ارزیابی روش‌های توافق کلید مبتنی بر ساختار Fuzzy Vault در شبکه‌های بی‌سیم روی بدن با استفاده از روش AHP فازی

مرتضی ابراهیمی، سیدحمیدرضا احمدی و مریم عباس‌نژاد آرا

چکیده: در سال‌های اخیر، استفاده از شبکه‌های حسگر بی‌سیم در حوزه‌هایی از کاربردهای پزشکی مطرح شده و به طور خاص در کاربردهایی که حسگرها روی بدن نصب می‌شوند، تحت عنوان شبکه‌های بی‌سیم روی بدن مورد بررسی قرار گرفته است. از آنجا که حفظ حریم خصوصی و امنیت داده‌های پزشکی دارای اهمیت بسیاری است، برقراری امنیت داده در این حوزه به عنوان یک چالش مهم مد نظر قرار گرفته است. یکی از مشکلات برقراری امنیت در شبکه‌های بی‌سیم، توافق کلید بین گره‌ها است که تحقیقات بسیاری روی آن انجام شده است. در شبکه‌های بی‌سیم روی بدن، الگوریتم‌های متعددی بر پایه یک ساختار ریاضی به نام Fuzzy Vault ارائه شده است که از ویژگی‌های سیگنال‌های فیزیولوژیکی برای توافق کلید استفاده می‌کند. با توجه به محدودیت‌های موجود در این شبکه‌ها که ناشی از کوچکی سایز گره‌های شبکه حسگر و ویژگی‌های ارتباط بی‌سیم می‌باشد، انتخاب طرح امنیتی مناسب از اهمیت زیادی برخوردار است. این مقاله با استفاده از روش تحلیل سلسله‌مراتبی فازی به ارزیابی الگوریتم‌های توافق کلید مبتنی بر Fuzzy Vault و انتخاب بهترین الگوریتم از میان الگوریتم‌های ارائه‌شده می‌پردازد. برای ارزیابی، از میان الگوریتم‌های توافق کلید ارائه‌شده بر پایه ساختار Fuzzy Vault، سه الگوریتم OPFKA، PSKA و ECG-IJS که دارای اهمیت بیشتری هستند در نظر گرفته شده‌اند تا با استفاده از روش AHP فازی، بهترین الگوریتم با در نظرگرفتن معیارهایی که در انتخاب بهترین گزینه اهمیت زیادی دارند، برگزیده شود. در تعیین معیارها باید ویژگی‌ها و محدودیت‌های شبکه‌های بی‌سیم روی بدن و همچنین نوع کاربرد و زمان مد نظر قرار گیرد. در نهایت، ارزیابی انجام‌شده نشان می‌دهد که الگوریتم توافق کلید موسوم به ECG-IJS نسبت به دو الگوریتم دیگر دارای اولویت بالاتری است و به عنوان طرح بهتر انتخاب می‌شود.

کلید واژه: **شبکه‌های بی‌سیم روی بدن، Fuzzy Vault، الگوریتم توافق کلید، تصمیم‌گیری چندمعیاره، فرایند تحلیل سلسله‌مراتبی فازی.**

۱- مقدمه

شبکه حسگر بی‌سیم شبکه‌ای است که از تعدادی گره‌های حسگر کوچک که در محل‌های مورد نظر مستقر هستند تشکیل شده است. این گره‌های حسگر متشکل از فرستنده و گیرنده‌های رادیویی و ریزپردازنده‌های جاسازی شده و سخت‌افزار حسگرها هستند و لذا قادر به پردازش و مخابره اطلاعات هم می‌باشند. این گره‌ها معمولاً در یک فاصله کوتاه و به وسیله ارتباط بی‌سیم برای انجام یک وظیفه مشترک با هم همکاری می‌کنند و دارای محدودیت‌هایی در قدرت پردازش، ظرفیت حافظه و توان منبع تغذیه هستند [۱].

یکی از حوزه‌های به کارگیری شبکه‌های حسگر بی‌سیم (WSN)[1]، حوزه سلامت است. در بعضی از کاربردهای این حوزه که موسوم به شبکه‌های بی‌سیم روی بدن (WBAN)[2] هستند، گره‌های کوچک هوشمند در لباس یا روی بدن و حتی در زیر پوست قرار داده می‌شوند و به این ترتیب توانایی اندازه‌گیری پارامترهایی مانند ضربان قلب و دمای بدن فراهم می‌گردد. برخی از کاربردهایی که با استفاده از WBANها قابل انجام می‌باشد عبارتند از پایش بیمار به طور مستمر و از راه دور، مراقبت از سالمندان و پایش سیگنال‌های حیاتی [۲].

با توجه به این که این کاربردها با اطلاعات و داده‌های پزشکی افراد سر و کار دارند، حفظ امنیت داده‌ها در WBANها از اهمیت ویژه‌ای برخوردار است و تأمین سطح مناسبی از امنیت در ارتباطات WBANها به عنوان یک چالش مهم مد نظر قرار گرفته است. برای تبادل اطلاعات به صورت امن، نیاز به رمزنگاری وجود دارد. از آنجا که در این شبکه‌ها با توجه به محدودیت‌های ناشی از کوچکی ابعاد و قابلیت‌های پایین محاسباتی و ارتباطی، رمزنگاری متقارن عملی‌تر از رمزنگاری نامتقارن است، نیاز به توافق و یا تبادل کلید رمز مشترک بین دو طرف ارتباط وجود دارد.

موضوع تبادل کلید رمز در WSNها به طور مستقل مورد توجه قرار گرفته و مکانیزم‌هایی هم برای آن ارائه شده است (برای مثال [۳]). این مکانیزم‌ها معمولاً نیازمند پیش‌توزیع[3] اطلاعات مربوط به تبادل کلید و همچنین تولید دنباله تصادفی[4] (برای استفاده به عنوان کلید رمز) می‌باشند که هر یک از این دو کار، محدودیت‌هایی را در کاربردها ایجاد می‌کند. اما در حوزه خاص WBANها، نیاز به پیش‌توزیع و نیاز به مدارهای مولد اعداد تصادفی از بین می‌رود. در حوزه WBANها، اتصال مستقیم حسگرها به بدن این امکان را فراهم می‌کند که از علایم حیاتی بدن انسان (سیگنال‌های فیزیولوژیکی مانند ECG[5] و PPG[6]) برای تولید دنباله تصادفی استفاده شود [۴]. سیگنال‌های فیزیولوژیکی به دلیل برخورداری از ویژگی‌های تصادفی‌بودن[7] و تمایزدهندگی[8] قابل استفاده در تولید کلید رمز هستند [۵]. همچنین قابلیت نمونه‌برداری از سیگنال‌های فیزیولوژیک در سراسر بدن، دسترسی مستقیم گره‌ها به اطلاعات لازم

این مقاله در تاریخ ۲۲ اسفند ماه ۱۳۹۲ دریافت و در تاریخ ۳ آذر ماه ۱۳۹۳ بازنگری شد.

مرتضی ابراهیمی، دانشکده علوم و فنون نوین، دانشگاه تهران، تهران، (email: mo.ebrahimi@ut.ac.ir).

سیدحمیدرضا احمدی، دانشکده علوم و فنون نوین، دانشگاه تهران، تهران، (email: hrahmadi@ut.ac.ir).

مریم عباس‌نژاد آرا، دانشجوی دانشکده علوم و فنون نوین، دانشگاه تهران، تهران، (email: m.abbasnejadara@ut.ac.ir).

1. Wireless Sensor Network
2. Wireless Body Area Network
3. Pre-Distribution
4. Random Number Sequence
5. Electrocardiogram
6. Photoplethysmogram
7. Randomness
8. Distinctiveness

جهت توافق کلید را برقرار می‌کند و در نتیجه نیاز به پیش‌توزیع را از بین می‌برد [۴]. در واقع خود بدن عملیات توافق کلید را انجام می‌دهد.

البته در تولید دنباله تصادفی از روی علایم حیاتی، این چالش وجود دارد که وقتی دو گره در شبکه حسگر به طور هم‌زمان یک سیگنال را اندازه‌گیری می‌کنند، مقادیر ثبت‌شده در دو طرف، مشابه اما دارای اندکی تفاوت هستند. برای حل این مشکل از یک ساختار ریاضی با عنوان Fuzzy Vault [۶] استفاده شده که می‌تواند از روی مقادیر اندازه‌گیری شده علایم حیاتی در دو طرف، کلید رمز یکسانی تولید نماید. ساختار Fuzzy Vault در مقالات متعددی برای توافق کلید مابین گره‌های شبکه بی‌سیم روی بدن مورد استفاده قرار گرفته که در بخش بعدی اجمالاً به آنها اشاره خواهد شد.

