مجلة جامعة تشرين للبحوث والدراسات العلمية _ سلسلة العلوم الهندسية المجلد (38) العدد (2) 2016
Tishreen University Journal for Research and Scientific Studies - Engineering Sciences Series Vol. (38) No. (2) 2016

تطوير تقنيات الحماية في بروتوكول التوجيه الجغرافي الضمني الآمن في شبكات الحساسات اللاسلكية

الدكتور مثنى القبيلي •
وائل حبيب ••

(تاريخ الإيداع 7 / 12 / 2015. قُبِل للنشر في 16/ 3 / 2016)

□ ملخّص □

تُنشَرْ شبكات الحساسات اللاسلكية في بيئات معادية، وتستعمل في التطبيقات الحرجة مثل مراقبة ساحة المعركة والمراقبة الطبية، لذا فإن ضعف الأمن يعد مصدر قلق كبير. إن القيود الصارمة على مصادر شبكات الحساسات اللاسلكية تجعل من الضروري البحث عن حلول أمنية مع الأخذ بالحسبان تلك المصادر.

يعد البروتوكول المدروس (Implicit Geographic Forwarding Protocol) (IGF) عديم الحالة، أي أنه لا يحوي جدول توجيه ولا يعتمد على معرفة طوبولوجيا الشبكة أو على وجود أو غياب أحد العقد من شبكة الحساسات اللاسلكية. طُوِّرَ هذا البروتوكول بتقديم مجموعة من الآليات لزيادة الأمن فيه. بحيث تبقي على ميزات ديناميكية الربط، وتؤمن دفاعات فعالة ضد الهجمات المحتملة. أمنت هذه الآليات التصدي لعدة هجمات منها هجوم الثقب الأسود وهجوم سايبل وهجوم إعادة الارسال، ولكن المشكلة كانت في عدم قدرة الآليات السابقة على التصدي للهجوم الفيزيائي.

يتناول هذا البحث دراسة مفصلة للبروتوكول SIGF–2 وتقترح تحسيناً له. يتضمن التحسين استخدام مفهوم معرفة الانتشار ضمن خوارزمية مجموعة المفاتيح العشوائية في إدارة المفاتيح للتصدي للهجوم الفيزيائي. وقد أثبت نتائج المحاكاة من خلال مجموعة من البارامترات أن الاقتراح المقدم قد حسن من أداء الخوارزمية المدروسة.

الكلمات المفتاحية: شبكات الحساسات اللاسلكية، بروتوكول التوجيه الجغرافي الضمني الآمن، الهجومات، إدارة مفاتيح التشفير، مفهوم معرفة الانتشار.

• مدرس، قسم هندسة الاتصالات والالكترونيات ، كلية الهندسة الميكانيكية والكهربائية، جامعة تشرين، اللاذقية سورية .
•• طالب دراسات عليا (ماجستير) ، قسم هندسة الاتصالات والالكترونيات ، كلية الهندسة الميكانيكية والكهربائية، جامعة تشرين، اللاذقية سورية.

مجلة جامعة تشرين للبحوث والدراسات العلمية _ سلسلة العلوم الهندسية المجلد (38) العدد (2) 2016
Tishreen University Journal for Research and Scientific Studies - Engineering Sciences Series Vol. (38) No. (2) 2016

Improving defence techniques In Secure Implicit Geographic Forwarding "SIGF " in Wireless Sensor Networks

Dr. Mothanna Alkubeily •
Wael Habeeb ••

(Received 7 / 12 / 2015. Accepted 16 / 3 / 2016)

□ ABSTRACT □

Wireless Sensor Networks (WSNs) are deployed in adversarial environments and used for critical applications such as battle field surveillance and medical monitoring, then security weaknesses become a big concern. The severe resource constraints of WSNs give rise to the need for resource bound security solutions.

The Implicit Geographic Forwarding Protocol (IGF) is considered stateless, which means that it does not contain any routing tables and does not depend on the knowledge of the network topology, or on the presence or absence of the node in WSN. This protocol is developed to provide a range of mechanisms that increase security in IGF. Thus it keeps the dynamic connectivity features and provides effective defenses against potential attacks. These mechanisms supported the security against several attacks as Black hole, Sybil and Retransmission attacks, but the problem was the inability of mechanisms to deal with physical attack.

This research deals with a detailed study of the SIGF-2 protocol and proposes an improvement for it, in which we use the concept of deployment knowledge from random key pool algorithm of keys management to defend against physical attack . The evaluation of simulation results, with different parameters, proved that our proposal had improved the studied protocol.

Key words: Wireless Sensor Networks, Secure Implicit Geographic Forwarding Protocol, Attacks, key management, Deployment Knowledge.

• **Assistant Professor, Departement of Communication and Electronics, Faculty of mechanical and electrical engineering, Tishreen University, Lattakia, Syria.**
•• **Postgraduate student, Departement of Communication and Electronics, Faculty of mechanical and electrical engineering, Tishreen University, Lattakia, Syria.**

مقدمة:

تعد شبكات الحساسات اللاسلكية (Wireless Sensor Network) والتي يرمز لها اختصاراً WSN ، إنجازاً علمياً في مجال تكنولوجيا الاتصالات والمعلومات، ذلك أنها فتحت المجال أمام ابتكار جيل جديد من التطبيقات في مجالات متنوعة مثل البيئة والمراقبة الصحية، وفحص سلامة الأبنية، والأمن مثل اكتشاف المتطفلين وحركة المرور والكشف المبكر عن الحرائق.

ترتبط هذه التكنولوجيا بشكل ملحوظ بتقدم التقنيات المستخدمة في بناء مكونات الحساسات، مثل طاقة البطارية، وحجم الذاكرة، وسرعة المعالجة. تلعب هذه الاعتبارات دوراً أساسياً في قوة الاتصال اللاسلكي، وتوفير الأمن ضد أي تطفل أو هجوم على هذه الشبكات. نظراً لأهمية وحساسية تطبيقات هذه الشبكات والتي قد تتعلق بالحياة كالتطبيقات الصحية أو بأمن الدول كالتطبيقات العسكرية، كان الأمن مطلباً جوهرياً لضمان نجاح أي تطبيق وذلك لضمان سلامة العمليات، وسرية البيانات المتحسسة، وخصوصية الأشخاص الموجودين في محيط الشبكة، وحمايتها من الاعتداءات الأمنية .

يفترض عادة في شبكات الحساسات اللاسلكية بأن المهاجم قد يعلم تقنيات الأمن المستخدمة ، وقد يكون قادراً على التحكم بإحدى عقد هذه الشبكة أو حتى سرقتها بشكل مباشر(فيزيائياً) ، وبسبب الكلفة العالية لنشر الحساسات المضادة للعبث فإن معظم عقد شبكات الحساسات اللاسلكية تعد غير مضادة للعبث، وهكذا فإنه عندما يسيطر المهاجم على أحد العقد فإنه يكون قادراً على سرقة المعلومات الخاصة بالأمن المخزنة في تلك العقدة، لذلك فقد توجهنا إلى التقليل من ضرر الهجوم الفيزيائي على البروتوكول المدروس قدر الإمكان.

أهمية البحث وأهدافه:

يستمد البحث أهميته من النقاط الآتية:

- الأهمية الكبيرة لبروتوكولات التوجيه الآمنة في شبكات الحساسات اللاسلكية، بسبب توجهها نحو مختلف المجالات بدءاً بالتطبيقات الطبية إلى الاتصالات الفضائية مروراً بالتطبيقات البيئية والخدمية والصناعية والعسكرية ، وغيرها من المجالات الحيوية.
- الفعالية الكبيرة لبروتوكولات التوجيه الجغرافية في شبكات الحساسات اللاسلكية ولإدارة المفاتيح ودمجهما سوياً في بروتوكول معين، ودراسة ما ينتج عن هذا الدمج من زيادة وانخفاض في بعض بارامترات الحساسات بغية معرفة نتائج تطبيق أدارة المفاتيح في بروتوكولات أخرى .

يهدف العمل على اقتراح آلية دفاع جديدة لبروتوكول SIGF-2 لمنع التأثير على كامل الشبكة عند حصول المهاجم على المفتاح المشترك للشبكة والحفاظ على آليات الأمن السابقة للبروتوكول SIGF-2 .

