Studying the Effect of Changing the Security Techniques Used in the MS-LEACH Protocol on the Energy Consumed in WSN Networks

Dr. Inas Laila*
Hla Alkhatib**

(Received 10 / 12 / 2019. Accepted 14 / 6 / 2020)

□ ABSTRACT □

Wireless sensor networks are pioneers in the field of technology, and it's being focused on employing them in different fields, it will also be the foundation stone of Internet Of Things (IOT). And data collected in some WSN applications may need to be confidential and arrive at its destination properly, and this is a major challenge in WSN due to its limited resources such as energy and computational capabilities, which makes finding appropriate protection mechanisms a difficult task. Symmetric cryptographic algorithms such as RC5, AES, and Skipjack are more suited for secrecy than asymmetric cryptographic algorithms, as they are faster to implement and less complicated in calculations. And CBC-MAC and HMAC technologies are also among the most important message integrity and sending node identity verification technologies.

In this research, we first evaluated the performance of the two secure hierarchical protocols SecLEACH and MS-LEACH in the steady-state phase, We implemented scenarios using MatLab, and we used two main metrics to evaluate performance: residual power and the number of alive nodes in the network. The results showed that the SecLEACH protocol is less energy consuming than the MS-LEACH protocol, but this protocol does not guarantee the confidentiality of the transmitted data, while the MS-LEACH protocol ensures that which results in consuming more energy compared to SecLEACH.

We then studied the effect of applying a range of security technologies such as RC5, Skipjack and HMAC in the MS-LEACH protocol in order to improve the energy efficiency of the network, and the results showed that the use of the Skipjack encryption algorithm and the HMAC authentication algorithm in the MS-LEACH protocol prolonged the network life and improved energy efficiency.

Keywords: security, WSN, Hierarchical Routing Protocols, Symmetric cryptography, Energy-cost, Secure routing, Block cipher, AES, RC5, Skipjack, Message authentication code, CBC-MAC, HMAC, MatLab

* **Assistant Professor, Department of Computer Networks and Systems, Faculty of Informatics Engineering, Tishreen University, Lattakia, Syria.**
** **Postgraduate Student (Master), Department of Computer Networks and Systems, Faculty Of Informatics Engineering, Tishreen University, Lattakia, Syria, hala.kha93@gmail.com.**

دراسة أثر تغيير التقنيات الأمنية المستخدمة في البروتوكول MS-LEACH على الطاقة المستهلكة في شبكات WSN

د. اناس ليلى*

حلا الخطيب**

(تاريخ الإيداع 10 / 12 / 2019. قُبِل للنشر في 14/ 6 / 2020)

□ ملخّص □

تعد شبكات الحساسات اللاسلكية رائدة في مجال التكنولوجيا ويتم التركيز على توظيفها في مجالات الحياة المختلفة، كما ستكون حجر الأساس في انترنت الأشياء Internet Of Things (IOT). وقد تحتاج البيانات التي يتم جمعها في بعض تطبيقات WSN إلى أن تكون سرية وتصل إلى وجهتها بشكل سليم، ويعتبر هذا تحدياً كبيراً في WSN وذلك نظراً لمحدودية مواردها كالطاقة والقدرات الحسابية مما يجعل إيجاد آليات حماية ملائمة مهمة صعبة. وتعد خوارزميات التشفير المتناظر مثل RC5 و AES و Skipjack أكثر ملاءمة لتحقيق السرية من خوارزميات التشفير الغير متناظر فهي أسرع من حيث التنفيذ وأقل تعقيداً من حيث العمليات الحسابية، كما تعد التقنيات CBC-MAC و HMAC من أهم تقنيات التحقق من سلامة الرسائل والتحقق من هوية العقدة المرسلة.

قمنا في هذا البحث أولاً بتقييم أداء البروتوكولين الهرميين الآمنين SecLEACH و MS-LEACH وذلك في مرحلة الاستقرار. وقمنا بتنفيذ السيناريوهات باستخدام برنامج MatLab، واستخدمنا لتقييم الأداء معيارين أساسيين هما الطاقة المتبقية وعدد العقد الحية في الشبكة. أظهرت النتائج أن البروتوكول SecLEACH أقل استهلاكاً للطاقة من البروتوكول MS-LEACH إلا أن هذا البروتوكول لا يضمن سرية البيانات المنقولة بينما يضمن البروتوكول MS-LEACH ذلك مما يجعله يستهلك طاقة أكبر.

ثم قمنا بدراسة أثر تطبيق مجموعة من التقنيات الأمنية مثل RC5 و Skipjack وHMAC في البروتوكول MS-LEACH وذلك بهدف تحسين كفاءة استهلاك الطاقة في الشبكة، وتبين لنا أن استخدام خوارزمية التشفير Skipjack وخوارزمية المصادقة HMAC في البروتوكول MS-LEACH أطال عمر الشبكة وحسن من كفاءة استهلاك الطاقة.

الكلمات المفتاحية: الأمن، شبكات الحساسات اللاسلكية، بروتوكولات التوجيه الهرمي، التشفير المتناظر، كلفة الطاقة، التوجيه الآمن، Block Cipher، LEACH, SecLEACH, MS-LEACH, AES, RC5, Skipjack، رمز مصادقة الرسالة، HMAC CBC-MAC , ماتلاب.

* مدرسة-قسم النظم والشبكات الحاسوبية-كلية الهندسة المعلوماتية- جامعة تشرين- اللاذقية – سورية.

** طالبة دراسات عليا(ماجستير)- قسم النظم والشبكات الحاسوبية- كلية الهندسة المعلوماتية- جامعة تشرين- اللاذقية-سورية- hala.kha93@gmail.com.

مقدمة:

تشكل شبكات الحساسات اللاسلكية Wireless Sensor Networks (WSN) ثورةً في عالم تكنولوجيا المعلومات والاتصالات اللاسلكية، إذ يتم توظيفها في تطبيقات الحياة المختلفة التي تخدم الإنسان من جوانب عديدة، وتتألف من عقد حساسات لاسلكية صغيرة منخفضة الكلفة تقوم بتحسس الوسط المحيط وجمع البيانات المطلوبة وإرسالها إلى المحطة القاعدية.

ونظراً لمحدودية موارد عقد الحساسات وخاصة مصدر الطاقة الذي هو عبارة عن بطارية غير قابلة لإعادة الشحن، وسعة التخزين الصغيرة، كان لا بد من إيجاد بعض الحلول التي تسهم في توفير استهلاك الطاقة فظهرت شبكات الحساسات ذات البنية الهرمية Hierarchical WSN حيث تنظم العقد ضمن عناقيد ويحوي كل عنقود رأس عنقود Cluster Head يقوم بتجميع البيانات التي ترسلها العقد الأعضاء إليه، ثم يرسلها إلى المحطة القاعدية، وهذا يسهم في تقليل عدد عمليات الإرسال المباشرة من عقد الحساسات إلى المحطة القاعدية مما يحفظ طاقة العقد ويطيل فترة عملها، ولقد اقترح الباحثون العديد من بروتوكولات التوجيه الهرمية لشبكات الحساسات اللاسلكية كان أولها البروتوكول LEACH (Low Energy Adaptive Clustering Hierarchy) القائم على العنقدة والذي تم تطويره بهدف تحسين كفاءة استهلاك الطاقة في شبكات الحساسات اللاسلكية. [7]

ثم توجه اهتمام الباحثين نحو الجانب الأمني في شبكات الحساسات اللاسلكية، وبما أنه لا يجب فصل الجانب الأمني عن جانب استهلاك الطاقة فهما محوران مترابطان فقد قام الباحثون في دراسات عديدة بتركيز أبحاثهم على تطوير البروتوكول LEACH، وعملوا على إطلاق إصدارات جديدة منه وذلك بإضافة المزايا الأمنية إلى آلية عمله كخوارزميات التشفير وخوارزميات المصادقة، وبذلك لم يهملوا محور كفاءة استهلاك الطاقة وتمكنوا من تقديم بروتوكولات هرمية آمنة وذات كفاءة جيدة في استهلاك الطاقة.[8][7]

الدراسات المرجعية:

ظهرت أبحاث عديدة تناولت بروتوكولات التوجيه الهرمية الآمنة والفعالة في استهلاك الطاقة، حيث ركز الباحثون على بروتوكول LEACH وبدأوا بإطلاق بروتوكولات محسنة منه تتمتع بمزايا أمنية عديدة تحميها من الهجمات الأمنية المختلفة:

فمثلاً قام الباحثون في المرجع [1] باقتراح البروتوكول SLEACH وهو تطوير للبروتوكول LEACH يستخدم آليات أمنية ويحافظ على البنية والقدرات التي يتمتع بها LEACH، ويحقق مطلبين أمنيين أساسيين هما موثوقية المصدر وحداثة الرسالة، حيث يقوم SLEACH بمصادقة رسائل الإعلام Sec-Adv فيمنع المهاجم من أن يصبح رأس عنقود في الشبكة وبالتالي يمنع وقوع الهجمات Selective forwarding, Sinkhole, Helloflood، لكنه لا يقوم بمصادقة رسائل طلب الانضمام Join-Req وبالتالي يمكن للمهاجم الانضمام إلى أحد العناقيد بهدف إرسال رسائل مزيفة إلى رأس العنقود مما يجعل رأس العنقود يوجه رسائل مزيفة إلى المحطة القاعدية فيستنزف طاقته، أو بهدف إزحام الجدول الزمني الذي ينشئه رأس العنقود مسبباً هجوم حجب الخدمة أو خفض إنتاجية رأس العنقود، لكن الرسائل التي ترسلها العقد تكون موثوقة بسبب إضافة قيمة الMAC (Message Authentication Code) إليها وبالتالي يمكن للمحطة القاعدية كشف الرسائل المزيفة والتخلص منها، أما بالنسبة لحداثة الرسالة فتتحقق من خلال عداد مشترك بين المحطة القاعدية وكل عقدة يضاف إلى الرسائل المتبادلة بينهم وذلك بهدف منع هجوم التكرار Replay attack.

