Quarterly Journal of Defense Technology Engineering Imam Ali University

Summer 2025, Vol. 40

Original Research

Gray wolf attack method using artificial neural network algorithm to enemy communication centers

Alireza rezaei [1], Seyed roohlah mirakbari[2] , Mehrdad kamarabi [3]

[1] Electrical Engineering Instructor, Faculty of Engineering and Flight, Imam Ali University, Tehran, Iran

[2] M.Sc. in Electrical Engineering, Faculty of Engineering and Flight, Imam Ali University, Tehran, Iran

[3] M.Sc. in Electrical Engineering, Faculty of Engineering and Flight, Imam Ali University, Tehran, Iran

ARTICLE INFO

Received: 2025.01.18

Accepted: 2025.02.15

Published: 2025.03.18

Keyword:

Artificial neural network
wireless network
security
gray wolf attack

***Corresponding Author:**

Alireza rezaei

Email:

alirezarezaei.543210@gmail.com

ABSTRACT

Artificial intelligence, as one of the top emerging technologies, occurs when a device becomes fully aware of its actions, has the ability to be intelligent, can store information, learn, make decisions, and take initiative.

One of the communication methods in which the artificial neural network algorithm can be well embedded is wireless communication networks. These networks have found many users due to their dynamic nature resulting from the random movement of nodes and the use of wireless communication, and also due to their advantages such as covering wider areas.Therefore, for the communication of command and control centers that need to store information, make the right decision and take initiative, the mentioned advantages of wireless communication networks and the characteristics of the artificial neural network algorithm are very suitable for the communication of command and control centers. However, the security of the communication of command-and-control centers in wireless networks against attacks becomes much more complex and vulnerable due to the dynamics of the network and the use of wireless communication. It is in the gray wolf attack method that the wireless network is penetrated using mathematical models. If the artificial neural network algorithm is used, it becomes easier to penetrate and disrupt the enemy's communication systems. In this research, the network security of the enemy's command and control centers is simulated using the artificial neural network algorithm and the gray wolf attack method

فصل نامه مهندسی فناوری‌های دفاعی دانشگاه افسری امام علی (ع)

زمستان 1403 ، دوره 40

مقاله پژوهشی

روش حمله گرگ خاکستری با استفاده از الگوریتم شبکه عصبی مصنوعی به مراکز ارتباطی دشمن

علیرضا رضائی[1]* ، سید روح‌الله میراکبری[2]، **مهرداد کمر آبی[3]**

[1] مربی مهندسی برق، دانشکده مهندسی و پرواز ، دانشگاه امام علی (ع)، تهران، ایران

[2] کارشناس ارشد مهندسی برق ، دانشکده مهندسی و پرواز ، دانشگاه امام علی (ع)، تهران، ایران

[3] کارشناس ارشد مهندسی برق ، دانشکده مهندسی و پرواز ، دانشگاه امام علی (ع)، تهران، ایران

اطلاعات مقاله

دریافت مقاله: 1403/10/30

پذیرش مقاله: 1403/12/04

انتشار مقاله: 1403/12/28

کلید واژگان:

شبکه عصبی مصنوعی

شبکه بی‌سیم

امنیت

حمله گرگ خاکستری

***نویسنده مسئول**

علیرضا رضائی

پست الکترونیکی:

alirezarezaei.543210@gmail.com

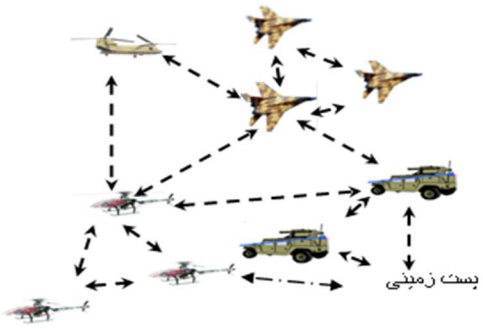
چکیده

هوش مصنوعی به عنوان یکی از برترین فناوری های نوظهور، زمانی اتفاق می‌افتد که یک دستگاه کاملا از اعمال خود آگاه شود، توانایی خردمندی را داشته باشد، بتواند اطلاعات را ذخیره کند، یاد بگیرد، تصمیم بگیرد و ابتکار عمل خود را داشته باشد.

