ارائه یک پروتکل احراز هویت در شبکه خودرویی در جهت نظارت ترافیک شهری

مهسا خلوصی زیرک
دانشجوی کارشناسی ارشد، گروه مهندسی کامپیوتر، واحد تهران جنوب، دانشگاه آزاد اسلامی، تهران، ایران
روشنک رفیعی نظری
عضو هیئت علمی، گروه فیزیک، واحد تهران جنوب، دانشگاه آزاد اسلامی، تهران، ایران
راضیه فرازکیش
عضو هیئت علمی، گروه مهندسی کامپیوتر، واحد تهران جنوب، دانشگاه آزاد اسلامی، تهران، ایران

چکیده
هدف از ارائه این مقاله تحقق امنیت در فرآیند تبادل اطلاعات در شبکه خودرویی در کنار بهبود ترافیک شهری می باشد. در جهت نیل به این هدف باید فرآیند احراز هویت انجام و گره های مجاز از غیر مجاز تشخیص داده شود. فرآیند تبادل اطلاعات باید در یک بستر امن انجام گردد. همچنین شیوه ارتباطی نیز باید مبتنی بر یک روش بهینه باشد. در نهایت تحقق این موارد منجر به بهبود امنیت و ترافیک می گردد. روش پیشنهادی در سه فاز ارائه می گردد. در فاز اول ابتدا خودرو ها به سرخوشه RSU در محدوده های جغرافیایی مختلف خوشه بندی می شوند. سپس یک روش رمزنگاری در جهت بهبود امنیت و انجام فرآیند احراز هویت در فاز دوم ارائه و در ادامه در فاز سوم الگوریتم بهینه سازی نهنگ در جهت بهبود تبادل اطلاعات ارائه می گردد. در نهایت روش پیشنهادی با روش های مشابه از نظر پارامترهای میزان تأخیر احراز هویت در مقابل تعداد مهاجمان، میزان دقت تشخیص در مقابل تعداد مهاجمان، سربار کلید در مقابل تعداد مهاجمان و نسبت تحویل بسته در مقابل تعداد مهاجمان مقایسه و برتری محسوسی دارد.

واژگان کلیدی: شبکه خودرویی، حمل و نقل هوشمند، بهبود ترافیک شهری، الگوریتم بهینه سازی نهنگ

مقدمه

مناطق شهری به دلیل افزایش جمعیت و جابجایی سریع مردم از روستاها به طور فزاینده ای شلوغ شده اند. روند نظارت بر ترافیک در این مناطق با توجه به جریان ترافیک گسترده در جاده‌ها موضوع مهمی است (Latif et al., ۲۰۲۳).

شبکه های بین خودرویی[1]یک سیستم حمل و نقل هوشمند[2] است که با بهره گیری از واحدهای کنار جاده[3]، تبادل اطلاعات را انجام می دهد. بهبود ایمنی رانندگی وکاهش تصادفات در جاده با استفاده از VANET محقق می گردد (Jithendra & Rekha, ۲۰۲۲).

با این حال، ارسال پیام RSU در زیر ارتباط خودرو به خودرو[4] و خودرو به زیرساخت[5] طبقه بندی می شود. VANETدر به حداقل رساندن تصادفات کنار جاده ای کمک می کند و موقعیت وسایل نقلیه در حال حرکت در یک مسیر را تشخیص می دهد. درVANET ، شناسایی وسایل نقلیه اضطراری، مانند اتومبیل های گشت و آمبولانس، آسان است. این فرآیند منوط به بدست آوردن مکان واقعی وسیله نقلیه در حال حرکت است (Latif et al., ۲۰۲۳).

در مرجع (Latif et al., ۲۰۲۳) قابلیت اطمینان، مقیاس‌پذیری و پایداری VANETهای متحرک سریع، با معرفی پروتکل‌های مسیریابی مبتنی بر خوشه برای ارتباطات V۲V و V۲I افزایش داده شده است.

به گفته نویسندگان مرجع (Panigrahy & Emany, ۲۰۲۳) سیستم های حمل و نقل هوشمند از اینترنت همه چیز[6] استفاده می کنند. همچنین ارتباطات مبتنی بر مکان در وسایل نقلیه متحرک کاربرد حیاتی در VANET دارد.

اشتراک منابع یکی از مسائل مهم در ارتباط با وسایل نقلیه است. اشتراک منابع در جابجایی وسایل نقلیه، مستلزم مصرف انرژی قابل توجهی است که یک مانع جدی در ارتباطات وسیله نقلیه است. مدیریت منابع توزیع شده برای بهینه سازی استفاده از منابع و کاهش سربار سیگنال شبکه مفید است (Goyal et al., ۲۰۲۲; Hamzah et al., ۲۰۲۳).

سیستم‌های نظیر به نظیر[7] با استفاده از شبکه‌های بی‌سیم به دلیل تکامل اینترنت محبوبیت دارند. این سیستم ها هنگام به اشتراک گذاری پیام ها و سایر منابع، عملکرد مطلوبی را ارائه می دهند. برنامه های کاربردی ایمنی جاده با استفاده از شبکه های بی سیم P۲P نیز به بخشی حیاتی از VANET برای نظارت بر ترافیک تبدیل شده اند (Hamdi et al., ۲۰۲۰; Singh et al., ۲۰۲۰).

برای ارتباط خودرو به خودرو و خودرو به زیرساخت، منطقه با تعیین یک خوشه خاص یا از طریق شعاع فاصله انتخاب می شود. یک سیستم هوشمند ترافیک، مزایای بی شماری را برای مدیریت ترافیک به ارمغان می آورد (Hsieh, ۲۰۲۳).

این مزایا شامل نظارت بر ترافیک در محل، تجزیه و تحلیل مناسب تراکم ترافیک، ارسال هشدارهای دقیق تخلفات ترافیکی به رانندگان، تجزیه و تحلیل زیرساخت ترافیک و ارسال پیام با استفاده از ارتباطات V۲V و V۲Iاست (Shen et al., ۲۰۲۲).

در یکITS ، میانگین زمان پاسخ پیام معمولاً تا ۱۰ بار در میلی ثانیه طول می کشد. خوشه یا معمولاً دارای محدوده شعاع تقریباً ۴۰۰ متر است. در شبکه VANET ارسال پیام می تواند از طریق اطلاعات متنی، گرافیکی و شنیداری انجام می شود. این شبکه باید در برابر حملات سایبری، دسترسی غیرمجاز، سرقت هویت و فیشینگ ایمن باشد (Sharma et al., ۲۰۲۲).

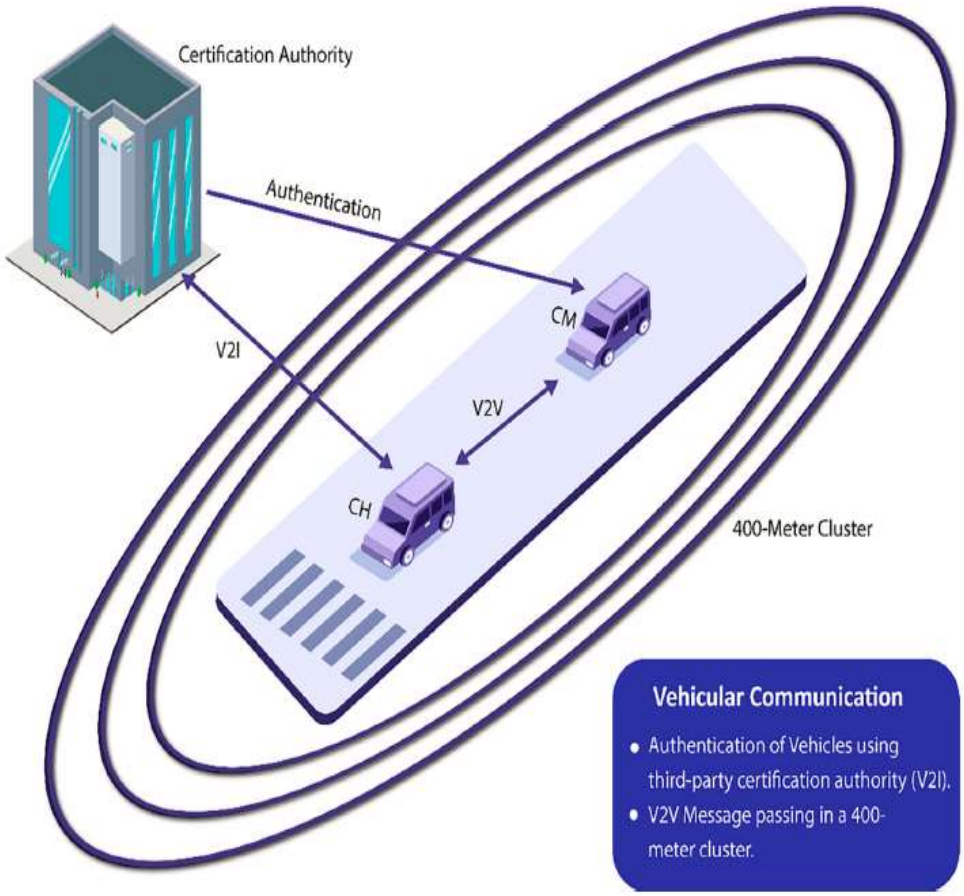
ممکن است گفته شود که امنیت VANET زمانی نقض می شود که شخصی به یک واحد داخلی خودرو[8] دسترسی غیرمجاز پیدا کند و می تواند مانع عملکرد اصلی خودرو شده و یا آنرا تغییر دهد. به دلیل ازدحام ترافیک یا زیرساخت ناکافی جاده، برخورد وسیله نقلیه امکان پذیر است (Gao et al., ۲۰۲۳).

