https://doi.org/10.37528/FTTE/9788673954899/POSTEL.2024.14

PRIMENA, ARHITEKTURE I BEZBEDNOST VANET MREŽA ZASNOVANIH NA SDN TEHNOLOGIJI

Aleksandra Kostić-Ljubisavljević, Branka Mikavica, Mirjana Stojanović, Momir Manović
Univerzitet u Beogradu - Saobraćajni fakultet,
a.kostic@sf.bg.ac.rs, b.mikavica@sf.bg.ac.rs
m.stojanovic@sf.bg.ac.rs, m.manovic@sf.bg.ac.rs

Rezime: *VANET (Vehicular Ad Hoc Network) mreže su prepoznate kao jedna od ključnih tehnologija koje mogu doprineti poboljšanju bezbednosti u saobraćaju. Problem komunikacije u VANET mrežama je izazovan, jer uključuje mobilnost čvorova, dinamičan kanal komunikacije i prepreke u komunikaciji. Za rutiranje paketa u mreži koriste se različiti distribuirani ad-hoc protokoli rutiranja. SDN (Software-Defined Networking) pretpostavlja novu ideju upravljanja mrežom, gde dolazi do razdvajanja kontrolne ravni i ravni podataka. Sve kontrolne funkcije smeštene su u centralizovani entitet koji se naziva kontroler. Inicijalno, SDN je bio namenjen isključivo mrežama sa žičnim medijumom prenosa, ali je vremenom razvijena podrška i za bežičnu komunikaciju. Ovo je omogućilo integraciju SDN mreža sa VANET mrežama i otvorilo brojna nova rešenja koja pre SDN-a nisu bila moguća u VANET-u. U ovom radu razmatrane su SDN VANET mreže, njihova arhitektura i problemi bezbednosti. Takođe, dat je pregled sajber napada koji su mogući u SDN mrežama, kao i simulacija jednog DDoS* (*Distributed Denial-of-Service*) *napada na SDN-VANET mrežu.*

Ključne reči: *Softverski definisane mreže, VANET, bezbednost, DoS, ARP flood*

1. Uvod

Inteligentni transportni sistemi (*Intelligent Transportation Systems,* ITS) predstavljaju aktivnu oblast istraživanja, jer veliki broj istraživača smatra da ITS ima potencijal za rešavanje brojnih problema u saobraćaju. Intenzivna urbanizacija prouzrokovala je migraciju velikog broja stanovnika u gradove što je dovelo do prenaseljenosti gradskih sredina. Sa porastom broja stanovnika, porastao je i broj vozila koja se svakodnevno nalaze na kolovozima gradova. Posledice su gužve u saobraćaju, zagađenje i veliki broj saobraćajnih nezgoda. Iako se saobraćajne regulative u oblasti bezbednosti saobraćaja stalno unapređuju, broj žrtava i dalje ostaje visok. Svetska zdravstvena organizacija (*World Health Organization,* WHO) je 2023. godine objavila podatak da godišnje 1,19 miliona ljudi strada u saobraćajnim nezgodama, od kojih su više od polovine ranjivi učesnici u saobraćaju, kao što su pešaci i biciklisti [1].

ITS pruža vozilima mogućnost komunikacije i razmene informacija koje mogu pomoći u izbegavanju problema u saobraćaju. Brojna istraživanja pokušavaju da iskoriste

ovu mogućnost za rešavanje problema bezbednosti u saobraćaju. Međutim, komunikacija između vozila predstavlja zaseban problem. Dinamični uslovi prenosa signala, koji su prouzrokovani mobilnošću čvorova otežavaju komunikaciju bez grešaka koja je neophodna za povećanje bezbednosti.

