الجمهورية العربية السورية
جامعة دمشق
كلية العلوم
قسم الرياضيات

نظرية البيان وتطبيقاتها للحد من مشكلات شبكات الاستشعار اللاسلكية

أطروحة مقدمة لنيل درجة الدكتوراه في الرياضيات

(فرع الرياضيات التطبيقية والمعلوماتية)

إعداد

ألاء حسن سلامة

إشراف

أ.م.د. سمير جعفر

أستاذ مساعد في قسم الرياضيات– كلية العلوم– جامعة دمشق

(2025–2026)

قرار لجنة الحكم، وتوقيعات لجنة المناقشة

شكر وتقدير

الحمد بداية لله عز وجل الذي أعانني على طريق العلم وقر عيني وعائلتي بتخرجي. الشكر الأول والامتنان **لمشرفي الفاضل الأستاذ الدكتور سمير جعفر** دمت نعم الأستاذ والناصح.

إلى روحي الغالية، **أبي** أينما كنت في علياء الجنة، هذا الإنجاز ثمرة دعواتك الطاهرة، وقطرة من بحر جميل صنعتك. رحمك الله وأسكنك فسيح جناته.

إلى **أمي** الحبيبة حفظك الله لي، أنت النبض الذي لا يتوقف حباً ودعاءً. كل حرف في هذه الأطروحة كان برفقة دعواتك الصادقة.

إلى سندي في هذه الحياة، **زوجي** الغالي من كان معي على كلمة، ومسح دمعتي في كل لحظة شك وتعب، وشاركني الفرحة قبل أن تكتمل. لا يكفيني حرف لأوفيك حقك، فأنت شريك النجاح الأول.

إلى ابنتي **ماريا** قرة عيني، أسال الله أن أكون لك قدوة حسنة وأن ترين من نفسك ما هو أعظم.

إلى **إخوتي** سند العمر وعزوة الظهر. وجودكم في حياتي نعمة لا تضاهى.

أتوجه بالشكر لرئيس قسم الرياضيات **أ.م.د محمد فراس الحلبي** على تقديم يد العون وجميع التسهيلات ولكل الأساتذة الذين أناروا العقل بنور العلم.

فهرس المحتويات

1 مفاهيم أساسية في نظرية البيان والبيان العشوائي

1-1- مقدمة.....28

1-2- تعاريف أساسية.....28

1-2-1. البيان(Graph) 28

1-2-2. العروة (Loop) 29

1-2-3. الضلع المضاعف (Multiple Edge) 29

1-2-4. البيان البسيط (Simple Graph) 29

1-2-5. القوس(Arc) 29

1-2-6. البيان الموجهة (Directed Graph).....29

1-2-7. البيان الموزون(Weighted graph).....29

1-2-8. المسار(Path).....30

1-2-9. البيان الأولري (Euler Graph).....30

1-2-10. مسار هاملتون (Hamiltonian Path).....30

1-2-11. دائرة هاملتون (Hamiltonian Graph).....30

1-2-12. عقدة المصدر(Source Node).....31

1-2-13. عقدة الهدف(Target Node).....31

1-2-14. درجة العقدة (Degree Of Vertex).....31

1-2-15. العقدة المعزولة (Isolated Vertex).....31

1-3- التمثيلات المصفوفية (Matrix Representations).....31

1-3-1. مصفوفة التأثير (Incidence Matrix).....32

1-3-2. مصفوفة التجاور (Adjacency Matrix).....32

1-4- البيان الديناميكي.....33

1-5- تطبيقات البيان 34

1-5-1. نظرية الالوان الاربعة.....34

1-5-2. معالجة الصور.....35

1-5-3. الشبكة الاجتماعية.....35

1-6- البيان العشوائي.....35

1-7- نماذج البيان العشوائي.....36

1-7-1. البيان العشوائي الموحد.....36

1-7-2. البيان العشوائي ذو الحدين (binomial random graph).....36

1-7-3. البيان العشوائي المعالج (Random Graph Process).....37

1-7-4. مقارنة بين النماذج.....37

1-8- البيان الهندسي العشوائي (Random Geometric Graph).....38

1-9- مصطلحات هامة في البيان العشوائي.....38

1-9-1. المكون العملاق (giant component).....38

1-9-2. معامل تجميع العقد (clustering coefficient).....40

1-9-3. انتقال الطور(phase transition).....40

1-9-4. توزيع الدرجة (Degree distribution).....41

1-9-5. متوسط طول المسار (Average path length).....41

1-9-6. نقطة العتبة (Threshold Point).....41

1-9-7. الديناميكية في البيان العشوائي (Dynamics in random graph)...41

1-10- أهمية البيانات العشوائية.....43

1-11- خلاصة الفصل.....44

2 مفاهيم أساسية في التشفير.....45

2-1- مقدمة.....45

2-2- تعاريف الأساسية في علم التشفير.....45

2-2-1. النص الصريح (Plaintext).....46

2-2-2. النص المشفر (Cipher text) 46

2-2-3. المفتاح (Key) 46

2-2-4. خوارزمية التشفير (Encryption Algorithm) 47

2-2-5. خوارزمية فك التشفير (Decryption Algorithm) 47

2-3- الخوارزميات التقليدية في علم التشفير.....47

2-3-1. شيفرة القيصر (Caesar Cipher) 48

2-3-2. شيفرة فيجنير (Vigenère Cipher).....48

2-3-3. شيفرة هيل (Hill Cipher) 48

2-4- التشفير الحديث وأمن الشبكات 49

2-4-1. أنواع التشفير.....50

2-5- دوال التقطيع (Hash Functions).....51

2-5-1. تعريف دوال التقطيع.....52

2-6- التوقيع الرقمي (Digital Signatures).....53

2-7- المصافحة (TLS Handshake)..... 53

2-8- التشفير باستخدام نظرية البيان.....54

2-8-1. خوارزمية التشفير بالاعتماد على تلوين البيان.....55

2-8-1-1. مقارنة مع أنظمة التشفير التقليدية.....55

2-8-2. خوارزمية التشفير بالاعتماد على بيان أويلر.....56

2-8-3. خوارزمية تعتمد على مصفوفات التجاور.....56

2-9- خلاصة الفصل.....**57**

3 مفاهيم أساسية في شبكات الاستشعار اللاسلكية.....**58**

3-1- مقدمة.....58

3-2- تعريف شبكات الاستشعار اللاسلكية **58**

3-3- مكونات شبكة الاستشعار اللاسلكية.....**59**

3-3-1. عقدة الاستشعار(Sensor Nodes).....59

3-3-2. محطة القاعدة (Base Station).....59

3-4- بنية الشبكة (Architecture).....**60**

3-4-1. بنية القفزة الواحدة.....60

3-4-2. بنية القفزات المتعددة.....61

3-5- طوبولوجيا شبكات الاستشعار اللاسلكية.....**61**

3-5-1. طوبولوجيا الناقل (Bus Topology) 62

3-5-2. الطوبولوجيا الشجرية (Tree Topology).....62

3-5-3. الطوبولوجيا النجمية(Star Topology).....63

3-5-4. طوبولوجيا المشبك(Mesh Topology).....64

3-6- تطبيقات شبكات الاستشعار اللاسلكية.....64

3-6-1. التطبيقات العسكرية.....65

3-6-2. التطبيقات البيئية.....65

3-6-3. التطبيقات الصحية.....66

3-6-4. التطبيقات المنزلية.....67

3-7- العوامل المؤثرة في تصميم شبكات الاستشعار اللاسلكية.....67

3-7-1. الطاقة 68

3-7-2. التغطية 68

3-7-3. الامن.....69

3-7-4. الموارد الحاسوبية.....69

3-7-5. النشر.....69

3-7-6. الموثوقية (Reliability).....70

3-7-7. الوقت الفعلي (Real-time).....70

3-8- خلاصة الفصل.....**71**

4 التسامح مع الأعطال في شبكات الاستشعار اللاسلكية.....**72**

4-1-مقدمة.....**72**

4-2-العطل.....**72**

4-2-1. أدارة الأعطال.....73

4-3-التسامح مع الأعطال (Fault Tolerance).....**73**

4-3-1. تحقيق التسامح مع الأعطال.....74

4-3-2. منع الأعطال.....74

4-3-3. اكتشاف الأعطال 74

4-3-4. عزل الأعطال وتحديدها.....74

4-3-5. استعادة العطل.....75

4-4-موثوقية النظام.....75

4-4-1. التكرار المادي.....75

4-4-2. التكرار في البرمجيات.....75

4-5-الأعطال في شبكات الاستشعار اللاسلكية.....76

4-5-1. تصنيف الأعطال.....77

4-5-2. الأعطال الامنية.....78

4-5-3. عطل نفاد طاقة العقد(Node Energy Exhaustion).....81

4-5-4. هجوم استنزاف طاقة العقد(Energy Depletion Attack).....81

4-6-أهمية تشخيص الأعطال في شبكات الاستشعار اللاسلكية.....82

4-7- طرق تشخيص الأعطال في شبكات الاستشعار اللاسلكية.....83

4-7-1. المنهجية المركزية (Centralized Approach).....83

4-7-2. المنهجية الموزعة (Distributed App).....83

4-7-3. المنهجية الهجينة (Hybrid Approach).....83

4-8- التسامح مع الأعطال في شبكات الاستشعار اللاسلكية.....84

4-8-1. تكرار العقد (التغطية_K).....84

4-8-2. تكرار العقد (الاتصال_K).....84

4-8-3. تكرار التوجيه 85

4-9- تقنيات منع الأعطال في شبكات الاستشعار اللاسلكية.....87

4-10- خلاصة الفصل.....88

5 نمذجة شبكات الاستشعار اللاسلكية باستخدام البيان.....89

5-1- مقدمة.....89

5-2- الدراسات السابقة.....89

5-3- النموذج المقترح.....90

5-3-1. مرحلة التخطيط.....91

5-3-2. النموذج الجزئي لبناء شبكة هرمية متعددة المستويات.....92

5-3-3. النموذج الجزئي لحساب الأوزان التراكمية.....93

5-3-4. التمثيل البياني والاستنتاج.....94

5-3-5. نموذج إدارة استهلاك الطاقة وتحسين متانة الشبكة.....95

5-3-6. محاكاة النموذج المقترح.....97

5-3-7. كفاءة النموذج المقترح.....100

5-3-8. المقارنة وتقييم فعالية اختيار البيان العشوائي الهندسي للنمذجة.....100

5-3-9. التعقيد الزمني للنموذج المقترح.....102

5-4- خلاصة الفصل.....102

6 نموذج الشبكة المتسامح مع الأعطال.....103

6-1- مقدمة.....103

6-2- النموذج المتسامح مع الأعطال.....103

6-2-1. الأعطال التي يعالجها النموذج.....104

6-2-2. آلية العمل.....104

6-2-3. البداية والإطار الزمني.....104

6-2-4. النمذجة الاحتمالية لزمن فشل العقدة.....105

6-2-5. الفحص الأولي للعقد باستخدام التوزيع الأسي.....106

6-2-6. تشكيل المكون العملاق المتسامح مع الأعطال.....107

6-2-7. آلية التعافي الديناميكي وإعادة توزيع الحمل بعد فقدان العُقد.....108

6-2-8. ضبط الحساسية الزمنية وإعادة التكيف.....109

6-2-9. خوارزمية إعادة توزيع الحمل بناءً على الطاقة المتاحة.....110

6-2-10. آلية التحديث عند تجاوز أحد العتبات.....111

6-3- التعقيد الزمني للنموذج المطور.....111

6-4- محاكاة النموذج المطور.....112

6-5-1. نتائج المحاكاة الكلية وتقييم فعالية النموذج المقترح إحصائياً.....115

6-5-2. المقارنة مع الدراسات السابقة.....119

6-5- خلاصة الفصل.....122

7 الخوارزمية المقترحة لتشفير بيانات النموذج.....123

7-1- مقدمة.....123

7-2- الخوارزمية المقترحة.....123

7-2-1. توليد المفتاح.....123

7-2-2. تجزئة البيانات.....124

7-2-3. ملء المصفوفة.....124

7-2-4. تبديل الأعمدة.....124

7-2-5. قلب البتات.....125

7-2-6. القراءة العامودية.....125

7-2-7. الضغط باستخدام RLE 125

7-2-8. فك التشفير.....125

7-3- ميزات الخوارزمية المقترحة.....126

7-4- محاكاة الخوارزمية المقترحة.....126

7-5- محاكاة فك التشفير.....129

7-6- التعقيد الزمني للخوارزمية المقترحة.....130

7-7- مقارنة بين الخوارزمية المقترحة وخوارزمية سابقة.....131

7-8- خلاصة الفصل.....133

فهارس الوسائل الإيضاحية والإجرائية في البحث

قائمة الاشكال

الشكل(1-1) البيان G_1.....33

الشكل(3-1) بنية شبكة الاستشعار.....60

الشكل (3-2) بنية القفزة الواحدة.....61

الشكل(3-3) طوبولوجيا الناقل.....62

الشكل(3-4) الطوبولوجيا الشجرية.....63

الشكل(3-5) الطوبولوجيا النجمية.....63

الشكل(3-6) طوبولوجيا المشبك.....64

الشكل(4-1) الشبكة المتشابكة.....85

الشكل (4-2) المسارات المنفصلة.....86

الشكل (5-1) توزيع مسافات العقد من المحطة.....98

الشكل (5-2) توزيع عدد العقد التابعة.....98

الشكل (5-3) الطاقة المتبقية مقابل المسافة.....99

الشكل (5-4) توزيع العقد على المستويات.....99

الشكل (5-5) الهيكل الهرمي للشبكة.....100

الشكل (6-1) تطور الأعطال مع الزمن.....105

الشكل (6-2) الطاقة المتبقية للعقد العاملة.....107

الشكل (6-3) التعقيد الزمني.....112

الشكل (6-4) محاكاة استهلاك الطاقة.....113

الشكل (6-5) النتائج النهائية والتعقيد الحسابي 113

الشكل (6-6) الطاقة النهائية للعقد النشطة.....114

الشكل (6-7) ديناميكية العقد مع الزمن.....115

الشكل (6-8) الجولات التي تفشل فيها عقد الشبكة.....117

الشكل (6-9) تحليل بنية الشبكة بدون التسامح.....117

الشكل (6-10) نسبة النجاح والطاقة المتبقية.....118

الشكل (6-11) حجم المكون العملاق.....118

الشكل (6-12) مقارنة بعمر الشبكة ومعدل النجاة النهائي.....119

الشكل (7-1) المصفوفة الأصلية.....127

الشكل (7-2) المصفوفة بعد تبديل الأعمدة.....127

الشكل (7-3) المصفوفة بعد قلب البتات.....128

الشكل (7-4) واجهة المستخدم لعملية التشفير 129

الشكل (7-5) واجهة المستخدم لعملية فك التشفير.....130

قائمة الجداول

الجدول(1-1) مقارنة بين النماذج العشوائية.....37

الجدول (2-1) مقارنة بين الشيفرات الكلاسيكية.....49

الجدول(2-2) مقارنة بين خوارزميات التشفير.....51

الجدول(2-3) مقارنة بين دوال التقطيع.....53

الجدول(4-1) مقارنة بين التكرار الساكن والتكرار الديناميكي.....76

الجدول (5-1) مقارنة بين البيانات.....101

الجدول (6-1) مقاييس الأداء.....116

الجدول (6-1) مقارنة بين النماذج.....121

الجدول (7-1) مقارنة بين خوارزمية التشفير المقترحة وخوارزميات تشفير أخرى.....132

المصطلحات العلمية

المصطلح الإنجليزي	المصطلح العربي
Graph	البيان
Random Geometric Graph	البيان الهندسي العشوائي
Vertex/Node	رأس /عقدة
Edge	ضلع
Adjacency Matrix	مصفوفة التجاور
Level Matrix	مصفوفة المستويات
Node Degree	درجة العقدة
Giant Component	المكون العملاق
Dominating Node	العقدة المسيطرة
Cumulative Weight	الوزن التراكمي
Path Cost	تكلفة المسار
Optimal Path	المسار الأمثل
Weighted Graph	البيان الموزون
Simple Graph	البيان البسيط
Undirected Graph	البيان غير الموجه
Transmission Radius	نصف قطر الإرسال
Critical Connectivity Threshold	العتبة الحرجة للاتصال

شبكة الاستشعار اللاسلكية	Wireless Sensor Network
عقدة الاستشعار	Sensor Node
المحطة الأساسية	Base Station-BS
النشر العشوائي	Random Deployment
الهيكل الهرمي	Hierarchical Structure
الطاقة الأولية	Initial Energy
الطاقة المتبقية	Remaining Energy
الطاقة المستهلكة	Consumed Energy
إدارة الطاقة	Energy Management
عمر الشبكة	Network Lifetime
توزان الحمل	Load Balancing
التوجيه	Routing
المسار البديل	Alternative Path
حزمة البيانات	Data Packet
رسالة الاستعلام	Query Message
رسالة الرد	Reply Message
معدل النجاة	Survival Rate
عقدة آمنة	Safe Node
عقدة مهددة	Threatened Node

عقدة حرجة	Critical node
التسامح مع الأعطال	Fault tolerance
العطل الفردي	Single fault
العطل المتعدد	Multiple fault
نفاد الطاقة	Energy depletion
هجوم استنزاف الطاقة	Energy drain attack
الفشل المفاجئ	Sudden failure
التدهور التدريجي	Progressive degradation
عتبة الاتصال البنيوي	Structural connectivity threshold
عتبة العقد الحرجة	Critical node threshold
الطبقة البنيوية	Structural layer
الطبقة التشغيلية	operational layer
طبقة المراقبة والتكيف	Monitoring and adaptation layer
زمن الفشل	Failure time
معدل الفشل	Failure rate
التوزيع الأسي	Exponential distribution
دالة الكثافة الاحتمالية	Probability density function
احتمال الفشل	Failure probability
احتمال البقاء	Survival probability

خاصية انعدام الذاكرة	Memory less probability
التشفير المتماثل	Symmetric encryption
قلب البتات	Bit flipping
مصفوفة المستويات	Level matrix
المحاكاة	simulation
المسافة الإقليدية	Euclidean distance
التعقيد الزمني	Time complexity

الملخص

تعتبر شبكات الاستشعار اللاسلكية من أهم الأنظمة التي لها مهام في العديد من المجالات سواء الاقتصادية أو الأمنية أو الزراعية ....إلخ. تنشر شبكات الاستشعار لإنجاز تلك المهام على مدى فترة من الزمن. لكن من الضروري أن تستمر الشبكة بالعمل حتى لو تعطلت بعض عقدها. تنشر شبكات الاستشعار اللاسلكية بطريقة تخفف من الأعطال أو تمكن من الوصول إلى عقدها لإصلاح العطل. لكن بعض المجالات تحتم النشر العشوائي لشبكات الاستشعار اللاسلكية مما يجعلها عرضة للعديد من الأعطال سواء الناتجة عن الظروف الجوية أو الأمنية. تهدف هذه الأطروحة إلى تطوير نموذج رياضي لتحقيق التسامح مع الأعطال في شبكات الاستشعار اللاسلكية المنشورة عشوائياً وغير المتجانسة، باستخدام البيان العشوائي الهندسي. يسعى البحث للإجابة عن كيفية تحسين كفاءة الشبكة وإطالة عمرها التشغيلي من خلال تحسين استهلاك الطاقة وإدارة الأعطال التلقائية. بدايةً تم نمذجة الشبكة بالاعتماد على بيان هندسي عشوائي يتضمن النموذج آليات لإدارة الطاقة وحذف الارتباطات غير الفعالة، بعد ذلك تطوير النموذج ليصبح متسامحاً مع الأعطال بتشكيل المكون العملاق. كما تم اقتراح خوارزمية تشفير مساعدة لحماية البيانات المنقولة بين العقد تعتمد على نظرية البيان. أظهرت محاكاة النموذج باستخدام برنامج MATLAB 2015 فعاليته في خفض استهلاك الطاقة، وإطالة عمر الشبكة، والحفاظ على توفر الاتصالات تحت ظروف الأعطال، مع تعقيد زمني مقبول.

الكلمات الرئيسية: شبكات الاستشعار اللاسلكية، التسامح مع الأعطال، نظرية البيان، البيان العشوائي الهندسي، نمذجة الشبكات، إدارة الطاقة، المكون العملاق، المحاكاة الرياضية.

مقدمة

تعد عمليات المراقبة عن بعد لأحداث حسية مختلفة ومتعددة، كالمراقبة البيئة والأمنية والصحية، ورصد اقتحام المناطق المحظورة، ورصد الأحوال الجوية، مجالات مهمة في العالم نتيجة التطور السريع الذي نشهده في يومنا هذا. كما أنها من أوسع تطبيقات شبكات الاستشعار اللاسلكية. تعتبر شبكات الاستشعار اللاسلكية ذات أهمية كبيرة في مجال الاتصال اللاسلكي والنظم الموزعة. عادة تكون شبكات الاستشعار اللاسلكية مستخدمة في بيئات قاسية وغير موثوقة، مما يجعل العقد تواجه تحديات كبيرة من حيث استهلاك الطاقة، وضعف الموارد الحاسوبية، وتأثرها بالأعطال. تعمل عقد الاستشعار في ظل قيود صارمة على الطاقة، مما يجعل كمية الطاقة المخصصة للاختبار وتحمل الأخطاء محدودة للغاية. تعد الطاقة العامل الأكثر تعقيداً لوظيفة الشبكة [1]. تسعى الأبحاث الحديثة لإيجاد نماذج متسامحة مع الأعطال لشبكات الاستشعار اللاسلكية. غالباً ما يتم تمثيل شبكات الاستشعار اللاسلكية ببيان، بحيث يتوافق الرأس من البيان مع عقدة الاستشعار، والضلع مع الاتصال بين عقدتين. تعتبر عملية دمج نظرية البيان مع نشر الشبكات أحد مجالات البحث العلمي النشطة جداً.

مشكلة البحث

تتسم شبكات الاستشعار اللاسلكية بطبيعة نشر عشوائية وغير متجانسة في كثير من التطبيقات العملية، كما تعمل في بيئات قاسية وغير موثوقة مما يعرضها لمختلف أنواع الأعطال، خاصة تلك الناتجة عن استنفاد الطاقة أو الهجمات الأمنية. مما يؤدي إلى تحديات جسيمة في استمرارية عمل الشبكة وموثوقية البيانات المنقولة. على الرغم من تطور النمذجة الرياضية وتحليل الشبكات، فإن النماذج القائمة غالباً ما تفترض معرفة مسبقة بهيكل الشبكة أو توزع عقدها، مما يحد من فعاليتها في نمذجة الشبكات غير المتجانسة والمنشورة عشوائياً. لذلك تبرز الحاجة إلى تطوير نموذج رياضي يعتمد على نظرية البيان العشوائي الهندسي لتحقيق التسامح مع الأعطال في مثل هذه الشبكات، مع ضمان تقليل استهلاك الطاقة والحفاظ على اتصال الشبكة تحت ظروف الأعطال المتعددة [2].

تساؤلات البحث

يرتكز البحث على تساؤلات عديدة نذكر منها الآتي:

1. كيف يمكن استخدام نظرية البيان العشوائي الهندسي لنمذجة شبكات الاستشعار اللاسلكية المنشورة عشوائياً وغير المتجانسة؟
2. ما هي الأدوات الرياضية والخوارزميات الفعالة لتحقيق التسامح مع الأعطال في هذه الشبكات مع تحسين إدارة الطاقة؟
3. كيف يمكن تشكيل مكون عملاق متسامح مع الأعطال لضمان استمرارية الاتصال في الشبكة رغم فقدان بعض العقد؟
4. ما هو التعقيد الزمني للنموذج المقترح، وكيف تقارن كفاءته مع النماذج التقليدية من حيث إطالة عمر الشبكة وخفض استهلاك الطاقة؟
5. كيف يمكن ضمان سرية البيانات المنقولة بخوارزمية تتناسب مع النموذج المقترح؟

هدف البحث

يهدف البحث إلى:

1. تطوير نموذج رياضي قائم على نظرية البيان العشوائي الهندسي لتحقيق التسامح مع الأعطال في شبكات الاستشعار اللاسلكية غير المتجانسة والمنشورة عشوائياً.
2. تحسين متانة الشبكة وإطالة عمرها التشغيلي من خلال تقليل استهلاك الطاقة في النموذج المقترح.
3. اقتراح خوارزمية تشفير مساعدة تعتمد على مفاهيم نظرية البيان لتعزيز أمن البيانات المنقولة في الشبكة.
4. محاكاة النموذج والخوارزمية المقترحين باستخدام بيئة الماتلاب لتقييم أدائهما والتحقق من فعاليتهما العملية.

أهمية البحث

تكمن أهمية هذا البحث في تناوله ضمان استمرارية وموثوقية عمل شبكات الاستشعار اللاسلكية في البيئات القاسية وغير الموثوقة، فالأعطال وخاصة الناجمة عن استنفاد الطاقة حتمية. يساهم هذا البحث من

خلال النموذج المقترح في محاولة سد فجوة النمذجة الرياضية للشبكات العشوائية غير المتجانسة، مع تقديم آليات عملية لإدارة الطاقة والتسامح مع الأعطال. كما أن دمج مفهوم التشفير القائم على البيان يضيف بُعداً أمنياً هاماً. النتائج المتوقعة لهذا البحث يمكن أن تُطَبَّق في مجالات حيوية مثل المراقبة البيئية والمراقبة الأمنية والرعاية الصحية الذكية، حيث تعتمد جودة القرارات على استمرارية تدفق البيانات الموثوقة.

مسوغات البحث

تعتبر الدافع الرئيسي هذا البحث هو الطبيعة الحرجة لتطبيقات شبكات الاستشعار اللاسلكية وانتشارها الواسع، مقترناً مع التحديات الكبيرة التي تواجهها بسبب مواردها المحدودة وبيئات عملها الصعبة. يسعى هذا البحث إلى الاستفادة من القوة الرياضية لنظرية البيان العشوائي الهندسي لتقديم نموذج أكثر واقعية وقدرة على الصمود، مما يسهم في تطوير حلول أكثر قوة وموثوقية لهذه الشبكات المهمة.

محدوديات البحث

يركز هذا البحث بشكل أساسي على معالجة أعطال استنفاد الطاقة والأعطال الناجمة عن الهجمات المستهدفة لاستنزاف الطاقة في سياق الشبكات العشوائية غير المتجانسة. تجدر الإشارة إلى أن النموذج المدروس لا يتناول كل أنواع الأعطال الأمنية أو الأعطال الفيزيائية الشاملة. بالإضافة إلى ذلك، فإن خوارزمية التشفير المقترحة تعمل على حماية عقد الاستشعار من الاختراق الأمني كالتنصت وتخدم النموذج المقترح وتتناسب مع طبيعة شبكات الاستشعار اللاسلكية لكنها أقل قوة مقارنة بمعايير التشفير القوية المعتمدة.

الدراسات المرجعية

يتمحور الإطار النظري والدراسات المرجعية لهذا البحث حول أربعة محاور رئيسية مترابطة تشكل الأساس الذي يُبنى عليه العمل المقترح. أولاً، يتم استعراض المفاهيم والأدوات الرياضية الأساسية في نظرية البيان، مع تركيز خاص على البيان العشوائي الهندسي الذي يشكل العمود الفقري للنموذج المقترح. ثانياً، يتم

تناول مفاهيم التشفير الحديثة ودورها في أمن الشبكات، بما في ذلك بعض المحاولات الرائدة لاستخدام نظرية البيان في التشفير. ثالثاً، يتم تقديم المفاهيم الأساسية لشبكات الاستشعار اللاسلكية، من حيث المكونات، والبنى، والتطبيقات، والتحديات التصميمية الرئيسية. رابعاً وأخيراً، يتم استعراض نظريات وآليات التسامح مع الأعطال بشكل عام، ثم التطبيقات والتقنيات الخاصة بشبكات الاستشعار اللاسلكية. كما سيتم تحليل واستعراض أهم الدراسات السابقة التي حاولت استخدام نماذج البيان (العادية والعشوائية) في نمذجة وتحسين أداء هذه الشبكات، مع تسليط الضوء على الثغرات التي يسعى هذا البحث لمعالجتها.

خلاصة الدراسات المرجعية

مكنتنا الدراسة المتعمقة للإطار النظري والدراسات السابقة من تحديد الفجوة البحثية بوضوح، حيث أظهرت محدودية الطاقة في شبكات الاستشعار اللاسلكية. كما وفرت لنا الأدوات الرياضية اللازمة (البيان العشوائي الهندسي) والمنطلقات التصميمية (إدارة الطاقة، تشكيل المكون العملاق) لتطوير نموذج رياضي متكامل. لقد استفدنا من آليات التسامح مع الأعطال وقمنا بتكييفها مع الطبيعة الديناميكية والعشوائية للشبكة المستهدفة. كما ألهمتنا بعض المحاولات في دمج التشفير مع نظرية البيان لتطوير خوارزمية تشفير تحمي بيانات العقد وتتناسب مع طبيعة النموذج المقترح.

منهج البحث وأدواته

اعتمد المنهج المتبع في هذا البحث على النهج التكاملي الذي يجمع بين النمذجة الرياضية والتصميم الخوارزمي والمحاكاة الحاسوبية. بدأ العمل بتطوير نموذج رياضي قائم على البيان العشوائي الهندسي لتمثيل الشبكة العشوائية غير المتجانسة. ثم تم تصميم خوارزميات هرمية لإدارة الطاقة وبناء المسارات المثلى، تلاها تطوير آلية ديناميكية لتشكيل مكون عملاق متسامح مع الأعطال يحافظ على اتصال الشبكة الأساسي رغم فقدان بعض العقد. بالتوازي، تم اقتراح خوارزمية تشفير تعتمد على تحويل البيانات وتبديل المصفوفات مستوحاة من مفاهيم نظرية البيان. تم تنفيذ النموذج المقترح بكافة مكوناته (النمذجة، إدارة الطاقة، التسامح مع الأعطال،

التشفير) واختباره باستخدام بيئة الماتلاب (MATLAB) لإجراء عمليات المحاكاة الواسعة، وتحليل التعقيد الزمني، وتقييم الأداء من حيث استهلاك الطاقة، وعمر الشبكة، وقدرتها على الحفاظ على الاتصال رغم الأعطال المختلفة.

خطة العمل

تم إعداد هذه الأطروحة بشكل يسهل متابعته حتى للقارئ غير المتخصص، حيث تبدأ بتأسيس المفاهيم النظرية اللازمة، ثم تنتقل إلى التطبيقات والنمذجة، وتختتم بالنتائج والتقييم. تتألف الأطروحة من سبعة فصول رئيسية توزعت وفق الخطة الآتية:

الفصل الأول: مفاهيم أساسية في نظرية البيان والبيان العشوائي

خصصنا هذا الفصل لدراسة المفاهيم الأساسية في نظرية البيان والتمثيلات المصفوفية. ثم تطرقنا إلى مفهوم البيان العشوائي وركزنا على البيان العشوائي الهندسي. ذكرنا أهمية كل من البيان والبيان العشوائي في العديد من التطبيقات.

الفصل الثاني: مفاهيم أساسية في التشفير

خصصنا هذا الفصل للتعرف على المفاهيم الأساسية في التشفير وأنواعه وخوارزميات التشفير وتطرقنا إلى إمكانية استخدام البيان في التشفير.

الفصل الثالث: مفاهيم أساسية في شبكات الاستشعار اللاسلكية

تطرقنا في هذا الفصل إلى المفاهيم الأساسية في شبكات الاستشعار اللاسلكية. بالإضافة إلى التعرف على طوبولوجيا الشبكة وتطبيقاتها، والعوامل المؤثرة في تصميم شبكات الاستشعار اللاسلكية.

الفصل الرابع: التسامح مع الأعطال في شبكات الاستشعار اللاسلكية

نتعرف في هذا الفصل على مفهوم التسامح مع الأعطال، وتقنياته، وأهميته وتطبيقه في شبكات الاستشعار. بالإضافة إلى التطرق لأعطال شبكات الاستشعار اللاسلكية وطرق تشخيصها.

الفصل الخامس: نمذجة شبكات الاستشعار باستخدام البيان

يعرض الفصل النموذج الخوارزمي المقترح لنمذجة شبكات الاستشعار اللاسلكية المنشورة عشوائياً وقدرته على تحسين استهلاك الطاقة.

الفصل السادس: نموذج الشبكة المتسامح مع الأعطال

يقدم الفصل تطوير للنموذج المقترح ليكون متسامحاً مع الأعطال من خلال تشكيل المكون العملاق.

الفصل السابع: الخوارزمية المقترحة لتشفير بيانات النموذج

يقدم الفصل خوارزمية تشفير مناسبة للنموذج المقترح ليصبح قادراً على الحفاظ على أمن البيانات المرسلة. تعتمد الخوارزمية على مفاهيم أساسية في البيان.

1 مفاهيم أساسية في نظرية البيان والبيان العشوائي

1-1-مقدمة

تعتبر نظرية البيان من أكثر مجالات الرياضيات نشاطاً والتي وجدت عدداً كبيراً من التطبيقات في مجالات متنوعة مثل علوم الحاسوب حيث يمكن تمثيل أي بنية معطيات بواسطة البيان بالإضافة للكيمياء والفيزياء والتاريخ والعديد من الفروع الاخرى. سنعرض في هذا الفصل أهم المفاهيم الأساسية في نظرية البيان، والتمثيلات المصفوفية بالإضافة للتطرق لنظرية البيان العشوائي وأهميته وتطبيقاته.

1-2- تعاريف أساسية

فيما يأتي نقدم بعض التعاريف الأساسية والمصطلحات في نظرية البيان والبيان العشوائي التي تفيد في توضيح دراستنا المرجعية [3].

1-2-1. البيان (Graph)

يتألف البيان G من مجموعة V غير خالية من العناصر تدعى مجموعة العقد، مع مجموعة E كل عنصر منها مؤلف من عنصرين من V، وتدعى هذه العناصر بالأضلاع. لنعرف التطبيق f كالآتي:

$$f: E \to \{\{x, y\}: x, y \in V\}$$

أي إذا كان $e \in E$ ضلعاً، وكانت $x, y \in V$ عقدتين بحيث: $f(e) = (x, y)$، عندها فإن الضلع e يربط العقدتين x, y، وندعو العقدتين x, y بطرفي الضلع e.

نسمي الثلاثية المرتبة $G = (V, E, f)$ بياناً. نقول إن الثلاثية (V, E, f) هي بيان منته إذا كانت كل من المجموعتين V و E مجموعة منتهية.

ملاحظة (1-1)

إذا كان $G = (V, E, f)$ بياناً، فإننا سنطابق كل ضلع مع صورته بواسطة التطبيق f، ولا نفرق بينهما. أي إذا كان e ضلعاً يربط بين العقدتين v و u، وبالتالي $f(e) = (u, v)$، فإننا نكتب $e = (u, v)$.

أي إننا نتجاهل التطبيق f، وعندها يمكننا أن نكتب الرمز $G = (V, E)$ بدلاً من الرمز $G = (V, E, f)$.

1-2-2. العروة (Loop)

العروة هي ضلع فيه عقدة البداية وعقدة النهاية نفسها أي $e = \{x\}$ ونسمي الضلع e عروة عند x.

1-2-3. الضلع المضاعف (Multiple Edge)

إذا كان $e_1 = e_2 = (x, y)$ بحيث $x \neq y$ عندئذ نسمي كلاً من e_1 و e_2 ضلعاً مضاعفاً. أما إذا كان $x = y$ عندئذ نسمي العروة e_1 والعروة e_2 عروة مضاعفة عند العقدة x.

1-2-4. البيان البسيط (Simple Graph)

نقول عن البيان إنه بسيط إذا لم يحتو على عرى أو أضلاع مضاعفة.

1-2-5. القوس (Arc)

القوس هو ضلع e مزود باتجاه ونرمز له بـ $\vec{e}$.

1-2-6. البيان الموجه (Directed Graph)

البيان الموجه هو بيان زودت أضلاعه باتجاه ويرمز للبيان الموجه بالثنائية المرتبة $\vec{G}$=(V,$\vec{E}$) حيث V هي مجموعة العقد وE هي مجموعة الأقواس.

1-2-7. البيان الموزون (Weighted Graph)

البيان الموزون هو الثلاثية $G = (V, E, w)$ حيث V مجموعة العقد و E مجموعة الأضلاع، و $w: E \to R$ دالة الوزن التي تعين لكل ضلع e وزناً يمثل قيمة عددية حقيقية، قد تكون موجبة أو سالبة.

1-2-8. المسار (Walk)

إن مفهوم المسارات في البيان له أهمية في نظرية البيان وخاصة في المجالات التطبيقية لنظرية البيان. ليكن $G = (V, E)$ بياناً، وليكن $a, b \in V$، وليكن $n \geq 1$ عدداً صحيحاً عندئذٍ نعرف المسار كالآتي:

إذا كانت $v_1, e_1, v_2, \dots, e_{n-1}, v_n$ متتالية متناوبة من الرؤوس والأضلاع، حيث $v_n = b$,$v_1 = a$ و $e_i = (v_i, v_{i+1})$ من أجل كل $i = 1, .., n-1$، عندها نسمي المتتالية السابقة مساراً من a إلى b.

المسار الموجه هو متتالية متناوبة من العقد والأقواس يكون فيه مصدر القوس $\overrightarrow{e_i}$ هو عقدة الهدف للقوس $\overrightarrow{e_{i-1}}$ من أجل $i = 1,2, \dots, n$.

كما نعّرف طول المسار (المسار الموجه) بأنه عدد الأضلاع (الأقواس) في المتتالية. يكون المسار مساراً مغلقاً إذا كانت عقدة البداية هي عقدة النهاية نفسها.

1-2-9. البيان الأولري (Euler Graph)

يعرَّف البيان الأولري بأنه بيان غير موجه يحتوي على دارة أولرية. الدارة الأولرية هي مسار مغلق يمر عبر كل ضلع في البيان مرة واحدة بالضبط دون تكرار. قد يُستخدم مصطلح البيان الأولري أحياناً ليشير إلى بيان درجة كل عقدة فيه عدداً زوجياً [4].

1-2-10. مسار هاملتون (Hamiltonian Path)

مسار هاملتون هو مسار يزور كل عقدة في البيان مرة واحدة بالضبط.

1-2-11. دائرة هاملتون (Hamiltonian Circuit)

تعرف دائرة هاملتون بأنها مسار هاملتوني مغلق، أي يبدأ وينتهي عند نفس العقدة.

1-2-12. بيان هاملتون (Hamiltonian Graph)

يُسمى البيان الذي يحتوي على دائرة هاملتون بياناً هاملتونياً. أما البيان الهاملتوني المتصل، هو البيان الذي يوجد بين كل زوج من رؤوسه مسار هاملتوني [4].

1-2-13. عقدة المصدر (Source Node)

ليكن لدينا البيان الموجه $\vec{G}=(V,\vec{E})$ ولتكن v_i عقدة من مجموعة العقد V. نسمي العقدة v_i عقدة مصدر إذا وفقط إذا كانت هذه العقدة عقدة بداية لجميع الأقواس المؤثرة فيها.

1-2-14. عقدة الهدف (Target Node)

ليكن لدينا البيان الموجه $\vec{G}=(V,\vec{E})$ ولتكن v_i عقدة من مجموعة العقد V. نسمي العقدة v_i عقدة هدف إذاً وفقط إذا كانت هذه العقدة عقدة نهاية لجميع الأقواس المؤثرة فيها.

1-2-15. درجة العقدة (Vertex Degree)

إذا كان G=(V,E) بياناً وكانت $x\in V$ فإننا نعرف درجة العقدة x بإنها عدد الأضلاع من البيان G المؤثرة في العقدة x مع الملاحظة أن العروة تؤثر على العقدة مرتين. نرمز لدرجة العقدة x بالرمز deg(x) ونلاحظ أن:

$$\deg(x) = |(e: e = (x,y) \forall y \in V \wedge x \neq y)| + 2|e: e = (x,x)|$$

أما درجة العقدة في البيان الموجه تنقسم إلى نوعين:

1. درجة الدخول للعقدة v هي عدد الأضلاع الداخلة إلى العقدة v ويرمز لها بـ deg−(v).
2. درجة الخروج للعقدة v هي عدد الأضلاع الخارجة من العقدة v ويرمز لها بـ deg+(v).

1-2-16. العقدة المعزولة (Isolated Vertex)

ليكن لدينا البيان G ندعو العقدة x بعقدة معزولة إذا لم يؤثر فيها أي ضلع من البيان G، أي إذا كانت درجة العقدة deg(x)=0.

1-3-التمثيلات المصفوفية (Matrix Representations)

لمصفوفات البيان أهمية كبيرة في تمثيل البيان. لذلك سنعرض عدة أنواع هامة من المصفوفات المستخدمة في نظرية البيان.

