نشریه علمی «پدافند الکترونیکی و سایبری»
سال هفتم، شماره ۱، بهار ۱۳۹۸؛ ص ۱۲۸-۱۱۳

ارائه یک مدل تحلیل رفتار دشمن با استفاده از مدل‌های مخفی مارکوف بر اساس مشاهدات جنگ الکترونیک در صحنه‌های جنگ پیچیده

مرتضی بابائی[1*]، حمیدرضا لشکریان[2]، مجید شیخ‌محمدی[3]

۱- دانشجوی دکتری، دانشگاه جامع امام حسین(ع)، ۲- استادیار، دانشگاه جامع امام حسین(ع)،
۳- استادیار، دانشکده مهندسی صنایع و سیستم‌ها، دانشگاه تربیت مدرس

(دریافت: ۹۶/۱۲/۰۷، پذیرش: ۹۷/۰۳/۰۶)

چکیده

مدل‌سازی، یکی از ابزارهای اساسی در طرح‌ریزی جنگ‌های پیچیده است. جنگ‌های امروزی به‌دلیل پیچیده و پویا بودن صحنه‌ها با جنگ‌های سنتی بسیار متفاوت شده و نیازمند فرماندهی و کنترل چابک و پویا هستند تا بتوانند به‌سرعت در برابر تغییرات صحنه نبرد واکنش نشان داده و تصمیم‌گیری نمایند. در عصر اطلاعات با پیچیده شدن صحنه‌های جنگ و دیجیتالی شدن میدان رزم، مشاهدات فرماندهان با استفاده از سامانه‌های جنگ الکترونیک صورت می‌گیرد. در این مقاله با استفاده از مدل‌های مخفی مارکوف بر اساس مشاهدات جنگ الکترونیک، فرآیند معناسازی محرک‌ها و اقدامات فیزیکی دشمن در صحنه جنگ که بیانگر درک شهودی ما از وضعیت است، مدل شده است. این مدل در تحلیل رفتار دشمن و تعیین مقاصد عملیاتی آن جهت فرآیند تصمیم‌سازی نظامی به‌منظور اتخاذ پاسخ مناسب به دشمن استفاده شده است. برای این منظور یک سناریوی جنگ احتمالی ا. م. آمریکا علیه ج. ا. ایران از منظر جنگ الکترونیک بررسی شده و مبنای این مدل‌سازی قرار گرفته است. مدل مخفی مارکوف مفروض از نوع مرتبه اول و تغییر ناپذیر با زمان درنظر گرفته شده است، بدین معنی که تمام احتمالات توصیف کننده این مدل در طول زمان تغییر نمی‌کنند. نتایج شبیه‌سازی‌ها نشان می‌دهد که این مدل، روش خوبی جهت تعیین مقاصد عملیاتی دشمن و فرآیند تصمیم‌سازی بر اساس مشاهدات جنگ الکترونیک از اقدامات فیزیکی در صحنه‌های جنگ پیچیده می‌باشد.

کلیدواژه‌ها: جنگ الکترونیک، صحنه‌های جنگ پیچیده، فرآیند تصمیم‌سازی، مدل تحلیل رفتار دشمن، مدل‌های مخفی مارکوف

۱- مقدمه

به‌طورکلی، همه عملیات‌های نظامی در سه حوزه اصلی قابل بحث و بررسی هستند: حوزه فیزیکی[1]، حوزه اطلاعاتی[2] و حوزه شناختی[3]. اقدامات عینی، در حوزه فیزیکی رخ می‌دهند، در حوزه اطلاعاتی ردیابی شده و به رده بالاتر گزارش می‌شوند، و در حوزه شناختی نحوه پاسخ به آن اقدامات (توسط فرماندهان در سطوح مختلف) شکل می‌گیرد. فرض وجود این سه حوزه، چارچوب ادراکی مناسبی است برای فهمیدن آنچه بر اثر یک فرآیند متعامل محرک- پاسخ[4] در ذهن انسان و سازمان‌های انسانی شکل می‌گیرد، و این‌که چطور اقدامات فیزیکی در یک حوزه، ممکن است به تأثیرات روانی در حوزه دیگر تبدیل شوند و در نهایت چرخه تصمیم‌سازی (خودی، دشمن و بی‌طرف) را تحت تأثیر خود قرار دهند. آگاهی از این فرآیند بسیار ارزشمند و پراهمیت است، زیرا چگونگی درک افراد و سازمان‌ها نسبت به یک اقدام یا محرک خاص، نحوه پاسخ به آن، و نهایتاً نحوه تغییر رفتار طرف مقابل را بیان می‌کند [۱].

حوزه فیزیکی دربرگیرنده همه محرک‌ها و اقدامات فیزیکی است که عاملی برای بروز تأثیرات فیزیکی و روانی موردنظر محسوب می‌شوند. این اقدامات فیزیکی ممکن است صرف مانور و استقرار تأثیرگذار یک نیروی رزمی در زمان و مکان مناسب باشد. وجود این نیرو ممکن است به‌عنوان یک موضوع و پدیده خارجی مشاهده و گزارش شود، و یا این‌که دست به عملیات زده و به‌عنوان یک حادثه در فضای رزم، تصمیم‌های متعاقب را تحت تأثیر قرار دهد.

حوزه اطلاعاتی شامل همه ابزارها و سازوکار لازم برای آگاهی از پدیده‌ها، حوادث و موقعیتی خاص است. برای مثال در سطح تاکتیکی، این حوزه دربرگیرنده همه عناصر ضروری، ابتدا برای مشاهده فضای رزم و سپس مدیریت اقدامات نیروهای خودی

*رایانامه نویسنده مسئول: mbabaei@ihu.ac.ir

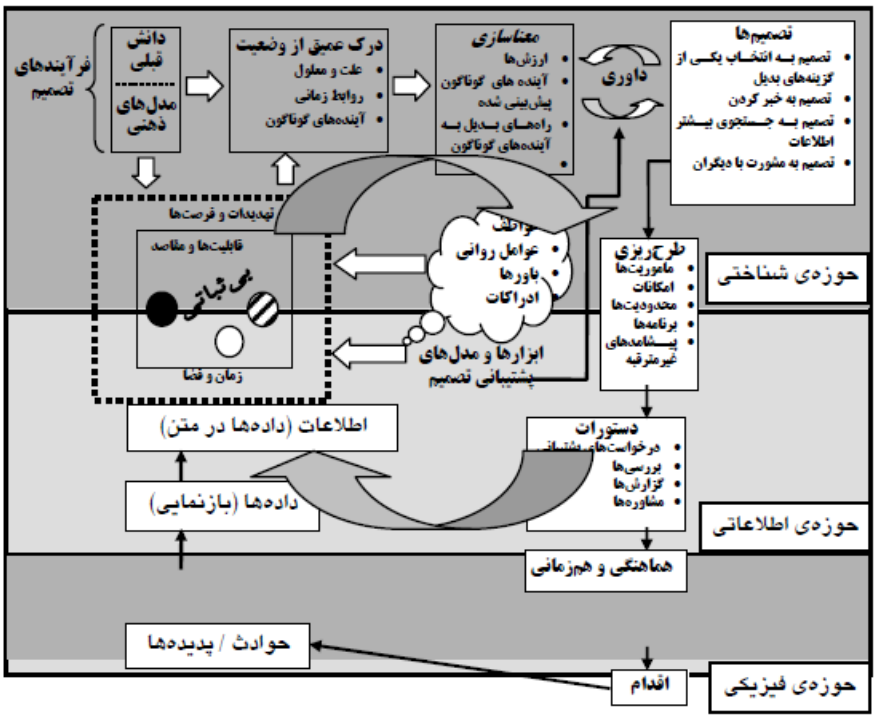
1- Physical Domain
2- Information Domain
3- Cognitive Domain
4- Stimulus-Response Interaction Process

برای نیل به اهداف موردنظر می‌باشد؛ یعنی مجموعه حسگرهای لازم برای مشاهده و جمع‌آوری داده‌ها، از حسگرهای الکترونیکی گرفته تا حسگرهای انسانی [۳-۲].

حوزه شناختی مکان بروز کارکردهایی مانند ادراک حسی، معناسازی، ارزیابی گزینه‌های بدیل، و تصمیم‌گیری در مورد یک راه‌کار است. بخشی از این فرآیند متکی بر استدلال هوشیار (قلمروی تعقل) و بخشی دیگر بر پایه مدل‌های ذهنی نیمه هوشیار (قلمرو باور) انجام می‌گیرد. تعقل و باور، هر دو متأثر از فرهنگ، تحصیلات و تجربه هستند [۳]. از منظر مدل محرک- پاسخ، حوزه شناختی جایی است که محرک‌ها به‌واقع باعث بروز پاسخ و تغییر رفتار می‌شوند.

به بیان دقیق‌تر، انسان یک موقعیت در حال بروز را ادراک می‌کند، آن را در ذهن خود معنامند می‌کند، گزینه‌های بدیل را ارزیابی می‌کند و درنهایت با انتخاب یک راه‌کار خاص تصمیم به اقدام می‌گیرد. بدین ترتیب، دانش قبلی و مدل‌های ذهنی بخش مهمی از زمینه لازم برای معناسازی[1] را فراهم می‌سازند. معناسازی فرآیندی است که طی آن تکه‌های جورچین (اطلاعات در کنار برساخته‌هایی از دانش قبلی، مدل‌های ذهنی، انتظارات، عواطف و ...) در قالب یک سناریو شکل می‌گیرند. این سناریو بیانگر درک شهودی[2] ما از یک وضعیت است. ارزش‌های فرهنگی، آینده‌های گوناگون پیش‌بینی‌شده و نیز راه‌های بدیل به آینده‌های گوناگون از جمله محتویات این سناریو محسوب می‌شوند. درواقع، فرآیند معناسازی مبنایی جهت تعیین راه‌کارهای در دسترس برای انجام پاسخ احتمالی است [۳].

بر اساس فرآیندی که در بالا گفته شد، نهایتاً اقدامات فیزیکی با هدف ایجاد تأثیرات فیزیکی و یا روانی بر دشمن و تغییر رفتار وی هدایت و اجرا می‌شود. درواقع همه فرآیند موردبحث، از اقدامات فیزیکی، تا جمع‌آوری داده‌ها و معناسازی گرفته تا اجرای پاسخ، تنها نیمی از یک چرخه فرضی است که هر طرف به‌نوبت اقدامات دیگری را مشاهده و به آنها پاسخ می‌دهند. بدین ترتیب، اقدامات فیزیکی ایجادشده در فرآیند طرح‌ریزی و اجرا، همان محرک‌هایی هستند که طرف مقابل آنها را مورد مشاهده و بررسی قرار داده و به آنها پاسخ می‌دهد. شکل (۱) این تعامل را به‌خوبی نشان می‌دهد. این چرخه تعاملی را چرخه عمل- عکس‌العمل[3] نیز می‌گویند.