معمولاً در مقالاتی که الگوریتم‌های مختلفی برای یک مسأله ارائه می‌گردد، مقایسه‌هایی با پیاده‌سازی‌ها یا الگوریتم‌های قبلی انجام می‌گیرد. این مقایسه‌ها معمولاً دارای چند اشکال هستند. یکی این که مقایسه بین همه الگوریتم‌ها انجام نمی‌شود و دیگر این که تمام پارامترهای ارزیابی، برای مقایسه مورد استفاده قرار نمی‌گیرند. اشکال مهم دیگر این است که درجه اهمیت نسبی پارامترهای ارزیابی در مقایسه لحاظ نمی‌گردد. یکی از ابزارهای ریاضی که می‌تواند برای انجام چنین مقایسه‌هایی مورد استفاده قرار گیرد و مشکلات فوق را حل نماید، تصمیم‌گیری چندمعیاره (MADM)[1] است. روش‌ها و مدل‌های مختلفی برای تصمیم‌گیری چندمعیاره وجود دارد که در شاخه‌های مختلفی از فناوری اطلاعات مورد استفاده قرار گرفته‌اند. در این مقاله، یکی از روش‌های تصمیم‌گیری چندمعیاره که موسوم به فرایند تحلیل سلسله‌مراتبی فازی (FAHP)[2] است، برای مقایسه جامع سه الگوریتم اصلی توافق کلید در WBAN مبتنی بر ساختار Fuzzy Vault (الگوریتم ECG-IJS در [۷]، الگوریتم PSKA در [۸]، و الگوریتم OPFKA در [۹]) مورد استفاده قرار گرفته است.

در ادامه ابتدا به مقالاتی که با استفاده از سیگنال‌های فیزیولوژیکی در WBANها عملیات توافق کلید را انجام داده‌اند اشاره خواهد شد. سپس توضیحاتی درباره تصمیم‌گیری چندمعیاره و فرایند تحلیل سلسله‌مراتبی فازی ارائه می‌شود. در نهایت، مراحل اجرای فرایند تحلیل سلسله‌مراتبی فازی برای ارزیابی، مقایسه و انتخاب بهترین الگوریتم توافق کلید و نتایج حاصل از آن ارائه خواهند شد.

۲- استفاده از سیگنال‌های فیزیولوژیک برای توافق کلید رمز در WBANها

استفاده از سیگنال‌های فیزیولوژیک در شبکه‌های بی‌سیم روی بدن با هدف ارائه سرویس‌های رمزنگاری، اولین بار در سال ۲۰۰۳ در [۴] مطرح شد. نویسندگان [۴] مطرح کردند که پارامترهای فیزیولوژیکی‌ای که از آنتروپی بالایی برخوردار هستند، قابلیت استفاده در تولید کلید رمز را دارند. در [۴] برای حل چالش تفاوت در مقدار اندازه‌گیری شده دو سیگنال فیزیولوژیکی از یک ساختار ریاضی به نام Fuzzy Commitment [۱۰] برای توافق کلید استفاده شده است. به دنبال این ایده در [۵] و [۱۱] از ویژگی استخراج‌شده از دامنه زمانی سیگنال‌های ECG و PPG (که به آن IPI[3] اطلاق می‌شود) برای تولید دنباله تصادفی (و توافق کلید رمز) استفاده شده است. در [۵] تأثیر نرخ نمونه‌برداری از سیگنال‌ها، تعداد IPIهای مورد استفاده در هر دنباله و تعداد بیت‌های مورد استفاده برای کدکردن ویژگی استخراج‌شده، بر میزان خطا مورد بررسی قرار گرفته است. همچنین در [۵] مناسب‌بودن IPI برای کاربرد رمزنگاری، ارزیابی شده و روشی جهت هم‌زمان‌سازی[4] زمان ثبت سیگنال توسط حسگرها آمده است. در [۱۱] علاوه بر تحلیل میزان تصادفی‌بودن و تمایزدهندگی دنباله‌های تولیدشده، این دنباله‌ها با دنباله‌های تولیدشده توسط روش‌های سخت‌افزاری مقایسه شده است.

در [۱۲] نویسنده استفاده از IPI برای تولید کلید رمز را زمان‌بر می‌داند و آن را برای کاربردهای بلادرنگ مناسب نمی‌داند. از این رو از اطلاعات سیگنال ECG در دامنه فرکانسی (به جای دامنه زمانی) استفاده کرده و با این کار زمان تولید کلید را کاهش داده است. در ادامه مقاله [۱۲]، یک پروتکل توافق کلید ارائه شده که در آن با رد و بدل کردن داده‌هایی که از سیگنال ECG در دو طرف تولید شده، کلید رمز اصلی ایجاد می‌شود.

ساختار ریاضی دیگری که برای حل چالش تفاوت در مقدار اندازه‌گیری شده دو سیگنال فیزیولوژیکی در دو طرف ارتباط ارائه شده، Fuzzy Vault نام دارد [۶] که در [۸]، [۱۳] و [۱۴] از این ساختار برای ارائه پروتکل توافق کلید استفاده شده است.

در [۱۳] و [۱۴] به ترتیب از اطلاعات دامنه فرکانسی سیگنال‌های PPG و ECG برای تولید دنباله تصادفی استفاده شده و در [۸] (که ادامه و تکمیل [۱۳] است) هر دو سیگنال مورد استفاده قرار گرفته است. هر سه مقاله از ساختار Fuzzy Vault یکسانی برای ایجاد یک پروتکل توافق کلید استفاده کرده‌اند و میزان امنیت و نرخ خطا را مورد بررسی قرار داده‌اند.

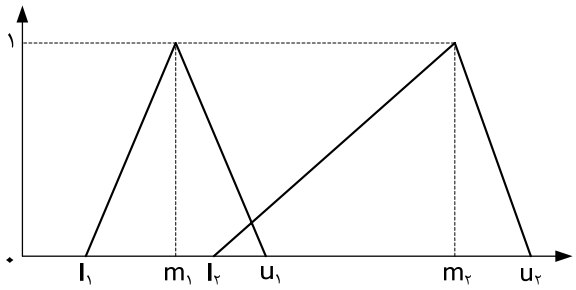
در [۷] از ویژگی‌های استخراج‌شده از دامنه فرکانسی سیگنال ECG به عنوان کلید رمز استفاده شده و در ادامه نویسنده برای کاهش سربار ارتباطی در ساختار اصلی Fuzzy Vault، تغییراتی روی آن اعمال کرده است. همچنین [۷] به مقایسه نرخ خطای ساختار جدید با ساختار اصلی و سپس تحلیل امنیتی آن پرداخته است. مقاله [۹] با کمک‌گرفتن از [۸] و اصلاح روش آن و بهره‌گیری از روش‌های مقالات قبلی و ادغام آنها، بهبودهایی را در توافق کلید حاصل کرده است. در [۱۵] و [۱۶] نیز تغییرات و اصلاحاتی بر روی ساختار اصلی Fuzzy Vault اعمال شده است که هدف آنها کاهش خطای سیستم و مقاوم‌شدن Fuzzy Vault در مقابل بعضی از انواع حمله‌ها (جهت شکستن رمز) است.

بر اساس محتوای این مقالات و با توجه به توضیحات فوق، می‌توان این گونه جمع‌بندی کرد که الگوریتم‌های ارائه‌شده در [۷] تا [۹]، نسخه‌های تکمیل‌شده و بهبودیافته الگوریتم‌های دیگر هستند و هر یک از این سه الگوریتم را می‌توان نماینده دسته‌ای از مقالات این حوزه دانست.

۳- تصمیم‌گیری چندمعیاره

در یک مسأله تصمیم‌گیری چندمعیاره، هدف انتخاب بهترین گزینه[5] از میان گزینه‌های موجود است. در این مسایل، تعدادی گزینه از منظر چندین معیار مورد تجزیه و تحلیل قرار می‌گیرند و در مورد آنها،

1. Multi-Attribute Decision Making
2. Fuzzy Analytical Hierarchy Process
3. Inter-Pulse Interval
4. Synchronization
5. Alternative



شکل ۱: توابع عضویت اعداد فازی مثلثی M_1 و M_2.

اولویت‌بندی انجام می‌شود. به عنوان مثال گزینه‌ها ممکن است الگوریتم‌های مختلف برای اجرای یک فرایند خاص یا انجام یک سری محاسبات باشند. معیارهای[1] مورد استفاده برای ارزیابی و اولویت‌بندی مسایل مورد نظر، باید توسط تصمیم‌گیرنده با دقت و زیر نظر متخصصین مشخص گردند [۱۷]. یکی از روش‌های تصمیم‌گیری چندمعیاره، فرایند تحلیل سلسله‌مراتبی است که در ادامه به معرفی آن خواهیم پرداخت.