1-3-1. مصفوفة التأثير (Incidence Matrix)

ليكن لدينا البيان البسيط $G = (V, E)$ حيث مجموعة العقد $V = \{x_1, x_2, \dots, x_n\}$، ومجموعة الأضلاع $E = \{e_1, e_2, \dots, e_m\}$. نعرف مصفوفة التأثير للبيان G بأنها المصفوفة $B = [b_{ij}]$ من البعد $n \times m$ حيث:

$$b_{ij} = \begin{cases} 1 & x_i \text{ يؤثر على } e_j \\ 0 & x_i \text{ لا يؤثر على } e_j \end{cases}$$

أما مصفوفة التأثير للبيان غير البسيط $G = (V, E)$ هي المصفوفة B_G التي أسطرها مرقمة حسب العقد وأعمدتها مرقمة حسب الأضلاع بحيث:

$$B_G[v, e] = \begin{cases} 0 & \text{إذا كانت } v \text{ ليس طرفاً لـ} e \\ 1 & \text{إذا كانت } v \text{ طرفاً لـ} e \\ 2 & \text{إذا كانت } e \text{ عروة حول} v \end{cases}$$

ليكن لدينا البيان الموجه $\vec{G} = (V, \vec{E})$. مصفوفة التأثير للبيان $\vec{G}$ تعطى بالشكل:

$$B_D[v, e] = \begin{cases} 0 & \text{إذا لم تكن } v \text{ طرفاً لـ } e \\ 1 & \text{إذا كانت } v \text{ عقدة مصدر لـ } e \\ -1 & \text{إذا كانت } v \text{ عقدة هدف لـ } e \\ 2 & \text{إذا كانت } e \text{ عروة حول } v \end{cases}$$

1-3-2. مصفوفة التجاور (Adjacency Matrix)

ليكن G(V, E) بياناً بسيطاً مجموعة عقده $V = \{v_1, v_2, \dots, v_n\}$ ومجموعة أضلاعه $E = \{e_1, e_2, \dots, e_m\}$. نعرف مصفوفة التجاور لـ G بأنها المصفوفة المربعة $A = [a_{ij}]$ من البعد $n \times n$ حيث:

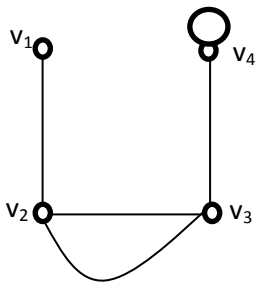
$$a_{ij} = \begin{cases} 1 & (v_i, v_j) \in E \\ 0 & (v_i, v_j) \notin E \end{cases}$$

أما مصفوفة التجاور لبيان غير البسيط $G(V, E)$ تعطى كما يلي :

$$a_{ij} = \begin{cases} 0 & (v_i, v_j) \notin E \\ 1 & (v_i, v_j) \in E \\ 2 & (v_i, v_i) \in E \end{cases}$$

مثال (1−1)

مصفوفة تجاور البيان G_1 الموضح في الشكل (1−1).



الشكل (1-1) البيان G_1

هي:

$$\begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 2 & 0 \\ 0 & 2 & 0 & 1 \\ 0 & 0 & 1 & 2 \end{bmatrix}$$

1−4−البيان الديناميكي

بعد التعرف على كل من البيان والبيان الموجه والبيان الموزون بالأضلاع. نلاحظ أن تعريفات البيان الثابت والشبكات تتضمن أربع مكونات: V (مجموعة من العقد)، E (مجموعة من الأضلاع)، f (تابع تعين أوزان العقد)، g (تابع تعين أوزان الاضلاع). يتم الحصول على بيان ديناميكي عندما يتغير أي مكون من المكونات الاربعة بمرور الوقت، وبالتالي هناك أربعة أنواع أساسية من البيانات الديناميكية.

1. بيان ديناميكي العقد، تختلف مجموعة العقد V بمرور الوقت وبالتالي يمكن إضافة بعض العقد أو إزالتها. عند إزالة العقد، يتم التخلص من الأضلاع أو الأقواس المرتبطة بها.

2. بيان ديناميكي الأضلاع، تختلف مجموعة الأضلاع E بمرور الوقت وبالتالي يمكن إضافة بعض الأضلاع أو إزالتها.

3. البيان الديناميكي الموزون للعقد، تختلف الدالة f مع الوقت وبالتالي تتغير أوزان للعقد.

4. البيان الديناميكي الموزون للأضلاع، تختلف الدالة g مع الوقت فتتغير الأوزان على الأضلاع.

يمكن أن نحتاج إلى بيان ديناميكي يستلزم جميع الأنواع المذكورة في الأعلى على سبيل المثال شبكة الحاسوب ذات النطاق الترددي المتغير (وزن الضلع)، تغير البنية (إضافة الأضلاع أو حذفها)، تغير قوة الحوسبة (تغير وزن العقد) وحالات تعطل أجهزة الحاسوب (تعطل العقد) واستعادتها للعمل.

1-5-تطبيقات البيان

يعد البيان أداة نمذجة ممتازة لنمذجة العديد من أنواع العلاقات وتمثيل مشاكل العالم الحقيقي. لتمثيل تطبيقات نظرية البيان تم النظر في نوعين من المشاكل الأول هو الجانب النظري للبيان والثاني هو المشاكل التطبيقية والتي تتركز على تنفيذ نظريات البيان. لا يمكن حصر تطبيقات البيان لذا سنذكر بعض تطبيقات خوارزميات نظرية البيان في حل المشكلات [5].

1-5-4. نظرية الألوان الأربعة

تنص نظرية الألوان الأربعة أنه بالنسبة لأي خريطة نحتاج إلى أربعة الوان فقط لتلوينها بحيث لا يكون هناك دولتين متجاورتين (لهما حدود مشتركة) اللون نفسه. أثبتت نظرية الالوان المطبقة على رسم الخرائط أنها مفيدة في تخطيط شبكات الاتصالات اللاسلكية. كما أنها مفيدة في خطة وضع الأبراج الخلوية اللاسلكية. يتم تمثيل كل قناة بث لبرج خلوي بلون ما، وتقتصر ألوان القناة على أربعة ألوان. وبالتالي فإن مهمة العثور على مكان وضع أبراج البث بشكل اقتصادي تتساوى مع مشكلة الألوان الأربعة. تكمن التحديات في:

1. القضاء على المناطق التي لا توجد فيها تغطية.
2. تخصيص قناة مختلفة في المواقع التي يحدث فيها تداخل القنوات. يتم تسليم إشارات الهاتف الخليوي إلى قناة مختلفة، ولذلك تستخدم كل منطقة برج مراقبة واحد بقناة محددة.

1-5-5. معالجة الصور

معالجة الصور أو تحليل الصور هي المنهجية التي يتم من خلالها استخراج المعلومات من الصور. يتم إجراء تحليل الصور بشكل رئيسي باستخدام تقنيات معالجة الصور الرقمية. يمكن تحسين معالجة الصور باستخدام نظرية البيان. تكمن تطبيقات البيان في معالجة الصور بكشف حدود الأجسام باستخدام خوارزميات البحث في البيان واستراتيجيات التجزئة، يمكن تحديد الحدود بين المناطق المختلفة في الصورة بدقة. وحساب هيكل الصورة عن طريق بناء أقل شجرة ممتدة حيث تمثل البكسلات العقد وتمثل الروابط بين البكسلات بالأضلاع وحساب المسافة بين البكسلات داخل الصورة باستخدام خوارزميات المسار الاقصر[5].

1-5-6. الشبكة الاجتماعية

إن الشبكة الاجتماعية هي بنية اجتماعية مكونة من أفراد ترتبط بأكثر من نوع واحد من أنواع الترابط، على سبيل المثال: القرابة، الصداقة، المصالح المشتركة. تعد الشبكة الاجتماعية جزءاً من علم الاجتماع حيث نقوم ضمن تحليل الشبكة الاجتماعية بعرض العلاقات الاجتماعية باستخدام نظرية البيان حيث تمثل العقد بالأشخاص والأضلاع بالعلاقات بينهم [5]. من الأمثلة على الشبكات الاجتماعية Facebook و Twitter. في مجموعة واسعة من الدراسات على الشبكات الاجتماعية تم اكتشاف التشابه على أساس الخصائص المشتركة. استطاعت هذه الدراسات أيضاً إثبات أن هذه التشابهات تزيد من فرص التواصل وتحديد المجتمعات والمواقف الاجتماعية. من أمثلة هذه التشابهات (العمر أو الجنس أو الصف الدراسة). إن الأفراد في علاقات التشابه يتشاركون في بعض السمات مثل المعتقدات والقيم والتعليم مما يعزز ويسهل من تكوين العلاقة وفي المقابل قد نجد أشخاصاً مغايرين أو علاقات مختلطة. لذلك نعمل على تمثيل الشبكات الاجتماعية بالبيان وتطبيق خوارزميات تماثل البيان عليهم مما يسهل علينا ايجاد التشابهات في هذه الشبكات [5].

1-6-البيان العشوائي

تم تعريف البيان العشوائي لأول مرة من قبل Erdós و Rényi في مقالهما "On random graph" المنشور عام 1959 حيث اقترح الباحثان ثلاثة نماذج بيانية عشوائية تحت مسمى البيانات العشوائية Erdos-

Renyi [6]. نعرف البيانات العشوائية بأنها بيانات تتكون من مجموعة عقد متصلة بواسطة أضلاع يتم انشاؤها بطريقة عشوائية. تستخدم هذه النماذج لدراسة الشبكات في ظروف غير محددة مسبقاً وتساعد على فهم الخصائص العامة للشبكات.

1-7-نماذج البيان العشوائي

تعد نماذج البيان العشوائي من الأدوات النظرية الأساسية في دراسة الشبكات المعقدة، إذ تتيح نمذجة وتحليل البنى الشبكية التي تنشأ بطريقة غير منظمة أو تخضع لعمليات احتمالية. ظهرت الحاجة للنماذج في سياقات متعددة تشمل الشبكات الاجتماعية، والأنظمة البيولوجية، وشبكات الاتصال، لوجود خصائص غير متوقعة تنجم عن التوزيع العشوائي للعلاقات أو الأضلاع. من نماذج البيان العشوائي:

1-7-1. البيان العشوائي الموحد (Uniform Random Graph)

البيان العشوائي الموحد هو نموذج رياضي يستخدم لإنشاء شبكات عشوائية باستخدام احتمالات متساوية لربط العقد في الشبكة. ليكن $L_{n,m}$ عائلة كل البيانات التي فيها $V = \{1,2,\dots,n\}$ هي مجموعة العقد و m مجموعة الأضلاع حيث $0 \le m \le \binom{n}{2}$ من أجل كل بيان $G \in L_{n,m}$.

نبدأ ببيان مؤلف من n عقدة معزولة، ثم نختار عشوائياً وباحتمالات متساوية مجموعة من m ضلع من بين جميع الأضلاع الممكنة. نرمز إلى مثل هذا البيان العشوائي بـ$G(n,m)$، ونسميه بياناً عشوائياً موحداً. يوفر هذا النموذج إطاراً مناسباً لتحليل البيانات التي تحافظ على كثافة معينة للأضلاع، ويستخدم عندما يكون عدد الأضلاع معلوماً مسبقاً. من أهم خصائص النموذج العشوائي الموحد أنه يسمح بدراسة سلوك البيانات العشوائية عند قيم ثابتة من الكثافة.

1-7-2. البيان العشوائي ذو الحدين (Binomial Random Graph)

البيان العشوائي ذو الحدين هو نموذج رياضي يستخدم لإنشاء شبكات عشوائية، بحيث يكون لكل ضلع احتمال مستقل للظهور. ليكن P عدداً حقيقياً حيث $0 \le P \le 1$ و لتكن $V = \{1,2,\dots.n\}$ مجموعة العقد لكل زوج من العقد ننشأ ضلع باحتمال P مستقل عن باقلي أزواج العقد الأخرى. نسمي مثل هذا البيان العشوائي

بالبيان ذو الحدين ونشير إليه بـ $G = (n, p)$. على الرغم من بساطته، يقدم النموذج رؤى قوية حول كيفية تشكيل الروابط في الشبكات العشوائية.

1-7-3. البيان العشوائي المعالج (Random Graph Process)

البيان العشوائي المعالج هو البيان الذي ينشأ وفق شروط أو قيود محددة مسبقاً. من أبرز هذه القيود فرض توزيع معين لدرجات العقد أو تطبيق مبدأ النمو التفضيلي (العقد الجديدة تتصل بعقد موجودة باحتمال يتناسب مع درجة تلك العقد). تتميز هذه النماذج بمرونة عالية، وتعد مناسبة لدراسة الشبكات الواقعية، لكنها تتطلب خوارزميات توليد أكثر تعقيداً وتستهلك موارد حسابية أعلى. يمكن تطبيق نموذج البيان العشوائي المعالج في مجالات متعددة مثل شبكات الحاسوب والشبكات الاجتماعية.

1-7-4. مقارنة بين النماذج

يوضح الجدول (1-1) مقارنة بين نماذج البيان العشوائي بالاعتماد على بعض المعايير.

النموذج	المرونة البنيوية	توزيع الأضلاع	عدد الأضلاع	تمثيل الشبكات الواقعية
G(n,m)	منخفضة	منتظم	ثابت	محدود
G(n,p)	متوسطة	احتمالي	متغير(ذو حدين)	متوسط
النموذج المعالج	عالية	مخصص	مقيد حسب الشروط	مرتفع

الجدول (1-1) مقارنة نماذج البيان العشوائي

ملاحظة (1-2)

تستخدم التوزيعات الاحتمالية في نمذجة البيانات العشوائية لتحديد كيفية توزيع العناصر في البيانات العشوائية. على سبيل المثال يمكن استخدام توزيع برنولي لنمذجة الربط العشوائي بين العقد في شبكة عشوائية.

حيث يتم تحديد احتمال الربط بين زوج من العقد كما يمكن استخدام توزيع بواسون لنمذجة عدد الأضلاع في شبكة عشوائية، أي يتم تحديد معدل الارتباط في الشبكة (عدد الأضلاع) من خلال الصيغة :

$$E = \frac{n(n-1)ג}{2}$$

ג هو احتمال الاتصال بين عقدتين [4].

1-8-البيان الهندسي العشوائي (Random Geometric Graph)

البيان العشوائي الهندسي هو نموذج رياضي يستخدم في علم البيانات لتمثيل الشبكات العشوائية التي تتكون من نقاط عشوائية في الفضاء الهندسي. في هذا النموذج يتم توليد نقاط عشوائية في الفضاء، ثم يتم ربط النقاط المتقاربة بأضلاع بناء على معيار هندسي محدد. نرمز للبيان العشوائي الهندسي بـ G(n,r) حيث n هي نقاط من الفضاء R^2 يتم ربط أي نقطتين مع بعضهما البعض بواسطة ضلع إذا كانت المسافة بينهما على الأكثر r.

1-9-مصطلحات هامة في البيان العشوائي

عند دراسة البيانات العشوائية، تبرز مجموعة من المفاهيم والمصطلحات المحورية التي تعد أداة رياضية قوية لتحليل بنية الشبكات المعقدة وفهم سلوكها تحت ظروف متعددة، لا سيما في سياق شبكات الاستشعار اللاسلكية، حيث تلعب العشوائية دوراً جوهرياً في تشكيل الروابط بين العقد نظراً للطبيعة المتغيرة للاتصال اللاسلكي واحتمالية الفشل أو الاخفاق في الوصلات. تمثل هذه المصطلحات بنية أساسية في النمذجة والتحليل النظري، وفيما يلي توضيح مفصل لأهم هذه المصطلحات:

1-9-1. المكون العملاق (Giant Component)

المكون العملاق مصطلح يستخدم لوصف أكبر مجموعة عقد في البيان بحيث يمكن الانتقال بين أي زوج من العقد داخل هذا المكون عبر سلسلة من الروابط. في الشبكات العشوائية لا يظهر هذا المكون إلا بعد تجاوز عدد معين من الروابط. يمكن استخدام المكون العملاق في دراسة الأخطاء في الشبكة من خلال تحديد

العقد الحساسة والروابط الحرجة التي إذا حذفت فإنها تؤدي إلى انهيار المكون العملاق [7]. يتم تحديد المكون العملاق من خلال الطرق الاتية:

1. استخدام خوارزميات البحث في العمق (DES) أو في العرض (BFS) لتحديد المجموعة الأكبر من العقد التي تتصل ببعضها البعض ويتم تحديد المجموعة الأكبر كمكون عملاق.
2. استخدام خوارزميات العنقدة: يمكن استخدام خوارزميات العنقدة (clustering algorithm) لتجزئة البيان إلى مجموعات صغيرة من العقد المتصلة ويتم تحديد المجموعة الأكبر كمكون عملاق.
3. البحث عن المجموعات الكبيرة والمؤثرة في البيان باستخدام خوارزميات الكشف عن المجتمعات (gommunities algorithms) ويمكن تحديد المجموعة الأكبر كمكون عملاق (giant component).

تختلف الطرق المستخدمة لتحديد المكون العملاق باختلاف الحالة والغرض من الدراسة، يمكن استخدام أكثر من طريقة لتحديد المكون العملاق في البيان.

ملاحظة (1-3)

من الممكن أن لا يحتوي البيان العشوائي على المكون العملاق.

مثال (1-2)

في شبكة استشعار موزعة عشوائياً عبر منطقة بيئية لمراقبة الحرارة، قد لا تكون جميع العقد متصلة ببعضها في البداية. لكن مع زيادة كثافة العقد أو زيادة مدى الإرسال، يظهر مكون عملاق يربط غالبية العقد، مما يضمن قدرة الشبكة على توصيل البيانات (data) إلى العقد المركزية أو إلى وحدة التحكم. غياب هذا المكون يعني أن الشبكة مجزأة وفاقدة للفعالية.

1-9-2. معامل تجميع العقد (Clustering Coefficient)

معامل تجميع العقد هو متوسط احتمال أن يكون مجاورات عقدة معينة مجاورين لبعضهم البعض. بمعنى آخر هو النسبة بين عدد الروابط الموجودة بين جميع الأزواج من العقد المتصلة مع عقدة محددة وعدد الأضلاع الأقصى بين هذه العقد.

من المحتمل أن يكون معامل تجميع العقد منخفضاً بشكل كبير حيث يتم اختيار الأضلاع عشوائياً دون أي ترتيب أو تفضيل للعقد المتصلة بعضها ببعض. بالتالي يعد معامل التجميع مهماً لتقييم مدى تجمع العقد في الشبكة وكيفية تأثير ذلك على سلوك النظام وانتشار الأخطاء وغيرها في الشبكة [8].

مثال (1-3)

في شبكات الاستشعار اللاسلكية، قد تكون بعض العقد متقاربة جغرافياً وتشكل "عنقوداً محلياً"، وهذا ينتج معامل تجميع مرتفع. مثل هذا التجمع يمكن أن يعزز من تسامح الشبكة مع الأعطال، إذ أن فشل عقدة واحدة لا يقطع الاتصال بين باقي الجيران.

1-9-3. انتقال الطور(Phase Transition)

قدم Erdos-Renyi في [9] مصطلح انتقال الطور لوصف تغيير كبير في خاصة معينة للبيان العشوائي عند تجاوز حد معين في أحد المعاملات (مثل عدد الأضلاع أو درجة العقد). في سياق البيانات العشوائية، يعد أهم انتقال هو ظهور المكون العملاق عند تجاوز حد توصيل معين.

مثال (1-4)

عند نشر عدد معين من عقد الاستشعار، قد تكون الشبكة مجزأة إلى مجموعات صغيرة. لكن بمجرد تجاوز عدد الروابط المتوقعة لكل عقدة إلى حد معين (مثلاً المتوسط 1.5 رابط لكل عقدة)، يحدث انتقال مفاجئ في بنية الشبكة، وتظهر فجأة شبكة مترابطة تشمل معظم العقد، وهي لحظة حرجة لضمان التوصيل الكامل.

1-9-4. توزيع الدرجة (Degree Distribution)

هو عدد الاتصالات (الروابط) التي تملكها كل عقدة في البيان. يستخدم مصطلح توزيع الدرجة لفهم هيكل الشبكة والعلاقات بين العقد بالإضافة إلى معرفة مقدار الترابط بين العقد في الشبكة والعثور على العقد الأكثر تأثيراً (المركزية) فيها. هذا ما يساعد على فهم سلوك الشبكة وتحليلها.

مثال (1-5)

في بعض شبكات الاستشعار اللاسلكية ترتبط العقد حسب قربها المكاني، بالتالي توزيع الدرجة قد يكون متقارباً. لكن في حال وجود عقد ذات قدرات إرسال أعلى (مثل العقد المركزية)، فقد تملك هذه العقد عدداً كبيراً من الروابط، مما يخلق توزيع غير متماثل. هذا التفاوت يجعل بعض العقد أكثر حساسية للأعطال.

1-9-5. متوسط طول المسار (Average Path Length)

يمثل متوسط عدد الروابط بين أي كل زوج من العقد في البيان. تأتي أهمية مصطلح متوسط طول المسار في حال نمذجة الشبكات باستخدام البيان العشوائي فأنه كلما كان هذا الطول أقصر، كانت الشبكة أكثر كفاءة في نقل البيانات (data).

1-9-6. نقطة العتبة (Threshold Point)

تمثل الحد الأدنى من الروابط أو العقد اللازمة لظهور خصائص هيكلية معينة في البيان، مثل الاتصال الكامل أو ظهور المكون العملاق.

1-9-7. الديناميكية في البيان العشوائي (Dynamics In Random Graph)

تعد ديناميكية البيان العشوائي من الخصائص الأساسية التي تميز هذا النموذج عن غيره من النماذج التقليدية، وهي خاصية تعكس قدرة البنية البيانية على التغير والتطور مع مرور الزمن أو تحت تأثيرات خارجية، سواء كانت مقصودة كإضافة عقد جديدة أو فقدان بعض العقد أو الأضلاع نتيجة أعطال أو تدخلات بيئية.

إن النماذج العشوائية للبيانات، مثل نموذج G(n,p)، توفر إطاراً رياضياً لدراسة هذه الديناميكية من خلال ربط احتمالية وجود الأضلاع بين العقد بمحددات مثل عدد العقد أو التوزيع الاحتمالي للاتصال. غير أن هذه النماذج، في صورتها الساكنة، لا تكفي لفهم الطبيعة الزمنية المعقدة لتغيرات الشبكة. ولهذا ظهرت الحاجة إلى تطوير نماذج بيانات عشوائية ديناميكية، والتي تعنى بدراسة تطور البنية البيانية عبر الزمن، وذلك إما من خلال تتابع زمني للبيانات (Dynamic Graph Sequences) أو عبر نماذج احتمالية تأخذ بعين الاعتبار زمن ظهور أو اختفاء الأضلاع والعقد [10].

تتولد نماذج البيانات العشوائية بدءاً من بعض الشروط الابتدائية على الوقت t=0 ، تظهر الأضلاع وتختفي في سلسلة من الأوقات الحقيقية، مثالاً على ذلك شبكة المكالمات الهاتفية التي يتم إعطاء وقت ومدة كل مكالمة تتم مراقبة الشبكة في مجموعة من الأوقات المتباعدة t=1,….,T. في هذا السياق، تلعب ديناميكية البيان العشوائي دوراً محورياً في تحليل استقرار الشبكة ومدى قدرتها على التحمل في مواجهة الأعطال. إذ إن التحليل الزمني لتغيرات البنية البيانية يمكن من تتبع تطور مكونات الشبكة أو فقدان التوصيل بين أجزائها. كما تسمح هذه النماذج بدراسة قدرة الشبكة على إعادة التشكيل الذاتي (Self-Reconfiguration) بعد حدوث الأعطال [10].

يعد نموذج البيان العشوائي الديناميكي (Dynamic Random Graph Model) امتداداً طبيعياً للنماذج العشوائية الساكنة، مثل نموذج Erdos-Renyi، وقد ظهر كاستجابة للحاجة المتزايدة لنمذجة الأنظمة الشبكية المعقدة التي تتغير بنيتها الطوبولوجية بمرور الوقت. ففي العديد من التطبيقات الواقعية، وعلى رأسها شبكات الاستشعار اللاسلكية، لا تظل الشبكة ثابتة في بنيتها، بل تتعرض لتغيرات مستمرة نتيجة لانضمام عقد جديدة، أو تعطل عقد قائمة، أو تغير جودة الروابط بسبب العوامل البيئية. وبالتالي، فإن النماذج الساكنة، التي تفترض فيها البنية البيانية مستقرة، تصبح غير كافية لتحليل مثل هذه الشبكات بصورة دقيقة. وهنا يبرز دور نموذج البيان العشوائي الديناميكي كإطار نظري أكثر ملاءمة لدراسة تطور الشبكة زمنياً، وتحليل قدرتها على التحمل والتكيف مع الأعطال [10].

1-9-8. أهمية البيانات العشوائية

تعتبر البيانات العشوائية (Random Graphs) من الأدوات الرياضية المحورية في نمذجة الأنظمة الشبكية المعقدة، وذلك لما توفره من قدرة كبيرة على تمثيل الأنماط المتغيرة التي تميز العديد من الشبكات الواقعية، مثل شبكات الاستشعار اللاسلكية، والشبكات الاجتماعية، وشبكات الحوسبة الموزعة وغيرها. وتكمن أهمية البيانات العشوائية في قدرتها على تجاوز القصور الذي تعاني منه النماذج التقليدية (Deterministic Models)، وذلك من خلال تبني مقاربة احتمالية تسمح بمحاكاة حالات متعددة ومتنوعة من التوصيل بين العقد، تعكس الواقع العشوائي لطبيعة الشبكة.

واحدة من أبرز مزايا البيانات العشوائية أنها تتيح تحليل الخصائص الطوبولوجية العامة للشبكة دون الحاجة إلى تحديد البنية الدقيقة لها. على سبيل المثال، يمكن باستخدام نموذج عشوائي بسيط مثل نموذج Erdos–Renyi دراسة احتمالية أن تكون الشبكة متصلة، أو تحديد النقطة التي يحدث فيها انتقال مفاجئ من شبكة غير متصلة إلى شبكة ذات مكون متصل ضخم، وهو ما يعرف بظاهرة العتبة الحرجة (Phase Transition). كما أن استخدام البيانات العشوائية يوفر إطاراً موحداً لتحليل سلوك الشبكة عند تغير عدد العقد أو كثافة الأضلاع، وهو ما يساعد الباحث على استنتاج قواعد عامة يمكن تطبيقها على أنواع متعددة من الشبكات.

علاوة على ذلك، تلعب البيانات العشوائية دوراً جوهرياً في تحليل مدى مرونة الشبكة (Network Robustness)، حيث تستخدم لمحاكاة سيناريوهات فقدان العقد أو الأضلاع بشكل عشوائي، مما يسمح بتقييم مدى قدرة الشبكة على البقاء متصلة أو فعالة رغم الأعطال. وتعد هذه القدرة ذات أهمية قصوى في شبكات الاستشعار اللاسلكية، التي تعمل في بيئات غير مستقرة ومعرضة لمخاطر متعددة كفقد الطاقة أو تلف العقد. وبالتالي باستخدام البيانات العشوائية، يمكن بناء نموذج يتوقع مدى تأثير هذه الأعطال على خصائص مثل التغطية، وزمن الاستجابة مما يسهم في تحسين تصميم الشبكة.

يستخدم البيان العشوائي في مجالات مختلفة منها الطبية لوصف المسارات المحتملة لانتشار الأمراض المعدية. حيث يتم استخدام نماذج البيانات لتحليل وتوضيح سير انتشار الامراض المعدية وعلاقات الاتصال بين الافراد والاماكن التي يزوروها. يتم ربط العقد بخطوط تمثل مسارات انتقال العدوى بين الافراد.

عادة يكون من الصعب تحديد البيان بالتفصيل لأن سير انتشار الأمراض المعدية يختلف باستمرار ويمكن أن يتغير بسرعة، لذلك يتم استخدام نموذج البيان العشوائي لتمثيل الانتشار المحتمل للعدوى بشكل عام والتركيز على الخصائص المهمة مثل الكثافة. بالتالي استخدام نماذج البيان العشوائي يمكن أن يساعد في التوضيح.

1-10- خلاصة الفصل

تناولنا في هذا الفصل مجموعةً من المفاهيم الأساسية في نظرية البيان، مع التركيز على التمثيلات المصفوفية وأبرزها مصفوفة التجاور. كما تم استعراض أنواع البيانات الرئيسية وتطبيقاتها العملية في حل المشاكل الواقعية. إلى جانب ذلك، تطرق الفصل إلى نظرية البيان العشوائي، حيث تم عرض أهم النماذج والمصطلحات ذات الصلة، مع تسليط الضوء على دور البيانات العشوائية وأهميتها في مجالات متنوعة.

2 مفاهيم أساسية في التشفير

2-1-مقدمة

يُعد علم التشفير (Cryptography) أحد أهم أعمدة أمن المعلومات في العصر الرقمي، إذ يوفّر الوسائل الرياضية والتقنية لحماية سرية البيانات (data) وضمان سلامتها والتحقق من هوية الأطراف المتراسلة. مع تزايد الاعتماد على الشبكات والأنظمة الموزعة، أصبح التشفير ضرورة لا غنى عنها في حماية الاتصالات والمعاملات الإلكترونية، سواء كانت مالية أو إدارية أو حتى اجتماعية. التشفير لا يقتصر على إخفاء المعلومات، بل يتجاوز ذلك ليشمل ضمان عدم العبث بها، والتأكد من مصدرها، ومنع إنكار المرسل لرسالته، وهو ما يُعرف بمبدأ عدم التنصّل (Non-repudiation) [11].

تطور التشفير عبر التاريخ من أساليب بدائية بسيطة مثل شيفرة القيصر التي تعتمد على إزاحة الحروف بعدد ثابت، إلى أنظمة أكثر تعقيدًا مثل شيفرة فيجنير (Vigenère cipher) وشيفرة هيل (Hill cipher) التي أدخلت مفاهيم الجبر الخطي والمصفوفات. مع تطور الرياضيات ونظرية الأعداد، ظهر التشفير الحديث الذي يعتمد على أسس رياضية قوية. هذه التطورات جعلت من التشفير علماً قائماً بذاته، يجمع بين النظرية والتطبيق، ويستفيد من فروع الرياضيات مثل الجبر، الاحتمالات، ونظرية المعلومات [12].

في هذا الفصل، نعرض المفاهيم الأساسية مثل النص الصريح والنص المشفر والمفتاح، وخوارزميات التشفير وفك التشفير، ونناقش تطبيقاته العملية في أمن الشبكات، مع تقديم أمثلة توضح كيفية عمل هذه الخوارزميات.

2-2-تعاريف أساسية في علم التشفير

يُبنى علم التشفير على مجموعة من المفاهيم الجوهرية التي تُشكّل الأساس لفهم كيفية عمل الأنظمة والخوارزميات المستخدمة في حماية البيانات (data).

2-2-1. النص الصريح (Plaintext)

النص الصريح هو البيانات الأصلية التي يرغب المرسل في إيصالها إلى المستقبل دون أي تعديل أو إخفاء. يكون النص الصريح أما رسالة نصية أو ملفاً رقمياً، أو حتى بيانات حساسة مثل كلمات المرور [12].

مثال (2-1)

إذا كانت الرسالة هي HELLO فإنها تمثل النص الصريح قبل تطبيق أي عملية تشفير. تكمن أهمية النص الصريح في أنه يمثل المعلومة المراد حمايتها، وبالتالي فإن أي ضعف في عملية التشفير قد يؤدي إلى كشفه بسهولة.

2-2-2. النص المشفر (Cipher text)

النص المشفر هو الناتج عن تطبيق خوارزمية التشفير باستخدام مفتاح محدد على النص الصريح. يتميز النص المشفر بأنه غير مفهوم للإنسان أو للأنظمة غير المصرح لها، ويبدو عشوائيًا من حيث التوزيع الإحصائي للأحرف أو البتات.

مثال(2-2)

إذا تم تشفير HELLO باستخدام خوارزمية تشفير ما، فإن النص المشفر هو الذي يُرسل عبر القنوات غير الآمنة مثل الإنترنت، ويُفترض أن يكون من المستحيل استرجاع النص الصريح منه دون معرفة المفتاح.

2-2-3. المفتاح (Key)

المفتاح هو العنصر السري الذي يُستخدم للتحكم في عملية التشفير وفك التشفير. يُعتبر المفتاح أهم جزء في النظام، إذ أن قوة التشفير لا تعتمد فقط على الخوارزمية، بل على سرية المفتاح وطوله. تكمن أهمية المفتاح في أنه الحاجز الوحيد بين النص المشفر والنص الصريح [11].

2-2-4. خوارزمية التشفير (Encryption Algorithm)

خوارزمية التشفير هي مجموعة من العمليات الرياضية والمنطقية التي تُحوّل النص الصريح إلى نص مشفر باستخدام المفتاح. حتى تكون الخوارزمية جيدة يجب أن تحقق ما يأتي:

- **الفعّالية الحسابية:** أي يمكن تنفيذها بسرعة مقبولة.
- **آمنة رياضياً:** أي أن كسرها يتطلب وقتًا أو موارد غير عملية [13].

2-2-5. خوارزمية فك التشفير (Decryption Algorithm)

خوارزمية فك التشفير هي العملية العكسية للتشفير، تُحوّل النص المشفر إلى النص الصريح باستخدام المفتاح المناسب [12]. في التشفير المتماثل تستخدم الخوارزمية نفسه المفتاح ولكن بترتيب عكسي. في التشفير غير المتماثل تستخدم الخوارزمية المفتاح الخاص لفك التشفير بينما يُستخدم المفتاح العام للتشفير.

ملاحظة(2-1)

تشكل هذه التعاريف الخمسة الأساس الذي يُبنى عليه علم التشفير. فالنص الصريح هو المعلومة المراد حمايتها، والنص المشفر هو الصورة غير المفهومة منها، والمفتاح هو العنصر السري الذي يربط بينهما، بينما تقوم خوارزميات التشفير وفك التشفير بتنفيذ العمليات الرياضية اللازمة لتحقيق الأمان. إن فهم هذه المفاهيم يُعتبر الخطوة الأولى نحو استيعاب الخوارزميات الأكثر تعقيدًا وتطبيقاتها في أمن الشبكات.

2-3-الخوارزميات التقليدية في علم التشفير

يُعتبر التشفير التقليدي الأساس الذي بُني عليه علم التشفير الحديث. رغم بساطته مقارنة بالخوارزميات المعاصرة، فإنه قدّم مفاهيم مهمة مثل الاستبدال (Substitution) والانتقال (Transposition)، التي لا تزال تُستخدم في تصميم الأنظمة الحديثة [11].

2-3-4. شيفرة القيصر (Caesar Cipher)

تعتمد شيفرة القيصر على إزاحة كل حرف في النص الصريح بعدد ثابت من المواقع في الأبجدية. لكن ما يعيب هذه الخوارزمية أنه يمكن كسرها بسهولة باستخدام تحليل التكرار أو تجربة جميع المفاتيح الممكنة إذ أن عدد المفاتيح لا يتجاوز 25 مفتاح.

مثال (2-3)

إذا كان النص الصريح HELLO والمفتاح (k = 3)، فإن النص المشفر يكون KHOOR.

2-3-5. شيفرة فيجنير (Vigenère Cipher)

تُعتبر تطويرًا لشيفرة القيصر، حيث يُستخدم مفتاح متعدد الحروف بدلاً من مفتاح واحد ثابت. تعد الشيفرة أكثر قوة من شيفرة القيصر، لكنها لا تزال قابلة للكسر باستخدام تحليل التكرار (Frequency Analysis) يمكن التعبير عنها كما يلي $C_i = (P_i + K_i)$ حيث (P_i) هو الحرف في الموقع i، K_i هو الحرف المقابل في المفتاح.

مثال(2-4)

إذا كان النص الصريح "HELLO" والمفتاح "KEY"، فإن التشفير يتم بإزاحة كل حرف وفقًا للقيمة العددية للحرف في المفتاح فيكون النص المشفر RIJVS.

2-3-6. شيفرة هيل (Hill Cipher)

تعتمد الخوارزمية على الجبر الخطي، حيث يُستخدم مفتاح على شكل مصفوفة قابلة للعكس. الصيغة الرياضية $C = P.K \pmod m$ حيث P هو متجهة النص الصريح، K مصفوفة المفتاح، m حجم الأبجدية. تعد شيفرة هيل أكثر قوة من الشيفرات السابقة لأنها تحقق خاصية الانتشار (Diffusion)، حيث يعتمد كل حرف مشفر على جميع أحرف النص الصريح في الكتلة. ومع ذلك، يمكن كسرها إذا لم يكن حجم المفتاح كبيرًا بما يكفي أو إذا تم الحصول على عدد كافٍ من أزواج النصوص الصريحة والمشفرة [11].

مثال(2−5)

إذا كان النص الصريح MOM ويُمثل بالأعداد (12, 14, 12), والمفتاح هو :

$$k = \begin{bmatrix} 3 & 4 & 7 \\ 2 & 11 & 8 \\ 5 & 12 & 9 \end{bmatrix}$$

فإن النص المشفر الناتج يكون (20, 12, 16) والذي يُترجم إلى SOU.

ملاحظة (2−2)

تمثل شيفرات القيصر وفيجنير، وهيل الخوارزميات الاولى لعلم التشفير. ورغم أن هذه الخوارزميات لم تعد تُستخدم في التطبيقات العملية الحديثة بسبب ضعفها أمام الهجمات، فإنها تُعتبر أدوات تعليمية مهمة لفهم المبادئ الأساسية التي يقوم عليها التشفير الحديث، مثل الاستبدال والانتشار والتحكم بالمفتاح يوضح الجدول (2−1) مقارنة بين الشيفرات الكلاسيكية المشروحة سابقاً.

الخوارزمية	نوع المفتاح	القوة	سهولة الكسر
قيصر	مفتاح واحد	ضعيفة	عالية
فيجنير	مفتاح متعدد	متوسطة	متوسطة
هيل	مصفوفة	قوية نسبياً	أصعب

الجدول (2-1) مقارنة بين الشيفرات الكلاسيكية

بعد أن استعرضنا الخوارزميات الكلاسيكية، سننتقل الآن إلى التشفير الحديث وأهميته في أمن الشبكات.

2−4−التشفير الحديث وأمن الشبكات

يمثل التشفير الحديث الركيزة الأساسية لأمن الشبكات والاتصالات الرقمية. يعتمد على خوارزميات قوية أثبتت فعاليتها في مواجهة الهجمات الرياضية والعملية. كما يمثل الأساس العملي لأمن الشبكات، حيث يُستخدم التشفير المتماثل AES لتأمين البيانات بسرعة وكفاءة، بينما يُستخدم التشفير غير المتماثل لتبادل المفاتيح والتواقيع الرقمية [13].

2-4-1- أنواع التشفير

ينقسم التشفير إلى نوعين:

1. **التشفير المتماثل (AES)**

يعتمد التشفير المتماثل على استخدام مفتاح واحد للتشفير وفك التشفير. ومن أبرز خوارزمياته الحديثة خوارزمية (Advanced Encryption Standard)، التي أصبحت معيارًا عالميًا منذ اعتمادها من قبل المعهد الوطني للمعايير والتكنولوجيا [13].

آلية عمل الخوارزمية

تعتمد AES على عمليات الاستبدال (Substitution) والخلط (Permutation) داخل مصفوفات ثنائية. تستخدم AES لتأمين الاتصالات عبر الإنترنت، حيث توفر سرية عالية وسرعة في التنفيذ مقارنة بالخوارزميات غير المتماثلة.

- تعمل على كتل بيانات بحجم 128 بت، مع مفاتيح بطول 128، 192، أو 256 بت.
- تتكون من عدة مراحل، حيث تشمل كل مرحلة العمليات التالية :
  - استبدال كل بايت وفق جدول ثابت(S-box).
  - تدوير الصفوف داخل المصفوفة.
  - خلط الأعمدة باستخدام عمليات جبرية.
  - دمج المفتاح مع الكتلة باستخدام عملية XOR.

2. التشفير غير المتماثل

يعتمد التشفير غير المتماثل على استخدام مفتاح للتشفير و مفتاح لفك التشفير. أهم الخوارزميات في التشفير غير المتماثل هي:

- **خوارزمية RSA**

تعمل الخوارزمية وفق الخطوات التالية:

- اختيار عددين أوليين كبيرين (p, q).
- حساب n = p x q و((p−1)x(q−1)) =T(n).
- اختيار عدد (e) بحيث (1 = gcd(e,T(n)).
- حساب المعكوس (d) بحيث(e x d = 1 modT(n)).
- المفتاح العام (e, n)، المفتاح الخاص (d, n).

▪خوارزمية ECC

تعتمد على خواص المنحنيات الإهليجية فوق الحقول المنتهية Z_p. توفر نفس مستوى الأمان الذي يقدمه RSA ولكن بمفاتيح أقصر بكثير. على سبيل المثال، مفتاح ECC بطول 256 بت يعادل في القوة مفتاح RSA بطول 3072 بت، يوضح الجدول (2−2) مقارنة بين بعض خوارزميات التشفير.