شکل (۱): چرخه عمل- عکس‌العمل [۱]

جنگ‌های امروزی به‌دلیل پیچیده و پویا بودن صحنه‌ها با جنگ‌های سنتی بسیار متفاوت شده و نیازمند فرماندهی و کنترل چابک و پویا هستند تا بتوانند به‌سرعت در برابر تغییرات صحنه نبرد واکنش نشان داده و تصمیم‌گیری نمایند. در گذشته‌ای دور، فرماندهان نظامی برای مشاهده صحنه نبرد و عملکرد نیروهای خودی و دشمن از دیده‌بانی در ارتفاعات مناسب استفاده می‌کردند. امروزه و در عصر اطلاعات با پیچیده شدن صحنه‌های جنگ، مشاهدات این فرماندهان با استفاده از حسگرهای

1- Sense making

2- Intuitive Appreciation
3- Action-Reaction Cycle

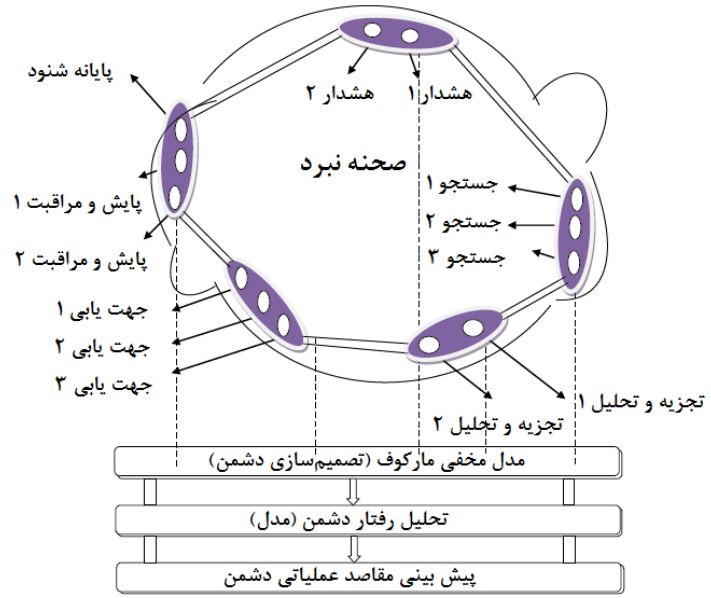
الکترونیکی و مخابراتی پیشرفته انجام می‌گیرد. به عبارت دیگر، فرماندهان اکنون روی «ارتفاعات الکترونیکی» ایستاده و نیازهای میدان جنگ را با تمام جزئیات آن مشاهده می‌کنند. بدیهی است که این پدیده به همراه تغییرات اساسی در پارامترهای جنگ حاصل انقلاب اطلاعات است. گرچه این ویژگی یک امتیاز منحصربه‌فرد برای فرماندهان محسوب می‌گردد، بااین‌حال به دلیل وابستگی آنان به تجهیزات الکترونیک باعث افزایش آسیب‌پذیری سامانه‌های آنها در برابر جنگ الکترونیک[1] شده است. ازاین‌رو، ارتش‌ها با صرف هزینه‌های گزاف سعی می‌کنند که از مزایای دیجیتالی شدن میدان رزم و افزایش نقش جنگ الکترونیک در صحنه نبرد برخوردار شوند. دکترین جنگ الکترونیک شامل پشتیبانی الکترونیکی[2]، تهاجم الکترونیکی[3] و حفاظت الکترونیکی[4] است و نقش تعیین‌کننده‌ای در دکترین مطرح جنگ اطلاعات[5]، عملیات اطلاعاتی[6] و جنگ فرماندهی[7] و کنترل در صحنه نبرد دیجیتالی دارد [۴].

در این مقاله، یک مدل تحلیل رفتار دشمن با استفاده از مدل‌های مخفی مارکوف بر اساس مشاهدات جنگ الکترونیک در صحنه‌های جنگ پیچیده ارائه شده است. در حقیقت، با استفاده از مدل‌های مخفی مارکوف فرآیند معناسازی محرک‌ها و اقدامات فیزیکی دشمن در صحنه جنگ، که بیانگر درک شهودی ما از وضعیت است، مدل شده است. این مدل در تحلیل رفتار دشمن و تعیین مقاصد عملیاتی آن جهت فرآیند تصمیم‌سازی نظامی به‌منظور اتخاذ پاسخ مناسب به دشمن استفاده شده است. برای این منظور یک سناریوی جنگ احتمالی ا. م. آمریکا علیه ج. ا. ایران از منظر جنگ الکترونیک بررسی شده و مبنای این مدل‌سازی قرار گرفته است.

در بخش دوم، معماری مدل شامل سامانه‌های پشتیبانی الکترونیکی، مدل مخفی مارکوف (تصمیم‌سازی دشمن)، تحلیل رفتار دشمن (مدل) و پیش‌بینی مقاصد عملیاتی دشمن ارائه شده است. در بخش سوم، به توصیف سناریوی جنگ احتمالی ا. م. آمریکا علیه ج. ا. ایران از منظر جنگ الکترونیک پرداخته شد. در بخش چهارم، روش پیشنهادی برای مدل‌سازی بیان گردیده و در بخش پنجم، نتایج شبیه‌سازی مدل ارائه‌شده موردبحث و بررسی قرار گرفته است. نتیجه‌گیری نیز در بخش ششم آورده شده است.

۲- معماری مدل

معماری کلی مدل ارائه‌شده مطابق با شکل (۲) است. همان‌طوری که در شکل (۲) نشان داده شده است، صحنه نبرد به کمک شبکه‌ای از سامانه‌های پشتیبانی الکترونیکی شامل حسگرهای الکترونیکی و مخابراتی پیشرفته مراقبت می‌شود. سپس، با استفاده از مدل‌های مخفی مارکوف و بر اساس مشاهدات جمع‌آوری شده از صحنه نبرد، سیستم تصمیم‌سازی دشمن مدل شده و بر طبق مدل به‌دست‌آمده، تحلیل رفتار دشمن و پیش‌بینی مقاصد عملیاتی آن صورت می‌گیرد.



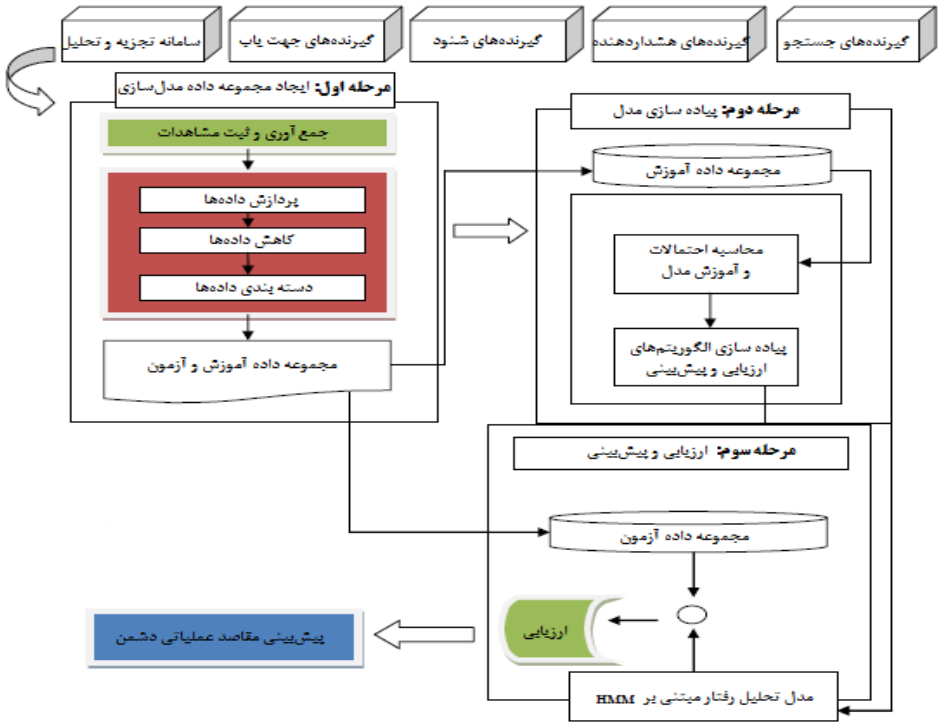
شکل (۲): معماری کلی مدل

1- Electronic Warfare
2- Electronic Support
3- Electronic Attack
4- Electronic Protect
5- Information Warfare
6- Information Operation
7- Command and Control Warfare

پشتیبانی الکترونیکی مؤلفه‌ای از جنگ الکترونیک برای شناسایی منابع منتشرکننده انرژی الکترومغناطیسی ارادی و غیرارادی دشمن است. عناصر پشتیبانی الکترونیکی، جستجو، رهگیری، هشداردهی، پایش و مراقبت، جهت‌یابی و تحلیل هستند. این اقدامات به‌منظور شناسایی و تفسیر تهدیدهای آنی به شکل آرایش الکترونیکی نبرد[1] می‌باشند. آرایش الکترونیکی نبرد به چیدمان و نحوه فعالیت آن دسته از تجهیزات راداری، ارتباطی و یا موشکی اطلاق می‌گردد که دارای تشعشعات الکترومغناطیس می‌باشند. به این ترتیب، در پشتیبانی الکترونیکی علاوه بر اطلاعات مربوط به فعالیت‌ها و تجهیزات دشمن، با رهگیری و کشف امواج حاصل از انتشار این تجهیزات راهبردهایی نیز برای عملیات تهاجم الکترونیکی حاصل می‌شود.

اقدامات پشتیبانی الکترونیکی معمولاً غیرفعال‌اند[2]، در حالی که اقدامات تهاجم الکترونیکی فعال[3] هستند. حفاظت الکترونیکی به هر دو روش فعال و غیرفعال وجود دارد. ازاین‌رو، سامانه‌های پشتیبانی الکترونیکی غالباً از سامانه‌های فعال دشمن به جمع‌آوری و تحلیل اطلاعات تاکتیکی می‌پردازند و در بسیاری از حالات می‌توانند ۶۰ تا ۸۰ درصد اطلاعات تاکتیکی دشمن را به‌دست آورند. بنابراین، عملکرد سامانه‌های پشتیبانی الکترونیکی تا حد زیادی به سایر فعالیت‌های جاسوسی وابسته است و اطلاعات به‌دست‌آمده از آن را می‌بایست با اطلاعات کسب‌شده توسط حسگرهای انسانی صحنه نبرد تطابق داد [۴]. این اطلاعات مجموعه داده آموزش برای مدل‌سازی را تشکیل می‌دهند و هر چه انطباق این اطلاعات با وقایع صحنه نبرد بیشتر باشد، مدل به‌دست‌آمده برای تحلیل رفتار دشمن دقیق‌تر خواهد بود. برای این منظور یک سناریوی جنگ احتمالی ا. م. آمریکا علیه ج. ا. ایران از منظر جنگ الکترونیک بررسی شده و مبنای این مدل‌سازی قرار گرفته است.

