno zagotoviti, da bodo do poslanih informacij prišli le tisti, katerim so te namenjene. Varnost in zasebnost ne smeta biti ogrožena zaradi lažje uporabe omrežij. Ker največji pritisk za zagon omrežja vozil prihaja s strani izdelovalcev vozil, je potrebno razviti varnostni sistem, ki bo deloval v vseh okoljih. Tako bodo lahko proizvajalci vozil te rešitve vgradili v svoja vozila in s tem odpravili potrebo po dodatni opremi.

Varnost in zasebnost morata biti dva večja vidika pri načrtovanju omrežja vozil. Slabo zasnovana omrežja, ki omogočajo napade, lahko resno ogrozijo nadaljnji razvoj. Ravno tako bo omrežje, ki omogoča neavtoriziran dostop do podatkov s strani tretje osebe, zagotovo zavrnjeno s strani uporabnikov.

4.1. Varnostni izzivi

Priprava robustne varnosti za omrežja vozil mora prevzeti tehnične, ekonomske in socialne izzive.[6]

4.1.1. Obseg in dinamika omrežja

Omrežja vozil bodo največja instanca samodejno organiziranih ad-hoc omrežij. Predvideva se, da bo njihova velikost več milijonov vozlišč, ki se bodo prepletala med različnimi ponudniki storitev. Problem razširljivosti je potrebno reševati na transparenten način, predvsem zato, ker se vse operacije izvajajo pri visokih hitrostih. S tem pa pridemo tudi do izziva mobilnosti, saj dve vozili, ki se srečata sredi avtoceste, lahko komunicirata le par sekund. V tem času si morata izmenjati vse pomembne informacije.

4.1.2. Zasebnost

Ena večjih skrbi v omrežju vozil je zasebnost in vplivanje na njo. Hitro namreč lahko pride do vdora v sistem in s tem ogrožanja zasebnosti. Čeprav obstajajo rešitve, ki omogočajo anonimnost voznika in vozila, to lahko negativno vpliva na odgovornost. Vozniki, ki bi imeli popolnoma anonimno vozilo, bi lahko v primeru nesreče preprosto pobegnili in se s tem izognili posledicam. Zato je potrebno zagotoviti uravnoteženo mero odgovornosti in zasebnosti voznika. En način je podoben sedanjemu »ročnemu« načinu in sicer dovoljenje za razkrivanje identitete bi bilo v rokah policije na podlagi sodnega naloga.

4.1.3. Zaupanje

Ključen element v varnostnem okolju je zaupanje. To še posebno velja za omrežja vozil, saj varnostne aplikacije zahtevajo visoko mero odgovornosti. Tudi uporabniki so vedno bolj zavedajo pomena zasebnosti. Vozniki tega ne bodo ogrožali le zato, da bi se pridružili nekemu omrežju. Kaj lahko bi se namreč zgodilo, da bi zaradi prehitre vožnje na dom dobili kazen s strani policije.

4.1.4. Stroški

Cena je dodaten vidni faktor pri vpeljavi omrežja vozil. Pravzaprav bi predstavitev novega standarda za proizvajalce vozil pomenila vgradnjo nove strojne rešitve, v končni fazi pa bi to najbolj občutili uporabniki s strani višjih cen vozil. Dodaten strošek predstavlja še infrastruktura, ki bo omogočala dostop do podatkovnih baz. Zato je ključno, da te stroške ohranjamo na minimalni ravni in hkrati zagotovimo dovolj podpore.

4.1.5. Dodatni varnostni izzivi[8]

- Časovna omejitev je pomemben faktor, saj so informacije, ki se izmenjujejo večinoma potrebne v realnem času, zamik pri oddaji pa je lahko do največ 100 ms.
- Skladnost podatkov – tudi avtorizirana vozila lahko postanejo napadalci in razpošiljajo lažna sporočila. S tem lahko povzročijo nesrečo ali celo motijo delovanje omrežja.
- Nizka toleranca napak – nekatere aplikacije uporabljajo protokole, ki se zanašajo na verjetnostne sheme za zagotavljanje varnosti. Zato je vsaka še tako majhna napaka lahko usodna in nesprejemljiva
- Dodeljevanje ključev se v omrežju vozil srečuje z različnimi izzivi. Vozila namreč izdeluje več proizvajalcev, zato bi nameščanje ključev v tovarni zahtevalo sodelovanje več institucij. Tudi zanašanje na certifikate ni smiselno, saj se vozila iz različnih držav ne bi mogla medsebojno avtorizirati, razen če bi zaupala vsem certifikatom, kar pripelje do zmanjšanja varnosti.
- Visoka mobilnost – ta izziv je mogoče doseči z izbiro optimalne programske ali strojne opreme za implementacijo kriptografskih algoritmov in prilagajanje šifriranja glede na podatke ki jih šifriramo.

4.2. Varnostne zahteve

Da bi omrežje kar najbolj zaščitili pred napadi, moramo upoštevati tudi varnostne zahteve, ki se v omrežju ITS malenkost razlikujejo glede na fiksno omrežje. Tako so v omrežju ITS pomembne zahteve navedene v naslednjih podpoglavjih.[8]

4.2.1. Razpoložljivost

Napadi z blokiranjem in razne preobremenitve lahko kot posledico prinesejo nedosegljivost omrežja. Zato je pomembno, da je omrežje vedno dosegljivo. Nerazpoložljivost omrežja lahko ublažimo z raziskovanjem številnih varnostnih mehanizmov, ki se lahko uporabljajo za odkrivanje napadalskih vozlišč in z različnimi radijskimi tehnikami, ki bi onemogočale napade z motenjem signala. Če povzamemo je razpoložljivost izredno pomemben faktor v omrežju ITS.

4.2.2. Integriteta sporočil

Integriteta sporočil je pomembna iz vidika aplikacij, saj je potrebno zagotoviti, da se vsebina sporočila med prenosom ne spremeni. Avtentičnost in celovitost sporočil je v praksi težko ločiti, saj ni načina, da bi ugotovili izvor sporočila, če je bilo le-to med prenosom spremenjeno.

4.2.3. Zaupnost

Inteligentni transportni sistem omogoča aplikacije, ki neposredno vplivajo na varnost ljudi. Če je v nesrečo udeleženo vozilo, ki v omrežju ni avtenticirano, se lahko v to nesrečo zapletejo tudi avtenticirana vozila. Zato je za dosego cilja omrežja ITS (to je varnost ljudi) nujno, da vsa vozila v tem omrežju zmorejo sprejeti in obdelati varnostne podatke.

4.2.4. Preverjanje izvora

V omrežju ITS je zahteva, da lahko podatke pošiljajo in sprejemajo le avtenticirana vozila, potrebno se je izogibati podatkov neavtenticiranih vozil. To se lahko doseže z zavračanjem podatkov, ki nimajo v izvornih podatkih dokaza o verodostojnosti. To je pomembno zaradi vidika varnosti, saj vsako vozilo v omrežju pričakuje prejetje varnostnih sporočil.

