https://doi.org/10.37528/FTTE/9788673955056/POSTEL.2025.28

PRISTUPI UPRAVLJANJA POVERENJEM U VANET MREŽAMA

Milica Kljajić, Mirjana Stojanović
Univerzitet u Beogradu - Saobraćajni fakultet,
m.kljajic@sf.bg.ac.rs, m.stojanovic@sf.bg.ac.rs

Rezime: *VANET (Vehicular Ad Hoc Networks) mreže su ključna komponenta inteligentnih transportnih sistema. One obezbeđuju manji broj saobraćajnih nezgoda, veću bezbednost na putevima i bolji ugođaj pri putovanju. Ipak, suočavaju se sa velikim brojem napada koji prete da ugroze njihovu bezbednost. Napadi na VANET mreže fokusiraju se na ranjavanje njenih najbitnijih tačaka, kao što su raspoloživost, autentifikacija i identifikacija, poverljivost, integritet i poverenje podataka, kao i neporicanje i odgovornost. Zbog napada na bezbednost VANET mreža, neophodni su efikasni i robusni mehanizmi. U ovom radu opisani su neki od najčešćih napada na bezbednost VANET mreža, ali su prikazane i šeme koje daju rešenja na pomenute napade. Prikazani su pristupi upravljanja poverenjem, koji uključuju šeme zasnovane na entitetima, podacima, kao i hibridne šeme, ali i šeme zasnovane na najnovijim tehnologijama. Neke od njih su šeme zasnovane na cloud-u, SDN-u (Software Defined Networking), fog/edge-u, blockchain-u, kao i šeme zasnovane na veštačkoj inteligenciji.*

Ključne reči: *VANET mreže, upravljanje poverenjem, bezbednost, cloud, SDN*

1. Uvod

Porast broja stanovnika dovodi i do zahteva za sve većim unapređenjem i razvojem društva i okruženja. Zahtevi ljudi postaju sve veći, pa je otkrivanje i projektovanje novih vrsta mreža neophodno. Razvoj pametnih gradova, pametnih kuća, pametnih vozila i pametnih elektroenergetskih mreža jedan je od ciljeva ka kojima se teži kako bi se zadovoljile želje i potrebe ljudi.

Inteligentni transportni sistemi (*Intelligent Transportation System*, ITS) se razvijaju kako bi se unapredilo iskustvo putovanja, a njihova ključna komponenta jesu VANET (*Vehicular Ad Hoc Networks*) mreže. Primarni cilj VANET mreža jeste povećanje bezbednosti na putu i smanjenje broja saobraćajnih nezgoda, a pored toga poboljšavaju i iskustvo putovanja korisnika, tj. kako vozača, tako i putnika.

Zbog velike brzine kretanja čvorova, tj. vozila, u VANET mrežama, velikog broja čvorova, tj. velikih dimenzija mreže, dinamične topologije mreže, kao i bežične komunikacije među čvorovima, VANET mreže su često na meti bezbednosnih napada. Meta napada su najranjivije tačke same mreže, dok su motivi napadača različiti, ali njihov cilj je uglavnom isti - ugrožavanje bezbednosti entiteta u VANET mrežama.

U radu su prikazani pristupi upravljanja poverenjem, tj. šeme zasnovane na entitetima, podacima, kao i hibridne šeme. Pored njih, prikazane su i različite šeme upravljanja poverenjem, neke od njih su zasnovane na tehnologijama poput *cloud*-a, SDN-a (*Software Defined Networking*), *fog*/*edge*-a, *blockchain*-a ili veštačke inteligencije (*Artificial Intelligence*, AI) [1].

Rad je sačinjen od pet poglavlja. U drugom poglavlju prikazane su opšte karakteristike i bezbednosni servisi u VANET mrežama. U trećem poglavlju nalaze se postojeći izazovi u VANET mrežama, prikazani su bezbednosni izazovi, kao i izazovi upravljanja poverenjem. U nastavku tog poglavlja prikazane su vrste bezbednosnih napada, kao i njihova klasifikacija. U četvrtom poglavlju opisane su šeme upravljanja poverenjem i data su neka rešenja zasnovana na datim šemama. Na samom kraju nalaze se zaključak i literatura.

2. Karakteristike i bezbednosni servisi u VANET mrežama

VANET mreže predstavljaju jednu od glavnih komponenti ITS-a, a često se nazivaju i inteligentnom transportnom mrežom (*Intelligent Transportation Network*). Veruje se da će VANET mreže evoluirati u Internet vozila (*Internet of vehicles*, IoV), odnosno u Internet autonomnih vozila (*Internet of autonomous vehicles*).

