مجلة جامعة تشرين للبحوث والدراسات العلمية _ سلسلة العلوم الهندسية المجلد (35) العدد (4) 2013
Tishreen University Journal for Research and Scientific Studies - Engineering Sciences Series Vol. (35) No. (4) 2013

استعراض مسببات هدر الطاقة في شبكات الحساسات اللاسلكية وتصنيف بعض الهجمات التي تستهدف منابع الطاقة المعتمدة على البروتوكول B-MAC

الدكتور رضوان دندة*
الدكتور قاسم قبلان**
مضر وينس***

(تاريخ الإيداع 27 / 1 / 2013. قُبِل للنشر في 27/ 5 / 2013)

∇ ملخّص ∇

نظراً للتطور التقني أصبحت شبكات الحساسات اللاسلكية WSN واسعة الانتشار، وأصبحت تستخدم في شتى المجالات المدنية والعسكرية والبحث العلمي. ومثل كل الشبكات فهي عرضه للاختراق، لكن تركيبتها البسيطة (قدرة المعالج والذاكرة) تفرض إيجاد تقنيات لصد الهجمات غير التقنيات المستخدمة في الشبكات العادية.

تهتم معظم أبحاث الأمان في شبكات الحساسات على سرية وسلامة البيانات، في هذا البحث سنقوم بالتركيز على الهجمات التي تستهدف موارد الطاقة والتي يطلق عليها اسم Denial of sleep (DoS) رفض الدخول بوضع الإثبات، وهي من أخطر الهجمات التي يمكن أن تتعرض لها، إذ يقوم المهاجم بإجبار الحساسات على العمل بشكل مستمر حتى تستنفد كامل مدخراتها.

قمنا في هذا البحث باستعراض مسببات هدر الطاقة في WSN وتصنيف الهجمات التي تستهدف منابع الطاقة وقمنا ببناء أنموذج محاكاة لتحليل استجابة البروتوكول B-MAC (الأوسع انتشاراً) لهجمات رفض الدخول في وضع الإثبات.

تم إجراء هذا البحث في جامعة تشرين في الفترة الواقعة بين 2012/7/1 و 2012/10/15.

الكلمات المفتاحية: شبكات الحساسات، رفض الدخول وضع حالة الإثبات، بروتوكولات ماك، الأمان.

* أستاذ - قسم النظم والشبكات الحاسوبية- كلية الهندسة المعلوماتية- جامعة تشرين- اللاذقية- سورية.
** مدرس - قسم النظم و الشبكات الحاسوبية- كلية الهندسة المعلوماتية- جامعة تشرين- اللاذقية- سورية.
*** طالب دراسات عليا (دكتوراه)- قسم النظم والشبكات الحاسوبية- كلية الهندسة المعلوماتية- جامعة تشرين- اللاذقية- سورية.

مجلة جامعة تشرين للبحوث والدراسات العلمية _ سلسلة العلوم الهندسية المجلد (35) العدد (4) 2013
Tishreen University Journal for Research and Scientific Studies - Engineering Sciences Series Vol. (35) No. (4) 2013

Review of the causes of energy waste in WSN and classification of some attacks that target source of energy based on B-MAC protocol

Dr. Radwan Dandeh [*]
Dr. Kassem Kabalan [**]
Muddar Wainis [***]

(Received 27 / 1 / 2013. Accepted 27 / 5 / 2013)

∇ ABSTRACT ∇

Wireless sensor network have become widely used in many civil and military issues. Like all other network, it is exposed to attacks but its simplicity structured (CPU & memory) prevent the traditional defense technic to be applied, so they need a special for defense.

Most security researches focus on data righteousness and privacy, in this research we focus on attacks that aimed to the power resources which are referred as Denial Of Sleep attacks (DoS), in this attacks the attacker try to keep the sensor in active phase causing the power source to be drained very quickly so that it is a very dangerous attack.

In this research we reviewed the sources of energy Loss in wireless sensor network and classified the attacks that target the power resource, we built a simulation module to analysis the B-MAC protocol response to denial of sleep attacks.

Key Words: WSN, Denial Of Sleep, MAC, Security

[*]**Professor, Department of Computer Systems and Networks, Faculty of Information Engineering, Tishreen University, Lattakia, Syria.**
[**]**Assistant Professor, Department of Computer Systems and Networks, Faculty of Information Engineering, Tishreen University, Lattakia, Syria..**
[***]**Postgraduate Student, Department of Computer Systems and Networks, Faculty of Information Engineering, Tishreen University, Lattakia, Syria.**

مقدمة:

الحساسات اللاسلكية عبارة عن مجموعة من أجهزة الاستشعار التي تستخدم في نقل أو متابعة ظاهرة فيزيائية أو كيميائية محددة (كالحرارة، الرطوبة، الاهتزاز، الضوء،... الخ) ومن ثم نقل المعلومات عن الظاهرة لاسلكياً إلى مركز معالجة البيانات للاستفادة منها دون توافر الإنسان في مكان الظاهرة الفيزيائية، وقد أصبحت مؤخراً واسعة الانتشار نظراً للتطور التقني، إذ أصبح من الممكن إنتاجها بأحجام صغيرة وتكلفة قليلة، وأصبحت تستخدم في شتى المجالات المدنية والعسكرية والبحث العلمي. ومثل كل الشبكات اللاسلكية فإن شبكات الحساسات اللاسلكية عرضه للاختراق، لكن بسبب بساطة تركيبة المعالج فيها ومحدودية الطاقة يتعذر استخدام تقنيات صد الهجمات التقليدية في الشبكات اللاسلكية. من أشهر البروتوكولات التي تستخدم في هذه الشبكات B-MAC [1] كون استخدامه يتطلب موارد قليلة من الذاكرة و المعالج [2]. سنقوم في هذا البحث بتحليل البروتوكول B-MAC ودارسة قابلية اختراقه لهجمات رفض الدخول في وضع الإثبات.

