



خلاصه مقاله‌ی "عنوان مقاله"
نام تهیه‌کنندگان: کهد آیینی، سارا آذرروش، پارسا محمدیان

بسمه تعالی

گزارش مقاله درس آزمایشگاه شبکه‌های کامپیوتری

UPPALAPATI SRILAKSHMI 1, (Member, IEEE), SALEH AHMED ALGHAMDI2, VEERA ANKALU VUYYURU3, NEENAVATH VEERAIAH 4, AND YOUSEEF ALOTAIBI	تهیه‌کننده:
A Secure Optimization Routing Algorithm for Mobile Ad Hoc Networks	عنوان مقاله:
IEEE Access	ژورنال:
رتبه‌بندی ژورنال: 1Q سال چاپ: ۲۰۲۲ تعداد ارجاع: ۴۳	

1- هدف از مطالعه مقاله

امروزه با پیشرفت وسایل الکترونیکی متحرک (Portable Devices) و فراگیری استفاده از آن‌ها، بحث مسیریابی این وسایل از مهم‌ترین دغدغه‌های دنیای شبکه می‌باشد. از طرفی این مسئله تفاوت‌هایی با مسیریابی و مسائل عادی شبکه دارد که همان‌طور که از نامش پیداست، متحرک بودن گره‌های شبکه، مشکل اصلی این مسائل است. با توجه به اهمیت این موضوع در دنیای امروز و همچنین محدودیت‌های خاص این مسئله، که در ادامه به تفصیل به آن پرداخته می‌شود، این مقاله در چنین حوزه‌ای انتخاب شد تا بهبودی در حل مسئله‌ی مسیریابی شبکه‌های متحرک را ببینیم.

2- کلیات و ادبیات موضوعی مقاله

1. شبکه‌های ad hoc: یک شبکه ad hoc مجموعه‌ای از دستگاه‌های متصل به هم است که بدون نیاز به یک مرکز مرکزی، با یکدیگر ارتباط برقرار می‌کنند. این شبکه‌ها معمولاً در محیط‌هایی که ارتباط با شبکه‌های ارتباطی سنتی ممکن نیست، مانند محیط‌های نظامی، استفاده می‌شوند.
2. مسیریابی: مسیریابی در شبکه‌های کامپیوتری به معنای یافتن مسیر مناسب برای انتقال داده میان دو یا چند دستگاه است. در شبکه‌های ad hoc، مسیریابی بسیار پیچیده است، زیرا دستگاه‌ها ممکن است به طور پویا تغییر مکان دهند.
3. الگوریتم‌های مسیریابی: الگوریتم‌های مسیریابی می‌توانند به دو دسته مسیریابی فاصله و مسیریابی وضعیت تقسیم شوند. در مسیریابی فاصله، هر دستگاه فقط به دستگاهی که فاصله کمتری از آن دارد، مسیریابی می‌کند. در مسیریابی وضعیت، هر دستگاه اطلاعاتی درباره وضعیت شبکه به دستگاه‌های دیگر می‌دهد تا بتوانند یک مسیر مناسب را پیدا کنند.

4. الگوریتم‌های مسیریابی امن: الگوریتم‌های مسیریابی امن برای جلوگیری از حملاتی مانند حملات ارتقاء، تزویر، حریم خصوصی و ... طراحی شده‌اند.

5. بهینه‌سازی: یک الگوریتم بهینه‌سازی سعی می‌کند بهترین راه‌حل ممکن را پیدا کند، با توجه به محدودیت‌های موجود. در شبکه‌های ad hoc، بهینه‌سازی به منظور کاهش هزینه‌های ارسال داده و بهبود عملکرد شبکه استفاده می‌شود.

6. جعلی: حمله‌ای است که در آن یک فرد شناسه یا اطلاعات دیگری را جعل می‌کند تا بتواند به شبکه دسترسی پیدا کند.

7. ردیابی: حمله‌ای است که در آن یک فرد می‌تواند حرکت و موقعیت دستگاه‌های شبکه را ردیابی کند.

8. تزریق داده‌ها: حمله‌ای است که در آن یک فرد داده‌های جعلی را در شبکه قرار می‌دهد تا بتواند اطلاعات را تغییر دهد یا دسترسی به آنها پیدا کند.

به طور خلاصه، مقاله به بررسی الگوریتمی مسیریابی امن و بهینه برای شبکه‌های ad hoc موبایل می‌پردازد که تلاش می‌کند بهترین مسیر را پیدا کند، با در نظر گرفتن محدودیت‌های موجود، به ویژه محدودیت‌های امنیتی. این الگوریتم با استفاده از یک رویکرد امنیتی جدید، که شامل یک سیستم احراز هویت و رمزنگاری است، امنیت داده‌ها را تضمین می‌کند. همچنین، با بهینه‌سازی مسیریابی، هزینه‌های ارسال داده را کاهش داده و عملکرد شبکه را بهبود می‌بخشد. این الگوریتم با استفاده از شبیه‌سازی‌های مختلف، نشان داده است که عملکرد بهتری نسبت به الگوریتم‌های مسیریابی موجود دارد.