---

[1] Vehicular Ad Hoc network(VANET)
[2] Intelligent Transportation System (ITS)
[3] Road Side Units (RSU)
[4] Vehicle-to-Vehicle (V2V)
[5] Vehicle-to-Infrastructure (V2I)
[6] Internet of Everything (IoE)
[7] peer-to-peer(P2P)
[8] Onboard Unit (OBU)

پیام "Crash Possibility" را می توان برای غلبه بر این مشکل به وسیله نقلیه منتقل کرد. اندازه گیری فاصله برای ایجاد یک پیام هشدار برخورد، ضروری است که می تواند با استفاده از دوربین و سنسور انجام شود (,.Lim et al۲۰۱۹).

در شکل 1 ارتباط وسائل نقلیه را در شعاع ۴۰۰ متر نمایش می دهد. CH به معنای سرخوشه است و CM نشان دهنده دیگر عضو خوشه است.



شکل 1 ارتباط وسائل نقلیه را در شعاع ۴۰۰ متر نمایش(,.Latif et al۲۰۲۳)

در این مقاله پروتکل‌های ارتباطی و احراز هویت مبتنی بر خوشه ایمن، برای ارتباطات V۲V و V۲I پیشنهاد می شود. همچنین ارتباطات ارتباطات V۲V و V۲I پیشنهاد شده مطابق شکل 1 می باشد.

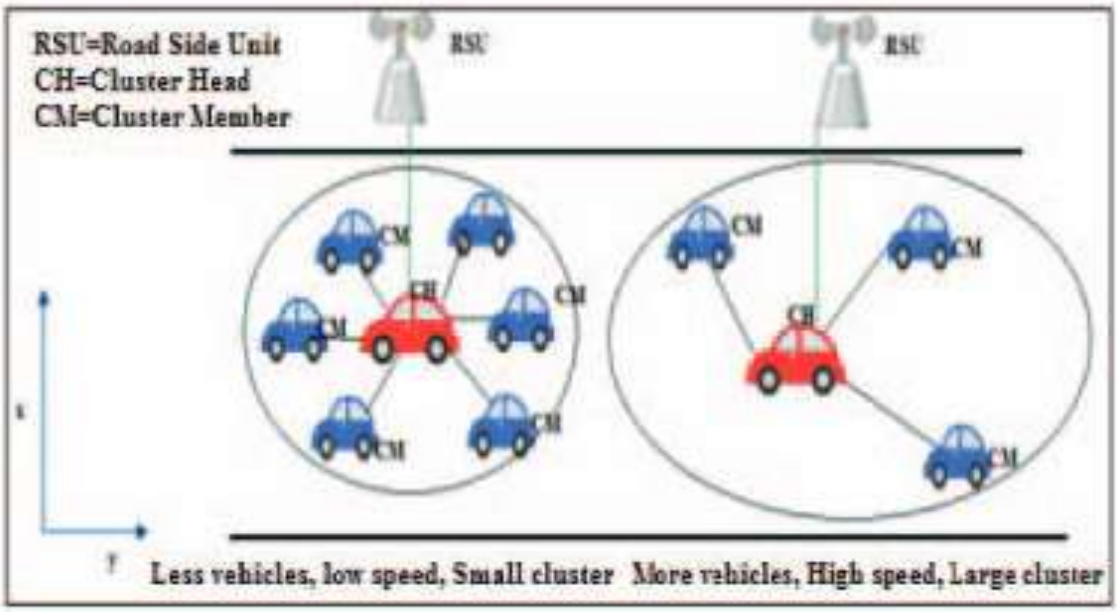
روش تحقیق

روش پیشنهادی در سه فاز ارائه می گردد. در فاز اول خوشه بندی با هدف بهبود ترافیک شهری بر روی داده ها انجام می شود. در فاز دوم ایمن سازی داده ها و آماده سازی آنها برای انجام تبادل اطلاعات به شکل ایمن انجام می شود. سپس در فاز سوم تبادل اطلاعات با استفاده از الگوریتم نهنگ انجام می گیرد.

فاز اول خوشه بندی داده ها

با توجه به اینکه خودروها به عنوان عضو اصلی شبکه خودرویی ماهیتی پویا و متحرک دارند، لذا خودروها در شبکه خودرویی، به شکل مداوم موقعیت جغرافیاییشان را تغییر می دهند. بر اساس همین تغییرات فرآیند خوشه بندی نیز باید در دوره های زمانی مشخصی بروز رسانی شود. بر همین اساس چندین عامل در انجام فرآیند خوشه بندی مورد نظر قرار خواهد گرفت.

در روش پیشنهادی شیوه خوشه بندی مورد استفاده در مرجع (,Bavalatti & Sutagundar۲۰۱۷) تغییر و یک روش خوشه بندی جدید ارائه می شود. در مرجع (,Bavalatti & Sutagundar۲۰۱۷) هر خودرو همانند شکل 2 به عنوان سرخوشه لحاظ می گردد.