Najznačajnije komponente VANET mreža jesu entiteti od poverenja (*Trusted Authority*, TA), uređaji pored puta (*Roadside Unit*, RSU), uređaji u vozilima (*Onborad Unit*, OBU) i aplikacioni uređaji u vozilima (*Application Unit*, AU). U zavisnosti od toga koji entiteti međusobno komuniciraju, najčešći tipovi komunikacije u VANET mrežama jesu komunikacija između vozila i infrastrukture (*Vehicle to Infrastructure*, V2I), vozila i vozila (*Vehicle to Vehicle*, V2V) i infrastrukture i infrastrukture (*Infrastructure to Infrastructure*, I2I).

Čvorovi u VANET mrežama kreću se velikim brzinama i zbog toga one imaju veoma dinamičnu topologiju. Vozila između sebe komuniciraju zahvaljujući *multihop* komunikaciji, odnosno posredstvom međučvorova. Kako se informacije prenose u otvorenom okruženju kom svi mogu da pristupe, bezbednost VANET mreža jedan je od ključnih izazova. Svaka VANET mreža mora da ispuni bezbednosne zahteve i zahteve za privatnošću. VANET mora da garantuje da poruke koje se prenose nisu ubačene u mrežu od strane napadača ili modifikovane, jer bilo kakva neautorizovana izmena poruka može da izazove velike pretnje po bezbednost vozača i putnika. Autentifikacija i poverenje su zato, u VANET mrežama, ključni zahtevi. Poruke koje se šalju sadrže privatne podatke o vozaču i trebalo bi da se šalju anonimno kako bi se obezbedila efikasna komunikacija.

Jedan od ključnih zahteva VANET mreža je PKI (*Public Key Infrastructure*). Nekoliko bezbednosnih rešenja zavisi od tradicionalnog PKI za detektovanje napada od strane napadača koji se nalaze izvan mreže. Ipak, PKI ne može da detektuje napadače unutar mreže jer su oni već učesnici i imaju verifikovane kredencijale. Zbog toga, istraživači predlažu koncept poverenja kao bezbednosni parametar koji može da detektuje napadače koji se nalaze unutar mreže na osnovu zajedničkih poruka. Ovaj koncept je još u ranim fazama istraživanja, ali njegova ideja je da svaki čvor na osnovu modela poverenja dodeli drugom čvoru stepen poverenja u toku komunikacije [1].

U tabeli 1 navedeni su bezbednosni servisi koji se moraju poštovati kako bi prenos informacija u VANET mrežama bio pouzdan i bezbedan.

Tabela 1. Bezbednosni servisi u VANET mrežama [1]

Servis	Opis
Raspoloživost	Jedan od najbitnijih bezbednosnih servisa, jer većina napada pravi problem protiv raspoloživosti servisa.
Autentifikacija	Znanje da li podaci dolaze sa legitimnog čvora ili ne.
Integritet podataka	Podaci koji dolaze sa legitimnog čvora trebalo bi da budu netaknuti i robusni, kako napadači ne bi mogli da ih menjaju.
Poverljivost	Kontroliše otkrivanje sadržaja poruke neovlašćenim entitetima kako bi se sačuvala privatnost korisnika tako što razmenjuje šifrovane podatke među čvorovima.
Neporicanje poruka	Sprečava da pošiljalac ili primalac odbiju poslatu poruku.

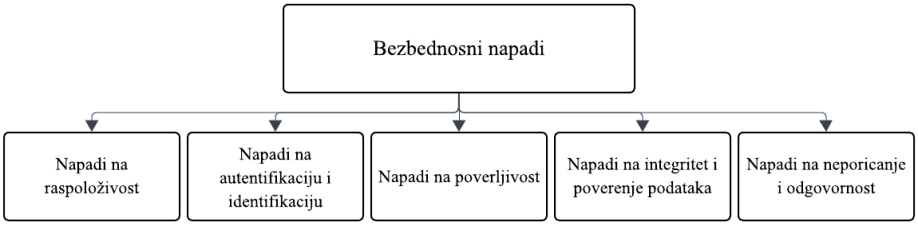
3. Izazovi

U VANET mrežama postoje različiti tipovi učesnika. Glavni učesnici koji razmenjuju informacije jesu vozači, vozila, tj. OBU, uređaji pored puta, tj. RSU, i treća lica koja mogu biti učesnici od (polu)poverenja. Ipak, pored njih, u VANET mrežama postoje i napadači koji značajno mogu da ugroze bezbednost same VANET mreže.

