مخطط جديد لتبادل المفاتيح السرية في شبكة الجسم اللاسلكية بالاعتماد على القياسات الحيوية

م. كريستين زينية [1]
د.م. محمد مازن المحايري [2]
د.م. مفيد حداد[3]

الملخص

شبكة الجسم اللاسلكية (Wireless Body Area Network WBAN) هي شبكة مكونة من حساسات لاسلكية تقوم بقياس ونقل البيانات الحيوية لجسم الإنسان، بهدف تقديم الرعاية الصحية. تعتبر سرية وسلامة المعلومات الصحية في WBAN ذات أهمية بالغة نظراً لما يمكن أن يكون للهجمات الأمنية من أثرٍ سلبي على حياة المريض. ويعتبر تبادل المفاتيح السرية من أهم القضايا الواجب تحقيقها بهدف حماية شبكات WBAN. في هذا البحث قمنا بتطوير مخطط جديد لتوليد وتبادل المفاتيح السرية بين حساسات WBAN بالاعتماد على خصائص القيم الحيوية المقاسة، وبالتحديد الخصائص الزمنية والترددية لإشارة التخطيط الكهربائي للقلب (Electrocardiogram ECG). استطعنا التوصل إلى مخطط يتمتع بالعديد من المزايا وهي: بساطة عمليات المعالجة، ديناميكية المفتاح السري المشترك أي إمكانية تغييره مع الزمن، العمل وفق طريقة Plug-n-Play (أي عدم الحاجة إلى التوزيع المسبق للمفاتيح)، تحقيق أمان شبكة WBAN في فترة إقلاعها، قابلية التحقق من وثوقية كافة الحساسات المتصلة مع بعضها البعض، التسامح مع ضعف التزامن بين الحساسات، وتجاوز المشاكل الناتجة عن الاختلافات الطفيفة للإشارة المقاسة من خلال عدة حساسات ضمن نفس الشبكة. قمنا ببناء هذا المخطط واختباره وتبيان ميزاته مقارنةً بالمخططات المقترحة في الدراسات السابقة.

الكلمات المفتاحية: شبكة الجسم اللاسلكية (WBAN)، مخطط تبادل المفاتيح السرية، المفتاح البيومتري، مخطط كهربائية القلب (ECG)، الوثوقية.

[1] طالبة دكتوراه وعضو هيئة فنية في قسم هندسة الحواسيب والأتمتة، كلية الهندسة الميكانيكية والكهربائية، جامعة دمشق.
[2] أستاذ مساعد في قسم هندسة الحواسيب والأتمتة، كلية الهندسة الميكانيكية والكهربائية، جامعة دمشق.
[3] مدرس في قسم هندسة الحواسيب والأتمتة، كلية الهندسة الميكانيكية والكهربائية، جامعة دمشق.

A New Biometric Based Secret Key Exchange Scheme for Wireless Body Area Networks

Eng. Christine Zenieh[(1)]
Dr.Eng. Mohamed Mazen Al-Mahairi[(2)]
Dr.Eng. Moufid Haddad[(3)]

Abstract

A Wireless Body Area Network (WBAN) is a wireless network of health monitoring sensors, designed to deliver healthcare. The confidentiality and integrity of the health information in WBAN is particularly important because of the negative effect of security attacks on the patient's life. Secret key exchange is one of the most important issues in WBAN security. In this paper, we propose a new secret key exchange scheme for the aim of generating and distributing secret keys between WBAN sensors. Our scheme depends on biomedical features for generating and distributing the secret keys. We specifically use the electrocardiogram signal features in the time domain and the frequency domain. Our proposed scheme has several advantages such as: simplicity of processing operations, ability of generating time variant secret key, operating through plug-n-play manner (no previous key distribution is needed), ensuring the security of WBAN in the startup time, ability to authenticate the communicated sensors, tolerance with poor synchronization between sensors, and tolerance with slight dissimilarity of signal measured by different sensors in the same network. We built our scheme, tested it, and demonstrated its advantages over the proposed scheme in previous studies.

Key words: Wireless Body Area Network (WBAN), Secret keys exchange scheme, Biometric key, Electrocardiogram (ECG), Authentication.

(1) PhD student and member of the technician assembly in Computer and Automation Engineering Department, Faculty of Mechanical and Electrical Engineering, Damascus University.

(2) Associate Professor, Computer and Automation Engineering Department, Faculty of Mechanical and Electrical Engineering, Damascus University.

(3) Lecturer, Computer and Automation Engineering Department, Faculty of Mechanical and Electrical Engineering, Damascus University.

1- مقدمة

شبكة الجسم اللاسلكية WBAN هي عبارة عن مجموعة من الحساسات الموضوعة على جسم الإنسان المتصلة مع بعضها البعض بهدف مراقبة الحالة الصحية للمرضى عن بعد [1]. تتكون من أنواع مختلفة من الحساسات التي يمكن وضعها على سطح جسم الإنسان أو حوله أو داخله. تُستخدم لقياس التغيرات في العلامات الحيوية للإنسان مثل مراقبة درجة حرارة الجسم، ضغط الدم، قياس معدل أكسجة الدم، التخطيط الكهربائي للقلب (ECG)، وغيرها [2]، [3]. يمكن استخدام شبكات WBAN في العديد من التطبيقات الطبية وغير الطبية. ففي أنظمة الرعاية الصحية الإلكترونية يمكن، على سبيل المثال، استخدام البيانات التي تم جمعها بواسطة الحساسات لتنبيه المختصين عند وقوع حدث يهدد الحياة[2].

تعد حماية الاتصالات بين الحساسات ضروريةً جداً للحفاظ ليس فقط على خصوصية البيانات الصحية، ولكن أيضاً لضمان تقديم الرعاية الصحية بشكل سليم [4]. حيث يمكن أن يتسبب التلاعب في البيانات بحوادث طبية خطيرة يمكن أن تصل إلى تهديد حياة المريض [5]. من الواضح أن نماذج الحماية التقليدية المصممة لشبكات الحساسات اللاسلكية (Wireless Sensor Networks WSN) التقليدية غير قابلة للتطبيق بشكل مباشر لحماية WBAN، وذلك لأن عقد WBAN محدودة الموارد من حيث الذاكرة واستخدام وحدة المعالجة المركزية واستهلاك الطاقة [2]،[5]. يعتبر إنشاء مفاتيح التشفير المشتركة بين عقد الحساسات إحدى أبرز التحديات في حماية WBAN [5]. حيث أن التوزيع المسبق للمفاتيح يؤدي إلى الاستمرار في استخدام نفس المفاتيح لفترات طويلة من الوقت، مما يعرضها للفضح [6]. كما أن استخدام الطرق التقليدية في تبادل المفاتيح لا يتناسب مع محدودية موارد حساسات شبكة WBAN، حيث أنها مكلفة للغاية [7].

