مجله علمی پژوهشی «پدافند الکترونیکی و سایبری»
سال ششم، شماره ۴، زمستان ۱۳۹۷؛ ص ۷۸-۶۱

# ارزیابی تهدید اهداف با استفاده از شبکه‌های فازی و احتمالاتی توأم مبتنی بر قواعد

**محسن یادگاری[1]، سید علیرضا سیدین[2]***

۱- دکتری برق، ۲- دانشیار، دانشکده مهندسی، دانشگاه فردوسی مشهد

(دریافت: ۱۳۹۶/۰۹/۲۷، پذیرش: ۱۳۹۷/۰۳/۰۶)

## چکیده

یکی از مهم‌ترین ارکان یک سامانه تلفیق داده، مسئله ارزیابی تهدید اهداف است. در این مقاله برای پیاده‌سازی یک شبکه کامل ارزیابی تهدید از دو الگوی ترسیمی نقشه شناختی فازی و شبکه بیزین استفاده شده است. ساختار این شبکه تعداد زیاد و متنوعی از متغیرهای ارزیابی تهدید را شامل شده و به‌طور مناسبی با یکدیگر مرتبط می‌سازد. با توجه به وجود عدم‌قطعیت در تمامی مسائل ارزیابی تهدید، انواع عدم قطعیت و روش‌های برخورد با آن در این مقاله موردتوجه قرار می‌گیرد. همچنین یک بررسی جامع بر روی انواع روش‌های لحاظ کردن هر دو نوع عدم قطعیت فازی و احتمالاتی انجام شده است و برای این موضوع روشی جدید ارائه می‌گردد. در این روش از دو شبکه فازی و بیزین مجزا برای لحاظ کردن عدم قطعیت‌ها استفاده شده که گام‌به‌گام روش پیشنهادی به‌طور کامل تشریح می‌گردد. همچنین در این مقاله چالش‌های بزرگ مسئله ارزیابی تهدید مطرح شده و نشان داده می‌شود که روش پیشنهادی قابلیت حل این مسائل را دارد. برای نشان دادن کارآمدی روش پیشنهادی مجموعه‌ای از معیارهای اعتبارسنجی کیفی و کمی در این مقاله ارائه شده است. یک رفتار حرکتی اهداف هوایی شبیه‌سازی شده و نتایج روش پیشنهادی به‌طور کیفی و کمی با دو روش نقشه شناختی فازی و شبکه بیزین مقایسه می‌شود. این نتایج بیانگر آن هستند که روش پیشنهادی ازلحاظ جذر میانگین مربعات خطا، درجه حساسیت کلی و جزئی و درجه تفکیک‌پذیری بهتر از دو روش دیگر عمل می‌کند. همچنین کارآمدی ساختار و روش پیشنهادشده مورد تأیید متخصصین حوزه مدیریت نبرد قرار گرفته است.

**واژه‌های کلیدی:** ارزیابی تهدید، نقشه شناختی فازی، شبکه بیزین، قواعد، عدم قطعیت فازی و احتمالاتی، معیارهای اعتبارسنجی

## ۱- مقدمه

در سامانه‌های مدیریت نبرد، تلفیق داده[1] یک قسمت اصلی و مهم و درواقع قلب سامانه است [۱]. در فرآیند تلفیق داده، داده‌ها و اطلاعات حسگرها و یا بخش‌های مختلف با یکدیگر ترکیب می‌شوند تا داده و یا اطلاعات بهتر و با عدم قطعیت کمتری حاصل شود. به‌عنوان‌مثال وقتی برای ره‌گیری یک هدف از ترکیب داده چند حسگر رادار استفاده می‌شود، با یک مسئله تلفیق داده روبرو هستیم. همچنین این ترکیب و تلفیق داده می‌تواند در سطوح بالاتری انجام شود. ترکیب نظرات چندین متخصص در رابطه با یک موضوع، ترکیب مفاهیم کیفی و ... مثال‌هایی از تلفیق سطح بالای داده‌هاست. در مسئله تلفیق داده، تنوع در نوع حسگر، تعداد حسگر، قابلیت اعتماد و عدم قطعیت هر حسگر بسیار مهم بوده و حسگرهای با خروجی‌های غیر همجنس و غیرهمگون می‌توانند دارای همپوشانی و یا وابستگی باشند [۲]. تنوع در نوع داده ورودی، نوع اهداف، شرایط محیط نبرد، نوع سلاح، نوع حمله و راهبرد نبرد ازجمله مواردی هستند که اهمیت مسئله تلفیق داده را نشان داده و درواقع می‌توان گفت که یک سامانه مدیریت نبرد قابل‌اطمینان، بدون استفاده از تلفیق داده تحقق‌پذیر نیست.

در طول زمانی که مفهوم تلفیق داده در سامانه‌های مهندسی و ناوبری به‌وجود آمده است، الگوهای مختلفی برای یک سامانه تلفیق داده ارائه شده است [۳]. این ناهمگونی در تعاریف و الگوها سدی در مقابل برقراری ارتباط بین محققان مختلف در این زمینه شده بود تا این‌که برای بهبود روابط میان محققان نظامی و مهندسین سامانه، گروه مدیران مشترک آزمایشگاه‌های تلفیق داده[2] (JDL)، در سال ۱۹۸۶، الگوی JDL را ارائه نمودند [۴]. در سطح ۱، این الگو اطلاعات از حسگرها استخراج شده و بعد از

* رایانامه نویسنده مسئول: seyedin@um.ac.ir

1- Data fusion

2- Joint Directors of Laboratories

پردازش‌های اولیه به‌صورت داده در اختیار سطوح بالاتر قرار می‌گیرد. در سطح ۲، ارزیابی وضعیت[1] انجام می‌شود که هدف از آن ایجاد یک بیان از ارتباطات فعلی میان موجودات و رویدادهای پیرامون آن به‌صورت پویا است. سطح ۳، این الگو مسئله ارزیابی تهدید[2] است که در آن شرایط فعلی صحنه به آینده مرتبط شده و استنتاجاتی در مورد تهدیدات دشمن، میزان آسیب‌پذیری دوست و دشمن و فرصت‌های مناسب برای اجرای عملیات، به دست می‌آید [۶-۵].

ارزیابی تهدید یک پردازش سخت و مشکل است، چراکه از یک‌سو با انبوهی از متغیرهای مرتبط با تهدید مواجه هستیم که می‌بایست به‌درستی پیاده‌سازی شده و مورد استنتاج قرار گیرد و از طرف دیگر بر مبنای شرایط فعلی باید نیت و قصد[3] دشمن، قدرت و قابلیت[4] دشمن و فرصت‌های[5] پیش روی دشمن ارزیابی شود [۸-۷].

همچنین مسئله لحاظ کردن عدم قطعیت‌های موجود در متغیرهای ارزیابی تهدید و رسیدن به یک استنتاج درست بسیار مهم است و ارزیابی نادرست از تهدید یک هدف ممکن است نتایج بسیار زیانباری برای مدیریت نبرد در پی داشته باشد.

فرآیند ارزیابی تهدید برای استفاده در سطوح بالاتر الگوی JDL و نیز درک مواردی چون میدان عمل، میزان قدرت انهدام دشمن، به‌کارگیری یگان نظامی، شبکه‌های در حال کار و تأثیرات محیطی و تخصیص سلاح استفاده می‌شود [۹].

تاکنون برای پیاده‌سازی یک شبکه ارزیابی تهدید روش‌های مختلفی ارائه شده است. با توجه به اینکه مسئله ارزیابی تهدید بیشتر جنبه کیفی داشته و داده‌ی عملیاتی برای روش‌های مبتنی بر یادگیری به‌سختی قابل فراهم کردن است، اکثر روش‌های موجود با استفاده از ساختارهای مبتنی بر دانش انجام می‌شود [۱۱-۱۰]. در این روش‌ها با استفاده از مجموعه‌ای از قوانین[6]، دانش یک خبره و متخصص پیاده‌سازی می‌شود. این قوانین معمولاً بسته به نوع عدم قطعیت متغیرها و شرایط می‌تواند به‌صورت قوانین فازی [۱۲] و یا قوانین احتمالاتی [۱۳] بیان شود. چالش اساسی در این روش‌ها در نظر گرفتن هم‌زمان هر دو عدم قطعیت فازی و احتمالاتی در متغیرهاست. در شرایط واقعی هر دو نوع عدم قطعیت وجود داشته، درنتیجه نیاز به روشی برای لحاظ کردن هر دو نوع عدم قطعیت، ضروری است.

در این مقاله مسئله ارزیابی تهدید به‌طور جامع موردبررسی قرار می‌گیرد، به‌گونه‌ای که مسائل و چالش‌های مطرح در پیاده‌سازی واقعی و عملی یک سامانه ارزیابی تهدید لحاظ می‌شود. هدف این مقاله، رسیدن به یک شبکه قدرتمند ارزیابی تهدید است به‌گونه‌ای که اهداف مهم زیر در آن تحقق یابد.

۱. پیاده‌سازی متغیرهای زیاد و متنوع و بیان ارتباط میان آن‌ها جهت رسیدن به فرصت، قابلیت، نیت و درنهایت میزان تهدید اهداف.

۲. ارائه ساختاری جهت لحاظ کردن هم‌زمان عدم قطعیت فازی و احتمالاتی متغیرها و قوانین حاکم بر آن.

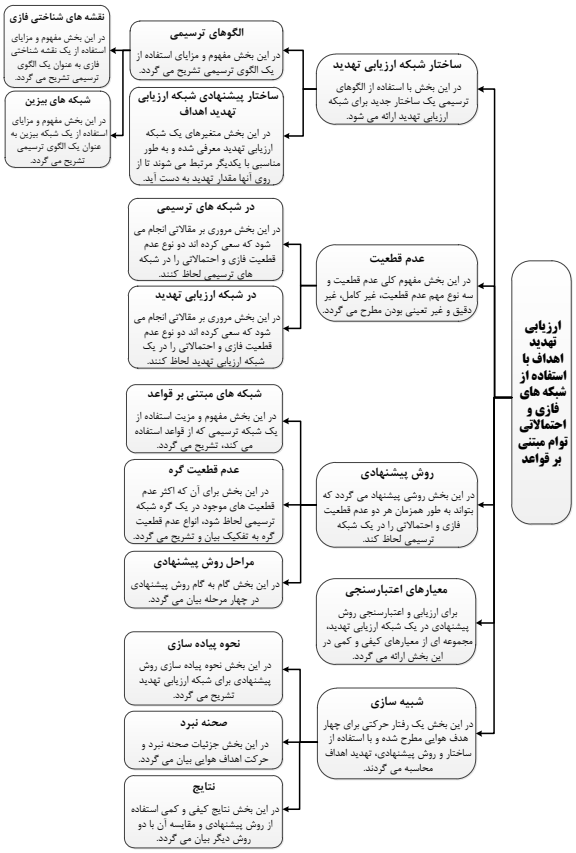
۳. چیره شدن بر چالش‌های رایج مسئله ارزیابی تهدید.

۴. ارائه معیارهایی مناسب جهت اعتبارسنجی و مقایسه روش‌های مختلف ارزیابی تهدید.

برای رسیدن به این اهداف و ارائه روشی جدید و کارآمد، مقالات و مراجع حوزه ارزیابی تهدید به‌طور عمیقی موردبررسی قرار گرفته و با استفاده از نظرات متخصصین حوزه مدیریت نبرد، روش پیشنهادی این مقاله ارائه شده است. همچنین روش پیشنهادی با استفاده از معیارهای مختلف کیفی و کمی مورد ارزیابی و اعتبارسنجی قرار گرفته است.

در بخش دوم این مقاله ساختار پیشنهادی مسئله ارزیابی تهدید بر اساس الگوهای ترسیمی بیان و تشریح می‌شود. در بخش سوم، بحث عدم قطعیت در متغیرهای ارزیابی تهدید مطرح می‌گردد. در بخش چهارم با توجه به مبانی بررسی‌شده در بخش سوم، اصول روش پیشنهادی جهت حل مسئله ارزیابی تهدید بررسی می‌شود. در بخش پنجم معیارهای اعتبارسنجی یک شبکه ارزیابی تهدید مطرح خواهد شد. در بخش ششم نیز ابتدا یک رفتار حرکتی اهداف هوایی مطرح شده سپس شبکه و روش‌های پیشنهادی بر روی آن مورد شبیه‌سازی قرار می‌گیرد و کارآمدی روش بر مبنای معیارهای اعتبارسنجی نشان داده خواهد شد. در انتها، نتیجه‌گیری و جمع‌بندی مباحث و نیز منابع تحقیق ارائه می‌گردد. نمودار مفهومی ساختار این مقاله در شکل (۱) نشان داده شده است.

1- Situation assessment
2- Threat assessment
3- Intent
4- Capability
5- Opportunity
6- Rule




**شکل (۱):** نمودار مفهومی ساختار مقاله

## ۲- ساختار شبکه ارزیابی تهدید

در این بخش ابتدا نحوه پیاده‌سازی یک شبکه بر اساس الگوهای ترسیمی موردبررسی قرار گرفته، سپس بر مبنای آن ساختار پیشنهادی شبکه ارزیابی تهدید ارائه می‌گردد.