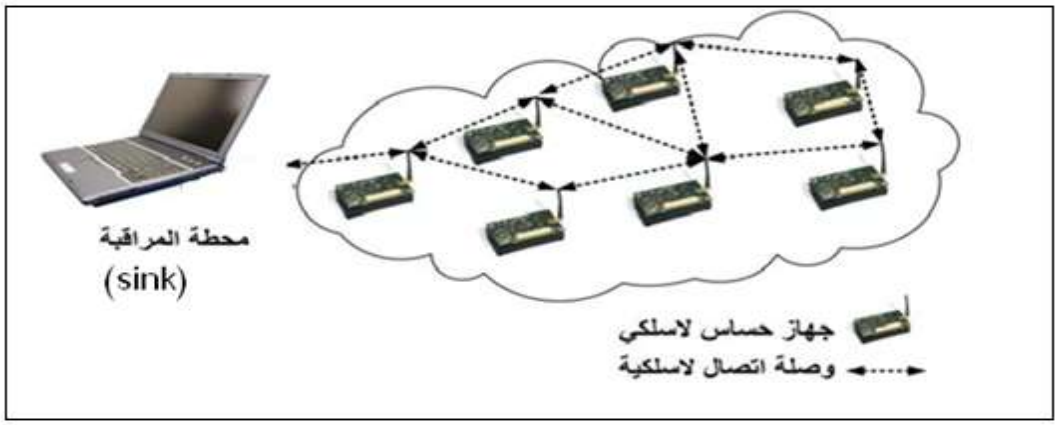
طرائق البحث ومواده:

من أجل المحاكاة استخدمنا لغة البرمجة (visual studio) ضمن بيئة العمل (NET.) وهي عبارة عن بيئة متكاملة من لغات البرمجة المختلفة. حيث تتيح كتابة البرمجيات باللغة المناسبة دون تعقيد من خلال مجموعة من الحزم والمكتبات والأدوات الجاهزة التي توفر الوقت والجهد. كما أن جميع لغات (NET.) متكاملة فيما بينها، فبرنامجك المصمم بـ Visual Basic .NET يمكن إضافة بعض العناصر والشيفرات المصدرية إليه من لغة Visual C#

NET. دون أي مشاكل، بل يمكن للمشروع الواحد أن يدمج شيفرات مصدرية من لغات متعددة مثل Java، Delphi ... الخ.

1 -تعريف شبكات الحساسات اللاسلكية (Wireless Sensor Networks):

تعرف شبكات الحساسات اللاسلكية [1] على أنها مجموعة من العقد (الأجهزة)، التي لها القدرة على الاتصال مع بعضها البعض، تقوم بمراقبة ظاهرة بيئية محددة (كمراقبة درجات الحرارة، ونسب الرطوبة، وتحركات المركبات، ومستويات الإضاءة، ودرجات الضغط الجوي، وتفاوت الأصوات، ...الخ). ويوضح الشكل (1) مثالاً عن هذه الشبكات.



الشكل (1) شبكات الحساسات اللاسلكية.

2- المتطلبات الأمنية في شبكات الحساسات اللاسلكية :

تصنف المتطلبات الأمنية في شبكات الحساسات اللاسلكية إلى [2,3]:

2-1 سرية البيانات (Data Confidentiality) :

تستخدم شبكات الحساسات اللاسلكية المثالية في البيئات التي تتطلب سرية عالية وحساسية عالية للبيانات. فيجب ألا تقوم حساسات هذه الشبكات بتسريب أية معلومات أو قراءات تقوم بها إلى أية شبكات أخرى مجاورة.

2-2 مصادقة العقد (Node Authentication) :

هو التحقق من هوية العقد التي تشارك في الاتصال.

2-3 صحة البيانات (Data Safety) :

هي التأكد من أن البيانات سليمة ولم يتم تخريبها أو تعديلها أثناء نقلها عبر الشبكة.

2-4 عدم الإنكار (Non-Repudiation) :

هو متعلق بحقيقة أنه إذا أرسل كيان رسالة ما، فإن ذلك الكيان لا يستطيع أن ينكر أن الرسالة أرسلت بواسطته. ويُمكن لمستقبل الرسالة أن يتعرف على مرسلها.

2-5 تكاملية البيانات (Data Integrity) :

هي ضمان الحفاظ على الرسالة المرسلة من التعديل فيها بشكل غير قانوني من مستخدم لا يملك الصلاحية.

6-2 التوافرية /الاستمرارية (Availability) :

وهو أن تكون مصادر الشبكة متوفرة للمستخدمين المصرح لهم باستخدامها طوال الوقت ودون تأخير يذكر.

3- تصنيف الهجمات المحتملة على شبكات الحساسات :

يمكن تصنيف هذه الهجمات إلى [4]:

1- الهجمات الخارجية والداخلية:

تعرف الهجمات الخارجية على أنها تلك الهجمات التي تسببها عقد خارجية لا تنتمي لشبكة الحساسات، بينما الهجمات الداخلية تحدث عندما تقوم عقدة شرعية من داخل الشبكة بالتصرف بطرائق غير شرعية.

2- الهجمات السلبية والفعالة :

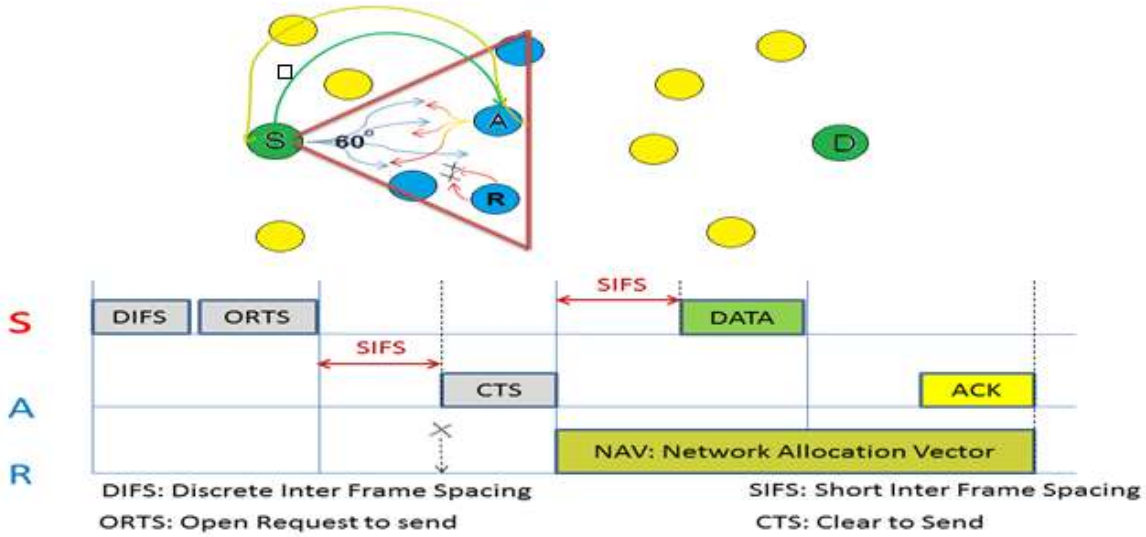
تتضمن الهجمات السلبية التنصت أو مراقبة تبادل رزم البيانات ضمن شبكات الحساسات اللاسلكية، بينما في الهجمات الفعالة يتم تعديل رزم البيانات أو إنشاء رزم جديدة خاطئة.

3- الهجمات العادية والمتطورة :

تعتمد على تطور أجهزة المهاجم، ففي الهجمات العادية يقوم المهاجم بالعملية باستخدام عقد ذات مواصفات مشابهة لعقد الشبكة، بينما في الهجمات المتطورة يستخدم المهاجم أجهزة أكثر قوة و تطوراً من عقد الشبكة.

4- آلية عمل بروتوكول التوجيه الجغرافي الضمني الآمن (Secure Implicit Geographic Forwarding) (IGF) :

تعتمد بروتوكولات التوجيه الجغرافية على المواقع الجغرافية للعقد بهدف إنشاء مسار فعال باتجاه الهدف [4]. وتكمن أهميتها في أنها تتطلب عدداً قليلاً من الحسابات والاتصالات وعمليات التحكم، لذا فهي تحسن التوسعية في الشبكات كبيرة الحجم ولا تحتاج لتخزين جداول توجيه عن الشبكة.



الشكل (2) آلية عمل بروتوكول التوجيه الجغرافي الضمني الآمن .

يبين الشكل (2) آلية عمل بروتوكول التوجيه الجغرافي الضمني الآمن ، حيث تأتي فترة زمنية (DIFS) (تباعد الإطار الداخلي المنفصل) كبداية [5،6] للتأكد من أن القناة فارغة ثم تقوم العقدة المصدر (S) بإرسال رسالة باتجاه

العقدة الهدف (D) فتبث إشارة (ORTS) (طلب إرسال مفتوح) في كل الاتجاهات متضمنة موقعها وموقع الهدف D وعامل يتعلق بمنطقة التوجيه. لكن مثاليا فإن العقد التي تتوضع ضمن نطاق 60 درجة من الخط الواصل بين الهدف والمرسل هي التي يجب أن تجيب لكي توجه الرسالة وندعو تلك العقد بالعقد المرشحة (candidate nodes) . تقوم هذه العقد بإرسال استجابة تدعى (CTS) (الجاهزية لاستقبال الارسال) بعد فترة زمنية (SIFS) (تباعد الإطار الداخلي القصير) وتلك الاستجابة هي عبارة عن حزمة بيانات تتعلق قيمتها ببعدها عن المصدر وطاقتها المتبقية وبعدها عن الخط الواصل بين (S) و (D). سرعة الاستجابة هذه تحدد أي من هذه العقد هي المفضلة لتكون القفزة التالية وعندما تنتهي هذه العقدة المفضلة من تحديد قيمة CTS ترسلها إلى (S) ويتم نقل البيانات ويسمى الزمن الأعظمي المسموح لاستقبال استجابات (CTS) من هذه العقد بالنافذة الزمنية للاستجابة (CTS response window) . بشكل مثالي فإن العقد الأخرى ضمن العقد المرشحة (candidate nodes) لتكون القفزة التالية يمكنها معرفة أنه تم ارسال حزمة (CTS) من عقدة أخرى وهي تستطيع ذلك نتيجة لميزة توضعها ضمن نطاق 60 درجة من البعد بين (S) و (D)، لذا عند معرفتها تقوم بإلغاء إرسال حزمة CTS الخاصة بها، أي نستطيع القول بأنه في بروتوكول IGF هناك عقدة وحيدة تستجيب لل (ORTS) وهي العقدة ذات زمن الاستجابة CTS الأقل.

