تقييم أداء نواة محاكي شبكات الحساسات اللاسلكية باستخدام خوارزمية المصادقة

د. مثنى القبيلي*

د. سامر سليمان**

غيداء محمَّد اسبر***

(تاريخ الإيداع 22 / 11 / 2020. قُبِل للنشر في 1/ 7 / 2021)

□ ملخّص □

تقدم برامج المحاكاة المستخدمة ضمن مجال شبكات الحساسات اللاسلكية تمثيلاً عن النظام الحقيقي دون الحاجة للقيام بعملية نشر فعلية للعقد وما يترافق مع ذلك من تكاليفٍ باهظة، وتكون العمليات المباشرة المعرفة ضمن الطبقة الفيزيائية في معظم هذه البرامج ضمنية وغير مقدمة بشكلٍ واضح، وهذا ما دفعنا إلى بناء نواة لنظام منصة محاكاة افتراضية، لنكون بذلك قادرين على محاكاة عمليات البروتوكولات والخوارزميات المطبقة ضمن شبكات الحساسات على مستوى وحدة المعالجة المركزية. تهدف منصة المحاكاة المقترحة إلى مراقبة تنفيذ العمليات على المستوى المنخفض للبنية الفيزيائية لعقد الحساسات مع القدرة على التعديل عند هذا المستوى. وباعتبار أن أمن التوجيه يشكل أحد أهم التحديات ضمن شبكات الحساسات، لذا سنطبق ضمن هذا العمل إحدى خوارزميات أمن التوجيه ضمن الواجهة المتعلقة بمنصة المحاكاة المقترحة ومراقبة التنفيذ على المستوى المنخفض لعمليات المعالج، الأمر الذي يتيح لنا إمكانية اكتشاف نقاط الضعف والعمل على تحسين الخوارزميات وتطويرها. طُبِّقت ثلاثة سيناريوهات لتقييم أداء منصة المحاكاة المقترحة، حيث بينت النتائج مرونة وفعالية عالية لهذه المنصة في تتبع سير العمليات المنجَزة ضمن عقد الحساسات على مستوى لغة الـ Assembly.

الكلمات المفتاحية: المصادقة (التوثيق)، المعالج الصغري، عقدة الحساس، المحاكاة، المنصة الافتراضية، شبكة الحساسات اللاسلكية.

* أستاذ مساعد، قسم هندسة الاتصالات والالكترونيات، كلية الهندسة الميكانيكية والكهربائية، جامعة تشرين، اللاذقية، سورية.

**مدرس، قسم هندسة الحاسبات والتحكم الآلي، كلية الهندسة الميكانيكية والكهربائية، جامعة تشرين، اللاذقية، سورية.

***طالبة (دكتوراه)، قسم هندسة الاتصالات والالكترونيات، كلية الهندسة الميكانيكية والكهربائية، جامعة تشرين، اللاذقية سورية.

Performance Evaluation of the Kernel Based Wireless Sensor Network Simulator Using an Authentication Algorithm

Dr. Mothanna ALKUBEILY*
Dr. Samer SULAIMAN **
Ghaidaa Mohammad ESBER***

(Received 22 / 11 / 2020. Accepted 1 / 7 / 2021)

□ ABSTRACT □

Wireless sensor network simulation programs provide representation for an actual system, without needing to deploy real testbed which is highly constrained by the available budget, and the direct operations inside physical layer in most of these programs are hidden and work implicitly. This is what motivated us to build a kernel for a virtual simulation platform to be able to simulate protocol operations and algorithms at the node processing unit level, The proposed system aims to observe the execution of operations at the low level of the wireless sensor physical infrastructure with the ability to modify at this level. Since secure routing is considered one of the most challenges in WSN field, so we apply in this paper one of the secure routing algorithms inside the GUI of the proposed system to observe execution at the low level of processor operations, which give us the ability to discover the weakness of algorithms and improve them. Three scenarios were applied to evaluate the performance of the proposed simulation platform. The results demonstrate a high flexibility and effectiveness of this platform in tracing the progress of operations performed within the wireless sensor nodes at the Assembly language level.

Keywords: Authentication, Microprocessor, Sensor node, Simulation, Virtual Platform, Wireless Sensor Network (WSN).

* **Associate Professor, Department of Communication and Electronics, Faculty of Mechanical and Electrical Engineering, Tishreen University, Latakia, Syria.**
** **Assistant Professor, Department of Computer and Automatic Control Engineering, Faculty of Mechanical and Electrical Engineering, Tishreen University, Latakia, Syria.**
*** **PhD. Student, Department of Communication and Electronics, Faculty of Mechanical and Electrical gineering, Tishreen University, Latakia, Syria.**

مقدمة:

تتألف شبكات الحساسات اللاسلكية من عدد من أجهزة الاستشعار صغيرة الحجم، ذاتية التغذية، تدعى عقد حساسة Sensor nodes، وتستخدم لمراقبة ظاهرة فيزيائية محددة في الوسط المحيط، ويمكن أن تزوَّد بتجهيزات إضافية خاصة كالكاميرات والمايكروفونات لتصبح قادرة على التعامل مع الوسائط المتعددة. تنقل هذه الأجهزة المعلومات عن هذه الظاهرة لاسلكياً إلى المحطة القاعدية (المركز) Base station (Sink) للاستفادة منها، وتتميز شبكات الحساسات اللاسلكية بقدرة العقد على جمع المعلومات ونقلها دون الحاجة لإشراف بشري مباشر عليها، وتستخدم هذه الشبكات ضمن مجال واسع من التطبيقات بدءاً من تطبيقات المراقبة والإشراف العسكرية وصولاً إلى مراقبة المرضى وتحسس الظواهر الطبيعية [1,2]، وتواجه عقد الحساسات المستخدمة ضمن هذه الشبكات الكثير من التحديات مثل محدودية الطاقة، محدودية عرض الحزمة، متطلبات جودة الخدمة، مقدرات المعالجة المحدودة، إضافة إلى تحديات الأمن.

تنفَّذ عملية نشر عقد الحساسات ضمن بيئة اختبار فعلية بهدف الحصول على نتائج دقيقة، لكنَّ ذلك يفرض وجود عدد من المعيقات التي تبدأ من الكلفة الباهظة، حيث أنهُ من الصعب شراء عد كبير من عقد الحساسات عند الحاجة لإجراء اختبار في بيئة ممتدة على مساحة واسعة ولاسيما الأبحاث العلمية الأكاديمية، إضافةً إلى عدم القدرة على تكرار الاختبار ضمن بعض البيئات ذات الظروف الخاصة كما هو الحال عند مراقبة البراكين، وهذا ما دعا لاستخدام نمذجة النظم ومحاكاتها والتي تقدم تمثيلاً لهذه النظم، حيث أنَّها تسمح للمستخدمين بأن يراقبوا النظام عن قرب دون الحاجة لإجراء تنفيذ فعلي له [3]، وخلال عملية الاختبار تطبَّق بارامترات مختلفة لدراسة سلوك النظام وبناء على ذلك يقرر المستثمرون فيما إذا كان النظام الحالي مناسباً أو بحاجةٍ للمزيد من التحسين. ركزت برامج المحاكاة الخاصة بشبكات الحساسات اللاسلكية على طبقات الشبكة المختلفة [4]، لكنها لم تقدم معلومات تفصيلية عن عمليات المعالجة ضمن معالج العقدة، حيث أنها تعتمد على قيم بارامترات معرفة مسبقاً من معالج العقدة وفقاً للخصائص المتعلقة بنوع المعالج المعرَّف ضمنَ العقدة، وتقدم نتائج المحاكاة دون إظهار تفاصيل عمليات المعالجة أو على الأقل لا تسمح بمراقبة تسلسل عمليات التنفيذ ضمن معالج العقدة، وهذا ما دفعنا لبناء نواة لنظام منصة محاكاة برمجية افتراضية خطوة – خطوة وذلك بهدف محاكاة الخوارزميات والبروتوكولات على مستوى لغة التجميع لنتمكن بذلك من أن نصف ونراقب بوضوح مجموعة العمليات المستخدمة لتنفيذ البروتوكولات ضمن معالج العقدة، مع القدرة على التعديل والتصحيح عند هذا المستوى.

إنَّ أمن التوجيه يشكل تحدياً أساسياً ضمن هذا النوع من الشبكات حيث أن وسط الاتصال المستخدم هو وسط لاسلكي، مما يسمح لأية عقدة خارجية تقع ضمن مجال الإرسال بالوصول إلى المعطيات المتبادلة والحصول على تلك المعطيات أو العمل على بث معطيات مزيفة ضمن الشبكة [5]، لذا سنطبق إحدى خوارزميات أمن التوجيه ضمن البيئة الافتراضية المصممة، وهي خوارزمية المصادقة بين عقدتين مستقلتين من عقد الحساسات [6] بهدف مراقبة تنفيذ عملياتها على المستوى المنخفض.

