Računarska mreža: Mozak savremenog automobila

Seminarski rad u okviru kursa
Metodologija stručnog i naučnog rada
Matematički fakultet

Bajić Ana, Krstić Dušica, Stanojević Kristina
ana.bajic13@gmail.com, dusica@omikron.org.rs, stanojevic.kristina@gmail.com

18. april 2018.

Sažetak

U ovom radu je prikazana trenutna arhitektura računarskih mreža u modernim vozilima, sa osvrtom na jedinice za kontrolu rada motora, kontrolu prenosa, kontrolu perifernih delova vozila i kontrole sistema protiv blokiranja kočnica. Zatim su razmatrani različiti protokoli komunikacije između kontrolnih jedinica, a nakon njihovog uvođenja je skrenuta pažnja na ozbiljan nedostatak odbrambenih mehanizama u vozilima. Prikazani su mogući napadi, motivi za njih i jedinice mreže koje su im meta. Na kraju, predstavljeni su već postojeći ali i planirani mehanizmi za odbranu.

Ključne reči — CAN, ECU, elektronski moduli, računarska mreža, kontrola vozila, bezbednost mreža

Sadržaj

1 Uvod

Glavna motivacija za razvoj mrežnih tehnologija u vozilima su bili napreci u elektronskoj industriji i nove zakonske regulative koje su postavile znatna ograničenja kako bi se smanjio negativan uticaj automobila na životnu sredinu. Sa striktno postavljenim zahtevima, postalo je nemoguće dostići propisani standard bez pomoći računara. Njihovo korišćenje u ovom domenu su omogućile mreže. Iako mreže nisu bile novo otkriće, njihova primena u automobilskoj industriji jeste. Uspešna implementacija je zahtevala nisku cenu implementacije, stabilnost, mogućnost funkcionisanja u lošim spoljašnjim uslovima, robusnost i pouzdanost.

2 Komponente računarskih mreža

Računarska mreža u vozilu je specijalizovana komunikaciona mreža koja povezuje komponente u vozilu. Glavni preduslovi za postizanje željene kontrole nad vozilom su brzo, "jeftino"i pouzdano razmenjivanje poruka između sistema za kontrolu, nekonfliktnost tih poruka, redundantno rutiranje i otpornost sistema na elektromagnetne smetnje.

U automobilskoj industriji do skorijeg vremena jedini elektronski uređaj u kolima je bio radio, ali danas skoro nijedna komponenata ne može da radi bez neke veze sa računarom - počevši od srca automobila, tj. motora, kako bi se njegove performanse dovele do maksimuma, pa do manje bitnih komponenti kao što je svetlo u kabini.

Od 1996. godine, počevši od Sjedinjenih Američkih Država, svi automobili koji su pušteni u prodaju moraju imati konektor za kontrolnu dijagnostiku sistema (eng. *On-Board Diagnostics*). OBD daje pristup statusima raznih podsistema u vozilu. Količina informacija, dostupnih kroz ovaj sistem[20], je evoluriala od jednostavnih svetlosnih signala do pružanja standardizovane serije dijagnostičkih kodova problema, što je za rezultat imalo brže identifikovanje i rešavanje problema u vozilu [22].

Glavne komponente računarskih mreža u današnjim vozilima uključuju:

1. Jedinicu za kontrolu rada motora (eng. *Engine Control Unit*)[19]
2. Jedinicu za kontrolu prenosa (eng. *Transmission Control Unit*)[21]
3. Sistem protiv blokiranja kočnica (eng. *Anti-lock Break System*)[16]
4. Module za kontrolu perifernih delova vozila (eng. *Body Control Module*)[17]

Dodavanjem senzora i kombinovanjem informacija, dostupnih kroz ove četiri komponente, mogu se implementirati razni drugi podsistemi u vozilu poput: sistema za regulaciju proklizavanja pogonskih točkova, sistema za sprečavanje blokiranja točkova pri intezivnom kočenju, sistema za regulaciju dinamike vožnje, elektronska regulacija prenosa snage na pogonske točkove, elektronska regulacija amortizera, sistem za kontrolu proklizavanja itd.

2.1 Elektronski kontrolni moduli

Svaki modul predstavlja zaseban čvor na računarskoj mreži, kontroliše određene komponente povezane sa njegovom funkcijom i komunicira sa određenim modulima po potrebi, koristeći standardne protokole za komunikaciju. Mreža kontrolne oblasti (eng. *Control Area Network*), koja predstavlja centralni deo mreže, sadrži prijemnik i odašiljač (eng. *transmitter*)

za komunikaciju između sistema za kontrolnu dijagnostiku i kontrolera, kao i za međusobno povezivanje između čvorova.