### ۲-۱- الگوهای ترسیمی

به‌طورکلی برای پیاده‌سازی یک سامانه، تاکنون روش‌های مختلف و متنوعی نظیر الگوهای فضای حالت[1]، شبکه‌های عصبی[2] و ... مطرح شده است.

یکی از روش‌های پرکاربرد در این حوزه الگوهای ترسیمی[3] هستند [۱۵-۱۴]. در این الگوها، مفاهیم، حالات، ورودی‌ها، خروجی‌ها و ... به‌صورت مجموعه‌ای از گره‌ها[4] نمایش داده می‌شوند. ارتباط بین این گره‌ها با یک‌رشته خطوط ارتباطی[5] مشخص می‌گردد. نقشه‌های شناختی فازی[6] (FCM) برای الگوهای فازی [۱۷-۱۶] و شبکه‌های بیزین[7] (BN) برای الگوهای احتمالاتی [۱۷] ازجمله مهم‌ترین الگوهای ترسیمی هستند.

الگوهای ترسیمی دارای این مزیت بزرگ هستند که هر گره در این الگوها، دارای یک مفهوم و واقعیت فیزیکی است و می‌توان بر روی هر گره یک استنتاج و تصمیم‌گیری داشت. درحالی‌که در بعضی الگوها نظیر شبکه‌های عصبی بعضی گره‌ها فقط جنبه ریاضی داشته و مفهوم خارجی ندارند. از سوی دیگر شبکه‌هایی نظیر شبکه عصبی برای ساخت و استنتاج نیازمند داده‌های آموزشی هستند؛ درحالی‌که می‌توان شبکه‌های ترسیمی را بدون داده آموزشی نیز ساخت. همچنین دانش و اطلاعات یک خبره در یک الگوی ترسیمی بسیار ساده‌تر و قابل‌فهم‌تر پیاده‌سازی می‌شود.

درنتیجه این نحوه پیاده‌سازی دارای مزایایی نظیر پیاده‌سازی سامانه‌های متنوع، قابلیت پیاده‌سازی دانش بشری، عدم نیاز به داده آموزشی[8]، قابل تفسیر بودن[9] و تصمیم‌گیری، انعطاف‌پذیری[10]، قابلیت تلفیق اطلاعات[11] و قابلیت نمایش عدم قطعیت است. به همین علت یکی از راه‌های مناسب برای محاسبه درجه تهدید از روی متغیرهای آن، استفاده از الگوهای ترسیمی است. در این الگوها متغیرهای ارزیابی تهدید و خود تهدید با یک گره در الگو نشان داده می‌شوند. ارتباط منطقی بین متغیرها نیز ارتباط بین گره‌ها را تشکیل می‌دهد.

#### ۲-۱-۱- نقشه‌های شناختی فازی

یکی از الگوهای ترسیمی پرکاربرد برای پیاده‌سازی سامانه‌های پویا، نقشه‌های شناختی فازی است [۱۸-۱۶]. این روش بر پایه منطق فازی لطفی‌زاده[12] و الگوهای شناختی اکسلرد [۱۹][13] اولین بار توسط آقای کاسکو[14] در سال ۱۹۸۶ معرفی گردید [۲۰].

در این روش یک سامانه با یک‌رشته گره‌ها[15] و خطوط جهتی[16] نشان داده شده و پیاده‌سازی می‌گردد. گره‌ها بیانگر حالات، خصوصیات، ورودی‌ها، خروجی‌ها و متغیرهای اثرگذار سامانه هستند. خطوط نیز روابط علی و معلولی بین گره‌ها را نشان می‌دهند.

1- State– Space modeling
2- Neural Network
3- Graphical Model
4- Node
5- Link
6- Fuzzy Cognitive Map

7- Bayesian Network
8- Learning data
9- Interpretability
10- Flexibility
11- Information fusion
12- Lotfi A. Zadeh
13- Robert Axelrod
14- Bart Kosko
15- Concept
16- Directed edge

در حقیقت FCM به دنبال آن است که یک سامانه همان‌گونه که درک می‌شود پیاده‌سازی گردد. این نقشه‌ها به علت سهولت درک و ساخت، انعطاف‌پذیری بالا، کاربرد گسترده و تطبیق‌پذیری با مسائل مختلف، توجه پژوهشگران زیادی را به خود جلب کرده است [۲۱]؛ اما بااین‌همه، نقشه‌های شناختی فازی تنها قابلیت برخورد و لحاظ کردن عدم قطعیت فازی را دارا هستند [۲۲].

یادگیری یک نقشه شناختی فازی می‌تواند بر اساس مجموعه‌ای از داده‌ها به‌صورت کمی و یا بر اساس نظرات متخصصین به‌صورت قوانین کیفی، انجام پذیرد.

### ۲-۱-۲- شبکه‌های بیزین

مبانی شبکه‌های بیزین بر روی نظریه احتمال استوار بوده و بر مبنای فعالیت‌ها و تحقیقات آقای Pearl به‌عنوان یک ابزار قدرتمند پیاده‌سازی، شکل گرفتند و در کاربردهای متنوعی به کار گرفته شدند [۲۳].

شبکه بیزین (که به‌عنوان شبکه باور بیزین[1] (BBN) نیز شناخته می‌شود)، یک الگوی ترسیمی است که یک سامانه را به‌صورت احتمالاتی پیاده‌سازی می‌کند [۲۴-۲۳]. در این الگو، گره‌ها متغیرهای تصادفی بوده که رخداد هر حالت آن با یک احتمال بیان می‌شود. گره‌ها بیانگر مفاهیم و متغیرهای سامانه هستند. در شبکه‌های بیزین ارتباط بین حالات دو گره متصل‌به‌هم به‌صورت احتمالاتی و توسط جدول احتمالات شرطی[2] (CPT) بیان می‌گردد. این جدول معمولاً توسط یک یا چند فرد خبره و متخصص بیان شده و یا در صورت در دسترس بودن داده‌های سامانه، می‌توان از طریق آموزش به آن رسید [۲۵]. درنتیجه شبکه‌ی بیزین یک گراف متشکل از گره‌ها و ارتباطات با تفاسیر زیر است.

- هر گره در شبکه نشان‌دهنده‌ی یک متغیر تصادفی است که می‌تواند چندین حالت داشته باشد. این حالت‌ها تشکیل‌دهنده فضای نمونه‌ای هستند که در آن متغیر تصادفی تعریف شده است.
- هر پیوند و ارتباط در شبکه، یک ارتباط یا وابستگی شرطی احتمالاتی بین دو متغیر بوده که توسط جدول احتمالات شرطی بیان می‌شود.
- مفهوم علیت بین دو گره مرتبط، توسط یک پیکان جهت‌دار از گره «علت» به گره «اثر» نشان داده می‌شود.
- هنگامی‌که توسط یک مشاهده‌گر بیرونی و یا یک اندازه‌گیری، حالت یک گره مشخص شود، به این مشاهدات، شواهد[3] گفته می‌شود.
- استنتاج در شبکه‌های بیزین بر مبنای استنتاج احتمالاتی بیز بوده و شبکه تنها قادر به لحاظ کردن عدم قطعیت‌های احتمالاتی است [۲۶].

## ۲-۲- ساختار پیشنهادی شبکه ارزیابی تهدید اهداف

در شبکه ارزیابی تهدید با انواع و اقسام داده‌ها و متغیرها مواجه هستیم [۲۸-۲۷]. بعضی از این متغیرها از حسگرها به‌دست‌آمده و بعضی متغیرها نتیجه پردازش هستند. همچنین یک‌رشته از متغیرها وابسته به نحوه حرکت اهداف و بعضی وابسته به شرایط محیطی هستند [۳۰-۲۹]. درنتیجه دسته‌بندی مناسب این متغیرها و نحوه ارتباط بین آن‌ها جهت قرار گرفتن در شبکه ارزیابی تهدید بسیار حائز اهمیت است.

با بررسی گسترده مقالات و مراجع مختلف در حوزه ارزیابی تهدید و سامانه‌های تلفیق داده، متغیرهای متنوع و کاملی برای استنتاج تهدید اهداف هوایی مورداستفاده قرار گرفت. این متغیرها در جدول (۱) نشان داده شده است. متغیرها به‌گونه‌ای تدوین شده‌اند که فرض بر این است که منابع خودی در سطح دریا بوده و تهدید اهداف هوایی نسبت به این منابع خودی سنجیده می‌شود.

**جدول (۱):** متغیرهای ارزیابی تهدید اهداف هوایی

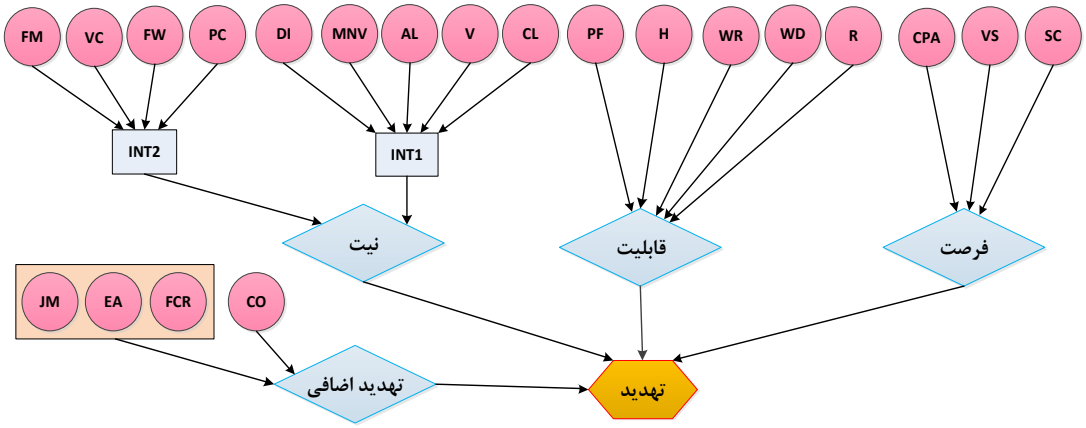
| ردیف | نام متغیر | مخفف | توضیحات |
|---|---|---|---|
| ۱ | Sea Condition | SC | شرایط دریا (سرعت آب، ارتفاع امواج و ...) |
| ۲ | Visibility | VS | میزان مشاهده‌پذیر بودن هدف |
| ۳ | Closing Point Approach | CPA | متغیری است که از روی فاصله، سرعت و جهت حرکت هدف به دست می‌آید. |
| ۴ | Range | R | فاصله هدف تا خودی |
| ۵ | Weapon Destruction | WD | میزان قدرت تخریب سلاح‌های هدف |
| ۶ | Weapon Range | WR | برد سلاح‌های هدف |
| ۷ | Height | H | ارتفاع هدف |
| ۸ | Platform | PF | نوع هدف |
| ۹ | Closing | CL | بیانگر دور یا نزدیک شدن هدف به سمت خودی است. |
| ۱۰ | Velocity | V | سرعت هدف |
| ۱۱ | Along | AL | میزان تبعیت یک هدف هوایی از مسیرهای تجاری مشخص‌شده |
| ۱۲ | Maneuver | MNV | مانور هدف |
| ۱۳ | Dive | DI | تغییرات ارتفاع هدف |
| ۱۴ | Political Climate | PC | شرایط سیاسی صحنه نبرد |
| ۱۵ | Feet Wet | FW | عبور از سطح آب هدف |
| ۱۶ | Voice Communication | VC | مشخص‌کننده برقراری یک مکالمه صوتی بین هدف و خودی |
| ۱۷ | Friendly Mode | FM | خروجی حسگر IFF |
| ۱۸ | Jamming | JM | عملیات جنگ الکترونیک |
| ۱۹ | ESM Alarm | EA | انواع هشدار حسگر ESM |
| ۲۰ | Fire Control Radar | FCR | خروجی رادار کنترل آتش |
| ۲۱ | Commander Opinion | CO | نظرات فرمانده |

1- Bayesian Belief Network
2- Conditional Probability Table
3- Evidence

با دسته‌بندی و مرتبط نمودن متغیرهای وابسته به یکدیگر و نیز بر مبنای اثرگذاری هر متغیر بر روی فرصت، قابلیت و یا نیت اهداف، شبکه پیشنهادی ارزیابی تهدید به‌صورت شکل (۲) تدوین شد. در این شکل هر متغیر ارزیابی تهدید در نقش یک گره ورودی ظاهر می‌شود.

شبکه پیشنهادی دارای چندین مزیت است. در این شبکه متغیرهای مرتبط با یکدیگر تفکیک‌شده و به‌صورت مناسبی به فرصت، قابلیت و یا نیت هدف مرتبط شده است. با این شبکه تعداد قوانین فازی و یا CPTهای موردنیاز برای استنتاج بسیار کم شده و کاملاً قابل بیان توسط یک خبره است. همچنین ساختار حساسیت مناسبی بین خروجی و ورودی‌ها برقرار می‌کند. در شبکه پیشنهادی، یک‌رشته از متغیرهای مهم و مؤثرتر در سنجش تهدید به‌طور مستقیم و به‌صورت یک مؤلفه تهدید اضافی به خروجی نهایی متصل شده است. این کار علاوه بر بالا بردن حساسیت ساختار به این متغیرها و نیز سایر متغیرها، اثر این متغیرها را نیز به‌صورت بهتری لحاظ می‌کند.

