Heterogénne smerovanie v kapilárnych sieťach internetu vecí s použitím kompozitnej metriky

Ondrej Perešíni
2. ročník, PhD. prezenčné štúdium
Školiteľ: Tibor Krajčovič

Fakulta informatiky a informačných technológií, Slovenská technická univerzita v Bratislave
Ilkovičova 2, 842 16 Bratislava 4
ondrej.peresini@stuba.sk

***Abstrakt*— Rozvoj zariadení internetu vecí je priamo závislý od dostupnosti lacnej a energeticky efektívnej komunikačnej technológie. Súčasne používané komunikačné technológie nedokážu efektívne zabezpečiť všetky kladené požiadavky a takto vzniknuté siete majú nedostatky v podobe obmedzenej priepustnosti, krátkeho dosahu alebo vysokej ceny. Neexistuje univerzálna technológia, ktorá by pokryla všetky popisované aspekty a z tohto dôvodu vzniká zoskupenie rôznych heterogénnych komunikačných technológií do jednej spoločnej kapilárnej siete. Rôzne aplikácie majú pritom aj rôzne požiadavky na komunikačné parametre a teda aj použitú komunikačnú technológiu. Súčasné smerovacie protokoly nedokážu efektívne pokrývať túto potrebu a na základe rôznych komunikačných požiadaviek dynamicky vyberať medzi rôznymi technológiami. Na zabezpečenie efektívnej komunikácie navrhujeme vylepšenie smerovacieho protokolu RPL a použitej hybridnej metriky zohľadňujúcej požiadavky aplikácií.**

Kľúčové slová—Kapilárne a heterogénne siete, Internet Vecí, sieťové smerovanie, protokol RPL

I. Úvod

Digitalizácia a inteligentné riadenie domácností sa stáva neoddeliteľnou súčasťou budovaných a aj existujúcich domácností. Vývoj takýchto systémov prináša množstvo otázok a výziev, ktoré smerujú najmä na oblasť ich zabezpečenia, komunikácie a kompatibility medzi rôznymi systémami. Práve do tejto oblasti vstupuje myšlienka internetu vecí (IoT), ktorej cieľom je pospájať všetky zariadenia do jedného systému, ktorý bude zdieľať pripojenie do internetu. Všetky takéto zariadenia pritom poskytujú určitú funkcionalitu, ktorá prináša dodatočnú hodnotu pre používateľa, keďže inteligentné objekty vzájomne kooperujú s fyzickými alebo virtuálnymi zdrojmi. Takéto zdroje sú charakteristické vysokým stupňom heterogénnosti, čím poskytujú rôznu funkcionalitu aj zariadeniam, ktoré boli pôvodne len jednoúčelové. Aby bolo možné takéto zariadenia vzájomne sieťovo poprepájať, tak je potrebné navrhnúť vhodný model kapilárnych sietí, ktorý pozostáva z rôznych bezdrôtových, mobilných a pevných sietí. Každý modul má individuálne a špecifické požiadavky na prenosové parametre a popri tom je nevyhnutné minimalizovať energetické nároky tak, aby niektoré moduly mohli na obmedzený zdroj energie fungovať aj niekoľko rokov.

II. Internet Vecí

Internet vecí je reprezentovaný množstvom zariadení, ktoré spolu vzájomne komunikujú a prinášajú dodatočnú funkcionalitu, ktorú by jednotlivé zariadenia samostatne nedokázali priniesť. Dobrým príkladom je napríklad domáca televízia a inteligentný termostat. Zatiaľ čo termostat obsahuje teplotný senzor vďaka ktorému dokáže posielať príkazy na regulovanie teploty, tak nedokáže zobrazovať nejaké podrobnejšie informácie o nameraných teplotách. A práve tu vstupuje idea internetu vecí, ktorá termostatu umožní využiť funkcie iných zariadení v sieti. V tomto konkrétnom prípade môžeme uvažovať napríklad o televízii, ktorá termostatu poskytne funkciu zobrazenia. Používateľ si vďaka tomu môže pozrieť grafické priebehy teploty a výkonu vykurovania alebo chladenia, čo by samostatný termostat nedokázal. Samozrejme aj termostat môže mať grafickú obrazovku, avšak to by zbytočne navyšovalo cenu a komplexnosť takéhoto senzoru, pričom práve myšlienka internetu vecí umožní získať takúto doplnkovú funkcionalitu bez zbytočného navyšovania ceny a komplexnosti riešenia.

