ELEKTROTEHNIŠKI VESTNIK 87(3): 102-108, 2020
IZVIRNI ZNANSTVENI ČLANEK

Protokol za zanesljiv prenos alarmnih sporočil prek interneta

Tomaž Dežman[1], **Sašo Tomažič**[2], **Grega Jakus**[2]

[1] *Aldia, d. o. o., informacijske storitve, Pot za Brdom 100, 1000 Ljubljana*
[2] *Univerza v Ljubljani, Fakulteta za elektrotehniko, Tržaška cesta 25, 1000 Ljubljana, Slovenija*
E-pošta: tomaz.dezman@aldia.si, saso.tomazic@fe.uni-lj.si, grega.jakus@fe.uni-lj.si

Povzetek. Sistem Intervencije.net je namenjen zbiranju in posredovanju informacij o nesrečah reševalnim službam. Že dalj časa obstaja potreba po samodejnem zbiranju in posredovanju tovrstnih informacij ter učinkovitejšem obveščanju članov reševalnih skupin. Sistem Intervencije.net smo zato nadgradili z novim komunikacijskim kanalom, ki temelji na internetnem omrežju in aplikacijskem protokolu za zanesljivo izmenjavo časovno kritičnih informacij med avtonomnimi napravami in jedrnim delom omrežja. Protokol, ki smo ga poimenovali IntP (Intervencije.net Protocol), smo v članku opisali po posameznih elementih specifikacije protokolov. Protokol IntP je trenutno v postopku preizkušanja v stvarnem okolju, pri čemer smo se najprej osredotočili na gasilska društva. Trenutno po protokolu komunicira 50 avtonomnih odjemalcev in dva strežnika. Skupaj delujejo že več kot 250 tisoč ur, v tem času pa nismo zaznali nepravilnosti v njihovem delovanju.

Ključne besede: protokol, alarm, reševanje, intervencija, internet

A protocol for a reliable transmission of alarm messages over the Internet

The Intervention.net system is intended for the collection and dissemination of information on accidents to emergency services. For a long time, there has been a need to automatically collect and provide this kind of information and to inform the members of the rescue teams more effectively. The paper presents the Intervention.net system upgraded with a new communication channel based on the Internet network and application protocol for a reliable exchange of critical information between autonomous devices and the core part of the network. The Intervention.net Protocol (IntP) is described by its individual specification elements. Currently, IntP is being tested in a real-world environment with the focus on firefighting brigades. 50 autonomous clients and two servers have been communicating using the presented protocol for over 250,000 hours without detecting any operational anomalies.

Keywords: protocol, alarm, intervention, Internet

1 UVOD

Uporaba sodobnih informacijsko-komunikacijskih tehnologij lahko pomembno vpliva na učinkovitost reševalnih služb. S hitrim posredovanjem natančnih informacij o nesreči lahko namreč močno skrajšamo odzivni čas reševalne službe. Uspešen primer uporabe informacijsko-komunikacijskih tehnologij na področju reševanja je sistem eCall, ki v primeru prometne nesreče pristojnim službam samodejno sporoči mesto nesreče [1]. Poleg skrajšanja odzivnega časa uporaba sodobnih sistemov za obveščanje omogoča še učinkovitejšo organizacijo intervencije, saj lahko s pomočjo teh sistemov posredujemo tudi informacije o tem, kdo se je na intervencijo odzval in kakšno opremo ima na voljo.

Da so hitre in natančne informacije ključne za uspešno organizacijo reševalnih dejavnosti, priča množica aktualnih projektov, med katerimi se večina osredotoča na organizacijo in vodenje intervencij na nacionalni ravni. Primera sta projekt NEXES [2], ki se ukvarja predvsem z geografskim usmerjanjem klicev v regijske centre za obveščanje, in 6InAction [3], ki je namenjen vzpostavitvi intervencijskega prenosnega omrežja v primeru obsežnih naravnih in drugih nesreč.

V Sloveniji od leta 2010 sicer uporabljamo sistem Intervencije.net [4], v katerega so vključene različne službe s področja zaščite in reševanja, kot so gasilska društva, bolnišnice, zdravstveni domovi, nujna medicinska pomoč, gorska in jamarska reševalna služba, kinološka zveza, zasebne reševalne službe nekaterih podjetij in druge. Danes tako v sistemu Intervencije.net deluje že več kot 940 reševalnih služb z več kot 36 tisoč reševalci.

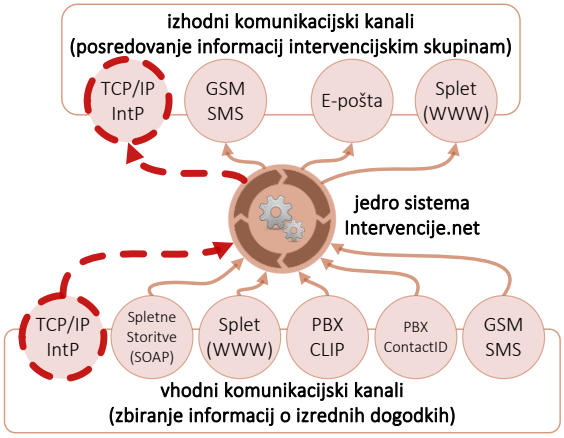
Sistem Intervencije.net ima pred preostalimi omenjenimi sistemi pomembno prednost. Gre namreč za sistem, ki je v Sloveniji že dobro preizkušen v lokalnih okoljih. Poleg tega pa, čeprav je namenjen predvsem podpori lokalnih reševalnih skupin, omogoča tudi integracijo s sistemi za vodenje intervencij na nacionalni ravni, saj lahko zanje zbira podatke iz lokalnih okolij.