4.2.5. Medsebojna avtentikacija, avtorizacija in kontrola dostopa

Skupna avtentikacija, avtorizacija in kontrola dostopa je koristna, saj lahko z njo zajezimo določene napade na omrežje. Ena izmed rešitev je vpeljava simetričnega ključa, ki si ga delijo vsa vozlišča v omrežju. Ta mehanizem se smatra za precej standardno rešitev, saj je omejen na precej majhno število vozil, ponavadi vseh, ki pripadajo istemu ponudniku. Za večja omrežja ima tak način dve večji nevarnosti. Prva je, da za razbitje varnosti sistema napadalec potrebuje ogroziti le eno vozilo, s tem pa ohromi celotno omrežje. Druga je, da se lahko vozila izdajajo za druga vozila, s tem pa lahko dostopajo do njihovih sporočil, s čimer ogrozijo zaupnost. Rešitev problema simetričnih ključev bi lahko bila uporaba javnega kriptiranja ključev z nekaj izboljšavami.

4.2.6. Nezmožnost zavrnitve pošiljanja sporočila

Vozilo, ki bi povzročilo nesrečo ali poskušalo poslati zlonamerno sporočilo, mora biti zanesljivo identificirano. Torej tako vozilo ne sme imeti možnosti zavrniti pošiljanja sporočila. V ta namen se lahko uporabi tudi digitalni podpis, vendar pa glavni razlog uporabe le-tega ni to, da bi lahko zavrnili pošiljanje sporočila, ampak da bi lahko zagotovili avtentikacijo med dvema voznikoma, ki se predhodno še nista srečala brez posredovanja tretje osebe.

4.2.7. Varovanje zasebnosti

Ljudje smo čedalje bolj nezaupljivi do tehnologij, ki potencialno posegajo v našo zasebnost in sledljivost, zato je zelo pomembno, da omogočimo tudi anonimnost. Ta anonimnost je le pogojna, saj je vseeno potrebno zagotoviti nezmožnost zavrnitve pošiljanja sporočil. Sledljivost je legalni proces za pravosodne organe in operaterje, za ostale pa mora ostati vozilo nesledljivo. Pod sledljivost v vozilu štejemo, kdo se pogovarja s kom, kaj pošilja, katero spletno stran pregleduje, kje se nahaja, ipd. V omrežju vozil se zahteva, da je sledljivost na voljo le pravosodnim organom.

Slika 14 – Prepletanje varnostnih izzivov in zahtev v omrežjih ITS in ostalih omrežjih

4.3. Varnostni pogled iz vidika aplikacij

Aplikacije v omrežju vozil VANET lahko iz vidika varnosti razdelimo na dve veji in sicer na varnostne aplikacije in ostale aplikacije. Pri varnostnih aplikacijah vozila ponavadi oddajo signal, ki vsebuje podatke o lokaciji, hitrosti in ostalih podatkih vozila. Prejemniki tega signala so ostala vozila v omrežju. Obstajajo tudi varnostne aplikacije, katere vozilu posreduje RSU. Drugače se obnašajo ostale aplikacije, saj se zahteva prenos večjega števila, manj pa zakasnitev prenosa podatkov.

4.3.1. Varnostni vidiki za varnostne aplikacije

Varnostne aplikacije so večinoma prisotne pri komunikaciji V2V, lahko pa jih najdemo tudi pri komunikaciji V2I. Varnostne zahteve, ki jih pri uporabi pričakujemo, so naslednje:[3]

- Zakasnitev – Ker so vozila izredno mobilna, hkrati pa se lahko premikajo pri visokih hitrostih, mora biti celoten čas zakasnitve od pričetka dogodka in pošiljanja sporočila do prejema le-tega s strani drugega vozila izredno kratek. Pričakuje se, da bo ta čas vedno manjši od 100 ms, vendar bi zaradi varnosti moral biti največ 20 ms.
- Varnostni cilji – Varnostne aplikacije bodo svoje poslanstvo opravile le, če bodo delovale tudi v primeru napada. Zato je potrebno zagotoviti prave kriptografske protokole. Zaupnost tu ni pogoj, saj se sporočila nanašajo na dogodke, ki so vidni vsem. Potrebno je tudi zagotoviti, da se poslano sporočilo lahko poveže s točno določenim vozilom, tako da ni dvoma o tem, kdo ga je poslal.
- Sporočila – Varnostne aplikacije vsebujejo podatke, ki si jih med seboj izmenjujejo vozila, prav tako pa podatke lahko posreduje RSU. Varnostna sporočila se oddajajo redno v intervalu od tri do desetkrat na sekundo, dodatna sporočila pa le na podlagi zahteve. Tako lahko sklepamo, da se v eni sekundi odda okoli 10 sporočil. Na avtocesti je v omrežju lahko tudi po 100 ali več vozil, zato mora biti enota OBU v vozilu sposobna obdelati vsaj med 1000 do 2500 sporočil v sekundi.
- Topologija – V večini primerov varnostne aplikacije pošljejo sporočilo le sosedom, ki so oddaljeni en hop. Vseeno pa ne smemo zanemariti varnostnih sporočil, ki bi obveščala tudi bolj oddaljena vozila, saj lahko s tem povečamo učinkovitost glede na vrsto nevarnega dogodka, ko se le-ta pripeti.
- Infrastruktura – Smiselno je uporabljati infrastrukturo javnih ključev PKI, saj je le-ta pod nadzorom ene same avtoritete, lahko pa se razdeli tudi na več avtoritet na hierarhični način. Vsa vozila so registrirana in imajo vsaj en certifikat.
- Zasebnost – Bistvena zahteva je zasebnost, le-to ponavadi zahtevajo kupci avtomobilov. Vozila, ki imajo vgrajeno opremo DRSC, redno oddajajo podatke o hitrosti in lokaciji. Ti informaciji lahko omogočata sledenje, kar bi napadalci lahko uporabili v svojih napadih. Lahko bi jo izkoristili tudi organi pregona, kot je policija, za izdajo kazni za prehitro vožnjo. Zato je potrebno v omrežjih VANET zagotoviti enako mero zasebnosti, kot jo imajo vozniki že sedaj.
- Zaznavanje in preklic – Za varnostne aplikacije je nujen zmogljiv mehanizem, ki zaznava zlonamerna vozila in jih hitro izloči iz sistema. Kriteriji, kdaj se vozilo smatra za sumljivo, še niso natančno določeni.