Kako bi se podržale sve akcije koje su određene nekim konkretnim modulom uz senzore se koriste i aktuatori. Podatke dobijene od senzora (za brzinu, temperaturu, pritisak, itd.), elektronski kontrolni moduli, koriste dalje u izračunavanjima i dobijene podatke razmenjuju između sebe, kako bi se omogućilo normalno funkcionisanje vozila. Ovo se postiže povezivanjem modula na mrežu. Ovakva arhitektura olakšava posao i proizvođačima jer je moguće dodavati i uklanjati podsisteme bez uticaja na celu arhitekturu [23].

2.1.1 Jedinica za kontrolu rada motora

Pre pojavljivanja jedinice za kontrolu rada motora, vreme paljenja, idealna brzina i mešavine vazduha i goriva su bili mehanički podešavani i dinamički kontrolisani preko mehaničkih i pneumatskih sredstava. Ova jedinica je tip elektronske kontrolne jedinice koja kontroliše seriju aktuatora na sus motoru, kako bi obezbedila otpimalne performanse motora. Ovo se realizuje skupljanjem podataka sa mnoštva senzora koji se nalaze u prostoru motora, interpretacijom tih podataka korišćenjem look-up tabela i prilagođavanjem aktuatora motora u skladu sa obrađenim podacima.

Ukoliko ECU ima kontrolu nad dotokom goriva, onda se naziva jedinica za kontrolu sus motora (eng. *Electronic Engine Management System*). Ceo mehanizam EEMS-a je kontrolisan od strane skupa senzora i aktuatora. Posebna kategorija ECU-a su oni koji nemaju fiksno ponašanje i mogu biti reprogamirani od strane korisnika. Oni su potrebni kada se na motoru rade razne izmene nakon proizvodnje. Može se desiti da nakon dodavanja određenih izmena stariji ECU ne podržava novu konfiguraciju, pa se zato priključuje ECU koji se može programirati.

Savremeni ECU koriste mikroprocesor koji omogućava real-time obradu informacija dobijenih od senzora motora. Sastoji se od hardvera i softvera. Hardver je sačinjen od elektronskih komponenti na štampanoj ploči i keramičkog ili tankog laminatnog supstrata. Glavna komponenta na štampanoj ploči je mikro kontrolni čip/centralno procesorska jedinica. Softver je skladišten u mikrokontroloru ili drugim čipovima na štampanoj ploči, obično na EPROM-ovima (eng. *Erasable Programmable Read-Only Memory* [3])ili flash memoriji, tako da se CPU može reprogramirati.

2.1.2 Jedinica za kontrolu prenosa

Jedinica za kontrolu prenosa je uređaj koji kontroliše moderne elektronske automatske prenose. TCU najčešće koristi senzore u vozilu, ali i podatke koje dobija od jedinice za kontrolu rada motora, da izračuna kako i kada treba promeniti brzinu vozila za optimalne performanse, ekonomičnu potrošnju goriva i pritom da to bude neprimetno putnicima u vozilu.

Dizajn elektronskih automatskih prenosa se menjao od čisto hidromehaničkih kontrola do elektronskih kontrola, koje su u upotrebi od kasnih osamdesetih godina prošlog veka. Do danas, razvoj je bio iterativan i današnji dizajn predstavlja nadogradnju pređašnjih. Aktuatori u menjaču su ključna komponenta u ovim kontrolnim jedinicama.

Evolucija modernog automatskog prenosa i integracija elektronskih kontrola su omogućile ogroman napredak u skorije vreme. Danas je moguće ostvariti bolju potrošnju goriva, smanjeno ispuštanje izduvnih gasova,

veću pouzdanost prilikom menjanja brzina, brže i neprimetnije menjanje brzina i bolju kontrolu nad celim vozilom. U nekim slučajevima se TCU i ECU spajaju u jednu jedinicu - pogonski kontrolni modul.

2.1.3 Sistem protiv blokade kočnica

Sistem protiv blokade kočnica je bezbednosni sistem koji dozvoljava točkovima na motornom vozilu da zadrže vučni kontakt sa površinom puta u skladu sa kočenjem vozača i sprečava prestanak rotacije točkova i nekontrolisano klizanje po putu. Ovo je automatizovan sistem koji koristi principe ritmičnog kočenja uz menjanje praga kočenja koji postiže mnogo bolju kontrolu i brže kočenje nego što bi većina iskusnih vozača uspela da ostvari.