وعلى الرغم من الإيجابيات التي قدمها البروتوكول SLEACH إلا أنه لم يمتلك آلية المصادقة بين رأس العنقود وأعضائه لذلك قام الباحثون في الدراسة [2] باقتراح البروتوكول SecLEACH حيث أضافوا تقنية جديدة وهي التوزيع المسبق العشوائي للمفاتيح قبل نشر العقد، وهنا لا يقتصر اختيار العقدة لرأس العنقود المناسب على قربه فقط بل أيضاً على وجود مفتاح مشترك بينهما لاستخدامه في مصادقة رسالة طلب الانضمام Join-Req، كما ضمن البروتوكول حداثة الرسائل.

ثم قام الباحثون في [3] باقتراح البروتوكول MS-LEACH لتحسين المستوى الأمني في SLEACH وذلك من خلال تحقيق المصادقة بين العقدة ورأس العنقود الذي تنتمي إليه عن طريق المفاتيح الثنائية، والسرية من خلال التشفير، ويستخدم عداد لضمان حداثة الرسائل، ويضيف قيمة MAC إلى الرسالة لضمان موثوقية المصدر وسلامة الرسالة من التعديل.

كما قام الباحثون في [4] بتطوير البروتوكول LEACH وذلك باستخدام خوارزمية التشفير المتناظر AES لتحقيق سرية البيانات خلال إرسالها حيث يتوجب تشفيرها قبل إرسالها في كل قفزة (من العقدة إلى رأس العنقود ومن رأس العنقود إلى المحطة القاعدية)، وقد افترض الباحثون أن المحطة القاعدية موثوقة وتستخدم كمركز لتوزيع المفاتيح حيث أنه غالباً ما نحتاج إلى عدة مفاتيح لتأمين أنماط الاتصالات المختلفة بين عقد الحساسات ورؤوس العناقيد والمحطة القاعدية في شبكات WSN الهرمية.

كما عمل الباحثون في [5] أيضاً على تحسين المستوى الأمني للبروتوكول LEACH فطرحوا بروتوكول جديد Secure-LEACH يستخدم المفاتيح المشتركة بين المحطة القاعدية وعقد الحساسات، تستخدم هذه المفاتيح لتوليد قيمة MAC مما يسمح للمحطة القاعدية بالتحقق من موثوقية العقد وسلامة الرسائل المتبادلة، فيتم منع المهاجمين من الانضمام إلى الشبكة كرؤوس عناقيد كما وتمكن للمحطة القاعدية من التخلص من الرسائل المزيفة، وفي هذا البحث قام الباحثون باستخدام خوارزمية RSA لتوليد المفاتيح، فعندما تقرر عقدة أن تكون رأس عنقود فإنها تقوم بإرسال رسالة إعلام آمنة تحوي معرفها و ال MAC الخاص بها، فتقوم العقد باستلام رسائل الإعلام وكذلك تستقبلها المحطة القاعدية فتقوم بالتحقق من موثوقيتها وتنشئ لائحة تحوي معرفات الرؤوس الموثوقة وتبث اللائحة مرفقة بقيمة MAC. وفي حال قام المهاجم بإرسال رسائل مزيفة مباشرةً إلى المحطة القاعدية فإن المحطة تقوم بحساب MAC لها وتدرك أنها غير مطابقة وتتخلص منها.

كما قام الباحثون في [6] بمحاولة تحسين المستوى الأمني للبروتوكول LEACH وذلك بإضافة خوارزمية التشفير المتناظر DES، حيث أنه وبعد أن تتشارك كل العقد والمحطة القاعدية مفتاح ابتدائي قبل النشر، تقوم كل عقدة حساس بجمع البيانات من الوسط المحيط وتشفرها ثم ترسلها إلى رأس العنقود الخاص بها، والذي يقوم بدوره بتجميع البيانات المشفرة الواصلة من العقد في عنقوده وإرسالها إلى المحطة القاعدية دون فك تشفيرها، وتعد المحطة القاعدية مسؤولة عن فك تشفير البيانات الواصلة إليها من رؤوس العناقيد واتخاذ الإجراء المناسب.

أهمية البحث وأهدافه:

تعد بروتوكولات التوجيه الآمنة واحدة من الطرائق المثالية لتحسين المستوى الأمني لشبكة الحساسات اللاسلكية وحمايتها من الهجمات المختلفة، ولاسيما الهرمية منها التي تحقق أيضاً توفيراً فعالاً في استهلاك الطاقة الأمر الذي يطيل زمن حياة الشبكة. ولقد قام الباحثون بتطوير العديد من بروتوكولات التوجيه الهرمية الآمنة حيث استخدموا في كل

منها تقنيات أمن مختلفة بغية تحقيق المتطلبات الأمنية المختلفة كالسرية والمصادقة والسلامة، وعليه فإن المقارنة بين بعض هذه البروتوكولات يساعدنا على تحديد أفضلها وفق ما يحتاجه التطبيق الذي تعمل من أجله الشبكة.

يهدف هذا البحث إلى مقارنة بروتوكولين هرميين آمنين هما SecLEACH و MS-LEACH في مرحلة الاستقرار ودراسة أثر كل منهما على زمن حياة الشبكة، ثم دراسة أثر تغيير التقنيات الأمنية المستخدمة في البروتوكول MS-LEACH من أجل تحسين كفاءة استهلاك الطاقة وإطالة عمر الشبكة.

طرائق البحث ومواده:

يبدأ هذا البحث بتعريف بروتوكول LEACH ثم ينتقل إلى ذكر بعض تقنيات الأمن المستخدمة، ثم ينتقل إلى دراسة نظرية للبروتوكولين المطورين SecLEACH وMS-LEACH و مراحل عمل كل منهما والتحليل الأمني لكل منهما، من ثم يتم شرح كيفية حساب كلفة الاتصال في عقدة الحساس وتأثرها بالتقنيات الأمنية المستخدمة، ثم ينتقل إلى الدراسة التجريبية وذلك عن طريق بناء نموذج شبكة الحساسات اللاسلكية وإجراء المحاكاة باستخدام MatLab بهدف مقارنة البروتوكولين وفقاً لمعايير مختلفة لتحديد البروتوكول الذي ينصح به وفق حاجة كل تطبيق. ونلخص عملية المحاكاة في أربع خطوات رئيسية وهي:

- تصميم النموذج.
- اختيار المقاييس.
- تنفيذ المحاكاة.
- تحليل النتائج.

طرائق وتقنيات الحماية المستخدمة في شبكات الحساسات اللاسلكية:

إن أهم متطلبات الأمن التي يجب تحقيقها في شبكات الحساسات اللاسلكية هي سرية البيانات المتناقلة في الشبكة ومصادقة العقد والتحقق من سلامة الرسائل، ويتم تحقيقها باستخدام خوارزميات التشفير وتقنيات المصادقة المختلفة.