الخاصية	AES (متماثل)	RSA (غير متماثل)	ECC (غير متماثل)
نوع المفتاح	مفتاح واحد	مفتاح عام/خاص	مفتاح عام/خاص
طول المفتاح	128−256 بت	1024−4096 بت	160−512 بت
سرعة التنفيذ	عالية	أبطأ	أسرع من RSA
الاستخدام	تشفير البيانات	تبادل المفاتيح والتوقيع	تبادل المفاتيح والتوقيع
الأمان	قوي جداً	قوي لكن يتطلب مفاتيح طويلة	قوي بمفاتيح قصيرة

الجدول (2-2) مقارنة بين خوارزميات التشفير

2−5−دوال التقطيع (Hash Functions)

تُعد دوال التقطيع من أهم الأدوات المستخدمة في علم التشفير وأمن الشبكات، إذ توفر وسيلة فعّالة للتحقق من سلامة البيانات وضمان عدم العبث بها أثناء النقل أو التخزين. تُستخدم أيضًا في إدارة كلمات المرور والتواقيع الرقمية، تعمل على تحويل البيانات ذات الطول المتغير إلى قيمة ثابتة الطول تُعرف باسم البصمة الرقمية [11].

2-5-1- تعريف دوال التقطيع

دالة التقطيع هي خوارزمية رياضية تأخذ مدخلًا رسالة أو بيانات وتُنتج مخرجات ثابتة الطول. تتميز الدالة بالخصائص التالية:

1. سهولة الحساب أي يمكن حساب قيمة التقطيع بسرعة.
2. صعوبة الانعكاس أي لا يمكن استرجاع النص الأصلي من التجزئة.
3. مقاومة التصادم (Collision Resistance) تقيس قدرة الخصم على إيجاد تصادم (مدخلين مختلفين لهما نفس المخرجات) لعنصر من عائلة دوال التقطيع.
4. حساسية المدخلات أي تغيير بسيط في النص الأصلي يؤدي إلى تغيير كبير في قيمة التقطيع [12].

تُعتبر دوال التقطيع مثل SHA-2 و SHA-3 حجر الأساس في أمن الشبكات، حيث تُستخدم في التحقق من سلامة البيانات وإدارة كلمات المرور، والتواقيع الرقمية. رغم أن SHA-2 لا يزال يُستخدم على نطاق واسع، فإن SHA-3 يوفر مرونة وأماناً إضافياً لمواجهة التهديدات المستقبلية [13]. ويوضح الجدول (2-3) مقارنة بين الدالتين SHA-2 و SHA-3.

الخاصية	SHA-2	SHA-3
سنة الاعتماد	2001	2015
البنية الداخلية	عمليات منطقية على كتل	دالة الإسفنج (Keccak)
طول المخرجات	224-512بت	متغير (حسب الحاجة)
مقاومة الهجمات	قوية جدًا	أقوى ضد بعض الهجمات
الاستخدامات	كلمات المرور، التواقيع	نفس الاستخدامات مع مرونة أكبر

الجدول (2-3) مقارنة بين دوال التقطيع

2-6-التوقيع الرقمي (Digital Signature)

التوقيع الرقمي هو قيمة مشفرة تُضاف إلى الرسالة باستخدام مفتاح خاص، بحيث يمكن لأي طرف يمتلك المفتاح العام للمرسل أن يتحقق من صحة الرسالة والتأكد من أنها لم تُعدّل أثناء النقل [12] يحقق التوقيع الرقمي ثلاث خصائص أساسية :

1. المصادقة (Authentication): أي التأكد من هوية المرسل.
2. سلامة البيانات (Integrity): هي ضمان عدم تغيير محتوى الرسالة.
3. عدم التنصّل (Non-repudiation): منع المرسل من إنكار إرساله الرسالة.

2-7-المصافحة (TLS Handshake)

هي سلسلة من الرسائل المتبادلة بين العميل (Client) والخادم (Server) تهدف إلى الاتفاق على خوارزمية التشفير وإنشاء مفتاح الجلسة. يمكن تلخيص خطواتها كما يلي:

1. **العميل والخادم**

- يرسل العميل رسالة تحتوي على قائمة بالخوارزميات التي يدعمها.
- يرسل أيضًا رقمًا عشوائيًا يُستخدم لاحقًا في توليد المفتاح.
- يرد الخادم باختيار خوارزمية التشفير المناسبة.
- يرسل رقمًا عشوائيًا آخر.
- يرسل شهادة رقمية تحتوي على مفتاحه العام للتحقق من هويته.

2. **تبادل المفاتيح**

- يتم تبادل المعلومات اللازمة لتوليد مفتاح الجلسة باستخدام خوارزميات مثل RSA أوECC.
- الهدف هو أن يتمكن الطرفان من حساب المفتاح نفسه دون أن يعرفه أي طرف ثالث.

3. **إنشاء قناة آمنة**

- بعد الاتفاق على المفتاح، يبدأ الطرفان باستخدامه لتشفير البيانات باستخدام خوارزميات متماثلة مثلAES.
- من هذه اللحظة، تصبح القناة مشفرة وآمنة.

بالرغم من المستويات العالية للأمان التي يوفرها التشفير الحديث اليوم، إلا أن وتيرة التطور التقني المتسارعة تدفع الباحثين إلى استكشاف أساليب جديدة، مثل تطبيق نظرية البيان في تطوير أنظمة التشفير المستقبلية.

2-8-التشفير باستخدام نظرية البيان

تبرز نظرية البيان كأداة رياضية غنية بالقواعد والمفاهيم التي يمكن تسخيرها لتعزيز أنظمة التشفير، خاصة في مواجهة التهديدات الإلكترونية المتزايدة. نوضح فيما يلي بعض خوارزميات التشفير باستخدام نظريات البيان [18].

2-8-1. خوارزمية التشفير بالاعتماد على تلوين البيان

تقدم هذه الخوارزمية تصوراً لآلية تشفير تعتمد على تحويل البيانات (data) إلى بيان وتطبيق عملية تلوين العقد عليها، مما يضيف طبقات من التعقيد الحسابي الذي يصعب اختراقه. يعتمد هذا النهج على فكرة أن مشكلة تلوين البيان بمجرد تجاوز لونين تُصنّف ضمن المسائل (NP-Complete)، أي أنه لا يوجد حاليًا خوارزمية ذات كفاءة زمنية حدودية (Polynomial Time) قادرة على حلها بشكل عام، مما يجعلها بيئة خصبة لتطبيقات التشفير.

تعتمد الطريقة المقترحة على تحويل النص الأصلي إلى بيان. بفرض أن النص الأصلي هو سلسلة رقمية مثل 1638940. يُحوّل هذا النص إلى بيان غير موجه، يمثل كل رقم عقدة، وتمثل الاضلاع العلاقة الترتيبية أو التجاور بين الأرقام في التسلسل. بعد بناء البيان، تُطبق عليه خوارزمية تلوين العقد، التي تهدف إلى تعيين ألوان للعقد بحيث لا تتشارك عقدتان متجاوران اللون نفسه. يُستخدم العدد الكروماتي (Chromatic Number) لأقل عدد ممكن من الألوان التي تحقق هذا الشرط.

يُشتق النص المشفر مباشرة من القيم الموجودة على القطر الرئيسي للمصفوفة المجاورة، والتي تمثل ألوان الرؤوس. أما المفتاح السري فيتم استخلاصه من بقية عناصر المصفوفة، عادةً من العناصر الواقعة تحت القطر الرئيسي أو فوقه. يُسجل المفتاح كسلسلة ثنائية أو رقمية طويلة. يتم إرسال النص المشفر علانية، بينما يُحفظ المفتاح سريًا بين الطرفين المتواصلين [18].

2-8-1-1. مقارنة مع أنظمة التشفير التقليدية

تختلف هذه الخوارزمية عن أنظمة التشفير التقليدية مثل RSA في نقطة جوهرية، فهي لا تعتمد فقط على التعقيد العددي أو العمليات الجبرية، بل على التعقيد الهيكلي للبيانات نفسها. بينما تعتمد أنظمة المفتاح العمومي على صعوبة تحليل الأعداد الكبيرة أو حل لوغاريتمات منفصلة، فإن هذا النهج يستغل صعوبة مشكلات التحسين التوافقية (Combinatorial Optimization). يمكن أيضًا دمج هذه الطريقة مع أنظمة موجودة لإنشاء هجين يزيد من صعوبة الهجوم.

2-8-2. خوارزمية التشفير بالاعتماد على بيان أويلر

تعتمد خوارزمية التشفير بشكل أساسي على مفهومين أساسيين من نظرية البيان، هما البيان الأويلري والدائرة الهاملتونية [33]. تقوم فكرة التشفير على تحويل كل حرف من النص الأصلي إلى تمثيل بياني أويلري، حيث تُستخدم الدائرة الهاملتونية المستخرجة من هذا البيان بمثابة المفتاح السري اللازم لفك التشفير. بهذا الأسلوب، يتم تمثيل الرسالة السرية ليس كنص أو أرقام تقليدية، بل كسلسلة من المصفوفات المجاورة التي تصف بنى بيانية معقدة. تبدأ عملية التشفير بمعالجة كل حرف على حدة وفق التسلسل التالي:

1. تحويل الحرف إلى قيمته في نظام ASCII.
2. تحويل القيمة إلى الصيغة الثنائية
3. إجراء عملية XOR بين القيمة الثنائية للحرف والتمثيل الثنائي للعدد 32.
4. يُستخدم عدد الواحدات في الناتج لتحديد عدد رؤوس البيان، ويُستخدم تسلسل الأصفار والواحدات لملء المصفوفة المجاورة المتناظرة التي تمثل ذلك البيان. يتم إرسال هذه المصفوفة التي تمثل الحرف المشفر إلى المستقبل.

2-8-3. خوارزمية تعتمد على مصفوفات التجاور

تعتمد هذه الخوارزمية منهجية تشفير تستخدم جدولين للتشفير. يتم تحويل النص الأصلي إلى نص مشفر باستخدام جدول تشفير عشوائي محدد مسبقاً ومشترك بين المستقبل والمرسل. بعد ذلك يتم تحويل النص المشفر إلى بيان باستخدام جدول تشفير أبجدي. نوضح فيما يلي خطوات الخوارزمية:

1. استبدال الأحرف: تحويل النص الأصلي إلى نص مشفر باستخدام جدول استبدال أحرف عشوائي متفق عليه بين الطرفين.

2. تمثيل النص كرسم بياني: كل حرف يمثل عقدة ويتم الربط بين بين كل عقدتين متتاليتين بضلع لتشكيل البيان.

3. تعين الأوزان: يتم إعطاء كل ضلع وزناً وفقاً لجدول تشفير أبجدي (مثل A=1, B=2).

4. ربط كل عقدة بجميع العقد الأخرى. تعطى الأضلاع الجديدة وزناً يساوي الوزن الأقصى في جدول التشفير+1
5. إنشاء مصفوفة التجاور K_1.
6. تطبيق خوارزمية كروسكال والحصول على مصفوفة التجاور K_2.
7. ضرب المصفوفات $K_1 \times K_2 = K_3$ وللحصول على النص المشفر نضرب K_3 بالمفتاح.

2-9-خلاصة الفصل

استعرضنا في هذا الفصل المفاهيم الأساسية لعلم التشفير، وتطرقنا إلى خوارزميات التشفير بدءاً من الخوارزميات الكلاسيكية وصولاً إلى تقنيات التشفير الحديث وأسس أمن الشبكات. كما تناولنا مجال التشفير باستخدام البيان، حيث تم عرض خوارزميتين رئيستين: الأولى تعتمد على تلوين البيان، والثانية تستند إلى مفاهيم بيان أويلر و دائرة هاملتون.

3 مفاهيم أساسية في شبكات الاستشعار اللاسلكية

3-1- مقدمة

تشكل شبكات الاستشعار اللاسلكية (WSNs) تقنية مبتكرة وحجر أساس في دعم مجموعة واسعة من التطبيقات الحيوية، بدءاً من مراقبة الظروف البيئية والتطبيقات العسكرية والأمنية، وصولاً إلى المتابعة الصحية عن بُعد، والممارسات الزراعية الحديثة، وتطوير البنى التحتية للمدن الذكية. قد أسهمت التقدمات الحديثة في مجالي النظم الكهرو ميكانيكية الدقيقة (MEMS) وتقنيات الاتصال اللاسلكي في إنتاج مستشعرات ذات كفاءة عالية، تتميز بانخفاض تكلفتها واستهلاكها للطاقة، وصغر حجمها، وقدراتها على المعالجة المتطورة. يتم نشر هذه العقد الاستشعارية عبر مساحات شاسعة لترتبط لاسلكياً، مهمتها تجميع المعلومات والبيانات من البيئة المحيطة ونقلها إما إلى محطة مركزية أو بين العقد نفسها، ليتم فيما بعد معالجة هذه البيانات وتحليلها للخروج برؤى وقرارات تستند إلى البيانات المجمعة. وبذلك، تمثل هذه الشبكات جسرًا يربط بين العالم المادي الملموس وعالم إنترنت الأشياء والحوسبة الرقمية. سندرس في هذا الفصل المفاهيم الأساسية لشبكات الاستشعار اللاسلكية ومكوناتها وتطبيقاتها ومحدوديتها.

3-2- تعريف شبكات الاستشعار اللاسلكية

تتألف شبكات الاستشعار اللاسلكية من مجموعة من الأجهزة الصغيرة المزودة بقدرات معالجة محدودة. تتمثل وظيفتها الأساسية في رصد البيانات من محيطها، ثم تقوم إما بمعالجتها محلياً بشكل أولي أو نقلها إلى وحدة معالجة مركزية. تتبنى هذه الشبكات نموذجاً لا مركزياً في العمل، حيث تترابط العقد وتتعاون فيما بينها لنقل المعلومات، مما يمنح النظام مرونة وكفاءة ملحوظتين. وتكمن إحدى مميزاتها الجوهرية في قدرتها على التشغيل دون الاعتماد على أي بنية تحتية مسبقة التجهيز، وهذا ما يميزها جوهرياً عن الشبكات التقليدية.

3-3-مكونات شبكة الاستشعار اللاسلكية

تتكون شبكات الاستشعار اللاسلكية من مكونين أساسيين هما:

3-3-1. عقدة الاستشعار (Sensor Nodes)

عقدة الاستشعار هي جهاز صغير الحجم يحتوي أربعة مكونات رئيسية هي وحدة الاستشعار التي تتكون عادةً من مستشعر واحد أو أكثر، إضافة إلى محولات الإشارة من التناظرية إلى الرقمية. حيث تقوم المستشعرات بمراقبة الظاهرة الفيزيائية وتوليد إشارات كهربائية تمثل هذه الظاهرة، فيما تعمل محولات الإشارة على تحويل هذه الإشارات الكهربائية إلى إشارات رقمية يتم تغذيتها لوحدة المعالجة. تحتوي وحدة المعالجة على معالج دقيق صغير يعالج البيانات الأولية ويتخذ قرارات محلية. أما وحدة الاتصالات فتتكون من جهاز لاسلكي قصير المدى مسؤول عن تنفيذ عمليات إرسال واستقبال البيانات عبر القناة الراديوية. تستخدم بروتوكولات لاسلكية لنقل البيانات إلى العقد المجاورة أو إلى محطة القاعدة. في حين تشتمل وحدة الطاقة على بطارية لتزويد جميع المكونات الأخرى في النظام بالطاقة اللازمة لتشغيله. إلى جانب ذلك، يمكن تجهيز العقدة الاستشعارية بوحدات إضافية أخرى تبعاً لمتطلبات التطبيقات المحددة. فعلى سبيل المثال، قد تتطلب بعض التطبيقات التي تعتمد على معلومات الموقع في عمل الشبكة وجود نظام تحديد المواقع العالمي (GPS).

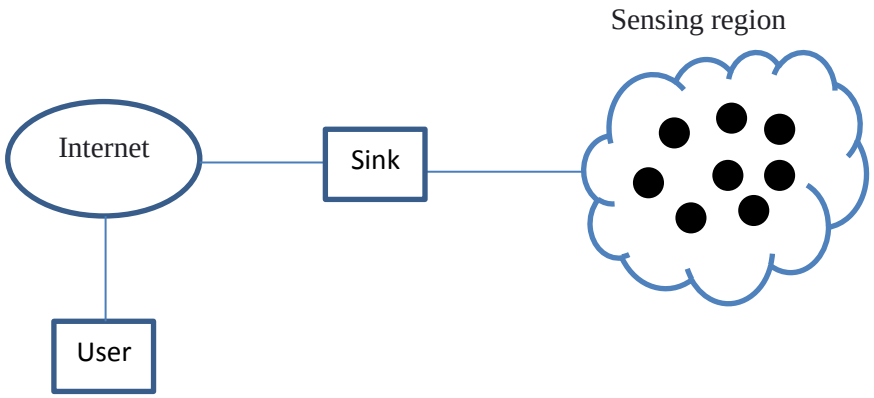
3-3-2. محطة القاعدة (Base Station)

تُعرف المحطة القاعدية في شبكات الاستشعار اللاسلكية على أنها كيان مركزي متصل بالطاقة، يتولى دوراً مزدوجاً يتمثل في إدارة عمليات الشبكة داخل منطقة الاستشعار وربطها بالشبكات الخارجية. تقوم المحطة القاعدية بوظائف رئيسية هي:

1. توجيه الشبكة :حيث تتولى إرسال الاستعلامات والأوامر إلى العقد الاستشعارية المنتشرة في الحقل.
2. تجميع البيانات: تعمل كنقطة تجمع مركزية تتلقى البيانات المُستشعَرة من العقد المختلفة والتي تعمل بشكل تشاركي لإنجاز المهمة الموكلة إليها.

3. البوابة الاتصالية: تمثل واجهة اتصال حيوية تربط الشبكة المحلية لعقد الاستشعار بالعالم الخارجي، كشبكة الإنترنت، حيث تقوم بمعالجة أولية للبيانات المجمعة قبل إرسال المعلومات ذات الصلة إلى المستخدمين النهائيين.

يوضح الشكل (3-1) تمثيل لبنية شبكة الاستشعار اللاسلكية



الشكل (3-1) بنية شبكة الاستشعار

3-4-بنية الشبكة (Network Architecture)

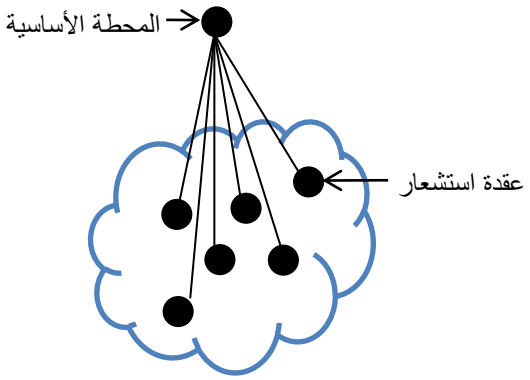
تتميز هندسة الشبكات في أنظمة الاستشعار اللاسلكية بأهمية بالغة عند نشر عدد كبير من العقد الاستشعارية في مناطق واسعة لرصد الظواهر الفيزيائية. لا يقتصر اتصال العقد في هذه الشبكات على الربط بين العقد المتجاورة فحسب، بل يشمل أيضاً الاتصال مع المحطة الأساسية عبر قنوات اتصال لاسلكية متخصصة. تقوم المحطة الأساسية بعد استقبال البيانات من العقد الاستشعارية بإجراء معالجة أولية للبيانات، ثم تنقل المعلومات المعالجة إلى المستخدمين النهائيين عبر شبكات الاتصال التقليدية أو شبكة الإنترنت [13].

يمكن تصنيف هيكلية الشبكات إلى نوعين رئيسيين:

3-4-1. بنية القفزة الواحدة.

لإرسال البيانات إلى محطة القاعدة ، يمكن لكل عقدة استشعار استخدام نمط الإرسال أحادي القفزة (Single-hop) لمسافات طويلة، مما يؤدي إلى إنشاء بنية القفزة الواحدة، كما هو موضح في الشكل (3-2). ومع ذلك، فإن الإرسال لمسافات طويلة مكلف من حيث استهلاك الطاقة، علماً بأن الطاقة المستهلكة من أجل

الاتصالات في شبكات الاستشعار تفوق بشكل كبير الطاقة المستهلكة في عمليات الاستشعار والحوسبة. علاوة على ذلك، يهيمن استهلاك الطاقة الخاص بعملية الإرسال على إجمالي الطاقة المستهلكة في الاتصال، ذلك لأن طاقة الإرسال المطلوبة تتناسب طرداً مع زيادة مسافة النقل [13].



الشكل (2-3) بنية القفزة الواحدة

3-4-2. بنية القفزات المتعددة

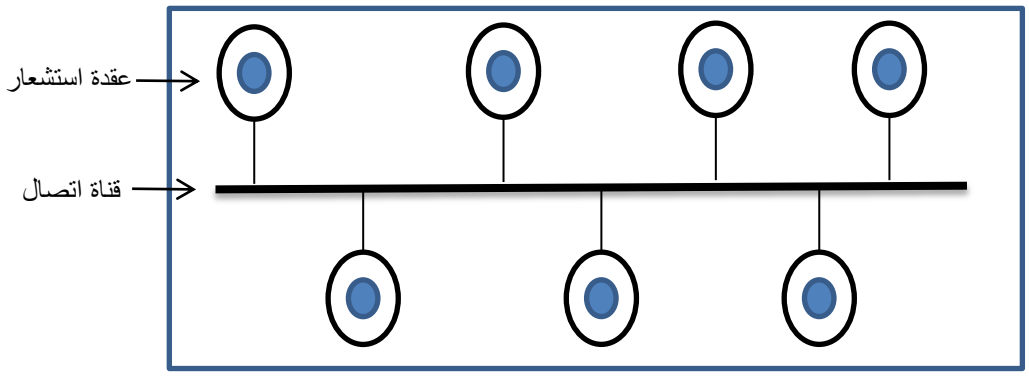
في معظم شبكات الاستشعار، يتم نشر العقد بكثافة عالية مما يجعل العقد المتجاورة قريبة من بعضها البعض، وهو ما يجعل الاتصال قصير المدى خياراً عملياً. في هذا النمط، تقوم العقدة بإرسال بياناتها إلى محطة القاعدة عبر عقدة وسيطة واحدة أو أكثر، مما يؤدي في النهاية إلى خفض استهلاك الطاقة الكلي مقارنةً بالنمط أحادي القفزة. لأن تخفيض حجم البيانات المرسلة ومسافة إرسالها يعد أمراً بالغ الأهمية لترشيد الطاقة وإطالة عمر الشبكة. وتحقيقاً لهذه الغاية، يفضل اعتماد نمط الاتصال متعدد القفزات لمسافات قصيرة. "تُصنَّف البنى التحتية للشبكات متعددة القفزات إلى نوعين أساسيين هما: البنية المسطحة (Flat) والبنية الهرمية(Hierarchical) [13].

3-5-طوبولوجيا شبكات الاستشعار اللاسلكية

تشكِّل طوبولوجيا شبكات الاستشعار اللاسلكية نسيجاً معمارياً ديناميكياً يُحدِّد آليات الترابط بين العقد لضمان تدفق البيانات. وقد استدعت الخصائص التطبيقية المتنوعة لهذه الشبكات بروز تصاميم هيكلية متعددة، يجسِد كل منها حل أمثل لسياق تشغيلي معين [15]. تأتي أبرز هذه التصاميم على النحو الآتي:

3-5-1. طوبولوجيا الناقل (Bus Topology)

تُعدُّ شبكة الناقل من أقدم نماذج الربط في الشبكات، حيث تُوصَل جميع العقد عبر قناة اتصال مشتركة. عند إرسال بيانات من عُقدة مُعيّنة، تنتقل الرزمة عبر قناة النفق المشتركة لتصل إلى جميع العقد المتصلة، غير أن العُقدة المُستهدفة فقط هي التي تقوم بمعالجة البيانات، بينما تتجاهلها باقي العقد. تتميز هذه البنية بسهولة التطبيق والتوسع، لكنها تعاني من تحدّيات رئيسة أبرزها ازدحام حركة البيانات ومحدودية مسار الاتصال الأحادي. وعليه، فإن هذا النموذج يكون فعالاً عندما يكون عدد العقد محدوداً، إذ إن زيادة عدد العقد تؤدي عادة إلى تراجع ملحوظ في الأداء. يوضح الشكل (3-3) تمثيل لطوبولوجيا الناقل.

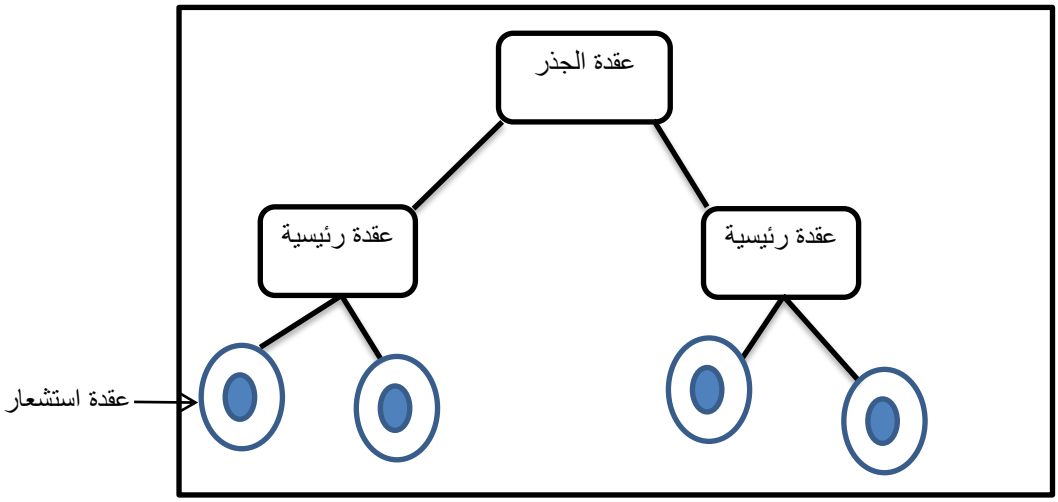


الشكل (3-3) طوبولوجيا الناقل

3-5-2. الطوبولوجيا الشجرية (Tree Topology)

تتبنى هذه الطوبولوجيا هيكلاً هرمياً، تُعرف عُقدته العليا باسم العقدة الجذرية (Root Node) والتي تمثل الموجه الرئيسي للاتصالات في الشبكة. تتفرع من هذه العقدة مستويات هرمية أدنى، حيث تُشكل كل عُقدة رئيسة مع العُقد التابعة لها شبكة نجمية (Star Network) على مستوى فرعي. في سياق شبكات الاستشعار، يتم نقل البيانات عبر مسارات قد تكون أحادية القفزة أو متعددة القفزات، تقوم العُقد الاستشعارية بجمع البيانات من البيئة المحيطة وإرسالها نحو المحطة القاعدية، حيث تعمل كل عُقدة على إعادة توجيه البيانات المستلمة من العُقد التابعة إلى العُقدة الأم. تكمن إحدى التحديات الرئيسية في هذه الطوبولوجيا في ضرورة إيجاد شجرة المسار الأقصر المثلى التي تحقق أقصى عمر تشغيلي للشبكة مع تقليل زمن التأخير، بالإضافة الى صعوبة تحقيق توازن الحمل (Load Balancing) بشكل فعال عبر المستويات المختلفة للشجرة. الاعتماد على مسار اتصال

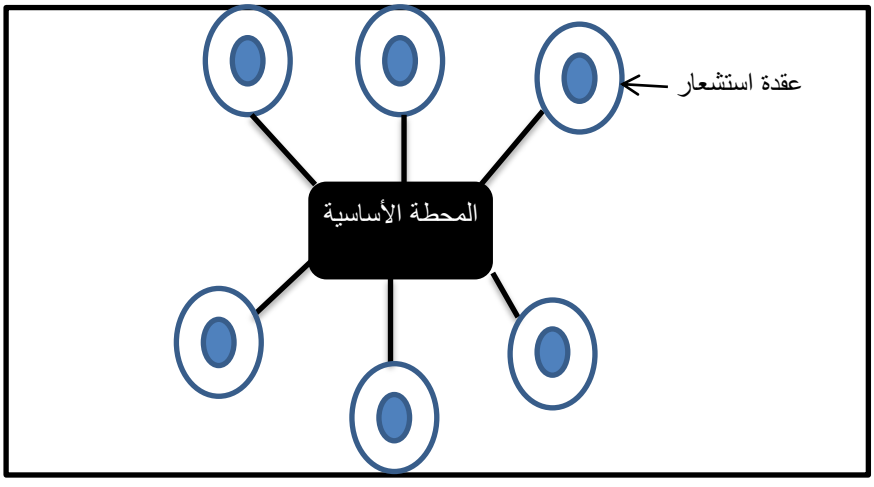
وحيد في بعض التصميمات يجعل النظام بأكمله عرضة للتعطّل الكامل في حال انقطاع هذه الوصلة. يوضح الشكل (3-4) تمثيلاً لطوبولوجيا الشجرية.



الشكل (3-4)الطوبولوجيا الشجرية

3-5-3. الطوبولوجيا النجمية (Star Topology)

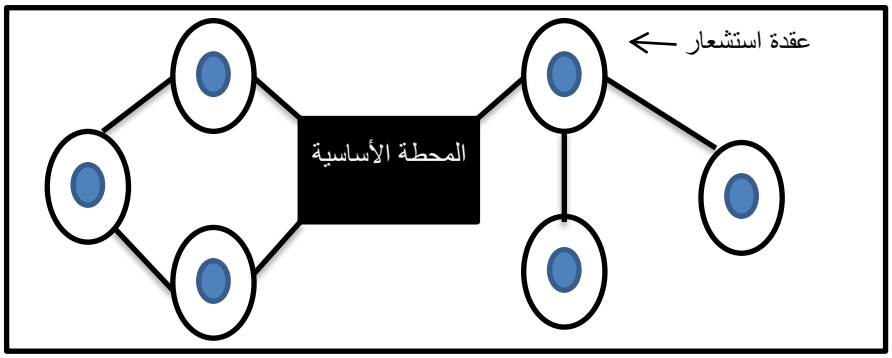
في الطوبولوجيا النجمية تتصل كل العقد مع المحطة الأساسية ولا تستطيع العقد التواصل مباشرةً مع بعضها البعض. يؤدي ذلك إلى قصور جوهري يتمثل في اعتمادها على مسار اتصال مركزي وحيد، يتم تُوجّيه جميع البيانات عبر المحطة الأساسية. يؤدي هذا التصميم إلى تعطل جمع البيانات، إذا تعطلت المحطة الأساسية أو انخفاض كفاءته يؤدي حتماً إلى شلل كامل في الشبكة وتعطيل جميع خدمات الاتصال. يوضح الشكل (3-5) تمثيلاً لطوبولوجيا النجمية [15].



الشكل(3-5)الطوبولوجيا النجمية

3-5-4. طوبولوجيا المشبك (Mesh Topology)

تتميز بنية شبكة التوصيل المتشابك بتوفيرها مسارات متعددة لانتقال البيانات بين العقد. تسمح الشبكة المتشابكة باختيار المسار الأكثر كفاءة. وتنقسم هذه البنية إلى نوعين رئيسيين :الشبكة المتشابكة الكاملة حيث كل عقدة متصلة مباشرة بجميع العقد الأخرى، والشبكة المتشابكة الجزئية التي تكتفي فيها بعض العقد بالاتصال غير المباشر مع العقد الأخرى عبر عقد وسيطة يوضح الشكل (3-6) تمثيلاً لطوبولوجيا المشبك [15].



الشكل(3-6) طوبولوجيا المشبك

3-6-تطبيقات شبكات الاستشعار اللاسلكية

تعدُّ تطبيقات شبكات الاستشعار اللاسلكية من الأساسيات التي تعطيها أهمية كبيرة ، نظراً لقدرتها على رصد البيانات البيئية بدقة عالية ونقلها ذاتياً دون تدخل بشري. تُعد العُقَد الاستشعارية مكونات أساسية في الأنظمة الحديثة، حيث تتيح القدرة على الرصد المستمر، وكشف الأحداث، وتحديد هويتها، ورصد المواقع الجغرافية، بالإضافة إلى التحكم المحلي في المشغلات، ويُعَد دمج تقنيات الاستشعار الدقيق مع الاتصال اللاسلكي بين هذه العُقَد نقلة نوعية تفتح آفاقاً جديدة في مجالات تطبيقية متعددة.

يمكن تصنيف هذه التطبيقات إلى مجالات رئيسة تشمل: الدفاع، والرصد البيئي، والرعاية الصحية، والأتمتة المنزلية، والتطبيقات التجارية الأخرى. كما يمكن توسيع هذا التصنيف ليشمل مجالات إضافية مثل الاستكشاف الفضائي، والمعالجة الكيميائية، وإدارة الكوارث، مما يعكس المرونة الوظيفية والاحتمالية العالية لهذه التقنيات في معالجة التحديات المعقدة. سنتعرف فيما يلي على بعض تطبيقات شبكات الاستشعار اللاسلكية [16].

3-6-1. التطبيقات العسكرية

تُعدُّ شبكات الاستشعار عنصراً جوهرياً في أنظمة القيادة والسيطرة والاتصالات والحوسبة والاستخبارات والمراقبة والاستطلاع واستهداف العدو في المجال العسكري. وتجعلُها خصائصُها المتعلقة بالنشر السريع، والقدرة على التنظيم الذاتي، وتحمل الأعطال، تقنيةً واعدةً للمراقبة في هذه الأنظمة. ونظراً لاعتماد هذه الشبكات على النشر الكثيف لعُقَدِ حساسات منخفضة التكلفة وقابلة للتلف، فإن تدمير بعض العُقَد بسبب الأعمال العدائية لا يؤثر على العملية العسكرية بقدر ما يؤثر تدمير أجهزة الاستشعار التقليدية، مما يجعلهَا أسلوبًا أكثر ملاءمةً لبيئات ساحات القتال. من بين التطبيقات العسكرية لشبكات الاستشعار اللاسلكية: رصد القوات والمعدات والذخيرة، ومراقبة ساحة المعركة، واستطلاع قوات العدو والتضاريس، وتحديد الأهداف، وتقييم الأضرار التي لحقت بالمعركة، والكشف عن الهجمات النووية والبيولوجية والكيميائية واستطلاعها. فعلى صعيد رصد القوات الصديقة والمعدات والذخيرة، يمكن للقادة والقادة العسكريين مراقبة الحالة المستمرة للقوات الصديقة، وحالة المعدات وتوافرها، والذخيرة في ساحة المعركة باستخدام شبكات الاستشعار، حيث يمكن توصيل حساسات صغيرة بكل جندي ومركبة ومعدة وذخيرة حاسمة تُبلغ عن حالتها. ثم تُجمَع هذه التقارير في عُقَدٍ مجمِّعةٍ تُرسَل إلى قادة الوحدات، كما يمكن تمرير البيانات إلى المستويات العليا في التسلسل القيادي مع تجميعها مع بيانات من وحدات أخرى عند كل مستوى [16].

3-6-2. التطبيقات البيئية

تُسهم شبكات الاستشعار في مجال المراقبة البيئية بعددٍ من التطبيقات الحيوية، والتي تشمل: تتبُّع حركة الطيور والحيوانات الصغيرة والحشرات، ومراقبة الظروف البيئية المؤثرة في المحاصيل والثروة الحيوانية، وإدارة عمليات الري، والرصد الأرضي واسع النطاق واستكشاف الكواكب، والكشف الكيميائي والبيولوجي، والزراعة الدقيقة، والرصد البيولوجي والأرضي والبيئي في السياقات البحرية والغلاف الجوي، فضلاً عن الكشف عن حرائق الغابات، والأبحاث المتعلقة بالأرصاد الجوية والجيوفيزياء، والكشف عن الفيضانات، ورسم خرائط للتعقيد الحيوي للبيئة، ودراسة التلوث [16].

في مجال الكشف عن حرائق الغابات، يمكن نشر عُقَدِ الاستشعار بشكل استراتيجي وعشوائي وكثيف داخل الغابة، مما يمكنها من نقل المعلومات الدقيقة عن بؤرة الحريق إلى المستخدمين النهائيين قبل أن تنتشر النيران بشكل لا يمكن السيطرة عليه. ويمكن دمج ملايين من هذه العقَد باستخدام ترددات الراديو أو الأنظمة البصرية. كما يمكن تجهيزها بأساليب فعالة لجمع الطاقة، مثل الخلايا الشمسية، نظرًا لأن أجهزة الاستشعار قد تظل عاملة دون صيانة لعدة أشهر أو سنوات. وتتعاون هذه العُقَد مع بعضها البعض لأداء مهمة الاستشعار الموزع، متغلبّةً على العوائق المادية مثل الأشجار والصخور التي قد تحجب خط الرؤية لأجهزة الاستشعار السلكية [16].

3-6-3. التطبيقات الصحية

تُعدُّ شبكاتُ الاستشعار اللاسلكية من التقنيات الواعدة في المجال الصحي، حيث تتعدد تطبيقاتها لتشمل: الرصد المتكامل لحالة المرضى، والتشخيص الطبي، وإدارة الأدوية داخل المستشفيات، ودراسة حركة الكائنات الحية، فضلاً عن المراقبة عن بُعد للبيانات الفيزيولوجية البشرية، وتتبع الأطباء والمرضى داخل المؤسسات العلاجية. في مجال الرصد عن بُعد للبيانات الفيزيولوجية، فتوفر هذه الشبكات إمكانية تخزين البيانات الصحية لفترات طويلة، مما يُمكّن من استخدامها في الأبحاث الطبية المستقبلية. كما يمكن لهذه الشبكات مراقبة سلوكيات كبار السن والكشف عن الحالات الطارئة مثل السقوط المفاجئ. وتتميز هذه التقنية بحجمها الصغير الذي يمنح المريض حرية أكبر، ويساعد الأطباء على الكشف المبكر عن الأعراض المرضية المُحددة مسبقاً. علاوة على ذلك، فهي تُحسّن جودة حياة المرضى مقارنة بالإقامة في المراكز العلاجية. ولاختبار جدوى هذه الأنظمة، تم تصميم المنزل الصحي الذكي في كلية الطب بمدينة غرونوبل الفرنسية كتجربة رائدة [16]. وفيما يخص تتبع الأطباء والمرضى داخل المستشفيات، يُزوَّد كل مريض بعدة عُقد استشعارية خفيفة الوزن، لمهمة طبية محددة، فمنها ما يرصد معدل ضربات القلب، وآخر لقياس ضغط الدم. كما يحمل الأطباء أجهزة استشعار تتيح تحديد مواقعهم داخل المنشأة الطبية. وفي سياق إدارة الأدوية، يُسهم تركيب العُقد الاستشعارية على عبوات الأدوية والمرضى معاً في تقليل خطر التبادل الدوائي، إذ تحمل العُقد المرفقة بالمرضى بيانات عن الحساسيات

والأدوية المطلوبة لكل منهم. وقد أثبتت النظم الحاسوبية المُطبقة في هذا المجال فعاليتها في الحد من الأحداث الدوائية الضارة [16].

3-6-4. التطبيقات المنزلية

مع تسارع التطور التقني، أصبح من الممكن دمج عُقد استشعارية ذكية ومشغِّلات في الأجهزة المنزلية مثل المكانس الكهربائية وأفران الميكروويف والثلاجات وأجهزة التسجيل. وتتيح هذه العُقد التفاعل بين الأجهزة المنزلية بعضها البعض ومع الشبكات الخارجية عبر الإنترنت أو الأقمار الاصطناعية، مما يُمكّن المستخدمين من إدارة هذه الأجهزة محلياً وعن بُعد بكفاءة عالية. يتبع تصميم البيئات الذكية منظورين رئيسيين: منظور يركز على الإنسان، وآخر يركز على التقنية. ففي المنظور الأول، يجب أن تتكيف البيئة الذكية مع احتياجات المستخدمين من حيث قدرات الإدخال والإخراج. أما في المنظور الثاني، فيتطلب تطوير حلول تقنية جديدة في مجال الأجهزة والشبكات وخدمات البرمجيات الوسيطة. ويمكن توضيح تطبيق هذه المفاهيم من خلال نموذج يُضمّن العُقد الاستشعارية في الأثاث والأجهزة المنزلية لتمكينها من التواصل مع خادم الغرفة، الذي بدوره يتفاعل مع خوادم الغرف الأخرى للاستفادة من الخدمات المشتركة مثل الطباعة والمسح الضوئي وإرسال الفاكس. كما يمكن دمج هذه المكونات مع الأجهزة المضمنة الحالية لإنظمة ذاتية التنظيم والتكيف تستند إلى نماذج نظرية التحكم. ويظهر مثال تطبيقي آخر في "المختبر السكني" بمعهد جورجيا للتكنولوجيا، الذي يُطبّق أنظمة حوسبة واستشعار تتسم بالموثوقية والشفافية [16].