3- چالش اصلی

به طور کلی این مقاله بر روی ضعف‌های شبکه‌های MANET یا Mobile Ad-hoc Network تمرکز دارد. در این مقاله سعی شده است که بهینه‌سازی‌هایی بر روی روش‌های مسیریابی یا Routing در شبکه‌های MANET انجام شود به طوری که امنیت کاربران به خطر نیفتد. با توجه به ماهیت این شبکه‌ها، از محدودیت‌ها و چالش‌هایی که در این مسائل با آن‌ها رو به رو هستیم می‌توان به محدوده‌های انتقال محدود، محدودیت‌های انرژی (باتری‌های موبایل)، متحرک بودن نودهای شبکه و خطرهای امنیتی اشاره کرد. با توجه به این محدودیت‌ها در شبکه‌های MANET مسیریابی با چالش‌هایی رو به رو است و راهکار پیشنهادی این مقاله به بهینه‌سازی این مسیریابی با توجه به محدودیت‌های MANET می‌پردازد.

4- راهکار پیشنهادی

راهکار پیشنهادی این مقاله در واقع به سه بخش تقسیم می‌شود. در مرحله‌ی اول خوشه‌بندی fuzzy clustering بین نودها انجام می‌شود و سرخوشه‌ها (cluster heads) با استفاده از اعتماد مستقیم، غیر مستقیم و اخیر انتخاب می‌شوند. در مرحله‌ی دوم نودهای نفوذی یا مزاحم‌شده (intruded nodes) با استفاده از میزان آستانه‌ی مشخص انتخاب می‌شوند. در این مرحله گره‌هایی که اعتمادی بیشتر از حد آستانه دارند را گره‌های نرمال و گره‌های دیگر را گره‌های مزاحم یا نفوذی می‌نامیم. این مرحله برای امنیت مسیریابی انجام شده تا مطمئن باشیم که گره‌هایی که ممکن است انتخاب کنیم حتما قابل اعتماد بوده‌اند و امنیت مسیر تضمین شده است. در مرحله‌ی سوم مسیر بهینه با استفاده از الگوریتم BFOA یا Bacteria Foraging Optimization Algorithm انتخاب می‌شود. این الگوریتم اهداف و ویژگی‌های مورد نظر ما مانند توان عملیاتی (throughput)، ظرفیت (capacity) و ارتباطات (communication) مسیر را در محاسبات خود دخیل می‌کند. این الگوریتم با پیش‌پردازش‌های انجام شده به ما مسیر بهینه با اطمینان از امنیت آن با زمان همگرایی حداقلی را ارائه می‌دهد.

همان طور که گفته شد این سه مرحله به صورت مجزا و به ترتیب اجرا می‌شوند تا مسیر امن و بهینه با توجه به محدودیت‌های MANET را محاسبه کنند. حال به بررسی کلی هر مرحله می‌پردازیم.

- بررسی اطمینان گره‌ها

این مرحله از الگوریتم، همان طور که در قبل اشاره شد به سه بخش جداگانه تقسیم می‌شود. در محاسبه و بررسی قابلیت اطمینان (trust) هر گره، سه پارامتر مختلف، یعنی اعتماد مستقیم، اعتماد غیر مستقیم و اعتماد اخیر، محاسبه شده و تصمیم‌گیری نهایی با توجه به آستانه با استفاده از این اعداد انجام می‌شود.

- اعتماد مستقیم (Direct Trust)

مدت زمان بر اساس زمان تخمین زده شده است برای برقراری ارتباط بین گره i ام و گره d ام می‌باشد. اعتماد مستقیم (DT) نیز به عنوان لیست اختلاف زمان‌های واقعی و زمان‌های پیش‌بینی شده‌ی گره‌ی i ام برای تصدیق کلید عمومی تولید شده توسط گره‌ی d ام می‌باشد.

$$DT_i^d(\tau) = \frac{1}{3} [DT_i^d(\tau - 1) - (\frac{\tau_{appx} - \tau_{est}}{\tau_{appx}}) + \omega]$$

τ_{appx} : پیش‌بینی شده زمان

τ_{appx} : زمان واقعی برای تصدیق کلید عمومی

ω : متغیری برای اندازه‌گیری نظر گره‌ها

- اعتماد غیر مستقیم (Indirect Trust)

$$IDT_i^d(\tau) = \frac{1}{r} \sum_{i=1}^r DT_i^d(d)$$

همسایه‌های گره r :