ABS generalno nudi poboljšanu kontrolu vozila i smanjuje zaustavno rastojanje na suvim i klizavim površinama, iako na površinama pokrivenim šljunkom ili snegom može povećati zaustavno rastojanje i dalje pružati bolju kontrolu nad vozilom. Skorije verzije ovog sistema ne samo da sprečavaju blokiranje točkova nego elektronski kontrolišu i odnos između kočenja prednjih i zadnjih točkova.

Uobičajeno, ABS se sastoji od elektronske kontrolne jedinice (ECU), četiri senzora za brzinu točkova i najmanje dva hidraulička ventila u okviru hidraulike kočnica. ECU konstantno nadgleda rotacionu brzinu svakog točka i u slučaju da se neki točak ne kreće u skladu sa brzinom vozila nego se okreće sporije ili brže, prilagođava ventile kako bi se smanjio ili povećao hidraulički pritisak na kočnice na točkovima, što za rezultat ima smanjenje ili povećanje kočione sile na tom točku pa on počinje da se brže ili sporije okreće.

Moderni ABS sistemi mogu primeniti individualni kočioni pritisak na svaki od četiri točka kroz kontrolni sistem senzora koji se nalazi na glavnini točkova povezanih sa mikrokontrolorom. Često su im dodata dva dodatna senzora, ugaoni senzor na volanu i žiroskopski senzor, koji pomažu sistemu da radi bolje. U slučaju nekog kvara na ABS sistemu, biće signalizirano na kontrolnoj tabli i ABS će biti onemogućen dok se nepopravi. ABS igra glavnu ulogu u podsistemu za zaštitu od proklizavanja vozila.

2.1.4 Sistem za kontrolu perifernih delova vozila

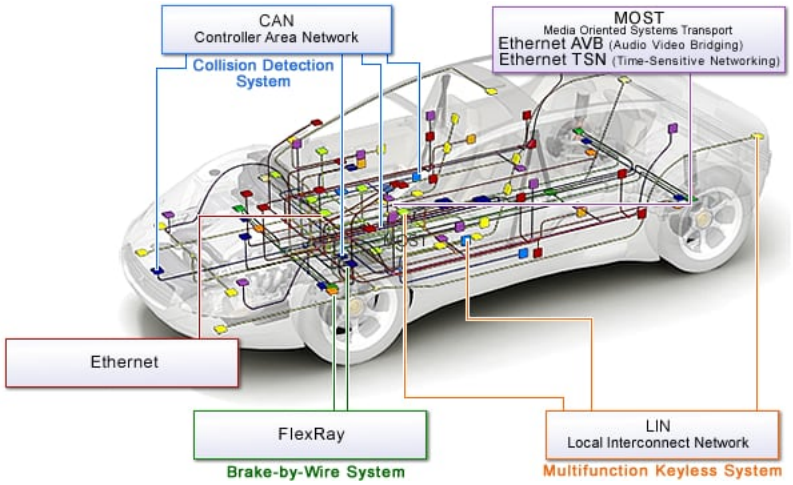
BCM je elektronska kontrolna jedinica odgovorna za nadgledanje i kontrolu raznih elektronskih dodataka u vozilu, poput: automatskih prozora, retrovizora, klima uređaja, centralnog zaključavanja itd. Komunicira sa drugim sistemima u vozilu preko računarske mreže vozila i njegova glavna primena je da kontroliše aktiviranje releja koji izvršavaju izdate akcije (npr. zaključavanje vrata).

3 Protokoli komunikacije

Računarske mreže u vozilima interno povezuju komponente unutar bilo koje vrste vozila. Svi uslovi koji bi trebalo da budu ispunjeni kada se govori o računarskim mrežama, poput sigurnosti u slanju poruka, rešavanje konflikta, minimalno vreme pristizanja poruka, efikasnost i slično, zahtevaju korišćenje protokola posebno definisanih za ovu problematiku. Različiti skupovi ovih modula zahtevaju različite tipove mreže. U dana–šnjim vozilima postoje dva tipa mreže: veoma brze mreže u delu za pogon i spore mreže u sistemu za kontrolu perifernih delova vozila. Podela mreže

je takva da predstavlja jednu lokalnu mrežu ili jednu funkcionalnu celinu. U ovim podeljenim mrežama, različiti delovi mreže mogu koristiti različite protokole. Na primer, jedna particija može da koristi CAN protokol, druga LIN protokol itd., kao što je prikazano na slici 1.