5- التحسينات التي طرأت على البروتوكول IGF:

قام مجموعة من الباحثين [7] بتقديم مجموعة من الآليات لزيادة الأمن في IGF . بحيث تبقي على ميزات ديناميكية الربط وتؤمن دفاعات فعالة ضد الهجمات المحتملة :

5-1 الدراسة الأولى: (بروتوكول IGF الامن عديم الحالة) SIGF-0:

يعد هذا البروتوكول كقاعدة للبروتوكولات الأخرى في عائلة SIGF وآلية عمله مشابهة لآلية عمل IGF مع وجود بعض التعديلات التي تضفي عليه صفة الأمن ضد بعض الهجمات الأخرى التي لا يستطيع IGF التصدي لها، وهذه التعديلات موضحة ضمن أنواعه.

له عدة أنواع :

5-1-1 SIGF-0 Priority:

تكون فيه نافذة الاختيار ذات زمن افتراضي (5 ms) ويتم انتقاء العقدة المثلى للقفزة التالية من مجموعة الخيارات المستقبلة خلال مدة النافذة الزمنية، حسب الأولوية التابعة لبعدها عن الوجهة.

5-1-2 Random SIGF-0:

يتم اختيار عقدة القفزة التالية بشكل عشوائي من بين الخيارات المتاحة في نافذة الاختيار بغض النظر عن الأولوية. ومما سبق نجد بأن SIGF-0 يمنح القدرة على التصدي لهجوم الثقب الأسود (BLACK HOLE)، الذي لم يكن IGF قادراً على التصدي له.

5-2 الدراسة الثانية: SIGF-1 Local – State Secure IGF :

تلخص هذه الحالة عبر قيمة الموثوقية من العقد المجاورة، والتي تؤثر على اختيار العقد المرشحة ليتم اختيارها في القفزة التالية. وطالما أن هذه الحالة لا يتم تشاركها مع العقد المجاورة، فإنه لا يوجد ارتباط مع التهيئة، أو التزامن أو الصيانة.

يتم الأخذ بالحسبان بأن جميع العقد المرشحة يجب أن يكون لها عامل موثوقية حدي R-threshold=0.45 . حيث يمنح هذا العامل لجميع العقد في الشبكة قبل أن تبدأ عملها من قبل مصمم الشبكة، لأن الهجوم قد يتم عند بدء

عمل الشبكة، لذا إن لم يتم منح هذه القيمة للعقد في البدء فإن هذه العقد ستملك عامل موثوقية مثل أي عقدة مهاجمة وعندها سيفقد SIGF−1 ميزته الأساسية، ومما سبق نجد بأن SIGF−1 يعد فعالاً ضد هجوم سايبل (Sybil) .

3−5 الدراسة الثالثة : SIGF−2 Shared State Secure IGF :

يعتمد على نفس آليات التوجيه والأمن المستخدمة في SIGF−0 و SIGF−1 مع زيادة الموثوقية والتي تؤمنها مفاتيح تشفير مستخدمة ومعروفة بين العقد وهذا يتم بعدة طرق :

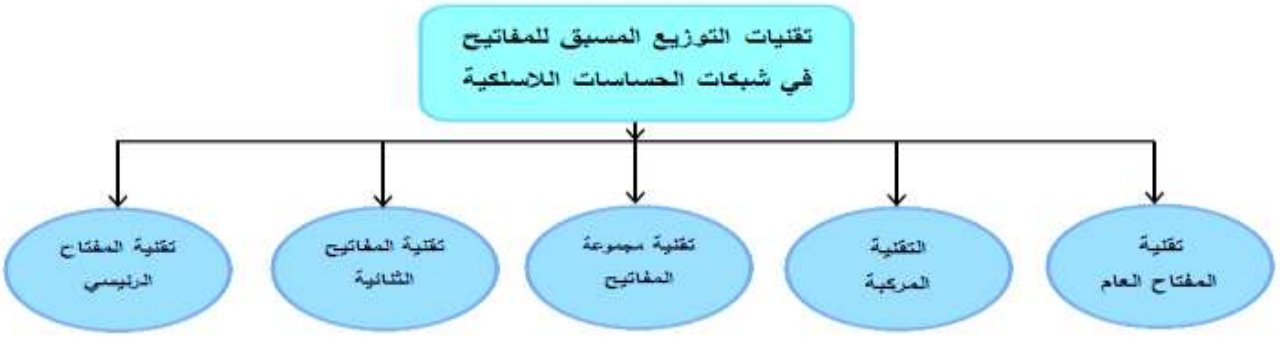
1 − توثيق الرسالة (message authentication) . 2− تسلسل الرسالة (message sequence) .

3− تشفير الحمل (payload encryption) .

مما سبق نجد بأن استخدام التوثيق والرقم التسلسلي في SIGF−2 يمنع هجوم DoS . ولكن يجب ألا ننسى بأن آليات دفاع SIGF−2 لوحدها تكون ضعيفة ضد الهجمات السابقة دون الاعتماد على خواص SIGF−0 و SIGF−1 .

6− تقنيات التوزيع المسبق للمفاتيح في wsn :

بعد دراستنا لكافة طرائق آليات إدارة مفاتيح التشفير في شبكات الحساسات اللاسلكية وجدنا أنها تقسم وفق الشكل الآتي:



الشكل (3) تقنيات توزيع المفاتيح في شبكات الحساسات اللاسلكية.

6−1− تقنية المفتاح الرئيسي (Master key) :

تتم في هذه التقنية مشاركة مفتاح رئيسي بين جميع العقد في الشبكة [8,9,10]. لكن هذه الطريقة غير مرنة وغير آمنة ضدّ الهجمات.

6−2− تقنية المفاتيح الثنائية (pair−wise) :

يخصص هنا زوج مفتاحي لكل عقدتين في الشبكة و يستخدم هذا الزوج من أجل انشاء اتصال آمن بين العقدتين[11]. هذه الطريقة مثالية تتميز بتقديم مستوى عالٍ من الأمن لكنها ليست عملية بالنسبة لشبكات الحساسات اللاسلكية بسبب المساحة المحدودة جداً للذاكرة. إضافة إلى صعوبة إضافة عقد جديدة إلى شبكة الحساسات [12] لما تسببه من تعقيد إضافي.

6−3− تقنية مجموعة المفاتيح (Key pool) :

تمتلك هذه التقنية العديد من نماذج خوارزميات إدارة المفاتيح منها ما يعمل في شبكات الحساسات اللاسلكية المتجانسة ومنها ما يعمل في شبكات الحساسات اللاسلكية الهجينة، وسنهتم في هذا البحث بهذه التقنية كون التقنيات

الباقية تملك مساوئ كبيرة موضحة مع شرح كل تقنية ، لا تسمح باستخدامها في شبكات الحساسات اللاسلكية بفعالية كبيرة. لذا سنشرح هذه التقنية.

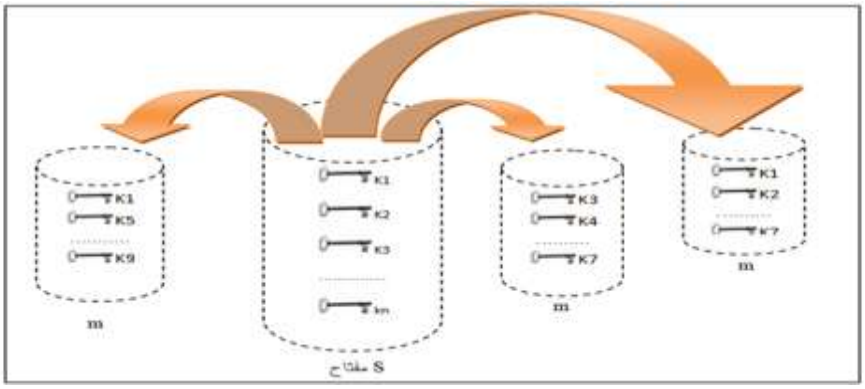
6-3-1 نماذج حلول إدارة المفاتيح في شبكات الحساسات اللاسلكية المتجانسة (WSN homogeneous):

من أهم هذه النماذج هي الخوارزمية الأساسية للتوزيع العشوائي المسبق للمفاتيح (the basic random key predistribution scheme) حيث تستخدم هذه الآلية مجموعة مفاتيح مكونة من عدد كبير من المفاتيح S ، كل عقدة في الشبكة تختار وبشكل عشوائي مجموعة جزئية من m مفتاح من هذه المجموعة الكلية، ويكون الاختيار مع إعادة .