3-7-العوامل المؤثرة في تصميم شبكات الاستشعار اللاسلكية

تُؤثِّر مجموعة من العوامل المتشابكة في تصميم شبكات الاستشعار، حيث تشمل: التسامح مع الأعطال، والتغطية، وتكاليف التصنيع، وبيئة التشغيل، وطوبولوجيا الشبكة، ووسائط الإرسال، واستهلاك الطاقة. وقد تناولت العديد من الدراسات هذه العوامل [17] ، إلا أن غياب رؤية متكاملة وشاملة تجمع بين جميع هذه العوامل المحددة لتصميم شبكات الاستشعار وعُقدها يظل قائماً. سنتعرف فيما يلي على بعض تحديات شبكات الاستشعار اللاسلكية.

3-7-1. الطاقة

تعَدُّ كفاءة استهلاك الطاقة واحدة من أبرز التحديات الحرجة في شبكات الاستشعار اللاسلكية. ففي ظلِّ التقنيات المتاحة حالياً، تعمل أجهزة الاستشعار ببطاريات ذات سعة محدودة، مما يفرض قيوداً صارمة على مواردها الطاقية. ينطوي هذا القيد على تحديات متعددة المستويات تشمل تطوير العتاد والبرمجيات، بالإضافة إلى تصميم البنى التحتية للشبكة والبروتوكولات الحاكمة لها. وتنعكس هذه الخصائص مجتمعةً على العمر التشغيلي للتطبيقات، مما يَجعلُ إطالة عمر الشبكة عنصراً أساسيّاً في مرحلة التصميم النظامي لهذه الشبكات. بدءاً من المكونات المادية والمنطقية ووصولاً إلى الهياكل الشبكية وآليات التواصل، مما يستدعي اتباع منهج شامل لتحقيق الاستدامة الطاقية في هذه الشبكات. تَبرُزُ إحدى الوسائل البارزة لتحقيق هذه الغاية من خلال جدولة نشاط أجهزة الاستشعار، بحيث تضمن وجود مجموعة نشطة منها قادرة على تنفيذ المهمة المطلوبة، بينما يمكن للأجهزة الزائدة عن الحاجة أن تنتقل إلى وضعية السكون (Sleep Mode). وأشار الباحثون [17] إلى أن استهلاك الطاقة في حالة السكون يقل بحوالي 15 مرة عنه في حالة النشاط. ومن أجل إطالة العمر التشغيلي للشبكة، يتعين مراعاة كفاءة استهلاك الطاقة في كل جانب من جوانب التصميم.

3-7-2. التغطية

تُعد التغطية إحدى الإشكاليات المحورية في مجال شبكات الاستشعار اللاسلكية، حيث يتمثل الهدف الأساسي منها في ضمان وقوع كل نقطة ضمن النطاق الجغرافي المستهدف داخل مدى الاستشعار لوحدة استشعار واحدة على الأقل. ونظراً للطبيعة العملية لنشر هذه الشبكات، غالباً ما يتم توزيع أجهزة الاستشعار بكثافة عالية، إذ يفوق العدد الفعلي للمستشعرات المنشورة العدد الأمثل المطلوب نظرياً. ويعزى هذا التفاوت بشكل رئيسي إلى صعوبة تحقيق وضعية دقيقة لأجهزة الاستشعار، خاصة عندما تكون المنطقة المستهدفة صعبة أو خطرة الوصول .

3-7-3. الامن

تُشكِّل شبكات الاستشعار اللاسلكية حجر زاوية في العصر القادم للحوسبة المنتشرة. ومع ذلك، فإن محدودية مواردها من حيث القدرة الحاسوبية والذاكرة والطاقة، وقابليتها للاختراق المادي واعتمادها على الاتصالات اللاسلكية، تجعل من الأمن التحدي الأبرز في تصميم هذه الشبكات. ويتطلب النطاق الواسع لنشرها اتخاذ قرارات مدروسة وإجراء مفاضلات دقيقة بين مختلف تدابير الأمن. وعلى الرغم من أن النشر الواسع لهذه الشبكات أصبح وشيكاً، وأنها تتجه لدور حيوي في التطبيقات العسكرية والحياة اليومية، إلا أن مخاوف الأمان تشكل عائقاً محتملاً أمام هذا الانتشار. علماً أن معظم الأبحاث الحالية تفترض بيئة موثوقة، مما يترك العديد من التحديات البحثية الملحة التي يجب معالجتها قبل الوثوق الكامل بهذه الشبكات للمهام المهمة [17].

3-7-4. الموارد الحاسوبية

تُعَدُّ محدودية الموارد الحاسوبية في عُقد الاستشعار، بما تشمله من قيود على قدرات المعالجة والتخزين، عاملاً معيقاً للوظائف الحاسوبية التي يمكن لهذه العُقد تنفيذها. وتنشأ عن هذه القيود الهيكلية تحديات منهجية في مجالي تطوير البرمجيات وتصميم بروتوكولات الشبكة لشبكات الاستشعار، حيث يتعين الأخذ بعين الاعتبار، بالإضافة إلى قيد استهلاك الطاقة، القدرات المحدودة للمعالجة والتخزين المتوفرة في عُقد الاستشعار [17].

3-7-5. النشر

يُعد النشر الواسع والعشوائي سمةً أساسية في تشكيل شبكات الاستشعار، حيث تتكون هذه الشبكات من أعداد هائلة من العقد تتراوح من المئات إلى الآلاف أو أكثر. ويعتمد أسلوب نشر هذه العُقد بشكل جوهري على طبيعة التطبيق، حيث يتراوح ما بين النشر اليدوي المنظم والنشر العشوائي. في السياقات العملية، غالباً ما يتم نشر العُقد بشكل عشوائي في منطقة مستهدفة، أو إسقاطها بكثافة في مناطق عدائية أو يتعذر الوصول إليها. لكن يترتب على هذا النمط من النشر (المتبع في اغلب شبكات الاستشعار اللاسلكية) ضرورة قيام العُقد بتنظيم ذاتها بشكل تلقائي ومستقل لتشكيل بنية شبكية اتصالية متكاملة، كشرط أساسي مسبق لبدء تنفيذ مهمة الاستشعار. وهذا ما يفرض قيد إضافي في تصميم شبكات الاستشعار اللاسلكية المنشورة بشكل عشوائي. حيث

تتنوع تطبيقات شبكات الاستشعار تنوعاً واسعاً، مما ينتج عنه متطلبات متباينة بشكل كبير من تطبيق لآخر. ونظراً لهذا التباين، لا يمكن لبروتوكول شبكي واحد أن يلبي متطلبات جميع التطبيقات. وعليه، فإن تصميم شبكات الاستشعار يكون محكوماً بخصوصية التطبيق وملبياً لمتطلباته الفريدة [17].

3-7-6. الموثوقية (Reliability)

يُعد معدل استقبال البيانات بشكل صحيح عند العقدة المستشعرة أو المحطة الأساسية معياراً مهماً في تقييم موثوقية الشبكات اللاسلكية للمستشعرات. وتتفاوت متطلبات هذه الموثوقية تبعاً لنطاق التطبيق وطبيعته، ففي المجالات الحساسة التي ترتبط بالأمن الشخصي أو المراقبة في ساحات القتال، تتطلب الشبكات مستوى عالي جداً من الموثوقية، حيث إن أي خطأ بسيط قد يؤدي إلى عواقب وخيمة. في المقابل، قد تكتفي التطبيقات الأقل حساسية، كتلك المستخدمة في المجال الزراعي، بمستوى أدنى من الموثوقية [17].

ترتبط الموثوقية ارتباطاً وثيقاً بالتكلفة الإجمالية للعقد المستشعرة، مما يثير تحدياً كبيراً في تحديد سعر المستشعرات بما يتناسب مع متطلبات الموثوقية في السيناريوهات العملية المتنوعة. كما أن البيئة التي تُنشر فيها هذه العقد تلعب دوراً حاسماً في التأثير على أداء الشبكة. ففي البيئات الصناعية، على سبيل المثال، تواجه الشبكات مجموعة من العوامل المعيقة، مثل طبيعة الموقع، ودرجات الحرارة، والموجات الكهرومغناطيسية المنبعثة من الآلات والأسلاك، بالإضافة إلى التأثيرات الكيميائية [17].

3-7-7. الوقت الفعلي (Real-time)

يُعد متوسط الوقت الذي تستغرقه حزمة البيانات للانتقال من العقدة المستشعرة إلى العقدة الاخرى أو المحطة الأساسية مقياساً شائعاً لتقييم الأداء الزمني للشبكات. وبشكل عام، تفرض التطبيقات العسكرية متطلبات أسرع بكثير لسرعة الاستجابة مقارنةً بغيرها من التطبيقات. يتحدد الأداء الزمني الفعلي في الأساس بعوامل رئيسية عدة، تشمل وقت إعادة الإرسال، والازدحام في الشبكة، وتأخير طبقة التحكم بالوصول إلى الوسط. تعود أسباب التأخير الزمني في مرحلة الاتصال إلى عوامل متعددة، منها ما هو متعلق بالظروف المناخية والبيئية، مثل الرياح والأمطار والثلوج والرطوبة ودرجات الحرارة المتطرفة والإشعاع الشمسي، والتي يمكن أن تؤثر سلباً

على جودة قناة الاتصال. كما أن هناك عوامل أخرى مسببة لضعف أداء الشبكة لا تعزى إلى الطبيعة، لا سيما في البيئات الصناعية حيث تُنشر العقد المستشعرة لمراقبة الجوانب المختلفة للعمليات والآلات. فحركة الآلات الدوارة، والأجسام المتحركة، بل وحتى المواد الكيميائية المتطايرة، يمكن أن تشكل عوائق مادية أو مصدراً للتداخل الكهرومغناطيسي، مما يؤثر على أداء الشبكة. وعليه، فإن العوامل المؤثرة في الأداء الزمني معقدة ومتشابكة، ويصعب تقديرها بدقة نظراً لتعدد مصادرها وتفاعلها [17].

3-8-خلاصة الفصل

تناول هذا الفصل شبكات الاستشعار اللاسلكية من خلال تعريفها ومكوناتها الأساسية، ثم الانتقال إلى مناقشة بنيتها وأنماط طوبولوجياتها المتنوعة. كما استعرضنا أهم تطبيقات هذه الشبكات ودورها الحيوي في مجالات متعددة، واختتم الفصل بشرح العوامل المؤثرة في تصميمها.

4 التسامح مع الأعطال في شبكات الاستشعار اللاسلكية

4-1-مقدمة

تعد شبكات الاستشعار اللاسلكية عرضة للأعطال نظراً لنشر العقد منخفضة التكلفة في بيئات قاسية أو غير خاضعة للرقابة. تتعرض شبكات الاستشعار للتعطل بشكل رئيسي بسبب عاملين: عُطل العقد نفسها و/أو عُطل الاتصالات. قد تعاني شبكة الاستشعار المُنشأة من أعطال عديدة لأسباب متعددة مثل التأثيرات البيئية، والعيوب في العتاد، والأخطاء البرمجية. يمكن أن تتسبب هذه الأعطال في معدلات فقدان مرتفعة للبيانات، أو تأخير طويل في الإرسال، أو حتى انقطاع في الشبكة، مما يؤثر سلبًا على العمليات الطبيعية للشبكة. وبالتالي، تصبح أعطال العقد ظاهرة حتمية يمكن أن تقلل بشكل كبير من العمر الإجمالي للشبكة وتجعل البنية التحتية للاتصالات غير قابلة للاستخدام [19]. سنتعرف في هذا الفصل على المفاهيم الأساسية في التسامح مع الأعطال وأهميته في استمرار الشبكة في العمل لأطول وقت ممكن. بالإضافة إلى التطرق إلى بعض أعطال شبكات الاستشعار اللاسلكية.

4-2-العطل

يحدث العطل في النظام عندما ينحرف الأداء الفعلي عن الأداء المتوقع. يعزى حدوث الأعطال إلى سببين رئيسيين: فشل في المكونات المادية أو خلل في البرمجيات [20].

تُهدد موثوقية النظام ثلاثة أنواع من التهديدات المترابطة التي تمثل سلسلة تطور العطل:

1. تعريف العطل (Fault)

السبب الكامن أو الخلل الأساسي في النظام، مثل عيب في التصميم أو عطل مادي. وهو المرحلة الأولية للتهديد.

2. الخطأ (Error)

المظهر الظاهري للعطل في حالة النظام، حيث يؤدي العطل إلى حدوث انحراف في الحالة الداخلية للمكون [20].

3. الفشل (Failure)

عدم قدرة النظام على تقديم الخدمة المطلوبة وفق المواصفات المحددة، ويحدث عندما يتجاوز الخطأ حدود التسامح [20].

4-2-1. أدارة الأعطال

تمثل هذه السلسلة (عطل ← خطأ ← فشل) التقدم الزمني للتهديد. فعلى سبيل المثال، قد يكون العطل (مثل تلف في الذاكرة) هو السبب الكامن، الخطأ (بيانات غير صحيحة في الحسابات)، وينتهي بفشل (توقف النظام عن الاستجابة). يعد فهم هذه التفرقة ضرورياً لتصميم آليات فعالة للتسامح مع الأعطال، حيث يمكن التركيز على كشف الأخطاء ومعالجتها قبل أن تتطور إلى فشل كامل في النظام. يمكن إدارة الأعطال في الشبكة بمنهجين:

1- آلية التسامح مع الأعطال: وتتضمن عمليات استعادة الأداء بعد حدوث العطل.

2- تقنيات منع الأعطال: وتركز على الوقاية من خلال تهيئة بيئة تشغيل آمنة.

4-3-التسامح مع الأعطال (Fault Tolerance)

تُعد الموثوقية الهدف الشامل لأي نظام، حيث تشمل قدرته على الاستمرار في العمل وفق المتطلبات الوظيفية وغير الوظيفية المحددة. أما التسامح مع الأعطال فهو أحد متطلبات الجودة غير الوظيفية التي تسهم في تحقيق هذه الموثوقية.

لضمان فعالية هذا المتطلب، يجب أن يكون قابلاً للقياس والتحقق بشكل كمي، من خلال صياغته بصورة دقيقة وقابلة للاختبار. على سبيل المثال: يجب أن يتحمل النظام عدد X من الأعطال أو فاصل زمني مقداره Y بين الأعطال [20].

4-3-1. تحقيق التسامح مع الأعطال

لتحقيق التسامح مع الأعطال نتبع مجموعة من الآليات والاستراتيجيات المصممة لضمان استمرارية عمل النظام وأدائه الوظيفي السليم عند حدوث أعطال غير متوقعة في بعض مكوناته. تمثل هذه المراحل عنصراً أساسياً في تعزيز موثوقية الأنظمة ومرونتها، خاصة في التطبيقات الحرجة [20] التي تتطلب درجة عالية من الاستمرارية التشغيلية وللتسامح مع الأعطال نقوم بما يأتي:

4-3-2. منع الأعطال

تُعد تقنيات منع الأعطال نهجاً استباقياً يهدف إلى تقليل احتمالية حدوث الأعطال في الشبكات من خلال اعتماد معايير دقيقة خلال مرحلتي التصميم والنشر، مع ضمان استمرارية المراقبة والتقييم لحالة الشبكة. تركز هذه التقنيات على تحقيق اتصال شامل وتغطية فعّالة، مع توفير مسارات احتياطية لضمان استمرارية نقل البيانات حتى في الظروف غير المثالية [20].

4-3-3. اكتشاف الأعطال

تُعد عملية اكتشاف الأعطال عنصراً حاسماً في إدارة الشبكات، حيث تعتمد منهجياتها على طبيعة التطبيق المحدد وأنواع الأعطال المتوقعة وتتنوع التقنيات المستخدمة في هذا المجال وفقاً لطبيعة البيئة التشغيلية ومتطلبات الأداء. من بين التقنيات المستخدمة لاكتشاف الأعطال تبادل رسائل جس النبض [20].

4-3-4. عزل الأعطال وتحديدها

تمثل مرحلة عزل الأعطال وتحديدها عملية تشخيص متقدمة تهدف إلى تحديد السبب الأساسي للعطل بدقة. تعتمد هذه العملية على تحليل منهجي للعلاقات بين الإنذارات الواردة من مختلف مكونات الشبكة بالاستناد إلى معرفة مسبقة بأنماط الأعطال المتوقعة وأسبابها المحتملة [20].

4-3-5. استعادة العطل

تُعرف عملية استعادة العطل بأنها الإجراء المنهجي الرامي إلى إزالة الآثار السلبية الناجمة عن العطل، وإعادة النظام إلى حالته التشغيلية الطبيعية بأقل وقت ممكن وأقل فقدان للبيانات. تمثل هذه المرحلة استمرارية الخدمة وتقليل وقت التعطل الفعلي للنظام [20].

4-4-موثوقية النظام

لتحقيق موثوقية النظام هناك عدة أساليب نذكر منها ما يأتي:

4-4-1. التكرار المادي (Hardware Redundancy)

يعتمد مفهوم التكرار المادي على مضاعفة العناصر المادية الحرجة في النظام، حيث تعمل هذه العناصر المتطابقة بالتوازي. يعد نظام التكرار الثلاثي TMR (Triple Modular Redundancy) أحد أبرز أشكال هذا التصميم، حيث يتم استخدام ثلاث وحدات متماثلة لأداء المهمة نفسها بشكل متزامن.

تعتمد آلية العمل على وجود دائرة مقارنة (آلية تصويت) تقوم بمقارنة مخرجات الوحدات الثلاث وتحديد القيمة الصحيحة بناءً على مبدأ الأغلبية. بهذه الطريقة، يمكن للنظام تحديد العطل في إحدى الوحدات وتجاوزه، مما يحافظ على استمرارية عمل النظام بشكل صحيح حتى في حالة فشل أحد المكونات [20].

4-4-2. التكرار في البرمجيات (Software Redundancy)

يتم تحقيق التكرار في البرمجيات من خلال:

1. **التكرار الساكن (Static Redundancy)**

يعتمد التكرار الساكن على تشغيل نسخ متعددة من البرنامج لأداء المهمة ذاتها. لا يحتاج التكرار الساكن إلى آلية كشف أخطاء منفصلة بل يعتمد على مقارنة مخرجات النسخ المختلفة لتحديد النتيجة الصحيحة.

2. التكرار الديناميكي (Dynamic Redundancy)

في التكرار الديناميكي يتم إنشاء نقاط فحص دورية تحفظ فيها حالة النظام، كما يستخدم آليات كشف الأخطاء لاكتشاف الأعطال، وعند اكتشاف عطل يعاد النظام إلى آخر نقطة فحص سليمة.

يوضح الجدول (4–1) مقارنة بين التكرار الساكن والتكرار الديناميكي.

الخاصية	التكرار الساكن	التكرار الديناميكي
آلية العمل	نسخ متعدد من البرنامج	نقاط فحص واستعادة
كشف الأخطاء	غير مطلوب	مطلوب
التعقيد	أعلى في التصميم	أعلى في التشغيل
الكفاءة	أقل من حيث الأداء	أعلى من حيث استغلال الموارد

الجدول (4–1) مقارنة بين التكرار الساكن والتكرار الديناميكي.

3. التكرار الزمني (Time Redundancy)

يشير التكرار الزمني إلى إعادة تنفيذ العملية الحسابية عدة مرات ومقارنة النتائج لتحديد وجود أي تباين. يُشير الاختلاف بين العمليات الحسابية المتعددة إلى وجود عطل عابر. يتم تنفيذ العملية الحسابية أكثر من مرة بفوارق زمنية دون الحاجة إلى آلية تصويت، ولكن تتم مقارنة النتائج لتحديد مدى اتساقها. يشير عدم الاتساق في النتائج إلى وجود عطل. عادة ما يكون هذا المخطط مفيداً عندما يكون العطل غير دائم، حيث لا فائدة من الاستمرار في الحساب والمقارنة في حالات الأعطال الدائمة.

4–5–الأعطال في شبكات الاستشعار اللاسلكية

تُعد العقد الاستشعارية في شبكات الاستشعار اللاسلكية عُرضة للأعطال بسبب انتشارها في بيئات غير خاضعة للإشراف المباشر وربما معادية. يمكن أن تظهر هذه الأعطال على مستويات مختلفة تشمل وحدة المعالجة، وجهاز الإرسال والاستقبال، ووحدة التخزين، ومصدر الطاقة، وأجهزة الاستشعار والمشغلات. ونظراً لحتمية حدوث الأعطال، يصبح تحديد العقد المعطلة والسليمة في الشبكة أمراً بالغ الأهمية [21].

4-5-1. تصنيف الأعطال

تتنوع الأعطال المحتملة في شبكات الاستشعار اللاسلكية لتشمل:

1. الأعطال الدائمة (Hard Faults)

تعرف الأعطال الدائمة [21] بأنها غير قابلة للإصلاح، وتنتج عن فشل بعض المكونات المادية فتصبح فيها عقدة الاستشعار غير قادرة على التواصل مع بقية الشبكة. يمكن تصنيف أسبابها على النحو الآتي:

- **أعطال في وحدات الاتصال:** وتشمل خللًا في الوحدات المسؤولة عن نقل البيانات، مثل وحدات الاتصال (Communication Modules) أو أجهزة الإرسال والاستقبال (Transceivers).
- **استنفاد الطاقة:** يعد نفاد شحن البطارية سبباً رئيسياً لهذا النوع من الأعطال، حيث يفقد النظام قدرته على التشغيل. تُعد عملية إعادة شحن البطاريات أو استبدال العقد الاستشعارية تحدياً كبيراً نظراً لطبيعة النشر الصعبة في البيئات المشار إليها سابقاً. لذلك، يصبح الاستثمار الاستراتيجي للطاقة المحدودة في العقد الاستشعارية عاملاً حاسماً لضمان إطالة عمر الشبكة.
- **انقطاع الاتصال بالشبكة:** يحدث هذا العطل عندما تخرج عقدة الاستشعار عن نطاق التغطية الكاملة للشبكة المتنقلة، مما يؤدي إلى انقطاع القدرة على التواصل.

2. الأعطال المؤقتة (Soft Faults)

تُعرّف الأعطال المؤقتة [21] بأنها أعطال عابرة أو متقطعة لا تؤدي إلى توقف العقدة عن العمل بشكل كلي، بل تستمر في أداء وظائفها ولكن بسلوك وظيفي شاذ (العقد المصابة بهذا النوع من الأعطال تتصرف بشكل غير منتظم ويصعب التنبؤ بسلوكها أو اكتشافه). ومن أبرز مظاهر هذه الأعطال:

- **السلوك البيزنطي (Byzantine):** تتصرف العقدة بشكل تعسفي أو خبيث، مما يهدد سلامة النظام دون أن يكون الفشل واضحاً.
- **فشل الإغفال (Omission):** يحدث عندما تفشل العقدة في الرد على الطلبات بشكل متقطع، مما يؤدي إلى انقطاع غير منتظم في الخدمة.

- **فشل التوقيت (Timing)**: يظهر هذا العطل عندما تستجيب العقدة خارج النطاق الزمني المحدد، وهو ما يمثل مشكلة حرجة في الأنظمة التي تتطلب أداءً زمنياً عالي الدقة.

4-5-2. الأعطال الامنية (Security failures)

تُعد الشبكات اللاسلكية عُرضة للهجمات الأمنية [21] بسبب طبيعة البث لوسط الإرسال المستخدم. كما تواجه شبكات الاستشعار اللاسلكية (WSNs) تحديات أمنية إضافية نظراً لانتشار العقد في بيئات غير آمنة أو معادية، حيث تفتقر غالباً للحماية المادية. وفي ظل الشبكات الاستشعارية واسعة النطاق، يصبح من غير العملي مراقبة كل عُقدة على حدة وحمايتها من الهجمات المادية أو المنطقية. يمكن للمهاجمين تطوير أنواع متعددة من التهديدات الأمنية لزعزعة استقرار نظام الشبكة. لذا، نُقدم بعض التهديدات الأمنية لشبكات الاستشعار اللاسلكية [21].

1. الهجمات على العقد

يمكن تصنيف الهجمات الأمنية على العقد في شبكات الاستشعار اللاسلكية إلى فئتين رئيسيتين بناءً على مصدر الهجوم:

- هجمات الخارج تشير إلى الهجمات التي تنفذها عقد لا تنتمي إلى الشبكة الاستشعارية، حيث يحاول المهاجم من خارج النظام اختراقه أو تعطيله.
- هجمات الداخل تحدث عندما تبدأ العقد الشرعية والمصرح لها ضمن الشبكة بالتصرف بطرق غير مقصودة أو غير مصرح بها، وذلك نتيجة اختراقها أو التلاعب بها من قبل مهاجم خارجي.

لمواجهة هذه التهديدات، يُوصى بعدد من التدابير الأساسية لتعزيز أمن الشبكة:

- المرونة في مواجهة هجمات الخارج من خلال آليات مثل المصادقة القوية والتشفير لمنع العقد غير المصرح لها من الانضمام إلى الشبكة أو الوصول إلى بياناتها.
- القدرة على الصمود أمام هجمات الداخل وذلك بتطوير أنظمة قادرة على الكشف عن التصرفات الشاذة للعقد المخترقة من الداخل والعزل التدريجي لتأثيرها.

- التدهور المتدرج في أداء الأمن: يجب أن يكون تصميم النظام قادراً على الحفاظ على مستوى مقبول من الوظائف والأمان حتى في ظل اختراق عدد محدود من العقد، دون انهيار كامل.
- مستويات أمنية واقعية: ينبغي أن تراعي آليات الأمن القيود الحاسوبية والطاقية للعقد، لتحقيق توازن عملي بين متطلبات الحماية وكفاءة أداء الشبكة [21].

2. اختراق المستخدم

يتضمن استهداف مستخدمي الشبكة عبر خداعهم لكشف معلومات حساسة مثل كلمات المرور أو المفاتيح المتعلقة بعقد الاستشعار.

3. اختراق العتاد

يشمل التلاعب المادي بالمكونات الصلبة لاستخراج شيفرة البرنامج والبيانات والمفاتيح المخزنة داخل العقدة. قد يحاول المهاجم أيضاً تحميل برامج ضارة على العقدة المُخترقة [21].

4. اختراق البرمجيات

يركز على استغلال الثغرات في البرامج التشغيلية أو التطبيقات التي تعمل على العقد، مثل ثغرات تجاوز سعة المخزن المؤقت، مما يسمح بالسيطرة على عمل العقدة.

5. الهجمات السلبية والهجمات النشطة

الهجمات السلبية هي هجمات لا يقوم فيها المهاجم بأي تعديل على البيانات، بل يقتصر على الاستماع غير المشروع أو مراقبة حزم البيانات المُتبادلة ضمن الشبكة. يهدف هذا النوع إلى انتهاك خصوصية البيانات دون التأثير على عملها. أما الهجمات النشطة على عكس السلبية، تشمل هذه الهجمات تعديل تدفق البيانات أو إنشاء تدفق كاذب. يقوم المهاجم هنا بالتلاعب بالبيانات أو حَقن بيانات مزيفة، مما يهدد سلامة البيانات ووظائف الشبكة [21].

6. هجمات المعلومات

في شبكات الاستشعار، تقوم العقد بمراقبة التغيرات في الوسطاء المحددة والإبلاغ عنها إلى المستقبل المركزي وفقاً للمتطلبات. أثناء إرسال التقارير، قد تتعرض البيانات المنقولة لهجمات بهدف تزويد المحطات

الأساسية أو المستقبلات بمعلومات خاطئة [21]. وتشمل هذه الهجمات:

- **التعطيل (Interruption)**

تفقد قنوات الاتصال في الشبكة الاستشعارية توافرها، مما يهدد استمرارية الخدمة. يتمحور الهدف الرئيسي حول شن هجمات حجب الخدمة، وتستهدف هذه الهجمات جميع طبقات الشبكة.

- **الاعتراض (Interception)**

يتمكن المهاجم من الوصول غير المصرح إلى العقدة أو بياناتها، كما في هجمات استيلاء العقدة. يهدد هذا النوع سرية الرسائل، ويهدف إلى التنصت على المعلومات المنقولة. غالباً ما تستهدف هذه الهجمات طبقة التطبيقات.

- **التعديل (Modification)**

يقوم طرف غير مصرح له، ليس بالوصول إلى البيانات فقط، بل بتغييرها أيضاً. مما يهدد سلامة الرسائل، ويهدف إلى تضليل الاطراف المعنية بالرسائل.

- **التزوير (Fabrication)**

يقوم المهاجم بحقن بيانات مزيفة، مما يقوض موثوقية المعلومات. يهدد هذا النوع مصداقية الرسائل، ويهدف إلى تضليل الأطراف المعنية بالرسائل. يمكن أن تساهم هذه العملية أيضاً في هجمات حجب الخدمة عبر إغراق الشبكة بالبيانات المزيفة.

- **إعادة إرسال الرسائل (Replaying)**

يهدد هذا النوع فعالية الرسائل. يتمحور هدفه الرئيسي حول تضليل الأطراف في البروتوكولات غير الحساسة لعنصر الزمن.

- **التشويش (Jamming)**

يُصنف هذا الهجوم ضمن هجمات حجب الخدمة، حيث يحاول المعتدي تعطيل عمل الشبكة عبر بث إشارات عالية الطاقة. وتنقسم هجمات التشويش في شبكات الاستشعار اللاسلكية إلى أربعة أنواع:

1. التشويش المستمر: يعمل على إتلاف الحزم أثناء إرسالها.
2. التشويش الخادع: يعني أن المهاجم يتظاهر بأنه عقدة شرعية ويقوم بإرسال حزم سليمة ولكنها مزيفة أو غير صالحة للاستخدام.
3. التشويش العشوائي: يهدف إلى ترشيد طاقة المهاجم. فهو لا يعمل باستمرار بل يبث في فترات عشوائية قصيرة تتخللها فترات توقف (سكون) مما يصعب اكتشافه.
4. التشويش التفاعلي: يبث إشارات التشويش عند استشعار وجود حركة مرورية.

4-5-3. عطل نفاد طاقة العقدة (Node Energy Exhaustion)

يحدث عطل نفاد طاقة العقدة عندما تستنفذ إحدى العقد طاقتها بالكامل، مما يؤدي إلى توقفها عن العمل وفقدان قدرتها على جمع البيانات أو نقلها إلى باقي العقد في الشبكة. يؤثر هذا العطل بشكل سلبي على أداء الشبكة ككل، خاصة إذا كانت العقدة المفقودة تشكل جزءاً أساسياً من مسار الاتصال بين العقد الأخرى.

تأثير العطل على أداء الشبكة

1. تدهور جودة الخدمة: يؤدي فقدان العقد إلى تأخير في وصول البيانات وربما فقدانها بالكامل.
2. انقطاع الاتصال: إذا كانت العقدة التي نفذت طاقتها تلعب دوراً رئيسياً في الربط بين أجزاء الشبكة، فقد يؤدي ذلك إلى تقسيم الشبكة إلى أجزاء منفصلة.
3. انخفاض عمر الشبكة: عندما تفقد الشبكة عدداً كبيراً من العقد، تصبح غير قادرة على العمل بكفاءة.

4-5-4. هجوم استنزاف طاقة العقدة (Energy Depletion Attack)

هو نوع من الهجمات التي تستهدف استهلاك طاقة عقد الاستشعار بشكل غير طبيعي، مما يؤدي إلى استنزاف البطاريات وتعطيل العقد المصابة. يمكن أن يؤدي هذا الهجوم إلى تقليل عمر الشبكة وفقدان البيانات، أو حتى انهيار الشبكة بالكامل.

- **تأثير الهجوم على الشبكة**

إن هجوم استنزاف الطاقة يؤدي إلى:

1. انخفاض عمر الشبكة بسبب نفاد طاقة العقد بسرعة.
2. زيادة فقدان البيانات نتيجة توقف العقد المستهدفة.
3. تدهور أداء الشبكة بسبب زيادة التأخير وإعادة الإرسال.
4. انقطاع الاتصال إذا تم استهداف العقد الأساسية في الشبكة.

4-6-أهمية تشخيص الأعطال في شبكات الاستشعار اللاسلكية

تعمل شبكات الاستشعار اللاسلكية في بيئات قاسية يصعب الوصول إليها. مما يؤدي حتماً مع مرور الوقت إلى تعطل هذه العُقَد أو توقفها بالكامل. وعندما لا يتم اكتشاف العُقَد المعطلة والتعامل معها بالشكل المناسب وفي الوقت المناسب، فإن النتائج السلبية تصبح حتمية، وتشمل تقليل موثوقية البيانات، استنزاف عرض النطاق الترددي للشبكة، التسبب في ازدحام مقاطع من مسارات الاتصال، وأخيرًا تقصير العمر التشغيلي للشبكة بالكامل [21]. انطلاقًا من هذه التحديات، تبرز أهمية تشخيص الأعطال كالتالي:

1. زيادة موثوقية البيانات

تتعرض العقد المستشعرة للأعطال ويفقد أداؤها المصداقية لأسباب متنوعة، تشمل عيوباً في الأجهزة أو البرمجيات، أو تأثيرات البيئة المحيطة، أو هجمات خبيثة تدفعها لتوليد بيانات مغلوطة. عند نقل هذه البيانات المعيبة إلى العقدة المُشغِّلة (SN) أو المحطة الأساسية(BS) ، فإنها تقوض دقة القرارات المتخذة. وفي سياق أنظمة الأتمتة والتحكم، يمكن لفشل العقد أن يؤدي إلى خسائر بشرية ومادية جسيمة، كما هو الحال في الشبكات المُخصصة للكشف عن تسرب الغازات السامة داخل المصانع الكيميائية. حيث يؤدي عدم تمكن الشبكة من رصد التسرب في الوقت المناسب إلى تعريض سلامة العامل للخطر [21].

2. إطالة عمر الشبكة

يُعدُّ عمر الشبكة مرتبطاً ارتباطاً مباشراً بالطاقة المتبقية في العُقد. حيث تبدأ العُقد في التعطّل بعد استهلاكها لمعظم طاقتها في تنفيذ عمليات الشبكة المختلفة ونقل البيانات. ويؤدي انخفاض شحن البطاريات إلى

تراجع جودة الاتصال بين العُقد، وعندما يصل هذا التراجع إلى حد حرج، تتوقف العُقد عن المشاركة في الشبكة، مما قد يتسبب في تجزئة الشبكة إلى أقسام منعزلة [21].

يساعد تشخيص الأعطال في تقليل نقل البيانات المعطوبة، مما يُسهم بدوره في خفض استهلاك الطاقة بشكل فعّال. كما أن تعطُّل العُقد يؤدي إلى استهلاك طاقة إضافية دون فائدة، خاصة إذا كانت العُقدة المعطّلة تؤدي دوراً توجيهاً في الشبكة، حيث قد يتسبب ذلك في حدوث حلقات توجيه (routing loops) تستنزف موارد الشبكة.

4-7-طرق تشخيص الأعطال في شبكات الاستشعار اللاسلكية

تُصنَّف منهجيات تشخيص الأعطال في ثلاثة أنواع رئيسية، بناءً على الموقع الذي يتم فيه تحديد حالة عُقْدَة المُسْتَشْعِرَة في حال كانت تعمل أو لا.

4-7-1. المنهجية المركزية (Centralized Approach)

في هذا النهج، تتحمل عقدة مركزية جغرافياً أو منطقياً مسؤولية إدارة أعطال الشبكة بأكملها. وتقوم عقدة محددة، مثل وحدة تحكم مركزية أو المحطة الأساسية، بجمع المعلومات من العقد المختلفة وتحليلها لتشخيص حالتها [21].

4-7-2. المنهجية الموزعة (Distributed Approach)

في هذا النهج، تتحول مركزية اتخاذ القرار من المحطة الأساسية إلى العقدة المستشعرة في الشبكة، حيث تُمنح كل عقدة مستشعرة القدرة على تشخيص حالتها واتخاذ القرارات المتعلقة بها بمستوى معين من الاستقلالية. يعتمد هذا الأسلوب على التعاون بين العقد المجاورة، حيث تتبادل المعلومات المحلية وتُجري الحسابات بشكل مستقل للوصول إلى تشخيص مبدئي أو نهائي حول صحتها أو صحة جيرانها [21].

4-7-3. المنهجية الهجينة (Hybrid Approach)

تجمع هذه المنهجية بين مزايا النهجين المركزي والموزع، حيث يُمنح كلاً من المحطة الأساسية والعقد العادية الحق في المشاركة في عملية اتخاذ قرار تشخيص حالة العقد ضمن الشبكة. يتم ذلك من خلال توزيع

المهام، فتقوم العقد العادية بالتشخيص المبدئي والمحلي للأعطال، بينما تتدخل المحطة الأساسية لتحليل الأعطال المعقدة أو التي تتطلب رؤية شاملة للشبكة، مما يوازن بين كفاءة الطاقة وفعالية التشخيص.

4-8-التسامح مع الأعطال في شبكات الاستشعار اللاسلكية

بعد التعرف على بعض الأعطال التي تتعرض لها شبكات الاستشعار اللاسلكية والمفاهيم الأساسية في التسامح مع الأعطال وتقنياتها وتحديد التكرار كتقنية رئيسية لتحمل الأعطال، يجدر بنا التطرق لأنواع التكرار المطبقة في شبكات الاستشعار اللاسلكية التي تتكون أساساً من العقد كمكون رئيسي [20]. يمكن توفير التكرار على النحو التالي:

4-8-1. تكرار العقد (التغطية_K)

يقوم مبدأ تكرار العقد الاستشعارية على توفير عدة طبقات من التغطية الاستشعارية للمنطقة ذاتها. يُصنف مجال الاستشعار على أنه ذو تغطية متراكبة من المستوى K عندما تكون كل نقطة ضمن هذا المجال مغطاة من قبل ما لا يقل عن K عقدة استشعارية مختلفة. في حال تعطل أي عقدة، يتوفر لكل نقطة ضمن نطاقها K−1 عقدة بديلة تقوم بمهام الاستشعار مكان العقدة المتعطلة. عند تحقيق تغطية جيدة ($K \geq 2$)، يضمن النظام:

1. دقة أعلى في القراءات.
2. موثوقية محسنة في جمع البيانات.
3. جودة خدمة مستمرة وفعالة.

4-8-2. تكرار العقد (الاتصال_K)

يشير مفهوم التوصيل في الشبكات إلى وجود مسار متصل بين أي زوج من العقد (n, n') يتكون من سلسلة عقد متجاورة حيث تكون المسافة بين أي عقدتين متتاليتين ضمن مدى الاتصال Rc. تعتبر الشبكة على أنها ذات توصيل متراكب من المستوى K عندما يتوفر بين أي عقدتين u وv عدد K من المسارات المنفصلة [20]. عند تحقيق توصيل بمستوى $K \geq 2$، يضمن للشبكة استمرار عملها حتى في حال:

1- تعطل أي عقدة فردية.

2- انقطاع أي وصلة اتصال بين العقد.

تتناسب قدرة المرونة في الشبكة طردياً مع قيمة K، حيث أن ارتفاع مستوى التوصيل المتراكب يؤدي إلى:

1- زيادة مسارات التوجيه البديلة.

2- تعزيز موثوقية الشبكة.

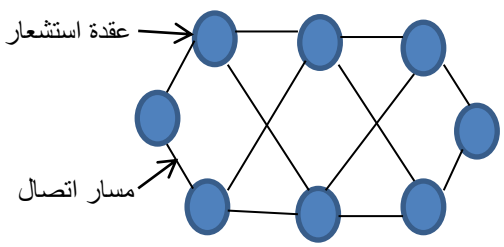
3- تحسين قدرة النظام على تحمل الأعطال.

4-8-3. تكرار التوجيه

يُعد استخدام المسارات المتعددة أسلوباً فعالاً لتحقيق توازن الحمل في الشبكة وتعزيز موثوقية إرسال البيانات من خلال توفير تكرار في مسارات التوجيه. وفي هذا السياق، يمكن تصنيف منهجيات توجيه المسارات المتعددة إلى ثلاثة أنواع رئيسية:

1. **التوجيه الشبكي متعدد المسارات (الشبكة المتشابكة)**

في هذا النهج، تقوم عقدة الاستشعار بتوجيه حزمة البيانات إلى عدة عقد مجاورة، طالما أن إجمالي الطاقة المستهلكة لا يزال ضمن الميزانية المخصصة. يتم تحديد عدد العقد المجاورة التي تُرسل إليها الحزم مسبقاً وبشكل ثابت. من مميزات هذا النهج الموثوقية الأعلى نظراً لوجود مسارات متعددة لتدفق البيانات، وملاءمة للشبكات الكثيفة حيث يتوفر عدد كبير من العقد المجاورة، والمرونة في مواجهة الأعطال حيث يستمر عمل الشبكة حتى مع تعطل بعض العقد يوضح الشكل (4-1) تمثيلاً للشبكة المتشابكة. أما التحديات التي تواجه هذا النهج هي زيادة محتملة في التأخير بسبب تعدد مسارات الإرسال، واستهلاك طاقة أعلى نتيجة الإرسال المتعدد. يُعد هذا النهج أمثل للبيئات التي تتطلب درجة عالية من الموثوقية، حتى لو كان ذلك على حساب بعض التأخير في إيصال البيانات [20].