یکی از روش‌های ارتباطی که می‌توان الگوریتم شبکه عصبی مصنوعی را در آن به خوبی بسترسازی کرد شبکه‌های ارتباطی بی‌سیم می‌باشند. این شبکه‌های به علت ماهیت پویایی که در نتیجه حرکت تصادفی گره‌ها و استفاده از ارتباط بی‌سیم، حاصل می‌شود و همچنین با توجه به مزایای آن مانند تحت پوشش قرار دادن مناطق گسترده‌تر، کاربرهای بسیاری پیدا کرده است. لذا برای ارتباط مراکز فرماندهی و کنترل که نیاز به ذخیره اطلاعات، اخذ تصمیم درست و ابتکار عمل دارند، مزایای ذکر شده شبکه‌های ارتباطی بی‌سیم و ویژگی‌های الگوریتم شبکه عصبی مصنوعی برای ارتباطات مراکز فرماندهی و کنترل بسیار مناسب است. ولی امنیت ارتباط مراکز فرماندهی و کنترل در شبکه‌های بی‌سیم در مقابل حملات، بعلت پویایی شبکه و استفاده از ارتباط بی‌سیم بسیار پیچیده‌تر و آسیب‌پذیر می‌شود. در روش حمله گرگ خاکستری است که با استفاده از مدل‌های ریاضی به شبکه بی‌سیم نفوذ می‌کند اگر از الگوریتم شبکه عصبی مصنوعی استفاده شود، نفوذ و مختل‌کردن سیستم‌های ارتباطی دشمن آسان‌تر می‌شود. در این تحقیق امنیت شبکه مراکز فرماندهی و کنترل دشمن با استفاده از الگوریتم شبکه عصبی مصنوعی و روش حمله گرگ خاکستری شبیه‌سازی می‌شود.

1- مقدمه

شبکه بی‌سیم را به صورت یک مدل شبکهٔ بی‌سیم سیار در نظر گرفته می‌شود. در این مدل، هر گره مطابق شکل شمارهٔ 1 به صورت یک گره بی‌سیم سیار است که می‌تواند به طور پویا در هر نقطه از فضای شبکه، بدون استفاده از ساختار مرکزی و زمینی، عملیات ارتباط و مسیریابی را بین مراکز کنترل انجام دهد و آزادانه بر اساس مقتضیات عملیات، جابجا شده و به عنوان میزبان برای تبادل فرامین یا به عنوان مسیریاب فعالیت نماید



شکل1- شبکهٔ ارتباطی بی‌سیم در یک طرح عملیاتی

مسیریابی در مدل شبکهٔ بی‌سیم سیار با استفاده از الگوریتم تک مسیریابی یا الگوریتم چند مسیریابی انجام می‌شود. دستگاه‌های بی‌سیم که از پروتکل‌های تک‌مسیریابی استفاده می‌کنند فقط یک مسیر را در نظر می‌گیرند، با از بین رفتن مسیر ارتباط بین مبدا و مقصد قطع می‌شود و باید دوباره فرآیند مسیریابی انجام شود که این کار، کارایی شبکه را کاهش می‌دهد. برای مثال از نظر امنیتی، اگر کنترل مسیر دست مهاجم بیفتد، ترافیک را به راحتی در دست می‌گیرد یا می‌تواند ارتباط را قطع کند. دستگاه‌های بی‌سیم که از پروتکل‌های تک‌مسیریابی استفاده می‌کردند در ابتدا برای شبکه‌های بی‌سیم سیار مفید به نظر می‌رسیدند، ولی با آشکار شدن نقاط ضعف آنها به ویژه از نظر امنیتی، طراحان مجبور شدند که برای رفع نقاط ضعف آنها پروتکل‌های چند مسیریابی را طراحی کنند.

دستگاه‌های بی‌سیم که از پروتکل‌های چند مسیریابی استفاده می‌کنند می‌توانند به کشف یک یا چند مسیر فعال برای ایجاد ارتباط اقدام می‌کنند. این دستگاه‌های بی‌سیم قادر هستند با توجه به شرایط محیطی مانند ازدحام، محدودیت توان ارسال، حملات و غیره خود را با شرایط وفق دهند و مسیر جانشین بهتری را با توجه به شرایط جایگزین کنند (Nasipuri.A,2006)

2- انواع حملات

الف) تقسیم‌بندی کلاسیک

در این تقسیم‌بندی حملات به دو نوع زیر تقسیم و نام گذاری می‌شوند:

1) حملات فعال:

که در آنها گره بدرفتار برای اجرای تهدید خودش باید هزینه‌ی انرژی آن را بپردازد. چنین گرهی اصطلاحاً گره مخرب یا بداندیش نامیده می‌شود. هدف از انجام این حمله گسستگی شبکه یا ضرر رساندن به گره‌های دیگر است.

2) حملات غیرفعال:

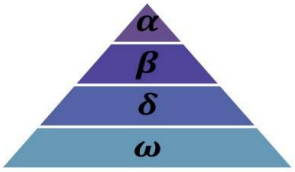
که در آنها گره نامطلوب به قصد ذخیره انرژی از همکاری امتناع می‌کند. هدف از انجام این حمله کاهش عملکرد شبکه یا تقسیم شبکه با شرکت نکردن در عملیات‌ها است.