۳-۱ فرایند تحلیل سلسله‌مراتبی

فرایند تحلیل سلسله‌مراتبی (AHP)[2] در سال ۱۹۷۰ ارائه شد. این روش همانند فرایندی که در مغز انسان انجام می‌شود به تجزیه و تحلیل مسایل می‌پردازد. روش AHP تصمیم‌گیرنده را قادر می‌سازد تا اثرات مختلف و متقابل بسیاری از وضعیت‌های پیچیده را تعیین کند و اولویت‌ها را بر اساس هدف، دانش و تجربه خود تنظیم نماید. برای حل مسایل تصمیم‌گیری از طریق AHP، باید مسأله را به دقت و با در نظر گرفتن تمام جزئیات، تعریف و تبیین کرد و جزئیات آن را به صورت یک ساختار سلسله‌مراتبی ترسیم نمود.

در روش AHP مسأله تصمیم‌گیری به مراحل اصلی زیر تقسیم می‌شود:

- ساختاردهی مسأله (ساخت سلسله‌مراتبی)
- ارزیابی اولویت‌های محلی
- محاسبه اولویت‌های نهایی (کلی)

مسأله تصمیم‌گیری AHP در سلسله‌مراتبی از سطوح مختلف ساختاردهی می‌شود که هر سطح شامل تعداد محدودی از عناصر تصمیم‌گیری است. بالاترین سطح از این سلسله‌مراتب، مربوط به هدف و پایین‌ترین سطح، مربوط به گزینه‌های ممکن است. سطوح میانی به عنوان معیارها و زیرمعیارها در نظر گرفته می‌شوند. موضوع مهم در مورد عناصر تصمیم‌گیری (وزن معیارها و امتیاز گزینه‌ها) این است که آنها به صورت غیر مستقیم از مقایسه قضاوت‌ها در طول مرحله دوم محاسبه می‌شوند. تصمیم‌گیرنده نیاز به فراهم‌کردن ترجیحات خود از طریق مقایسه تمام معیارها و گزینه‌ها دارد که این مقایسه‌ها به کمک افراد خبره صورت می‌گیرد [۱۸].

۳-۲ فرایند تحلیل سلسله‌مراتبی فازی

اگرچه افراد خبره از شایستگی‌ها و توانایی‌های ذهنی خود برای انجام مقایسه‌ها استفاده می‌نمایند اما باید به این نکته توجه داشت که فرایند تحلیل سلسله‌مراتبی معمولی، امکان انعکاس سبک تفکر انسانی را به طور کامل ندارد. به عبارت بهتر، استفاده از مجموعه‌های فازی، سازگاری بیشتری با توضیحات زبانی و بعضاً مبهم انسانی دارد و بنابراین بهتر است

1. Criteria
2. Analytical Hierarchy Process

جدول ۱: مقیاس‌های زبانی و اعداد فازی مثلثی مرتبط.

مقیاس زبانی	عدد فازی مثلثی	معکوس عدد فازی مثلثی
اهمیت برابر	(۱ ۱ ۱)	(۱ ۱ ۱)
نسبتاً مهم‌تر	(۱/۵ ۱ ۲)	(۰/۵ ۱ ۰/۶۶)
مهم‌تر	(۲ ۱/۵ ۱)	(۱ ۰/۶۶ ۰/۵)
خیلی مهم‌تر	(۲/۵ ۲ ۱/۵)	(۰/۶۶ ۰/۵ ۰/۴)
بسیار مهم‌تر	(۳ ۲/۵ ۲)	(۰/۵ ۰/۴ ۰/۳۳)
بی‌نهایت مهم‌تر	(۳/۵ ۳ ۲/۵)	(۰/۴ ۰/۳۳ ۰/۲۸)

که با استفاده از مجموعه‌های فازی (به کارگیری اعداد فازی) به پیش‌بینی بلندمدت و تصمیم‌گیری در دنیای واقعی پرداخت. به این معنی که برای انجام مقایسه‌ها، به هر نسبتِ مقایسه‌ای یک عدد فازی اختصاص داده می‌شود و سپس از این اعداد برای تجزیه و تحلیل نتایج استفاده می‌شود. اعداد فازی مورد استفاده در این روش اعداد فازی مثلثی هستند. مقیاس‌های فازی مورد استفاده در فرایند تحلیل سلسله‌مراتبی فازی در جدول ۱ نشان داده شده اند [۱۹] و [۲۰].

اعداد فازی مثلثی به شکل ۳تایی $(l\ \ m\ \ u)$ نشان داده می‌شوند [۱۹]. برای دو عدد فازی مثلثی $M_1=(l_1\ \ m_1\ \ u_1)$ و $M_2=(l_2\ \ m_2\ \ u_2)$ که توابع عضویت[3] آنها در شکل ۱ نمایش داده شده است، عملگرهای ریاضی به صورت (۱) تا (۳) تعریف می‌شود [۲۰] و [۲۱]

$$M_1+M_2=(l_1+l_2\ \ m_1+m_2\ \ u_1+u_2) \quad (۱)$$

$$M_1\times M_2=(l_1\times l_2\ \ m_1\times m_2\ \ u_1\times u_2) \quad (۲)$$

$$M_1^{-1}=\left(\frac{1}{u_1}\ \ \frac{1}{m_1}\ \ \frac{1}{l_1}\right)$$
$$M_2^{-1}=\left(\frac{1}{u_2}\ \ \frac{1}{m_2}\ \ \frac{1}{l_2}\right) \quad (۳)$$

برای مقایسه بزرگی اعداد فازی مثلثی نیز هرگاه M_1 و M_2 دو عدد فازی مثلثی باشند، درجه بزرگی M_1 نسبت به M_2، به صورت (۴) تعریف می‌شود

$$V(M_1\geq M_2)=\begin{cases}1 & ,\ m_1\geq m_2\\ 0 & ,\ l_2\geq u_1\\ \dfrac{u_1-l_2}{(u_1-l_2)+(m_2-m_1)} & ,\ \text{otherwise}\end{cases} \quad (۴)$$

همچنین میزان بزرگی عدد فازی مثلثی M_1 نسبت به اعداد فازی مثلثی $M_2,M_3,\ldots,M_k$ از (۵) به دست می‌آید

$$V(M_1\geq M_2,\ldots,M_K)=\min[V(M_1\geq M_2),\ldots,V(M_1\geq M_K)] \quad (۵)$$

پس از این که ساختار سلسله‌مراتبی برای مسأله تصمیم‌گیری تشکیل داده شد، ماتریس‌های تصمیم مربوط به مقایسه‌های زوجی میان شاخص‌ها و مقایسه‌های زوجی میان گزینه‌ها (با توجه به هر شاخص) ساخته می‌شوند. سپس برای هر یک از سطرهای ماتریس مقایسه‌های زوجی، یک مقدار S_k که خود یک عدد فازی مثلثی است به صورت (۶) محاسبه می‌شود

$$S_k=\sum_{j=1}^{n}M_{kj}\times\left[\sum_{i=1}^{m}\sum_{j=1}^{n}M_{ij}\right]^{-1} \quad (۶)$$

3. Membership Function

که k بیانگر شماره سطر ماتریس و i و j به ترتیب نشان‌دهنده شماره گزینه‌ها و معیارها هستند.

در مرحله بعد، پس از محاسبه S_kها باید درجه بزرگی آنها را نسبت به هم به دست آورد. در واقع برای تمامی سطرهای هر ماتریس مقایسه‌های زوجی گزینه‌ها (نسبت به شاخص‌های مختلف)، یک مقدار S_k محاسبه می‌شود. سپس با استفاده از (۴)، درجه بزرگی این S_kها دو به دو نسبت به هم به دست می‌آیند و نهایتاً درجه بزرگی هر S_k نسبت به دیگر مقادیر با استفاده از (۵) به دست می‌آید. به بیان دیگر در ماتریس مقایسه‌های زوجی گزینه‌ها نسبت به شاخص j ام (در این مقاله با توجه به وجود هشت معیار در مسأله تصمیم‌گیری، داریم: $j=1,2,\ldots,8$)، برای گزینه‌های $A_1=OPFKA$ ، $A_2=PSKA$ و $A_3=ECG-IJS$ به ترتیب سه مقدار S_1^j، S_2^j و S_3^j به دست می‌آید. در نتیجه بر اساس (۵) مقادیر زیر را (که به تعداد گزینه‌ها هستند) به دست می‌آوریم

$$\begin{aligned} V(S_1^j \geq S_2^j, S_3^j) &= \min[V(S_1^j \geq S_2^j), V(S_1^j \geq S_3^j)] \\ V(S_2^j \geq S_1^j, S_3^j) &= \min[V(S_2^j \geq S_1^j), V(S_2^j \geq S_3^j)] \\ V(S_3^j \geq S_1^j, S_2^j) &= \min[V(S_3^j \geq S_1), V(S_3^j \geq S_2^j)] \end{aligned} \quad (۷)$$

