مجلة جامعة تشرين للبحوث والدراسات العلمية _ سلسلة العلوم الهندسية المجلد (40) العدد (4) 2018
Tishreen University Journal for Research and Scientific Studies - Engineering Sciences Series Vol. (40) No. (4) 2018

تحسين التجميع الآمن للبيانات في شبكات الحساسات اللاسلكية المتنقلة

د. بشرى معلا•
حلا محمد••

(تاريخ الإيداع 19 / 4 / 2018. قُبِل للنشر في 19/ 7 / 2018)

□ ملخّص □

تمثل شبكات الحساسات اللاسلكية المتنقلة تقنية حديثة جذبت الباحثين نظراً لمزاياها وتطبيقاتها المتعددة في مختلف المجالات. تعد خوارزميات التجميع في هذه الشبكات التقنية الأكثر تطبيقاً من أجل تقليل عدد الرزم المرسلة في الشبكة وذلك بسبب محدودية مصادر العقد الحساسة من حيث طاقة الإرسال، مدى الاتصال وحجم الذاكرة. وقد جعلت خصائص هذا النوع من الشبكات مثل الاتصال اللاسلكي والنشر في بيئات غير متحكم بها هدفاً سهلاً للهجمات. لذلك يعد الأمن قضية جوهرية لشبكات الحساسات اللاسلكية المتنقلة لحماية المعلومات من التطفل والهجوم.

نقدم في هذا البحث خوارزمية تجميع آمن للبيانات في شبكات الحساسات اللاسلكية المتنقلة. تعتمد هذه الخوارزمية على تقنية المفاتيح الثنائية وعلى تابع البعثرة. بهدف تقييم أداء الخوارزمية المقترحة تمت دراسة عدد من البارامترات الهامة وهي زمن التنفيذ والتأخير نهاية إلى نهاية إضافة إلى عدد المفاتيح المخزنة. وقد أظهرت النتائج أن الخوارزمية المقترحة قد قدمت أداءً جيداً من الناحية الأمنية والتأخير الزمني.

الكلمات المفتاحية : شبكات الحساسات اللاسلكية المتنقلة، التجميع الآمن للبيانات، خوارزمية المفاتيح الثنائية المعدلة المعتمدة على تجميع البيانات.

• أستاذ مساعد، قسم هندسة الاتصالات والالكترونيات، كلية الهندسة الميكانيكية والكهربائية، جامعة تشرين، اللاذقية، سوريا
•• طالبة ماجستير، قسم هندسة الاتصالات والالكترونيات، كلية الهندسة الميكانيكية والكهربائية، جامعة تشرين، اللاذقية، سوريا

مجلة جامعة تشرين للبحوث والدراسات العلمية _ سلسلة العلوم الهندسية المجلد (40) العدد (4) 2018
Tishreen University Journal for Research and Scientific Studies - Engineering Sciences Series Vol. (40) No. (4) 2018

Enhancend Secure Data Aggregation In Mobile Wireless Sensor Networks (MWSNs)

Dr. Boushra Maala*
Halla Mohammed**

(Received 19 / 4 / 2018. Accepted 19 / 7 / 2018)

□ ABSTRACT □

Mobile Wireless Sensor Network (MWSN) is an emerging technology for attraction of researchers with its research advantage and various application domains. Due to limited resources of sensor nodes such as transmission power, communication capability and size of memory, data aggregation algorithms are the most practical technique that reduces large amount of transmission in this network. Security is an important criterion to be considered because, wireless sensor nodes are deployed in a remote or hostile environment area that is prone to attacks easily. Therefore, security are essential issue for MWSN to protect information against attacks.

In this research, we offered an algorithm of secure data aggregation in MWSN based on pair-wise keys technology and hash function. We studied important parameters such as execution time, end-to-end delay and number of storied keys. Results showed that our suggested algorithm has a good performance in security issues and end-to-end delay.

Keywords: mobile wireless sensor networks، secure data aggregation, modified pair-wise key based data aggregation algorithm (PWDA).

* **Assistant Professor, Department of Communication and Electronics, Factually of Mechanical and Electrical Engineering, Tishreen University, Lattakia, Syria.**
****Postgraduate Student, Department of Communication and Electronics, Factually of Mechanical and Electrical Engineering, Tishreen University, Lattakia, Syria**

مقدّمة:

تعد شبكات الحساسات اللاسلكية المتنقلة Mobile Wireless Sensor Network (MWSN) جيلاً جديداً مطوَّراً عن شبكات الحساسات اللاسلكية الثابتة. تتحسس العقد الحساسة للبيئة المحيطة ومن ثم تنقل البيانات لاسلكياً إلى مركز المعالجة الرئيسي. تعتمد هذه الشبكات على وجود حركية ضمن الشبكة سواء من العقد الحساسة أو من مركز المعالجة الرئيسي وذلك حسب نموذج قابلية الحركية المستخدم[1,2,3,4] . تم اقتراح هذا النموذج من الشبكات من أجل تجاوز مشكلة استهلاك الطاقة كهدف أساسي ومحاولة تحسين أداء هذا النوع من الشبكات بهدف إطالة عمر الشبكة. تستخدم شبكاتMWSNs في تطبيقات هامة وحساسة[1,3,5] قد تتعلق بالحياة كالتطبيقات الصحية أو بأمن الدول كالتطبيقات العسكرية. وقد جعلت خصائص هذا النوع من الشبكات مثل الاتصال اللاسلكي والنشر في بيئات غير متحكم بها هدفاً سهلاً لعدة نماذج من الهجمات، تؤدي هذه الهجمات في بعض الأحيان إلى إيقاف التطبيق بشكل كامل، أو تتسبب في وصول معلومات معدلة تؤدي إلى اتخاذ قرار خاطئ من قبل المعنيين بالتطبيق. وخاصة عند تطبيق عمليات التجميع على البيانات المرسلة، مما يجعل إمكانية اكتشاف تعديل هذه البيانات أمراً صعباً، هذا ما من جعل الضروري إيجاد خوارزميات تجميع آمن للبيانات لحماية المعلومات من التطفل والهجوم، وتضمن وصول المعلومات بشكل صحيح وموثوق، وتحقق متطلبات الأمن الأساسية في الشبكة.

أهمية البحث وأهدافه :

تأتي أهمية هذا البحث من حيث أنه يتناول موضوعاً حديثاً نسبياً. تتركز الدراسات لإيجاد خوارزميات للتجميع الآمن للبيانات في شبكات الحساسات اللاسلكية مع إمكانية إضافة قابلية الحركة للعقد الحساسة. حيث افترضت معظم الأبحاث في هذا المجال أن العقد الحساسة في الشبكة هي عقد ثابتة، وبالتالي تعاني من مشكلة التأخير الزمني.

يهدف هذا البحث إلى إيجاد خوارزمية تجميع آمن للبيانات مع إمكانية إضافة قابلية الحركة للعقد بحيث يكون التأخير الزمني أقل ما يمكن مع ضمان المتطلبات الأساسية للأمن وتقييم أداء هذه الخوارزمية.

طرائق البحث ومواده:

طبق سيناريو المحاكاة على برنامج NS-2 الإصدار2.35. ويعد هذا المحاكي غنياً جداً بالعديد من مكونات وبروتوكولات الشبكات التي يتم التعبير عنها بشكل غرضي Object، ويعتمد في عمله داخلياً على لغات C++، OTCL.

إن NS هو اختصار لـ (Network Simulator) وهو محاكي شبكات شائع جداً ومتاح للعموم. حيث يقوم بنمذجة النظام كأحداث نقوم بمحاكاتها، حيث كل حدث يحدث في لحظة زمنية افتراضية ويأخذ قيمة عشوائية من الزمن الحقيقي. إنه عبارة عن حزمة برمجية مفتوحة المصدر وتم بناؤه ليعمل على نظام التشغيل لينوكس، ويعد هذا المحاكي من أكثر المحاكيات الشبكية استخداماً.