Vozač je najvažniji element koji učestvuje u bezbednosti VANET mreže jer ima ulogu u donošenju veoma važnih odluka. OBU se odnosi na vozilo, ali i na vozača, dok se RSU odnosi na uređaje pored puta koji prikupljaju informacije od OBU uređaja, kao i drugih RSU. Pod pojmom treće lice smatraju se svi učesnici koji na neki način učestvuju u ITS-u, na primer regulatori transporta, proizvođači vozila, saobraćajna policija, sudije itd. U kontekstu bezbednosti VANET mreža, napadač je jedan ili više entiteta koji žele da naruše bezbednost same mreže, kao i bezbednost vozila kojima se veruje, korišćenjem različitih tehnika. Oni utiču na bezbednost mreže i prave probleme drugim entitetima tako što menjaju poruke koje drugi entiteti međusobno razmenjuju. Postoji više različitih vrsta napadača, a neke od njih su: pasivni, aktivni, insajderski, autsajderski, zlonamerni, racionalni i iracionalni napadači [2].

Kako se u VANET mrežama podaci šalju preko bežičnih veza koje su ranjive na napade zlonamernih čvorova, bezbednost predstavlja jedan od najvažnijih aspekata njihovog funkcionisanja. Ukoliko su aplikacije koje se koriste napadnute, može doći do ozbiljnih posledica po učesnike u saobraćaju, zbog čega je neophodno da VANET mreže garantuju autentičnost i integritet poruka koje se razmenjuju između entiteta. U heterogenim mrežama visoke mobilnosti, sa dinamičnim promenama topologije i kratkotrajnim komunikacijama između čvorova, često je teško otkriti zlonamerne aktivnosti, posebno kada napadači koriste identitete legitimnih čvorova kako bi ugrozili mrežu. Ovi problemi bezbednosti i privatnosti direktno su povezani sa upravljanjem poverenjem, pa su mnogi istraživači posvetili pažnju razvoju mehanizama autentifikacije i modela zasnovanih na poverenju radi očuvanja privatnosti i povećanja pouzdanosti VANET mreža.

VANET mreže predstavljaju kompleksan i heterogen sistem sa nekim slabostima. U zavisnosti od slabosti mreže koju napadači napadaju, postoje različite vrste napada, slika 1.



Slika 1. Opšta klasifikacija bezbednosnih napada (na osnovu [1])

Raspoloživost mreže je veoma važan faktor kod VANET mreža, ona garantuje da je mreža funkcionalna i da su korisne informacije raspoložive u svakom trenutku. Zbog svoje važnosti u VANET mrežama jedna je od glavnih tačaka napada. Postoji veliki broj napada na raspoloživost, a neki od njih su: distribuirano onemogućavanje servisa (*Distributed Denial of Service*, DDoS), *spamming*, *jamming*, *black hole*, *grey hole*, napad zlonamernih programa i *greedy* ponašanje [3, 4].

Autentifikacija predstavlja ključni izazov bezbednosti VANET mreža. Svi entiteti pre pristupanja mreži ili servisima moraju da prođu kroz proces autenfitikacije, kako bi se sprečili insajderski i autsajderski napadi zasnovani na lažnom identitetu. Postoji nekoliko tipova napada na autentifikaciju i identifikaciju, a oni su: Sibil napad, tunelovanje, lažno predstavljanje (*impersonation*), replikovanje ključa (*key replication*), *worm hole*, *free riding* i GPS (*Global Positioning System*) lažiranje (GPS *spoofing*) [3, 4].

Poverljivost je veoma važan bezbednosni parametar u VANET mrežama jer obezbeđuje da podatke čitaju samo autorizovani entiteti. U slučaju da mehanizam koji obezbeđuje poverljivost podataka koji se razmenjuju između čvorova ne funkcioniše, podaci su veoma ranjivi na napade. Napadi na poverljivost su: prisluškivanje (*eavesdropping*), analiziranje saobraćaja, *man in the middle* i *social* napad [3].