Zariadenia internetu vecí musia vzájomne komunikovať, pričom táto komunikácia nemusí byť riešená pomocou jedného typu siete, ale je možné aplikovať heterogénne kapilárne siete. Kapilárne siete vznikajú najmä z dôvodu rozdielnych komunikačných požiadaviek zo strany rôznych zariadení. Zatiaľ čo senzory nepotrebujú vysokú dátovú priepustnosť, tak kamerový systém si nevystačí s úzkym komunikačným pásmom. Každá komunikačná technológia tak prináša rôzne výhody a zároveň nevýhody a vhodným prepojením takýchto technológií je možné dosiahnuť optimálne komunikačné vlastnosti.

III. Kapilárne siete

Bez možnosti zdieľania si informácií sú IoT zariadenia len jednoúčelové bez ďalšej pridanej hodnoty. Pre zabezpečenie vhodného komunikačného prepojenia je nutné použiť kapilárne siete, ktoré pozostávajú z pevných, mobilných a bezdrôtových sietí. Zatiaľ čo smerovanie v pevných a mobilných sieťach je štandardizované, tak pri bezdrôtových sieťach existuje vysoký potenciál pre ďalšie zlepšenia. V tejto práci sa sústreďujeme na infraštruktúrne založené bezdrôtové siete a Ad-Hoc siete.

A. Infraštruktúrny model a Ad-Hoc siete

Väčšina súčasne používaných bezdrôtových sietí je založená na infraštruktúrnom modeli, ktorý obsahuje zariadenia dvoch kategórií: prístupové body a koncové zariadenia. Základnou vlastnosťou takýchto sietí je, že všetky koncové zariadenia sa pripájajú len na zvolený prístupový bod, cez ktorý realizujú všetky svoje dátové prenosy. Komunikáciu moderuje a riadi centrálna autorita, ktorá je reprezentovaná jedným alebo viacerými prístupovými bodmi a tie určujú ktoré koncové zariadenia môžu v danom čase vysielať na zdieľanom komunikačnom kanále. Nevýhodou infraštruktúrnych sietí je vyššia cena na vybudovanie, citlivosť na útoky, ktoré dokážu narušiť alebo úplne znemožniť komunikáciu s centrálnou autoritou, ale aj maximálna dosahovaná komunikačná rýchlosť.

Ad-Hoc sieť pozostáva z rovnocenných zariadení ktoré neobsahujú centrálnu riadiacu autoritu, ale všetky bezdrôtové zariadenia sú rovnocenné a spadajú pod jednu komunikačnú doménu. Každý komunikačný uzol tak dokáže komunikovať so susedným uzlom aj bez použitia prístupového bodu. Toto prináša autonómnosť od bezdrôtovej infraštruktúry, väčšie pokrytie bezdrôtovej domény, menšiu energetickú náročnosť pri použití nízkoenergetických komunikačných technológií ale aj rýchlu konfiguráciu nových modulov. Nespornou výhodou je aj nízka cena, ktorá sa nezvyšuje o cenu prístupových bodov a flexibilita celého modelu, ktorý nie je závislý od niekoľkých modulov v sieti, čo prináša flexibilitu a umožňuje samo-uzdravovanie takejto siete v prípade výpadku určitých komunikačných uzlov.

B. Jednotný model Ad-hoc sietí

Zariadenia komunikujú v rámci svojej bezdrôtovej domény priamo so susednými zariadeniami, avšak v prípade vzdialenejších uzlov je nutné použiť viacskokové (Multi-hop) spojenie a zodpovedajúce smerovacie protokoly. Použitie vhodných smerovacích protokolov výrazne ovplyvňuje parametre vzniknutej Ad-hoc siete a vo veľkej miere určuje maximálnu priepustnosť a oneskorenie v rámci takejto siete. Je mimoriadne dôležité použiť optimálny smerovací protokol, ktorý sprístupní plný potenciál vzniknutej Ad-hoc siete.

