

بسمه تعالی

کنترل جریان و ازدحام شبکه‌های حسگر بی‌سیم

۴	چکیده
۴	مقدمه
۵	پس زمینه
۵	۱- مدیریت ازدحام
۵	۱-۱ تشخیص ازدحام
۶	۱-۲ کنترل ازدحام
۸	۲- کنترل جریان
۸	۳- نیاز به کنترل جریان و ازدحام در WSN ها
۱۰	۴- چالشها
۱۰	۴-۱ محدودیت منابع
۱۰	۴-۲ الگوهای ترافیکی
۱۱	۴-۳ معماری شبکه
۱۱	۴-۴ معیارهای کارایی متناوب
۱۱	۴-۵ افزونگی داده
۱۱	۵- طبقه بندی روشهای کنترل جریان و ازدحام
۱۲	۵-۱ مکانیسم شناسایی ازدحام
۱۲	۵-۲ اهداف کنترل ازدحام
۱۲	۵-۳ مکانیسمهای کنترل سرعت

۱۳	۴-۵ عدالت و/یا کیفیت خدمات
۱۳	۵-۵ هدف مدل کاربردی
۱۳	۶-۵ دیگر معیارها
۱۳	۶-۶ کنترل جریان و ازدحام چند به یک در WSN ها
۱۴	۶-۱ رویکردهای شبکه مرکزی
۲۱	۶-۲ رویکردهای کاربرد خاص
۲۵	۶-۳ رویکرد ترکیبی
۲۶	۶-۴ نیاز قابلیت اعتماد در WSN ها
۲۹	۶-۵ فعالیتهای وابستهی دیگر

چکیده

در این مقاله روش‌های کنترل ازدحام و دسته‌بندی آنها بر اساس پارامترهای مختلف نظیر مکانیسم-های مورد استفاده برای تشخیص و کنترل ازدحام، مدل تحویل داده و پشتیبانی از قابلیت اعتماد بررسی می‌شود. همچنین به سه نوع از ارتباط کاربردی حسگرها توجه می‌شود:

- یک به یک
- یک به چند
- چند به یک

مطالعات گسترده‌ای بر روی ارتباطات یک به یک و یک به چند چه در شبکه‌های سیمی و چه در ویژه‌ی بی‌سیم^۱ صورت گرفته است. اما ارتباط چند به یک شامل فرصت‌های مختلفی است که عمده توجه محققان را به خود جلب کرده است. در این مقاله نیز توجه اصلی بر روی روش‌های کنترل جریان و ازدحام الگوهای ترافیکی چند به یک است.

مقدمه

گره‌های حسگر بی‌سیم عموماً به دلیل محدودیت منابع ذخیره، پردازش، انرژی و ارتباطی ایجاد می‌شوند. هر شبکه‌ی حسگر بی‌سیم ترکیبی از چندین گره‌ی حسگر است که اطلاعات را جمع‌آوری کرده و آنها را به ناظر تحویل می‌دهند.

ناظر می‌تواند گره‌ی مرکزی (ایستگاه پایه) یا گره‌ی سیاری باشد که اطراف شبکه حرکت می‌کند و داده‌ها را جمع‌آوری می‌کند. در هر دو مورد گفته شده، فرض می‌شود ناظر توانایی ذخیره، پردازش و تحلیل داده‌ی جمع‌آوری شده از منابع را دارد.

شبکه‌های حسگر بی‌سیم به دلایل زیر متفاوت از شبکه‌های سنتی هستند:

- ۱- داده محوری: در WSN، ناظرها مایل به جمع‌آوری درست و به موقع داده هستند. در مقابل شبکه‌های سنتی روی ارتباط بین نقاط مختلف شبه تمرکز دارند.
- ۲- الگوهای ترافیکی منحصر به فرد: در WSNها اغلب داده‌ها از زیر مجموعه‌ای از حسگرها به سمت ناظر به صورت قیفی حرکت می‌کنند. از آنجایی که این ارتباطات شامل چندین فرستنده و تنها یک گیرنده است، آن را الگوی ترافیکی چند به یک می‌نامند.

^۱ - wireless ad hoc network

در این مقاله، پروتکل‌های مدیریت ازدحام شبکه‌های حسگر بی‌سیم طبقه‌بندی و بررسی می‌شوند. ازدحام مشکل شبکه‌های سوئیچ بسته است که در آنها سرعت منابع بالا رفته و در نتیجه‌ی آن ظرفیت شبکه در یک یا چند گره‌ی میانی (مسیربازها) پر و منجر به از دست رفتن بسته می‌شود. کنترل ازدحام اصالتاً همان مسأله‌ی تخصیص منابع است که نوع ابتدایی آن سرعت منابع را جهت جلوگیری با تعدیل ازدحام تنظیم می‌کند. کنترل جریان هم در مواردی است که ارسال داده در فرستنده‌ها سریع‌تر از مصرف آنها در گیرنده‌ها است.

یکی از اهداف مهم کنترل ازدحام و جریان در WSN، ایجاد سطح مطلوبی از قابلیت اعتماد در گره-ی sink است که ضمانت تحویل موفق داده را می‌کند. قابلیت اعتماد بهترین مقیاس در کاربردهای خاص (مانند صحت داده یا اطمینان در شناسایی رخداد) است.

پس زمینه

در این بخش مسائل مدیریت ازدحام و کنترل جریان در شبکه‌ها بررسی می‌شود. سپس دلیل منحصر به فرد بودن نیازمندی‌های هر دو در WSN‌ها بیان می‌شود.

۱- مدیریت ازدحام

ازدحام به علت پر شدن ظرفیت بافر گره‌های میانی به وجود می‌آید. کنترل ازدحام یا قبل از شروع آن با رویت شدن علائم شناسایی و بهبود می‌یابد (اجتناب از ازدحام) و یا اینکه بعد از شروع آن شناسایی می‌شود (تعدیل ازدحام). الگوریتم‌های مدیریت ازدحام در چگونگی تشخیص و کنترل متفاوت هستند. تشخیص ممکن است در منابع یا گره‌های میانی انجام شود. ولی کنترل با کاهش نرخ ارسال از منابع صورت می‌گیرد. این رویکرد به صورت دقیق در زیر بیان شده است.

۱-۱ تشخیص ازدحام

تشخیص ازدحام مرحله‌ی ابتدایی و مهم در هر الگوریتم کنترل ترافیک است. ازدحام می‌تواند هم در گره‌ی میانی و هم در گره‌ی sink (ابتدای و انتهایی) تشخیص داده شود. در گره‌ی میانی، ازدحام می‌تواند بر اساس فاکتورهای نظیر اشغال صف جاری، زمان سرویس بسته یا ترکیبی از شرایط کنونی و گذشته‌ی کانال از لحاظ بار اعمال شده روی آن استنباط شود. برای نمونه، تشخیص ترافیک بر اساس اشغال صف در مکانیسم‌های DECbit و تشخیص به موقع تصادفی (RED)^۲ استفاده می‌شود. DECbit اخطار صریح از ترافیک را می‌دهد در حالی که RED

^۲ -Random Early Detection

اخطار مجازی آن را می‌دهد، که یا وضعیت ازدحام با سواری کردن^۳ آن در بسته ارسال می‌شود و یا بسته رها می‌شود. شناسایی ازدحام در نقاط ابتدایی و انتهایی از طریق فاکتورهایی نظیر اتمام زمانی، ACKهای تکراری، تاخیر بسته‌ی ورودی و ... مطرح می‌شود. پروتکل کنترل انتقال (TCP) ازدحام را بر اساس ACKهای تکراری و یا اتمام زمان، تشخیص می‌دهد. بنابراین، به محض دریافت سه پیام تصدیق تکراری مازول بازبایی TCP به سرعت وقوع ترافیک را مطرح می‌کند.

۲-۱ کنترل ازدحام

پس از شناسایی ازدحام لازم است مکانیسم کنترل آن آغاز شود. کنترل ترافیک می‌تواند یا به صورت جلوگیری از شدید شدن آن یا تعدیل ازدحامی که هم اکنون در شبکه رخ داده است، صورت گیرد.

این دو مکانیسم به طور خلاصه در زیر بیان شده است:

۱-۲-۱ اجتناب از ازدحام^۴

استراتژی اجتناب از ازدحام شامل تشخیص به موقع علائم و شروع اقدامات پیشگیرانه برای جلوگیری از شدید شدن آن است. برای نمونه، TCP Vegas سعی در شناسایی ترافیک در مراحل ابتدایی، به وسیله‌ی مقایسه‌ی نرخ توان عملیاتی اندازه‌گیری شده با نرخ توان عملیاتی مورد انتظار در فرستنده، صورت می‌گیرد. دیگر مکانیسم‌های اجتناب از ازدحام شامل RED و DECbit هستند که علائم ازدحام را به موقع شناسایی کرده و به نقاط انتهایی اطلاع می‌دهند. این کار با نظارت صف اشغالی در گره‌های میانی صورت می‌گیرد.

۲-۲-۱ تعدیل ازدحام^۵

به محض شدت ازدحام با کاهش بار اضافی از طرف منابع، ازدحام تعدیل داده می‌شود. در موارد شبکه‌های سیمی و ویژه‌ی بی‌سیم، جریان داده نقطه به نقطه است. پس، در چنین شبکه‌هایی، فرض بر این است که ازدحام در میان رقابت منابع اتفاق می‌افتد، و بنابراین اطمینان از عدالت بین منابع موضوعی است. این مسئله به این دلیل درست است که کنترل ازدحام توسط منابع مختلف انجام می‌شود.

^۳-piggybacking

^۴- Congestion avoidance

^۵- Congestion mitigation

در wsn ها، رقابت بر سر منابع^۶ اغلب در بین چندین منبع^۷ که پاسخ به پرسش مشابهی را می‌دهند، است.