1- التشفير المتناظر Symmetric Cryptography:

ويدعى أيضاً تشفير المفتاح السري secret-key يستخدم المفتاح السري في عمليتي التشفير وفك التشفير، يعتبر أكثر ملاءمة لشبكات الحساسات لأنه يستهلك طاقة أقل، كما يعتبر أسرع من الخوارزميات التشفير الغير متناظرة لأن عملية التشفير تكون أقل تعقيداً [10]، وتقسم خوارزميات التشفير المتناظر إلى فئتين هما Stream-cipher وفيها يتم تشفير البيانات على هيئة دفق من البتات، وBlock-cipher وفيها يتم تشفير البيانات على هيئة بلوكات وكل بلوك مؤلف من عدة بتات، وفي شبكات الحساسات اللاسلكية ركزت الدراسات العلمية على Block-ciphers [13]لأنها أكثر كفاءة في استهلاك الطاقة وأقل تأخيراً مقارنةً بغيرها، ومن الأمثلة عليها: AES, RC5, Skipjack ويوضح الجدول (1) مقارنة بينها من حيث المتانة [11]:

الجدول (1): بعض خوارزميات التشفير المتناظر

Block cipher scheme	Block size (bit)	Key size (bit)	Security strength
AES	128	128	Secure for 10 rounds
RC5	32	128	Secure for more than 16 rounds
Skipjack	64	80	Currently considered unbreakable for 32 rounds

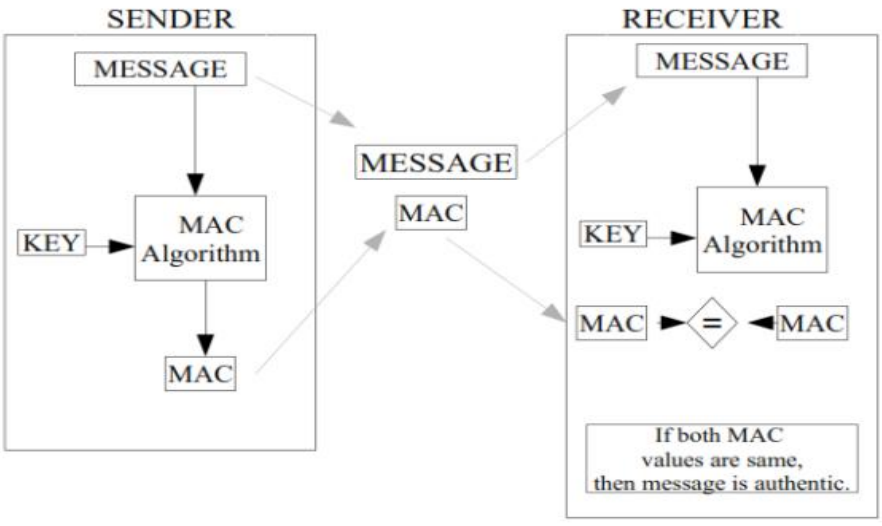
AES (Advanced Encryption Standard): ويدعى أيضاً خوارزمية Rijndael وتم تبنيه كمعيار للتشفير من قبل حكومة الولايات المتحدة، وهو أحد أشهر خوارزميات التشفير المتناظر، ويتميز بسرعته وسهولة تحقيقه، ويعمل على مصفوفة حجمها 4x4 كدخل وهي نص حجمه 128-bit, ويستخدم مفتاح بأطوال (128, 192, 256-bit) ويعمل وفق عدد محدد من الدورات 10,12,14 على الترتيب [13] [12] [11] .

RC5 (Rivest Cipher 5) : صممت من قبل Ronald Rivest في عام 1994، وتتميز هذه الخوارزمية بمرونتها، فهي توفر أحجام مختلفة لبلوكات البيانات (32, 64, 128-bit) وعدد دورات عملها يتراوح بين (0…255) وطول المفتاح (0…255 bits) وهذا يساعد في تحديد المستوى الأمني للخوارزمية، كما تتميز ببساطتها من حيث العمليات الرياضية التي تستخدمها، وفي الغالب تعمل على 12 دورة، وتحدد قيم البارامترات السابقة درجة أمن الخوارزمية [13] [11].

Skipjack: تم تطويرها من قبل وكالة الأمن العالمية في الولايات المتحدة (NSA(National Security Agency، وهي تعمل وفق 32 دورة وتستخدم مفتاح طوله 80-bit للتشفير وفك التشفير وحجم البلوك 64-bit ، وهذا يشير إلى أنها ليست مرنة مثل AES و RC5 [13] [11].

2- رموز مصادقة الرسالة (MACs(Message authentication Codes:

وتستخدم لضمان سلامة البيانات وعدم تعرضها لأي تعديل خلال النقل بالإضافة إلى مصادقة العقد، ويتم اختيار خوارزمية MAC الملائمة وفق المتطلبات الأمنية والفعالية الحسابية، ويوضح الشكل (1) [5] خوارزمية توليد رمز المصادقة والتحقق بين طرفين المتراسلين، وأبرز هذه الخوارزميات المستخدمة في شبكات الحساسات اللاسلكية HMAC, CBC-MAC.

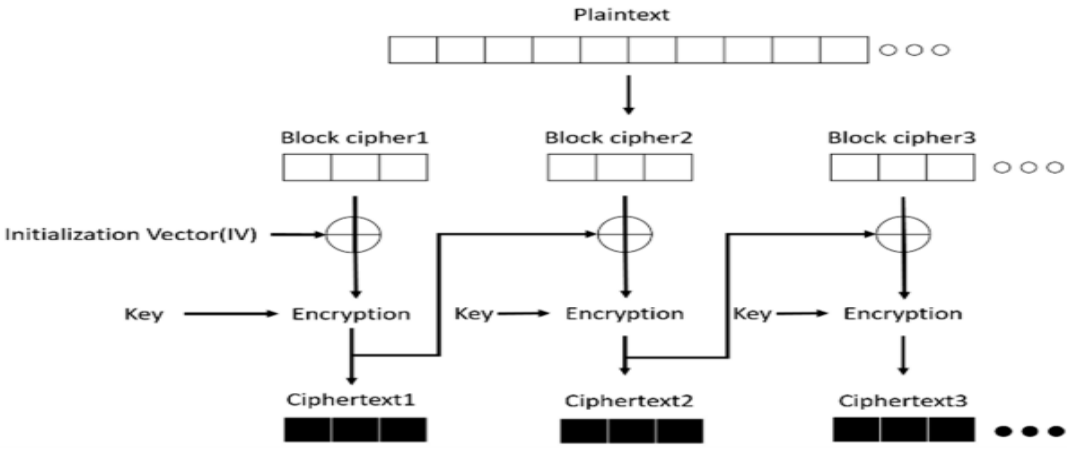


الشكل (1): خوارزمية توليد رمز مصادقة الرسالة [5]

إن القوة والمتانة الأمنية لرمز مصادقة الرسالة تعتمد على طوله حيث تستخدم بروتوكولات الحماية التقليدية رموز ذات أطوال Byte (8-16)، لكن في شبكات الحساسات اللاسلكية WSN يستخدم رمز مصادقة بطول Byte-4.[13]

2-1- تقنية (Cipher Block Chaining Message Authentication Code)CBC-MAC:

وهي تقنية تستخدم لحساب قيمة MAC بالاعتماد على block cipher، حيث يتم تشفير الرسالة باستخدام خوارزمية block cipher بالنمط CBC لإنشاء سلسلة من البلوكات [11] [14]، وقيمة MAC التي تضاف إلى الرسالة هي القيمة الناتجة عن تشفير آخر بلوك (بضع بتات (4-Byte))، وبهذه الطريقة فإن أي تعديل بأي بت من الرسالة سيؤدي إلى تغيير البلوك الأخير المشفر الذي لا يمكن معرفته دون معرفة مفتاح خوارزمية التشفير. تستخدم هذه التقنية مفتاحين مختلفين أحدهما تستخدمه خوارزمية التشفير والآخر هو شعاع ابتدائي صفري Initialization Vector، ويوضح الشكل(2) [20] آلية عمل التقنية : من أجل رسالة plaintext يتم تقسيمها إلى بلوكات BlockCiphers ويتم تنفيذ الجمع الثنائي XOR بين كل بلوك والشعاع الصفري، ثم يتم تشفير النتيجة باستخدام مفتاح سري key بأحد خوارزميات التشفير، ثم يتم إجراء XOR بين نتيجة التشفير وبلوك جديد من الرسالة وتشفر النتيجة باستخدام نفس المفتاح وهكذا، ثم تستخدم بضع بتات (4-Byte) من البلوك الأخير كقيمة MAC تضاف إلى الرسالة.



الشكل (2): آلية عمل تقنية المصادقة CBC-MAC

2-2- تقنية (Keyed-Hash Message Authentication Code)HMAC:

هي تقنية لحساب قيمة الMAC ولكنها لا تستخدم خوارزميات التشفير Block-ciphers بل تستخدم توابع الاختزال وحيدة الاتجاه one way hash functions مثل SHA-1 و MD5 بالإضافة إلى مفتاح سري k لمصادقة المعلومات المتناقلة عبر الشبكة [11] [13]، حيث تقوم هذه التوابع بتحويل نصوص ذات أحجام مختلفة إلى قيم ذات حجم ثابت باستخدام توابع الضغط، وتقوم الفكرة الأساسية لتقنية HMAC على أن المفتاح يتم اختزاله مع الرسالة [14] كما توضح العلاقة (1):

$$m = \mathrm{MAC}_k(x) = h(k||x) \quad \ldots (1)$$

حيث أن: h هو تابع الاختزال، K هو المفتاح السري و X هي الرسالة التي يراد توليد رمز المصادقة لها، أما m فهي رمز المصادقة.

