An Efficient Scheme for Cryptographic Key Agreement in a Wireless Body Sensor Network Using Biometrics

Khadijeh Iskander *
Dr. Boushra Maala **

(Received 12 / 5 / 2025. Accepted 31 / 8 / 2025)

□ ABSTRACT □

Wireless Body Sensor Networks (WBSNs). consist of small, resource-constrained sensor nodes that can be permanently or semi-permanently implanted inside the patient's body, or placed on the skin surface for specific medical purposes, sensing biometrics. The use of biometric features is one of the most effective ways to protect communications in WBSNs, rather than traditional protection schemes that consume limited network resources. Although the use of traditional biometric features has increased the level of security within protection systems, it has had several drawbacks, which has led to the development of new, more effective biometric features such as ElectroCardioGram (ECG) sensors and electroencephalography (EEG).

In this paper, we present a new security scheme to agree on the encryption key between two sensor nodes in a WBSN, based on the characteristics of both ECG and EEG signals. In this scheme. We implemented this proposed scheme, tested it, and then evaluated it against previous key management schemes, and the results showed the effectiveness of this scheme, which achieve a high level of reliability, and achieve security requirements in WBSNs.

Keywords: Wireless body sensor network(WBSN), Key management, Biometrics, ElectroCardioGram (ECG), Electroencephalography (EEG).

* **PhD Student, Department of Communication and Electronics, Faculty of Mechanical and Electrical Engineering, Latakia University (Formerly Tishreen), Lattakia, Syria.**
khadijeh.iskander@tishreen.edu.sy.
** **Associate Professor, Department of Communication and Electronics, Faculty of Mechanical and Electrical Engineering, Latakia University (Formerly Tishreen), Lattakia, Syria.**
boushra.maala@gmail.com

مخطط فعال للاتفاق على مفتاح التعمية في شبكة حساسات الجسم اللاسلكية باستخدام العلامات الحيوية

خديجة اسكندر•

د. بشرى معلا••

(تاريخ الإيداع 12 / 5 / 2025. قُبِل للنشر في 31 / 8 / 2025)

□ ملخّص □

تتكون شبكة حساسات الجسم اللاسلكية من عقد حساسة صغيرة الحجم ومحدودة الموارد قابلة للزرع بشكل دائم أو شبه دائم داخل جسم المريض، أو تتوضع على سطح الجلد لأغراض طبية محددة، تتحسس العلامات الحيوية من جسم المريض. يعدّ استخدام العلامات الحيوية من أكثر الطرائق الفعالة في القضايا الأمنية و حماية الاتصالات ضمن هذه الشبكات، بدلاً من مخططات الحماية التقليدية والتي تستهلك موارد الشبكة المحدودة. ورغم أن استخدام العلامات الحيوية التقليدية قد رفع مستوى الأمن ضمن أنظمة الحماية إلا أنه كان لها العديد من السلبيات، مما دفع التوجه إلى علامات حيوية جديدة أكثر فعالية مثل حساسات تخطيط كهربائية القلب وحساسات تخطيط كهربائية الدماغ . سنقدم في بحثنا هذا مخططا أمنياً جديداً للاتفاق على مفتاح التشفير ببين عقدتي حساس ضمن شبكة حساسات الجسم اللاسلكية، وذلك بالاعتماد على مميزات كل من إشارتي تخطيط القلب وتخطيط الدماغ. نفذنا هذا المخطط المقترح واختبرناه ومن ثم أجرينا مقارنة مع مخططات إدارة المفاتيح السابقة، فبينت النتائج فعالية هذا المخطط من ناحية استهلاك موارد الشبكة، وتحقيق مستوى وثوقية عالٍ، إضافة لتحقيق متطلبات الأمن في هذا النوع من الشبكات.

الكلمات المفتاحية: شبكة حساسات الجسم اللاسلكية WBSNs ، مخططات إدارة المفاتيح، العلامات الحيوية، إشارة تخطيط القلب ECG ، إشارة تخطيط الدماغ EEG .

•طالبة دكتوراه، قسم هندسة الاتصالات والالكترونيات، كلية الهندسة الميكانيكية والكهربائية، جامعة اللاذقية(تشرين سابقاً)، اللاذقية، سوريا khadijeh.iskander@tishreen.edu.sy

•• أستاذ مساعد، قسم هندسة الاتصالات والالكترونيات، كلية الهندسة الميكانيكية والكهربائية، جامعة اللاذقية(تشرين سابقاً)، اللاذقية، سوريا boushra.maala@gmail.com

مقدمة:

ساهم التطور في مجال الالكترونيات وتقنيات الاتصالات اللاسلكية وتصميم وحدات المعالجة والحساسات صغيرة الحجم والتي تستهلك مقدار منخفض من الطاقة في توجه الباحثين إلى تطوير نمط جديد من الشبكات يُعرف بشبكات حساسات الجسم اللاسلكية Wireless Body Sensor Networks (WBSNs). والتي تُعدّ تقنية للمراقبة المستمرة عن بعد للنشاط الفيزيولوجي والسلوكي لجسم الإنسان فهي بذلك تلعب دوراً كبيراً في تأمين الرعاية الصحية عن بعد. إذ تتألف هذه الشبكة من عقد حساسة صغيرة الحجم، ذاتية التغذية ومحدودة الموارد قابلة للزرع بشكل دائم أو شبه دائم داخل جسم المريض أو تتوضع على سطح الجلد لأغراض طبية محددة، إذ تتحسس بارامترات معينة من جسم المريض مثل تخطيط كهربائية القلب ElectroCardioGram (ECG) وتخطيط كهربائية الدماغ (EEG) ElectroEncephaloGraphy، ومراقبة الحركة، وضغط الدم، وحرارة الجسم، ونسبة السكر في الدم،....الخ [1] .