^۶-resources
^۷-source

۲- کنترل جریان

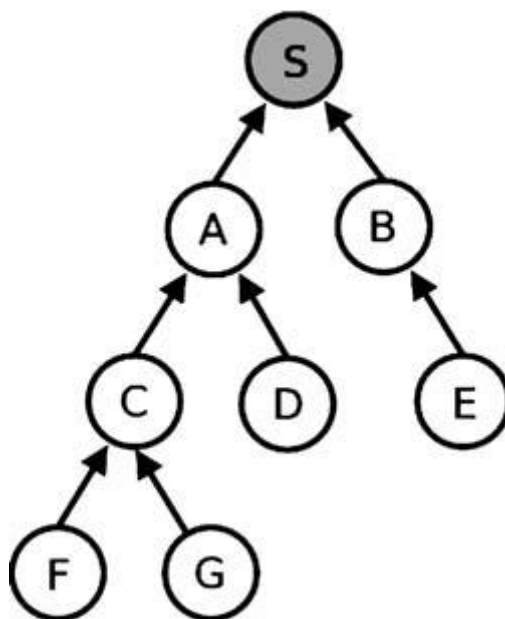
کنترل جریان مکانیسمی برای هماهنگی بین فرستنده‌ها و گیرنده‌های با سرعت نابرابر است. به بیان دیگر کنترل جریان اجازه نمی‌دهد نرخ ارسال فرستنده از نرخ مصرف گیرنده تجاوز کند. دو مکانیسم برای کنترل جریان وجود دارد:

۱- کنترل جریان حلقه-بسته: در این تکنیک گیرنده به طور مستقیم بازخوردی به فرستنده ارسال می‌کند تا بر اساس آن نرخ ارسال تنظیم شود.

۲- کنترل جریان حلقه-باز: در این روش مستقیماً بازخوردی ارسال نمی‌شود، بلکه بازخوردها به صورت گام به گام^۸ به فرستنده انتقال داده می‌شوند.

۳- نیاز به کنترل جریان و ازدحام در wsn‌ها

نحوه‌ی گزارش‌دهی حسگرها به گره‌ی پایه در wsn‌ها مبتنی بر توپولوژی مسیریابی درخت است که گره‌ی پایه (sink) در آن در حکم ریشه می‌باشد.



توپولوژی مسیریابی بر اساس درخت

^۸-hop by hop

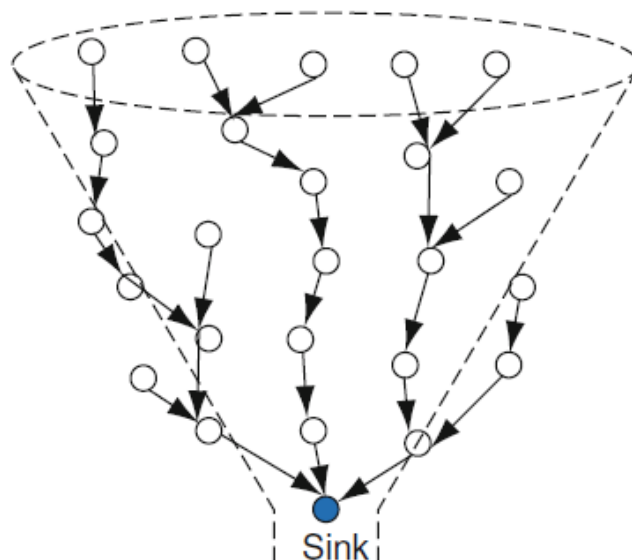
در شکل فوق گرهی s به عنوان ریشه‌ی درخت (sink) است و دیگر گره‌ها به عنوان ایجاد کننده یا حمل کننده‌ی داده هستند. گره‌های نزدیک به منابع را گره‌های بالا ریشه^۹ و گره‌های نزدیک به گره-ی ریشه را پایین ریشه^{۱۰} می‌نامند. بنابراین G و F گره‌های بالا ریشه و A گرهی پایین ریشه برای C هستند. همچنین همسایه‌ی on-hop را که در مسیر انتقال داده به سمت ریشه است، گرهی پدر می‌نامند. بنابراین گرهی A پدر گره‌های C و D است. زیر درخت گرهی A از گره‌های بالا رشته‌ی C، D، F و G تشکیل می‌شود.

برخورد با ازدحام و مکانیسم‌های جلوگیری از آن توسط Tilak و همکارانش شناخته شد. آنها به طور خاص تاثیر افزایش نرخ گزارش داده و تراکم حسگر را روی کیفیت اطلاعات دیده شده توسط ناظر در کاربرد کیفی شکل داده، مطالعه کردند. اگرچه تراکم بالای حسگر فرصت خوبی برای دریافت دقیق‌تر فراهم می‌کند، اما چنانچه ازدحام کنترل نشود در کارایی شبکه مضر خواهد شد. زیرا بار بیشتری روی کانال بی‌سیم تقسیم می‌شود و شبکه سریع‌تر اشباع می‌شود. علاوه بر این نیاز است به اطمینان از اینکه نرخ گزارش‌دهی حسگرها از ظرفیت شبکه تجاوز نکند. بنابراین مهم است که حداقل نیازهای صحت کاربرد خاص در شبکه برآورده شود تا انرژی اضافی برای دستیابی آن صرف نشود.

برای پشتیبانی از نیازهای کاربردی معادله‌ی زیر باید برقرار باشد:

$$C_{application} \leq \sum b(S_i) \leq \alpha C_{total}$$

$C_{application}$ ظرفیت کانال جهت برطرف کردن نیاز کاربرد است. C_{total} هم ظرفیت کل کانال است. α کسری از ظرفیت است که خود تداخلی است که از ارتباطات چند گامی ناشی می‌شود (معمولاً 0.25 است). $\sum b(S_i)$ کل داده‌ی عبوری از M حسگر تشخیص رخداد است.



حرکت کیفی داده‌ها در wsn

^۹-upstream
^{۱۰}-downstream

سطح دقت مطلوب مورد نیاز ناظر در کاربردهای مختلف با الگوهای جریان مختلف، متفاوت است. برای مثال، ترافیک ایجاد شده‌ی چندین گره در پاسخ به تنها یک رخداد، افزونه است و بنابراین متحمل زبان می‌شود. این ترافیک سطح دقت مورد نیاز ریشه را کاهش می‌دهد. در ادامه ازدحام نزدیک گره‌ی sink با ازدحام نزدیک منابع مقایسه می‌شوند:

- ازدحام نزدیک منابع:

تشخیص یک رخداد، انفجاری ناگهانی ترافیک از گره‌های حسگر در منطقه‌ی رخداد ایجاد می‌کند که موجب تصادف و از دست رفتن قابل توجه بسته‌ها در نزدیکی منابع می‌شود. این مشکل به ویژه زمانی که تراکم گره‌های شناسایی علاوه برای نرخ تولید داده بالا می‌رود، برجسته می‌شود. جهت حل آن ارسال سیگنال به صورت گام به گام برای کاهش نرخ گزارش‌دهی مطرح شده است.

- ازدحام نزدیک ریشه:

ترافیک ایجاد شده در چندین گره‌ی منبع به سمت ریشه منتقل می‌شود. به ویژه در مواردی از تشخیص رخداد، که داده‌ها در گره‌های منبع تقریباً در زمان مشابهی تولید می‌شوند، این موضوع شدیدتر است. بنابراین بار ترافیک به سمت ریشه افزایش می‌یابد و منجر به الگوی ارتباطی کیفی مانند می‌شود.

دیگر شکل‌های ترافیکی نظیر یک به یک یا یک به چند در WSN‌ها رخ می‌دهد. در این ارتباطات چالش‌های مدیریت ازدحام نیز مطرح می‌شود.

۴- چالش‌ها

شبکه‌های حسگر بی‌سیم بعضی مسائل سطح طراحی یکتا را به علت محدودیت دریافت، پردازش، ظرفیت ذخیره و توانایی ارتباط گره‌های حسگر، الگوهای مختلف ترافیک و الگوهای مختلف گسترش، ارائه می‌دهند. بنابراین محاسبه‌ی چالش‌های مختلف مرتبط با WSN‌ها قبل از توسعه‌ی مکانیسم‌های کنترل جریان و ازدحام کارآمد، مهم است.

۴-۱ محدودیت منابع

یکی از چالش‌های اصلی موجود در شبکه‌های حسگر بی‌سیم، محدودیت‌های توان باتری، توان پردازش، حافظه و ظرفیت ذخیره‌ی گره‌های حسگر است. ارتباطات رادیویی عملیات با ارزشی در رابطه با مصرف انرژی است.

۴-۲ الگوهای ترافیکی

دیگر تفاوت شبکه‌های سنتی و WSN‌ها، الگوهای واحد ارتباطی است. در بیشتر شبکه‌های سنتی ارتباط نظیر به نظیر حکم فرما است. در صورتی که در WSN‌ها ارتباط چند به یک متداول است. این ارتباط به گونه‌ای است که داده از چندین گره‌ی حسگر به یک ناظر به طور پیوسته یا در پاسخ به

پرسش یا رخدادی ارسال می‌شود. همچنین ارتباطات یک به چند از طریق بهینه‌سازی الگوریتم‌های پخش امکان‌پذیر است. این ارتباط به صورت انتشار یک پرسش یا اطلاعات رویداد مهم در شبکه ایجاد می‌شود. در کاربردهای که از منبع ذخیره استفاده می‌کنند، الگوهای پیچیده‌ی ارتباطی دیگری می‌تواند ایجاد شود. این الگوهای ترافیکی نقش مهمی در چگونگی آشکارسازی ازدحام بازی می‌کنند و راه‌حلهایی برای کنترل آن می‌دهند.

۳-۴ معماری شبکه

معماری شبکه‌های حسگر به دو صورت مسطح^{۱۱} و چند لایه^{۱۲} طبقه‌بندی می‌شود. در معماری مسطح همه‌ی گره‌های حسگر از یک نوع هستند و مسئولیت‌های مشابهی دارند. در این نوع معماری یک تغییر کوچک باید به تمام شبکه انتشار داده شود. در توپولوژی چند لایه گره‌های منابع محصورشده^{۱۳} در لایه‌های پایین‌تر و گره‌های منابع با ارزش در ردیف‌های بالاتر قرار می‌گیرند. معماری براین اساس ظرفیت شبکه و توان اجرایی آن را بالا می‌برد. همچنین این معماری افزایش توانایی مدیریت و گسترش‌پذیری را ایجاد می‌کند.