معماری داخلی مدل تحلیل رفتار دشمن مبتنی بر مدل‌های مخفی مارکوف در شکل (۳) نمایش داده شده است. همان‌طوری که در شکل (۳) مشاهده می‌شود، معماری داخلی مدل شامل سه مرحله به نام‌های ایجاد مجموعه داده مدل‌سازی، پیاده‌سازی مدل، و ارزیابی[4] و پیش‌بینی[5] می‌باشد. معماری ترسیم‌شده در این شکل، سازوکار تحلیل رفتار دشمن مبتنی‌بر مدل‌های مخفی مارکوف و پیش‌بینی مقاصد عملیاتی دشمن را بر اساس مشاهدات جنگ الکترونیک از صحنه‌های نبرد پیچیده معرفی می‌نماید.



شکل (۳): معماری داخلی مدل

1- Electronic Order of Battle (EOB)
2- Passive
3- Active
4- Evaluation
5- Prediction

در مرحله اول؛ اقدامات زیر جهت ایجاد مجموعه داده مدل‌سازی انجام می‌شود:

- **جمع‌آوری و ثبت مشاهدات:** مشاهدات انجام‌شده از صحنه نبرد به کمک سامانه‌های پشتیبانی الکترونیک شامل: گیرنده‌های جستجو، گیرنده‌های هشداردهنده، گیرنده‌های شنود (مراقبت و کنترل)، گیرنده‌های جهت‌یاب و سامانه‌های تجزیه‌وتحلیل، جمع‌آوری شده و بر اساس تاریخ و زمان دریافت ثبت و ذخیره‌سازی می‌گردد.
- **پردازش داده‌ها:** برخی پیش‌پردازش‌ها روی داده‌های جمع‌آوری‌شده صورت می‌گیرد تا داده‌ها به کیفیت قابل قبولی برای آموزش مدل برسند.
- **کاهش داده‌ها:** داده‌های پیش‌پردازش شده تجمیع شده و داده‌های تکراری حذف می‌گردند.
- **دسته‌بندی داده‌ها:** داده‌ها دسته‌بندی شده و هر کدام در یکی از دسته اقدامات دشمن (مفروض در سناریوی جنگ احتمالی) قرار می‌گیرند. با توجه به این‌که هر یک از دسته اقدامات مفروض نیز می‌توانند در وضعیت‌های مختلف مقاصد عملیاتی دشمن رخ دهند، می‌توان به هریک از داده‌ها یک حالت یا وضعیت عملیاتی نسبت داد.
- **مجموعه داده آموزش و آزمون:** داده‌های جمع‌آوری‌شده پس از طی مراحل فوق آماده آموزش مدل مخفی مارکوف می‌باشند. معمولاً بخش بزرگی از داده‌های جمع‌آوری‌شده برای آموزش مدل و بخش کوچکی از داده‌ها برای آزمودن مدل آموزش‌دیده (آزمون) مورد استفاده قرار می‌گیرند. منظور از آموزش مدل محاسبه احتمالات جهت پیاده‌سازی مدل می‌باشد.

مجموعه داده‌های آموزش و آزمون را می‌توان بر اساس گیرنده دریافت‌کننده آن (با یک کد شناسایی منحصربه‌فرد)، تاریخ دریافت، زمان دریافت، دسته اقدام و حالت یا وضعیت عملیاتی مربوطه ثبت و ذخیره‌سازی نمود. در جدول (۱) قالب ذخیره‌سازی مجموعه داده‌های مدل‌سازی نمایش داده شده است.

در مرحله دوم؛ اقدامات زیر جهت پیاده‌سازی مدل صورت می‌گیرد:

- **محاسبه احتمالات و آموزش مدل:** برای آموزش مدل بر اساس مجموعه داده آموزش، احتمالات مورد نیاز مدل مخفی مارکوف شامل: توزیع احتمال حالت آغازین (احتمال شروع از حالات)، ماتریس احتمال انتقال (احتمال جابجایی بین حالات) و ماتریس احتمال توزیع مشاهدات (احتمال انجام یک فعالیت یا اقدام خاص) محاسبه می‌گردد.
- **پیاده‌سازی الگوریتم‌های ارزیابی و پیش‌بینی:** الگوریتم‌های ارزیابی شامل الگوریتم‌های پیشرو[1] و پسرو[2] جهت محاسبه احتمال میزان تعلق مشاهدات یا اقدامات به هر حالت مدل و الگوریتم پیش‌بینی شامل الگوریتم ویتربی[3] جهت محاسبه بیشینه این احتمالات تعلق و معرفی حالت دارای بیشینه احتمال به‌عنوان حالت یا وضعیت عملیاتی هدف می‌باشد.

مرحله سوم؛ مرحله ارزیابی و پیش‌بینی است. در این مرحله با استفاده از مدل تحلیل رفتار مبتنی بر مدل‌های مخفی مارکوف به‌دست‌آمده در مرحله دوم می‌توان مجموعه داده‌های آزمون را مورد ارزیابی و پیش‌بینی قرار داد. یعنی با استفاده از الگوریتم‌های ارزیابی، احتمال تعلق مشاهدات آزمون را محاسبه کرد و با استفاده از الگوریتم ویتربی، حالت یا وضعیت عملیاتی مرتبط با مشاهدات آزمون را پیش‌بینی نمود.

جدول (۱): نمایش مجموعه داده‌های مدل‌سازی

تاریخ	زمان	گیرنده (کد شناسایی)	اقدام	وضعیت مربوطه
۰۱-۱۰-۲۰۱۶	۰۱:۲۸:۳۹	S01	Y1	S1
۲۰-۱۰-۲۰۱۶	۰۳:۲۸:۴۰	W03	Y2	S2
۰۲-۱۲-۲۰۱۶	۲۰:۴۰:۲۵	I04	Y3	S3
۲۰-۱۲-۲۰۱۶	۱۸:۱۰:۴۵	D15	Y4	S4
۲۱-۱۲-۲۰۱۶	۰۸:۲۰:۵۸	A20	Y5	S5
۲۱-۱۲-۲۰۱۶	۰۸:۲۲:۱۵	D02	Y6	S5

1- Forward
2- Backward
3- Viterbi

۳- توصیف سناریوی مبنای مدل‌سازی

بر اساس مطالعات جامع و مرور پیشینه تاریخی مناقشه بین ا. م. آمریکا و ج. ا. ایران، یک سناریوی جنگ احتمالی بین ا. م. آمریکا و ج. ا. ایران در نظر گرفته شده و مبنای این مدل‌سازی قرار گرفته است. در تهیه این سناریو، ضمن استفاده از نظرات خبرگان نظامی، از نتایج گزارش‌های تحلیلی دفاعی معتبر نیز استفاده شده است. در این سناریو، ا. م. آمریکا پنج راهبرد احتمالی یا مقصود عملیاتی علیه ج. ا. ایران خواهد داشت و در هر کدام از حالات یا وضعیت‌ها اقداماتی در صحنه نبرد انجام خواهد داد که در ادامه تشریح می‌شوند.

گزینه‌های راهبردی یا مقاصد عملیاتی ا. م. آمریکا در نبرد با ج. ا. ایران عبارت‌اند از:

۱. **غیرجنگی:** شکل‌های دیگر نبرد غیر از جنگی شامل نبرد در سطح رسانه و افکار عمومی با استفاده از شبکه‌های ماهواره‌ای و فضای سایبری جهت ایجاد نارضایتی و ناامیدی
۲. **پیش از نبرد:** کلیه اقدامات جاسوسی یا جمع‌آوری اطلاعات جهت حمله نظامی
۳. **حمله محدود:** حمله محدود و کاری به مراکز خاص کشور برای رسیدن به مقاصد محدود و برای ایجاد ممانعت در دست‌یابی به اهداف خاص (به‌طور مثال برنامه هسته‌ای ایران)
۴. **حمله گسترده:** حمله گسترده به پادگان‌های نظامی، مراکز اقتصادی، شاهراه‌های ارتباطی و زیرساخت‌های کشور برای بازگرداندن کشور به دوران پیش از سازندگی
۵. **حمله بسیار گسترده:** حمله بسیار گسترده همراه با اشغال کشور

این سناریو توسط متخصصان و خبرگان نظامی کشور در حوزه جنگ الکترونیک بررسی‌شده و اقدامات احتمالی و قابل مشاهده دشمن در صحنه نبرد با استفاده از نتایج گزارش‌های میدانی جنگ‌های اخیر آمریکا و مانورهای نظامی آمریکا در منطقه از منظر جنگ الکترونیک تدوین و گردآوری شده است. در ادامه فهرستی از این اقدامات و مشاهدات انجام‌شده به‌صورت دسته‌بندی‌شده ارائه می‌گردد.

- **حمله رسانه‌ای:**

۱- نبرد در سطح رسانه و افکار عمومی با استفاده از فضای سایبری و شبکه‌های ماهواره‌ای جهت فریب افکار عمومی و ایجاد نارضایتی عمومی و سلب اعتماد به نظام مقدس ج. ا. ایران و کاهش اعتقادات دینی و روحیه مقاومت و ایثار در صورت تهاجم دشمن (غیرجنگی، پیش از نبرد)

۲- حمله به فرستنده‌های مهم تلویزیونی کشور، اخراج شبکه‌های ماهواره‌ای ما از ماهواره‌ها با ترفندهای سیاسی و مالی و حمله سنگین روانی با استفاده از ماهواره‌های خود در (حمله محدود، گسترده و بسیار گسترده)

- **جاسوسی یا جمع‌آوری اطلاعات:**

۱- افزایش پرواز هواپیماهای جاسوسی مجهز به سامانه‌های جمع‌آوری اطلاعات سیگنالی[1] (SIGINT) (غیرجنگی، پیش از نبرد، محدود، گسترده و بسیار گسترده)

۲- افزایش فعالیت ماهواره‌های جاسوسی زمین‌گرد[2] (LEO)- گذر چند روز یک‌بار از فراز یک نقطه زمین و به‌روز نبودن اطلاعات (غیرجنگی و پیش از نبرد)

۳- افزایش پرواز پرنده‌های بدون سرنشین[3] مجهز به دوربین‌های دید در شب و مادون‌قرمز[4] (غیرجنگی، پیش از نبرد، محدود، گسترده و بسیار گسترده)

۴- افزایش فعالیت رادارهای SAR[5] (غیرجنگی و پیش از نبرد)

۵- افزایش شدید حجم ورود تجهیزات پیشرفته آمریکا به منطقه (غیرجنگی، پیش از نبرد، محدود، گسترده و بسیار گسترده)

۶- افزایش فعالیت جاسوس‌های انسانی (غیرجنگی، پیش از نبرد، محدود، گسترده و بسیار گسترده)

۷- ورود انواع بمب‌افکن‌های بزرگ و بلندپرواز به منطقه (پیش از نبرد، گسترده و بسیار گسترده)

۸- ورود ناوهای مجهز به موشک‌های کروز دوربرد به دریاهای نزدیک ایران (پیش از نبرد، محدود)

