

پروتکلی مبتنی بر اتوماتاهای یادگیر برای کنترل دسترسی به رسانه انتقال در شبکه های موردي سیار

محمد رضا میبدی

دانشکده مهندسی کامپیوتر و فناوری اطلاعات،
دانشگاه صنعتی امیرکبیر، تهران، ایران
mmeybodi@aut.ac.ir

ناصر فرج زاده

دانشکده مهندسی کامپیوتر،
دانشگاه آزاد اسلامی، واحد اهر، ایران
n-farajzadeh@iau-ahar.ac.ir

چکیده - در این مقاله پروتکلی مبتنی بر اتوماتاهای یادگیر برای کنترل دسترسی به رسانه انتقال در شبکه های موردی سیار پیشنهاد شده است. در این پروتکل هر یک از ایستگاههای سیار مجهز به یک اتوماتای یادگیر هستند. اتوماتای یادگیر هر ایستگاه تصمیم میگیرد که آیا ایستگاه اجازه ارسال اطلاعاتش را دارد یا نه. با استفاده از شبیه سازی کامپیوتربی کارایی پروتکل پیشنهادی (*MAHLAP*) از نظر تعداد ارسال های موفق و تعداد ارسال های ناموفق مورد ارزیابی قرار گرفته و سپس با پروتکل های *AHLAP IEEE 802.11 DCF* و *DCC-V* مقایسه شده است. نتایج بدست آمده حاکی از کارایی بالای پروتکل پیشنهادی است.

کلید واژه- اتوماتاهای یادگیر، شبکه های موردی سیار، کنترل دسترسی

همچنین، بعلت متحرك بودن ایستگاهها و فقدان کنترل مرکزی در شبکه های موردی سیار، مشکلات عدیدهای نظیر مشکل ایستگاههای پنهان و ایستگاههای آشکار در این شبکه ها رخ می دهند که باید در طراحی پروتکل های دسترسی به رسانه انتقال آنها را مد نظر قرار داد [۴ و ۵].

پروتکل ALOHA اولین پروتکلی می باشد که برای کنترل دسترسی به رسانه انتقال طراحی شده است. اساس کار این پروتکل بسیار ساده است، هر زمان که ایستگاهی نیاز به انتقال داده هایی دارد، آنها را ارسال می کند. پایین بودن کارایی این پروتکل به این خاطر است که دسترسی کورکورانه ایستگاهها به کانال های ارتباطی باعث بوجود آمدن تصادمهای فراوان بسته ها می شود. پروتکل اصلاح شده ALOHA، به نام پروتکل با بازه زمانی، زمان را به بازه های زمانی تقسیم می کند و ارسال بسته ها تنها در شروع هر بازه زمانی امکان پذیر می باشد. پروتکل ALOHA با بازه زمانی، کارایی پروتکل ALOHA را بهبود بخشیده است [۶].

یکی دیگر از پروتکل های موجود در این زمینه، استاندارد IEEE 802.11 DCF است [۷]. روش دسترسی در این

۱- مقدمه

شبکه های موردی سیار مجموعه ای از ابزارهای مستقل متحرکی است که در محیطی بی سیم با هم دیگر در ارتباط بوده و بصورت توزیع شده برای ایجاد شبکه ای بدون ساختاری ثابت همکاری می کنند [۱]. یکی از مسائل مهم در شبکه های موردی سیار کنترل دسترسی به رسانه انتقال است. در کنترل دسترسی به رسانه انتقال مساله این است که وقتی برای دسترسی به رسانه ای انتقال بین ایستگاه های ارسال کننده داده رقابت وجود دارد، چگونه می توان تعیین کرد که چه کسی باید از رسانه ای انتقال استفاده کند [۲]. طراحی و پیاده سازی پروتکل کنترل دسترسی به رسانه انتقال که در زیر لایه MAC صورت می گیرد، در شبکه های سلوی و یا شبکه های محلی بی سیم تفاوت های اساسی با شبکه های موردی سیار دارد [۳]. نرخ خطای بیت (BER) در شبکه های موردی سیار خیلی بیشتر از نرخ خطای بیت در شبکه های سلوی و شبکه های محلی بی سیم است. علاوه بر این، خطای در شبکه های موردی سیار بصورت متواالی رخ می دهد در حالیکه در شبکه های سلوی و شبکه های محلی بی سیم، خطای بطور تصادفی رخ می دهد.