همچنین جهت سهولت بیان قوانین و با توجه به تعداد ورودی‌های زیاد گره نیت، از دو گره میانی INT1 و INT2 استفاده شده است.




**شکل (۲):** شبکه ارزیابی تهدید اهداف هوایی

## ۳- عدم قطعیت

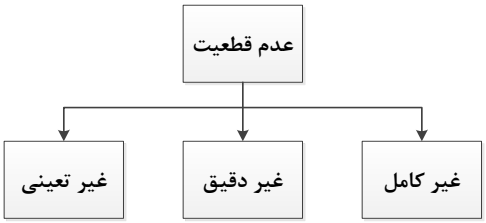
عدم قطعیت یکی از مسائل جدی و موردتوجه سامانه‌های امروزی است. علاوه‌بر این که در پیاده‌سازی یک سامانه می‌بایست عدم قطعیت لحاظ شود، گاهی اوقات عدم قطعیت، خود انتخاب ساختار الگو را نیز تحت تأثیر قرار می‌دهد. در سامانه‌هایی که با داده‌های کیفی و یا کمی کار می‌کنند، در هرکدام به‌نوعی با عدم قطعیت و یا جهل[1] روبرو هستیم. درک اشتباه از یک سامانه، نظرات مختلف متخصصین، شرایط مختلف فیزیکی و محیطی سامانه، خطای حسگرها، نقص داده[2]، ماهیت متفاوت داده‌ها[3]، داده‌های جعلی[4]، داده‌های متناقض[5] و ... همه از انواع و دلایل عدم قطعیت در سامانه‌ها می‌باشند [۳۱].

در یک شبکه ارزیابی تهدید معمولاً با انبوهی از داده‌ها و متغیرها با جنس‌ها و ماهیت‌های متفاوت و عدم قطعیت‌های مختلف روبرو هستیم [۳۲]. یک سامانه مؤثر ارزیابی تهدید باید بتواند این متغیرها را به‌صورت مناسبی تلفیق کرده و به یک استنتاج درست برای تهدید برسد. این تلفیق یک تلفیق سطح بالای داده‌هاست[6] و بسته به نوع عدم قطعیت داده‌ها از روش‌های متفاوتی برای تلفیق استفاده می‌شود.

در یک سامانه واقعی ممکن است انواع عدم قطعیت‌ها نظیر غیر کامل بودن اطلاعات[7]، غیر دقیق[8] و غیر تعینی[9] بودن داده‌ها، هم‌زمان اتفاق افتد [۳۳]. در چنین شرایطی دنبال روشی هستیم که بتواند تمام این موارد را لحاظ کند.

این طبقه‌بندی عدم قطعیت که در عمل کاربرد زیادی دارد، در شکل (۳) نشان داده شده است.

1- Ignorance
2- Data imperfection
3- Data modality
4- Outliers and spurious data
5- Conflicting data
6- High level data fusion
7- Incompleteness
8- Imprecision
9- Uncertainty




**شکل (۳):** یک طبقه‌بندی کاربردی از انواع عدم قطعیت [۳۳]

این تقسیم‌بندی از عدم قطعیت دارای تعابیر زیر است:

**غیرکامل:** هنگامی است که یک قسمت از اطلاعات بیان نشود. به‌عنوان‌مثال اگر نوع یک هدف متحرک بیان شود اما سرعت آن مشخص نگردد.

**غیردقیق:** هنگامی است که یک اطلاعات قطعی اما غیردقیق بیان شود. به‌عنوان‌مثال اگر گفته شود: سرعت هدف کم است. این عبارت بیانگر آن است که به‌طور قطع سرعت هدف کم است اما به‌طور دقیق مشخص نیست که سرعت چه مقداری دارد.

**غیرتعینی:** هنگامی است که یک اطلاعات غیرقابل تعین و غیریقینی بیان شود. به‌عنوان‌مثال اگر گفته شود: سرعت هدف احتمالاً $20\frac{m}{s}$ است. این جمله یک اطلاعات غیرتعینی اما درعین‌حال دقیق به دست می‌دهد.

برای نمایش اطلاعات غیردقیق می‌توان به‌خوبی از نظریه فازی استفاده کرد. این نظریه بر پایه منطق فازی می‌تواند اطلاعات غیر دقیق و فازی را نمایش دهد. برای نمایش اطلاعات غیرتعینی نیز می‌توان به‌خوبی از نظریه احتمال استفاده کرد. این نظریه بر پایه روابط احتمالاتی می‌تواند اطلاعات غیریقینی و تصادفی را نمایش دهد.

در حالت کلی می‌توان عدم قطعیت را به دو دسته عدم قطعیت تصادفی و غیرتصادفی تقسیم کرد [۳۴]. در بسیاری از کاربردها، الگوسازی احتمالاتی مناسب برای عدم قطعیت تصادفی و الگوسازی فازی مناسب برای عدم قطعیت غیر تصادفی است [۳۶-۳۵]. عدم قطعیت فازی معمولاً ناشی از اندازه‌گیری نادرست، یا درک نادرست فرآیند محیط است. وقتی‌که تصمیم‌گیری‌ها مبتنی بر تصمیم انسانی است و مرزها مشخص نیستند [۳۷].

عدم قطعیت احتمالاتی ناشی از طبیعت سامانه، اغتشاش و نویز خارجی، ناکافی بودن نمونه‌های داده و داده‌های گمشده است [۳۸].

از دیگر سو تمرکز عدم قطعیت احتمالاتی مبتنی بر آینده و عدم قطعیت فازی مبتنی بر گذشته و حال است [۳۹]. درنتیجه این دو عدم قطعیت مکمل هم هستند [۳۶] و در بسیاری از مسائل نیازمند آن هستیم که هر دو نوع عدم قطعیت باهم لحاظ شوند.

## ۳-۱- در شبکه‌های ترسیمی

در یک شبکه ترسیمی، به‌علت وجود منابع مختلف خطا و عدم قطعیت در گره‌ها، نحوه برخورد کردن با عدم قطعیت بسیار مهم است. این عدم قطعیت ممکن است ناشی از مشاهدات، ناکامل بودن اطلاعات متغیرها و یا مبهم بودن اطلاعات آن و یا غیریقینی بودن ارتباط بین متغیرها باشد [۴۰].

با توجه به این‌که شبکه‌های شناختی و بیزین برای پیاده‌سازی بسیاری از سامانه‌ها مناسب بوده اما هرکدام دو نوع مختلف عدم قطعیت را لحاظ می‌کنند، بعضی محققین به فکر استفاده هم‌زمان این دو شبکه افتاده‌اند؛ اما تمام این تلاش‌ها به این سمت رفته است که شبکه شناختی به بیزین و یا بر عکس تبدیل شود و یا این‌که دو شبکه با یک‌رشته تبدیلات و محدودیت‌ها در یک شبکه تجمیع گردند که معمولاً این روش‌ها منجر به از دست دادن بخشی از اطلاعات می‌شوند [۴۱].

در بعضی تحقیقات نحوه تبدیل شبکه شناختی به شبکه بیزین بحث شده است. در [۴۲] دو شبکه فازی و بیزین با یکدیگر مقایسه و بیان شده که بهتر است استخراج دانش به عهده یک شبکه فازی و استنتاج با شبکه بیزین باشد. در [۴۳] ساختار این نحوه تبدیل بیان شده است به‌گونه‌ای که ابتدا یک شبکه علّی ساخته شده و بعد، از روی آن یک شبکه بیزین بانام شبکه علّی بیزین[1] و یا شبکه بیزین شناختی[2] طراحی می‌شود. مشکل بزرگ این روش‌ها از دست دادن اطلاعات هنگام تبدیل است.

در بعضی تحقیقات دیگر به یک شبکه فازی، عدم قطعیت احتمالاتی اضافه شده است. در [۴۴] یک شبکه ادراکی فازی احتمالاتی[3] پیشنهاد شده است. در این شبکه عدم قطعیت احتمالاتی فقط در گره‌ها لحاظ می‌شوند و فرض بر این است که گره‌ها دارای نویز گوسی هستند. به‌عبارت‌دیگر هر گره یک پیشامد فازی در نظر گرفته می‌شود؛ که این فرضیات در بعضی مسائل همواره درست نیست.

یک دسته دیگر از روش‌ها، موسوم به شبکه‌های فازی بیزین[4] روش‌هایی هستند که مبنای آن‌ها یک شبکه بیزین بوده و در آن یا منطق فازی در شبکه به‌گونه‌ای به احتمالات تبدیل می‌شود [۴۵] و یا از منطق فازی به‌عنوان یک گسسته‌ساز در ورودی شبکه بیزین استفاده می‌شود [۴۶]. در این‌گونه روش‌ها هم با از دست دادن اطلاعات مواجه هستیم.

1- Bayesian Causal Map
2- Cognitive Bayesian Network
3- Probabilistic Fuzzy Cognitive Map
4- Fuzzy Bayesian Network

در [۴۱] کاربرد هر دو شبکه فازی و بیزین در تحلیل علیت ریشه[1] بررسی شده و یک BN به FCM تبدیل می‌شود.

در [۴۷] هم یک شبکه شناختی احتمالاتی تعریف شده، به‌گونه‌ای که اثرهای آن احتمالاتی هستند. در این مقاله نیز اثرات علی و معلولی به احتمالات تبدیل شده‌اند و مشکل از دست دادن اطلاعات وجود دارد.

### ۳-۲- در شبکه ارزیابی تهدید

بحث عدم قطعیت و لحاظ کردن آن در یک سامانه ارزیابی تهدید مسئله بسیار مهمی است [۴۸]. در عمل یک سامانه ارزیابی تهدید متشکل از گره‌ها و ارتباطات هم فازی و هم احتمالاتی است [۴۹]. استفاده از منطق فازی و روش بیزین نیز جزء روش‌های اصلی محاسبه ارزیابی تهدید به‌حساب می‌آیند [۲۷]؛ اما تاکنون تمام سامانه‌های پیاده شده ارزیابی تهدید به یکی از سه صورت زیر بوده است.

۱- تمام سامانه به‌صورت فازی پیاده‌سازی شده است [۱۲, ۲۸, ۵۴-۵۰]. لذا روش پیشنهادی این مقالات قابلیت در نظر گرفتن عدم قطعیت احتمالاتی را ندارد.

۲- تمام سامانه به‌صورت احتمالاتی پیاده‌سازی شده است [۵۸-۵۵]. درنتیجه روش پیشنهادی این مقالات قابلیت در نظر گرفتن عدم قطعیت فازی را ندارد.

۳- از روابط تبدیل فازی به احتمال و یا بالعکس استفاده شده و درنهایت یک سامانه فازی و یا احتمالاتی پیاده شده است [۵ و ۴۹]. روش پیشنهادی این مقالات نیز مشکل از دست دادن اطلاعات و درست لحاظ نکردن عدم قطعیت را دارد.

درنتیجه می‌توان برای یک سامانه ارزیابی تهدید به‌خوبی از روش پیشنهادی شرح داده‌شده در بخش بعدی استفاده کرد.

## ۴- روش پیشنهادی

در این بخش روش پیشنهادی این مقاله برای لحاظ کردن هردو نوع عدم قطعیت فازی و احتمالاتی در یک شبکه ترسیمی برای ارزیابی تهدید مطرح می‌گردد. ابتدا ساختار شبکه‌های مبتنی بر قواعد به‌عنوان یک ساختار مبنا بررسی شده، سپس نحوه لحاظ کردن عدم قطعیت در گره‌های شبکه و مراحل روش پیشنهادی ارائه می‌گردد.

### ۴-۱- شبکه‌های مبتنی بر قواعد

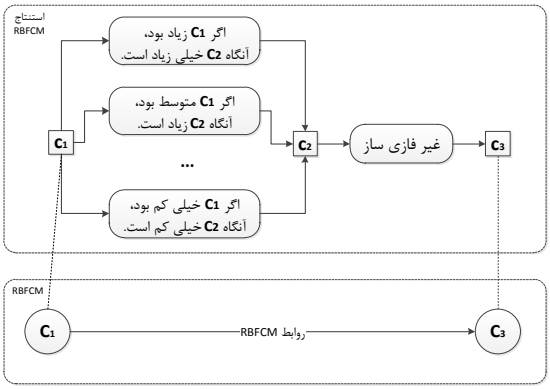
در ساختار پایه‌ای و متداول FCM، وزن هر ارتباط عددی در بازه [۱،۱-] است که وزن ۱، نشان‌دهنده ارتباط کامل مستقیم و وزن ۱- بیانگر ارتباط کامل معکوس است. اعداد بین این دو عدد میزان نسبی ارتباط را نشان می‌دهند.

این ساختار پایه‌ای FCM دارای یک‌رشته محدودیت‌ها و کمبودهای جدی است. ازجمله این‌که در شبکه FCM متداول رابطه بین دو گره بر مبنای یک مجموعه اعداد توصیف می‌شود و این موضوع باعث می‌شود که ساختار تنها قادر به توصیف روابط خطی بین دو گره باشد. درحالی‌که در بسیاری از مواقع روابط بین دو گره حالت غیرخطی دارند [۵۹]. برای حل این مشکل کاروالو و تام پیشنهاد شبکه مبتنی بر قواعد (RBFCM)[2] را دادند [۶۱-۶۰]. در این شبکه روابط بین دو گره بر اساس مجموعه‌ای از قوانین و قواعد تعریف می‌شود.