۴-۴ معیارهای متناوب کارایی

از آنجایی که شبکه‌های حسگر کاربرد محور هستند، مکانیسم‌های کنترل جریان و ازدحام ایده‌آل باید حفظ معیار کیفیت داده‌ی سطح کاربرد را هدف قرار دهد. به طور کلی، منابع در مقابل ازدحام شبکه با کاهش نرخ تولید داده به وسیله‌ی زمان‌بندی بسته‌ها یا رها کردن آنها واکنش نشان می‌دهند. در نتیجه‌ی آن مقدار کیفیت داده در sink کاهش می‌یابد. چندین شناسایی رخداد در شبکه‌های حسگر می‌تواند در سطوح مختلف اهمیت باشد. بنابراین، می‌توان مکانیسمی برای تعیین الویت داده به وسیله‌ی اهمیت بالاتر در زمان وقوع ازدحام، ایجاد کرد.

۵-۴ افزونگی داده

افزونگی داده به معیارهای سطح کاربرد وابسته است. تلاش برای کاهش افزونگی از طریق کنترل نرخ انتشار منبع جهت کاهش مقدار ارتباطات در شبکه مهم است.

۵- طبقه بندی روش‌های کنترل جریان و ازدحام

بین پروتکل‌های کنترل ازدحام که در ادامه شرح داده می‌شود، تفاوت‌هایی وجود دارد:

^{۱۱} -flat
^{۱۲} -multi-tiered
^{۱۳} - mote

۵-۱ مکانیسم شناسایی ازدحام

مکانیسم‌های شناسایی ازدحام به دو صورت محلی و سراسری تقسیم می‌شوند. تشخیص محلی در گره‌های میانی اتفاق می‌افتد، که در آن شناسایی ازدحام با نظارت شاخص‌های محلی نظیر اشغال صف یا وضعیت کانال، انجام می‌شود. از طرف دیگر شناسایی ازدحام سراسری در گره‌ی پایه، که در آن خواص نقطه به نقطه‌ای نظیر تاخیر بسته و اتلاف فرکانس دلیل بر ازدحام است، انجام می‌شود.

۵-۲ اهداف کنترل ازدحام

پروتکل‌های انتقال، پردازش کنترل حلقه بسته را به کار می‌گیرد. در این پردازش سعی در کنترل ارسال‌های منابع، جهت دستیابی به نقطه‌ی عملیاتی موثری است. تعدادی از پروتکل‌های WSN که مبتنی بر رویکردهای کنترل ازدحام سنتی هستند، معیارهای کارایی شبکه مرکزی نظیر توان عملیاتی یا قابلیت اعتماد نقطه به نقطه را بررسی می‌کنند. چنین روش‌هایی را به عنوان روش‌های کنترل ازدحام شبکه مرکزی می‌نامند. خاصیت کاربرد محور WSN‌ها، پروتکل‌های دیگری را می‌طلبد که در آن پروتکل تلاش در جهت دستیابی معیارهای کاربرد خاص کارایی را می‌کند. به این نوع رویکردها، رویکردهای کاربرد خاص کنترل ازدحام می‌گویند.

۵-۳ مکانیسم‌های کنترل سرعت

مکانیسم‌های کنترل سرعت در WSN‌ها به دو بخش مکانیسم متمرکز کنترل منبع و توزیع شده‌ی برگشت به عقب گام به گام تقسیم می‌شود. مکانیسم کنترل منبع در گره‌ی جمع کننده‌ی داده (sink) انجام می‌شود. بر این اساس وقتی ازدحام یا نشانه‌های اولیه‌ی آن شناسایی می‌شود، گره‌ی پایه، منابع را برای تنظیم نرخ انتشارشان هدایت می‌کند.

در حالیکه مکانیسم برگشت به عقب گام به گام در گره‌های میانی انجام می‌شود، که در آن گره‌ی میانی گره‌های بالا رشته‌ی خود را جهت تنظیم نرخ انتشار بر اساس وضعیت ازدحام محلی‌شان راهنمایی می‌کند.

۵-۴ عدالت و/یا کیفیت خدمات^{۱۴}

نیاز اساسی به تخصیص منابع در هنگام ازدحام پیش می‌آید. کنترل ازدحام موظف به جلوگیری از ازدحام با کاهش نرخ ارسال است. بهبود بیشتر کنترل منابع، که نیازهای اضافی تخصیص منابع را حفظ می‌کند، امکانپذیر است.

این موضوع، برای نمونه، روش‌هایی که تلاش به برقراری عدالت جهت برقراری عدالت میان جریان‌های رقابتی در زمان وقوع ازدحام می‌کند را شامل می‌شود.

به این ترتیب رویکردهای کیفیت خدمات سعی در تخصیص منابع با توجه به اهمیت جریان یا سطوح ذخیره‌سازی می‌کنند.

۵-۵ هدف مدل کاربردی

بیشتر پروتکل‌ها به مدل ارتباطی چند به یک با داده‌ی قیفی شده به گره‌ی پایه توجه دارند. به هر حال بعضی پروتکل‌ها روی فرضیاتشان در این مدل، نظیر فرضیه‌ی جریان‌های نرخ بالا یا چندین پرسش به چندین sink و دیگر مدل‌های تحویل داده نظیر مدل ارتباطی چند به چند رخدادها یا یک به چند پرسش‌ها تفاوت دارند.

۵-۶ دیگر معیارها

معیارهای دیگر وجود دارد که موجب تفاوت پروتکل‌ها می‌شود. بعضی پروتکل‌ها نیاز به پشتیبانی اضافی دارند. (MAC یا ظرفیت اضافی شبکه). علاوه بر این بعضی پروتکل‌ها توجه خاصی به بازدهی انرژی دارند.

۶- کنترل جریان و ازدحام چند به یک در WSNها

بر خلاف الگوریتم‌های مدیریت ازدحام سنتی شبکه‌های سیمی یا ویژه‌ی بی‌سیم، بیشتر پروتکل‌های موجود در WSNها روی کاربردهایی شامل الگوی ارتباطی چند به یک با داده‌های قیفی از حسگرها به طرف sink یا تولیدکننده‌ی پرسش متمرکز اند. بنابراین، روش‌های مطرح شده در این بخش بر اساس الگوی ترافیکی چند به یک در شبکه‌های حسگر بی‌سیم هستند. در ابتدا پروتکل-

^{۱۴} - Quality of Service(QoS)

های شبکه مرکزی، بدنبال آن پروتکل‌های با کاربرد خاص و در آخر روشی که هر دو مکانیسم را پشتیبانی می‌کند، مطرح می‌شود.

۶-۱ رویکردهای شبکه مرکزی

همانطور که قبلاً گفته شد روش‌های کنترل ازدحام شبکه مرکزی معیارهای کارایی شبکه مرکزی سنتی نظیر توان عملیاتی یا قابلیت اعتماد نقطه به نقطه را در نظر دارد. در ادامه بعضی روش‌های مناسب نسبت به WSN ها شرح داده می‌شود.

۶-۱-۱ CODA^{۱۵}: انرژی موثر تشخیص و اجتناب ازدحام

تشخیص و اجتناب از ازدحام در شبکه‌های حسگر^{۱۶} با رویکردهای کلاسیک در نگهداری انرژی، توجه به نقاط مهم^{۱۷} گذرا و پایدار و تنظیم منحصر به فرد نرخ انتشار بالاتر تولید گرہ‌های حسگر نسبت به دیگران، متفاوت است.

CODA مکانیسم تشخیص ازدحام محلی و حرکت به عقب گام به گام را علاوه بر کنترل منبع متمرکز مانند مکانیسم‌های کنترل سرعت، استفاده می‌کند. CODA شامل سه مکانیسم است:

- تشخیص ازدحام بر اساس گیرنده
- حرکت به عقب گام به گام حلقه باز
- تنظیم چند منبعی حلقه بسته

مکانیسم تشخیص ازدحام بر اساس گیرنده در گرہی پایه علاوه بر گرہ‌های میانی استفاده می‌شود که بر اساس مکانیسم تشخیص ازدحام صریحی نظیر اشغال صف و وضعیت کانال در گیرنده است. به محض تشخیص ازدحام، چنانچه زودگذر باشد، تکنیک حرکت به عقب گام به گام برای تعدیل سریع آن استفاده می‌شود. اما اگر ازدحام پایدار باشد، کنترل سرعت در منابع لازم است و مکانیسم تنظیم چند منبعی حلقه بسته به کار برده می‌شود. شرح جزئی‌تر سه مکانیسم در ادامه بیان شده است:

۱- تشخیص ازدحام بر اساس گیرنده: اشغال بافر در الگوریتم‌های تشخیص ازدحام سنتی

به عنوان مقیاس سطح ازدحام استفاده می‌شد. در این مقاله مولفان ثابت می‌کنند که اشغال بافر به تنهایی مقیاس مناسبی برای ازدحام در شبکه‌های بی‌سیم به دلیل طبیعت کانال اشتراکی نیست. در CODA، گیرنده‌ها نه تنها اشغال بافر را نظارت می‌کنند، بلکه شرایط بکارگیری کانال در گذشته و حال را برای شناسایی ازدحام اندازه می‌گیرند. در

^{۱۵} - Congestion Detection and Avoidance

^{۱۶} -CODA

^{۱۷} -hotspots

هنگام ازدحام، بار کانال معمولاً سریعتر از اشغال صف افزایش می‌یابد. به بیان دیگر تعداد بسته‌های دریافتی به وسیله‌ی گیرنده معمولاً کمتر از تعداد بسته‌های انتقالی توسط ارسال کننده، به دلیل تداخل روی مسیر است. CODA از یک نمونه شِما که نظارت کانال محلی را تحت شرایط معینی مانند زمانی که بافر ارسال خالی نیست (به منظور ذخیره‌ی انرژی) فعال می‌کند.

۲- حرکت به عقب گام به گام حلقه بسته: وقتی گیرنده ازدحام را تشخیص می‌دهد، سیگنال‌هایی را به منابع در زمانی که وضعیت ازدحام پایدار است، ارسال می‌کند. این سیگنال‌ها می‌توانند به همه‌ی منابع یا تنها گره‌های میانی، بسته به ازدحام محلی، منتشر شوند. پروتکل‌های مسیریابی می‌توانند از اطلاعات سیگنال‌های ارسالی راهنمایی گرفته و مسیرهای ارتباطی بدون ازدحام بهتری را انتخاب کنند.