۹- ورود انواع هواپیماها و موشک‌های مدرن به پایگاه‌های نظامی آمریکا در منطقه و کشورهای همسایه ایران (پیش از نبرد، حمله محدود، گسترده و بسیار گسترده)

۱۰- برگزاری مانورهای مشترک با کشورهای همسایه برای ورود تسلیحات و تجهیزات (پیش از نبرد)

۱۱- کلیه اقدامات و مانورهای نظامی جهت شناسایی لایه‌های مختلف پدافند هوایی اعم از سامانه‌های حمله الکترونیکی نرم

1- Signal Intelligence
2- Low Earth Orbit
3- Unmanned aerial vehicle
4- Infrared
5- Synthetic-aperture radar

(جمر[1])، پدافند موشکی دوربرد، میان برد و نزدیک برد و پدافند نقطه‌ای (غیرجنگی و پیش از نبرد)

- **حمله فضایی و موشکی:**

۱- حمله به تأسیسات هسته‌ای ایران (حمله محدود)

۲- حمله به فرودگاه‌های نظامی با استفاده از موشک‌های کروز از پایگاه‌های نظامی آمریکا و ناوهای اطراف (حمله گسترده و بسیار گسترده)

۳- حمله به سکوهای موشک‌های استراتژیک ایران، با توجه به قابل‌حمل بودن آنها احتمال ضعیف دارد و غافلگیرکننده نخواهد بود. (حمله محدود)

۴- استفاده آمریکا از سلاح‌های مدرن مثل موشک‌های مجهز به بمب‌های الکترومغناطیس جهت آسیب رساندن جدی به اهداف در عمق زمین بدون نیاز به رسوخ فیزیکی- با توجه به تمایل آمریکا به کمترین اصطکاک فیزیکی احتمال آن بسیار زیاد است. (حمله محدود)

۵- افزایش فعالیت فرکانس سیگنال‌های SATCOM[2] جهت ایجاد لینک ارتباطی راه دور برای نیروهای نفوذکننده در عمق کشور شامل هواپیماهای بدون سرنشین و نیروهای زمینی (حمله محدود و گسترده)

۶- انهدام جمرهای GPS[3] و سامانه‌های آنها جهت تأمین فضای فرکانسی GPS به‌دلیل استفاده از سامانه ناوبری GPS در ادوات مؤثر آمریکا (حمله محدود و گسترده)

- **حمله هوایی:**

۱- پرواز هواپیماهای اخلال الکترونیک (جمر بیرونی[4]) جهت اخلال در سامانه‌های شناسایی و رادارهای مرزی برای ورود هواپیماهای جنگنده و بمب‌افکن در نزدیکی مرزهای ایران (حمله گسترده و بسیار گسترده)

۲- پرواز هواپیماهای جنگنده و بمب‌افکن مجهز به خود حفاظتی[5] جهت انجام عملیات مؤثر در داخل خاک ایران (حمله گسترده و بسیار گسترده)

۳- افزایش پرواز هواپیماهای بدون سرنشین و باسرنشین جاسوسی نظیر هواپیماهای آواکس[6] (حمله گسترده و بسیار گسترده)

۴- دریافت لینک‌های رادیویی هواپیماهای جنگنده و مهاجم دشمن (حمله گسترده و بسیار گسترده)

۵- حمله به سامانه‌های پدافند هوایی، واحد فرماندهی و کنترل و رادارهای ردگیری هدف[7] با استفاده از چند اسکادران جنگنده، بمب‌افکن و هواپیمای جنگ الکترونیک (حمله گسترده و بسیار گسترده)

۶- ایجاد اهداف کاذب[8] در رادارهای جستجو و مراقبت با استفاده از پرنده‌های دورایستا[9] جهت فریب رادارها و فرماندهان در پشتیبانی حملات هوایی (حمله گسترده و بسیار گسترده)

۷- حمله به شبکه فرماندهی و کنترل شامل: شنود شبکه و کسب اطلاعات در مورد تحرکات ما (ساده بودن)، عملیات فریب و در صورت عدم تأثیر، اقدام به اخلال (پیچیده بودن)، (حمله گسترده و بسیار گسترده)

- **حمله زمینی:**

۱- اخلال در سامانه‌های شناسایی پرتابه و انهدام آنها (حمله بسیار گسترده)

۲- استفاده از سامانه‌های مکان‌یابی بی‌سیم جهت مکان‌یابی فرستنده‌های بی‌سیم و انهدام آنها (حمله بسیار گسترده)

۳- استفاده از بالگردهای حامی نیروهای زمینی مجهز به رادارهای برد کوتاه و ارتفاع پایین (حمله بسیار گسترده)

- **حمله دریایی و زیرسطحی:**

۱- ورود ناوهای جنگی غول‌پیکر به آب‌های جنوبی- به‌دلیل دور بودن از نقاط استراتژیک کشور حمله محدود و کاری بعید است. (حمله گسترده و بسیار گسترده)

۲- استفاده از زیردریایی‌ها و سکوهای زیرسطحی در عمق دریا جهت شلیک به ناوها و کشتی‌ها و در نزدیکی ساحل جهت انتقال نیروها به ساحل (حمله بسیار گسترده)

1- Jammer
2- Satellite Communications
3- Global Positioning System
4- Off-board Jammer
5- Self-Protection
6- AWACS (Airborne Warning and Control System)
7- Target Tracking Radar
8- False Target
9- Stand-Off

۳- استفاده از شبکه‌ای از اخلال‌کننده‌ها برای ممانعت از رهیابی موشک‌های فعال (هدایت‌شده با رادار) به نزدیک کشتی‌ها (حمله بسیار گسترده)

۴- استفاده از روش‌های فریب[1] موشک‌های دریایی مانند چف[2] و فلیر[3] (حمله بسیار گسترده)

۵- استفاده از روش دیوار آتش[4] جهت مقابله با قابلیت مانورهای پیچیده موشک‌های دریایی (حمله بسیار گسترده)

دسته اقدامات فوق به‌صورت $Y_k, k = 1,2,\dots,6$ نمایش داده می‌شوند. همان‌طوری که در بالا ملاحظه می‌گردد، مشاهدات گردآوری‌شده در دسته اقدامات شش‌گانه حمله رسانه‌ای، جاسوسی یا جمع‌آوری اطلاعات، حمله فضایی و موشکی، حمله هوایی، حمله زمینی، و حمله دریایی و زیرسطحی دسته‌بندی‌شده و ارتباط هر مشاهده با مقاصد عملیاتی دشمن که حالات یا وضعیت‌های مدل می‌باشند مشخص گردیده است. بر اساس این دسته‌بندی و ارتباط با حالات می‌توان مدل مخفی مارکوف (تصمیم‌سازی دشمن) را پیاده‌سازی نمود. این مسئله در بخش چهارم مقاله به‌طور مفصل تشریح خواهد شد.

۴- روش پیشنهادی برای مدل‌سازی

روش‌های آماری می‌توانند در قالب یک سیستم هوشمند به کمک متخصصان در زمینه‌های مختلف بشتابند. در سال‌های اخیر کاربرد روش‌های آماری و ابزارهای مدل‌سازی در حوزه‌های مختلف به‌طور گسترده در حال افزایش است و گرایش به سمت این روش‌ها افزایش یافته است [۵]. در این راستا روش آماری مدل مخفی مارکوف از مفاهیمی بوده که نظر بسیاری از پژوهش‌گران را به خود جلب کرده و به جهت آن‌که بر اساس یادگیری و کشف رابطه نهفته در فرآیند به حل مسئله می‌شتابد، در زمره روش‌های داده‌کاوی، یادگیری ماشین و هوشمند نیز محسوب شده است [۶-۷].

مدل‌های مخفی مارکوف در اواخر دهه ۱۹۶۰ میلادی معرفی گردید و در حال حاضر به‌سرعت در حال گسترش دامنه کاربردها می‌باشد. دو دلیل مهم برای این مسئله وجود دارد. اول اینکه این مدل از لحاظ ساختار ریاضی بسیار قدرتمند است و به همین دلیل مبانی نظری بسیاری از کاربردها را شکل داده است. دوم اینکه مدل مخفی مارکوف اگر به‌صورت مناسبی ایجاد شود می‌تواند برای کاربردهای بسیاری مورد استفاده قرار گیرد [۸].

بیشتر مطالعات مبنی بر مدل‌های مخفی مارکوف در زمینه‌هایی غیر از علوم دفاعی (مثلاً در شناسایی گفتار [۹]، علوم کامپیوتر [۱۰]، علوم پزشکی [۱۱]، اقتصاد [۱۲]، مخابرات [۱۳]، روان‌شناسی [۱۴] و ...) صورت گرفته است و کاربرد آن در زمینه علوم دفاعی بسیار اندک بوده است. مطالعه حاضر در زمرد اولین مطالعاتی است که از مدل‌های مخفی مارکوف جهت پیش‌بینی مقاصد عملیاتی دشمن در حوزه دفاعی استفاده می‌کند. هدف اصلی این پژوهش، تحلیل رفتار دشمن و تعیین نیات و مقاصد عملیاتی دشمن در صحنه نبرد با استفاده از مدل مخفی مارکوف بر اساس مشاهده اقدامات دشمن در صحنه نبرد از منظر جنگ الکترونیک است. در این بخش از مقاله، به توصیف این روش پیشنهادی می‌پردازیم.

مراقبت از صحنه نبرد با کمک شبکه‌ای از سامانه‌های پشتیبانی الکترونیکی، به لحاظ ساختاری، سامانه‌ای پیچیده با عملکردهای مختلف است، از این جهت فرماندهان در مشاهده صحنه نبرد و عملکرد نیروهای خودی و دشمن با کثرتی از داده‌ها روبه‌رو هستند و تحلیل رفتار دشمن و تصمیم‌گیری امری زمان‌بر است. ازاین‌رو، روش‌های آماری مانند مدل مخفی مارکوف می‌توانند با افتراق و طبقه‌بندی حالت‌های عملیاتی مختلف دشمن به‌عنوان کمک‌یار فرماندهان در زمان تصمیم‌گیری صرفه‌جویی به‌عمل آورند.

مدل مخفی مارکوف یک روش آماری است که بر پایه زنجیر مارکوف استوار است. این مدل ابزاری قدرتمند در پردازش و مدل‌سازی فرآیندهای تصادفی محسوب می‌شود و به‌عنوان یک روش در پیش‌بینی و طبقه‌بندی داده‌ها در بین روش‌های آماری مطرح است [۱۵]. همچنین، مدل مخفی مارکوف به‌عنوان یک سیستم پیشگوی قوی به خوبی بر داده‌ها منطبق می‌گردد و نتایج بسیار دقیقی ارائه می‌دهد، این عبارت توسط افراد مختلفی هنگام استفاده از مدل مخفی مارکوف در مقالات متعددی ذکر شده است [۹، ۱۱-۱۳].