تعتبر هذه التقنية أفضل لشبكات الحساسات اللاسلكية من تقنية CBC-MAC التي تسبب آلية عملها زيادة في التكاليف الحسابية وهذا يؤثر على كفاءة استهلاك الطاقة، إضافةً إلى أن عمليات HMAC أسرع في التنفيذ وأقل استهلاكاً للطاقة [19]، وأفضل توابع الاختزال التي يمكن استخدامها في HMAC هو MD5 (يكون دخلها بلوك حجمه 512 bit وخرجها 128 bit) لأن زيادة تعقيد تابع الاختزال المستخدم تخفض الأداء بشكل واضح [19].

البروتوكول LEACH (Low Energy Adaptive Clustering Hierarchy) :

هو أول بروتوكول توجيه هرمي قائم على أساس العنقدة الاحتمالية الديناميكية، وهو أحد أهم بروتوكولات التوجيه الهرمية التي تحقق كفاءة عالية في استهلاك الطاقة أثناء عمل الشبكة، و يعمل على عدة دورات rounds، وينقسم في آلية عمله إلى مرحلتين أساسيتين [7]:

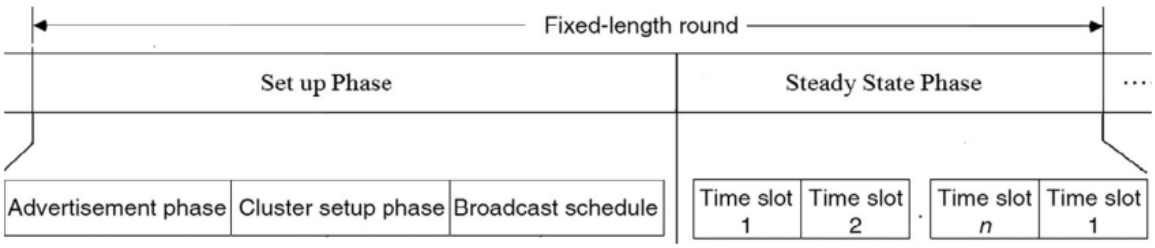
مرحلة الإعداد Set-up phase:

في هذه المرحلة تمتلك كل العقد نفس الأحقية في أن تصبح رأس عنقود Cluster Head(CH)، ويتم الانتخاب بشكل ذاتي من قبل كل عقدة. حيث تقوم كل عقدة باختيار رقم عشوائي بين 0 و1، وتقارن هذا الرقم مع عتبة معينة Threshold t(n) فإذا كان الرقم أصغر من العتبة تصبح العقدة رأس عنقود للدورة الحالية، ويتم حساب العتبة وفق العلاقة (2)[5]:

$$t(n) = \begin{cases} \frac{p}{1-p*(r \bmod \frac{1}{p})} & if \quad n \in G, \\ 0 & if \quad n \notin G. \end{cases} \quad \ldots(2)$$

حيث أن: P رقم يعبر عن احتمالية أن تصبح العقدة CH، (P=0.05)، r رقم الدورة الحالية، G مجموعة العقد التي لم تصبح CHs حتى الآن.

بعد تحديد الCHs يقوم كل منها ببث رسالة بث عام وهي إعلان advertisement إلى العقد المجاورة باستخدام البروتوكول CSMA-MAC(Carrier Sense Multiple Access-Media Access Control) لمنع التصادم، وبدورها كل عقدة تختار CH المناسب وفق قوة إشارة الرسالة المستلمة وترسل له رسالة طلب انضمام Join-req باستخدام CSMA-MAC ، ثم يقوم CH بتوليد جدول زمني TDMA schedule وتوزيعه على العقد برسالة بث عام باستخدام CSMA-MAC، يحدد فيه الفاصل الزمني المخصص لكل عقدة لديه لترسل خلاله البيانات التي تلتقطها كما يوضح الشكل(3)[5].

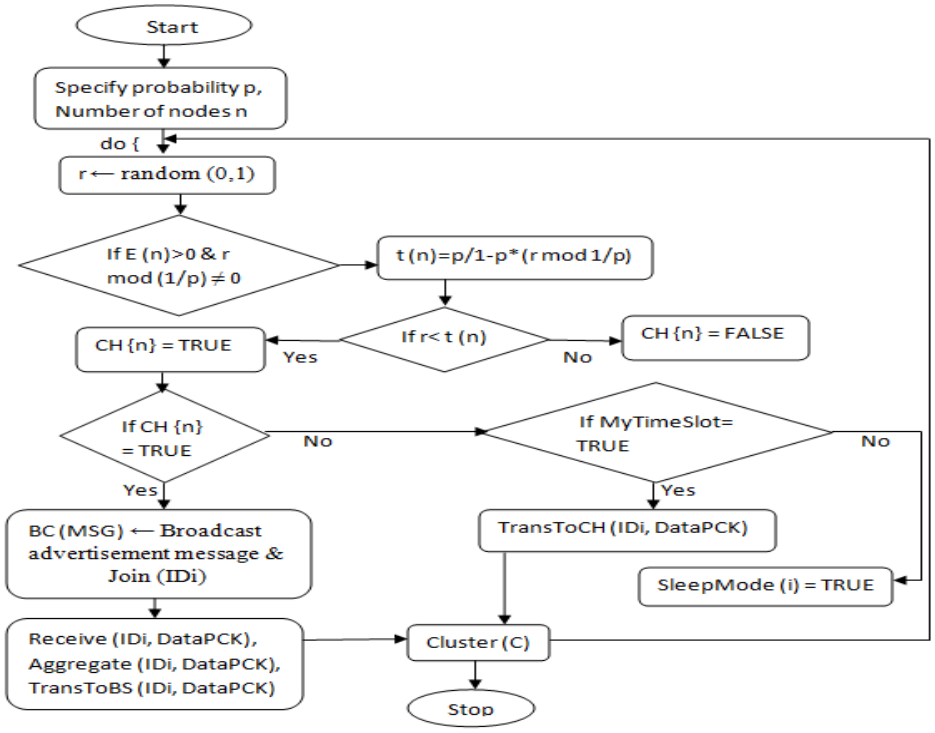


الشكل (3): مرحلة الإعداد set up phase و مرحلة الاستقرار steady state phase في بروتوكول LEACH [5]

مرحلة الاستقرار Steady-state:

بعد انتهاء عملية تقسيم الشبكة إلى عناقيد في الدورة الحالية، تبدأ عملية التراسل، حيث تقوم العقد بتسجيل المعلومات من الوسط المحيط وتقوم بإرسالها إلى CH خلال الفاصل الزمني المخصص لها، ويقوم الCH بتجميع البيانات من العقد الأعضاء ويرسلها إلى المحطة القاعدية Base station(BS).

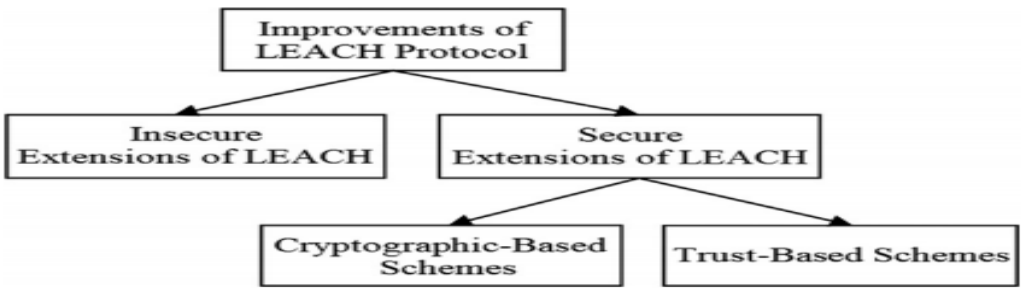
يلخص الشكل (4) مرحلتي الإعداد والاستقرار في البروتوكول LEACH [7]:



الشكل (4): مخطط تدفقي لمراحل عمل بروتوكول LEACH

بروتوكولات التوجيه المطورة من بروتوكول LEACH:

اهتم البروتوكول LEACH فقط بمحور توفير استهلاك الطاقة ولم يأخذ بعين الاعتبار محور الأمن وحماية الشبكة من الهجمات الأمنية المختلفة، لذلك ظهرت بروتوكولات مطورة من البروتوكول LEACH اهتم الباحثون في بعضها بتحسين مستوى الأمن والحماية في الشبكة، كما يوضح الشكل (5) [8]:



الشكل (5): أنواع البروتوكولات المطورة من بروتوكول LEACH [8]

وفيما يلي سنقوم بدراسة أهم البروتوكولات المطورة عن LEACH والتي تصنف تحت إطار النماذج القائمة على التشفير.