Sistem Intervencije.net zbira informacije o nesrečah prek različnih kanalov, ki vključujejo (slika 1):

- *spletne storitve*, prek katerih so v sistem posredovani alarmi iz požarnih central in sporočila, ki jih regijski centri za obveščanje sicer pošiljajo reševalcem prek njihovih pozivnikov;

Prejet 13. januar, 2020
Odobren 7. april, 2020

- *spletno stran*, prek katere lahko član intervencijske skupine ali dispečer obvesti preostale člane;
- *klic na predpisano telefonsko številko*, pri čemer kombinacija kličoče in klicane številke določa intervencijsko enoto, ki bo aktivirana;
- *samodejno javljanje alarmov* nadzornim centrom z uporabo protokola ContactID [5], ki ga uporabljajo alarmne naprave;
- *SMS-sporočila*, ki jih pošiljajo uporabniki sistema ali naprave z vgrajenim modulom GSM.



Slika 1: Vhodni in izhodni kanali v sistemu Intervencije.net.

Sistem informacije o nesrečah posreduje udeležencem intervencij prek SMS-sporočil, elektronske pošte ali prek naprav interneta stvari (slika 1). Uporabnik se lahko na sporočilo o intervenciji odzove s klicem na predpisano telefonsko številko ali z uporabo namenske mobilne aplikacije. Sistem omogoča vodji intervencije tudi pregled odzivov na intervencijo prek spletne strani.

Čeprav je obveščanje s pomočjo sistema Intervencije.net preizkušeno v praksi, ima sistem še vedno nekaj omejitev, zaradi katerih je potrebna njegova nadgradnja:

- Sistem lahko uporabnikom posreduje le informacije o nesrečah, o katerih je nekdo že obvestil center za obveščanje. Samodejno obveščanje v veliki večini primerov ni mogoče.
- Obveščanje osebja reševalnih služb, ki ne uporabljajo sistema tihega alarmiranja z uporabo pozivnikov, je mogoče le prek spletne aplikacije oziroma s pošiljanjem SMS-sporočila ali prek klica na predpisano telefonsko številko. Veliko lažje bi bilo, če bi o intervenciji osebje obvestili s pritiskom na gumb.
- Pojavila se je potreba po avtomatizaciji nekaterih postopkov ob pozivu na intervencijo. Primer je samodejno obveščanje članov intervencijske skupine, ki imajo opravljen izpit iz prve pomoči, ko je zaznana uporaba samodejnega zunanjega defibrilatorja (AED). Gasilska društva želijo tudi samodejno odpiranje garažnih vrat gasilskega doma in opozarjanje ljudi v okolici s svetlobnimi in zvočnimi signali v primeru intervencije.

Poleg omenjenih zahtev mora biti nadgradnja sistema dosegljiva čim širšemu krogu uporabnikov in zato cenovno sprejemljiva ter enostavna za uporabo.

Da bi izpolnili postavljene zahteve, smo se odločili za nadgradnjo obstoječega sistema Intervencije.net z vhodno-izhodnim komunikacijskim kanalom, prek katerega avtonomne naprave jedrnemu delu posredujejo informacije o zaznanih izrednih dogodkih (npr. požaru), hkrati pa se odzivajo na ukaze jedrnega dela sistema (npr. za odpiranje vrat). Komunikacija med odjemalci in jedrnim delom temelji na obstoječem internetnem omrežju, nadgrajenim z aplikacijskim protokolom za podporo prenosu časovno kritičnih informacij (slika 1, prekinjena črta), ki smo ga poimenovali IntP (Intervencije.net Protocol).

2 Protokol IntP

Zaradi asimetrične strukture omrežja Intervencije.net (s centraliziranim jedrnim delom se povezuje večje število prostorsko razpršenih odjemalcev) ima tudi protokol IntP asimetrično zasnovo. Prostorsko razpršene avtonomne naprave imajo tako vlogo odjemalcev, ki se povezujejo s partnerskim protokolnim osebkom v vlogi strežnika v jedrnem delu sistema.

Komunikacijski protokol v razslojeni protokolni arhitekturi opredeljujejo štiri sestavine, in sicer

- nabor storitev, ki jih protokol ponuja uporabniku,
- specifikacija (navideznega) kanala, ki ga protokol potrebuje za zagotavljanje svojih storitev,
- nabor in format protokolnih sporočil, ter
- protokolna pravila.

Posamezne sestavine protokola IntP so opisane v nadaljevanju.

2.1 Storitve protokola IntP

Protokol IntP je povezavno naravnan protokol, ki svojemu uporabniku nudi:

- zanesljiv prenos uporabniških sporočil s časovno kritično vsebino,
- overjanje odjemalcev,
- šifriranje in dešifriranje sporočil, ter
- odkrivanje izpada komunikacijske poti.