Osnovni zahtevi koje bi trebalo ispuniti jesu efikasno trošenje goriva, eliminisanje bregastih osovina u motoru i delova koji crpe energiju, smanjenje težine vozila, povećanje sigurnosti. U vozilima se često koriste dve serijske magistrale, jedna za sistem koji kontroliše pogon, a druga za periferne delove. Proizvođači se trude da proizvedu što sigurnije vozilo i sa što boljim sistemom za upravljanje vozilom. U tabeli 1 se može videti koje protokole koriste neki od proizvođača u zavisnosti od tipa vozila.



Slika 1: Primer korišćenja protokola u automobilu

Postoje različiti tipovi protokola [9] koji se mogu koristiti. Neki od tih protokola su:

- **CAN** - (eng. *Controller Area Network*) Protokol koji se najčešće koristi kao LAN mreža vozila. Spada u sporu mrežu sa serijskom magistralom za prenos poruka, a koristi Non Return to Zero (NRZ) kodiranje. Sadrži 5 mehanizama za detekciju grešaka.
- **FlexRay** - Brza mreža koja omogućava visok stepen fleksibilnosti i pouzdanosti. Koristi point-to-point topologiju zvezde. Magistrala sa ovim protokolom dobro podnosi greške.
- **LIN** - (eng. *Local Interconnect Network*) Koristi se u serijskim magistralama koje služe za komunikaciju između inteligentnih senzora, kao i za periferne uređaje poput klima uređaja, vrata, sedišta i slično.
- **MOST** - (eng. *Media Oriented Systems Transport*) Najčešći protokol kada su u pitanju multimedijalne mreže. Dizajniran tako da omogući prenos audio i video sadržaja kao i podataka visokog kvaliteta.
- **D^{2}B** - (eng. *Domestic Digital Bus*) Multimedijalni interfejs velike brzine. Koristi se u optičkim magistralama koje povezuju audio, video, kompijuterske i telefonske komponente u jednu prstenastu strukturu.
- **Byteflight** - Koristi se u sistemima koji se odnose na sigurnost (na primer za aktiviranje vazdušnog jastuka).

- **J1850** - Za deo vozila koji sadrži dijagnostičke aplikacije i aplikacije za deljenje podataka.
- **IEBus** - Protokol zasnovan na CSMA/CD (eng. *Carrier Sense Multiple Access/Collision Detection*) pristupu mreži. Prenos podataka se vrši kroz dve linije, Data+ i Data-, u dva smera.
- **J1708** - Koristi se samo u fizičkom sloju i to u serijskim magistralama, za komunikaciju između mikrokompjutera u vozilu.
- **A^2B** - (eng. *Automotive Audio Bus*) Protokol audio distribucije. Ovim protokolom se dobija visoka vernost zvuka (eng. *High fidelity*, Hi-Fi) uz smanjenje težine kablova i veće efikasnosti u trošenju goriva [5].

Tip protokola	**Godina početka**	**Proizvođač**	**Tip vozila**
CAN	1986	Bosch	razno
J1850	-	GM Ford	automobili
	2008	Chrysler	
FlexRay		BMW Volkswagen Daimler AG	
	-	General Motors	
MOST	?	Ford BMW Daimler GM	
VAN	2000	PSA Peugeot Citroën	
J1708	1985	Volvo AB	teški terenac

Tabela 1: Koje protokole koriste neki od proizvođača

4 Bezbednost mreža

Svaki računarski sistem može biti preplavljen propustima i slabostima koje napadač može da iskoristi ako je povezan na sistem [15]. Elektronskim kontrolnim jedinicama (ECU) nije lako pristupiti van vozila, te implementacija bezbednosnih mehanizama u računarskim mrežama u vozilima nije bila velika briga proizvođača.

Umrežavanje je trend današnjice. Moderna vozila često poseduju interfejse koji omogućavaju kako komunikaciju preko magistrala tako i bežičnu komunikaciju. Uvođenjem API-ja (eng. *Application Programming Interface* [4]) za bežičnu komunikaciju, mreže u automobilima su prestale da budu zatvorene i sajber-napadi su postali realnost.

4.1 Razlozi napada

Napadači računarskih mreža u automobilima mogu imati jedan ali i više motiva za napad. U nastavku se razmatraju neki od njih, kao i njihove posledice.