في كثير من الأحيان، في مخططات حماية شبكات WBAN تُستخدم البيانات الحيوية التي تم جمعها بواسطة الحساسات لاستخراج مفتاح يسمى مفتاح بيومتري (biometric key) [2]. تأتي فكرة استخدام خصائص الإشارات الحيوية من أجل الاتفاق على المفاتيح السرية، من ملاحظة أن جسم الإنسان ديناميكي ومعقد، وأن الحالة الحيوية للجسم فريدة تماماً في لحظة معينة [4]. يتيح استخدام الإشارات الحيوية المقاسة في الحساسات إمكانية التوصل إلى قيم مشتركة فيما بينها، وذلك عندما يتم قياس إشارات نفس الجسم وبشكل متزامن. يقضي ذلك على الحاجة إلى التوزيع الصريح للمفاتيح أو التوزيع المسبق للمفاتيح (أي يسمح بالعمل وفق طريقة plug-n-play)، كما يسمح لأجهزة الاستشعار الاتفاق على المفتاح السري عند الحاجة أي تغيير المفتاح بشكل ديناميكي [4]. إن استخدام الخصائص الحيوية يزيد فعالية شبكة WBAN كما أن القيم الحيوية تظهر خصائص عشوائية كافية يمكن استخدامها لتوليد مفاتيح التشفير بدلاً من استخدام مولدات الأرقام العشوائية التي تستهلك الكثير من الطاقة وقدرة المعالجة [6]، [8]. يمكن استخدام مخطط كهربية القلب، وهو تسجيل بياني للتيارات الكهربائية التي تولدها عضلة القلب أثناء الانقباضات، لبناء مخططات آمنة وفعالة لإدارة المفاتيح البيومترية [2].

سنستعرض في هذا المقال أبرز الأعمال السابقة في توليد وتبادل المفاتيح البيومترية في شبكة WBAN، وذلك في القسم الثاني. نورد في القسم الثالث شرحاً تفصيلياً للمخطط المقترح. أما القسم الرابع فيعرض النتائج العملية لتطبيق المخطط. كما يعرض القسم الخامس بعض الاستنتاجات حول مزايا المخطط المقترح مقارنةً بالأعمال السابقة.

2- الأعمال السابقة

تركز كافة الأعمال السابقة في مجال تبادل المفاتيح بالاعتماد على القياسات الحيوية على الاستفادة من تشابه

القيم الحيوية المقاسة بشكل متزامن في عدة حساسات موضوعة على نفس الجسم، وتجاوز العقبات الناتجة عن الاختلافات الطفيفة بين تلك القيم.

في [7] اقترح الباحثون طرقتين لتبادل المفاتيح البيومترية، الأولى هي: الإدارة الغامضة للمفتاح أحادية النقطة (Single-point Fuzzy Key Management). وفيها يتم إنشاء مفتاح التشفير في حساس واحد، ثم يتم توزيعه على باقي الحساسات. يتم استخدام قيم الفاصل الزمني بين نبضتي قلب متتاليتين (Inter pulse interval) IPI كخصائص حيوية مشتركة بين الحساسات وذلك من أجل تبادل المفاتيح فقط وليس من أجل إنشائها. يتم حساب قيم IPI اعتباراً من إشارة ECG. طالما أن IPI المشتقة من الحساس المرسِل مشابهة بدرجة كافية لـ IPI المشتقة من الحساس المستقبِل، يجب أن ينجح تبادل المفاتيح. ولكن عملياً، الخانات الأدنى من IPI تختلف عند قياسها في حساسين مختلفين بدرجة تجعل استعادة المفتاح غير عملي حتى لو تم استخدام توابع تصحيح الأخطاء. في [7] أيضاً، عرض الباحثون طريقة ثانية وهي: الإدارة الغامضة للمفتاح متعددة النقاط (Multipoint Fuzzy Key Management). وفيها يتم تشكيل المفتاح اعتباراً من قيم IPI المقاسة في كل عقدة. يتم استخدام كل قيمة IPI لتوليد 8 بتات فقط. بالتالي، يكون الوقت المطلوب لتشكيل المفتاح يساوي54 ثانية تقريباً كما أن المفتاح الناتج قد لا يكون عشوائياً بدرجة كافية. بالتالي يمكن استنتاج أن هذه الدراسة تحتاج عملياً لزمنٍ كبيرٍ جداً في التنفيذ لضمان عشوائية قيم المفتاح. تم اختبار تلك الدراسة باستخدام إشارة تخطيط القلب السليم ولكن قد يحتاج تشكيل المفتاح اعتباراً من بيانات مرضى القلب زمناً أطول.

تقدم الورقة [4] مخطط PSKA، وهو مخطط يعمل بطريقة plug-n-play. يعتمد على مبادئ Fuzzy Vault [9] لإخفاء المفتاح. لا يتم استخدام الإشارات الحيوية في إنشاء المفاتيح وإنما في تبادلها والاتفاق عليها فقط. تمت معالجة الإشارات الحيوية في المجال الترددي، بدلاً من المجال الزمني. بدراسة هذه الطريقة يمكننا استنتاج أن الرسالة اللازم إرسالها إلى المستقبل لتكوين المفتاح طويلة جداً، وذلك بسبب احتوائها على نقاط الضجيج المستخدمة في مخطط Fuzzy Vault، حيث يزداد الأمان بازدياد عدد تلك النقاط.

في [10] قدم الباحثون مخطط تبادل مفاتيح جديد، ECG-IJS، يسمح للحساسات بتبادل مفتاح سري مشترك تم إنشاؤه بالاعتماد على إشارات ECG. يعمل المخطط المقترح بطريقة plug-n-play. لا يستخدم نقاط الضجيج لإخفاء السر (المفتاح)، فهو يعمل وفق طريقة Fuzzy Vault المعدلة. يعتمد هذا المخطط على تشكيل كثير حدود من قيم شعاع الخصائص المشتركة بين الحساسين وإرسال فقط جزء من معاملات كثير الحدود إلى المستقبل دون تشفيرها. يتكون شعاع الخصائص من القمم المستخرجة عن تحويل فورييه السريع FFT لعينات ECG المقاسة لمدة 4 ثواني. بدراسة هذه الطريقة وعند محاولة تجريبها بشكل عملي، تبين أن اعتماد مجموعة الخصائص الناتجة عن مؤشرات القمم لناتج FFT لأشخاص مصابين بأمراض قلبية وفق الطريقة المقترحة غير عملي، لأن تلك المؤشرات لا تكون متشابهة بين الطرفين بما يكفي لتطبيق الطريقة المقترحة.