Uporabniški proces mora vnaprej poznati nabor storitev, ki mu jih ponuja protokol za komunikacijo z oddaljenim partnerjem, vključno z načinom, kako te storitve zahteva in pridobi rezultat njihovega izvajanja. Interakcijo med protokolnim osebkom in njegovim uporabnikom v teoriji protokolov opišemo s t. i. *primitivi* [6]. V izvedbi protokolnega osebka so primitivi za uporabo njegovih storitev pogosto udejanjeni v obliki klicev predpisanih funkcij programskega vmesnika protokolnega osebka, primitivi za obveščanje uporabnika pa kot asinhroni povratni klici predpisanih uporabnikovih funkcij protokolnega osebka. Primitivi protokola IntP so predstavljeni v tabelah 1 in 2.

Tabela 1: Primitivi za uporabo storitev protokola IntP.

primitiv	parametri	opis
oddaja sporočila	*id odjemalca, sporočilo*	pošiljanje uporabniškega sporočila z uporabo protokola IntP
sprejem odjemalca	*id odjemalca, šifrirni ključ*	sprejem odjemalca, o katerem protokolni osebek predhodno obvesti uporabnika s primitivom »nov odjemalec«
odjava odjemalca	*id odjemalca, razlog*	zahteva, da se komunikacijski kanal med strežnikom in odjemalcem zapre ter se sprostijo vsi zaseženi viri

Tabela 2: Primitivi za obveščanje uporabnika protokola IntP

primitiv	parametri	opis
nov odjemalec	*id odjemalca*	v strežnik se je povezal nov odjemalec
prijava odjemalca	*id odjemalca*	novi odjemalec se je uspešno overil
napaka v komunikaciji	*id odjemalca, razlog*	komunikacija z odjemalcem ni mogoča iz navedenega razloga
novo sporočilo	*id odjemalca, sporočilo*	obvestilo o novem sporočilu partnerja

2.2 Kanal, ki ga potrebuje protokol IntP

Protokol IntP se za zagotavljanje zanesljivosti prenosa zanaša na protokol transportnega sloja, ki mora poskrbeti za ohranjanje vrstnega reda sporočil, odkrivanje in odpravljanje napak v sporočilih, odkrivanje in nadomeščanje izgubljenih sporočil ter odkrivanje in izločanje podvojenih sporočil. Najprimernejši kandidat za transportni protokol je tako protokol TCP (Transmission Control Protocol).

Protokol IntP je sporočilno naravnan protokol (vsako uporabniško sporočilo prenaša v lastnem protokolnem sporočilu), TCP pa je tokovno naravnan (čaka, da se nabere toliko podatkov, da napolni celotno protokolno sporočilo). V primeru prenosa alarmnih sporočil takšno čakanje ni zaželeno, zato lahko v ta namen protokol TCP prilagodimo tako, da izključimo Naglov algoritem [7].

2.3 Nabor in formati sporočil

Protokol IntP vsebuje 11 vrst sporočil. Ta so namenjena overjanju odjemalcev, prenosu uporabniške informacije, upravljanju strežnika in odjemalcev ter nadzoru razpoložljivosti transportnega kanala. Formati sporočil se razlikujejo glede na vrsto sporočila, vsa pa vsebujejo glavo in rep (slika 2, tabela 3).

V glavah vseh sporočil je polje za označbo vrste sporočila (TYPE), ki obsega dva znaka, nekatera sporočila pa vsebujejo tudi polje z zaporedno številko sporočila (SN). Rep sporočil sestavlja zaporedje znakov za prehod na začetek nove vrstice (t. i. CR LF, angl. *Carriage Return, Line Feed*), ki označuje konec sporočila. Polje z vsebino je prisotno le v sporočilih CHAP, DATA in PAR, ki so podrobneje predstavljena v razdelkih, ki sledijo.

Protokol IntP je znakovno naravnan protokol, kar pomeni, da morajo biti binarna zaporedja v posameznih poljih tolmačena po eni izmed kodnih tabel, pri čemer IntP uporablja 8-bitno ASCII-tabelo.

glava		vsebina	rep
TYPE (2 znaka)	**SN** (4 znaki)	uporabniško sporočilo ali druga vsebina	**CR LF** (2 znaka)
vrsta sporočila	zaporedna št. sporočila (razen pri CHAP in HB)		znaka za konec sporočila

Slika 2: Splošni format sporočil protokola IntP. Razmejilni znak med posameznimi polji je znak '|'.

Tabela 3: Nabor sporočil v protokolu IntP.