الشكل (4-1)الشبكة المتشابكة

2. المسارات المنفصلة

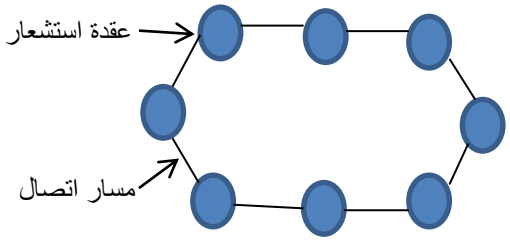
تعتمد هذه التقنية على إنشاء مسارات مستقلة بين المصدر والمستقبل، بحيث لا تتشارك هذه المسارات في أي عقدة وسيطة. يتكون النظام من مسار رئيسي واحد أو أكثر يوضح الشكل (4–2) تمثيلاً بسيطاً للمسارات المنفصلة. يتميز هذا النهج بما يأتي:

- تأخير أقل مقارنة بالنهج الشبكي.
- كفاءة في استهلاك الطاقة.

أما عيوبه فتكمن فيما يلي:

- موثوقية أقل من النموذج الشبكي.
- وجود نقاط فشل حرجة في كل مسار.
- أي عطل في عقدة وسيطة يؤدي لانقطاع المسار بالكامل.

تُستخدم هذه التقنية عندما تكون سرعة نقل البيانات أولوية تفوق متطلبات الموثوقية القصوى.



الشكل (4-2)المسارات المنفصلة

3. المسارات المُجدّلة (Braided Multipath)

يتميز هذا النموذج بتصميم يشبه الضفيرة حيث يتم إنشاء مسارات بديلة متشابكة حول المسار الرئيسي. من أجل كل عقدة في المسار الرئيسي، يتم إنشاء مسار بديل لا يمر عبر تلك العقدة تحديداً. يتميز هذا النموذج بما يلي:

1. تكلفة تشغيلية منخفضة أي لا يضيف عبئاً كبيراً على الشبكة.
2. لا يؤثر سلباً على زمن الانتقال في المسار الرئيسي في حال تعطل عقدة واحدة أو قليل من العقد. لكن عند تعطل المسار الرئيسي بالكامل، يلزم اكتشاف مسار جديد.

3. يركز هذا الأسلوب على نقل البيانات عبر المسار الرئيسي مع الحفاظ على عدد محدود من المسارات البديلة الجاهزة، مما يوفر توازناً أمثلاً بين الكفاءة والموثوقية.

4-9-تقنيات منع الأعطال في شبكات الاستشعار اللاسلكية

تمثل تقنيات منع الأعطال نهجاً استباقياً مختلفاً عن مفهوم التسامح مع الأعطال، حيث يركز على منع حدوث الأعطال أساساً بدلاً من التعامل معها بعد وقوعها. وتلعب المراقبة المستمرة دوراً محورياً في هذا النهج. حيث تتم مراقبة الشبكة عن طريق المحطة الأساسية أو عن طريق المراقبة الذاتية التعاونية فيتم كشف أي سلوك غير طبيعي في الشبكة ومعالجته قبل أن يتسبب في المزيد من الأضرار. نذكر فيما يأتي بعض ما يتم مراقبته في شبكات الاستشعار اللاسلكية [20].

1. مراقبة حالة العقدة

تشمل مراقبة حالة العقد، تتبع الحالة الفيزيائية لها من أجل الكشف عن العقد التالفة أو المعطلة [5]. كما تتضمن مراقبة الموارد الحرجة وأبرزها الطاقة المتبقية، تجدر الإشارة إلى أن موثوقية الشبكة والتنبؤ بسلوكها تعد شكلاً من أشكال إدارة الطاقة والتنبؤ بها.

تمكّن أنظمة إدارة الطاقة والتنبؤ بحالة العقدة من رصد السلوك الديناميكي للشبكة بشكل فعال، مما يسهم في التنبؤ بالأعطال الشبكية واتخاذ الإجراءات الوقائية المناسبة. وبذلك يمكن الحفاظ على موثوقية الشبكة في بيئات شبكات الاستشعار الديناميكية.

2. مراقبة الازدحام الشبكي

يحدث ازدحام الشبكة عندما تصل كمية البيانات المنقولة عبر وصلة أو عقدة إلى حد يؤدي إلى تدهور جودة الخدمة، مما ينتج عنه تأخير أو فقدان للحزم أو انقطاع في الاتصالات الجديدة. من أجل التحكم في الازدحام يوجد تقنيات متعددة، منها نظام الكشف عن الازدحام وتجنبه في شبكات الاستشعار اللاسلكية CODA (Congestion Detection and Avoidance) وهو نظام فعال في استهلاك الطاقة يعتمد على ثلاث آليات رئيسية:

1. كشف الازدحام من خلال أخذ عينات دورية من حمل القناة المحلية بمعدل مناسب للتقدير الدقيق لحالة الازدحام.
2. عند اكتشاف الازدحام، ترسل العقد إشارات إلى جيرانها.
3. تنظيم تدفق البيانات من مصادر متعددة.

4-10- خلاصة الفصل

عرضنا في هذا الفصل المفاهيم الأساسية للأعطال والتسامح معها، واستعرضنا طرق تعزيز موثوقية الأنظمة. ثم ركزنا على أعطال شبكات الاستشعار اللاسلكية، بأنواعها الأمنية والموقَّتة والدائمة. بعد ذلك، ناقشنا أهمية وآليات تشخيص الأعطال في هذه الشبكات. اخيراً عرضنا تقنيات التسامح مع الأعطال واستراتيجيات منع العطل لضمان استمرارية العمل.

5 نمذجة شبكات الاستشعار اللاسلكية باستخدام البيان

5-1-مقدمة

تعرفنا سابقاً أن الطاقة من الموارد المحدودة في شبكات الاستشعار اللاسلكية، والتي لها أثر كبير على أداء هذه الشبكات وفترة حياة الشبكة من الخصائص الأساسية الواجب تحسينها من خلال ضمان استهلاك الطاقة في عقد الاستشعار. كما هو معلوم تعتبر الشبكة مثالاً واضحاً على البيان وإن عملية دمج نظرية البيان مع الشبكات قضية مهمة في مجال البحث العلمي.

لا تنشأ جميع الشبكات بشكل منظم فبعض الشبكات يمكن أن تنشأ بشكل عفوي وتتطور بشكل تدريجي عبر الوقت، وهذا ما أدى إلى تعريف البيان العشوائي الذي تطرقنا له في الفصل الأول.

قمنا في هذا الفصل باقتراح نموذج جديد لبناء شبكات الاستشعار اللاسلكية التي تنشر عشوائياً. وسنتعرف عليه ونعرض محاكاته في بيئة الماتلاب وندرس تعقيده الزمني.

5-2-الدراسات السابقة

نظراً لأهمية نظرية البيان في نمذجة العلاقات بين الكائنات وقدرتها على تمثيل العديد من مشاكل العالم الحقيقي، أصبحت أداةً مهمة في نمذجة العديد من التطبيقات. ونظراً لأهمية شبكات الاستشعار اللاسلكي وتطبيقاتها في الكثير من مجالات الحياة توجه العديد من الباحثين لدراسة استخدام البيان في شبكات الاستشعار اللاسلكية في [22] تطرق البحث إلى مشكلة موازنة الحمل في شبكات الاستشعار اللاسلكية. هي عبارة عن طريقة لنقل الحمل من العقدة المحملة بشكل كبير إلى عقدة محملة بشكل أقل. تم تقديم نهج باستخدام نظرية البيان لموازنة الحمل من أجل تعظيم الأداء وذلك بالاعتماد على مصفوفة لابلاس للبيان. أما في [23] فقد تم اقتراح مخطط جديد لإدارة معدل استهلاك الطاقة لأجهزة الاستشعار اللاسلكية، يعتمد بشكل كبير على نظرية البيان في أدارة معدل استهلاك الطاقة المناسب. تمكن هذه التقنية عقد الاستشعار من الانتظار في وضع السكون حتى الحصول على معلومات تحكم جديدة والانتقال من موقع إلى آخر تحت منطقة التغطية الراديوية. وضمت

النتائج التجريبية أن النظام المقترح في نظرية البيان يمتلك نتائج مقبولة في خفض كمية الطاقة المستهلكة لأجهزة الاستشعار حيث يعتمد على تحديد أفضل مسار بين المصدر والوجهة. لكن ما يواجه تلك الأبحاث من ثغرات هي أنه لا يمكن تطبيقها على الشبكات المنشورة عشوائياً، حيث يفترض الباحث معرفة توزيع العقد في الشبكة والتوصيلات التي تتم بين العقد وعدم وجود العشوائية في التوزيع. لذلك توجه بعض الباحثين إلى دراسة البيان العشوائي وعلاقته مع الشبكات. أظهر الباحثين في [24] أن البيانات الهندسية العشوائية يمكن أن تستخدم للحصول على تمثيل للشبكات اللاسلكية. كان الهدف من هذه الورقة [24] هو إنشاء علاقة رياضية بين عدد العقد ومساحة النشر لضمان درجة اتصال معينة. تمثل المنهجية المقترحة حلاً سريعاً لاختيار كمية العقد التي يجب نشرها على السطح. على الرغم من أهميتها في مرحلة التخطيط الأولي للشبكة إلا أنها لا تعالج خصائص جوهرية لشبكات الاستشعار مثل استهلاك الطاقة والأعطال. أما في [25] تمت مناقشة خصائص الاتصال والتغطية لشبكات الاستشعار اللاسلكية غير المتجانسة بناء على نموذج البيان العشوائي الهندسي الذي يعتمد على أن العقد قادرة على الحركة والتنقل ويستخدم مفهوم السيطرة على المجموعة في نظرية البيان للاتصال. لكن من عيوب هذا البحث هو أنه تطرق إلى مشكلة التغطية والاتصال دون النظر في طاقة الشبكة ضمن هذا النموذج. ما سنقوم به هو ضمان كفاءة استهلاك الطاقة ضمن الشبكة من خلال نمذجة شبكات الاستشعار اللاسلكية المنشورة عشوائياً وغير المتجانسة بالنسبة لنطاق الإرسال والطاقة، باستخدام البيان الهندسي العشوائي وضمان إرسال العقدة لبياناتها(Data) للمحطة الأساسية من خلال أفضل المسارات.

5-3-النموذج المقترح

في إطار السعي لتطوير أداء شبكات الاستشعار اللاسلكية، نقدم في هذا الفصل نموذجاً رياضياً متقدماً يسعى إلى تحقيق هدفين رئيسيين يتمثلان في تحقيق تقليل استهلاك الطاقة إلى أقل حد ممكن، بالإضافة إلى تحديد المسارات المثلى لنقل حزم البيانات بين العقد المختلفة داخل الشبكة. يفترض النموذج أن عدد n من عقد الاستشعار يتم نشرها وتوزيعها بشكل عشوائي في حيز مكاني، مع تخصيص رقم تعريف فريد لكل عقدة على حدة. كما يتم تحديد موقع المحطة الأساسية بشكل ثابت ومعلوم مسبقاً ضمن هذا النطاق، وتتميز عقد الشبكة

بعد عملية النشر العشوائي، بأنها غير متجانسة حيث تختلف فيما بينها من حيث نطاق الإرسال الخاص بكل منها ومستوى الطاقة المتاح لديها.

يرتكز الهيكل الأساسي للنموذج المقترح على الإطار النظري للبيان العشوائي الهندسي، حيث يُعرف النموذج على النحو التالي: ليكن بياناً هندسياً عشوائياً $G(V,r_i)$، تمثل V فيه مجموعة جميع عقد الاستشعار في الشبكة، بينما يمثل r_i نصف قطر أو نطاق الإرسال الخاص بالعقدة i. يتم تمثيل هذا البيان العشوائي الهندسي في فضاء إحداثي ثنائي الأبعاد.

5-3-1. مرحلة التخطيط

r_{eff} قيمة تمثل القدرة الاتصالية العامة للشبكة:

$$r_{eff} = \sqrt{\frac{1}{n}\sum_{i=1}^{n} {r_i}^2}$$

نشر العقد عشوائياً في المساحة A نحسب: $r_c = \sqrt{\frac{\ln n}{\pi n}}\sqrt{A}$ إذا تحقق:

$$r_{eff} \geq r_c$$

فإن الشبكة قابلة للاتصال وإلا نزيد من كثافة العقد.

لنفترض أن المتجهة $X_i=(x_i,y_i)$ تمثل موقع وإحداثيات العقدة i في هذا الفضاء الثنائي، وبالمثل، فإن المتجهة $X_j = (x_j, y_j)$ تمثل الإحداثيات المقابلة للعقدة j. بناءً على ذلك، يتم تعريف وجود ضلع أو رابط اتصال مباشر بين العقدتين i و j وفقاً للعلاقة الرياضية التالية:

$$f(X_{ij}) = \begin{cases} 1 & \|X_i - X_j\| \leq r_i \\ 0 & \|X_i - X_j\| > r_i \end{cases} \quad \text{.....(1)}$$

بمعنى آخر، يتوقف اكتمال الرابط على تحقيق شرط اتصال محدد يعتمد على المواقع النسبية للعقدتين ومقادير نطاقات الإرسال الخاصة بكل منهما.

يأتي هذا النموذج لمعالجة التحديات الكامنة في الطبيعة الديناميكية والعشوائية لشبكات الاستشعار، سعياً لتعظيم العمر الافتراضي للشبكة وضمان موثوقية نقل البيانات من خلال مسارات فعالة من حيث استهلاك الطاقة.

سنعمل على تقسيم النموذج المقترح إلى ثلاثة نماذج جزئية نوضح كل منها بخطوات مرتبة. كما هو موضح في الفقرات اللاحقة.

5-3-2. النموذج الجزئي لبناء شبكة هرمية متعددة المستويات

بناءً على نطاق الإرسال نوضح النموذج في الخطوات الآتية:

الخطوة الأولى: تهيئة المستوى الصفري (المحطة الأساسية).

- تعتبر المحطة الأساسية k أعلى نقطة في التسلسل الهرمي (وتكون في المستوى 0).

الخطوة الثانية: إنشاء المستوى الأول.

- يتم تحديد مجموعة العقد i التي تقع ضمن نطاق الإرسال المباشر $f(X_{ik})$ للمحطة الأساسية k.
- تُشكل هذه المجموعة المستوى الأول L_1 للشبكة.
- يتم إنشاء رابط اتصال مباشر بين كل عقدة $i \in L_1$ والمحطة الأساسية k.

الخطوة الثالثة: إنشاء المستويات اللاحقة (مستوى تلو الآخر).

- من أجل كل عقدة i في المستوى الحالي L_m حيث $(m > 1)$ نقوم بما يلي:
- تُعتبر العقدة i عقدة مركزية مؤقتة للمرحلة الحالية.
- يتم تحديد مجموعة العقد j التي تستوفي الشرطين التاليين:
  1. تقع العقدة j ضمن نطاق الإرسال $f(X_{ij})$ للعقدة i.
  2. J لا تقع في مستوى i.
- يتم تعيين جميع العقد j التي تم ربطها من خلال عقد L_m إلى المستوى التالي L_{m+1}.
- تتكرر هذه العملية بشكل تسلسلي حتى لا تتبقى أي عقدة في الشبكة بدون مستوى مخصص لها.

الخطوة الرابعة: تمثيل الهيكل من خلال مصفوفة المستويات

لتمثيل الهيكل الهرمي رياضياً، ننشئ مصفوفة تسمى مصفوفة المستويات M (Levels Matrix)، وتعرف كالتالي:

- الأسطر: يمثل كل سطر رقم المستوى m على سبيل المثال السطر 1 للمستوى L_1، السطر 2 للمستوى L_2 وهكذا.
- الأعمدة: تمثل الأعمدة في كل سطر أرقام أو معرفات العقد التي تنتمي إلى ذلك المستوى.
- قيم المصفوفة 1 إذا كانت العقدة ضمن المستوى و0 إذا لم تكن العقدة ضمن المستوى.

مثال توضيحي (5-1)

لنفترض شبكة نهائية مكونة من 6 عقد بالإضافة إلى المحطة الأساسية k، وتم بناء 3 مستويات للشبكة. لنفترض أن الطاقة الأولية لكل عقدة (Energy) معروفة. بناءً على الخوارزمية والترتيب المعياري، تكون مصفوفة المستويات M كالتالي:

$$\begin{bmatrix} 0 & 0 & 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 \end{bmatrix}$$

- المستوى L_1 السطر الأول يحتوي على العقدتين 6 و3.
- المستوى L_2 السطر الثاني يحتوي على العقد 1,2. وكذلك الأمر بالنسبة للمستوى الثالث.

5-3-3. النموذج الجزئي لحساب الأوزان التراكمية

الوزن التراكمي هو مجموع أوزان الأضلاع على المسار من العقدة إلى المحطة الأساسية. وفقاً للهيكل الهرمي المنشأ في الشبكة متعددة المستويات، يهدف النموذج إلى حساب الوزن التراكمي (Cumulative Weight) أو تكلفة المسار (Path Cost) من كل عقدة في الشبكة باتجاه المحطة الأساسية، مع الأخذ بالاعتبار المسار الأكثر كفاءة عبر التسلسل الهرمي. نوضح النموذج من خلال الخطوات الآتية:

الخطوة الأولى: وزن الأضلاع في المستوى الأول.

- لكل عقدة i في المستوى الأول L_1 تملك ضلع مباشر يربطها بالمحطة الأساسية k. الوزن التراكمي للعقدة i يساوي ببساطة المسافة بين العقدة والمحطة الاساسية ونرمز له بالرمز Wc(i).

الخطوة الثانية: وزن الأضلاع في المستوى الثاني.

- لكل عقدة j في المستوى الثاني L_2 ضلع يربطها بعقدة i في المستوى الأول L_1 وفقاً لهيكل المستويات.

الوزن التراكمي للعقدة j يُحسب كمجموع:

1. المسافة W(j,i) بين العقدة j والعقدة i.
2. الوزن التراكمي Wc(i) للعقدة i.

$$Wc(j) = W(j,i) + Wc(i)$$

يُحمل الضلع الذي يربط i بالعقدة j بالوزن التراكمي Wc(j).

الخطوة الثالثة: وزن الأضلاع في المستوى الثالث L_3 والمستويات الأعلى.

- لكل عقدة v في المستوى L_m (حيث $m \geq 3$) ضلع يربطها بعقدة j من المستوى L_{m-1}. الوزن التراكمي Wc(v) للعقدة v يُحسب كمجموع:

1. المسافة W(v, j) بين العقدة v والعقدة j.
2. أقل وزن تراكمي بين الأضلاع المرتبطة بالعقدة j لان العقدة j قد تكون مرتبطة بعدة عقد في المستوى L_{m-2}. نأخذ أقل وزن تراكمي من بين هذه الارتباطات. وليكن Wc(v) عندها:

$$Wc(v) = w(v, j)+Wc(j)$$

يُحمل الضلع (v, j) بالوزن التراكمي Wc(v).

5-3-4. التمثيل البياني والاستنتاج

يتم رسم البيان حيث تمثل رؤوسه عقد الاستشعار وتمثل أضلاعه الاتصالات بين تلك العقد.

- يحمل كل ضلع في البيان الوزن التراكمي كما هو موضح في اعلاه.
- يمثل هذا الوزن التراكمي للضلع، أقل تكلفة مسار معروفة من العقدة إلى المحطة الأساسية ضمن قيود الهيكل الهرمي الحالي.

يتم حساب تكلفة المسار الأمثل لكل عقدة بناءً على المسار الذي يحمل أقل وزن تراكمي.

5-3-5. نموذج إدارة استهلاك الطاقة وتحسين متانة الشبكة

يهدف هذا النموذج إلى تقييم جدوى الطاقة لكل عقدة في الشبكة بناءً على عبء العمل التوجيهي الموكَل إليها، واتخاذ الإجراءات الصحيحة لضمان استدامة عمل الشبكة ومنع انهيار العقد بسبب استنفاد الطاقة. نفرض أن E_j هي طاقة العقدة الأولية وترمز المعادلة 2 إلى تقدير استهلاك الطاقة لأي عقدة بناءً على إجمالي البيانات التي ترسلها وتستقبلها من وإلى جميع العقد المتصلة بها مباشرةً.

$$T(j) = \sum_{i=1}^{n} \varepsilon_{jiq} * N_{jiq} + \varepsilon_{jir} * N_{jir} \quad \text{.....(2)}$$

ε_{jiq} :هو مقدار الطاقة المستهلكة إذا مرت رسالة رد واحده عبر المستشعر j.

ε_{jir} :هو مقدار الطاقة المستهلكة إذا مرت رسالة استعلام واحده عبر المستشعر j.

N_{jiq} :عدد رسائل الاستعلام التي تمر عبر المستشعر j إلى المستشعر i.

N_{jir} :عدد رسائل الرد التي تمر عبر المستشعر j إلى المستشعر i.

آلية تقييم حالة الطاقة واتخاذ القرار

يتم حساب صافي الطاقة المتبقية ET للعقدة j بعد أداء مهام التوجيه كالتالي:

$$ET(j) = E(j) - T(j)$$

بناءً على الناتج يتم تصنيف حالة العقدة j واتخاذ الإجراء المناسب:

1. الحالة الأولى$ET(j) < 0$: حالة تجاوز السعة.

- التشخيص: أي استهلاك الطاقة $T(j)$ فاق الطاقة الأولية $E(j)$، مما يشير إلى أن العقدة j مثقلة بعدد كبير جداً من الارتباطات(المهام).
- الإجراء: يجب تقليل العبء عن العقدة j. يتم ذلك عن طريق تقليل عدد العقد التابعة (المرتبطة بالعقدة) التي توجّه حركة مرورها عبر j.

2. الحالة الثانية $ET(j) > 0$: الحالة المستقرة.

- التشخيص: الطاقة الأولية كافية لتغطية الاستهلاك الحالي.
- الإجراء: الحفاظ على هيكل الارتباطات الحالي للعقدة j ، حيث أنها تعمل ضمن حدود طاقتها.

3. الحالة الثالثة $ET(j) = 0$: الحالة الحرجة (الحدية).

- التشخيص: استهلكت العقدة كل طاقتها الأولية بالضبط. وهي على حافة التوقف عن العمل.
- الإجراء: تطبيق سياسة وقائية تتضمن حذف أحد ارتباطات العقدة j (على الأقل) لتقليل $T(j)$ ومنحها هامش طاقة إضافي لتجنب الفشل الكامل.

آلية تحديد عدد الارتباطات المراد إلغاؤها

في حالتي الحذف (الحالة الأولى والثالثة)، يتم حساب عدد الارتباطات الزائدة أو الحرجة التي يجب إلغاؤها من العقدة j باستخدام العلاقة التالية:

$$l = \frac{T(j)}{s} \quad .....(3)$$

حيث l هي الطاقة التي تستهلكها العقدة j، و s هو عدد العقد التي ترتبط مع العقدة j. نحدد m عدد العقد التي يمكن لـ j تحملها $m = \frac{E(j)}{l}$. بعد ذلك نقوم بعملية حذف العقد الفائضة من العقدة j والتي عددها $Hj=s-m$. تتم عملية الحذف كما يلي:

1. نبدأ من المستوى الأخير وليكن y.

2. نأخذ أول عقدة من المستوى y من مصفوفة المستوى ولتكن e نحذف He من ارتباطاتها مع العقد من المستوى الأقل.

3. يتم أولاً حذف العقد التي ترتبط مع e وأضلاعها موزونة بأكبر مقدار من المسافة مع e.

4. عند تساوي المسافة بين عقدتين والعقدة e نقوم بحذف العقدة ذات الطاقة الأقل ذلك بالاعتماد على مصفوفة المستوى نتبع نفس الطريقة لكل عقد المستوى.

5. ننتقل للمستوى الذي يليه نبدأ بأول عقدة من المستوى نحافظ على ارتباطها مع العقد في المستوى الأعلى، نتبع نفس الطريقة للحذف من المستوى الأقل.

6. نكرر الخطوات السابقة لكل المستويات ماعدا المستوى الأول فلا نحذف ارتباط أي عقدة مع المحطة الأساسية، لذلك عند نشر العقد نحاول جاهداً أن يتم نشر العقد ذات الطاقة الاعلى عند المحطة الاساسية.
7. بعد الانتهاء من عملية الحذف نشكل مصفوفة التجاور للبيان.
8. نقوم بوزن العقد بنسبة الطاقة المتبقية لها وفق العلاقة:

$$L(j) = \frac{E(j) - \sum_{i=1}^{m} \varepsilon_{jiq} * N_{jiq} + \varepsilon_{jir} * N_{jir}}{E(j)} \dots\dots\dots (4)$$

يعمل هذا النموذج على تحويل شبكة عشوائية إلى هيكل هرمي مستقر ، حيث:

1. يتم الحفاظ على العقد ذات الطاقة المرتفعة والتي تقع في مواقع حساسة (مثل المستوى الأول).
2. يتم إزالة المسارات الأقل كفاءة (الأطول مسافة) والأكثر استهلاكًا للطاقة.
3. يتم توزيع الحمل بشكل متوازن بين العقد، مما يطيل من عمر الشبكة الكلي.

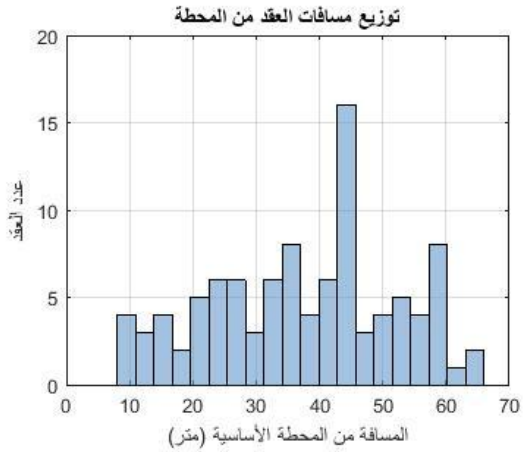
يمثل الناتج النهائي لمصفوفة التجاور وقيم L(j) للبيان الأمثل الذي يحقق أفضل توازن بين استهلاك الطاقة وكفاءة المسار نحو المحطة الأساسية.

5-3-6. محاكاة النموذج المقترح

تم أجراء محاكاة شاملة للنموذج الرياضي ويهدف إلى تحقيق تقليل استهلاك الطاقة إلى أدنى حد ممكن، وأطالة عمر الشبكة. استخدمنا بيئة MATLAB 2015 لتنفيذ المحاكاة على شبكة مكونة من 100 عقدة استشعار موزعة في مساحة $1000m^2$. فتصميم الشبكة كان كما يلي:

1. عدد العقد: 100 عقدة استشعار بالإضافة للمحطة الأساسية.
2. نطاق الإرسال: تتراوح بين 35-75 متر حسب بعد العقدة عن المحطة.
3. الطاقة الأولية: متنوعة حسب نوع العقد.

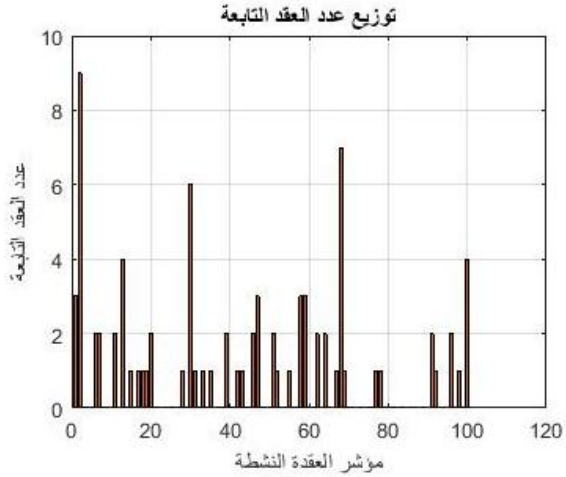
أما الرسوم التوضيحية للمحاكاة فأولاً تتوزع العقد تبعاً لبعدها عن المحطة الأساسية يظهر الشكل (5–1) توزيع المسافات بين العقد والمحطة الأساسية. يمثل المحور الأفقي فئات المسافات بالمتر ويمثل المحور العامودي عدد العقد في كل فئة.



الشكل (5-1) توزيع مسافات العقد من المحطة

يظهر أن 20% من العقد تقع ضمن مسافة 0–20 متر من المحطة و 35% من العقد في مدى 20–40 متر و40% في مدى 40–60 متر و5% فقط في مدى 60–70 متر. هذا التوزيع يتوافق مع نصف القطر الفعال.

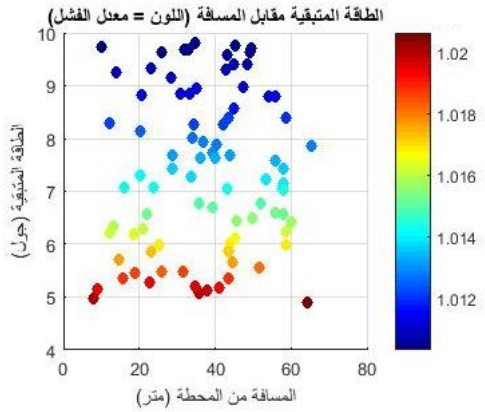
ثانياً يوضح الشكل (5–2) توزيع عبء العمل على العقد المختلفة. يمثل المحور الأفقي مؤشر العقد النشطة(رقم العقد في الهيكل الهرمي)، ويمثل المحور العامودي عدد العقد التي لديها هذا العدد من التابعين.



الشكل (5-2) توزيع عدد العقد التابعة

نلاحظ أن معظم العقد (حوالي 70%) لديها 1–3 عقد تابعة فقط وحوالي 20% من العقد لديها 4–6 عقد تابعة و10% فقط من العقد (العقد المركزية) لديها 7–10 عقد تابعة.

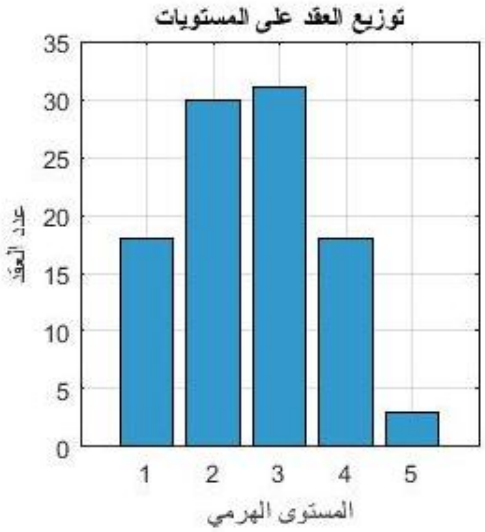
ثالثاً يظهر الشكل (5–3) مخططاً مبعثراً للطاقة المتبقية مقابل المسافة. يمثل المحور الأفقي المسافة من المحطة الأساسية بالمتر ويمثل المحور العامودي الطاقة المتبقية (كنسبة مئوية من الطاقة الأولية).



الشكل (5-3) الطاقة المتبقية مقابل المسافة

تمثل النقاط الزرقاء العقد المستقرة والنقاط الصفراء العقد الحرجة والنقاط الحمراء العقد التي تجاوزت السعة.

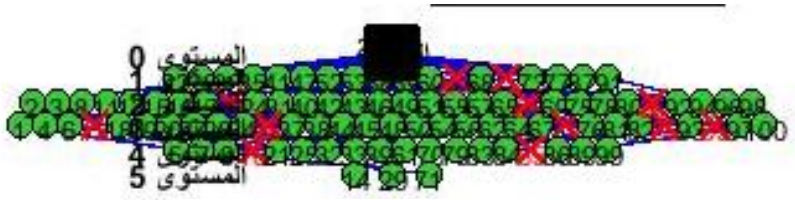
رابعاً يظهر الشكل (5–4) المخطط الشريطي للتوزيع الهرمي



الشكل (5-4) توزيع العقد على المستويات

نلاحظ أن المستويات الوسطى (المستوى 2 و3) تحتوي على أكبر عدد من العقد، وهو ما يتوافق مع التوزيع العشوائي للعقد في الفضاء ثنائي الأبعاد. المستوى الأول يحتوي على عدد محدود من العقد (10–20 عقدة فقط)، بسبب محدودية نطاق إرسال المحطة الأساسية المستويات العليا (4 فما فوق) تحتوي على عدد أقل من العقد، مما يعكس التوزيع التدريجي الطبيعي.

خامساً يوضح الشكل (5–5) الهيكل الهرمي للشبكة.



الشكل (5-5) الهيكل الهرمي للشبكة

المستوى 0 المحطة الأساسية (المربع الأسود) والمستوى 1 العقد المتصلة مباشرة بالمحطة (5 عقد تقريباً) والمستوى 2 العقد المتصلة بعقد المستوى الأول (10–15 عقدة) والمستوى 3–5 توزيع هرمي منتظم يضمن تغطية كاملة للمنطقة.

5–3–7. كفاءة النموذج المقترح

إن أهمية استخدام البيان العشوائي لنمذجة شبكات الاستشعار اللاسلكية تكمن في توفير فهم أعمق لتصميم هذه الشبكات وتحليل أدائها. وقد اخترنا النمذجة باستخدام البيان العشوائي الهندسي بشكل خاص لأنه لكونه نموذجاً مؤثراً وشاملا للشبكات، كما أنه يتيح لنا الحصول على نتائج دقيقة من خلال ضمان اتصال العقد ضمن نطاق إرسالها فتكون على الرغم من عشوائية النشر للعقد إلا أننا قمنا بجعل العقد ترسل بياناتها ضمن مسارات محدده. ولما كان لبرنامج الماتلاب قوة في تحليل البيانات وتصور النتائج بشكل بصري استخدمناه كأداة لمحاكاة النموذج المقترح حيث يوفر منهجية واضحة لتقديم وتحليل النتائج.

5–3–8. المقارنة وتقييم فعالية اختيار البيان العشوائي الهندسي للنمذجة

سنقدم فيما يلي مقارنة بين النموذج المقترح من حيث نمذجة شبكات الاستشعار باستخدام البيان الهندسي والبيان العشوائي والبيان العادي.

1. النمذجة بالبيان العشوائي

تتميز النمذجة باستخدام البيان العشوائي بالبساطة، حيث يتم توصيل العقد بشكل عشوائي باحتمال ثابت p، دون اعتبار للموقع الجغرافي. يعد البيان العشوائي ملائم لنمذجة الشبكات حيث يكون الاتصال معتمداً

على عوامل غير المسافة (كشبكات التواصل الاجتماعي). لذلك، هو أقل ملاءمة للتطبيق المطلوب رغم أنه يعالج العشوائية. لكن من ناحية استخدمه لنمذجة شبكات الاستشعار اللاسلكية فهو أقل واقعية من النموذج الهندسي العشوائي ، لأنه لا يأخذ المسافة المادية بعين الاعتبار، وهو عامل حاسم في الاتصال اللاسلكي.

2. النمذجة بالبيان العادي

تتميز النمذجة باستخدام البيان العادي بافتراض معرفة كاملة بتوزيع العقد والاتصالات بينها. لكن استخدام البيان العادي غير قابل للتطبيق على الشبكات المنشورة عشوائياً في العالم الحقيقي، وهي الثغرة الرئيسية التي سلط النص عليها الضوء. حيث يفترض وجود بيئة مثالية ومتحكم بها، مما يجعله الأقل واقعية من بين الخيارات للتطبيقات العملية لشبكات الاستشعار.

3. النمذجة المقترحة

يعتبر النموذج المقترح الأفضل حيث يجمع بين المزايا الرئيسية للبيان العادي والبيان العشوائي. فهو يتميز بنمذجة التوزيع العشوائي للعقد في الفراغ (مثل توزيع أجهزة الاستشعار في حقل بشكل عشوائي). كما يأخذ بعين الاعتبار نطاق الإرسال الثابت، حيث تتصل عقدتان إذا كانت المسافة بينهما أقل من نصف قطر اتصال معين، مما يجعله الأكثر واقعية في تمثيل شبكات الاستشعار اللاسلكية الفعلية. يوضح الجدول(5−1) المقارنة بين النماذج.

نوع النموذج	الواقعية في التمثيل	معالجة العشوائية	ملاءمة لشبكات الاستشعار
البيان الهندسي العشوائي	عالية جداً	يعالج	مثالي
البيان العشوائي	متوسطة إلى منخفضة	يعالج	ضعيف
البيان العادي	منخفضة جداً	لا يعالج	غير ملائم

الجدول (5-1) مقارنة بين البيانات

5-3-9. التعقيد الزمني للنموذج المقترح

سندرس الآن التعقيد الزمني للنموذج المقترح، بفرض أننا سنقوم بنشر n عقدة الاستشعار. بعد نشر هذه العقد يطلب من المستخدم تزويد النموذج المقترح بموقع العقدة ونطاق إرسالها بالتالي نحتاج إلى حلقة تكرارية لإدخال النطاق الترددي للعقد وتخزينه ضمن متجهة من البعد n ومنه نحتاج إلى n تكرار تكون كلفة الحلقة كحد أعلى هي n أما نطاق إرسال العقدة فنحتاج إلى تكراريين الأول يدخل فواصل النقاط والأخر يدخل التراتيب ويتم تخزين المعلومات ضمن مصفوفة فتكون التكلفة كحد أعلى هي n^2 بالتالي $T_1=O(n^2)+O(n)=O(n^2)$ حيث O هو الحد الأعلى. ربط العقد وترتيبها ضمن مستويات بالإضافة إلى ترتيب العقد ضمن مصفوفة المستويات يتطلب حلقة تكرارية ضمنها فتكون الكلفة كحد أعلى n^2 ومن ثم نحتاج إلى ترتيب العقد فتكون الكلفة كحد أعلى هي $nlog_2n$ ومنة التعقيد الزمني للمرحلة $T_2=O(n^2)+O(nlog_2n)$. وزن الأضلاع يتطلب بالتالي التعقيد الزمني $T_3=O(n^2)$. أما الكلفة عندما ما نقوم بحساب استهلاك الطاقة في العقد ثم حذف العقد الواجب حذفها (كما هو موضح في النموذج) هو $T_4=O(n)$. وبالتالي فإن الكلفة الكلية هي:

$$T_1+T_2+T_3+T_4=O(n^2)+O(nlog_2n)+O(n^2)+O(n)=O(n^2).....(5)$$

5-4-خلاصة الفصل

قدمنا في هذا الفصل نموذجاً رياضياً للحد من استهلاك الطاقة لشبكات الاستشعار اللاسلكية المنشورة بشكل عشوائي وغير المتجانسة بالنسبة لنطاق الإرسال والطاقة. استخدمنا في عملية النمذجة مفهوم البيان العشوائي الهندسي بالإضافة لبعض المعادلات الرياضية. يعد النموذج المقترح فعالاً من ناحية التعقيد الزمني لعملية بناء الشبكة $O(n^2)$. كما أثبتنا فعاليته وكفاءته في الحد من استهلاك طاقة العقد من خلال محاكاة رياضية للنموذج المقترح باستخدام تطبيق الماتلاب. اختتمنا الفصل بمقارنة بين استخدام البيان الهندسي العشوائي والبيان العادي والبيان العشوائي في نمذجة شبكات الاستشعار اللاسلكية.

6 نموذج الشبكة المتسامح مع الأعطال

6-1- مقدمة

تستخدم شبكات الاستشعار اللاسلكية في كثير من الأحيان ضمن بيئات غير موثوقة وظروف قاسية، مما يعرّض العقد فيها لتحديات جسيمة تتعلق بالاستهلاك السريع للطاقة ، وضعف القدرات الحاسوبية، وارتفاع معدلات الأعطال.

تعرفنا على هذه الأعطال في الفصل الثالث حيث وجدنا أنها تنتج عن عوامل متعددة، من بينها انخفاض شحن البطارية، والتقلبات الجوية العنيفة، والتداخلات الخارجية. نتيجة لذلك، تطرح شبكات الاستشعار اللاسلكية مجموعة من التحديات التقنية الفريدة أمام الباحثين في مجال تحمل الأعطال والذي يُعرف بأنه قدرة الشبكة على الحفاظ على أدائها الوظيفي حتى في حال حدوث أعطال في بعض العقد أو مسارات الاتصال. تتعدد الأسباب التي تجعل الحديث في شبكات الاستشعار المتسامحة مع الأعطال جديرًا بالاهتمام البحثي، حيث في مقدمها التعقيد التقني والتكنولوجي الكامن في تركيب العقد نفسها، والتي تمثل أنظمة شديدة التعقيد والدقة.