- اعتماد اخیر (Recent Trust)

$$RT_i^d(\tau) = \alpha * DT_i^d(\tau) + (1 - \alpha) * IDT_i^d(\tau)$$

$$\alpha = 0.3$$

- انتخاب سرخوشه با استفاده از Fuzzy Clustering

سرخوشه‌ها بر اساس بیشترین درجه اعتماد گره در میان گره‌ها در الگوریتم خوشه بندی fuzzy انتخاب می‌شوند. در محاسبات، گره دریافت کننده بهترین سرخوشه آن را به گره دیگر برمی‌گرداند.

$$J_f = \sum_{i=1}^r \sum_{j=1}^p u_{ij}^f * ||n_i - H_j||^2 \quad 1 \leq f \leq inf$$

n_i : گره i ام در MANET

H_j : سرخوشه‌ی j ام

p : تعداد کل سرخوشه‌ها

u_{ij}^f : فاصله‌ی اقلیدسی گره i ام تا سرخوشه‌ی j ام

شرط سرخوشه شدن یک گره، بیشینه‌سازی تابع M می‌باشد که در زیر آمده است:

$$M = \frac{1}{3}(D + I + R)$$

اعتماد مستقیم: D :

اعتماد غیر مستقیم: I :

اعتماد اخیر: R :

حال در انتهای این مرحله (همچنین می‌توان این بخش را مانند مقاله، یک مرحله‌ی جداگانه دانست)، بر اساس پارامتر اعتماد هر گره، گره‌های نفوذی یا مزاحم را از شبکه حذف می‌کنیم تا مسیرهای به دست آمده در مراحل بعد، مطمئن و امن باشند.

• اجرای الگوریتم BFOA

هدف از اجرای این مرحله، یافتن مسیر مناسب با توجه به پارامترهای هدف و محدودیت‌های مسئله می‌باشد. در نتیجه سعی می‌کنیم این متغیرها را در یک تابع سازگاری (fitness function) دخیل کنیم و بر اساس بیشینه شدن این تابع مسیر نهایی را انتخاب کنیم.

سه متغیر انرژی، خروجی و ارتباط مسیر برای تشکیل تابع سازگاری تعریف شده‌اند.

$$F = \frac{1}{3}(e + t + c)$$

انرژی گره‌ها: e :

خروجی گره‌ها: t :

ارتباط مسیر C:

حال به بررسی هر کدام از این متغیرها می‌پردازیم.

$$E^{remain}(\tau) = E^{remain}(\tau - 1) - E^{transmit}(\tau - 1, \tau) - E^{receive}(\tau - 1, \tau)$$

انرژی هر گره طبق فرمول بالا بر اساس پارامترهای انرژی باقی‌مانده (E^{remain}), انرژی لازم برای انتقال داده ($E^{transmit}$) و انرژی دریافتی از یک بیت داده ($E^{receive}$) محاسبه می‌شود.

$$u = \frac{v}{\tau} bps$$

نرخ مجموع بیت‌های انتقال یافته از یک مسیر بر ثانیه، طبق فرمول بالا بر اساس تعداد بیت‌های ارسال شده از مبدا به مقصد (v) و زمان لازم برای برقراری ارتباط بین دو گره از طریق لینک دو طرفه (τ) که برابر با فرمول زیر است، محاسبه می‌شود.

$$y = \frac{1}{g} \sum_{i=1}^g \frac{y_i}{cc}$$

مجموع تعداد ارتباطات CC:

درجه اتصال هر نود y_i :

تعداد گره‌ها g:

الگوریتم بهینه‌سازی باکتری جستجو (BFOA) در مراحل زیر عمل می‌کند:

1. مقداردهی اولیه: ابتدا، پارامترهای الگوریتم مانند تعداد باکتری‌ها، اندازه محیط، مقادیر آستانه و سایر پارامترهای مربوطه تعیین می‌شوند.

2. مرحله حرکت باکتری: در این مرحله، هر باکتری به صورت تصادفی در محیط حرکت می‌کند. حرکت باکتری‌ها می‌تواند شامل جابجایی تصادفی و جستجو در محیط باشد.

3. محاسبه مقادیر سازگاری: پس از حرکت باکتری‌ها، مقادیر سازگاری (سطح سلامتی) هر باکتری محاسبه می‌شود. این مقادیر معیاری برای ارزیابی عملکرد هر باکتری است.

4. تکثیر باکتری: در این مرحله، باکتری‌های با مقادیر سازگاری بالا تکثیر می‌شوند. تعداد و مکان تکثیر باکتری‌ها بر اساس قوانین مشخصی انجام می‌شود.

5. مرحله معیار گذاری: در این مرحله، مقادیر سازگاری هر باکتری با مقادیر سازگاری باکتری‌های جدید مقایسه می‌شود و باکتری‌های بهتر جایگزین می‌شوند.