4.3.2. Varnostni vidiki za ostale aplikacije

Pri uporabi ostalih aplikacij bodo imele veliko vlogo enote RSU. Zahteve pri teh aplikacijah niso tako točno določene, saj pri varnosti ne igrajo ključne vloge. So pa te zahteve bolj raznolike in se zanašajo na uporabljene aplikacije. Nekaj značilnih zahtev je:[3]

- Zakasnitev in sporočila – V večini primerov zakasnitev ni pomembna, tudi število poslanih sporočil je manjše kot pri varnostnih aplikacijah. Vozila redno ne oddajajo sporočil, pač pa to počnejo enote RSU.
- Varnostni vidiki – Ponavadi se zahteva integriteta in verodostojnost sporočil, saj se želimo izogniti škodoželjnim napadom. Zaupnost se zahteva za vsa sporočila, ki vsebujejo osebne podatke. Komercialna sporočila ne potrebujejo zaščite, zagotoviti je potrebno le, da niso spremenjena.
- Infrastruktura – tudi tu pride v poštev infrastruktura javnih ključev PKI.
- Zasebnost – Tudi pri ostalih aplikacijah je bistvena zahteva zasebnost.
- Zaznavanje in preklic – Aplikacije si veliko sporočil izmenjujejo z enotami RSU, ki bodo povezane s centralnim sistemom, lahko je to tudi internet. Sumljiva vozila, ki bi si izmenjavala sporočila z RSU, se lahko odkrijejo na običajen način. Preklic certifikata se lahko prenese na vse centralne strežnike. Ker je splošna miselnost, da so nevarnostne aplikacije lažje ranljive, je ravno za te vrste aplikacij potrebna višja stopnja varnosti.

5. NAPADI V OMREŽJU VOZIL

Napadi na omrežja vozil bodo zaradi specifičnosti in razširjenosti po vsej verjetnosti zelo pogosti. Zato je nujno, da se zagotovi primeren nivo varnosti. Ker gre za novo vrsto omrežij, je težko napovedati, kakšne vrste napadov si bodo napadalci izmislili, vseeno pa bom v tem poglavju predstavil možne vrste napadov, prav tako pa bom predstavil tudi različne možne profile napadalcev.

5.1. Napadalci

Napadalci imajo ponavadi dostop do omrežja, v primeru omrežij VANET pa sklepamo, da imajo tudi dostop do opreme DRSC. Zato lahko poslušajo na različnih kanalih in prebirajo vsa sporočila, ki so poslana v tem omrežju. Prav tako lahko napadalci pošiljajo sporočila, odgovarjajo na njih, ter jih prepošiljajo na druge lokacije. Čeprav imajo napadalci na voljo strojno opremo, ki je bolj zmogljiva, kot bodo povprečne enote OBU v vozilih, pa bodo le-ti vseeno omejeni s tehnologijo, ki bo na voljo v času napada.

Napadalce povezuje nekaj glavnih lastnosti in zmožnosti:[3]

- Zunanji/notranji
  Napadalec ima lahko dostop do notranjega znanja. Raven notranjega znanja sega od izčrpnega poznavanja podomrežja do poznavanja tajnih ključev. Notranje znanje se lahko razširja tudi brez bojazni morebitnega napada. Zunanje znanje vključuje poznavanje omrežja VANET ter podatkov o konfiguraciji omrežja.
- Pokritost omrežja
  Napadalec je zmožen pokriti določen del cestne infrastrukture. Napadalec z osnovnim znanjem nadzoruje le eno napravo DRSC in pokriva le razdaljo okoli 1000 m, medtem ko lahko napreden napadalec postavi in nadzoruje mrežo nekaj sto enot DRSC.
- Tehnično znanje
  Sklepamo lahko, da ima napadalec majhne možnosti, da ogrozi varno omrežje in pridobi zaupne podatke. Zato lahko pod tehnično znanje uvrstimo napadalčevo sposobnost, da pridobi nadzor nad enotami OBU in RSU.
- Viri
  Napadalci imajo omejene denarne prilive, kot tudi pomoč drugih ljudi. Dogaja se, da so napadalci povezani v skupine, katerih glavni cilj je pridobiti denarna sredstva. Možno pa je tudi, da so napadalci le skupina radovednih ljudi, ki raziskujejo meje varnosti.

5.2. Vrste napadalcev

5.2.1. Radoveden napadalec

Radoveden napadalec nima nikakršnega notranjega znanja, pozna le to, kar je javno objavljeno na internetu. Imajo zelo omejena sredstva, ugotovitve pa objavijo na internetu. Lahko se tudi povežejo v navidezne skupine, ki jih povezuje internet. Take skupine lahko postanejo izredno številčne, če imajo enak skupni cilj. Nekaj podobnega se trenutno dogaja pri skupinah, ki se trudijo vdreti v Applov varnostni sistem mobilnika iPhone. Nivo tehničnega znanja niha, saj ima lahko napadalec čisto osnovno, ali pa bolj zahtevno znanje. V nekaj skrajnih primerih ima napadalec možnost uporabe najbolj napredne tehnologije in orodij v službenih prostorih. En sam napadalec ima omejene vire, povezana skupina pa ima virov več. Zaradi prej naštetih razlogov se pričakuje, da bodo napadalci te vrste bolj orientirani na potrošniške produkte, kot pa na omrežja. Če bodo svojo pozornost obrnili na omrežja, pa bodo po vsej verjetnosti le analizirali obstoječe aplikacije.

5.2.2. Akademski napadalec

Akademski napadalci so precej povezani z radovednimi napadalci. To so navadno študenti in profesorji na univerzah, ki delujejo v raziskovalne namene. Imajo dostop do najnovejše tehnologije in vrhunskega znanja. Svoje ugotovitve lahko izmenjujejo z drugimi akademskimi ustanovami, včasih pa tudi z radovednimi napadalci. Če se varnostne luknje pokažejo v sistemih določenega operaterja, ga navadno o tem obvestijo in mu omogočijo odpravo napak, še preden objavijo svoja dognanja na internetu.

5.2.3. Škodoželjen napadalec

Škodoželjen napadalec bo škodo povzročal namenoma. Zbiral bo podatke iz interneta, ter sodeloval z radovednimi napadalci, katerim ne bo razkril svoje namere. Delujejo lahko brez globljega motiva, lahko pa imajo tudi teroristične namene. Zgodi se tudi, da imajo dostop do velikih finančnih virov, s katerimi kupijo strokovno znanje in ljudi, tudi njim navadno ne razkrijejo svojih namenov. Kombinacija teh virov in škodoželjnosti pa naredi napadalce te vrste izredno nevarne.

5.2.4. Organizacijski napadalec

Organizacijskega napadalca poganja točno določen motiv. V večini primerov je motiv finančne narave. V skupino organizacijskih napadalcev lahko uvrščamo tudi vladne organizacije, ki uporabljajo metode dela, ki so izven zakonskih okvirjev. Pri svojem delu so racionalni, na voljo imajo veliko virov in strokovnega znanja, to znanje pa uporabijo za čim večji obseg napada. Možno je, da imajo dostop do notranjega znanja, do tega znanja lahko pridejo tudi s podkupovanjem. Redno preverjajo po internetu o dosežkih ostalih napadalcev, nasprotno pa svojega dela nikoli javno ne objavijo. Navadno objavijo le informacijo, da so

vdrli v določen sistem. Organizacijski napadalci so resna grožnja, vseeno pa delujejo racionalno, saj je njihov glavni cilj čim večji dobiček.