في [11] تم استخدام ECG لإنشاء وتوزيع مفاتيح تشفير متناظرة بشكل موثوق وآمن. يعتمد النهج المقترح على ثلاث كيانات لإنشاء المفتاح. تلك الكيانات هي عبارة عن عقدتين تريدان تبادل المفتاح فيما بينهما، وعقدة ثالثة مسؤولة عن توفير هذه العملية بشكل آمن. لتحقيق ذلك، يجب أن تمتلك العقد الثلاث إشارة ECG مسجلة بشكل متزامن. بدراسة هذه الطريقة استنتجنا أن الحاجة إلى كيان ثالث تؤدي إلى زيادة استهلاك الطاقة والموارد بالإضافة إلى الحاجة لعدد كبير من المراحل وعدد كبير من عمليات التشفير وتصحيح الخطأ. هذه الطريقة تفرض قيوداً صارمةً

جداً على التزامن بين الحساسات في تحصيل إشارة ECG. كما يمكن أن تفشل عملية تشكيل المفاتيح في العديد من المرات نتيجة الاختلاف البسيط بين القيم المقاسة بالتزامن في عدة حساسات موضوعة على نفس الجسم.

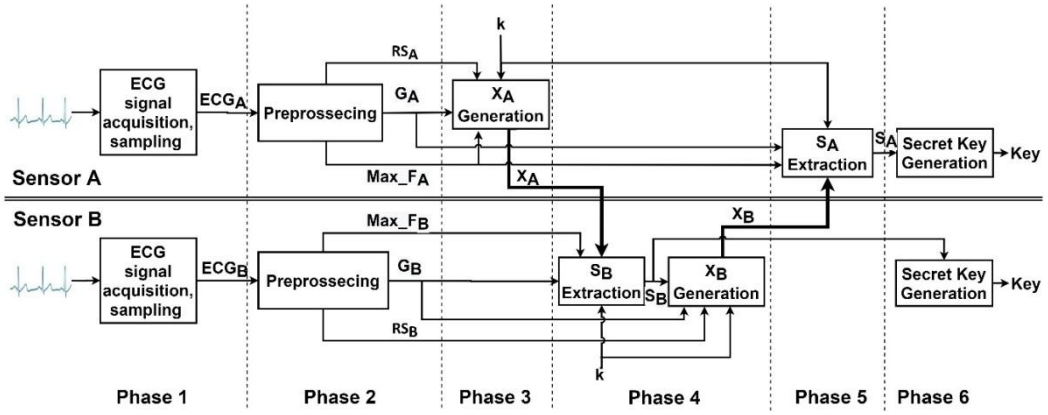
من الدراسات السابقة تبين لنا أن إيجاد مخطط تبادل مفاتيح سرية لشبكة WBAN لا يزال بحثاً مفتوحاً ذو أهمية عالية نظراً لشروط الأمان الصارمة التي يجب تحقيقها ونظراً للمحدودية الكبيرة في الموارد.

3- مخطط توليد وتبادل المفاتيح المقترح

يبين الشكل (1) المخطط المقترح لتبادل المفاتيح بين حساسين موضوعين على نفس الجسم وهما الحساس A والحساس B. يتكون هذا المخطط من 5 مراحل:

المرحلة الأولى:

تحصيل إشارة نبضات القلب من مخطط كهربائية القلب ECG وفق معدل اعتيان محدد، ولمدة زمنية محددة وذلك بشكل متزامن في كلا الحساسين



الشكل (1) مخطط توليد وتبادل المفاتيح المقترح

حيث: ECG هي إشارة التخطيط الكهربائي للقلب، Max_F مجموعة مؤشرات القمم لناتج FFT إشارة ECG، G مجموعة قيم IPI، RS مجموعة القيم العشوائية، k مفتاح التشفير وفق TEA، X مصفوفة الحساس المتبادلة، S مجموعة القيم المشتركة بين الحساسين، Key المفتاح السري المشترك الناتج.

المرحلة الثانية:

وهي مرحلة المعالجة المسبقة. تتألف هذه المرحلة من عدة خطوات يتم تنفيذها في كل من الحساسين A و B كلٌ حسب قيم ECG المحصلة لديه.

الخطوة A: تطبيق تحويل فورييه السريع FFT على الإشارة المحصلة في كل من الحساسين لعدد محدد من العينات، n عينة، اعتباراً من لحظة زمنية محددة. بعد ذلك يتم في كل من الحساسين استخلاص نفس العدد من أدلة المركبات الترددية العظمى، سنطلق عليها اسم مؤشرات القمم (Peaks indexes) وليكن عددها L. تختلف قيم مؤشرات القمم لنفس الجسم من قياس لآخر وذلك بسبب التباين الزمني لإشارة ECG.

بعد استخلاص مؤشرات القمم، يتم ترتيبها تصاعدياً وتخزينها في المجموعتين Max_F_A بالنسبة للحساس A وMax_F_B بالنسبة للحساس B. بعد تشكيل المجموعتين Max_F_A وMax_F_B، سنلاحظ أن هناك عدد كبير من العناصر المشتركة فيما بينها. كما نلاحظ أن عدد العناصر المشتركة بين حساسين موضوعين على جسمين مختلفين يكون صغيراً جداً. نسعى من خلال هذا المخطط إلى جعل كل من الحساسين المنتميين لنفس الشبكة قادراً على التوصل إلى أكبر عدد ممكن من عناصر المجموعة $Max\_F_A \cap Max\_F_B$ نطلق عليها المجموعة S. بإيجاد S

في كل من الحساسين يتم التوصل إلى قيم مشتركة بينهما يمكننا تشكيل المفتاح السري المشترك Key اعتباراً منها.

الخطوة B: استخلاص المجموعة G_A في الحساس A والمجموعة G_B في الحساس B، حيث كل منهما عبارة عن مجموعة مكونة من قيم IPI (سنرمز لها بـ R-R دلالةً على الفاصل الزمني بين قمتي R في نبضتين متتاليتين [12]) لعدة نبضات متتالية وليكن عددها L، تأخذ الشكل التالي:

$$G_A=\{R\text{-}R_{A1}, R\text{-}R_{A2}, \ldots, R\text{-}R_{AL}\},$$
$$G_B=\{R\text{-}R_{B1}, R\text{-}R_{B2}, \ldots, R\text{-}R_{BL}\}$$

يتم ذلك في كلا الحساسين بشكل متزامن اعتباراً من لحظة محددة، حيث تكون $R\text{-}R_{Ai}$ و$R\text{-}R_{Bi}$ هي الفاصل الزمني بين النبضتين i-1 و i نفسهما ولكن $R\text{-}R_{Ai}$ تم قياسها في الحساس A و$R\text{-}R_{Bi}$ تم قياسها في الحساس B. حسب الدراسات السابقة ومنها الدراسة الواردة في [7] وحسب النتائج التجريبية فإن قيمة R-R المقاسة بشكل متزامن في حساسين مختلفين موضوعين على نفس الجسم تكون متقاربةً جداً. كما أن قيم R-R للنبضات المتتالية تختلف عن بعضها بشكل عشوائي.

الخطوة C: توليد المجموعتين RS_A وRS_B في الحساسين A و B على التوالي، حيث كل منهما عبارة عن مجموعة مكونة من 200 قيمة عشوائية طولها 32 بت. يمكن توليد تلك القيم بالاعتماد على إشارة ECG المحصلة بدلاً من استخدام مولدات الأرقام شبه العشوائية التقليدية التي تعاني من استهلاكها الكبير للموارد [13]،[14].