6. شروع مجدد: پس از تکرار مراحل 2 تا 5 برای تعداد دفعات مشخص، الگوریتم به مرحله شروع مجدد بازمی‌گردد و محاسبات را تکرار می‌کند.

7. خاتمه الگوریتم: الگوریتم به پایان می‌رسد و بهترین نتیجه بدست آمده در مسئله به عنوان پاسخ نهایی گزارش می‌شود.

در مراحل اجرای الگوریتم BFOA، باکتری‌ها به صورت متداول متناسب با اطلاعات محیطی حرکت می‌کنند، مقادیر سازگاری برای ارزیابی عملکرد هر باکتری استفاده می‌شود و تکثیر باکتری‌ها باعث افزایش تعداد و تنوع باکتری‌ها می‌شود. این الگوریتم در نهایت به دست آوردن جوابی بهینه برای مسئله بهینه‌سازی کمک می‌کند.

این الگوریتم با الهام از جستجوی باکتری برای علوفه طبق مراحل گفته شده طراحی شده است. پیاده‌سازی این الگوریتم دقیقاً به همین روش در شبکه و با استفاده از گره‌های مسیر است که به چهار فاز کموتاکسی

(Chemotaxis)، ازدحام (Swarming)، بازتولید (Reproduction) و حذف-پراکندگی (Elimination-Dispersal) تقسیم می‌شود.

5- روش‌های پیشین، که در بخش آزمایش‌ها، راهکار ارائه شده با آنها مقایسه شده است

1. روش DSR: روش DSR (Dynamic Source Routing) در مقاله "Dynamic Source Routing in Ad Hoc Wireless Networks" معرفی شده است. در این الگوریتم مسیریابی، هر گره در شبکه دارای یک جدول مسیر است و برای ارسال بسته‌ها، بسته به صورت بی‌سیم از دستگاه به دستگاه منتقل می‌شود.

2. روش AODV: روش AODV (Ad hoc On-demand Distance Vector) در مقاله "Ad Hoc On-Demand Distance Vector (AODV) Routing" معرفی شده است. در این الگوریتم مسیریابی، هر گره در شبکه دارای یک جدول مسیر است و برای ارسال بسته‌ها، بسته به صورت بی‌سیم از دستگاه به دستگاه منتقل می‌شود. این الگوریتم از روش‌های پیشرفته‌تری نسبت به DSR برخوردار است.

3. روش OLSR: روش OLSR (Optimized Link State Routing) در مقاله "The Optimized Link State Routing Protocol (OLSR)" معرفی شده است. در این الگوریتم مسیریابی، هر گره در شبکه دارای یک جدول مسیر است و برای ارسال بسته‌ها، بسته به صورت بی‌سیم از دستگاه به دستگاه منتقل می‌شود. این الگوریتم برای شبکه‌های Ad Hoc با چگالی بالا و تعداد گره‌های زیاد مورد استفاده قرار می‌گیرد.

4. روش TORA: روش TORA (Temporally-Ordered Routing Algorithm) در مقاله "Temporally-Ordered Routing Algorithm for Wireless Ad Hoc Networks" معرفی

شده است. این الگوریتم مسیریابی به طور خاص برای شبکه‌های Ad Hoc طراحی شده است و برای مدیریت مسیرها از فرآیندهای بالاپایه‌ای استفاده می‌کند.

در مقاله مذکور، با انجام آزمایش‌ها و مقایسه عملکرد روش پیشنهادی با روش‌های فوق، نشان داده شده است که روش پیشنهادی دارای عملکرد بهتری در مقایسه با روش‌های مقایسه شده است. به طور خاص، روش پیشنهادی عملکرد بهتری در مقایسه با روش AODV و DSR در شبکه‌های با تعداد گره‌های بیشتر و با ترافیک بالاتر دارد.

6- فرضیات

1. شبکه‌ی مورد بررسی، یک شبکه‌ی ad hoc موبایل است.
2. ترافیک شبکه، با توزیع Poisson تولید شده است.
3. گره‌های شبکه، با توزیع تصادفی در محدوده‌ی مشخص شده قرار گرفته‌اند.
4. تمامی گره‌ها، دارای توان مشخصی برای ارسال و دریافت داده‌ها هستند.
5. ارتباط بین گره‌ها، با استفاده از فرآیند انتشار گسسته‌ی پیغام انجام می‌شود.
6. شبیه‌سازی به صورت یک‌باره انجام شده است و به طور میانگین بر روی چند بار تکرار شده است.
7. الگوریتم پیشنهادی، برای هر پیغام درخواستی، یک مسیر با بهترین عملکرد را انتخاب می‌کند.
8. هیچ گره‌ای در شبکه، قابلیت بلوکه شدن توسط حملات را ندارد.