Integritet razmenjenih podataka u sistemu obezbeđuje da podaci prilikom prenosa nisu promenjeni. Mehanizmi integriteta pomažu u zaštiti informacija od modifikacija, brisanja ili dodavanja. U VANET mrežama napadi na integritet i poverenje podataka uglavnom ciljaju na V2V komunikaciju, jer je ona, u poređenju sa V2I komunikacijom, ranjivija. Jedna od tehnika koja olakšava ove napade jeste laka manipulacija senzorima u vozilu. Napadi na integritet podataka su: maskiranje (*masquerading*), ponovno slanje paketa, iluzija i menjanje poruka [3].

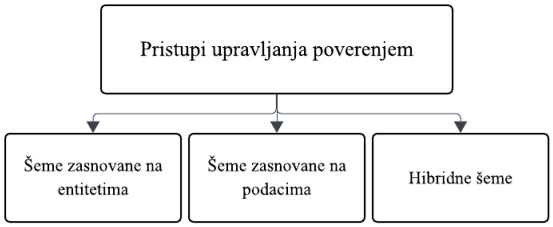
Neporicanje označava mogućnost verifikacije da su pošiljalac i primalac stvarno entiteti koji su potvrdili slanje ili prijem neke poruke. Ako ni pošiljalac ni primalac ne potvrde da su stvarno oni poslali ili primili poruku, onda se samo potvrđuje da je poruka poslata ili primljena, ali se ne zna sa kog i do kog čvora. Imajući u vidu da je bezbednost VANET mreža veoma bitna, trebalo bi da u svakom trenutku bude moguće identifikovati hardverske i softverske promene, bezbednosna podešavanja i aplikacije. Jedan od najpoznatijih napada ove vrste jeste napad na neporicanje [3].

4. Klasifikacija šema upravljanja poverenjem

U ovom poglavlju prikazana je klasifikacija šema upravljanja poverenjem, kao i klasifikacija šema zasnovanih na tehnologiji.

4.1. Pristupi upravljanja poverenjem

Pristupi upravljanja poverenjem dele se na šeme zasnovane na entitetima, šeme zasnovane na podacima, kao i na hibridne šeme, slika 2.



Slika 2. Pristupi upravljanja poverenjem (na osnovu [1])

Šeme zasnovane na entitetima modeluju poverenje na nivou čvorova u mreži, pri čemu svaki entitet ima stepen poverenja koji se dinamički menja tokom vremena. Nivo poverenja procenjuje se na osnovu reputacije, uzimajući u obzir prethodno ponašanje čvora, njegove aktivnosti i preporuke susednih čvorova.

- U radu [5] predložen je model poverenja koji koristi autoritetni čvor za upravljanje reputacijom. Na osnovu ocene reputacije odlučuje se da li čvor može ili ne može pristupiti mreži. Niska ocena reputacije označava opoziv, dok visoka ocena omogućava komunikaciju sa ostalim entitetima.
- U radu [6] predstavljena je šema upravljanja poverenjem PBTMS (*Path-Backtracking-based Trust Management Scheme*) za VANET mreže, koja procenjuje pouzdanost vozila prema istoriji interakcija i ponašanju. Iako koristi informacije o putanji radi preciznije detekcije, šema je entitetski orijentisana jer poverenje izvodi iz reputacije i doslednosti vozila, omogućavajući efikasno prepoznavanje zlonamernih čvorova i adaptivno ažuriranje praga poverenja.

Šeme zasnovane na podacima procenjuju verodostojnost samih poruka, što znači da se zasnivaju na sadržaju i njihovoj korisnosti u odnosu na kontekst događaja. Faktori poput vremena, blizine, događaja i uloge čvora utiču na tu procenu. Ovakav pristup je pogodniji za VANET mreže zbog dinamične prirode i kratkotrajnih veza između entiteta.

- U radu [7] predložena je šema za detekciju zlonamernih čvorova u VANET mrežama zasnovana na sličnosti poruka. Na osnovu brzine i gustine, svaki čvor izračunava svoju *flow* vrednost koristeći *Green-shields* model, a zatim upoređuje procenu sa primljenom porukom. Ako se vrednosti ne podudaraju, pošiljalac se označava kao sumnjiv i prijavljuje.
- U radu [8] predstavljen je sistem upravljanja poverenjem za IoV zasnovan na *blockchain*-u, koji procenjuje poverenje prema kredibilitetu i konzistentnosti podataka, a ne reputaciji čvorova. Verifikacijom i beleženjem informacija na *blockchain*-u obezbeđuje se transparentnost i sprečava manipulacija, čime se poboljšava detekcija lažnih podataka i smanjuje kašnjenje u mreži.