به‌عنوان‌مثال یک قانون در این روش می‌تواند به‌صورت زیر باشد.

اگر مقدار گره A کم بود، آن‌گاه مقدار گره B زیاد است.

مراحل استنتاج بین دو گره $C_1$ و $C_3$ در روش RBFCM در شکل (۴) نشان داده شده است.




**شکل (۴):** استنتاج در روش RBFCM [۶۲]

ساختار شبکه بیزین به ساختار شبکه RBFCM بسیار نزدیک است. چراکه می‌توان جدول احتمالات شرطی CPT مرتبط بین گره‌ها را به‌صورت قوانین مرتبط کننده گره‌ها در نظر گرفت. همچنین از قوانین فازی می‌توان در شبکه بیزین استفاده کرد. به‌عنوان‌مثال در [۶۳] روشی برای تولید CPT از روی قوانین فازی پیشنهاد شده است.

یک روش ساده برای استفاده از قوانین فازی در تولید CPT نگاشت مستقیم هر قانون به یک عضو جدول CPT است [۶۵-۶۴]. با این روش می‌توان هم از روی قوانین، CPT ساخت و هم بالعکس از روی CPT می‌توان به قوانین فازی رسید. درنتیجه می‌توان از این روش برای تولید دو شبکه FCM و بیزین مشابه بهره برد.

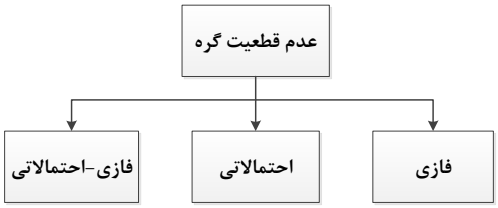
1- Root cause analysis

2- Rule Based Fuzzy Cognitive Map

### ۴-۲- عدم قطعیت گره

در الگوهای ترسیمی چنانچه مقدار هر گره تغییر کند، اثر آن بر روی کل شبکه ایجاد می‌شود. درنتیجه برای استنتاج نیازی نیست که همه گره‌ها مقدار گیرند. درنتیجه این الگوها به‌نوعی با ناکامل بودن اطلاعات کنار می‌آیند. چنانچه بتوان اطلاعات غیردقیق و غیرتعینی را نیز در این الگوها لحاظ کرد تا حد زیادی می‌توان انواع عدم قطعیت‌هایی که در مسائل و الگوهای واقعی اتفاق می‌افتد و در شکل (۳) نشان داده شد را در نظر گرفت.

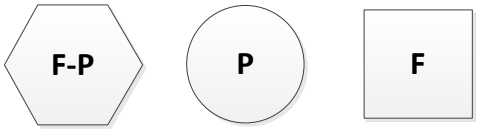
چنانچه برای نمایش عدم قطعیت از دو عدم قطعیت فازی و احتمالاتی بخواهیم استفاده کنیم، اطلاعات یک گره می‌تواند طبق شکل (۵) به‌صورت فازی، احتمالاتی و یا هر دو نمایش داده شود.




**شکل (۵):** انواع عدم قطعیت گره

درنتیجه می‌توان هم اطلاعات غیردقیق و هم غیرتعینی را در گره‌های یک الگوی ترسیمی نشان داد.

جهت نمایش بهتر عدم قطعیت، در شکل (۶) گره فازی با نماد مربع، گره احتمالاتی با دایره و گره فازی- احتمالاتی با شش ضلعی نشان داده شده است.




**شکل (۶):** نمایش گره‌های فازی، احتمالاتی و فازی-احتمالاتی

باید توجه داشت چون در شبکه‌های ترسیمی مقدار یک گره از روی گره‌های والد خود نتیجه می‌شود، درنتیجه فازی بودن یا تصادفی بودن یک گره، به گره‌های فرزند خود منتقل می‌شود.

### ۴-۳- مراحل روش پیشنهادی

در روش پیشنهادی برای در نظر گرفتن عدم قطعیت فازی و احتمالاتی به‌طور توأم، از یک سامانه ترکیبی تشکیل‌شده از نقشه شناختی فازی و شبکه بیزین استفاده می‌شود؛ اما برخلاف سایر روش‌ها که دو شبکه با یکدیگر ترکیب شده و یک شبکه واحد تشکیل می‌شود، در روش پیشنهادی از شیوه‌ای متفاوت و کارآمدتر استفاده می‌شود. در این روش دو شبکه به‌صورت جداگانه‌ای استفاده می‌گردند. متغیرها و عدم قطعیت‌های فازی توسط نقشه شناختی فازی پیاده‌سازی شده و متغیرها و عدم قطعیت‌های احتمالاتی توسط شبکه بیزین پیاده‌سازی می‌شوند. با این روش هم ماهیت عدم قطعیت‌های فازی و هم احتمالاتی حفظ شده و هم اینکه سامانه همان‌گونه که هست پیاده‌سازی می‌شود. گام‌به‌گام روش پیشنهادی در شکل (۸) تشریح شده است. در بخش‌های بعدی هر مرحله از روش توضیح داده خواهد شد.

#### ۴-۳-۱- تعیین حالات و توابع عضویت هر گره

ابتدا هر گره شبکه را با $x_k, k = 1,2,\dots,m$ نمایش می‌دهیم. هر گره دارای $n_k$ حالت بوده و هر حالت به‌صورت ریاضی با $X_k^{v_k},\ v_k = 1,2,\dots,n_k$ نمایش داده می‌شود. همچنین به هر حالت، یک تابع عضویت اختصاص داده می‌شود که با $f_{X_k^{v_k}}(x_k)$ بیان می‌گردد. درنتیجه موارد زیر در شبکه ترسیمی موردبحث، ابتدا می‌بایست مشخص گردند.

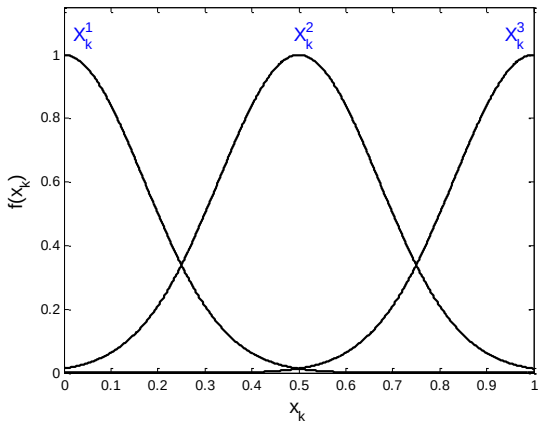
۱- نوع عدم قطعیت هر گره (فازی، احتمالاتی و یا فازی-احتمالاتی)

۲- تعداد حالت اختصاص‌یافته به هر گره= $X_k^{v_k},\ v_k = 1,2,\dots,n_k$

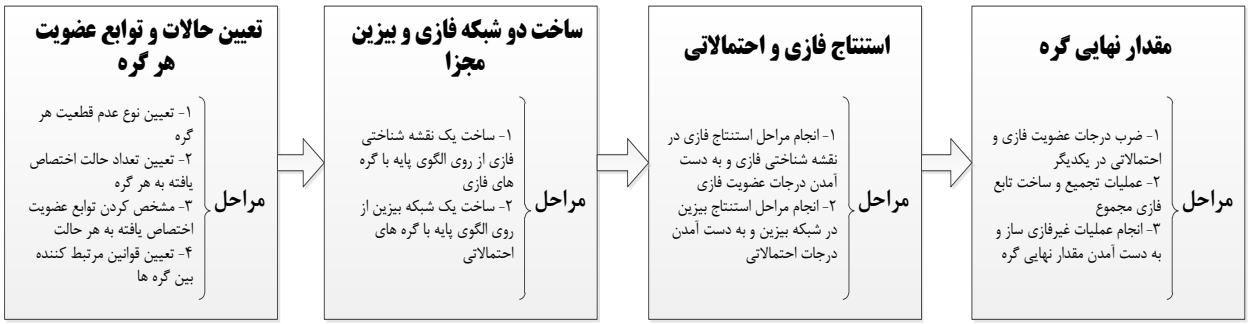
۳- توابع عضویت اختصاص‌یافته به هر حالت,$f_{X_k^{v_k}}(x_k)$ $v_k = 1,2,\dots,n_k$

۴- تعیین قوانین مرتبط کننده بین گره‌ها

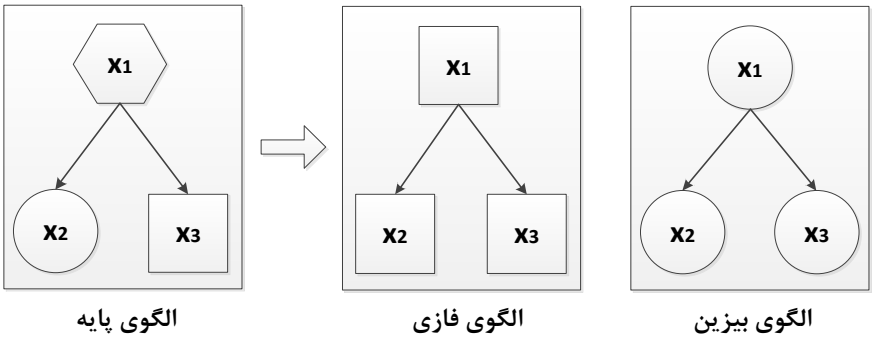
به‌عنوان‌مثال در شکل (۷) فرض شده است که گره نوعی $x_k$ دارای سه حالت با توابع عضویت گوسی است.




**شکل (۷):** توابع عضویت اختصاص‌یافته به حالات یک گره




**شکل (۸):** گام نمای روش پیشنهادی




**شکل (۹):** ساخت دو الگو با گره والد فازی – احتمالاتی

### ۴-۳-۲. ساخت دو شبکه فازی و بیزین مجزا

در این قسمت، از روی شبکه‌ای که شامل هم گره‌هایی با عدم قطعیت فازی و هم احتمالاتی است، دو شبکه مجزا ساخته می‌شود. یک شبکه FCM که در آن تمام گره‌های فازی حضور دارند و یک شبکه BN که در آن تمام گره‌های احتمالاتی قرار گرفته‌اند.

برای گره‌های ریشه که هیچ گره والدی ندارند، چنانچه گره فازی باشد، این گره در الگوی فازی و اگر تصادفی باشد در الگوی بیزین اضافه می‌شود و چنانچه گره فازی- احتمالاتی باشد، در هر دو الگو اضافه می‌گردد. به‌عبارت‌دیگر یک گره فازی- احتمالاتی تبدیل به دو گره می‌شود. در چنین حالتی تعداد و بازه حالت‌های در نظر گرفته‌شده برای گره در دو الگو یکسان است.

برای گره‌های غیر ریشه که دارای والد هستند، اگر گره فازی- احتمالاتی باشد، همانند قبل به هر الگو یک گره اضافه می‌شود. اگر گره فازی باشد و والدین آن‌هم فقط فازی باشند گره فقط در الگوی فازی اضافه می‌شود؛ اما اگر تنها یکی از والدین آن حالت احتمالاتی داشته باشد، چون این حالت احتمالاتی والد روی فرزند هم اثر دارد یک گره به الگوی بیزین هم اضافه می‌شود. به همین ترتیب، اگر گره احتمالاتی باشد و والدین آن‌هم فقط احتمالاتی باشند گره فقط در الگوی بیزین اضافه می‌شود؛ اما اگر تنها یکی از والدین آن حالت فازی داشته باشد، چون این حالت فازی والد روی فرزند هم اثر دارد یک گره به الگوی فازی هم اضافه می‌شود.

به‌عنوان نمونه در شکل (۹) فرض شده که گره والد فازی- احتمالاتی باشد و با این فرض از روی الگوی پایه دو الگوی فازی و بیزین ساخته شده است.

ازآنجایی‌که طبق قانون احتمالات همواره جمع احتمالات، یک است، توابع عضویت در شبکه بیزین طبق رابطه (۱) به‌هنجار[1] می‌شوند.

$$f^{N}{}_{X_k^{v_k}}(x_k) = \frac{f_{X_k^{v_k}}(x_k)}{\sum_{v_k=1}^{n_k} f_{X_k^{v_k}}(x_k)} \qquad (۱)$$

برای به‌دست آوردن روابط بین گره‌ها هم طبق توضیحات بخش ۴-۱ از تبدیل قوانین فازی به CPT و یا بالعکس استفاده می‌شود.

به‌عنوان‌مثال اگر والد گره $x_3$ دو گره $x_1$ و $x_2$ باشند، آن‌گاه نحوه تبدیل یک قانون فازی به CPT و یا بالعکس در جدول (۲) نشان داده شده است.