7- شبیه‌ساز استفاده شده

برای شبیه‌سازی عملکرد الگوریتم پیشنهادی، از شبیه‌ساز 3-NS استفاده شده است. 3-NS یک شبیه‌ساز آزاد و متن‌باز برای شبکه‌های کامپیوتری است که اغلب برای شبیه‌سازی شبکه‌های بی‌سیم استفاده می‌شود. این شبیه‌ساز قابلیت شبیه‌سازی شبکه‌های ad hoc موبایل را نیز دارد و از آن برای بررسی عملکرد الگوریتم‌های مسیریابی در این شبکه‌ها استفاده می‌شود. 3-NS دارای ابزارها و ماژول‌های مختلفی برای شبیه‌سازی مختلف قسمت‌های شبکه مانند لایه‌های فیزیکی، لایه‌های واسط شبکه، لایه‌های انتقال و ... است که این ابزارها به محققان و توسعه‌دهندگان کمک می‌کند تا بتوانند عملکرد و عملیات شبکه‌های مختلف را شبیه‌سازی کنند و نتایجی را کسب کنند.

3-NS یک شبیه‌ساز آزاد و متن‌باز برای شبکه‌های کامپیوتری است که تحت مجوز 2GNU GPLv منتشر می‌شود. این شبیه‌ساز برای شبیه‌سازی شبکه‌های بی‌سیم و سیمی استفاده می‌شود و محققان و توسعه‌دهندگان می‌توانند از آن برای بررسی و آزمایش پروتکل‌ها و الگوریتم‌های مختلف شبکه‌های کامپیوتری استفاده کنند.

3-NS دارای ماژول‌های مختلفی است که به کاربران اجازه می‌دهد تا شبکه‌های مختلفی را شبیه‌سازی کنند. برخی از ماژول‌های مهم 3-NS عبارت‌اند از:

1. ماژول مسیریابی: این ماژول به کاربران اجازه می‌دهد تا الگوریتم‌های مسیریابی مختلف را در شبکه‌های مختلف شبیه‌سازی کنند.

2. ماژول فیزیکی: این ماژول به کاربران اجازه می‌دهد تا خصوصیات فیزیکی سیگنال‌های بی‌سیم را شبیه‌سازی کنند، مانند انتشار، جذب، بازتاب و

3. ماژول MAC: این ماژول به کاربران اجازه می‌دهد تا پروتکل‌های MAC مختلف را شبیه‌سازی کنند، مانند 802.11 و ...

4. ماژول شبکه: این ماژول به کاربران اجازه می‌دهد تا پروتکل‌های شبکه مختلف را شبیه‌سازی کنند، مانند TCP، IP و ...

شبیه‌ساز 3-NS دارای قابلیت‌هایی برای تحلیل و نمایش داده‌های تولید شده توسط شبیه‌سازی است. برای مثال، کاربران می‌توانند زمان پاسخگویی، پهنای باند، تعداد بسته‌های از دست رفته و ... را برای شبکه‌های مختلف شبیه‌سازی کنند و نتایج را به شکل نمودار و نمایش‌گرها مشاهده کنند.

استفاده از شبیه‌ساز 3-NS در مقالات علمی و تحقیقاتی به محققان کمک می‌کند تا بتوانند مدل‌های پیش‌بینی‌کننده‌تری از تحولات شبکه‌های کامپیوتری ارائه دهند.

8- ایرادات نسبت به راهکار ارائه شده و پیشنهادات برای بهبود آن

در بخش نتایج مقاله، می‌توانیم اندازه‌گیری‌های به دست آمده توسط شبیه‌سازی الگوریتم را بر اساس پارامترهای مختلف ببینیم و با روش‌های پیشین مقایسه کنیم.