۳- تنظیم حلقه بسته‌ی چند منبعی: CODA مکانیسم کنترل ازدحام حلقه بسته را روی گره‌ی پایه برای تنظیم چندین منبع در موارد ازدحام پایدار اجرا می‌کند. بطور اساسی هنگامیکه نرخ انتقال منبعی از ماکزیمم توان عملیاتی تئوری تجاوز کند (S_{max})، منبع، گره‌ی پایه را با تنظیم بیتی در هر بسته‌ای که به آن انتقال می‌دهد، تا زمانیکه سرعت انتقال بالاتر از S_{max} است، آگاه می‌سازد. در پاسخ گره‌ی پایه ارسال ACK‌های را به منبع تا زمان تشخیص ازدحام، آغاز می‌کند. وقتی ازدحام را تشخیص داد، ارسال ACK‌ها را تا تعدیل ازدحام، متوقف می‌کند.

۶-۱-۲ Fusion: آگاهی از اولویت بسته

اگرچه CODA ازدحام را تعدیل می‌دهد، اما ضمانت عادلانه‌ای در میان منابع فراهم نمی‌کند. Fusion این مشکل را نظارت می‌کند و همچنین الویت‌بندی MAC (مکانیسمی برای به صف کردن گره‌هایی که دچار ازدحام شده‌اند) را انجام می‌دهند. مشابه CODA، Fusion مکانیسم حرکت به عقب گام به گام جهت کنترل نرخ را به کار می‌برد. علاوه بر این، Fusion روش تشخیص ازدحام محلی را نیز استفاده می‌کند. در ادامه روش‌های Fusion به صورت جزئی‌تر بیان شده است:

۱- کنترل جریان گام به گام: این مکانیسم شبیه همان در CODA است، با این تفاوت که Fusion مکانیسم مفهومی^{۱۸} سریعتر از پیام‌رسانی صریح^{۱۹} CODA را استفاده می‌کند. در این روش گره‌ها، بسته‌های ارسال شده توسط والد خود را جهت بررسی اینکه آیا بیت ازدحام قرار داده شده است، جستجو می‌کنند. در این حرکت به عقب گام به گام، در

^{۱۸} - implicit
^{۱۹} - explicit

صورتی که ازدحام پایدار باشد می‌توان به منبع گره‌ها رسید. توقف کامل گره‌های فرزند از انتقال بسته‌ها، به محض تشخیص ازدحام در گرهی پدر، می‌تواند انتشار فشار به عقب بیشتر به سمت گره‌های منبع را مسدود کند. برای اجتناب از این مسئله، هر گرهی فرزند، تنها مجاز به ارسال یک بسته حاوی بیت ازدحام است، بنابراین فرزندانش اجازه دارند از فاصله‌ی دور ازدحام را بررسی کنند.

۲- محدود کردن نرخ منابع: این مکانیسم مسئله‌ی اتلاف بسته‌ها در نزدیکی گرهی پایه که از منابعی دور سرچشمه شده‌اند را نشان می‌دهد. این اتلاف به علت ازدحام پیش می‌آید. برای رفع آن، روشی بر اساس جستجوی غیر فعال استفاده می‌شود. هر حسگر به ازدحام پدر خود برای تعیین تعداد کل گره‌ها (N) گوش می‌دهد. زمانی که پدر N بسته را انتقال می‌دهد، هر فرزند یک توکن می‌گیرد. فرزند اجازه‌ی ارسال کردن تا زمانی که حداقل دارای یک توکن است را دارد. این روش ساده بر اساس توکن امکان هماهنگی سرعت ارسال با سرعت فرزندان را می‌دهد. برای کار کردن این طرح فرض می‌شود که همه‌ی حسگرها بار ترافیکی مشابهی دارند و درخت مسیریابی نامتوازن نیست.

۳- الویت‌دهی MAC: CSMA به لایه‌ی MAC شانس مساوی ارسال به تمام گره‌های حسگر می‌دهد. این مسئله در مواردی از ازدحام، که گرهی حسگری مایل به رها کردن بسته‌ها در صورت پر بودن صف داخلی‌اش است، گیج کننده می‌باشد. در این صورت دادن الویت به گرهی پدری که از پیش متراکم شده در دستیابی به رسانه‌ی بی‌سیم مهم می‌شود. این مشکل با استفاده از تکنیک پیشنهادی Aad و Castelluccia حل شده است. آنها پیشنهاد داده‌اند که طول هر backoff تصادفی حسگر تابعی از وضعیت ازدحام محلی خود باشد. بنابراین مدت backoff گرهی متراکم شده به یک چهارم مدت backoff گرهی بدون ازدحام تنظیم می‌شود. بدین وسیله شانس دستیابی گرهی متراکم شده در دستیابی به رسانه‌ی بی‌سیم افزایش می‌یابد.

در کل، مکانیسم کنترل جریان گام به گام می‌تواند جلوی ارسال‌های هر پیوندی در شبکه را بگیرد، درحالی‌که تکنیک محدود کردن سرعت عدالتی را جهت تولید داده توسط هر منبع فراهم می‌کند. علاوه بر این الویت‌دهی MAC عدالتی را با الویت‌دهی ترافیک عبوری فراهم می‌کند. این استراتژی‌ها در کنار هم یکدیگر را کامل می‌کنند، درنتیجه دستیابی به سطح بالایی از کارایی حتی بعد از اشباع شبکه امکان‌پذیر می‌شود.

۶-۱-۳ کنترل عادلانه نرخ توزیع شده

Ee و همکارانش روش دیگری ارائه کردند که نیاز به پشتیبانی از ضمانت عادلانه را علاوه بر مکانیسم تعدیل ازدحام در CODA بر طرف می‌کند. مشابه CODA این رویکرد از مکانیسم تشخیص ازدحام محلی که بر اساس نظارت اشغال صف است، بهره می‌برد. همچنین الگوریتم کنترل سرعت بر اساس مکانیسم حرکت به عقب گام به گام است. برای بکارگیری عدالت، هر گره، نرخ‌های انتقال منصفانه‌ای را به گره‌های بالا رشته‌ی خود اختصاص می‌دهد. مکانیسم کنترل ازدحام پایه‌ای، یک الگوریتم کنترل حلقه بسته است که در هر گره حرکت به عقب را روی گره‌های بالا رشته‌ی خود وقتی صف گره پر یا در حال پر شدن است، به کار می‌برد. به طور مشابه وقتی صف خالی شود، گره نرخ انتشار بالاتری را به گره‌های بالا رشته‌ی خود اختصاص می‌دهد. برای اجتناب از ایجاد تداخل به علت همزمانی ارسال گره‌ها در سطح مشابه، تعدادی لرزش^{۲۰} معرفی می‌شود. الگوریتم کنترل ازدحام شامل مراحل زیر است:

۱- متوسط میزان نرخ ارسال بسته (r): با فرض مساوی بودن اندازه‌ی بسته‌ها، نرخ

ارسال بسته معکوس زمان مورد نیاز برای انتقال یک بسته است. پارامتر t زمانی است که لایه‌ی انتقال ابتدا بسته را به لایه‌ی شبکه می‌فرستد و لایه‌ی شبکه رسیدن آن را به لایه‌ی انتقال اعلام می‌کند.

۲- اختصاص نرخ مناسب تولید بسته به گره‌های بالا رشته: میانگین نرخ انتقال

بسته به تعداد گره‌های بالا رشته (n) برای تعیین نرخ تولید بسته‌ی داده تقسیم می‌شود:
$$r_{data} = r/n$$

برای محاسبه‌ی n کافی است هر گره‌ای اندازه‌ی زیر درخت خود را در بسته‌ای قرار داده و آن را به گره‌ی پدر ارسال کند. گره‌ی پدر تمام زیر درخت‌ها را شمارش کرده و مجموع آنها را در بسته‌ای قرار داده و به گره‌ی پایه ارسال می‌کند. وقتی که صف‌ها پر یا نزدیک به پر شدن می‌شوند، گره نرخ پایین‌تری را برای تولید بسته اختصاص می‌دهد.

۳- مقایسه‌ی سرعت r_{data} با سرعت $r_{data,parent}$ مربوط به گره‌ی پدر و انتشار

سرعت کمتر به گره‌های بالا رشته: $r_{data,parent}$ هم می‌تواند مربوط به بسته‌های ارسالی توسط گره‌ی پدر و هم مربوط به ارسال جداگانه‌ای به عنوان پیام کنترلی باشد

^{۲۰}-jitter

این رویکرد با روش‌های قبلی در ارائه‌ی تداخل آگاهانه‌ی برای کنترل ازدحام متفاوت است. IFRC از الگوریتم تشخیص کنترل ازدحام بر اساس نظارت بر صف اشغالی استفاده می‌کند. همچنین عدالت را در شبکه پشتیبانی می‌کند. یک گره نرخ تمام گره‌ها را (انتقال‌های تداخلی با انتقالات خود) به جای کنترل فقط فرزندانش بررسی می‌کند. کار اصلی IFRC شناسایی مجموعه گره‌هایی که روی سرعت گره‌ی متراکم شده تاثیر می‌گذارند و طراحی مکانیسمی با سربار کم ولی در عین حال کارآمد برای تقسیم انبوه اطلاعات در دیگر گره‌ها است.

IFRC فرض بر این دارد که پروتکل MAC بر اساس CSMA استفاده می‌شود و لایه‌ی MAC ارسال مجدد به لایه‌ی پیوند را برای بازیابی بسته گم شده فراهم می‌کند. همچنین فرض می‌شود پروتکل مسیریابی بر اساس کیفیت پیوند استفاده می‌شود که ساختار درختی شامل گره‌ی پایه به عنوان ریشه را می‌سازد. در نهایت فرض می‌شود هر گره تنها یک جریان را تولید می‌کند. IFRC به رسیدگی تداخل گره‌ی n_j که عاملی تداخلی با n_i است، می‌پردازد. در مدل چند به یک، مجموعه عوامل تداخل‌گر گره‌ی n_i شامل گره‌های همسایه، گره‌های همسایه‌ی والد n_i ، و زیر درختی از گره‌ی پدر علاوه بر همسایه‌های آن، می‌باشد. سه فاز اصلی طراحی IFRC در ادامه بیان می‌شود:

۱- تشخیص ازدحام: IFRC از وزن نمایی میانگین حرکت صف اشغالی به عنوان

مقیاسی از ازدحام استفاده می‌کند.

$$q_{avg} = (1 - w_q) q_{avg} + w_q q_{inst}$$

IFRC ازدحام را با رسیدن طول صف به بیشتر از حد آستانه (U) تشخیص می‌دهد. به محض شناسایی ازدحام، IFRC سرعت تولید داده (r_i) را نصف می‌کند. سپس شروع به افزایش آن به صورت جمع، می‌کند. از آنجایی که استفاده از آستانه‌ی بالایی واحد، ممکن است گره را در وضعیت ازدحام نگه دارد (حتی بعد از نصف کردن سرعت) مولفان پیشنهاد استفاده از چندین حدود آستانه، $U(K)$ ، را داده‌اند. این موضوع اجازه می‌دهد گره تا زمانی که صف به طرف به کاهش داده برود، سرعت تولید داده‌ی خود را کاهش بدهد.