Trenutno najčešći način komunikacije između vozila je bežična *ad-hoc* komunikacija, a mreža vozila koja koriste ovaj način komunikacije naziva se VANET (*Vehicle Ad Hoc Network*) mreža. *Ad hoc* komunikacija podrazumeva direktnu komunikaciju između vozila, kao i komunikaciju između vozila i infrastrukture. Glavna karakteristika ovih mreža su česte promene topologije, što otežava održavanje pouzdanog kanala komunikacije tokom dužeg vremenskog perioda. Ovaj problem danas je tema velikog broja istraživanja, čiji je cilj pronalaženje efikasnog algoritma rutiranja [2-3].

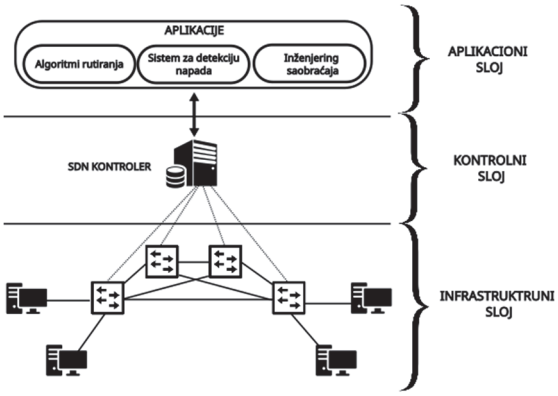
Softverski definisano umrežavanje (*Software Defined Networking*, SDN) omogućuje nov način upravljanja mrežama. Osnovna ideja SDN mreža je u razdvajanju kontrolne ravni i ravni podataka postavljanjem kontrolne ravni u centralizovani entitet koji se naziva kontroler. Kontroler je lokacija sa koje se vrši upravljanje celom mrežom. U početku su SDN mreže bile namenjene isključivo za mreže sa žičnim medijumom prenosa. Međutim vremenom je SDN našao primenu i u bežičnim mrežama.

Centralizovana struktura SDN mreže ima brojne prednosti, ali i nedostatke. Glavni nedostaci centralizovane strukture su problemi skalabilnost i bezbednosti. Postojanje jedne tačke otkaza (*Single Point of Failure*, SPF) otežava efikasnu odbranu sistema od napada. Kao odgovor na ovaj problem razmatrane su različite promene u arhitekturi, kao i brojni algoritmi za detekciju i prevenciju napada [4].

Rad je struktuiran na sledeći način. Nakon uvodnih razmatranja, u drugom poglavlju prikazane su različite arhitekture SDN VANET mreža, kao i njihove prednosti i mane. U trećem poglavlju razmatran je problem bezbednosti i prikazana je simulacija DDoS (*Distributed Denial-of-Service)* napada u SDN VANET mreži. Poglavlje četiri prikazuje rezultate i posledice napada. Poglavlje pet sadrži zaključna razmatranja.

2. Arhitektura SDN-VANET mreže

SDN mreža ima troslojnu arhitekturu koja se sastoji od: infrastrukturnog sloja, kontrolnog sloja i aplikacionog sloja. SDN arhitektura prikazana je na Slici 1.



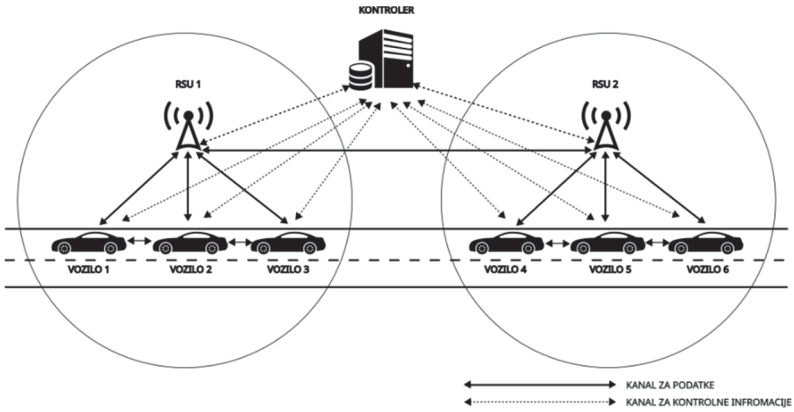
Slika 1. SDN arhitektura

Infrastrukturnom sloju pripadaju uređaji koji podržavaju *OpenFlow* protokol i prosleđuju pakete na osnovu pravila koje definiše kontroler. Kontroler se nalazi u kontrolnom sloju i predstavlja posrednika između aplikacija i uređaja. On je zadužen za prevođenje instrukcija aplikacionog sloja u instrukcije koje su razumljive uređajima za prosleđivanje. Aplikacije koje se nalaze u aplikacionom sloju obavljaju funkcije koje su neophodne za rad svake mreže, kao što su: rutiranje, balansiranje saobraćaja, detekcija napada i druge.