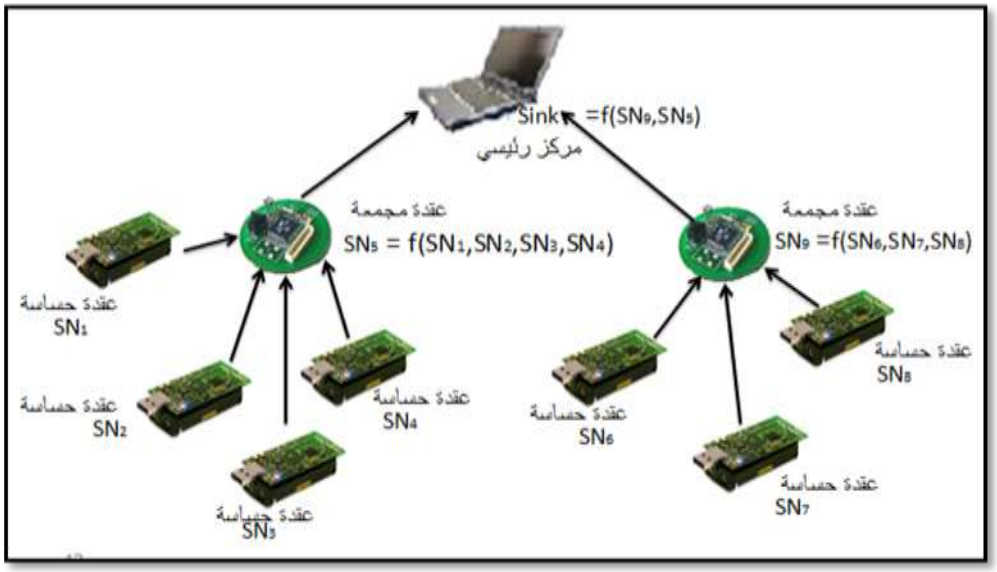
التجميع الآمن للبيانات :

إن تجميع البيانات عبارة عن عملية يتم فيها جمع بيانات الحساسات، حيث تقوم عقد تدعى بالعقد المجمعة بتجميع البيانات من عدة عقد ومن ثم إرسالها إلى مركز المعالجة الرئيسي لتقليل حجم البيانات التي يتم إرسالها ضمن الشبكة بدلاً من أن تقوم جميع عقد الشبكة بهذه العملية[4,6,7,8].

ويقصد بتجميع البيانات إما عملية الضغط لتقليل الحجم أو استخدام بعض الحسابات الرياضية كالمتوسط الحسابي للبيانات الواصلة إلى العقدة المجمعة أو حساب القيمة الأعظمية أو أي عمليات أو توابع رياضية أخرى، حيث تتميز هذه الآلية بتقليل كلفة الاتصالات لأنها تقلل من استهلاك الطاقة وكذلك من حجم الذاكرة المستخدم، ولكنها تعاني من زيادة في التأخير الزمني[7,9,10,11,12]. يبين الشكل(1) تجميع البيانات في شبكات الحساسات اللاسلكية.

وكما ذكرنا سابقاً، تستخدم شبكات MWSNs في تطبيقات هامة وحساسة قد تتعلق بالحياة كالتطبيقات الصحية أو بأمن الدول كالتطبيقات العسكرية، لذلك يعد الأمن قضية جوهرية لحماية المعلومات من التطفل والهجوم.

هناك دراسات مرجعية كثيرة حول تطبيق تقنية التجميع الآمن للبيانات في شبكات الحساسات اللاسلكية الثابتة، لكن التحدي الأساسي يكون بتطبيق هذه التقنية مع إضافة قابلية الحركة للعقد الحساسة والذي بدأ العمل به حديثاً.



الشكل(1): تجميع البيانات في شبكات الحساسات اللاسلكية

الدراسات المرجعية:

أجريت العديد من الأبحاث والدراسات عن طرائق التجميع الآمن للبيانات في شبكات اللاسلكية الثابتة.

قام الباحثون في [13,14] بإجراء دراسة عن خوارزميات التجميع الآمن للبيانات وهي خوارزمية التشفير عقدة إلى عقدة(hop-to-hop)، حيث يتم التشفير و فك التشفير عند كل عقدة على طول مسار الشبكة. تمنع هذه الطريقة حصول الهجمات التي تقوم بحقن معلومات خاطئة في الشبكة، ولكنها تتطلب الكثير من عمليات التشفير وفكه في الشبكة وينتج عن ذلك وقت أطول للحصول على المعلومات.

في [15,16] اقترح الباحثون استخدام خوارزمية التشفير نهاية إلى نهاية أي عند عقدتي المصدر والهدف (end-to-end)، حيث يتم التشفير عند المصدر و فك التشفير عند الهدف. هنا تبقى البيانات سرية لا يعرفها إلا عقدتي

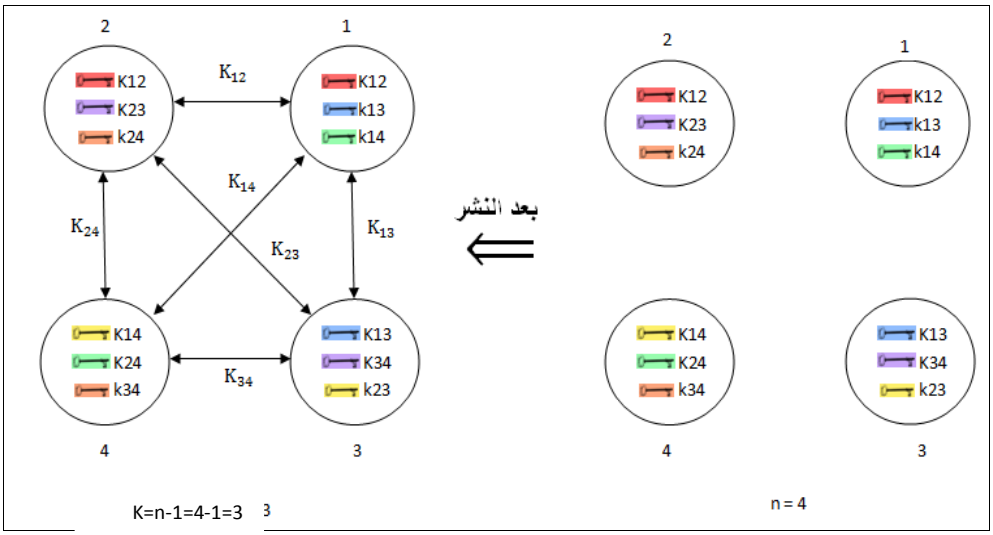
المصدر والهدف وأما بقية العقد فلا تستطيع قراءة البيانات بل تكتفي بتمريرها، ولكنها تسبب فائضاً كبيراً سيمرر عبر الشبكة.

أجرى الباحثون في [17] دراسة تطرح إمكانية التجميع الآمن للبيانات في شبكات الحساسات اللاسلكية بالاعتماد على النموذج المتعدد المجمعات، وكذلك على البنية الهرمية من أجل بناء شبكة الحساسات اللاسلكية. باستخدام هذا النموذج، تم التقليل من زمن التأخير حيث تم استبدال عمليات فك التشفير والتحقق بالمراحل الثلاث (البيانات المشفرة، التوقيع الرقمي، المفاتيح العامة) وكذلك التقليل من استهلاك الطاقة مما يؤدي إلى زيادة زمن حياة الشبكة، لكنها أدت إلى زيادة حجم الذاكرة المستخدم.