سپس، با استفاده از مقادیر فوق، بردار اهمیت نسبی زیر را به دست می‌آوریم که بیان‌کننده ارزش و اهمیت نسبی سه گزینه مسأله از لحاظ معیار j ام می‌باشد

$$W_j = [V(S_1^j \geq S_2^j, S_3^j), V(S_2^j \geq S_1^j, S_3^j), V(S_3^j \geq S_1^j, S_2^j)]^T \quad (۸)$$
$$, \quad j=1,\ldots,8$$

در مرحله بعد، بردار به دست آمده W_j را با تقسیم هر مؤلفه بر مجموع مؤلفه‌های آن، به هنجار[1] می‌کنیم. برای تمامی ماتریس‌های مقایسه‌های زوجی گزینه‌ها نسبت به شاخص‌ها، چنین برداری را به دست می‌آوریم. با توجه به این که در مسأله تصمیم‌گیری ارائه‌شده در این مقاله هشت شاخص مختلف معرفی شده است، متناظر با این هشت ماتریس مقایسه‌های زوجی، هشت بردار اهمیت نسبی مربوط به گزینه‌ها به دست می‌آید که به هنجار شده آنها را به عنوان بردارهای ستونی ماتریس W_A در نظر می‌گیریم

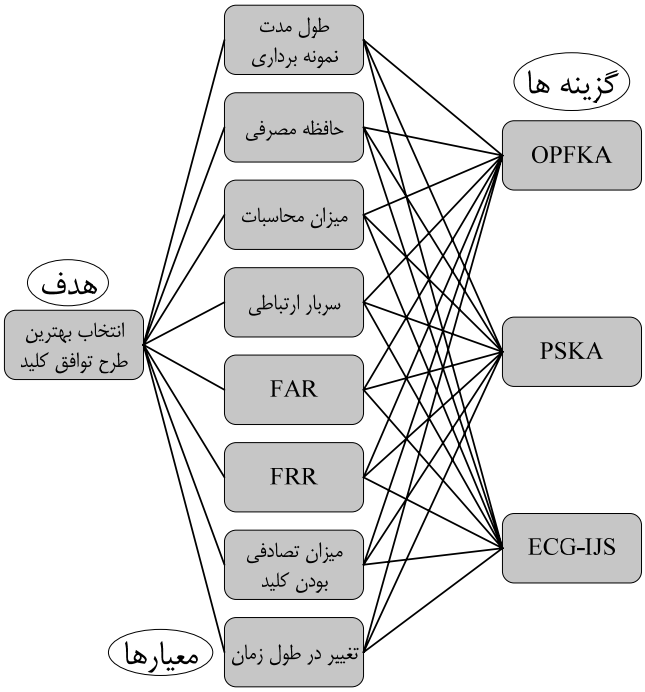
$$W_A = [W_1^N \ W_2^N \ W_3^N \ W_4^N \ W_5^N \ W_6^N \ W_7^N \ W_8^N] \quad (۹)$$

که در آن W_j^N به هنجار شده W_j می‌باشد.

در گام بعد همانند آنچه برای ماتریس‌های مقایسه‌های زوجی گزینه‌ها نسبت به شاخص‌ها انجام دادیم، برای ماتریس مقایسه‌های زوجی شاخص‌ها نسبت به یکدیگر نیز پس از محاسبه S_kها و تعیین درجه بزرگی آنها نسبت به یکدیگر، به بردار W_C می‌رسیم که بیانگر وزن و ارزش معیارها در قیاس با یکدیگر می‌باشد

$$W_C = \begin{bmatrix} V(S_1 \geq S_2, S_3, S_4, S_5, S_6, S_7, S_8) \\ V(S_2 \geq S_1, S_3, S_4, S_5, S_6, S_7, S_8) \\ V(S_3 \geq S_1, S_2, S_4, S_5, S_6, S_7, S_8) \\ V(S_4 \geq S_1, S_2, S_3, S_5, S_6, S_7, S_8) \\ V(S_5 \geq S_1, S_2, S_3, S_4, S_6, S_7, S_8) \\ V(S_6 \geq S_1, S_2, S_3, S_4, S_5, S_7, S_8) \\ V(S_7 \geq S_1, S_2, S_3, S_4, S_5, S_6, S_8) \\ V(S_8 \geq S_1, S_2, S_3, S_4, S_5, S_6, S_7) \end{bmatrix} \quad (۱۰)$$

1. Normalized



شکل ۲: ساختار سلسله‌مراتبی برای مسأله تصمیم‌گیری.

در گام آخر حاصل‌ضرب ماتریس W_A و بردار W_C^N (که به هنجار شده بردار W_C است) را به دست می‌آوریم و بر اساس مقادیر به دست آمده از این حاصل‌ضرب، گزینه‌ها را رتبه‌بندی می‌کنیم.

٤- استفاده از AHP فازی در انتخاب بهترین الگوریتم توافق کلید

در این بخش، اجرای مراحل متوالی فرایند تحلیل سلسله‌مراتبی فازی، برای حل مسأله تصمیم‌گیری درباره انتخاب بهترین الگوریتم توافق کلید از میان الگوریتم‌های مطرح شده در بخش ۲ شرح داده خواهد شد.

٤-١ ساختار سلسله‌مراتبی

چنان که در بخش ۳-۱ بیان شد، بالاترین سطح از سلسله‌مراتب، مربوط به هدف مسأله تصمیم‌گیری و پایین‌ترین سطح مربوط به گزینه‌های در حال ارزیابی است. سطوح میانی به عنوان معیارها در نظر گرفته می‌شوند. ساختار سلسله‌مراتبی برای مسأله تصمیم‌گیری مورد نظر در این مقاله در شکل ۲ نشان داده شده است. عناصر تشکیل‌دهنده این سلسله‌مراتب در ادامه توضیح داده خواهند شد.

٤-١-١ هدف

هدف از به کار بردن روش AHP فازی در این مقاله، انتخاب بهترین الگوریتم توافق کلید در شبکه‌های بی‌سیم روی بدن است.

٤-١-٢ معیارها

در تعیین معیارهای مقایسه، ویژگی‌ها و محدودیت‌های WBANها که از کوچکی سایز گره‌ها و ارتباط بی‌سیم ناشی می‌شود را مد نظر قرار داده‌ایم. همچنین نوع کاربرد و استفاده از این شبکه‌ها در پایش از راه دور و اهمیت زمان نیز برای تعیین معیارها مد نظر قرار گرفته است. با توجه به این که در نهایت، برقراری امنیت هدف اصلی الگوریتم‌های مورد ارزیابی می‌باشد، ویژگی‌های کلید رمز یعنی میزان تصادفی‌بودن، متمایزبودن و تغییر در طول زمان نیز اهمیت زیادی دارند. معیارهای مقایسه و ارزیابی الگوریتم‌ها در زیر فهرست شده و به اختصار توضیح داده شده است:

- میزان تصادفی‌بودن کلید: کلیدهای رمز توافق‌شده باید از نظر طول و تصادفی‌بودن به گونه‌ای باشند که از حمله‌های آزمون جامع فضای کلید[1] جلوگیری به عمل بیاید.
- تمایزدهندگی: ویژگی‌های استخراج‌شده از سیگنال‌های فیزیولوژیک (که به منظور تولید کلید و یا توافق کلید مورد استفاده قرار می‌گیرند) باید به اندازه کافی بین دو فرد تمایز ایجاد کنند و امکان حدس زده شدن این کلید توسط گره‌های دیگر روی بدن فرد دیگر وجود نداشته باشد. معمولاً برای ارزیابی این معیار از دو مقدار قابل محاسبه به نام‌های نرخِ اشتباه در رد (FRR)[2] و نرخِ اشتباه در قبول (FAR)[3] استفاده می‌شود [۸] که برای الگوریتم‌های توافق کلید به صورت زیر تعریف می‌شوند:
  - FRR: نشان‌دهنده نرخی است که دو گره که در یک شبکه بی‌سیم روی بدن واحد قرار دارند- یعنی هر دو گره روی بدن یک فرد قرار گرفته‌اند- موفق به توافق کلید نمی‌شوند (به دلیل این که تعداد ویژگی‌های مشترک حاصل از تحلیل سیگنال‌های فیزیولوژیکی نمونه‌برداری شده توسط دو گره از حد آستانه کمتر است).
  - FAR: نشان‌دهنده نرخی است که دو گره که در دو شبکه بی‌سیم روی بدن مختلف قرار دارند- یعنی دو گره روی بدن دو نفر قرار گرفته‌اند- به اشتباه موفق به توافق کلید می‌شوند (به دلیل این که تعداد ویژگی‌های مشترک حاصل از تحلیل سیگنال‌های فیزیولوژیکی نمونه‌برداری شده توسط دو گره از حد آستانه بیشتر است).
- تغییر در طول زمان[4]: برخورداری کلید رمز از این ویژگی به این معنی است که ویژگی‌های حاصل از تحلیل سیگنال‌های فیزیولوژیکی نمونه‌برداری شده در یک زمان مشخص نباید قابل استفاده در تولید و توافق کلیدی در زمان‌های دیگر باشند [۹].
- حافظه مصرفی
- طول مدت نمونه‌برداری: مدت زمان نمونه‌برداری از سیگنال فیزیولوژیکی باید تا حد ممکن کوتاه باشد.
- سربار ارتباطی که بر روی انرژی مصرفی تأثیر مستقیم دارد.
- میزان محاسبات که بر روی انرژی مصرفی تأثیر مستقیم دارد.