لقد أثبتت شبكات WBSN أنها أساساً هاماً في منظومة العناية الصحية، ولذلك فإن استخدامها يلحظ انتشاراً واسعاً في السنوات الأخيرة، ونظراً لحساسية البيانات المنقولة عبر الشبكة والتي تتعلق بالحالة الصحية للمريض فإن قضايا الأمن والخصوصية تُعدّ أمراً مهماً للدراسة، إذ أنّ أي تسريب أو تلاعب في سجلات المريض قد تودي بحياته، ومن الممكن استغلال هذه السجلات لأغراض أخرى. ويلخص الجدول الآتي الهجومات التي يمكن أن تتعرض لها شبكات WBSN ومتطلبات الأمن فيها[2]:

الجدول (1): الهجومات ومتطلبات الأمن في WBSN

الهجومات	متطلبات الأمن
التنصت على بيانات المريض الطبية	السرية والخصوصية (confidentiality)
العبث ببيانات المريض، إدخال بيانات مزيفة، تعديل الاتصالات	تكاملية البيانات (Integrity)
انتحال هوية المبرمج أو العقدة الحساسة أو الجهاز الخارجي المساعد	مصادقة أصل البيانات (Authentication)
هجوم حجب الخدمة	التوافرية (Availability)
إنكار الهوية	عدم التنصل (Non-repudiation)
مهاجمة بروتوكولات التوجيه	التوجيه الآمن (secure routing)

اقترحت العديد من تقنيات الحماية لضمان متطلبات الأمن في هذه الشبكات مع مراعاة محدودية موارد العقد الحساسة وقيود الشبكة، وتُعدّ دراسة إدارة المفاتيح من أهم هذه التقنيات. إذ تُعرف عملية إدارة المفاتيح بأنها مجموعة الخوارزميات والقواعد والتقنيات التي تدعم عملية تأسيس، توزيع، إلغاء مفاتيح التعمية بين الجهات المتصلة مع بعضها. تُصنّف مخططات إدارة المفاتيح في شبكات الـ WBSN إلى صنفين أساسيين، مخططات تعتمد على العلامات الحيوية، ومخططات لا تعتمد على العلامات الحيوية.

في مخططات إدارة المفاتيح المعتمدة على القيم الفيزيولوجية، تقوم عقدتا حساسات أو أكثر– بشكل مستقل– بقياس الإشارة الفيزيولوجية لنفس الجسم، ليتم بعدها معالجة هذه الإشارة لتشكيل مفتاح تشفير أو لحماية مفتاح سري مشترك.

وأثبتت الدراسات أن استخدام العلامات الحيوية في مخططات إدارة المفاتيح يجعلها أكثر فعالية من المخططات التقليدية ضمن شبكات الـ WBSN ، ويعود ذلك لكون معاملات العلامات الحيوية تعطي مستوى أمن أعلى إذ أنها تنتج مفاتيح تشفير أكثر عشوائية وتميّزاً وبالتالي أكثر أمناً، إضافة إلى أنها أقل استهلاك لذاكرة التخزين المطلوبة في العقدة ولفائض الاتصالات في الشبكة [3].

رغم أن استخدام العلامات الحيوية مثل بصمة الإصبع أو الوجه أو الصوت وخط اليد قد رفع مستوى الأمن ضمن أنظمة الحماية، ولكن تم الاعتماد في كثير من الأنظمة المتقدمة على بصمة الإصبع والقزحية والوجه معاً لزيادة السوية الأمنية لها، إلا أنها قد تكون مكشوفة للعلن وغير سرية، بمعنى أن التقاط صورة للوجه أو تسجيل صوت المستخدم أو سرقة بصمة الأصابع يُعدّ أمراً ممكناً.

كل ما سبق دفع للتوجه لعلامات حيوية جديدة لا تمتلك نقاط الضعف الموجودة في العلامات الحيوية التقليدية ونذكر منها إشارات حساسات تخطيط كهربائية القلب (ElectroCardioGram (ECG، وتخطيط كهربائية الدماغ ElectroEncephaloGraphy(EEG)، وتخطيط الصورة الضوئية PhotoPlethymoGram(PPG) .

أهمية البحث وأهدافه:

إن تطور شبكات WBSN ودورها الفعال والمهم في الرعاية الصحية والمراقبة الطبية عن بعد للمرضى والمسنين بالإضافة إلى تطبيقاتها العديدة، جعل هذا النوع من الشبكات قضية مهمة في الكثير من البلدان، ونظراً لحساسية المعلومات المرسلة عبر هذه الشبكة، والخطورة الناتجة عن اختراق هذه المعلومات والتي قد تودي بحياة الإنسان في بعض الحالات، هذا بدوره جعل تحقيق متطلبات الأمن والعمل على توفير الحماية لهذا النوع من الشبكات أمراً هاماً.

إن محدودية موارد العقد الحساسة في الشبكة فرضت قيود على تطبيق المخططات الأمنية اللازمة لتوليد المفاتيح وتوزيعها بما يحقق الحفاظ على سرية بيانات المريض، الأمر الذي دفع إلى البحث حول توفير أساليب أمنية تناسب إمكانيات العقد الحساسة وتحقق سوية أمنية عالية مع الحفاظ على زمن حياة الشبكة.

يهدف بحثنا هذا إلى تطوير مخطط أمني يعتمد على علامات حيوية متعددة (ECG , EEG) مقاسة من جسم المريض، من أجل الاتفاق على المفتاح السري بطريقة فعالة وبسوية أمنية عالية مع مراعاة محدودية موارد الشبكة والعقد الحساسة.

طرائق البحث ومواده:

حصلنا على إشارة تخطيط القلب الكهربائية من قاعدة البيانات MIT-BIH Arrhythmia المضمنة في PhysioBank التي تعدّ من أشهر قواعد البيانات المستخدمة لأغراض التصنيف ودراسة القضايا الأمنية المتعلقة بالعلامات الحيوية. تتضمن قاعدة البيانات هذه العديد من تسجيلات إشارة ECG لأشخاص من الجنسين تتراوح أعمارهم من 23 وحتى 89 سنة، مدة كل منها 30 دقيقة، وتردد أخذ العينات هو 360عينة في الثانية [4] . اعتمدت هذه الدراسة على قاعدة البيانات waveform (WFDB) وهي عبارة عن حزمة برمجية تتضمن العديد من المودولات التي تتعامل مع إشارة تخطيط القلب الكهربائية من خلال قراءتها وتحليل بارامتراتها [5].

بينما حصلنا على إشارة تخطيط الدماغ الكهربائية من قاعدة البيانات EEG Motor Movement/Imagery Dataset V1.0.0 المضمنة في PhysioBank أيضاً [6]. وبرمجت جميع خطوات المخطط المقترح هنا باستخدام لغة الـ Python الإصدار 3.10 [7].