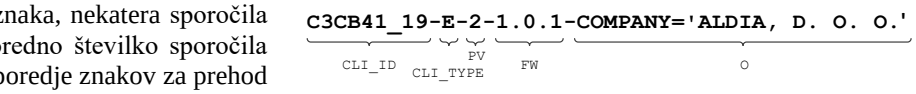
vrsta in opis sporočila	vsebina v TYPE	polje SN	polje vsebina
CHAP0 – Identifikacija odjemalca strežniku	C0	NE	DA
CHAP1 – Strežnik posreduje izziv za overjanje	C1	NE	DA
CHAP2 – Odgovor odjemalca na izziv iz CHAP1	C2	NE	DA
CHAP3 – Rezultat overjanja	C3	NE	DA
DATA – Prenos uporabniške informacije	DA	DA	DA
ACK – Potrditev predaje sporočila uporabniku	AY	DA	NE
NACK – Negativna potrditev – predaja sporočila lokalnemu uporabniku ni uspela	AN	DA	NE
HEARTBEAT – Nadzor razpoložljivosti transportnega kanala	HB	NE	NE
PING – Meritve odzivov protokolnih osebkov	P0	DA	NE
PONG – Odgovor na PING	P1	DA	NE
PAR – Prenos parametrov povezave	PA	NE	DA

2.3.1 Sporočila CHAP

Sporočila CHAP so namenjena overjanju uporabnika po postopku *izziv in odgovor*, ki je predstavljen v razdelku 2.4.1. Struktura vsebine sporočila CHAP0 je predstavljena v tabeli 4, slika 3 pa prikazuje primer vsebine sporočila. Struktura sporočil CHAP1, CHAP2 in CHAP3 je preprostejša od strukture sporočila CHAP0, saj vsebina teh sporočil ni strukturirana (tabela 5).

Tabela 4: Format vsebine sporočila CHAP0

polje	št. znakov	opis
CLI_ID	7 .. 11	enolična oznaka odjemalca
CLI_TYPE	1	vrsta strojne opreme za komunikacijo z okolico
PV	1 .. 5	različica protokola IntP
FW	1 .. 10	različica programske opreme odjemalca
O	0 .. 255	druge poljubne informacije



Slika 3: Primer vsebine sporočila CHAP0. Razmejilni znak med polji v sporočilu je znak '-'.

Tabela 5: Vsebina sporočil CHAP1, CHAP2 in CHAP3

vrsta	vsebina
CHAP1	izziv za odjemalca, sestavljen iz globalnega enoznačnega identifikatorja (GUID), identifikacije odjemalca v decimalni obliki in treh naključnih znakov
CHAP2	rezultat zgoščevalne funkcije SHA-1
CHAP3	rezultat primerjave izvlečkov: 'OK' ali 'ERR, wrong HASH'

2.3.2 *Sporočilo DATA*

Sporočila DATA so namenjena prenosu uporabniške informacije med odjemalcem in strežnikom. Ta lahko vključuje ukaze, alarme in meritve. Z ukazi strežnik od odjemalca zahteva vklop ali izklop določenega digitalnega izhoda oziroma releja ali drugače nadzoruje odjemalca. Alarmi vsebujejo informacije o izrednih dogodkih, ki jih odjemalec zazna v svoji okolici prek digitalnih in analognih vhodov ter o njih obvesti strežnik. Meritve vsebujejo vrednosti fizikalnih veličin, na primer temperature ali vlage, ki jih odjemalec meri s pomočjo nanj priključenih senzorjev. Primeri vsebine ukaza, alarma in meritve so prikazani v tabeli 6.

Tabela 6: Primeri vsebine sporočila DATA.

vsebina	**opis**
OUT*x*=ON	vklop digitalnega izhoda z oznako *x*
COMMAND=u	ukaz za nadzor odjemalca (ponovni zagon, javljanje stanja vhodno-izhodnih priključkov itd.)
INx=ON	aktiviran alarm z oznako *x*
MEx=y	vrednost *y*, izmerjena na senzorju z oznako *x*

2.3.3 *Sporočilo PAR*

S sporočili vrste PAR strežnik odjemalcem posreduje parametre protokola IntP (tabela 7), kot sta perioda pošiljanja sporočil HB in odložni čas T_c, katerega pomen je opisan v poglavju 2.4.6.

Tabela 7: Parametri protokola IntP.

parameter	**opis**	**nabor vrednosti**
THB	perioda pošiljanja sporočil HB	0 .. 120 s
T_c	odložni čas	0 .. 30 s

2.4 *Protokolni mehanizmi in pravila*

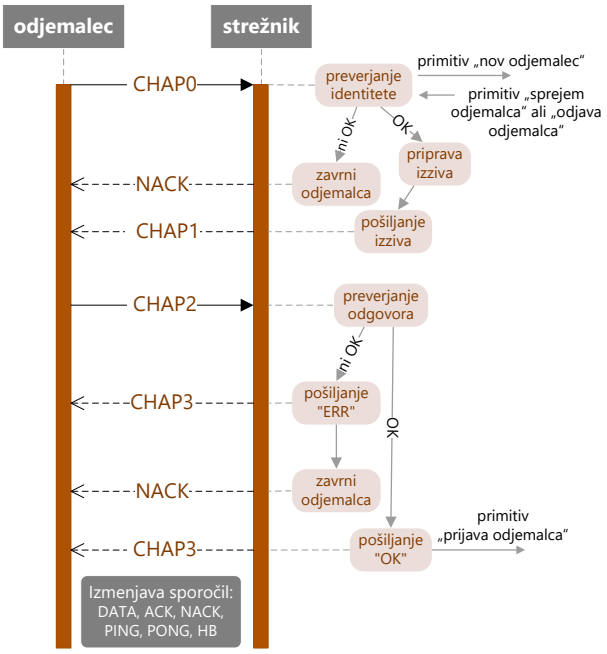
Vzpostavitev povezave med odjemalcem in strežnikom v protokolu IntP vključuje *identifikacijo in overjanje odjemalca*, čemur sledi *izmenjava uporabniške vsebine* (alarmov, ukazov, parametrov in meritev). Vsi omenjeni postopki zahtevajo *šifriranje* vsebine sporočil in *potrjevanje njihovega prejema*.