في [18] درس الباحثون إمكانية التجميع الآمن للبيانات في شبكات الحساسات اللاسلكية المتنقلة. و ذلك من خلال اقتراحهم لثلاثة بروتوكولات تجميع آمن للبيانات وهي TSP (Time Stamp Protocol), PPSP (Polynomial Points Sharing Protocol) and SSP (Secret Sharing Protocol) . تعتمد هذه البروتوكولات على شبكة حساسات هرمية Hierarchical Sensor Network (HSN) وتستخدم عقدة تدعى مجمع البيانات المتنقل Mobile Data Collector (MDC) تقوم بتجميع البيانات من قادة العناقيد ومن ثم نقلها لمركز المعالجة الرئيسي. يستخدم البروتوكول TSP الطابع الزمني(TS) لتمييز الرسائل المكررة وكذلك عمليات تشفير وفك تشفير بسيطة من أجل تحقيق عملية المصادقة بين قائد العنقود ومجمع البيانات المتنقل. أما البروتوكول PPSP، يستخدم عمليات تشفير وفك تشفير أكثر تعقيداً من البروتوكول TSP وذلك بالاعتماد على كثيرات الحدود المولدة عشوائياً. يدمج البروتوكول SSP بين آليتي البروتوكولين السابقين TSPوPPSP. يستخدم الطابع الزمني بالإضافة إلى عمليات تشفير وفك تشفير ذات درجة تعقيد عالية وذلك بالاعتماد على كثيرات الحدود المولدة عشوائياً. في هذه الدراسة يقدم كل من بروتوكولي PPSP وSSP درجة أمن ومقاومة أعلى ضد أي هجوم أو اختراق للشبكة وذلك من وجهة نظر التحليل الأمني أما بالنسبة لتحليل الطاقة يظهر بروتوكول TSP فعالية أكثر مقارنة مع PPSP و SSP حيث تستهلك عمليات التشفير وفك التشفير المستخدمة في هذين البروتوكولين طاقة أعلى، لكنها تعاني من زيادة زمن التأخير حيث يتم فك تشفير والتحقق من كل الرسائل المستقبلة في كل مرحلة.

الخوارزمية المقترحة:

يعتمد اقتراحنا على استخدام تقنية المفاتيح الثنائية (Pair-Wise)[11,19,20,21]، لذا أطلقنا عليه اسم PWDA (**P**air-**W**ise key based **D**ata **A**ggregation algorithm). في تقنية المفاتيح الثنائية تحمل عقد الشبكة بـ (N-1) مفتاحاً سرياً للتبادل مع بقية العقد(بفرض N العدد الكلي لعقد الشبكة) وذلك قبل مرحلة نشر العقد. يمثل الشكل(2) مثالاً يوضح الطريقة الأساسية لتقنية المفاتيح الثنائية.



الشكل(2): الطريقة الأساسية لتقنية المفاتيح الثنائية

يعود اختيار هذه التقنية إلى كون المفاتيح محملة بشكل مسبق في العقد وهذا يدعم توجهنا في مراعاة بارامتر التأخير الزمني. أي لا تستهلك زمن على عمليات توليد المفاتيح وتوزيعها على العقد لأن كل ذلك يتم قبل مرحلة النشر. كما أن السيطرة على عقدة يؤثر على وصلات هذه العقدة فقط دون غيرها.

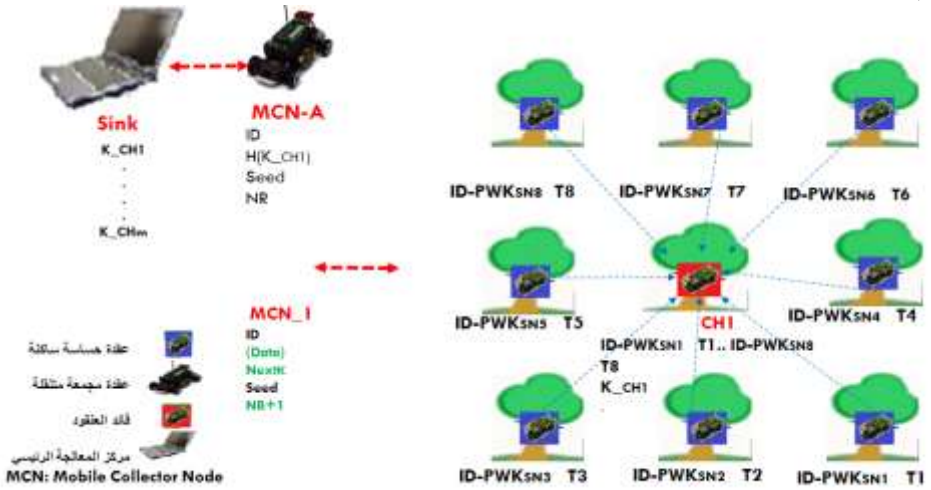
نموذج الشبكة:

تتألف شبكتنا الهجينة من N عقدة حساسة تم نشرها بشكل يدوي وضمن مواقع ذات أبعاد فاصلة متساوية لتعطي شكلاً منتظماً، وهذا يناسب التطبيقات الصحية مثلاً وتطبيقات المراقبة ضمن الأبنية أو حتى تطبيقات مراقبة الحرائق ضمن أماكن محددة المساحة كحديقة أو بستان. "وهي مكونة من نموذجين من العقد:

أ. عقد قوية: عقد قليلة العدد ذات طاقة عالية ومدى اتصال وقدرة تخزين كبيرة. تمثل هذه العقد قادة العناقيد (Cluster heads)CHs والعقد المجمعة المتنقلة (Mobile Collector Nodes)MCNs.

ب. عقد بسيطة: هي عقد كثيرة العدد ذات قدرة أقل من حيث الطاقة ومدى الاتصال والتخزين. تمثل هذه العقد عقد حساسة للوسط المحيط (Sensor Nodes) SNs.

يظهر الشكل(3) نموذجاً لهذه الشبكة.



الشكل(3): نموذج جزئي للشبكة

يراعي استخدام خوارزمية تجميع البيانات في نموذجنا المقترح محدودية مصادر العقد الحساسة ومنها تخفيض استهلاك الطاقة من خلال استخدام نمطين من عقد التجميع، العقدة المجمعة الأولى هي قائد العنقود ودورها تجميع القيم من عدة عقد، والعقدة المجمعة الثانية هي العقدة المجمعة المتنقلة والتي ستوفر إمكانية إرسال باستطاعة إرسال منخفضة من قبل قائد العنقود لأنها ستمر في نقطة أقرب ما يكون على قائد العنقود لجمع الرسائل عند توزيعها. فكما هو معلوم، كلما كان مدى الإرسال أكبر كلما كان استهلاك الطاقة أكبر.

آلية توزيع المفاتيح في الشبكة:

تبعاً لنموذج الشبكة المقترح فإنه بالإمكان توزيع المفاتيح على العقد قبل النشر بشكل دقيق يضمن الاتصال الآمن حيث يتم اعتماد طريقة تخزين ثنائية ولكن معدلة حيث:

- ستختزن كل عقدة حساسة مفتاح ثنائي لتتصل بشكل آمن باستخدامه مع قائد العنقود التابعة له فقط، لأننا نفترض عدم وجود اتصال بين العقد الحساسة لعدم الحاجة إليه.
- سيختزن قائد كل عنقود عدداً من المفاتيح الثنائية تساوي عدد العقد التي توجد في العنقود، إضافة إلى جميع المعلومات السرية اللازمة لتوليد مفتاح تشفير يستخدمه قائد العنقود لتشفير البيانات التي تصل إلى المركز مارة بالعقدة المجمعة المتنقلة ليصار إلى فك تشفيرها في المركز.
- يخزن المركز، وليس العقدة المجمعة المتنقلة، جميع المفاتيح المستخدمة لتشفير البيانات الخارجة من قادة العناقيد، لأننا نفترض أن فك التشفير يتم في المركز وليس في العقدة المجمعة المتنقلة.

الهدف من ذلك جعل التطبيق أكثر أمناً في حال تم السيطرة على العقدة المجمعة المتنقلة فالمركز هو عقدة آمنة في معظم النماذج المقترحة.

مراحل عمل الشبكة:

باعتمادنا السيناريو السابق، ستكون الخوارزمية المطبقة مكونة من ثلاث مراحل بهدف الحصول على تجميع آمن للبيانات.

1 مرحلة التحسس:

تتحسس العقد ضمن العنقود لدرجة الحرارة T (Temperature) ثم تشفرها بالمفتاح الثنائي المشترك بينها وبين قائد العنقود التابعة له وترسلها له، نرمز لهذا المفتاح بـ (Pair-Wise Key$_{\text{Sensor Nodei-Cluster Headj}}$) PWK$_{\text{SNi-CHj}}$.