اقترح Eschenauer و Gligor طريقة التوزيع العشوائي المسبق للمفاتيح [13,14]. تقسم هذه الطريقة إلى مرحلتين:

1. مرحلة ما قبل نشر العقد (مرحلة التهيئة):

يبين الشكل (3) هذه المرحلة حيث أن كل عقدة تملك m مفتاح من مجموعة المفاتيح الكلية S وكل عقدتين متجاورتين تشتركان بمفتاح واحد وفقاً لاحتمال ما p .



الشكل (4) مرحلة ما قبل النشر.

2. مرحلة ما بعد النشر (مرحلة إيجاد المفاتيح المشتركة):

بعد نشر العقد في وسط التطبيق، تقوم العقد أولاً باستكشاف المفاتيح المشتركة مع العقد المجاورة لها. يتم استكشاف المفاتيح المشتركة من خلال تخصيص محدد (Identifier) قصير لكل مفتاح أولي يُراد نشره، وتقوم كل عقدة ببث محددات مفاتيحها. العقد التي تكتشف أنها تملك في حلقة مفاتيحها مفتاحاً مشتركاً مع غيرها تتحقق من أن جاراتها تملك فعلاً هذا المفتاح باستخدام بروتوكول الاستجابة للتحدي (Challenge Response).

تم تطوير الطريقة السابقة باستخدام مخطط إدارة المفاتيح لشبكات الحساسات اللاسلكية باستخدام معرفة الانتشار (A Key Management Scheme for Wireless Sensor Networks Using Deployment Knowledge)

حيث يمكن للعقدتين أن تحتفظا بجزء من المفاتيح m والذي تحتاجانه فقط بدلاً من الاحتفاظ بكامل المجموعة، لذا فإن التوزع الأولي للمفاتيح باستخدام معرفة الانتشار يمكن أن يحسن بشكل جوهري اتصالية شبكة (من ناحية الوصلات الآمنة) ويعطي مرونة ضد اختراق العقد ويقلل كمية الذاكرة المطلوبة [15,16] .

6-4- التقنية المركبة (Combined) :

تُقسَّمْ الشبكة في هذه التقنية إلى عناقيد أو مناطق مختلفة. حيث تُطبَّق تقنية توزيع مفاتيح مختلفة ضمن كل منطقة. إن تقسيم الشبكة إلى عناقيد يمكن أن يتم على أساس اعتبارات أمنية [17] .

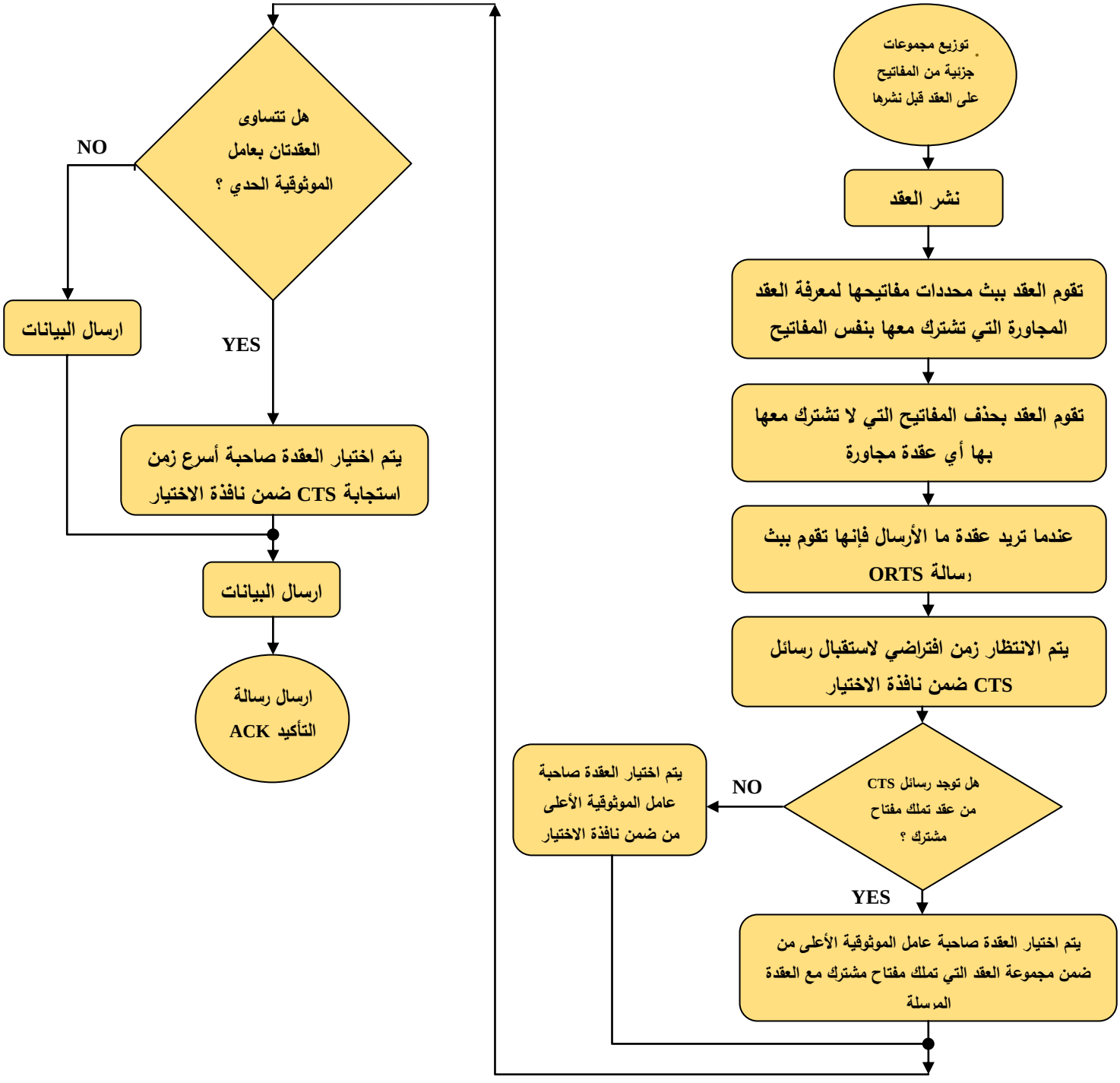
6-5- تقنية المفتاح العام (Public Key Approach) :

تطبق هذه التقنية في الشبكات الهجينة وتعتمد على العناقيد الموجودة ضمن الشبكة [18] . لكن سيئة هذه الطريقة أن العقد العادية تستهلك مقداراً كبيراً من الطاقة.

بعد الدراسة التفصيلية لهذه التقنيات، وجدنا أن طريقة معرفة الانتشار (Deployment Knowledge) في طريقة مجموعة المفاتيح المتجانسة (Homogeneous Key pool) ضمن طرق تقنية المفتاح العام هي الأنسب لمقاومة الهجوم الفيزيائي في بروتوكولنا المقترح **SIGF-3** . واستخدمنا المفاتيح المتجانسة كون العقد في البروتوكول المدروس هي عقد متجانسة وليست هجينة، كما هو موضح في آلية عمل البروتوكول **SIGF** .

7- آلية عمل البروتوكول SIGF-3:

سيتم تعديل آلية عمل البروتوكول SIGF-2 بإدخال طريقة معرفة الانتشار ضمن تقنية مجموعة المفاتيح كونها أكثر طريقة تناسب البروتوكول المدروس وسنسمي البروتوكول الجديد باسم SIGF-3 والمخطط الآتي يوضح آلية عمل البروتوكول الجديد .



الشكل (5) آلية عمل البروتوكول SIGF-3 .

8- المحاكاة وإظهار النتائج :

8-1- بيئة المحاكاة :

و قد انطلقنا في دراستنا من الفرضيات الآتية:

1 - بيئة العمل مثالية بغض النظر عن التصادمات والأحوال الجوية.

2 – جميع العقد متماثلة في الطاقة وفي مجال البث /عقد متجانسة/.

3 – جميع العقد ثابتة في مواقعها.

4 – جميع العقد المهاجمة ثابتة في مواقعها.

5 – موقع العقدة Sink ثابت ومعلوم من قبل كافة العقد.

6 – عدد العقد في التطبيق المدروس 24nodes.