یک مدل مخفی مارکوف از تعدادی حالت تشکیل‌شده که در هر حالت تعدادی خروجی تولید می‌شود. حالات متغیرهای تصادفی هستند که می‌توانند پیوسته یا گسسته در زمان باشند. اگر هر حالت فقط به حالت قبل وابسته باشد و به چند حالت قبلی وابسته نباشد به این فرآیند، مارکوف می‌گویند. همچنین، اگر حالات ممکن مخفی باشند به آن، فرآیند مخفی مارکوف

1- Deception Techniques
2- Chaff
3- Flare
4- Fire Wall

می‌گویند. مدل یک سیستم با فرآیند مخفی مارکوف و خروجی‌های تولیدشده در هر حالت را مدل مخفی مارکوف می‌گوییم. اگر در یک مدل مخفی مارکوف حالت بعدی به k حالت قبلی وابسته باشد، به آن مدل مخفی مارکوف مرتبه k ام گفته می‌شود. مدل مخفی مارکوف مرتبه اول متداول‌ترین مدل است که در آن حالت بعدی تنها به حالت فعلی وابسته است [۸].

یکی از رویکردهای فرماندهان در طرح‌ریزی نظامی و فرآیند تصمیم‌سازی، فرآیند تصمیم مارکوف است [۱۷-۱۶] ، زیرا در آن نتایج تا حدودی تصادفی و تا حدودی تحت کنترل یک تصمیم‌گیر است [۱۸]. این رویکرد خصوصاً در صحنه‌های نبرد پیچیده و شرایط عدم قطعیت، رویکرد مناسبی جهت طرح‌ریزی نظامی و مدل‌سازی فرآیند تصمیم است [۱۹]. در این مسئله، آینده‌های قابل پیش‌بینی یا تصمیمات ممکن دشمن، حالات یا وضعیت‌های مدل هستند که گسسته می‌باشند. ما از تصمیمات دشمن در صحنه نبرد بی‌اطلاع هستیم و فقط اقدامات دشمن در صحنه نبرد را مشاهده می‌کنیم، بنابراین، تصمیمات یا مقاصد عملیاتی دشمن مخفی هستند. خروجی‌های مدل نیز همان مشاهدات یا رخدادهای صحنه نبرد هستند که می‌توانند گسسته یا پیوسته باشند. با توجه به‌عدم امکان دسترسی به داده‌های یک صحنه نبرد واقعی، در این مطالعه از داده‌های جمع‌آوری‌شده در یک سناریوی نبرد احتمالی استفاده شده است. به‌دلیل کمبود داده‌ها در سناریوی استفاده شده برای مدل‌سازی، خروجی‌های مدل ایجادشده گسسته می‌باشند. همچنین در این مسئله، مدل مخفی مارکوف مفروض از نوع مرتبه اول و تغییرناپذیر با زمان درنظر گرفته شده است، بدین معنی که تمام احتمالات توصیف‌کننده این مدل در طول زمان تغییر نمی‌کنند. اگر امکان دسترسی به داده‌های یک صحنه نبرد واقعی به‌وجود آید، با دریافت داده‌ها از طریق سامانه‌های پشتیبانی الکترونیک که در بخش دوم توضیح داده شد، می‌توان احتمالات توصیف‌کننده مدل را به کمک الگوریتم‌های آموزش به‌روزرسانی نمود و در این صورت مدل مخفی مارکوف تغییرپذیر با زمان خواهد شد.

یک مدل مخفی مارکوف را می‌توان با تعیین پارامترهای زیر ایجاد نمود:

تعداد حالات ممکن $S = \{s_1, \dots, s_n\}$: تعداد حالات (وضعیت‌های) مقاصد عملیاتی دشمن است. در این مطالعه مقاصد عملیاتی دشمن دارای ۵ حالت مختلف می‌باشد پس $S = \{s_1, \dots, s_5\}$ است.

تعداد مشاهدات $O = \{x_1, \dots, x_t\}$: برای هر حالت عملیاتی ذکرشده در بالا تعدادی مشاهده داریم. در این مطالعه مشاهدات همان اقدامات ثبت‌شده برای هر حالت یا وضعیت عملیاتی دشمن است.

احتمالات انتقال a_{ij} : احتمال انتقال (جابجایی) از وضعیت عملیاتی حالت i به وضعیت عملیاتی حالت j :

$$1 \le i, j \le n = 5, \qquad (۱)$$

$$\sum_{j=1}^{n} a_{ij} = 1, \quad a_{ij} \ge 0, \quad a_{ij} = p(s_j | s_i)$$

ماتریس احتمالات انتقال $A = [a_{ij}]$: یک مجموعه از احتمالات انتقال در بین حالت‌هاست. در این مطالعه چون وضعیت‌های عملیاتی دشمن ۵ حالت دارد ماتریس احتمال انتقالات به شکل زیر در می‌آید:

$$A = \begin{bmatrix} & s_1 & s_2 & s_3 & s_4 & s_5 \\ s_1 & a_{11} & a_{12} & a_{13} & a_{14} & a_{15} \\ s_2 & a_{21} & a_{22} & a_{23} & a_{24} & a_{25} \\ s_3 & a_{31} & a_{32} & a_{33} & a_{34} & a_{35} \\ s_4 & a_{41} & a_{42} & a_{43} & a_{44} & a_{45} \\ s_5 & a_{51} & a_{52} & a_{53} & a_{54} & a_{55} \end{bmatrix} \qquad (۲)$$

در مطالعه حاضر حالت ۱ تا ۵ به ترتیب مربوط به وضعیت‌های عملیاتی غیرجنگی، پیش از نبرد، حمله محدود، حمله گسترده و حمله بسیار گسترده است.

احتمال توزیع مشاهدات b_{jk}: احتمال تعلق داشتن هر مشاهده (اقدام) به هر حالت را نشان می‌دهد:

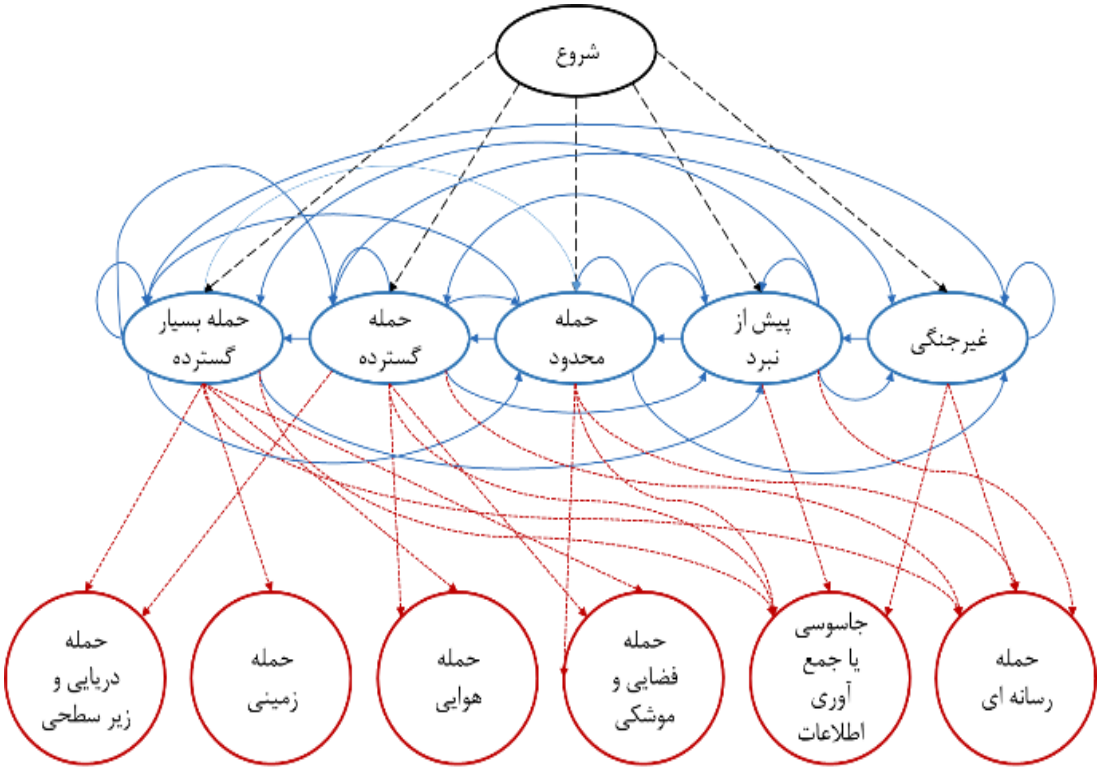
$$b_{jk} = p(O = x_k | S = s_j), \qquad (۳)$$

$$1 \le k \le t = 6\,, \;\; 1 \le j \le n = 5$$

$$\sum_{k=1}^{t} b_{jk} = 1, \quad b_{jk} \ge 0, \qquad 1 \le j \le n$$

ماتریس احتمال توزیع مشاهدات $B = [b_{jk}]$: در این مطالعه ۶ دسته مشاهده (اقدام) و ۵ حالت عملیاتی داریم، بنابراین، ماتریس احتمال توزیع مشاهدات به‌صورت زیر خواهد بود:

$$B = \begin{bmatrix} & x_1 & x_2 & x_3 & x_4 & x_5 & x_6 \\ s_1 & b_{11} & b_{12} & b_{13} & b_{14} & b_{15} & b_{16} \\ s_2 & b_{21} & b_{22} & b_{23} & b_{24} & b_{25} & b_{26} \\ s_3 & b_{31} & b_{32} & b_{33} & b_{34} & b_{35} & b_{36} \\ s_4 & b_{41} & b_{42} & b_{43} & b_{44} & b_{45} & b_{46} \\ s_5 & b_{51} & b_{52} & b_{53} & b_{54} & b_{55} & b_{56} \end{bmatrix} \qquad (۴)$$



شکل (۴): مدل مخفی مارکوف مفروض مبتنی بر سناریوی نبرد احتمالی

توزیع احتمال حالت آغازین $\pi = \{\pi_0(1), \ldots\ldots, \pi_0(n)\}$:
برای هر حالت عملیاتی یک احتمال اولیه رخداد وجود دارد که زنجیر مارکوف با آن احتمال اولیه از آن حالت شروع به‌کار می‌کند. به این ترتیب ما می‌توانیم یک مدل مخفی مارکوف با توزیع احتمال گسسته را با مشخص کردن ۳ پارامتر $\lambda = (A, B, \pi)$ به‌دست آوریم.

