Zbornik radova Fakulteta tehničkih nauka, Novi Sad

UDK: 004.9
DOI: https://doi.org/10.24867/10BE11Vujakovic

KOMUNIKACIONE TEHNOLOGIJE INTERNETA STVARI SA PRIMENOM U INDUSTRIJI

COMMUNICATION TECHNOLOGIES OF THE INTERNET OF THINGS FOR USAGE IN THE INDUSTRY

Miljana Vujaković, *Fakultet tehničkih nauka, Novi Sad*

Oblast – ELEKTROTEHNIKA I RAČUNARSTVO

Kratak sadržaj – *U radu je prezentovana komparativna analiza komunikacionih CoAP i MQTT komunikacionih tehnologija za internet stvari. Dodatno, eksperimentalno su određivani faktori performansi CoAP, MQTT protokola. Predstavljena je ideja hijerarhijskog, multiprotokolskog rešenja za online nadgledanje bandera pametnih mreža oslanjanjem na analizirane protokole.*

Ključne reči: *internet stvari, komunikacioni protokoli, CoAP, MQTT, pametne mreže, nadgledanje bandera*

Abstract – *The paper presents the comparative analysis of CoAP and MQTT communication technologies essential for the Internet of Things. Additionaly, performance factors of CoAP, MQTT protocols are determined experimentally. The idea of hierarchical, multiprotocol solution for online monitoring of smart grid poles by relying on the analyzed protocos was presented.*

Keywords: *Internet of Things, Communication protocols, CoAP, MQTT, Smart Grid, Utility Pole Surveillance*

1. IOT PARADIGMA

Sintagma *Internet of Things* referiše na distribuirani sistem čiju srž čine mnogobrojni entiteti povezani preko komunikacionih mreža na Internet, a generički pojam „stvar“ (eng. *Thing*) ukazuje na širok doseg interneta stvari. Značaj se uočava kroz aplikacije orijentisane ka potrošaču (nosivi uređaji, pametne kuće..) i posebno kroz poslovne aplikacije gde se svrstava i primena IoT-a u industriji. Industrijski IoT je osnaživanje industrijskog inženjerstva senzorima i softverom sa ciljem blagovremenog uočavanja problema, i kreiranja efikasnih, ekonomičnih i optimalnih procesa. Značajna IIoT aplikacija je pametna mreža koja predstavlja evoluciju elektroenergetskih sistema (EES) integracijom savremenih informaciono-komunikacionih tehnologija u svaki od EES podsistema (proizvodnja, prenos, distribucija, potrošnja), sa ciljem obezbeđivanja kontrolisane, pouzdane, efikasne, stabilne i bezbedne isporuka električne energije. Za realizaciju povezivanja, automatizacije, kontrolisanja i praćenja brojnih infrastrukturnih elemenata pametne mreže koji poseduju različite mehanizme konektivnosti je potrebna dvosmerna komunikaciona infrastruktura, prisutna u IoT tehnologiji. U poglavlju 4. je obrađen jedan od primera upotreba IoT tehnologije u distributivnom podsistemu za nadzor bandera.

NAPOMENA:
Ovaj rad proistekao je iz master rada čiji mentor je bio dr Srđan Vukmirović, vanr.prof.

2. KOMUNIKACIJE U IOT EKOSISTEMU

Protokoli TCP/IP modela su namenjeni upotrebi u mrežama računara opšte namene, gde su performanse računara zadovoljavajuće. Zbog svojstava IoT rešenja, pojavio se niz novih tehnologija za senzorske i telekomunikacione mreže. Od mnogo faktora koji utiču na performanse IoT rešenja, komunikacija na aplikativnom nivou je jedan od glavnih i u nastavku su predstavljeni MQTT i CoAP aplikativni protokoli.