AHLAP) که اصلاح شده پروتکل (Modified AHLAP) است، برای کنترل دسترسی به رسانه انتقال در شبکه‌های موردي سیار پیشنهاد میگردد. از طریق شبیه سازی کامپیوتری کارایی پروتکل پیشنهادی (MAHLAP) از نظر تعداد ارسال‌های موفق و ارسال‌های ناموفق مورد ارزیابی IEEE 802.11 DCF با پروتکل‌های IEEE 802.11 DCC_V AHLAP و AHLAP مقایسه شده است. ادامه مقاله به این صورت سازماندهی شده است. در بخش ۲ اتماتاهای یادگیر به اختصار شرح داده می‌شود. در بخش ۳ پروتکل پیشنهادی و در بخش ۴ نتایج شبیه سازی‌ها ارایه می‌گردد. بخش پایانی مقاله بخش نتیجه گیری می‌باشد.

۲- آتماتای یادگیر

اتوماتای یادگیر یک ماشین با حالات محدود است که می‌تواند تعداد محدودی عمل را انجام دهد. هر عمل انتخاب شده توسط یک محیط تصادفی ارزیابی شده و پاسخی به اتماتای یادگیر داده می‌شود. اتماتای یادگیر از این پاسخ استفاده نموده و عمل خود را برای مرحله بعد انتخاب می‌کند. در طی این فرآیند، اتماتای یادگیر فرا می‌گیرد که چگونه بهترین عمل را از بین اعمال مجاز خود انتخاب نماید. شکل (۱) ارتباط بین اتماتای یادگیر و محیط را نشان می‌دهد.

اتوماتای یادگیر به دو گروه اتماتاهای یادگیر با ساختار ثابت و اتماتاهای یادگیر با ساختار متغیر تقسیم می‌شوند. در این مقاله از اتماتاهای یادگیر با ساختار متغیر استفاده شده است که در ادامه این بخش توضیح داده می‌شود.

اتوماتاهای یادگیر با ساختار متغیر: اتماتای یادگیر با ساختار متغیر توسط ۴ تایی $\{a, b, p, T\}$ نشان داده می‌شود که در آن $a = \{a_1, a_2, K, a_r\}$ مجموعه عمل‌های اتمات، $b = \{b_1, b_2, K, b_m\}$ مجموعه ورودی‌های اتمات، $p = \{p_1, p_2, K, p_m\}$ بردار احتمال انتخاب اعمال و $T[a(n), b(n), p(n)] = p(n+1) = T[a(n), b(n), p(n)]$ الگوریتم یادگیری هستند. در این نوع از اتماتاهای یادگیر، اگر عمل a_i در مرحله n انجام شود و پاسخ مطلوب از محیط دریافت نماید، احتمال $p_i(n)$ افزایش یافته و سایر احتمال‌ها کاهش می‌یابند. در هر حال، تغییرات به گونه‌ای صورت می‌گیرد تا حاصل جمع (n) p_i ها همواره ثابت و مساوی یک

استاندارد CSMA/CA است که تا حدودی به روش CSMA/CD شباهت دارد. در روش CSMA/CA ایستگاه‌های کاری قبل از ارسال داده کانال رادیویی را کنترل کرده و در صورت آزاد بودن کانال اقدام به ارسال می‌کنند و در صورتی که کانال رادیویی اشغال باشد بر طبق الگوریتم خاصی مدتی صبر کرده و مجدد اقدام به کنترل کانال رادیویی می‌کنند [۲].