1 - Normalized

**جدول (۲)**: نحوه تبدیل یک قانون فازی به CPT و یا بالعکس

Rule: $\boldsymbol{IF} x_1 is\ X_1^i\ \ AND\ \ x_2\ is\ X_2^j\ \ \boldsymbol{THEN}\ \ x_3\ is\ X_3^q$

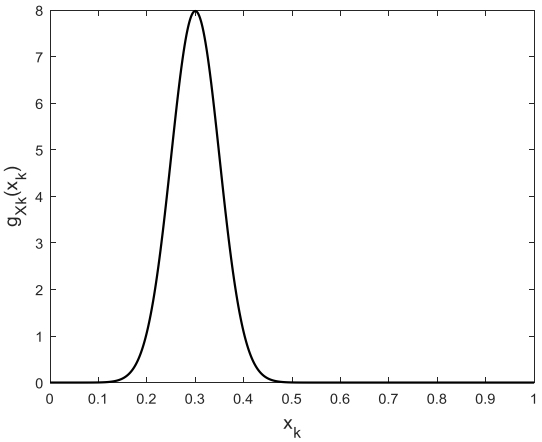
CPT

| | $x_1$ | $X_1^1$ … | | | $X_1^i$ | | | …$X_1^{v_1}$ | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | $x_2$ | $X_2^1$… | $X_2^j$ | …$X_2^{v_2}$ | $X_2^1$ … | $X_2^j$ | …$X_2^{v_2}$ | $X_2^1$ … | $X_2^j$ | …$X_2^{v_2}$ |
| $x_3$ | $X_3^1$ | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| | … | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| | $X_3^q$ | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 |
| | … | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| | $X_3^{v_3}$ | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

برای تشریح بیشتر موضوع، حالتی موردبحث قرار می‌گیرد که در مسائل عملی بسیار اتفاق می‌افتد. فرض می‌کنیم که یکی از گره‌های شبکه FCM دارای نویز احتمالاتی باشد. درنتیجه این گره هم جنبه فازی و هم احتمالاتی دارد. تابع چگالی احتمال نویز را با $g_{X_k}(x_k)$ نشان می‌دهیم. برای سهولت هم فرض بر این است که توابع عضویت اختصاص‌یافته به حالات هر گره و نیز تابع چگالی احتمال نویز، گوسی باشد. در رابطه (۲) ضابطه تابع چگالی احتمال نویز و در شکل (۱۰) یک نمونه تابع چگالی نشان داده شده است.

$$g_{X_k}(x_k) = \frac{1}{\sqrt{2\pi\sigma_g^2}} e^{-\frac{(x_k - x_{0_k})^2}{2\sigma_g^2}} \qquad (۲)$$

در این رابطه $x_{0_k}$ میانگین تابع چگالی احتمال و $\sigma_g^2$ پراکندگی[1] آن می‌باشد.

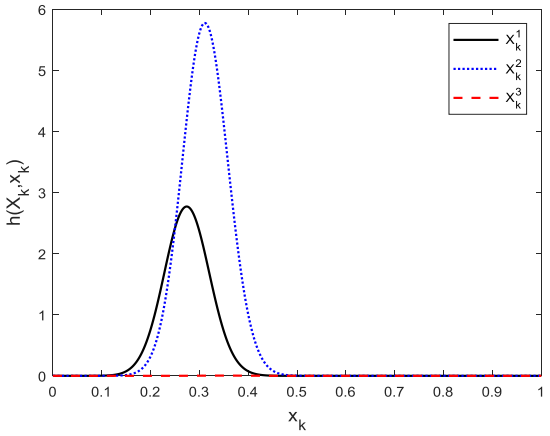



**شکل (۱۰)**: تابع چگالی احتمال نویز گوسی

با داشتن تابع چگالی نویز و توابع بهنجار در شبکه بیزین می‌توان تابع توأمان چگالی احتمال[2] $\mathrm{h}_{X_k^{v_k},X_k}(X_k^{v_k},x_k)$ را به‌صورت رابطه (۳) به دست آورد.

$$\mathrm{h}_{X_k^{v_k},X_k}(X_k^{v_k},x_k) = P(X_k^{v_k}|x_k)\,g_{X_k}(x_k) = f^{N}{}_{X_k^{v_k}}(x_k)\,g_{X_k}(x_k) \qquad (۳)$$

در شکل (۱۱) بر اساس شکل (۱۰) و توابع عضویت شکل (۷) تابع توأمان چگالی احتمال برای هرکدام از حالات نشان داده شده است.




**شکل (۱۱)**: تابع توأمان چگالی احتمال

در شبکه بیزین بر اساس تابع توأمان چگالی احتمال، درجات احتمال محاسبه می‌گردد. به‌عبارت‌دیگر از روی $\mathrm{h}_{X_k^{v_k},X_k}(X_k^{v_k},x_k)$ درجات احتمال $p_k^{v_k}, v_k = 1,2,\dots,n_k$ که همان شواهد نرم[3] هستند، طبق رابطه (۴) حاصل می‌شود.

1- Variance

2- Joint Probability Density Function
3- Soft evidence

$$p_k^{v_k} = \mathrm{p}\left(X_k^D = X_k^{v_k}\right) = \int \mathrm{h}_{X_k^{v_k}, X_k}\left(X_k^{v_k}, x_k\right) dx_k = \int f^{N}_{X_k^{v_k}}(x_k) g_{X_k}(x_k) dx_k \quad (۴)$$

که در آن، $X_k^D$ یک متغیر گسسته تصادفی است که مقادیر ممکن آن $X_k^{v_k}$ می‌باشد.

در رابطه (۴) جمع احتمالات طبق قانون احتمالات همواره برابر با یک است. اثبات این مطلب در رابطه (۵) بیان شده است.

$$\sum_{v_k=1}^{n_k} p_k^{v_k} = \int \left[\sum_{v_k=1}^{n_k} f^{N}_{X_k^{v_k}}(x_k) g_{X_k}(x_k)\right] dx_k = \int g_{X_k}(x_k) dx_k = 1 \quad (۵)$$

### ۴-۳-۳- استنتاج در دو شبکه FCM و BN

بعد از ساخت دو شبکه مجزای فازی و بیزین در هر شبکه استنتاج انجام می‌شود. گره‌ای که قرار است استنتاج بر روی آن انجام شود، گره تصمیم نامیده می‌شود.

در شبکه FCM از روی توابع $f_{X_k^{v_k}}(x_k)$ و طبق قوانین فازی (نظیر Max-Min یا Max-Product) درجات عضویت $\mu_k^{v_k},\ v_k = 1,2,\dots,n_k$ برای گره تصمیم حاصل می‌شود. همچنین از عملیات غیرفازی‌ساز[1] در گره‌های میانی اجتناب شده و فقط برای گره نهایی تصمیم این عملیات انجام می‌شود. این کار باعث انتقال بهتر اطلاعات به گره تصمیم شده و استنتاج دقیق‌تری انجام می‌پذیرد.

در شبکه بیزین بعد از مشخص شدن درجات احتمال گره طبق رابطه (۴)، برای گره تصمیم درجات احتمال $p_k^{v_k},\ v_k = 1,2,\dots,n_k$ محاسبه می‌گردد. این درجات بر مبنای روابط استنتاج بیزین و نیز از روی CPT حاصل می‌شود.

بدین ترتیب برای هر حالت گره تصمیم، درجات عضویت فازی و درجات احتمالاتی به‌دست می‌آید. از این درجات می‌توان برای تصمیم‌گیری استفاده کرد.

### ۴-۳-۴- مقدار نهایی گره

بعد از عملیات استنتاج می‌توان مقدار نهایی گره تصمیم را به دست آورد. همان‌طور که مشاهده شد با استفاده از عملیات استنتاج هر الگو، برای گره نوعی $x_k$ درجات عضویت $\mu_k^{v_k}$ روی مجموعه فازی $\tilde{x}_k$ و درجات احتمال $p_k^{v_k}$ روی مجموعه تصادفی $\bar{x}_k$ به‌دست می‌آید. $\tilde{x}_k$ یک مجموعه فازی با درجات عضویت $\mu_k^{v_k}$ و $\bar{x}_k$ یک مجموعه تصادفی با درجات احتمال $p_k^{v_k}$ تعریف‌شده روی مقادیر گره $x_k$ با حالات $X_k^{v_k},\ v_k = 1,2,\dots,n_k$ می‌باشد.

ازآنجایی‌که درجات احتمال به‌خوبی تغییرات تصادفی ناشی از نویز را در شبکه لحاظ می‌کنند، از آن‌ها برای تصحیح درجات عضویت روی گره تصمیم استفاده می‌شود. درجات عضویت اصلاح‌شده طبق رابطه (۶) از ضرب درجات عضویت $\mu_k^{v_k}$ و درجات احتمال $p_k^{v_k}$ به‌دست می‌آیند.

$$\acute{\mu}_k^{v_k} = \mu_k^{v_k}\, p_k^{v_k} \quad (۶)$$

در مرحله بعدی برای گره $x_k$ در شبکه FCM بر مبنای درجات عضویت اصلاح‌شده $\acute{\mu}_k^{v_k}$ و با استفاده از توابع عضویت $f_{X_k^{v_k}}(\tilde{x}_k)$ و عملیات تجمیع[2]، یک تابع فازی مجموع $M_{x_k}(\tilde{x}_k)$ حاصل می‌شود. از روی این تابع تجمیع و با استفاده از عملیات غیرفازی‌ساز مرکز جرم[3] COG، طبق رابطه (۷)، یک مقدار عددی حاصل می‌شود [۶۶].

$$x_k{}^r = \frac{\int M_{x_k}(\tilde{x}_k)\, x_k\, dx_k}{\int M_{x_k}(\tilde{x}_k)\, dx_k} \quad (۷)$$

## ۵- معیارهای اعتبارسنجی

با توجه به این‌که مسئله ارزیابی تهدید بیشتر جنبه کیفی دارد [۶۷-۶۹]، لذا در مقالات این حوزه نتایج سنجش تهدید بیشتر به‌صورت تشریحی و کیفی بیان شده است. برای حل این مشکل و ممکن شدن مقایسه بهتری بین روش‌های مختلف، معیارهای اعتبارسنجی ارزیابی تهدید به‌صورت زیر پیشنهاد می‌شود.

- **معیار کیفی**

بهترین معیار کیفی برای اعتبارسنجی نتایج یک شبکه ارزیابی تهدید، استفاده از نظرات خبرگان و متخصصین است. یک خبره و متخصص با بررسی رفتار و متغیرهای اهداف و مشاهده نتایج به‌دست‌آمده از شبکه و مقایسه آن، با آنچه دانش و تجربه او حکم می‌کند و در واقعیت انتظار می‌رود، می‌تواند اعتبار نتایج یک روش را مشخص کند.

1- Defuzzification

2 - Aggregation

3 - Center Of Gravity

- **معیارهای کمی**

برای یک شبکه ارزیابی تهدید معیارهای کمی زیر جهت مقایسه پیشنهاد می‌شود.

۱- حجم محاسبات: با توجه به این‌که شبکه ارزیابی تهدید به‌طورمعمول درون یک سامانه تلفیق داده جای دارد و نتایج آن برای سایر سطوح سامانه موردنیاز است، حجم محاسبات و سرعت استنتاج شبکه حائز اهمیت است. با در نظر گرفتن تعداد عملیات محاسباتی یک شبکه و یا زمان موردنیاز برای پردازش، می‌توان به یک معیار کمی برای حجم محاسبات رسید.

۲- جذر میانگین مربعات خطا[1]: در شبیه‌سازی یک شبکه ارزیابی تهدید می‌توان فرض کرد که متغیرها بدون هیچ‌گونه نویزی بوده و بر این مبنا می‌توان مقدار تهدید را حساب کرد. با در نظر گرفتن حالت واقعی یک متغیر و لحاظ کردن نویز، به مقدار متفاوتی برای میزان تهدید می‌رسیم. درنتیجه می‌توان از تفاضل دو مقدار به‌دست‌آمده، مقدار خطا و نیز جذر میانگین مربعات خطای تهدید، RMSE را طبق رابطه (۸) به‌دست آورد. در این رابطه میانگین RMSE تمام اهداف حاضر در یک صحنه نبرد محاسبه شده است.

$$RMSE_{Threat} = \frac{1}{N}\sum_{n=1}^{N}\sqrt{\frac{1}{L}\sum_{i=1}^{L}(T_n(i)-T_n^{noisy}(i))^2} \quad (۸)$$

N تعداد اهداف حاضر در صحنه، L تعداد نمونه‌های تهدید محاسبه‌شده در زمان، $T_n(i)$ میزان تهدید هدف $n$-ام در لحظه $i$-ام در حالت بدون نویز و $T_n^{noisy}(i)$ در حالت نویزی است.