Krađa

Svakako najočiglednija i najčešća vrsta napada. Napadač može da iskoristi neki prisutni propust u bežičnoj komunikaciji i na taj način tiho i neprimetno otključa automobil i zatim deaktivira alarm.

Elektronska podešavanja

Napadač je upravo vlasnik ciljanog automobila. Vlasnik može da pristupi kodu ili podacima i promeni ih. Na primer, može da smanji kilometražu automobila pre prodaje, izvrši podešavanje motora i dobije više snage ili instalira nedozvoljene programe.

Sabotaža

Sabotaža podrazumeva deaktivaciju ECU, menjanje njihovog softvera ili DOS (eng. *Denial Of Service* [2]) napade na mrežu. Posledice ovih napada se protežu od minornih (zaključavanje klima uređaja) do potencijalno smrtonosnih (zaključavanje kočnica).

Intelektualna krađa

Napadač može da pokuša da pristupi poverljivim informacijama o mreži ciljanog vozila. To se može postići prisluškivanjem magistrale ili pristupanjem izvornom kodu neke ECU. Ovakvi napadi mogu da omoguće proizvodnju falsifikovanih ECU.

Povreda privatnosti

Sa povećanjem broja elektronskih komponenti, povećava se i količina privatnih informacija koje te komponente skupljaju. Napadač može da pristupi telefonskom imeniku vlasnika kao i istoriji poziva ili istoriji GPS koordinata.

4.2 Unutrašnji napadi

Održavanje bezbednosti mreža je postalo značajan problem s obzirom na to da posledice napada mogu biti veoma ozbiljne, a napadi se mogu lakše izvesti zahvaljujući izuzetno brzom razvoju mreža. Unutrašnji napadi podrazumevaju napade kod kojih napadač ima direktan pristup vozilu.

4.2.1 Ranjivost magistrale

Ranjivosti koje postoje u trenutnim protokolima, prvenstveno CAN, su detaljno opisane u [24], [7]. Pokazano je da CAN ne može da garantuje sledeće osobine:

- Poverljivost:

  Dizajn je takav da se svaka poruka poslata na CAN i fizički i logički šalje svakom čvoru. Ovo omogućava zlonamernim čvorovima da prisluškuju magistralu i čitaju sadržaj svakog paketa.

- Autentifikacija:

  CAN paket ne podrazumeva polje za autentifikaciju svog pošiljaoca. Dakle, svaki čvor može da pošalje poruku koju bi trebalo da može da šalje samo jedan specifičan čvor.

- Dostupnost:

  Veoma je lako izazvati DOS napad na magistrali. Na primer, neka jedinica može da preplavi magistralu paketima visokog prioriteta i time zaustavi prenos paketa ostalih ECU.

- Integritet:

  CAN koristi CRC (eng. *Cyclic Redundancy Check* [18]) da proveri da li je poruka promenjena usled greške. Ovaj mehanizam ne može da spreči napadača koji želi da promeni ispravnu poruku jer je lako napraviti ispravan CRC za lažnu poruku.

4.2.2 Lokalni napadi

Napadi na magistralu se mogu izvršiti ili povezivanjem uređaja na magistralu ili preko OBD (eng. *On Board Diagnostics*) porta. OBD predstavlja sposobnost vozila da identifikuje i prijavi postojeće probleme. Preko ovog porta se može prisluškivati komunikacija na magistrali ali mogu se slati i paketi.

Postoje mnogi dokumentovani primeri napada bazirani na direktnom pristupu unutrašnjoj mreži. Napad počinje iz 'black-box' perspektive [7]. Na taj način, napadač se upoznaje sa značenjem paketa i njihovih identifikatora. Zatim, zlonamerna ECU može da ponovi kontrolne instrukcije i pošalje ih drugim ECU, predstavljajući se kao validan izvor instrukcija [8]. Neke ECU je čak moguće i reprogramirati kroz mrežu [11], čime se vozilo ostavlja u kompromitovanom stanju.

Koscher u svom radu [11] prikazuje način napada na ECU koja se nalazi na delu magistrale koji se razlikuje od ulazne tačke napadača. Napad se može izvršiti tako što se prvo ciljaju i reprogramiraju ECU koje predstavljaju kapiju između magistrala.