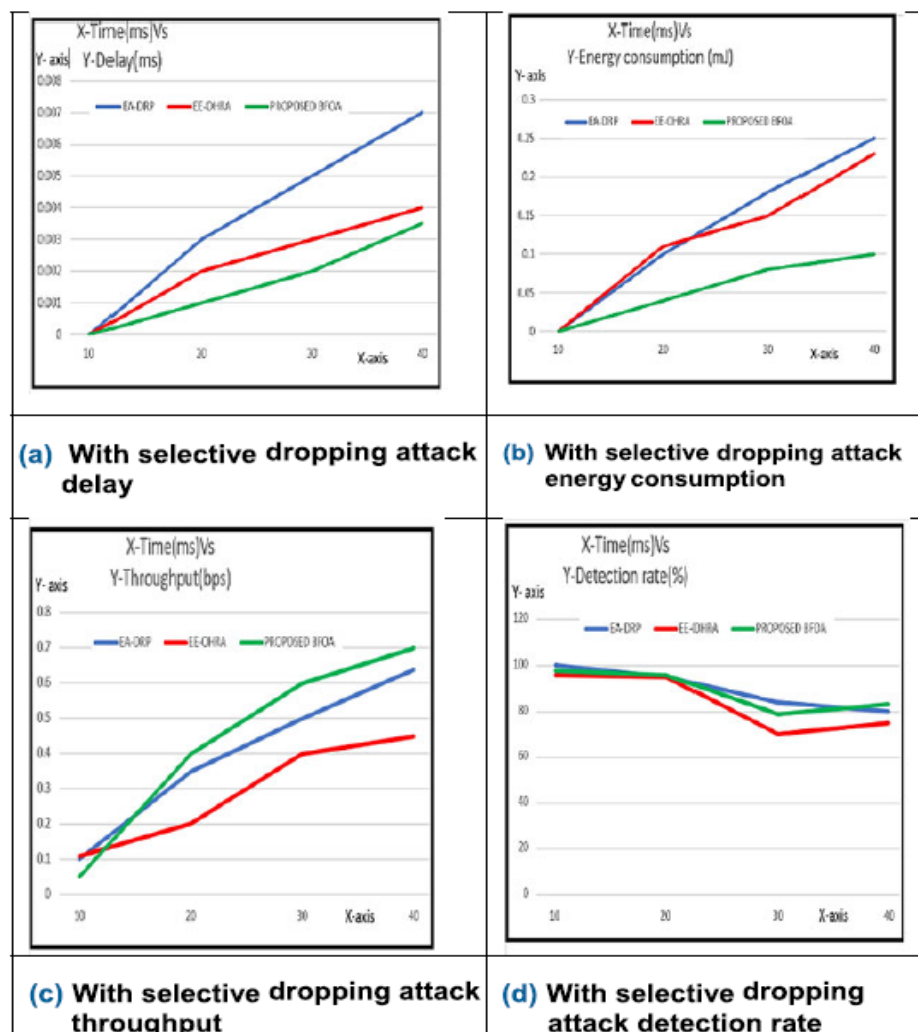


FIGURE 6. With selective dropping attack delay (b) With selective dropping attack energy consumption (c) With selective dropping attack throughput (d) With selective dropping attack detection rate.

همان طور که در نتایج بالا می بینیم، این الگوریتم در مصرف انرژی، تأخیر و خروجی مسیر بسیار خوب عمل کرده است و نتایج و عملکرد بهتری نسبت به روش های پیشین داشته، اما امنیت این الگوریتم در مسیر انتخابی تا حدی نامناسب بوده و به عنوان مثال روش EA-DROP امنیت بالاتری داشته است. امنیت پایین به این معناست که در طی این الگوریتم گره های نفوذی، مزاحم و یا مختل انتخاب شده اند که امنیت مسیر و در نتیجه کاربران را به خطر می اندازد. این مشکل به این دلیل به وجود آمده که در مرحله اول از سه مرحله الگوریتم که گره های نفوذی را مشخص و حذف می کردیم، خوب عمل

نکردیم. تشخیص این گره‌ها همان طور که در بخش راهکار پیشنهادی به تفصیل توضیح داده شده است، بر اساس سه پارامتر اعتماد مستقیم، اعتماد غیر مستقیم و اعتماد اخیر و همچنین آستانه‌ی انتخابی برای مطمئن شناختن یک گره، انجام می‌شود. همان طور که پیداست مشکل اصلی این الگوریتم از همین بخش می‌آید و باید تغییراتی را در این بخش اعمال کنیم تا اطمینان مسیر بالاتر رود. ذیل، سه روش پیشنهادی برای بهبود میزان اطمینان مسیر آمده است.

- محاسبه‌ی هر نوع اعتماد

در بخش راهکار پیشنهادی روش محاسبه‌ی هر سه نوع اعتماد را دیدیم. با تغییر فرمول یا توصیف یک پارامتر جدید، می‌توان اعتماد سنجی بهتری انجام داد تا به اطمینان مسیر پیشنهادی افزود.

- محاسبه‌ی برآیند اعتمادها

پس از محاسبه‌ی سه اعتماد مختلف، برآیند اعتمادها، که سرخوشه‌ها بر اساس آن برگزیده می‌شوند، با میانگین‌گیری از سه اعتماد، محاسبه شد. می‌توان با تغییر این فرمول، به طور مثال تبدیل میانگین به میانگین وزن دار به دلیل ارجحیت اعتماد مستقیم به اعتماد غیر مستقیم، به بهبود اطمینان الگوریتم کمک کرد. این پیشنهاد از آنجایی بر می‌آید که این سه اعتماد، ارزش یکسانی برای ما ندارند و هر کدام میزان اطلاعات مختلفی را به ما می‌دهند پس می‌توانیم برآیند آنها را از روش‌های دیگری جز میانگین‌گیری ساده محاسبه کنیم.