أهمية البحث وأهدافه:

بسبب ما ذكرناه من أهمية شبكات الحساسات اللاسلكية وانتشارها الواسع في مختلف المجالات أصبح لحماية البيانات وضمان سلامة وصولها إلى مركز المعالجة أمراً مهماً، وبما أن اتصالية الشبكة في الحساسات اللاسلكية تعتمد على كل الحساسات في طريق البيانات إلى مركز المعالجة فإن خروج بعض الحساسات عن العمل يؤدي إلى تعطل الشبكة أو جزء منها، وبما أن مصدر الطاقة المستخدم فيها محدود (بطاريات) فإن إشغال الحساسات بمعالجة بيانات مهاجم قد يؤدي إلى استنفاد مصدر الطاقة في الحساسات ويؤدي ذلك إلى تخفيض عمر الشبكة من عدة سنوات إلى عدة ساعات، ونظراً لوجود هذه الحساسات (غالباً) في مناطق مفتوحة مثل الغابات أو واسعة الانتشار كالصحارى أو يصعب الوصول إليها كمراقبة البراكين فإن استبدال البطاريات يصبح أمراً غير ممكن، لذلك كان من الأهمية بمكان البحث عن آليات للكشف عن الهجمات التي تستهدف الحساسات وصدها.

طرائق البحث ومواده:

تم إجراء هذا البحث باستخدام بيئة المحاكاة OMNet++ بالإضافة إلى البنية MiXiM والتي تحتوي أنموذجاً للبروتوكول B-MAC.

استهلاك الطاقة في الحساسات اللاسلكية:

إن تصميم البرتوكول MAC لشبكات الحساسات اللاسلكية يجب أن يراعي مسألتين أساسيتين الأولى هي البنية التحتية (كونه سيتم نشر عدد كبير من الحساسات، ويجب أن تحقق هذه الحساسات اتصالية فيما بينها) المسألة الثانية هي أن تتشارك الحساسات في وسط الاتصال بشكل عادل وفعال، كما ويجب أن يحقق أكبر توفير ممكن للطاقة[3] . تستخدم بروتوكولات MAC خوارزميات مختلة لتوفير طاقة البطاريات مثل إطفاء المستقبلات اللاسلكية عند عدم الحاجة لها (عندما لا يقوم بإرسال أو استقبال بيانات). يبين الجدول (1) أهمية جعل دورة الخمول للعقد أعظمية وذلك بملاحظة أن طاقة الإرسال والاستقبال أكبر بثلاث مراتب عشرية من الطاقة في وضع الخمول[4].

الجدول (1) استهلاك الطاقة لبعض أنواع الحساسات

		Mica2	Tmote Sky
Power Consumption(mW)	Receive	36.81	64.68
	Transmit	87.90	55.20
	Sleep	0.090	0.114

ويمكن تحديد عمر الحساس من المعادلة (4.1) و (4.2)

$$T_{sensoorliftme} = \frac{C_{battery(mWh)}}{(R_{sleep})(P_{sleep(mw)})+(1-R_{sleep})(P_{active(mW)})} \qquad (4.1)$$

حيث دورة الخمول R_{sleep}

$$R_{sleep} = T_{sleep}/(T_{active} + T_{sleep}) \qquad (4.2)$$

T_{sleep} و T_{active} زمن الخمول والتشغيل على التوالي.

P_{sleep} و P_{active} الاستطاعة المستهلكة في وضع الخمول والتشغيل على التوالي، و $C_{battery}$ سعة البطارية (ميلي واط ساعي) وبما أن P_{active} أكبر بثلاث مراتب عشرية من P_{sleep} لذلك يجب إبقاء العقدة في وضع الخمول لأطول مدة ممكنة. بسبب الفرق بين الاستقبال والخمول يمكن زيادة عمر الشبكة بشكل أسي كلما زدنا زمن الخمول[4]. أما بالنسبة للمهاجم فإن تخفيض زمن الخمول لبضع درجات بالمئة يؤدي إلى أثر كبير من ناحية تخفيض عمر الشبكة.

مسببات هدر الطاقة في WSN:

توجد أربعة أنواع أساسية تؤدي إلى هدر الطاقة في شبكات الحساسات اللاسلكية:**[6][5]**

- التصادمات Collisions
- التسميع Overhearing
- رزم التحكم الزائدة Control packet overhead
- الإصغاء في حالة لاعمل Idle listening

1 التصادمات Collisions

عندما تكون رزم البيانات المرسلة مخربة نتيجة التداخل فإنه يجب أن ترفض ويعاد إرسالها، علماً أن إعادة الإرسال يؤدي إلى استهلاك طاقة زائد و يسبب تأخيراً في زمن الوصول.

2 التسميع Overhearing

إن عملية استقبال العقدة لرزمة بيانات خاصة بعقدة أخرى يطلق عليه اسم التسميع. ويؤدي استقبال هذه الرزم من قبل عقدة ما إلى استهلاك طاقة غير ضروري.

3 رزم التحكم الزائدة Control packet overhead

إن إرسال واستقبال رزم التحكم بين العقد يؤدي إلى زيادة في استهلاك الطاقة.

4 الإصغاء في حالة لاعمل Idle listening

الطاقة المهدورة في العقدة التي يكون فيها الراديو في حالة الاستقبال عند عدم وجود للإرسال يسمى الإصغاء في حالة اللاعمل.