۳- درجه همواری: چنانچه تغییرات متغیرهای ارزیابی تهدید در طول زمان به‌صورت هموار و بدون نوسانات سریع صورت گیرد، انتظار می‌رود که مقدار تهدید نیز در طول زمان به‌صورت هموار تغییر کند. درجه همواری یک معیار کمی است که میزان هموار بودن نمودار مقادیر تهدید برحسب زمان را اندازه می‌گیرد. این معیار از مفهوم مشتق یک کمیت برحسب زمان برای داشتن معیاری از تغییرات سریع و سنجشی از میزان همواری استفاده می‌کند و به‌صورت رابطه (۹) تعریف می‌شود.

$$Smoothing\ Degree = 100 - 100\alpha\frac{1}{L}\sum_{i=1}^{L}(T(i)-T(i-1))^2 \quad (۹)$$

در این رابطه، $T(i)$ درجه تهدید (بین ۰ تا ۱) هدف در لحظه $i$-ام، $L$ تعداد نمونه‌های زمانی نمودار تهدید و $\alpha$ یک ضریب تغییر مقیاس است. به هراندازه نمودار تهدید هموارتر باشد، درجه همواری مقدار بیشتری دارد. چنانچه تهدید در طول زمان ثابت باشد، درجه همواری برابر ۱۰۰ است.

۴- درجه حساسیت: به‌طورمعمول انتظار می‌رود در یک شبکه ارزیابی تهدید حساسیت قابل قبولی بین مقدار تهدید و متغیرهای ورودی برقرار شود. برای داشتن یک معیار کمی برای حساسیت می‌توان دو نوع درجه حساسیت تعریف کرد.

- درجه حساسیت کلی: در این نوع سنجش حساسیت، در یک رفتار حرکتی مشخص، تفاضل حداکثر و حداقل مقدار تهدید به‌دست‌آمده، طبق رابطه (۱۰) به‌عنوان معیاری برای درجه حساسیت کلی روش نسبت به متغیرها در نظر گرفته می‌شود.

$$Total\ Sensitivity\ Degree = 100 \times \{max(T)-min(T)\}_{i=1:L} \quad (۱۰)$$

- درجه حساسیت جزئی: در این نوع سنجش حساسیت، تغییرات تهدید برحسب حداکثر تغییرات یک متغیر با فرض ثابت بودن سایر متغیرها به دست می‌آید. مجموع این تغییرات به‌عنوان درجه حساسیت جزئی طبق رابطه (۱۱) تعریف می‌شود.

$$Trivial\ Sensitivity\ Degree = 100\sum_{j=1}^{P}\frac{\Delta T}{\max\{\Delta C_j\}} \quad for\ i=1:P, i\neq j, C_i = const \quad (۱۱)$$

در این رابطه، $C_i$ متغیر $i$-ام ارزیابی تهدید و $P$ تعداد کل متغیرهاست.

۵- درجه تفکیک‌پذیری: ازلحاظ عملیاتی انتظار می‌رود هنگامی‌که در یک صحنه نبرد بیش از یک هدف حضور دارد، بین مقادیر تهدید اهداف، تفاوت باشد تا بتوان تمایز قابل قبولی بین اهداف ایجاد کرد و بر مبنای آن تصمیم‌گیری انجام شود. درجه تفکیک‌پذیری معیاری کمی است که بر مبنای اختلاف مقادیر تهدید اهداف در طول زمان طبق رابطه (۱۲) محاسبه می‌شود.

$$Seperation\ Degree = 100\sqrt{\frac{1}{L}\sum_{i=1}^{L}(T_1(i)-T_2(i))^2} \quad (۱۲)$$

در این رابطه، $T_1$ و $T_2$ مقدار تهدید دو هدف مختلف هستند.

1 - Root Mean Square Error

## ۶- شبیه‌سازی

برای شبیه‌سازی و بررسی عملکرد ساختار و روش پیشنهادی، شکل (۲) را موردتوجه قرار می‌دهیم. تعداد حالات، توابع عضویت و قوانین ارتباطی بین گره‌ها توسط خبرگان مدیریت نبرد ارائه گشته است. همچنین به علت کیفی بودن مسئله ارزیابی تهدید و نیز دشوار بودن تهیه یک پایگاه داده جهت یادگیری، از نظرات متخصصین برای تشکیل و یادگیری شبکه‌ها استفاده شده است. شبکه شکل (۲) را می‌توان با استفاده از روابط فازی و روش FCM پیاده‌سازی کرد. در این ساختار فرض می‌شود مقادیر گره فاصله از یک حسگر رادار تأمین می‌گردد که دارای نویز تصادفی گوسی است. درنتیجه این گره علاوه بر عدم قطعیت فازی دارای عدم قطعیت احتمالاتی هم بوده و نوع این گره، فازی- احتمالاتی به‌حساب می‌آید. همچنین به علت والد بودن گره فاصله، عدم قطعیت احتمالاتی این گره تا گره تهدید انتشار می‌یابد. برای بررسی عملکرد روش پیشنهادی، این شبکه با دو روش FCM و BN در رفتار حرکتی مطرح‌شده مقایسه می‌شود.

### ۶-۱- نحوه پیاده‌سازی

جهت پیاده‌سازی روش پیشنهادی بر روی شبکه ارزیابی تهدید، مراحل بیان‌شده در بخش ۴-۳ تشریح می‌گردد.

ابتدا مقادیر تمام گره‌های ورودی شبکه بین صفر تا یک به‌هنجار می‌شود. توابع عضویت اختصاص‌یافته به هر گره یک تابع گوسی بوده و میزان پراکندگی هر تابع بسته به تعداد آن متقارن در نظر گرفته شده است. تعداد و نام توابع عضویت هر گره در جدول (۳) ذکر شده است.

قوانین بین گره‌ها براساس ماهیت هر گره، روابط بین گره‌ها و نظر متخصصین بیان می‌گردد. به‌عنوان نمونه یک قانون بین گره‌های مرتبط با گره قابلیت به‌صورت زیر است.

اگر فاصله هدف تا خودی زیاد، قدرت تخریب سلاح‌های هدف کم، برد سلاح‌های هدف کم، ارتفاع هدف زیاد و نوع هدف مسافربری باشد، آن‌گاه قابلیت هدف خیلی کم است.

با توجه به این‌که گره فاصله دارای نویز تصادفی است. این گره و تمام گره‌های فرزند آن دارای عدم قطعیت احتمالاتی علاوه‌بر عدم قطعیت فازی می‌باشند. درنتیجه در شبکه FCM ساخته‌شده تمام گره‌ها حضور دارند، ولی در شبکه بیزین تنها گره‌های با عدم قطعیت احتمالاتی شبکه را تشکیل می‌دهند.

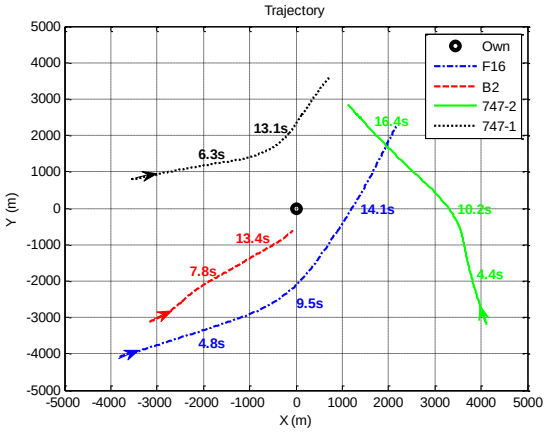
استنتاج در شبکه FCM بر اساس قوانین فازی و روابط Max-Product انجام می‌شود. همچنین در شبکه بیزین، استنتاج بیزین برای رسیدن به درجات احتمال در گره تهدید استفاده می‌شود؛ و درنهایت مقدار نهایی گره تهدید طبق رابطه (۷) محاسبه می‌گردد.

**جدول (۳):** تعداد و نام توابع عضویت هر گره

| ردیف | نام گره | تعداد و نام توابع عضویت |
|---|---|---|
| ۱ | SC | ۳ (خوب، متوسط، بد) |
| ۲ | VS | ۳ (کم، متوسط، زیاد) |
| ۳ | CPA | ۳ (کم، متوسط، زیاد) |
| ۴ | R | ۳ (کم، متوسط، زیاد) |
| ۵ | WD | ۳ (کم، متوسط، زیاد) |
| ۶ | WR | ۳ (کم، متوسط، زیاد) |
| ۷ | H | ۳ (کم، متوسط، زیاد) |
| ۸ | PF | ۴ (مسافربری، باری، بمب‌افکن، شکاری) |
| ۹ | CL | ۳ (نزدیک شونده، عمودی، دور شونده) |
| ۱۰ | V | ۳ (کم، متوسط، زیاد) |
| ۱۱ | AL | ۳ (کم، متوسط، زیاد) |
| ۱۲ | MNV | ۳ (کم، متوسط، زیاد) |
| ۱۳ | DI | ۳ (کم، متوسط، زیاد) |
| ۱۴ | PC | ۳ (خوب، متوسط، بد) |
| ۱۵ | FW | ۲ (منفی، مثبت) |
| ۱۶ | VC | ۲ (منفی، مثبت) |
| ۱۷ | FM | ۳ (دوست، نامشخص، دشمن) |
| ۱۸ | JM | ۲ (منفی، مثبت) |
| ۱۹ | EA | ۴ (هشدار ۱، هشدار ۲، هشدار ۳، هشدار ۴) |
| ۲۰ | FCR | ۲ (منفی، مثبت) |
| ۲۱ | CO | ۳ (کم، متوسط، زیاد) |
| ۲۲ | فرصت | ۵ (خیلی کم، کم، متوسط، زیاد، خیلی زیاد) |
| ۲۳ | قابلیت | ۵ (خیلی کم، کم، متوسط، زیاد، خیلی زیاد) |
| ۲۴ | نیت | ۵ (خیلی کم، کم، متوسط، زیاد، خیلی زیاد) |
| ۲۵ | تهدید | ۵ (خیلی کم، کم، متوسط، زیاد، خیلی زیاد) |

### ۶-۲- صحنه نبرد

جهت شبیه‌سازی و اجرای روش‌های مختلف، یک صحنه نبرد به ابعاد $100\ Km \times 100\ Km$ در نظر گرفته می‌شود. مسئله موردنظر، سنجش تهدید هر هدف نسبت به منابع خودی است. منابع خودی در مبدأ قرار داشته و چهار هدف پیرامون آن در حال حرکت هستند [۵۵، ۶۷]. هدف اول یک هواپیمای جنگی F16 است که به هدف خودی نزدیک شده و سپس دور می‌شود. هدف دوم یک هواپیمای بمب‌افکن B2 است که در حال نزدیک شدن به خودی است. هدف سوم و چهارم هم دو هواپیمای مسافربری ۷۴۷ می‌باشند. کل زمان شبیه‌سازی ۲۰ ثانیه با فواصل زمانی نمونه‌برداری شده ۰/۱ ثانیه است. نحوه حرکت اهداف و بعضی از زمان‌های مهم در شکل (۱۲) نشان داده شده است. سایر متغیرهای ارزیابی تهدید بر مبنای مشخصات واقعی اهداف هوایی با نوع‌های مشخص‌شده تنظیم شده است. در شبیه‌سازی فرض شده است که اندازه‌گیری مقادیر فاصله با نویز گوسی با مقدار پراکندگی ۰/۰۰۱ همراه بوده است.




**شکل (۱۲):** رفتار حرکتی چهار هدف هوایی

### ۶-۳- نتایج

جهت پیاده‌سازی روش‌های ارزیابی تهدید از محیط نرم‌افزار MATLAB بر روی سیستم‌عامل Windows 7 با ۸ GB حافظه و ۴/۳ GHz سرعت یک i5 CPU بهره گرفته شده است.

نتیجه ارزیابی تهدید برای هر هدف و با استفاده از روش پیشنهادی و دو روش FCM و BN در شکل (۱۳) نشان داده شده است. در قسمت (الف) شکل، نتیجه ارزیابی تهدید با استفاده از روش FCM و با فرض بدون نویز بودن گره فاصله نمایش داده شده است. در سایر قسمت‌ها گره فاصله با مقادیر نویزی همراه بوده است. در قسمت (ب) نتیجه روش FCM با در نظر گرفتن نویز، در قسمت (ج) نتیجه پیاده‌سازی ساختار شکل (۲) با یک شبکه بیزین و در قسمت (د) نتیجه روش پیشنهادی به نمایش درآمده است.

نتایج این ارزیابی مورد تأیید چندین خبره قرار گرفته است. به‌عنوان مثال همان‌گونه که انتظار می‌رود تهدید دو هدف جنگی F16 و بمب‌افکن B2 از تهدید دو هواپیمای مسافربری ۷۴۷ بیشتر است. همچنین تغییرات تهدید هر هدف متناسب با تغییرات متغیرهای تهدید و قوانین حاکم بر آن است. به‌عنوان‌مثال تهدید هدف دوم در ثانیه ۲ تا ۸ به علت تغییر در نوع تشخیص حسگر IFF (از حالت ناشناس به دشمن) افزایش داشته است.

با استفاده از معیارهای اعتبارسنجی کمی می‌توان به مقایسه‌ی خوبی بین روش‌ها رسید. نتایج استفاده از معیارهای اعتبارسنجی در جدول (۴) آورده شده است. در این جدول معیار حجم محاسبات بر مبنای زمان شبیه‌سازی و برحسب ثانیه لحاظ شده است. سایر معیارها طبق روابط (۸) تا (۱۲) به‌دست آمده‌اند.

تمام نتایج به‌دست‌آمده در جدول (۴) با آنچه از ماهیت هر روش انتظار می‌رود انطباق دارد. این نتایج به‌صورت زیر قابل‌تحلیل هستند.