7 – حجم المفتاح 128 bytes.

8 – حجم الرزمة: 32 بايت.

تمت محاكاة الخطوات التفصيلية لآلية عمل البروتوكولات IGF و SIGF–2 و SIGF–3 باستخدام لغة البرمجة Visual Basic .NET وذلك على حاسب ذو مواصفات مبينة في الجدول الآتي :

نظام التشغيل Operating system	المعالج Processor	ذاكرة الوصول العشوائي Random Access Memory
Windows 7 Ultimate	Intel(R) Celeron(R) cpu 3.2GHz	2 GB

سنأخذ بالحسبان مجموعة من النقاط الأساسية في عملية المحاكاة ذكرت في بداية البحث.

يبين الشكل الآتي توزع العقد ضمن واجهة البرنامج :

الشكل (6) توزع العقد ضمن واجهة البرنامج.

تتألف لوحة تحكم البرنامج من العناصر الآتية:

1– نوع البروتوكول المستخدم (Protocol Type) :

تتيح لنا هذه الخيارات معرفة البروتوكول المستخدم حالياً ضمن واجهة التطبيق، ويمكننا تغيير البروتوكول المستخدم من ضمن هذه اللوحة .

2– نوع الهجوم (Attacking Type) يتألف من أربعة خيارات وهي:

الأول None : أي عدم وجود أية هجوم على الشبكة.

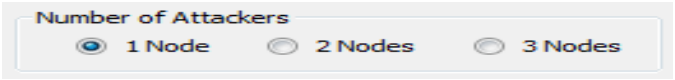
الثاني هجوم حجب الخدمة Denial Of Service : تطبيق هجوم DoS على الشبكة عند التنفيذ.

الثالث هجوم Sybil : تطبيق هجوم سايبل على الشبكة عند التنفيذ.

الرابع الهجوم الفيزيائي physical : تطبيق هجوم فيزيائي على الشبكة .

يتيح لنا الاختيار بين عدة هجمات ممكنة على الشبكة، والتبديل بين هذه الهجمات.

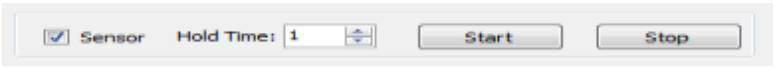
3- عدد العقد المهاجمة ويتم فيه اختيار إما عقدة مهاجمة واحدة أو اثنين أو ثلاثة.



4- الخيار Sensor يجب اختياره وذلك للسماح بتحديد مكان وقوع الحدث في الشبكة.

الخيار Hold Time يتيح لنا مجال [1-10] للتحكم بسرعة تنفيذ البرنامج.

Start لبدأ تنفيذ البرنامج، وStop لإيقاف تنفيذ البرنامج.



5- Statistics يسمح بإظهار النتائج على شكل رسم بياني. يدل المحور الأفقي على عدد العقد المهاجمة والمحور الشاقولي على نسبة الرزم المسلمة للـ Sink.

8-2- نتائج المحاكاة:

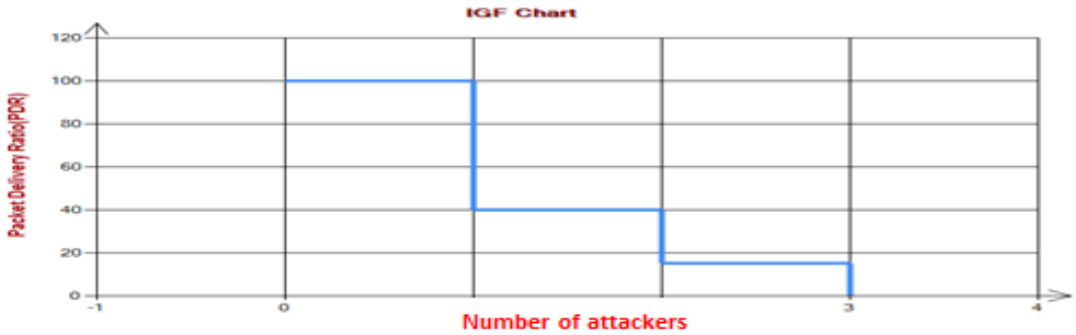
1) العلاقة بين نسبة تسليم الرزم packet delivery ratio (PDR) وعدد العقد المهاجمة في IGF:

يبين الشكل (6) العلاقة بين عدد العقد المهاجمة ونسبة تسليم في البروتوكول الأساسي IGF. حيث نلاحظ ما يلي:

1- عند عدم وجود أي هجوم فإن البروتوكول يقوم بعمله الطبيعي وتكون الشبكة في أدائها الأفضل.

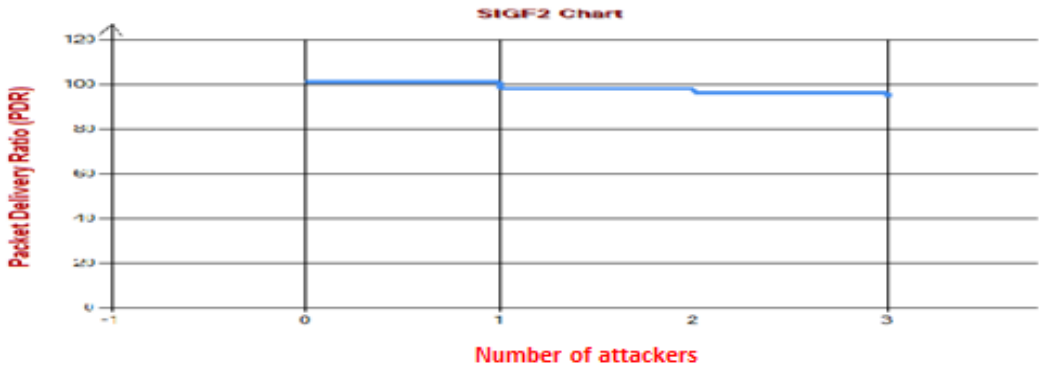
2- عند وجود عقدة أو عقدتين مهاجمتين (هجوم غير فيزيائي) تنخفض نسبة تسليم الرزم وهذا الانخفاض يكون بحسب نسبة وقوع الأحداث ضمن مجال العقد المهاجمة .

3- أما عند وجود ثلاثة عقد مهاجمة فإن نسبة تسليم الرزم تصبح معدومة في مثالنا المطروح .



الشكل (7) العلاقة بين عدد العقد المهاجمة ونسبة تسليم الرزم (PDR) في البروتوكول IGF .

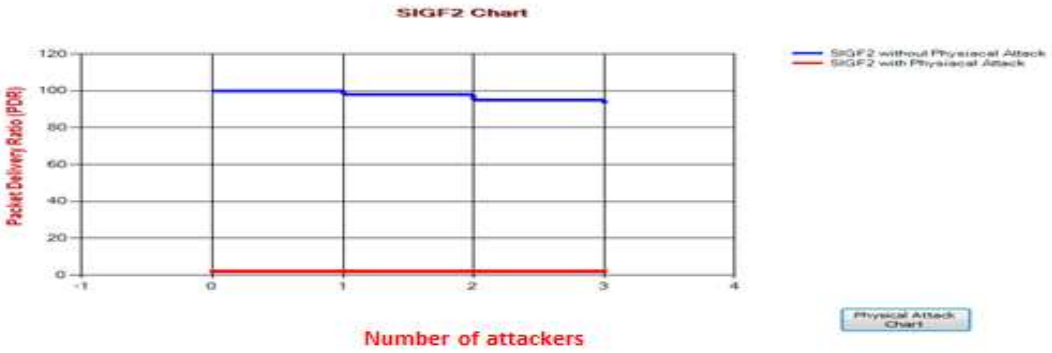
2) **العلاقة بين نسبة تسليم الرزم وعدد العقد المهاجمة مع هجوم غير فيزيائي في SIGF-2:**



الشكل(8) العلاقة بين عدد العقد المهاجمة بهجوم غير فيزيائي ونسبة تسليم الرزم في البروتوكول SIGF-2 .

نلاحظ أن أداء الشبكة كما هو موضح في الشكل (7) لا يتأثر بازدياد عدد العقد المهاجمة (بهجوم غير فيزيائي) لذا فإن الشبكة تحافظ على أدائها عند استخدام البروتوكول SIGF-2 .

3) **العلاقة بين نسبة تسليم الرزم وعدد العقد المهاجمة مع هجوم فيزيائي في SIGF-2:**



الشكل (9) العلاقة بين عدد العقد المهاجمة ونسبة تسليم الرزم دون هجوم فيزيائي ومع وجود هجوم فيزيائي للبروتوكول SIGF-2 .

نلاحظ أن نسبة تسليم الرزم في البروتوكول SIGF-2 دون هجوم فيزيائي كانت قريبة من حدها الأعظمي، بينما عند تعرضه لهجوم فيزيائي بأي عدد من العقد، فإن العقدة المهاجمة تسيطر على المفتاح العام للشبكة، لذا فإنها تسيطر على جميع الاتصالات بين العقد وتنخفض نسبة تسليم الرزم إلى حدها الأدنى كما هو موضح في الشكل (8).