Zaradi redke narave prometa (alarmov, ukazov) je večino časa kanal neizkoriščen, zato protokolni osebek ne more vedeti, ali je prehoden, saj v tem času ne prejema potrditev prejema od svojega partnerja. A ker mora biti, ko se zgodi izredni dogodek in je treba strežniku poslati sporočilo, kanal prehoden, je treba morebitno neprehodnost kanala odkriti in razrešiti takoj, ko se ta pojavi. V ta namen vsak odjemalec periodično izvaja *nadzor razpoložljivosti* transportnega kanala.

Navedeni mehanizmi protokola IntP so v neformalni obliki podrobneje predstavljeni v nadaljevanju.

2.4.1 *Identifikacija in overjanje odjemalca*

Zanesljiv prenos sporočil zahteva povezavno naravnan protokol, za kar pa je potrebna začetna uskladitev med odjemalcem in strežnikom, ki ji pravimo vzpostavitev povezave. Pri protokolu IntP je njen namen predvsem overjanje odjemalcev (slika 4).



Slika 4: Overjanje odjemalca po postopku izziv in odgovor.

Overjanje poteka po različici postopka *izziv in odgovor* (angl. *Challenge and Response Protocol*) [8]. Po tem postopku se odjemalec po vzpostavitvi TCP-povezave predstavi strežniku s sporočilom CHAP0, v katerem se identificira s poljem CLI_ID (slika 3).

Strežnik odgovori odjemalcu s sporočilom CHAP1 (tabela 5), v katero doda naključno besedilo. Odjemalec izračuna izvleček prejetega besedila z zgoščevalno funkcijo SHA-1 in ključem, ki odjemalcu pripada. Rezultat nato pošlje strežniku v sporočilu CHAP2.

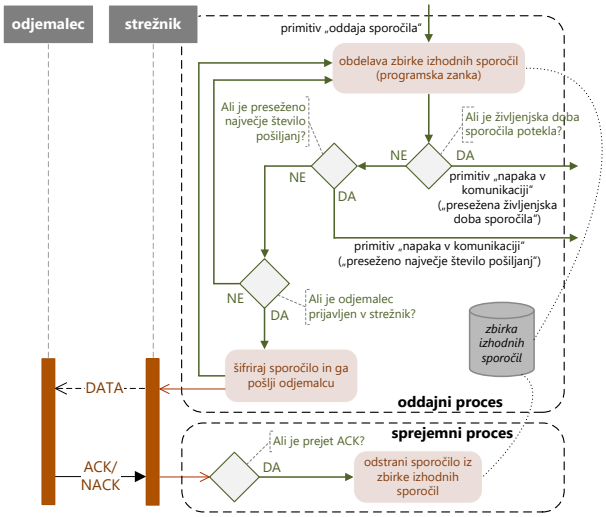
Strežnik primerja prejeti izvleček z izvlečkom, ki ga izračuna sam, ter o rezultatu obvesti odjemalca s sporočilom CHAP3 (tabela 5). Če se izvlečka ujemata, obvesti tudi svoj uporabniški proces s primitivom »nov odjemalec«, v nasprotnem primeru pa sprosti povezavo.

2.4.2 *Izmenjava uporabniških sporočil*

Uspelemu overjanju sledi izmenjava uporabniških sporočil. Ko strežnik prejme takšno sporočilo od odjemalca, najprej preveri, ali je ta že overjen. Neoverjenega odjemalca strežnik zavrne z negativno potrditvijo (NACK), v nasprotnem primeru pa dešifrira odjemalčevo sporočilo in preveri skladnost njegove strukture. Nato preda sporočilo s primitivom »novo sporočilo« lokalnemu uporabniškemu procesu, čemur sledi pošiljanje sporočila ACK odjemalcu.

Sporočila, namenjena odjemalcu, izroči strežniški uporabniški proces protokolnemu osebku IntP s primitivom »oddaja sporočila« (slika 5). Ta najprej preveri, ali

je prejemnik prijavljen v strežnik, nato pa sporočilo šifrira in pošlje odjemalcu. Če odjemalec še ni prijavljen, sporočilo zavrže in o tem obvesti uporabniški proces.



Slika 5: Pošiljanje sporočila DATA odjemalcu.

2.4.3 *Potrjevanje sporočil*

Strežnik in odjemalec morata prejeta sporočila potrjevati s pozitivnimi (ACK) ali negativnimi potrditvami (NACK). Sporočilo ACK potrjuje, da je sprejemni osebek sporočilo, na katero se potrditev nanaša, uspešno dešifriral in predal svojemu uporabniškemu procesu. Ta lahko namreč v primeru neustrezne vsebine sporočila ali napake pri njegovi obdelavi sporočilo tudi zavrne. V takem primeru (pa tudi v primeru neuspelega dešifriranja) osebek odgovori s sporočilom NACK, ki posredno predstavlja zahtevo za ponovno pošiljanje sporočila, na katero se negativna potrditev nanaša. Primer pošiljanja potrditvenih sporočil je prikazan na spodnjem delu slike 5.