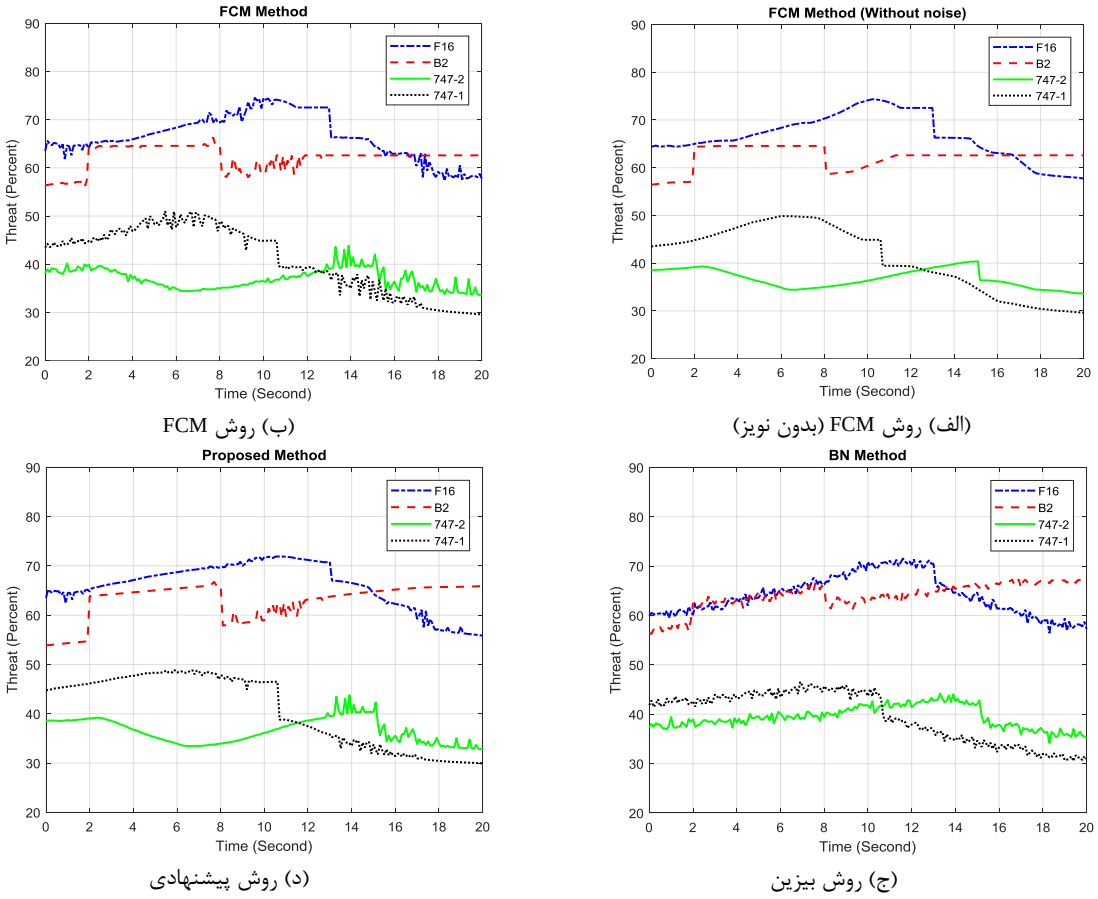
۱- روش BN به‌علت عدم نیاز به انجام محاسبات سنگین عملیاتی نظیر غیرفازی‌ساز، کمترین حجم محاسبات را دارد. حجم محاسبات روش پیشنهادی به علت استفاده از هر دو روش FCM و BN کمی از حجم محاسبات روش FCM بیشتر است.

۲- روش پیشنهادی به علت در نظر گرفتن هر دو نوع عدم قطعیت فازی و احتمالاتی کمترین میانگین مجذور خطا را دارد.

۳- روش BN بیشترین درجه همواری را دارد. درجه همواری روش پیشنهادی نیز بیشتر از روش FCM است.

۴- از لحاظ درجه حساسیت جزئی و کلی روش پیشنهادی بهترین حساسیت را دارد. حساسیت روش FCM هم از روش BN بیشتر است.

۵- از لحاظ درجه تفکیک‌پذیری روش پیشنهادی بهترین تفکیک‌پذیری را دارد. تفکیک‌پذیری روش FCM هم از روش BN بیشتر است.




(الف) روش FCM (بدون نویز)

(ب) روش FCM

(ج) روش بیزین

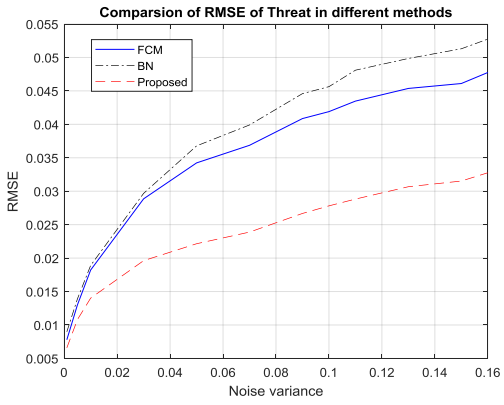
(د) روش پیشنهادی

**شکل (۱۳):** نتیجه ارزیابی تهدید چهار هدف هوایی با استفاده از روش‌های مختلف

**جدول (۴):** استفاده از معیارهای اعتبارسنجی برای روش‌های مختلف

| معیار / روش | حجم محاسبات | جذر میانگین مربعات خطا | درجه هموارى | درجه حساسیت کلی | درجه حساسیت جزئی | درجه تفکیک‌پذیری |
|---|---|---|---|---|---|---|
| روش FCM | ۰/۷۴ | ۰/۰۰۷۷۸ | ۴۰/۴۸ | ۱۴/۵۳ | ۷۷/۶۵ | ۱۹/۸۳ |
| روش BN | ۰/۰۳ | ۰/۰۰۸۹۸ | ۶۶/۸۳ | ۱۳/۲۵ | ۷۲/۸۸ | ۱۸/۴۳ |
| روش پیشنهادی | ۰/۷۹ | ۰/۰۰۵۵۳ | ۶۵/۸۲ | ۱۴/۶۲ | ۸۰/۲۳ | ۲۰/۴۶ |

میانگین RMSE تهدید چهار هدف هوایی در طول زمان حرکت اهداف، شبیه‌سازی شده و با استفاده از روش‌های FCM، BN و روش پیشنهادی در شکل (۱۴) نشان داده شده است. در این شکل مقادیر RMSE به‌ازای مقادیر مختلف پراکندگی نویز گره فاصله محاسبه شده است. مشاهده می‌شود که در تمام مقادیر پراکندگی نویز، RMSE روش پیشنهادی مقدار کمتری نسبت به RMSE هر دو روش FCM و BN دارد. همچنین قابل‌توجه است که مزیت روش پیشنهادی زمانی مشخص‌تر می‌شود که نویز، پراکندگی بیشتری دارد. با افزایش پراکندگی نویز و یا همان توان نویز، جنبه عدم قطعیت احتمالاتی گره افزایش می‌یابد. درنتیجه هر دو نوع عدم قطعیت فازی و احتمالاتی به‌طور عمده‌ای در شبکه حضور دارند. در این حالت روش پیشنهادی برخلاف دو روش دیگر به‌خوبی هر دو نوع عدم قطعیت را لحاظ می‌کند.




**شکل (۱۴):** مقایسه RMSE تهدید روش‌های مختلف

## ۷- نتیجه‌گیری

در این مقاله جهت پیاده‌سازی یک سامانه ارزیابی تهدید روش جامع و کارآمدی مطرح شد. این روش قابلیت لحاظ کردن متغیرهای زیاد و متنوعی داشته و می‌تواند ارتباط میان متغیرهای ارزیابی تهدید را به‌خوبی بیان کند. همچنین دارای ساختاری است که در آن عدم قطعیت فازی و احتمالاتی متغیرها و قوانین حاکم بر آن‌ها به‌خوبی لحاظ می‌شوند.

مسئله ارزیابی تهدید یک مسئله پیچیده است، به‌گونه‌ای که برای رسیدن به فرصت، قابلیت، نیت و درنهایت میزان تهدید اهداف، چالش‌هایی نظیر نحوه دسته‌بندی متغیرهای ارزیابی تهدید، بیان ارتباطات بین متغیرها، در نظر گرفتن عدم قطعیت، ایجاد حساسیت مناسب، نحوه بیان قوانین توسط خبره، معیارهای مناسب اعتبارسنجی و ... وجود دارد. در این مقاله تمام این چالش‌ها موردنظر قرار گرفتند و نشان داده شد که با استفاده از ساختار و روش پیشنهادی می‌توان بر این چالش‌ها چیره شد.

با بررسی مقالات و مراجع گوناگون مهم‌ترین و کاربردی‌ترین متغیرهای ارزیابی تهدید استخراج شدند. این متغیرها درون یک ساختار ابتکاری، منسجم و کاربردی قرار گرفتند و بر مبنای روش پیشنهادی، یک شبکه کامل ارزیابی تهدید شکل گرفت.

در شبکه‌های ترسیمی با در نظر گرفتن عدم قطعیت فازی و عدم قطعیت احتمالاتی دسته بزرگی از عدم قطعیت‌های موجود لحاظ می‌شوند. مسئله چالش‌برانگیز زمانی است که هردو نوع عدم قطعیت به‌صورت هم‌زمان در یک شبکه ارزیابی تهدید وجود داشته باشند. در این مقاله روشی کارآمد و مفید برای در نظر گرفتن هر دو نوع عدم قطعیت فازی و احتمالاتی در شبکه‌های ترسیمی ارزیابی تهدید مبتنی بر قواعد پیشنهاد شد.

روش پیشنهادی با رویکردی جدید عدم قطعیت‌های مسئله را همان‌گونه که هست در نظر می‌گیرد. برای این منظور ابتدا نوع عدم قطعیت هر گره در الگوی ترسیمی شناسایی شده و سپس از روی شبکه اصلی دو شبکه فازی و احتمالاتی مجزا ساخته می‌شود. از شبکه شناختی فازی برای لحاظ کردن عدم قطعیت فازی و از شبکه بیزین برای لحاظ کردن عدم قطعیت احتمالاتی بهره گرفته می‌شود. استنتاج در هر شبکه به‌صورت مجزا انجام می‌گیرد و در انتها بر روی گره تهدید می‌توان از ترکیب نتایج دو شبکه استفاده کرد. بدین ترتیب از تبدیل شبکه فازی به بیزین و یا بالعکس اجتناب کرده و هر دو نوع عدم قطعیت بدون تبدیل در مسئله لحاظ می‌شود.

در این مقاله روش پیشنهادی در یک رفتار حرکتی اهداف هوایی مورد ارزیابی قرار گرفت و این روش با دو روش FCM و BN بر مبنای معیارهای کمی حجم محاسبات، میانگین مجذور خطا، درجه هموواری، درجه حساسیت کلی و جزئی و درجه تفکیک‌پذیری مورد مقایسه قرار گرفت. همچنین نتایج تهدید اهداف در طول زمان به‌صورت کیفی بررسی شدند. نتایج شبیه‌سازی نشان می‌دهد که روش پیشنهادی ازلحاظ جذر میانگین مربعات خطا، درجه حساسیت کلی و جزئی و درجه تفکیک‌پذیری بهتر از دو روش دیگر عمل می‌کند.

## ۸- منابع


[1] R. Gholami and M. Okhovat, "Designing Radar and IR Sensors Data Fusion System for Target Tracking in Noise Jamming Conditions," Journal Of Electronical & Cyber Defence, vol. 5, 2017. (In Persian).

[2] M. E. Liggins, D. L. Hall, and J. Llinas, "Handbook of multisensor data fusion: theory and practice," ed: Taylor & Francis, 2009.

[3] V. Akbari and S. M. S. Homami, "A Framework For The Status Estimation In Distributed Denial-Of-Service Attacks By Data Fusion of Human-And-Technical Sensors Based on Fuzzy Logic," Journal of Electronical & Cyber Defence, vol. 5, 2017. (In Persian).

[4] D. L. Hall and J. Llinas, "An introduction to multisensor data fusion," Proceedings of the IEEE, vol. 85, pp. 6-23, 1997.

[5] J. Yun, B. Choi, M.M. Han, and S.-H. Kim, "Air Threat Evaluation System using Fuzzy-Bayesian Network based on Information Fusion," Journal of Internet Computing and Services, vol. 13, pp. 21-31, 2012.

[6] N. P. Rao, S. K. Kashyap, and G. Girija, "Situation assessment in air-combat: A fuzzy-bayesian hybrid approach," International Conference on Aerospace Science and Technology, 2008.

[7] J .J. Salerno, S. J. Yang, I. Kadar, M. Sudit, G. P. Tadda, and J. Holsopple, "Issues and challenges in higher level fusion: Threat/impact assessment and intent modeling (a panel summary)," 13th Conference on Information Fusion, 2010.

[8] E. Shahbazian, G. Rogova, and M. J. de Weert, "Harbour protection through data fusion technologies," Springer Science & Business Media, 2008.

[9] E. G. Little and G. L. Rogova, "An ontological analysis of threat and vulnerability," 9th Conference on Information Fusion, 2006.