تُعد إدارة الطاقة عنصراً محورياً في تحقيق التسامح مع الأعطال في شبكات الاستشعار اللاسلكية، إلا أن إمدادات الطاقة في كل عقدة تظل محدودة، كما أن استبدال البطاريات بشكل دوري ليس حلاً عملياً في معظم التطبيقات، حيث تعمل عقد الاستشعار في إطار قيود طاقة صارمة، مما يحد بشدة من ميزانية الطاقة المخصصة لأنشطة الاختبار وتصحيح الأخطاء، وهذا ما يجعل الطاقة أحد العوامل الأكثر تعقيداً وتأثيراً على أداء الشبكة بشكل عام. في هذا السياق، تركّز الجهود البحثية الحديثة على تطوير نماذج فعالة لشبكات الاستشعار اللاسلكية القادرة على التسامح مع الأعطال [25]. في هذا الفصل سنقدم تطوير للنموذج المقترح ليصبح متسامحاً مع أعطال نفاد طاقة العقد.

6-2- النموذج المتسامح مع الأعطال

نقدم في هذه الفقرة شرحاً مفصلاً للنموذج المتسامح مع الأعطال، حيث نبدأ بتحديد الأعطال التي سنقوم بالتسامح معها.

6-2-1. الأعطال التي يعالجها النموذج

يعالج النموذج نوعين أساسين من الأعطال هما:

1. نفاد طاقة العقدة بسبب مدة عملها.
2. هجوم يؤدي لاستنزاف طاقة العقدة.

6-2-2. آلية العمل

يهدف النموذج إلى فهم سلوك الشبكة في حالتها المستقرة الأولية، والتنبؤ بمواطن الضعف قبل تفاقمها، مما يمكّن من اتخاذ إجراءات استباقية للحفاظ على متانة الشبكة تم تقسيم النموذج المقترح إلى ثلاث طبقات رئيسية هي:

1. **الطبقة البنيوية (Structural layer)**

تعمل قبل التشغيل أو عند حدوث تغيرات كبيرة فقط. مسؤولة عن تحديد بنية الشبكة ككل.

2. **الطبقة التشغيلية (operational layer)**

تعمل أثناء التشغيل الفعلي للشبكة ومسؤولة عن التوجيه واختيار المسارات.

3. **طبقة المراقبة والتكيف (Monitoring and adaptation layer)**

تراقب أداء الشبكة تقرر متى يجب إعادة تفعيل التحليل البنيوي.

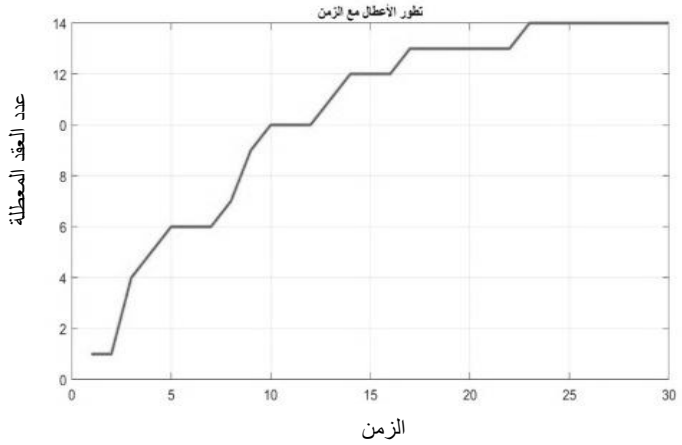
أما بالنسبة للتعامل مع الأعطال يقسم إلى :

1. أعطال فردية استبدال العقدة فوريا بعقدة من نفس المستوى.
2. أعطال متعددة استخدام المسارات البديلة وتجنب العقد الحرجة.
3. أعطال واسعة النطاق تفعيل التحليل البنيوي مجدداً إعادة تصنيف العقد.

6-2-3. البداية والإطار الزمني

في لحظة البدء (t=0)، التي تمثل نقطة انطلاق عملية الرصد، تكون الشبكة في حالتها المثالية حيث تعمل جميع العُقد دون أي أعطال. في هذه اللحظة، تمتلك المحطة الأساسية تمثيلاً كاملاً ودقيقاً للشبكة على

شكل مصفوفة تجاور أولية (M_0). تمثل هذه المصفوفة العلاقات الاتصالية بين جميع العُقد، وفق النموذج المقترح في الفصل الرابع. لكن مع مرور الزمن تتطور الأعطال في الشبكة بازدياد العقد المعطلة كما هو موضح في الشكل (6-1).



الشكل (6-1) تطور الأعطال مع الزمن

6-2-4. النمذجة الاحتمالية لزمن فشل العقدة

لتمثيل اللحظة العشوائية التي تفشل فيها عُقدة ما لأول مرة، نعرّف t متغيراً عشوائياً مستمراً. يتم وصف هذا المتغير من خلال دالة كثافة احتمالية f(t)، والتي تحدد احتمالية فشل العُقدة في فترة زمنية معينة. يُعتبر التوزيع الأسي هو الأنسب لنمذجة زمن الفشل في هذا النموذج، وذلك للأسباب التالية:

1. ملاءمة طبيعة الأجهزة الإلكترونية: يعد التوزيع الأسي من أكثر التوزيعات استخداماً في نظرية الموثوقية لتمثيل "زمن العطل" للمكونات الإلكترونية، فهو يناسب الظاهرة بدقة.
2. البساطة والكفاءة: يتميز التوزيع الأسي ببساطة صياغته الرياضية، مما يسهل عملية المحاكاة والتحليل دون إضافة تعقيدات غير ضرورية.
3. خاصية انعدام الذاكرة: هذه هي الخاصية الأكثر أهمية. وتعني أن احتمالية فشل العُقدة في اللحظة القادمة لا تعتمد على المدة التي قضتها في العمل. بمعنى آخر، عُقدة عملت لمدة 100 ساعة لديها احتمالية

الفشل نفسها في الساعة التالية مثلها مثل عُقدة أخرى بدأت العمل للتو. هذه الخاصية تنطبق بشكل كبير على المكونات الإلكترونية، حيث أن الفشل غالباً ما يكون مفاجئاً وليس ناتجاً عن استهلاك تدريجي للطاقة.

4. تمثيل الانتقال الثابت بين الحالتين: يعبر هذا التوزيع بشكل جيد عن الانتقال المفاجئ والثابت للعُقدة من حالة عمل إلى حالة فشل، دون مراحل وسطى معقدة.

6-2-5. الفحص الأولي للعقد باستخدام التوزيع الأسي

الزمن المتوسط حتى وقوع الفشل بالعقدة i يعطى بالعلاقة $T_i = \frac{1}{\tau_i}$ حيث τ_0 معدل الفشل الثابت و معدل فقدان العقدة لطاقتها الأولية E_i أو ببساطه معدل نفاد طاقة العقدة E_{max} أقصى طاقة أولية بين جميع العقد ومنه يمكننا استخلاص معدل الفشل للعُقدة i كما يلي:

$$\tau_i = \tau_0 \frac{E_{max}}{E_i} \quad \text{.....(5)}$$

توضح العلاقة (5) أن معدل الفشل τ_i ليس ثابتاً. عندما تكون الطاقة E_i عالية، يكون τ_i صغيراً (أي احتمالية فشل منخفضة). بينما يزداد τ_i بشكل كبير كلما اقتربت طاقة العُقدة من النفاد، مما يعكس زيادة خطر الفشل.

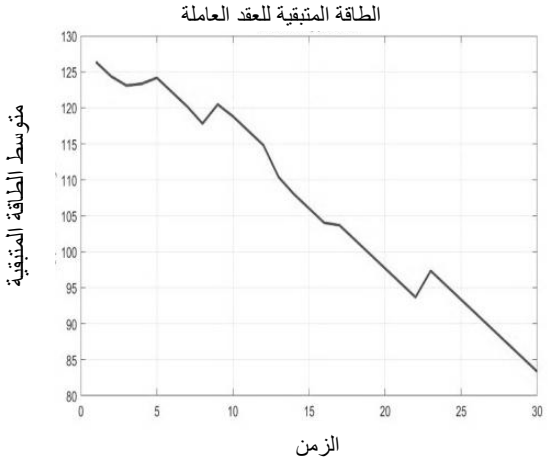
نأخذ دالة التوزيع الاحتمالي التي تعبر عن احتمال فشل العقدة ضمن المجال [0,t] والتي تعرف رياضياً بالعلاقة:

$$P_i = \int_0^t f(u)\, du = 1 - e^{-\tau t} \quad \text{.....(6)}$$

أما احتمال أن تبقى العقدة على قيد الحياة طيلة الفترة [0,t] هو:

$$R(t) = 1 - P_i = 1 - \int_0^1 f(u)du = e^{-\tau t} \quad \text{.....(7)}$$

ربط هذا الإطار الرياضي بشكل ديناميكي بين الطاقة المتبقية للعُقدة واحتمالية بقائها عاملة، الشكل (6-3) يوضح العلاقة بين متوسط الطاقة المتبقية للعقدة بمرور الزمن.



الشكل (6-2) الطاقه المتبقية للعقد العاملة

يسمح للنموذج بمحاكاة واقعية لسلوك الشبكة مع مرور الزمن وتناقص موارد الطاقة، وهو أمر بالغ الأهمية لتطوير استراتيجيات متسامحة مع الأعطال تعتمد على الحالة الفعلية للشبكة. كما يتم تصنيف العقد إلى ثلاث فئات:

عقدة آمنة عند الزمن t إذا كان $P_i < 0.2$

عقدة مهددة عند الزمن t إذا كان $0.2 < P_i < 0.5$

عقدة حرجة زمنياً عند الزمن t إذا كان $P_i > 0.5$

6-2-6. تشكيل المكون العملاق المتسامح مع الأعطال

مع تقدم الزمن وحدوث أعطال في العُقد، تقوم المحطة الأساسية بتحديث مصفوفة التجاور عند حدوث فشل لتعكس التغيرات في طوبولوجيا الشبكة. يتم هذا التحديث مع مراعاة اختفاء الأضلاع المرتبطة بالعُقد التي تعطلت، مما يضمن تمثيلاً دقيقاً لمسارات الاتصال الفعلية القائمة في كل لحظة زمنية. تم تصميم النظام ليكون متسامحاً مع الأعطال بدرجة عالية، حيث يضمن الحفاظ على متانة الشبكة وفق المبادئ التالية:

1. عدم فقدان الاتصال مع أي مسار: يضمن النموذج أن فقدان أي عُقدة مفردة لا يؤدي إلى انقطاع المسارات الحيوية أو عزل أجزاء من الشبكة.
2. التسجيل الزمني للمعلومات: في كل لحظة زمنية t، يتم توثيق معلومات العُقدة المفقودة وموقعها بدقة، مما يتيح تحليل تأثيرات الفشل واتخاذ القرارات المستنيرة للتعويض عنها.

- **تشكيل المكون العملاق**

لتحقيق أهداف التسامح مع الأعطال، تقوم الآلية الأساسية بتشكيل مكون عملاق يضم مجموعة العُقد الأساسية أو المسيطرة في كل مستوى. يمثل هذا المكون العملاق البنية التحتية للشبكة التي تضمن استمرارية الاتصال وتبادل البيانات. نعرض فيما يلي الخوارزمية المقترحة لتشكيل المكون العملاق المتسامح مع الأعطال.

المدخلات: البيان وفق النموذج المقترح لشبكة الاستشعار العشوائية G(V,E).

المخرجات: المكون العملاق المؤلف من العقد المسيطرة.

1. $C = \varphi$
2. نبدأ بالمستوي الأول، اختار عقد آمنة ولها أكبر درجة ارتباط أضفها إلى C. كما تعتبر هذه العقدة مسيطرة في مستواها، ونكرر ذلك لكل المستويات للحصول على العقد المسيطرة.
3. $For: i \geq 2$ (i ترمز لرقم المستوى)
   - $v \in$ i
   - افحص $N(v)$ (مجاورات العقدة في المستوى الأقل).
   - إذا لم تكن v مرتبطة بعقدة مسيطرة: أضف العقدة الآمنة في $N(v)$ إلى C.
4. كرر حتى تغطية جميع المستويات.
5. أنشئ المكون العملاق.
6. معالجة الحالة الحرجة (فشل عُقد المستوى الأول): عند فشل عقد المستوي الأول تتوقف الخوارزمية لعدم القدرة على الوصول للمحطة الأساسية.

تتميز الخوارزمية بقدرتها على تحسين استهلاك الطاقة حيث يعطي معيار اختيار العُقد ذات الطاقة الأعلى أولوية، مما يطيل من عمر الشبكة الكلي.

6-2-7. آلية التعافي الديناميكي وإعادة توزيع الحمل بعد فقدان العُقد

لضمان استمرارية تدفق البيانات ومنع فقدان الاتصال عند تعطل أي عُقدة، يتم تنفيذ الآلية التالية:

1. الإرسال الاستباقي للبيانات: عند توقع تعطل عُقدة ما (بناءً على انخفاض طاقتها دون عتبة محددة)، تقوم هذه العُقدة بإرسال بياناتها ذات الأولوية العالية بشكل استباقي إلى العُقدة المسيطرة المرتبطة بها ضمن نفس المستوى. لكن في حال كانت العقدة المسيطرة منخفضة الطاقة يتم نقل البيانات إلى العقدة المسيطرة في المستوى الأدنى.

1. إعادة توجيه المسارات: تقوم العُقد المسيطرة بدورها بإعادة توجيه هذه البيانات بالاعتماد على دالة الكلفة المستخدمة لاختيار المسار الافضل وهي:

$$\text{Scor} = \alpha \frac{E_{res}}{D} - \beta C_{struct} - \gamma P_i$$

حيث α معامل يحدد أهمية الطاقة المتبقية مقارنة بالمسافة. و $C_{struct} \begin{cases} 1 & \text{عقدة حرجة} \\ 0 & \text{عقدة عادية} \end{cases}$

$\beta \epsilon [0.2,0.3]$ وزن الخطر البنيوي، $\gamma \in [0.2,0.4]$ وزن الخطر الزمني.

عقد ذات طاقة أعلى وخطر زمني أقل، وتأثير بنيوي محدود على استقرار الشبكة.

2. الحفاظ على استمرارية الخدمة: تضمن هذه الآلية أن البيانات لا تُفقد أثناء عملية التعافي، وأن الخدمة تستمر بأقل قدر ممكن من الانقطاع.

6-2-8. ضبط الحساسية الزمنية وإعادة التكيف

يعاد التحليل البنيوي عند تجاوز أحد العتبات المحددة التالية :

1. عتبة حجم المكون العملاق

$$\frac{|GC|}{|V|} \geq Q$$

حيث $Q \in [0.5,0.95]$ أي Q هي النسبة الدنيا المطلوبة من العقد لتكون ضمن المكون العملاق. إذا انخفضت النسبة عنQ، يتم إعادة التحليل.

3. عتبة العقد الحرجة

$$\frac{N_{critical}}{N} \leq 0.15$$

إذا تجاوزت نسبة العقد الحرجة 15% نقوم بإعادة التحليل.

6-2-9. خوارزمية إعادة توزيع الحمل بناءً على الطاقة المتاحة

نوضح فيما يلي خطوات خوارزمية إعادة توزيع الحمل:

- **الفرضيات**

1. لنفترض أن العُقدة v_i قد تعطلت.
2. مجموعة العُقد المجاورة لها هي $\{v_j\}$ حيث $j \in V$.
3. الحمل الكلي الذي كانت تعالجه العُقدة v_i هو W_i.
4. الطاقة المتاحة لكل عُقدة مجاورة v_j هي E_j.

- **خطوات التوزيع**

1. حساب إجمالي الطاقة المتاحة للعقد المجاورة:

$$E_{total} = \sum_{j \in V} E_j$$

يتم توزيع الحمل W_i الذي كانت تعالجه العقدة v_i على العقد v_j بناءً على الطاقة المتاحة لكل عقدة مجاورة.

2. حساب النسبة المئوية للتوزيع:

$$W_j = W_i \times \frac{E_j}{E_{total}}$$

حيث W_j هو جزء من الحمل الذي يتم توزيعه على العقدة v_j.

- **معايير التوزيع**

1. يتم توزيع الحمل بشكل يتناسب طرداً مع الطاقة المتبقية لكل عُقدة.
2. العُقدة الآمنة تتلقى جزءاً أكبر من الحمل، مما يضمن عدالة التوزيع وإطالة عمر الشبكة.

6-2-10. آلية التحديث عند تجاوز أحد العتبات

يتم إعادة حساب الطاقة المتبقية لجميع العُقد التي لم تعطل. حساب المكون العملاق يأخذ الحساب في الاعتبار الطاقة الأولية للعُقدة، الطاقة المستهلكة في العمليات السابقة، الحمل الجديد الموزع على العُقدة. وإعادة تصنيف العقد يتم تزويد المحطة الأساسية بـ:

1. مصفوفة المستوى يتم تعديل توزيع العُقد على المستويات في حال أدى تعطل بعض العُقد إلى تغيير في الهيكل الهرمي للشبكة.
2. مصفوفة التجاور حيث تعكس المصفوفة المُحدثة التغيرات في العُقد المعطلة (يتم حذفها)، الروابط المنقطعة (يتم إزالتها).

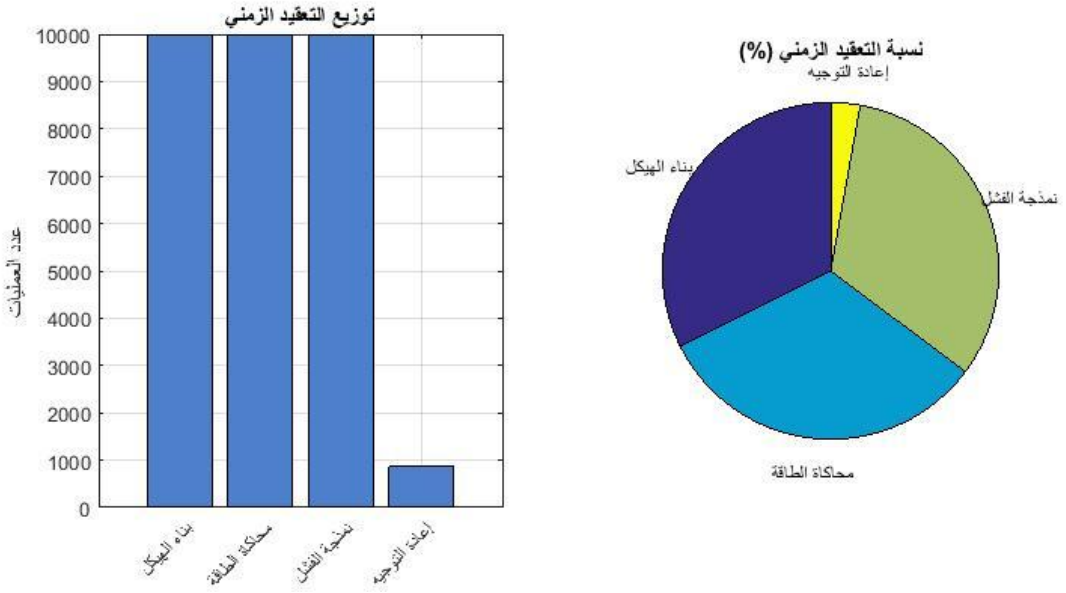
6-3- التعقيد الزمني للنموذج المطور

سنقوم بدراسة التعقيد الزمني، عند نشر n عقدة استشعار وجدنا أن التعقيد الزمني للنموذج هو $T_1=O(n^2)$ وفق (4-4-6). لحساب العقد التي لها أكبر قدر من الطاقة والمجاورات نحتاج إلى حلقة تكرارية بالتالي تكون الكلفة كحد أعلى هي $T_2=O(n)$. أما بالنسبة لإجراء اختبار الزمن حسب حساسية النموذج نحتاج إلى حلقة تكرارية فتكون كلفة الحلقة كحد أعلى هي n وبداخل هذه الحلقة يوجد تكرار حتى يتم إيجاد احتمال بقاء كل عقدة على قيد الحياة من خلال التوزيع الأسي بالاضافة إلى تكرار أخر حتى يتم حذف العقد التي احتمال بقائها على قيد الحياة هو صفر من الشبكة بالتالي تصبح كلفة الحلقة كحد أعلى هي $T_3=O(n^3)$ أما في حال عدم تحقق الشرط والخروج من الحلقات فإن كلفة عمليات الطباعة في المخطط هي كحد أعلى $T_4=O(3)$ ومنه التعقيد الزمني للنموذج بعد تطويره حيث O كحد أعلى هو:

$$T = T_1 + T_2 + T_3 + T_4 = O(n^2) + O(n) + O(n^3) + O(3) = O(n^3)$$

يمثل التعقيد البنيوي من الدرجة الثالثة الحد الأعلى النظري للنموذج، بينما يعتمد التشغيل الفعلي على مكونات خطية من الدرجة الأولى أو الثانية، حيث يعاد استدعاء التحليل البنيوي فقط عند تحقق شروط حرجة محددة،

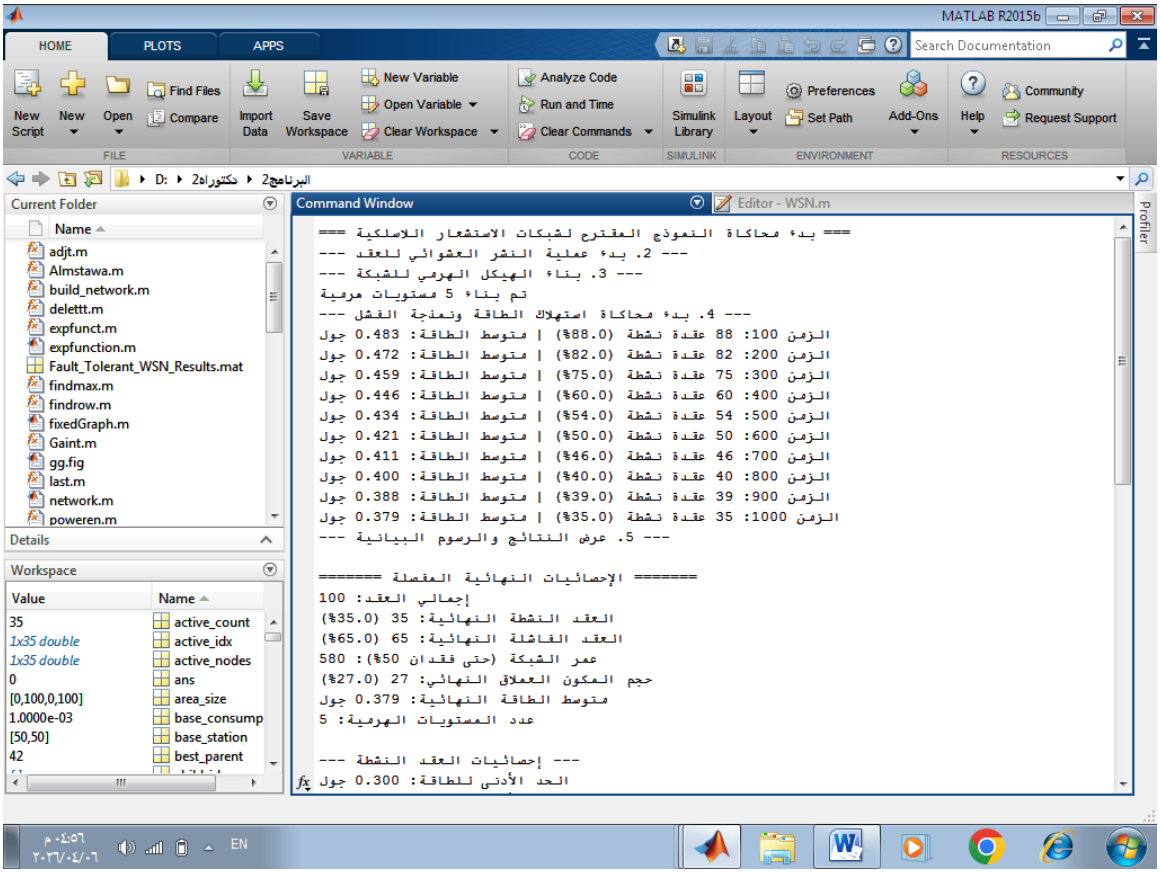
مما يقلل من الكلفة الحسابية العملية للنظام. يوضح الشكل (6–3) التوزيع الفعلي للتعقيد الزمني الناتج عن محاكاة النموذج باستخدام MATLAB 2015.



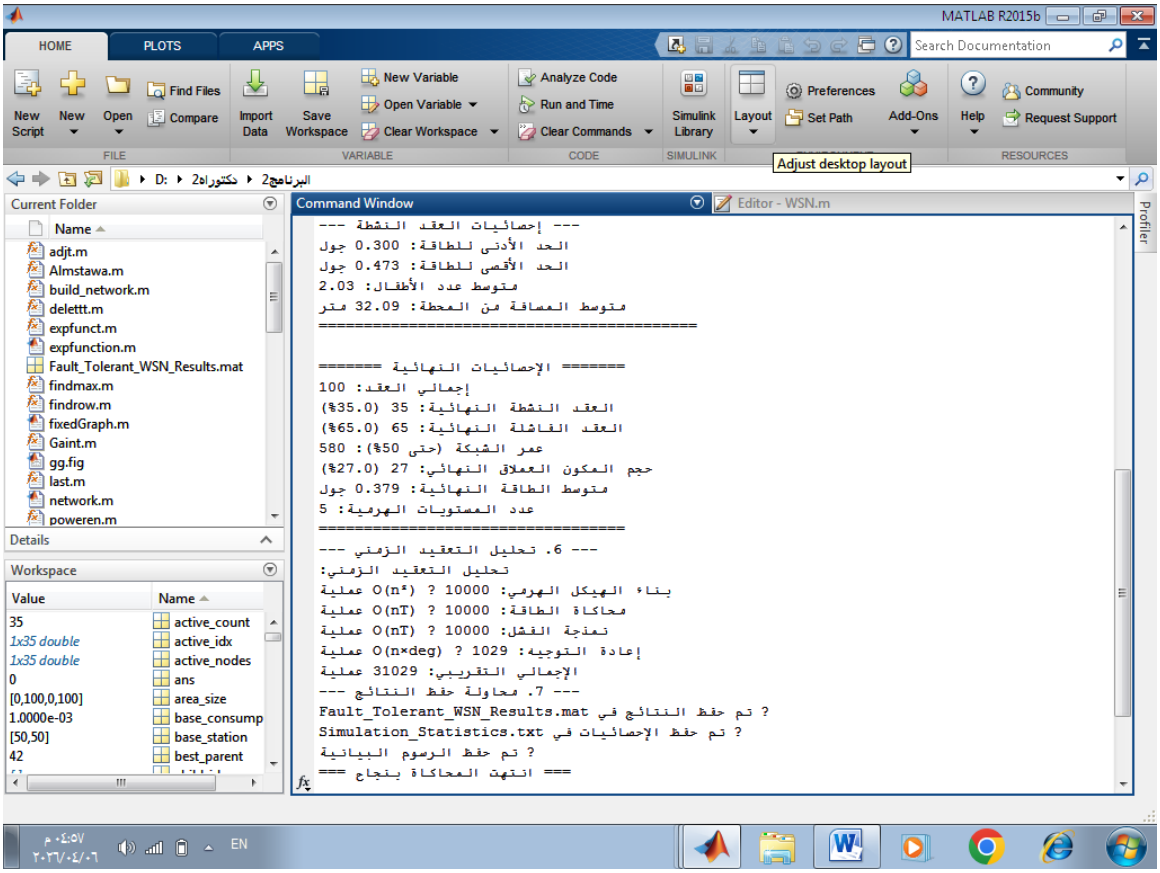
الشكل (6-3) التعقيد الزمني

6–4– محاكاة النموذج المطور

قمنا بتنفيذ محاكاة شاملة للنموذج المطور باستخدام بيئة MATLAB 2015، حيث تمت محاكاة شبكة الاستشعار المكونة من 100 عقدة يظهر الشكل (6–4) محاكاة استهلاك الطاقة ونمذجة الفشل بالإضافة الى عدد العقد النشطة والفاشلة وعمر الشبكة. كما يظهر الشكل (6–5) النتائج النهائية وتحليل التعقيد الزمني.

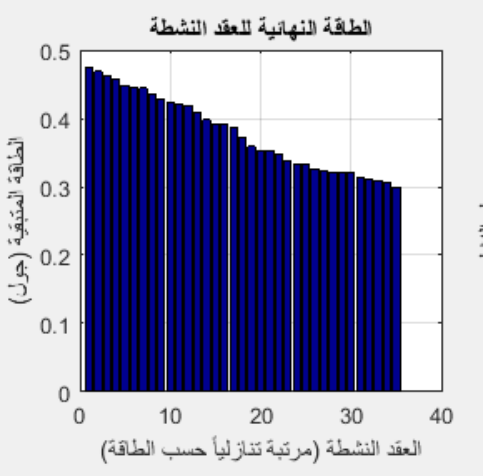


الشكل (6-4) محاكاة استهلاك الطاقة



الشكل (6-5) النتائج النهائية والتعقيد الحسابي

يوضح الشكل (6–6) التوزيع الطاقي المتدرج للعقد التي حافظت على نشاطها حتى نهاية فترة المحاكاة، حيث تم ترتيب العقد تنازلياً حسب طاقتها المتبقية على المحور الأفقي، بينما يمثل المحور العمودي قيمة الطاقة المتبقية بالجول. يظهر التوزيع منحنى طاقة مميز يتدرج من أعلى قيمة طاقة إلى أدنى قيمة، مع وجود عدد محدود من العقد في الطرف الأعلى للطاقة وعدد أكبر في المنطقة المتوسطة والمنخفضة. يمثل هذا التوزيع نجاحاً واضحاً لاستراتيجيات التسامح مع الأعطال، حيث أن العقد ذات الطاقة الأعلى تشكل عادةً العقد المركزية في المستويات الهرمية الأولى والثانية، بينما تشغل العقد منخفضة الطاقة مواقع طرفية أو أدواراً محدودة الاستهلاك. التدرج السلس في المنحنى (بدون قفزات حادة) يدل على فعالية آلية إعادة توزيع الحمل الديناميكية التي منعت الإرهاق المفاجئ لأي عقدة معينة.



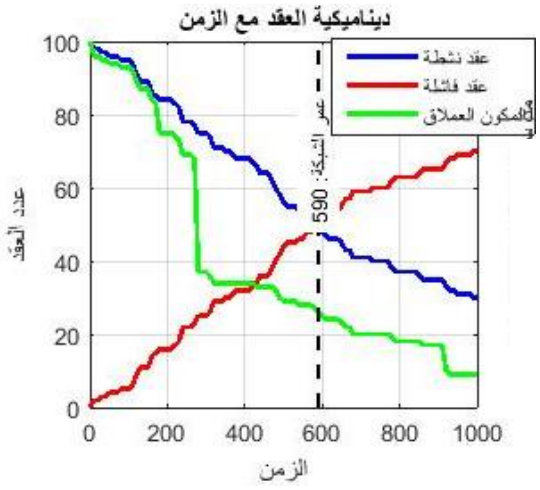
الشكل (6-6) الطاقة النهائية للعقد النشطة

يوضح الشكل (6–7) التغير الزمني في توزيع العقد بين الحالات المختلفة خلال فترة المحاكاة الكاملة. يتمثل المحور الأفقي في الزمن بالوحدات الزمنية، بينما يمثل المحور العمودي عدد العقد في الشبكة. تظهر ثلاثة منحنيات رئيسية تعكس الأداء الديناميكي للنموذج المقترح:

1. منحنى العقد النشطة (الأزرق): يبدأ من 100 عقدة ويتناقص تدريجياً ليصل إلى 35 عقدة نشطة في نهاية المحاكاة. يشير الاستقرار النسبي في نهاية المنحنى إلى أن الشبكة قد وصلت إلى حالة توازن طاقي.

2. منحنى العقد الفاشلة (الأحمر): يتبع نمطاً معاكساً تماماً للمنحنى الأزرق، حيث يبدأ من الصفر ويزداد بوتيرة متسقة مع انخفاض العقد النشطة، ليصل إلى 65 عقدة فاشلة في النهاية. الملاحظة الهامة هي غياب الانهيار المفاجئة في هذا المنحنى، مما يدل على غياب ظاهرة الفشل الكلي.
3. منحنى المكون العملاق (الأخضر): يحافظ على مسافة قريبة من منحنى العقد النشطة خلال فترة المحاكاة. هذا يشير إلى أن معظم العقد النشطة ظلت متصلة بالمحطة الأساسية عبر مسارات فعالة.

تُبرز النتائج أن النموذج المقترح أدى إلى تنوع واضح في الأحمال والطاقة المستهلكة بين العقد، التنوع أدى إلى توزيع أفضل للأحمال ضمن المستويات الهرمية، مما سمح بتأخير فشل العقد بشكل تدريجي وتخفيف الانهيار المفاجئ للمكون العملاق، كما يظهر الانحدار المتفاوت للخطوط الزرقاء والخضراء والحمراء. وبالتالي، تثبت هذه المحاكاة أن النموذج المقترح قادر على تحسين متانة الشبكة واستقرارها التشغيلي عبر التكيف مع فروق الطاقة والأحمال بين العقد، وهو ما يعزز فعالية النموذج في سيناريوهات الشبكات الكبيرة والمتنوعة الطاقة.



الشكل (6-7) ديناميكية العقد مع الزمن

6-4-1 نتائج المحاكاة الكلية وتقييم فعالية النموذج المقترح إحصائيًا

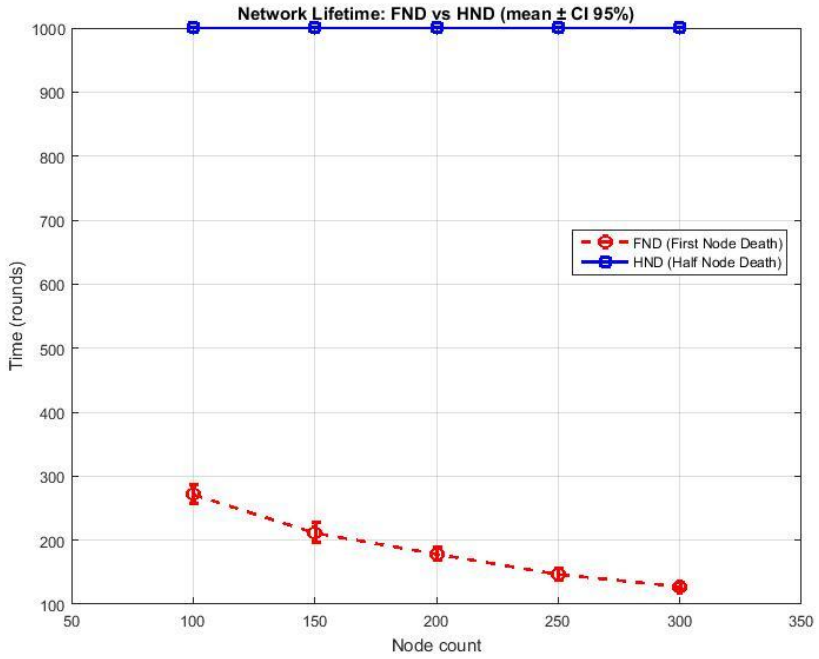
تم تنفيذ 150 تشغيلة مستقلة موزعة على خمسة أحجام شبكة (100، 150، 200، 250، 300 عقدة)، بواقع 30 تشغيلة لكل حجم، مع تغيير البذرة العشوائية لكل تشغيلة لضمان تمثيل سيناريوهات نشر متنوعة. تم تحليل النتائج باستخدام مقاييس موضحة في الجدول (6-1).

المقياس	معنى المقياس
FND (First Node Death)	أول جولة تموت فيها أول عقدة (تفشل تماماً).
HND (Half Node Death)	الجولة التي تموت فيها 50% من العقد.
معدل النجاة (%)	النسبة المئوية للعقد التي لا تزال حية بعد 1000 جولة.
الطاقة المتبقية (%)	متوسط الطاقة المتبقية في الشبكة بعد 1000 جولة.
GC (Giant Component)	حجم أكبر مكون متصل في الشبكة في النهاية (يعبر عن تماسك الشبكة).
المستويات الهرمية	عدد القفزات من أبعد عقدة إلى المحطة.
درجة الاتصال	متوسط عدد الجيران لكل عقدة.

الجدول (6-1) مقاييس الأداء

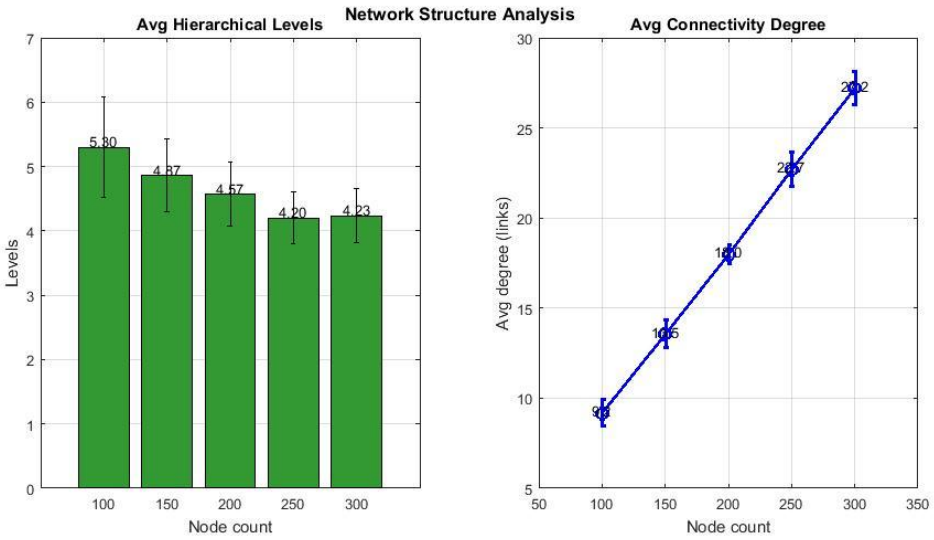
يوضح الشكل (6–8) نتائج عملية محاكاة الشبكات أظهرت النتائج أن متوسط FND يتناقص بشكل منتظم مع زيادة عدد العقد، من 251.8 جولة (σ=35.2) عند n=100 إلى 132.8 جولة (σ=21.5) عند n=300، مع فاصل ثقة 95% لا يتجاوز ±13.0 جولة في أصغر حجم و±7.9 جولة في أكبر حجم. تعكس قيم الانحراف المعياري (21.5–35.2) تبايناً طبيعياً ناتجاً عن العشوائية المستقلة في توزيع العقد، طاقتها الابتدائية (0.4–0.6 J)، نصف قطر إرسالها (15–25 m)، ومعدل فشلها الاحتمالي τ.

في المقابل، سجل متوسط زمن انهيار نصف الشبكة (HND) قيمة 1000 جولة لجميع الأحجام، مما يعني أن الشبكة لم تفقد 50% من عقدها خلال كامل زمن المحاكاة (1000 جولة). يتوافق هذا مع متوسط نسبة النجاة الذي تراوح بين 64.5% و67.0%، ومتوسط الطاقة المتبقية بين 63.2% و65.3%، مما يشير إلى أن آلية إعادة التوجيه الهرمية المقترحة تحافظ على استمرارية الشبكة رغم فقدان نحو ثلث العقد تراكماً خلال 1000 جولة.



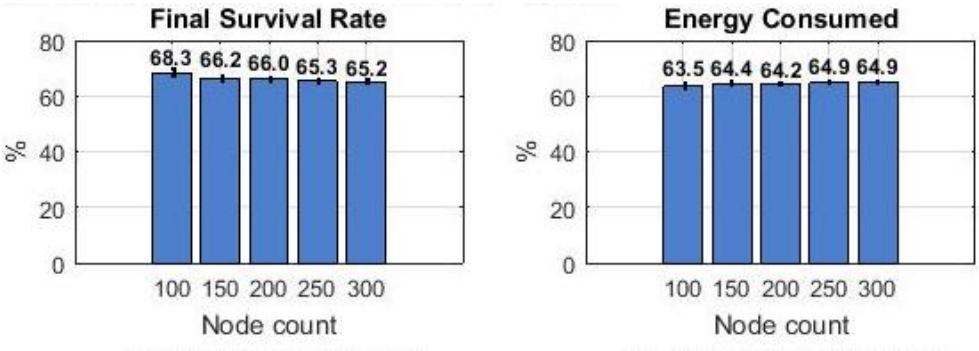
الشكل (6-8) الجولات التي تفشل فيها عقد الشبكة

كما يوضح الشكل (6–9) التحليل الإحصائي للهيكل الهرمي ودرجة الاتصال عن اتجاهين مزدوجين: الاول انخفاض عدد المستويات الهرمية من 5.80 (σ=0.73) عند n=100 إلى 4.23 (σ=0.35) عند n=300، والثاني ارتفاع درجة الاتصال من 9.19 (σ=0.62) إلى 27.22 (σ=0.42) على التوالي. الانخفاض الملحوظ في الانحراف المعياري للمستويات الهرمية (0.73→0.35) مع زيادة الكثافة يعكس ثباتاً متزايداً في أداء الخوارزمية.