المرحلة الثالثة:

تشكيل المصفوفة X_A في الحساس A ثم إرسالها إلى الحساس B. تبين من التجارب أنه إذا كانت L=20، أي عدد عناصر Max_F هو 20 عنصر، تكون الغالبية العظمى من مؤشرات القمم ذات قيم أصغر من 200. بناءً على ذلك جعلنا المصفوفة X_A مكونة من 200 عنصر. كل عنصر هو عبارة عن قيمة من نمط uint32.

يتم تكوين المصفوفة X_A وفق الخطوات التالية:

الخطوة A: إعطاء عناصر المصفوفة X_A قيم وفق ما يلي:

- العناصر التي دليلها يساوي إحدى قيم عناصر المصفوفة Max_F_A ستملأ بإحدى قيم R-R من المجموعة G_A كما يلي:

$$X_A[i] = R - R_{A[(int)(i/10)+1]} \times 10^6 \quad (1)$$

حيث i هو دليل العنصر في المصفوفة X_A.

قمنا بعملية الضرب بـ 10^6 كي تتوافق القيمة الناتجة مع النمط uint32.

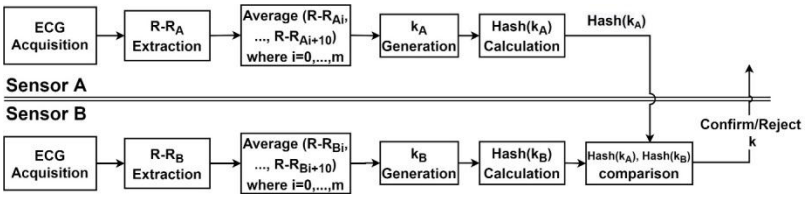
- أما باقي العناصر، يتم ملؤها بالقيم العشوائية المولدة، أي بقيم المجموعة RS_A.

الخطوة B: تشفير بعض عناصر المصفوفة X_A وفق خوارزمية Tiny Encryption Algorithm (TEA). وهي خوارزمية بسيطة جداً لا تستهلك طاقة كبيرة أو زمن كبير وهي تقوم بتشفير كتل كل منها مكون من عنصرين من نمط uint32 باستخدام مفتاح k مكون من 4 عناصر من نمط uint32.

يتم تشفير عناصر X_A التي دليلها يساوي أحد عناصر Max_F_A مع عنصر X_A السابق أو التالي كما ما يلي:

- إذا كان دليل العنصر المراد تشفيره فردي يتم تشفيره مع العنصر السابق له (والذي هو عبارة عن قيمة عشوائية).
- إذا كان دليل العنصر المراد تشفيره زوجي يتم تشفيره مع العنصر التالي له (والذي هو عبارة عن قيمة عشوائية).
- إذا كان هناك عنصرين متتاليين يجب تشفيرهما وكان الأول زوجي والثاني فردي بالتالي يجب تشفيرهما معاً مرة واحدة فقط.

أما بالنسبة لـ k فهو مفتاح تشفير متناظر يجب توليده في التاليتين: كلا الحساسين. من أجل توليد k نميز الحالتين



الشكل (2): توليد المفتاح k في الدورة الأولى لتنفيذ مخطط تبادل المفاتيح المقترح

حيث: ECG هي إشارة التخطيط الكهربائي للقلب، R-R الفاصل الزمني بين نبضتين متتاليتين، k مفتاح التشفير وفق TEA والمراد تبادله.

الحالة الأولى، في الدورة الأولى لتنفيذ المخطط المقترح:

كما ذكرنا سابقاً، فإن المخطط المقترح يسمح بديناميكية المفتاح السري الناتج، أي تغييره بشكل دوري. لتحقيق ذلك، تم افتراض أن المخطط المقترح يتم تنفيذه بشكل مستمر بفواصل زمنية يمكن تحديدها بحسب المعدل المطلوب لتغيير المفتاح. بالتالي يتم تنفيذ هذا المخطط عدد كبير من الدورات وفي كل دورة يتم توليد وتبادل مفتاح سري Key جديد. في الدورة الأولى لتنفيذ المخطط، يتم حساب k اعتباراً من قيم R-R كما في الشكل (2). لتوليد k في كل من الحساسين، يتم حساب وسطي كل 10 قيم متتالية لـ R-R المقاسة اعتباراً من لحظة زمنية معينة. ثم استخلاص ثاني رقم بعد الفاصلة لكل من القيم الناتجة، وذلك بعد تقريب الوسطي إلى أقرب رقمين بعد الفاصلة. يتم تكرار العملية m مرة ثم يتم تجميع الأرقام المستخلصة بشكل متتالي واستخدامها كمفتاح. يتم التجميع بحيث نقوم بملء المراتب الدنيا من العناصر الأربعة للمفتاح أولاً ثم المرتبة الأعلى وهكذا.

بناءً على التجربة العملية وبما أن الحساسين موضوعين على نفس الجسم، تكون فرصة تطابق كافة قيم وسطي R-R في الحساس A مع مقابلاتها في الحساس B لا بأس بها، وذلك عندما يتم حساب قيم R-R بشكل متزامن اعتباراً من لحظة زمنية معينة. في حال تطابق هذه القيم بين الحساسين يكون المفتاح المتشكل k متطابق أيضاً. سنرمز للمفتاح المتشكل في الحساس A بالرمز k_A والمفتاح المتشكل في الحساس B بالرمز k_B. لكي نتحقق أن $k_A = k_B = k$ يقوم الحساس A بحساب قيمة هاش المفتاح k_A أي $Hash(k_A)$ وإرسال الناتج إلى الحساس B الذي بدوره يحسب المفتاح k_B بنفس طريقة حساب k_A، ثم يحسب $Hash(k_B)$. إذا كان $Hash(k_A) = Hash(k_B)$ يرسل الحساس B إلى الحساس A رسالة تؤكد التطابق، وإلا فيرسل رسالة تؤكد عدم التطابق. في حال عدم التطابق يجب إعادة تشكل k من جديد واختباره مرةً أخرى. يستمر تكرار عملية تشكيل k واختباره إلى أن يتحقق الشرط $k_A = k_B = k$.

لم نتمكن من اعتماد هذه الطريقة لتشكيل المفتاح السري بين الحساسين بدلاً من كامل المخطط المقترح للأسباب التالية:

أولاً: قد نضطر لتطبيق هذه الطريقة عدة مرات حتى نتوصل إلى مفتاح مشترك بين الحساسين وذلك بسبب عدم التطابق التام بين قيم R-R المقاسة على التزامن في الحساسين. يؤدي ذلك إلى استهلاك كبير في الطاقة وهدراً في الزمن.

ثانياً، تحتاج هذه الطريقة إلى زمن تحصيل إشارة كبير جداً.

ثالثـاً، قـد تكـون المفـاتيح الناتجـة غيـر عشـوائية بمـا يكفي، وخاصـةً لـدى الأشـخاص الأصـحاء الـذين يتمتعون بانتظام نبضات القلب إلى حد ما.