Smerovacie protokoly musia byť dostatočne robustné a zároveň aj dostatočne rýchle, tak aby sa dokázali efektívne vysporiadať so stratovosťou datagramov a prípadnej mobilite zariadení. Nemenej dôležitým aspektom je energetická spotreba, ktorá sa zvyšuje s vyššou frekvenciou komunikácie z dôvodu zmeny polohy a smerovacích algoritmov ako aj výpočtových nárokov samotných algoritmov. Jednou z možností redukcie zmien v smerovaní je zväčšenie veľkosti bezdrôtovej domény, avšak táto zmena by sa negatívne prejavila na celkovej komunikačnej kapacite Ad-hoc siete. Súčasným trendom je minimalizácia veľkosti komunikačných domén, čo s narastajúcim počtom zariadení kladie vyššie nároky na návrh a optimalizáciu smerovacích algoritmov. Horná hranica prenosovej kapacity pre Ad-hoc sieť nerastie, avšak existuje niekoľko metód ako túto kapacitu alternatívne navyšovať:

- minimalizovať počet preposielaní v doméne
- použiť rôzne komunikačné technológie (kapilárne siete)
- minimalizovať interferencie
- použiť viacero komunikačných frekvencií (kanálov)
- použiť rôzne polarizované a umiestnené antény
- zmeniť formu komunikácie na lokálnu (umiestniť najčastejšie komunikujúce uzly čo najbližšie k sebe)
- komunikačné brány prepojiť inou vysokorýchlostnou linkou a odbremeniť tak zvyšok siete

C. Smerovanie v Ad-hoc sieťach

V Ad-hoc sieti fungujú všetky uzly ako smerovače a podieľajú sa na budovaní a udržiavaní smerovacích tabuliek. Cieľový uzol môže byť dosiahnuteľný rôznymi trasami a je potrebné zabezpečiť smerovací algoritmus výberu najvhodnejšej cesty podľa rôznych kritérií na prenos. Takéto uzly môžu v čase meniť svoju polohu a tým vstupovať alebo sa strácať z dosahu ostatných uzlov. Zložité smerovacie algoritmy prinášajú zvýšené nároky na prenosový kanál a spotrebu energie.

Najjednoduchším spôsobom šírenia datagramu je záplava (flooding), kde odosielateľ pošle datagram všetkým susedným uzlom. Každý takýto uzol následne prepošle prijatý datagram ďalším susedom a keďže sa jedná o všesmerové vysielanie, tak takýto datagram sa dostane aj k uzlom, ktorý ho už prijali. Datagram nemusí dosiahnuť cieľový uzol v prípade ak je takýto uzol osamostatnený mimo dosahu akéhokoľvek uzla v segmente, alebo nastane problém skrytého terminálu a vzájomnej kolízii viacerých datagramov. Medzi výhody záplavy patrí jednoduchosť a nenáročnosť na hardvérové a softvérové prostriedky uzlov. V prípade nízkej frekvencie posielania datagramov môže byť takéto riešenie aj efektívnejšie ako zložité smerovacie protokoly. Nevýhodou sú extrémne rýchlo rastúce nároky na priepustnosť siete v prípade vysokého počtu uzlov a datagramov.

Smerovacie protokoly pre Ad-hoc siete rozdeľujeme na trojicu hlavných kategórií [1]:

- proaktívne protokoly, ktoré si trvalo udržiavajú aktívnu smerovaciu tabuľku. Do tejto kategórie patria tradičné Link-State a Distance-Vector protokoly
- reaktívne protokoly budujú smerovacie tabuľky len v prípade požiadavky na komunikáciu.
- hybridné, ktoré sú kombináciou predošlých kategórií.