ونفذت على جهاز حاسب ذو مواصفات مبينة في الجدول الآتي:

الجدول (2): بعض مواصفات الجهاز المستخدم في الدراسة

نظام التشغيل Operating system	المعالج Processor	نوع النظام System type	ذاكرة الوصول العشوائي RAM
Windows 10 pro	Intel(R)Core(TM)i5-2410M CPU @2.30GHz	64-bit	4GB

1- الدراسات المرجعية:

تعتمد كافة مخططات الاتفاق على المفتاح باستخدام العلامات الحيوية على فكرة الاستفادة من التشابه بين قيم العلامات الحيوية المقاسة بشكل متزامن في عدة حساسات متموضعة على نفس الجسم، مع الأخذ بالحسبان التسامح في الاختلافات الطفيفة بين تلك القيم والناتجة عن عوامل عديدة. ونستعرض فيما يأتي أهم الأبحاث في مجال تبادل المفاتيح في شبكات WBANs المعتمدة على القياسات الحيوية:

بداية في المرجع[8] : وضع المخطط PSKA لتبادل المفتاح السري بين العقد الحساسة بالاعتماد على الإشارات الفيزيولوجية (تخطيط القلب ECG وتخطيط الصورة الضوئية PPG)، اعتمدت هذه الدراسة في تخبئة المفتاح وإعادة استخراجه على خوارزمية الخزنة الضبابية، وتمت معالجة الإشارة الفيزيولوجية في المجال الترددي بدلاً من المجال الزمني، ويتميز هذا المخطط بعدم الحاجة لأي تحميل مسبق لبارامترات أو مفاتيح معينة (plug- n –play) ، ولكن يعاني هذا المخطط من فائض الاتصالات الكبير والناجم عن الطول الكبير جداً للرسالة اللازم إرسالها إلى المستقبل لتكوين المفتاح والاتفاق عليه، وذلك بسبب احتوائها على نقاط الضجيج (النقاط العلامة) المستخدمة في الخزنة الضبابية، إذ يرتبط أمان هذه الطريقة بازدياد عدد تلك النقاط.

في المرجع [9]: طور الباحثون المخطط OPFKA لتجنب السلبيات الموجودة في مخطط PSKA ، حيث وضعوا مخططاً يسمح لعقدتين بالاتفاق على مفتاح التعمية المولد من معاملات إشارة ECG الفيزيولوجية المستخرجة باستخدام تحويل فوريه السريع FFT ،حيث تم الاعتماد على الفواصل الزمنية بين القمم في إشارة ECG (IPI) ، وتمكن هذا المخطط مقارنة بمخطط PSKA من تقليل استهلاك الذاكرة والاستطاعة مع تحقيق نفس السوية الأمنية.

في المرجع [10]: يسمح المخطط ECG-IJS للحساسات بتبادل مفتاح سري مشترك منشأ بالاعتماد على إشارات ECG ويعمل بطريقة plug-n-play ، هنا حُسّن مخطط الخزنة الضبابية بالنتيجة لا داع لاستخدام النقاط العلامة لإخفاء المفتاح وهذا بدوره قلل من فائض الاتصالات وحفظ طاقة البطارية. يعتمد هذا المخطط على تشكيل كثير حدود من مميزات إشارة ECG المقاسة لدى الحساسين وإرسال فقط جزء من معاملات كثير الحدود إلى المستقبل دون تشفيرها. شعاع المميزات مستخرج باستخدام تحويل فوريه السريع FFT من قمم إشارة ECG المقاسة لمدة 4 ثواني. ولكن كانت سلبية هذه الدراسة بأنه في بعض الأحيان لا تكون مجموعة المميزات المستخلصة متشابهة بما يكفي بين الطرفين للاتفاق على المفتاح بهذه الطريقة.

في المرجع [11]: وضع مخطط MBPSKA للاتفاق على المفتاح يعتمد على المميزات المستخلصة من العلامات الحيوية (تخطيط القلب ECG وبصمة الإصبع)، استخدمت خوارزميات الخزنة الضبابية والالتزام الضبابي لإخفاء

المفتاح والاتفاق عليه، يتم هنا تحميل مسبق لمميزات علامة بصمة الإصبع. استخلصت قيم IPI من إشارة ECG حيث أُخذت 4 نبضات متتالية ومن كل IPI أُخذت 4 بتات الأقل أهمية لتشكيل 16 بت. طالما أن IPI المستخلصة من الحساس المرسل مشابهة بدرجة كافية لـ IPI المستخلصة من الحساس المستقبل، فإن عملية تبادل المفاتيح المفروض أنها تنجح ولكن عملياً الخانات الأدنى من IPI تختلف عند قياسها في حساسين مختلفين بدرجة تجعل استعادة المفتاح غير عملي، كما أن فائض الاتصالات كبير بسبب النقاط العلامة المستخدمة في الخزنة الضبابية.

في المرجع [12]: اقترح بروتوكول من أجل توليد وتوزيع مفاتيح التعمية بالاعتماد على إشارة ECG ، ولكن هذا البروتوكول يعتبر وجود طرف ثالث موثوق ينظم عملية تبادل الرسائل ما بين المرسل والمستقبل. حقق هذا المخطط العديد من المزايا ولكن يجب أن تمتلك العقد الثلاثة إشارة ECG المسجلة بشكل متزامن وهذا بدوره يؤدي إلى زيادة استهلاك الموارد. إضافة إلى عدد كبير من المراحل وعدد كبير من عمليات التشفير وتصحيح الخطأ.

في المرجع [13]: وضع مخطط للاتفاق على المفتاح يقلل من استهلاك موارد الشبكة بالاعتماد على استخراج المميزات باستخدام تحويل FFT المعدل من إشارة ECG المقاسة لفترة لا تقل عن 4 ثواني. يعتمد هذا المخطط على تبادل بارامترات معينة بين المرسل والمستقبل من أجل الاتفاق على المفتاح وذلك عند دورة التنفيذ الأولى، بينما تُختصر هذه البيانات المتبادلة في دورات التنفيذ الأخرى وهذا بدوره يقلل من فائض الاتصالات، تُحدَد مرحلة التنفيذ بالاعتماد على بارامتر P والذي يعتمد بشكل أساسي على مستوى طاقة الحساس ومعدل تردد الاتصال ما بين المرسل والمستقبل.

من خلال الدراسات السابقة نستنتج أنه لا يزال هناك حاجة ومجال لدراسة وضع مخططات أمنية لتبادل مفاتيح التعمية في شبكات WBSNs تحقق الشروط الأمنية اللازمة بما يتناسب مع القيود التي تفرضها موارد الشبكة المحدودة. كما أن تطور تقنيات الحساسات اللاسلكية أتاح إمكانية الاستفادة من مميزات إشارات فيزيولوجية أخرى غير مدروسة سابقاً لاستخدامها في مخططات إدارة المفاتيح.