2.1 CoAP

U julu 2013, Internet Engineering Task Force (IETF) je objavio CoAP - Constrained Application Protocol [1] (IETF RFC725260) protokol aplikativnog nivoa prilagođen za resursno ograničene uređaje male potrošnje u Internet mreži. Realizuje zahtev/odgovor komunikacioni obrazac. U CoAP IoT sistemu interakcija je bazirana na peer-to-peer klijent-server obrascu i svaki uređaj označen kao CoAP endpoint izlaže REST API. CoAP bazirana mreža se jednostavno povezuje sa HTTP mrežom koristeći proksi uređaje. Zahtevi i odgovori se razmenjuju asinhrono preko CoAP poruka. Može biti implemetiran preko UDP-a ili bilo kog drugog transportnog mehanizma baziranog na datagram-u. Da bi se omogućio kvalitet servisa na nivou aplikacije - postoje dva režima u kojima se poruke razmenjuju između CoAP čvorova (klijenata i servera): ne zahtevaju potvrdu prispeća (eng. Non-confirmable) i zahtevaju potvrdu prispeća (eng. Confirmable) od servera.

2.2 MQTT

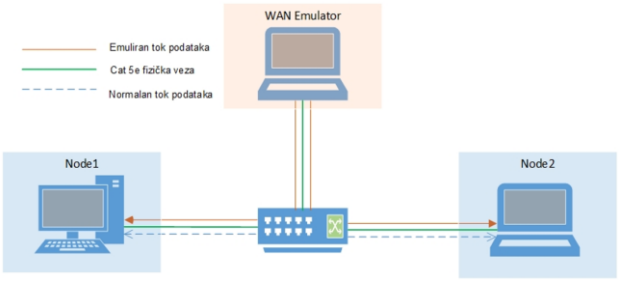
MQTT [2] je protokol za razmenu poruka aplikativnog sloja, razvijan od strane IBM-a krajem 1990-ih, no danas je otvoreni protokol. Razvijan je za komunikaciju preko nepozdanih satelitskih veza, sa udaljenim lokacijama, gde je propusni opseg mreže ograničen. Koristi se u okruženjima sa malim kapacitetom programske i radne memorije. Bazira se na objavi-pretplati komunikacionom obrascu i dobar je za sisteme koji se odlikuju nestabilnom mrežom sa prekidima veze, gubicima paketa, malim brzinama prenosa i velikim kašnjenjem. MQTT je ustaljen, stabilan protokol sa velikom podrškom na tržištu. MQTT se oslanja na TCP transportni protokol što omogućava pouzdanost u komunikaciji. MQTT klijenti se karakterišu ulogama objavljivača odnosno pretplatnika na poruke na određenim temama, dok je broker centralna komponenta koja upravlja razmenom poruka u objavi-pretplati komunikaciji. Na nivou pojedinačne specificira QoS koji se

odnosi na garanciju isporuke poruke. Razlikuju se QoS 0 koji garantuje isporuku poruka najviše jednom, QoS 1 za garanciju da će bar jedna poruka doći na odredište i QoS 2 koji garantuje da će poruka biti isporučena tačno jednom bez duplikata.

3. EKSPERIMENT

U eksperimentu je određivano zauzeće komunikacionog kanala u zavisnosti od veličine poruke na koju uticaj imaju: format sadržaja, odabrani protokol (MQTT, CoAP), upotreba mehanizama bezbednosti. Takođe je određivana i latencija kao funkcija veličine razmenjivane poruke, i kao posledica nepovoljnih uslova mreži.

U testnom scenariju (slika 1) se transportuju podaci od čvora Node1, koji ima ulogu agregatora na nižem nivou, do čvora Node2 koji je na višem nivou u hijerarhije u IoT rešenju. Razmena podataka između čvorova Node1 i Node2 se vrši protokolima MQTT, odnosno CoAP. Za kontrolu uslova u mreži korišćen je WANem alat emulator mreže širokog područja.