لازم به ذکر است که انرژی مصرفی به عنوان یک معیار واحد در نظر گرفته نشده و تأثیر آن در ارزیابی و مقایسه گزینه‌ها، در معیارهای دیگر (مانند سربار ارتباطی و میزان محاسبات) لحاظ گردیده است.

٤-١-٣ گزینه‌ها

در بخش ۲ به مجموعه مقالاتی که برای توافق کلید در WBANها از سیگنال‌های فیزیولوژیکی استفاده کرده‌اند اشاره‌ای داشتیم. از این مجموعه، سه مورد از الگوریتم‌های ارائه‌شده که روش آنها با یکدیگر متفاوت است و نسبت به الگوریتم‌های مشابه، تکمیل‌تر و بهبودیافته‌تر هستند، برای ارزیابی توسط روش AHP فازی انتخاب شدند. این سه الگوریتم عبارتند از:

– الگوریتم ارائه‌شده در [۹] با نام OPFKA[5]

– الگوریتم ارائه‌شده در [۸] با نام PSKA[6]

– الگوریتم ارائه‌شده در [۷] با نام ECG-IJS[7]

در الگوریتم OPFKA دو گره که متعلق به یک شبکه بی‌سیم روی بدن هستند، بر سر یک کلید متقارن که از هم‌پوشانی ویژگی‌های استخراج‌شده از سیگنال‌های فیزیولوژیک حاصل می‌شود، توافق می‌کنند. بر همین اساس از پیش‌توزیع اطلاعات لازم برای تولید کلید در هر گره جلوگیری می‌شود. ویژگی‌های به دست آمده از سیگنال فیزیولوژیک یکسان که در قسمت‌های مختلف بدن فرد نمونه‌برداری می‌شود تا حد زیادی هم‌پوشانی دارند، اما کاملاً یکسان نیستند. برای غلبه بر این چالش در این الگوریتم یک راه حل مبتنی بر ترتیب (order) از پیش مشخص شده برای ویژگی‌های استخراج‌شده به همراه افزودن نویز (Chaff Point) ارائه شده است [۹].

در الگوریتم PSKA برای توافق کلید از یک چندجمله‌ای استفاده می‌شود که ضرایب این چندجمله‌ای کلید رمز است. در طرف فرستنده با جایگذاری ویژگی‌های استخراج‌شده از سیگنال فیزیولوژیک در چندجمله‌ای و محاسبه مقدار چندجمله‌ای به ازای این مقادیر، تعدادی زوج مرتب حاصل می‌شود. در ادامه تعدادی زوج مرتب دیگر (Chaff Point) که در چندجمله‌ای صدق نمی‌کنند با این زوج‌های مرتب ترکیب شده و برای گره مورد نظر ارسال می‌شوند. گیرنده با استفاده از ویژگی‌هایی که خود استخراج کرده، اقدام به بازسازی چندجمله‌ای و در نتیجه استخراج کلید رمز می‌کند [۸].

در الگوریتم ECG-IJS نیز از یک روش مبتنی بر چندجمله‌ای بهره گرفته شده است، اما در این روش با اعمال تغییراتی، نیاز به استفاده از Chaff Pointها به جهت افزایش امنیت از بین رفته است [۷].

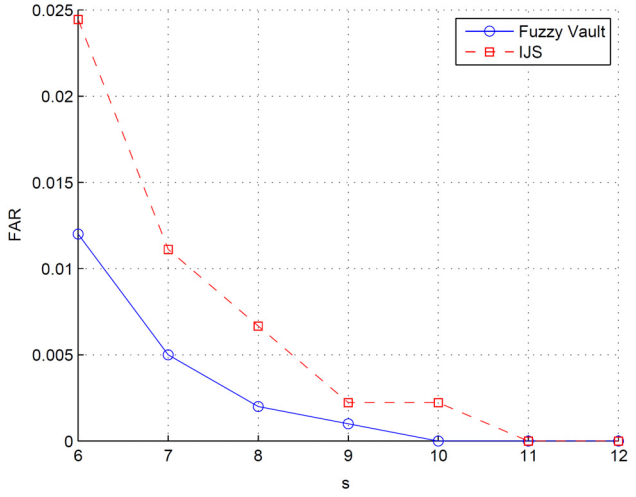
٤-٢ تشکیل ماتریس‌های مقایسه‌های زوجی

٤-٢-١ مقایسه زوجی معیارها

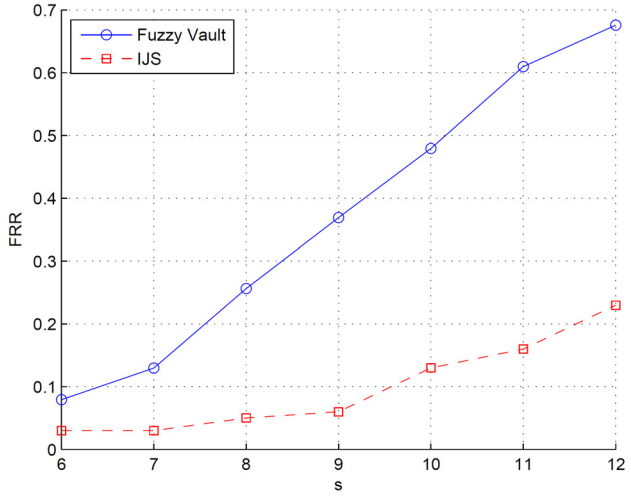
هر یک از معیارهایی که برای مقایسه گزینه‌های موجود در ساختار مورد استفاده قرار می‌گیرند، دارای اهمیت متفاوتی نسبت به یکدیگر می‌باشند. در واقع همه معیارها از لحاظ ارزش مقایسه‌ای وزن یکسانی ندارند. در مرحله اول با مقایسه زوجی معیارها نسبت به یکدیگر، اهمیت و ارزش نسبی معیارها مشخص می‌شود. برای تعیین اهمیت و ارزش نسبی معیارهای مختلف، چنین استدلال شده است:

۱) به علت محدودبودن ابعاد گره‌ها و در نتیجه عدم امکان استفاده از منبع انرژی (باتری) بزرگ، مسأله مصرف انرژی در WBANها دارای اهمیت زیادی است. معمولاً محاسبات سهم چندانی از مصرف این انرژی محدود ندارند و ارتباطات در گره‌ها نسبت به سایر عملیات پرهزینه‌تر هستند [۲۲]. بنابراین عددی که در تقاطع مربوط به دو معیار سربار ارتباطی و میزان محاسبات قرار می‌گیرد باید حاکی از اهمیت بیشتر سربار ارتباطی نسبت به میزان محاسبات باشد. یعنی از آنجایی که ارتباطات نسبت به محاسبات انرژی بیشتری را مصرف می‌کنند، از جهت مقایسه گزینه‌ها دارای وزن بیشتری نیز خواهند بود [۲۲].

1. Brute Forcing
2. False Rejection Rate
3. False Acceptance Rate
4. Temporal Variance
5. Ordered-Physiological-Feature-Based Key Agreement
6. Physiological-Signal-Based Key Agreement
7. Electrocardiogram-Improved Jules Sudan



شکل ۳: مقایسه نرخ FAR در طرح PSKA و ECG-IJS [۷].



شکل ۴: مقایسه نرخ FRR در طرح PSKA و ECG-IJS [۷].

جدول ۲: مقایسه زوجی معیارها.