ب) تقسیم‌بندی غیر کلاسیک

از دیدگاهی دیگر می‌توان حملات را به سه بخش زیر تقسیم کرد که هر کدام از این بخشها را می‌توان جزئی از حمله‌ی فعال ذکر شده در بخش قبل نیز محسوب کرد .(Ali Ghaffari. 2020)

3- روش حمله گرگ خاکستری

در جنگ کسانی که اول حرکت کند و زمان و مکان و وسیله تهاجم خود را انتخاب کند پیروز میدان است. همچنین با شناسایی اهداف و تمرکز بر روی اهداف موثرتر اقدامات خود را پیاده‌سازی می‌کنند. گرگ‌های خاکستری بیشتر ترجیح می‌دهند به‌صورت گروهی زندگی کنند. اندازه گروه به طور متوسط بین 5 تا 12 نفر است. آنها یک سلسله مراتب بسیار سخت غالبِ اجتماعی دارند که در شکل شماره (2) نشان داده شده است. رهبران گروه یک جنس نر و یک ماده هستند که آلفا نامیده می‌شوند. آلفا عمدتاً مسئول تصمیم‌گیری در مورد شکار، محل خواب، زمان بیداری و غیره هستند. تصمیمات آلفا به گروه دیکته شده است؛ بااین‌حال نوعی رفتار دموکراتیک نیز مشاهده شده است که در آن یک آلفا از دیگر گرگ‌های گروه پیروی می‌کند. با توجه به این که دستورات آلفا باید توسط گروه پیروی شود، گرگ آلفا را گرگ غالب نیز می‌نامند. (a. h. Gandomi,2021).



شکل شماره 2: سلسله مراتب گرگ خاکستری سلطه از بالا به پایین کاهش می یابد.

سطح دوم در سلسله‌مراتب گرگ‌های خاکستری، بتا است. گرگ‌های بتا، گرگ‌های زیردست هستند که به آلفا در تصمیم‌گیری‌ها یا فعالیت‌های دیگر گروه کمک می‌کنند. گرگ بتا دستورات آلفا را در سراسر گروه اجرا کرده و بازخورد آن را به آلفا ارجاع می‌دهد. پایین‌ترین رتبه را در گرگ‌های خاکستری، امگا دارد. امگا نقش قربانی را بازی می‌کند. گرگ امگا همیشه باید مطیع دیگر گرگ‌های غالب باشد. مراحل اصلی شکار گرگ‌های خاکستری به شرح زیر است:

* ردیابی، تعقیب و نزدیک شدن به طعمه.
* تعقیب، محاصره و آزار طعمه تا زمانی که از حرکت بازایستد.
* حمله به سمت طعمه.

این مراحل در شکل شماره (3) نشان داده شده‌اند. در ادامه، این روش شکار و سلسله مراتب اجتماعی گرگ‌های خاکستری به منظور طراحی و انجام بهینه‌سازی، به‌صورت ریاضی مدل شده است.



شکل3- رفتار شکار گرگ‌های خاکستری: (الف) تعقیب، نزدیک شدن و ردیابی طعمه، (ب)، (ج)،)(د) تعقیب، محاصره و آزار طعمه

و (ه) وضعیت ثابت و حمله،

2-2- مدل ریاضی و الگوریتم GWO

در این بخش مدل‌های ریاضی مربوط به سلسله مراتب اجتماعی، ردیابی، محاصره و حمله به طعمه ارائه شده است. سپس الگوریتم GWO مربوطه مشخص می‌شود.

2-3 سلسله مراتب اجتماعی

در هنگام طراحی، به‌منظور مدل‌کردن ریاضی سلسله‌مراتب اجتماعی گرگ‌ها مناسب‌ترین راه‌حل را به‌عنوان آلفا در نظر می‌گیریم. درنتیجه از بین بهترین راه‌حل‌ها، دومین و سومین آن‌ها را بتا و دلتا نام‌گذاری می‌کنیم. مابقی راه‌حل‌های کاندید شده امگا در نظر گرفته می‌شوند. در الگوریتم، فرایند شکار (بهینه‌سازی) توسط β، α و δ هدایت می‌گردد. گرگ‌های ω از این سه گروه پیروی می‌کنند.

2-4 محاصره طعمه

همان‌طور که در بالا ذکر شد، گرگ‌های خاکستری طعمه را در طول شکار محاصره می‌کنند. به منظور مدل‌کردن این رفتار محاصره به صورت ریاضی، معادلات زیر ارائه شده‌است.

