

Warszawa, 11 listopada 2015

dr hab. inż. Krzysztof Rządca  
Instytut Informatyki  
Uniwersytet Warszawski  
krz@mimuw.edu.pl

**Recenzja rozprawy doktorskiej**  
**mgra Marcina Kardasa**  
**z tytułu "Szybkie i Energetycznie Efektywne**  
**Protokoły dla Radiowych Sieci Ad Hoc"**

### **Problematyka Rozprawy**

Przedstawiona rozprawa dotyczy algorytmów dla klasycznych problemów systemów rozproszonych: wyboru lidera, k-selekcji (czyli wyboru podzbioru węzłów) oraz estymacji wielkości sieci. Zagadnieniem spajającym rozprawę jest analiza złożoności energetycznej przedstawionych algorytmów.

Problem określania złożoności energetycznej algorytmów w ostatnich latach staje się coraz bardziej istotny. Podstawowym zastosowaniem są właśnie wspomniane w rozprawie sieci sensorowe z komunikacją radiową: ponieważ sensory zasilane są zazwyczaj bateriami, a komunikacja radiowa wymaga relatywnie dużo energii, używane algorytmy komunikacji powinny uwzględniać ten koszt, by przedłużyć czas działania całego systemu. Ograniczenie zużycia energii ma znaczenie także w innych dziedzinach informatyki: np. w obliczeniach wysoko-wydajnych (HPC, high performance computing) podstawową barierą w dalszym skalowaniu superkomputerów jest zużycie energii (bezpośrednio związane z ilością ciepła wydzielaną przez procesory).

Podsumowując, rozważane problemy są fundamentalne dla systemów rozproszonych, a kąć ich analizy — aktualny.

### **Uzyskane Rezultaty**

Rozprawa składa się z trzech części poświęconych kolejno problemowi wyboru lidera, k-selekcji (wyboru k stacji) oraz estymacji rozmiaru sieci. Uzyskane rezultaty to algorytmy dla tych problemów, które pozwalają na osiągnięcie kompromisu między czasem działania a zużyciem energii (kompromis ten sterowany jest zwykle parametrem, którego wartość wybierana jest przez użytkownika). W pracy zaproponowano również dolne ograniczenia zużycia energii dla problemu k-selekcji i czasu działania dla problemu estymacji rozmiaru sieci.

Pierwsza, druga i połowa trzeciej części pracy zakładają użycie slotowego modelu komunikacji: czas podzielony jest na sloty; stacje nadają lub nasłuchują w kolejnych slotach. Model ten wymaga zatem precyzyjnego zsynchronizowania zegarów fizycznych stacji. Ostatni rozdział używa mniej wymagającego modelu, w którym wskazania zegarów fizycznych mogą się różnić o zakładane maksymalne przesunięcie.

## Wybór lidera

Część pierwsza proponuje nowy algorytm wyboru lidera nazwany FEELE. Kluczowym elementem FEELE jest wprowadzenie tzw. slotów kontrolnych: stacje które przegrały wybory, wyłączają swoje radia, by oszczędzać energię; by dowiedzieć się, kto został wybrany liderem, czekają z włączeniem radia i nasłuchiowaniem na następny slot kontrolny. Pomysł slotów kontrolnych pozwala zatem na oszczędzanie energii kosztem zwiększenia czasu działania algorytmu — w FEELE kompromis ten można kontrolować za pomocą parametru  $\alpha$  określającego liczbę iteracji pierwszej fazy algorytmu.

Rozprawa zawiera dowód poprawności algorytmu oraz analitycznie wyznaczone górne ograniczenia na oczekiwany czas działania i zużycie energii.