2.4.4 *Šifriranje podatkov in transparentni prenos*

Protokol IntP zahteva šifriranje vsebine sporočil DATA s simetričnim šifrirnim postopkom AES (Advanced Encryption Standard) [9], ki je dovolj enostaven tudi za manj zmogljive mikrokrmilnike.

V nasprotju s čistopisom, ki po kodni tabeli ASCII vsebuje le znake z vrednostmi od 32 do 127, lahko v šifropisu najdemo katerikoli znak iz omenjene tabele (z vrednostmi med 0 in 255). V tem razponu sta problematična predvsem znaka za začetek nove vrstice z vrednostma 13 in 10 (CR in LF), ki v protokolu IntP označujeta konec sporočila (slika 2). Da protokolni osebek takega zaporedja ne bi napačno tolmačil kot konec sporočila, pretvorimo šifropis v šestnajstiški zapis, pri čemer vsako števko zapišemo z znaki iz tabele ASCII. S tem omejimo uporabljene znake na števke med 0 in 9 ter črke med A in F, ki pa so po tabeli ASCII zapisane z vrednostmi med 48 in 57 ter med 97 in 102. Okteta z decimalnima vrednostma 13 in 10 se tako pretvorita v zaporedje znakov '0', 'D' oziroma '0', 'A'.

2.4.5 *Nadzor razpoložljivosti kanala*

Ker v protokolnem skladu TCP/IP ni primernega mehanizma za nadzor razpoložljivosti transportnega kanala, tega v protokolu IntP zagotavljamo s sporočilom HB (angl. *HeartBeat*, slov. srčni utrip). Komunicirajoča osebka si sporočilo pošiljata, ko nimata na voljo drugih sporočil. Prejem sporočila HB (ali kateregakoli drugega sporočila) osebku namreč pove, da je pot do partnerja prehodna, pri čemer mora ponastaviti časovnik razpoložljivosti kanala. V primeru izteka časovnika osebek predvideva, da je kanal do partnerja neprehoden in o tem s primitivom »napaka v komunikaciji« obvesti svojega uporabnika.

Sporočilo HB nima vsebine in ne zahteva potrditve prejema in obveščanja uporabnika o njegovem prejemu, ampak se zavrže. Interval pošiljanja sporočila je nastavljiv s sporočilom PAR.

Sporočili PING in PONG sta namenjeni merjenju odzivnosti partnerja. Ko osebek prejme sporočilo PING, mora odgovoriti s sporočilom PONG. Strežnik lahko tako izračuna hitrost odziva posameznega odjemalca in temu prilagaja časovnik za ponovno pošiljanje sporočil.

2.4.6 *Ponovna vzpostavitev povezave*

Ob izpadu strežnika ali transportnega kanala se povezanim odjemalcem kmalu izteče časovnik razpoložljivosti kanala. V tem primeru bodo vsi prej s strežnikom povezani odjemalci poskušali ponovno vzpostaviti povezavo. To lahko povzroči preobremenitev strežnika, saj je lahko število odjemalcev, ki so bili povezani z nekim strežnikom, zelo veliko. Da bi preprečili preobremenitev strežnika, mora vsak odjemalec pred vsakim ponovnim poskusom vzpostavitve povezave počakati odložni čas T_c.

Strežnik lahko s sporočilom PAR prilagaja odložni čas številu vzpostavljenih povezav ali potencialnih odjemalcev. Če odjemalec od strežnika še ni prejel podatka o odložnem času, uporabi shranjeno privzeto vrednost (30 s). Ta je določena tako, da obstaja le minimalna verjetnost preobremenitve strežnika, po drugi strani pa se odjemalci vanj prijavljajo počasneje, kot bi se lahko, če bi od strežnika prejeli odložni čas, ki odraža dejansko stanje v omrežju in zmogljivosti strežnika.

2.4.7 *Časovniki*

Namen časovnikov v nekem protokolu je zagotoviti periodičnost dogodkov ali preprečiti čakanje na neki dogodek (npr. prejem pričakovanega sporočila), ki pa se nikoli ne zgodi. Protokol IntP ima tri časovnike:

- *Časovnik utripa* zagotavlja periodično pošiljanje sporočil HB, s pomočjo katerih lahko partner preverja razpoložljivost kanala.
- *Časovnik razpoložljivosti kanala* določa najdaljši čas čakanja na sporočilo partnerja. Če se časovnik

izteče, je uporabniški proces obveščen s primitivom »napaka v komunikaciji«.

- *Časovnik za ponovno pošiljanje sporočil* se sproži ob oddaji sporočila, ustavi pa ga prejeta potrditev ACK za to sporočilo. Če se časovnik izteče, je treba sporočilo ponovno poslati. Ponovno pošiljanje sporočila se ob ponavljajočem se iztekanju časovnika izvaja, vse dokler sporočilu na poteče življenjska doba (TTL, angl. *Time to Live*) oziroma je doseženo največje število pošiljanj. V tem primeru protokolni osebek obvesti uporabniški proces s primitivom »napaka v komunikaciji«.