Slika 1. Postavka testnog okruženja

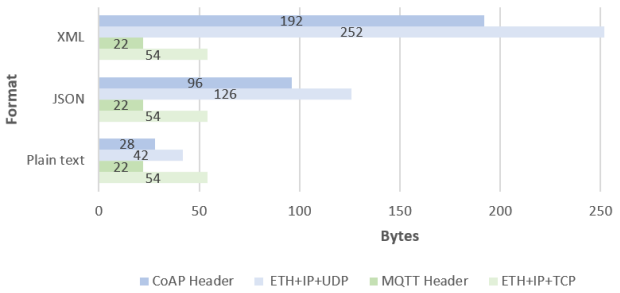
Sadržaj poruke predstavlja agregaciju merenja temperature i vlažnosti vazduha sa 3 emulirana uređaja sloja opažanja (kratke/male poruke) i sa 30 uređaja (dugačke/velike poruke). Latencija je određivana tokom slanja paketa po povratnoj putanji (RTT).

Za testiranje MQTT protokola je potrebna implementacija brokera i klijenta. Zbog lakoće podešavanja i korišćenja, odabran je **mosquito** broker koji je u testnom scenariju instaliran na čvoru Node1, dok je **M2Mqtt** biblioteka upotrebljena u .NET Core MQTT klijentskim aplikacijama koje se izvršavaju na čvorovima Node1 i Node2. Jedina funkcionalna CoAP .NET Core/.NET Framework implementacija u trenutku izvršavanja eksperimenta je **Com.AugustCellar/CoAP** implementacija. Opcija koja omogućava transferovanje velikih reprezentacija se zove block-wise transfer. U ovoj implementaciji je uočen problem sa block-wise transferom enkriptovanih poruka.

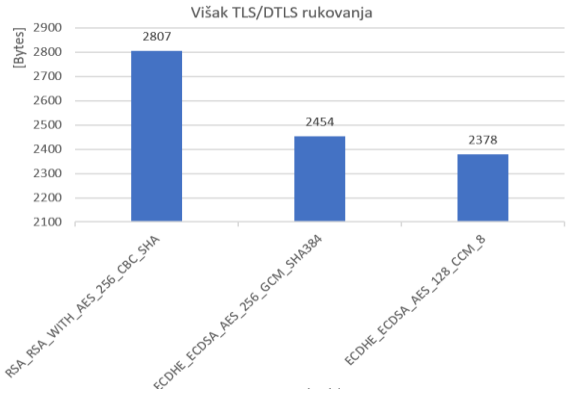
3.1. Analiza rezultata

Veličina sadržaja je ista za oba protokola, ali zavisi od formata poruke. Za prenos informacije preko male poruke, u Plain tekst, JSON, XML formatima je potrebno 39, 121, 401 bajtova, a za prenos informacije velike poruke se koristi 392, 1227 i 2563 bajtova.

Na grafiku 1. je prikazan ukupan višak koji korišćenje MQTT i CoAP protokola unosi u saobraćaj. Vidi se da prilikom transfera većih poruka protokoli nižeg nivoa MQTT steka unose po 54 bajta, i MQTT zaglavlje unosi 22 bajta. Protokoli koji se koriste uz CoAP unose veće opterećenje u saobraćaj, jer se velike poruke šalju u blokovima.

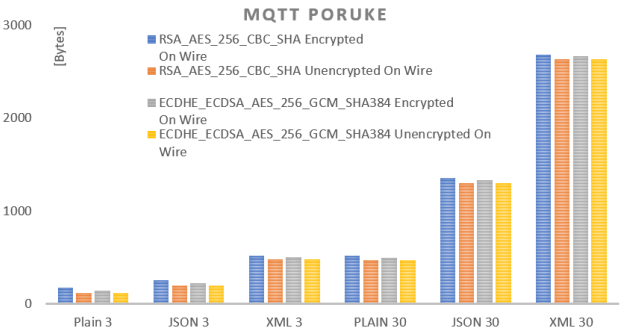


Grafik 1. *Ukupan broj prenetih bajtova u zavisnosti od protokola, bez prikazivanja bajtova sadržaja*