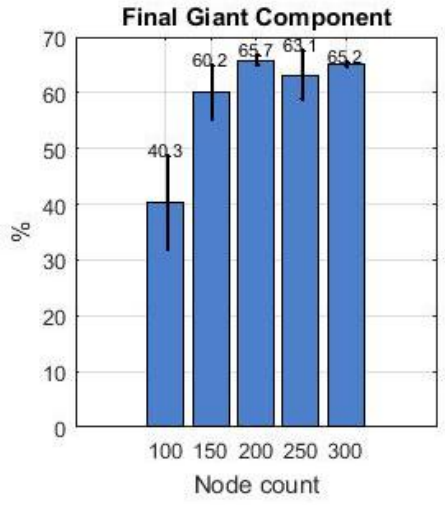
الشكل (6-9) تحليل بنية الشبكة بدون التسامح

يوضح الشكل (6–10) تراوح متوسط معدل النجاة (النسبة المئوية للعقد النشطة بعد 1000 جولة) بين 68.3% و 65.2%، حيث سُجل أعلى قيمة عند n=100 وأدنى قيمة عند n=300. بالمثل، كان متوسط الطاقة المستهلكة مستقراً بين 63.5% و 64.9%. الانحراف المعياري لهذين المقياسين لم يتجاوز 2.4% في أي حجم. هذا الثبات والضيق الإحصائي يدلان على أن آلية إعادة التوجيه توزع الحمل بعدالة نسبية بين العقد بغض النظر عن كثافة الشبكة. تجدر الإشارة إلى أن الطاقة المستهلكة تقترب من معدل النجاة، وهو ما يتسق مع نموذج الفشل الاحتمالي $\tau(i)$ حيث تفشل العقد تراكمياً بسبب الاحتمالية المرتبطة بالاستنزاف قبل أن تفرغ طاقتها بالكامل.



الشكل (6-10) نسبة النجاح والطاقة المتبقية

في حين يوضح الشكل (6–11) أن حجم المكون العملاق النهائي (GC) فكان منخفضاً عند n=100 بسبب التفكك السريع للشبكة قليلة الكثافة، ثم استقر بين 58.8% و66.2% للأحجام الأكبر حيث (σ=2.7)، مما يؤكد أن الكثافة الأعلى (n≥150) توفر بدائل توجيه كافية للحفاظ على تماسك الشبكة رغم الأعطال.

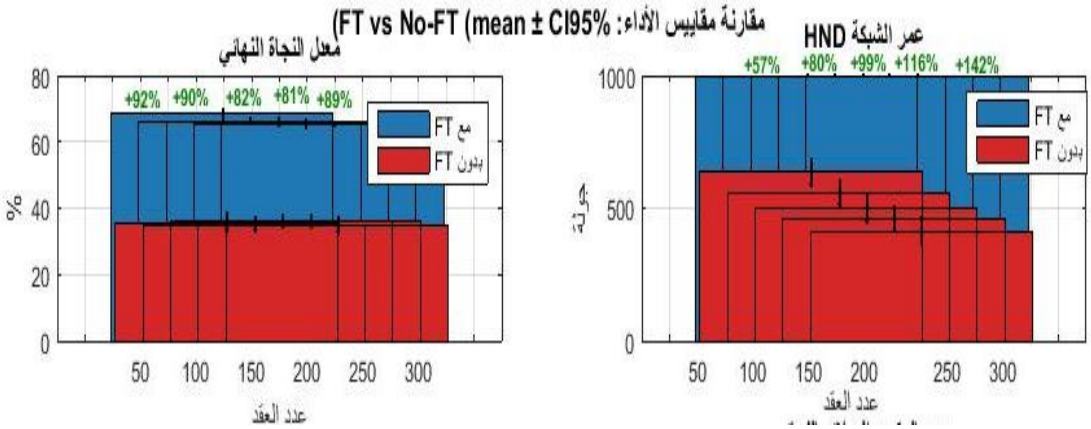


الشكل (6-11) حجم المكون العملاق

تؤكد هذه النتائج، المستمدة من 150 تشغيلة مستقلة، أن النموذج المقترح يُظهر سلوكاً منتظماً وقابلاً للتوسع، مع تباين طبيعي ضمن الحدود المتوقعة لمحاكاة شبكات الاستشعار اللاسلكية.

يوضح الشكل (6–12) أنه في حالة عدم التسامح مع الأعطال ، يتراوح متوسط HND بين 180 و 420 جولة حسب كثافة الشبكة، مع تدهور ملحوظ عند الأحجام الكبيرة. بالمقابل، في نموذج المتسامح مع الأعطال يصل HND إلى 1000 جولة (نهاية المحاكاة) لجميع الأحجام، أي أن الشبكة لم تفقد نصف عقدها خلال 1000 جولة. هذا يعني أن آلية التسامح مع الأعطال تطيل عمر الشبكة.

كما يوضح الشكل غياب آلية التسامح، يؤدي إلى إنهيار معدل النجاة بشكل حاد مع زيادة حجم الشبكة، بينما في النموذج المقترح المتسامح مع الأعطال يبقى المعدل مستقراً بين 64.5% و 67.0% عبر جميع الأحجام.



الشكل (6-12) مقارنة بعمر الشبكة ومعدل النجاة النهائي

6–4–2 المقارنة مع الدراسات السابقة

من أجل تقييم كفاءة النموذج المقترح، وبيان مدى ملاءمته للتطبيق في شبكات الاستشعار اللاسلكية، تمت مقارنتها مع عدد من الدراسات السابقة.

ركزت الدراسة في [31] على تحسين استقرار المسارات وتقليل استهلاك الطاقة من خلال بروتوكول توجيه متقدم، إلا أنها تعالج المشكلة من منظور محلي محدود يقتصر على اختيار المسار، دون تحليل التأثير التراكمي للأعطال البنيوية أو تغير خصائص الشبكة مع الزمن. وبذلك فإن استقرار التوجيه الذي تحققه الدراسة يبقى مرهوناً بسلامة البنية الأساسية للشبكة، وهي فرضية لا تصمد دائماً في بيئات الاستشعار القاسية.

أما في [32] تم معالجة مسألة التوجيه المتسامح مع الأعطال مع تحسين كفاءة الطاقة في شبكات الاستشعار اللاسلكية، من خلال اقتراح آلية توجيه تهدف إلى الحفاظ على استمرارية نقل البيانات عند فشل بعض العقد، مع تقليل استهلاك الطاقة أثناء عملية التوجيه. لكن حصر التسامح مع الأعطال في طبقة التوجيه يؤدي إلى معالجة عرضية للمشكلة، دون فهم التأثير التراكمي لفشل العقد على بنية الشبكة واستمراريتها.

أما بالنسبة للدراسات التي تطرقت لاستخدام البيان الهندسي العشوائي وقد ذكرناها في الفقرة (2-5)، فإن [24] على الرغم من دقتها الرياضية العالية، إلا أنها تفترض بيئة ثابتة وعقداً متجانسة، وتتجاهل القيود الأساسية مثل الطاقة، وعدم استقرار الروابط. بالتالي فإن نتائجها تبقى صالحة لمرحلة التخطيط الأولي فقط.

أما بالنسبة لـ [25] فقد ركز على دراسة الاتصال والتغطية في شبكات الاستشعار اللاسلكية بالاعتماد على RGG لكن افترض وجود عقد قوية أو محطات أساسية مهيمنة. على الرغم من أهمية النتائج النظرية والمحاكاة إلا أن النموذج يفترض بنية شبكية جاهزة ومستقرة نسبياً تطبق فوقها آلية التوجيه. كما أن تحسين استهلاك الطاقة أثناء الأرسال لا يمنع الانهيار البنيوي للشبكة.

يوضح الجدول (2-6) ملخص المقارنة بين الدراسات السابقة والنموذج المقترح.

المعيار	المقالة [31]	المقالة [32]	المقالة [25]	المقالة [24]	النموذج المقترح
نوع النموذج	بروتوكول توجيه	خوارزمية توجيه	بيان عشوائي هندسي ديناميكي	بيان عشوائي هندسي تحليلي ثابت	بيان هندسي عشوائي متعدد المستويات
هدف الدراسة	استقرار التوجيه	التعامل مع الأعطال وتوفير الطاقة	الاتصال والتغطية	تخطيط الشبكة وتحديد عدد العقد	التسامح مع الأعطال + إطالة عمر الشبكة
تجانس العقد	غير متجانسة	محدود	غير متجانسة عقد قوية وعادية	متجانسة	غير متجانسة
معالجة الطاقة	تحسين أثناء التوجيه	تحسين محلي أثناء الأرسال	معالجة محدودة	غير مدروس	نموذج صريح لإدارة الطاقة
الديناميكية الزمنية	جزئية	محدودة جداً	جزئية	غير مدروس	مدروسة بشكل أساسي في النموذج
قابلية التطبيق العلمي	عالية	متوسطة	متوسطة	منخفضة	عالية جداً
تأثير الأعطال على البنية	غير مدروس	غير مدروس	غير مدروس	غير مدروس	مدروس بعمق

الجدول (6-2) مقارنة بين النماذج

6-5- خلاصة الفصل

قدمنا في هذا الفصل تطوير للنموذج المقترح في الفصل الخامس بالاعتماد على مفهومي المكون العملاق في البيان العشوائي والعقد المسيطرة ليصبح النموذج قادراً على التسامح مع الأعطال التي تحدث نتيجة فقدان العقدة لطاقتها سواء بعطل فني أو هجمات استنزاف الطاقة. كما أثبتنا فعاليته وكفاءته في التسامح مع أعطال الطاقة في العقد من خلال محاكاة رياضية للنموذج المقترح باستخدام تطبيق الماتلاب واجراء دراسة إحصائية على عدد كبير من الشبكات.

7 الخوارزمية المقترحة لتشفير بيانات النموذج

7-1- مقدمة

في ظل حساسية التطبيقات في شبكات الاستشعار اللاسلكية، وخاصة العسكرية منها، أصبح التشفير ضرورة حتمية لضمان سرية البيانات المنقولة بين العقد. ولا يقتصر دوره على إخفاء المحتوى فحسب، بل يمتد ليشمل ضمان تكامل البيانات وعدم العبث بها، والتأكد من مصدرها الأصلي، ومنع إنكار إرسالها. ولتلبية هذه المتطلبات، قمنا باقتراح خوارزمية ضمن فئة خوارزميات التشفير المتماثل حيث تعتمد على استخدام مفتاح واحد في عمليتي التشفير وفك التشفير، كما أنها تعمل على تقسيم البيانات إلى مقاطع ثابتة الطول ومعالجتها بشكل مستقل. صممت الخوارزمية لتجمع بين خصائص الاستبدال (Substitution) والترتيب (Permutation)، مع إضافة مرحلة ضغط بيانات لتحسين الكفاءة.

7-2- الخوارزمية المقترحة

تعتمد الخوارزمية على نظرية البيان حيث يتم ترتيب البيانات في مصفوفة مربعه، وتنقسم الخوارزمية المقترحة إلى عدة مراحل سوف نقدم شرحاً تفصيلاً لكل مرحلة على حدة.

7-2-1. توليد المفتاح

يعتمد إيجاد المفتاح على مصفوفة التجاور التي يزودها النموذج المقترح في (5-7)، ولكل عقدة لها رقم. كما يتم توليد مفتاح سري عشوائي لكل عقدة في الشبكة منذ البداية. يُستخدم هذا المفتاح في تحديد ترتيب الأعمدة داخل المصفوفة، ويعتمد المفتاح على مصفوفة التجاور الخاصة بالعقد المجاورة، مما يضيف عنصراً من التخصيص لكل عقدة. نوضح فيما يلي خطوات إنشاء المفتاح للعقدة i:

المدخلات: العقد المجاورة للعقدة i المراد توليد المفتاح لها يتم ارفاقها من خلال مصفوفة التجاور التي يقدمها النموذج المقترح.

المخرجات: المفتاح السري.

1. ترتيب المجاورات عشوائياً.

2. نضعها في سلسلة رقمية.

3. إذا كان طول السلسلة أقل من 4، يتم أضافة أرقام عشوائية في نهاية السلسلة.

هذه الآلية تحقق خاصية الاعتماد على المفتاح (Key Dependency)، حيث تختلف نتائج التشفير باختلاف المفتاح المستخدم.

7-2-2. تجزئة البيانات

تُقسم البيانات إلى مقاطع بطول n، حيث n هو طول المفتاح. إذا لم يكن طول البيانات من مضاعفات n.، يتم إضافة أصفار في النهاية لضمان اكتمال المصفوفة.

7-2-3. ملء المصفوفة

نقوم بإنشاء مصفوفة n*n ويتم وضع البتات لبيانات العقدة في القطر الرئيسي للمصفوفة، ثم تُملأ الخانات المتبقية ببتات مع مراعاة عدم وضع قيم متشابهة بجوار بعضها (أي تجنب وضع 1 بجوار 1 أو 0 بجوار 0). هذه الآلية تضيف عنصرًا من الانتشار(Diffusion)، حيث يتوزع تأثير البتات الأصلية على كامل المصفوفة المنشأة.

7-2-4. تبديل الأعمدة

تُستخدم عناصر المفتاح لإعادة ترتيب الأعمدة داخل المصفوفة. كل عنصر ينتقل للعامود المقابل للمفتاح في نفس الصف وبالتالي لن ننشأ مصفوفة أكبر من n*n اذا فرضنا أن المفتاح هو 4859 فالمصفوفة هي 4 اسطر و4 اعمدة، عناصر المفتاح ستأخذ ترتيب الاعمدة تصاعدياً أي الرقم 4 في المفتاح يشير الى العامود الاول ورقم 5 الى العامود الثاني 8 الى الثالث اما 9 الى العامود الرابع. هذه العملية تحقق خاصية الخلط (Permutation)، وتزيد من صعوبة استنتاج العلاقة بين النص الصريح والنص المشفر.

7-2-5. قلب البتات

بعد إعادة الترتيب، يتم قلب جميع البتات (تحويل 1 إلى 0 والعكس). هذه الخطوة تضيف عنصرًا من الاستبدال (Substitution)، وتزيد من تعقيد النص المشفر.

7-2-6. القراءة العامودية

تُقرأ المصفوفة الناتجة بترتيب عامودي (من اسفل اخر عامود إلى أعلى العمود الأول)، مما يُنتج سلسلة خطية مشفرة. من خلال هذه الخطوة يتم تُحويل البنية المصفوفية إلى نص مشفر جاهز للإرسال عبر قنوات الاتصال غير الآمنة.

7-2-7. الضغط باستخدام RLE

يتم ضغط السلسلة الناتجة باستخدام تقنية RLE (Run Length Encoding)، وهي تقنية بسيطة تعتمد على استبدال التكرارات المتتالية بعدد مرات التكرار والقيمة [26]. هذه المرحلة تقلل من حجم البيانات بنسبة تصل إلى 20–25% في بعض الحالات، مما يُعتبر ميزة عملية في تقليل استهلاك التخزين أو عرض النطاق الترددي. ترسل الرسالة كاملةً بعد تشفيرها وضغطها.

7-2-8. فك التشفير

يتم استلام الرسالة الكلية وتتم عملية فك التشفير بعكس الخطوات السابقة:

1. فك الضغط باستخدام RLE.
2. التجزئة وتتم وفق مربع طول المفتاح وتشكيل المصفوفة بترتيب البتات في الأعمدة بدءاً من أسفل العامود الاخير إلى أعلى العمود الأول.
3. قلب البتات مرة أخرى.
4. أعادة ترتيب الأعمدة وفق المفتاح.
5. وقراءة عناصر القطر الرئيسي لاستعادة النص الأصلي.

7-3- ميزات الخوارزمية المقترحة

تتميز الخوارزمية المقترحة بما يأتي:

1. **بساطة التنفيذ:** تعتمد الخوارزمية على عمليات واضحة وبسيطة مثل ترتيب الأعمدة، قلب البتات، والضغط.
2. إدخال المفتاح في عملية تبديل الأعمدة يضيف عنصرًا من التعقيد ويجعل النص المشفر يعتمد بشكل مباشر على المفتاح المستخدم، وهو ما يحقق خاصية الاعتماد على المفتاح.
3. **خاصية الانتشار:** أي إعادة توزيع البتات داخل المصفوفة وقلبها تؤدي إلى نشر تأثير التغيير في النص الصريح على كامل النص المشفر، مما يزيد من صعوبة التنبؤ بالعلاقة بين النصين.
4. **دمج التشفير مع الضغط:** إن إضافة مرحلة الضغط (RLE) بعد التشفير تقلل من حجم البيانات بنسبة ملحوظة، وهو ما يُعتبر ميزة عملية في تقليل استهلاك التخزين أو عرض النطاق الترددي.
5. **إمكانية التوسع:** يمكن تعديل طول المفتاح أو حجم المصفوفة بسهولة، مما يسمح بزيادة مستوى الأمان أو تحسين الأداء حسب الحاجة.

7-4- محاكاة الخوارزمية المقترحة

قمنا بمحاكاة الخوارزمية المقترحة باستخدام بيئة الماتلاب ونوضح المحاكاة لكل عملية من خلال مثال شامل.

- نفترض مفتاح سري عشوائي مثل [4,8,5,9,1,2].
- بفرض الجزء الاول من السلسلة الأصلية 101010.
- يتم إنشاء مصفوفة 6*6.
- وضع البتات في القطر الرئيسي.
- ملء الخانات المتبقية مع تجنب وضع 1 بجوار 1 أو 0 بجوار 0. فتكون مصفوفة الخرج كما هي موضحة في الشكل (7-1).



الشكل (7-1) المصفوفة الأصلية

وبناءاً على المفتاح السري العشوائي الذي تم افتراضه [485912] وعلى السلسلة التي تم ادخالها[101010]

فتكون التحويلات التي يجب ان تتم كالتالي:

العمود الأصلي 1 ← ينتقل إلى العمود 3 في المصفوفة الجديدة.

العمود الأصلي 2 ← ينتقل إلى العمود 5 في المصفوفة الجديدة.

العمود الأصلي 3 ← ينتقل إلى العمود 4 في المصفوفة الجديدة.

العمود الأصلي 4 ← ينتقل إلى العمود 6 في المصفوفة الجديدة.

العمود الأصلي 5 ← ينتقل إلى العمود 1 في المصفوفة الجديدة.

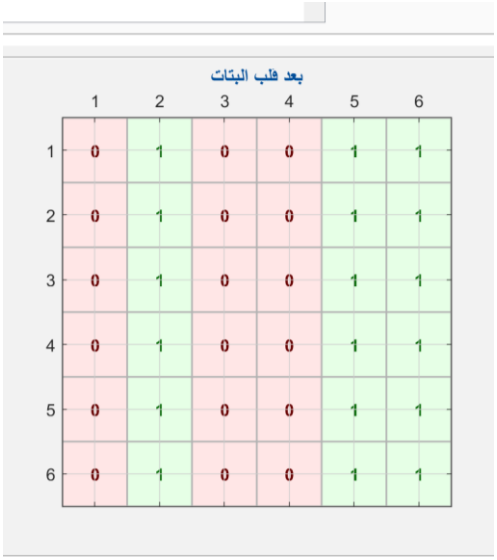
العمود الأصلي 6 ← ينتقل إلى العمود 2 في المصفوفة الجديدة.

يوضح الشكل (7–2) عملية تبديل الأعمدة وفق المفتاح السري.



الشكل (7-2) المصفوفة بعد تبديل الأعمدة

يتم بعد ذلك قلب البتات كما في الشكل (7–3)



الشكل (7-3) المصفوفة بعد قلب البتات

قراءة المصفوفة بترتيب عامودي ويكون الخرج كسلسلة خطية فتكون السلسلة الناتجة:

111111111110000000000001111110000000

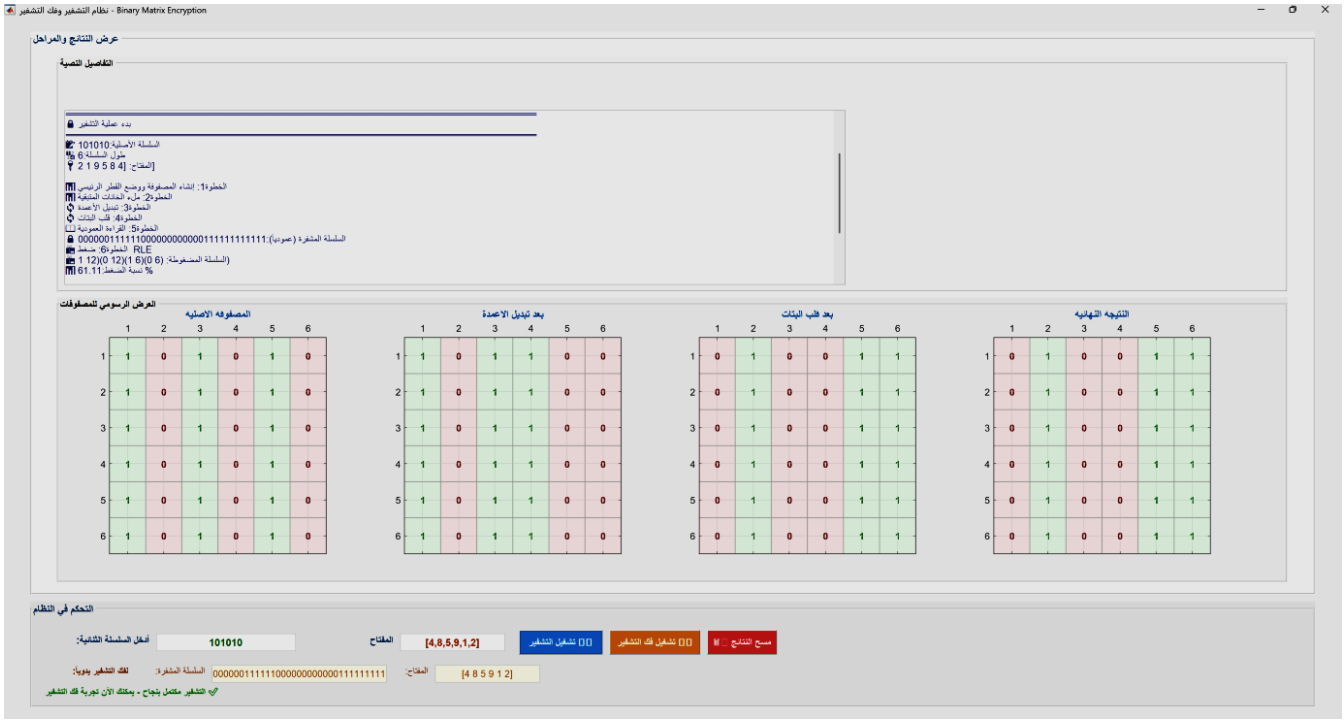
طول السلسلة الناتجة: 36 بت.

ضغط التسلسل الناتج باستخدام RLE ويكون خرج نتيجة ضغط RLE:

السلسلة المضغوطة: (6 0)(6 1)(12 0)(12 1)

نسبة الضغط : 61.11%

يوضح الشكل (7–4) واجهة المستخدم لعملية التشفير. يتم إدخال السلسلة المطلوب تشفيرها والمفتاح بعد ذلك يعرض المحاكي النتائج بشكل تفاصيل نصية وعرض رسومي للمصفوفات المطلوبة.



الشكل (7-4) واجهة المستخدم لعملية التشفير

7-5- محاكاة فك التشفير

يتم محاكاة فك التشفير ايضاً وفق واجهة المستخدم الموضحة في الشكل (7-5). تتم عملية فك التشفير بشكل عكسي لعملية التشفير حيث تتم القراءة العامودية وإنشاء المصفوفة ثم إعادة قلب البتات وإعادة الترتيب حتى يتم الحصول على المصفوفة الاصلية.



الشكل (7-5) واجهة المستخدم لعملية فك التشفير

7-6- التعقيد الزمني للخوارزمية المقترحة

سنقوم بدارسة التعقيد الزمني لكل خطوة في الخوارزمية المقترحة بشرح تفصيلي كما يلي:

1. توليد المفتاح

يقوم النموذج المقترح بتزويد الخوارزمية بمصفوفة التجاور وبذلك أول خطوة لنا التعقيد الزمني للنموذج المقترح ومع فكرة التسامح مع الأعطال له هي $T_1=O(n^2)$ بعد ذلك تبدأ الخوارزمية بتوليد السلسلة التي تشكل المفتاح وهنا كلفة الخطوة كحد أعلى إلى $T_2=O(m)$.

2. تجزئة البيانات

تقسيم البيانات إلى كتل كلفة الخطوة كحد أعلى O(L) حيث L طول البيانات.

3. ملء المصفوفة

كلفة إنشاء مصفوفة من البعد nxn كحد أعلى هو $O(n^2)$. كلفة ملء القطر الرئيسي هي O(n). وملء الخلايا المتبقية: $O(n^2)$. يكون تعقيد إجمالي المرحلة : $O(n^2)$.

4. تبديل الأعمدة

الحد الأعلى لكلفة تبديل الأعمدة هي $O(n^2)$.

5. قلب البتات

الحد الأعلى لكلفة قلب البتات هي $O(n^2)$، نكون بحاجة حلقتين تكراريتين لاستبدال البتات في المصفوفة.

6. القراءة العامودية

الحد الأعلى لكلفة قراءة جميع الخلايا عاموديا $O(n^2)$.

7. الضغط باستخدام RLE:

الحد الأعلى لكلفة الضغط باستخدام RLE هي $O(n^2)$. التعقيد الإجمالي لتشفير كتلة من البيانات هو $O(n^2)$.

7-7- مقارنة بين الخوارزمية المقترحة وخوارزميات سابقة

من أجل تقييم كفاءة الخوارزمية المقترحة، وبيان مدى ملاءمتها للتطبيق في شبكات الاستشعار اللاسلكية، تمت مقارنتها مع عدد من خوارزميات التشفير المعتمدة على نظرية البيان والمذكورة في الفقرة (2-8) ذلك باتباع معاير أساسية في المقارنة الموضحة في الجدول (7-1).

المعيار	خوارزمية التشفير باستخدام بيان أويلر	خوارزمية التشفير باستخدام تلوين البيان	خوارزمية تشفير تعتمد على مصفوفات التجاور	الخوارزمية المقترحة
نوع التشفير	متماثل	متماثل	متماثل	متماثل
مستوى التشفير	حرفي	على مستوى الرموز	نصي مع مفتاح بياني	كتلي
تمثيل البيانات	رسم بياني لكل حرف	بيان + مصفوفة تجاور	تمثيل عددي	مصفوفة nxn
العمليات الحسابية	عد+ تتبع مسار+XOR	إنشاء بيان + تلوين	ضرب مصفوفات	تبديل أعمدة+ قلب بتات
التعقيد الزمني	$O(n^2)$	مرتفع	$O(n^3)$	$O(n^2)$
استهلاك الذاكرة	مرتفع نسبياً	مرتفع نسبياً	متوسط	منخفض
الملاءمة لشبكات الاستشعار	متوسطة	ضعيفة	متوسطة	عالية

الجدول (7-1) مقارنة خوارزمية التشفير المقترحة مع خوارزميات تشفير أخرى

يبين جدول المقارنة أن خوارزمية التشفير المعتمدة على تحويل كل رمز إلى بيان، مثل خوارزمية Euler Graph، تؤدي إلى استهلاك الذاكرة وزيادة حجم البيانات المرسلة نتيجة الحاجة إلى أرسال مصفوفة تجاور لكل رمز. مما يؤدي إلى فرض عبء إضافي على الموارد المحدودة لعقد الاستشعار.

تعتمد خوارزمية التشفير باستخدام البيان على إنشاء بيان وتطبيق خوارزمية تلوين البيان عليه، وهي مشكلة من نوع Np−Complete مما يوفر أساساً نظرياً قوياً للأمان إلا أن هذا الأسلوب يفرض عبئاً حسابياً مرتفعاً. ونظراً لمحدودية الموارد الحسابية والطاقية في شبكات الاستشعار اللاسلكية، فإن الخوارزميات التي تعتمد على مشكلات معقدة مثل تلوين البيان تعد أقل ملاءمة للتطبيق العملي.

من جهة أخرى الخوارزمية التي تعتمد على مصفوفات التجاور على الرغم من أنها تتميز بأمان عالي لمن اعتمادها على ضرب المصفوفات يرفع من تعقيدها الحسابي. مما يقلل من ملاءمتها للتطبيق في البيئات محدودة الموارد.

استناداً إلى التحليل السابق، يمكن الاستنتاج أن الخوارزمية المقترحة تحقق توازناً أفضل بين مستوى الأمان والكفاءة الحسابية مقارنة بخوارزميات التشفير المعتمدة على نظرية البيان. فبينما توفر الخوارزميات البيانية أماناً أعلى، إلا أن الخوارزمية المقترحة تعد أكثر عملية وملاءمة للتطبيق في شبكات الاستشعار اللاسلكية، نظراً لانخفاض استهلاكها للموارد وتقليلها للعبء الاتصالي.

7-8- خلاصة الفصل

في هذا الفصل، قمنا بتطوير النموذج المقترح من خلال دمج خوارزمية تشفير مُصمَّمة خصيصًا لضمان حماية البيانات وملاءمتها لطبيعة وقدرات شبكات الاستشعار اللاسلكية. تندرج هذه الخوارزمية ضمن فئة التشفير المتماثل، وترتكز في أساسها على استخدام مصفوفة التجاور للبيان كأساس عملياتي. ولدراسة كفاءة الخوارزمية المقترحة، تم تنفيذها وتطبيقها في بيئة محاكاة MATLAB، حيث قمنا بتطوير برنامج كامل يعمل على عمليتي التشفير وفك التشفير للبيانات، مما يُتيح تحليل أدائها وفحص موثوقيتها بشكل عملي.

الخاتمة

قدمنا في هذا البحث نموذجاً رياضياً متكاملاً لتعزيز متانة وأداء شبكات الاستشعار اللاسلكية. انطلق البحث من تشخيص التحديات الرئيسية التي تواجه هذه الشبكات، والمتمثلة في طبيعة النشر العشوائي، وعدم تجانس العقد، وحتمية الأعطال خاصةً تلك المرتبطة باستنفاد الطاقة. قام البحث على أربعة أركان أساسية: أولا: تأسيس إطار نظري متين اشتمل على مفاهيم نظرية البيان، وخاصة البيان العشوائي الهندسي، وأسس التسامح مع الأعطال ومبادئ التشفير. ثانياً: التعرف على أعطال شبكات الاستشعار اللاسلكية. ثالثاً: تصميم وتطوير نموذج هرمي ديناميكي يحوّل الشبكة العشوائية إلى هيكل منظم، مع آليات ذكية لإدارة الطاقة واختيار المسارات المثلى. رابعاً: تطوير هذا النموذج ليكون متسامحاً مع الأعطال عبر تشكيل المكون العملاق، مع اقتراح خوارزمية تشفير مساعدة لتعزيز الأمن. أظهرت نتائج المحاكاة باستخدام برنامج الماتلاب فعالية النموذج المقترح في تحقيق أهدافه، حيث أسهم:

1. إطالة العمر التشغيلي للشبكة من خلال تحسين استهلاك الطاقة وتوزيع الحمل بشكل عادل.
2. الحفاظ على اتصال الشبكة تحت ظروف الأعطال المتعددة عبر آلية المكون العملاق.
3. تقديم تعقيد زمني مقبول للنموذج المطور مما يجعله قابلاً للتطبيق عملياً.

نتائج البحث

تكمن نتائج البحث بالنقاط الآتية:

1. تطوير نموذج رياضي جديد قائم على نظرية البيان العشوائي الهندسي لنمذجة شبكات الاستشعار اللاسلكية المنشورة عشوائياً وغير المتجانسة، مما يوفر تمثيلاً أكثر واقعية مقارنة بالنماذج التقليدية.
2. تحسين كفاءة إدارة الطاقة وإطالة العمر التشغيلي للشبكة من خلال آلية هرمية ديناميكية تقوم باختيار المسارات المثلى.

3. تحقيق تسامح فعّال مع الأعطال عبر آلية لتشكيل مكون عملاق ديناميكي ومتسامح مع الأعطال، يضمن استمرارية الاتصال الأساسي للشبكة حتى مع فقدان عدد من العقد، مع الحفاظ على قدرتها على نقل البيانات.
4. اقتراح خوارزمية تشفير مساعدة تعتمد على تحويل البيانات وتبديل المصفوفات مستوحاة من مفاهيم نظرية البيان، لتعزيز أمن البيانات المنقولة ضمن الإطار العام للنموذج.
5. التحقق العملي من فعالية النموذج عبر محاكاة شاملة باستخدام بيئة الماتلاب، حيث أظهرت النتائج تحسناً ملحوظاً في استهلاك الطاقة، وزيادة في عمر الشبكة، وقدرة عالية على الحفاظ على الاتصال تحت ظروف أعطال متعددة.
6. تحليل التعقيد الزمني للنموذج الأساسي والمطور، وأظهر التحليل تعقيداً مقبولاً بالنسبة لحجم الشبكة، مما يدعم قابليته للتطبيق.

التوصيات والمقترحات

يمكن التوجه في العمل المستقبلي إلى توسيع نطاق النموذج، أي تطوير النموذج ليعالج أنواعاً أوسع من الأعطال، مثل الأعطال الأمنية المعقدة، والعمل على تحسين التعقيد الزمني للنموذج المطور، دون المساس بفعالية النتائج بشكل كبير، والتكامل مع بروتوكولات قياسية، أي دراسة إمكانية دمج الآليات المقترحة (إدارة الطاقة، تشكيل المكون العملاق) مع بروتوكولات توجيه وإدارة طاقة معيارية معروفة في شبكات الاستشعار. والتطبيق العملي والاختبار الميداني: نقترح تحويل النموذج إلى حزمة برمجية قابلة للنشر على منصات عقد استشعار حقيقية، وإجراء تجارب ميدانية محدودة للتحقق من أدائه في بيئات حقيقية.

المراجع العلمية

[1] Martincic, F.; and Schwiebert, L. (2005). Introduction to wireless sensor networking. **In Handbook of sensor networks: Algorithms and architecture**. 1-40.

[2] Krishnaraj, N.; Kumar, R.B.; Rajeshwar, D.; Kumar, T.S. (2020). Implementation of energy aware modified distance vector routing protocol for energy efficiency in wireless sensor networks. **In 2020 International Conference on Inventive Computation Technologies (ICICT)**. 201-204. IEEE.

[3] Ramadan, W. (2019). Study about Graph Coloring. Master. Mathematics. Faculty of science. **Damascus: Syria**.1- 143.

[4] Amudha, P., Sagayaraj, A.C.C., & Sheela, A.C.S. (2018). An application of graph theory in cryptography. International Journal of Pure and Applied Mathematics, 119(13), 375-383

[5] Somkunwar, R.; Vaze, V. M. (2017). A Comparative Study of Graph Isomorphism Applications. **International Journal of Computer Applications**. Vol: 162, No:7. 34-37. St. Gallen: Switzerland Foundation of Computer Science.

[6] Vallier, T. (2007). **Random graph models and their applications**. Centre for Mathematical Sciences, Lund University.

[7] Newman, M.E.J. (2009). Random graphs with clustering. **Physical Review Letters**. Vol: 103, No: 5, 058701.

[8] Joos, F., Perarnau, G., Rautenbach, D. and Reed, B. (2018). How to determine if a random graph with a fixed degree sequence has a giant component. **Probability Theory and Related Fields**. Vol:170, No:1-2, 263-310.

[9] Zdeborova, L.; Krzakala, F. (2007). Phase transitions in the coloring of random graphs. **Physical Review E**. vol:76, No:3, 031131.

[10] Zhang, X.; Moore, C.; Newman, M. E. J. (2017). Random graph models for dynamic networks. **The European Physical Journal B**. Vol:90, No:1, 1-14.

[11] Bourke, C. (2015). Cryptography and computer security. **Department of Computer Science & Engineering, University of Nebraska–Lincoln**. (Lecture Notes).

[12] Bellare, M.; Rogaway, P. (2005). **Introduction to modern cryptography**. UC Davis. (Lecture Notes).

[13] National Institute of Standards and Technology (NIST). (2001). **Advanced Encryption Standard (AES)**. (FIPS Publication 197)

[14]Ghasem, F.; Yusif, G. (2016). Wireless Sensor Networks Architecture. **International Research Journal of Computer Science (IRJCS)**. Vol:3, No:1

[15] Sharma, D.; Verma, S.; Sharma, K. (2013). Network topologies in wireless sensor networks: A review. **International Journal of Electronics & Communication Technology**. Vol:4, No: Spl-3. 93-97.

[16] Akyildiz, I. F.; Su, W.; Sankarasubramaniam, Y.; Cayirci, E. (2002). Wireless sensor networks: A survey. **Computer Networks**. Vol:38 No:4. 393-422.

[17] García-Hernández, C. F.; Ibargiengoytia-González, P. H.; García-Hernández, J.; Pérez-Díaz, J. A. (2007). Wireless sensor networks and applications: a survey. **IJCSNS International Journal of Computer Science and Network Security**. Vol: 7, No:3, 264-273.

[18] Kamalakannan, S.; Amudha, P. (2016). A study of cryptography using graph theory. **Global Journal of Pure and Applied Mathematics**. Vol:12, No:2. 390-395.

[19]Krishnaraj, N.; Kumar, R.B.; Rajeshwar, D.; Kumar, T.S. (2020) Implementation of energy aware modified distance vector routing protocol for energy efficiency in wireless sensor networks. **In 2020 International Conference on Inventive Computation Technologies (ICICT)**. 201-204. IEEE.

[20] Alrajci, N.; Fu, H. (2014). A Survey on Fault Tolerance in Wireless Sensor Networks. **Proceedings of the 2014 ASEE North Central Section Conference**.

[21] Zhang, Z.; Mehmood, A.; Shu, L.; Huo, Z.; Zhang, Y.; Mukherjee, M. (2018). **A Survey on Fault Diagnosis in Wireless Sensor Networks**. IEEE Access. Vol: 6. 11350-11364.

[22] Mamatha, G., Premasudha, B. G.; Hegde, R. (2010). **A Graph Theory Approach to Load Balancing in Wireless Sensor Network**.

[23] Ameen, A. S.; Alheeti, K. M. A.; Aliesawi, S. A. (2020). **Employing Graph Theory in Enhancing Power Energy of Wireless Sensor Networks**. J. Inf. Sci. Eng.. Vol:36, No:2. 323-335.

[24] Ferrero, R.; Gandino, F. (2017). Analysis of random geometric graph for wireless network configuration. **Tenth International Conference on Mobile Computing and Ubiquitous Network (ICMU)**. 1-6. IEEE.

[25] Norman, J. (2011). Connectivity and coverage in hybrid wireless sensor networks using dynamic random geometric graph model. **International journal on applications of graph theory in wireless ad hoc networks and sensor networks**. Vol:3, No:3. 39.

[26] Fiergolla, S., & Wolf, P. (2021). **Improving run length encoding by preprocessing**. arXiv preprint arXiv:2101.05329.

[27] Li, B., &, S. (2022). Energy-Efficient Fault-Tolerant Routing in Wireless Sensor Networks. **IEEE Transactions on Wireless Communications**. Vol:3, No:21 ,1892-1905.

[28] Khan, A., Zhang, B., Li, C. and Chen, D. (2022). Lightweight Security Protocol for IoT-Based Wireless Sensor Networks. **IEEE Internet of Things Journal**, Vol: 9, No: 15, 13476-13486.

[29] Katti, A. (2022). Target coverage in random wireless sensor networks using cover sets. **Journal of King Saud University-Computer and Information Sciences**, Vol: 3, NO:34, 734–746.

[30] Xie, K., Ning, X., Wang, X., Xie, D., Cao, J. and Wen, J. (2020). Recover corrupted data in sensor networks: A matrix completion solution. **IEEE Transactions on Mobile Computing**, Vol 19(2), 273-289.

[31] Shukry, S. (2021). Stable routing and energy-conserved data transmission over wireless sensor networks. **EURASIP Journal on Wireless Communications and Networking**, Vol: 36, NO: 1.

[32] Nakas, C., Kandris, D., & Visvardis, G. (2020). **Energy efficient routing in wireless sensor networks: A comprehensive survey.** Algorithms, Vol: 13, No: 3, 72.

[33] Amudha, P.; Sagayaraj, A.C.C.; Sheela, A.C.S. (2018). An application of graph theory in cryptography. **International Journal of Pure and Applied Mathematics**. Vol: 119, No: 13, 380–384.

ملحق رقم(1)

يشمل الملحق برمجة النموذج المقترح باستخدام برنامج MATLAB 2015 بالإضافة لخوارزمية التشفير.