3 IZVEDBA IN PREIZKUŠANJE PROTOKOLA

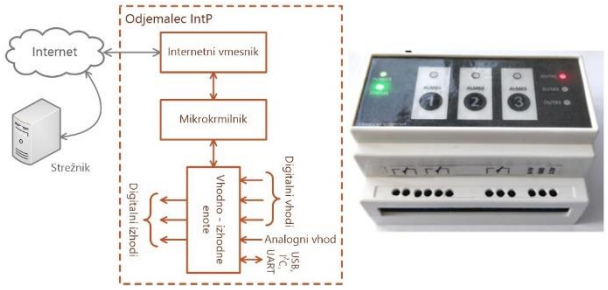
Protokolne osebke, ki delujejo kot IntP-odjemalci, smo izdelali v obliki mikrokrmilniških programov, strežnik pa kot storitev v okviru operacijskega sistema Windows.

3.1 Odjemalec

Odjemalec IntP je udejanjen kot proces na avtonomni napravi, ki pošilja v sistem Intervencije.net informacije o dogodkih in vrednostih, kot so pritisnjen gumb na napravi, sklenjene vhodne priključne sponke, izmerjena vrednost na analognem vhodu ali podatki, ki jih prejme iz komunikacijskih vodil, kot sta I2C (Inter-Integrated Circuit) in UART (Universal Asynchronous Receiver-Transmitter), prek katerih komunicira z drugimi napravami in senzorji.

Poleg tega lahko odjemalec alarme in ukaze s strežnika tudi sprejema ter jih posreduje svojemu uporabniškemu procesu in priključenim napravam prek digitalnih izhodov ali komunikacijskih vodil.

Načelna shema odjemalca IntP in njegova izvedba sta prikazani na sliki 6. Odjemalce smo izdelali na osnovi modula WEMOS D1 mini [10], ki med drugim vsebuje mikrokrmilnik ESP8266 z vgrajeno komunikacijo za komunikacijo prek brezžičnih omrežij in protokolnega sklada TCP/IP, napetostni stabilizator, 11 vhodno-izhodnih povezav, analogno-digitalni pretvornik ter povezavo USB.



Slika 6: Shema in izvedba odjemalca IntP.

3.2 Strežnik

Strežnik IntP je proces, ki se izvaja v jedru sistema Intervencije.net (slika 1). Njegova naloga je odziv na sporočila in zahteve odjemalcev ter posredovanje informacij drugim komponentam sistema.

Strežnik smo razvili z uporabo Microsoftovih tehnologij .Net Framework (aplikacijski del) in SQL Server (podatkovni del) ter se izvaja kot storitev na operacijskem sistemu Windows. Zaradi boljše preglednosti in preprostejšega vzdrževanja smo strežnik razdelili na odjemalsko, poslovno in podatkovno plast. Medtem ko prva predstavlja izvedbo protokola IntP na strežniku, je poslovna plast neposredni uporabnik protokola IntP in kot taka izvaja vsebinsko komunikacijo z odjemalci. Njene naloge vključujejo

- vodenje zbirke aktivnih odjemalcev,
- sprejem sporočil z odjemalske plasti ter njihovo posredovanje podatkovni plasti in v obratni smeri,
- odziv na izredne dogodke, kot je neprehodna povezava do nekega odjemalca.

Naloga *podatkovne plasti* je zagotoviti dostop do podatkov v podatkovni zbirki sistema Intervencije.net.

3.3 Namestitev in preizkus

Protokol IntP je trenutno v postopku preizkušanja v stvarnem okolju, pri čemer smo se najprej osredotočili na gasilska društva (slika 7). Posebno natančno smo testirali stabilnost delovanja odjemalcev in zanesljivost mehanizmov za preverjanje razpoložljivosti kanala ter ponovno vzpostavitev povezave s strežnikom, ki sta najbolj kritična elementa protokola.

Slika 7: Naprava IntP v električni omarici in tipka pred garažo gasilskega doma.

Trenutno sistem sestavljajo dva strežnika in 50 odjemalcev (21 v gasilskih društvih po celotni Sloveniji, 29 pa je pripravljenih za preizkuse). Skupaj delujejo več kot 250 tisoč ur, v tem času pa nismo zaznali nepravilnosti v

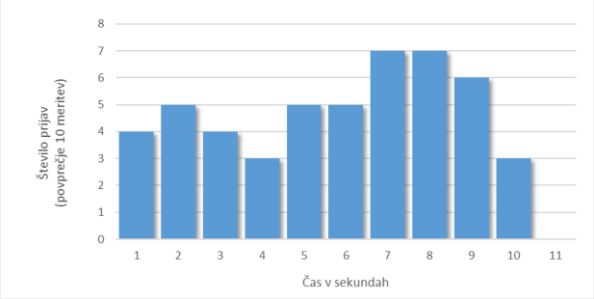
njihovem delovanju, razen v primeru izpada transportnega kanala, katerega razlog je bil pokvarjen usmerjevalnik gasilskega društva.

Mehanizem ponovne vzpostavitve strežnika smo testirali s periodo signala HB T_{HB} = 5 s in odložnim časom T_c = 10 s. Vsi odjemalci so se povezovali z istim strežnikom. V okviru preizkusa smo strežnik zaustavili za 30 s, da so vsi odjemalci z gotovostjo zaznali, da strežnik ni več dosegljiv. Sledil je ponoven vklop strežnika. Ko je bil strežnik pripravljen sprejemati zahteve odjemalcev za vzpostavitev povezave, smo te začeli beležiti. Opisan preizkus smo ponovili desetkrat.