الهدف الرئيس لبروتوكولات MAC في شبكات الحساسات اللاسلكية هو تقليل استهلاك الطاقة الناجم عن الإصغاء في حالة اللاعمل والتسميع والتصادمات.

الأمان في شبكات الحساسات اللاسلكية:

ترتكز معظم أبحاث الأمان في شبكات الحساسات على سلامة وسرية البيانات بالإضافة إلى حماية الشبكات من هجمات رفض الخدمة لشبكات الحساسات اللاسلكية. سنقوم هنا بالتركيز على الهجمات التي تستهدف استنفاد الطاقة في شبكات الحساسات اللاسلكية والتي يطلق عليها اسم Denial Of Sleep (DoS) رفض الدخول بوضع الإثبات، إذ يقوم المهاجم بمحاولة إبقاء مستقبلات العقدة في حالة عمل دائم وبالتالي يؤدي إلى استهلاك موارد الطاقة (المحدودة) في العقدة.

1 تصنيف هجمات رفض الثبات للطبقة MAC في شبكات الحساسات اللاسلكية:

يمكن تصنيف هجمات رفض الدخول في وضع الإثبات للطبقة MAC في شبكات الحساسات اللاسلكية بالاعتماد على مستوى معلومات البروتوكول المستخدم ومستوى اختراق الشبكة من قبل المهاجم. و يقصد بمستوى الاختراق قدرة المهاجم على قراءة وإرسال سيل بيانات (Traffic) موثوق في الشبكة. في حال كانت بروتوكولات الشبكة معرفة فإن ذلك يجعلها أكثر عرضة للاختراق وخاصة إن لم يتم استخدم تقنيات تشفير أو كانت تقنيات التشفير مكشوفة. لكن وبسبب محدودية الموارد في شبكات الحساسات اللاسلكية فإن التقنيات المستخدمة للاتصال والتشفير لا تكون قوية كما في الشبكات التقليدية. إن أبسط أنواع الهجمات هو إحداث تزاحم على الطبقة الفيزيائية لكنه أسلوب غير فعال في تنفيذ هجمات رفض الإثبات في شبكات الحساسات اللاسلكية كونه يتطلب من المهاجم موارد طاقة كبيرة لإحداث الأثر المطلوب. إستراتيجية الهجوم الأكثر فاعلية هي استخدام معلومات البروتوكولات MAC لتوليد هجوم يؤدي إلى استنزاف مصدر الطاقة للحساس. بهذا تجعل الشبكة عديمة الجدوى وتبطل أي وسلية أمان أخرى. مما سبق يتنج ثلاثة أنواع لهجمات رفض الدخول في حالة الثبات للطبقة MAC

1- **النوع الأول لاتوجد معلومات عن البروتوكول ولاتوجد إمكانية لاختراق الشبكة:** دون وجود معلومات عن البروتوكول MAC المستخدم تقتصر الهجمات الممكنة على التزاحم في الطبقة الفيزيائية وهجمات الإعادة غير الذكية عن طريق تسجيل سيل البيانات وإعادة إرساله ضمن الشبكة، يؤدي ذلك إلى صرف طاقة إضافية لاستقبال ومعالجة هذه الرزم الإضافية. يتم نقل سيل البيانات المعاد إرساله ضمن الشبكة من قبل كل العقد على المسار إلى العقدة الهدف مسبباً استهلاك طاقة إضافي في كل العقد على طول المسار.

2- **النوع الثاني معرف كاملة بالبروتوكول ولا توجد قابلية لاختراق الشبكة:** يمكن تحديد البروتوكول المستخدم من خلال تحليل سيل البيانات. وبمعرفة البروتوكول المستخدم يمكن توسيع إمكانية الهجوم ليشمل التزاحم الذكي، من خلال إرسال سيل البيانات في الشبكة، أو يكون أكثر انتقائية حول إعادة إرسال سيل البيانات السابق. التزاحم الذكي [7] يستخدم معلومات بروتوكول طبقة الاتصال ليخفف إنتاجية الشبكة دون الاعتماد على إشارة تزاحم ثابتة. يتميز هذا النوع من الهجمات بالمقارنة مع هجمات التزاحم الثابتة على الطبقة الفيزيائية في أنه يحافظ على طاقة المهاجم في حال كانت العقدة المهاجمة لها موارد محدودة مثل العقد المستهدفة. ويبقى لهذا الهجوم أهميته حتى لو لم يكن لاستهلاك

الطاقة عند المهاجم أهمية كونه يمكن استخدام التزاحم الذكي لجعل اكتشاف الهجوم على الشبكة أكثر صعوبة. إن تم إضافة عنوان مصدر وهدف صالحين من قبل المهاجم، ينجم عن ذلك أن تبقى العقدة نشطة لتلقي الرزم، حتى لو كانت ستهمل فيما بعد بسبب عدم التخويل، فإن كانت الرزم مشفرة يجب أن تتلقى العقدة كامل الرزمة قبل فك التشفير ورفضها.

3-**النوع الثالث معلومات كاملة عن البروتوكول والشبكة مخترقة:** يمكن أن تكون الهجمات في هذا النوع فتاكة بالنسبة لشبكات الحساسات اللاسلكية. فبالمعرفة الكاملة للبروتوكول MAC وإمكانية إرسال سيل البيانات موثوق يمكن أن يولد المهاجم سيل البيانات ليكسب أكبر احتمال من الهجمات رفض الدخول في حالة الإثبات.

4-**النوع الرابع لاتوجد معلومات عن البروتوكول لكن توجد إمكانية لاختراق الشبكة:** لم تأخذ بالحسبان كون إمكانية اختراق الشبكة تتطلب معرفة كاملة ببروتوكول MAC.