1- البروتوكول SecLEACH (Secure LEACH):

تم تصميمه من أجل تحسين البروتوكول SLEACH الذي هو أول نسخة مطورة من بروتوكول LEACH تستخدم طرائق أمنية [9]. حيث يتم تزويد المحطة القاعدية بمجموعة كبيرة من المفاتيح S قبل نشر الشبكة، ثم يتم تزويد كل عقدة بحلقة m من المفاتيح من المجموعة S وكل حلقة تحوي ثنائيات مؤلفة من المفتاح ومعرفه، كما يتم تزويدها بمفتاح مشترك مع BS [9].

في البروتوكول LEACH تختار العقدة رأس العنقود الأقرب إليها لتوفير الطاقة، أما في SecLEACH ونظراً لتشارك المفاتيح ليست كل CHs مناسبة وإنما يتوقف ذلك على المفاتيح المشتركة بينها، ويتم تنفيذ البروتوكول وفق الخطوات التالية:

مرحلة الإعداد Set-up phase:

1- يقوم كل CH ببث رسالة تحوي معرفه وإعلام adv و nonce (رقم عشوائي) بالإضافة إلى معرفات المفاتيح الموجودة في الحلقة لديه، ثم تختار كل عقدة CH المناسب حسب قوة إشارة الرسالة المستلمة وتقوم بتحديد موقع المفتاح المشترك بينهما.

2- ترسل كل عقدة رسالة انضمام Join-req إلى CH الذي اختارته تحوي معرفها ومعرف CH وموقع المفتاح المشترك بينهما، بالإضافة إلى قيمة MAC للرسالة يتم توليدها باستخدام هذا المفتاح، ولضمان حداثة الرسالة يتم إضافة nonce المستخدم في الخطوة الأولى إلى الرسالة.

3- ثم يقوم كل CH ببث الجدول الزمني إلى أعضائه.

مرحلة الاستقرار Steady-State:

4- تبدأ كل عقدة باستشعار البيانات وتضعها في رسالة تحوي معرفها ومعرف CH والبيانات المسجلة، ويتم توليد قيمة MAC للرسالة باستخدام المفتاح المشترك مع رأس العنقود، ويتم إضافة قيمة محسوبة باستخدام nonce و رقم دورة التقرير الحالية (j)reporting cycle في الدورة الحالية إلى الرسالة لضمان حداثة الرسالة.

5- يقوم CH بتجميع البيانات في رسالة تحوي معرفه ومعرف BS، ويقوم بتوليد قيمة MAC للرسالة باستخدام المفتاح المشترك بينه وبين BS، ويتم إضافة العداد المشترك بينه وبين BS إلى الرسالة، ويتم زيادة هذا العداد بعد كل عملية إرسال.

التحليل الأمني للبروتوكول SecLEACH:

إن SecLEACH يتيح المصادقة بين رأس العنقود وأعضائه لأن رسالة طلب الانضمام أصبحت موثوقة، وبالتالي ليس واجباً على BS التحقق من العقد قبل قبول البيانات المجمعة الواصلة من CHs، وهذا يمنع المهاجم من الانضمام على الشبكة، بالإضافة إلى أن البيانات التي تلتقطها العقد مضمنة في حساب الMAC للرسالة وهذا يضمن سلامة الرسالة أثناء نقلها عبر الشبكة، وبالرغم من ذلك مازال SecLEACH يعاني من بعض العيوب التي يعاني منها SLEACH وهي [9]:

1- لا يوجد ضمان لسلامة رسالة الجدول الزمني، وهذا يسمح للمهاجم بمقاطعة الاتصالات في الشبكة، حيث يمكن أن يقوم المهاجم بتبديل الجدول الزمني بآخر فقد ينتج عن ذلك تصادم للبيانات بسبب محاولة عقدتين إرسال

بياناتهما في نفس الوقت، أو قد يحاول المهاجم إرسال البيانات في الوقت المخصص لعقدة معينة، لذلك فإن المصادقة والتشفير إجراءان ضروريان لحماية رسالة الجدول الزمني من التعديل.

2- البيانات التي تلتقطها العقد لا يتم تشفيرها وهذه مشكلة إذا كانت البيانات المنقولة حساسة.

2 – بروتوكول (Modified Secure LEACH)MS-LEACH:

تم تصميمه لتحسين مستوى الحماية في بروتوكول SLEACH، من خلال توفير سرية البيانات والمصادقة بين رؤوس العناقيد والأعضاء من خلال مفتاح مشترك بينها [9]. في البداية وخلال نشر العقد في الشبكة، تمتلك كل عقدة مفتاحين تناظريين، الأول يدعى مفتاح الشبكة وتتشاركه كل العقد مع BS وهو آخر مفتاح في سلسلة مفاتيح S مخزنة لدى BS حيث تتولد هذه السلسلة من تطبيق تابع الاختزال وحيد الاتجاه one way hash function عدة مرات على مفتاح ابتدائي K0 يتم تزويد BS به عند بداية تشكيل الشبكة كما توضح العلاقة (3)[9]، والثاني هو مفتاح مشترك بين كل عقدة و الBS.

$$(S = k_0, k_1, \dots, k_{j-1}, k_j \text{ where } f(k_j) = k_{j+1}) \quad \dots\dots (3)$$

حيث تحتفظ BS بالسلسلة بشكل سري لديها وتتشارك مع العقد المفتاح الأخير منها فقط في كل دورة.

مرحلة الإعداد Set-up phase:

1-1- يقوم الCH ببناء رسالة تحوي معرفه و sec_adv و عداد Counter مشترك مع BS وقيمة mac للرسالة يتم حسابها باستخدام المفتاح المشترك مع BS ، ثم يقوم ببث عام لهذه الرسالة إلى كل العقد المجاورة.

بدورها العقد تحتفظ بمعرفات رسائل الإعلام التي تصلها، وتقوم BS بإعادة حساب قيمة mac لكل رسالة تصلها فإذا حصلت على نفس النتيجة يكون CH موثوق وتضع المعرف الخاص به ضمن لائحة V تحوي معرفات الCHs الموثوقة.

1-2- تقوم BS بإرسال اللائحة V إلى كل العقد برسالة بث عام مع قيمة mac يتم حسابها باستخدام آخر مفتاح في سلسلة مفاتيح S مخزنة لديها.

1-3- كما ترسل هذا المفتاح أيضاً برسالة بث عام، وتحذفه من السلسلة S.

بدورها كل عقدة تتحقق من صلاحية المفتاح عبر تطبيق التابع وحيد الاتجاه f عليه فإذا نتج عنه المفتاح الموجود لديها مسبقاً فهو مفتاح صالح، وتستخدمه لحساب mac اللائحة V والتحقق منها، وبهذه الطريقة أصبحت العقد تمتلك معرفات الCHs الموثوقة في الشبكة، وتختار CH المناسب حسب قوة إشارة رسالة الإعلام المستلمة.

2- تقوم كل عقدة ببناء رسالة تحوي طلب انضمام join-req مع معرف العقدة ومعرف الرأس المناسب، وترسل هذه الرسالة إليه.

3- يقوم CH وعقده بتوليد مفتاح ثنائي مشترك بينه وبين كل عقدة في عنقوده من دون تكاليف اتصال إضافية بعد إرسال رسالة طلب الانضمام من خلال تابع لتوليد المفتاح باستخدام بروتوكول إدارة المفاتيح LEAP [16].

4- يقوم CH بإرسال رسالة الجدول الزمني مشفرة إلى كل عقدة في عنقوده باستخدام المفتاح المشترك مع كل عقدة ويتم توليد قيمة mac للرسالة المشفرة باستخدام نفس المفتاح.

مرحلة الاستقرار Steady-State:

5- تقوم كل عقدة بتشفير البيانات التي التقطتها باستخدام المفتاح الثنائي المشترك مع CH، وتولد قيمة mac للبيانات المشفرة باستخدام نفس المفتاح.

6- يقوم CH بتجميع البيانات التي التقطها من العقد الأعضاء ويضعها مع معرفه في رسالة يشفرها باستخدام المفتاح المشترك مع BS، إضافة إلى توليد قيمة mac للرسالة المشفرة باستخدام نفس المفتاح.

التحليل الأمني للبروتوكول MS-LEACH:

يعاني هذا البروتوكول من الثغرات التالية [9]:

1- لا يؤمن عملية المصادقة لتوثيق رسالة طلب الانضمام join-req، وهذا يسمح لأي مهاجم بإرسال طلب انضمام لأي CH في الشبكة، وعلى الرغم من أن المهاجم لا يمتلك آخر مفتاح في السلسلة S ليقوم بتوليد مفتاح مشترك مع CH وبالتالي لا يمكنه فك تشفير رسالة الجدول الزمني، إلا أن CH قام بتخصيص فاصل زمني للمهاجم في الجدول الزمني، وهذا يسبب تعطيل لعمل الشبكة.