پروتکل دیگری که برای کنترل دسترسی به رسانه انتقال در شبکه‌های موردي سیار گزارش شده است، پروتکلی مبتنی بر اتماتاهای یادگیر به نام AHLAP است [۸]. در این پروتکل هر ایستگاه سیار، مجهز به یک اتماتای یادگیر است. اتماتای یادگیر هر ایستگاه تصمیم میگیرد که آیا ایستگاه اجزاء ارسال اطلاعاتش را دارد یا نه. در پروتکل AHLAP فرض بر این است که اگر ایستگاهی بسته یا بسته‌هایی برای ارسال در لحظه t دارد (حتی اگر این ارسال‌ها ارسال‌های مجدد باشند) با احتمال زیاد در لحظه $t+1$ نیز بسته یا بسته‌هایی برای ارسال خواهد داشت به همین دلیل، احتمال انتخاب آن ایستگاه برای مراحل بعد بر طبق الگوریتم یادگیری افزایش می‌یابد و اگر ایستگاهی اعلام کند که بسته‌ای برای ارسال ندارد، آنگاه احتمال انتخاب آن بر طبق الگوریتم یادگیری کاهش می‌یابد. این پروتکل مابین یک ارسال جدید و یک ارسال مجدد تمایزی قائل نشده و در هر صورت احتمال انتخاب ایستگاه ارسال کننده را برای مراحل بعدی افزایش می‌دهد و این مساله که ممکن است ارسال بعضی از بسته‌ها ناموفق باشد در بروز رسانی بردار احتمال اتماتاهای یادگیر دخالت داده نمی‌شود.

بدلیل اینکه در شرایط واقعی نمی‌توان آگاهی کامل از وضعیت رسانه انتقال حاصل کرد، بنابراین در دسته‌ی دیگری از الگوریتم‌های کنترل دسترسی به رسانه انتقال، سعی در وفق دادن CW بر اساس استفاده از یکسری مقادیر آماری شده است [۹، ۱۰ و ۱۱]. یکی از این الگوریتم‌ها، الگوریتم DCC_V است [۱۱]. این الگوریتم فرآیند رخ داد تصادم‌ها را فرآیندی غیر ثابت در نظر گرفته و مقدار CW را بر اساس استفاده از میانگین و واریانس فرآیند رخ داد تصادم‌ها محاسبه می‌کند.

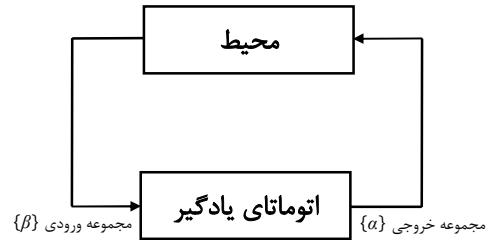
در این مقاله پروتکلی به نام MAHLAP

انتخاب ایستگاه ارسال کننده را برای مراحل بعد افزایش می‌دهد و به عبارتی دیگر این مساله که ممکن است ارسال بعضی از بسته‌ها ناموفق باشند در بروز رسانی بردار احتمال اوتوماتاهای یادگیر در نظر گرفته نشده است. ارسال‌های انجام گرفته توسط ایستگاه انتخاب شده ممکن است بدلیل یکی از عوامل: وجود ازدحام در شبکه، گم و یا خراب شدن بسته‌ها، از کار افتادن یکی از ایستگاه‌های میانی (در صورتی که ارسال داده‌ها بصورت چندگامی باشد) و یا بروز تصادم با خاطر وجود ایستگاه‌های پنهان موقفيت آميز نباشند و نياز به ارسال مجدد داشته باشند.