$$\vec{D} = |\vec{C}.\vec{X}_p(t) - \vec{X}(t)| \quad (1\text{-}2)$$

$$\vec{X}(t+1) = \vec{X}_p(t) - \vec{A}.\vec{D} \quad (2\text{-}2)$$

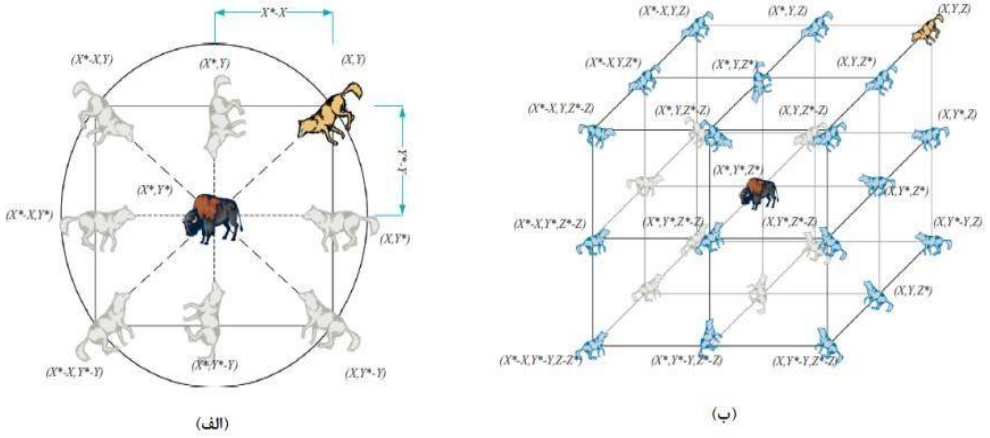
در معادلات فوق، t مبین تعداد تکرار فعلی است. A و C مبین بردارهای ضریب، X p مبین بردار موقعیت شکار و X مبین بردار موقعیت یک گرگ خاکستری است. بردارهای A وC به‌صورت زیر محاسبه می‌شوند:

$$\vec{A} = 2\vec{a}.\vec{r}_1 - \vec{a} \quad (3\text{-}2)$$

$$\vec{C} = 2\vec{r}_2 \quad (4\text{-}2)$$

در معادلات فوق، a در طول تکرار به‌صورت خطی از 2 تا صفر کاهش می‌یابد.

متغیرهای r_2 و r_1 مبین بردارهای تصادفی در بازه محدود هستند. برای دیدن نتایج معادلات، معادلات فوق به همراه یک بردار مکان دوبعدی و تعدادی همسایگی احتمالی در شکل شماره(4-الف) نشان داده شده‌اند.



شکل شماره4: بردارهای مکان دوبعدی و سه بعدی و موقعیت احتمالی بعدی آن‌ها

همان‌طور که در شکل فوق مشاهده می‌شود یک گرگ خاکستری که در مکان(X,Y) قرار دارد، می‌تواند موقعیت خود را باتوجه‌به موقعیت طعمه (X* ,Y*) عوض کند. مکان‌های مختلف موجود در اطراف بهترین عامل را می‌توان باتوجه‌به موقعیت فعلی آن و تنظیم و تغییر مقدار بردارهای A و C به دست آورد. مکان‌های احتمالی به‌روز شده مربوط به یک گرگ خاکستری در فضای سه‌بعدی در شکل (4-ب) نشان‌داده‌شده است. باید توجه داشت که بردارهای تصادفی r_1,r_2 به گرگ‌ها اجازه دستیابی به هر موقعیتی مابین نقاط نشان‌داده‌شده در شکل را می‌دهند؛ بنابراین یک گرگ خاکستری می‌تواند موقعیت خود را در داخل فضایی که طعمه را دربرگرفته، به‌صورت تصادفی و با استفاده از معادلات زیر تغییر دهد.

همین مفهوم را می‌توان به یک فضای جستجوی n بعدی تعمیم داد. در این حالت گرگ‌های خاکستری پیرامون بهترین راه‌حل به‌دست‌آمده در ابعادی بیشتر از ابعاد مکعب حرکت می‌کنند.

5-2 شکار :

روش گرگ خاکستری برای رسیدن به هدف خود با الگوبرداری از الگوریتم‌های هوش مصنوعی کار خود را آسان‌تر می‌کند. در حمله گرگ خاکستری این توانایی وجود دارد که محل طعمه را تشخیص داده و آن را محاصره کند. روند شکار معمولاً توسط آلفا هدایت می‌شود. گرگ‌های بتا و دلتا نیز گاهی اوقات ممکن است در شکار شرکت کنند. متأسفانه در یک فضای جستجو انتزاعی هیچ ایده‌ای در مورد موقعیت بهینه (طعمه) وجود ندارد. به‌منظور شبیه‌سازی ریاضی رفتار شکار گرگ‌های خاکستری، فرض می‌کنیم آلفا بهترین راه‌حل موجود، بتا و دلتا در مورد مکان بالقوه طعمه آگاهی بهتری دارند؛ بنابراین سه تا از بهترین راه‌حل‌های به‌دست‌آمده را ذخیره کرده و دیگر عوامل جستجو

ازجمله گرگ‌های امگا را وادار می‌کنیم تا موقعیت خود را باتوجه‌به موقعیت بهترین عوامل جستجو به‌روزرسانی نمایند. شکل شماره(5) چگونگی به‌روزرسانی موقعیت یک عامل جستجو را در یک فضای جستجوی دوبعدی، باتوجه‌به موقعیت آلفا، بتا و دلتا نشان می‌دهد.