أهمية البحث وأهدافه:

تكمن أهمية البحث وأهدافه بالتركيز على مراقبة تنفيذ الخوارزميات والبروتوكولات المستخدمة ضمن شبكات الحساسات اللاسلكية وتحسينها من خلال تصميم نواة لمنصة محاكاة برمجية افتراضية، والتي تأخذ بالحسبان عمليات المستوى المنخفض(عمليات المعالج الصغري) مع وجود إمكانية المراقبة والتعديل على هذا المستوى، الأمر الذي لا يكون متاحاً لدى معظم برامج المحاكاة، والتي تهمل البارامترات المتعلقة بالمعالج وتعتمد على قيم معرفة مسبقاً وفقاً للخصائص المتعلقة بنوع المعالج المعرَّف ضمنَ العقدة، وتقدم النتائج دون إظهار تفاصيل عمليات المعالجة.

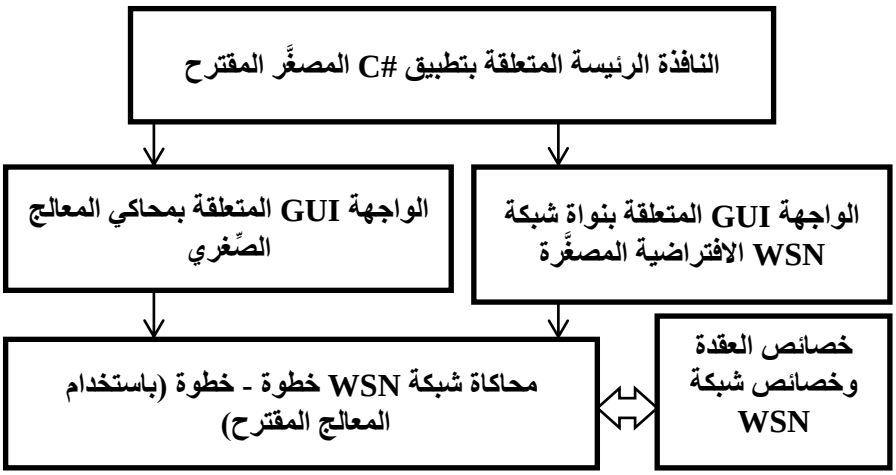
طرائق البحث ومواده:

سنعتمد ضمن طرائق البحث على الجانب التحليلي من خلال دراسة وتحليل عمل خوارزمية المصادقة بين عقدتين مستقلتين من عقد الحساسات واستعراض الخطوات اللازمة لتنفيذها بشكلٍ مفصل، كما سنعتمد على الجانب التجريبي، وذلك من خلال تطبيق هذه الخطوات ضمن بيئة منصة المحاكاة الافتراضية المقترحة.

استخدمنا لبناء تعليمات الخوارزمية التي ستطبق ضمن المعالج المقترح لغة C# (Microsoft Visual Studio C# 2015 language) والتي تعتبر لغة مرنة عند بناء تطبيقات تصميم الواجهات Graphical User Interface (GUI) [7]، وهذا ما سوف يعطينا سهولةً كبيرة ومجالاً واسعاً من خياراتِ التطوير لكامل منصة المحاكاة المقترحة في المستقبل.

1- نواة المنصة البرمجية الافتراضية المصغرة:

اقتُرِحَ في البحث [8] طريقة جديدة لبناء نموذج نواة لنظام منصة محاكاة (خطوة – خطوة) لمحاكاة تفاصيل العمليات المتعلقة بالبروتوكولات وذلك على مستوى منخفض (مستوى لغة الAssembly)، حيث يصف هذا النموذج عن قرب مجموعة عمليات المعالج، والخوارزميات المستخدمة لتنفيذ البروتوكولات ضمن معالج عقدة الحساس، ويبين الشكل (1) مخططاً يوضح العلاقات الوظيفية ضمن تطبيق المحاكي الافتراضي.



الشكل (1): العلاقات الوظيفية ضمن تطبيق المحاكي الافتراضي المصغر المقترح

وبُنِي معالج صغري افتراضي ضمن بيئة المحاكي المقترحة يستخدم مجموعة جزئية من تعليمات المعالج MIPS(Million instructions per second) [9] والتي تستخدم في نمط المستخدم user mode وذلك بهدف تبسيط الخوارزميات المستخدمة ضمن التطبيق من جهة، ولأن هذه المجموعة الجزئية من تعليمات MIPS تكون فعالة بشكلٍ كافٍ لبرمجة أية خوارزمية باستخدام لغة التجميع من جهةٍ أخرى، (ولتحقيق ذلك تم بناء مترجم compiler مبسط، مرن وقابل لإضافة تعليمات جديدة).

كما اعتُمِد المعالج المذكور لبناء نواة محاكي WSN، وهذا يعني أنّهُ بالإمكان إضافة أي عدد من العقد والتي تستخدم المعالج المقترح كخطوة أولى، مع الأخذ بالحسبان الخصائص الزمنية المتعلقة بالإرسال والاستقبال وذلك بالاعتماد على نوع التعديل وبعض الافتراضات المتعلقة بالمكونات الداخلية لوحدة الإرسال والاستقبال Transceiver Unit وذلك بهدف التبسيط والتسهيل.

تمتلك بيئة المحاكي عدد من الميزات نذكر منها:

- سهولة برمجة هذه البيئة الافتراضية، حيث أننا نستخدم التعليمات والأدوات الأساسية المتوفرة في Microsoft visual studio 2015 (windows forms applications)، إضافةً إلى أنَّvisual studio يعطينا سهولة بعملية اختبار أي كود برمجي، وذلك باستخدام خاصية الـ debug والتي تؤمن مرونة بمقدرات التعديل لنتمكن عبر ذلك من تضمين أية خاصية ضمن واجهة المنصة.
- إمكانية تطبيق خاصية اكتشاف الأخطاء وتصحيحها debugging procedure خلال تنفيذ التعليمات ضمن تطبيقنا، الأمر الذي يمكننا من مراقبة نتائج كل عملية واكتشاف الأخطاء التي يمكن أن تكون موجودة، إضافةً إلى إمكانية ضبط الـ clock المتعلق بكل تعليمة وفقاً لنوع المعالج المقترح.
- إظهار قيم مواقع الذاكرة والمسجلات وفق نظام العد الثنائي، العشري، والست عشري، والقدرة على تعديل هذه القيم عند الضرورة، إضافة لإمكانية إظهار source code format لكل تعليمة.
- إمكانية إضافة، حذف، تحريك العقد ضمن الواجهة المقترحة وتغيير خصائص هذه العقد مثل نصف قطر الإرسال المتعلق بالعقدة.

2. خوارزمية المصادقة بين عقدتين مستقلتين من عقد الحساسات عبر الواجهة المصممة Authentication Scheme between Two Individual Sensor Nodes :

يشكل التوجيه Routing جزءاً مهماً من العمليات الأساسية ضمن شبكات الحساسات اللاسلكية WSN والتي تحافظ على تشغيل الشبكة واستمرار عملها بالشكل الصحيح، ويحتل أمن التوجيه Secure Routing أهميةً متزايدة في مجال شبكات الحساسات اللاسلكية لاسيما عندما تُنشَر ضمن بيئة معادية Hostile Environment إذ تكون معرضة لأنواع مختلفة من الهجمات، وتعود هذه الهجمات للعديد من العوامل نذكر منها الطبيعة غير الآمنة لقنوات الاتصال اللاسلكية من جهة، ونتيجة للضعف الموجود ضمن البنى التحتية المقاومة لعمليات التلاعب بعمليات التوجيه من جهة أخرى. لذا كان اختيارنا إحدى خوارزميات أمن التوجيه المستخدمة في شبكات WSN وهي خوارزمية المصادقة بين عقدتين مستقلتين من عقد الحساسات Authentication Scheme between Two Individual Sensor Nodes [6]، وذلك لاختبارها ضمن بيئتنا الافتراضية المصممة من أجل تقييم أدائها، وسنورد فيما يلي تسلسل عملياتها وآلية تحقيق المصادقة بين العقد:

عندما تريد عقدة الحساس أن تجري اتصالاً آمناً مع عقدة حساس أخرى تحتاج أولاً كل عقدة أن تتحقق من هوية العقدة الأخرى (إجراء المصادقة)، وفي هذه الهيكلية سنفترض أنه لن تُخزَّن معلومات المفاتيح في عقد حساسات فردية، وبدلاً من ذلك كل معلومات المفاتيح ستُخزَّن ضمن عقد حساسات طرفية ذات مستوى عالي High End Sensor Node(Master Node)، ومن خلال حماية الـ Master Node يمكننا جعل كامل شبكة الحساسات آمنة وفق الآتي:

- لنفرض وجود عقدتين A,B ضمن الشبكة وتريدان أن تتصلا مع بعضهما البعض بشكلٍ آمن.
- يجب أن تحتوي العقدة ذات المستوى العالي Master Node على المفاتيح المتعلقة بكل عقد الحساسات K1,K2,K3,…,Kn وهوية هذه العقد IDs والصيغة المشفرة من هذه الهويات مع المفاتيح المرتبطة بها أي (IDA)K1,(IDB)K2,(IDC)K3…… وذلك قبل نشر العقد.