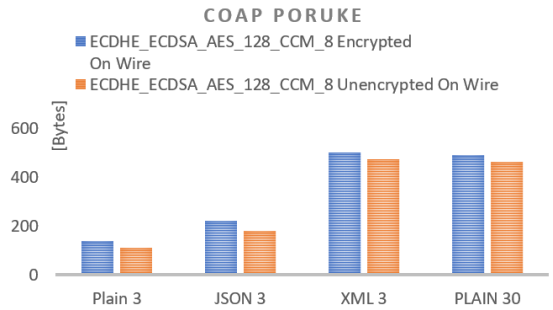


Grafik 2. *Višak TLS i DTLS rukovanja*

Grafik 2. pokazuje da je uočljivo da upotreba eliptičnih kriva (ECDSA) doprinosi manjem višku protokola rukovanja u odnosu na RSA.



Grafik 3. *Poređenje veličine šifrovanih i nešifrovanih MQTT poruka*



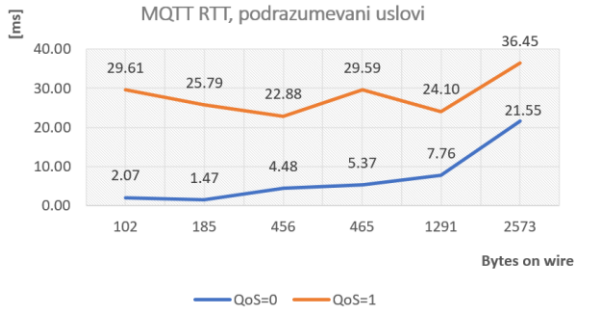
Grafik 4. *Poređenje veličine šifrovanih i nešifrovanih CoAP poruka*

Određivan je višak (Grafik 3, 4) na nivou pojedinačne poruke, za svaku od malih i velikih poruka prethodno korišćenih u eksperimentu. Na nivou razmenjivanih poruka za MQTT/TLS višak je skoro zanemarljiv, i iznosi prosečno 50 bajtova na nivou poruke za RSA_AES_256_CBC_SHA, dok za ECDHE_ECDSE_AES_256_GCM_SHA384 iznosi 29 bajtova. Višak na nivou poruke za

CoAP/DTLS za ECDHE_ECDSE_AES_128_CCM_8 iznosi 30 bajtova. Za CoAP/DTLS su prikazane samo 4 poruke, zato što su to poruke koje su dovoljno male da se ne šalju u blokovima i za njih korišćene implementacije funkcionišu.

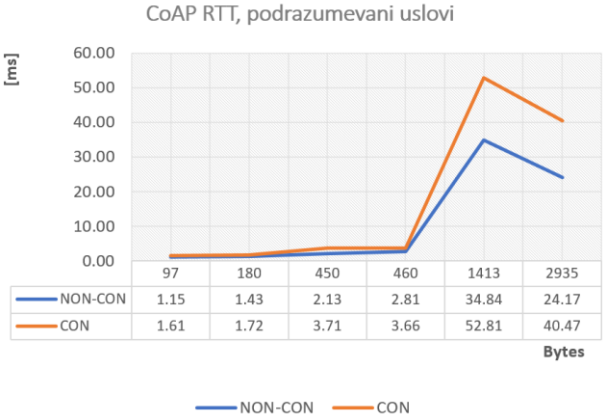
Latencija je merena kao funkcija veličine prenošene poruke, za oba protokola. Podrazumevani uslov je opseg od 85Mbps, kao i 0% gubitaka paketa. Za dobijanje rezultata, experiment je izvršavan 5 puta (N=5).