در اين بخش پروتکلي به نام MAHLAP که اصلاح شده پروتکل AHLAP است، برای کنترل دسترسی به رسانه انتقال در شبکه‌های موردي سيار پيشنهاد ميگردد. در اين پروتکل مانند پروتکل AHLAP، هر ایستگاه سيار مجهز به يك اوتوماتاي یادگير شده است. هر يك از اين اوتوماتاهای تصميم مي‌گيرند که آيا ایستگاه مربوطه مجاز به ارسال اطلاعاتش است يا نه. اوتوماتاي یادگير هر يك از ایستگاه‌ها، بردار احتمالات خود را بر خلاف پروتکل AHLAP که آنرا فقط بر اساس ارسال بسته و بدون توجه به موفق و يا ناموفق بودن آن بروز می‌کرد، بر اساس دو عامل الگوي ترافيكی ایستگاه‌ها و ارسال‌های موفق و ناموفق بروز می‌کند. به اين ترتيب در پروتکل پيشنهادي، احتمال انتخاب ایستگاهی که برای ارسال برگزيرde شده است بشرطی افزایش می‌يابد که ارسالش موفق باشد و در صورتی که ارسال ناموفقی داشته باشد احتمال انتخابش کاهش می‌يابد. لازم به ذكر است که عدم توجه به ارسال‌های ناموفق در چنین شبکه‌هایی که انرژی محدودی دارند، باعث کاهش طول عمر شبکه خواهد گردید. شکل (۲) شبه کد پروتکل پيشنهادي را که توسط ایستگاه i اجرا می‌شود، نشان می‌دهد.

۴- نتایج شبیه سازی‌ها

برای مقایسه پروتکل‌های IEEE 802.11 DCF و MAHLAP، دو متريک تعداد ارسال‌های موفق و تعداد ارسال‌های ناموفق (با خاطر تصادم یا پر بودن بافرها) در نظر گرفته شده است. همچنین از NS2 [۱۳] برای شبیه سازی‌ها استفاده شده است. جهت



شکل ۱: ارتباط بین اوتوماتای یادگیر و محیط

باقي بماند. الگوريتم زير نمونه‌اي از الگوريتم‌های یادگير خطوي است.

الف- پاسخ مطلوب

$$p_i(n+1) = p_i(n) + a[1 - p_i(n)] \\ p_j(n+1) = (1-a)p_j(n) \quad \forall j \neq i$$

ب- پاسخ نامطلوب

$$p_i(n+1) = (1-b)p_i(n) \\ p_j(n+1) = \frac{b}{r-1} + (1-b)p_j(n) \quad \forall j \neq i$$

در روابط فوق، a پارامتر پاداش و b پارامتر جريمeh است. با توجه به مقادير a و b سه حالت را می‌توان در نظر گرفت. زمانیکه a و b با هم برابر باشند، الگوريتم را L_{RP} ، زمانیکه b از a خيلي كوچکter باشد، الگوريتم را L_{RE} و زمانیکه b مساوي صفر باشد، الگوريتم را L_{RI} می‌ناميم. برای اطلاعات بيشتر درباره اوتوماتاهای یادگير و کاربردهای آن می‌توان به [۱۲] مراجعه نمود.

۳- پروتکل پيشنهادي

در پروتکل AHLAP [۸]، اوتوماتای یادگير هر ایستگاه تصميم مي‌گيرد که آيا اين ایستگاه اجازه ارسال اطلاعاتش را دارد يا نه. در اين پروتکل فرض بر اين است که اگر ایستگاهی بسته یا بسته‌هایی برای ارسال در لحظه t دارد (حتی اگر اين ارسال‌ها ارسال‌های مجدد باشند) با احتمال زياد در لحظه $t+1$ نيز بسته یا بسته‌هایی برای ارسال خواهد داشت، به همين دليل احتمال انتخاب آن ایستگاه برای دفعات بعد بر طبق الگوريتم یادگيری افزایش مي‌يابد و بالعکس. پروتکل AHLAP بين يك ارسال جديد و يك ارسال مجدد تمایزی قائل نشهde و در هر دو صورت احتمال

مواجه با یکی از مشکلات عمدۀ در شبکه‌های بی‌سیم، یعنی وجود ایستگاه‌های پنهان و آشکار، نیز مورد بررسی قرار گرفته است. بهمین دلیل، مختصات نهایی ایستگاه‌ها به طریق تعیین شده است که نهایتاً روی یک خط مستقیم قرار گیرند. نتایج آزمایشات انجام شده در شکل‌های (۳) (۵) و جدول (۳) ارائه گردیده است. لازم به ذکر است که در نتایج نشان داده شده، بسته‌های از بین رفته در نتیجه وجود نویز و خطای بیت، در نظر گرفته نشده‌اند. الگوریتم‌های MAHLAP و AHLAP هر دو از اتوماتای پادگیر L_{RP} با پارامترهای پاداش و جریمه برابر با ۰.۱ استفاده می‌کنند.