2- الجزء العملي:

نقدم في هذا الجزء المخطط المقترح من أجل الاتفاق على مفتاح التعمية المشترك بين عقدتي حساس في شبكة WBSN، وذلك بالاعتماد على العلامات الحيوية ECG وEEG.

2-1- الإعدادات الأولية والفرضيات:

- يُسجل حساس تخطيط الدماغ النشاط الكهربائي لدماغ الشخص، ومن ثم تُجرى المعالجة المناسبة لتوليد سلسلة بتات عشوائية بطول 512 بت، وفق الآلية المتبعة في بحثنا السابق، حيث اعتمدنا على إشارات تخيل الحركة للدماغ وبعد إجراء المعالجة الأولية لهذه الإشارات استخلصنا المميزات الزمنية والترددية المرغوبة من أجل تشكيل سلاسل ثنائية بطول 512 بت [14]، ومن ثم يُخزن هذه السلسلة في كل من الحساسين المرسل والمستقبل مسبقاً.
- نفرض أن عقدتي الحساس المرسل والمستقبل تتوضعان على نفس الجسم وتقيسان نفس العلامة الحيوية ECG بشكل متزامن عند بدء عملية الاتفاق على المفتاح.
- عندما يريد الحساس رقم (1) الاتصال مع الحساس رقم (2) لإرسال بيانات ما أو بالعكس، فإنهما بداية يتفقان على مفتاح التشفير المتناظر والسري فيما بينهما لتأمين هذا الاتصال.

2-2- المخطط المقترح للاتفاق على المفتاح:

1- يولد المرسل أرقام صحيحة بشكل عشوائي من خلال تابع برمجي Random بحيث يكون عددها 16 عدد صحيح ضمن المجال (0 وحتى 511)، وهذه الأرقام هي بمثابة فهارس ستستخدم لاحقاً لاستخراج البيانات من إشارة تخطيط الدماغ المخزنة EEG. ومن ثم تُخزن هذه الأرقام الصحيحة المولدة في ذاكرة الحساس المرسل.

2- يقيس الحساس المرسل إشارة تخطيط القلب ECG، ويعالجها لاستخراج المميزات، ومنها توليد سلسلة بتات عشوائية BS بطول 381 بت وفق الآلية المقترحة في المرجع [15] والمبينة في الخوارزمية (1).

3- تغليف الأرقام الصحيحة لحمايتها بالاعتماد على مميزات العلامة الحيوية ECG المقاسة من قبل هذا الحساس، وذلك بتطبيق خوارزمية الالتزام الضبابي (fuzzy commitment) والتي تتسامح مع الاختلاف الطفيف ما بين إشارتي ECG مقاستين بالتزامن في نفس الجسم. وفيما يلي خطوات خوارزمية **الالتزام الضبابي:**

- تطبيق ترميز تصحيح الخطأ Reed Solomon Error correction على سلسلة الأعداد الصحيحة بعد تحويلها إلى سلسلة بتات string1 ومنه الحصول على السلسة المرمزة string2 .

srtring2 = encoding (string1)

- إجراء عملية xor ما بين سلسلة البتات BS المستخلصة من مميزات إشارة ECG و السلسلة المرمزة string2 .

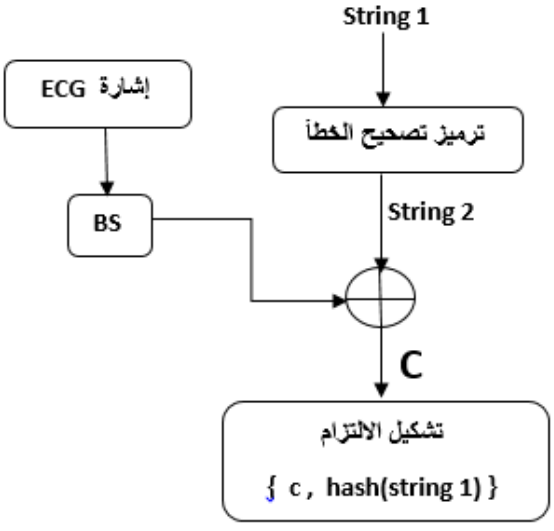
c = BS xor string2

- تطبيق تابع وحيد الاتجاه SHA-256 على السلسة string1

a= hash(string1)

- تشكيل الالتزام {c , a}

ويبين الشكل الآتي مخطط تطبيق الالتزام :



الشكل (1): تطبيق الالتزام الضبابي

4- يرسل المرسل إلى المستقبل رسالته والتي تتضمن: (معرف المرسل، معرف المستقبل، طابع زمني، الالتزام {c,a})

5- يستقبل الحساس المستقبل الرسالة الواصلة إليه من الحساس المرسل ويستخرج منها الالتزام {c,a} .

6- يطبق المستقبل عملية **فك الالتزام الضبابي** كما يأتي:

- يعتمد المستقبل على سلسلة البتات المستخلصة من مميزات إشارة تخطيط القلب الخاص به BS' (والتي قاسها بالتزامن مع الحساس المرسل) وذلك لاستخلاص السلسة string2 ' من خلال إجراء عملية xor كما يأتي:

$$String2' = c \text{ xor } BS'$$

- تطبيق فك ترميز تصحيح الخطأ على السلسلة String2 ' ومنها نحصل على string1'

$$string1' = decoding\ (\ string2')$$

- تطبيق تابع وحيد الاتجاه SHA-256 على السلسة string1'

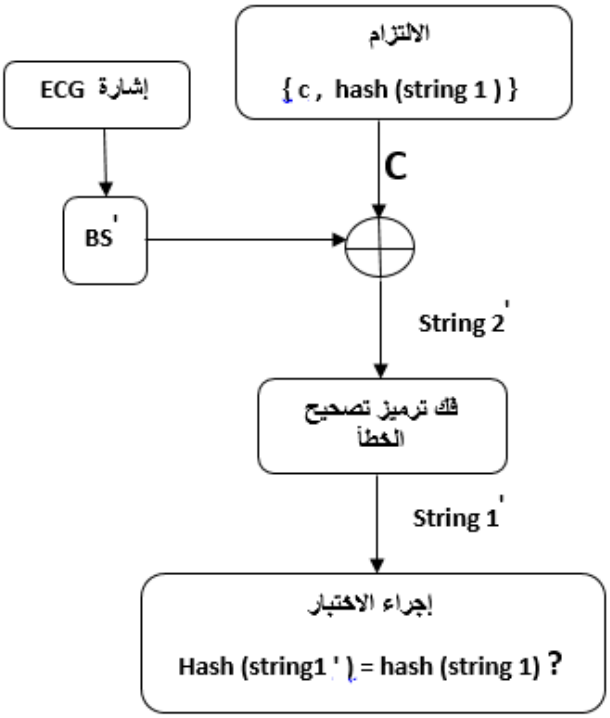
$$a' = hash(string1')$$

ويبين الشكل (2) خطوات فك الالتزام الضبابي.