Analiza teoretyczna uzupełniona jest symulacjami. W modelu mocnym, czyli zakładającym jednakowy koszt energetyczny nadawania i odbierania komunikatów, nawet dla stosunkowo dużej liczby stacji ( $2^{17}$ ), FEELE (w wersji z jedną iteracją pierwszej fazy,  $\alpha = 1$ ) zużywa nieznacznie mniej energii w stosunku do algorytmu referencyjnego (Nakano-Olariu). W modelu słabym (koszt odbierania można pominąć) FEELE z dwiema i trzema iteracjami ma podobne zużycie energii co algorytm Nakano-Olariu do ok.  $2^{18}$  stacji. Dla większej liczby stacji zużycie energii FEELE jest kilkukrotnie niższe (w obu modelach). Podsumowując, przedstawione symulacje pokazują, że kompromis oferowany przez FEELE jest istotny głównie w sieciach z dużą liczbą stacji.

## Selekcja

Część druga zawiera dwa główne rezultaty: dolne ograniczenie na zużycie energii przez jednorodny algorytm k-selekcji (rozdział 7), oraz algorytm k-selekcji uogólniający algorytm Maseya i zmniejszający zużycie energii (rozdział 8).

Przedstawione dolne ograniczenie na zużycie energii wynika z analizy prawdopodobieństw ciszy, transmisji i kolizji dla systemu  $n$  stacji nadających na wspólnym łączu.

Zaproponowany w rozdziale 8 algorytm k-selekcji opiera się na błyskotliwej reprezentacji przebiegu wykonania algorytmu k-selekcji za pomocą drzewa trie. W oryginalnym algorytmie Maseya stacje wchodzące ze sobą w konflikt w danym slotie rozwiązywały ten konflikt rekurencyjnie: każda ze stacji wybierała jeden z dwóch slotów, w którym następnie próbowała transmisji (i, być może, wchodziła w kolejny konflikt). Przedstawiony algorytm uogólnia algorytm Maseya poprzez zwiększenie wybór slotów z dwóch do  $m$ ; dla odpowiednio dużego  $m$  ( $m = k^\alpha$ ) pozwala to na ograniczenie zużycia energii w modelu słabym do  $O(1)$ . Przedstawiona analiza opiera się na zapisie historii wykonania algorytmu za pomocą drzewa trie: liczby losowe, z których korzystają stacje, można reprezentować jako słowa w alfabecie o  $m$  symbolach; między stacjami zachodzi seria

konfliktów, gdy stacje wybiorą słowa o tym samym prefiksie. Reprezentacja ta pozwala na wykorzystanie rezultatów dotyczących wysokości losowych drzew trie do ograniczenia czasu działania i zużycia energii algorytmu.

Przedstawione wyniki symulacji pokazują, że parametr  $\alpha$  algorytmu reguluje kompromis między czasem działania a zużyciem energii: dla  $\alpha$  między 0,075 a 2,5, czas działania jest (w dużym przybliżeniu) wykładniczy z parametrem  $\alpha$ ; natomiast zużycie energii jest proporcjonalne do  $2/\alpha$  — zmierzone w symulacjach zużycie energii mieści się w teoretycznie wyznaczonych ograniczeniach  $[2/\alpha, 2/\alpha + 1]$ .

## Estymacja rozmiaru sieci

Ostatnia część pracy zawiera dwa główne wyniki: dolne ograniczenie na czas działania algorytmu estymującego rozmiar sieci (rozdział 10); oraz algorytm estymacji rozmiaru RAR (rozdział 11).

W części tej autor dwukrotnie zmienia model komunikacji: w rozdziale 10 jest to kanał z wykrywaniem fali nośnej (zamiast używanego do tej pory kanału z detekcją kolizji), w rozdziale 11 kanał z wykrywaniem fali nośnej i, dodatkowo, asynchroniczny model komunikacji (zamiast używanego do tej pory modelu slotowego).