۲- تقسیم ازدحام: در IFRC گره‌ی وضعیت سرعت و ازدحام خود را علاوه بر گره‌ی

دچار ازدحام شده‌ی فرزندش با سواری مجانی^{۲۲} روی داده، ارسال می‌کند. این اطلاعات به صورت بازگشتی در شبکه با کمک جستجو کردن^{۲۳} به اشتراک گذاشته می‌شود.

^{۲۱} - Interference-Aware Fair Rate Control

^{۲۲} - piggyback

^{۲۳} - snooping

بنابراین هدف IFRC اختصاص دادن حداقل سرعت عادلانه به هر جریانی است که با قواعد زیر به دست می‌آید:

قاعده‌ی ۱: سرعت هر گره باید کمتر از سرعت گره‌ی پدر خود باشد.

قاعده‌ی ۲: سرعت هر گره باید کمتر از سرعت گره‌ی همسایه‌ی متراکم خودش یا فرزند متراکم شده‌ی همسایه‌ای باشد.

۳- نرخ سازگاری: نرخ سازش در IFRC بر اساس قانون افزایش جمعی و کاهش

ضربی^{۲۴} است. در هر زمان انتقال داخلی بسته‌ی $(1/rate)$ گره‌ی n_i سرعت با $(\delta/rate)$ افزایش داده می‌شود، که در آن δ شدت افزایش را نشان می‌دهد. به طور مشابه سرعت در هنگام تشخیص ازدحام نصف می‌شود. برای جلوگیری از پرش سرعت از $rate_{min}$ به $rate_{max}$ در یک مرحله، لازم است $rate_{min} \ll \delta/rate$ باشد که معادله‌ی زیر را می‌دهد:

$$\delta = \varepsilon rate_{min}^2$$

ε عدد مثبت کوچکی است که برای شبکه‌های کوچک و تنک به صورت:

$$\varepsilon < F_j / 8U_0$$

و برای شبکه‌های بزرگ به صورت زیر است:

$$\varepsilon < 9U_1 / 2s^2 F_j$$

U_0 و U_1 حدود آستانه صف، s میانگین عمق درخت و F_j تابعی از توپولوژی و اندازه‌ی شبکه است.

۵-۱-۶ RCRT: کنترل ازدحام با قابلیت اعتماد نقطه به نقطه^{۲۵}

روش‌هایی که تاکنون بررسی شدند انتقال داده با قابلیت اعتماد را پشتیبانی نمی‌کردند. برای نمونه در ساختار کاربردی نظارت، تخمین شکل مُد ساختار می‌تواند با خواندن به صورت مرتبط با هم از چندین حسگر به دست آید. فقدان نمونه‌ها نتیجه‌ی تخمین را اشتباه می‌کند. برای رفع این مسئله، RCRT قابلیت اعتماد نقطه به نقطه را علاوه بر مکانیسم کنترل سرعت حمایت می‌کند.

RCRT به ارتباطات داده‌ای نرخ بالا با نیاز قابلیت اعتماد 100% توجه دارد. این روش از مکانیسم تشخیص ازدحام سراسری در گره‌ی پایه که بر اساس تغییر زمان رفت و برگشت^{۲۶} میان منبع و گره‌ی sink است، استفاده می‌کند. مکانیسم کنترل سرعت در sink انجام می‌شود زیرا sink دید جامعی از وضعیت شبکه دارد. در مقایسه با IFRC، RCRT رشته‌های همزمان از هر گره‌ی حسگر

^{۲۴} - Additive increase multiplicative decrease AIMD

^{۲۵} - Congestion Control with End-to-End Reliability

^{۲۶} - Round-Trip Time (RTT)

را علاوه بر سیاست‌های متفاوت تخصیص نرخ برای جریان‌های مختلف بر اساس تقاضا، حمایت می‌کند. جزئیات این روش در زیر بیان می‌شود:

۱- قابلیت اعتماد نقطه به نقطه: RCRT قابلیت اعتماد 100% را با استفاده از

مکانیسم استاندارد بازخورد بر اساس NACK پشتیبانی می‌کند. مطابق این روش sink لیستی از بسته‌های مفقود شده در هر جریان را نگه می‌دارد و این لیست را به هر منبع جهت بازیابی ارسال می‌کند. همچنین لیستی از بسته‌های نامرتب در هر جریان را برای تحویل به صورت مرتب، حفظ می‌کند.

۲- تشخیص ازدحام: RCRT از مکانیسم تشخیص ازدحام ضمنی استفاده می‌کند.

تعداد RTT‌های لازم برای بازیابی متعلقات مفقود شده‌ی جریان منبع i برابر

$$L_{norm,i} = L_i / r_i RTT_i$$

است، که L_i طول لیست بسته خارج از ترتیب منبع i و r_i سرعت اختصاص داده شده به منبع i است. RCRT ازدحام را در صورتی تشخیص می‌دهد که وزن نمایی میانگین حرکت $L_{norm,i}$ ، که با C_i نشان داده می‌شود، از آستانه‌ی U بزرگتر باشد. به طور ایده‌آل فقدان باید در یک RTT جبران شود. بنابراین، وقتی $C_i > 2$ می‌شود، شبکه نزدیک به حالت ازدحام است.

۳- نرخ سازگاری: RCRT از روش AIMD جهت کنترل سرعت، $R(t)$ ، استفاده می‌کند.

هنگامیکه شبکه ازدحام ندارد، مقدار $R(t)$ افزایش می‌یابد:

$$R(t+1) = R(t) + A$$

A مقداری ثابت است. بطور مشابه وقتی شبکه دچار ازدحام می‌شود، سرعت با

معادله‌ی زیر کاهش داده می‌شود:

$$R(t+1) = M(t)R(t)$$

$M(t)$ فاکتور کاهش وابسته به زمان است.

بعد از تنظیم سرعت، sink به اندازه‌ی $2RTT_i$ منتظر دریافت بازخورد تغییر نرخ می‌ماند. همچنین

راه بهتری برای تعیین مقدار M نسبت به مقدار ثابت $M=0.5$ با TCP استفاده می‌کند.

$M(t)$ بر اساس فقدان سرعت آزمایش شده توسط f_i محاسبه می‌شود. چنانچه نسبت تحویل بسته-

ی f_i برابر p_i باشد، مقدار ترافیک میان منبع i و sink برابر $r_i (1 - p_i) / p_i$ می‌شود.

وقتی جریان واحدی دچار ازدحام می‌شود، RCRT سرعت $R(t)$ را در همه جا با تنظیم $M(t)$ تعدیل

می‌دهد:

$$M(t) = P_i(t) / 2 - p_i(t)$$

۴- تخصیص سرعت: RCRT سرعت‌های $r_i(t)$ را برای هر جریان بر اساس سیاست

تخصیص سرعت P ، تخصیص می‌دهد. RCRT هم اکنون سه سیاست تخصیص

سرعت را پشتیبانی می‌کند:

- متناسب با تقاضا^{۲۷}
- محدودیت تقاضا^{۲۸}: هیچ منبعی بیشتر از تقاضا سرعت را نمی‌گیرد
- تخصیص سرعت عادلانه^{۲۹}

۶-۲ رویکردهای کاربرد خاص

همانطور که گفته شد نیازهای قابلیت اعتماد شبکه‌های حسگر بی‌سیم کاربرد خاص هستند و کاملاً متفاوت از شرایط قابلیت اعتماد ارائه شده در پروتکل‌های انتقال شبکه‌های مرکزی هستند. WSNها شامل پروتکل‌های کاربرد محوری هستند که موفقیت در آنها نسبت به ماموریت شبکه تعریف می‌شود. بنابراین در نوعی کاربرد بر اساس مجموعه داده، که رخدادها توسط حسگرهای collocated شناسایی و به ایستگاه اصلی ارسال می‌شوند، کاربر تشخیص همه‌ی رخدادها با قابلیت اعتماد را، نسبت به دریافت مطمئن هر بسته ترجیح می‌دهد. همچنین کاربر مایل به دانستن رخدادهای بحرانی با بیشترین سرعت ممکن، در هنگام مقایسه با رخدادها با حداقل اهمیت است. در ادامه پروتکل‌هایی که برای این نیازهای خاص کاربرد به حساب می‌آیند شرح داده می‌شود.

۶-۲-۱ ESRT: کاربرد خاص کنترل نرخ متمرکز

پروتکل انتقال معتبر رویداد به sink^{۳۰}، روی تنظیم نرخ انتشار منابع برای دستیابی رویداد مورد نیاز قابل اعتماد در sink با به کارگیری حداقل منابع تمرکز دارد. بر طبق رده‌بندی رویکرد، ESRT از مکانیسم شناسایی ازدحام محلی استفاده می‌کند. همچنین مکانیسم کنترل سرعت بر اساس رویکرد کنترل منبع است.

اساساً، ESRT از مکانیسم کنترل ازدحام حلقه بسته در پردازش‌هایی که معمولاً در sink انجام می‌شوند، استفاده می‌کند. ESRT فرض می‌کند که گره‌های sink به اندازه‌ی کافی برای رسیدن به همه‌ی گره‌های منبع در شبکه، به وسیله‌ی عمل پخش، قدرتمند هستند. هدف کلیدی ESRT راهنمایی گره‌های منبع جهت تنظیم فرکانس انتشارشان بر اساس مقیاس قابلیت اعتماد در sink و ازدحام موجود در شبکه است.