مهم‌ترین موضوع در کاربرد مدل مخفی مارکوف موضوع آموزش و ارزیابی مدل است. معمولاً آموزش مدل مخفی مارکوف از طریق یکی از الگوریتم‌های بام- ولچ[1] یا بیشینه‌سازی امید ریاضی[2] انجام می‌شود. برای این کار، علاوه بر ارائه داده‌های جمع‌آوری‌شده از صحنه نبرد (مشاهدات انجام‌شده) به مدل، به سه پارامتر مورد نیاز مدل (A, B, π) هم اعداد تصادفی در باز صفر و یک می‌دهیم. الگوریتم پس از آموزش یافتن، مقداری بهینه برای سه پارامتر ارائه می‌دهد. ارزیابی مدل نیز از طریق الگوریتم‌های پیشرو و پسرو امکان‌پذیر است. در این بخش، مدل با دریافت تعدادی از مشاهدات یا اقدامات که در امر آموزش شرکت نداشته‌اند، میزان تعلق این مشاهدات به هر حالت مدل را با یک احتمال نشان می‌دهد. اگر هر حالت مدل به‌عنوان یک مقصود عملیاتی دشمن در نظر گرفته شود، آنگاه الگوریتم ویتربی بیشینه این احتمالات تعلق را در نظر گرفته و مقصود عملیاتی (حالتی) را که دارای بیشینه احتمال است به‌عنوان مقصود عملیاتی هدف پیش‌بینی می‌کند. الگوریتم ویتربی یک روش قدرتمند است که می‌تواند به‌طور ماهرانه‌ای بیشینه تخمین پسین[3] مشاهدات را در دنباله بیابد [۲۰]. معمولاً در قسمت آموزش مدل از ۷۵ درصد داده‌ها استفاده و از ۲۵٪ باقی‌مانده داده‌ها برای ارزیابی مدل استفاده می‌شود.

در این مطالعه به‌دلیل عدم امکان دسترسی به داده‌های یک صحنه نبرد واقعی و کمبود داده‌های جمع‌آوری‌شده در یک سناریوی نبرد احتمالی، به‌جای الگوریتم‌های بام- ولچ و بیشینه‌سازی امید ریاضی از محاسبه احتمالات بر اساس تعداد مشاهدات جنگ الکترونیکی هر اقدام در هر حالت یا وضعیت عملیاتی جهت آموزش مدل مخفی مارکوف استفاده شده است. مدل مخفی مارکوف مفروض مبتنی بر سناریوی نبرد احتمالی ا. م. آمریکا علیه ج. ا. ایران در شکل (۴) نمایش داده شده است. در این شکل، پیکان‌های خط‌چین از حالت شروع به حالت‌های عملیاتی با مقادیر احتمال حالت آغازین $\pi_0(i)$، پیکان‌های خط پر بین حالت‌های عملیاتی با مقادیر احتمال انتقال (جابجایی) بین حالت‌ها a_{ij} و پیکان‌های نقطه‌چین از حالت‌های عملیاتی به مشاهدات (اقدامات) با مقادیر احتمال توزیع مشاهدات b_{jk} مقداردهی (وزن‌دهی) می‌شوند.

1- Baum-Welch
2- Expectation Maximization (EM)
3- Posterior Estimation

مقادیر احتمال حالت آغازین $\pi_0(i),\ i = 1,2,\dots,5$ ، بیانگر عدم قطعیت ما در مورد وقوع حالات در زمان شروع تحلیل است. این احتمالات، در این سناریو به‌طور پیش‌فرض به‌صورت زیر درنظر گرفته می‌شود که فرض‌های منطقی است و دور از واقعیت نمی‌باشد:

$$\pi_0(1) > \pi_0(2) > \pi_0(3) > \pi_0(4) > \pi_0(5) \qquad (۵)$$

احتمال (غیرجنگی) $\pi_0(1) = 0.3$،

احتمال (پیش از نبرد) $\pi_0(2) = 0.25$،

احتمال (حمله محدود) $\pi_0(3) = 0.2$،

احتمال (حمله گسترده) $\pi_0(4) = 0.15$،

احتمال (حمله بسیار گسترده) $\pi_0(5) = 0.1$.مقادیر احتمال انتقال در بین حالت‌ها $a_{ij},\ i,j = 1,2,\dots,5$، بیانگر چگونگی تغییر حالات است. در مدل مخفی مارکوف مفروض، به‌طور پیش‌فرض احتمال همه جابجایی‌های ممکن بین حالات (انتقالات) یکسان درنظر گرفته می‌شود، ولی ترجیحات راهبردی دشمن می‌تواند احتمال این جابجایی‌ها را تغییر دهد. ماتریس انتقال (جابجایی) بین حالت‌ها در سناریوی نبرد احتمالی ا. م. آمریکا علیه ج. ا. ایران، بر اساس ترجیحات راهبردی آمریکا به‌صورت جدول (۲) به‌دست آمده است. در این سناریو تمایل ا. م. آمریکا به حداقل سطح درگیری سخت با ج. ا. ایران می‌باشد و ا. م. آمریکا هیچ‌گاه به‌طور مستقیم از حالت غیرجنگی به یکی از حالت‌های جنگی تغییر حالت نمی‌دهد.

جدول (۲): ماتریس انتقال (جابجایی) بین حالت‌ها

تعداد جابجایی بین حالات (N_{ij})	غیرجنگی	پیش از نبرد	محدود	گسترده	بسیار گسترده	تعداد جابجایی هر حالت (N_i)
غیرجنگی	۱	۲	۰	۰	۰	۳
پیش از نبرد	۲	۱	۱	۱	۱	۶
محدود	۲	۳	۱	۱	۱	۸
گسترده	۲	۳	۴	۱	۱	۱۱
بسیار گسترده	۲	۳	۴	۵	۱	۱۵

طبق جدول (۲)، ماتریس احتمالات انتقال به‌صورت زیر محاسبه می‌گردد:

$$A = \{a_{ij}\} = \left\{\frac{N_{ij}}{N_i}\right\} = \qquad (۶)$$

$$\begin{bmatrix} 0.33 & 0.67 & 0 & 0 & 0 \\ 0.32 & 0.17 & 0.17 & 0.17 & 0.17 \\ 0.25 & 0.375 & 0.125 & 0.125 & 0.125 \\ 0.18 & 0.28 & 0.36 & 0.09 & 0.09 \\ 0.13 & 0.2 & 0.27 & 0.33 & 0.07 \end{bmatrix},\ \mathrm{i,j} = 1,2,\dots,5$$

مقادیر احتمال توزیع مشاهدات،

$b_{jk},\ j = 1,2,\dots,5,\ k = 1,2,\dots,6$

بیانگر میزان علاقه‌مندی به انجام اقدامات در هر حالت است. در مدل مخفی مارکوف مفروض، احتمال انجام اقدامات در هر حالت بر اساس تعداد مشاهدات جنگ الکترونیکی هر اقدام در سناریوی جنگ احتمالی ا. م. آمریکا علیه ج. ا. ایران مطابق جدول (۳) به‌دست می‌آید.

جدول (۳): ماتریس توزیع مشاهدات (اقدامات) در هر حالت

تعداد مشاهدات هر اقدام (N_{jk})	حمله رسانه‌ای	جاسوسی اطلاعات	حمله فضایی و موشکی	حمله هوایی	حمله زمینی	حمله دریایی و زیرسطحی	تعداد مشاهدات هر حالت (N_j)
غیرجنگی	۱	۷	۰	۰	۰	۰	۸
پیش از نبرد	۱	۱۱	۰	۰	۰	۰	۱۲
محدود	۱	۶	۵	۰	۰	۰	۱۲
گسترده	۱	۶	۳	۷	۰	۱	۱۸
بسیار گسترده	۱	۶	۱	۷	۳	۵	۲۳

طبق جدول (۳)، ماتریس احتمال توزیع مشاهدات به‌صورت زیر محاسبه می‌گردد:

$$B = \{b_{jk}\} = \left\{\frac{N_{jk}}{N_j}\right\}$$

$$= \begin{bmatrix} 0.125 & 0.875 & 0 & 0 & 0 & 0 \\ 0.08 & 0.92 & 0 & 0 & 0 & 0 \\ 0.08 & 0.5 & 0.42 & 0 & 0 & 0 \\ 0.05 & 0.34 & 0.17 & 0.39 & 0 & 0.05 \\ 0.04 & 0.26 & 0.04 & 0.31 & 0.13 & 0.22 \end{bmatrix},$$

$$j = 1,2,\dots,5,\ \ k = 1,2,\dots,6 \qquad (۷)$$

پس از محاسبه مقادیر اولیه احتمالات مورد نیاز مدل (A, B, π)، اگر امکان دسترسی به داده‌های یک صحنه نبرد واقعی به وجود آید، با دریافت داده‌ها از طریق سامانه‌های پشتیبانی الکترونیک می‌توان احتمالات توصیف‌کننده مدل را به کمک الگوریتم‌های آموزش به‌روزرسانی نمود و در این صورت مدلی ایده‌آل برای صحنه‌های نبرد واقعی به‌دست آورد. هدف از آموزش به دست آوردن مدلی است که خواص آماری را از مجموعه داده آموزش استخراج کرده و آنها را نمایش دهد. به این ترتیب، برای هر حادثه‌ای که در صحنه نبرد رخ می‌دهد، باید پارامترهای مورد نیاز مدل (A, B, π) را با استفاده از روش بازتخمین بام- ولچ تخمین زد. این روش شانس داده‌های مشاهده شده آموزش را برای حوادث غیرمبهم افزایش می‌دهد [۲۱]. شرط اولیه در آموزش مدل مخفی مارکوف این است که الگوریتم تا زمانی ادامه یابد که مقدار برآورد شده برای سه پارامتر مدل به میزانی بهینه رسیده و با مقدار برآورد شده در تکرار قبلی الگوریتم تفاوت چندانی نداشته باشد [۲۲].

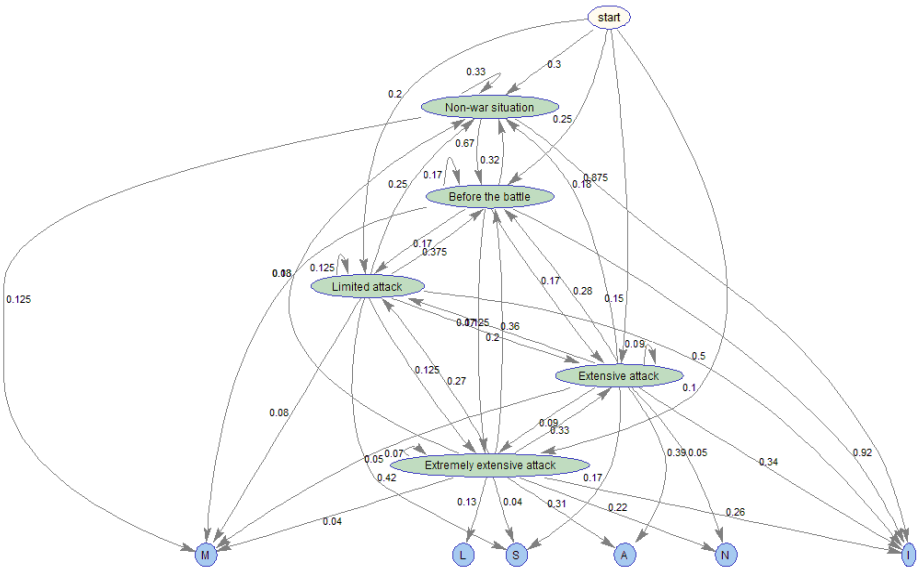
با توجه به این‌که هدف اصلی این پژوهش، ارائه یک مدل تحلیل رفتار و تعیین مقاصد عملیاتی دشمن در صحنه نبرد با استفاده از مدل مخفی مارکوف و بر اساس مشاهده اقدامات دشمن در صحنه نبرد از منظر جنگ الکترونیک می‌باشد، در

اینجا به شبیه‌سازی مدل ارائه‌شده با نرم‌افزار MATLAB پرداخته و سپس عملکرد مدل شبیه‌سازی‌شده با استفاده از یک سری مشاهدات فرضی ارزیابی می‌گردد.