در شکل‌های (۳-الف) و (۳-ب)، پروتکل‌های IEEE 802.11 DCF و MAHLAP، DCC_V، AHLAP از نظر تعداد ارسال‌های موفق و تعداد ارسال‌های ناموفق مقایسه شده‌اند. همانطوریکه در این شکل‌ها مشاهده می‌شود، در ابتدای کار هر دو پروتکل AHLAP و MAHLAP کارایی کمتری از خود نشان می‌دهند و تقریباً یکسان عمل می‌کنند. با گذشت زمان (از ثانیه ۲۰ تا بعد) و یادگیری مشخصات محیط توسط این پروتکل‌ها، کارایی هر دو بیکباره افزایش پیدا می‌کند. با توجه به سناریوی شبکه، بار واردۀ بر شبکه از ثانیه ۴۰ تا بعد به حداقل اندازه خود می‌رسد و بنابراین ازدحام نسبتاً بالایی در شبکه بوجود می‌آید. ملاحظه می‌شود که در این شرایط هر دو پروتکل AHLAP و MAHLAP عملکرد بهتری از خود به نمایش گذاشته‌اند. از ثانیه ۷۱ تا ۷۲ م رفته (ثانیه به ثانیه) بار واردۀ به شبکه کاهش پیدا می‌کند تا جاییکه در ثانیه ۷۳ تا ۷۴، بجز ایستگاه شماره ۴، ایستگاه دیگری تمایل به ارسال از خود نشان نمی‌دهد. از این‌رو، از ثانیه ۷۳ تا انتهای شبیه‌سازی، کارایی هر چهار پروتکل تقریباً یکسان می‌باشد.

در شکل‌های (۴-الف) و (۴-ب)، پروتکل‌های IEEE 802.11 DCF و MAHLAP، DCC_V، AHLAP از نظر تعداد ارسال‌های موفق و تعداد ارسال‌های ناموفق مقایسه شده‌اند. ملاحظه می‌شود که با یادگیری مشخصات محیط توسط پروتکل‌های AHLAP و MAHLAP تقریباً از ثانیه ۳۰ تا بعد، کارایی هر دو پروتکل بنحو چشمگیری از کارایی پروتکل‌های 802.11

```

P = Create_probabilities_vector();
Initialize_probabilities_vector(P);

while (TRUE)
{
    /* Select a transmitting station according to the action
    probability vector of learning automata */
    transmitter = Select_transmitting_station(P);

    if (transmitter == i)
    {
        if (Queue_size(i) > 0) // Is there a packet to send?!
        {
            Send_packets(i);
            feedback = Wait_for_ACK();

            if (feedback == NO_FEEDBACK)
                Decrease(Pi); // Penalize action i
            else
                Increase(Pi); // Reward action i
        }
        else
        {
            Remain_silent();
            Decrease(Pi); // Penalize action i
        }
    }
    else
    {
        feedback = Get_network_feedback();

        if (feedback == DATA_PACKET OR
            feedback == ACK_PACKET)
            Increase(Pi); // Reward action i
        else if (feedback == IDLE_SLOT)
            Decrease(Pi); // Penalize action i
        if(feedback == DATA_PACKET AND
           destination_station(feedback) == i)
            Send_ACK_PACKET(i);
    }
}