$$\vec{D_\alpha} = |\vec{C_1}.\vec{X_\alpha} - \vec{X}| \quad (2\text{-}5)$$

$$\vec{D_\beta} = |\vec{C_2}.\vec{X_\beta} - \vec{X}| \quad (2\text{-}6)$$

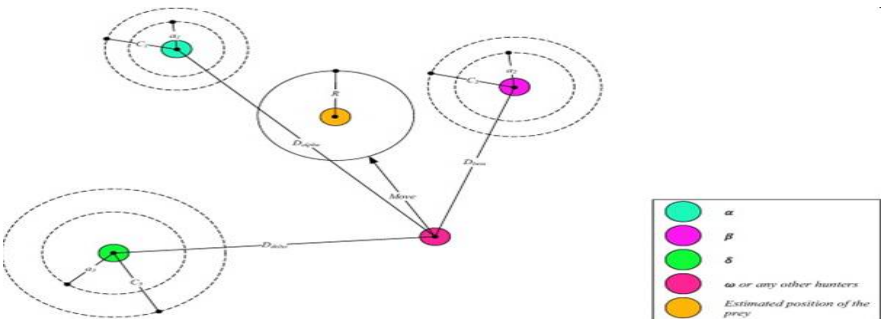
$$\vec{D_\delta} = |\vec{C_3}.\vec{X_\delta} - \vec{X}| \quad (2\text{-}7)$$

$$\vec{X_1} = \vec{X_\alpha} - \vec{A_1}.(\vec{D_\alpha}) \quad (2\text{-}8)$$

$$\vec{X_2} = \vec{X_\beta} - \vec{A_2}.(\vec{D_\beta}) \quad (2\text{-}9)$$

$$\vec{X_3} = \vec{X_\delta} - \vec{A_3}.(\vec{D_\delta}) \quad (2\text{-}10)$$

$$\vec{X}(t+1) = \frac{\vec{X_1} + \vec{X_2} + \vec{X_3}}{3} \quad (2\text{-}11)$$



شکل شماره 5: به روز رسانی موقعیت در الگوریتم GWO

مشاهده می‌شود که موقعیت نهایی حاصل شده در مکانی تصادفی و در داخل دایره‌ای قرار دارد که باتوجه به موقعیت آلفا، بتا و دلتا تعریف شده است. به عبارت دیگر استفاده از الگوریتم‌های هوش مصنوعی، آلفا، بتا و دلتا موقعیت شکار را بهتر برآورد می‌کنند و دیگر گرگ‌ها موقعیت خود را به‌صورت تصادفی در ناحیه اطراف شکار به‌روزرسانی می‌نمایند (a. h. Gandomi,2021).

6-2 - الگوریتم شبکه عصبی مصنوعی

الگوریتم شبکه عصبی مصنوعی یک مدل یادگیری ماشین از مغز انسان هست. که اجزای اصلی آن گره‌ها، وزن‌ها، بایاس و تابع فعال سازی هست.

مرحله اول: گره‌ها در هر لایه انتخاب بطوریکه به لایه قبلی و بعدی متصل هستند سپس به ارتباط بین گره‌ها، وزن داده می‌شود، که میزان اهمیت سیگنال‌ها را مشخص می‌کند.

مرحله دوم: ورودی‌ها در وزن‌ها ضرب می‌شوند و سپس تابع فعال‌سازی اعمال می‌شود. نتایج به لایه بعدی منتقل می‌شوند تا به خروجی برسند.

$$Z = \sum (X_i \times W_i)$$

$$a = F(a)$$

مرحله سوم : با استفاده از تابع هزینه تفاوت خروجی پیش‌بینی شده و واقعی محاسبه می‌شوند.

$$E = = \frac{1}{n}\sum_{i=0}^{n}(y_i - \hat{y}_i)^2$$

مرحله چهارم : خطا از خروجی‌ها فیدبک، گرفته می‌شود و با استفاده از گرادیان نزولی اصلاح می‌شوند. $W=W-\eta*\frac{dE}{dW}$

مرحله پنجم : فرایند فوق برای تمام داده‌ها چندین بار تکرار می‌شود تا خطا کاهش یابد (kwon, D and Kim, G,2017).

7-2 -نحوه حمله گرگ خاکستری به مراکز فرماندهی و کنترل شبکه‌های بی‌سیم بـا اسـتفاده از الگوریتم‌های هوش مصنوعی

در جنگ، برای فریب دشمن و کسب اطلاعات، تمرکز بر روی ارتباط و داده‌های ارسالی است. اگر بتوانیم به اهداف خود برسیم کارایی مراکز فرماندهی و کنترل را کاهش و افکار و اهداف خود را به سیستم تحمیل می‌کنیم. لذا از ضروریات مراکز فرماندهی و کنترل داشتن ارتباط سالم و امن با زیر مجموعه، رده بالاتر یا همتراز است و این ارتباط زمانی که عناصر شبکه متحرک می‌شوند اهمیت بیشتری پیدا می‌کند لذا استفاده از یک شبکهٔ بی‌سیم سیار، علاوه بر آسیب‌پذیری ارتباطات بی‌سیم، مشکلات امنیتی خاص مانند وجود گره‌های متخاصم و بسته‌های داده دروغین را نیز دارد.