الجدول(2) يصنف أنواع الهجمات رفض الدخول في حالة الإثبات المتوافرة بالاعتماد على معلومات المهاجم عن البروتوكول المستخدم وقابلية اختراق الشبكة.

الجدول (2) أنواع الهجمات رفض الدخول في حالة الثبات

نوع الهجوم	ازدحام ثابت	ازدحام مخادع	ازدحام عشوائي	ازدحام ذكي	إرسال غير موثوق	إعادة غير ذكي	إعادة ذكي	احتلال كامل
لاتوجد معلومات عن البروتوكول لاتوجد إمكانية لاختراق الشبكة	√	√	√			√		
معرف كاملة بالبروتوكول ولاتوجد قابيلة لاختراق الشبكة	√	√	√	√	√	√	√	
معلومات كاملة عن البروتوكول والشبكة مخترقة	√	√	√	√	√	√	√	√

البروتوكول (B-MAC) :

البروتوكول (B-MAC) هو أحد البروتوكولات التي تعتمد على النفاذ المتعدد بتحسس الحامل (CSMA) مع آلية للاستهلال (Preamble) [8]. و يستخدم البروتوكول B-MAC تقنية التنصت منخفض القدرة (LPL) لتوفير استهلاك الطاقة عن طريق تنشط المستقبلات خلال دور ثابت والقيام بفحص القناة اللاسلكية للبحث عن بايتات استهلال صالحة من عقد أخرى. تقوم العقد التي لديها بيانات لإرسالها بإرسال استهلال أطول من دور فحص القناة اللاسلكية للمستقبل وذلك للتأكد من أن كل العقد المجاورة ستتمكن من اكتشاف الاستهلال واستقبال البيانات.إن دور فحص القناة يتم تحديده بحسب عدد العقد ومعدل النقل في الشبكة، في [9] بين Polastre et al أنه في ظروف مثالية يمكن أن تكون دورة العمل للبروتوكول B-MAC هي 1% في الشبكات ذات سيل البيانات المنخفض، الشكل (1) يشرح العمليات الأساسية للبروتوكول B-MAC.

1 أنموذج الطاقة في البروتوكول B–MAC:

يتألف أنموذج الطاقة في البروتوكول B–MAC من خمسة عناصر تستهلك الطاقة وهي طاقة الإرسال E_{tx} وطاقة الاستقبال E_{rx} وطاقة التنصت E_{listen} وطاقة لتحسس بيانات العينات E_{sensor} والطاقة في وضع الخمول E_{sleep} [10]. تقاس الطاقة إما بالميلي جول أو الميلي واط فتكون الطاقة الكلية كما في المعادلة (7.1):

$$E= E_{tx} + E_{rx} + E_{listen} + E_{sensor} + E_{sleep} \quad (7.1)$$

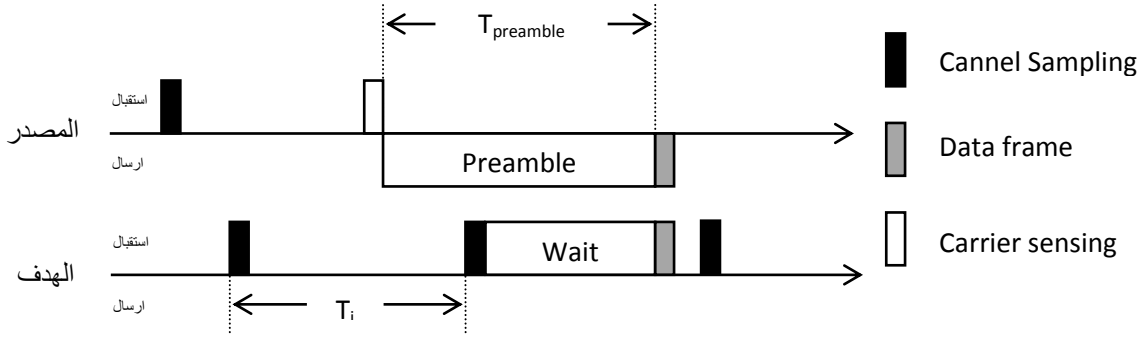
يلزم لكل عقدة زمن T_{sensor} لتشغيل حساساتها وأخذ العينات وجمع البيانات. فإذا كان جمع البيانات خلال T_s دقيقة فإن معدل أخذ العينات يعطى بالمعادلة (7.2) :

$$r_s = \frac{1}{T_S \times 60} \quad (7.2)$$

يتم تحديد معدل أخذ العينات بحسب التطبيق المطلوب وظروف الشبكة. وتعطى علاقة طاقة أخذ العينات من المعادلتين (7.3) و (7.4):

$$T_d = T_{sensor} \times r_s \quad (7.3)$$
$$E_{sensor} = T_d . C_{sensor} . V \quad (7.4)$$

حيث Td هو تردد أخذ العينات و C_{sensor} هو التيار المستجر أثناء أخذ العينات و V هو الجهد المستخدم.



الشكل (1) العمليات الأساسية للبروتوكول B–MAC

تعطى الطاقة المستهلكة خلال الإرسال من طول رزمة الاستهلال $N_{preamble}$ ورزمة البيانات N_{data} ومعدل رزم البيانات المولدة من التطبيق من العلاقتين (7.5) و (7.6):

$$T_{tx} = r_s \times \left(N_{preamble} + N_{data}\right) . T_{txb} \quad (7.5)$$
$$E_{tx} = T_{tx} . C_{txb} V \quad (7.6)$$

حيث T_{tx} تردد إرسال الرزم، C_{txb} التيار المستجر عند إرسال بايت واحد و T_{txb} عبارة عن الزمن اللازم لإرسال بايت واحد. طاقة الاستقبال في العقدة عبارة عن عدد الرزم المستقبلة من n عقدة مجاورة بغض النظر عن العقدة الهدف. لذلك فإن الطاقة المستهلكة خلال الاستقبال تعطى من العلاقة (7.7) و (7.8):

$$T_{rx} \leq n . r_s \times \left(N_{preamble} + N_{data}\right) . T_{rxb} \quad (7.7)$$
$$E_{rx} = T_{rx} . c_{rxb} V \quad (7.8)$$

حيثT_{rx} هي تردد إرسال الرزم،C_{rxb} التيار المستجر عند استقبال بايت واحد وT_{rxb} الزمن اللازم لاستقبال بايت واحد.