SDN VANET koristi istu troslojnu arhitekturu sa razlikom u infrastrukturnom sloju. U klasičnoj SDN mreži ulogu prosleđivanja imaju *OpenFlow* svičevi, dok u SDN VANET-u prosleđivanje na osnovu definisanih tokova mogu vršiti: vozila, putna infrastruktura (*Road Side Units*, RSU), kao i bazne stanice [5-6].

U SDN VANET-u postoje tri osnovna tipa arhitektura koje se koriste u implementaciji, a to su: centralizovana arhitektura, distribuirana ili hijerarhijska arhitektura i hibridna arhitektura [7].

Centralizovana arhitektura je najbliža klasičnoj ideji SDN mreže, u kojoj postoji jedan centralizovani kontroler koji je zadužen za upravljanje celom mrežom. Prednost ove arhitekture je pregled svih dešavanja u mreži u realnom vremenu. Vozila koja se nalaze u mreži periodično šalju *beacon* signale koji sadrže podatke o trenutnoj lokaciji vozila, vektoru brzine, stanja na putu i druge. Kontroler pomoću dobijenih informacija može da formira graf trenutnog stanja u mreži na osnovu koga, korišćenjem heurističkih algoritama, može da vrši optimizaciju rute između čvorova po različitim kriterijumima. Na Slici 2 prikazana je SDN VANET mreža sa centralizovanom arhitekturom.



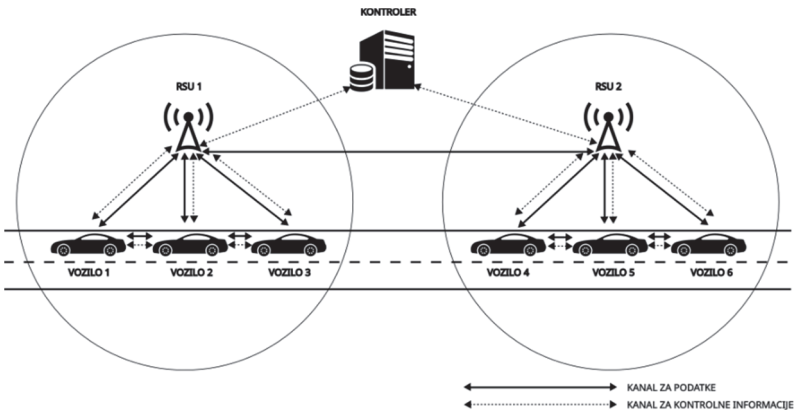
Slika 2. Centralizovana arhitektura

Problemi ove arhitekture su skalabilnost, bezbednost i kašnjenje. Veliki broj korisnika u mreži implicira i veliki broj zahteva koje treba opslužiti. Posledica ovoga može biti zauzeće svih resursa, nakon čega nije moguće uslužiti nove zahteve. Ovo stanje mreže može uzrokovati pad kvaliteta servisa ili potpuni prekid. Kao odgovor na ovu mogućnost, sva vozila u mreži kada detektuju da je veza sa kontrolerom prekinuta prelaze na *ad-hoc* način komunikacije.

Centralizovana arhitektura je takođe osetljiva na sajber napade. Najčešći napadi su DoS (*Denial of Service*) napadi koji za cilj imaju prekid servisa ili narušavanje kvaliteta servisa. Vrste napada koji se koriste su: TCP (*Transmission Control Protocol*) *flood*, ICMP (*Internet Control Messaging Protocol*) *flood* i ARP (*Address Resolution Protocol*) *flood* napadi.