معیارها	طول مدت نمونه‌برداری	حافظه مصرفی	سربار ارتباطی	میزان محاسبات	FRR	FAR	تصادفی‌بودن کلید	تغییر در طول زمان
طول مدت نمونه‌برداری	(۱ ۱ ۱)	(۰٫۵ ۱ ۱٫۵)	(۱ ۱٫۵ ۲)	(۱ ۱٫۵ ۲)	(۰٫۵ ۰٫۶۶ ۱)	(۰٫۵ ۰٫۶۶ ۱)	(۰٫۵ ۰٫۶۶ ۱)	(۰٫۵ ۰٫۶۶ ۱)
حافظه مصرفی	(۰٫۶۶ ۱ ۲)	(۱ ۱ ۱)	(۰٫۵ ۰٫۶۶ ۱)	(۰٫۵ ۰٫۶۶ ۱)	(۰٫۴ ۰٫۵ ۰٫۶۶)	(۰٫۴ ۰٫۵ ۰٫۶۶)	(۰٫۴ ۰٫۵ ۰٫۶۶)	(۰٫۴ ۰٫۵ ۰٫۶۶)
سربار ارتباطی	(۰٫۵ ۰٫۶۶ ۱)	(۰٫۵ ۰٫۶۶ ۱)	(۱ ۱ ۱)	(۱ ۱٫۵ ۲)	(۰٫۶۶ ۱ ۲)	(۰٫۶۶ ۱ ۲)	(۰٫۶۶ ۱ ۲)	(۰٫۶۶ ۱ ۲)
میزان محاسبات	(۰٫۵ ۰٫۶۶ ۱)	(۱ ۱٫۵ ۲)	(۰٫۵ ۰٫۶۶ ۱)	(۱ ۱ ۱)	(۰٫۵ ۰٫۶۶ ۱)	(۰٫۵ ۰٫۶۶ ۱)	(۰٫۵ ۰٫۶۶ ۱)	(۰٫۵ ۰٫۶۶ ۱)
FRR	(۱ ۱٫۵ ۲)	(۱٫۵ ۲ ۲٫۵)	(۰٫۵ ۱ ۱٫۵)	(۱ ۱٫۵ ۲)	(۱ ۱ ۱)	(۱ ۱ ۱)	(۱ ۱ ۱)	(۱ ۱ ۱)
FAR	(۱ ۱٫۵ ۲)	(۱٫۵ ۲ ۲٫۵)	(۰٫۵ ۱ ۱٫۵)	(۱ ۱٫۵ ۲)	(۱ ۱ ۱)	(۱ ۱ ۱)	(۱ ۱ ۱)	(۱ ۱ ۱)
تصادفی‌بودن کلید	(۱ ۱٫۵ ۲)	(۱٫۵ ۲ ۲٫۵)	(۰٫۵ ۱ ۱٫۵)	(۱ ۱٫۵ ۲)	(۱ ۱ ۱)	(۱ ۱ ۱)	(۱ ۱ ۱)	(۱ ۱ ۱)
تغییر در طول زمان	(۱ ۱٫۵ ۲)	(۱٫۵ ۲ ۲٫۵)	(۰٫۵ ۱ ۱٫۵)	(۱ ۱٫۵ ۲)	(۱ ۱ ۱)	(۱ ۱ ۱)	(۱ ۱ ۱)	(۱ ۱ ۱)

جدول ۳: مقایسه زوجی گزینه‌ها از جنبه تمایزدهندگی (FAR).

گزینه‌ها	OPFKA	PSKA	ECG-IJS
OPFKA	(۱ ۱ ۱)	(۰٫۵ ۰٫۶۶ ۱)	(۰٫۶۶ ۱ ۲)
PSKA	(۱ ۱٫۵ ۲)	(۱ ۱ ۱)	(۱ ۱٫۵ ۲)
ECG-IJS	(۰٫۵ ۱ ۱٫۵)	(۰٫۵ ۰٫۶۶ ۱)	(۱ ۱ ۱)

۲) با توجه به این که شبکه‌های بی‌سیم روی بدن در کاربردهای مختلف حوزه سلامت باید از سرعت عمل بالایی در انتقال اطلاعات برخوردار باشند (خصوصاً برای شرایط اورژانسی که کاربرد بلادرنگ به حساب می‌آید)، مسأله زمان از اهمیت بیشتری نسبت به انرژی مصرفی برخودار است. در نتیجه، معیار مدت زمان نمونه‌برداری نسبت به معیارهای وابسته به مصرف انرژی (یعنی سربار ارتباطی و میزان محاسبات) از اهمیت بالاتری برخوردار است.

۳) با توجه به این که الگوریتم‌های مورد ارزیابی (گزینه‌ها) در واقع به دنبال برقراری ارتباط امن بر اساس توافق کلید رمز هستند، معیارهایی که مشخص‌کننده امنیت این الگوریتم‌ها هستند (یعنی تصادفی‌بودن کلید، تغییر در طول زمان، FAR و FRR) اهمیت بیشتری نسبت به معیارهای دیگر دارند.

ماتریس به دست آمده از مقایسه زوجی معیارها بر اساس استدلال های فوق، در جدول ۲ نمایش داده شده است.

٤-۲-۲ مقایسه زوجی گزینه‌ها بر مبنای معیارها

در این مرحله با مقایسه زوجی گزینه‌ها بر مبنای هر یک از معیارها، ارزش و اولویت نسبی گزینه‌ها از جهات مختلف مشخص می‌شود.

به عنوان مثال با استناد به شکل ۳ (ارائه‌شده در [۷])، معیار FAR در الگوریتم PSKA اندکی بهتر از همین معیار در الگوریتم ECG-IJS می‌باشد. بر این اساس و همچنین با توجه به نتایج ارائه‌شده در [۸] و [۹]، گزینه‌ها از لحاظ معیار FAR با یکدیگر مقایسه شده و نتیجه در جدول ۳ با اعداد فازی مثلثی نشان داده شده است.

به طور مشابه، شکل ۴ نتایج ارائه‌شده در [۷] برای مقایسه FRR را

جدول ۴: مقایسه زوجی گزینه‌ها از جنبه تمایزدهندگی (FRR).

گزینه‌ها	OPFKA	PSKA	ECG-IJS
OPFKA	(۱ ۱ ۱)	(۰/۶۶ ۱ ۲)	(۰/۵ ۰/۶۶ ۱)
PSKA	(۰/۵ ۱ ۱/۵)	(۱ ۱ ۱)	(۰/۴ ۰/۵ ۰/۶۶)
ECG-IJS	(۱ ۱/۵ ۲)	(۱/۵ ۲ ۲/۵)	(۱ ۱ ۱)

جدول ۵: مقایسه زوجی گزینه‌ها از جنبه هزینه زمانی.

گزینه‌ها	OPFKA	PSKA	ECG-IJS
OPFKA	(۱ ۱ ۱)	(۱ ۱ ۱)	(۱ ۱ ۱)
PSKA	(۱ ۱ ۱)	(۱ ۱ ۱)	(۱ ۱ ۱)
ECG-IJS	(۱ ۱ ۱)	(۱ ۱ ۱)	(۱ ۱ ۱)

جدول ۶: مقایسه زوجی گزینه‌ها از جنبه سربار ارتباطی.

گزینه‌ها	OPFKA	PSKA	ECG-IJS
OPFKA	(۱ ۱ ۱)	(۱ ۱/۵ ۲)	(۰/۴ ۰/۵ ۰/۶۶)
PSKA	(۰/۵ ۰/۶۶ ۱)	(۱ ۱ ۱)	(۰/۳۳ ۰/۴ ۰/۵)
ECG-IJS	(۱/۵ ۲ ۲/۵)	(۲ ۲/۵ ۳)	(۱ ۱ ۱)

جدول ۷: مقایسه زوجی گزینه‌ها از جنبه حافظه مصرفی.

گزینه‌ها	OPFKA	PSKA	ECG-IJS
OPFKA	(۱ ۱ ۱)	(۱ ۱/۵ ۲)	(۰/۴ ۰/۵ ۰/۶۶)
PSKA	(۰/۵ ۰/۶۶ ۱)	(۱ ۱ ۱)	(۰/۳۳ ۰/۴ ۰/۵)
ECG-IJS	(۱/۵ ۲ ۲/۵)	(۲ ۲/۵ ۳)	(۱ ۱ ۱)

جدول ۸: مقایسه زوجی گزینه‌ها از جنبه میزان محاسبات.

گزینه‌ها	OPFKA	PSKA	ECG-IJS
OPFKA	(۱ ۱ ۱)	(۱ ۱/۵ ۲)	(۰/۵ ۱ ۱/۵)
PSKA	(۰/۵ ۰/۶۶ ۱)	(۱ ۱ ۱)	(۰/۶۶ ۱ ۲)
ECG-IJS	(۰/۶۶ ۱ ۲)	(۰/۵ ۱ ۱/۵)	(۱ ۱ ۱)

نشان می‌دهد که این معیار در الگوریتم ECG-IJS بسیار بهتر از همین معیار در PSKA می‌باشد. جدول ۴ نتیجه مقایسه گزینه‌ها از لحاظ معیار FRR را با اعداد فازی مثلثی نشان می‌دهد.