3 -تحليل الهجمات على البروتوكول B-MAC:

3-1 النوع الأول هجوم الازدحام الثابت: عند تعرض العقد التي تستخدم B-MAC لهجوم ازدحام ثابت يقوم البروتوكول بفحص القناة اللاسلكية دورياً ويستخدم العينات السابقة لتحديد قيمة العتبة للضجيج، فيتم التعامل مع هجوم الازدحام الثابت كضجيج ويتم إهماله. لذلك فإن هذا الهجوم يمنع العقد من تبادل المعلومات ولكنه لا يمنعها من الدخول في طور الإثبات.

3-2 النوع الثاني هجوم الإرسال غير المخول: يمكن تحقيق هذا الهجوم بإرسال سيل من الرزم في الشبكة توافق كل قواعد البروتوكول من توقيت ومعاملة التصادمات. حيث يتم استقبال هذه الرسائل من قبل كل العقد و يتم رفضها بسبب عدم التخويل لكن و بالرغم من عدم التخويل فإن بقاء العقد في حالة تنشط لاستقبال الرسالة يؤدي إلى تقليص عمر الشبكة. حيث على العقد أن تبقى في حالة تنصت بمعدل نصف طول الاستهلال مضافا إليه زمن رزمة البيانات المعادلة (7.9) حيث $T_{preamble}$ وT_{pkt} هما زمن الاستهلال و زمن رزمة البيانات على التعاقب:

$$awake\ percentage = \left[\frac{\left(\frac{T_{preamble}}{2}+T_{pkt}\right)}{(T_{preamble}+T_{pkt})}\right] \qquad (7.9)$$

يمكن للمهاجم أيضاً أن يسجل إرسال أطول رزمة للبيانات ويعيد إرسالها إلى الشبكة. كلا الهجومين له نفس أثر رفض الدخول في حالة الإثبات.

3-3 النوع الثالث هجوم الاحتلال الكامل: أكثر الهجمات فعالية ضد البروتوكول B-MAC هو التزاحم المخادع. وعلى العكس من التزاحم الثابت فإن التزاحم المخادع يمنع العقد التي تستخدم البرتوكول B-MAC من الدخول في طور الإثبات. فحالما تتنشط العقد التي تستخدم B-MAC وتكتشف وجود استهلال تبدأ دورة استقبال البايتات وتبحث عن بايتات التزامن التي تشير إلى رزمة البيانات المتوقع استقبالها. وبالتالي ستقوم العقدة المهاجمة بمعالجة الاستهلالات المستقبلة بشكل مستمر بحثاً عن البيانات ذلك الأمر يؤدي إلى بقائها في حال تشغيل بشكل دائم. لذلك فهو هجوم فعال من هجمات رفض الدخول في حالة الإثبات، لكن على المهاجم أيضاً أن يبقى يعمل كامل الوقت، ما يجعله غير فعال إن كان المهاجم محدود الموارد. لكن بالرغم من عدم فعاليته، فإن هذا الهجوم يبقي الضحية في حالة عمل لكامل الوقت وهو سهل التطبيق، فالمعلومة الوحيدة التي يحتاج إليه المهاجم أنه يتم استخدام B-MAC حتى يبقي جميع العقد في الشبكة في حالة استقبال لاستنفاد مدخراتها بسرعة كبيرة.

النتائج والمناقشة :

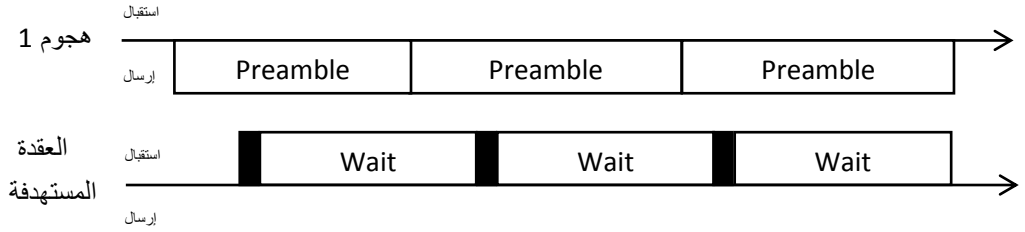
تم اختيار بيئة المحاكاة ++OMNet وهي محاكي شبكات مفتوح المصدر، وهو متوافر بشكل مجاني للعمل الأكاديمي وقمنا بتنصيب البنية MiXiM (mixed simulator) وهي عبارة عن بنية لمحاكات للشبكات اللاسلكية والنقالة في ++OMNet وهي نتيجة لدمج مجموعة من بيئات محاكاه المتوافرة، حيث تم أخذ البنية الأساسية وإدارة الوصلات بين العقد ودعم حركة العقد من البنية Mobility Framework [11] ، وتم أخذ أنموذج انتشار الراديو من

البنية (channel simulator) ChSim [12]، ومكتبة البروتوكولات من البنيات Mac Simulator [13] و Positif Framework [14] و Mobility Framework . وهي متوافرة بشكل مجاني على الانترنت.