5.2.5. Končni uporabniki

Kot največje število napadalcev se šteje končne uporabnike, ki na svoje sisteme nameščajo in uporabljajo programe, ki so jih razvili prej omenjeni napadalci. O njih in njihovem delovanju dobijo vse potrebne podatke na internetu, tako da sami pravzaprav ne potrebujejo skoraj nikakršnega tehničnega znanja. Delovanje samega napada jih ne zanima, vseeno pa njegovo delovanje in pridobljene podatke uporabijo za svoj cilj (npr. lociranje sosedov, nadzor prometnih znakov na poti v službo, prenos digitalnih vsebin iz vozila na domači sistem ...). Končni uporabniki s tem ogrožajo tako voznike kot tudi podjetja, čeprav se tega včasih niti ne zavedajo.

5.3. Klasifikacija napadov

Pomemben faktor pri zagotavljanju varnosti je tudi prepoznavanje vrste napada, ki ogroža komunikacijo v omrežju. Obstajajo lahko različne vrste napadov glede na okolje, kot tudi glede na uporabo. Napade lahko tako razvrstimo glede na naslednje lastnosti:[8]

- Notranji ali zunanji napad
  Notranji napad lahko izvede avtoriziran član omrežja vozil. Tega člana ostali člani prepoznajo kot legitimnega člana. Napad te vrste je verjetno najbolj kritičen, saj ga izvede zaupanja vreden član. Zunanji napad izvede nekdo, ki ni avtoriziran član omrežja, s strani legitimnih članov se smatra za vsiljivca. Zunanji napadalec lahko glede na notranjega izvede manjše število napadov.
- Namerni ali nenamerni napad
  Namerni napad napadalec izvede z namenom onemogočiti delovanje omrežja, nenamerni napad pa se zgodi pomotoma, ponavadi zaradi napake v omrežju ali pri prenosu podatkov.
- Aktivni ali pasivni napad
  Aktivni napad izvede napadalec, ki ustvarja ali spreminja pretok podatkov. Pri pasivnem napadu napadalec v omrežju le prisluškuje in pridobiva podatke za kasnejšo uporabo.
- Neodvisni ali usklajeni napad
  Neodvisni napad izvede en sam napadalec, usklajeni napad pa sproži skupina napadalcev, ki jih združuje isti cilj.

5.4. Napadi

Vse vrste napadov, ki se lahko zgodijo v omrežju, je nemogoče napovedati, saj napadalci dnevno izumljajo nove načine. Zato bom v tem poglavju predstavil napade, ki so danes že znani in ki bi se lahko pripetili v omrežju vozil. Napadi se lahko zgodijo na različnih plasteh referenčnega modela OSI.

5.4.1. Referenčni model OSI

Referenčni model OSI je bil prvič predstavljen leta 1983 s strani mednarodne organizacije za standardizacijo ISO. Sestavljen je iz sedmih plasti, na vsaki izmed njih so določene posamezne omrežne funkcije. Načrtovan je kot zgled za implementacijo komunikacijskih modelov, vendar je le referenčni model. V celoti ni nikdar zaživel, v omrežjih se namesto njega uporablja model TCP/IP.

Sedem plasti referenčnega modela OSI:

- Fizična plast
  Skrbi za prenos podatkov preko prenosnega medija. Naloge fizične plasti so npr. prenos digitalne informacije po prenosnem mediju in pretvarjanje električnih signalov v obliko, primerno za prenos po prenosnem mediju.
- Povezovalna plast
  Prenaša podatkovne okvirje med dvema točkama. Osnovna naloga je odkrivanje napak, ki se zgodijo med prenosom po fizičnem prenosnem mediju.
- Omrežna plast
  Skrbi za prenos transportnega segmenta od začetnega do končnega računalnika. Skrbi za usmerjanje paketov skozi topologijo omrežja. Izvaja usmerjevalne algoritme.
- Transportna plast
  Izvaja transport podatkov med dvema končnima računalniškima aplikacijama.
- Sejna plast
  Je namenjena storitvam, ki podpirajo logično povezovanje oddaljenih procesov med seboj – skrbi za potek dialoga med dvema aplikacijama.
- Predstavitvena plast
  Skrbi za združljivost predstavitve podatkov v različnih računalniških okoljih. Skrbi tudi za zaščito podatkov (kriptografija, stiskanje podatkov).
- Aplikacijska plast
  Vsebuje vrsto standardnih aplikacij, brez katerih si danes ne moremo predstavljati informacijsko-komunikacijskega sistema (elektronska pošta, SMTP, FTP …). Je vmesnik med uporabnikom in referenčnim modelom OSI.

ISO OSI plasti	TCP/IP plasti
Aplikacijska	Aplikacijska
Predstavitvena	
Sejna	(združeno)
Transportna	Transportna
Omrežna	Omrežna
Povezovalna	Povezovalna
Fizična	(združeno)

Tabela 3 – Primerjava plasti modela OSI in TCP/IP

5.4.2. Napadi v omrežju vozil glede na plasti referenčnega modela OSI

Napade v omrežju vozil lahko razvrstimo med štiri plasti:

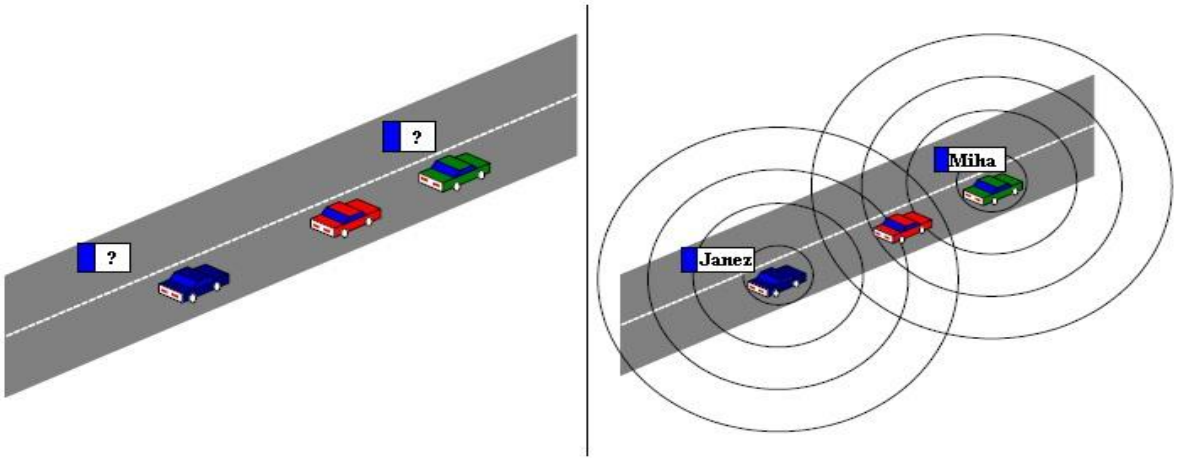
ISO OSI plast	Vrsta napada
Aplikacijska plast	• Virusi, • Črvi, • zlonamerna koda, • napad z lažnimi podatki, • sledenje, • finančno izkoriščanje.
Omrežna plast	• Napad na usmerjanje. • Napad na prenos paketov.
Povezovalna plast	• Ranljivost zaščite WEP. • Napad z razkritjem identitete. • Sledenje gibanja. • Napad DOS.
Fizična plast	• Napad na fizični medij. • Napad z reprodukcijo. • Prisluškovanje.