7- إجراء مقارنة ما بين a و' a، إذا لم تكونا متطابقتين يعني هناك خطأ ما قد حصل، فيرسل الحساس المستقبل رسالة خطأ error إلى المرسل، ليعيد عملية الاتفاق من جديد، أم إذا كانتا متطابقتين نكون قد حصلنا على السلسلة string1 والتي تمثل السلسلة الثنائية للأعداد الصحيحة.

8- استخراج الأعداد الصحيحة والتي تمثل مواقع 16 بت ضمن إشارة EEG المخزنة في ذاكرة الحساس.

9- نستخلص من إشارة EEG الخانات الثنائية الموجودة في (الخانات الأربعة التي بعدها والخانات الأربعة التي قبلها) فيتشكل لدينا سلسلة بتات بطول 128بت(16*8=128) والتي تشكل المفتاح السري المشترك بين الحساسين.

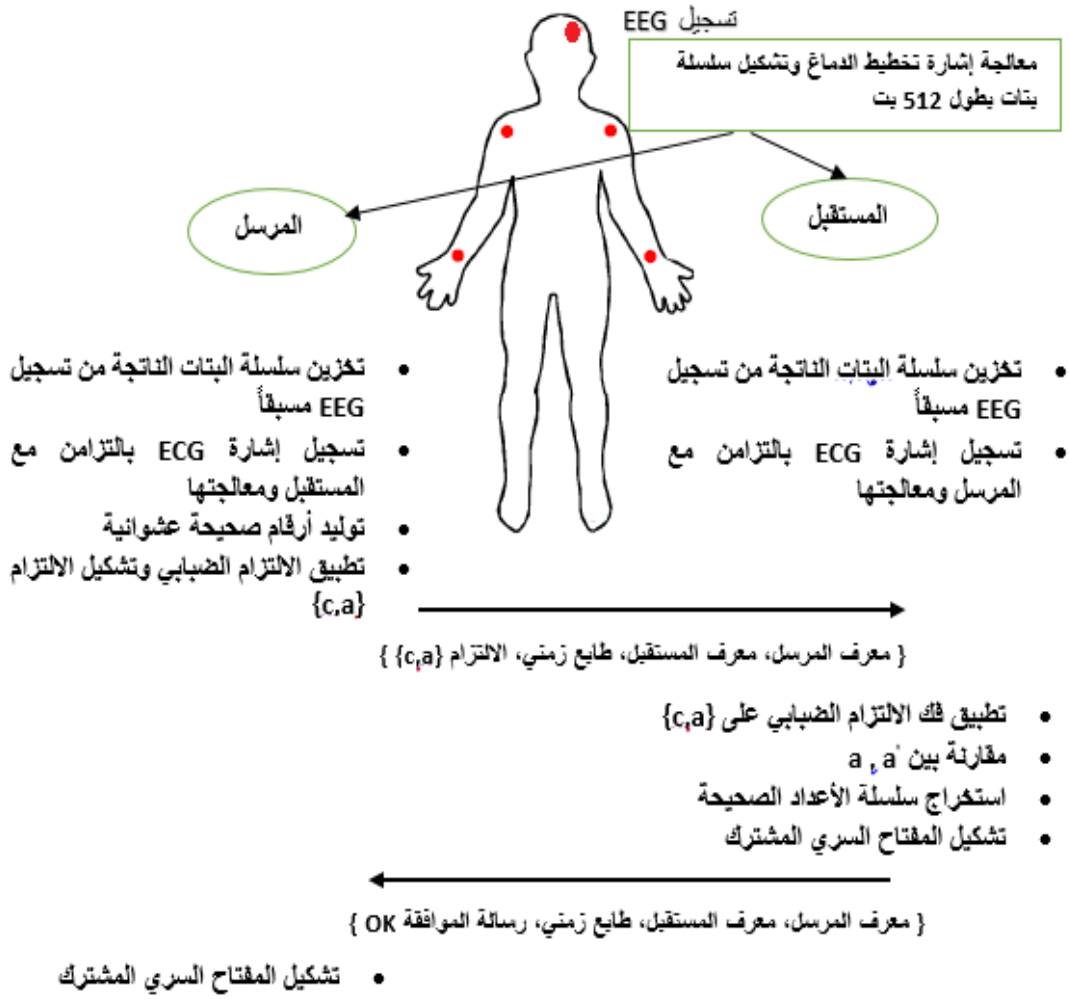


الشكل (2): خطوات فك الالتزام الضبابي

10- يرسل المستقبل رسالة التحقق للمرسل (OK) لإعلامه بتشكيل المفتاح بنجاح.

11- بعد وصول رسالة التحقق من المستقبل يشكل المرسل المفتاح ذاته وبنفس الآلية ، ليكون كل من المرسل والمستقبل فيما بعد قادرين على تشفير وفك تشفير اتصالاتهم من خلال هذا المفتاح المتناظر.