^{۲۷} - demand-proportional

^{۲۸} - demand-limited

^{۲۹} - fair rate allocation

^{۳۰} - event to sink reliable transport (ESRT)

از طرف دیگر، هنگامی که اندازه‌ی قابلیت اعتبار در sink کمتر از نیاز باشد، چنانچه ازدحامی در شبکه نباشد، sink منابع را به افزایش نرخ انتشارشان هدایت می‌کند. اما اگر در شبکه ازدحام باشد، منابع را به کاهش نرخ انتشارشان راهنمایی می‌کند. از طرف دیگر اگر مقیاس قابلیت اعتماد در sink بالاتر از نیاز باشد، sink منابع را به کاهش نرخ انتشار جهت ذخیره‌ی انرژی هدایت می‌کند. ESRT دارای ۲ پارامتر است:

(۱) شاخص قابلیت اعتماد، η ، محاسبه شده توسط sink

(۲) وضعیت ازدحام جاری

Sink، η_i را برای دوره‌ی i به صورت زیر محاسبه می‌کند:

$$\eta_i = r_i / R_i$$

r_i نشان دهنده‌ی قابلیت اعتبار رخداد و R_i قابلیت اعتبار مطلوب رخداد در sink است. برای آگاهی از وضعیت جاری ازدحام در sink هر گره‌ی حسگر اندازه‌ی صف خودش را نظارت می‌کند و اگر تکه‌ی بعدی داده‌ی منبع توانایی ایجاد سرریز بافر در گره را داشته باشد، بیت ازدحام را در بسته‌ی به طرف sink می‌گذارد. کنش‌های ESRT بر اساس مشاهداتی است که افزایش نرخ انتشار تحت ازدحام ممکن است کیفیت داده را کاهش دهد. با استفاده از این پارامترها گره‌ی sink وضعیت شبکه‌ی جاری را به ۵ دسته‌ی مختلف تقسیم می‌کند:

۱- بدون ازدحام، قابلیت اعتماد پایین^{۳۱}: منابع نرخ انتشار را به منظور بالا بردن

قابلیت اطمینان افزایش می‌دهند.

۲- بدون ازدحام، قابلیت اعتماد بالا^{۳۲}: شبکه ازدحام ندارد، اما دیده می‌شود که

قابلیت اطمینان بالاتر از حد لازم است. بنابراین sink، گره‌های منبع را به کاهش نرخ

انتشارشان برای برقراری قابلیت اطمینان مورد نیاز اما با سربار کمتر، هدایت می‌کند.

۳- با ازدحام، قابلیت اعتماد بالا^{۳۳}: شبکه ازدحام دارد اما قابلیت اعتبار بیشتر از حد

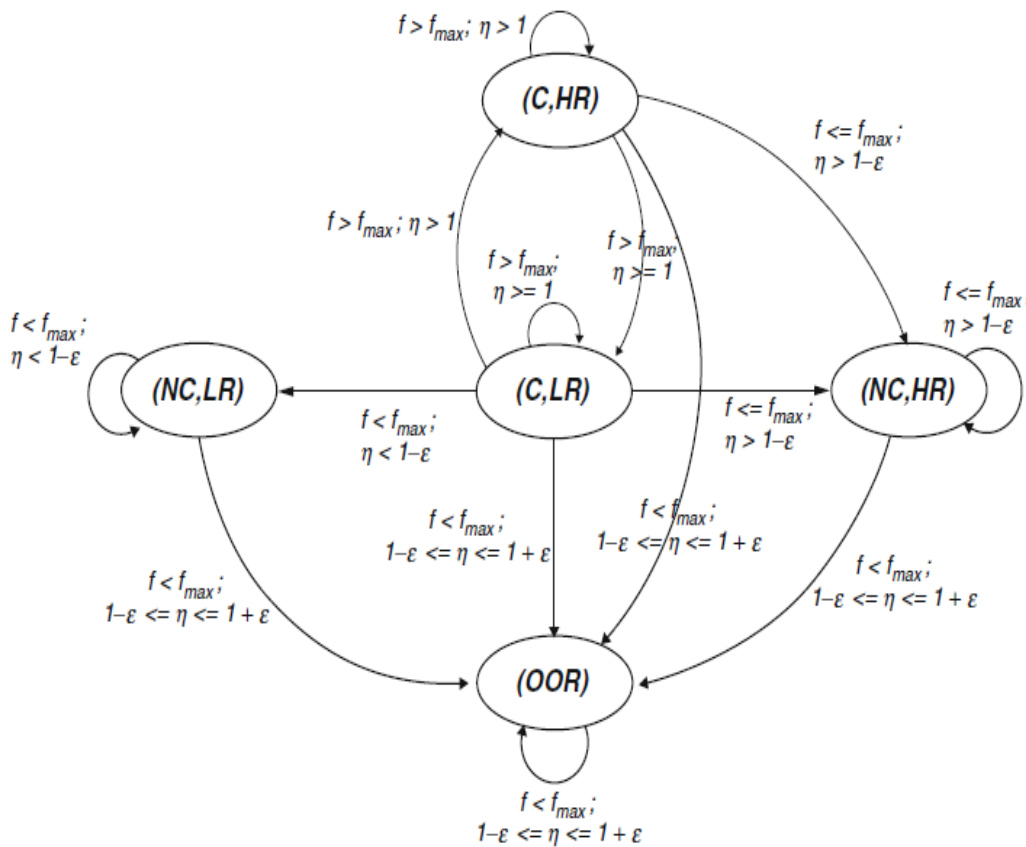
مورد نیاز است. بنابراین نرخ انتشار تا زمان برطرف شدن ازدحام یا پایین آمدن قابلیت

اطمینان از حد بیان شده، کاهش می‌یابد.

^{۳۱}- No Congestion, Low Reliability (NC, LR)

^{۳۲}- No Congestion, High Reliability (NC, HR)

^{۳۳}- Congestion, High Reliability (C, HR)



مدل وضعیت پروتکل ESRT و انتقال

۴- با ازدحام، قابلیت اعتماد پایین^{۳۴} : این رده بدترین وضعیت ممکن است. در این حالت نرخ انتشار به صورت نمایی برای خلاص شدن از ازدحام و بهتر شدن قابلیت اطمینان، کاهش می‌یابد.

۵- منطقه‌ی عملیات بهینه^{۳۵} : در این رده نرخ انتشار به اندازه‌ی کافی برای قابلیت اعتبار مورد نظر است. بطور دقیق‌تر، $1-\epsilon \leq \eta \leq 1+\epsilon$ ، که در آن ϵ تفاوت خطای کوچک برای فراهم کردن ثبات و پایداری است. هدف ESRT همیشه برقراری وضعیت شبکه در این رده است.

^{۳۴} - Congestion, Low reliability

^{۳۵} - Optimal Operation Region (OOR)

۶-۲-۲ COMUT^{۳۶}: کنترل ازدحام بر اساس اهمیت داده

در شبکه‌های حسگر بعضی از رخدادها مهم‌تر هستند. بنابراین، جریان‌های رویداد با سطوح متفاوت اهمیت، نیاز به راه‌های مختلفی برای اطمینان از این موضوع دارند که جریان‌های با اهمیت بالاتر به sink تحویل داده می‌شوند. COMUT به این موضوع توجه کرده و مکانیسم کنترل ازدحام بر اساس خوشه را برای آن فراهم کرده است. مکانیسم تشخیص ازدحام COMUT محلی است، بطوری که بر اساس اشغال صف جاری گره است. همچنین مکانیسم کنترل سرعت COMUT مبتنی بر رویکرد متمرکز کنترل منبع است که در سطح سر خوشه^{۳۷} اجرا می‌شود. هر گره سطح ازدحام محلی خود را به گرهی نگهبان^{۳۸} اطلاع می‌دهد. نگهبان، سطح ازدحام خوشه‌ی خود را همراه با بالاترین سطح اهمیت جریان رویداد ناشی از آن، با دیگر نگهبان‌های موجود در مسیر sink، معاوضه می‌کند. با این روش هر نگهبانی اعضایش را به تنظیم نرخ تولید داده‌هایشان بر اساس اهمیت داده و وضعیت ازدحام روی مسیر، هدایت می‌کند.

۱- آرایش خوشه^{۳۹}: COMUT از روش خوشه‌بندی برای کنترل ازدحام استفاده می‌کند. هر خوشه دارای یک سر خوشه است که شروع ازدحام را در حوزه‌ی محلی خود پیشگویی و نظارت می‌کند. سرخوشه با استفاده از یک متد زمانی تصادفی توسط اعلان احتمالی از یک نگهبان موجود انتخاب می‌شود. به عبارت دیگر هر گرهی منبع برای یک زمان تصادفی منتظر می‌ماند. اگر گره اعلان پیام نگهبانی را از دیگر گره‌ها در آن زمان دریافت کند، به خوشه می‌پیوندد. در مقابل اگر زمان تمام شود، آن گره خودش را به عنوان یک سر خوشه با احتمال P_n معرفی می‌کند و زمان تصادفی جدیدی با احتمال $(1 - P_n)$ تنظیم می‌کند. P_n تابعی از n است که در آن n تعداد دفعاتی است که گرهی حسگر بعد از اتمام زمان، خودش را به عنوان نگهبان انتخاب نمی‌کند. پس مقدار زمان بعدی به صورت زیر محاسبه می‌شود:

$$P_{n+1} = (1 - P_n)(1 - e^{-an}) + P_n$$

a درجه‌ی موثر افزایش P_n با n است.

۲- تخمین شدت ترافیک و تنظیم سرعت^{۴۰}: هر حسگر بار صف محلی خود را نظارت کرده و آن را به سرخوشه در مدت زمان ثابت گزارش می‌دهد. سر خوشه مجموع تخمین بار را با استفاده از خواندن محلی از هر عضو خوشه محاسبه می‌کند. مجموع تخمین‌های سر

^{۳۶} - Congestion Control for multi-class traffic

^{۳۷} - cluster-head

^{۳۹} - cluster forming

^{۴۰} - Traffic intensity estimation and rate regulation

^{۳۸} - سر خوشه

خوشه‌های در مسیر sink، با هم مرتبط می‌شوند تا تخمین شدت ترافیک یا همان سطح ازدحام بدست آید. سرخوشه به صورت دوره‌ای مقادیر محاسبه شده‌ی سطح ازدحام را علاوه بر مهمترین سطح جریان به دیگر نگهبان‌های روی مسیر به گره‌های منبع ارسال می‌کند. جهت ذخیره‌ی انرژی، سطح ازدحام به جای ارسال دوره‌ای می‌تواند در زمانی که از حد آستانه بالاتر بود، فرستاده شود. سیاست تنظیم نرخ پیشنهاد شده بر اساس سیاست افزایش به صورت جمع و کاهش به صورت ضرب است^{۴۱}. برای پشتیبانی از چندین کلاس از سطوح مهم، این سیاست به گونه‌ای اصلاح می‌شود که اگر سطح ازدحام بالاتر از حد آستانه است یا چنانچه جریانی با اهمیت بالا در طول مسیر sink وجود دارد، نرخ تولید به کمترین مقدار برای جریان‌های کم اهمیت افت داده شود.