Dakle, ako napadač kontroliše makar jedan čvor mreže, trenutna arhitektura i protokoli su takvi da mu je omogućeno da preuzme kontrolu nad bilo kojom ECU vozila. Mogao bi se postaviti argument da je potreban direktan, fizički pristup kako bi se izvršio bilo koji od navedenih napada. Sa druge strane, moderni automobili poseduju mogućnost bežične komunikacije. Napadačima više nije potreban direktan pristup ciljanom vozilu. U sledećem odeljku će biti prikazani takvi napadi.

4.3 Spoljašnji napadi

2011. godine, Checkoway je uspeo da reprodukuje napade opisane u prethodnom odeljku pronašavši i iskoristivši ranjivosti u interfejsu za komunikaciju, bez fizičkog pristupa samoj mreži [11]. Spoljašnji napadi mogu biti grupisani na sledeći način, po distanci: indirektan pristup, bežični pristup malog dometa i bežični pristup širokog dometa. Svaki od ovih pristupa će u nastavku biti opisan i biće dati neki mogući scenariji napada.

4.3.1 Indirektan pristup

U ovom odeljku, pažnja je posvećena napadima koji se oslanjaju na kompromitovanim uređajima koji će biti povezani sa vozilom. Za razliku od unutrašnjih napada, povezivanje sa mrežom ne čini napadač, već vlasnik vozila.

- OBD port:

  Ranije (odeljak 4.2.2) je prikazano kako se sam OBD port može koristiti u napadima. U ovom slučaju, meta napada je uređaj za dijagnostiku koji je priključen na port. Taj uređaj se kontroliše putem laptopa preko WiFi-a: ranjivosti u API-u za komunikaciju su omogućile da se ubaci shell skripta u taj uređaj preko drugog

laptopa na istoj WiFi mreži. Zatim bi uređaj emitovao zlonamerne pakete preko mreže vozila svaki put kad bi bio priključen [1].

- CD plejer:
  U radu [1] su identifikovane dve ranjivosti u CD plejeru. Ubacivanje CD-a na kome se nalazi datoteka specifičnog imena može da zavara plejer da pomisli da je u pitanju neko fabričko ažuriranje. Uređaj će zatim instalirati novi, maliciozni softver. Još jedan propust je u dekodovanju audio datoteka - moguće je napraviti datoteku koja će izazvati slanje poruka preko magistrale dok je plejer čita.

4.3.2 Napadi malog dometa

Ovi napadi koriste bežične komunikacione tehnologije. Mogu biti direktni, gde se napada komunikacioni modul vozila, i indirektni, gde se napada uređaj vozača koji se može priključiti na vozilo.

- Bežično povezivanje sa mobilnim uređajem:
  Savremena vozila je moguće spojiti sa različitim uređajima putem Bluetooth konekcije. Implementacije ovakvih protokola mogu imati propuste. Ti propusti se mogu iskoristiti za osluškivanje konverzacija, prikupljanje podataka kao i samo kompromitovanje ECU [1].
- Komunikacija između vozila:
  Komunikacija između vozila je u razvoju. Vozilo će moći da komunicira sa drugim vozilima na putu tako što će ih obaveštavati o svom statusu. Na primer, vozilo će moći da obavesti svog vozača o mogućoj nesreći (ako vozilo ispred naglo zakoči ili ako ima nadolazećih vozila na raskrsnici) ili će moći samo da se prilagodi novonastalim uslovima. Analizom rizika došlo se do zaključaka da se komunikacija između vozila može prisluškiavti, mogu se slati lažni podaci kako bi se izazvale neprikladne rekacije vozila kao i da se mogu kompromitovati ECU odgovorne za ovu komunikaciju [12].

4.3.3 Napadi širokog dometa

U ovu kategoriju spadaju napadi koji se prenose preko bežičnih komunikacionih tehnologija dalekog dometa. Potreban je kanal za prenos dugih signala kao i kompromitovanje uređaja posrednika.

- Mobilna telefonija:
  Checkoway je otkrio nekoliko ranjivosti u uređaju za telekomunikaciju [1]. Iskoristivši to, uspeo je da izvrši proizvoljan kod koji je preuzeo putem 3G mreže i time kompromituje vozilo.
- Aplikacije:
  Slično trendu koji je prisutan na pametnim telefonima, neki proizvo–đači vozila nude aplikacije koje je moguće preuzeti sa njihovih web prodavnica. Uspešan napad na samu prodavnicu, ili pak postavljanje programa koji sadrži virus bi mogao da ima veoma ozbiljne posledice na mrežu vozila.