Tabela 4 – Napadi glede na plasti referenčnega modela OSI

5.5. Primeri napadov v omrežju vozil

5.5.1. Razkritje identitete

Napadalec pri tem napadu aktivno spremlja promet, saj želi pridobiti identiteto vozila. Poleg identitete lahko pridobi tudi naslov IP, naslov MAC, torej vse pomembne informacije. Četudi poslana sporočila ne vsebujejo teh podatkov, lahko napadalec na podlagi ene same vrstice, ki se pojavlja v več sporočilih, določi identiteto vozila. Napadalec lahko identiteto ugotovi tudi iz radijskega signala, ki ga neko vozilo oddaja.



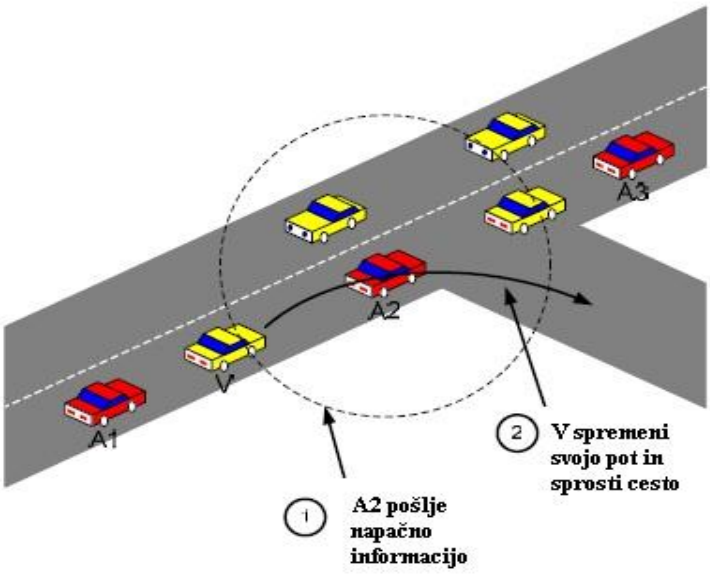
Slika 15 – Napadalec razkrije identiteto neznanih vozil

Primer napada

Vozilo A se po avtocesti vozi na repu kolone. Ker ga zanima prometna situacija pred njim, pošlje signal vsem ostalim udeležencem, s katerim želi izvedeti, kdo se vozi v koloni z njim, ter kakšna je prometna situacija. Vsa vozila v koloni na to povpraševanje odgovorijo s podatkom kdo so, ter kakšna je situacija na cesti. Vendar pa se v koloni nahaja tudi vozilo, ki nima namena posredovati identitete in informacije, pač pa želi le pridobiti podatke o ostalih vozilih, ki bi jih kasneje lahko voznik uporabil v svojo korist. Tako prestreže povratne informacije vseh vozil v koloni in le-te shrani. S tem razkrije identiteto vseh udeležencev. Vsi udeleženci vseeno dobijo pravilne podatke in se prisotnosti napadalca niti ne zavedajo.

5.5.2. Spreminjanje informacij

Napadalec pri tem napadu posreduje v omrežje napačno informacijo in s tem vpliva na obnašanje ostalih vozil. Napadalec lahko tako odda sporočilo, da je pred njim zastoj, in s tem sprosti cesto, saj ostala vozila na prvem možnem odcepu zavijejo na drugo cesto. Napadalec lahko tudi oddaja napačne podatke o lokaciji.



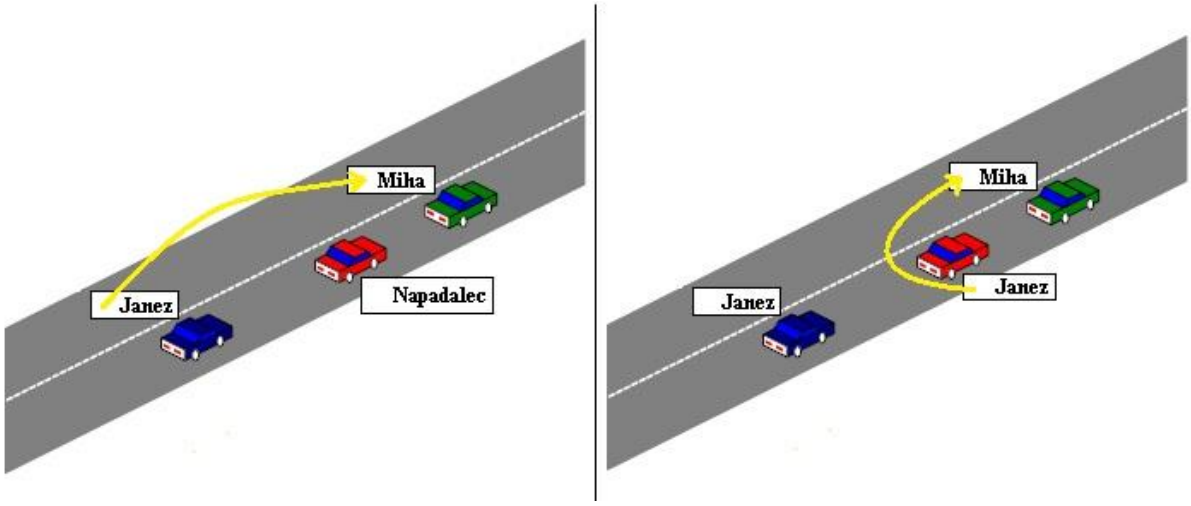
Slika 16 – Napadalec A2 pošlje napačno informacijo in sprosti pot napadalcu A1

Primer napada

Napadalec se na avtocesti približuje koloni vozil, ki prehiteva počasne tovornjake. Ker se mu mudi, želi čim hitreje prazno cesto. Zato pošlje vsem udeležencem signal z napačno informacijo, da se je pred njimi zgodila prometna nesreča. V informaciji predlaga, da naj vsa vozila uporabijo prvi izvoz iz avtoceste in pot nadaljujejo po lokalnih cestah. Ker napadalec informacijo zavije v uradno obvestilo, ki jo posredujejo tudi obcestne enote, jo vsi vozniki upoštevajo ter zavijejo iz avtoceste. S tem si je napadalec pripravil prazno pot.

5.5.3. Pretvarjanje

Pri tem napadu napadalec uporablja lažno identiteto in se tako pretvarja, da je neko drugo vozilo in s tem pridobi privilegije drugega vozila. Lahko se tudi pretvarja za več vozil hkrati. Napadalec lahko uporabi več identitet in umetno zgosti promet, tako da ostali vozniki mislijo, da morajo izbrati drugo pot.