Grafik 5. pokazuje rezulate latencije za MQTT poruke različite veličine, u slučaju postavljanja vrednosti kvaliteta servisa na 0, odnosno na 1. Uočljivo je da je za QoS=1 latencija veća od QoS=0 za ~23ms. Skok na kraju kod prenošenja velike XML poruke je uzrokovan time što se na nižem nivou poruka prenosi iz dva IP paketa jer je MTU 1500 bajtova, dok je veličina prenošenog sadržaja veća.



Grafik 5. *Latencija MQTT poruka*

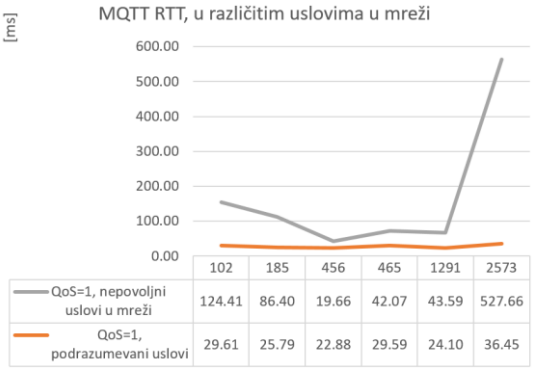
Uočava se i da na početku prenošenja poruka sa QoS=1 ne prati linearan trend kao kod QoS=0. Dolazi se do zaključka da implementaciji klijenta odnosno M2Mqtt biblioteki treba „vreme" da inicijalno počne da upravlja porukama sa višim kvalitetom servisa, učita potrebne module i/ili startuje procedure.



Grafik 6. *Latencija CoAP poruka*

Na grafiku 6. su predstavljeni rezultati za CoAP latenciju za slanje CoAP poruka koje ne očekuju potvrdu prispeća (NON-CON) i onih koje očekuju (CON) što odgovara MQTT kvalitetima servisa QoS 0 odnosno QoS 1 respektivno. U podrazumevanim uslovima, latencija je niska i za NON-CON i za CON poruke, do momenta slanja velike poruke koja mora da se fragmentuje i šalje u blokovima. Očekivano je duža latencija za NON-CON poruke. Takođe, bibilioteka ima problem sa procesiranjem enkriptovanih blokova. Izvršeno je po 5 iteracija za NON-CON i CON poruke, i trend je takav da je latencija duža za prvu poruku koja se transferuje iz blokova, u našem slučaju 1413 bajtova, nego za sledeću, duplo dužu poruku.

Latencija kao posledica nepovoljnih uslova u mreži je prikazana na graficima 7. i 8. Kvalitet servisa poruka je postavljen za MQTT QoS=1, CoAP CON, da bi se osigurali da će poruke sigurno doći na destinaciju. Uslovi su podešeni WANem-om tako da stopa gubitaka paketa u mreži bude 20% i da dostupni opseg bude 40 Mbps, što predstavlja oko 47% polaznog, podrazumevanog opseg 85Mbps. Oba grafika prikazuju, kao referentnu tačku, i latenciju u podrazumevanim uslovima, sa istim nivoom kvaliteta servisa.

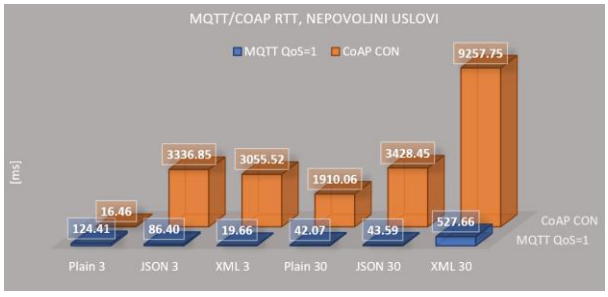


Grafik 7. *MQTT latencija u podrazumevanim i nepovoljnim uslovima u mreži*

Uočava se da je za MQTT (grafik 7), latencija porasla u uslovima mreže sa gubljenjem paketa (ima retransmisija) i smanjenjem opsega, pa tako imamo latenciju malo veću od 1/2s za velike XML poruke.