يكون المفتاح متوفراً فقط عند الـ Master Node، حيث تحوي العقدة A على الهوية IDA و (IDA)K1 وتحوي العقدة B على الهوية IDB و (IDB)K2.

- تولد العقدة A رقماً عشوائياً Nonce A وتحسب رمز مصادقة الرسائل MAC (Message Authentication Code) باستخدام الـ Nonce A والـ (IDA)K1.
- تقوم العقدة A بإرسال الرسالة التالية للعقدة B:

IDA||Nonce A||MAC{(IDA)K1||NonceA}

- عند استقبال الرسالة، تحاول العقدة B حساب الـMAC من أجل المصادقة، ولكنّ المفتاح (IDA)K1 متوفر فقط عند الـ Master Node لذا تولد العقدة B رقماً عشوائياً بعد استقبال الرسالة من العقدة A وهو Nonce B.
- ثمَّ ترسل لـ Master node الرسالة التالية بهدف التحقق من العقدة.

IDA||H{(IDB)K2}||Nonce A||Nonce B|| IDB، حيث يعبِّر H{(IDB)K2} عن تابع البعثرة المتعلق بـ (IDB)K2.

- تجري العقدة (Master node) المصادقة من خلال حساب تابع البعثرة Hash Function عبر (IDB)K2 والذي يكون مع الـ Master node، وبعد مصادقة العقدة B من خلال الرسالة المستقبلة من العقدة B والتأكد من صحة الرسالة ترسل (IDA)K1 للعقدة B.
- تحسب العقدة B {MAC{(IDA)K1||Nonce A ومقارنته مع الـ MAC المقدم ضمن الرسالة القادمة من العقدة A، وإذا تساوت قيم الـ MAC مع بعضها البعض تتأكد عندئذ العقدة B من أن العقدة A هي عقدة موثوقة ضمن الشبكة وتتصل معها بشكلٍ آمن.

وأثناء اتصال العقدة B مع الـ Master Node، إذا تمكن المهاجم من الاستحواذ على كامل البيانات المرسلة فإنه لن يستخدم المفتاح (IDB)K2 المتعلق بالعقدة B حيث أن العقدة B تكون قد غيرت مسبقاً المفتاح ليصبح (IDB)K2+Nonce A وتكون الـ Master Node قد غيرت مفتاحها أيضاً من (IDB)K2 إلى (IDB)K2+Nonce A وبذلك فإن البيانات المتبادلة بين الـ Master Node والعقدة B لن تُستخدَم حتى لو اعتُرِضت. وحالما تصادق العقدة Master Node العقدة B فإنَّها ترسل مباشرةً Nonce B للعقدة A. وهكذا تحدِّث العقدة A الـ (IDA)K1 إلى (IDA)K1+Nonce B والتحديث ذاته أيضاً يُنفَّذ من قبل الـ Master Node وهكذا تُنجَز المصادقة بين عقدتي حساسات ضمن الهيكلية المذكورة.

3. بعض النقاط المتعلقة بآلية اختبار وتنفيذ الخوارزمية المذكورة ضمن البيئة المقترحة:

سنهيئ مواقع الذاكرة المتعلقة بالعقد A, B, and Master node أثناء تطبيق الخوارزمية وفق الجدول (1):

الجدول (1): قيم مواقع الذاكرة المتعلقة بالعقد A, B, and Master node

	Node A		Node B		Master Node
0	IDA(12)	0	IDB(25)	0	K Master(44)
1	KA(129)	1	KB(135)	1	KA(129)
2	IDA(KA)	2	IDB(KB)	2	KB(135)
3	Value1 for Nonce A Calculation (12)	3	Value1 for Nonce B calculation (6)	3	ID Master(105)
4	Value2 for Nonce A Calculation (129)	4	Value2 for Nonce B Calculation (12)	4	IDA(12)
5	Value3 for Nonce A Calculation (9)	5	Value3 for Nonce B Calculation (45)	5	IDB(25)
6	Nonce A	6	Nonce B	6	IDA(KA)
7	Value of MAC{(IDA)K1||Nonce A}	8	Value to indicate that node B is waiting response from Master node (1)	7	IDB(KB)
9	Value to indicate that node A is waiting response from another node (1)	10	Value to indicate that there is an error (1)	10	Value to indicate that there is an error (1)
10	Value to indicate that there is an error (1)	11	Received value(IDA)	14	Received value(Nonce A)
		12	Received value(Nonce A)	15	Received value(Nonce B)
		13	Received value(MAC{(IDA)K1||Nonce A})	16	Received value(IDB)
		19	Received value(IDA(KA))	17	Received value H{(IDB)K2}
				18	Received value(IDA)
				21	Positive response for node B(1)

ويمكن الإشارة إلى بعض الملاحظات التوضيحية المتعلقة بالجدول المدرج أعلاه:

- تعبِّر الأرقام الواردة بين الأقواس ضمن الجدول عن قيم المتحولات المعرفة إلى جانبها، فمثلاً تشير IDA(12) إلى أن قيمة المُعرِّف (الهوية) المتعلقة بالعقدة A هي 12، وذلك ضمن نظام العد العشري Decimal Numerical System، وهكذا بالنسبة لبقية القيم، مع التنويه لإمكانية إظهار جميع القيم بالصيغ العشرية، الثنائية، والست عشرية ضمن واجهتنا المصمَّمة.
- اخترنا العناوين المتعلقة بمواقع الذاكرة بما يوضح سير العمليات ضمن معالج العقدة وفقاً لخطوات تنفيذ الخوارزمية المذكورة، مع التنويه لإمكانية اختيار مجموعة أخرى من العناوين، فالمهم هنا هو استخدام العدد المناسب من المواقع اللازم لتنفيذ خطوات الخوارزمية المذكورة بمعزل عن عناوين هذه المواقع، ويتم ذلك عادةً خلال برمجة

العمليات ضمن العقد، حيث تتحدد ضمن عملية البرمجة عناوين مواقع الذاكرة الخاصة بتخزين القيم الابتدائية والقيم المحسوبة الناتجة عن سير العمليات.

ومن أجل التحقق من سلامة ودقة نتائج الخوارزمية المطبقة على المحاكي المقترح، سنستخدم صيغاً مبسطة عند إجراء الحسابات المتعلقة بتابع مصادقة الرسالة MAC{(IDA)K1||NonceA} و بتابع البعثرة Hash Function المتعلق بـ (IDB)K2 أي (H{(IDB)K2})، حيث سنعتمد لحساب MAC{(IDA)K1||NonceA} التابع mod{(NonceA+IDA(KA))/5}، كما سنستخدم لحساب H{(IDB)K2} التابع mod {IDB(K2)/7} ، كما سنقوم بحساب الرقم العشوائي Nonce المتعلق بالعقدتين A,B بجمع محتوى المواقع المخصصة لقيم الـ Nonce معاً.

ويعود سبب اختيار هذه الصيغ المبسطة إلى أننا نركز بشكلٍ أساسي على توضيح سير العمليات المتعلقة بالواجهة المصممة، وآلية العمل ضمنها دون الدخول بتفاصيل عمليات التوابع، لذا تجنبنا اختيار الصيغ المعقدة لهذه التوابع، واستخدمنا عوضاً عن ذلك صيغاً مبسَّطة لها كحساب بقية القسمة على رقم معين كما هو الحالة في تابعي المصادقة والبعثرة، أو جمع عدة قيم معاً كما هو الحال في تابع حساب الرقم العشوائي، ليكون التركيز بشكلٍ أساسي على عمليات البيئة المقترحة.