Slika 17 – Napadalec uporablja identiteto drugega vozila

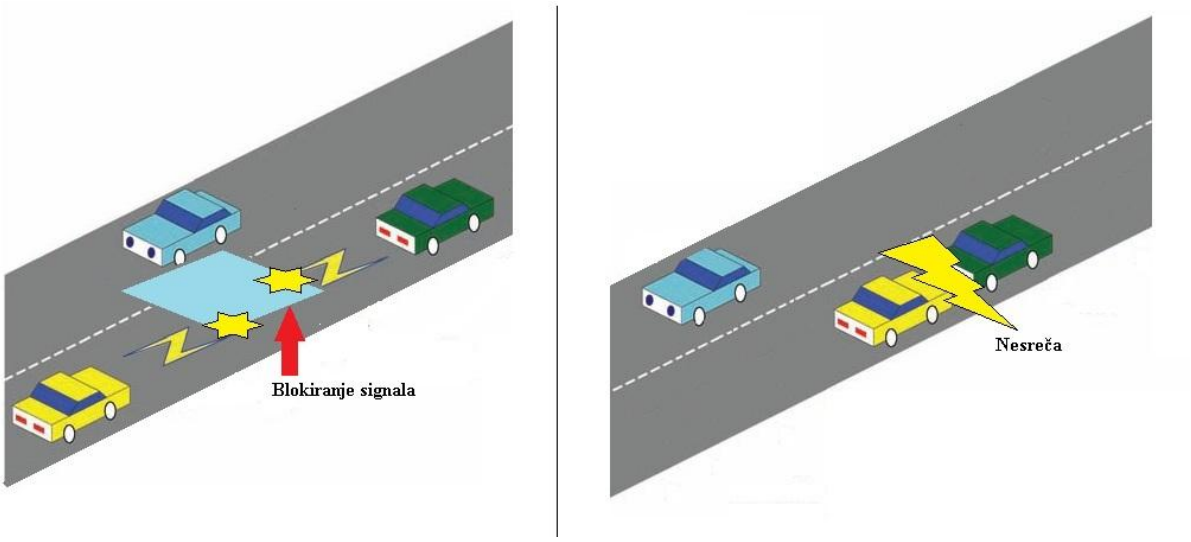
Primer napada

Napadalec se vozi sredi kolone in ima že informacijo o vseh ostalih udeležencih v prometu (pridobil jo je s predhodnim napadom za razkritje identitete). Odloči se, da bo vozilom posredoval informacijo, da je njegovo vozilo uradno vozilo na nujni vožnji (policija, reševalno vozilo). Sporoči jim, da se je zgodila nesreča in od njih zahteva, naj se čim prej umaknejo na skrajni desni pas, se po potrebi ustavijo, ali celo zapustijo avtocesto. S tem si sprosti vozni pas za nemoteno nadaljevanje vožnje.

Napadalec se lahko pretvarja tudi, da je neko drugo vozilo v koloni (na sliki Janez) in vozilu pred njim (na sliki Miha) sporoči napačne podatke o svoji trenutni lokaciji in nadaljevanju poti. Če sta vozili na skupni poti (npr. na poti na dopust), lahko tako napadalec precej pokvari prvotne načrte voznikov.

5.5.4. Napad DOS

Pri napadu DOS napadalec bodisi moti komunikacijski kanal bodisi preplavi razpoložljive vire vozila in s tem izključi točno določeno vozilo ali vsa vozila v dosegu. To lahko stori z motenjem radijskega signala ali s preobremenitvijo omrežja. Napadalec lahko tudi preprečuje izmenjavo varnostnih sporočil med vozili in s tem povzroči nesrečo.



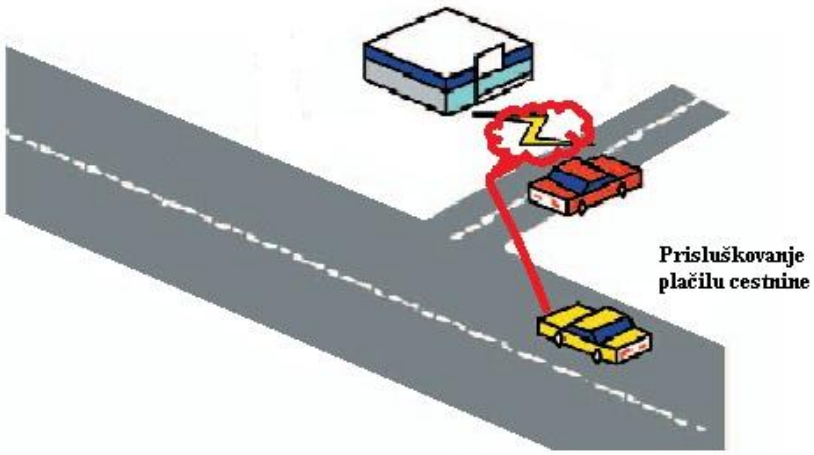
Slika 18 – Primer napada DOS z motenjem radijskega signala

Primer napada

Napadalec na nasprotnem voznem pasu opazi prometno nesrečo. Med nadaljevanjem poti vidi, da se tej nesreči z nezmanjšano hitrostjo približujeta vozili. Prvo vozilo takrat opazi nesrečo pred seboj in začne takoj pošiljati signal z informacijo o nesreči ter potrebnimi ukrepi za preprečitev nesreče (zaviranje v sili, prižiganje vseh štirih smernikov …). Točno v tem trenutku pa napadalec preplavi komunikacijski kanal z velikim številom zahtevkov in tako preobremeni omrežje. Pomembna informacija tako ne pride do ostalih udeležencev v prometu in zelo verjetno je, da bo posledica tega početja trčenje. Tega manevra bi se lahko poleg škodoželjnih ljudi posluževali tudi različni avtomobilski servisi ali zavarovalnice, vendar pa je to početje moralno sporno.

5.5.5. Prisluškovanje

S prisluškovanjem napadalec nadzira promet in s tem pridobi potrebne informacije. Tako lahko dobi podatke, kot so npr. gesla, ki jih lahko uporabi za lastno korist. Ta napad bi lahko uporabila policija za izdajanje kazni za prehitro vožnjo, lahko pa bi se tega prijema posluževala tudi podjetja in s tem pridobila podatke o vedenju voznikov.



Slika 19 – Primer napada s prisluškovanjem komercialni transakciji

Primer napada

Napadalec na postajališču prestreza signal, ki ga vozniki pošiljajo ostalim udeležencem in obcestnim enotam RSU. S tem pridobi podatke o vozilih, lokaciji, hitrosti, razna gesla in ostale informacije. Te podatke nato shrani in jih koristi po potrebi.

Tovrstnega napada bi se lahko posluževala policija, čeprav je to moralno sporno. Tako bi policijska enota le prestrezala podatke o identiteti in hitrosti vozila, ter na podlagi teh podatkov izstavljala plačilne naloge kršiteljem.

5.5.6. Virusi, črvi in zlonamerna koda

Z virusi, črvi in zlonamerno kodo napadalec napade enote OBU in RSU. Če mu uspe, lahko napadenega voznika izrabi za širjenje lažnih informacij, s čimer moti promet. Te napade lahko ublažimo s pravilno izbiro operacijskega sistema.