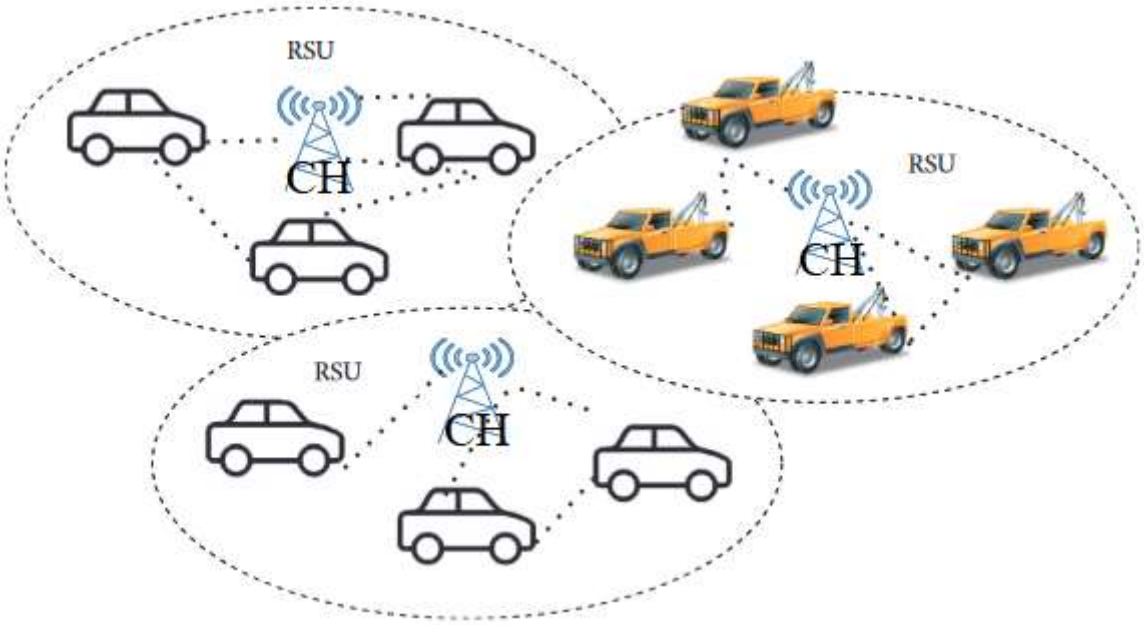


شکل 2 خوشه بندی خودروها با سرخوشه از نوع خودرو

در اغلب روش های خوشه بندی، سرخوشه ها غالبا خودرو می باشد. در واقع از خوردوها در فرآیند خوشه بندی استفاده می شود. با توجه به این موضوع که خودرو ها، علی الخصوص خودرو سرخوشه بسیار سریع از دسترس نزدیکترین RSU مورد نظر خارج می شود. بر همین اساس ارائه فرآیند خوشه بندی به این سبک در فرآیند بروز رسانی خوشه ها به دلیل تغییرات مکرر گره سرخوشه افزونگی بسیار زیادی را ایجاد می نماید. بر همین اساس روش بهینه نیست. از دیگر مشکلات قرار دادن خودروها به عنوان سرخوشه ارسال به موقع داده ها از سمت سرخوشه به گره RSU است، چون امکان دارد که خودرو مورد نظر(سرخوشه) از محدوده مورد پوشش RSU خارج و امکان ارسال داده ها از نظر ساختار وجود نداشته باشد که این امر باعث افزایش میزان بسته های از دست رفته شبکه می شود. همچنین جابجایی داده ها بین سرخوشه قبلی و جدید میزان حجم داده ها تبادل شده را افزایش می دهد.

لذا در جهت بهبود این ضعف، روش خوشه بندی ارائه شده در مرجع (,Bavalatti & Sutagundar۲۰۱۷) انتخاب مناسبی می باشد. در سناریو پیشنهاد شده در این مرجع RSU به عنوان سرخوشه استفاده می شود. ساختار به این شکل عمل می کند که RSU مورد نظر که در موقعیت جغرافیایی ثابتی قراردارد به عنوان سرخوشه انتخاب و تنها خودرهایی که هستند تغییر می کنند و همواره سرخوشه ثابت است. در واقع مزیت این روش این است که داده ها از دست نمی رود و کلیه اطلاعات و داده های ترافیکی از خودروهای عضو خوشه به سرخوشه که RSU می باشد ارسال می گردد. در واقع سرخوشه همواره از وضعیت شبکه با خبر است و داده ای از دست نمی رود. در واقع حتی اگر یک خودرو از محدوده مورد پوشش یک RSU خارج و وارد محدوده مورد پوشش RSU بعدی گردید، عضو RSU جدید می شود و داده ها را برای RSU جدید ارسال می کند و لذا داده ای از دست نمی رود.

بر همین اساس مدل خوشه بندی مطابق شکل 3 انجام می شود.



شکل 3 مدل خوشه بندی خودرو ها با سرخوشه RSU

فرض بر این است که C1 ، C2، C3،… Cnخودروها هستند که در سیستم تک خط با سرعت های گوناگونی در حرکت می باشند. کلیه اطلاعات خودرو مانند شناسه خودرو، سرعت خودرو، لیست همسایگان و موقعیت خودرو توسط گره RSUجمع آوری می شود.
در معادله ۱ سرعت میانگین و سرعت نهایی محاسبه می شود.
معادله 1

$$S_{Avg} = \sum_{i=1}^{n} \frac{S_i}{\rho}$$

$$S = \frac{Distance\ Travelled}{Time}$$

در معادله 1 ρ تراکم خودروها می باشد.
یکی از مهمترین موضوعات تغییر RSU هر خودرو می باشد. در واقع زمانی که یک خودرو از محدوده سرخوشه خود که RSU می باشد خارج و به محدوده RSU دیگری وارد می شود چه اتفاقی برایش رخ می دهد. برای تعیین تکلیف این وضعیت باید تعدادی پارامتر به شرح زیر لحاظ نمود:

- فاصله گره خودرو تا گره RSU
- ترافیک بین گره خودروها تا گره RSU
- میانگین حداکثر سرعت مجاز گره خودرو در محدوده گره RSU

در واقع باید با استفاده از این سه عامل فرآیند خوشه بندی انجام و یک تابع هدف نهایی تعیین گردد. برای هر RSU که در محدوده جغرافیایی خودرو مورد نظر است تابع هدف محاسبه و در نهایت RSU که بهترین(کمترین) مقدار تابع هدف را داراست به عنوان سرخوشه برای آن خودرو به آن خوشه ملحق می شود. این فرآیند مداوم و در بازه های زمانی مشخص بروز رسانی می گردد.
برای محاسبه مقدار فاصله هر خودرو تا RSU از معادله ۲ استفاده می شود.

معادله ۲

$$d = \Delta x + \Delta y$$

همچنین برای محاسبه نمودن ترافیک بین هر خودرو تا RSU از معادله ۳ استفاده می شود.

معادله ۳

$$\mathbf{T} = \frac{\boldsymbol{\rho}}{۲\pi d^{۲}}$$

در حالتی که میان گره خودرو و گره RSU فقط یک خیابان وجود داشت میانگین سرعت مجاز برابر با سرعت مجاز همان خیابان است که این مقدار از قبل تعیین شده است. اما اگر بین آنها دو و یا چندین خیابان قرار داشت میانگین سرعت مجاز برابر مجموع سرعت های مجاز هر خیابان تقسیم بر تعداد خیابان ها است. این مقدار در معادله ۴ محاسبه می شود.

معادله ۴

$$V_{avg} = \begin{cases} S_{avg} & if\ between\ Car\ and\ Rsu\ One\ Street \\ \frac{\sum_{i}^{number\_street} S_i}{number\_street} & if\ between\ car\ More\ Street \end{cases}$$

تابع هدف خوشه بندی در معادله ۵ ارائه می گردد. ضرایب α و β و γ مقدار وزن و اهمیت هر هدف را مشخص می نماید.

با توجه به این موضوع که مقادیر اهداف فاصله و ترافیک باید مقدار حداقل و هدف سرعت باید مقدار حداکثر شود در تابع هدف لحاظ شده است. همچنین باید مجموع وزن های α و β و γ برابر یک باشد.

معادله ۵

$$fitness = \frac{\alpha * d + \beta * T}{\gamma * V_{avg}} \quad \alpha + \beta + \gamma = ۱ \quad \alpha, \beta, \gamma \leq ۰.۵$$

بر این اساس برای هر گره خودرو مقدار معادله ۵ با لحاظ کردن کلیه RSU هایی که خودرو مورد نظر در محدوده اش قرار دارد محاسبه می شود. سپس کمترین مقدار محاسبه شده بین کلیه مقادیر انتخاب و خودرو مورد نظر در نهایت عضو خوشه ای می شود که آن RSU سرخوشه اش است. بر همین اساس سناریو اول پایان می پذیرد.

فاز دوم ایمن سازی داده ها

روش رمزگذاری نامتقارن برای معرفی روش پیشنهادی انتخاب شده است. RSA یک روش رمزنگاری نامتقارن است. الگوریتم RSA مانند همه روش های رمزگذاری نامتقارن، از یک کلید عمومی و یک کلید خصوصی برای انجام فرآیند رمزگذاری و رمزگشایی استفاده می کند.

در این مقاله از روش جدیدی برای انتخاب کلید عمومی استفاده شده است که مبتنی بر ویژگی های متغیر و غیر ثابت خودروها می باشد. لذا بر همین اساس در جدول ۱ پارامترهای تاثیرگذار بر تشکیل کلید عمومی تعیین می گردد.