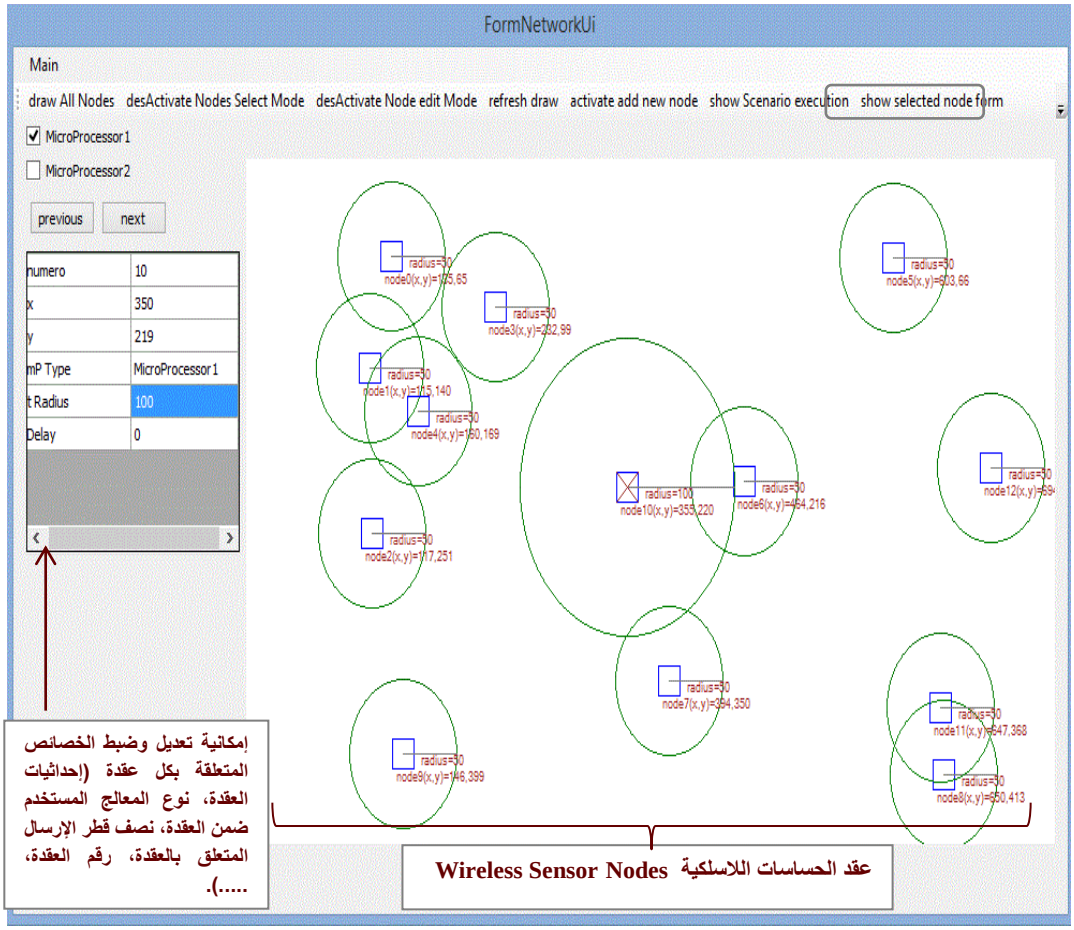
كما سنعتمد بروتوكولاً مبسطاً ضمن ترويسة الرسالة بهدف تمييز وجهة الرسالة، ويأخذ هذا البروتوكول القيم المدرجة ضمن الجدول (2) بعين الاعتبار:

الجدول (2): معلومات ترويسة الرسالة لتحديد وجهة الرسالة ضمن الخوارزمية المدروسة

Message Header (1 Byte)	Message Type
01010010	رسالة طلب إجراء اتصال آمن. (العقدة A ---------> العقدة B)
01010011	رسالة استجابة (رد على رسالة طلب اتصال آمن). (العقدة B ---------> العقدة A)
10010001(part1) 00100001(part2)	رسالة طلب معلومات من العقدة ذات المستوى العالي Master. (العقدة B ---------> العقدة Master)
01010000	رسالة استجابة من العقدة ذات المستوى العالي Master. (العقدة Master ---------> العقدة B)

النتائج والمناقشة:

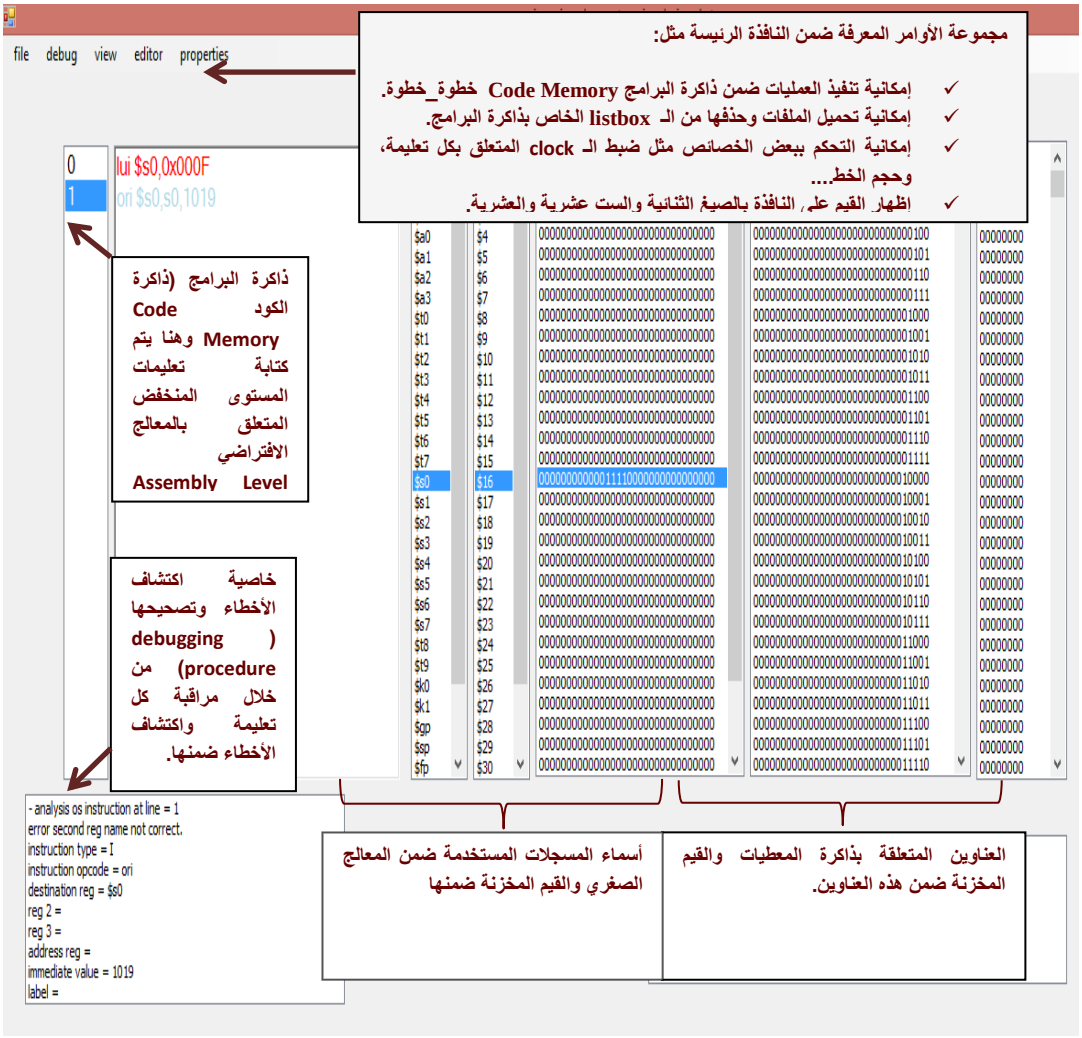
بدايةً وقبل البدء بتنفيذ الاختبار، سنستعرض الواجهة الرئيسة GUI المعبرة عن نواة محاكي WSN الافتراضية المصممة، والتي يعبر عنها الشكل(2).



الشكل(2): الواجهة GUI المعبرة عن نواة محاكي WSN الافتراضية المصممة

حيث يمكن ضمن هذه الواجهة إضافة العدد المطلوب من عقد الحساسات مع وجود إمكانية تحريك، إضافة، حذف العقد، بالإضافة إلى إمكانية تحديد واختيار أي عقدة بهدف ضبط الخصائص المتعلقة بها مثل رقم العقدة، نصف قطر الإرسال، الإحداثيات ونوع المعالج المستخدم ضمنها.

وباختيار الزر show selected node form تظهر الواجهة GUI المعبرة عن عمليات المعالج الصغري الافتراضي المستخدم ضمن كل عقدة مدرَجَة ضمن واجهة الشبكة، والتي يعبر عنها الشكل(3).