Rastojanje između čvorova i kontrolera koji se nalazi na centralizovanoj lokaciji unosi dodatno kašnjenje u sistem, što je još jedan problem centralizovane strukture.

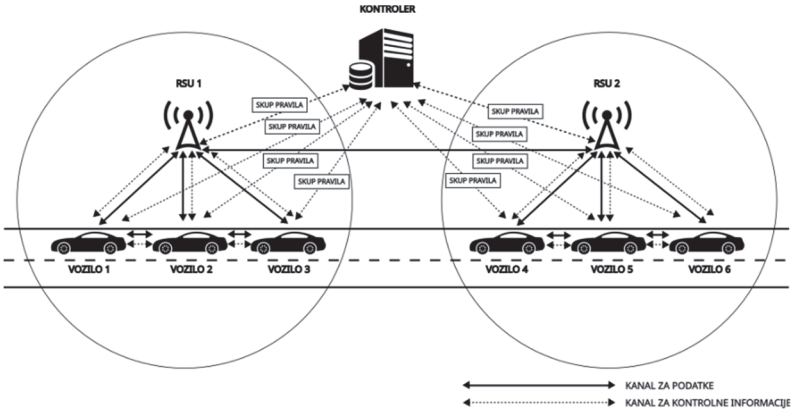
Za razliku od centralizovane arhitekture u kojoj se svi zahtevi za pronalaženje rute prosleđuju kontroleru, distribuirana arhitektura primarno dodeljuje zadatak pronalaženja ruta krajnjim čvorovima, na sličan način kao kod *ad-hoc* komunikacije. Ako vozila ne uspeju da pronađu rutu do odredišta, zahtev se prosleđuje RSU koji pokušava da pronađe odredište. Ako RSU pronađe odredište on definiše odgovarajuće tokove u krajnjim uređajima, u suprotnom slučaju zahtev se prosleđuje kontroleru koji pronalazi odredište. Na Slici 3 prikazana je SDN VANET mreža sa distribuiranom arhitekturom.



Slika 3. Distribuirana arhitektura

Ova arhitektura rešava problem skalabilnosti. Međutim, mehanizam pronalaženja rute može uneti dodatna kašnjenja.

Hibridna arhitektura, prikazana na Slici 4, pokušava da spoji prethodne dve ideje i iskoristi njihove prednosti, a odbaci mane. U ovoj arhitekturi kontroler može da preuzme potpunu kontrolu nad mrežom što stvara centralizovanu strukturu, ali takođe može da sve odluke prepusti krajnjim čvorovima kao kod distribuirane arhitekture. U najčešćem slučaju, mreža je konfigurisana tako da kontroler centralizovano upravlja putnom infrastrukturom, a krajnjim uređajima dopušta da samostalno donose odluke. Postavljanje upravljačkog dela u RSU približava kontroler krajnjim korisnicima što smanjuje kašnjenje i poboljšava kvalitet servisa.



Slika 4. Hibridna arhitektura

3. Bezbednost SDN VANET-a

Svi servisi koje SDN omogućava zavise od komunikacije između kontrolera i krajnjih uređaja. Ukoliko je kanal komunikacije kompromitovan, to može dovesti do ozbiljnih posledica po bezbednost vozača. Bežični medijum komunikacije u SDN VANET mreži stvara dodatni problem [8-11].

Sajber napadi u SDN VANET-u mogu se kategorizovati na sledeći način:

1. Napadi autentifikacije – Da bi mreža bila bezbedna neophodno je da kontroler autentifikuje sve čvorove u mreži. Neautentifikovani čvorovi predstavljaju potencijalne zlonamerne korisnike koji mogu izvršiti brojne napade na mrežu kao što su: *DoS*, *Man-in-the-middle*, *Spoffing*, *Black hole* napadi.