جدول ۱ پارامترهای تاثیرگذار بر تشکیل کلید عمومی

id_s	کد (شناسه منحصر به فرد) گره فرستنده پیام(خودرو یا RSU)
id_r	کد (شناسه منحصر به فرد) گره گیرنده پیام(خودرو یا RSU)
x_s	طول جغرافیایی گره فرستنده پیام (خودرو یا RSU)
y_s	عرض جغرافیایی گره فرستنده پیام(خودرو یا RSU)
x_r	طول جغرافیایی گره گیرنده پیام (خودرو یا RSU)
y_r	عرض جغرافیایی گره گیرنده پیام (خودرو یا RSU)
V_s	سرعت گره فرستنده پیام(خودرو یا RSU)

V_r	سرعت گره گیرنده پیام(خودرو یا RSU)

بر اساس پارامترهای مطرح شده در جدول ۱ کلید عمومی موقت جهت انجام فرآیند رمزنگاری در معادله ۳-۶ محاسبه می گردد. بر طبق معادله ۶ و کلید عمومی موقت محاسبه شده، کلید عمومی نهایی در معادله ۳-۷ ساخته می شود.

معادله ۶ $$Temp_{public} = \mathrm{id_{sender}} + \mathrm{id_{rec}} + |x_s - x_r| + |y_s - y_r| + V_s + V_r$$

k_{rnd1} عددی تصادفی بین $\mathrm{id_s}$ و $Temp_{public}$ و k_{rnd2} نیز عدد تصادفی بین $\mathrm{id_{rec}}$ و $Temp_{public}$ می باشد. از مقادیر k_{rnd1} و k_{rnd2} در معادله ۳-۷ جهت محاسبه کلید عمومی نهایی استفاده می شود. در معادله ۷ کلید عمومی نهایی محاسبه شده است.

معادله ۷ $$Key_{public} = Temp_{public} * k_{rnd1} * k_{rnd2}$$

RSA، (Tao et al., ۲۰۱۴) یکی از روش های رمزگذاری نامتقارن است که به ترتیب از کلید عمومی و کلید خصوصی برای رمزگذاری و رمزگشایی استفاده می کند. در الگوریتم RSA سه مرحله تولید کلید خصوصی، رمزگذاری و رمزگشایی وجود دارد. در معادله ۸ کلید خصوصی تولید می شود.

معادله 8

۱. Choose p and q as the prime number
۲. $n = p \times q$
۳. $\varphi(n) = (p - 1) \times (q - 1)$
۴. Choose K_{public} e such that gcd $(\varphi(n), e) = 1$
۵. Private Key $d = e^{-1} \bmod \phi(n)$

معادله 9 فرآیند رمزنگاری را بر اساس معادله ۸ انجام می دهد.

معادله 9 $$C = (M)^e \bmod N$$

معادله ۱۰ داده ها را رمزگشایی می کند.

معادله ۱۰ $$M = (C)^d \bmod N$$

در ادامه فاز سوم تبادل اطلاعات می باشد.

فاز سوم تبادل اطلاعات

الگوریتم بهینه سازی نهنگ در سه گام به شرح زیر ارائه می شود:

گام اول شکار محاصره ای: در این مرحله شکار توسط نهنگ ها محاصره می شود.

گام دوم فاز بهره برداری: در این گام فرآیند بهره برداری با روش حمله به حباب تور توسط نهنگ ها انجام می شود.

گام سوم مرحله اکتشاف: در مرحله اکتشاف فرآیند جستجوی شکار توسط نهنگ ها انجام می شود.

- **گام اول شکار محاصره ای:** نهنگ ها می توانند به خوبی مکان جغرافیایی شکار را شناسایی نمایند. نهنگ ها بر اساس مکان جغرافیایی شکار را محاصره می نمایند. با توجه به این موضوع که مکان جغرافیایی بهینه در فضای جستجو از راه مقایسه

حاصل نمی شود، الگوریتم پیشنهادی فرض می نماید که بهترین راه حل کاندید حال حاضر، شکار هدف می باشد و یا نزدیک به حالت مطلوب است. بعد از اینکه بهترین عامل جستجو(بهترین نهنگ) شناسایی گردید، عوامل دیگر جستجو(سایر نهنگها) سعی می کنند مکان جغرافیایی خود را نسبت به بهترین عامل جستجو(بهترین نهنگ)، به روزرسانی نمایند. این رفتار از طریق معادله ۱۱بیان شده است (Mirjalili & Lewis, ۲۰۱۶).

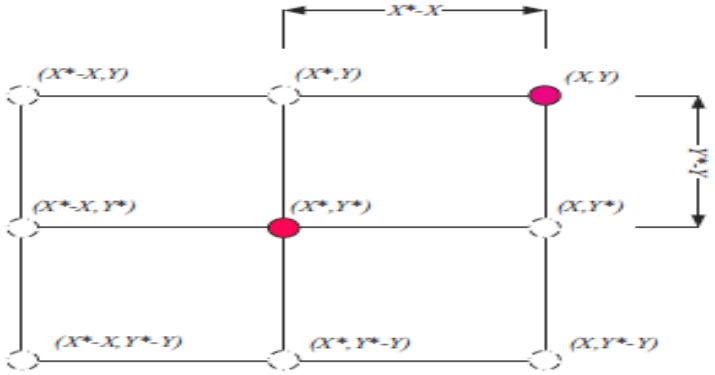
$$\vec{D} = \left|C.\overrightarrow{X^*}(t) - \vec{X}(t)\right| \qquad ۱۱$$
$$\vec{X}(t+۱) = \overrightarrow{X^*}(t+۱) - \vec{A} * \vec{D}$$

که در آن t تکرار جاری را نشان می دهد، A و C بردارهای ضرائب ، X* بردار مکان بهترین راه حل بدست آمده در حال حاضر و X بردار مکان است. لازم به ذکر است که در صورت وجود راه حل بهتر، X* در هر تکرار باید بروز شود. بردار A و C به صورت معادله 12 محاسبه می گردد.

$$\vec{A} = ۲\vec{a}.\vec{r} - \vec{a} \qquad 12$$
$$\vec{C} = ۲r$$

که در معادله 12، a به شکل خطی از مقدار ۲ تا ۰ در نوسان است. مقدار a در طی تکرار های روش پیشنهادی در هر دو گام اکتشاف و استخراج کاهش می یابد. همچنین مقدار r بردار تصادفی در فاصله ۰ تا ۱ است.

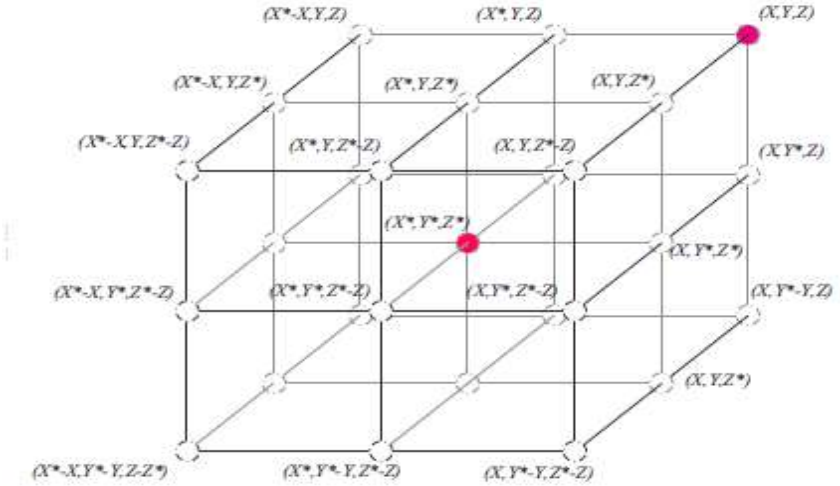
شکل 4 منطق معادله ۱۱ را برای یک مشکل دو بعدی نشان می دهد. موقعیت (X,Y)یک عامل جستجو را می توان با توجه به موقعیت بهترین رکورد فعلی (X*,Y*) به روز کرد.



شکل 4 بردارهای موقعیت دوبعدی و مکان‌های بعدی احتمالی آنها(Mirjalili & Lewis, 2016)(X*)

با تنظیم مقدار بردارهای A و C می توان مکان های مختلف اطراف بهترین عامل را با توجه به موقعیت فعلی به دست آورد. موقعیت احتمالی به روز رسانی یک عامل جستجو در فضای سه بعدی نیز در شکل 5 نشان داده شده است.