Primer napada

Napadalec poizkusi napasti obcestne enote RSU, ki so v njegovem dosegu. Med desetimi enotami najde eno, ki ni bila nadgrajena na najnovejšo programsko opremo in ima varnostno luknjo. Preko te namesti zlonamerno kodo ali virus, ki se nato preko te enote razširi do vseh ostalih enot v omrežju. Vsako vozilo, ki nato izmenja podatke z RSU, tudi na svojo enoto v vozilu OBU, dobi zlonamerno kodo ali virus. S tem napadalec posredno pridobi veliko število podatkov, ki bi mu lahko v bodoče omogočili izkoriščanje. Lahko pa v primeru virusa le okuži vse enote v omrežju, s tem pa razen lastnega zadovoljstva ne pridobi pomembnih podatkov.

5.5.7. Kršitev zasebnosti

Napadalec bi lahko sledil vozilom in njihovim voznikom, da bi s tem pridobil informacije o njihovem vedenju (kar bi mu omogočilo izsiljevanje). Naprednejši napadalec lahko za svoje napade uporablja celotno mrežo enot RSU, lahko pa se osredotoči le na eno samo enoto v vozilu OBU in s tem pridobi podatke o eni sami možni tarči. Vse pridobljene informacije lahko poveže z ostalimi informacijami, ki jih poseduje.

Primer napada

Napadalec prestreza promet med vozilom in obcestno enoto. S tem pridobi informacijo o identiteti, lokaciji, hitrosti, gesla, ipd. Ko prestreže podatke iskane tarče, si le-te shrani za kasnejšo uporabo. Ko od voznika, katerega podatke je prestregel, nekaj potrebuje, ga s pomočjo pridobljenih podatkov enostavno kontaktira in mu v odkup ponudi pridobljene informacije. Če se žrtev s tem ne strinja, ali če obvesti policijo, lahko napadalec podatke uporabi in s tem žrtvi povzroči precej škode, tako poslovne kot zasebne.

5.5.8. Napad z reprodukcijo

V omrežju VANET obstaja veliko število enot RSU, ki so v primeru slabe zaščite možna tarča napadalca. Če bi mu napad uspel, bi to enoto RSU lahko uporabil kot orodje pri lansiranju napadov na omrežje.

Primer napada

Napadalec preplavi omrežje s povpraševanji in tako najde enoto RSU, ki je bodisi slabo zaščitena, bodisi ni nadgrajena na zadnjo različico programske opreme (in ima zato varnostno luknjo). Le-to nato napade in jo nato uporabi za svoje napad tako, da uporabi njene podatke in se v omrežju začne predstavljati kot ta enota. Vsa vozila bi nato z njim izmenjevala vse podatke, saj bi mislila, da se pogovarjajo s pravo obcestno enoto RSU. Napadalec s tem pridobi vse potrebne podatke za nadaljnje napade.

5.5.9. Finančno izkoriščanje

Za razliko od predhodno opisanih primerov, ki so namenjeni osebnemu zadovoljstvu, preprečevanju pregona ali motnjam omrežja, predvidevamo, da bo večina napadov dejansko uperjena na pridobivanje finančnih sredstev. Takšni napadi se bodo izvajali kot kombinacija več različnih napadov. Za primer lahko navedem izdajanje za drugo vozilo in s tem brezplačno uporabljanje avtoceste, saj bi cestnino plačala žrtev napada.

Primer napada

Napadalec se vozi po cesti in se bliža plačilu cestnine. Pred njim je kolona več vozil. Zato uporabi več različnih metod, s katerimi pridobi podatke o identiteti ter kodi za plačilo cestnine vozil pred seboj. Ko se sam približa mestu za plačilo cestnine, si izbere podatke enega izmed vozil in le-te uporabi za plačilo cestnine za svoje vozilo. S tem je prihranil pri plačilu cestnine in oškodoval drugega voznika.

5.5.10. Napad na usmerjanje in prenos paketov

Pod napad na usmerjanje štejemo vsa dejanja, ki imajo za posledico napačno posodobitev usmerjevalne tabele. Pri napadu na prenos paketov napadalec doseže, da se paketi dostavijo na način, ki ni v skladu z usmerjevalno tabelo.

Primer napada

Napadalec si za tarčo izbere obcestno enoto RSU in njeno usmerjevalno tabelo. Le-to spremeni tako, da za določene ali vse poti navede, da je on najboljša možna oz. edina pot. Ko ostala vozila komunicirajo z napadeno enoto RSU, le-ta prejete podatke zaradi zastrupljene usmerjevalne tabele pošilja napadalcu. Ta podatke napadalec hrani za kasnejšo uporabo, ali pa jih preprosto zavrže.

5.6. Možni načini obrambe pred napadi v omrežju vozil

V prejšnjem odseku sem navedel različne vrste napadov na omrežje vozil, ki bi se lahko pripetili. Kako pa se pred takimi napadi obraniti? V fiksnih omrežjih je znanih že kar nekaj mehanizmov, ki preprečujejo napade. Te mehanizme lahko vpeljemo tudi v omrežja vozil. Potrebno pa bo dodati tudi nove rešitve, ki bodo primerni za omrežje, kjer se dogajajo hitre spremembe vozlišč.

Nekaj mehanizmov za zaščito pred napadi na omrežje:

- avtentikacija (strežnik Radius),
- dodeljevanje ključev,
- vpeljava certifikatov,
- zaščita WEP, WPA in WPA2,
- filtriranje MAC naslovov,
- statično dodeljevanje IP naslova.

Glede na specifiko omrežja vozil je statično dodeljevanje IP naslova in filtriranje MAC naslovov v tem omrežju neprimeren pristop, predvsem zaradi velikega števila vozlišč, kot tudi hitrih sprememb lokacije vozil.

Pri preprečevanju napadov na omrežja vozil je potrebno povzeti korake zaščite fiksnih omrežij. Preprečiti je potrebno fizični dostop do omrežnih elementov s strani nepooblaščenih oseb (tako obcestnih enot RSU kot vozil). Nato je potrebno vpeljati zaščito brezžičnega signala in izbrati tisto, ki ponuja največjo mero zaščite (npr. WPA2).

Najprimernejša in najpogosteje omenjena zaščita v omrežju vozil je uporaba ključev. Pri tem bo vsakemu vozilu v omrežju dodeljen javni in privatni ključ, ki ga bo nato sistem uporabil pri podpisovanju varnostnih sporočil. Prejemnik sporočila bo ravno tako imel nameščene

potrebne ključe, da bo prejeto sporočilo lahko dešifriral. Ob uporabi ključev je potrebno zagotoviti napravo, ki bo omogočala njihovo varno hrambo.

Druga možnost je vpeljava elektronske registrske tablice. Le-te bodo dodatek klasičnim registrskim tablicam na vozilu, njihova prednost pa je v samodejnem preverjanju dokumentacije vozila (npr. podatki o tehničnem pregledu in lastniku). Omogočale bodo tudi identifikacijo ukradenih vozil in s tem preprečevale vdor nepooblaščenih oseb v sistem. Smiselno je, da elektronske registrske tablice izdaja država, kjer je vozilo registrirano.