گروه گرگ‌های خاکستری برای یافتن نقاط ضعف شبکه به شرح ذیل عمل می‌کند:

1) حمله به گره‌های بحرانی که برای از کار انداختن مسیرهای ارتباطی استفاده می‌شود

2) با انتخاب بهترین موقعیت برای عناصر خود در شبکه بی‌سیم، شناسایی مراکز فرماندهی و کنترل و ارسال داده‌های غلط به مرکز آسیب‌پذیر، سعی می‌نماید کنترل ارتباط مرکز با زیر مجموعه، رده بالاتر یا همتراز بدست آورد.
3) استفاده از حمله سیاه چاله، که در این حمله گره خرابکار همه داده‌ها را به سمت خود جذب می‌کند.

امنیت لازم برای عملکرد درست اعمال شبکه، توسط گروه گرگ خاکستری با مخاطره مواجه می‌شود بنابراین بدون امنیت، تضمینی برای انجام صحیح این اعمال وجود ندارد و به راحتی می‌توانند یکپارچگی شبکه را بر هم بزنیم.

اعضا گروه گرگ خاکستری در ابتدا با در نظر گرفتن موقعیت گرگ آلفا، موقعیت خود را در شبکه مشخص کرده و در بین عناصر ارتباطی مراکز فرماندهی و کنترل خود را جا می‌دهند و با حرکت گره‌های شبکه هماهنگ می‌شوند. با دریافت داده در حال تبادل در شبکه، اطلاعات و داده‌ها را تجزیه و تحلیل می‌کنند و آنها را به گرگ آلفا گزارش می‌نمایند. در مرحله بعد تبادل اطلاعات گروه گرگ خاکستری به نتیجه‌گیری مناسب منجر می‌شود و یک هدف مناسب تعیین می‌شود، هدف یکی از مراکز فرماندهی و کنترل است.

عناصر گروه گرگ خاکستری با محاصره این مرکز و قرار گرفتن در خطوط ارتباطی آن با دیگر مراکز فرماندهی و کنترل، سعی در بدست آوردن کنترل ارتباط مرکز مورد نظر می‌شوند. در ابتدا با ایجاد اختلال در ارتباط مرکز، ارتباط آنرا با دیگر عناصر شبکه قطع می‌کنند و سپس با بدست آوردن کنترل ارتباط مرکز می‌تواند داده‌ها و اطلاعات خود را جایگزین اطلاعات درست کند و اهداف خود را در شبکه اعمال نماید.

الگوریتم شبکه عصبی مصنوعی با الگوریتم گرگ خاکستری به خوبی تلفیق می‌شود، زیرا قادر به یادگیری، پیش‌بینی الگو رفتاری گره‌ها و شناسایی گره‌های آسیب‌پذیر است.

در این حمله تلفیقی وظیفه شبکه عصبی تحلیل سیگنال‌های بی سیم و تشخیص نوع سیگنال است. الگوریتم شبکه عصبی مصنوعی ضمن پیش‌بینی الگوی استفاده دشمن از فرکانس یا زمانبندی، بهترین روش حمله را انتخاب می‌کند. دشمن برای جلوگیری از شناسایی نوع ارتباط خود از تکنیک‌های پرش فرکانسی، رمزنگاری زمانی یا ارسال تصادفی استفاده می‌کند. تشخیص اینکه دشمن در چه زمانی و در چه فرکانسی پیام ارسال می‌کند کار نفوذ به شبکه ارتباطی دشمن را برای ما راحتر می‌کند. الگوریتم حمله گرگ خاکستری فرآیند آموزش خود را با شبکه عصبی مصنوعی ارتقاء داده و در یافتن بهترین وزن‌ها و بایاس‌ها (با کمترین خطا) برای تشخیص یا پیش‌بینی به شبکه عصبی مصنوعی کمک می‌کند و با بهینه‌سازی تابع هزینه شبکه، دقت حمله افزایش می‌یابد.

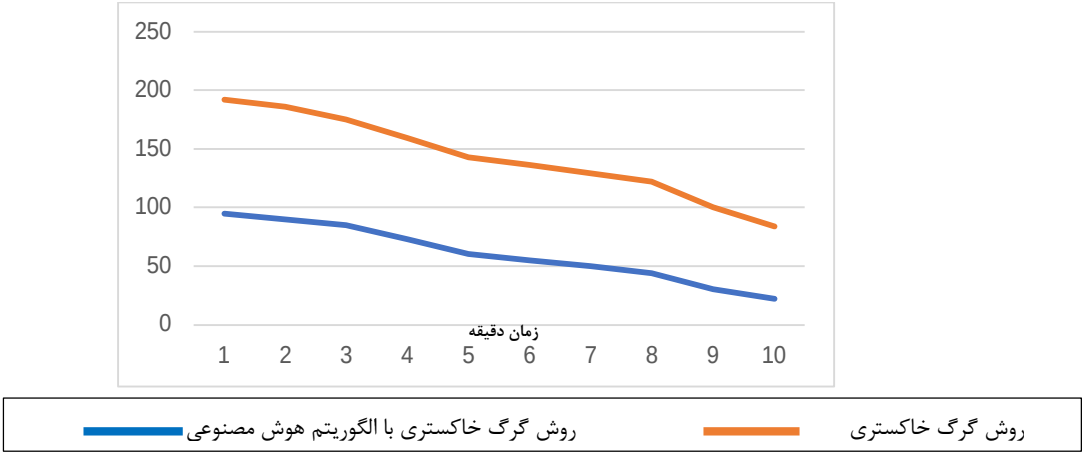
گروه گرگ‌های خاکستری با استفاده از الگوریتم‌های هوش مصنوعی و ایجاد مشکل امنیتی که در