به طور کلی در مواردی که برای تولید کلید رمز از ویژگی‌های حوزه فرکانسی سیگنال PPG و ECG استفاده شود، زمان نمونه‌برداری در حدود چند ثانیه کافی خواهد بود در حالی که استفاده از IPI (ویژگی‌های حوزه زمانی) نیازمند زمان نمونه‌برداری در حدود یک تا دو دقیقه می‌باشد. از طرف دیگر زمان محاسبات در روش اول به دلیل استفاده از تبدیل فوریه و عملیات تشخیص قله‌ها نسبت به روش دوم بیشتر خواهد بود. الگوریتم‌های مورد نظر از جهت هزینه زمانی تقریباً همسان هستند. جدول ۵ نتیجه این مقایسه‌ها را نشان می‌دهد.

وضعیت سربار ارتباطی و حافظه مصرفی در الگوریتم ECG-IJS به دلیل عدم استفاده از Chaff Pointها نسبت به دو روش دیگر به شکل قابل ملاحظه‌ای بهتر است [۷]. همچنین سربار ارتباطی و حافظه مصرفی روش OPFKA نسبت به روش PSKA به دلیل کوچک‌تر بودن اندازه هر یک از Chaff Pointها کمتر است [۹]. جداول ۶ و ۷ نتایج این مقایسه‌ها را نشان می‌دهند.

در این الگوریتم‌ها، سربار محاسباتی بیشتر ناشی از عملیات بازسازی چندجمله‌ای است. در روش OPFKA به دلیل این که الگوریتم مورد استفاده برای توافق کلید، مبتنی بر یک ترتیب از پیش مشخص شده است و مانند دو روش دیگر از چندجمله‌ای استفاده نمی‌شود، سربار محاسباتی کمتر خواهد بود. همچنین با توجه به تحلیلی که در [۷] آمده است، سربار محاسباتی در الگوریتم ECG-IJS کمتر می‌باشد. نتیجه این مقایسه‌ها در جدول ۸ نشان داده شده است.

الگوریتم PSKA برای تولید کلید رمز از یک مولد اعداد شبه‌تصادفی[1] استفاده می‌کند و کلید تولیدشده را به عنوان ضرایب چندجمله‌ای استفاده می‌کند. سپس ویژگی‌های استخراج‌شده از سیگنال‌های فیزیولوژیکی برای عملیات توافق کلید مورد استفاده قرار می‌گیرند. در دو الگوریتم دیگر، ویژگی‌های استخراج‌شده به عنوان کلید رمز مورد استفاده قرار می‌گیرند و از آنجا که منبع تولید کلید، سیگنال فیزیولوژیکی (بیومتریک) است نیاز به مولد اعداد شبه‌تصادفی وجود ندارد و این اعداد از سطح تصادفی خوبی برخوردار هستند. جدول ۹ نتیجه این مقایسه‌ها را نشان می‌دهد.

بر اساس اطلاعات ارائه‌شده در [۷] تا [۹] می‌توان بیان کرد که معیار تغییر در طول زمان، برای سیگنال PPG نسبت به سیگنال ECG بیشتر می‌باشد و با چندجمله‌ای‌هایی با درجه کمتر نتیجه بهتری حاصل می‌شود. در مورد IPI نیز باید گفت که تغییر در طول زمان آن مناسب نیست. با توجه به موارد بیان‌شده و اطلاعات مقالات دیگر، مقایسه‌های انجام‌شده در جدول ۱۰ نشان داده شده است.

1. Pseudo-Random Number Generator

جدول ۹: مقایسه زوجی گزینه‌ها از جنبه میزان تصادفی‌بودن کلید.

گزینه‌ها	OPFKA	PSKA	ECG-IJS
OPFKA	(۱ ۱ ۱)	(۰٫۵ ۱ ۱٫۵)	(۱ ۱ ۱)
PSKA	(۰٫۶۶ ۱ ۲)	(۱ ۱ ۱)	(۰٫۶۶ ۱ ۲)
ECG-IJS	(۱ ۱ ۱)	(۰٫۵ ۱ ۱٫۵)	(۱ ۱ ۱)

جدول ۱۰: مقایسه زوجی گزینه‌ها از جنبه تغییر در طول زمان.

گزینه‌ها	OPFKA	PSKA	ECG-IJS
OPFKA	(۱ ۱ ۱)	(۱ ۱ ۱)	(۰٫۵ ۱ ۱٫۵)
PSKA	(۱ ۱ ۱)	(۱ ۱ ۱)	(۰٫۵ ۱ ۱٫۵)
ECG-IJS	(۰٫۶۶ ۱ ۲)	(۰٫۶۶ ۱ ۲)	(۱ ۱ ۱)

جدول ۱۱: بردار ارزش نسبی معیارها (به هنجار شده).

تغییر زمانی	تصادفی‌بودن	FAR	FRR	میزان محاسبات	سربار ارتباطی	حافظه	زمان
۰٫۱۴۸۹	۰٫۱۴۸۹	۰٫۱۴۸۹	۰٫۱۴۸۹	۰٫۰۹۰۸	۰٫۱۳۳۹	۰٫۰۶۶۴	۰٫۱۱۳۲

جدول ۱۲: ماتریس امتیاز نسبی گزینه‌ها بر مبنای معیارها (به هنجار شده).

معیارها / گزینه‌ها	تغییر زمانی	تصادفی‌بودن	FAR	FRR	میزان محاسبات	سربار ارتباطی	حافظه	زمان
OPFKA	۰٫۳۳۳۳	۰٫۳۳۳۳	۰٫۲۹۶۸	۰٫۲۸۸۶	۰٫۳۶۹۴	۰٫۲۲۷۰	۰٫۲۲۷۰	۰٫۳۳۳۳
PSKA	۰٫۳۳۳۳	۰٫۳۳۳۳	۰٫۴۳۰۱	۰٫۲۰۵۹	۰٫۳۰۰۰	−۰٫۲۸۵۴	−۰٫۲۸۵۴	۰٫۳۳۳۳
ECG-IJS	۰٫۳۳۳۳	۰٫۳۳۳۳	۰٫۲۷۳۱	۰٫۵۰۵۵	۰٫۳۳۰۷	۱٫۰۵۸۴	۱٫۰۵۸۴	۰٫۳۳۳۳

جدول ۱۳: رتبه‌بندی نهایی گزینه‌ها.

رتبه‌بندی نهایی گزینه‌ها	
OPFKA	۰٫۳۰۳۲
PSKA	۰٫۲۰۱۸
ECG-IJS	۰٫۴۹۵۰

٤-۳ رتبه‌بندی نهایی گزینه‌ها

پس از تشکیل ماتریس‌های مقایسه‌های زوجی نوبت به انجام مراحل بعدی می‌رسد. برای این کار، روشی که در بخش ۳-۲ توضیح داده شد، توسط برنامه نوشته‌شده در نرم‌افزار MATLAB بر روی ماتریس‌ها اعمال گردید. مقادیر به دست آمده برای بردار به هنجار شده ارزش نسبی معیارها (بردار W_C^N) در جدول ۱۱ و مقادیر به دست آمده برای ماتریس به هنجار شده امتیاز نسبی گزینه‌ها بر مبنای یکایک معیارها (ماتریس W_A) در جدول ۱۲ ارائه شده است.

رتبه‌بندی نهایی گزینه‌ها با ضرب‌کردن ماتریس W_A (جدول ۱۲) در بردار W_C^N (جدول ۱۱) مشخص می‌گردد که نتیجه آن به صورت به هنجار شده در جدول ۱۳ ارائه شده است. با توجه به جدول ۱۳ الگوریتم توافق کلید ECG-IJS به عنوان بهترین گزینه برگزیده شده و سپس الگوریتم OPFKA و بعد از آن PSKA قرار گرفته‌اند.

٤-٤ ارزیابی نتایج روش AHP فازی

لازم به ذکر است که بر خلاف مقایسه جامعی که در این مقاله با استفاده از روش AHP فازی انجام دادیم، در مقالات ارائه‌دهنده این الگوریتم‌ها مقایسه جامعی بین آنها انجام نشده است. به همین دلیل، مقایسه‌هایی که خود این مقالات انجام داده‌اند را نمی‌توان به عنوان عاملی برای تشخیص میزان دقت و موفقیت روش AHP فازی به کار گرفت.

اما در عین حال، الگوریتم ECG-IJS با حذف‌کردن Chaff Pointها از مدل رمزنگاری، موفق به کاهش‌دادن حجم اطلاعات و کم‌کردن حجم ارتباطات شده و در [۷] نیز همین موضوع به عنوان مهم‌ترین قابلیت این الگوریتم مورد تأکید قرار گرفته است. با توجه به اهمیت این معیارها، مشخص می‌شود که این الگوریتم باید نسبت به بقیه الگوریتم‌ها (که مبتنی بر استفاده از Chaff Pointها هستند) موفق‌تر باشد و نتایج مقایسه روش AHP فازی نیز همین مطلب را تأیید می‌کند.