2. **Napadi na raspoloživost –** Cilj ove vrste napada je da naruše normalan rad kontrolera i na taj način ugroze vozila koja zavise od pravovremenih informacija koje kontroler pruža. U ovu grupu spadaju sve vrste *DoS* i *Jamming* napada.

3. Napadi na poverljivost podataka – Podaci koji se razmenjuju između vozila i kontrolera mogu sadržati veoma poverljive informacije. Primer ovog tipa informacije je trenutna lokacija vozila koja se šalje kontroleru u realnom vremenu. Ovaj problem je još ozbiljniji ako se uzme u obzir da sva vozila koriste isti medijum za prenos.

4. Napad na integritet podataka – Pored očuvanja poverljivosti podataka važno je obezbediti da sadržaj paketa nije menjan tokom prenosa do korisnika. Kako bi verovatnoća uspešnosti napada na poverljivost i integritet bila smanjena na minimum, neophodna je autentifikacija svakog korisnika kao i korišćenje algoritama enkripcije podataka.

5. Napad na neporecivost – U mreži je važno kreirati sistem tako da je nemoguće poreći da je određeni korisnik primio ili poslao paket. Na ovaj način sprečava se mogućnost slanja ručno kreiranih paketa koji se mogu koristiti za: *Replay* i *Man-in-the-middle* napade.

4. DDoS napad na centralizovanu arhitekturu: simulacija i rezultati

DDoS napadi su najčešća vrsta napada u SDN mrežama. Razlog česte upotrebe je jednostavnost kreiranja napada i visok stepen uspešnosti. Ideja DoS napada je da istroši sve resurse na serveru kako bi došlo do prekida servisa. Način na koji se to postiže je „plavljenjem“ servera velikim brojem zahteva koje je potrebno obraditi. Razlika između klasičnog DoS napada i DDoS napada je u broju napadača. Kod klasičnog DoS napada postoji jedan napadač koji generiše saobraćaj, dok kod DDoS napada postoji više napadača u mreži na različitim lokacijama. Zbog distribuiranosti, odnosno činjenice da svaki napadač generiše relativno male količine saobraćaja, DDoS napade je teže uočiti i sprečiti.

DoS napadi su posebno efektivni u SDN mrežama jer je cilj napada jasno određen. Takođe, napadač ne mora da poznaje javnu IP (*Internet Protocol*) adresu servera da bi započeo napad, jer je svaki paket koji uređaj za prosleđivanje ne može da obradi direktno prosleđen kontroleru.

Za simulaciju napada u SDN VANET mreži korišćen je *mininet* emulator i ONOS (*Open Network Operating System*) kontroler.

U simulaciji je korišćen računar sa procesorom AMD Ryzen 7 5700X i 32 GB RAM (*Random Access Memory*) memorije. Kontroler je kreiran kao *Docker* kontejner za koga su rezervisana četiri jezgra procesora i 4 GB RAM memorije.

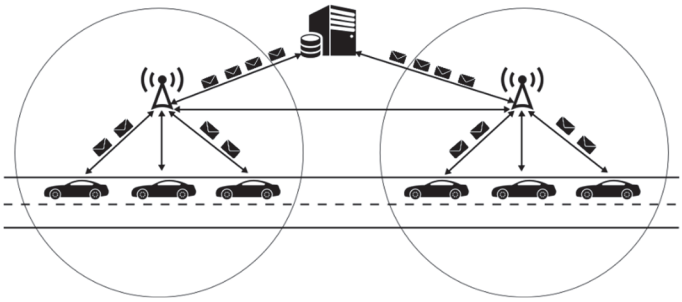
SDN VANET mreža korišćena u simulaciji prikazana je na Slici 2. U mreži se nalazi šest vozila koja za međusobnu komunikaciju i komunikaciju sa infrastrukturom koriste Wi-Fi (*Wireless-Fidelity*) standard 802.11g. Međusobne veze između RSU-a, kao i veze između RSU-a i kontrolera su žične veze.