الشكل(3): الواجهة GUI المعبرة عن بيئة محاكي المعالج الصغري الافتراضي

1. سيناريوهات العمل:

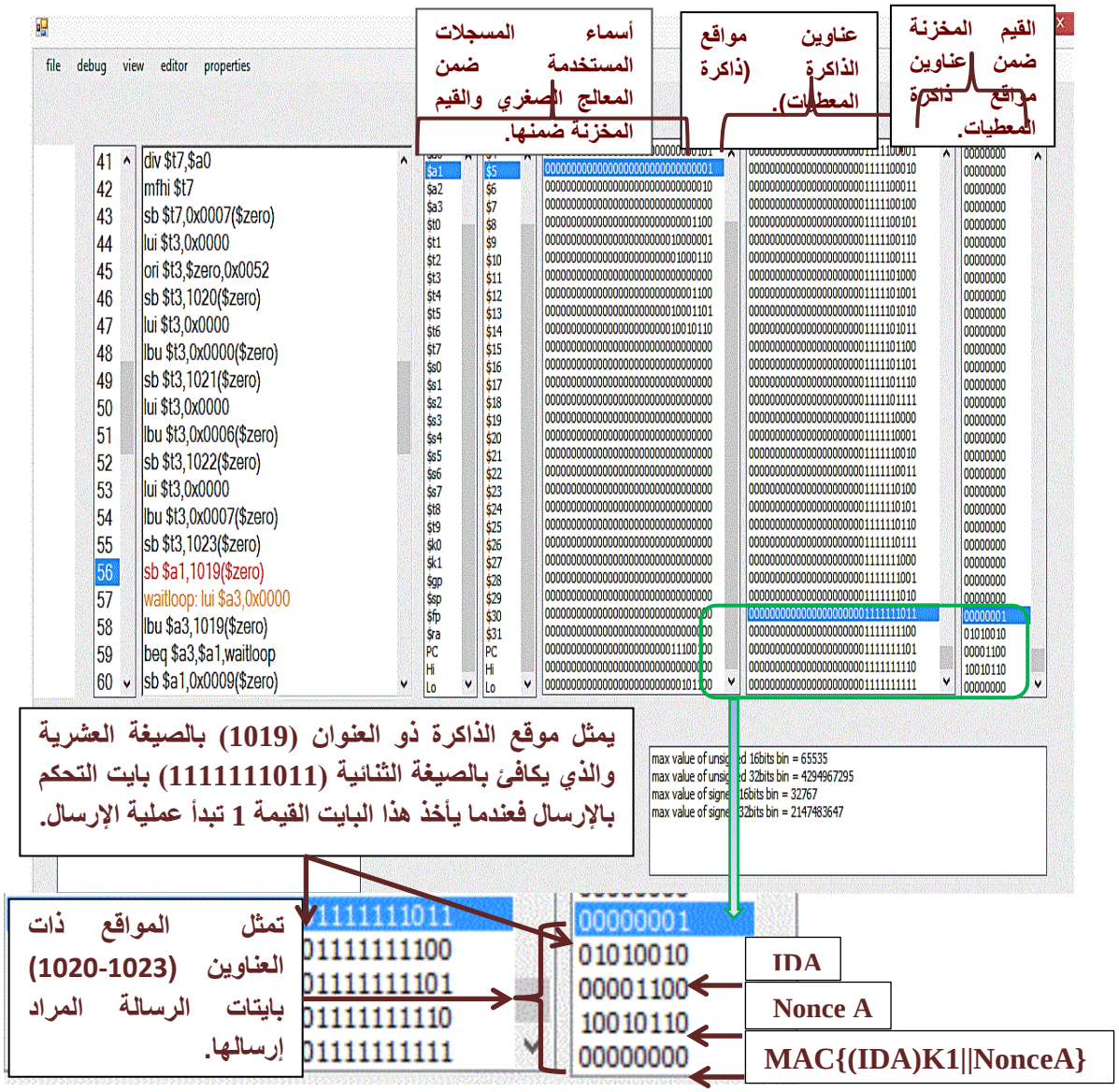
سننفذ الاختبار وفقاً للخطوات الآتية:

1. إضافة ثلاث عقد: العقدة A (node0)، العقدة B (node1)، والعقدة ذات المستوى العالي (node2, Master Node).
2. تحميل ملف الـ Assembly الذي يتضمن تهيئة العقد بالقيم الابتدائية، بالإضافة لإجراء الحسابات المتعلقة بخطوات تنفيذ الخوارزمية المذكورة (مثل حساب قيمة الـMAC والرقم العشوائي (Nonce A, Nonce B) ضمن كل عقدة.
3. البدء بالتنفيذ (خطوة_ خطوة) ومراقبة تنفيذ العمليات ضمن المعالج المقترح المتعلق بكل عقدة.
4. تكرار التنفيذ ضمن الواجهة GUI المتعلقة بالمنصّة المقترحة وفق السيناريوهات الآتية، وبمعدل عشر مرات لكل سيناريو، حيث أنَّ هذا العدد كافٍ لتأكيد نتائج المحاكاة، ومقاربتها بصورةٍ صحيحة.

1-1. السيناريو الأول: تريد العقدة A إجراء اتصال آمن مع العقدة B، ولكنها تقع على مسافة بعيدة عن العقدة A وذلك بافتراض أن العقد نُشِرت بشكلٍ عشوائي:

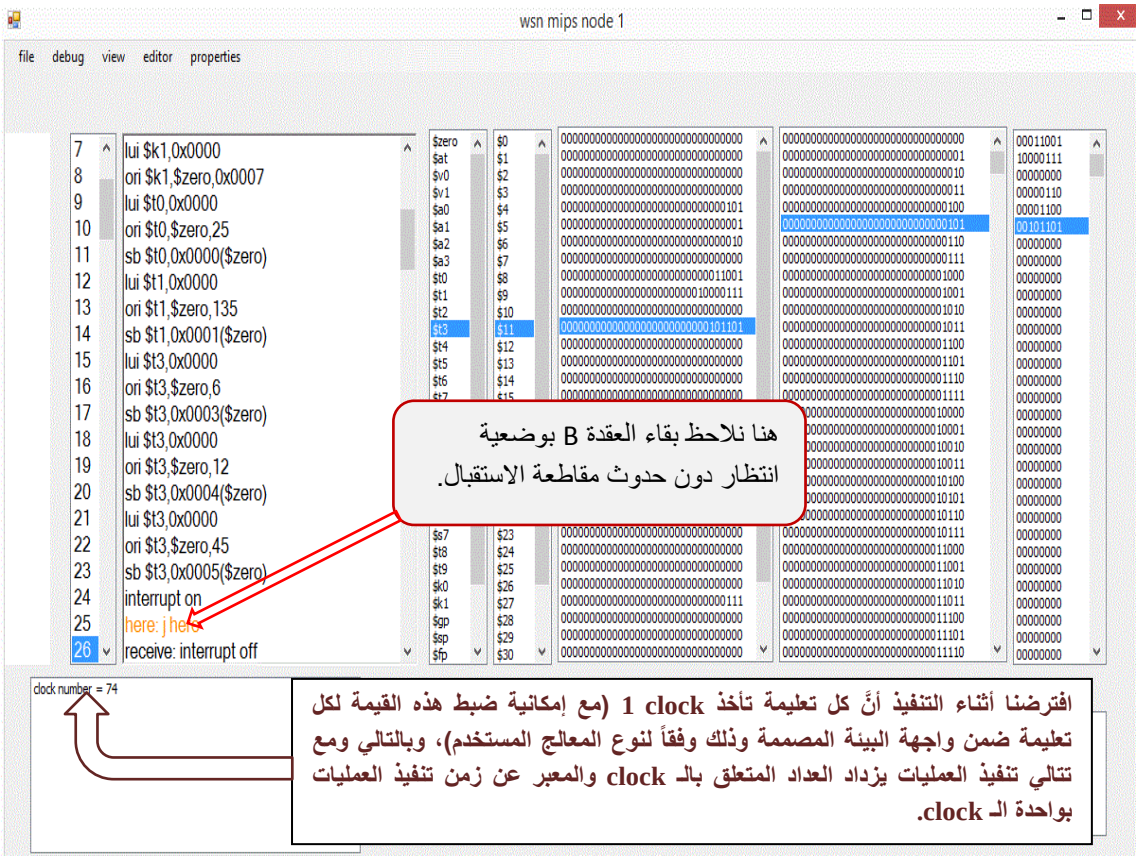
1-1-1. نتائج السيناريو الأول:

بدايةً، وبعد إجراء العقدة A لعمليات التهيئة المتعلقة بها، فإنَّها ستحسب رمز مصادقة الرسائل MAC باستخدام الـ Nonce A والـ (IDA)K1، ثم تبدأ بإرسال الرسالة IDA||Nonce A||MAC{(IDA)K1||NonceA} للعقدة B كما هو مبين بالشكل (2) وذلك بهدف إجراء اتصال آمن معها، بينما تكون بقية العقد بوضع الانتظار.



الشكل(2): إرسال العقدة A للرسالة {IDA||Nonce A||MAC{(IDA)K1||NonceA} إلى العقدة B

لن تظهر أية استجابة من العقدة B ولن تستقبل الرسالة، وذلك لأن العقدة A تقع خارج مجال الاستقبال المتعلق بالعقدة B كما هو مبين بالشكل(3).