Kod hibridnih šema, poverenje se računa na osnovu pouzdanosti entiteta, ali i razmenjenih podataka. Ukoliko veliki broj entiteta neke podatke označi kao pouzdane u VANET mrežama, oni se i drugim čvorovima u mreži predstavljaju kao pouzdani.

- U radu [9] autori su kombinovali faktore ponašanja i sličnosti kako bi definisali robusnu i hibridnu šemu upravljanja poverenjem u VANET mrežama. Teži se ka tome da se detektuju zlonamerni podaci koji se unose u mrežu putem Sibil napada. Stepen poverenja se uspostavlja na osnovu verifikacije sličnosti između stvarnog i pretpostavljenog ponašanja čvora.
- U radu [10] predstavljena je hibridna šema upravljanja poverenjem za VANET mreže koja kombinuje pristupe zasnovane i na entitetima i na podacima radi veće bezbednosti i pouzdanosti. Poverenje vozila procenjuje se na osnovu istorije interakcija i kredibiliteta poruka, dok se dva nivoa poverenja integrišu pomoću subjektivne logike i ponderisanog glasanja. Ovaj pristup efikasno otkriva zlonamerne čvorove i lažne informacije, poboljšavajući tačnost i adaptivnost u dinamičnim okruženjima.

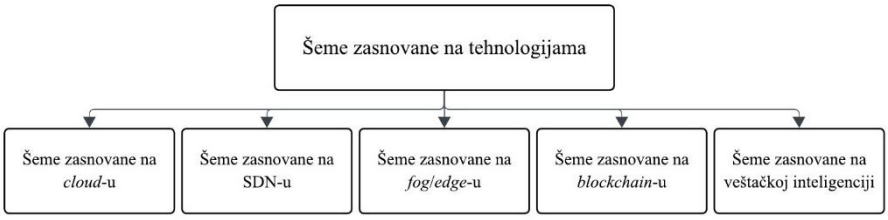
U tabeli 2 prikazane su različite šeme, kao i korišćene metrike, alati i parametri.

Tabela 2. Paralelni prikaz pristupa upravljanja poverenjem (adaptirano prema [1])

Lit.	Klasa	Korišćena metrika	Alati	Parametri
[5]	Entiteti	Reputacija	Metoda eliptične krive	Troškovi računanja
[6]		Preciznost, odziv i F-mera	Simulator ONE (*Opportunistic Network Environment*)	Broj vozila, prag poverenja i težinski koeficijenti
[7]	Podaci	Svojstva čvora, blizina i faktori okruženja	Definisane formule	Prosečna gustina i stepen uspešnosti
[8]		Stepen poverenja i tačnost	*Blockchain* i *smart-contract* mehanizmi	Broj čvorova, vreme obrade i potrošnja resursa
[9]	Hibridni	Znanje i svojstva čvora	Definisane formule	Stopa detekcije i prosečno kašnjenje
[10]		Tačnost detekcije i stopa lažnih alarma	Veins platforma	Broj čvorova, brzina vozila i prag poverenja

4.2. Klasifikacija šema zasnovanih na tehnologijama

Veštačka inteligencija i tehnologije kao što su *cloud*, SDN, *fog/edge* i *blockchain* predstavljaju korisne alate u procesu razvijanja modela poverenja, slika 3.



Slika 3. Klasifikacija šema zasnovanih na tehnologijama (na osnovu [1])

Autori rada [11] predložili su model upravljanja poverenjem u VANET mrežama, koji upravlja procesom izračunavanja. Model se sastoji iz tri osnovna koraka. Prvi korak zasniva se na predobradi podataka koja se obavlja pomoću DST-a (*Decision Support Techniques*). U sledećem koraku se koristi *Fuzzy* analizator kako bi se odredile vrednosti stepena poverenja čvorova u mreži. Na kraju se koriste algoritmi koji se baziranju na principima dodeljivanja nagrada dobronamernim čvorovima i kažnjavanja zlonamernih čvorova. U ovakvom pristupu, svaki čvor može da zatraži vrednost stepena poverenja nekog drugog čvora putem *cloud* servera.

U radu [12] kombinovani su geografski protokoli rutiranja sa SDN pristupom radi formiranja modela rutiranja zasnovanog na poverenju i enkripciji. Predložena šema grupiše čvorove u klastere, pri čemu se za glavni čvor (*Cluster Head*, CH) bira onaj koji ima najpovoljnije faktore mape, visok stepen poverenja i stabilne beacon signale susednih čvorova. Ovakva struktura omogućava sigurnije i efikasnije rutiranje u VANET mrežama.