2- بالرغم من أن رسالة الجدول الزمني مشفرة ومحمية من التعديل، إلا أنها رسالة فردية من CH إلى كل عقدة في عنقوده على حدى وهذا يسبب استنزاف طاقة CH بشكل كبير.

ويوضح الجدول (2) الخدمات الأمنية التي يوفرها كل من البروتوكولين MS-LEACH و SecLEACH:

الجدول (2): الخدمات الأمنية التي يوفرها كل من البروتوكولين MS-LEACH و SecLEACH

الخدمات الأمنية	SecLEACH	MS-LEACH
سلامة البيانات	من خلال إضافة قيمة MAC إلى الرسالة	من خلال إضافة قيمة MAC إلى الرسالة
المصادقة بين العقد	من خلال إضافة قيمة MAC إلى الرسالة	من خلال إضافة قيمة MAC إلى الرسالة
سرية البيانات	غير محققة	من خلال خوارزميات التشفير المتناظر
حداثة الرسائل	من خلال عداد	من خلال عداد

كلفة الاتصال في شبكات الحساسات اللاسلكية وتأثرها بتقنيات الأمن:

لقياس كلفة الاتصال يجب معرفة حجم الرسالة ومسافة الإرسال، ويمكن توضيح كلفة الاتصال في عمليتي إرسال واستقبال رسالة مؤلفة من K-bit وعلى مسافة d عن الهدف، وفق العلاقة (4) [17]:

$$E_{\text{trans}}(k,d) = \begin{cases} kE_{\text{elec}} + k\varepsilon_{fs}d^2 & (d < d_0), \\ kE_{\text{elec}} + k\varepsilon_{mp}d^4 & (d \geq d_0). \end{cases} \quad \ldots. (4)$$

حيث Eelec=ETX=ERX تمثلان طاقتا الإرسال والاستقبال للبت الواحد على الترتيب، Efs طاقة المضخم لنقل بت واحد على مسافات قصيرة free space, و Emp طاقة المضخم لنقل بت واحد على مسافات الكبيرة multipath fadedوالعتبة d0= Sqrt(Efs/Emp) ويتم تمييز حالتين:

1-d0 =< d: أي المسافة بين المرسل والمستقبل أكبر من العتبة، وبالتالي الطاقة المستهلكة من كل عقدة في الإرسال كبيرة.

2-d0 > d: أي المسافة بين المرسل والمستقبل أصغر من العتبة.

إن الطاقة المستهلكة في خوارزميات التشفير المتناظر تتأثر بحجم مفتاح التشفير وحجم البيانات المدخلة إلى الخوارزمية وعدد الدورات، لذلك يمكن التعبير عن الطاقة الكلية المستهلكة في نقل البيانات الآمنة عبر الشبكة

TotalSecureDataCommEnergy من خلال عملية جمع الطاقة المستهلكة في التشفير والطاقة المستهلكة في المصادقة والطاقة المستهلكة في إرسال البيانات كما توضح العلاقة (5) [18]:

TotalSecureDataCommEnergy=[DataSize×(EncryptionEnergy{keysize,Block-)Size, Encryption Rounds})]+MAC Energy +Transmission-Energy ….. (5)

حيث: DataSize تمثل حجم البيانات، EncryptionEnergy تمثل الطاقة المستهلكة في التشفير، MACEnergy تمثل الطاقة المستهلكة في توليد قيمة MAC ، Transmission–Energy تمثل الطاقة المستهلكة في الإرسال.

يوضح الجدول (3) الطاقة المستهلكة لبعض تقنيات التشفير والمصادقة من اجل نوعين مختلفين من الحساسات [11]:

الجدول (3): الطاقة المستهلكة لبعض خوارزميات التشفير وتقنيات المصادقة

	Security technique	Energy per 128 bit data block (µJ)					
		MicaZ			TelosB		
Block Cipher Techniques	AES	146.6			425.49		
	RC5	137.92			58.26		
	Skipjack	27.58			13.3		
MAC Techniques		AES	RC5	Skipjack	AES	RC5	Skipjack
	CBC-MAC	160.39	178.78	123.61	112.2	98.45	75.97
	HMAC	278.39			57.37		

الدراسة التجريبية:

سنقوم في هذا القسم ببناء سيناريوهين أساسيين، سنقوم في السيناريو الأول بتقييم أداء البروتوكولين SecLEACH و MS–LEACH في مرحلة الاستقرار، بينما سنقوم في السيناريو الثاني بدراسة تأثير تغيير التقنيات الأمنية المستخدمة في البروتوكول MS–LEACH على زمن حياة الشبكة، وذلك من أجل عقد حساسات ثابتة، وسنستخدم برنامج ماتلاب للحصول على النتائج.

يوضح الجدول (4) قيم البارامترات المستخدمة من أجل كل من نموذجي الشبكة والطاقة المستخدمين في المحاكاة:

الجدول (4) القيم العددية المتعلقة بنموذج الشبكة ونموذج الطاقة المستخدمين في عملية المحاكاة

مساحة الشبكةmxm	100x100
عدد العقد الكلي n	100
موقع المحطة القاعدية BS (x,y)	(50X120)
احتمالية أن تكون العقدة CH (p)	0.05
الطاقة الابتدائية التي تزود بها كل عقدة (E0)	1J
طاقة الإرسال للبت الواحد ETX	50*0.000000001J

طاقة الاستقبال للبت الواحد ERX	50*0.000000001J
طاقة تجميع البيانات للبت الواحد EDA	5*0.000000001J
حجم الباكيت التي يتم إرسالها من العقد	4096 bit
طاقة المضخم للمسافات القصيرة للبت الواحد Efs	10 p j / bit / m^2
طاقة المضخم للمسافات الكبيرة للبت الواحد Emp	0.0013 p j / bit /m^4
العتبة d0	Sqt(Efs/Emp)

مقاييس الأداء:

سنقوم في هذا البحث بتقييم الأداء بالاعتماد على مقياسين أساسيين هما: عدد العقد الحية والطاقة المتبقية، ويعرفان كما يلي:

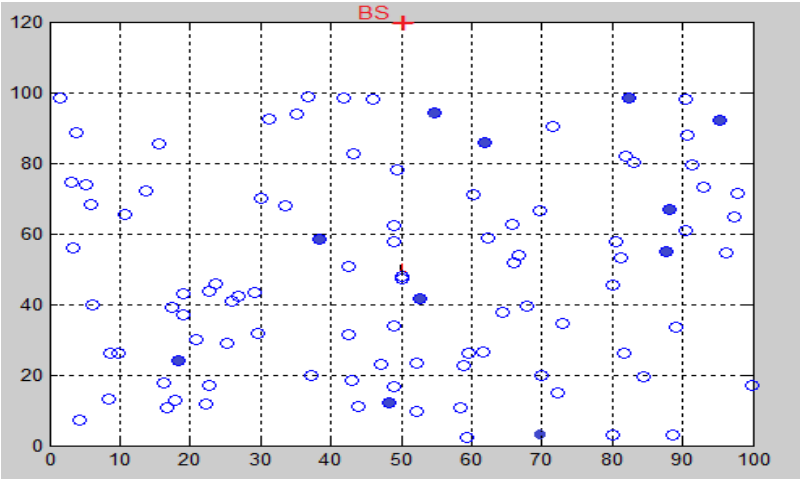
- **عدد العقد الحية في الشبكة Number of alive nodes:** ويقصد به عدد عقد الحساسات التي لم تفقد كامل طاقتها بعد في كل دورة زمنية.
- **الطاقة المتبقية في الشبكة Remaining Energy:** وهي مجموع الطاقات المتبقية في كل عقدة من أجل كل دورة زمنية.

السيناريو الأول: تقييم أداء البروتوكولين SecLEACH و MS-LEACH في مرحلة الاستقرار:

قمنا بدايةً ببناء نموذج لشبكة WSN وفقاً للجدول (4) والجدول (3) تستخدم البروتوكول SecLEACH كبروتوكول توجيه ونموذج آخر لنفس الشبكة ولكن مع تغيير بروتوكول التوجيه ليصبح MS-LEACH.

إن الفرق بين البروتوكولين SecLEACH و MS-LEACH في مرحلة الاستقرار Steady-state هو أن البروتوكول SecLEACH يستخدم تقنية AES-CBC-MAC كآلية حماية لضمان سلامة الرسائل المتبادلة من أي تعديل وتحقيق المصادقة بين العقد المتراسلة، بينما يستخدم البروتوكول MS-LEACH خوارزمية التشفير المتناظر AES لتحقيق سرية البيانات بالإضافة إلى استخدامه تقنية AES-CBC-MAC لمصادقة العقد وضمان سلامة الرسائل.