Dobrodošla pri razreševanju nepojasnjenih dogodkov je vpeljava »črne škatle«, kot jo poznamo v letalskem prometu. Z njo bi v vozilu beležili vse pomembne parametre, še posebno v primeru nesreč ali vdorov v sistem. Te podatke bi kasneje uporabili za rekonstrukcijo nepredvidenih dogodkov ali za odpravo varnostnih lukenj v sistemu.

Ker veliko napadov uporablja lokacijske podatke, je pomembno, da je sporočena lokacija vedno pravilna. Sporočeno GPS lokacijo lahko preverimo z izračunom lokacije glede na različne točke v omrežju (npr. glede na ostala vozila). Izračunana lokacija se ne sme bistveno razlikovati od sporočene GPS lokacije.

Najverjetneje bodo za zaščito vozil poskrbeli že proizvajalci sami. Potrebno pa bo zagotoviti posodabljanje zaščite in krpanje varnostnih lukenj. To delo bi lahko prevzeli tako proizvajalci vozil kot vzdrževalci omrežja, saj bodo le-ti že tako posodabljali obcestno infrastrukturo. Zagotoviti bo potrebno tudi zaščito vseh aplikacij, napisanih za uporabo v omrežju vozil s strani nepooblaščenih oseb, predvsem bodo tu na udaru varnostne aplikacije.

Ker pa so napadalci navadno vedno korak pred vzdrževalci sistemov, bo v bodoče potrebno vseskozi spremljati novosti na področju zaščite omrežij, hkrati pa bodo morali vzdrževalci sami aktivno sodelovati pri odkrivanju in odpravljanju varnostnih lukenj.

6. SKLEPNE UGOTOVITVE

Na slovenskih cestah se število smrtnih žrtev vsako leto zmanjšuje. K temu pripomore tako boljša pasivna varnost v vozilih kot tudi vedno novejši vozni park. Če bi proizvajalci vpeljali v vsako vozilo še tehnologijo, ki sem jo obravnaval v tej diplomski nalogi, bi se število smrtnih žrtev v prometu lahko približalo tudi številki nič.

Kdaj bodo proizvajalci vpeljali tehnologijo v vozila, je odvisno od cestne infrastrukture. Tehnologija, ki bi to omogočala, danes obstaja in je že dodobra razširjena. Potrebno bi bilo le malo napora in sodelovanja med državnimi institucijami, operaterji in proizvajalci, da bi tak sistem zaživel. Nekateri proizvajalci v svoja vozila že danes vgrajujejo zametke sistemov, ki bodo v prihodnosti reševali življenja. To so predvsem moduli za dostop do WiFi in UMTS omrežja in različne informativne aplikacije.

Ker se vozila v omrežje vozil priključijo in ga uporabljajo pri visokih hitrostih, je potrebno zagotoviti nemoteno delovanje tudi pri tem elementu. Poleg tega je potrebno zagotoviti še hitro odzivnost in visoko razpoložljivost omrežja. Omrežje vozil ima potencialno velik obseg, saj bo potrebno tako omrežje zagotoviti v vseh državah. Uporaba le znotraj ene države pravzaprav ni smiselna.

V veliki meri bo uspešnost vpeljave sistema odvisna tudi od varnosti. Potrebno bo zagotoviti izredno varno omrežje, ki praktično ne bo omogočalo vdorov in napadov. Napadov se v celoti sicer ne da izključiti, saj napadalci dnevno izumljajo nove načine vdorov. V tej diplomski nalogi sem preučil primere napadov na omrežje vozil in na podlagi tega lahko trdim, da bodo napadi v omrežju večinoma povezani, saj s samo eno vrsto napada napadalec ne pridobi vseh potrebnih podatkov. Najbolj problematični napadi bodo tisti, ki bodo neposredno vplivali na varnost potnikov, kot tudi napadi, s katerimi se bodo napadalci finančno okoristili.

Ne smemo pa pri načrtovanju omrežja, aplikacij in varnosti pozabiti na zasebnost in zaupanje. Zasebnost bo potrebno upoštevati že ob načrtovanju omrežja vozil in opreme, zaupanje pa bodo morali vzpostaviti uporabniki sami.

KAZALO SLIK

KAZALO TABEL

SEZNAM VIROV LITERATURE

[1] David N. Cottingham, Vehicular wireless communications, 2009. Dostopno na: http://128.232.0.20/techreports/UCAM-CL-TR-741.pdf

[2] Pedro Fernandes, Urbano Nunes, Vehicle communications: a short survey, 2007. Dostopno na:
http://www.isr.uc.pt/~pedro/iadis2007.pdf

[3] Hannes Hartenstein, Kenneth P. Laberteaux, Vehicular Applications and Inter-Networking Tehnologies, 2010.

[4] E. Hossain et al., Vehicular telematics over heterogeneous wireless networks: A survey, Comput. Commun., 2010.

[5] Chung-Ming Huang, Yao-Chung Chang, Telematics Communication Tehnologies and Vehicular Networks: Wireless Architectures and Applications, 2009.

[6] M. Raya, J.-P. Hubaux, Security Aspects of Inter-Vehicle Communications, 2005. Dostopno na:
http://infoscience.epfl.ch/record/33742/files/RayaH05A.pdf

[7] M. Raya, J.-P. Hubaux, The Security of Vehicular Networks, 2005. Dostopno na: http://ic2.epfl.ch/publications/documents/IC_TECH_REPORT_2005009.pdf

[8] Hassnaa Moustafa, Yan Zhang, Vehicular Networks: Tehniques, Standards and Applications, 2009.

[9] José Santa, Antonio F. Gómez-Skarmeta, Marc Sánchez-Artigaz, Architecture and evaluation of a unified V2V and V2I communication system based on cellular networks, 2007.
Dostopno na:
http://202.114.89.42/resource/pdf/2731.pdf

[10] Wikipedia: Controller area network. Dostopno na:
http://en.wikipedia.org/wiki/Controller_area_network

[11] Wikipedia: GSM. Dostopno na:
http://en.wikipedia.org/wiki/gsm

[12] Wikipedia: IEEE 802.11. Dostopno na:
http://en.wikipedia.org/wiki/802.11

[13] Wikipedia: IEEE 802.20. Dostopno na:
http://en.wikipedia.org/wiki/802.20

[14] Wikipedia: Intelligent transportation system. Dostopno na:
http://en.wikipedia.org/wiki/Intelligent_Transport_Systems

[15] Wikipedia: OSI model. Dostopno na:
http://en.wikipedia.org/wiki/OSI_model

[16] Wikipedia: Universal Mobile Telecommunications System. Dostopno na:
http://en.wikipedia.org/wiki/Umts

[17] Wikipedia: Vehicular communication systems. Dostopno na:
http://en.wikipedia.org/wiki/Vehicular_communication_systems

[18] Wikipedia: Wireless security. Dostopno na:
http://en.wikipedia.org/wiki/Wireless_security

[19] Wikipedia: ZigBee. Dostopno na:
http://en.wikipedia.org/wiki/ZigBee

[20] ZigBee Alliance. Dostopno na:
http://www.zigbee.org/