Grafik 8. *CoAP latencija u podrazumevanim i u mreži sa nepovoljnim uslovima*

Grafik 8. prikazuje latenciju kao posledicu nepovoljnih uslova u mreži, za CoAP poruke. Uočava se izuzetno visoka latencija, posebno za velike CON poruke, što se pripisuje gubljenju velikog broja paketa (20%).



Grafik 9. *MQTT i CoAP latencija u mreži sa nepovoljnim uslovima*

Na kraju (Grafik 9) je predstavljeno poređenje latencija za MQTT QoS=1, CoAP CON poruke, u mrežama sa nepovoljnim uslovima. Uočava se da je za velike poruke,

latencija za CoAP izuzetno visoka. Aplikativni sadržaj se deli na blokove od 512 bajtova, što znači da velika XML poruka zauzima >5 blokova , svaki se pakuje u zaseban UDP datagram i očekuje se potvrda dostavljanja. Sa stopom gubitaka od 20%, u smanjenom opsegu, ima puno retransmisija.

4. UPOTREBA IOT KOMUNIKACIONIH TEHNOLOGIJA ZA NADZOR BANDERA

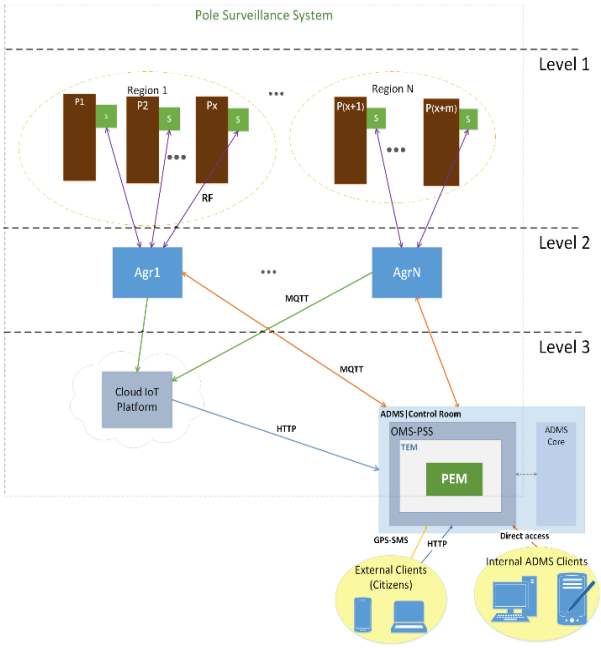
Rizik po bandere predstavljaju saobraćajne nesreće, oluje (sneg, vetar, led), poplave, zemljotresi, sadnice/drveće neodgovarajuće veličine u neposrednoj blizini, životinje (insekti, ptice). Padovi ili naginjanja bandera, zajedno sa propratnom opremom, predstavljaju incidente u mreži koji se mogu kategorisati na ispade (eng. *Outage*) koji dovode do deenergizacije i incidente koji predstavljaju smetnje/poremećaje u. Postoji rizik da čovek pokuša sam da popravi banderu, ili priđe srušenoj banderi sa svom njenom opremom smatrajući je deenergizovanom i na taj način se dovede u opasnost od strujnog udara. Zbog nepredvidive dinamike ljudskog faktora u okruženju bandera nužno je osigurati ih.

U pametnim mrežama se koristi sistem za upravljanje ispadima (eng. *Outage Management System* OMS), kao jedna od ključnih komponenti naprednog sistema za upravljanje distributivnom mrežom (eng. *Advanced Distribution Managament System* ADMS), za upravljanje svim planiranim i neplaniranim radovima u mreži, uključujući ispade, manipulisanje prekidačkom opremom, saniranje opasnosti, održavanje.