بهدف خفض استهلاك الطاقة، اعتمدنا في عملية إرسال القيم المتحسسة على أن العقدة لا ترسل القيم المتكررة لقراءات متتالية. فعندما ترسل قيمة ما لا تعيد عملية إرسال نفس القيمة لمرتين متتاليتين.

من الناحية الأمنية، إن استخدام هذا المفتاح الثنائي يجعل متطلب الموثوقية محقق من حيث أنه فقط العقدة الحساسة وقائد العنقود الذي تنتمي إليه يمتلكان المفتاح. إضافة إلى كون اختلاف المفاتيح من وصلة إلى أخرى يجعل السيطرة على وصلة أي على مفتاح بمعنى آخر لا يؤثر على البيانات المتنقلة باستخدام الوصلات الأخرى. إضافة إلى أن استخدام التشفير بالمفاتيح الثنائية يضمن عدم تعديل البيانات وهذا ما يحقق بدوره متطلب تكاملية البيانات.

2- مرحلة التجميع:

يقوم قائد العنقود بمقارنة محدد المفتاح الثنائي المستقبل مع محدد المفتاح الثنائي المخزن فيه في حال عدم التطابق، يعلن أنها عقدة مهاجمة. أما في حال التطابق، يعلن أنها عقدة موثوقة ثم يقوم بعملية فك تشفير البيانات المستقبلة باستخدام المفتاح PWK$_{\text{Sni-CHj}}$ ، ثم يجميع البيانات عن طريق استخدام تابع رياضي(تابع القيمة العظمى مثلاً)، ثم

يشفرها بالمفتاح مشترك بينه وبين مركز المعالجة الرئيسي يدعى $Next_K$ (secret computed Key by Cluster Head)، ويتم حسابه أثناء عمل الشبكة وفق المعادلة الآتية:

$$Next_K = ID\_MCN \bmod(seed + m) \quad (1)$$

حيث Seed: رقم عشوائي يرسله مركز المعالجة الرئيسي إلى MCN عند كل جولة.

M: عدد قادة العناقيد.

ومن ثم يرسلها إلى MCN بعد أن تقوم بعملية مصادقة معه باستخدام تابع البعثرة وفق الآلية الآتية:

1. ترسل MCN الرسالة الآتية إلى CH_1: $ID\_MCN \,||\, H(K\_CHj) \,||\{seed \oplus NR\}_{K\_CHj}$

حيث ID_MCN: محدد العقدة MCN.

$H(K\_CHj)$: تابع البعثرة للمفتاح السري المشترك بين قائد العنقود ومركز المعالجة الرئيسي.

NR: رقم الجولة(Number of Round).

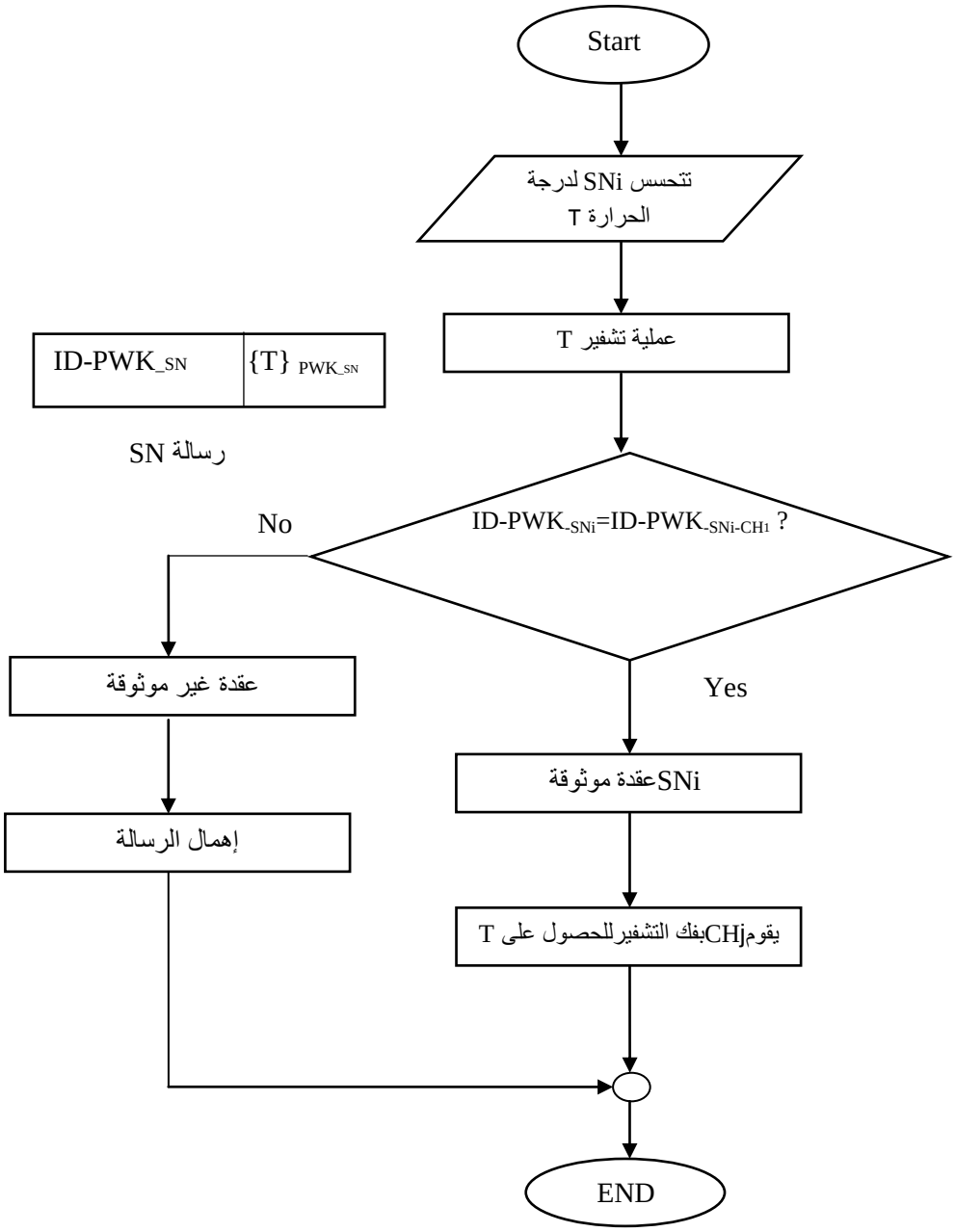
2. يقوم CH_1 بحساب $H(K\_CH_1)$ ومن ثم مقارنته مع $H(K\_CHj)$ المستقبل، في حال عدم التطابق، يعد أنها عقدة مهاجمة. أما في حال التطابق، يعد أنها عقدة موثوقة.
3. يقوم CH_1 بحساب المفتاح $Next_K$.
4. تزيد NR بمقدار واحد في كل من العقدتين CH_1 و MCN.

إذا ناقشنا ما ذكر سابقاً من الناحية متطلبات الأمنية، نلاحظ بأن دور العقدة المجمعة المتنقلة MCN هو فقط تجميع للبيانات المشفرة دون أن تقوم بعملية فك التشفير، وهذا ما يجعل البيانات محمية بشكل كبير لأن السيطرة على العقدة المتحركة من قبل مهاجم ما ستعطيه الفرصة للحصول على معلومات مشفرة فقط، وبذلك لن يكون قادراً على كشف المعلومات الحقيقية المرسلة، بذلك يكون متطلب الموثوقية محققاً. كما أن متطلب تكاملية البيانات محقق لاستخدام التشفير الثنائي بين قائد العنقود والمركز دون تدخل العقدة المجمعة في التشفير وفك التشفير. هذا إضافة إلى أن استخدام seed يعد تحدي يمكن اعتماده كوسيلة للتحقق من أن العقدة MCN هي عقدة موثوقة و أنها هي فعلاً العقدة التي تعد مسؤولة عن التجميع الآمن وهذا بدوره يجعل متطلب السرية محققاً، لا سيما أن مفتاح $Next_K$ يتم تجديده عند كل جولة للـ MCN.