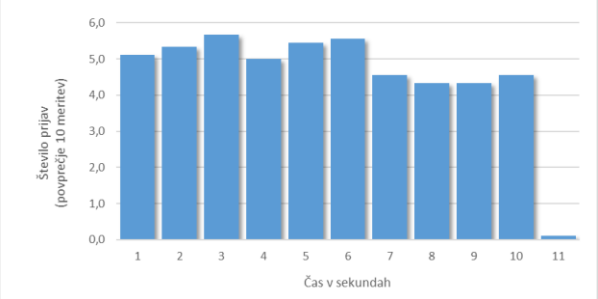
V vseh izvedenih poskusih je vseh 50 odjemalcev uspešno vzpostavilo povezavo s strežnikom v največ 11 sekundah. Največje število zahtevkov v intervalu ene sekunde je bilo 13. Povprečno število zahtevkov je bilo 4,5 na sekundo.

Slika 8 prikazuje rezultat ene izmed meritev, slika 9 pa povprečje vseh desetih meritev, ki je blizu optimalne razporeditve. Zaželeno je namreč, da se odjemalci čim bolj enakomerno razporedijo v časovnem intervalu, ki ga strežnik določi z odložnim časom T_c.

Testiranje smo ponavljali z različnimi vrednostmi parametrov. V primeru T_c = 100 ms in T_{HB} = 5 s se je na primer vseh 50 odjemalcev povezalo v le 140 ms, kar pa ni zaželeno, saj je strežnik v tem kratkem času zelo obremenjen.



Slika 8: Primer razporeditev zahtevanih povezav na strežnik (časovni intervali so razdeljeni na 1 sekundo).



Slika 9: Povprečna razporeditev zahtevanih povezav na strežnik vseh desetih meritev (časovni intervali so razdeljeni na 1 sekundo).

4 ZAKLJUČEK

V okviru dosedanjega preizkušanja nismo odkrili večjih pomanjkljivosti protokola IntP, kljub temu pa nameravamo protokol v prihodnosti preizkusiti še pri zelo velikem številu odjemalcev (več kot 1.000) in večjem številu strežnikov. V primeru slednjega bomo mehanizem povezovanja s strežniki nadgradili tako, da se bodo zahteve za vzpostavitev povezave čim bolj enakomerno razporedile med razpoložljive strežnike.

V prihodnosti nameravamo nadgraditi tudi sam sistem Intervencije.net. V okviru načrtovanih nadgradenj nameravamo predvsem dodati rezervni komunikacijski kanal v obliki SMS-sporočil za primere, če pride do prekinitve internetne povezave.

LITERATURA

[1] ETSC – Europan Transport Safety Council: New Pan-European Emergency Call System, september 2013, http://www.roadsafetyobservatory.com

[2] NEXES – NEXt generation Emergency Services, http://nexes.eu/

[3] Gen 6, 6 in Action – Smart communications solution in emergency situations, http://www.6inaction.net/

[4] Aldia, d. o. o.: Predstavitev sistema Intervencije.net., september 2015, https://www.intervencije.net

[5] Security Industry Association, Digital Communication Standard-Ademco® Contact ID Protocol-for Alarm System Communications.http://www.voip-sip-sdk.com/attachments/583/contact_id.pdf

[6] ISO/IEC 10731:1994, Information technology — Open Systems Interconnection — Basic Reference Model — Conventions for the definition of OSI services, december 1994, https://www.iso.org/standard/18824.html

[7] J. Nagle, Congestion Control in IP/TCP Internetworks, Network Working Group, Request for Comments 896, januar 1984, https://tools.ietf.org/html/rfc896

[8] C. A., Van Tilborgm Henk, S. Jajodia, Encyclopedia of Cryptography and Security. Springer Science & Business Media, julij 2014.

[9] Announcing the ADVANCED ENCRYPTION STANDARD (AES), Federal Information Processing Standards Publication 197. United States National Institute of Standards and Technology (NIST). november, 2001.

[10] WEMOS Electronics: D1 mini [WEMOS Electronics], https://wiki.wemos.cc/products:d1:d1_mini

Tomaž Dežman je leta 2015 diplomiral, leta 2018 pa magistriral na Fakulteti za elektrotehniko Univerze v Ljubljani. Zaposlen je v podjetju Aldia, d. o. o. Njegova raziskovalna zanimanja vključujejo naprave IoT in informacijske sisteme.

Sašo Tomažič je redni profesor na Fakulteti za elektrotehniko Univerze v Ljubljani in predstojnik Laboratorija za informacijske tehnologije. Njegova raziskovalna področja vključujejo obdelavo signalov, varnost v telekomunikacijah, elektronsko poslovanje in informacijske sisteme.

Grega Jakus je leta 2007 diplomiral, leta 2012 pa doktoriral na Fakulteti za elektrotehniko Univerze v Ljubljani. Leta 2013 je bil izvoljen v naziv docent za področje elektrotehnike. Njegovo glavno raziskovalno področje vključuje interakcijo med napravami in njihovimi uporabniki, aktiven pa je tudi na področju raziskav in razvoja telekomunikacijskih protokolov.