رغـم نقـاط الضـعف المـذكورة، إلا أن اسـتخدام هـذه الطريقة في سياق المخطط المقترح لن يؤدي إلى إضعافه.

الحالة الثانية، اعتباراً من الدورة الثانية لتنفيذ المخطط:

مـن أجـل تقلـيص زمـن التنفيـذ وطاقـة المعالجـة، يـتم الاعتماد في كل دورة تنفيذ على قيم Key الناتجة في دورة التنفيـذ السـابقة. وبالتـالي نجعـل قيمـة k مسـاوية لقيمـة المفتاح السري المشترك Key المتفق عليه بين الحساسين في دورة التنفيذ السابقة أو لجزء منه. فإذا كانت دورة التنفيذ الحاليـة هـي الدورة i، نجعل قيمـة k مساوية لقيمـة Key_{i-1} أو لجزء منه.

الخطوة C: إرسال المصفوفة X_A إلى الحساس B.

المرحلة الرابعة:

استنتاج القيم المشتركة بين الحساسين في الحساس B (أي استنتاج المجموعة S_B)، ثم تشكيل X_B وإرسالها إلى الحساس A.

تتألف هذه المرحلة من الخطوات التالية:

الخطوة A: تكوين المجموعة S_B في الحساس B. يتم ذلك وفق المراحل التالية:

- **فك تشفير بعض عناصر المصفوفة X_A كما يلي:**

العنصـر الـذي دليلـه يسـاوي أحـد عناصـر المجموعـة Max_F_B يتم فك تشفيره وفق خوارزمية TEA بالمفتاح k الذي تم الاتفاق عليه بين الحساسين. يتم فك تشفير ذلك العنصر مع العنصر السابق أو التالي له وفق ما يلي:

- إذا كان دليل العنصر المراد فك تشفيره فردي يتم فك تشفيره مـع العنصـر السـابق لـه (والـذي هـو عبـارة عـن قيمة عشوائية).
- إذا كان دليل العنصر المراد فك تشفيره زوجي يتم فك تشفيره مـع العنصـر التـالي لـه (والـذي هـو عبـارة عـن قيمة عشوائية).
- إذا كـان هنـاك عنصـرين متتـاليين يجـب فـك تشـفيرهما وكـان الأول زوجـي والثـاني فـردي يجـب فـك تشـفيرهما معاً مرة واحدة فقط.

بعد ذلك يتم مقارنة القيمـة الناتجـة عن فك التشفير بعد تقسيمها على 10^6، أي مقارنة $X_A[i]/10^6$، مع إحدى قيم المجموعـة G_B وهـي $R - R_{B[(int)(i/10)+1]}$، حيث i هو دليـل عنصـر المصـفوفة X_A الـذي نقـوم باختبـاره. إذا كـان الاخـتلاف بينهمـا أقـل أو يسـاوي عتبـة معينـة Th سـيتم إضـافة دليـل العنصـر i إلـى المجموعـة S_B. أمـا إذا كـان الاختلاف بينهما أكبر من العتبة Th بالتالي قيمة الدليل i ليسـت إحـدى مؤشـرات القمـم المشـتركة بـين الطـرفين ويـتم إهمالهـا. إذا كانـت قيمـة مؤشـر القمـة i مشـتركة بـين الحساسين، أي مشتركة بين Max_F_A وMax_F_B، تكون قيمـة العنصـر i مـن المصـفوفة X_A بعـد فـك تشـفيرها وتقسـيمها علـى 10^6 مسـاوية إلـى قيمـة العنصـر $R - R_{A[(int)(i/10)+1]}$ مـن المجموعـة G_A والـذي يكـون ذو قيمة قريبةً جداً من قيمة العنصر المقابل له في G_B وهو $R - R_{B[(int)(i/10)+1]}$، أي يكـــــــــــــــــــون $R - R_{A[(int)(i/10)+1]} = R - R_{B[(int)(i/10)+1]} \mp Th$. بالتـالي Th تمثـل عتبـة الاخـتلاف المقبـول بـين كـل عنصـر مـن المجموعـة G_A ومقابلـه فـي G_B (أي عتبـة الاخـتلاف المقبـول بـين قيمتـي R-R لـنفس النبضـتين المتتاليتين والتي تم قياسهما من خلال حساسين مختلفين موضـوعين علـى نفـس الجسـم). ممـا سـبق نلاحـظ أننـا اسـتطعنا التوصـل إلـى قـيم مؤشـرات القمـم المشـتركة بـين الحساسين A و B.

- **يتم إهمال باقي عناصر المصفوفة X_A.**

الخطـوة B: تشـكيل المصـفوفة X_B بالاعتمـاد علـى المجموعةS_B وعلى المجموعة G_B.

تتكون المصفوفة X_B من 200 عنصر كل منها هو عبارة عن قيمة من نمط uint32. يتم تشكيل X_B بطريقة مشابهة لتشكيل X_A ولكن يتم ذلك في الحساس B وباستخدام المجموعتين G_B وRS_B، كما يتم استخدام المجموعة S_B بدلاً من Max_F_A. يتم تشفير عناصر المصفوفة X_B التي دليلها يساوي إحدى قيم عناصر S_B مع العنصر السابق أو التالي وفق خوارزمية TEA بنفس الطريقة المستخدمة في تشفير عناصر المصفوفة X_A. يتم التشفير بالمفتاح k المتفق عليه بين الحساسين.

الخطوة C: إرسال المصفوفة X_B إلى الحساس A.

المرحلة الخامسة:

استنتاج القيم المشتركة بين الحساسين في الحساس A (أي استنتاج المجموعة S_A) بنفس الطريقة المتبعة لاستنتاج S_B في الحساس B ولكن باستخدام المجموعتين Max_F_A وG_A.

المرحلة السادسة:

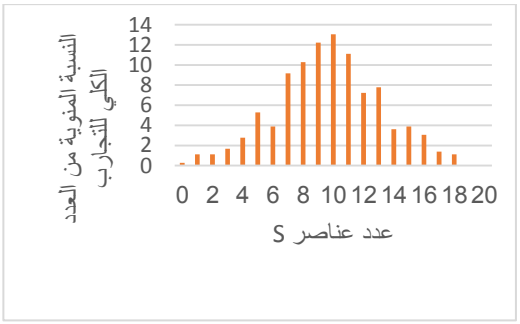
توليد المفتاح السري المشترك في كل من الحساسين اعتباراً من S_A وS_B. فقد أصبح لدينا مجموعة من القيم المشتركة بين الحساسين وهي $S_A=S_B=S$ يمكن تشكيل المفتاح السري المشترك بين الحساسين Key اعتباراً منها. يمكن على سبيل المثال تطبيق أحد توابع هاش على قيم S لتشكيل Key.