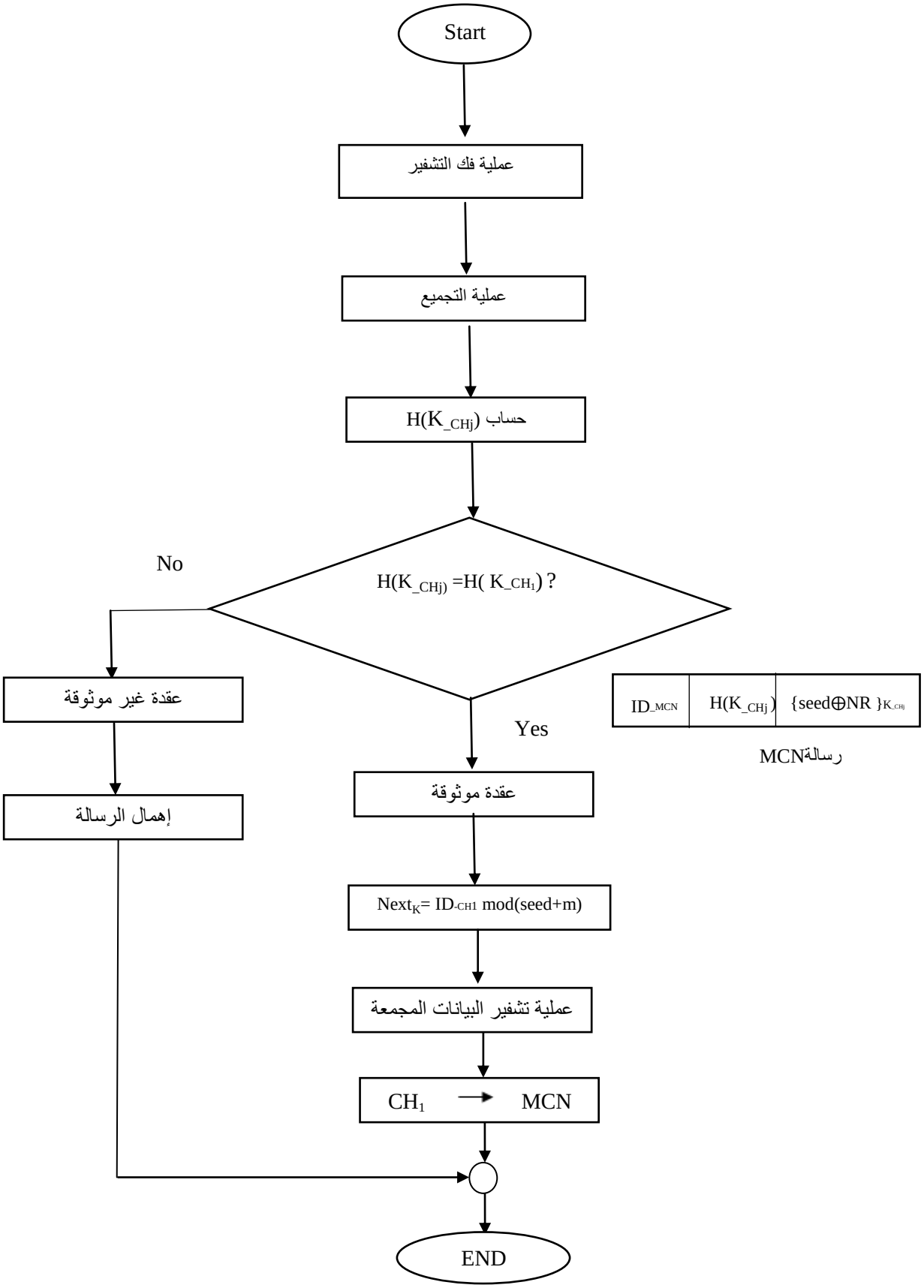
3- مرحلة اتخاذ القرار:

ترسل العقد المجمعة المتنقلة MCNs البيانات المشفرة المجمعة إلى مركز المعالجة الرئيسي، وهذا الأخير يقوم بدوره بفك تشفير البيانات باستخدام المفتاح $Next_K$ ومن ثم اتخاذ القرار المناسب.

يظهر الشكلان (4) و(5) المخططات التدفقية لخوارزمية الحل المقترحة:



الشكل (4): خوارزمية الإرسال منSNإلى CH



الشكل (5): خوارزمية الإرسال منCHإلى MCN

المحاكاة وإظهار النتائج:

إن إضافة الأمن لبرنامج NS-2 قضية هامة جداً وضرورية في نمذجة الشبكات، حيث أنه لا يملك أية مكتبة لدعم قضايا الأمن ما لم تتم إضافة بعض البروتوكولات والخوارزميات له.

من أجل ذلك قمنا في بحثنا هذا بتقديم طريقة لإضافة قضايا الأمن لهذا المحاكي وذلك بإضافة الأكواد المتعلقة بقضايا الأمن مثل عمليات التشفير وفك التشفير.

1 سيناريو المحاكاة:

في بحثنا تم استخدام نموذج الشبكات الذي يكون فيه جزء من العقد الحساسة في حالة حركة ومركز المعالجة الرئيسي ثابت وهو النموذج الأكثر استخداماً في تطبيقات MWSN [1,3] بحيث :

1- الشبكة ذات حجم متوسط مؤلفة من 39 عقدة حساسة موزعة في غابة/بستان محدود المساحة على الشكل الآتي:

- أربعة عناقيد، حيث يتكون كل عنقود من قائد العنقود وثماني عقد حساسة تابعة له.
- عقدتان مجمعتان متنقلتان MCN_A ، MCN_B. تجمع العقدة MCN_A المعلومات من قائدي العنقودين الأول والثاني(CH_1-CH_2) أما العقدة MCN_B، فتجميع المعلومات من قائدي العنقودين الثالث والرابع(CH_3- CH_4).
- عقدة واحدة تمثل مركز المعالجة الرئيسي.

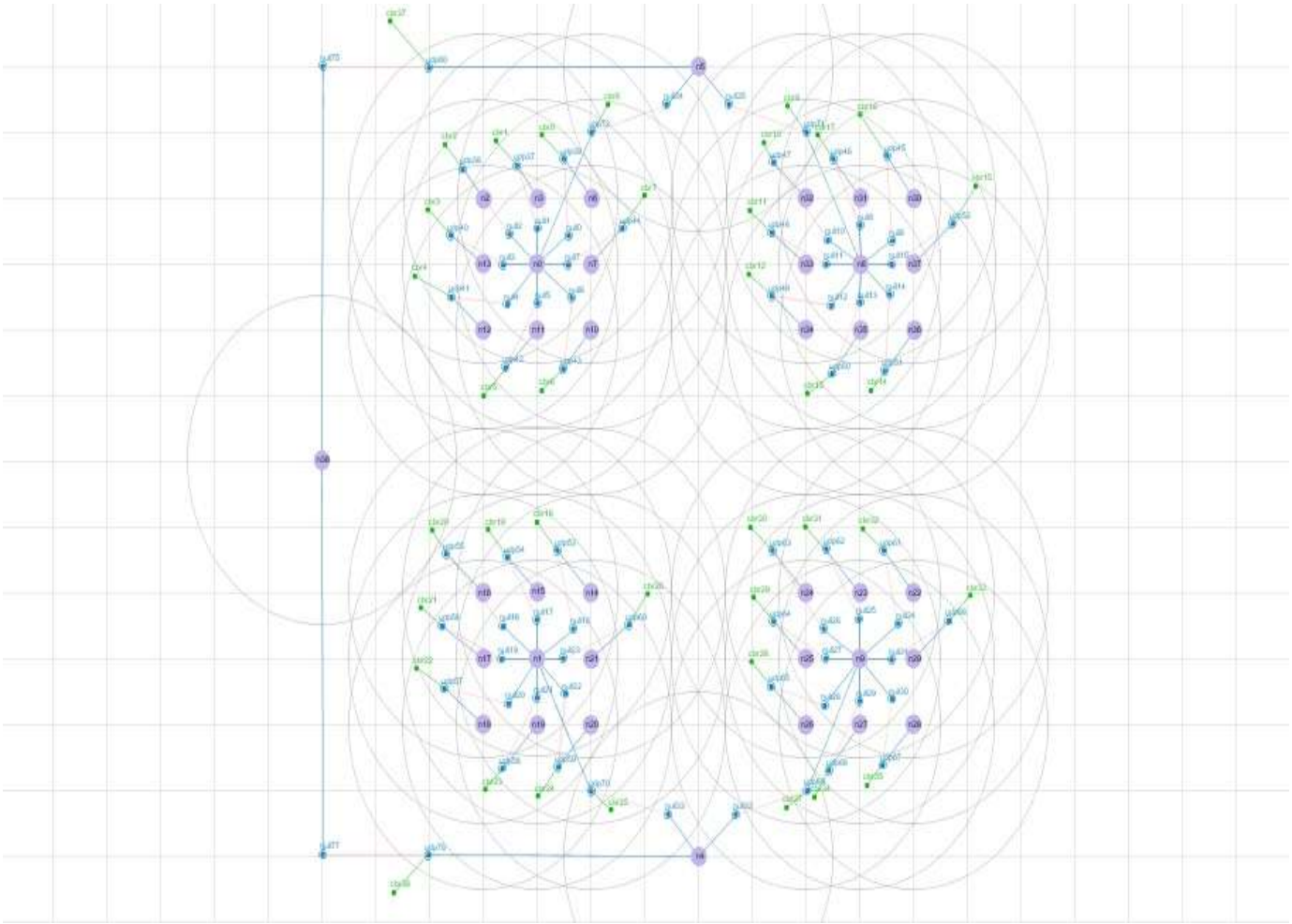
2- النشر يدوي.