4.1. Predlog rešenja

Predlaže se sistem za online nadgledanje bandera (eng. *Pole Surveillance System* PSS) baziran na IoT tehnologijama, za rano detektovanje promena položaja bandera, kao i promena u okruženju odnosno potencijalnih incidenata/ispada u mreži uzrokovanih problemima sa banderama. Sistem je predložen kao proširenje tipičnih SG OMS sistema i namenjen je da se koristi integrisan sa ostalim komponentama rešenja za upravljanje ispadima. Fokus je na komponenti za upravljanje događajima sa bandera (eng. *Poles Events Manager* PEM) čija osnovna ideja je opametnjivanje bandera tako da kroz online nadzor, u slučaju naginjanja odnosno rušenja bandere, kontrolni centar/OMS može da bude obavešten/upozoren. Rešenje je hijerarhijsko i raspodela entiteta u rešenju je tronivojska. Na slici 2. je prikazan dijagram OMS-PSS sistema sa označenim komunikacionim tehnologijama koje se koriste između određenih komponenti.

Na nivou grada postoji veliki broj bandera, grupisanih u regije, na koje se instaliraju merni čvorovi. Za podskup geografski bliskih bandera, postoji nadređen agregator. Za agregatore je nadređen ADMS/OMS odnosno kontrolni čvor. Prisutna je opciona Cloud IoT platforma. Merni čvor omogućuje detekciju: nepogoda (požara, zemljotresa), pozicije (nagib/srušenost, lokacija) bandere. Slanje podataka sa mernih čvorova ka agregatorima se vrši modulima radio tehnologije (RF) modulima koji mogu da imaju domet i do 5km. Agregator dobavlja podatke sa mernih čvorova, obrađuje ih i potom prosleđuje u kontrolni centar upotrebom LTE, WiMAX, WiFi ili žične tehnologije. Za primanje podataka sa podređenih mernih čvorova koristi RX RF modul. Kontrolna soba ima potpuni uvid u stanje svih ispada u mreži. Web aplikacija OMS-PSS sistema omogućava korisnicima da pristupe ažurnim informacijama o trenutnim problemima. Preko istog portala je moguće i prijavljivanje problema u mreži.



Slika 2. – Globalni prikaz OMS-PSS sistema

Komunikacija između mernih čvorova i agregatora je dvosmerna, odnosno postoje dva RF modula (RX i TX). Za komunikaciju se koristi UART. Komunikacija između agregatora i kontrolnog centra ili clouda, se dešava preko WiFi, LTE, ili WiMAX tehnologije. Aplikativni protokol je MQTT.

5. ZAKLJUČAK

Zaključak je da su arhitekture IoT rešenja kombinovane i na određenim nivoima komunikacije su uposleni protokoli bazirani na drugačijim komunikacionim modelima. U vezi sa eksperimentalnim delom, u daljem radu je poželjno testirati protokole podešavanjem veličine MTU-a, tako da odgovara različitim protokolima nižih nivoa. Implementirati custom enkripciju za MQTT i koristiti OSCORE za CoAP. Cilj je temeljnije se baviti problemom bezbednosti.

6. LITERATURA

[1] Z. Shelby, K. Hatke, and C. Bormann, "The Constrained Application Protocol (CoAP)," RFC Editor, 2014

[2] [mqtt-v3.1.1] MQTT Version 3.1.1. Edited by Andrew Banks and Rahul Gupta. 29 October 2014. OASIS Standard., 2014.

Kratka biografija:

Miljana Vujaković je rođena 14.09.1994. godine u Novom Sadu. Fakultet tehničih nauka u Novom Sadu je upisala školske 2013/2014. godine. Diplomirala je 2018. godine na odseku za Elektrotehniku i računarstvo, smer „Primenjeno softversko inženjerstvo", i iste godine je upisala master studije na smeru „Primenjeno softversko inženjerstvo".