4) **العلاقة بين نسبة تسليم الرزم وعدد العقد المهاجمة لـ Sink مع هجوم فيزيائي في SIGF-3:**

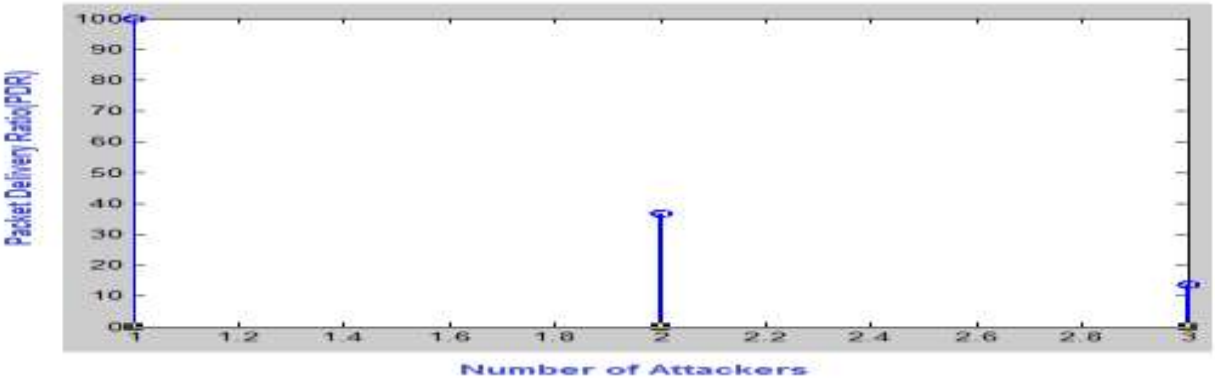
إن العلاقة بين عدد العقد المهاجمة ونسبة تسليم الرزم هي علاقة أسية علماً أن نسبة تسليم الرزم في SIGF-3 عند تعرضه لهجوم تتعلق بحجم الشبكة والمسافة بين العقدة المهاجمة والعقدة الرئيسية (sink) وعدد العقد المهاجمة .

أي أن شكل العلاقة يصبح كالآتي :

$$\text{Packet delivery ratio (PDR)} = \alpha \,/\, \exp(\text{number of attackers})$$

حيث (α) عامل يتعلق بحجم الشبكة وبالمسافة بين العقدة المهاجمة والعقدة الرئيسية (sink) .

وفي مثالنا المعروض فإن (α) يعد ثابتاً، وعند تحليل المعادلة السابقة باستخدام برنامج الـ (MATLAB) ، وبفرض أن الثابت يملك القيمة التجريبية (α =271.23) لسهولة النمذجة، كون هذه القيمة تجعل الخط البياني للمعادلة يبدأ من قيمة (100%) وهي نسبة تسليم الرزم المثالية، ينتج لدينا الشكل (9).



الشكل (10) العلاقة بين عدد العقد المهاجمة ونسبة تسليم الرزم في SIGF-3 باستخدام برنامج ال (MATLAB).

نلاحظ أن نسبة تسليم الرزم دون وجود عقد مهاجمة كان مثالياً، وعند تعرضه للهجوم الفيزيائي من قبل عقدة واحدة فإن نسبة تسليم الرزم تنخفض. ثم عند زيادة العقد المهاجمة لعقدتين تنخفض بشكل أكبر، وعندما تصبح ثلاثة عقد مهاجمة فإنه في حالة الشبكة المدروسة لدينا يتم السيطرة على معظم اتصالات الشبكة كوننا افترضنا أن العقد التي تتعرض للهجوم هي عقد رئيسية (متوضعة في أماكن حساسة في الشبكة **وهي الحالة الأسوء**) .

8-3- بارامترات تقييم الأداء :

تستخدم البارامترات الآتية [19] لتقييم فعالية طرق إدارة المفاتيح في شبكات الحساسات اللاسلكية وهذه البارامترات هي:

1 - درجة المقاومة ضد السيطرة على العقدة Resistance Degree against node capture (RD) .

2 - الذاكرة المطلوبة لتخزين المفاتيح key Storage Overhead (KSO) .

3 - مفهوم الطاقة Energy Consumption (EC).

سنقوم بدراسة البارامترات الثلاثة في حالة البروتوكول SIGF-2 وفي حالة البروتوكول SIGF-3 بالنسبة لعقدة محيطية وعقدة مركزية ضمن الشبكة المدروسة وفي حالة شبكة موسعة .

1 - درجة المقاومة ضد السيطرة على العقدة (RD) :

تعرف بأنها نسبة عدد الوصلات غير المسيطر عليها إلى نسبة الوصلات الكلية في الشبكة عند السيطرة على عقدة ضمن الشبكة، وتعطى بالعلاقة: $RD = 1 - \frac{Ncl}{Ntl}$

حيث: Ncl تمثل عدد الوصلات المسيطر عليها عند الاستيلاء على عقدة واحدة ضمن الشبكة.

Ntl تمثل عدد الوصلات الكلية في الشبكة.

1 ǂ - في حال كان البروتوكول المطبق في الشبكة هو **SIGF-2** :

فإنه يوجد لدينا مفتاح مشترك وحيد، لذا فإن الهجوم الفيزيائي على إحدى عقد الشبكة سيؤدي للسيطرة على كامل الوصلات في الشبكة. أي تصبح قيمة البارامتر (RD =1-1= 0).

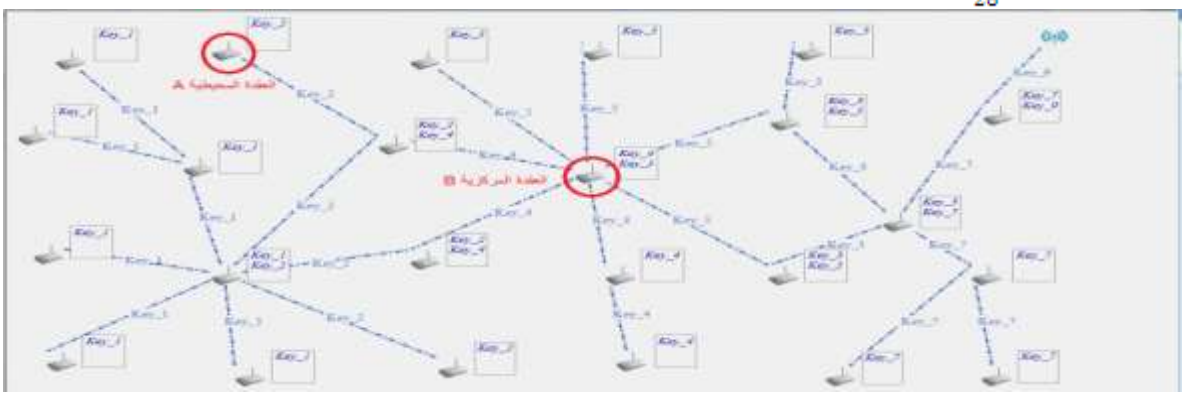
1 -2 - في حال كان البروتوكول المطبق في الشبكة هو **SIGF-3** :

فإن قيمة البارامتر بالنسبة للعقدة المحيطية (A) الموضح موقعها ضمن الشبكة المدروسة في الشكل (10) هي:

$$RD= 1-\frac{1}{26} = 0.96 = 96\ \%$$

وتكون قيمة البارامتر بالنسبة للعقدة المركزية (B) الموضح موقعها ضمن الشبكة المدروسة في الشكل (10) هي :

$$RD= 1-\frac{7}{26} = 0.73 = 73\ \%$$



الشكل (11) توزع عقد الحساسات ضمن واجهة البرنامج .