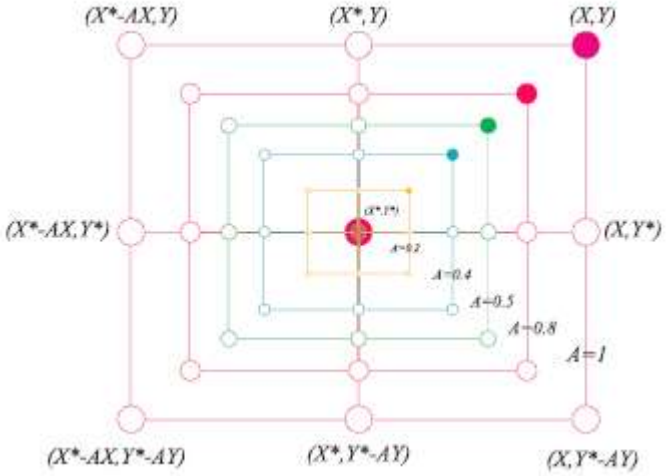
لازم به ذکر است که با تعریف بردار تصادفی (r) می توان به هر موقعیتی در فضای جستجوی واقع بین نقاط کلیدی نشان داده شده در شکل 6 رسید. بنابراین، معادله ۱۱ به هر عامل جستجو اجازه می دهد تا موقعیت خود را در همسایگی بهترین راه حل فعلی به روز کند و احاطه کردن طعمه را شبیه سازی می کند. همین مفهوم را می توان به فضای جستجو با n بعد تعمیم داد و عوامل جستجو در ابر مکعب ها در اطراف بهترین راه حل به دست آمده تا کنون حرکت خواهند کرد. نهنگ‌های گوژپشت نیز با استراتژی شبکه حباب به طعمه حمله می‌کنند. در ادامه این روش به صورت ریاضی بیان می شود.



شکل 5 بردارهای موقعیت سه بعدی و مکان‌های بعدی احتمالی آنها(X*) (Mirjalili & Lewis, ۲۰۱۶)

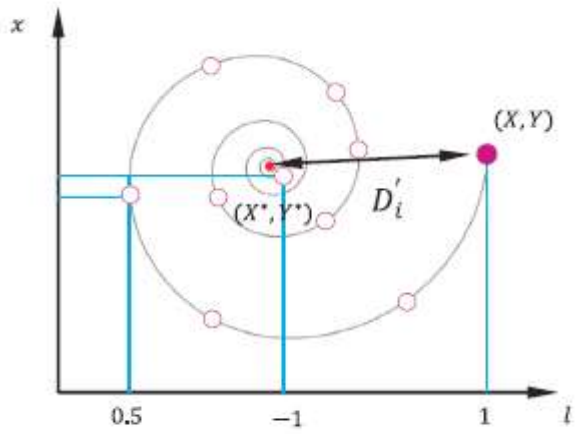
- **گام دوم فاز بهره برداری روش حمله به حباب تور:** جهت مدلسازی ریاضی رفتار حباب تور وال ها، طی دو روش طراحی شده است:

- **روش اول مکانیزم محاصره انقباضی:** این رفتار به از طریق افزایش مقدار a در معادله ۱۲حاصل می شود. محدوده نوسان A بوسیله a کاهش می یابد. به عبارت دیگر، A مقداری تصادفی در فاصله a تا a- است و a در طی تکرارها، از مقدار ۲ تا ۰ کاهش می یابد. با انتخاب مقادیر تصادفی A در فاصله ی ۱ تا ۱- ، می توان مکان جدید عامل جستجو را در هر کجای بین مکان اصلی عامل و مکان بهترین عامل کنونی، تعریف کرد. شکل 6 موقعیت‌های ممکن را از (X, Y) به سمت (X*, Y*) نشان می‌دهد که می‌توان با $0 \leq A \leq 1$ در یک فضای دو بعدی به دست آورد.



شکل 6 مکانیزم محاصره انقباضی (Mirjalili & Lewis, ۲۰۱۶)

- **بروزرسانی موقعیت مارپیچی:** همانطور که در شکل ۷ مشاهده می شود، این روش در ابتدا فاصله بین وال قرار گرفته در مختصات (X, Y) و طعمه موجود در(X*, Y*) را محاسبه می کند. معادله ۱۳ معادله ای مارپیچی بین موقعیت نهنگ و طعمه ایجاد می شود تا حرکت حلزونی شکل نهنگ گوژپشت را تقلید کند.



شکل ۷ بروزرسانی موقعیت مارپیچی (Mirjalili & Lewis, ۲۰۱۶)

$$\vec{X}(t+1) = \vec{D}.e^{bi}.\cos(2\pi l) + \overrightarrow{X^*}(t) \qquad ۱۳$$

که در این معادله $\vec{D}$ به فاصله ۱ امین نهنگ تا طعمه اشاره دارد (بهترین راه حل بدست آمده تا اینجا)، b ثابتی برای تعریف شکل مارپیچ لگاریتمی است و اعددی تصادفی بین ۱ تا ۱- می باشد. لازم به ذکر است که نهنگ گوژپشت، حول طعمه در امتداد یک دایره انقباضی و همزمان در مسیر مارپیچی شکلی به شنا در می آید. جهت مدلسازی این رفتار همزمان، فرض شده است که نهنگ با احتمال ۵۰ درصد از بین مکانیزم محاصرهی انقباضی و یا مدل مارپیچی یکی را انتخاب می کند تا موقعیت نهنگ ها در طول بهینه سازی به روز رسانی شود. مدل ریاضی به شکل معادله۱۴ است.

$$\vec{X}(t+1) = \begin{cases} \overrightarrow{X^*}(t) - \vec{A}.\vec{D} & if\ p < 0.5 \\ \vec{D}.e^{bi}.\cos(2\pi l) + \overrightarrow{X^*}(t)\ if\ p \geq 0.5 \end{cases} \qquad ۱۴$$

که در آن P عددی تصادفی بین ۰ تا ۱ است. علاوه بر روش حباب تور، نهنگ های گوژپشت به صورت تصادفی به دنبال طعمه می گردند. مدل ریاضی جستجو بدین صورت است.

- **فاز سوم مرحله اکتشاف جستجوی شکار:** روشی مشابه بر مبنای واریاسیون بردار A را می توان جهت جستجوی شکار (اکتشاف) به کار گرفت. در حقیقت، نهنگ های گوژپشت، بر طبق مکان یکدیگر، به صورت تصادفی به جستجو می پردازند. بنابراین، بردار A را با مقادیر تصادفی بزرگتر از او یا کمتر از ۱- به کار گرفته شده تا عامل جستجو را مجبور به دور شدن از نهنگ مرجع کند. بر خلاف فاز استخراج، جهت بروزرسانی موقعیت عامل جستجو در فاز اکتشاف به جای استفاده از داده های

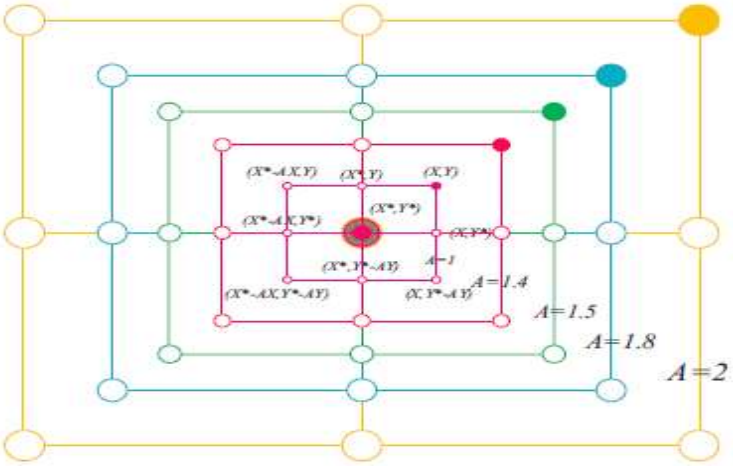
بهترین عامل جستجو، از انتخاب تصادفی عامل بهره برده شده است. این مکانیزم به همراه A >۱ بر اکتشاف تاکید دارند و به الگوریتم WOA اجازه می دهند تا جستجویی سراسری را به انجام رساند. مدل ریاضی به شکل معادله ۱۵ است:

$$\vec{D} = |\vec{C}.\overrightarrow{X_{rand}} - \vec{X}| \qquad ۱۵$$

$$\vec{X}(t+۱) = \overrightarrow{X_{rand}} - \vec{A}.\vec{D}$$

در این معادله، $\overrightarrow{X_{rand}}$ بردار موقعیت تصادفی انتخاب شده (نهنگ تصادفی) از جمعیت جاری است.