4- النتائج والمناقشة

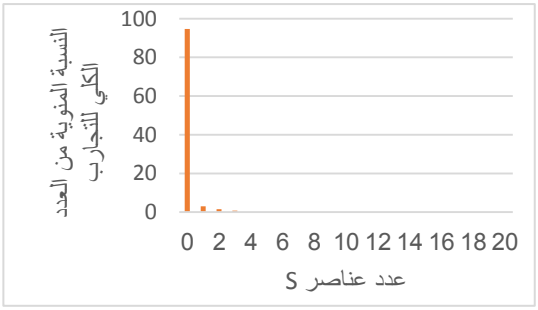
قبل البدء باستعراض النتائج ومناقشتها، نرغب أن ننوه إلى أنه في المخطط المقترح، وكذلك الأمر في الأعمال السابقة، تم افتراض أن الحساسات متزامنة وأنه لا يمكن لأي شخص غير مصرح له أن يحصل على إشارة ECG المريض.

4-1- النتائج التجريبية

تم إجراء كافة التجارب باستخدام بيانات 12 شخص. في دراستنا اعتمدنا على قاعدة بيانات PhysioBank MIT-BIH-Arrythmia Database، وهي قاعدة بيانات لأشخاص يعانون من بعض التشوهات في شكل إشارة ECG وعدم تماثل مطلق بين الإشارتين المقاستين من خلال حساسين موضوعين في مكانين مختلفين من الجسم. معدل اعتيان الإشارة هو 360 عينة في الثانية.



(أ) الحساسين موضوعين على نفس الجسم



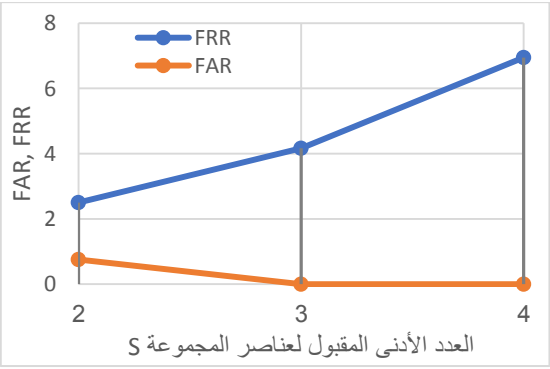
(ب) الحساسين موضوعين على جسمين مختلفين

الشكل (3) النسب المئوية للتجارب بحسب عدد عناصر S الناتجة

يبين الشكل (3) النسب المئوية لعدد عناصر المجموعة S الناتجة (حيث $S=S_A=S_B$)، أي القيم المشتركة بين الحساسين عندما L=20 (طول كل من Max_F_A وMax_F_B يساوي 20 عنصر) والعتبة Th=0.01. حيث Th، وكما ذكرنا سابقاً، تعبر عن عتبة الاختلاف المقبول بين عنصرين متقابلين من المجموعتين G_A وG_B المقاستين بالتزامن من خلال حساسين مختلفين موضوعين على نفس الجسم.

في الشكل (3–أ) تظهر النسب المئوية للتجارب بحسب عدد عناصر S الناتجة عندما يكون الحساسين موضوعين على نفس الجسم. تم إجراء 360 تجربة في لحظات بدء مختلفة وعشوائية. نلاحظ أن النسبة المئوية للتجارب التي فيها عدد عناصر S صغير جداً وبالتحديد أصغر من 3 عناصر هي 4.1%. أما في الشكل (3–ب)، الحساسان موضوعان على جسمين مختلفين. تم إجراء 360 تجربة أيضاً في لحظات بدء مختلفة وعشوائية. نلاحظ أن النسبة المئوية للتجارب التي فيها عدد عناصر S أكبر من 3 عناصر هي 0%. أي أن عدد عناصر S المتشكلة بين الحساسين الموضوعين على جسمين مختلفين صغير جداً وأصغر من 3 عناصر.

فيما يلي وبالاعتماد على التجارب السابقة سنقوم بتحديد عتبة معينة للعدد الأدنى لعناصر S (أي أدنى عدد من القيم المشتركة الناتجة بين الحساسين) المسموح به لتشكيل المفتاح Key، فإذا كان عدد عناصر S أقل من تلك العتبة سيكون هناك شك أن أحد الحساسين غير شرعي أو غير موضوع على نفس الجسم. لتحديد عدد عناصر S التي تجعلنا نحكم بنجاح عملية تبادل المفاتيح وفيما إذا كان الحساسان شرعيين وموضوعين على نفس الجسم سنعتمد على معيارين وهما: معدل القبول الخاطئ (False Acceptance Rate FAR) ومعدل الرفض الخاطئ (False Rejection Rate FRR).



الشكل (4) معدل القبول الخاطئ FAR ومعدل الرفض الخاطئ FRR

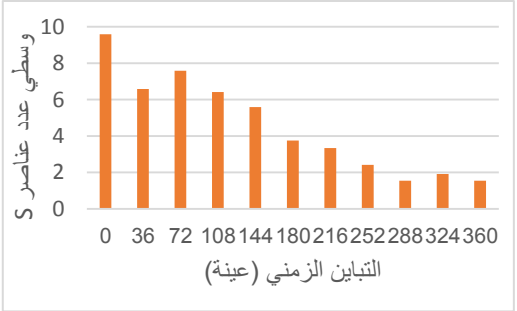
FAR: هو معدل قبول عقد خبيثة على أنها عقد شرعية في شبكة WBAN محددة، وبالتالي هو معدل تشكيل مفتاح سري مشترك مع عقد غير شرعية واعتبارها عقد شرعية. FRR: وهو معدل رفض عقد شرعية من قبل عقد أخرى ضمن نفس شبكة WBAN واعتبارها عقد غير موثوقة، وبالتالي هو معدل رفض تشكيل مفتاح سري مشترك مع عقد شرعية.

يبين الشكل (4) كل من FAR وFRR وذلك من أجل قيم مختلفة للعدد الأدنى المقبول لعناصر S (أي عدد عناصر S التي تدل على أن الحساسين موضوعين على نفس الجسم وبالتالي إمكانية تشكيل المفتاح السري المشترك بينهما) والذي جعلناه مساوي لـ 2 أو 3 أو 4، ومن أجل Th=0.01. إذا كان العدد الأدنى المقبول لعناصر S الذي يدل على أن الحساسين موضوعان على نفس الجسم هو 2، تكون FAR=0.75% ولكن FRR=2.5%. إذا كان العدد الأدنى المقبول لعناصر S هو 3، تكون FAR=0% ولكن FRR=4.1%. وإذا كان العدد الأدنى المقبول لعناصر S هو 4 نلاحظ أن FAR=0% ولكن FRR=6.9%.

مما سبق، نلاحظ أنه كلما ازداد العدد الأدنى المقبول لعناصر S سيكون FRR أكبر وبالتالي أسوأ. كما نلاحظ أنه يجب أن تكون FAR=0% لأننا لا نريد أن يتم قبول حساسات غير شرعية على أنها عقد شرعية في الشبكة. بالمقابل فإن عدم قبول عقد شرعية في بعض الحالات (أي إذا كان FRR > 0)، لا يشكل نفس الخطر والأثر السلبي لقبول عقد غير شرعية وإنما يؤدي حدوث ذلك إلى إعادة عملية تبادل المفاتيح مرة ثانية. نلاحظ أن أفضل نسبة لـ FRR مقابلة لـ FAR=0% هي عندما كان أصغر عدد مقبول لعناصر S هو 3.