ارتباط بی‌سیم بین مراکز فرماندهی و کنترل ایجاد شده است، می‌تواند در بین ارتباط دو مرکز فرماندهی مبدأ و مقصد قرار گیرد و خواسته‌های خود را اعمال نمایند و کل شبکه را به اهداف و نتایج خطا و غلط هدایت کنند. الگوریتم هوش مصنوعی خطاهای روش گرگ خاکستری را سریعتر تصحیح، اتخاذ تصمیم مناسب را آسان‌تر می‌کند.

4- شبیه‌سازی و تحلیل نتایج

در جنگ‌ها، ابتدا جامعه هدف کاملا شناسایی و سپس برنامه‌ریزی و ابزارهای مناسب برای رسیدن به هدف مهیا می‌شود تا نتیجه مطلوب بدست آید. بنابراین در این تحقیق شبکه هدف، شبکه بی‌سیم دشمن است. لذا در شبیه‌سازی شبکه بی‌سیم ، از ابزار شبیه‌سازی NS2 استفاده شده و محیط شبیه‌سازی در وسعت 300 x300 متر مربع در نظر گرفته شده است که شامل 30 گره که در کل شبکه پخش شده است. شبکه عصبی تحلیل سیگنال‌های بی سیم و تشخیص نوع سیگنال را انجام می‌دهد. تشخیص اینکه دشمن در چه زمانی و در چه فرکانسی پیام ارسال می‌کند کار نفوذ به شبکه ارتباطی دشمن را ساده‌تر می‌کند. الگوریتم حمله گرگ خاکستری فرآیند یافتن بهترین وزن‌ها و بایاس‌ها (با کمترین خطا) برای تشخیص یا پیش‌بینی با کمک شبکه عصبی مصنوعی سریعتر انجام می‌شود.

ارتباط بی‌سیم در روش گرگ خاکستری با استفاده از الگوریتم شبکه عصبی با افزایش زمان نرخ دریافت بسته‌ها کاهش می‌یابد، اما مهمترین نکته در این روش، استفاده هوشمندانه از امکانات جدید بطوری که هویت مبدا و مقصد در مسیرهای انتخابی با دقت بیشتری انتخاب و برای حمله مورد استفاده قرار می‌گیرد.



شکل شمارهٔ 6: متوسط تحویل بسته‌ها در ارتباط بی‌سیم با روش حمله گرگ خاکستری با الگوریتم هوش مصنوعی

نتایج شبیه‌سازی، متوسط مسیرهای امن پیدا شده، در ارتباط بی‌سیم با الگوریتم چند مسیریابی بین مبدا و مقصد در شرایطی که زمان، افزایش می‌یابد، در شکل شمارهٔ 6 نمایش داده شده است. روش گرگ خاکستری، امنیت ارتباط بی‌سیم بین مبدا و مقصد را با دریافت پیام‌های ارسالی و جایگزینی کلید رمز جعلی، به خطر می‌اندازد. اما دشمن با گذشت زمان سعی در پیداکردن خطوط ارتباطی امن می‌گردد تا ضعف خود را جبران نمایند

در روش گرگ خاکستری با استفاده از شبکه عصبی مصنوعی، پیام‌ها جعلی در دستگاه‌های بی‌سیم با قابلیت الگوریتم چند مسیریابی، بر روی چندین مسیر بارگذاری می‌شوند. برای شناسایی نقاط ضعف امنیتی شبکه الگوریتم‌های هوش مصنوعی به کمک روش مذکور می‌آید. طبیعتاً عدم توفیق در انتقال داده‌ها منجر به ارسال مجدد می‌شود که باعث افزایش سربار می‌گردد یا حتی منجر به عدم موفقیت در انتقال بسته، افت در عملکرد شبکه و جستجو برای دستهٔ مسیر جدید نیز می‌شود.

در روش ارئه شده همانطور که در شکل شماره (6) مشاهده می‌شود با گذشت زمان، کارایی شبکه دشمن کم می‌شود و متوسط داده‌های درست رسیده به مقصد، کاهش می‌یابد. گذشت زمان باعث افزایش دقت حمله به مسیرهای ارتباطی بی‌سیم امن دشمن می‌شود. در حالی که استفاده تنها از حمله الگوریتم گرگ خاکستری به نفع دشمن است زیرا با گذشت زمان نقاط ضعف خود را اصلاح می‌کند.