برخی از موقعیت های ممکن در اطراف یک راه حل خاص با $\vec{A} > ۱$ در شکل ۸ نشان داده شده است.



شکل ۸ مکانیزم اکتشاف(Mirjalili & Lewis, ۲۰۱۶)

الگوریتم WOA با مجموعه ای از راه حل های تصادفی شروع به کار می کند. در هر تکرار، عوامل جستجو موقعیت خود را با توجه به عامل جستجویی که تصادفی انتخاب شده و با بهترین راه حل بدست آمده ی جاری، به روزرسانی می کنند. پارامتر a جهت فراهم آوردن اکتشاف و استخراج، به ترتیب از مقدار ۲ تا ۰ کاهش می یابد. یک عامل جستجوی تصادفی در حالت $|\vec{A}|>1$ انتخاب می شود، این در حالی است که بهترین راه حل زمانی انتخاب می شود که جهت بروزرسانی موقعیت عوامل جستجو، $|\vec{A}|<1$ باشد. بسته به مقدارp ، الگوریتم WOA این قابلیت را دارد تا بین حـرکت دایروی و یا مارپیچی یکـی را انتخاب کند . در نهایت، الگوریتم WOA با ارضای شرایط خاتمـه، پایان می پذیرد.

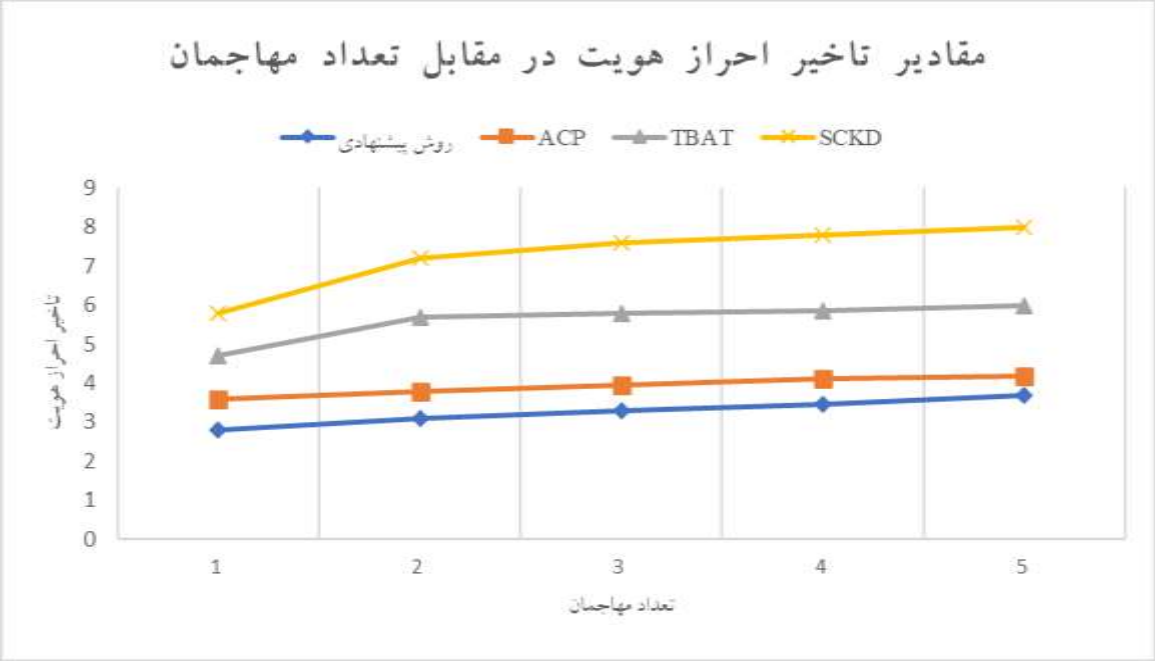
یافته ها

در جدول ۲ نتایج روش پیشنهادی از نظر تأخیر احراز هویت در مقابل تعداد مهاجمان در کنار نتایج مرجع (Latif et al., ۲۰۲۳) نمایش می دهد.

جدول ۲ تاخیر احراز هویت در مقابل تعداد مهاجمان

الگوریتم ها	تعداد حمله ها				
	۱	۲	۳	۴	۵
روش پیشنهادی	۲/۸	۳/۱	۳/۳	۳/۴۵	۳/۷
ACP	۳/۶	۳/۸	۳/۹۵	۴/۱	۴/۱۸
TBAT	۴/۷	۵/۷	۵/۷۹	۵/۸۵	۵/۹۸
SCKD	۵/۸	۷/۲	۷/۶	۷/۸	۸

بر طبق نتایج کسب شده در فرآیند شبیه سازی و بر اساس جدول ۲، در شکل ۹ مقادیر تاخیر فرآیند احراز هویت در مقابل تعداد مهاجمان روش پیشنهادی با روش های موجود در مرجع (,.Latif et al۲۰۲۳) نمایش داده شده است.



شکل ۹ مقادیر تاخیر احراز هویت در برابر تعداد مهاجمان

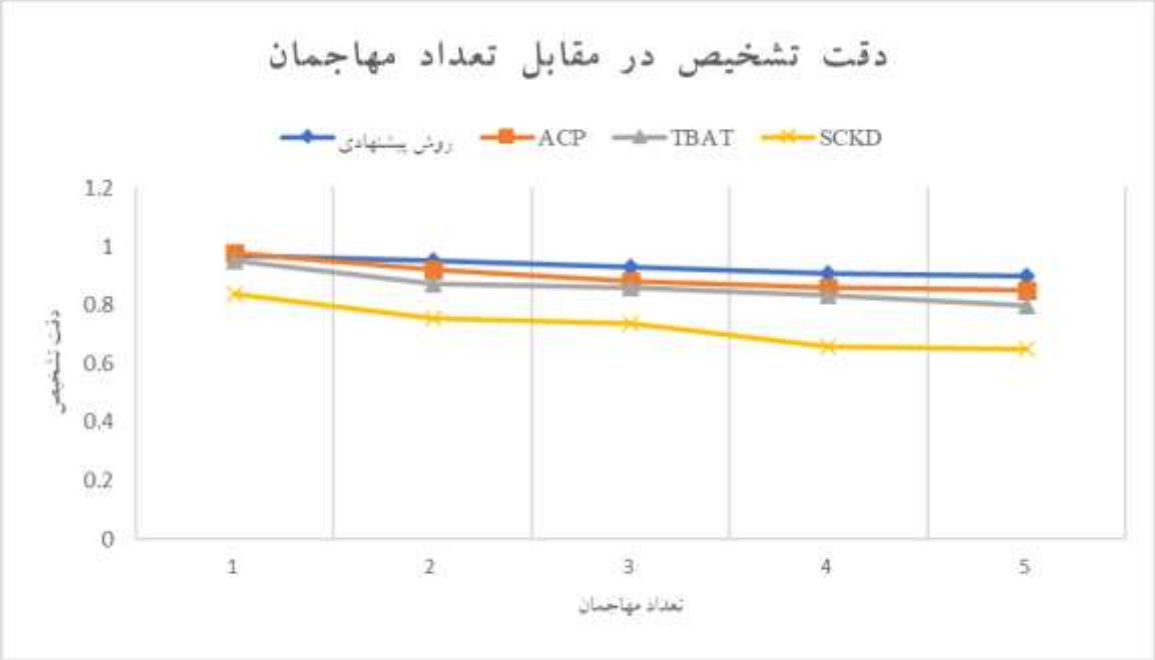
بر طبق نتایج مکسوبه پارامتر تاخیر روش پیشنهادی به ترتیب میزان ۲۰، ۷۱ و ۱۲۲ درصد برتری نسبت به الگوریتم های TBAT،ACP و SCKD را دارا می باشد. دلیل برتری روش پیشنهادی از نظر پارامتر تاخیر استفاده بهینه و مناسب از روش خوشه بندی، رمزنگاری و همچنین اتخاذ روش مناسب تبادل اطلاعات با استفاده از الگوریتم نهنگ می باشد.

در جدول ۳ نتایج روش پیشنهادی از نظر دقت تشخیص در مقابل تعداد مهاجمان در کنار نتایج مرجع (,.Latif et al۲۰۲۳) نمایش می دهد.