الشكل(3):عدم استقبال العقدة B للرسالة المرسلة من العقدة A

1-1-2. السيناريو الثاني: تريد العقدة A إجراء اتصال آمن مع العقدة B، ولكنها مهيأة بقيم أولية غير دقيقة لحساب رمز مصادقة الرسائل (عقدة خبيثة تحاول الاتصال بالشبكة أو خطأ أثناء إرسال البيانات).

1-1-2-1. نتائج السيناريو الثاني:

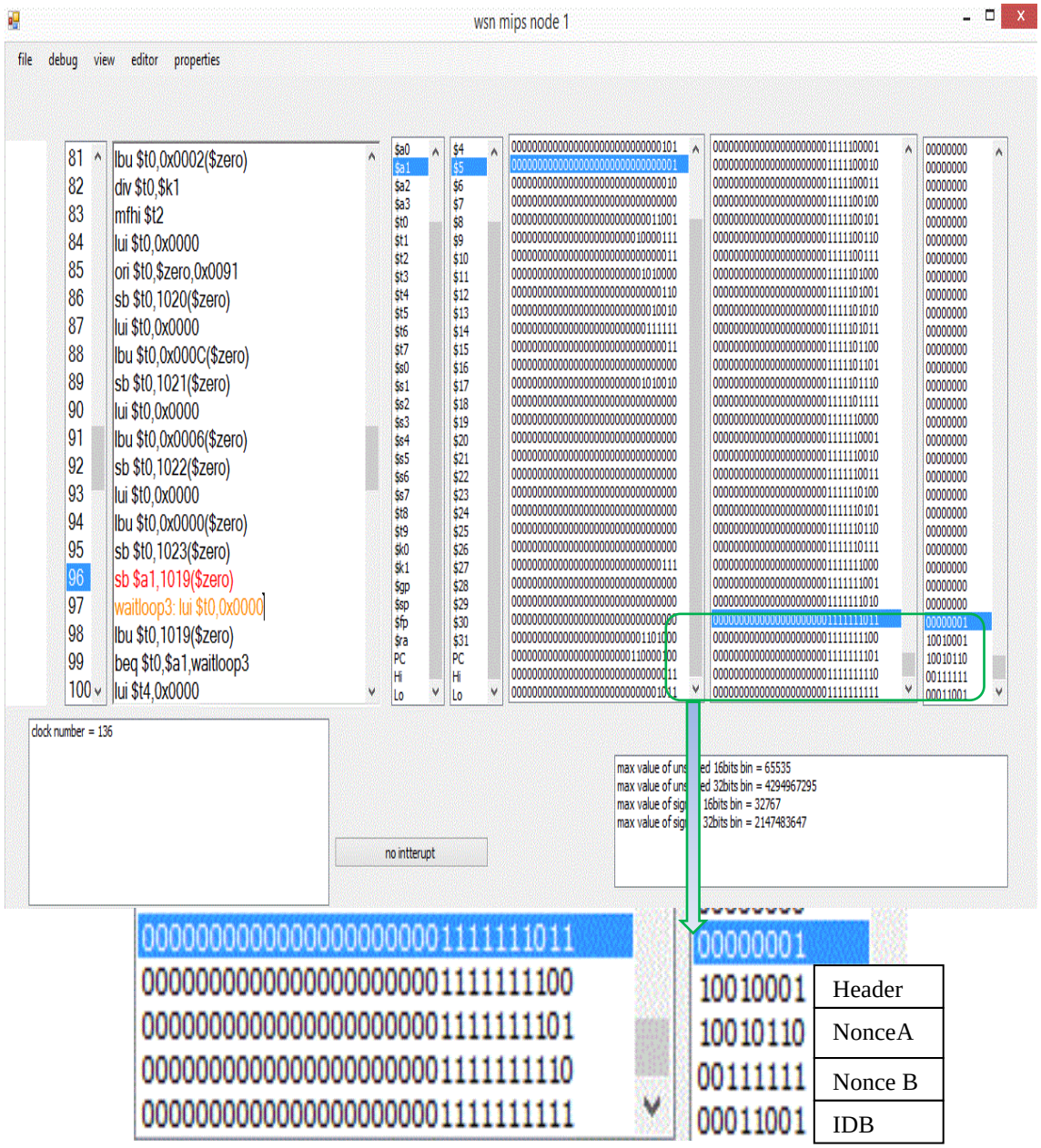
تستقبل العقدة B الرسالة المرسلة لها من قبل العقدة A بعد إجرائها لعمليات التهيئة المتعلقة بها، ولكي تحسب MAC{(IDA)K1||NonceA} بهدف التحقق، فإنها تحتاج لـ (IDA)K1 لذا تراسل العقدة Master للحصول عليه، حيث تحسب H{(IDB)K2 ثم ترسل الرسالة على جزأين كما هو مبين بالشكل(4) و الشكل(5) وذلك باعتبار أن الـ Buffer المتعلق بالـ transceiver وفقاً لافتراضنا هو4Byte، حيث يبين الجدول (3) الجزء الأول الذي يُرسَل ويبين الجدول (4) الجزء الثاني الذي يُرسَل.

الجدول (3): الجزء الأول من الرسالة المرسلة من العقدة B إلى العقدة Master

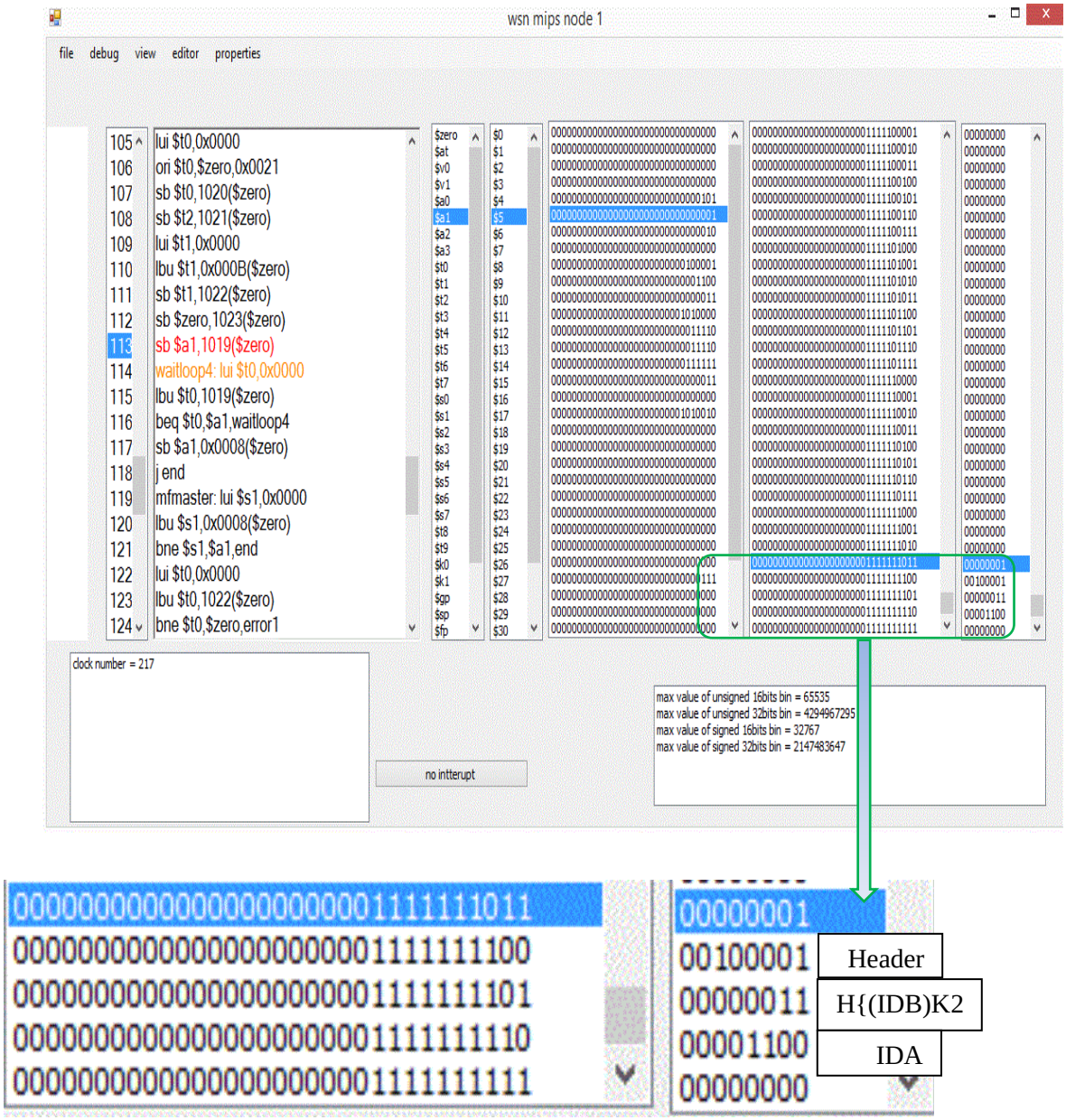
Message Header	Nonce A	Nonce B	IDB
10010001	10010110	00111111	00011001