3- نوع الشبكة هجينة.

4- بارامتر الطاقة المستهلكة لن يؤخذ بالحسبان: سنفترض أن التطبيق يسمح باستبدال بطاريات الحساسات.

5- التطبيق: كشف حريق في غابة محدودة المساحة.

يظهر الشكل(6) نموذجاً للشبكة المقترحة



الشكل(6): نموذج الشبكة

يوضح الجدول(1) البارامترات المستخدمة في المحاكاة.

الجدول(1): بارامترات المحاكاة المستخدمة

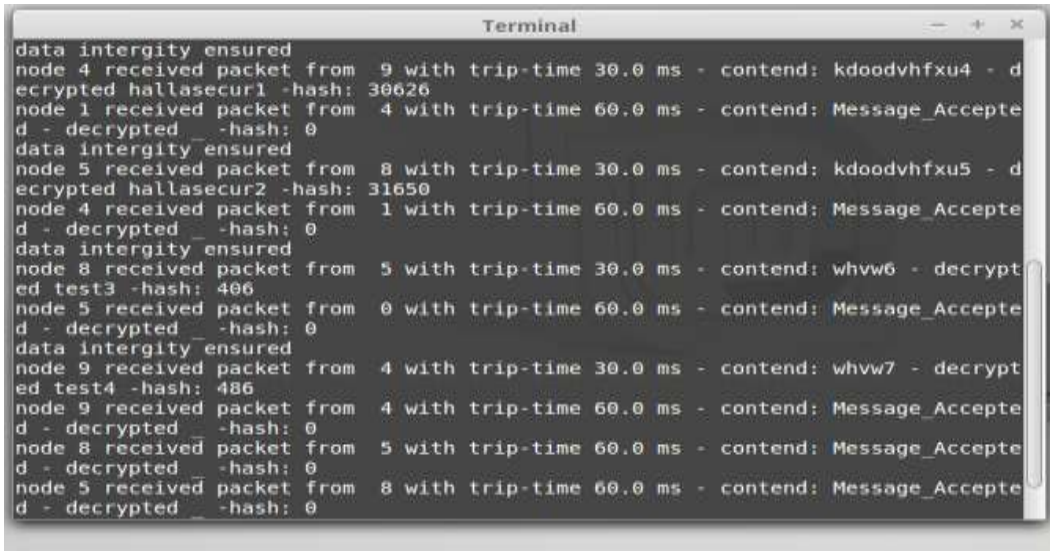
المصطلح العربي	البارامتر
المساحة المستخدمة في المحاكاة	$(500x500)m^2$
عدد قادة العناقيد	4
عدد العقد الحساسة في كل عنقود	8
عدد العقد المجمعة المتنقلة	2
نموذج الانتشار الراديوي	Tow Ray Groundmodel
نمط قناة الاتصال	Wireless
نموذج الهوائي	Omni directional Antenna
نوع الطاقة	Battery(AA)
زمن المحاكاة	20s

النتائج والمناقشة:

سنورد فيما يلي مناقشة النتائج التي حصلنا عليها وتحليل بعض البارامترات الخاصة بالخوارزمية.

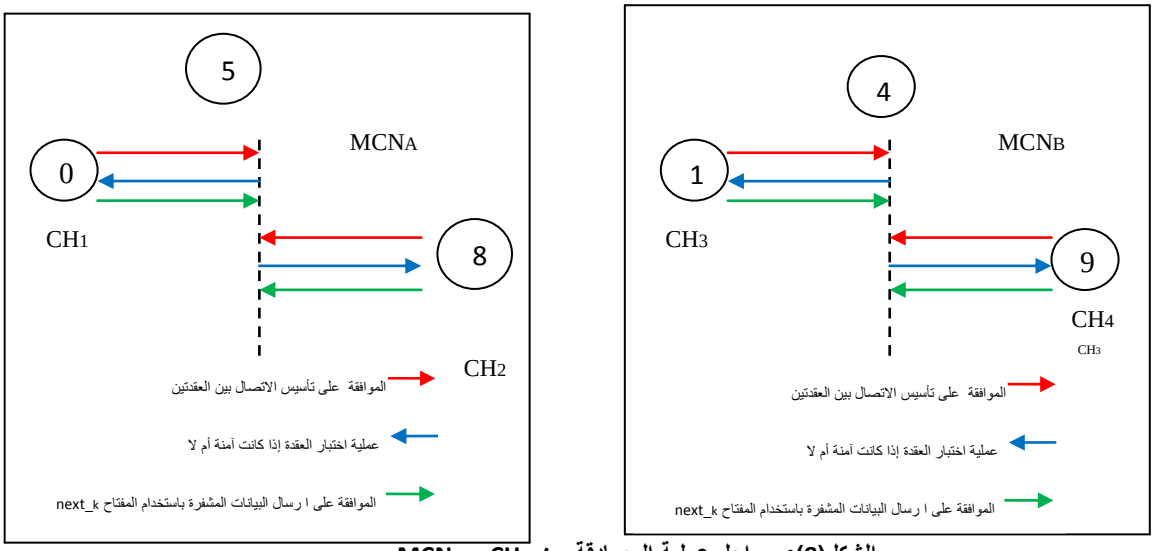
1. زمن التنفيذ:

طبقنا الخوارزمية المقترحة على مستوى العقدتين المجمعتين المتنقلتين وقادة العناقيد الأربعة. وزمن التنفيذ هو عبارة عن الزمن اللازم لإنجاز عملية المصادقة بين قائد العنقود والعقدة المجمعة المتنقلة مضافاً إليه زمن التشفير الذي يستغرقه قائد العنقود لتوليد الرسالة المشفرة من الرسالة الأصلية. نلاحظ من الشكل(7) أن خوارزمية PWDA تحقق أداء جيّداً من ناحية سرعة تنفيذ العمليّات، فهي تحتاج لـ 60ms لتنفيذ التقنية المستخدمة، وهذا يُعدّ ميّزة هامّة لهذه الخوارزمية عند استخدامها في تطبيقات الزمن الحقيقي.