Okrem rozdielu v implementácii sú rôzne kategórie smerovacích protokolov odlišné najmä v dĺžke oneskorenia komunikácie a množstve komunikačných dát nutných pre vybudovanie spojenia. Zatiaľ čo si proaktívne smerovacie protokoly udržujú aktuálnu smerovaciu tabuľku, tak reaktívne protokoly musia pred zahájením komunikácie najskôr vybudovať spojenie pomocou viacerých dopytov na jednotlivé uzly. Tieto dopyty oneskorujú nadviazanie spojenia a generujú ďalšie koordinačné prenosy. Naopak proaktívne protokoly musia udržiavať aktívne spojenia a smerovacie tabuľky, čo je energeticky náročnejšie. Medzi hlavných zástupcov Ad-hoc smerovacích protokolov patrí proaktívny Distance-Vector smerovací protokol RPL (IPv6 Routing Protocol for Low-Power and Lossy Networks) a reaktívny protokol LOAD-ng (Lightweight On-demand Ad-hoc Distance vector routing

protocol - next generation). Pre Ad-hoc siete s vysokým počtom komunikačných uzlov a preposielaných datagramov sú výhodnejšie proaktívne protokoly. Pri priamom porovnaní smerovacích protokolov RPL a LOAD-ng vykazuje RPL výhodnejšie komunikačné vlastnosti aj parametre a preto sme ho vybrali ako najvhodnejší protokol pre zabezpečenie smerovania vo vzniknutej sieti [1].

IV. Vybraný protokolový zásobník heterogénnych sietí

Pri budovaní rozsiahlych heterogénnych sietí pre zariadenia internetu vecí je možné využiť viacero komunikačných technológií a protokolov. Protokolový zásobník musí byť nezávislý od použitej komunikačnej technológie na fyzickej vrstve. Medzi najpoužívanejšie komunikačné technológie fyzickej vrstvy v rámci zariadení internetu vecí patrí IEEE 802.11 (Wi-Fi), IEEE 802.15.1 (Bluetooth) a IEEE 802.15.4. Každá technológia má pritom iný protokol sieťovej vrstvy, pričom prevládajú protokoly štandardizované medzinárodnou organizáciou IETF. Zatiaľ čo v robustnejších (Wi-Fi) sieťach sa používa plnohodnotný protokol IPv6, tak v energeticky efektívnych a pomalších sieťach je využívaný skrátený a rýchlejší protokol 6LoWPAN [2]. Takéto siete sú zväčša založené na Ad-hoc modeli s protokolom RPL, ktorý umožňuje efektívnu komunikáciu medzi viacerými decentralizovanými uzlami. Na vyšších vrstvách môže byť následne použitý protokol TCP alebo UDP a aplikačný protokol CoAP zabezpečujúci interoperabilitu medzi rôznorodými systémami.

A. Smerovací protokol RPL (IPv6 Routing Protocol for LLNs)

RPL je Distance-Vector smerovací protokol fungujúci na sieťovej vrstve protokolového zásobníka komunikujúci cez protokol IPv6 v LLN (6LoWPAN). Pre zabezpečenie smerovania vytvára protokol RPL smerovo orientovaný acyklický graf (Destination Oriented Directed Acyclic Graph DAG) [3]. Graf je vytváraný pomocou funkcie výpočtu metriky (Objective Function OF), ktorá je v základe založená len na počte skokov medzi zdrojovým a cieľovým uzlom. DAG graf minimalizuje vzdialenosť medzi hraničným smerovacím uzlom LBR (LLN Boarder Router) [4] a akýmkoľvek iným uzlom v sieti tak, že popisuje najkratšiu vzdialenosť medzi takýmito uzlami. Hraničný DAG uzol pripojený k IPv6 chrbticovej sieti má v grafe pridelenú metriku s hodnotou 1 pričom okolitým uzlom posiela informácie prostredníctvom DIO informačného rámca (DAG Information Option). Susedné uzly po prijatí DIO rámca následne vypočítajú svoju metriku na základe informácií v DIO a vzdialenosti od susedného uzla od ktorého prijali DIO rámec. Každý uzol si pritom na základe najnižšej metriky z DIO rámcov zvolí suseda, cez ktorého bude smerovať svoju komunikáciu k hraničnému uzlu [5]. Výpočet metriky na základe údajov od susedných uzlov a hodnotou hrán medzi nimi je znázornený v rovniciach (1-4).