ويبين الشكل الآتي المخطط المقترح:



الشكل (3): مخطط الاتفاق على المفتاح المقترح

ونورد في الشكل الآتي أحد الأمثلة عن التطبيق العملي للمخطط المقترح:

```
=== SENDER SIDE ===
[Sender] 1) Secret key integers (0..511): [502, 32, 345, 225, 216, 21, 145, 272, 45, 269, 303, 136, 143, 290, 432, 398]
[Sender] 2) Secret key bitstring length: 144

[Sender] (Extra) EEG-based partial key: 011101100101011000010100011101000000110001110100010111100000110010111010000000010110000101110000010101111000011
11101011100001100
[Sender] (Extra) Length of EEG-based partial key: 128
[Sender] 2.1) Converted key into bytes, length: 18
[Sender] 3) Reed-Solomon encoding done. Encoded bytes length: 38
[Sender] 4) Encoded key bitstring length: 304
[Sender] 5) XOR done. c length: 304
[Sender] 6) Computed SHA-256 hash of the original key: f86d2f84973584942450cd552a3853dd12feeb312213d966fb5cbd3669cbe1c2

=== RECEIVER SIDE ===
[Receiver] 2) XOR done. Encoded key bitstring length: 304
[Receiver] 2.2) Encoded key bytes length: 38
[Receiver] 3) Reed-Solomon decode successful.
[Receiver] 4) Recovered key bitstring length (with possible padding): 144
[Receiver] 5) Computed hash of recovered key: f86d2f84973584942450cd552a3853dd12feeb312213d966fb5cbd3669cbe1c2
[Receiver] 5) Hash matches! Key is correct.
[Receiver] Key recovered successfully!
[Receiver] Recovered key (integers): [502, 32, 345, 225, 216, 21, 145, 272, 45, 269, 303, 136, 143, 290, 432, 398]
[Receiver] (Extra) EEG-based partial key: 011101100101011000010100011101000000110001110100010111100000110010111010000000010110000101110000010101111000
1111101011100001100
[Receiver] (Extra) Length of EEG-based partial key: 128
```

الشكل (4): مثال عن التطبيق العملي لمخطط الاتفاق على المفتاح

الخوارزمية (1): استخراج مميزات ECG

```
**Read ECG data:**
    Read specific channel from file using a library (wfdb)
**Detect QRS peaks:**
   Use a QRS detection algorithm (XQRS)
**Calculate R-R feature:**
   Compute average distance between QRS peaks
**Extract segments around QRS peaks:**
   Define segment length based on average R-R
   **FOR EACH** QRS peak:
       Extract segment around peak
 **Extract individual P, Q, R, S, T peaks:**
    **FOR EACH** segment:
       Find maximum value (R peak)
       Find minimum value after half of R (Q peak)
       Find maximum value before Q (P peak, handle edge cases)
       Find minimum value after R (S peak)
       Find maximum value after S (T peak)
 **Calculate feature values:**
    Calculate P-Q, P-R, Q-R, R-S, R-T, S-T features
```

2-3- تحديث المفتاح:

يمكن تحديث مفتاح التشفير المشترك المتفق عليه وفق المخطط الذي اقترحناه من خلال الآليتين الآتيتين:

1- بشكل دوري من خلال تغيير إشارة EEG من خلال تغيير الحركة التي يتخيلها الشخص أثناء تسجيل النشاط الكهربائي لدماغه.

2- من خلال إعادة توليد أرقام صحيحة عشوائية مختلفة.

النتائج والمناقشة:

تمكنا من خلال المخطط المقترح في هذا البحث من التوصل إلى اتفاق عقدتي الحساس على مفتاح سري مشترك بينهما، وسنورد فيما يأتي تقييم نتائج هذا المخطط المقترح:

أولاً: تقييم الموثوقية:

لكي نحكم على نجاح عملية تبادل المفاتيح، ونتأكد فيما إذا كان الحساسان شرعيين ومتموضعين على نفس الجسم سوف نعتمد على بارامترين وهما FAR (False Acceptance Rate) وهو معدل القبول الخاطئ، أي ما هو احتمال تشكيل مفتاح سري مشترك مع عقدة غير شرعية واعتبارها عقدة شرعية؟

FRR (False Rejection Rate) وهو معدل الرفض الخاطئ، يعني ما هو احتمال رفض تشكيل مفتاح سري مشترك مع عقدة شرعية واعتبارها عقدة غير شرعية؟.

من أجل قياس FAR أجرينا 120 تجربة وفي كل مرة نأخذ تسجيل تخطيط القلب من جسمين مختلفين (أي الحساسين متموضعين على جسمين مختلفين) وفي كل مرة يفشل المخطط في تشكيل مفتاح سري مشترك بين هذين الحساسين ومنه نستنتج أن FAR=0%

من أجل قياس FRR : طبقنا عدة تجارب وفي كل مرة نغير البارامتر rs parity في ترميز reed Solomon والذي يعبر عن بتات فحص الإنجابية، إذ أجرينا 120 تجربة من أجل سلاسل مولدة من نفس الجسم فكان لدينا:

من أجل rs parity=10 تكون النسبة المئوية للتجارب التي رفضت تشكيل المفتاح FRR= 4.1 % ، ومن أجل rs parity=15 يكون لدينا FRR= 1.6 %، ومن أجل rs parity=20 يكون لدينا FRR= 0.8 %.

نلاحظ من النتائج السابقة أنه كلما زادت قيمة بارامتر الإنجابية في ترميز reed Solomon أي زيادة عدد بتات فحص الإنجابية فإن هذا الترميز يكون قادراً على تصحيح عدداً أكبر من الأخطاء، وبالتالي التسامح مع عدد أكبر من الاختلافات ما بين السلسلتين ومنه يكون احتمال الرفض الخاطئ(FRR) أصغر.

ثانياً: تقييم الأمن:

يحقق المخطط المقترح في هذه الدراسة متطلبات الأمن الهامة في شبكات WBSNs وهي:

1- **سرية البيانات:** حُقّق هذا المتطلب من خلال الآتي:

- تشفير البيانات بين المرسل والمستقبل من خلال مفتاح سري مشترك متفق عليه بطريقة آمنة وفعالة باستخدام العلامات الحيوية ECG و EEG.

- المفتاح المشترك هو بيانات من إشارة EEG استخلصت من خلال أرقام صحيحة محمية بمميزات إشارة ECG والتي تدل على مواقع هذه البيانات.

فعلى فرض أنه لو تمكن المهاجم من الحصول على إشارة EEG – على الرغم من صعوبة هذا الأمر– إلا أنه لن يستطيع معرفة البيانات المأخوذة منها والتي تشكل المفتاح.

وعلى فرض تمكن المهاجم من الحصول على سلسلة الأرقام الصحيحة المحمية بمميزات إشارة ECG وفق خوارزمية الالتزام الضبابي فلن يستطيع فك الالتزام واستخلاص هذه الأرقام إلا إذا امتلك نفس إشارة ECG وهذا الأمر غير ممكن كما ذكرنا سابقاً.

- الأرقام الصحيحة عشوائية ولا يمكن التنبؤ بها.