U radu [13] iskorišćen je *fog computing* za upravljanje poverenjem u VANET mrežama kroz dvoslojnu arhitekturu: sloj sa *cloud* serverom i lokalnim autoritetom, i sloj sa vozilima i *edge* čvorovima. Stepen poverenja pošiljaoca i pouzdanost poruka ocenjuju se na osnovu lokacije, tipa vozila i istorije ponašanja, dok *edge* čvorovi dodeljuju i čuvaju nivoe autentifikacije, prijemni čvor proverava nivo predajnog čvora slanjem upita ka *edge*-u. Autori predlažu i upotrebu *Cuckoo* filtera za efikasnije upravljanje velikim količinama podataka.

Autori rada [14] predložili su kombinaciju *blockchain*-a i *deep learning* tehnike učenja kako bi se poboljšalo upravljanje poverenjem u VANET mrežama. Zamisao ove šeme je da svaki čvor može da obavesti RSU da je određeni čvor zlonameran, nakon procene svih primljenih poruka od obližnjih čvorova. Nakon toga, RSU pomoću *blockchain*-a proverava autentičnost kredencijala zlonamernog čvora, i dalje eliminiše čvor iz mreže.

Pristupi koji se baziraju na veštačkoj inteligenciji integrišu klasterovanje i tehnike učenja potkrepljivanjem (*Reinforcement Learning*, RL), *Fuzzy* logiku i tehnike teorije igara u cilju upravljanja poverenjem u VANET mrežama.

Autori rada [15] predložile su model CSKAS-VANET (*Clustering Signcryption Key Agreement Scheme*), koji integriše RBMA algoritam (*Restricted Boltzmann Machine Algorithm*) sa hipereliptičkom kriptografijom (*Hyperelliptic Curve Cryptography*, HECC) i *signcryption* tehnikom. RBMA omogućava inteligentan izbor CH na osnovu poverenja, trajanja veze i nivoa bafera, dok HECC-baziran *signcryption* obezbeđuje efikasnu i bezbednu autentifikaciju. Kombinacijom veštačke inteligencije i kriptografske zaštite, model poboljšava stabilnost komunikacije, isporuku paketa i otpornost na uobičajene napade u VANET mrežama.

U radu [16] predložen je zasnovan na RL okvir za izbor suseda u VANET mrežama koji kombinuje adaptivno upravljanje poverenjem sa *Q-learning* algoritmom. Svako vozilo funkcioniše kao RL agent koji bira čvorove za prosleđivanje poruka prema poverenju i trajanju veze, dok se pouzdanost čvorova dinamički ažurira korišćenjem Bajesovog i Yagerovog zaključivanja. Prilagođavanjem stope učenja brzini vozila, model se adaptira promenama topologije, smanjuje gubitak paketa i efikasno detektuje napade poput *blackhole* i *grayhole*.

U radu [17] predstavljen je model upravljanja poverenjem zasnovan na *fuzzy* logici za *edge*-orijentisane VANET mreže, koji smanjuje neizvesnost uzrokovanu

mobilnošću i nestabilnom komunikacijom. Šema koristi tri *fuzzy* faktora poverenja, gubitak paketa, ubacivanje lažnih paketa i izmenu sadržaja, kao i NTF (*Network Topology Factor*) za detekciju manipulacija u *multihop* vezama. Primena *fuzzy* inferencije i prenosa poverenja između *edge* servera obezbeđuje veću tačnost i manja kašnjenja u odnosu na postojeće šeme.

Višeslojna šema za otkrivanje neovlašćenih upada u VANET mrežu prikazana je u radu [18]. Autori su koristili tehnike teorije igara sa distribuiranim algoritmom izbora CH. Klasifikaciju zlonamernih čvorova izvršava klasifikator neuronske mreže. Kako bi poboljšali performanse mreže, tako što će biti izabran optimalan CH, autori su koristili *Vickey-Clarke-Groves* metodu. Metoda podrazumeva da RSU čuvaju ocene reputacije čvorova, kako bi procenili verodostojnost glave klastera.

U tabeli 3 dat je paralelni prikaz šema zasnovanih na *cloud*, SDN, *fog/edge*, *blockchain* tehnologiji, kao i na veštačkoj inteligenciji. U tabeli su prikazane korišćena metrika, alati i parametri datih radova.