جدول ۳ دقت تشخیص در مقابل تعداد مهاجمان

الگوریتم ها	تعداد حمله ها				
	۱	۲	۳	۴	۵
روش پیشنهادی	۰/۹۷	۰/۹۵	۰/۹۳	۰/۹۱	۰/۹
ACP	۰/۹۸	۰/۹۲	۰/۸۸	۰/۸۶	۰/۸۵
TBAT	۰/۹۵	۰/۸۷۵	۰/۸۶	۰/۸۳۵	۰/۸
SCKD	۰/۸۴	۰/۷۵۵	۰/۷۳۵	۰/۶۶	۰/۶۵

بر طبق نتایج کسب شده در فرآیند شبیه سازی و بر اساس جدول ۳، در شکل ۱۰ مقادیر دقت تشخیص در مقابل تعداد مهاجمان روش پیشنهادی با روش های موجود در مرجع (,.Latif et al۲۰۲۳) نمایش داده شده است.



شکل ۱۰ مقادیر دقت تشخیص در برابر تعداد مهاجمان

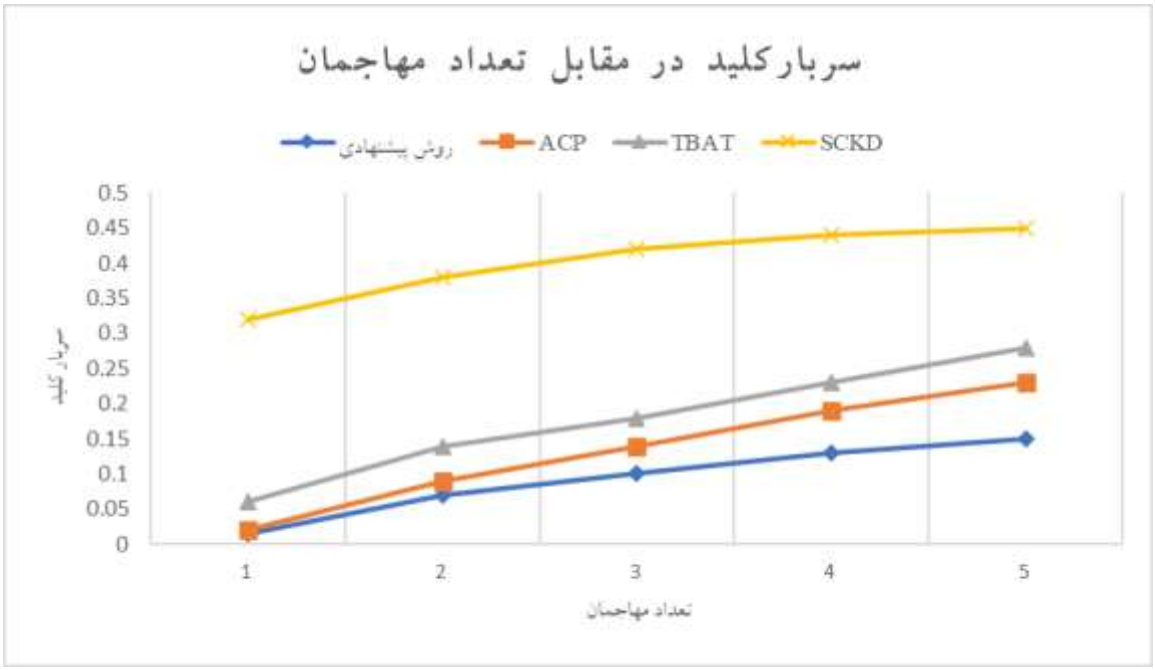
بر طبق نتایج مکسوبه پارامتر دقت روش پیشنهادی به ترتیب میزان ۳، ۷ و ۲۱ درصد برتری نسبت به الگوریتم های TBAT،ACP و SCKD را دارا می باشد. دلیل برتری روش پیشنهادی از نظر پارامتر تاخیر استفاده بهینه و مناسب از روش خوشه بندی، رمزنگاری و همچنین اتخاذ روش مناسب تبادل اطلاعات با استفاده از الگوریتم نهنگ می باشد.

در جدول ۴ نتایج روش پیشنهادی از نظر سربار کلید در مقابل تعداد مهاجمان در کنار نتایج مرجع (,.Latif et al۲۰۲۳) نمایش می دهد.

جدول ۴سربار کلید در مقابل تعداد مهاجمان

الگوریتم ها	تعداد حمله ها				
	۱	۲	۳	۴	۵
روش پیشنهادی	۰/۰۱۵	۰/۰۷	۰/۱	۰/۱۳	۰/۱۵
ACP	۰/۰۲	۰/۰۹	۰/۱۴	۰/۱۹	۰/۲۳
TBAT	۰/۰۶	۰/۱۴	۰/۱۸	۰/۲۳	۰/۲۸
SCKD	۰/۳۲	۰/۳۸	۰/۴۲	۰/۴۴	۰/۴۵

بر طبق نتایج کسب شده در فرآیند شبیه سازی و بر اساس جدول ۴، در شکل ۱۱ مقادیر سربار کلید در مقابل تعداد مهاجمان روش پیشنهادی با روش های موجود در مرجع (,.Latif et al۲۰۲۳) نمایش داده شده است.



شکل ۱۱ سرباز کلید در مقابل تعداد مهاجمان

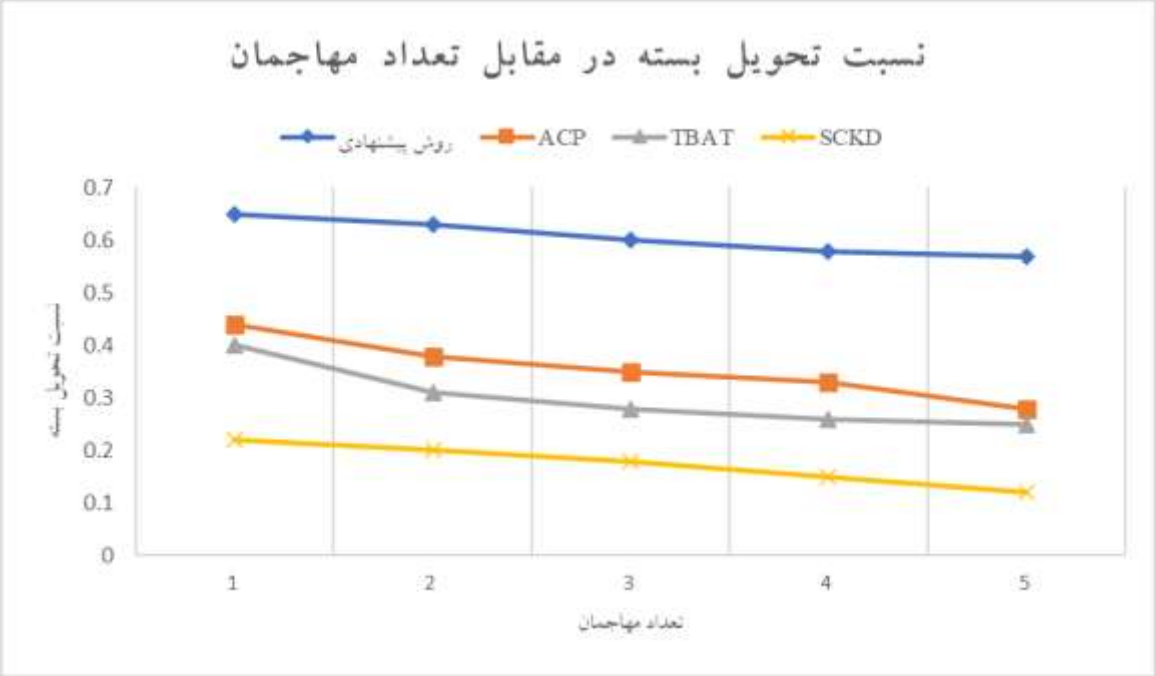
بر طبق نتایج مکسوبه پارامتر سربار کلید روش پیشنهادی به ترتیب میزان ۴۴، ۹۱ و ۳۳۲ درصد برتری نسبت به الگوریتم های TBAT،ACP و SCKD را دارا می باشد. دلیل برتری روش پیشنهادی از نظر پارامتر تاخیر استفاده بهینه و مناسب از روش خوشه بندی، رمزنگاری و همچنین اتخاذ روش مناسب تبادل اطلاعات با استفاده از الگوریتم نهنگ می باشد.