5- نتیجه‌گیری

جنگ‌های امروزی به شدت به فناوری ارتباطی و اطلاعاتی جدید متکی است. لذا تمرکز اولیه بر تضعیف همکاری و ارائه اطلاعات نادرست است. یکی از بهترین راه‌های برای رسیدن به هدف، شبکه‌های بی‌سیم مراکز فرماندهی و کنترل است. شبکه‌های بی‌سیم که به علت ماهیت پویایی که در نتیجه حرکت تصادفی گره‌ها و استفاده از ارتباط بی‌سیم، حاصل می‌شود و همچنین با توجه به مزایای آن مانند تحت پوشش قرار دادن مناطق گسترده‌تر، کاربرهای بسیاری پیدا کرده است. با توجه به ماهیت پویایی که در نتیجه حرکت تصادفی گره‌ها در ارتباط بی‌سیم، حاصل می‌شود، امنیت کانال و ارتباط مرکز بیشتر مورد تهدید متخاصم قرار می‌گیرد.

در جنگ کسانی که اول حرکت کند و زمان و مکان و وسیله تهاجم خود را انتخاب کند پیروز میدان است. همچنین با شناسایی اهداف و تمرکز بر روی اهداف موثرتر اقدامات خود را پیاده‌سازی می‌کنند. در جنگ‌های برای جلوگیری از دریافت داده‌های نادرست، باید داده‌ها از راه‌های مختلف، و مجاز اخذ و پس از تطبیق اطلاعات، اطلاعات یا داه‌ها تحلیل و تجزیه شوند. در روش گرگ خاکستری با استفاده از الگوریتم هوش مصنوعی، پیام‌ها جعلی در دستگاه‌های بی‌سیم با قابلیت الگوریتم چند مسیریابی، بر روی چندین مسیر بارگذاری می‌شوند. برای شناسایی نقاط ضعف امنیتی شبکه

الگوریتم‌های هوش مصنوعی به کمک روش مذکور می‌آید. طبیعتاً عدم توفیق در انتقال داده‌ها منجر به ارسال مجدد می‌شود که باعث افزایش سربار می‌گردد یا حتی منجر به عدم موفقیت در انتقال بسته، افت در عملکرد شبکه و جستجو برای دستهٔ مسیر جدید نیز می‌شود.

بنابراین با روش حمله گرگ خاکستری و الگوریتم شبکه عصبی مصنوعی اطلاعات درستی از توپولوژی شبکه و نقاط ضعف امنیتی شبکه بدست آورد. نتایج شبیه‌سازی، چگونگی نرخ دریافت بسته‌ها را در شرایطی که زمان افزایش می‌یابد. البته لازم به ذکر است اگر تعداد زمان خیلی افزایش پیدا کنند این روش دارای عملکرد مناسبتر می‌شود زیرا سربار دیتاها زیاد شده و باعث کندی سیستم می‌شود. به نظر می‌رسد استفاده از الگوریتم‌های خیلی پیشرفته هوش مصنوعی می‌تواند برای اخلال شبکه دشمن موثرتر واقع شود که لازم است در تحقیق‌های آتی این موضوع مورد بررسی قرار گیرد.

مراجع :

A. Nasipuri and S.R. Das. (2006). "AOMDV: On-Demand Multipath Routing for Mobile AD Hoc Networks" , Proceedings of the 8th Int. CONF. ON Computer Communications and Networks (IC3N), Boston, MA.

Buckley, N.; Nagar, A.; Arumugam,(2013) S. “Evolution of Visual Cryptography Basis Matrices with Binary Chromosomes”; IEEE 8th EUROSIM Congress on Modelling and Simulation.

Shirmarz, Alireza, and Ali Ghaffari. (2020). "Performance issues and solutions in SDN-based data center: a survey." The Journal of Supercomputing 76 (10):7545-7593

, Amir Hossein Gandomi,(2021) Comprehensive Metaheuristics: Algorithms and Applications 1st Edition S Ali Mirjalili

Revenkar, P. S.; Anjum, A.; Gandhare, W(2010). “ urvey of Visual Cryptography chemes”; Int. J. Security and Its Applications, 4, 49-56.

Ateniese, G.; Blundo, C.; De Santis, A.; Stinsonc, D. R.(2001) “E tended Capabilities for Visual Cryptography”; Theoretical Computer Sci., 250, 143-161.

Mirghaderi, A.; Jolfaei, A. (2019)“A Novel Chaotic Image Encryption Scheme Using Chaotic Maps”; Adv. Defence Sci. Technol., 2, 111-124.

kwon, D.; Kim, G. (2017)“survey of deep learing-based network anomaly detection”; cluster computing. vol.. 22, pp, 994-961.