تم أيضاً دراسة مدى التسامح مع ضعف التزامن بين الحساسين من خلال حساب وسطي عدد قيم S الناتجة بين حساسين موضوعين على نفس الجسم لدى كل تباين

زمني بينهما، كما هو مبين بالشكل (5). لدراسة ذلك تم إجراء 132 تجربة حيث Th=0.01 والعدد الأدنى المقبول لعناصر S هو 3. نلاحظ أنه وسطياً يصبح عدد قيم عناصر S أصغر من 3، أي يتم رفض تشكيل مفتاح سري بين الحساسين، عندما يكون التباين الزمني بينهما أكبر من 252 عينة أي أكبر من 0.7 ثانية.



الشكل (5) التسامح مع ضعف التزامن بين حساسين موضوعين على نفس الجسم

4-2- دراسة الأمان والأداء

دراسة الأمان:

من الفقرات السابقة يمكن استنتاج أن المخطط المقترح يحقق:

- **السرية:** نتيجة تكوين مفتاح سري مشترك بين الطرفين.
- **المصادقة:** نتيجة التحقق من أن الحساسين المتصلين موضوعين على نفس الجسم وأنهما موثوقين.
- **الحداثة:** يمكن ضمان حداثة المفتاح فهو يتكون من قيم تم قياسها في لحظة معينة حديثة. لا يمكن لمهاجم يملك مفاتيح قديمة أن ينجح بعملية التزوير باستخدامها.

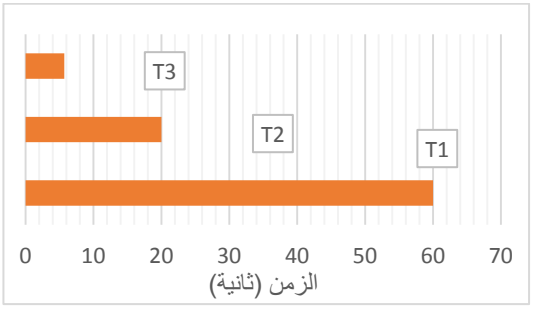
دراسة الأداء:

A. زمن تنفيذ المخطط المقترح

الزمن اللازم لتنفيذ المخطط يختلف بين الدورة الأولى للتنفيذ من جهة وباقي الدورات من جهة أخرى.

زمن دورة التنفيذ الأولى:

في الدورة الأولى يكون لدينا أزمان التنفيذ التالية (الشكل 6)



الشكل (6) زمن تنفيذ الدورة الأولى للمخطط المقترح

- T1: زمن تكوين مفتاح التشفير k. إذا قمنا باستخدام حوالي 60 قيمة R-R (أي m=6) التي ينتج عنها مفتاح مكون من 6 أرقام عشرية. يستغرق ذلك زمن قياس 60 نبضة قلب، أي حوالي أقل من 60 ثانية.
- T2: زمن تشكيل المجموعة G التي تحتاج إلى 20 قياس لـ R-R، أي زمن 20 نبضة. يستغرق ذلك حوالي أقل من 20 ثانية.
- T3: زمن تحصيل عدد معين من عينات ECG لتطبيق FFT عليها. بالتطبيق العملي إذا تم إجراء FFT لـ 2048 عينة بالتالي نحتاج إلى تحصيل الإشارة لمدة 5.7 ثانية.

قد نجعل T1 و T2 و T3 متوازية مع بعضها كما في الشكل (6). أما الزمن اللازم للمعالجة فهو يعتبر مهمل أمام الأزمنة السابقة.

زمن دورة التنفيذ الثانية وما بعدها:

في دورة التنفيذ الثانية وما بعدها من دورات تنفيذ، يتم اختصار الزمن اللازم لتحصيل إشارة توليد المفتاح k (أي إلغاء T1). أما باقي الأزمان فتبقى كما هي. مع ملاحظة أن T2، T3، يمكن أن تتم بالتوازي مع بعضها البعض وبالتالي يكون زمن تنفيذ الخوارزمية حوالي أقل من 20 ثانية.

B. ذاكرة التخزين المطلوبة

نحن بحاجة لذاكرة دائمة تتسع فقط لتخزين المفتاح السري المشترك المكون في الدورة الأخيرة للتنفيذ. أما الذاكرة اللازمة للمعالجة فيجب أن تتسع لتخزين: المجموعة Max_F، المجموعة G، كل من المصفوفتين X_A وX_B، والمجموعة S. بناءً على ما سبق حجم الذاكرة الكلي اللازم للمعالجة هو ما يقارب 1 Mbyte وبالتأكيد نحن بحاجة إلى حجم إضافي لعمليات المعالجة.

C. استهلاك الطاقة

الطاقة المستهلكة في كل حساس هي عبارة عن محصلة الطاقة اللازمة لإرسال المصفوفة X، الطلاقة اللازمة لاستقبال المصفوفة X، والطاقة اللازمة لكافة المعالجات السابقة والتي تكون مرتبطة بالتعقيد الحسابي للعمليات. وكما هو واضح أن التعقيد الحسابي للعمليات صغير جداً مقارنةً بتعقيد طرق تبادل المفاتيح الأخرى.

5- ميزات المخطط المقترح والاستنتاجات

في المخطط المقترح، يمكن لأي حساس أن يتحقق من أن الحساس الآخر الذي يسعى لتشكيل اتصال آمن معه هو حساس شرعي ويقع على نفس الجسم، وذلك من خلال عدد عناصر S المشتركة بينهما. كما برهنا أنه يكفي أن يتشابه عدد معين من مؤشرات القمم، وليس بالضرورة الغالبية العظمى منها، كي يعطي المخطط نتائج صحيحة. واستنتجنا أيضاً ميزة التسامح مع ضعف التزامن.

تم استخدام القيم الحيوية لتوليد المفتاح السري المشترك وأيضاً لتحقيق عملية تبادل المفتاح بشكل سري. كما تم الاستفادة من كل من الخصائص الزمنية (قيم R-R) والخصائص الترددية (مؤشرات قمم ناتج FFT) لإشارة ECG. تم اختيار مؤشرات قمم FFT كخصائص للأسباب التالية: 1) سهلة الاكتشاف مع تعقيد حسابي منخفض، 2) تميز الشخص بشكل جيد للغاية بالتالي توفر آلية مصادقة فعالة، 3) تتغير هذه الخاصة ديناميكياً مع الزمن [4].

لاحظنا من خلال هذا المخطط أن اختلاف ترتيب الخصائص الترددية المشتركة أو اختلاف بعض قيمها بين الحساسين لم يؤثر سلباً على القدرة على استعادة القيم المشتركة وقد تم استخدام المصفوفات وأدلة المصفوفات لتجاوز المشاكل الناتجة عن الاختلاف.