ويوضح الشكل (6) نموذج شبكة الحساسات اللاسلكية الثابتة التي تم بناؤها وذلك بعد مرحلة الإعداد واختيار رؤوس العناقيد:

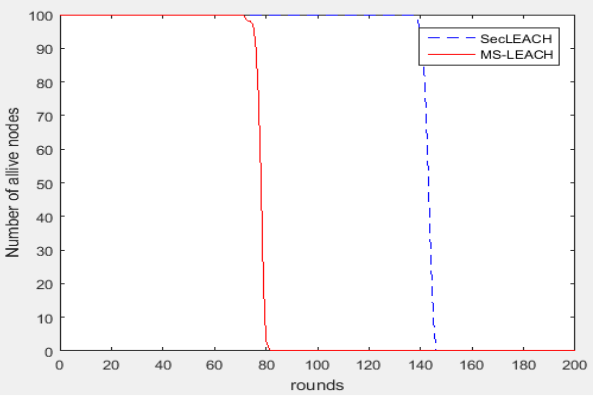


الشكل (6): اختيار رؤوس العناقيد في شبكة الحساسات اللاسلكية

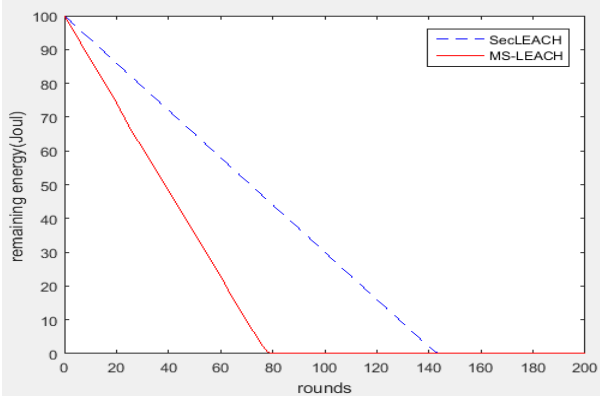
حيث: تمثل + المحطة القاعدية BS، تمثل O عقد الحساسات، تمثل ● رؤوس العناقيد.

سنقوم في المحاكاة بالاعتماد على نموذج الطاقة الموضح في العلاقات (4) و (5) وذلك لحساب الطاقة المتبقية في كل عقدة من أجل كل دورة، حيث تتوقف المحاكاة عند نفاذ طاقة جميع العقد في الشبكة.

يظهر كلاً من الشكلين (7) و (8) أن استخدام البروتوكول SecLEACH في الشبكة أفضل من البروتوكول MS–LEACH من حيث استهلاك الطاقة، حيث استمرت الشبكة بالعمل حتى 140 دورة زمنية تقريباً، بينما كان عمر الشبكة 80 دورة عند استخدام MS–LEACH:



الشكل (7): مقارنة بين SecLEACH و MS–LEACH من حيث عدد العقد الحية



الشكل (8): مقارنة بين SecLEACH و MS–LEACH من حيث الطاقة المتبقية

ويعود السبب في ذلك إلى أن البروتوكول SecLEACH لا يستخدم خوارزمية تشفير لضمان سرية البيانات المنقولة بين العقد، بينما يستخدم البروتوكول MS–LEACH خوارزمية التشفير المتناظر AES الأمر الذي أدى إلى استهلاك طاقة إضافية لتشفير البيانات وتوفير سريتها وذلك مبرر في حال تطلب التطبيق الذي نشرت من أجله شبكة WSN ذلك.

ويمكن تلخيص النتائج في الجدول (5):

الجدول (5): عدد الدورات الزمنية لعمل الشبكة في السيناريو الأول

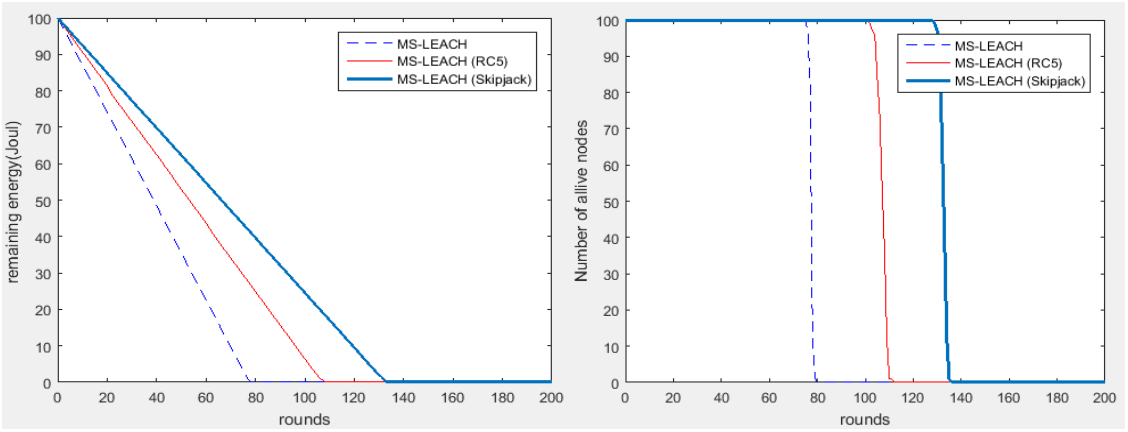
البروتوكول الآمن	SecLEACH	MS–LEACH
عمر الشبكة مقدراً بعدد الدورات الزمنية	140	80

السيناريو الثاني: دراسة تأثير تغيير التقنيات الأمنية المستخدمة في البروتوكول MS–LEACH على استهلاك الطاقة:

نعلم أن البروتوكول MS–LEACH أفضل من البروتوكول SecLEACH بالرغم من أنه يستهلك طاقة إضافية وذلك بسبب المستوى الأمني الجيد الذي يحققه للشبكة. سنقوم في هذا السيناريو بدراسة تأثير استخدام تقنيات أمنية مختلفة (خوارزميات التشفير وتقنيات المصادقة) في البروتوكول MS–LEACH، وذلك من أجل بارامترات الشبكة ذاتها التي تم تحديدها في الجدول (4)، وبالاعتماد على القيم في الجدول (3) والتي تعبر عن الطاقة المستهلكة عند تنفيذ عدة تقنيات أمنية في حساسات TelosB:

سنقوم أولاً باستبدال خوارزمية التشفير المستخدمة في MS-LEACH بخوارزمية RC5 ، ومن ثم سنقوم بتغيير خوارزمية التشفير لتصبح Skipjack، وذلك مع ترك تقنية المصادقة كما هي حيث سنقوم بحساب الطاقة المتبقية في كل عقدة من أجل الحالتين السابقتين:

فنلاحظ من الشكلين (9) و (10) أن كفاءة استهلاك الطاقة في الشبكة أصبحت أفضل وطال عمر الشبكة بمقدار 30 دورة زمنية عند استخدام خوارزمية RC5 في تشفير البيانات مقارنةً بالبروتوكول الأصلي حيث تستمر الشبكة بالعمل حتى 110 دورات زمنية تقريباً.



الشكل (9): عدد العقد الحية عند تغيير خوارزمية التشفير المستخدمة في MS-LEACH

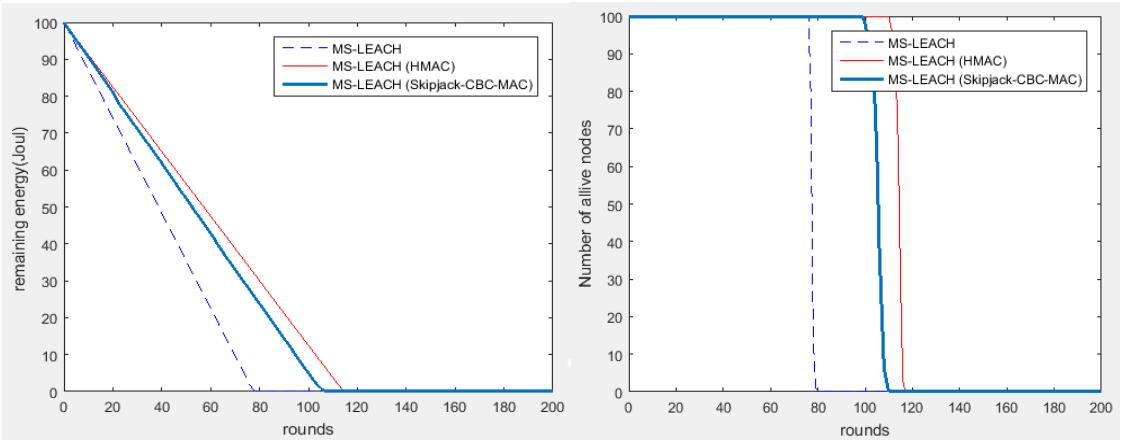
الشكل (10): الطاقة المتبقية عند تغيير خوارزمية التشفير المستخدمة في MS-LEACH

كما يظهر الشكلين السابقين أن استخدام الخوارزمية التشفير Skipjack كان لها التأثير الأفضل حيث أنها قللت من استهلاك الطاقة وأطالت عمر الشبكة بمقدار 55 دورة مقارنةً بالبروتوكول الأصلي حيث تستمر الشبكة بالعمل حتى 135 دورات زمنية تقريباً.