Tabela 3. Paralelni prikaz šema zasnovanih na tehnologijama (adaptirano prema [1])

Lit.	**Klasa**	**Korišćena metrika**	**Alati**	**Parametri**
[11]	*Cloud*	Reputacija i znanje	*Flipit* igra i simulaciona igra, MATLAB	Verovatnoća kontrolisanja servisa *cloud*-a
[12]	SDN	Uspešnost isporuke paketa i prosečno kašnjenje	NS2 simulator sa VanetMobiSim za mobilnost	Broj čvorova, brzina vozila i gustina klastera
[13]	*Fog/Edge*	Tačnost, preciznost, odziv i komunikaciono opterećenje	*Fuzzy* logika i K-najbliži sused	Gustina i brzina vozila i procenat zlonamernih čvorova
[14]	*Blockchain*	Preciznost, odziv i komunikaciono opterećenje	NS2, SUMO i duboko učenje	Preciznost i opoziv zlonamernih čvorova
[15]	AI – klasterovanje	Odnos isporučenih paketa, kašnjenje i propusnost	NS3 i SUMO simulatori	Poverenje, životni vek veze, bafer i gustina čvorova
[16]	AI - RL	Broj isporučenih paketa, broj hopova i vreme odziva	NS2 i *Q-learning* simulacije	Brzina vozila, broj čvorova, prag poverenja i stopa učenja
[17]	AI – *fuzzy* logika	Preciznost, odziv, kašnjenje i broj poruka po paketu	OMNet++ i *fuzzy* logika	Broj vozila i zlonamernih čvorova i broj *hop*-ova
[18]	AI – teorija igara	Reputacija	*Vickey-Clarke-Groves* metoda	Stopa otkrivanja zlonamernih čvorova

5. Zaključak

Upravljanje poverenjem u VANET mrežama predstavlja jedan od ključnih izazova u razvoju bezbednih i pouzdanih inteligentnih transportnih sistema. Dinamična priroda mreže, visoka mobilnost čvorova i heterogenost okruženja zahtevaju mehanizme koji mogu pravovremeno da otkriju zlonamerne entitete i lažne poruke, a da pri tom ne ugroze performanse mreže. Analiza postojećih pristupa pokazuje da šeme zasnovane na entitetima pružaju dobar okvir za evaluaciju reputacije čvorova, dok šeme zasnovane na podacima bolje odgovaraju dinamičnim uslovima saobraćaja. Hibridne šeme kombinuju njihove prednosti i nude uravnoteženo rešenje između pouzdanosti i efikasnosti.

Dalji razvoj upravljanja poverenjem sve više se oslanja na integraciju savremenih tehnologija kao što su *cloud*, SDN, *fog/edge*, *blockchain* i veštačka inteligencija. Ovi pristupi omogućavaju decentralizovano odlučivanje, prediktivnu analizu ponašanja i adaptivno reagovanje u realnom vremenu. U budućnosti se očekuje da će kombinacija ovih tehnologija omogućiti stvaranje autonomnih i samoupravljivih VANET mreža, koje će biti otpornije na napade i sposobne za samostalno donošenje odluka u kompleksnim saobraćajnim scenarijima.

Literatura

[1] H. Amari, Z. A. El Houda, L. Khoukhi, L. H. Belguith, "Trust Management in Vehicular Ad Hoc Networks: Extensive Survey", *IEEE Access*, vol. 11, pp. 47659-47680, April 2023

[2] M. K. Saggi, R. K. Sandhu, "A Survey of Vehicular Ad Hoc Network on Attacks & Security Threats in VANETs", *International Conference on Research and Innovations in Engineering and Technology* (ICRIET), December 2014

[3] M. Gayathri, C. Gomathy, "A Deep Survey on Types of Cyber Attacks in VANET", *Journal of Critical Reviews*, vol. 8, December 2021

[4] J. Mahmood, Z. Duan, Y. Yang, Q. Wang, J. Nebhen, M. N. M. Bhutta, "Security in Vehicular Ad Hoc Networks: Challenges and Countermeasures", *Security and Communication Networks*, June 2021

[5] J. Cui, X. Zhang, H. Zhang, Z. Ying, L. Liu, "RSMA: Reputation System-Based Lightweight Message Authentication Framework and Protocol for 5G-Enabled Vehicular Networks", *IEEE Internet of Things Journal*, vol. 6, no. 4, pp. 6417-6428, August 2019