- آستانه‌ی اعتماد

در آخر نیز می‌توانیم به سادگی با تغییر و بالا بردن آستانه‌ی اعتماد، گره‌های نفوذی بیشتری را حذف کنیم. یعنی تعریف گره‌ی نرمال را با بالاتر بردن آستانه تغییر می‌دهیم و با این کار، گره‌های جدید در مرحله‌ی اول الگوریتم از شبکه حذف می‌شوند.

نکته‌ی بسیار مهمی که باید به آن توجه داشت این است که چهار پارامتر، خروجی، مصرف انرژی، تاخیر و اطمینان مسیر به یکدیگر وابسته هستند و با تغییر یکی از این پارامترها قطعا یک یا چند پارامتر دیگر نیز کم یا زیاد خواهند شد. به عنوان مثال در این بخش گفتیم که با سه روش می‌توانیم اطمینان مسیر را افزایش دهیم که یعنی گره‌های جدیدی را از شبکه حذف کردیم. این کار واضحا خروجی و مصرف انرژی مسیر را به ترتیب کاهش و افزایش می‌دهد. زیرا در این صورت ما گره‌های کمتری برای انتخاب مسیر داریم و هر گره به طور میانگین بار بیشتری را تحمل کرده و انرژی بیشتری را مصرف می‌کند.

در نهایت باید توجه داشت که چون این چهار پارامتر با یکدیگر در ارتباط کامل هستند، می‌توان با آزمون و خطا و تکرار شبیه‌سازی و آزمایش به تنظیمات بهینه (مثل تنظیم آستانه‌ی اعتماد) رسید که به طور کلی و در برآیند چهار پارامتر به ایده‌آل‌ترین حالت دلخواه برسیم.

9- مراجع

[1] S. Uppalapati, "Energy-efficient heterogeneous optimization routing protocol for wireless sensor network," Instrum. Measure Metrol., vol. 19, no. 5, pp. 391397, Nov. 2020.

[2] S. Bharany, S. Sharma, S. Badotra, O. I. Khalaf, Y. Alotaibi, S. Alghamdi, and F. Alassery, "Energy-efficient clustering scheme for flying ad-hoc networks using an optimized LEACH protocol," Energies, vol. 14, no. 19, p. 6016, Sep. 2021.

[3] U. Srilakshmi, N. Veeraiah, Y. Alotaibi, S. A. Alghamdi, O. I. Khalaf, and B. V. Subbayamma, "An improved hybrid secure multipath routing protocol for MANET," IEEE Access, vol. 9, pp. 163043163053, 2021.

- [4] B. Rajkumar and G. Narsimha, "Secure multipath routing and data transmission in MANET," *Int. J. Netw. Virtual Organizations*, vol. 16, no. 3, pp. 236252, 2016.
- [5] G. Anjaneyulu, V. M. Viswanatham, and B. Venkateswarlu, "Secured and authenticated transmission of data using multipath routing in mobile AD-HOC networks," *Adv. Appl. Sci. Res.*, vol. 2, no. 4, pp. 177186, 2011.
- [6] R. Prasad P and S. Shankar, "Efficient performance analysis of energy aware on demand routing protocol in mobile Ad-Hoc network," *Eng. Rep.*, vol. 2, no. 3, p. e12116, Mar. 2020.
- [7] S. V. Kumar and V. AnurathaEnergy, "Efficient routing for MANET using optimized hierarchical routing algorithm (Ee-Ohra)," *Int. J. Sci. Technol. Res.*, vol. 9, no. 2, pp. 21572162, Feb. 2020.
- [8] N.-C. Wang and Y.-L. Su, "A power-aware multicast routing protocol for mobile ad hoc networks with mobility prediction," presented at the IEEE Conf. Local Comput. Netw. 30th Anniversary (LCN), Sydney, NSW, Australia, Nov. 17, 2005, p. 8 and 417.
- [9] R. Rout, P. Parida, Y. Alotaibi, S. Alghamdi, and O. I. Khalaf, "Skin lesion extraction using multiscale morphological local variance reconstruction based watershed transform and fast fuzzy C-Means clustering," *Symmetry*, vol. 13, no. 11, p. 2085, Nov. 2021.