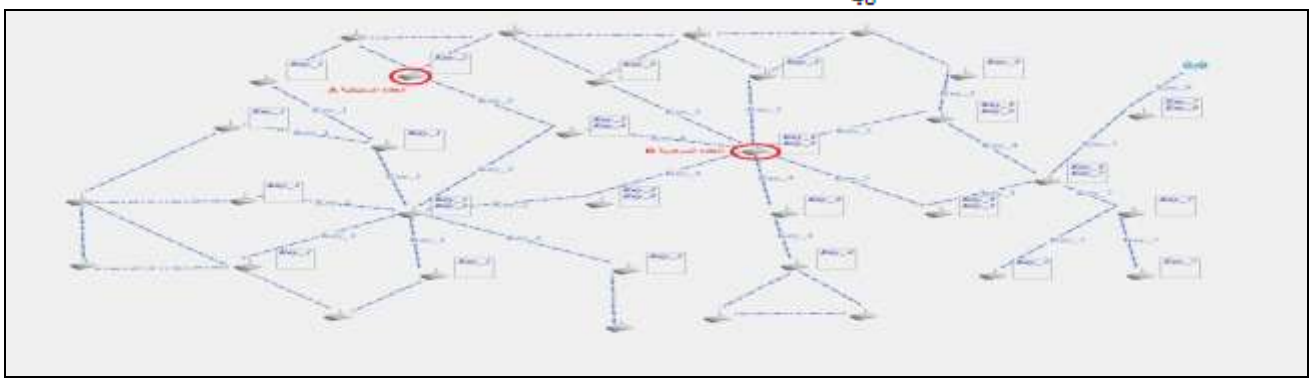
1 -3 - وفي حال توسيع الشبكة وكان البروتوكول المطبق في الشبكة هو **SIGF-3** :

بعد القيام بإضافة عقد جديدة على الشبكة، فإن قيمة البارامتر بالنسبة للعقدة المحيطية (A) الموضح موقعها ضمن الشبكة الموسعة في الشكل (11) هي:

$$RD= 1-\frac{3}{48} = 0.93 = 93\ \%$$

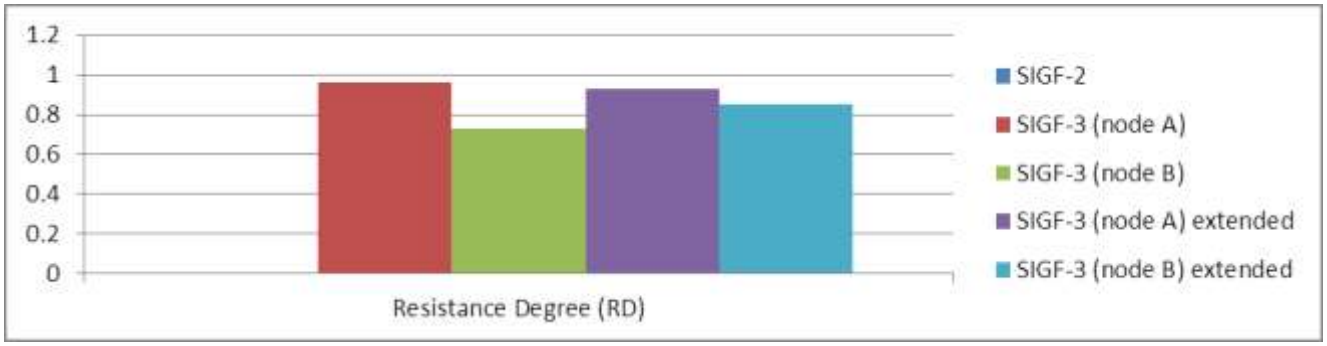
وتكون قيمة البارامتر بالنسبة للعقدة المركزية (B) الموضح موقعها ضمن الشبكة الموسعة في الشكل (11) هي:

$$RD= 1-\frac{7}{48} = 0.85 = 85\ \%$$



الشكل (12) توزع عقد الحساسات ضمن واجهة البرنامج بعد توسيعها.

والشكل الآتي يوضح قيم بارامتر المقاومة ضد السيطرة على العقد في جميع الحالات السابقة .



الشكل (13): درجة المقاومة ضد السيطرة على العقدة في حالة البروتوكول SIGF-2 وفي حالة البروتوكول SIGF-3 بالنسبة لعقدة محيطية وعقدة مركزية ضمن الشبكة المدروسة وفي حالة شبكة موسعة.

2 - الذاكرة المطلوبة لتخزين المفاتيح (K_{so}) :

تعرف بأنها حجم الذاكرة المطلوبة في كل عقدة لتخزين المفاتيح المطلوبة ضمن الطريقة المستخدمة، وتعطى بالعلاقة: $K_{so}= n_{stored\ key} * Key\ size\ (bytes)$

حيث: n stored key تمثل عدد المفاتيح المخزنة في العقدة.

Key size (bytes) تمثل حجم المفتاح وهي ثابتة وتساوي في شبكتنا المدروسة القيمة (128 bytes).

2 - 1 في حال كان البروتوكول المطبق في الشبكة هو **SIGF-2** :

فإنه يوجد لدينا مفتاح مشترك وحيد أي قيمة البارامتر هي (128 bytes = 128* 1=KSO).

2 - 2 في حال كان البروتوكول المطبق في الشبكة هو **SIGF-3** :

فإن قيمة البارامتر بالنسبة للعقدة المحيطية (A) الموضح موقعها ضمن الشبكة المدروسة في الشكل (10) هي:

$K_{so}=1 * 128 = 128$ bytes

وتكون قيمة البارامتر بالنسبة للعقدة المركزية (B) الموضح موقعها ضمن الشبكة المدروسة في الشكل (10) هي :

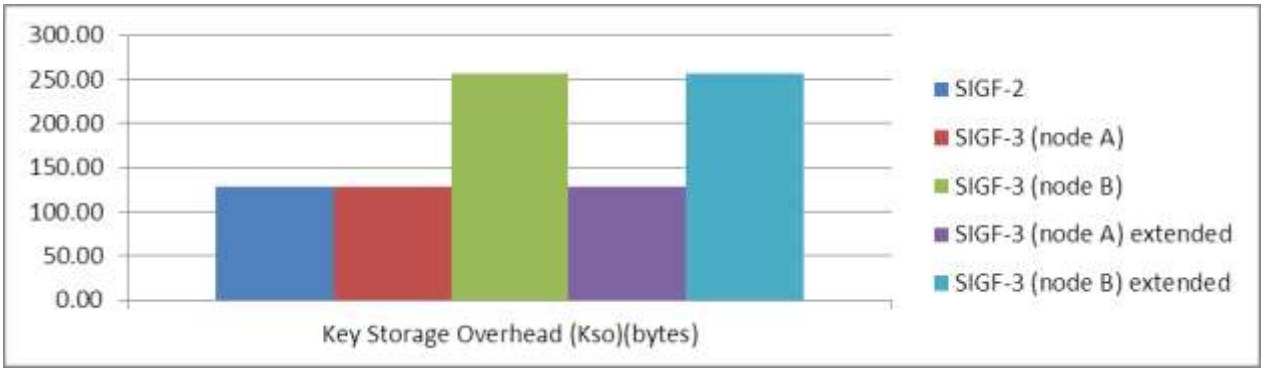
$K_{so}= 2 * 128 = 256$ bytes

2 - 3 وفي حال توسيع الشبكة وكان البروتوكول المطبق في الشبكة هو **SIGF-3** :

قيمة البارامتر بالنسبة للعقدة المحيطية (A) الموضح موقعها ضمن الشكل (11) لن تتغير عن قيمتها في الشبكة الأساسية لأنه لم نزد عدد المفاتيح المخزنة ضمن كل عقدة وتلك القيمة هي: $K_{so}=1 * 128 = 128$

وأيضاً قيمة البارامتر بالنسبة للعقدة المركزية (B) الموضح موقعها ضمن الشبكة الموسعة في الشكل (11) لن تتغير عن قيمتها في الشبكة الأساسية وتلك القيمة هي : $K_{so}= 2 * 128 = 256$ bytes

والشكل التالي يوضح قيم بارامتر الذاكرة المطلوبة لتخزين المفاتيح في جميع الحالات السابقة .



الشكل (14): الذاكرة المطلوبة لتخزين المفاتيح في حالة البروتوكول SIGF-2 وفي حالة البروتوكول SIGF-3 بالنسبة لعقدة محيطية وعقدة مركزية ضمن الشبكة المدروسة وفي حالة شبكة موسعة.

3 - مفهوم الطاقة (EC) :

تعرف بأنها الطاقة المصروفة في إرسال واستقبال الرسائل المطلوبة لعقدة واحدة لكي تحقق اتصالاتها الآمنة، وتعطى بالعلاقة: $E_c = n_t * w_t * c_t + n_r * w_r * c_r$

حيث n_t , n_r : تمثل عدد الرسائل المرسلة والمستقبلة .

w_r،w_t : تمثل حجم الرسالة المرسلة والمستقبلة (bytes) وهي ثابتة وفي الشبكة المدروسة فإن هذه القيمة تساوي (32 bytes).

c_t, c_r : تمثل الطاقة المحسوبة باستخدام المرسل والمستقبل الالكتروني (energy/byte).

وبما أن الطاقة المحسوبة باستخدام المرسل والمستقبل الالكتروني ثابتة فإنه يمكن كتابة العلاقة السابقة بالشكل:

$E_c = n_t * w_t + n_r * w_r$

3 - 1 في حال كان البروتوكول المطبق في الشبكة هو **SIGF-2** :

فإنه تصبح قيمة البارامتر ($E_c = 1*32 + 1*32 = 64$ nJ).