1 تصميم عقدة مهاجمة:

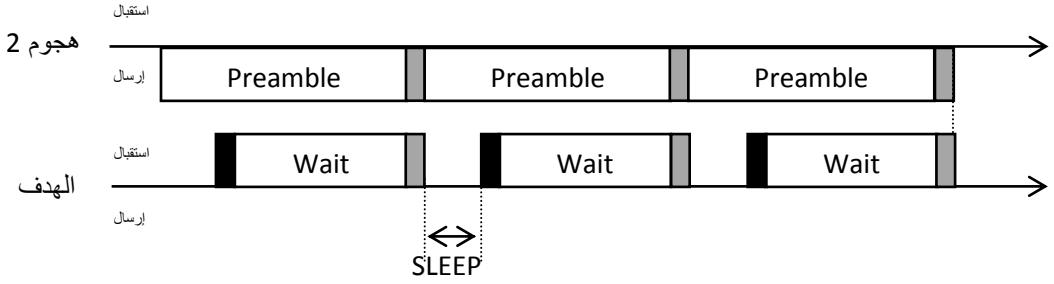
قمنا بتصميم عقد تحقق هجوم رفض الدخول في حالة الإثبات بثلاث طرق كما يلي:

العقدة المهاجمة الأولى بما أنه في التزاحم الثابت يتم إرسال حزم بيانات بشكل دائم بحيث تسبب تزاحماً في الوسط الفيزيائي، الذي يؤدي إلى تعطيل إرسال البيانات ولا يحقق حالة رفض الدخول في حالة الإثبات لم نقم بنمذجته، لكن قمنا بنمذجة (التزاحم المخادع) حيث قمنا بكتابة أنموذج بالاعتماد على الأنموذج B–Mac فيMiXiM المكتوب بلغة C++ فقما بإجراء تعديلات على الملف المصدر لتقوم العقدة بإرسال Preamble بشكل مستمر الشكل (2).



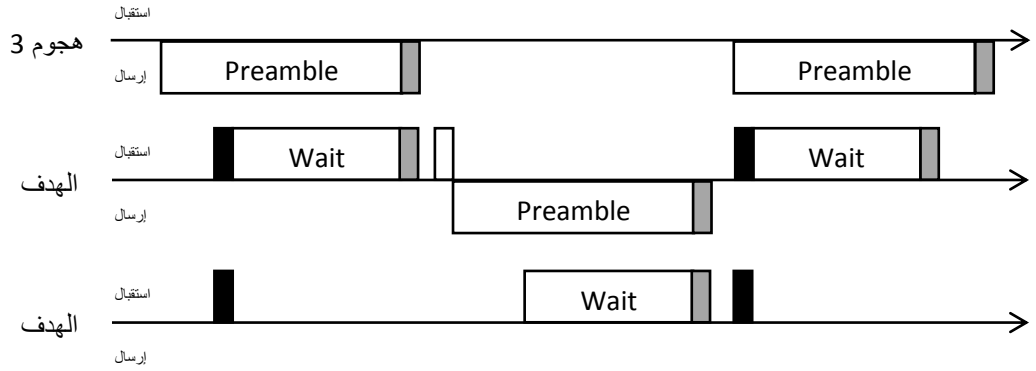
الشكل (2) استجابة البروتوكول B–MAC للهجوم الأول

العقدة المهاجمة الثانية على افتراض أننا لدينا معلومات البرتوكول ولا توجد قابلية لاختراق الشبكة (البيانات مشفرة). فقد تم تعديل الملف المصدر للعقدة السابقة لترسل مع الاستهلال بيانات عشوائية بحيث تحقق هجوم الإرسال غير المخول الشكل (3) حيث ستضطر العقدة المعرضة للهجوم لكن إلى استقبال كامل رزمة البيانات وبعدها تقوم برفض البيانات المستقبلة بسب عدم التخويل.



الشكل (3) استجابة البروتوكول B–MAC للهجوم الثاني

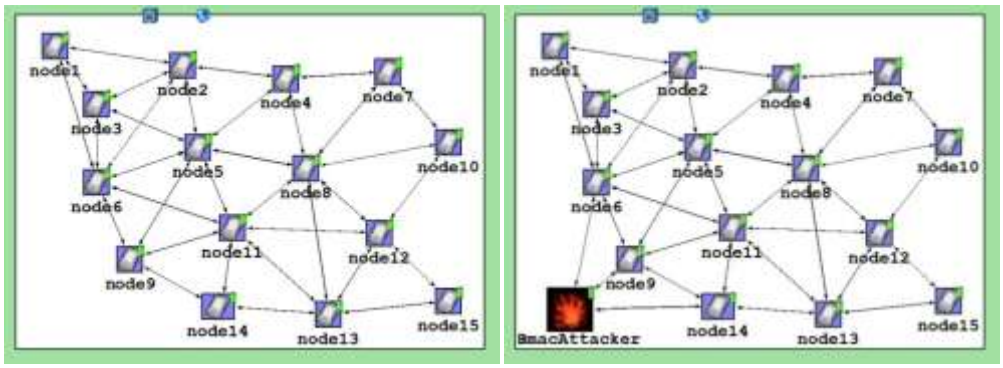
العقدة المهاجمة الثالثة بافتراض أن معلومات البروتوكول معروفة والشبكة مخترقة قمنا باستخدام الأنموذج B–MAC في MiXiM وقمنا بتعديله ليقوم بإرسال بيانات موثوقة بشكل مستمر(بما أن كامل معلومات البروتوكول معلومة من قبل المهاجم) وبفواصل زمنية تتيح إمكانية تمرير البيانات إلى عقد أخرى وبما أن البيانات المرسلة تحقق متطلبات البروتوكول فإنه سيتم تمريرها عبر عقد الشبكة إلى العقدة الهدف الشكل (4).