$$Metri\ '_i = Metric_j + w_{i,j} \quad (1)$$

$$Metric"_i = Metric_k + w_{i,k} \quad (2)$$

$$Metric'_i < Metric"_i \quad (3)$$

$$Metric_i = \min\{Metrica'_i, Metric"_i\} \quad (4)$$

Pre proaktívne získanie DAG informácií si uzly môžu preposielať aj DIS rámce (DODAG Information Solicitation). Na nasledujúcom obrázku je znázornený proces propagácie DIO rámcov pre sformovanie DAG grafu. Zatiaľ čo prerušenými čiarami sú znázornené komunikačné cesty, tak plná čiara indikuje hrany acyklického DAG grafu a teda aj sformované spoje medzi susednými uzlami.

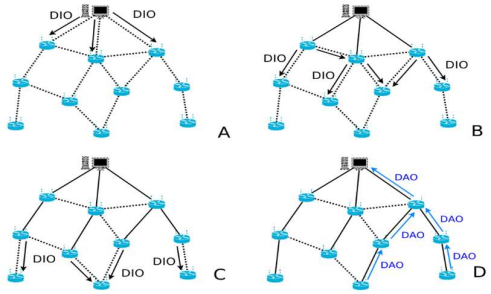

Fig. 1. Šírenie DIO rámcov pre výpočet metriky [6].

DIO rámce sú periodicky preposielané z každého uzla po uplynutí časového intervalu stanoveným minimálnou hodnotou *Imin*. Tento interval sa exponenciálne zvyšuje, čím minimalizuje dátovú výmenu a zahltenie siete po rýchlom sformovaní sieťovej topológie, ktorá trvá len niekoľko kôl výmeny DIO rámcov. V prípade straty komunikácie medzi uzlom a jeho susednou komunikačnou bránou sa aktivuje mechanizmus lokálnej opravy, ktorá zruší platnosť lokálnej subdomény DAG grafu a spustí prepočet novej komunikačnej brány a DAG grafu. Taktiež dôjde k zresetovaniu hodnoty časového intervalu posielania DIO rámcov na hodnotu *Imin*, čím sa urýchli formovanie grafu. Hraničný DAG uzol taktiež preposiela DIO správy, ktoré umožňujú vykonať globálnu opravu v prípade výraznej zmeny topológie.

Uzly po pripojení do DAG grafu alebo po zmene komunikačnej brány prepošlú svoju adresu a všetky dostupné adresy uzlov zo svojej DAG subdomény v DAO rámci (Destination Advertisement Option) [7], ktorý je prešírený až k hraničnému DAG uzlu. Tento mechanizmus slúži na budovanie smerovacej tabuľky hraničného uzla pre smerovanie ku koncovým uzlom.

B. Návrh rozšírenej metriky pre smerovací algoritmus

Výpočet metriky založený na počte skokov (Hop Count) je pre nami zadefinované pokročilé smerovanie na základe aplikačných požiadaviek nedostatočné a preto navrhujeme rozšírenie o ďalšie elementárne metriky, ktoré zodpovedajú rôznorodým komunikačným parametrom v rámci IoT siete. Hodnota opisovaných metrík stúpa so zhoršujúcou sa komunikačnou linkou a preto je pre zabezpečenie komunikácie vybraná linka s najnižšou metrikou. Jednotlivé elementárne metriky môžeme rozdeliť na metriku linky a metriku uzla podľa toho či zodpovedá stavu uzla alebo linky medzi dvoma uzlami. Výpočet navrhovaných elementárnych metrík je znázornený v rovniciach (5-13).