3 - 2 في حال كان البروتوكول المطبق في الشبكة هو **SIGF-3** :

-إن كل عقدة ترسل محددات مفاتيحها برسالة إلى العقد المجاورة وتستقبل محددات مفاتيح تلك العقد وبالتالي :

فإن قيمة البارامتر بالنسبة للعقدة المحيطية (A) الموضح موقعها ضمن الشبكة المدروسة في الشكل (10) هي:

$E_c = 1*32 + 4*32 = 160$ nJ

وتكون قيمة البارامتر بالنسبة للعقدة المركزية (B) الموضح موقعها ضمن الشبكة المدروسة في الشكل (10) هي :

$E_c = 1*32 + 7*32 = 256$ nJ

3 - 3 وفي حال توسيع الشبكة وكان البروتوكول المطبق في الشبكة هو **SIGF-3** :

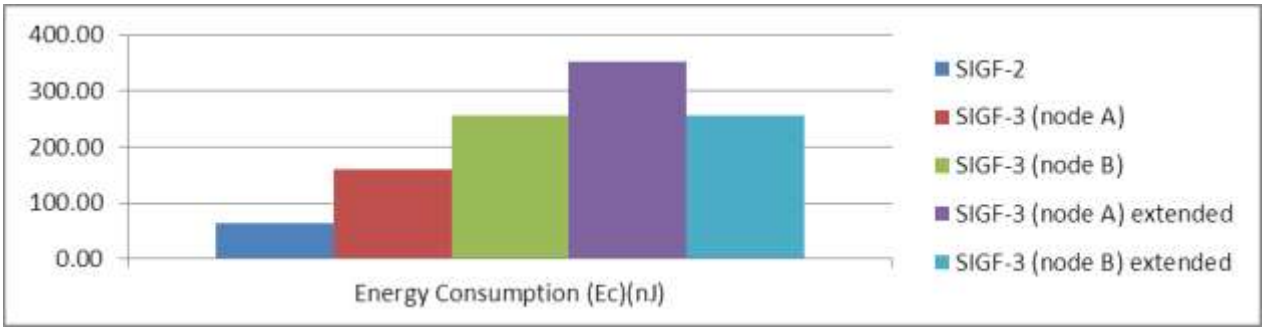
-في حال توسع الشبكة وانضمام عقد جديدة إليها فإن العقد المحيطية ستستقبل رسائل جديدة بمحددات مفاتيح تلك العقد الجديدة وبالمقابل سترسل محددات مفاتيحها – التي بقيت محتفظة بها– إلى تلك العقد، لذا سيزداد استهلاك الطاقة ضمنها .وتكون قيمة البارامتر بالنسبة للعقدة المحيطية (A) الموضح موقعها ضمن الشبكة الموسعة في الشكل (11) هي:

$E_c = 2*32 + 9*32 = 352$ nJ

أما قيمة البارامتر بالنسبة للعقدة المركزية (B) الموضح موقعها ضمن الشبكة الموسعة في الشكل السابق فإنها لن تتغير عن قيمتها في الشبكة الأساسية كون تلك العقد المركزية لن ترسل أو تستقبل رسائل من العقد الجديدة هي :

$E_c = 1*32 + 7*32 = 256$ nJ

والشكل التالي يوضح قيم بارامتر الطاقة في جميع الحالات السابقة .



الشكل (15): مفهوم الطاقة في حالة البروتوكول SIGF-2 وفي حالة البروتوكول SIGF-3 بالنسبة لعقدة محيطية وعقدة مركزية ضمن الشبكة المدروسة وفي حالة شبكة موسعة.

الاستنتاجات والتوصيات:

1- إن درجة المقاومة للعقدة (RD) تكون معدومة في حال كان البروتوكول المطبق في الشبكة هو (SIGF-2) ، بينما عند تطبيق البروتوكول المقترح (SIGF-3) فإنها تزداد وتكون قيمتها بالنسبة لعقدة محيطية أكبر من عقدة مركزية كون الأخيرة تملك عدد وصلات آمنة أكبر بكثير مع العقد المجاورة. أما عند توسيع الشبكة فإن قيمة البارامتر تزداد بالنسبة للعقدة المركزية نفسها لأن عدد الوصلات الآمنة الكلي في الشبكة ازداد، بينما بالنسبة للعقدة المحيطية فإن قيمة البارامتر انخفضت بسبب زيادة عدد الوصلات الآمنة المتعلقة بها .

2- تكون الذاكرة المطلوبة لتخزين المفاتيح (KSO) ثابتة في جميع العقد عند تطبيق البروتوكول (SIGF-2)، بينما تزداد بالنسبة للبروتوكول المقترح (SIGF-3) وتكون قيمتها بالنسبة لعقدة مركزية أكبر مما لدى عقدة محيطية، وعند توسيع الشبكة تبقى قيمة البارامتر ثابتة بالنسبة للعقد المحيطية والمركزية كون العقد لم تحتفظ بأي مفتاح جديد.

3- إن قيمة البارامتر (EC) عند تطبيق البروتوكول (SIGF-2) أقل مما هي لدى تطبيق البروتوكول المقترح (SIGF-3). حيث تكون قيمة البارامتر في البروتوكول المقترح أكبر في العقد المركزية مما لدى العقد المحيطية ، وعند توسيع الشبكة فإن قيمة البارامتر تبقى ثابتة بالنسبة للعقد المركزية، أما المحيطية فإن قيمتها ستزداد بسبب انضمام عقد جديدة .

المراجع:

[1] J.Sen, "*A Survey on Wireless Sensor Network Security*", International Journal of Communication Networks and Information Security (IJCNIS) , USA , 1(2): 55-74, August (2009).

[2] A.Erring , R.Szewczyk , V.Wen, D.Culler,.J.D. Tygar , " *SPINS: Security Protocols for Sensor Networks*" , Intel Research Berkely, USA , Vol.9,No.2, April (2001).

[3] L.Mcgrath , C.weiss , " *Wireless Sensor Networks Security*" , CS-591 Fundamentals of Computer and Network Security, Colorado.(2005).

[4] Y.Wang, G.Attebury, B.V ramamurthy, " *A Survey of Security Issues in Wireless Sensor Networks* " , The Electronic magazine of original peer reviewed survey articles ,USA , 8(2): 1-19, (2006).

[5] A. D. Wood , L. Fang , J. A. Stankovic and T. He "*SIGF: A family of configurable, secure routing protocols for wireless sensor networks*", Proc. 4 th ACM Workshop Security of Ad hoc Sensor Networks, pp.35-48.(2006).

[6] Brian Blum, Tian He, Sang Son, and John Stankovic." *IGF: A state-free robust communication protocol for wireless sensor networks*". Technical Report CS-2003-11, Univ. of Virginia, Charlottesville, VA, (2003).

[7] J.N. Al-karaki, A.E. Kamal, " *Routing Techniques in Wireless Sensor Networks*", Wireless communications, IEEE, Vol 11.No 6, pp 6-28. Dec.(2004).

[8] B. Dutertre and J. Cheung, S.and Levy " *Lightweight key management in wireless sensor networks by leveraging initial trust* " Technical Report SRI-SDL-0402, System Design Laboratory, April (2004).

[9] B. Lai, S. Kim, and I. Verbauwhede " *Scalable session key construction protocol for wireless sensor networks* " In IEEE Workshop on Large Scale Real Time and Embedded Systems (LARTES), Austin, Texas, December (2002).

[10] R. Anderson and M. Kuhn, " *Tamper resistance - a cautionary note*" in Proceedings of the Second Usenix Workshop on Electronic Commerce, pp1–11, November(1996).

[12] L. Eschenauer and V. D. Gligor, "*A key-management scheme for distributed sensor networks*", in Proceedings of the 9th ACM conference on Computer and communications security, Washington, DC, USA, pp.41–47, November 18-22 (2002).

[13] R.Merkle, " *Secure communication over insecure channels*", Communications of the ACM vol.21,no.4,pp.294–299,(1978).

[14] W. Du, J. Deng, Y. Han, S. Chen, and P. Varshney " *A key management scheme for wireless sensor networks using deployment knowledge* ", In IEEE INFOCOM'04, pages 586–597, Hongkong, China, 7-11 March (2004).

[15] C. Blundo, A. De Santis, Amir Herzberg, S. Kutten, U. Vaccaro, and M.Yung. " *Perfectly-secure key distribution for dynamic conferences* " In Advances in Cryptology Crypto '92, Lncs 740, pages 471–486, (1993).

[16] H. Chan, A. Perrig, and D. Song " *Random key predistribution schemes for sensor networks* " In IEEE Symposium on Research in Security and Privacy, (2003).

[17] Y. Law, R. Corin, S. Etalle, and P. Hartel " *A formally verified decentralized key management for wireless sensor networks* " In Personal Wireless Communications (PWC), pages 27–39, (2003).

[18] S. Zhu, S. Setia, and S. Jajodia " *LEAP: Efficient security mechanisms for large scale distributed sensor networks* " In 10th ACM Conference on Computer and Communications Security (CCS'03), pages 62–72, October (2003).

[19] B.Maala ," *Security in Wireless Sensor Networks: Key management in WSN* " , PhD Thesis University of Technology at Compiegne (UTC),(2010).