الجدول (4): الجزء الثاني من الرسالة المرسلة من العقدة B إلى العقدة Master

Message Header	H{(IDB)K2	IDA	Zero
00100001	00000011	00001100	00000000

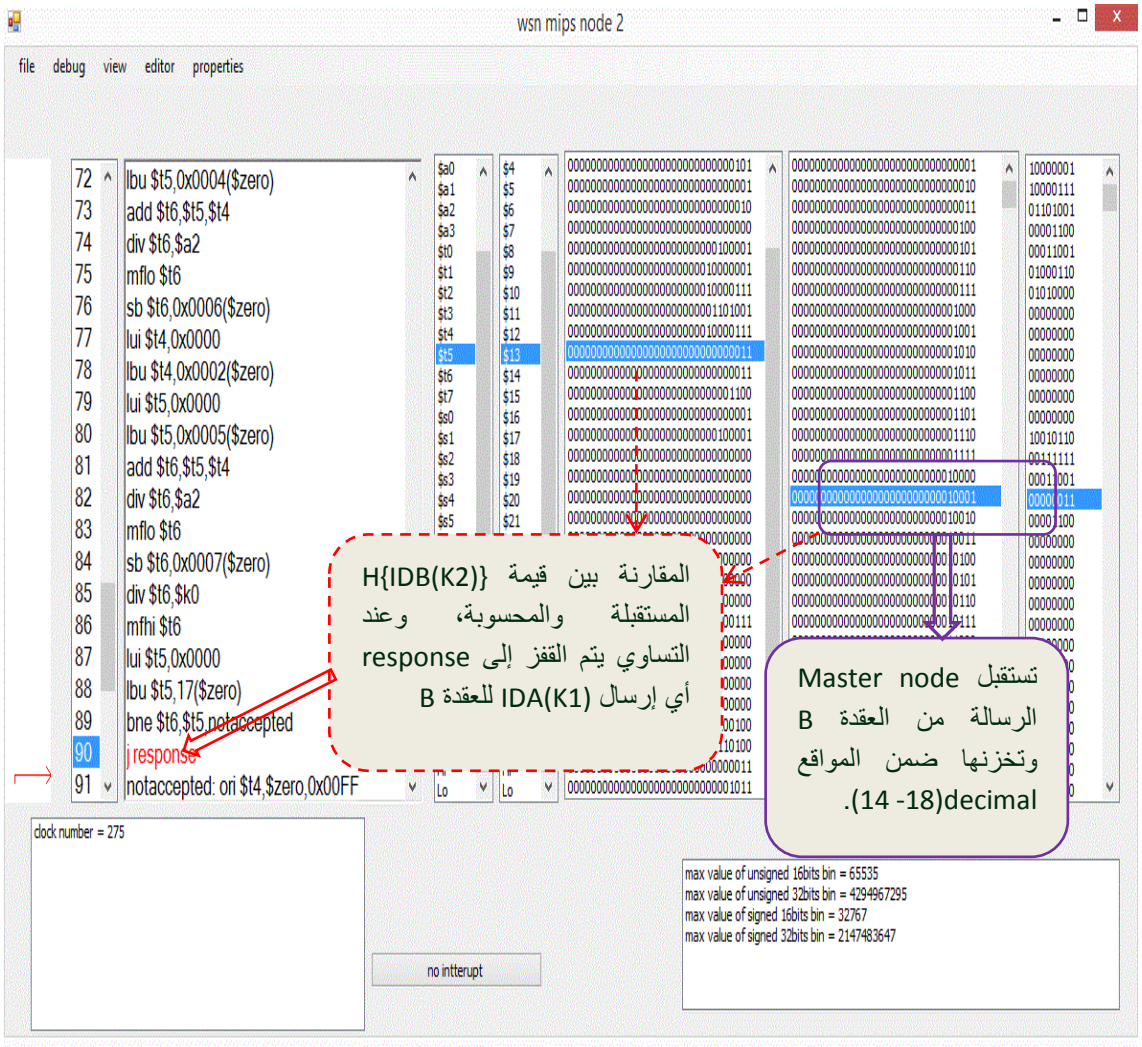


الشكل(4): إرسال العقدة B للجزء الأول من الرسالة (Nonce A||Nonce B|| IDB) إلى العقدة ذات المستوى العالي Master Node



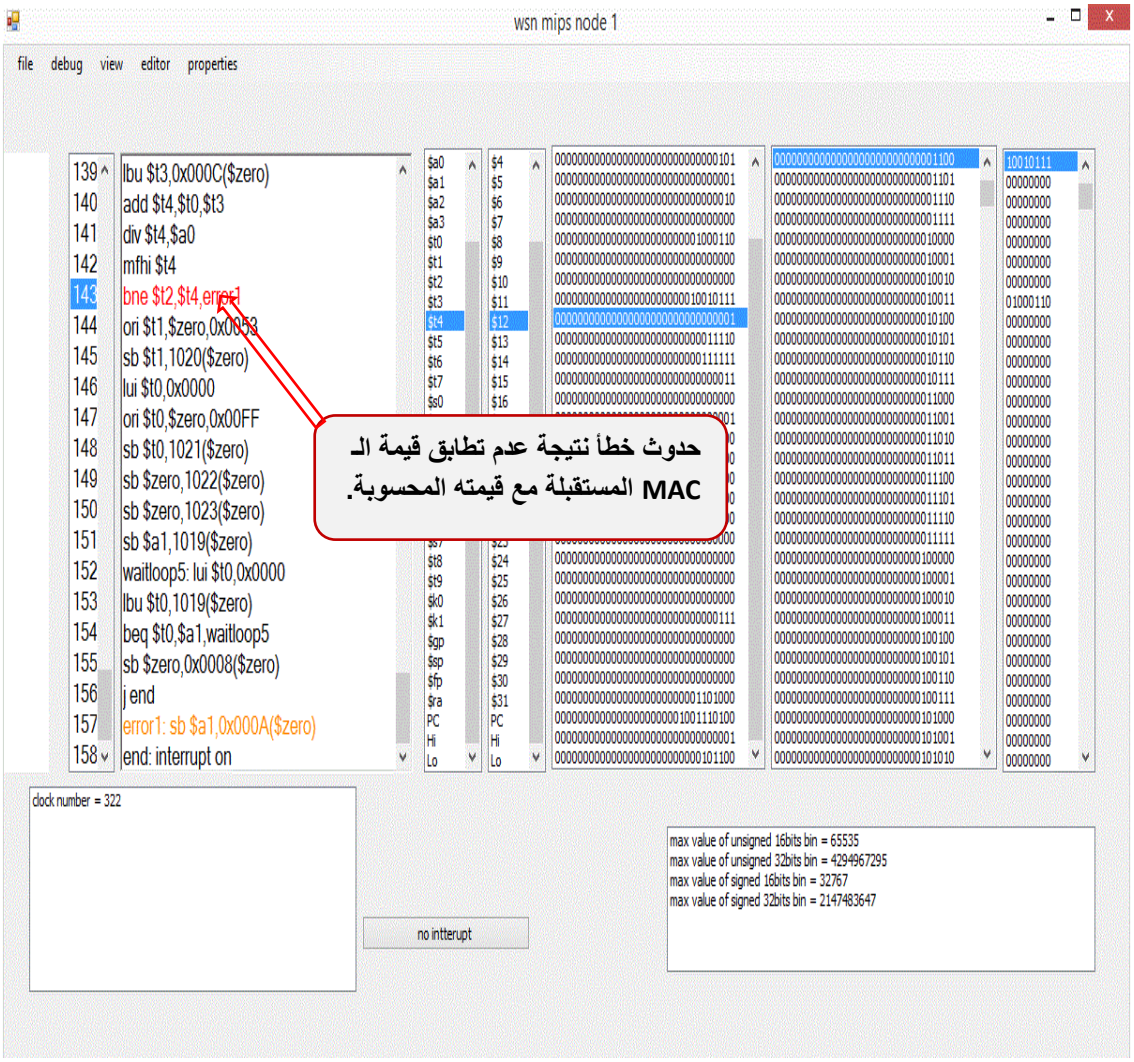
الشكل(5): إرسال العقدة B للجزء الثاني من الرسالة (H{(IDB)K2}||IDA) إلى العقدة ذات المستوى العالي Master Node

بعد ذلك تحسب العقدة Master H{(IDB)K2} وفقاً للتابع{IDB(K2)/7} mod (قيمة المسجل $t6) ثم تقارنه مع القيمة التي استقبلتها من العقدة B وهي القيمة المخزنة ضمن الموقع (17 in Decimal) (قيمة المسجل $t5) وبحال تساوي القيمتين تقوم العقدة Master بالقفز نحو اللافتة label: response والتي تُرسَل ضمنها (IDA)K1 للعقدة B حيث يبين الشكل (6) هذه المقارنة.