$$\textbf{Hop Count} = HC^{i,j} = w_{i,j} = w(i \oplus \mathrm{j}) \geq 1 \quad (5)$$

$$\textbf{Link Load} = LL^{i,j} = \sum_i^{j-1} \frac{Cap^{i,i+1}}{Cap^{i,i+1} - Load^{i,i+1}} \geq 1 \quad (6)$$

$$\textbf{Link Quality} = LQL^{i,j} = \sum_i^{j-1} \left(\sum_{k=1}^{7} p_k^{i,i+1} * k \right) \geq 1 \quad (7)$$

$$\textbf{Trip Time} = RTT^{i,j} = \sum_i^{j-1} \tau(i, i+1) = t_j - t_i \geq 1 \quad (8)$$

$$\textbf{Secure Level} = STL^{i,j} = \sum_i^j s_i \geq 1; \quad 1 \leq s_i \leq def_{max} \quad (9)$$

$$\textbf{Expected Tx. Count} = ETX^{i,j} = \frac{s+f}{s} \geq 1 \quad (10)$$

$$\textbf{Fwd. Cnt} = EFX^{i,j} = \frac{1}{P_{succ(i,j)}} = \prod_i^j \frac{sf_i + ff_i}{sf_i} \geq 1 \quad (11)$$

$$\textbf{Sleep} = SS^i = \frac{1}{Duty^i{}_{cycle}} \geq 1; \quad 0 \leq Duty^i{}_{cycle} \leq 1 \quad (12)$$

$$\textbf{Remaining Energy} = RE^i = \frac{Volt^i{}_{max}}{Volt^i{}_{curr}} \geq 1 \quad (13)$$

Medzi doplňujúce metriky môžeme zaradiť aj dostupnosť zdroja napájania, použité spektrum, použitú komunikačnú technológiu, či čas poslednej komunikácie. Kombináciou všetkých elementárnych metrík do jednej komplexnej kompozitnej metriky získame presnejšie správanie sa smerovania zodpovedajúce požadovaným komunikačným parametrom. Vplyv elementárnych častí metriky na celkovú kompozitnú metriku $M^{i,j}$ môžeme vypočítať podľa vzorca (14).

$$\alpha, \beta, \gamma, \delta, \varepsilon, \zeta, \eta, \vartheta, \kappa \geq 0 \quad (14)$$

$$M^{i,j} = \alpha * LL^{i,j} + \beta * LQL^{i,j} + \gamma * RTT^{i,j} + \delta * STL^{i,j} + \varepsilon * \\ * ETX^{i,j} + \zeta * EFX^{i,j} + \eta * HC^{i,j} + \vartheta * \sum_i^j SS^i + \kappa * \sum_i^j RE^i$$

Kompozitná metrika tak môže zodpovedať základnému správaniu sa smerovania na základe metriky Hop Count, ale zároveň môže detailnejšie charakterizovať jednotlivé parametre komunikačných liniek. Dôležité je pritom zachovať podmienku, aby pre každý jeden DAG graf boli koeficienty kompozitnej metriky rovnaké pre všetky uzly a z tohto dôvodu zavádzame viacero RPL inštancií. Počet inštancií počas komunikácie je možné dynamicky zvyšovať alebo znižovať podľa aktuálne dostupných výpočtových a pamäťových prostriedkov. Každá aplikácia vyššej vrstvy si tak na základe preferencií komunikačných parametrov vyberie alebo vytvorí nový konkrétny smerovací profil zodpovedajúci jej požiadavkám. Keďže počet takýchto profilov je obmedzený z dôvodu zachovania nízkych výpočtových nárokov, tak podľa kategórie jednotlivých zariadení môže protokol pracovať v dvoch režimoch: ukladací a transparentný (Storing a Non-Storing). V transparentnom (Non-Storing) režime si uzly neukladajú žiadne smerovacie informácie okrem údajov o susednom uzle cez ktorý komunikujú s hraničným DAG smerovačom. Tento režim umožňuje efektívnu komunikáciu medzi koncovými uzlami a hraničným uzlom, avšak horizontálna komunikácia medzi jednotlivými koncovými uzlami musí byť vždy smerovaná cez hraničný uzol, čo zvyšuje zahltenie siete. V ukladacom (Storing) režime si všetky uzly ukladajú smerovacie informácie o ostatných uzloch zo svojej DAG subdomény, čím urýchľujú komunikáciu medzi koncovými uzlami v rámci jednej subdomény DAG grafu. Nevýhodou takéhoto riešenia je vysoká náročnosť na pamäťové a výpočtové prostriedky, ktoré lineárne narastajú s počtom uzlov v DAG subdoméne a počtom použitých profilov. Pre siete pozostávajúce z obrovského počtu uzlov s obmedzenými prostriedkami by nebolo možné použiť ukladací režim a z tohto dôvodu sa používa agregácia IPv6 adries a aj nové hybridné režimy MERPL [8], ktoré kombinujú výhody oboch riešení. Vhodnou kombináciou hybridného režimu MERPL a navrhovanej kompozitnej metriky je možné dosiahnuť presnejšie správanie smerovacieho algoritmu pri minimálnom náraste výpočtových nárokov. Komunikácia v rámci takto vzniknutej sieti je schopná detailnejšie rozlišovať medzi častokrát protichodnými sieťovými požiadavkami rôznych aplikácií a zabezpečiť optimálne smerovacie parametre bez výrazných zásahov do existujúcej sieťovej infraštruktúry.