- [10] U. Venkanna, J. K. Agarwal, and R. L. Velusamy, "A cooperative routing for MANET based on distributed trust and energy management," *Wireless Pers. Commun.*, vol. 81, no. 3, pp. 961979, Apr. 2015.
- [11] N. Veeraiah, O. I. Khalaf, C. V. Prasad, Y. Alotaibi, A. Alsufyani, S. A. Alghamdi, and N. Alsufyani, "Trust aware secure energy efficient hybrid protocol for MANET," *IEEE Access*, vol. 9, pp. 120996121005, 2021.
- [12] A. Mallikarjuna and V. C. Patil, "PUSR: Position update secure routing protocol for MANET," *Int. J. Intell. Eng. Syst.*, vol. 14, no. 1, pp. 93102, Feb. 2021.
- [13] M. Rajashanthi and K. Valarmathi, "A secure trusted multipath routing and optimal fuzzy logic for enhancing QoS in MANETs," *Wireless Pers. Commun.*, vol. 112, no. 1, pp. 7590, May 2020.
- [14] S. R. Halhalli, S. R. Sugave, and B. N. Jagdale, "Optimisation driven-based secure routing in MANET using atom whale optimisation algorithm," *Int. J. Commun. Netw. Distrib. Syst.*, vol. 27, no. 1, p. 77, 2021.
- [15] R. Nithya, K. Amudha, A. S. Musthafa, D. K. Sharma, E. H. Ramirez-Asis, P. Velayutham, V. Subramaniaswamy, and S. Sengan, "An optimized fuzzy based ant colony algorithm for 5G-MANET," *CMC-Comput., Mater. Continua*, vol. 70, no. 1, pp. 10691087, 2022.

- [16] V. Alappatt and J. P. P. M., "Trust-based energy efficient secure multipath routing in MANET using LF-SSO and SH2E," *Int. J. Comput. Netw. Appl.*, vol. 8, no. 4, p. 400, Aug. 2021.
- [17] N. N. Panda and B. K. Pattanayak, "ACO-based secure routing protocols in MANETs," in *New Paradigm in Decision Science and Management (Advances in Intelligent Systems and Computing)*, S. Patnaik, A. Ip, M. Tavana, and V. Jain, Eds. Singapore: Springer, 2019, pp. 195206.
- [18] T.-A.-N. Abdali, R. Hassan, R. C. Muniyandi, A. H. M. Aman, Q. N. Nguyen, and A. S. Al-Khaleefa, "Optimized particle swarm optimization algorithm for the realization of an enhanced energy-aware location-aided routing protocol in MANET," *Information*, vol. 11, no. 11, p. 529, Nov. 2020.
- [19] M. B. Dsouza and D. H. Manjaiah, "Energy and congestion aware simple ant routing algorithm for MANET," in *Proc. 4th Int. Conf. Electron., Commun. Aerosp. Technol. (ICECA)*, Coimbatore, India, Nov. 2020, pp. 744748.
- [20] N. Veeraiah and B. T. Krishna, "An approach for optimal-secure multi-path routing and intrusion detection in MANET," *Evol. Intell.*, vol. 5, pp. 115, Mar. 2020.
- [21] S. Palanisamy, B. Thangaraju, O. I. Khalaf, Y. Alotaibi, S. Alghamdi, and F. Alassery, "A novel approach of design and analysis of a hexagonal fractal antenna

array (HFAA) for next-generation wireless communication," *Energies*, vol. 14, no. 19, p. 6204, Sep. 2021.

[22] S. Palanisamy, B. Thangaraju, O. I. Khalaf, Y. Alotaibi, and S. Alghamdi, "Design and synthesis of multi-mode bandpass filters for wireless applications," *Electronics*, vol. 10, no. 22, p. 2853, Nov. 2021.

[23] A. F. Subahi, Y. Alotaibi, O. I. Khalaf, and F. Ajesh, "Packet drop battling mechanism for energy aware detection in wireless networks," *CMC-Comput., Mater. Continua*, vol. 66, no. 2, pp. 20772086, 2021.

[24] D. Chander and R. Kumar, "QoS enabled cross-layer multicast routing over mobile ad hoc networks," *Proc. Comput. Sci.*, vol. 125, pp. 215227, Jan. 2018.

[25] P. Parthiban, G. Sundararaj, and P. Maniiarasan, "Maximizing the network lifetime based on energy efficient routing in ad hoc networks," *Wireless Pers. Commun.*, vol. 101, no. 2, pp. 11431155, Jul. 2018.

[26] V. Nithya, B. Ramachandran, and G. V. Devi, "Energy efficient tree routing protocol for topology controlled wireless sensor networks," *Int. J. Commun. Antenna Propag. (IRECAP)*, vol. 5, no. 1, pp. 16, 2015.

[27] P. Rajendra and P. Shankar, "Improvement of battery lifetime of mobility devices using efficient routing algorithms," *Asian J. Eng. Technol. Appl.*, vol. 1, pp. 1320, Mar. 2017.

[28] Srilakshmi, U., Alghamdi, S.A., Vuyyuru, V.A., Veeraiah, N. and Alotaibi, ``A Secure Optimization Routing Algorithm for Mobile Ad Hoc Networks ,"IEEE Access., vol. 10, pp. 14260--14269, 2022.