Napad korišćen u simulaciji je ARP *flood* napad. Razlog korišćenja ARP paketa je posledica toga što se u centralizovanoj arhitekturi pronalaženje svih hostova u mreži vrši posredstvom kontrolera. Svaki uređaj koji koristi tabelu tokova za prosleđivanje sadrži tok koji sve ARP pakete prosleđuje kontroleru. Ovo pravilo prikazano je na Slici 5.

```
table=0, n_packets=4, n_bytes=168, send_flow_rem priority=40000,arp actions=CONTROLLER:65535,clear_actions
table=0, n_packets=75, n_bytes=10425, send_flow_rem priority=40000,dl_type=0x8942 actions=CONTROLLER:65535,clear_actions
table=0, n_packets=3, n_bytes=294, send_flow_rem priority=5,ip actions=CONTROLLER:65535,clear_actions
table=0, n_packets=75, n_bytes=10425, send_flow_rem priority=40000,dl_type=0x88cc actions=CONTROLLER:65535,clear_actions
```

Slika 5. Inicijalna tabela tokova nakon pokretanja uređaja za prosleđivanje

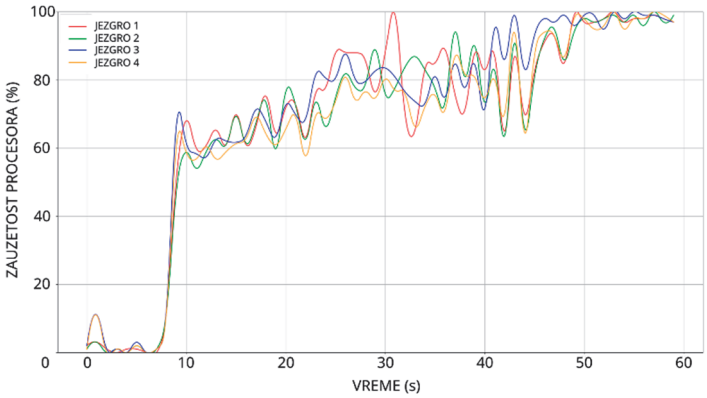
U simulaciji četiri hosta generišu ARP pakete sa intenzitetom 10000 ARP paketa u sekundi u periodu od 60 sekundi. Dva hosta se nalaze u oblasti pokrivanja RSU-a 1, a dva u oblasti pokrivanja RSU-a 2. Kao što je prikazano na Slici 6, RSU-ovi ne pokušavaju samostalno da pronađu hosta, već pakete prosleđuju direktno kontroleru.



Slika 6. DDoS ARP flood napad

4.1. Rezultati simulacije

Rezultati u ovom poglavlju prikazuju kako je u realnom vremenu napad uticao na iskorišćenost procesorskih resursa servera. Na Slikama 7 i 8, respektivno, prikazana je zauzetost pojedinačnih jezgara i prosečna zauzetost jezgara tokom napada.

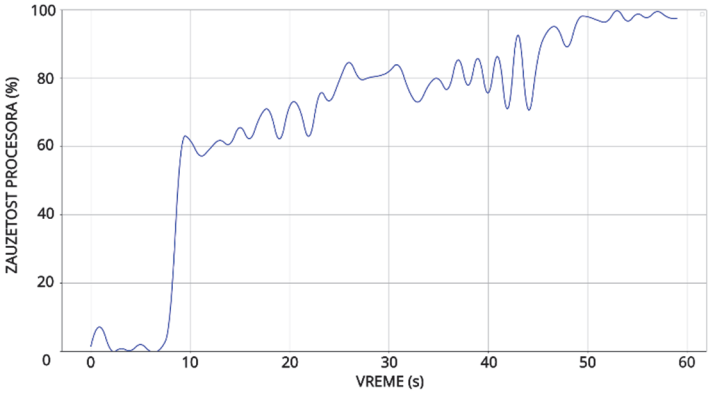


Slika 7. Zauzetost pojedinačnih jezgara tokom napada

Sa Slika 7 i 8 može se videti da napad započinje u sedmoj sekundi nakon početka monitoring resursa procesora. U trenutku napada iskorišćenost resursa se naglo povećava, međutim, nisu svi resursi zauzeti odmah. Zauzetost se povećava linearno sa vremenom pri istom intenzitetu napada. Nakon 50 sekundi napada, server nije u stanju da obrađuje zahteve iz mreže i dolazi do prekida servisa.