الشكل(7): نتائج تطبيق خوارزمية الأمن بين CHs و MCNs

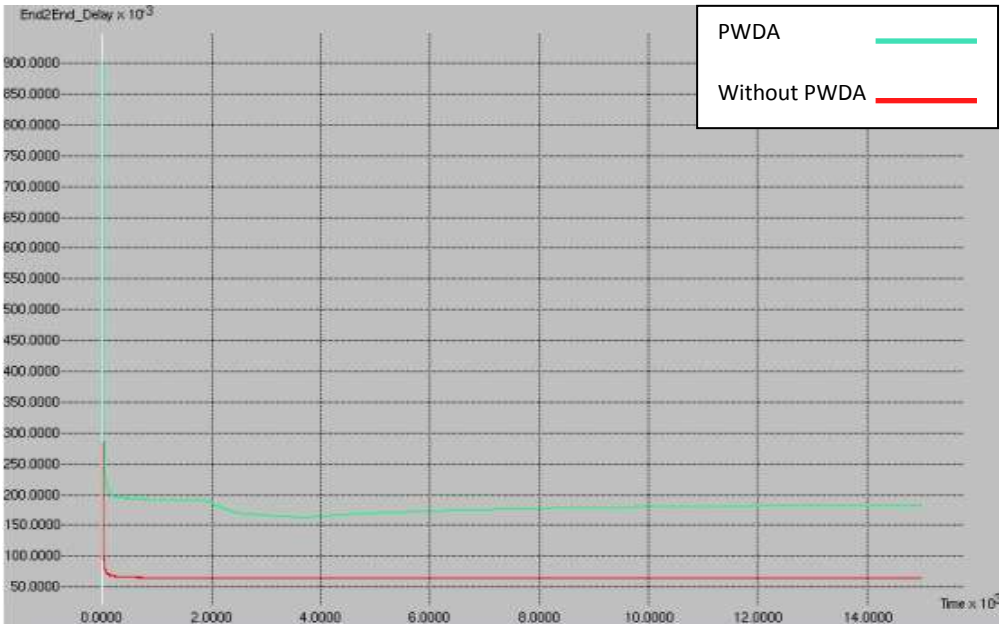
بملاحظة نتائج تنفيذ الخوارزمية نلاحظ أنها تجري كما يظهر الشكل (8).



الشكل(8): مراحل عملية المصادقة بين CHs و MCNs

2. التأخير الزمني:

وهو عبارة عن الزمن اللازم لإرسال البيانات من المصدر إلى الهدف. يظهر الشكل (9) التأخير الزمني للشبكة الناتج قبل تطبيق خوارزمية PWDA والتأخير الزمني للشبكة الناتج بعد تطبيقها مقارنة مع زمن تنفيذ سيناريو المحاكاة. هنا نلاحظ فرق التأخير الزمني الناتج هو 100ms وهذا يناسب تطبيقات الزمن الحقيقي، ويعود هذا الفرق الزمني المنخفض لاستخدام خوارزمية أمن غير معقدة لاتحتاج لتوابع رياضية معقدة وتستخدم عملية تشفير واحدة وعملية فك تشفير واحدة فقط من أجل إنجاز عملية المصادقة بين العقدتين CH_1 و MCN_A .



الشكل(9): مقارنة التأخير الزمني في الشبكة مع و دون تطبيق خوارزمية PWDA

3. عدد المفاتيح المخزنة:

إن التقنية المعتمدة في توزيع المفاتيح، كما ذكرنا سابقاً، هي تقنية معدلة عن آلية توزيع المفاتيح الثنائية التقليدية .

ففي الخوارزمية التقليدية (PW):

بفرض أن عدد العقد في كل عنقود هو S سيكون عدد المفاتيح المخزنة في كل عقدة هو R:

$$R = S - 1 \qquad (2)$$

أي أن عدد المفاتيح الكلية في كل عنقود هو W:

$$W = (S * R) + 1 = (S * (S - 1)) + 1 = S^2 - S + 1 \qquad (3)$$

أي أن عدد المفاتيح الكلية في كامل الشبكة هو Z:

$$Z = (S^2 - S + 1) * m \qquad (4)$$

حيث m هو عدد العناقيد في الشبكة.

أما في الخوارزمية المعدلة (PWDA):

كل عقدة حساسة تخزن مفتاح واحد فقط. فيكون عدد المفاتيح المحملة في قائد العنقود هو y:

$$y = (S - 1) + 1 = S \qquad (5)$$

وعدد المفاتيح الكلية في كل عنقود هو w:

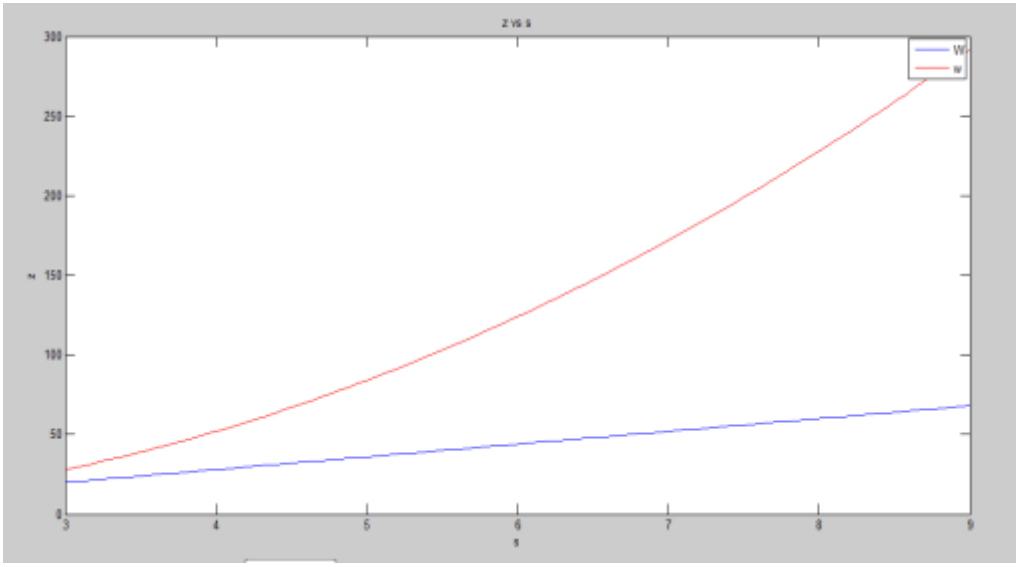
$$w = (1 * (S - 1)) + S = 2S - 1 \qquad (6)$$

أي أن عدد المفاتيح الكلية في كامل الشبكة هو z:

$$z = (2S - 1) * m \qquad (7)$$

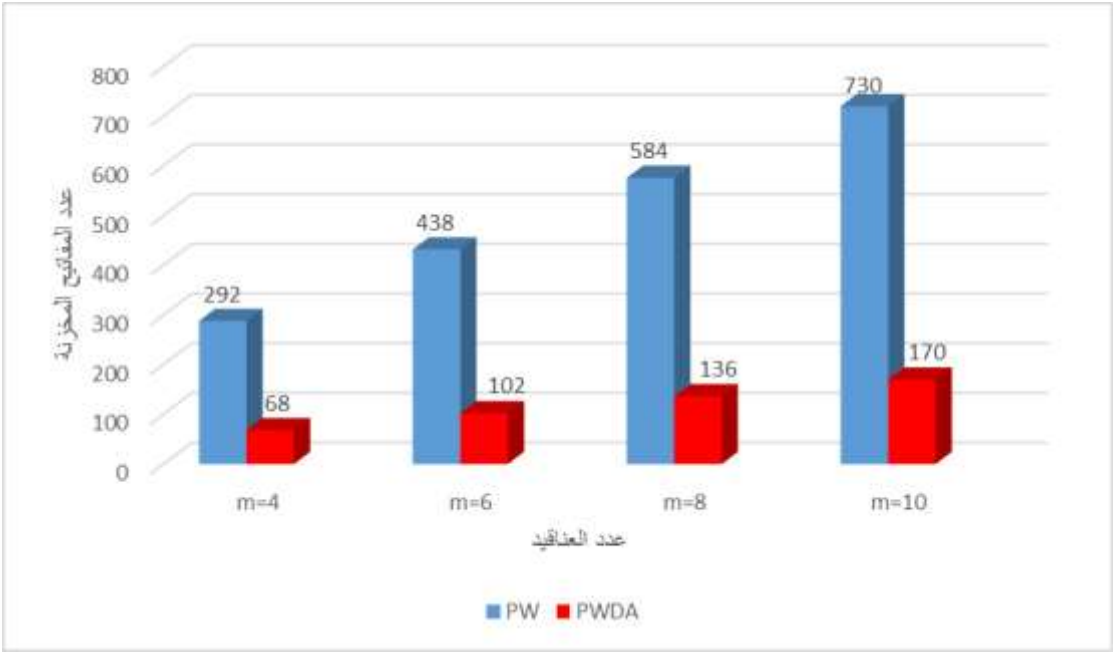
حيث m هو عدد العناقيد في الشبكة.