الشكل (4) استجابة البروتوكول B-MAC للهجوم الثالث

2 أنموذج الشبكة المختبر:

لاختبار أثر الهجمات من كل نوع تم وضع سناريو لشبكة مؤلفة من 15عقدة تستخدم البروتوكول B-MAC وتم توزيعها كما في الشكل (5). لقد تم اختيار عدد العقد وكيفية توضعها بحيث تكون بعض العقد (6-9-14) ضمن المجال اللاسلكي للمهاجم، وبعض العقد (11-12-13-15) تؤمن مسار بيانات لتلك العقد إلى الهدف وأخرى بعيدة عن الهجوم المباشر وليست في مسار البيانات إلى الهدف للعقد المهاجَمة.



A) عند عدم وجود هجوم **B) عند التعرض لهجوم**

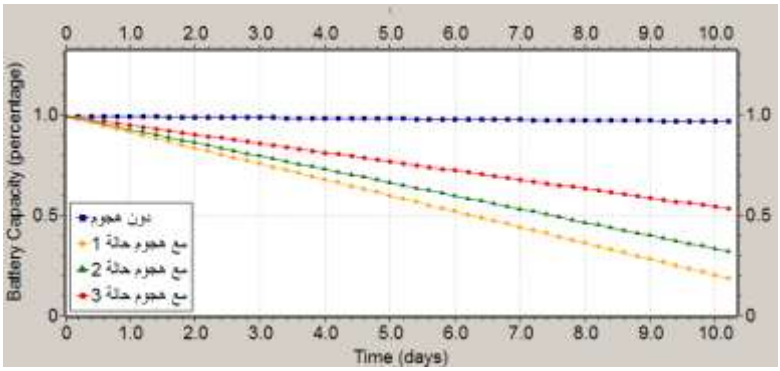
الشكل (5) أنموذج الشبكة المختبر

تم استخدام محددات الطاقة المذكورة في الجدول (3) على اعتبار أن شريحة (الإرسال الاستقبال) المستخدمة هي CC2420 [15]. وتم تنفيذ السيناريو لمدة 10 أيام وذلك في أربع حالات: دون وجود هجوم ومع وجود هجوم لكل من الأنواع الثلاث المذكورة في 7-1 وبعد جمع البيانات وتمثليها بيانياً حصلنا على النتيجة في الشكل (6) والذي يعبر عن الطاقة المتبقية في البطارية للعقدة الواحدة التي تعرضت للهجوم خلال مدة التشغيل في كل حالة. والشكل (7) يبين الطاقة المستهلكة في كل العقدة عند كل حالة.

الجدول (3) المحددات المستخدمة في النمذجة

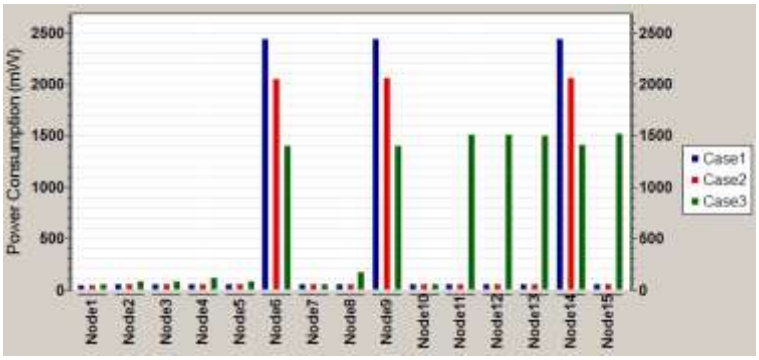
Frequency	2.4 GHz	التردد
Sleep Current	0.02 mA	تيار الإثبات
Tx Current	17 mA	تيار الإرسال
Rx Current	16.4 mA	تيار الاستقبال
Battery capacity	1000 mAh	سعة البطارية
Check Interval	0.1s	دور الاستهلال

نلاحظ من الشكل (6) أن استهلاك الطاقة في الحالة الطبيعة (دون وجود مهاجم) وبعد عشرة أيام لم يتجاوز 3.5% من سعة البطارية أما في حالة وجود مهاجم من النوع الأول كانت الطاقة المصروفة تشكل 80% من سعة البطارية و67% للحالة الثانية و46% للحالة الثالثة، أي أن استهلاك الطاقة يكون أعظمياً عند استخدام العقدة المهاجمة من النوع الأول.



الشكل(6) الطاقة المتبقية في البطاريات خلال 10 أيام عمل

لكن بملاحظة الشكل (7) نلاحظ أن تأثير الهجوم باستخدام النوع الأول والثاني اقتصر على العقد 6-9-14 وهي العقد التي تقع ضمن المجال الراديوي للمهاجم بينما لم تتأثر باقي العقد. و بالرغم من خروج جزء من الشبكة عن العمل لكن الشبكة حافظت على الاتصالية (حسب السناريو المفترض لكن يمكن في توزيع آخر للعقد أو توضع مختلف للمهاجم أن يؤدي إلى تعطل الشبكة بالكامل).



الشكل(7) استهلاك الطاقة في العقد خلال 10 أيام

نلاحظ أيضاً أن زيادة استهلاك الطاقة في حالة استخدام مهاجم من النوع الثالث تمتد بالإضافة للعقد 6-9-14 التي تقع ضمن المجال الراديوي للمهاجم إلى العقد 11-12-13-15 التي تقع في مسار البيانات حيث يرتفع فيها استهلاك الطاقة من(56mW) في الحالة الطبيعية إلى (1407mW) عند الهجوم من النوع الثالث، وكون هذه العقد تقع في مسار البيانات إلى الهدف فإن هذا الاستهلاك الكبير للطاقة يؤدي إلى نفاد مدخراتها وبالتالي قطع في مسار البيانات وتعطل الشبكة عن العمل.