۵- نتیجه‌گیری

در این مقاله با استفاده از روش تحلیل سلسله‌مراتبی فازی، به انتخاب بهترین الگوریتم توافق کلید در شبکه‌های بی‌سیم روی بدن پرداختیم. با توجه به اصول عملکردی این روش و همچنین صحت نتایجی که در مورد الگوریتم‌های توافق کلید حاصل گردید، به نظر می‌رسد که روش تحلیل سلسله‌مراتبی فازی می‌تواند به عنوان ابزار موفقی برای انجام‌دادن مقایسه‌های جامع در حوزه فنی و مهندسی مورد استفاده قرار گیرد.

مراجع

[1] B. Latre, B. Braem, I. Moerman, C. Blondia, and P. Demeester, "A survey on wireless body area networks," *Wireless. Network*, vol. 17, no. 1, pp. 1-18, Jan. 2011.

[2] L. Schwiebert, S. K. S. Gupta, and J. Weinmann, "Research challenges in wireless networks of biomedical sensors," in *Proc. of the 7th Annual Int. Conf. on Mobile Computing and Networking, MobiCom'01,* pp. 151-165, Rome, Italy, Jul. 2001.

[3] L. Eschenauer and V. D. Gligor, "A key-management scheme for distributed sensor networks," in *Proc. of the 9th ACM Conf. on Computer and Communications Security, CCS'02,* Washington DC, US, pp. 41-47, Nov. 2002.

[4] S. Cherukuri, K. K. Venkatasubramanian, and S. K. S. Gupta, "BioSec: a biometric based approach for securing communication in

wireless networks of biosensors implanted in the human body," in *Proc. of the 2003 Int. Conf. on Parallel Processing Workshops, ICPPW'03,* pp. 432-439, Kaohsiung, Taiwan, Oct. 2003.
[5] C. C. Y. Poon, Y. T. Zhang, and S. D. Bao, "A novel biometrics method to secure wireless body area sensor networks for telemedicine and m-health," *IEEE Commun. Mag.*, vol. 44, no. 4, pp. 73-81, Apr. 2006.
[6] A. Juels and M. Sudan, "A fuzzy vault scheme," *Des. Codes Cryptogr.*, vol. 38, no. 2, pp. 237-257, Feb. 2006.
[7] Z. Zhang, H. Wang, A. V. Vasilakos, and H. Fang, "ECG-cryptography and authentication in body area networks," *IEEE Trans. Inf. Technol. Biomed.*, vol. 16, no. 6, pp. 1070-1078, Nov. 2012.
[8] K. K. Venkatasubramanian, A. Banerjee, and S. K. S. Gupta, "PSKA: usable and secure key agreement scheme for body area networks," *IEEE Trans. Inf. Technol. Biomed.*, vol. 14, no. 1, pp. 60-68, Jan. 2010.
[9] C. Hu, X. Cheng, F. Zhang, D. Wu, X. Liao, and D. Chen, "OPFKA: secure and efficient ordered-physiological-feature-based key agreement for wireless body area networks," in *Proc. of the IEEE INFOCOM INFOCOM Workshops 2013,* pp. 2274-2282, Turin, Italy, 14-19 Apr. 2013.
[10] A. Juels and M. Wattenberg, "A fuzzy commitment scheme," in *Proc. of the 6th ACM Conf. on Computer and Communications Security, CCS'99,* pp. 28-36, *Singapore*, Nov. 1999.
[11] G. H. Zhang, C. C. Y. Poon, and Y. T. Zhang, "Analysis of using interpulse intervals to generate 128-bit biometric random binary sequences for securing wireless body sensor networks," *IEEE Trans. Inf. Technol. Biomed.*, vol. 16, no. 1, pp. 176-182, Jan. 2012.
[12] K. K. Venkatasubramanian, A. Banerjee, and S. K. S. Gupta, "EKG-based key agreement in body sensor networks," in *Proc. of the IEEE INFOCOM Workshops 2008,* 6 pp., Phoenix, AZ, USA, Apr. 2008.
[13] K. K. Venkatasubramanian, A. Banerjee, and S. K. S. Gupta, "Plethysmogram-based secure inter-sensor communication in body area networks," in *Proc. of the IEEE Military Communications Conf., MILCOM'08,* 7 pp., San Diego, CA, USA, Nov. 2008.
[14] F. Miao, L. Jiang, Y. Li, and Y. T. Zhang, "Biometrics based novel key distribution solution for body sensor networks," in *Proc. of the 2009 IEEE Annual Int. Conf. on Engineering in Medicine and Biology Society, EMBC'09,* pp. 2458-2461, Minneapolis, MN, USA, Sep. 2009.
[15] F. Miao, S. D. Bao, and Y. Li, "A modified fuzzy vault scheme for biometrics-based body sensor networks security," in *Proc. of the 2010 IEEE Global Telecommunications Conf., GLOBECOM'10,* 5 pp., Miami, FL, USA, Dec. 2010.
[16] C. Z. Cao, C. G. He, S. D. Bao, and Y. Li, "Improvement of fuzzy vault scheme for securing key distribution in body sensor network," in *Proc. of the 2011 IEEE Annual Int. Conf. on Engineering in Medicine and Biology Society, EMBC'11,* pp. 3563-3567, Boston, MA, USA,, Aug./Sep. 2011.
[17] J. Lu, G. Zhang, and D. Ruan, *Multi-Objective Group Decision Making: Methods, Software, and Applications with Fuzzy Set Techniques*, London, UK: Imperial College Press, 2007.
[18] L. Mikhailov and P. Tsvetinov, "Evaluation of services using a fuzzy analytic hierarchy process," *Appl. Soft Comput.*, vol. 5, no. 1, pp. 23-33, Dec. 2004.
[19] K. Asai, *Fuzzy Systems for Management*, Burke, VA, USA: IOS Press, 1995.
[20] A. Kaufmann and M. M. Gupta, *Fuzzy Mathematical Models in Engineering and Management Science*, New York, NY, USA: Elsevier Science Inc, 1988.
[21] G. J. Klir and B. Yuan, *Fuzzy Sets and Fuzzy Logic: Theory and Applications*, New Jersey, USA: Prentice Hall PTR, 1995.
[22] G. H. Zhang, C. C. Y. Poon, and Y. T. Zhang, "A review on body area networks security for healthcare," *ISRN Communications and Networking*, vol. 2011, Jan. 2011.

مرتضی ابراهیمی تحصیلات خود را در مقطع کارشناسی ریاضی محض و کارشناسی ارشد و دکتری ریاضی کاربردی به‌ترتیب در سال‌های ۱۳۷۷ و ۱۳۸۰ و ۱۳۸۸ در دانشگاه علم و صنعت ایران به پایان رسانده است و هم‌اکنون استادیار دانشکده علوم و فنون نوین دانشگاه تهران می‌باشد. زمینه‌های تحقیقاتی مورد علاقه ایشان عبارتند از: حل مسائل معکوس مبتنی بر معادلات دیفرانسیل با مشتقات جزئی در حوزه علوم شبکه، تصمیم‌گیری چند معیاره فازی، بهینه‌سازی چند هدفه و طراحی و ساخت سامانه‌های تصمیم‌یار.

سیدحمیدرضا احمدی تحصیلات خود را در مقطع کارشناسی و کارشناسی ارشد مهندسی برق (گرایش الکترونیک) و دکتری مهندسی کامپیوتر به‌ترتیب در سال‌های ۱۳۷۷ و ۱۳۸۰ و ۱۳۹۰ در دانشگاه تهران به پایان رسانده است و هم‌اکنون استادیار دانشکده علوم و فنون نوین دانشگاه تهران می‌باشد. زمینه‌های تحقیقاتی مورد علاقه ایشان عبارتند از: الگوریتم‌های رمزنگاری و سخت‌افزارهای رمز، امنیت داده و امنیت شبکه، پنهان‌نگاری در تصویر و واترمارکینگ، فشرده‌سازی انواع داده، و سیستم‌های چندرسانه‌ای.

مریم عباس‌نژاد آرا مدرک کارشناسی مهندسی فناوری اطلاعات خود را در سال ۱۳۹۰ از دانشگاه صنعتی شاهرود و مدرک کارشناسی ارشد مهندسی فناوری اطلاعات پزشکی را در سال ۱۳۹۴ از دانشگاه تهران دریافت نموده است. تحقیقات نام‌برده در دوره کارشناسی ارشد روی الگوریتم‌های تبادل کلید و احراز هویت در شبکه‌های بی‌سیم حوزه پزشکی متمرکز بوده است.