2- **المصادقة:** وتعني التحقق من هوية العقدة المصدر التي أرسلت الرسالة ومنع عقدة مزيفة من انتحال هوية عقدة شرعية. حُقّق هذا المتطلب من خلال اعتمادنا على إشارة ECG في تشكيل الالتزام لحماية الأرقام الصحيحة ولن يتمكن من فك هذا الالتزام إلا إشارة ECG المقاسة بالتزامن معها ضمن نفس الجسم والتي تكون مميزاتها مطابقة لها أو قريبة منها بشكل كاف.

3- **تكاملية المعطيات:** تعني التأكد من عدم تعديل البيانات المرسلة، وحقق هذا المتطلب من خلال استخدام تابع hash، إذ أن أي تعديل أو تغيير في البيانات أثناء إرسالها لن يعطينا تابع الـ hash نفس النتيجة المطلوبة.

4- **تحديث المفتاح:** يضمن الأمن المستقبلي والأمن الماضي، إن كل مفتاح جلسة مشترك بين عقدتين يُولد بشكل مستقل، ويُحدث هذا المفتاح بشكل دوري عند كل بداية جلسة، فحتى لو تمكن المهاجم من سرقة المفتاح لجلسة اتصال سابقة فلن يتمكن من فك تشفير رسائل الجلسة الحالية من خلاله، وحتى لو تمكن المهاجم من معرفة مفتاح الجلسة الحالية فلن يتمكن من فك تشفير رسالة في جلسة اتصال سابقة.

أيضاً المفاتيح محمية من خلال الاختلاف الزمني لمميزات إشارة ECG فحتى لو عرف المهاجم مميزات ECG القديمة فلن يستطيع معرفة المفاتيح المحمية بمميزات ECG الحالية.

5- استخدام الطابع الزمني (زمن حياة) يمنع من هجوم إعادة الإرسال.

ثالثاً: تقييم الأداء:

- **فائض الاتصالات:**

تتضمن الرسائل المتبادلة لإنجاز المخطط المقترح (معرف المرسل، معرف المستقبل، طابع زمني، الالتزام {c, a})، إضافة إلى رسالة الاتفاق (معرف المرسل، معرف المستقبل، طابع زمني، OK).

(1 بايت لكل من معرف المرسل ومعرف المستقبل، 1 بايت للطابع الزمني، a=32 byte خرج تابع الهاش المستخدم، c= 48 byte ناتج عملية XOR، 2 بايت رسالة الاتفاق OK)، وبالنتيجة يكون لدينا حجم البيانات المتبادلة:

1+1+1+32+48+1+1+1+2= 88 بايت

- **استهلاك الطاقة:**

تبين معنا من خلال الدراسات السابقة أن مجمل الطاقة المستهلكة هي عبارة عن محصلة الطاقة اللازمة للإرسال والطاقة اللازمة للاستقبال والطاقة اللازمة لعمليات المعالجة والتي ترتبط بالتعقيد الحسابي لهذه العمليات. إذ إن إرسال بايت واحد من البيانات يتطلب 59.2 ميكرو جول، واستقباله يتطلب 28.6 ميكرو جول [16] .

بالنسبة للمخطط الأمني المقترح في دراستنا هذه تُهمل طاقة عمليات المعالجة نظراً لانخفاض التعقيد الحسابي (إذ استخدمنا في بحثنا عمليات بسيطة مثل xor ذات التعقيد الحسابي O (1)، أما بالنسبة لترميز تصحيح الخطأ فاستخدمنا في بحثنا الترميز reed Solomon ذو التعقيد الحسابي المنخفض ($O(n^2)$). أما بالنسبة للطاقة المستهلكة

في عملية تبادل الرسائل فهي الطاقة اللازمة لإرسال واستقبال (معرف المرسل، معرف المستقبل، طابع زمني، الالتزام {c, a})، إضافة إلى الطاقة اللازمة لإرسال واستقبال رسالة الاتفاق (معرف المرسل، معرف المستقبل، طابع زمني، OK).

نحتاج 1 بايت لكل من معرف المرسل والمستقبل، و1 بايت للطابع الزمني، و2 بايت لرسالة الموافقة OK، أما بالنسبة للالتزام {c, a} فنحتاج لـ (637=256+381) بت أي 80 بايت، وبالنتيجة يكون لدينا الطاقة الكلية المستهلكة هي: 7.5 mJ =(59.2+28.6) *88 =(59.2+28.6)*(1+1+1+80+1+1+1+2)

- **ذاكرة التخزين المطلوبة:**

بداية نحتاج لتخزين سلسلة البتات المستخلصة من إشارة تخطيط الدماغ EEG وحجمها 512 بت.

وتخزين سلسلة البتات المستخلصة من إشارة ECG وحجمها 381 بت. وتخزين سلسلة الأعداد الصحيحة المولدة وحجمها 144 بت (كل عدد صحيح تم تمثيله ب 9 خانات ثنائية وهو العدد اللازم لتمثيل العدد 512 (باعتبار أن مجال الأرقام الصحيحة من 0 وحتى 512) فأصبح لدينا 16*9=144 بت). وبالنتيجة نكون بحاجة لتخزين حوالي 1037 بت أي ما يعادل 130 بايت تقريباً، وبالتأكيد نحن بحاجة إلى حجم إضافي لإنجاز عمليات المعالجة.

- **زمن التنفيذ:**

عند تنفيذ المخطط المقترح للاتفاق على المفتاح على جهاز الحاسوب الموصوف سابقاً وجدنا أن زمن تنفيذ عمليات المعالجة صغير جداً ويُهمل أمام الزمن اللازم لتسجيل إشارة ECG للحصول على ثلاث نبضات على الأقل في التسجيل المحصل والتي تستغرق وسطياً 3–5 ثواني.

يبين الجدولين الآتيين قيم نتائج كل من المخطط المقترح في بحثنا هذا والدراسات المرجعية السابقة.