4.4 Mehanizmi zaštite

Vozila poseduju mnoge komunikacione kanale koji lako mogu postati ulazne tačke u mrežu za napadače. Što je više napada, i što su oni napredniji, to se više kontramera sprovodi. U ovom odeljku su predstavljene tehnike zaštite koje su trenutno u razvoju.

Postoji veliki broj odbrambenih mehanizama za slične napade na regularne računare. Za razliku od njih, računari u vozilima imaju neka ograničenja. Najveće ograničenje predstavlja hardver [25]. Računari u vozilima poseduju malu, ograničenu memoriju i snagu, te ECU ne mogu da izvršavaju napredne kriptografske funkcije kojima se postiže jaka enkripcija. Takođe, za izvođenje kompleksnih instrukcija je potrebno više vremena, a potrebno je da aplikacije rade brzo kako bi se osigurala bezbednost vozila i putnika. Dakle, bezbednosni mehanizmi ne smeju previše uticati na performanse softvera.

Hardver mora biti proizveden tako da dugo traje i bude izdržljiv (neke komponente moraju da izdrže visoke temperature, pritisak itd.). Softver za zaštitu bi trebalo proizvesti tako da ga je lako ažurirati. Nije lako ni jeftino, a čak ni moguće, zameniti i unaprediti hardver na kome se nalazi softver za zaštitu.

4.4.1 Zaštita spoljašnje komunikacije

Kao što je prikazano u prethodnom odeljku 4.2.2, jedan propust u rukovođenju komunikacijama je dovoljan da se kompromituje celo vozilo. Prvi korak je zaštita tih kanala. Mnogi od navedenih napada su bili mogući zbog mana u implementaciji samog softvera ili neslaganja sa specifikacijama proizvođača. Neki od njih su mogli biti sprečeni striktnim pridržavanjem dobrih programerskih praksi i postojećih preporuka o komunikacionim protokolima [13].

Sa druge strane, postoji mnogo različitih proizvođača koji imaju različite standarde, te je nemoguće napisati softver koji je saglasan sa svim preporukama i specifikacijama. Proizvođači vozila su postali svesni ovih problema i počeli su da finansiraju velike projekte. Neki od njih, na primer SEVECOM [10], PRESERVE [14] i EVITA [6], imaju za cilj dizajniranje bezbednih arhitektura za komunikaciju unutar i između vozila.

4.4.2 Unutrašnja zaštita

Trenutno se razmatra više rešenja kad je u pitanju bezbednost CAN magistrale. Možemo ih grupisati u tri kategorije: kriptografska rešenja za autentifikaciju i enkripciju paketa koji se šalju preko magistrale, rešenja za detekciju anomalija koje se javljaju u sistemu i rešenja koja osiguravaju integritet softvera.

- Kriptografija

  Kriptografska rešenja omogućuju autentifikaciju ECU, provere integriteta i enkripcju poslatih paketa, čime ga samo čvorovi koji poseduju ispravan ključ mogu pročitati. Kako kriptografski algoritmi ne bi ometali izvršavanje ostalih funkcija sistema, mogu se koristiti hardverski moduli koji isključivo služe za izvršavanje kriptografskih operacija.

- Detekcija anomalija

  Prate se podaci koji se prenose između ECU i potvrđuje se njihova ispravnost. Na primer, prati se razmak između dva poslata paketa i, ako je on prekratak, ECU koji ih je poslao se blokira. Drugo rešenje je da se svakom paketu dodeli poseban identifikator koji predstavlja ECU koji može da ga šalje. Time je obezbeđeno da taj paket može poslati samo jedna ECU.

- Integritet ECU softvera

  Preduzimaju se mere koje štite kritični softver vozila. Na primer, EVITA definiše pouzdanu platformu vozila, čime se štiti ECU namenjen multimediji. Ovime se razdvaja kritični softver (koji može da šalje pakete preko magistrale) od potencijalno nepouzdanih modula. Ti moduli se postavljaju u posebne virtualne mašine, koje su odvojene od kritičnih delova mreže.

5 Zaključak

Komunikacione mreže se brzo razvijaju i novi tipovi su neophodni na tržištu zbog novih ideja klijenata, zadovoljavanja zahteva bezbednosti i postizanja optimalnih performansi. Sledeće što se u budućnosti očekuje jeste povezivanje komponenti preko interneta, upravo zato što količina podataka koju treba prenositi vremenom raste. U vozila će se ubaciti sistemi zasnovani na Ethernet-u. Svaka komponenta vozila će imati svoju IP adresu, tako da centralizovani računar i ruter u vozilu mogu da šalju i usmeravaju velike količine podataka brzo i efikasno. U razvoju su i automatizovana, samovozeća vozila, koja predstavljaju budućnost automobilske industrije. Zbog velikih troškova ali i zbog povećane pažnje posvećene kvalitetu bezbednosti, napredak na ovom polju je spor, ali neminovan.