در زمان برپایی^{۴۲} شبکه، سیل جریان داده به سمت سر خوشه‌ها، می‌تواند موجب هدر رفتن انرژی و ایجاد ازدحامی، قبل از بدست آوردن شانس جهت تخمین سطح ازدحام برای نگهبان شود. برای حل این مشکل COMUT از مکانیسم شروع آهسته استفاده می‌کند. این مکانیسم تعدادی فواصل دوره‌ی تنظیم سرعت^{۴۳} اختصاص می‌دهد که حسگر باید قبل از افزایش سرعتش منتظر باشد.

۳-۶ رویکرد ترکیبی

در این بخش Siphon رویکردی ترکیبی برای پشتیبانی از مکانیسم‌های کنترل ازدحام سنتی شبکه مرکزی علاوه بر مکانیسم‌های کنترل ازدحام کاربرد خاص فراهم می‌کند. قبلاً بیان شد که طرح کنترل ازدحام سعی در اجتناب یا تسکین ازدحام توسط محدود کردن نرخ تولید داده در منبع یا افت بسته‌ها دارند. Siphon از مکانیسم تشخیص ازدحام محلی مانند CODA برای پشتیبانی از کنترل ازدحام شبکه مرکزی در سطح گره و مکانیسم تشخیص کنترل سراسری برای کنترل ازدحام کاربرد خاص در گره‌ی پایه استفاده می‌کند. Siphon در این روش یک تعداد کمی از sink‌های مجازی چند رادیو سراسر میدان حسگر توزیع می‌دهد، که بار ترافیکی حسگرها در شروع ازدحام را می‌گیرد و به sink انتقال می‌دهد. Siphon از گره‌های ستاره‌ای^{۴۴} به عنوان sink مجازی استفاده می‌کند که به وسیله‌ی یک نقطه رادیویی کم قدرت اصلی و رادیوی دور برد فرعی مجهز می‌شوند. در ادامه به طور خلاصه الگوریتم‌هایی برای سیاست‌های سطح طراحی Siphon آورده شده است.

^{۴۱} -AIMD (Additive increase and multiplicative decrease)

^{۴۲} - setup time

^{۴۳} - Rate Regulation Epoch (RRE)

^{۴۴} -stagate

۶-۴ نیاز قابلیت اعتماد در WSN ها

همانطور که گفته شد یک کلاس مهم عبور و مرور در شبکه‌ی حسگر جریان چند به یک است. از دیگر کلاس‌های ترافیکی موجود در WSN ها ارتباطات یک به یک و یک به چند است. برای نمونه در یک سیستم ذخیره‌ی داده محور، داده‌ی حس شده در یک حسگر نیاز دارد در حسگرهای دیگری ذخیره شود. در کل پروتکل استاندارد TCP که قابلیت اعتماد نقطه به نقطه را پشتیبانی می‌کند، انتخاب مناسبی برای شبکه‌های حسگر نیست، زیرا سربارهای بزرگ TCP فشار زیادی برای گره‌های حسگر باشد. همچنین پروتکل TCP فرض بر فرستنده‌ی هوشمند و گیرنده‌ی ساده دارد که مناسب مدل شبکه‌های حسگر نیست. چرا که در آنها نیاز است فرستنده ساده باشد و گیرنده (ایستگاه پایه) نیز می‌تواند پیچیده باشد. علاوه بر این اگر داده، افزونه باشد، قابلیت اعتماد مطلقی که توسط TCP فراهم می‌شود بی‌فایده است، تا زمانی که اطلاعات کافی به وسیله‌ی ایستگاه پایه جهت دستیابی به کیفیت نظارت مطلوب، دریافت شود.

قابلیت اعتماد در بعضی کاربردها بطور خاص مهم است زیرا حتی از دست رفتن تنها یک بسته از تمام تصویر برنامه، می‌تواند موجب شکست هدف شود. پرس و جوها در شبکه‌ی حسگر معمولاً از یک گره تولید شده و به سراسر شبکه ارسال می‌شوند و این باز الگویی از چند به یک است. در آخر برای اداره‌ی برنامه‌ی کاربردی که ممکن است شامل همه‌ی انواع جریان‌های ترافیک باشند، مکانیسم ضمانت قابلیت اعتماد عمومی باید استفاده شود.

۶-۴-۱ RMST: لایه‌ی انتقال روی پروتکل مسیریابی پخش مستقیم

RMST پروتکل لایه‌ی انتقال است که هدف آن پشتیبانی از ایجاد ضمانت تحویل تکه تکه شدن و جمع شدن مجدد پیام است. برای ایجاد قابلیت اعتماد از پروتکلی بر اساس nack در هر گره‌ی گیرنده یا میانی استفاده می‌کند. بازیافت سریع در پاسخ به nack با استفاده از حافظه‌های نهان محلی گره‌های سراسر مسیر منبع به دست می‌آید. اگر گره‌ای میانی یک کپی از بسته‌ی مورد نیاز nack داشته باشد، درخواست انتقال مجدد توسط این گره پاسخ داده می‌شود و به این ترتیب سربار انتقال مجدد نقطه به نقطه کاهش می‌یابد.

۶-۴-۲ RMBTS: قابلیت اعتماد برای انتقال بلاک داده

قابلیت اطمینان در WSN ها معمولاً با انتقال مقادیر کوچک داده نظیر فرکانس پایین مرتبط است. کلاسی از کاربردهای مهم در WSN ها موجود است که اکثریت داده‌ی انتقالی را نیاز دارد. برای نمونه، در کاربرد تشکیل پرتوی آکوستیک، که در آن داده‌های خام نیاز به انتقال به یک محل

متمرکز دارند ، یا کاربردهایی شامل شبکه‌ی حسگرهای تصویر، که در آن داده‌های تصویری بدون افزونه به ایستگاه پایه ارسال می‌شوند، سرویسی برای اعتبار ارتباطات داده‌ای انبوه لازم است. برای ایجاد اعتبار، گزینه‌ی استفاده از پیام‌های افزونه، چنانچه پهنای باند به حد کافی در دسترس باشد، می‌تواند کمک کند. البته این روش توان عملیاتی را در موارد انتقال انبوه داده، تنزل می‌دهد. در مقابل هزینه‌ی اضافی استفاده از پیام‌های کنترلی جهت ایجاد قابلیت اعتماد در موارد انفجار بسته-های طولانی پذیرفتنی است. به همین دلیل، RMBTS از MAC قابل اعتماد استفاده می‌کند. از آنجایی که MAC قابل اعتماد می‌تواند اتلاف بسته به علت خطای انتقالی و بر خورد را کاهش دهد، مکانیسم انتقال مجدد نقطه به نقطه بر اساس nack می‌تواند برای بازیابی باقیمانده‌ی بسته‌های گم شده استفاده شود. همچنین سرویس نظارت پیوندی روی هر گره برای جمع کردن آمار پیوندهای متصل به گره‌های همسایه با ارسال پیام‌های سیگنالی صوتی^{۴۵} دوره‌ای و حفظ اثر پاسخ از هر همسایه ، استفاده می‌شود. این اطلاعات می‌تواند به وسیله‌ی گره برای انتخاب الگوی بهتر در پردازش ساختمان درخت پوشای دارای ایستگاه پایه به عنوان ریشه به کار برده شود.

۳-۴-۶ RBC: قابلیت اعتماد انفجار ترافیک چند به یک

این مورد معمولاً مکانیسم‌های بازیابی گام به گام بسته نظیر ack صریح همزمان^{۴۶} و ACK بی شرط توقف انتظار^{۴۷} را نشان می‌دهد. SEA، که دریافت بسته را با پیام ACK فوری اطلاع می‌دهد، مشکلات از دست دادن ACK را در پی دارد. اما در SWIA، که ACK را سواری مجانی^{۴۸} روی بسته‌ی انتقالی می‌دهد، مشکل افزایش احتمال از بین رفتن ACK‌های سوار شده به علت طولانی‌تر شدن اندازه‌ی بسته‌ها وجود دارد.

برای اداره‌ی این مشکل RBC از طرح بلاک تصدیق window-less که در آن نیاز منظم بودن بسته‌های داده کم می‌شود، استفاده می‌کند. در زمانبندی ارسال مجدد، RBC الویت بالاتر در دسترسی به کانال را به بسته‌هایی که به تعداد کمتر انتقال داده شده‌اند، می‌دهد. وقتی چندین گره دارای بسته‌هایی با الویت یکسان برای ارسال هستند، تقدم به گره‌ای داده می‌شود که دارای صف بیشتری از بسته‌ها است. در آخر، RBC از مدیریت تایمر fine-grained برای مقابله با نتایج متفاوت تاخیر ack به علت تغییر وضعیت شبکه و تسریع ارسال مجدد بسته‌های گم شده، استفاده می‌کند.

^{۴۵} - ping

^{۴۶} - synchronous explicit ACK(SEA)

^{۴۷} - stop-and-wait implicit ACK(SWIA)

^{۴۸} -piggybacked

۶-۴-۴ PSFQ: قابلیت اعتماد الگوی ترافیکی یک به چند

PSFQ پروتکل انتقال مناسبی برای مسیریابی یک به چند است. یک کاربرد مهم در زمینه‌ی شبکه‌های حسگر برنامه‌نویسی مجدد گره‌های حسگر بر اساس نیازهای کاربردی است. قابلیت اعتبار در بعضی کاربردها به طور ویژه مهم است، زیرا حتی از بین رفتن یک بسته از تمام تصویر برنامه موجب شکست در رسیدن به هدف می‌شود. ایده‌ی اصلی در پشت طرح PFSQ ارسال داده با سرعت آهسته‌تر است، در حالی که گیرنده، بازیابی محلی سریعی توسط واکنشی قسمت‌های گمشده از همسایه را انجام می‌دهد. الگوریتم PSFQ حاوی سه مرحله است:

۱- **عملیات پمپ**: قبل از ارسال داده، منبع برای یک دوره‌ی زمانی بین t_{min} و t_{max} منتظر می‌ماند.