يوضح الشكل (10) المعادلتان (4) و(7)



الشكل(10): مقارنة بينالخوارزمية التقليدية PW والخوارزمية المعدلة PWDA من حيث عدد المفاتيح الكلية المخزنة في الشبكة

يوضح الشكل (11) التالي مقارنة بين الخوارزمية التقليدية PW والخوارزمية المعدلة PWDA من حيث عدد المفاتيح المخزنة في الشبكة مقارنة مع عدد العناقيد.



الشكل (11): يبين مخططاً لمقارنة الخوارزمية التقليدية PW مع الخوارزمية المعدلة PWDA من حيث عدد المفاتيح المخزنة في الشبكة مقارنة مع عدد العناقيد.

نلاحظ أن خوارزميتنا المقترحة تجد حلّاً متوازناً مابين الأمن وبارامتر التأخير الزمني بحيث يكون أقل مايمكن، وهذا يدعم توجهنا في هذا البحث.

الاستنتاجات والتوصيات:

بعد هذه الدراسة، يمكننا التوصل للاستنتاجات الآتية:

- إن تطبيق الخوارزمية المقترحة حقق المتطلبات الأساسية للأمن وهي الموثوقية وتكاملية البيانات والسرية.
- إن التأخير الزمني الناتج عند تطبيق الخوارزمية المقترحة منخفض مما يجعلها تناسب تطبيقات الزمن الحقيقي.
- تراعي الخوارزمية المقترحة محدودية الذاكرة مقارنة مع الخوارزمية الأساسية، إذ تحتاج إلى عدد منخفض من المفاتيح مقارنة مع الأساسية.

يمكن تلخيص التوصيات في النقاط الآتية:

- دراسة إمكانية تطبيق هذه الخوارزمية من أجل تطبيقات مكونة من عدد كبير من العقد.
- إن نموذج الحركة المستخدم في دراستنا هذه هو النموذج الأول (أي جزء من العقد الحساسة في حالة حركة ومركز المعالجة الرئيسي ثابت)، يمكن دراسة إمكانية تطبيق الخوارزمية المقترحة على نماذج الحركة الأخرى أي العقد الحساسة ثابتة ومركز المعالجة الرئيسي في حالة حركة – العقد الحساسة ومركز المعالجة الرئيسي في حالة حركة.
- دراسة إمكانية استخدام خوارزمية توزيع المفاتيح العشوائية كخطوة بديلة عن استخدام المفاتيح الثنائية وتطبيقها على سيناريو الشبكة المقترح.

المراجع

[1] J. REZAZADEH, M. MORADI, and A. SAMAD ISMAIL. *Mobile Wireless Sensor Networks Overview*. In International Journal of Computer Communications and Networks (IJCCN), Volume 2, NO 1, February 2012,pp. 17-21.

[2] M. ARSHAD, N.M. SAAD, N. KAMEL and N. ARMI. *Routing Strategies in Hierarchical Cluster Based Mobile Wireless Sensor Networks*. In IEEE INECCE, Pahang, Malaysia ,June 2011,pp. 65-69.

[3] L. ZHU . *Secure and Privacy-Preserving Data Communication in Internet of Things*SpringerBriefs in Signal Processing, 2017,pp. 3-12.

[4] A. ANITHA, K. ARTHI KRISHNA and K.R. ESWARAN AASAN. *A Secure Data Aggregation Technique for Wireless Sensor Networks*. In International Science Press IJCTA, Mach 2017, pp. 119-125.

[5] J. ZHENG, W. JIA, and G. WANG. *Data Management of Mobile Object Tracking Applications in Wireless Sensor Networks*. In Journal of Computers , Volume 4, NO. 9, September 2009,pp. 845-851.

[6] G.PRABHU and K.A.DHAMOTHARAN. *A Survey on Secure Data Aggregation Scheme for Wireless Sensor Networks.* International Journal of Science, Engineering and Technology Research (IJSETR), Volume 3, Issue 2, February 2014,pp. 329-334.

[7] M. PRIYANKA. *Collusion Attacks: Secure Data Aggregation Technique for Wireless Sensor Network*. International Journal of Advanced Technology and Innovative Research Volume. 08, No.21, November-2016,pp. 4014-4020.

[8] A. NIHARIKA and P. PADMAJA. *Secure Data Aggregation Technique for Wireless Sensor Networks in the Presence of Collision Attack*. International Journal of Scientific Engineering and Technology Research Volume.04, No.37, September 2015,pp.7991 -7995.

[9] X. XU, J. LUO, and Q. ZHANG. *Delay Tolerant Event Collection in Sensor Networks with Mobile Sink*. In IEEE INFOCOM, 2010,pp. 4244-5837.

[10] Z. SHA, JIA-LIANG LU, XU LI, and MIN-YOU WU. *An Anti-Detection Moving Strategy for Mobile Sink.* In proceeding of IEEE wireless communications and Networking Conference, 2010.

[11] J. SHIHALL, V. SHIRWALKAR, K. PATIL and S. AJNADKAR. *Secure Data Aggregation Technique for WSN*. In International Journal on Computer Science and Engineering (IJCSE) Vol. 6, April 2017,pp. 67-71.

[12] N.SANDHYA RANI, and O. SRINIVASARAO. *Efficient Implementation of Data Aggregation in WSNs by Mobile Agent Paradigm*. In International Journal on Computer Science and Engineering (IJCSE) Vol. 3 No. 9 september 2011,pp 3254-3257.

[13] WU. K, DREEF. D and SUN. B. *Secure data aggregation without persistent cryptographic operations in wireless sensor networks*. In Ad hoc Netw , Volume 5, NO1,2007,pp.100–111.

[14] YANG Y, WANG X AND ZHU S. *A Secure hop-by-hop data aggregation protocol for sensor networks.* In ACM Trans Inf Syst Secur (TISSEC), 2008,pp. 18.

[15] ZHOU. Q, YANG. and, HE. L. *A secure-enhanced data aggregation based on ECC in wireless sensor networks*. In ACM workshop on Security of ad hoc and sensor networks Sensors, 2014, pp. 6701–6721.

[16] OZDEMIR. S and XIAO. Y. *Integrity protecting hierarchical concealed data aggregation for wireless sensor networks*. In International Journal of Computer Communications and Networks (IJCCN) Volume 55, NO 8, 2011,pp. 1735–1746.

[17] V. KUMAR,S. MADRIA and J. MCCARVILLE-SCHUETHS. *A test-bed for Secure Hierachical Data Aggregation in Wireless Sensor Networks*. In proceeding of IEEE wireless communications and Networking Conference, 2010.

[18] A.S.POOMIMA, B.B.AMBERKER. *Secure Data Collection using mobile data collector in clustered wireless sensor network*. In the Journal of Institution of Engineering and Technology (IET), Volume 1, 2011, pp. 85-95.

[19] D. LIU and P. NING. *Location-based pairwise key establishments for static sensor networks* . In SASN ’03: Proceedings of the 1st ACM workshop on Security of ad hoc and sensor networks, Fairfax, Virginia, USA, 2003, pp. 72–82.

[20] S. CAMTEPE and B. YENER. *Key distribution mechanisms for wireless sensor networks: a survey*. Technical report,PRI,TR-05-07, 23 March 2005,pp. 5-8.

[21] V.JAYARAJ, M.INDHUMATHI and U.DURAI. *Secure Data Aggregation using Efficient Key Management Technique in Wireless Sensor Network* . In International Journal on Computer Applications Vol. 89 No. 9, March 2014, pp. 6-9.