6 Zahvalnice

Zahvaljujemo se kolegi Momirov Đorđu na sugestijama i prevodima na srpski jezik i kolegi Nemec Miodragu na recenziranju rada i pruženim konstruktivnim kritikama. Takođe se zahvaljujemo svim anonimnim recezentima koji su doprineli kvalitetu rada.

Literatura

[1] Checkoway, McCoy, Kantor, Anderson, Shacham, Savage, Koscher, Czeskis, Roesner, and Kohno. Comprehensive experimental analyses of automotive attack surfaces. 2011.

[2] TechTerms Christensson, Per. Denial of Service Definition, 2011. on-line at: https://techterms.com/definition/denial_of_service.

[3] TechTerms Christensson, Per. PROM Definition, 2011. on-line at: https://techterms.com/definition/prom.

[4] TechTerms Christensson, Per. API Definition, 2016. on-line at: https://techterms.com/definition/api.

[5] Analog Devices. A better design experience. A more dynamic automotive experience. ADI's A^2B technology delivers both, 2018. on-line at: http://www.analog.com/en/landing-pages/001/a2b.html.

[6] Henniger, Ruddle, Seudié, Weyl, Wolf, and Wollinger. Securing vehicular on-board it systems: the evita project. 2009.

[7] Hoppe, Kiltz, and Dittmann. Automotive it-security as a challenge: Basic attacks from the black box perspective on the example of privacy threats. 2009.

[8] Hoppe, Tobias, and Dittman. Sniffing/replay attacks on can buses: A simulated attack on the electric window lift classified using an adapted cert taxonomy. 2007.

[9] Interfacebus. Automotive Buses, 2018. on-line at: http://www.interfacebus.com/Design_Connector_Automotive.html.

[10] Kargl, Papadimitratos, Buttyan, Müter, Schoch, Wiedersheim, Thong, Calandriello, Held, Kung, and Hubaux. Secure vehicular communication systems: implementation, performance, and research challenges. November 2008.

[11] Koscher, Czeskis, Roesner, Patel, Kohno, Checkoway, McCoy, Kantor, Anderson, Shacham, and Savage. Experimental security analysis of a modern automobile. May 2010.

[12] Moalla, Labiod, Lonc, and Simoni. Risk analysis study of its communication architecture. Nov 2012.

[13] John Padgette, Karen Scarfone, and Lily Chen. *Guide to Bluetooth Security: Recommendations of the National Institute of Standards and Technology (Special Publication 800-121 Revision 1)*. 2012.

[14] Preserve project. About Preserve project, 2018. on-line at: https://www.preserve-project.eu/.

[15] Studnia, Nicomette, Alata, Deswarte, Kaâniche, and Laarouchi. Survey on security threats and protection mechanisms in embedded automotive networks. June 2013.

[16] Wikipedia. Anti-lock braking system, 2018. on-line at: https://en.wikipedia.org/wiki/Anti-lock_braking_system.

[17] Wikipedia. Body control module, 2018. on-line at: https://en.wikipedia.org/wiki/Body_control_module.

[18] Wikipedia. Cyclic Redundancy Check, 2018. on-line at: https://en.wikipedia.org/wiki/Cyclic_redundancy_check.

[19] Wikipedia. Engine control unit, 2018. on-line at: https://en.wikipedia.org/wiki/Engine_control_unit.

[20] Wikipedia. On-board diagnostics, 2018. on-line at: https://en.wikipedia.org/wiki/On-board_diagnostics.

[21] Wikipedia. Transmission control unit, 2018. on-line at: https://en.wikipedia.org/wiki/Transmission_control_unit.

[22] Wikipedia. Vehicle bus, 2018. on-line at: https://en.wikipedia.org/wiki/Vehicle_bus.

[23] Ben Wojdyla. How it works: The computer inside your car, 2012. on-line at: https://www.popularmechanics.com/cars/how-to/a7386/how-it-works-the-computer-inside-your-car/.

[24] Wolf, Weimerskirch, and Paar. Security in automotive bus systems. 2018.

[25] Wolf, Weimerskirch, and Wollinger. State of the art: Embedding security in vehicles. Jun 2007.