الشكل (6): تحقق القعدة ذات المستوى العالي من موثوقية العقدة B قبل أن ترسل لها IDA(K1)

تحسب العقدة B بعد حصولها على IDA(K1) MAC{(IDA)K1||NonceA} وتقارنها مع القيمة المستقبلة من العقدة A كما هو مبين بالشكل (7) ونتيجةً لعدم تساوي القيمتين تعتبر العقدة B أن العقدة A هي عقدة غير موثوقة ضمن الشبكة، وترفض إجراء اتصال آمن معها.



الشكل(7): مقارنة العقدة B بين قيمة الـMAC المستقبلة وقيمته المحسوبة

1-1-3. <u>السيناريو الثالث</u>: تريد العقدة A إجراء اتصال آمن مع العقدة B وهي مهيأة بقيم أولية صحيحة لحساب رمز مصادقة الرسائل.

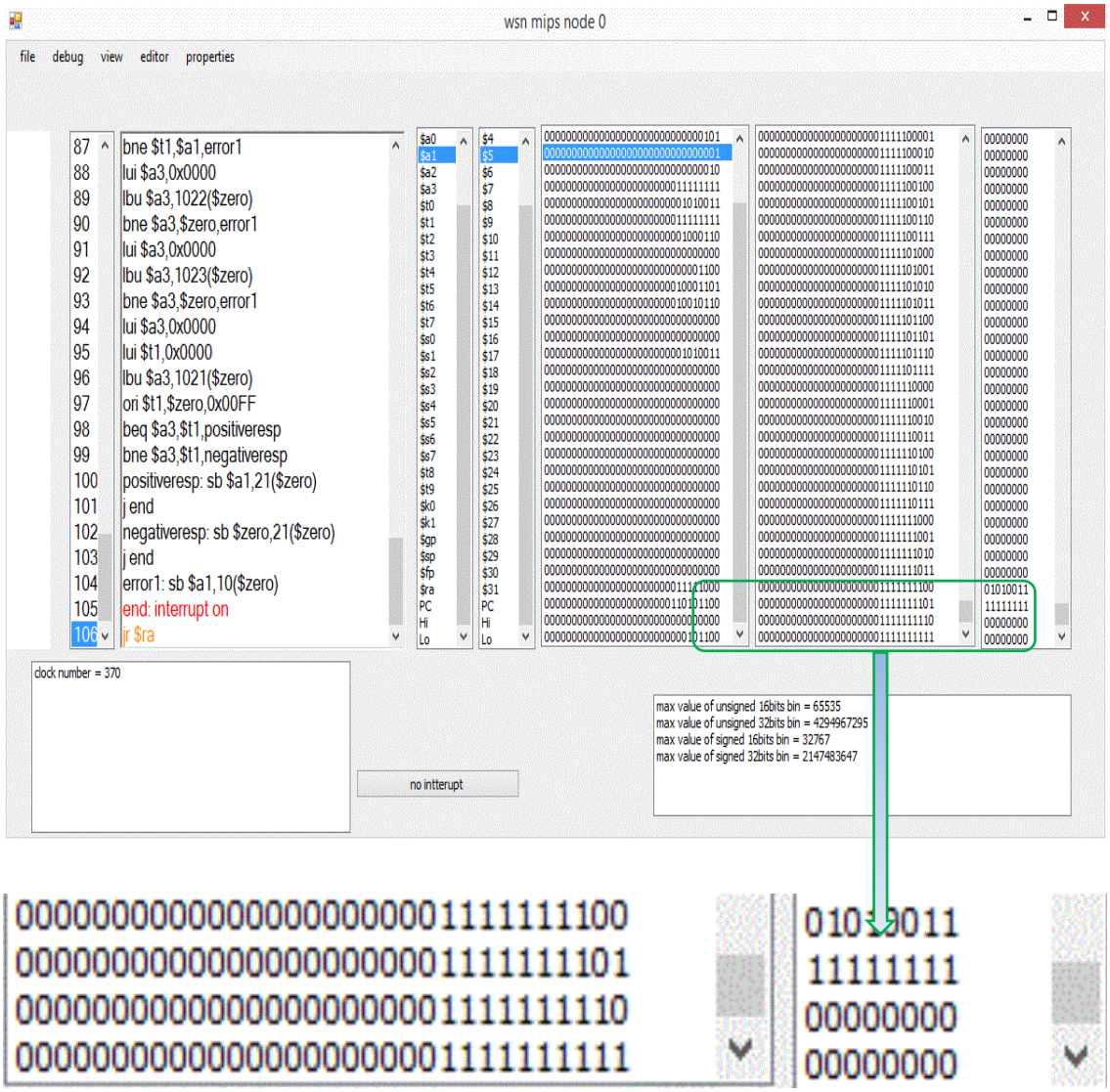
1-1-3-1. نتائج السيناريو الثالث:

هنا تتكرر نفس خطوات المذكورة ضمن الحالة الثانية باستثناء الخطوة الأخيرة، حيث أن قيمة الـ MAC تكون متساوية وعندئذٍ تقبل العقدة B طلب العقدة A بإجراء اتصال آمن معها، وذلك من خلال إرسال الرسالة المبينة بالجدول (5) لها:

الجدول (5): الرسالة المرسلة من العقدة B إلى العقدة A لإعلامها ببدء إجراء اتصال آمن معها

Message Header	Secure Connection		
01010011	11111111	00000000	00000000

حيث تستقبل العقدة A وكما هو مبين بالشكل (14) هذه الرسالة لتبدأ بذلك إجراء الاتصال الآمن مع العقدة B.



الشكل (8): استقبال العقدة A للرسالة الواردة ضمن الجدول (5) من العقدة B للإعلام ببدء إجراء اتصال آمن معها

الاستنتاجات والتوصيات:

طبقنا ضمن هذه المقالة إحدى خوارزميات أمن التوجيه وهي خوارزمية المصادقة بين عقدتين مستقلتين من عقد الحساسات، وذلك ضمن بيئة المحاكي المقترح، الأمر الذي أتاح لنا إمكانية مراقبة وتتبع تسلسل تنفيذ العمليات على المستوى المنخفض، واختبار آلية مبسطة لتحديد وجهة الرسالة على مستوى لغة الـAssembly، حيث طُبِّقت ثلاثة سيناريوهات مختلفة من أجل تقييم أداء منصة المحاكاة المقترحة. تبين النتائج مرونة وفعالية المنصة المقترحة في تتبُّع سير العمليات ضمن عقد الحساسات اللاسلكية على مستوى لغة الـAssembly. وعليه سيتم مستقبلاً تطوير هذه المنصة عن طريق إضافة معالج مستخدم فعلياً ضمن شبكات الحساسات اللاسلكية بكامل تعليماته وخصائصه، بالإضافة إلى بناء محرر لكتابة سيناريوهات العمل وربطها مع نواة المحاكي، وذلك بالاعتماد على مبدأ Discrete Event Simulation.

References:

[1] SINGH,M; AMIN,S.I; IMAM,S.A; SACHAN,V.K; CHOUDHARY, A,"*A Survey of Wireless Sensor Network and its types*", International Conference on Advances in Computing, communication Control and Networking (ICACCCN2018),October 12-13,2018, Greater Noida (UP), India, IEEE Xplore: 01 July 2019.

[2] OTHMAN,M.F; SHAZALI,KH, "*Wireless Sensor Network Applications: A Study in Environment Monitoring System*", International Symposium on Robotics and Intelligent Sensors 2012.

[3] ISSARIYAKUL,T; HOSSAIN,E, "*Simulation of Computer Networks*", In *Introduction to Network Simulator NS2,2nd ed.* New York: Springer Science and Business Media Spring,2012,pp.5-7.

[4] CHARFI,W; MASMOUDI,M; DERBEL,F,"*A layered model for wireless sensor networks*", 6th International Multi-Conference on Systems, Signals and Devices, March 23-26,2009, Djerba, Tunisia, IEEE Xplore**:** 19 May 2009.

[5] GUERRERO-ZAPATA,M; ZILAN,R; BARCEL-ORDINAS,J; BICAKCI,K; TAVLI,B, "T*he future of security in Wireless Multimedia Sensor Networks*", Telecommunication Systems, December, 2009.

[6] SAHOO,S; MISHRA,P; SATPATHY,R, "*Secure Routing in Wireless Sensor Networks"*, IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 1, No 2, January 2012

[7] C. Price, *"MIPS IV Instruction Set Revision". 3.2ed*. MIPS Technologies, Inc., USA, September,1995.

[8] NAKOV,S; CO., "*Introduction to Programming*", In *Fundamentals Of Computer Programming With C#*, ISBN 978-954-400-773-7,Bulgary, Sofia,2013.