```

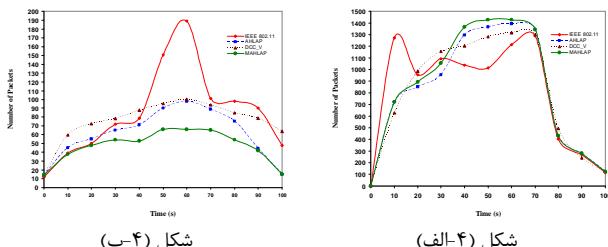
شکل ۲: شبۀ کد پروتکل **MAHLAP**

شبیه سازی رفتار هر یک از ایستگاه‌های سیار در محیطی بی‌سیم و بدون ساختار مشخص، سه شبکه ۱، ۲ و ۳ به ترتیب با مشخصات $N = 10$, $Q = 10$, $N = 5$, $Q = 10$ و $N = 20$, $Q = 20$ در نظر گرفته شده است که N تعداد ایستگاه‌های سیار و Q حداکثر طول هر یک از صفحه‌ای واسط می‌باشد. سناریوی ترتیب داده شده برای شبکه ۱ در جدول ۱ و سناریوی ترتیب داده شده برای شبکه ۲ و ۳ در جدول ۲ آمده است. تنها تفاوت شبکه‌های شماره ۲ و ۳ در طول صفحه‌ای واسط آنهاست و از نظر سناریو با یکدیگر تفاوتی ندارند. اطلاعاتی که برای هر سناریو در جداول آمده است عبارتند از نقطه‌ی اسقطرار اولیه‌ی هر یک از ایستگاه‌ها، نقطه‌ی هدف هر یک از ایستگاه‌ها، سرعت حرکت هر یک از ایستگاه‌ها و زمان شروع و اختتام برقراری ارتباط هر ایستگاه با ایستگاه دیگر. در این سناریوها سعی شده است که کارآیی پروتکل‌های ذکر شده برای هر دو ترافیک سبک و سنگین ارزیابی و مقایسه شوند. همچنین کارآیی پروتکل‌ها در

و ۳ در طول صفحه‌ای وسط است (در شبکه ۳ طول هر یک از بافرها برابر با ۲۰ و در شبکه ۲، برابر با ۱۰ است)، هر دو پروتکل مبتنی بر اتماتاهای یادگیر دارای عملکرد بهتری در مقایسه با پروتکلهای IEEE 802.11 و DCC_V می‌باشند.

۵- نتیجه‌گیری

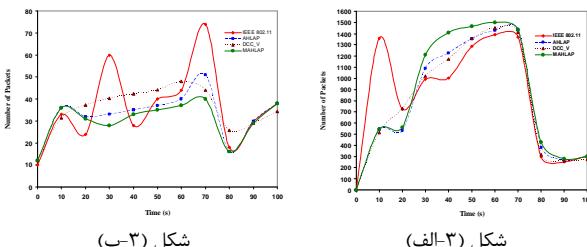
در این مقاله پروتکلی مبتنی بر اتماتاهای یادگیر برای کنترل دسترسی به رسانه انتقال در شبکه‌های موردنی سیار ارائه شد. با استفاده از شبیه سازی کامپیوترا کارایی پروتکل پیشنهادی (MAHLAP) مورد ارزیابی قرار گرفت و با پروتکلهای IEEE 802.11 DCF و AHLAP IEEE 802.11 DCC_V مقایسه گردید. نتایج بدست آمده کارایی پروتکل پیشنهادی را نشان داده است.



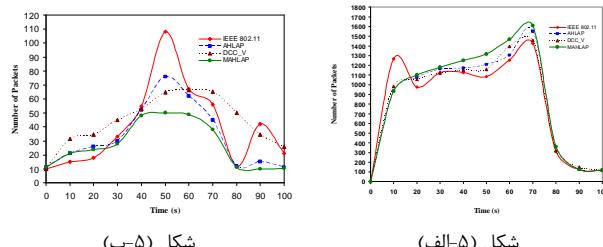
شکل ۴: مقایسه پروتکلهای IEEE 802.11، DCC_V، AHLAP و IEEE 802.11 DCF در شبکه ۲. (الف) تعداد بسته‌های ارسال شده موفق، (ب) تعداد بسته‌های ارسال شده ناموفق

DCC_V و DCF بهتر شده است. این اختلاف کارایی از ثانیه ۵۴ (زمانیکه همه ایستگاهها تمایل به ارسال دارند) تا انتهای ثانیه ۷۸ (زمانیکه تنها ایستگاه ۹ تمایل به ارسال دارد) به حداکثر خود می‌رسد. همچنین شکل (۴-ب) این واقعیت را نشان می‌دهد که با وجود سبک شدن ترافیک از AHLAP و MAHLAP در شکل ۷۸ به بعد، هر دو پروتکل IEEE 802.11 DCF و DCC_V بهتری از خود نشان داده و بسته‌های کمتری را از دست می‌دهند. عبارتی در مواجه با مشکلات ایستگاه‌های مخفی و آشکار بهتر عمل می‌کنند.