۵- نتایج شبیه‌سازی

در این مطالعه ۷۳ مشاهده جنگ الکترونیکی از اقدامات احتمالی دشمن در صحنه نبرد مرتبط با حالت‌های مختلف عملیاتی دشمن شامل ۸ مشاهده غیرجنگی، ۱۲ مشاهده پیش از نبرد، ۱۲ مشاهده حمله محدود، ۱۸ مشاهده حمله گسترده و ۲۳ مشاهده حمله بسیار گسترده مورد بررسی قرار گرفت. مشاهدات شامل ۶ دسته اقدام فیزیکی بود که در بخش سوم توصیف شده‌اند.

مدل مخفی مارکوف پیشنهادی بر اساس مقادیر احتمالات (A, B, π) به‌دست‌آمده در بخش قبل، از مشاهدات جنگ الکترونیکی سناریوی نبرد احتمالی ا. م. آمریکا علیه ج. ا. ایران تولید و شبیه‌سازی گردید. مدل مخفی مارکوف شبیه‌سازی‌شده مبتنی بر سناریوی نبرد احتمالی با احتمالات توصیف‌کننده مدل در شکل (۵) نمایش داده شده است. لازم به‌ذکر است که مقادیر اولیه به‌دست‌آمده برای پارامترهای (A, B, π)، با توجه به‌عدم دسترسی به مشاهدات یک صحنه نبرد واقعی و ناکافی بودن مشاهدات سناریوی نبرد احتمالی، فرضی هستند و به‌دست آوردن مقادیر بهینه پارامترهای فوق در صورت وجود مجموعه داده کافی از مشاهدات جنگ الکترونیکی یک صحنه نبرد امکان‌پذیر خواهد بود.



شکل (۵): مدل مخفی مارکوف شبیه‌سازی‌شده

همان‌طور که مشاهده می‌گردد، مقادیر به‌دست‌آمده برای ماتریس احتمالات انتقال بین حالت‌های مختلف عملیاتی دشمن به شرح ماتریس A است که در آن حالت ۱ غیرجنگی[1]، حالت ۲ پیش از نبرد[2]، حالت ۳ حمله محدود[3]، حالت ۴ حمله گسترده[4] و حالت ۵ حمله بسیار گسترده[5] را نشان می‌دهد. برای مثال احتمال این‌که حالت عملیاتی غیرجنگی ناگهان به حالت عملیاتی جنگی از نوع حمله گسترده تغییر کند صفر است $(a_{14} = 0)$ و احتمال آن‌که قبل از حمله به حالت پیش از نبرد رفته و آمادگی نبرد کسب کند برابر ۶۷٪ است $(a_{12} = 0.67)$. همچنین احتمال این‌که در همان وضعیت غیرجنگی بماند ۳۳٪ است $(a_{11} = 0.33)$.

مقادیر به‌دست‌آمده برای ماتریس احتمال توزیع مشاهدات نیز بر اساس مشاهدات جنگ الکترونیکی صحنه نبرد در سناریوی نبرد احتمالی بررسی شده به شرح ماتریس B می‌باشد که در آن سطر ۱ احتمال وقوع اقدامات در حالت غیرجنگی، سطر ۲ احتمال وقوع اقدامات در حالت پیش از نبرد، سطر ۳ احتمال وقوع اقدامات در حالت حمله محدود، سطر ۴ احتمال وقوع اقدامات در حالت حمله گسترده و سطر ۵ احتمال وقوع اقدامات در حالت حمله بسیار گسترده می‌باشد. همان‌طور که ملاحظه می‌شود، در حالت غیرجنگی احتمال وقوع اقدامات جنگی به‌طور مثال حمله محدود صفر است $(b_{13} = 0)$ و احتمال وقوع اقدامات از نوع جاسوسی و جمع‌آوری اطلاعات ۸۷/۵٪ است

1- Non-War Situation
2- Before the Battle
3- Limited Attack
4- Extensive Attack
5- Extremely Extensive Attack

($b_{12} = 0.875$) و احتمال وقوع اقدامات از نوع حملات رسانه‌ای از طریق شبکه‌های ماهواره‌ای و سایبری ۱۲/۵٪ است ($b_{11} = 0.125$).

در مدل مخفی مارکوف شبیه‌سازی‌شده (شکل ۵)، اقدامات حمله رسانه‌ای با نماد "M"، جاسوسی و جمع‌آوری اطلاعات با نماد "I"، حمله فضایی و موشکی با نماد "S"، حمله هوایی با نماد "A"، حمله زمینی با نماد "L" و حمله دریایی و زیرسطحی با نماد "N" نمایش شده است. برای ارزیابی عملکرد مدل تحلیل رفتار شبیه‌سازی شده فرض می‌کنیم یک دنباله مشاهدات در صحنه نبرد احتمالی شامل حمله رسانه‌ای (M)، جاسوسی و جمع‌آوری اطلاعات (I)، جاسوسی و جمع‌آوری اطلاعات (I)، حمله فضایی و موشکی (S) و حمله هوایی (A) $\{M, I, I, S, A\}$ به‌وسیلهٔ شبکه‌ای از سامانه‌های پشتیبانی الکترونیک ثبت شده است، ارزیابی مدل از طریق الگوریتم‌های پیشرو و پسرو میزان تعلق این مشاهدات به هر حالت مدل را با یک احتمال مشخص نموده، آن‌گاه الگوریتم ویتربی بیشینه این احتمالات تعلق را در نظر گرفته و مقصود عملیاتی (حالتی) را که دارای بیشترین احتمال است به‌عنوان مقصود عملیاتی دشمن پیش‌بینی می‌کند. نتایج حاصل از ارزیابی مدل مخفی مارکوف شبیه‌سازی شده و پیش‌بینی مقاصد عملیاتی در جدول (۴) ذکر شده است.

همان‌طور که ملاحظه می‌گردد، احتمال تعلق مشاهدات به هر حالت عملیاتی توسط الگوریتم پیشرو محاسبه شده (ماتریس آلفا[1]) و به‌صورت ستونی در زیر هر یک از مشاهدات نمایش داده شده است. همچنین، الگوریتم پسرو احتمال جزئی دنباله مشاهدات در یک حالت (ماتریس بتا[2]) را محاسبه می‌کند. به‌طور مثال در دنباله مشاهدات مفروض، احتمال این‌که اولین مشاهده (M) متعلق به حالت غیرجنگی باشد ۴۸٪ و از همه احتمالات دیگر بیشتر است. الگوریتم ویتربی نیز با محاسبه ماتریس گاما[3] و بیشینه احتمالات تعلق هر مشاهده، محتمل‌ترین دنباله حالات تولیدکننده این دنباله مشاهدات را یافته و به‌عنوان دنباله مقاصد عملیاتی پیش‌بینی‌شده به‌صورت دنباله حالت {غیرجنگی، غیرجنگی، پیش از نبرد، حمله محدود، حمله گسترده} اعلام می‌نماید. مجموع احتمالات هر ستون در ماتریس آلفا، احتمال کل تولید هر مشاهده را در این دنباله مشاهدات به‌وسیله مدل مخفی مارکوف به‌دست‌آمده در سناریوی نبرد احتمالی نشان می‌دهد. مجموع این احتمالات، احتمال کل تولید دنبالهٔ مشاهدات است که در این دنباله از مشاهدات برابر ۸۹/۹٪ می‌باشد و نشان از آن است که وقوع چنین دنباله‌ای از مشاهدات در سناریوی نبرد احتمالی بررسی شده بالا است.

جدول (۴): نتایج حاصل از ارزیابی مدل و پیش‌بینی مقاصد عملیاتی

Observation sequence:	M	I	I	S	A
Probability of the whole observation sequence:			0.899025		
Trellis diagram, Forward algorithm (Alpha):					
Probabilities:					
Non-war situation:	+0.0375000000	+0.0225531250	+0.0173396661	0	0
Before the battle:	+0.0200000000	+0.0184690000	+0.0127832744	0	0
Limited attack:	+0.0160000000	+0.0101562500	+0.0075828625	+0.0046404410	0
Extensive attack:	+0.0075000000	+0.0065093000	+0.0047077078	+0.0017221420	+0.3900000000
Extremely extensive attack:	+0.0040000000	+0.0041470000	+0.0030696257	+0.0003450641	+0.3100000000
Column Sums of Probabilities:					
Probability:	+0.0850000000	+0.0618346750	+0.0454831366	+0.0067076471	+0.7000000000
Trellis diagram, Viterbi algorithm (Gamma):					
Probabilities:					
Non-war situation:	+0.0375000000*	+0.0108281250*	+0.0064722000	0	0
Before the battle:	+0.0200000000	+0.0231150000	+0.0066744562*	0	0
Limited attack:	+0.0160000000	+0.0017000000	+0.0019647750	+0.0004765562*	0
Extensive attack:	+0.0075000000	+0.0011560000	+0.0013360470	+0.0001928918	+0.0000232321*
Extremely extensive attack:	+0.0040000000	+0.0008840000	+0.0010216830	+0.0000453863	+0.0000184666
Prediction:					
State transition:	Non-war situation	Non-war situation	Before the battle	Limited attack	Extensive attack

1- Alpha Matrix
2- Beta Matrix
3- Gamma Matrix

۶- نتیجه‌گیری

مدل‌سازی، یکی از ابزارهای اساسی در طرح‌ریزی جنگ‌های پیچیده است. در این مقاله یک مدل تحلیل رفتار دشمن با استفاده از مدل‌های مخفی مارکوف بر اساس مشاهدات جنگ الکترونیک در صحنه‌های جنگ پیچیده ارائه شده است. برای این منظور، یک سناریوی جنگ احتمالی ا. م. آمریکا علیه ج. ا. ایران از منظر جنگ الکترونیک بررسی شده و به‌عنوان یک جنگ پیچیده مبنای این مدل‌سازی قرار گرفته است. نتایج حاصل از شبیه‌سازی مدل ارائه شده نشان می‌دهد که این مدل، روش خوبی جهت تعیین مقاصد عملیاتی دشمن و فرآیند تصمیم‌سازی بر اساس مشاهدات جنگ الکترونیک از اقدامات فیزیکی در صحنه‌های جنگ پیچیده می‌باشد.