در جدول ۵ نتایج روش پیشنهادی از نظر نسبت تحویل بسته در مقابل تعداد مهاجمان در کنار نتایج مرجع (,.Latif et al۲۰۲۳) نمایش می دهد.

جدول ۵ نسبت تحویل بسته در مقابل تعداد مهاجمان

الگوریتم ها	تعداد حمله ها				
	۱	۲	۳	۴	۵
روش پیشنهادی	۰/۶۵	۰/۶۳	۰/۶	۰/۵۸	۰/۵۷
ACP	۰/۴۴	۰/۳۸	۰/۳۵	۰/۳۳	۰/۲۸
TBAT	۰/۴	۰/۳۱	۰/۲۸	۰/۲۶	۰/۲۵
SCKD	۰/۲۲	۰/۲	۰/۱۸	۰/۱۵	۰/۱۲

بر طبق نتایج کسب شده در فرآیند شبیه سازی و بر اساس جدول ۴-۴، در شکل ۱۲ نسبت تحویل بسته در مقابل تعداد مهاجمان روش پیشنهادی با روش های موجود در مرجع (,.Latif et al۲۰۲۳) نمایش داده شده است.



شکل ۱۲ نسبت تحویل بسته

بر طبق نتایج مکسوبه پارامتر نسبت تحویل بسته روش پیشنهادی به ترتیب میزان ۴۱، ۵۰ و ۷۱ درصد برتری نسبت به الگوریتم های TBAT،ACP و SCKD را دارا می باشد. دلیل برتری روش پیشنهادی از نظر پارامتر تاخیر استفاده بهینه و مناسب از روش خوشه بندی، رمزنگاری و همچنین اتخاذ روش مناسب تبادل اطلاعات با استفاده از الگوریتم نهنگ می باشد.

بر اساس نتایج کسب شده که در شکل های ۹، ۱۰، ۱۱ و ۱۲ به تصویر کشیده شده است روش پیشنهادی به علت استفاده بهینه از روش خوشه بندی، رمزنگاری بهینه و همچنین اتخاذ روش مناسب تبادل اطلاعات با استفاده از الگوریتم نهنگ از برتری محسوسی نسبت به روش های موجود در مرجع (,.Latif et al۲۰۲۳) برخوردار است.

ما در آزمایش خود که در محیط شبیه سازی OMNET++ انجام گردید در شکل ۹ تأخیر احراز هویت در مقابل تعداد مهاجمان را محاسبه کردیم. نتایج کسب شده شکل ۹ نشان می دهد که روش پیشنهادی از نظر میزان تاخیر برتری محسوسی بر روش های مرجع (,.Latif et al۲۰۲۳) دارد. همچنین نتایج شبیه سازی انجام شده از نظر دقت تشخیص در مقابل تعداد مهاجمان که در شکل ۱۰ ارائه شده است نیز نشان می هد که روش پیشنهاد شده به دلیل انجام خوشه بندی دقیق، امنیت مناسب با راهکار رمزنگاری و همچنین استفاده مناسب از الگوریتم نهنگ نسبت به روش های مرجع (,.Latif et al۲۰۲۳) برتری محسوسی را دارد. همچنین ما سربار کلید در مقابل تعداد مهاجمان را در نرم افزار شبیه سازی محاسبه و نتایج آن را در شکل ۱۱ به تصویر کشیده ایم. نتایج کسب شده نشان از برتری روش پیشنهادی نسبت به روش های مرجع (,.Latif et al۲۰۲۳) دارد که دلیل برتری خوشه بندی بهینه و دقیق، رمزنگاری امن و تبادل اطلاعات با استفاده از الگوریتم نهنگ است. نتایج کسب شده فرآیند شبیه سازی از نظر پارامتر نسبت تحویل بسته در مقابل تعداد مهاجمان در شکل ۱۲ نشان می دهد که فرآیند پیشنهادی برتری محسوسی نسبت به روش های مرجع (,.Latif et al۲۰۲۳) دارد.

بحث و نتیجه‌گیری

در فاز اول خوشه بندی خودروها با استفاده از یک رهیافت بهینه انجام گرفته است. استفاده از RSU به عنوان سرخوشه تا حد بسیار زیادی تاخیر، دقت، سربار کلید و نرخ تحویل بسته را بهبود بخشیده است. اما خوشه بندی به تنهایی جوابگو حل چالش ها نیست.

همچنین امنیت به عنوان یک چالش بسیار مهم مطرح می باشد. جهت حل چالش امنیتی فاز دوم ارائه گردید. اما در نهایت جهت تبادل اطلاعات سیستم به یک روش بهینه جهت تبادل اطلاعات نیازمند است. استفاده از الگوریتم نهنگ فرآیند تبادل اطلاعات را تسریع، دقیق و بهینه می کند.

منابع

Bavalatti, A., & Sutagundar, A. V. (2017). Multi-agent based stable clustering in VANET. 2017 International Conference on Smart Technologies for Smart Nation (SmartTechCon),

Gao, Z., Xu, X., Hu, Y., Wang, H., Zhou, C., & Zhang, H. (2023). Based on Improved NSGA-II Algorithm for Solving Time-Dependent Green Vehicle Routing Problem of Urban Waste Removal with the Consideration of Traffic Congestion: A Case Study in China. *Systems*, *11*(4), 173.

Goyal, A. K., Agarwal, G., Tripathi, A. K., & Sharma, G. (2022). 3 SystematicofVANET Study. *Green Computing in Network Security: Energy Efficient Solutions for Business and Home*, 33.

Hamdi, M. M., Audah, L., Rashid, S. A., Mohammed, A. H., Alani, S., & Mustafa, A. S. (2020). A review of applications, characteristics and challenges in vehicular ad hoc networks (VANETs). 2020 international congress on human-computer interaction, optimization and robotic applications (HORA),

Hamzah, M., Islam, M. M., Hassan, S., Akhtar, M. N., Ferdous, M. J., Jasser, M. B., & Mohamed, A. W. (2023). Distributed Control of Cyber Physical System on Various Domains: A Critical Review. *Systems*, *11*(4), 208.

Hsieh, F.-S. (2023). Improving Acceptability of Cost Savings Allocation in Ridesharing Systems Based on Analysis of Proportional Methods. *Systems*, *11*(4), 187.

Jithendra, H., & Rekha, D. (2022). Secured Trusted Authentication with Trust-Based Congestion Scheme for V2V Communication. *Cloud and Fog Computing Platforms for Internet of Things*, 157-168.

Latif, R. M. A., Jamil, M., He, J., & Farhan, M. (2023). A Novel Authentication and Communication Protocol for Urban Traffic Monitoring in VANETs Based on Cluster Management. *Systems*, *11*(7), 322.

Lim, K., Tuladhar, K. M., & Kim, H. (2019). Detecting location spoofing using ADAS sensors in VANETs. 2019 16th IEEE annual consumer communications & networking conference (CCNC),

Mirjalili, S., & Lewis, A. (2016). The whale optimization algorithm. *Advances in engineering software*, *95*, 51-67.

Panigrahy, S. K., & Emany, H. (2023). A survey and tutorial on network optimization for intelligent transport system using the internet of vehicles. *Sensors*, *23*(1), 555.

Sharma, S. K., Rao, R. S., Singh, P., & Khan, S. A. (2022). Evaluation of VANETs routing protocols for data-based smart health monitoring in intelligent transportation systems. *International Journal of Mathematical, Engineering and Management Sciences*, *7*(2), 211.

Shen, X., Lu, Y., Zhang, Y., Liu, X., & Zhang, L. (2022). An Innovative Data Integrity Verification Scheme in the Internet of Things assisted information exchange in transportation systems. *Cluster Computing*, *25*(3), 1791-1803.

Singh, M., Kumar, C., & Nath, P. (2020). P2P Applications in 4G/5G Networks Using D2D Communication Based on Social Attributes of Users. 2020 Fourth World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4),

Tao, J., Ma, J., Keranen, M., Mayo, J., Shene, C.-K., & Wang, C. (2014). RSAvisual: a visualization tool for the RSA cipher. Proceedings of the 45th ACM technical symposium on Computer science education,