در شکل‌های (۵-الف) و (۵-ب) پروتکلهای IEEE 802.11 DCF، DCC_V، AHLAP و MAHLAP در شبکه ۳ از نظر تعداد ارسال‌های موفق و تعداد ارسال‌های ناموفق مقایسه شده‌اند. با توجه به اینکه تنها تفاوت شبکه ۲



شکل ۵: مقایسه پروتکلهای IEEE 802.11، DCC_V، AHLAP و IEEE 802.11 DCF در شبکه ۳. (الف) تعداد بسته‌های ارسال شده موفق، (ب) تعداد بسته‌های ارسال شده ناموفق



شکل ۶: مقایسه پروتکلهای IEEE 802.11، DCC_V، AHLAP و IEEE 802.11 DCF در شبکه ۳. (الف) تعداد بسته‌های ارسال شده موفق، (ب) تعداد بسته‌های ارسال شده ناموفق

جدول ۱: سناریوی ترتیب داده شده برای شبکه ۱

ایستگاه	مختصات اولیه (متر)	مختصات نهایی (متر)	زمان شروع حرکت (ثانیه)	سرعت حرکت (k/h)	ایستگاه مورد نظر جهت برقراری ارتباط	زمان شروع ارتباط (ثانیه)	زمان خاتمه ارتباط (ثانیه)
.	(۳۰۰ و ۶۰۰)	(۴۰۰ و ۱۰۰)	۷	۱۰	۱	۱	۷۰
۱	(۲۰۰ و ۱۰۰)	(۴۰۰ و ۳۰۰)	۱۵	۹	۲	۲	۷۱
۲	(۴۰۰ و ۱۰۰)	(۵۰۰ و ۴۰۰)	۲۰	۱۱	۳	۳	۷۲
۳	(۳۰۰ و ۲۰۰)	(۴۰۰ و ۷۰۰)	۲	۱۳	۴	۴	۷۳
۴	(۳۰۰ و ۵۰۰)	(۴۰۰ و ۹۰۰)	۲۵	۱۵	۰	۴۰	۱۰۰

جدول ۲: سناریویی ترتیب داده شده برای شبکه ۲ و ۳

ایستگاه	مختصات اولیه (متر)	مختصات نهالی (متر)	زمان شروع حرکت (ثانیه)	سرعت حرکت (k/h)	ایستگاه مورد نظر جهت برقراری ارتباط	زمان شروع ارتباط (ثانیه)	زمان خاتمه ارتباط (ثانیه)
•	(۹۰۰ و ۷۰۰)	(۱۰۰ و ۵۰۰)	۱	۲۰	۱	۱	۷۰
۱	(۶۰۰ و ۲۰۰)	(۲۰۰ و ۵۰۰)	۵	۱۹	۲	۶	۷۱
۲	(۷۰۰ و ۴۰۰)	(۳۰۰ و ۵۰۰)	۱۰	۱۸	۳	۱۲	۷۲
۳	(۳۰۰ و ۱۰۰)	(۴۰۰ و ۵۰۰)	۱۵	۱۷	۴	۱۸	۷۳
۴	(۹۰۰ و ۴۰۰)	(۵۰۰ و ۵۰۰)	۲۰	۱۶	۵	۲۴	۷۴
۵	(۱۰۰ و ۸۰۰)	(۴۰۰ و ۵۰۰)	۲۵	۱۶	۶	۳۰	۷۵
۶	(۶۰۰ و ۱۰۰)	(۷۰۰ و ۵۰۰)	۳۰	۱۷	۷	۳۶	۷۶
۷	(۶۰۰ و ۸۰۰)	(۸۰۰ و ۵۰۰)	۳۵	۱۸	۸	۴۲	۷۷
۸	(۲۰۰ و ۶۰۰)	(۹۰۰ و ۵۰۰)	۴۰	۱۹	۹	۴۸	۷۸
۹	(۱۰۰ و ۳۰۰)	(۱۰۰۰ و ۵۰۰)	۴۵	۲۰	•	۵۴	۱۰۰