V. Zhodnotenie

Súčasné smerovacie algoritmy sa sústreďujú len na jednu komunikačnú technológiu s jednoduchou metrikou. Použitím kapilárnych sietí sa tieto protokoly stávajú zastaranými. V rámci práce sme navrhli niekoľko nových metód na tvorbu optimálnej kompozitnej metriky pre smerovanie v kapilárnych sieťach. Aplikáciou kompozitnej metriky dokážu IoT zariadenia efektívnejšie využívať dostupné prostriedky a zohľadňovať jednotlivé komunikačné parametre tak, aby čo najviac zodpovedali rôznorodým a častokrát aj protichodným požiadavkám aplikácií. Implementácia takéhoto smerovacieho algoritmu v kapilárnych sieťach aktívne prispeje k zlepšeniu a akcelerácii komunikácie medzi IoT zariadeniami.

Poďakovanie

Autori ďakujú za finančnú podporu v rámci projektu Vega 1/0616/14.

Referencie

[1] Radoi, I.E., Shenoy, A., Arvind, D.K.: Evaluation of Routing Protocols for Internet-Enabled Wireless Sensor Networks. ICWMC 2012. 978-1-61208-203-5. Copyright 2012 IARIA.

[2] Mulligan, G.: The 6LoWPAN Architecture. 6LoWPAN Working Group, IETF. EmNets2007, 25-26.6.2007, Cork, Ireland. Copyright 2007 ACM.

[3] Yunis, J.P., Dujovne, D.: Energy efficient routing performance evaluation for LLNs using combined metrics. 978−1−4799−4269−5/14, Copyright 2014 IEEE.

[4] Vasseur, J.P., Agarwal, N., Hui, J., Shelby, Z., Bertrand, P., Chauvenet, C.: RPL: The IP routing protocol designed for low power and lossy networks. Internet Protocol for Smart Objects (IPSO) Alliance. 2011.

[5] Karkazis, P., Leligou, H.C., et al.: Design of primary and composite routing metrics for RPL-compliant Wireless Sensor Networks. 2012.

[6] Tripathi, J., Oliveira, J.C.: Proactive versus Reactive Revisited: IPv6 Routing for Low Power Lossy Networks. 978-1-4673-5239-0/13. IEEE.

[7] Tsvetkov, T.: RPL: IPv6 Routing Protocol for Low Power and Lossy Networks. Seminar SN SS2011, 10.2313/NET-2011-07-1_09, July 2011.

[8] Gan, W., Shi, Z., Zhang, Ch., Sun, L., Ionescu, D.: MERPL: A More Memory-efficient Storing Mode in RPL. ICON 2013. 978-1-4799-2084-6/13, Copyright 2013 IEEE.