[6] C. Cheong, Y. Song, Y. Zhang, Y. Cao, C. Y. Leow, X. Wang, "A Path-Backtracking-Based Trust Management Scheme for VANETs", *2024 IEEE 99th Vehicular Technology Conference (VTC2024-Spring)*, pp. 1-6, June 2024

[7] K. Zaidi, M. Milojević, V. Rakočević, M. Rajarajan, "Data-Centric Rogue Node Detection in VANETs", *13th International Conference on Trust, Security and Privacy in Computing and Communications*, pp. 398-405, September 2014

[8] F. Alharbi, A. Alenezi, M. Alshamrani, M. Aloqaily, "Blockchain-Based Trust Management Systems in the Internet of Vehicles: A Comprehensive Survey," *IEEE Access*, vol. 12, pp. 48585–48610, April 2024

[9] B. Placzek, M. Bernas, "Detection of Malicious Data in Vehicular Ad Hoc Network for Traffic Signal Control Applications", *Springer*, vol. 608, pp. 72-82, June 2016

[10] H. Byeon, M. E. Seno, A. K. Srivastava, A. AlGhamdi, I. Keshta, M. Soni, K. D. V. Prasad, D. Abdurakhimova, M. W. Bhatt, "Trust Management Scheme for Securing Vehicular Ad Hoc Networks Against Malicious Nodes and False Message Anomaly", *Transactions on Emerging Telecommunications Technologies*, vol. 36, March 2025
[11] B. K. Chaurasia, K. Sharma, "Trust Computation in VANET Cloud", *Springer*, 2019
[12] L. Alouache, M. Maachaoui, R. Chelouah, "Securing Hybrid SDN-Based Geographic Routing Protocol Using a Distributed Trust Model", *Advances in Science, Technology and Engineering Systems Journal*, vol. 5, no. 2, pp. 567-577, 2020
[13] S. A. Soleymani, S. Goudrazi, M. H. Anisi, N. Kama, S. A. Ismail, A. Azmi, M. Zareei, A. Hanan Abdullah, "A Trust Model Using Edge Nodes and a Cuckoo Filter for Securing VANET undes NLoS Condition", *Symmetry*, vol. 12, no. 4, p. 609, 2020
[14] C. Zhang, W. Li, Y. Lou, Y. Hu, "AIT: An AI-Enabled Trust Management System for Vehicular Networks Using Blockchain Technology", *IEEE Internet of Things Journal*, vol. 8, no. 5, pp. 3157-3169, December 2021
[15] M. Gayathri, C. Gomathy, "Design of CSKAS-VANET model for stable clustering and authentication scheme using RBMA and signcryption," *Frontiers in Computer Science*, vol. 6, May 2024
[16] O. Sarker, H. Shen, M. A. Babar, "Reinforcement Learning Based Neighbour Selection for VANET with Adaptive Trust Management," *Proceedings of the 2023 IEEE 22nd International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, pp. 585–594, November 2023
[17] M. Hasan, M. Jahan, and S. Kabir, "A Trust Model for Edge-Driven Vehicular Ad Hoc Networks Using Fuzzy Logic," *IEEE Transactions on Intelligent Transportation Systems*, vol. 24, no. 12, pp. 14037–14050, December 2023
[18] B. Subba, S. Biswas, S. Karmakar, "A Game Theory Based Multi Layered Intrusion Detection Framework for VANET", *Future Generation Computer Systems*, vol. 82, pp. 12-28, May 2018

Abstract: *Vehicular Ad Hoc Networks (VANETs) represent a key component of Intelligent Transportation Systems (ITS), contributing to reduced traffic accidents, enhanced road safety, and improved driving comfort. Nevertheless, VANETs face numerous security challenges that threaten their reliability and overall performance. Security attacks often target the most critical aspects of these networks, including availability, authentication and identification, confidentiality, data integrity and trust, as well as non-repudiation and accountability. To mitigate these threats, the development of efficient and robust protection mechanisms is essential. This paper provides an overview of the most common security attacks in VANETs and presents several schemes designed to address them. Furthermore, it examines trust management approaches, namely entity-based, data-based, hybrid, and emerging technology-driven schemes. These include solutions based on cloud computing, Software-Defined Networking (SDN), fog/edge computing, blockchain, and Artificial Intelligence (AI).*

Keywords: *VANET networks, trust management, security, cloud, SDN*

TRUST MANAGEMENT APPROACHES IN VANET NETWORKS

Milica Kljajić, Mirjana Stojanović