جدول ۳: مقایسه توان عملیاتی پروتکل‌های MAHLAP و DCC_V و AHLAP IEEE 802.11 DCF

شبکه	پروتکل	توان عملیاتی بسته‌های ارسال شده موفق (Packet/Sec)	توان عملیاتی بسته‌های ارسال شده ناموفق (Packet/Sec)
۱	802.11 DCF	89.81	3.39
	AHLAP	85.61	3.60
	DCC_V	85.10	3.85
	MAHLAP	91.31	3.35
۲	802.11 DCF	86.62	9.29
	AHLAP	87.63	6.61
	DCC_V	87.28	8.28
	MAHLAP	90.68	5.15
۳	802.11 DCF	88.11	4.38
	AHLAP	90.10	3.56
	DCC_V	89.10	4.11
	MAHLAP	94.63	3.12

مراجع

- wireless LANs: A Learning Automata Based Approach”, Ad hoc Networks, pp. 419-431, 2004.
- [9] L. Bononi, M. Conti and L. Donatiello, “Design and Performance of a Distributed Contention Control (DCC) Mechanism for IEEE 802.11 Wireless Local Area Networks”, Proc. of the 1st ACM International Work-shop on Wireless Mobile Multimedia, pp. 59-67, 1998.
- [10] J. Hu and K. Erriksson, “A New Distributed Contention Control Protocol for the IEEE 802.11 MAC Layer”, Special Session on TCP and MAC Protocols in Wireless and Wired Networks, Proc. of the 1st Int. Conf. on E-Business and Telecommunication Networks (ICETE 2004), pp. 393-401, 2004.
- [11] J. Hu and C.D. Raymond, “A Statistics Based Design of MAC Protocols with Distributed Collision Resolution for Ad Hoc Networks”, Int. Conf. on Wireless Networks, Communications and Mobile Computing, pp. 917-922, 2005.
- [12] K.S. Narendra, M.A.L. Thathachar, Learning Automata: An Introduction, Prentice Hall, Englewood Cliffs, NJ, 1989.
- [13] The Network Simulator – NS 2, <http://www.isi.edu/nsnam/ns/>
- [1] S. Basagni, M. Conti, S. Giordano and I. Stojmenovic, Ad Hoc Networking, IEEE Press Wiley, New York, 2003.
- [2] S. Tanenbaum, Computer Networks, Forth Edition, Prentice-Hall International Inc., 2003.
- [3] P. Nicopolitidis, M. S. Obaidat, G. I. Papadimitriou and A. S. Pomportsis, Wireless Networks, Wiley, New York, 2003.
- [4] I. Chlamtac, M. Conti and J. J. Liu, “Mobile Ad-hoc Networking: Imperatives and Challenges”, Ad-Hoc Networks, Vol. 1, No. 1, pp. 13–64, 2003.
- [5] T. Issariyakul, E. Hossain and D. In Kim, “Medium Access Control Protocols for Wireless Mobile Ad hoc Networks: Issues and Approaches”, Wireless Communication Mobile Computing, pp. 935-958. 2003.
- [6] R. Nelson and L. Kleinrock, “The Spatial Capacity of a Slotted ALOHA Multihop Packet Radio Network with Capture”, IEEE Trans. Communication, Vol. 32, No. 6, pp. 684–694, 1984.
- [7] IEEE Standard for Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, 1997.
- [8] P. Nicopolitidis, G.I. Papadimitriou and A. S. Pomportsis, “Distributed Protocols for Ad hoc