[10] J. Llinas and R. T. Antony, "Blackboard concepts for data fusion applications," International journal of pattern recognition and artificial intelligence, vol. 7, pp. 285-308, 1993.

[11] A. J. Rashidi, K. D. Ahmadi, and F. S. Khodadad, "Projection of Muli Stage Cyber Attack Based on Belief Model and Fuzzy Inference," Journal of Electronical & Cyber Defence, vol. 3, 2015. (In Persian)

[12] S. Kumar and A. M. Dixit, "Threat evaluation modelling for dynamic targets using fuzzy logic approach," International Conference on Computer Science and Engineering, 2012.

[13] L. Man and F. Xinxi, "Situation assessment based on bayesian networks," 4th International Conference on Wireless Communications, Networking and Mobile Computing, 2008.

[14] C. M. Bishop, "Graphical models," Pattern recognition and machine learning, vol. 4, pp. 359-422, 2006.

[15] M. I. Jordan and C. Bishop, "An introduction to graphical models," unpublished book, 2001.

[16] E. I. Papageorgiou, "Fuzzy cognitive maps for applied sciences and engineering," ed: Springer, 2014.

[17] A. Mittal, "Bayesian Network Technologies: Applications and Graphical Models," IGI Global, 2007.

[18] P. P. Groumpos, "Fuzzy cognitive maps: Basic theories and their application to complex systems," in Fuzzy cognitive maps, ed: Springer, pp. 1-22, 2010.

[19] R. Axelrod, "Structure of decision: The cognitive maps of political elites," Princeton University Press, 1976.

[20] B. Kosko, "Fuzzy cognitive maps," International Journal of man-machine studies, vol. 24, pp. 65-75, 1986.

[21] E. I. Papageorgiou and J. L. Salmeron, "A review of fuzzy cognitive maps research during the last decade," IEEE Transactions on Fuzzy Systems, vol. 21, pp. 66-79, 2013.

[22] C. D. Stylios and P. P. Groumpos, "Modeling complex systems using fuzzy cognitive maps," IEEE Transactions on Systems, Man, and Cybernetics-Part A: Systems and Humans, vol. 34, pp. 155-162, 2004.

[23] J. Pearl, "Probabilistic reasoning in intelligent systems: Networks of plausible inference," ed: Morgan Kaufmann Publishers, Los Altos, 1988.

[24] R. G. Cowell, P. Dawid, S. L. Lauritzen, and D. J. Spiegelhalter, "Probabilistic networks and expert systems: Exact computational methods for Bayesian networks," Springer Science & Business Media, 2006.

[25] O. Pourret, P. Naïm, and B. Marcot, "Bayesian networks: a practical guide to applications," vol. 73, John Wiley & Sons, 2008.

[26] R. Neut, "Uncertainty analysis in Bayesian networks," Master thesis, Utrecht university, 2014.

[27] M. L. Hinman, "Some computational approaches for situation assessment and impact assessment," 5th Conference on Information Fusion, 2002.

[28] Y. Liang, "An approximate reasoning model for situation and threat assessment," 4th International Conference on Fuzzy Systems and Knowledge Discovery, 2007.

[29] M. J. Liebhaber and B. Feher, "Air threat assessment: Research, model, and display guidelines," Space and Naval Warfare Systems Command San Diego CA, 2002.

[30] J. Baghmalayi and H. Sahami, "Investigation of Threat Measurement Indicators and Analysis of Ports Security Based on Vulnerability Assessment Model (Risk&Threat Analysis Matrix TRAM)," 13th Marine Industries Conference, 2011. (In Persian)

[31] M. J. Wierman, "An Introduction to the Mathematics of Uncertainty," Creighton University, 2010.

[32] M. J. Liebhaber and C. Smith, "Naval air defense threat assessment: Cognitive factors and model," Pacific Science And Engineering Group Inc San Diego CA, 2000.

[33] S. K. Das, "High-level data fusion," Artech House, 2008.

[34] A. H. Meghdadi and M.-R. Akbarzadeh-T, "Probabilistic fuzzy logic and probabilistic fuzzy systems," 10th IEEE International Conference on Fuzzy Systems, 2001.

[35] M. Laviolette and J. W. Seaman, "Unity and diversity of fuzziness-from a probability viewpoint," IEEE Transactions on Fuzzy Systems, vol. 2, pp. 38-42, 1994.

[36] L. A. Zadeh, "Discussion: Probability theory and fuzzy logic are complementary rather than competitive," Technometrics, vol. 37, pp. 271-276, 1995.

[37] E. Kentel and M. M. Aral, "Probabilistic-fuzzy health risk modeling," Stochastic Environmental Research and Risk Assessment, vol. 18, pp. 324-338, 2004.

[38] H.-X. Li, X. Duan, and Z. Liu, "Three-dimensional fuzzy logic system for process modeling and control," Journal of Control Theory and Applications, vol. 8, pp. 280-285, 2010.

[39] A. F. Shapiro, "Fuzzy random variables," Insurance: Mathematics and Economics, vol. 44, pp. 307-314, 2009.

[40] S. Nadkarni and P. P. Shenoy, "A Bayesian network approach to making inferences in causal maps," European Journal of Operational Research, vol. 128, pp. 479-498, 2001.

[41] Y. Y. Wee, W. P. Cheah, S. C. Tan, and K. Wee, "A method for root cause analysis with a Bayesian belief network and fuzzy cognitive map," Expert Systems with Applications, vol. 42, pp. 468-487, 2015.

[42] W.-P. Cheah, K.-Y. Kim, H.-J. Yang, S.-H. Kim, and J.-S. Kim, "Fuzzy Cognitive Map and Bayesian Belief Network for Causal Knowledge Engineering: A Comparative Study," The KIPS Transactions: PartB, vol. 15, pp. 147-158, 2008.

[43] W. P. Cheah, Y. S. Kim, K.-Y. Kim, and H.-J. Yang, "Systematic causal knowledge acquisition using FCM constructor for product design decision support," Expert Systems with Applications, vol. 38, pp. 15316-15331, 2011.

[44] H.-J. Song, Z.-Q. Shen, C.-Y. Miao, Z.-Q. Liu, and Y. Miao, "Probabilistic fuzzy cognitive map," IEEE International Conference on Fuzzy Systems, 2006.

[45] A. Eleye- Datubo, A. Wall, and J. Wang, "Marine and Offshore Safety Assessment by Incorporative Risk Modeling in a Fuzzy- Bayesian Network of an Induced Mass Assignment Paradigm," Risk Analysis, vol. 28, pp. 95-112, 2008.

[46] J. T. Brignoli, M. M. Pires, S. M. Nassar, and D. Sell, "A fuzzy-Bayesian model based on the superposition of states applied to the clinical reasoning support," SAI Intelligent Systems Conference (IntelliSys), 2015.

[47] A. Le Dorze, B. Duval, L. Garcia, D. Genest, P. Leray, and S. Loiseau, "Probabilistic Cognitive Maps Semantics of a Cognitive Map when the Values are Assumed to be Probabilities," International Conference on Agents and Artificial Intelligence (ICAART), 2014.

[48] Y. Deng, "A threat assessment model under uncertain environment," Mathematical Problems in Engineering, 2015.

[49] J. Fang, J. Huang, and M. Liu, "The Research on Fuzzy Bayesian Network Model for the Network Public Opinion Situation and Threat Assessment," Third International Conference on Networking and Distributed Computing, 2012.

[50] J. Chen, G.-h. Yu, and X.-g. Gao, "Cooperative t hreat assessment of multi-aircrafts based on synthetic fuzzy cognitive map," Journal of Shanghai Jiaotong University (Science), vol. 17, pp. 228-232, 2012.

[51] C. Dongfeng, F. Yu, and L. Yongxue, "Threat assessment for air defense operations based on intuitionistic fuzzy logic," Procedia Engineering, vol. 29, pp. 3302-3306, 2012.

[52] E. Azimirad and J. Haddadnia, "Target threat assessment using fuzzy sets theory," International Journal of Advances in Intelligent Informatics, vol. 1, pp. 57-74, 2015.

[53] Y. Lu, Y. Wang, Y. Lei, and Y. Wang, "Air targets threat assessment based on fuzzy rough reasoning," 27th Chinese Conference on Control and Decision (CCDC), 2015.

[54] M. Fatahi and s. garocy, "Threat Evaluation Using Fuzzy Logic," 6th National Conference of Iran's Scientific on Command, Control, Communications, Computer & Intelligence, 2012. (In Persian)

[55] F. Johansson and G. Falkman, "A Bayesian network approach to threat evaluation with application to an air defense scenario," 11th International Conference on Information Fusion, 2008.

[56] X. T. Nguyen, "Threat assessment in tactical airborne environments," Proceedings of the Fifth International Conference on Information Fusion, 2002.

[57] N. Okello and G. Thoms, "Threat assessment using Bayesian networks," Proceedings of the 6th International Conference on Information fusion, 2003.

[58] J. F. Brancalion, D. de Oliveira Marques, and K. H. Kienitz, "Framework for situation assessment and threat evaluation with application to an air defense scenario," 18th International Conference on Information Fusion (Fusion), 2015.

[59] J. Aguilar, "A survey about fuzzy cognitive maps papers," International journal of computational cognition, vol. 3, pp. 27-33, 2005.

[60] J. Carvalho and J. A. Tomè, "Rule based fuzzy cognitive maps and fuzzy cognitive maps-a comparative study," 18th International Conference of the North American, Fuzzy Information Processing Society, 1999.

[61] J. P. Carvalho, "Rule based fuzzy cognitive maps in humanities, social sciences and economics," Soft Computing in Humanities and Social Sciences, Springer, pp. 289-300, 2012.

[62] E. I. Papageorgiou and J. L. Salmeron, "Methods and algorithms for fuzzy cognitive map-based modeling," Fuzzy Cognitive Maps for Applied Sciences and Engineering, Springer, pp. 1-28, 2014.

[63] K. F.-R. Liu, J.-Y. Kuo, K. Yeh, C.-W. Chen, H.-H. Liang, and Y.-H. Sun, "Using fuzzy logic to generate conditional probabilities in Bayesian belief networks: a case study of ecological assessment," International Journal of Environmental Science and Technology, vol. 12, pp. 871-884, 2015.

[64] P. Baraldi, M. Conti, M. Librizzi, E. Zio, L. Podofillini, and V. Dang, "A Bayesian network model for dependence assessment in human reliability analysis," Proceedings of the Annual European Safety and Reliability Conference, ESREL, 2009.

[65] P. Baraldi, L. Podofillini, L. Mkrtchyan, E. Zio, and V. N. Dang, "Comparing the treatment of uncertainty in Bayesian networks and fuzzy expert systems used for a human reliability analysis application," Reliability Engineering & System Safety, vol. 138, pp. 176-193, 2015.

[66] W. Van Leekwijck and E. E. Kerre, "Defuzzification: criteria and classification," Fuzzy sets and systems, vol. 108, pp. 159-178, 1999.

[67] F. Johansson and G. Falkman, "A comparison between two approaches to threat evaluation in an air defense scenario," International Conference on Modeling Decisions for Artificial Intelligence, 2008.

[68] Q. Changwen and H. You, "A method of threat assessment using multiple attribute decision making," 6th International Conference on Signal Processing, 2002.

[69] E. Mahboobi, M. Vahedian, and M. Hedayati, "Investigation and comparison of threat assessment methods in marine battles and suggestion of proposed model," 15th Marine Industries Conference, 2013. (In Persian)

Journal of Electronical & Cyber Defence
Vol. 6, No. 4, 2019, Serial No. 24

# Target Threat Assessment using Rule-Based Joint Fuzzy and Probabilistic Networks

**M. Yadegari, S. A. Seyedin***
*Ferdowsi University of Mashhad
(Received: 18/12/2017, Accepted: 27/05/2018)

## ABSTRACT

*Threat assessment is one of the most important pillars of data fusion systems. In this paper, we use two graphical models: fuzzy cognitive map and bayesian network to implement a complete threat assessment network. The structure of this network includes numerous variables of threat assessment and relates them well to each other. Given the uncertainty in all threat assessment issues, various types of uncertainty and how to deal with them are considered in this article. A comprehensive review has also been carried out on a variety of methods for incorporating both types of fuzzy and probabilistic uncertainties and a new approach is proposed. In this method, two separated fuzzy and bayesian networks are used to consider uncertainties. The approach of the proposed method is fully described, step-by-step. Furthermore, this paper addresses the major challenges of the threat assessment problem and shows that the proposed method is capable of solving these issues. To illustrate the effectiveness of the proposed method, a set of qualitative and quantitative validation criteria is presented. As a test a scenario for air targets is simulated and the results of the proposed method are qualitatively and quantitatively compared with fuzzy cognitive map and bayesian network methods. These results indicate that the proposed method works better than other methods regarding root mean square error, total and trivial sensitivity degree and seperation degree. Moreover, the effectiveness of the proposed structure and method has been confirmed by experts in the field of battle management.*

**Keywords:** Threat assessment, Fuzzy Cognitive Map, Bayesian Network, Rules, Fuzzy and Probabilistic uncertainty, Validation criteria

* Corresponding Author Email: seyedin@um.ac.ir