ويعود السبب في ذلك إلى أن الخوارزمية RC5 تستهلك طاقة أقل في مرحلة تشفير البيانات مقارنةً بالخوارزمية AES لاستغراقها زمن أقل في التنفيذ [13]، أما بالنسبة للخوارزمية Skipjack فهي تحقق الاستهلاك الأقل في الطاقة لأنها لا تتضمن مرحلة إعداد مفتاح key-setup وبالتالي لا يوجد طاقة إضافية مستهلكة لإعداد مفتاح التشفير كما في خوارزميتي التشفير AES و RC5.

سنقوم الآن بدراسة تأثير استخدام تقنيات المصادقة Skipjack-CBC-MAC و HMAC في البروتوكول MS-LEACH مع ترك خوارزمية التشفير كما هي، وذلك لدراسة استهلاك كل منها للطاقة في الشبكة:

فنلاحظ من الشكلين (11) و(12) أن البروتوكول MS-LEACH يستهلك الطاقة الأقل عند استخدام لتقنية المصادقة HMAC حيث تستمر الشبكة بالعمل حتى 120 دورة زمنية تقريباً، بينما توقفت الشبكة عن العمل في الدورة 110 عند استخدام Skipjack-CBC-MAC كتقنية للمصادقة، حيث حسنت كل من التقنيتين من كفاءة استهلاك الطاقة في الشبكة بالمقارنة مع البروتوكول الأصلي:



الشكل (11): عدد العقد الحية عند تغيير تقنية المصادقة المستخدمة في MS–LEACH

الشكل (12): الطاقة المتبقية عند تغيير تقنية المصادقة المستخدمة في MS–LEACH

ويعود السبب في ذلك إلى أن تقنية HMAC تستخدم تابع الاختزال MD5 الذي يعد أقل استهلاكاً للطاقة مقارنة بتوابع الاختزال وخوارزميات التشفير الأخرى، فهو من أول توابع الاختزال التي ظهرت ومع تطور توابع الاختزال يزيد تعقيد العمليات الحسابية فيها ويزيد استهلاكها للطاقة.

الاستنتاجات والتوصيات:

نستنتج مما سبق ما يلي:

1- إن طرائق تحقيق الأمن المستخدمة من خوارزميات التشفير وتقنيات المصادقة تؤثر بشكل كبير على كمية الطاقة المستهلكة من قبل العقد في شبكة الحساسات اللاسلكية وبالتالي تؤثر على زمن حياة الشبكة، وكلما زاد عدد التقنيات الأمنية المستخدمة في آلية عمل البروتوكول يزيد استهلاك الطاقة وينخفض زمن حياة الشبكة.

2- يتم اختيار البروتوكول الآمن الملائم وفقاً للمتطلبات الأمنية التي يراد تحقيقها في التطبيق الذي تعمل فيه الشبكة، حيث لاحظنا أن بروتوكول SecLEACH يستهلك طاقة أقل مقارنةً بالبروتوكول MS–LEACH لأن التقنيات الأمنية المستخدمة فيه أقل، لكن البروتوكول MS–LEACH يتمتع بمزايا أمنية أكبر وبالتالي فإن الطاقة الإضافية المستهلكة هي نتيجة المستوى الأمني الجيد الذي يوفره للشبكة.

3- يفضل استخدام بروتوكول SecLEACH إذا كان المطلب الأمني هو ضمان سلامة البيانات المتناقلة والمصادقة المتبادلة بين العقد في شبكة الحساسات اللاسلكية، واستخدام بروتوكول MS–LEACH إذا كان المطلب الأمني هو ضمان سلامة البيانات المتناقلة والمصادقة المتبادلة بين العقد وتحقيق سرية البيانات المنقولة في شبكة الحساسات اللاسلكية.

4- يمكن تغيير التقنيات الأمنية المستخدمة ضمن البروتوكول MS–LEACH بهدف تقليل الطاقة المستهلكة وإطالة زمن حياة الشبكة، بحيث نستخدم خوارزمية Skipjack للتشفير و HMAC للمصادقة.

References:

[1] Adrian Carlos Ferreira, Marcos Aur´elio Vilaca , Leonardo B. Oliveira, Eduardo Habib, Hao Chi Wong, Antonio A.Loureiro, On the Security of Cluster-based

Communication Protocols for Wireless Sensor Networks, 4th IEEE international Conference on Networking (ICN.05), volume 3420 of Lecture Notes in Computer Science, Reunion Island, pages 449.458, April 2005.
[2] Leonardo B. Oliveira, Hao C. Wong, M. Bern, Ricardo Dahab, A. A. F. Loureiro, SecLEACH – A Random Key Distribution Solution for Securing Clustered Sensor Networks, Fifth IEEE International Symposium on Network Computing and Applications, 2006.
[3] Mona El_Saadawy, Eman Shaaban, Enhancing S-LEACH Security for Wireless Sensor Networks, IEEE International Symposium on Network Computing and Applications, 2012.
[4] K. Ravi Kishore, N.V.S. Narasimha Sarma, AES based secure low energy adaptive clustering hierarchy for WSN's ,International Conference on Communication and Electronics System Design, 2013.
[5] Prof. P. Sasikumar, Prof. K. S. Preetha, Performance analysis of secure leach based clustering protocol in wireless sensor networks, International Journal of Applied Engineering Research ISSN 0973-4562 Volume 10, Number 14 (2015), January 2015.
[6] Deepika, Manpreet, A Research Paper on Security Enhancement In Leach Protocol, International Journal of Engineering Development and Research (Volume 4) ,2016.
[7] Deeksha Verma, Arun Kumar Tripathi, Efficient Cluster based Adaptive Routing for Wireless Sensor Network, Communications on Applied Electronics (CAE) – ISSN : 2394-4714 Foundation of Computer Science FCS, New York, USA Volume 1– No.3, February 2015.
[8] Mohammad Masdari, Sadegh Mohammadzadeh Bazarchi, Moazam Bidaki, Analysis of Secure LEACH-Based Clustering Protocols in Wireless Sensor Networks, Journal of Network and Computer Applications 36 (2013).
[9] Triana Mugia Rahayu, Sang-Gon Lee, Hoon-Jae Lee, Survey on LEACH-based Security Protocols, ISBN 978-89-968650-2-5, ICACT2014, February 2014.
[10] Madhumita Panda, Security in Wireless Sensor Networks using Cryptographic Techniques, American Journal of Engineering Research (AJER) e-ISSN : 2320-0847 p-ISSN : 2320-0936 Volume-03, Issue-01, pp-50-56,2014.
[11] Iman Almomani, Maha Saadeh, Security Model for Tree-based Routing in Wireless Sensor Networks: Structure and Evaluation, KSII TRANSACTIONS ON INTERNET AND INFORMATION SYSTEMS VOL. 6, NO. 4, 26 December 2014.
[12] Madhumita Panda, Data Security in Wireless Sensor Networks via AES Algorithm, IEEE Sponsored 9th International Conference on Intelligent Systems and Control (ISCO), 2015.
[13] Jongdeog Lee, Krasimira Kapitanova, Sang H. Son, The price of security in wireless sensor networks, Computer Networks 54 (2010) 2967–2978, doi:10.1016/j.comnet.2010.05.011, 2010.
[14] Prof. Dr.-Ing. Christof Paar, Dr.-Ing. Jan Pelzl , Understanding Cryptography A Textbook for Students and Practitioners, Springer-Verlag Berlin Heidelberg 2010.
[15] Syeda Iffat Naqvi, Adeel Akram, Pseudo-random Key Generation for Secure HMAC-MDS, 978-1-61284-486-2/111$26.00 ©2011 IEEE,2011.
[16] Delan Alsoufi, Khaled Elleithy, Tariq Abuzaghleh, Ahmad Nassar, SECURITY IN WIRELESS SENSOR NETWORKS – IMPROVING THE LEAP PROTOCOL, International Journal of Computer Science & Engineering Survey (IJCSES) Vol.3, No.3, June 2012.
[17] Fuzhe Zhao, You Xu, Ru Li, Improved LEACH Routing Communication Protocol for a Wireless Sensor Network, International Journal of Distributed Sensor Networks, 19 November 2012.
[18] M. Razvi Doomun, KM Sunjiv Soyjaudah, Devesh Bundhoo, Energy Consumption and Computational Analysis of Rijndael-AES, IEEE, 2008.

[19] Brian D. Caravantes, Enhancements of Security in Wireless Sensor Networks, UMM CSci Senior Seminar Conference, April 2018.
[20] Chung-Wen Hung,Wen-Ting Hsu, Power Consumption and Calculation Requirement Analysis of AES for WSN IoT, Sensors 2018, 18, 1675; doi:10.3390/s18061675, 23 May 2018.