الجدول (3) : قيم بارامترات الموثوقية الناتجة في المخطط المقترح في دراستنا والدراسات المرجعية:

الدراسة	FAR	FRR
PSKA [8]	0.4701 %	0.2139 %
OPFKA [9]	0.4271 %	0.1250 %
ECG-IJS [10]	0.08 %	0.01 %
MBPSKA [11]	0.28 %	0.12 %
[12]	0 %	0 %
[13]	0.0556 %	0.2044 %
المخطط المقترح	0 %	0.8 % من أجل rs=20

الجدول (4): نتائج تقييم الأداء لكل من المخطط المقترح في دراستنا والدراسات المرجعية:

الدراسة	فائض الاتصالات (byte)	استهلاك الطاقة (mJ)	ذاكرة التخزين (byte)
PSKA [8]	13516.8	1189.688	20362
OPFKA [9]	2560	228.367	3863
[13]	258	11.274	311
المخطط المقترح	88	7.5	130

الاستنتاجات والتوصيات:

تمكنا في بحثنا هذا من تقديم مخطط جديد للاتفاق على مفتاح التعمية بين عقدتين في شبكة WBSN وذلك بالاعتماد على مميزات القياسات الحيوية لكل من إشارتي تخطيط القلب وتخطيط الدماغ، وبعد تنفيذ هذا المخطط واختباره توصلنا إلى القيم التي عرضناها في الفقرة السابقة، وبناءً عليها نستنتج ما يلي:

1- اعتمدنا في بحثنا على علامات حيوية غير تقليدية، وعالجناها بطريقة فعالة لاستخلاص المميزات الفريدة من أجل الاستفادة منها في عملية الاتفاق على المفتاح.

2- اعتمدنا في بحثنا على خوارزمية الالتزام الضبابي والتي تتسامح مع الاختلافات الطفيفة بين قياسات العلامات الحيوية لنفس الجسم.

3- نلاحظ من الجدول (3) أن المخطط المقترح يحقق النسبة المثالية للبارامتر FAR، ولكن تبقى نسبة البارامتر FRR مرتفعة مقارنة بالدراسات السابقة، فكلما انخفض بارامتر ترميز تصحيح الخطأ rs parity زادت معه نسبة FRR. وعلى الرغم من ذلك فإن عدم قبول عقدة شرعية في بعض الحالات أي (FRR>0) لا يشكل نفس الخطورة والأثر السلبي عند قبول عقدة غير شرعية وإنما يؤدي حدوث ذلك إلى إعادة عملية تبادل المفتاح مرة ثانية. لذلك نستطيع القول أن هذا المخطط يحقق مستوى وثوقية عالٍ.

4- يتميز هذا المخطط ببساطة عمليات المعالجة وانخفاض التعقيد الحسابي، فكما نلاحظ في الجدول (4) بأن هذا المخطط أكثر فعالية من المخططات السابقة من ناحية الأداء (فائض الاتصالات، ذاكرة التخزين، واستهلاك الاستطاعة)، وهذا بدوره يحفظ موارد الشبكة المحدودة.

5- فعالية هذا المخطط من ناحية الزمن اللازم للاتفاق على المفتاح.

6- حقق هذا المخطط المتطلبات الأمنية في شبكات WBSNs، كما أتاح إمكانية تحديث المفتاح.

مما سبق نستنتج بأنه تمكنا في هذا البحث من تقديم مخطط أمني فعال للاتفاق على مفتاح التعمية يحقق المتطلبات الأمنية اللازمة، ومناسب للتطبيق في شبكات حساسات الجسم اللاسلكية WBSNs. نقترح في المستقبل إمكانية تطوير هذا المخطط من خلال الاستفادة من خوارزميات الذكاء الصنعي بغية تحقيق نسبة موثوقية 100%. كما نسعى لزيادة طول مفتاح التعمية المتفق عليه ليكون بطول أكبر من 128 بت، ويكون مناسب للتطبيق مع خوارزميات التعمية الشهيرة.

References:

[1] M. Yaghoubi , K. Ahmed, and Y. Miao, "Wireless Body Area Network (WBAN): A Survey on Architecture, Technologies, Energy Consumption, and Security Challenges". Intelligent Technology Innovation Lab (ITIL), Victoria University, Ballarat Road, Footscray, Melbourne, VIC 3011, Australia, Vol.11, Issue 4, 2022.

[2] L. Zhong , S. He; J. Lin, J. Wu, X. Li, Y. Pang, and Z. Li, "Technological Requirements and Challenges in Wireless Body Area Networks for Health Monitoring: A Comprehensive Survey". Sensors, Vol.22, Issue 9, 2022.

[3] P. Kaur, N. Kumar, and M. Singh, "Biometric cryptosystem: a comprehensive survey". Multimed Tools Appl, Vol.82, PP.16635-16690, 2023.

[4] MIT-BIH Arrhythmia Database. https://physionet.org/content/mitdb/1.0.0/. Last visit at November 2024.

[5] https://wfdb.readthedocs.io/en/latest/index.html . Last visit at November 2024.

[6] EEG Motor Movement/Imagery Dataset. https://physionet.org/content/eegmmidb/1.0.0/. Last visit at November 2024.
[7] https://www.python.org/downloads/release/python-31011/. Last visit at January 2025.
[8] K. Venkatasubramanian , A. Banerjee, and S. Gupta, PSKA: "Usable and Secure Key Agreement Scheme for Body Area Networks", IEEE transactions on information technology in biomedicine, 2009.
[9] CH. 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", IEEE INFOCOM, pp.2274-2282, 2013.
[10] Z. Zhang, H. Wang, A. Vasilakos, and H. Fang, "ECG-Cryptography and Authentication in Body Area Networks", IEEE transactions on information technology in biomedicine, Vol. 16, No. 6, pp. 1070-1078, 2012.
[11] M. Reshan, CH. Hu, J. Yu, and H. Liu, "MBPSKA: Multi-Biometric and Physiological Signal-Based Key Agreement for Body Area Networks", IEEE, Vol.7, pp.78484-78502, 2019.
[12] A. Sammoud, M. Chalou, O. Hamdi, N. Montavont, and A. Bouallegue, "A new biometrics-based key establishment protocol in WBAN: energy efficiency and security robustness analysis", computers & security, Vol. 96, 2020.
[13] Y. AL-saeed, E. Eldaydamony, A. Atwan, M. Elmogy, and O. Ouda," Efficient Key Agreement Algorithm for Wireless Body Area Networks Using Reusable ECG-Based Features", Electronics, Vol. 10, 2021.
[14] B. Maala, and KH. Iskander, "Generating random number sequences using ElectroEncephaloGraphy (EEG) signals", Lattakia University, Journal engineering science series (in Arabic), Vol.47, No. 2, 2025.
[15] B. Maala, and KH. Iskander," Generation secured cryptography keys in Wireless Body Sensor Networks using electrocardiogram (ECG) signals", Lattakia University, Journal engineering science series (in Arabic), Vol.46, No. 5, 2024.
[16] A. Wander, N. Gura, H. Eberle, V. Gupta, and S. Shantz , "Energy analysis of public-key cryptography for wireless sensor networks", IEEE PerCom, pp. 324–328, 2005.