Zaproponowany w rozdziale 11 algorytm RAR w elegancki sposób sprowadza problem estymacji rozmiaru sieci do modelu łuków na okręgu. Stacje wybierają losowe przesunięcia początkowe, a następnie nadają swój sygnał i czekają przez dłuższy czas  $T$  nasłuchując innych sygnałów.  $K$ -krotne powtórzenie cyklu nadawania-nasłuchiwanie zapewnia odebranie w  $k$ -tym cyklu sygnałów wszystkich innych stacji (mających różne przesunięcia fazowe, wynikające z przesunięć zegara i losowego przesunięcia początkowego). RAR wyznacza ilość stacji na podstawie łącznego czasu ciszy w  $k$ -tym cyklu. Rozprawa zawiera dowód poprawności algorytmu (krótki i przejrzysty) oraz dowody obciążenia i koncentracji estymatora: te dwa ostatnie korzystają z zaawansowanych metod analizy zespolonej (których oceny poprawności nie podejmuję się wykonać).

Podobnie jak w poprzednich częściach algorytm RAR weryfikowany jest również symulacjami, porównującymi wyniki estymacji przez RAR z wynikami algorytmu Linear Counting. Przedstawione wyniki pokazują, że estymacje RAR są znacząco bardziej dokładne już dla sieci o wielkości rzędu 1.000 stacji (a różnice stają się jeszcze bardziej widoczne dla sieci mających między 2.000 a 10.000 stacji).

## Uwagi

Rozprawa pisana jest po polsku, co wymagało od autora dużo pracy, jako że podstawę stanowi pięć publikacji pisanych po angielsku. Widać, że autor włożył wysiłek nie tylko w poprawne przetłumaczenie terminologii, ale również w utrzymanie jasnego, poprawnego stylu. Praca napisana jest niezwykle starannie — w prawie stu stronach tekstu zauważyłem zaledwie kilka literówek.

W odróżnieniu od bardzo sprawnego użycia języka, nie przekonał mnie styl niektórych dowodów. Styl dowodzenia jest nierówny: czasem autor szczegółowo (wraz z pod-

stawieniami) tłumaczy użycie znanych przekształceń matematycznych, a innym razem ogranicza się do znaku nierówności. Brak niektórych przekształceń nie pozwala na łatwe zrozumienie całości.

Niektóre z dowodów wymagają intuicyjnego zrozumienia sposobu działania algorytmów, co największym problemem było dla mnie w przypadku FEELE (rozdział 5): główny algorytm ma 24 linie i wywołuje 3 procedury po kilkanaście linii każda. Podczas dowodzenia dobrze byłoby przypomnieć, z których konkretnie własności FEELE dane przekształcenie korzysta (np. komentując pierwsze dwa równania ze strony 37, albo ograniczenie na liczbę slotów kontrolnych w dowodzie Lematu 5.6).

Podobnie, analiza z rozdziału 7. byłaby czytelniejsza, gdyby autor bardziej formalnie zdefiniował czas działania algorytmu w rozdziale 7.3, rozwinął przejście  $\sum_{i=1}^{\infty} \mathcal{P}(T \geq i) = \mathbb{E}(T)$  w dowodzie lematu 7.2, czy wyjaśnił zastosowanie nierówności Chernoffa w dowodzie twierdzenia 7.1. W rozdziale 10. przydałoby się rozpisać zastosowanie nierówności Höldera w dowodzie Lematu 10.2, oraz szerzej skomentować definicję  $H_k$  w dowodzie Twierdzenia 10.1.

W modelu używanym w rozdziale 11 nie jest jasno określone, że  $\Delta t$ , różnica między wskazaniem zegarów stacji, jest jedynym dopuszczanym rodzajem niezynchronizowania (tzn. że zegary stacji mogą być wzajemnie poprzysuwane, ale działają z identyczną i niezmienną precyzją, czyli wszystkie w ten sam sposób zmierzają długość danego okresu czasu).

Podsumowując problemy z dowodami, chcę zaznaczyć, że o ile taki styl dowodzenia używany jest czasem w pracach czysto teoretycznych, to raczej nie jest akceptowany w pracach o charakterze bardziej praktycznym (systemowym). Ponieważ przedstawione rezultaty są inspirowane praktycznymi problemami, autor powinien mieć ambicję utrzymania stylu czytelnego dla obu środowisk. Rozprawa używa różnorodnych technik matematycznych: od analizy algorytmów randomizowanych, przez zaawansowane struktury danych, po analizę zespoloną. Tak szeroki zestaw może tłumaczyć, dlaczego trudno było autorowi wyczuć, w których miejscach czytelnik może mieć kłopoty.