در این مطالعه، تعداد حالات مدل در سناریوی نبرد احتمالی با نظر متخصصان و خبرگان نظامی کشور برابر ۵ در نظر گرفته شد که این تعداد در سناریوهای مختلف قابل تغییر است. همچنین، برخلاف مطالعات دیگر که از مدل مخفی مارکوف برای پیش‌بینی مسائل مختلف استفاده نموده‌اند، مقادیر اولیه پارامترهای مدل، عددی بین صفر و یک اتخاذ نشده بلکه از محاسبه احتمالات بر اساس تعداد مشاهدات جنگ الکترونیکی هر اقدام در سناریوی نبرد احتمالی استفاده شده است. در مجموع اگرچه حجم داده مطالعه حاضر از حجم داده یک صحنه نبرد واقعی کمتر بوده اما نتایج قابل قبولی از ارزیابی و پیش‌بینی مدل مخفی مارکوف شبیه‌سازی شده حاصل شده است که با دسترسی به داده‌های یک صحنه نبرد واقعی و به‌روزرسانی احتمالات توصیف کننده مدل به کمک الگوریتم‌های آموزش می‌توان مدلی ایده‌آل برای صحنه‌های نبرد واقعی به‌دست آورد.

در مطالعه حاضر، با توجه به مجموعه مشاهدات گسسته از صحنه نبرد، مدل مخفی مارکوف به کار رفته از نوع گسسته و تغییرناپذیر با زمان در نظر گرفته شد که در صورت ایجاد یک شبکه حسگری و دریافت لحظه‌ای داده‌ها می‌توان از یک مدل مخفی مارکوف پیوسته و تغییرپذیر با زمان برای ارزیابی داده‌های صحنه نبرد و پیش‌بینی مقاصد عملیاتی دشمن استفاده کرد و این حاکی از توانمندی بالای مدل مخفی مارکوف در پیش‌بینی و طبقه‌بندی داده‌هاست که در تحقیقات آتی می‌تواند مورد بررسی قرار گیرد.

از مزیت‌های اصلی این مطالعه گزارش و تفسیر ماتریس احتمالات انتقال است. با توجه به آنکه تعداد حالات مدل برابر ۵ حالت عملیاتی در نظر گرفته شد، برای اعداد ذکر شده در ماتریس احتمالات انتقال تفسیر مناسبی وجود دارد، مثلاً $a_{12} = 0.67$ بدان معناست که احتمال انتقال از حالت اول عملیاتی (غیرجنگی) به حالت دوم عملیاتی (پیش از نبرد) در سناریوی نبرد مورد مطالعه ۶۷ درصد بوده است. همچنین احتمالات کوچکتر از ۰/۱ در جدول (۲) بیانگر این موضوع است که احتمال انتقال بسیار ضعیف است؛ مانند انتقال از حالت عملیاتی غیرجنگی به حالت‌های عملیاتی جنگی و یا احتمال انتقال از حالت عملیاتی حمله گسترده به حمله بسیار گسترده.

ارزیابی مدل و پیش‌بینی مقاصد عملیاتی دشمن با توجه به اطلاعات داده شده به مدل نیز صورت گرفت و نتایج حاکی از توانمندی بالای مدل مخفی مارکوف بود، به‌طوری که این روش برای پیش‌بینی دنباله حالت‌های عملیاتی دشمن بر اساس مشاهدات جنگ الکترونیکی از اقدامات فیزیکی دشمن در صحنه نبرد کارساز بود.

یکی از محدودیت‌های اصلی این مطالعه عدم امکان دسترسی به داده‌های یک صحنه نبرد واقعی و کمبود داده‌های جمع‌آوری شده در سناریوی نبرد احتمالی بود که این به نوبهٔ خود تأثیر چشم‌گیری بر دقت مدل نهایی داشت و در صورت ایجاد چنین امکانی می‌توان مدلی ایده‌آل برای صحنه‌های نبرد واقعی به دست آورد.

در نتیجه‌گیری از پژوهش حاضر می‌توان گفت تحلیل رفتار دشمن و تعیین مقاصد عملیاتی آن جهت فرآیند تصمیم‌سازی نظامی در صحنه‌های جنگ پیچیده از طریق سیستم‌های هوشمند (به‌طور مثال با استفاده از مدل‌های مخفی مارکوف و بر اساس مشاهدات جنگ الکترونیک) سریع‌تر، دقیق‌تر و کم هزینه‌تر است که این امر در مسائل نظامی و دفاعی بسیار حائز اهمیت است. لذا به‌کارگیری مدل مخفی مارکوف در زمینه تحلیل رفتار و تعیین مقاصد عملیاتی دشمن و فرآیند تصمیم‌سازی نظامی پیشنهاد می‌شود.

۷- منابع

[1] S. H. Mohammadi Najm, "Cognitive war, the fifth dimension of the war," 1st ed., Tehran: Center for Future Studies of Defense Science and Technology, Institute for Defense Research and Training, 2009. (In Persian)

[2] E. A. Smith, "Complexity, Networking, and Effects-Based Operations: Approaching the" how to" of EBO," DTIC Document, 2005.

[3] E. A. Smith, "Effects based operations: Applying network centric warfare in peace, crisis, and war," DTIC Document, 2006.

[4] M. Frater and M. Ryan, "Electronic warfare for the digitized battlefield," Artech House, Inc., Norwood, MA, USA, 2001.

[5] R. Wolfe and M. J. Abramson, "Modern statistical methods in respiratory medicine," Respirology, vol. 19, no. 1, pp. 9-13, 2014.

[6] M. A. Pimentel, M. D. Santos, D. B. Springer, and G. D. Clifford, "Heart beat detection in multimodal physiological data using a hidden semi-Markov model and signal quality indices," Physiological Measurement, vol. 36, no. 8, p. 1717, 2015.

[7] C. Zhou, S. Huang, N. Xiong, SH. Yang, H. Li, Y. Qin, et al., "Design and Analysis of Multimodel-Based Anomaly Intrusion Detection Systems in Industrial Process Automation," IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics), vol. 45, no. 10, pp. 1345-1360, 2015.

[8] M. H. Moattar, "Hidden Markov Model and Training Algorithms," Dept. of Computer Engineering and Information Technology, AmirKabir University of Technology, Tehran, 2006. (In Persian)

[9] R. Marxer and H. Purwins, "Unsupervised Incremental Online Learning and Prediction of Musical Audio Signals," IEEE/ACM Transactions on Audio, Speech, and Language Processing, vol. 24, no. 5, pp. 863-874, 2016.

[10] B. B. Vizzotto, B. Zatt, M. Shafique, S. Bampi, and et al., "Model Predictive Hierarchical Rate Control With Markov Decision Process for Multiview Video Coding," IEEE Transactions on Circuits and Systems for Video Technology, vol. 23 , no. 12, pp. 2090-2104, 2013.

[11] K. Vimala, "Stress Causing Arrhythmia Detection from ECG Signal using HMM," IJIRCCE, vol. 2, no. 10, pp. 6079-6085, 2014.

[12] S. Nootyaskool and W. Choengtong, "Hidden Markov Models predict foreign exchange rate," Communications and Information Technologies (ISCIT), 14th International Symposium on Incheon, pp. 99-101, 2014.

[13] X. Chen, H. Zhang, AB. MacKenzie, and M. Matinmikko, "Predicting Spectrum Occupancies Using a Non-Stationary Hidden Markov Model," IEEE Wireless Communications Letters, vol. 3, no. 4, pp. 333-336, 2014.

[14] S. Keshvari, S. Bejani, A. R. Keshvari, and M. Abbasi, "Predicting the Level of Combatants' Readiness to Carry out Military Missions Using a Hidden Markov Model," Journal of military Psychology, vol. 7, no. 27, pp. 21-39, Autumn, 2016 (In Persian).

[15] L. Rabiner and B. H. Juang, "An introduction to hidden Markov models," IASSP, vol. 3, no. 1, pp. 1-4, 1986.

[16] D. Aberdeen, S. Thiebaux, and L. Zhang, "Decision Theoretic Military Operations Planning," In International Conference on Automated Planning and Scheduling (ICAPS), pp. 402-412, 2004.

[17] Y. K. Kevin, R. Mitchell, M. Solomon, and N. Lam, "Time Latency of Information in Networked Operations: Effect of "Human in the Loop," 2008.

[18] R. A. Howard, "Dynamic Programming and Markov Processes," the M.I.T. Press, 1960.

[19] M. Naghian Fesharaki, S. Sadati, A. H. Momeni Azndarian, and S. M. Hosseini, "Design Online Collaborative Planning Service Based on Markov Process in Command and Control Domain," Advanced Defense Sci. & Tech. vol. 7, pp. 147-159, 2017 (In Persian).

[20] A. J. Viterbi, "Error bounds for convolutional codes and an asymptotically optimal decoding algorithm," IEEE Trans Inf. Theory IT, vol. 13, no. 3, pp. 260-269, 1967.

[21] A. Babakura, MN. Sulaiman, N. Mustapha, and T. Perumal, "HMM-based decision model for smart home environment," International Journal of Smart Home, vol. 8, no.1, pp. 129-138, 2014.

[22] F. Madadizadeh, M. Montazeri, and A. Bahrampour, "Predicting of liver disease using Hidden Markov Model," RJMS, vol. 23, no. 146, pp. 66-74, 2016 (In Persian).

Journal of Electronical & Cyber Defence
Vol. 7, No. 1, 2019, Serial No. 25

The Presentation of a Model for Analyzing the Behavior of the Enemy Using Hidden Markov Models Based on Electronic Warfare Observations in Complex War Scenes

M. Babaei*, H. R. Lashkarian, M. Sheikhmohammady

*Imam Hossein Comprehensive University

(Received: 12/01/2018, Accepted: 26/02/2018)

ABSTRACT

Modeling is one of the basic tools for planning complex wars. Today's wars are very different due to the complexity and dynamism of the scenes compared with traditional wars and require the rapid and dynamic command and control so that they can react quickly against the changes in the battle scene and make decisions. In the information age, with the complexity of the battle scenes and the digitization of the battlefield, the observations of commanders are made using electronic warfare systems. In this paper, the sensemaking process of the stimuli and physical actions of the enemy in the war scene, which expresses our intuitive appreciation of the situation, has been modeled using hidden Markov models (HMM) based on the electronic warfare observations. This model has been used to analyze the behavior of the enemy and determine his operational objectives for the military decision-making process in order to adopt an appropriate response to the enemy. For this purpose, a possible United States' war scenario against the Islamic Republic of Iran has been studied from an electronic warfare perspective and used as the base of modeling. The time-invariant hidden Markov model of the first-order type has been considered, implying that all probabilities that describe the model do not change with time. The results of simulations show that this model is a good way to determine the enemy's operational objectives and the decision-making process based on the electronic warfare observations of physical actions in complex war scenes.

Keywords: Electronic Warfare, Complex War Scenes, Decision-making Process, Enemy's Behavior Analysis Model, Hidden Markov Models

* Corresponding Author Email: mbabaei@ihu.ac.ir