Kao mera ublažavanja napada mogu se koristiti statičke konfiguracije u kojima se definiše granična vrednost broja zahteva u jedinici vremena na nivou uređaja, ili na nivou interfejsa. Ukoliko broj zahteva nadmaši definisanu vrednost sistem to prepoznaje kao napad i sve dalje zahteve odbacuje, a MAC (*Medium Access Control*) adresu uređaja koji je slao zahteve stavlja na „crnu listu“. Prednost ovog tipa konfiguracije je jednostavnost, međutim, u slučajevima DDoS napada detekcija je otežana jer se za napad koristi više različitih tokova koji pojedinačno ne prelaze graničnu vrednost, ali prilikom agregiranja

saobraćaja ka kontroleru broj zahteva postaje preveliki. Kao unapređenje statičkih konfiguracija mogu se koristiti sistemi za detekciju napada zasnovani na mašinskom učenju. SDN kontroler u realnom vremenu prikuplja velike količine informacija o dešavanjima u mreži. Ove informacije se mogu koristiti kao ulazni parametri za istrenirane neuronske mreže koje na izlazu izračunavaju verovatnoću da se napad dešava u mreži.



Slika 8. Prosečna zauzetost jezgara tokom napada

5. Zaključak

Softverski definisane mreže predstavljaju nov koncept upravljanja koji se višestruko primenjuje. Jedna od mogućih primena je korišćenje SDN za upravljanje VANET mrežama. VANET mreže koriste distribuirane *ad hoc* protokole rutiranja. SDN pokušava da centralizuje upravljanje tako što svi uređaji u mreži šalju informacije kontroleru na osnovu kojih je moguće formirati graf povezanosti čvorova u mreži. Nakon formiranja grafa, moguće je efikasno upravljanje mrežom. Međutim, formiranje grafa u slučaju mreža sa velikim brojem čvorova nije jednostavan proces i može preopteretiti kontroler. Kao rešenje ovog problema predložene su različite arhitekture mreže koji imaju hijerarhijske osobine.

Pored skalabilnosti mreže, jedan od ključnih problema SDN mreža je bezbednost. Centralizovane arhitekture su česte mete različitih sajber napada. Razlog je kontroler koji predstavlja tačku otkaza celog sistema, i većina napada je direktno usmerena na njega. Narušavanje normalnog rada kontrolera može imati velike posledice po mrežu, posebno u situacijama gde kontroler obavlja funkcije koje su ključne za bezbednost u saobraćaju.

U ovom radu prikazane su posledice DDoS napada na centralizovanu arhitekturu SDN VANET mreže. Ovaj jednostavan napad doveo je do potpunog otkaza kontrolera i prekida servisa. Kako bi ovi napadi bili sprečeni, neophodno je implementirati odgovarajuće algoritme za detekciju i prevenciju napada u mreži.

Literatura

[1] "Road traffic injuries." Accessed: Sep. 23, 2024. [Online]. Available: https://www.who.int/news-room/fact-sheets/detail/road-traffic-injuries

[2] K. P. Sampoornam, S. Saranya, S. Vigneshwaran, P. Sofiarani, S. Sarmitha, and N. Sarumathi, "A Comparative Study on Reactive Routing Protocols in VANET," in *2020 4th International Conference on Electronics, Communication and Aerospace Technology (ICECA)*, Coimbatore, India: IEEE, Nov. 2020, pp. 726–731. doi: 10.1109/ICECA49313.2020.9297550.

[3] T. Marinov, "Comparative analysis of AODV, DSDV and DSR routing protocols in VANET," in *2022 57th International Scientific Conference on Information, Communication and Energy Systems and Technologies (ICEST)*, Ohrid, North Macedonia: IEEE, Jun. 2022, pp. 1–4. doi: 10.1109/ICEST55168.2022.9828684.