Pierwsza, druga i połowa trzeciej części pracy zakładają użycie slotowego modelu komunikacji, który wymaga bardzo dokładnego zsynchronizowania fizycznych zegarów (model alternatywny, wymagający jedynie ograniczonego wzajemnego przesunięcia zegarów, używany jest w ostatnim rozdziale). Model ten jest używany w wielu pracach teoretycznych, co oczywiście uzasadnia używanie go w tej rozprawie. Natomiast dokładne zsynchronizowanie zegarów w praktycznych systemach jest bardzo trudne, co ogranicza zastosowanie przedstawionych rezultatów. Autor proponuje wyposażenie stacji w odbiorniki GPS, co, po pierwsze, znacząco zwiększa ich koszt, po drugie, zużycie energii (o czym autor wspomina na s. 77), a po trzecie, wyklucza środowiska, w których sygnał GPS jest zagłuszany. Alternatywą jest zsynchronizowanie zegarów do sygnału wysyłanego przez wybraną stację — ale to wymaga uprzedniego wybrania tej stacji, czyli wykonania algorytmu wyboru lidera (który z kolei wymaga zsynchronizowania zegarów). Dlatego cenne jest stopniowe osłabianie założeń przyjętego modelu komunikacji w ostatniej części pracy: autor najpierw rezygnuje z założenia o możliwości detekcji kolizji, a później również z synchronizacji zegarów stacji.

W przeglądzie literatury do trzeciej części pracy zabrakło mi jasnego opisu wkładu

twórczego (w szczególności algorytmu RAR) w odniesieniu do cytowanych rezultatów. Zabrakło również porównania z wynikami pracy Cattaniego („Lightweight neighborhood cardinality estimation in dynamic wireless networks”, M. Cattani i inni, Proc. IPSN 2014).

Zdecydowanie teoretyczny charakter rozprawy uzupełniony jest badaniami symulacyjnymi proponowanych algorytmów. Badania symulacyjne stanowią świetne uzupełnienie rezultatów teoretycznych, pozwalając sprawdzić zachowanie algorytmów w średnim przypadku. Algorytmy uruchamiane były wielokrotnie (np. 10.000 razy w rozdziale 5, czy 100.000 razy w rozdziale 8), co jest bardzo dobrą praktyką, jako że algorytmy używają randomizacji. Niestety, oprócz rozdziału 11, wykresy pokazują jedynie wynik średni, a brakuje informacji o zmienności wyników (np. odchyłeń standardowych).

Wyniki symulacyjne algorytmu RAR (rozdział 11) porównywane są z algorytmem Linear Counting, zaproponowanym w 1990. Pozwoliło to na ciekawą ilościową analizę zysku ze stosowania ciągłego procesu w RAR (w przeciwieństwie do dyskretnego Linear Counting). Przydałoby się jednak również porównanie RAR z algorytmami bardziej współczesnymi — np. wspomnianą już przeze mnie pracą Cattaniego.

## Podsumowanie

Recenzowana rozprawa zasługuje na miano rozprawy doktorskiej w dziedzinie nauk matematycznych w zakresie informatyki.

Moje uwagi do rozprawy dotyczą głównie prezentacji wyników, natomiast wkład twórczy całości rozprawy jest bezdyskusyjny. Autor wykazał umiejętność precyzyjnego stawiania problemów w aktualnej tematyce, projektowania algorytmów oraz ich analizy z wykorzystaniem zarówno badań symulacyjnych, jak i bardzo szerokiego zestawu technik matematycznych: od probabilistyki, przez zaawansowane struktury danych, do analizy zespolonej.

Część z przedstawionych wyników została już opublikowana (w czterech pracach konferencyjnych i jednej w czasopiśmie).

Podsumowując, stwierdzam, że autor w pełni zasługuje na dopuszczenie go do dalszych etapów przewodu doktorskiego.

Krzysztof Rządko