۲- **عملیات واکنشی**: به محض شناسایی تعداد متوالی گپ، گیرنده می‌تواند عملیات واکنشی با ارسال NACKها به گره‌های همسایه شروع کند.

۳- **عملیات گزارش**: این عملیات برای آگاهی منابع از ارسال موفق است. گزارش‌گیری از دورترین گرهی مقصد آغاز شده و گره‌های میانی گزارش‌های خود را روی آن سواری مجانی می‌دهند. به این ترتیب انبوهی از گزارش از سراسر مسیر به دست می‌آید.

۶-۴-۵ STCP: قابلیت اعتماد الگوی ترافیکی مختلط

یک پروتکل لایه انتقال است که کاربردهای ناهمگن نظیر جریان پیوسته یا کاربردهای رویداد محور را پشتیبانی می‌کند. همچنین سرویس‌های کنترل ازدحام و قابلیت اعتبار را برای آنها فراهم می‌آورد. STCP در کاربردهای جریان متوالی، برای اجرای قابلیت اعتبار از NACKها بهره می‌برد. علاوه بر این STCP اداره‌ی جریان‌های متفاوت را توسط نیازهای قابلیت اعتماد مختلف پشتیبانی می‌کند. برای مثال، چنانچه قابلیت اعتماد ناظر بزرگتر از مقدار مورد انتظار است، گرهی پایه NACKها را برای بسته‌های گم شده ارسال نخواهد کرد. در موارد کاربردهای داده محور، STCP از آنجایی که تعداد منابع شناسایی رویدادی می‌تواند بسیار زیاد باشد، قابلیت اعتماد بر اساس ACK را فراهم نمی‌کند، زیرا تصدیق هر منبع، انرژی شبکه را تهی می‌کند.

STCP کنترل ازدحام را در گره‌های میانی، با تنظیم بیت ازدحام بر اساس اشغال بافر آنها اجرا می‌کند. به محض دریافت بسته‌هایی با بیت ازدحام، sink به منابع آگاه‌سازی لازم نظیر کاهش نرخ انتشار یا انتخاب مسیر بدون ازدحام را می‌دهد.

- **فاز تصدیق:** این فاز بعد از اتمام انتقال داده‌ی منبع آغاز می‌شود، که در آن sink درخواست ارسال مجدد با فراهم کردن NACK را می‌دهد.
- **فاز درستی بررسی^{۵۲}:** به محض دریافت تمام داده، sink درستی داده را بررسی می‌کند و چنانچه درستی داده رد شود، درخواست تازه‌ای ارسال می‌کند.

در ادامه دو هدف مهم Flush در دستیابی به تحویل مطمئن و زمان انتقال کمینه شرح داده می‌شود.

۶-۵-۱-۱ پروتکل قابلیت اطمینان

در طی ارسال داده از منبع به sink ممکن است بعضی بسته‌ها به علت شکست انتقال مجدد یا سرریز صف از بین بروند. زمانی که sink بر این باور است که انتقال داده‌ی منبع تمام شده است، NACKهایی را به منبع می‌فرستد، که در آن هر بسته‌ی NACK حاوی همه‌ی شماره‌های متوالی گم شده است. به جای ارسال یک سری بسته‌ی NACK حاوی این شماره‌های ترتیبی، Flush الگوریتم را به این صورت ساده کرده است که در هر زمان تنها یک بسته‌ی NACK ارسال می‌شود، تا وقتی که همه‌ی بسته‌ها با موفقیت به وسیله‌ی sink دریافت شوند.

۶-۵-۱-۲ مکانیسم پویای کنترل نرخ

Flush مدل خط لوله‌ی ساده‌ای برای ارسال داده سرتا سر گره‌های متصل به صورت خطی (از منبع به sink) را ارائه می‌دهد: وقتی گره‌ای داده را به گره‌ی بعدی خود ارسال می‌کند، باید تا هنگامی که (i) گره‌ی بعدی بسته را ارسال می‌کند و (ii) همه‌ی گره‌ها در سراسر مسیر نیز بسته را انتقال می‌دهند، منتظر بماند. بنابراین الگوریتم پویای کنترل نرخ توسط دو قانون اداره می‌شود:

قانون اول: یک گره باید تنها وقتی که گره‌ی بعدی‌اش تداخل ندارد، عمل انتقال را انجام دهد. (این کار برای پشتیبانی از مدل خط لوله است)

قانون دوم: نرخ ارسال گره نباید بیشتر از نرخ ارسال گره‌ی بعدی باشد. (برای جلوگیری از عدم تطابق سرعت)

بنابراین پس از ارسال یک بسته میزان تاخیر گره‌ی i برای ارسال بعدی برابر است با:

$$d_i = \delta_i + (\delta_{i-1} + f_{i-1})$$

در این فرمول δ_i زمان گرفته شده توسط گره‌ی i برای ارسال بسته است و f_{i-1} زمان مصرف شده توسط دیگر گره‌ها برای ارسال بسته‌هایی است که با گره‌ی بعدی می‌توانند تداخل داشته باشند ($i-1$ گره)

^{۵۲} - integrity-check phase

۶-۵-۲ پروتکل‌های یک به چند

Broadcast یا flooding روش‌های عمومی انتقال داده در مدلیک به چند است. اما این روش موجب مصرف زیاد انرژی می‌شود زیرا به علت برخورد‌ها در لایه‌ی MAC و ارسال افزونه گره‌ها در مسیرهای مختلف، بسته رها می‌شود. مشکل سابق را می‌توان با استفاده از رویکردهای شایعه پراکنی اداره کرد که در آن ایده‌ی کلیدی ارسال بسته تنها به یک گره‌ی مورد انتخاب تصادفی همسایه به جای ارسال به همه‌ی گره‌های همسایه است.

Tilak و همکارانش پروتکلی برای پخش اطلاعات غیر همسان در شبکه‌های حسگر ارائه دادند که در آن فرض اصلی بر این است که اطلاعات پیرامون یک رخداد برای گره‌هایی که به رخداد نزدیک‌ترند مهم است. به بیان دیگر، گره‌هایی که از منبع رخداد دور هستند می‌توانند ائتلاف مقداری از اطلاعات را تحمل کنند.

مجموعه پروتکل‌های دیگری در زمینه‌ی شبکه‌های ویژه‌ی بی‌سیم و ویژه‌ی سیار پیشنهاد شده‌اند. در الگوریتم مبتنی بر مکان (LBA)، یک گره اطلاعات مکان خود را در بسته وارد می‌کند، به طوری که گره‌ی گیرنده می‌تواند تصمیم بگیرد که آیا انتشار آن پوشش کافی برای ارسال با ارزش فراهم می‌کند. در پروتکل انتشار ویژه (ABHP) اطلاعات همسایه‌ی ۲ گامی^{۵۳} جمع آوری می‌شود تا مجموعه همسایه‌های ۱ گامی برای انتشار مجدد بسته انتخاب شوند، به طوری که همه‌ی همسایه‌های ۲ گامی را تحت پوشش قرار می‌دهد.

برای محیط‌هایی با نرخ خطای ارسال زیاد، طرحی نظیر انتشار پوشش دو برابری^{۵۴} (DCB) به کار می‌رود. در DCB، گره‌های جلویی به گونه‌ای انتخاب می‌شوند که همسایه‌های ۲ گام فرستنده و ۱ گام جلویی تحت پوشش قرار می‌گیرند.

۶-۵-۳ ARC: پروتکل MAC با پشتیبانی از کنترل نرخ توافقی

ARC یک پروتکل MAC کارآمد با مکانیسم کنترل نرخ سازگار با هدف دسترسی عادلانه به کانال برای تمام گره‌های WSN است. ARC از حامل حس دسترسی چندگانه^{۵۵} (CSMA) استفاده می‌کند، همچنین تلاش می‌کند به وسیله‌ی عبور مرور همزمان تصادفی، برخورد را کاهش دهد. به طور خاص، ARC تاخیرهای ارسال تصادفی را مطرح می‌کند و از فاز تغییر مکان‌دهی^{۵۶} در مدت backoff استفاده می‌کند. فرجه‌ی backoff دوره‌ی زمانی است که گره بعد از تلاش برای گرفتن

^{۵۳} - 2-hop

^{۵۴} - double covered broadcast

^{۵۵} - carrier sense multiple access

^{۵۶} - shifting

کانال بعد از آخرین فرجه، منتظر می ماند. ARC طرح کنترل سرعت توافقی که مبتنی بر سیاست افزایش به صورت جمع و کاهش به صورت ضرب (AIMD) است، را به کار می برد. تصمیم گیری های نرخ توافقی به صورت مستقل توسط هر گره گرفته می شود. این تصمیم گیری وابسته به توانایی گره-ی والد در ارسال موفق بسته اش است.

	Congestion control support	Reliability guarantee	Congestion detection mechanism	Congestion control goal	Rate control mechanism	Fairness/QoS support	Target application model
CODA	Yes	No	Local	Network-centric	Hop-by-hop backpressure	No	Many-to-one
Fusion	Yes	No	Local	Network-centric	Hop-by-hop backpressure	No	Many-to-one
Ee et al.	Yes	No	Local	Network-centric	Hop-by-hop backpressure	Fairness	Many-to-one
IFRC	Yes	No	Local	Network-centric	AIMD	Fairness	Many-to-one
RCRT	Yes	Yes	Global	Network-centric	Centralized, source-control	No	Many-to-one
ESRT	Yes	Yes	Local	Application-specific	Centralized, source-control	No	Many-to-one
COMUT	Yes	No	Local	Application-specific	Centralized, source-control	Event-importance based QoS	Many-to-one
Siphon	Yes	No	NA	Hybrid	Using additional network capacity	Constant reporting rate	Many-to-one
RMST	No	Yes	NA	NA	NA	No	One-to-one
RMBTS	No	Yes	NA	NA	NA	No	One-to-one
RBC	No	Yes	NA	NA	NA	No	Many-to-one
PSFQ	No	Yes	NA	NA	NA	No	One-to-Many
STCP	Yes	Yes	Local	Network-centric	Centralized, source-control	No	Hybrid
Flush	Yes	Yes	Local	Network-centric	Dynamic rate control	No	One-to-one

جدول مقایسه‌ی پروتکل‌های قابلیت اعتماد و کنترل ازدحام