تم تصميم هذا المخطط بطريقة تمكننا من تغيير المفتاح السري المشترك بشكل دوري أو عند الطلب، وذلك بفضل اختلاف الخصائص الترددية والزمنية لإشارة ECG مع الزمن. يزيد ذلك أمان الشبكة ويقلل من احتمال فضح المفتاح السري.

في المخطط المقترح لاحظنا أننا لسنا بحاجة لتثبيت القيم في الحساسات بشكل مسبق قبل تفعيل الشبكة، فهو يعمل وفق طريقة Plug-and-play. ولا تشكل الفترة الأولية لتكوين المفاتيح فترة خطر لأنه لا يتم إرسال المعلومات السرية أو المفاتيح السرية بشكلها الصريح. بعبارة أخرى لا يفترض المخطط المقترح أن الفترة الأولية للتشغيل آمنة.

يتميز المخطط المقترح عن باقي المخططات ببساطة العمليات. على الرغم من أن الطريقتين المقدمتين في [7] تتطلبان نقل بيانات بكميات أقل، إلا أن مخططنا يتفوق عليهما بعدة نقاط وهي زمن تحصيل الإشارة المطلوبة واستخدام القيم الحيوية ليس فقط في تبادل المفاتيح وإنما في توليدها أيضاً. أما بالنسبة للمخطط PSKA [4] فهو يحتاج لزمن أقل من مخططنا في تحصيل الإشارة المطلوبة ولكنه يعتمد فقط على دليل المركبة الترددية العظمى لإشارة ECG المحصلة من حساسين على نفس الجسم والذي في معظم الأحيان لا يكون متطابقاً. كما أن PSKA يحتاج لنقل كمية كبيرة جداً من البيانات ويحتاج في إنجاز عملية Vault Unlocking لكمية معالجة ضخمة جداً، بالتالي تعقيده الحسابي كبير. بالنسبة للمخطط ECG-IJS [10] فهو يحتاج لزمن تحصيل إشارة أقل من مخططنا المقترح وتكون فيه كمية البيانات المتبادلة أقل، ولكن في مخططنا لا يتعلق مقدار الأمان بكمية

البيانات المرسلة كما في ECG-IJS. كما أن ECG-IJS يحتاج إلى توليد عدد كبير من القيم العشوائية ويتم تشكيل مفتاح جديد لكل رسالة. بالنسبة للمخطط المعروض في [11] فكمية البيانات المرسلة أقل من مقابلتها في مخططنا ولكنه يعاني من عدم التسامح مع ضعف التزامن، الحاجة إلى 3 كيانات وبالتالي زيادة التعقيد، وتحصيل الإشارة من 3 حساسات وبالتالي استهلاك كبير للطاقة. كما أنه يعتمد على إشارة ECG كما هي وذلك ليس عملي، فقيم عينات ECG تختلف عن بعضها بشكل كبير لدى قياسها في حساسين مختلفين.

مما سبق يمكننا استنتاج أننا استطعنا التوصل إلى مخطط تبادل مفاتيح بيومترية يحقق كافة المواصفات المطلوبة للعمل بالشكل الأمثل ضمن شبكة WBAN ويضمن جودة وأمان وفعالية عملية تبادل المفاتيح. أما بما يتعلق بالآفاق المستقبلية، فنسعى إلى تطوير المخطط المقترح بهدف تقليل حجم البيانات المتبادلة بين الحساسين وتخفيض الزمن اللازم لإتمام عملية تبادل المفاتيح.

References المراجع

[1] Al-Janabi, S., Al-Shourbaji, I., Shojafar, M., & Shamshirband, S. (2017). Survey of main challenges (security and privacy) in wireless body area networks for healthcare applications. Egyptian Informatics Journal, 18(2), 113-122.

[2] Masdari, M., Ahmadzadeh, S., & Bidaki, M. (2017). Key management in wireless Body Area Network: Challenges and issues. Journal of Network and Computer Applications, 91, 36-51.

[3] Negra, R., Jemili, I., & Belghith, A. (2016). Wireless body area networks: Applications and technologies. Procedia Computer Science, 83, 1274-1281.

[4] Venkatasubramanian, K. K., Banerjee, A., & Gupta, S. K. S. (2009). PSKA: Usable and secure key agreement scheme for body area networks. IEEE Transactions on Information Technology in Biomedicine, 14(1), 60-68.

[5] Zhao, H., Chen, C., Hu, J., & Qin, J. (2015). Securing body sensor networks with biometric methods: A new key negotiation method and a key sampling method for linear interpolation encryption. International Journal of Distributed Sensor Networks, 11(8), 764919.

[6] Raazi, S. M. K. U. R., Lee, H., Lee, S., & Lee, Y. K. (2010). BARI+: a biometric based distributed key management approach for wireless body area networks. Sensors, 10(4), 3911-3933.

[7] Bui, F. M., & Hatzinakos, D. (2007). Biometric methods for secure communications in body sensor networks: resource-efficient key management and signal-level data scrambling. EURASIP Journal on Advances in Signal Processing, 2008, 1-16.

[8] Malik, M. S. A., Ahmed, M., Abdullah, T., Kousar, N., Shumaila, M. N., & Awais, M. (2018). Wireless body area network security and privacy issue in e-healthcare. International Journal of Advanced Computer Science and Applications, 9(4).

[9] Juels, A., & Sudan, M. (2006). A fuzzy vault scheme. Designs, Codes and Cryptography, 38(2), 237-257.

[10] Zhang, Z., Wang, H., Vasilakos, A. V., & Fang, H. (2012). ECG-cryptography and authentication in body area networks. IEEE

Transactions on Information Technology in Biomedicine, 16(6), 1070-1078.

[11] Sammoud, A., Hamdi, O., Chalouf, M. A., & Bouallegue, A. (2018, June). A new protocol for an efficient and green biometric-based security key establishment in WBAN's. In 2018 14th International Wireless Communications & Mobile Computing Conference (IWCMC) (pp. 762-767). IEEE.

[12] Peter, S., Pratap Reddy, B., Momtaz, F., & Givargis, T. (2016). Design of secure ECG-based biometric authentication in body area sensor networks. Sensors, 16(4), 570.

[13] Camara, C., Peris-Lopez, P., Martín, H., & Aldalaien, M. A. (2018). ECG-RNG: A random number generator based on ECG signals and suitable for securing wireless sensor networks. Sensors, 18(9), 2747.

[14] Pirbhulal, S., Zhang, H., Wu, W., Mukhopadhyay, S. C., & Zhang, Y. T. (2018). Heartbeats based biometric random binary sequences generation to secure wireless body sensor networks. IEEE Transactions on Biomedical Engineering, 65(12), 2751-2759.

Received	**2021/6/1**	**إيداع البحث**
Accepted for Publ.	**2021/8/9**	**قبول البحث للنشر**