يمكن أن يستمر عمل الشبكة في الحالة الطبيعية دون استبدال البطاريات لمدة تتجاوز العام، لكن تعرض الشبكة لهجمات من النوعين الأول والثاني يؤدي إلى تدمير جزء الشبكة الذي يقع ضمن المجال الراديو للمهاجم (العقد 6-9-14) خلال 15يوم، وعندما يكون الهجوم من النوع الثالث تنهار الشبكة خلال 20 يوم ويكون التخريب على نطاق أوسع (يشمل العقد6-9-14-11-12-13-15).

الاستنتاجات والتوصيات:

قمنا في هذا البحث باستعراض مسببات هدر الطاقة في شبكات الحساسات اللاسلكية وتصنيف الهجمات التي تستهدف منابع الطاقة وبعد استعراض طريقة عمل البروتوكول B-MAC وتحليل الهجمات التي قد تستهدف الطاقة في العقد التي تستخدم البروتوكول B-MAC قمنا بنمذجة عقد تحاكي عمل هجمات رفض الدخول في حالة الإثبات وتم تطبيقها على سيناريو مفترض ومنها بينا أثر هذه الهجمات على عمل الشبكة.

مما تقدم نلاحظ الأثر الكبير للهجمات التي تستهدف مصدر الطاقة في شبكة الحساسات اللاسلكية (هجمات رفض الدخول في حالة الإثبات). وحيث أن معظم أبحاث الأمان في شبكات الحساسات اللاسلكية تعتمد على سرية البيانات وموثوقيتها فيجب الأخذ بالحسبان مسألة الطاقة التي تضمن استمرارية عمل الشبكة. من دون تأمين آلية لصد الهجمات أو التنبيه لوجودها يتيح للمخترق إمكانية تعطيل عمل الشبكة أو جزء منها، يمكن متابعة البحث لإيجاد آليات لصد الهجمات من نوع رفض الدخول في حالة الإثبات أو التخفيف من أثرها.

المصطلحات:

Berkeley Medium Access Control (B-MAC)	بروتوكول بركلي للتحكم بالنفاذ للوسط
Carrier Sense Multiple Access (CSMA)	النفاذ المتعدد بتحسس الحامل
Collisions	التصادمات
Control packet overhead	رزم التحكم الزائدة
Denial of sleep (DoS)	رفض الدخول بوضع الإثبات
Low-Power Listening (LPL)	التنصت منخفض القدرة
Overhearing	التسميع
Preamble	الاستهلال
Traffic	سيل البيانات
Wireless Sensor Network (WSN)	شبكات الحساسات اللاسلكية

المراجع:

1-FORSTER, A. ,*Implementation of the B-MAC Protocol for WSN in MiXiM*. Networking Laboratory, University of Applied Sciences of Southern SwitzerlandK 2009, 2pages.

2-STANKOVIC, J. A. *Wireless Sensor Networks.* University of Virginia, Charlottesville Virginia , 2006, 20 pages.

3- YADAV, R. et al. *A survey of MAC protocols for wireless sensor networks.* UbiCC journal, 2009, 7Pages.

4- RAYMOND, D. *Effects of Denial-of-Sleep Attacks on Wireless Sensor Network MAC Protocols.* IEEE Transactions on Vehicular Technology , vol. 58, no. 1, 2009, 14Pages.

5- WEI, Y.; HEIDEMANN, J. ; ESTRIN D. *An Energy-Efficient MAC Protocol for Wireless Sensor Networks*. IEEE INFOCOM, New York, Vol. 2, 2002, pp. 1567-1576 .

6- VANDAM, T. ; Langendoen, K. *An Adaptive Energy Efficient MAC Protocol for Wireless Networks*. in Proceedings of the First ACM Conference on Embedded Networked Sensor Systems ,2003, PP 171- 180.

7-NEGI, R. ; PERRIG, A. *Jamming analysis of MAC protocols*. Carnegie Mellon Univ, Pittsburgh, PA, 2003, Pages4.

8-SINGH, H. ; BISWAS, B. *Comparison of CSMA based MAC protocols of wireless sensor networks*. International Journal of AdHoc Network Systems, Vol2, N2, 2012, Pages 10.

9-POLASTRE, J. ;HILL J. ;CULLER D. *Versatile low power media access for wireless sensor networks*. in Proc. 2nd ACM Int. Conf. Embedded Netw. Sensor Syst., 2004, pp. 95–107.

10- AHMAD, M. ; DUTKIEWICZ E. ; HUANG X. *A Survey of Low Duty Cycle MAC Protocols in Wireless Sensor Networks*. Emerging Communications for Wireless Sensor Networks, 2010, Pages 23.

11- Mobility framework (MF) for simulating wireless and mobile networks using OMNeT++. 1/12/2012. <http://mobility-fw.sourceforge.net>.

12- PAWLAK, T. ;VALENTIN, S. *ChSim a wireless channel simulator for OMNeT++*. TKN Simulation Workshop 2006, Technical University of Berlin, Germany, 2006, 2/12/2012 <http://wwwcs.upb.de/cs/chsim>.

13- MAC simulator. 25/11/2012. <http://www.consensus.tudelft.nl/software.html>.

14- Positif localization simulation framework. 1/12/2012, <http://www.consensus.tudelft.nl/software.html>.

15- Chipcon Corporation, CC2420 DataSheet [Online]. 1/12/2012, <http://inst.eecs.berkeley.edu/~cs150/Documents/CC2420.pdf>