[4] O. Sadio, I. Ngom, and C. Lishou, "SDN Architecture for Intelligent Vehicular Sensors Networks," in *2018 UKSim-AMSS 20th International Conference on Computer Modelling and Simulation (UKSim)*, Cambridge: IEEE, Mar. 2018, pp. 139–144. doi: 10.1109/UKSim.2018.00036.

[5] I. Ku, Y. Lu, M. Gerla, R. L. Gomes, F. Ongaro, and E. Cerqueira, "Towards software-defined VANET: Architecture and services," in *2014 13th Annual Mediterranean Ad Hoc Networking Workshop (MED-HOC-NET)*, Slovenia: IEEE, Jun. 2014, pp. 103–110. doi: 10.1109/MedHocNet.2014.6849111.

[6] N. H. Hussein *et al.*, "SDN-Based VANET Routing: A Comprehensive Survey on Architectures, Protocols, Analysis, and Future Challenges," *IEEE Access*, pp. 1–1, 2024, doi: 10.1109/ACCESS.2024.3355313.

[7] Md. M. Islam, M. T. R. Khan, M. M. Saad, and D. Kim, "Software-defined vehicular network (SDVN): A survey on architecture and routing," *J. Syst. Archit.*, vol. 114, p. 101961, Mar. 2021, doi: 10.1016/j.sysarc.2020.101961.

[8] O. S. Al-Heety, Z. Zakaria, M. Ismail, M. M. Shakir, S. Alani, and H. Alsariera, "A Comprehensive Survey: Benefits, Services, Recent Works, Challenges, Security, and Use Cases for SDN-VANET," *IEEE Access*, vol. 8, pp. 91028–91047, 2020, doi: 10.1109/ACCESS.2020.2992580.

[9] F. R. Almehrezi, C. Y. Yeun, P. D. Yoo, E. Damiani, Y. A. Hammadi, and H. Yeun, "An Emerging Security Framework for Connected Autonomous Vehicles," in *2020 7th International Conference on Behavioural and Social Computing (BESC)*, Bournemouth, United Kingdom: IEEE, Nov. 2020, pp. 1–4. doi: 10.1109/BESC51023.2020.9348317.

[10] M. Arif *et al.*, "SDN-based VANETs, Security Attacks, Applications, and Challenges," *Appl. Sci.*, vol. 10, no. 9, p. 3217, May 2020, doi: 10.3390/app10093217.

[11] R. Sultana, J. Grover, and M. Tripathi, "Security of SDN-based vehicular ad hoc networks: State-of-the-art and challenges," *Veh. Commun.*, vol. 27, p. 100284, Jan. 2021, doi: 10.1016/j.vehcom.2020.100284.

Abstract: *VANET (Vehicular Ad Hoc Network) networks are recognized as one of the key technologies that can contribute to increasing traffic safety. The problem of communication in VANET networks is challenging, because it involves node mobility, dynamic communication channel, and communication obstacles. Different distributed ad-hoc routing protocols are used to route packets in the network. SDN (Software Defined Networking) represent a new idea of network management, where the control plane and the data plane are separated. All control functions are placed in a centralized entity called the controller. Initially, SDN was intended exclusively for networks with a wired transmission medium, but over time, support for wireless communication was also developed. This enabled the integration of SDN networks with VANET networks and opened up a number of new solutions that were not possible in VANET before SDN. In this paper, we discuss SDN VANET networks, their architecture, and problems. Also, an overview of cyber attacks that are possible in SDN networks and a simulation of a DDoS attack on an SDN-VANET network are presented.*

Keywords: *Software-defined networks, VANET, security, DoS, ARP flood*

APPLICATION, ARCHITECTURES AND SECURITY OF SDN BASED VANET NETWORKS

Aleksandra Kostić-Ljubisavljević, Branka Mikavica, Mirjana Stojanović, Momir Manović