النموذج المقترح

```
%% إعداد بيئة المحاكاة الكاملة للنموذج المقترح
clear all; close all; clc;
warning('off', 'all');

disp('=== بدء محاكاة النموذج المقترح لشبكات الاستشعار اللاسلكية ===');

% المعلمات العامة
n = 100;
area_size = [0 100 0 100];
base_station = [50, 50];
simulation_time = 1000;
time_step = 10;

energy_params.initial_min = 0.40;
energy_params.initial_max = 0.60;
energy_params.elec = 50e-9;
energy_params.amp = 100e-12;
packet_size = 4000;

range_params.min = 15;
range_params.max = 25;

failure_params.tau0 = 0.0001;       % معدل فشل أقل
failure_params.critical_threshold = 0.7;
failure_params.threatened_threshold = 0.3;

%% 2. تهيئة العقد
disp('--- 2. بدء عملية النشر العشوائي للعقد ---');

nodes = struct();
nodes.id = zeros(n, 1);
nodes.position = zeros(n, 2);
nodes.range = zeros(n, 1);
nodes.initial_energy = zeros(n, 1);
nodes.current_energy = zeros(n, 1);
nodes.level = zeros(n, 1);
nodes.status = cell(n, 1);
nodes.parent = zeros(n, 1);
```

```
nodes.children = cell(n, 1);
nodes.neighbors = cell(n, 1);
nodes.failure_probability = zeros(n, 1);
nodes.failure_rate = zeros(n, 1);

for i = 1:n
   nodes.id(i) = i;
   nodes.position(i, :) = [rand*(area_size(2)-area_size(1)), ...
                           rand*(area_size(4)-area_size(3))];
   nodes.range(i) = range_params.min + rand*(range_params.max -
range_params.min);
   nodes.initial_energy(i) = energy_params.initial_min + ...
                             rand*(energy_params.initial_max - energy_params.initial_min);
   nodes.current_energy(i) = nodes.initial_energy(i);
   nodes.status{i} = 'active';
   nodes.children{i} = [];
   nodes.neighbors{i} = [];
end

% إضافة المحطة الأساسية
nodes.id(n+1) = n+1;
nodes.position(n+1, :) = base_station;
nodes.range(n+1) = 40;
nodes.initial_energy(n+1) = Inf;
nodes.current_energy(n+1) = Inf;
nodes.level(n+1) = 0;
nodes.status{n+1} = 'active';
nodes.parent(n+1) = 0;
nodes.children{n+1} = [];
nodes.neighbors{n+1} = [];

disp('--- 3. بناء الهيكل الهرمي للشبكة ---');

connection_matrix = zeros(n+1, n+1);
for i = 1:n+1
   for j = i+1:n+1
      distance = norm(nodes.position(i,:) - nodes.position(j,:));
      if distance <= nodes.range(i) && distance <= nodes.range(j)
         connection_matrix(i,j) = 1;
         connection_matrix(j,i) = 1;
         nodes.neighbors{i} = [nodes.neighbors{i}, j];
         nodes.neighbors{j} = [nodes.neighbors{j}, i];
      end
   end
end
```

```
% بناء المستويات الهرمية
level_matrix = cell(20, 1);
level_matrix{1} = n+1;

level1_nodes = [];
for i = 1:n
   if connection_matrix(i, n+1) == 1
      level1_nodes = [level1_nodes, i];
      nodes.level(i) = 1;
      nodes.parent(i) = n+1;
      nodes.children{n+1} = [nodes.children{n+1}, i];
   end
end

[~, sort_idx] = sort(nodes.initial_energy(level1_nodes), 'descend');
level1_nodes = level1_nodes(sort_idx);
level_matrix{2} = level1_nodes;

current_level = 1;
unassigned_nodes = setdiff(1:n, level1_nodes);

while ~isempty(unassigned_nodes)
   current_level_nodes = level_matrix{current_level+1};
   next_level_nodes = [];

   for parent_node = current_level_nodes
      for child_node = unassigned_nodes
         if connection_matrix(parent_node, child_node) == 1 &&
nodes.level(child_node) == 0
            nodes.level(child_node) = current_level + 1;
            nodes.parent(child_node) = parent_node;
            nodes.children{parent_node} = [nodes.children{parent_node}, child_node];
            next_level_nodes = [next_level_nodes, child_node];
         end
      end
   end

   if ~isempty(next_level_nodes)
      [~, sort_idx] = sort(nodes.initial_energy(next_level_nodes), 'descend');
      next_level_nodes = unique(next_level_nodes(sort_idx));
      level_matrix{current_level+2} = next_level_nodes;
      unassigned_nodes = setdiff(unassigned_nodes, next_level_nodes);
      current_level = current_level + 1;
   else
      break;
   end
```

```
end

num_levels = current_level;
disp(['تم بناء ' num2str(num_levels) ' مستويات هرمية']);

disp('--- 4. بدء محاكاة استهلاك الطاقة ونمذجة الفشل ---');

results = struct();
results.time = 0:time_step:simulation_time;
results.active_nodes = zeros(length(results.time), 1);
results.failed_nodes = zeros(length(results.time), 1);
results.avg_energy = zeros(length(results.time), 1);
results.giant_component_size = zeros(length(results.time), 1);
results.network_lifetime = 0;

results.active_nodes(1) = n;
results.failed_nodes(1) = 0;
results.avg_energy(1) = mean(nodes.current_energy(1:n));
results.giant_component_size(1) = n;

for t_idx = 2:length(results.time)
   current_time = results.time(t_idx);

   for i = 1:n
      if strcmp(nodes.status{i}, 'active')
         if nodes.current_energy(i) > 0
            energy_ratio = nodes.initial_energy(i) / max(nodes.current_energy(i),
0.001);
            nodes.failure_rate(i) = failure_params.tau0 * energy_ratio;
         else
            nodes.failure_rate(i) = 10;
         end

         nodes.failure_probability(i) = 1 - exp(-nodes.failure_rate(i) * current_time);
      end
   end

   % 2. محاكاة الفشل
   failed_this_step = 0;
   for i = 1:n
      if strcmp(nodes.status{i}, 'active')
         P_fail_step = 1 - exp(-nodes.failure_rate(i) * time_step);

         if rand < P_fail_step
            nodes.status{i} = 'failed';
            failed_this_step = failed_this_step + 1;
```

```
            % إعادة توجيه العقد التابعة
            for child_idx = nodes.children{i}
               best_parent = 0;
               min_distance = Inf;

               for potential_parent = 1:n+1
                  if potential_parent ~= i && ...
                    ~strcmp(nodes.status{potential_parent}, 'failed') && ...
                    connection_matrix(potential_parent, child_idx) == 1

                     distance = norm(nodes.position(child_idx,:) - ...
                                nodes.position(potential_parent,:));
                     if distance < min_distance
                        min_distance = distance;
                        best_parent = potential_parent;
                     end
                  end
               end

               if best_parent > 0
                  nodes.parent(child_idx) = best_parent;
                  nodes.children{best_parent} = [nodes.children{best_parent},
child_idx];
               end
            end
            nodes.children{i} = [];
         end
      end
   end

   % 3. حساب استهلاك الطاقة
   for i = 1:n
      if strcmp(nodes.status{i}, 'active')
         base_consumption = 0.001;

         if nodes.parent(i) > 0
            distance_to_parent = norm(nodes.position(i,:) -
nodes.position(nodes.parent(i),:));
            parent_consumption = packet_size * (energy_params.elec +
energy_params.amp * distance_to_parent^2);
         else
            parent_consumption = 0;
         end

         children_consumption = 0;
```

```
        for child_idx = nodes.children{i}
            distance_to_child = norm(nodes.position(i,:) - nodes.position(child_idx,:));
            children_consumption = children_consumption + ...
                packet_size * (energy_params.elec + energy_params.amp *
distance_to_child^2) * 0.1;
        end

        total_consumption = base_consumption + parent_consumption +
children_consumption;

        if total_consumption > nodes.current_energy(i) * 0.1
            total_consumption = nodes.current_energy(i) * 0.1;
        end

        nodes.current_energy(i) = nodes.current_energy(i) - total_consumption;

        if nodes.current_energy(i) < 0
            nodes.current_energy(i) = 0;
            nodes.status{i} = 'failed';
        end
    end
end

% 4. تحديث الإحصائيات
active_count = 0;
total_energy = 0;
for i = 1:n
    if strcmp(nodes.status{i}, 'active')
        active_count = active_count + 1;
        total_energy = total_energy + nodes.current_energy(i);
    end
end

results.active_nodes(t_idx) = active_count;
results.failed_nodes(t_idx) = n - active_count;

if active_count > 0
    results.avg_energy(t_idx) = total_energy / active_count;
else
    results.avg_energy(t_idx) = 0;
end

% 5. حساب المكون العملاق
visited = zeros(n+1, 1);
stack = [n+1];
giant_size = 0;
```

```
    while ~isempty(stack)
        current = stack(end);
        stack(end) = [];

        if ~visited(current)
            visited(current) = 1;
            if current <= n
                giant_size = giant_size + 1;
            end

            for neighbor_idx = nodes.neighbors{current}
                if ~visited(neighbor_idx) && ~strcmp(nodes.status{neighbor_idx}, 'failed')
                    stack = [stack, neighbor_idx];
                end
            end
        end
    end

    results.giant_component_size(t_idx) = giant_size;

    if active_count <= n/2 && results.network_lifetime == 0
        results.network_lifetime = current_time;
    end

    if mod(current_time, 100) == 0
        disp(['الزمن ' num2str(current_time) ': ' ...
              num2str(active_count) ' عقدة نشطة (' ...
              num2str(100*active_count/n, '%.1f') '%) | ' ...
              'متوسط الطاقة: ' num2str(results.avg_energy(t_idx), '%.3f') ' جول']);
    end
end

. ** عرض النتائج - **
disp('--- 5. عرض النتائج والرسوم البيانية ---');

figure('Position', [100, 100, 1200, 600]);

% ** الرسم 1: توزيع العقد والروابط **
subplot(2,3,1);
hold on;

plot(base_station(1), base_station(2), 'ks', 'MarkerSize', 20, ...
    'MarkerFaceColor', 'k', 'LineWidth', 2, 'DisplayName', 'المحطة الأساسية');

% 2. (للعقد النشطة فقط) أولاً: رسم جميع الروابط الهرمية
```

```
drawn_links = zeros(n+1, n+1);

active_nodes = find(strcmp({nodes.status{1:n}}, 'active'));
failed_nodes = find(strcmp({nodes.status{1:n}}, 'failed'));

for i = active_nodes
   if nodes.parent(i) > 0 && ~strcmp(nodes.status{nodes.parent(i)}, 'failed')
      if drawn_links(i, nodes.parent(i)) == 0
         parent_pos = nodes.position(nodes.parent(i), :);

         if nodes.parent(i) == n+1
            % رابط مع المحطة الأساسية
            line_color = [0.8 0.2 0.2]; % أحمر داكن
            line_width = 1.5;
            line_style = '-';
         else
            % رابط مع عقدة أخرى
            line_color = [0.2 0.2 0.8]; % أزرق
            line_width = 1;
            line_style = '-';
         end

         plot([nodes.position(i,1), parent_pos(1)], ...
              [nodes.position(i,2), parent_pos(2)], ...
              line_style, 'Color', line_color, 'LineWidth', line_width);

         drawn_links(i, nodes.parent(i)) = 1;
         drawn_links(nodes.parent(i), i) = 1;
      end
   end
end

level_colors = [
   0.2 0.8 0.2;   % المستوى 1: أخضر
   0.2 0.6 0.8;   % المستوى 2: أزرق
   0.8 0.6 0.2;   % المستوى 3: برتقالي
   0.8 0.2 0.6;   % المستوى 4: بنفسجي
   0.6 0.2 0.8;   % المستوى 5: أرجواني
];

for i = active_nodes
   if nodes.level(i) <= size(level_colors, 1)
      node_color = level_colors(nodes.level(i), :);
   else
      node_color = [0.5 0.5 0.5]; % رمادي للمستويات الأعلى
   end
```

```
    % تحديد حجم العقدة حسب الطاقة المتبقية
    energy_ratio = nodes.current_energy(i) / nodes.initial_energy(i);
    marker_size = 5 + 10 * energy_ratio;

    % رسم العقدة
    plot(nodes.position(i,1), nodes.position(i,2), 'o', ...
        'MarkerSize', marker_size, ...
        'MarkerFaceColor', node_color, ...
        'MarkerEdgeColor', 'k', ...
        'LineWidth', 1);
end

for i = failed_nodes
    plot(nodes.position(i,1), nodes.position(i,2), 'x', ...
        'MarkerSize', 10, 'Color', [0.8 0.1 0.1], ...
        'LineWidth', 2, 'DisplayName', 'عقد فاشلة');
end


theta = linspace(0, 2*pi, 100);
x_circle = nodes.range(n+1) * cos(theta) + base_station(1);
y_circle = nodes.range(n+1) * sin(theta) + base_station(2);
plot(x_circle, y_circle, ':', 'Color', [0.7 0.2 0.2], ...
    'LineWidth', 1, 'DisplayName', 'نطاق المحطة');

xlabel('المحور X (متر)');
ylabel('المحور Y (متر)');
title('توزيع العقد والهيكل الهرمي');
axis equal;
grid on;

h1 = plot(NaN, NaN, 'ks', 'MarkerSize', 10, 'MarkerFaceColor', 'k', 'DisplayName',
'المحطة الأساسية');
h2 = plot(NaN, NaN, 'o', 'MarkerSize', 8, 'MarkerFaceColor', [0.2 0.8 0.2], ...
        'MarkerEdgeColor', 'k', 'DisplayName', 'عقد نشطة (مستوى 1)');
h3 = plot(NaN, NaN, 'o', 'MarkerSize', 8, 'MarkerFaceColor', [0.2 0.6 0.8], ...
        'MarkerEdgeColor', 'k', 'DisplayName', 'عقد نشطة (مستوى 2+)');
h4 = plot(NaN, NaN, 'x', 'MarkerSize', 10, 'Color', [0.8 0.1 0.1], ...
        'LineWidth', 2, 'DisplayName', 'عقد فاشلة');
h5 = plot(NaN, NaN, '-', 'Color', [0.8 0.2 0.2], 'LineWidth', 1.5, 'DisplayName', 'روابط مع
المحطة');
h6 = plot(NaN, NaN, '-', 'Color', [0.2 0.2 0.8], 'LineWidth', 1, 'DisplayName', 'روابط
هرمية');

legend([h1, h2, h3, h4, h5, h6], 'Location', 'bestoutside');
```

```
xlim([0 100]);
ylim([0 100]);

% الرسم 2: العقد النشطة مع الزمن
subplot(2,3,2);
plot(results.time, results.active_nodes, 'b-', 'LineWidth', 2);
hold on;
plot(results.time, results.failed_nodes, 'r-', 'LineWidth', 2);
plot(results.time, results.giant_component_size, 'g-', 'LineWidth', 2);

if results.network_lifetime > 0
   plot([results.network_lifetime, results.network_lifetime], [0, n], 'k--', 'LineWidth',
1.5);
   text(results.network_lifetime, n/2, ['عمر الشبكة: ' num2str(results.network_lifetime)],
...
       'Rotation', 90, 'BackgroundColor', 'w', 'FontSize', 9);
end

xlabel('الزمن');
ylabel('عدد العقد');
title('ديناميكية العقد مع الزمن');
legend('عقد نشطة', 'عقد فاشلة', 'المكون العملاق', 'Location', 'best');
grid on;

% الرسم 3: متوسط الطاقة
subplot(2,3,3);
plot(results.time, results.avg_energy, 'm-', 'LineWidth', 2);
xlabel('الزمن');
ylabel('متوسط الطاقة المتبقية (جول)');
title('تطور الطاقة مع الزمن');
grid on;

% الرسم 4: توزيع المستويات
subplot(2,3,4);
level_counts = zeros(num_levels, 1);
for i = 1:n
   if nodes.level(i) > 0
      level_counts(nodes.level(i)) = level_counts(nodes.level(i)) + 1;
   end
end
bar(1:num_levels, level_counts, 'FaceColor', [0.2 0.6 0.8]);
xlabel('المستوى الهرمي');
ylabel('عدد العقد');
title('توزيع العقد على المستويات');
grid on;
```

```
% الرسم 5: الطاقة النهائية للعقد
subplot(2,3,5);
final_energy = nodes.current_energy(1:n);
active_idx = find(~strcmp({nodes.status{1:n}}, 'failed'));

if ~isempty(active_idx)
   % استخدام ألوان متدرجة حسب الطاقة
   [sorted_energy, sort_idx] = sort(final_energy(active_idx), 'descend');
   sorted_idx = active_idx(sort_idx);

   bar(1:length(sorted_idx), sorted_energy, 'FaceColor', 'flat');
   colormap(jet);

   % تلوين الأشرطة حسب الطاقة
   for k = 1:length(sorted_idx)
      % استخدام نفس شريط الألوان
   end

   xlabel('العقد النشطة (مرتبة تنازلياً حسب الطاقة)');
   ylabel('الطاقة المتبقية (جول)');
   title('الطاقة النهائية للعقد النشطة');
   grid on;
else
   bar(1, 0);
   xlabel('مؤشر العقدة');
   ylabel('الطاقة المتبقية (جول)');
   title('لا توجد عقد نشطة');
   grid on;
end

% الرسم 6: معدلات الفشل
subplot(2,3,6);
active_idx = find(strcmp({nodes.status{1:n}}, 'active'));
failed_idx = find(strcmp({nodes.status{1:n}}, 'failed'));

if ~isempty(active_idx)
   % رسم العقد النشطة بلون حسب الطاقة
   scatter(active_idx, nodes.failure_rate(active_idx), 50, ...
         nodes.current_energy(active_idx), 'filled');
   hold on;

   % رسم العقد الفاشلة باللون الرمادي
   if ~isempty(failed_idx)
      scatter(failed_idx, nodes.failure_rate(failed_idx), 40, ...
            [0.5 0.5 0.5], 'x', 'LineWidth', 2);
   end
```

```
    % إضافة خطوط إرشادية
    plot([0, n+1], [failure_params.tau0, failure_params.tau0], 'g--', 'LineWidth', 1);
    plot([0, n+1], [failure_params.tau0*5, failure_params.tau0*5], 'y--', 'LineWidth', 1);
    plot([0, n+1], [failure_params.tau0*10, failure_params.tau0*10], 'r--', 'LineWidth',
1);

    xlabel('مؤشر العقدة');
    ylabel('معدل الفشل');
    title('معدلات الفشل (اللون = الطاقة المتبقية)');
    colorbar;
    colormap(jet);
    set(gca, 'YScale', 'log');
    grid on;

    legend('عقد نشطة', 'عقد فاشلة', '??', '5??', '10??', 'Location', 'best');
else
    plot(1:n, nodes.failure_rate(1:n), 'r-', 'LineWidth', 2);
    xlabel('مؤشر العقدة');
    ylabel('معدل الفشل');
    title('معدلات الفشل (لا توجد عقد نشطة)');
    grid on;
end

%% 6. إضافة نافذة رسومية جديدة للتوضيح
figure('Position', [150, 150, 900, 700], 'Name', 'توضيح الهيكل الهرمي والاتصالات');

% مخطط شجري مبسط للهيكل الهرمي
subplot(2,2,1);
hold on;

% إنشاء هيكل شجري
tree_x = zeros(n+1, 1);
tree_y = zeros(n+1, 1);

% وضع المحطة الأساسية في الأعلى
tree_x(n+1) = 0;
tree_y(n+1) = num_levels + 1;

% وضع العقد حسب المستوى
for level = 1:num_levels
    level_nodes = find(nodes.level(1:n) == level);
    num_in_level = length(level_nodes);

    if num_in_level > 0
        % توزيع العقد أفقيًا في هذا المستوى
```

```
        x_positions = linspace(-num_in_level/2, num_in_level/2, num_in_level);

        for j = 1:num_in_level
            node_idx = level_nodes(j);
            tree_x(node_idx) = x_positions(j);
            tree_y(node_idx) = num_levels - level + 1;
        end
    end
end

% رسم الروابط
for i = 1:n
    if nodes.parent(i) > 0
        plot([tree_x(i), tree_x(nodes.parent(i))], ...
             [tree_y(i), tree_y(nodes.parent(i))], 'b-', 'LineWidth', 1);
    end
end

% رسم العقد
for i = 1:n+1
    if i == n+1
        % المحطة الأساسية
        plot(tree_x(i), tree_y(i), 'ks', 'MarkerSize', 20, ...
             'MarkerFaceColor', 'k', 'LineWidth', 2);
        text(tree_x(i), tree_y(i)+0.1, 'المحطة', ...
             'HorizontalAlignment', 'center', 'FontWeight', 'bold');
    elseif strcmp(nodes.status{i}, 'active')
        % العقد النشطة
        plot(tree_x(i), tree_y(i), 'o', 'MarkerSize', 8, ...
             'MarkerFaceColor', [0.2 0.8 0.2], 'MarkerEdgeColor', 'k');
        text(tree_x(i), tree_y(i)-0.15, num2str(i), ...
             'HorizontalAlignment', 'center', 'FontSize', 8);
    else
        % العقد الفاشلة
        plot(tree_x(i), tree_y(i), 'rx', 'MarkerSize', 10, 'LineWidth', 2);
        text(tree_x(i), tree_y(i)-0.15, num2str(i), ...
             'HorizontalAlignment', 'center', 'FontSize', 8, 'Color', 'r');
    end
end

% إضافة تسميات المستويات
for level = 0:num_levels
    text(-num_levels-1, num_levels - level + 1, ['المستوى ' num2str(level)], ...
         'HorizontalAlignment', 'right', 'FontWeight', 'bold');
end
```

```
axis equal off;
title('(الهيكل الهرمي للشبكة (تمثيل شجري)');
legend('روابط', 'المحطة الأساسية', 'عقد نشطة', 'عقد فاشلة', 'Location', 'best');

% مخطط المسافات من المحطة الأساسية
subplot(2,2,2);
distances = zeros(n, 1);
for i = 1:n
    distances(i) = norm(nodes.position(i,:) - base_station);
end

histogram(distances, 20, 'FaceColor', [0.4 0.6 0.8], 'EdgeColor', 'k');
xlabel('(المسافة من المحطة الأساسية (متر)');
ylabel('عدد العقد');
title('توزيع مسافات العقد من المحطة');
grid on;

% مخطط الطاقة المتبقية مقابل المسافة
subplot(2,2,3);
active_idx = find(strcmp({nodes.status{1:n}}, 'active'));
if ~isempty(active_idx)
    scatter(distances(active_idx), nodes.current_energy(active_idx), 40, ...
        nodes.failure_rate(active_idx), 'filled');
    xlabel('(المسافة من المحطة (متر)');
    ylabel('(الطاقة المتبقية (جول)');
    title('(الطاقة المتبقية مقابل المسافة (اللون = معدل الفشل)');
    colorbar;
    colormap(jet);
    grid on;
else
    text(0.5, 0.5, 'لا توجد عقد نشطة', 'HorizontalAlignment', 'center');
    axis off;
end

% مخطط عدد الأطفال لكل عقدة
subplot(2,2,4);
children_counts = zeros(n, 1);
for i = 1:n
    children_counts(i) = length(nodes.children{i});
end

active_idx = find(strcmp({nodes.status{1:n}}, 'active'));
if ~isempty(active_idx)
    bar(active_idx, children_counts(active_idx), 'FaceColor', [0.8 0.4 0.2]);
    xlabel('مؤشر العقدة النشطة');
    ylabel('عدد العقد التابعة');
```

```
    title('توزيع عدد العقد التابعة');
    grid on;
else
    text(0.5, 0.5, 'لا توجد عقد نشطة', 'HorizontalAlignment', 'center');
    axis off;
end

%% 7. عرض الإحصائيات المفصلة
disp(' ');
disp('======= الإحصائيات النهائية المفصلة =======');
disp(['إجمالي العقد: ' num2str(n)]);
disp(['العقد النشطة النهائية: ' num2str(results.active_nodes(end)) ...
      ' (' num2str(100*results.active_nodes(end)/n, '%.1f') '%)']);
disp(['العقد الفاشلة النهائية: ' num2str(results.failed_nodes(end)) ...
      ' (' num2str(100*results.failed_nodes(end)/n, '%.1f') '%)']);
disp(['عمر الشبكة (حتى فقدان 50%): ' num2str(results.network_lifetime)]);
disp(['حجم المكون العملاق النهائي: ' num2str(results.giant_component_size(end)) ...
      ' (' num2str(100*results.giant_component_size(end)/n, '%.1f') '%)']);
disp(['متوسط الطاقة النهائية: ' num2str(results.avg_energy(end), '%.3f') ' جول']);
disp(['عدد المستويات الهرمية: ' num2str(num_levels)]);

% إحصائيات إضافية
if ~isempty(active_idx)
    disp(' ');
    disp('--- إحصائيات العقد النشطة ---');
    disp(['الحد الأدنى للطاقة: ' num2str(min(nodes.current_energy(active_idx)), '%.3f') ' ...
جول']);
    disp(['الحد الأقصى للطاقة: ' num2str(max(nodes.current_energy(active_idx)), '%.3f') ' ...
جول']);
    disp(['متوسط عدد الأطفال: ' num2str(mean(children_counts(active_idx)), '%.2f')]);
    disp(['متوسط المسافة من المحطة: ' num2str(mean(distances(active_idx)), '%.2f') ' متر']);
end

%% 6. عرض الإحصائيات
disp(' ');
disp('======= الإحصائيات النهائية =======');
disp(['إجمالي العقد: ' num2str(n)]);
disp(['العقد النشطة النهائية: ' num2str(results.active_nodes(end)) ...
      ' (' num2str(100*results.active_nodes(end)/n, '%.1f') '%)']);
disp(['العقد الفاشلة النهائية: ' num2str(results.failed_nodes(end)) ...
      ' (' num2str(100*results.failed_nodes(end)/n, '%.1f') '%)']);
disp(['عمر الشبكة (حتى 50%): ' num2str(results.network_lifetime)]);
disp(['حجم المكون العملاق النهائي: ' num2str(results.giant_component_size(end)) ...
      ' (' num2str(100*results.giant_component_size(end)/n, '%.1f') '%)']);
disp(['متوسط الطاقة النهائية: ' num2str(results.avg_energy(end), '%.3f') ' جول']);
disp(['عدد المستويات الهرمية: ' num2str(num_levels)]);
```

```
%% 7. تحليل التعقيد
disp('--- 6. تحليل التعقيد الزمني ---');

complexity = struct();
complexity.hierarchical = n^2;  % بناء الهيكل: O(n²)
complexity.energy = n * (simulation_time/time_step);  % محاكاة الطاقة: O(nT)
complexity.failure = n * (simulation_time/time_step); % نمذجة الفشل: O(nT)
complexity.routing = n * mean(cellfun(@length, nodes.neighbors(1:n))); % التوجيه:
O(n×deg)

disp('تحليل التعقيد الزمني:');
disp(['بناء الهيكل الهرمي: O(n²) ? ' num2str(complexity.hierarchical) ' عملية']);
disp(['محاكاة الطاقة: O(nT) ? ' num2str(complexity.energy) ' عملية']);
disp(['نمذجة الفشل: O(nT) ? ' num2str(complexity.failure) ' عملية']);
disp(['إعادة التوجيه: O(n×deg) ? ' num2str(complexity.routing) ' عملية']);

total_ops = complexity.hierarchical + complexity.energy + complexity.failure +
complexity.routing;
disp(['الإجمالي التقريبي: ' num2str(total_ops) ' عملية']);

% تحليل متقدم للتعقيد
figure('Position', [100, 50, 800, 400]);
operations = [complexity.hierarchical; complexity.energy; complexity.failure;
complexity.routing];
labels = {'بناء الهيكل', 'محاكاة الطاقة', 'نمذجة الفشل', 'إعادة التوجيه'};

subplot(1,2,1);
bar(operations, 'FaceColor', [0.3 0.5 0.8]);
set(gca, 'XTickLabel', labels, 'XTickLabelRotation', 45);
ylabel('عدد العمليات');
title('توزيع التعقيد الزمني');
grid on;

subplot(1,2,2);
pie(operations, labels);
title('نسبة التعقيد الزمني (%)');


        fprintf(fid, 'الإحصائيات النهائية لمحاكاة النموذج المقترح\n');
        fprintf(fid, '========================================\n');
        fprintf(fid, 'تاريخ المحاكاة: %s\n', datestr(now));
        fprintf(fid, 'عدد العقد الكلي: %d\n', n);
        fprintf(fid, 'وقت المحاكاة: %d وحدة زمنية\n', simulation_time);
        fprintf(fid, 'العقد النشطة النهائية: %d (%.1f%%)\n', ...
            results.active_nodes(end), 100*results.active_nodes(end)/n);
        fprintf(fid, 'عمر الشبكة: %.2f\n', results.network_lifetime);
```

```
        fprintf(fid, 'حجم المكون العملاق: %d (%.1f%%)\n', ...
            results.giant_component_size(end), ...
100*results.giant_component_size(end)/n);
        fprintf(fid, 'متوسط الطاقة النهائية: %.3f جول\n', results.avg_energy(end));
        fprintf(fid, 'عدد المستويات الهرمية: %d\n', num_levels);

disp('=== انتهت المحاكاة بنجاح ===');
```

خوارزمية التشفير

```
function encryption_decryption_gui()
    % إنشاء النافذة الرئيسية
    fig = figure('Name', 'نظام التشفير وفك التشفير - Binary Matrix Encryption', ...
                 'NumberTitle', 'off', ...
                 'Position', [100, 100, 1400, 800], ...
                 'MenuBar', 'none', ...
                 'ToolBar', 'none', ...
                 'Resize', 'on', ...
                 'Color', [0.95, 0.95, 0.95]);

    % تعريف المتغيرات الرئيسية كخاصية للنافذة
    setappdata(fig, 'encryptionData', []);
    setappdata(fig, 'statusText', []);

    % إنشاء لوحة التحكم
    controlPanel = uipanel('Parent', fig, ...
                           'Title', 'التحكم في النظام', ...
                           'Position', [0.02, 0.02, 0.96, 0.15], ...
                           'FontSize', 12, ...
                           'FontWeight', 'bold', ...
                           'BackgroundColor', [0.9, 0.9, 0.9], ...
                           'ForegroundColor', [0, 0.2, 0.4]);

    % إنشاء لوحة العرض
    displayPanel = uipanel('Parent', fig, ...
                           'Title', 'عرض النتائج والمراحل', ...
                           'Position', [0.02, 0.18, 0.96, 0.80], ...
                           'FontSize', 12, ...
                           'FontWeight', 'bold', ...
                           'BackgroundColor', [1, 1, 1], ...
                           'ForegroundColor', [0, 0.2, 0.4]);

    % إنشاء عناصر الواجهة
    createGUIElements(fig, controlPanel, displayPanel);
```

```
% دالة إنشاء عناصر الواجهة
function createGUIElements(fig, controlPanel, displayPanel)
    handles = struct();

    % عناصر التحكم في لوحة التحكم
    uicontrol('Parent', controlPanel, ...
            'Style', 'text', ...
            'String', 'أدخل السلسلة الثنائية:', ...
            'Position', [20, 80, 150, 25], ...
            'HorizontalAlignment', 'right', ...
            'FontSize', 11, ...
            'BackgroundColor', [0.9, 0.9, 0.9], ...
            'ForegroundColor', [0, 0.2, 0.4], ...
            'FontWeight', 'bold');

    handles.binaryInput = uicontrol('Parent', controlPanel, ...
                        'Style', 'edit', ...
                        'String', '1010', ...
                        'Position', [180, 80, 200, 25], ...
                        'FontSize', 11, ...
                        'BackgroundColor', 'white', ...
                        'ForegroundColor', [0, 0.4, 0], ...
                        'FontWeight', 'bold');

    uicontrol('Parent', controlPanel, ...
            'Style', 'text', ...
            'String', 'المفتاح', ...
            'Position', [400, 80, 120, 25], ...
            'HorizontalAlignment', 'right', ...
            'FontSize', 11, ...
            'BackgroundColor', [0.9, 0.9, 0.9], ...
            'ForegroundColor', [0, 0.2, 0.4], ...
            'FontWeight', 'bold');

    handles.keyInput = uicontrol('Parent', controlPanel, ...
                    'Style', 'edit', ...
                    'String', '[4,8,5,9]', ...
                    'Position', [530, 80, 150, 25], ...
                    'FontSize', 11, ...
                    'BackgroundColor', 'white', ...
                    'ForegroundColor', [0.6, 0.2, 0], ...
                    'FontWeight', 'bold');

    % أزرار التحكم
    handles.encryptBtn = uicontrol('Parent', controlPanel, ...
                     'Style', 'pushbutton', ...
```

```
                'String', '    تشغيل التشفير', ...
                'Position', [700, 75, 120, 35], ...
                'FontSize', 11, ...
                'FontWeight', 'bold', ...
                'BackgroundColor', [0.1, 0.5, 0.8], ...
                'ForegroundColor', 'white', ...
                'Callback', @runEncryption);

handles.decryptBtn = uicontrol('Parent', controlPanel, ...
                'Style', 'pushbutton', ...
                'String', '    تشغيل فك التشفير', ...
                'Position', [830, 75, 130, 35], ...
                'FontSize', 11, ...
                'FontWeight', 'bold', ...
                'BackgroundColor', [0.8, 0.5, 0.1], ...
                'ForegroundColor', 'white', ...
                'Callback', @runDecryption);

handles.clearBtn = uicontrol('Parent', controlPanel, ...
                'Style', 'pushbutton', ...
                'String', '  مسح النتائج', ...
                'Position', [970, 75, 100, 35], ...
                'FontSize', 11, ...
                'FontWeight', 'bold', ...
                'BackgroundColor', [0.8, 0.2, 0.2], ...
                'ForegroundColor', 'white', ...
                'Callback', @clearResults);

% معلومات الإدخال اليدوي
uicontrol('Parent', controlPanel, ...
        'Style', 'text', ...
        'String', 'لفك التشفير يدوياً:', ...
        'Position', [20, 35, 120, 25], ...
        'HorizontalAlignment', 'right', ...
        'FontSize', 10, ...
        'BackgroundColor', [0.9, 0.9, 0.9], ...
        'ForegroundColor', [0.5, 0.2, 0], ...
        'FontWeight', 'bold');

uicontrol('Parent', controlPanel, ...
        'Style', 'text', ...
        'String', 'السلسلة المشفرة:', ...
        'Position', [150, 35, 100, 25], ...
        'HorizontalAlignment', 'right', ...
        'FontSize', 10, ...
        'BackgroundColor', [0.9, 0.9, 0.9], ...
```

```
        'ForegroundColor', [0.5, 0.2, 0]);

    handles.manualEncryptedInput = uicontrol('Parent', controlPanel, ...
                            'Style', 'edit', ...
                            'String', '', ...
                            'Position', [260, 35, 250, 25], ...
                            'FontSize', 10, ...
                            'BackgroundColor', [1, 1, 0.9], ...
                            'ForegroundColor', [0.6, 0.3, 0]);

    uicontrol('Parent', controlPanel, ...
            'Style', 'text', ...
            'String', 'المفتاح:', ...
            'Position', [520, 35, 50, 25], ...
            'HorizontalAlignment', 'right', ...
            'FontSize', 10, ...
            'BackgroundColor', [0.9, 0.9, 0.9], ...
            'ForegroundColor', [0.5, 0.2, 0]);

    handles.manualKeyInput = uicontrol('Parent', controlPanel, ...
                        'Style', 'edit', ...
                        'String', '', ...
                        'Position', [580, 35, 150, 25], ...
                        'FontSize', 10, ...
                        'BackgroundColor', [1, 1, 0.9], ...
                        'ForegroundColor', [0.6, 0.3, 0]);

    % حالة النظام
    handles.statusText = uicontrol('Parent', controlPanel, ...
                    'Style', 'text', ...
                    'String', 'جاهز... أدخل سلسلة ثنائية واضغط على زر التشفير', ...
                    'Position', [20, 5, 500, 25], ...
                    'HorizontalAlignment', 'left', ...
                    'FontSize', 10, ...
                    'BackgroundColor', [0.9, 0.9, 0.9], ...
                    'ForegroundColor', [0, 0.5, 0], ...
                    'FontWeight', 'bold');

    % منطقة عرض النتائج في لوحة العرض
    resultsPanel = uipanel('Parent', displayPanel, ...
                    'Title', 'التفاصيل النصية', ...
                    'Position', [0.02, 0.55, 0.96, 0.43], ...
                    'FontSize', 11, ...
                    'FontWeight', 'bold', ...
                    'BackgroundColor', [0.98, 0.98, 0.98]);
```

```
    handles.resultsText = uicontrol('Parent', resultsPanel, ...
                        'Style', 'edit', ...
                        'String', {'    مرحباً في نظام التشفير وفك التشفير باستخدام المصفوفات الثنائية'; ...
'═══════════════════════════════════════════════════════════════════════
═══'; ...
                                   '• أدخل سلسلة ثنائية (أصفار وواحدات)'; ...
                                   '• اضغط على زر "تشغيل التشفير" لبدء العملية'; ...
                        'Position', [10, 10, 1120, 250], ...
                        'FontSize', 10, ...
                        'BackgroundColor', [1, 1, 1], ...
                        'ForegroundColor', [0.1, 0.1, 0.4], ...
                        'HorizontalAlignment', 'left', ...
                        'Max', 100);

    % محاور للعرض الرسومي
    axesPanel = uipanel('Parent', displayPanel, ...
                        'Title', 'العرض الرسومي للمصفوفات', ...
                        'Position', [0.02, 0.02, 0.96, 0.52], ...
                        'FontSize', 11, ...
                        'FontWeight', 'bold', ...
                        'BackgroundColor', [0.95, 0.95, 0.95]);

    % إنشاء 4 محاور لعرض المراحل المختلفة
    handles.ax1 = axes('Parent', axesPanel, 'Position', [0.02, 0.1, 0.22, 0.8]);
    handles.ax2 = axes('Parent', axesPanel, 'Position', [0.26, 0.1, 0.22, 0.8]);
    handles.ax3 = axes('Parent', axesPanel, 'Position', [0.50, 0.1, 0.22, 0.8]);
    handles.ax4 = axes('Parent', axesPanel, 'Position', [0.74, 0.1, 0.22, 0.8]);

    % حفظ المقابض في بيانات التطبيق
    setappdata(fig, 'handles', handles);

    % تهيئة المحاور
    initializeAxes(handles);
end

% دالة تهيئة المحاور
function initializeAxes(handles)
    axesList = {'ax1', 'ax2', 'ax3', 'ax4'};
    titles = {'المصفوفة الأصلية', 'بعد تبديل الأعمدة', 'بعد قلب البتات', 'النتيجة النهائية'};

    for i = 1:4
        if isfield(handles, axesList{i}) && ishandle(handles.(axesList{i}))
            ax = handles.(axesList{i});
            cla(ax);
            set(ax, 'Color', [0.98, 0.98, 0.98]);
```

```
            text(0.5, 0.5, 'في انتظار البيانات...', ...
                'Parent', ax, ...
                'HorizontalAlignment', 'center', ...
                'FontSize', 12, ...
                'Color', [0.5, 0.5, 0.5]);
            title(ax, titles{i}, 'FontSize', 11, 'FontWeight', 'bold', 'Color', [0, 0.3, 0.6]);
            set(ax, 'XTick', [], 'YTick', [], 'Box', 'on');
        end
    end
end

% دالة لعرض المصفوفات بشكل منسق
function displayFormattedMatrix(ax, matrix, titleStr)
    if ishandle(ax)
        cla(ax);
        [n, m] = size(matrix);

        % عرض المصفوفة كجدول نصي
        if n <= 10 && m <= 10 % عرض المصفوفات الصغيرة فقط
            % خلفية المصفوفة
            imagesc(matrix, 'Parent', ax);
            colormap(ax, [1 1 1; 0.8 0.9 1]); % ألوان فاتحة

            % إضافة القيم كنص
            for i = 1:n
                for j = 1:m
                    if matrix(i,j) == 1
                        color = [0, 0.4, 0]; % أخضر غامق للواحدات
                        bgColor = [0.9, 1, 0.9]; % خلفية خضراء فاتحة
                    else
                        color = [0.4, 0, 0]; % أحمر غامق للأصفار
                        bgColor = [1, 0.9, 0.9]; % خلفية حمراء فاتحة
                    end

                    % رسم خلفية للخلية
                    rectangle('Position', [j-0.5, i-0.5, 1, 1], ...
                              'FaceColor', bgColor, ...
                              'EdgeColor', [0.7, 0.7, 0.7], ...
                              'LineWidth', 1, ...
                              'Parent', ax);

                    % إضافة النص
                    text(j, i, sprintf('%d', matrix(i,j)), ...
                        'HorizontalAlignment', 'center', ...
                        'VerticalAlignment', 'middle', ...
                        'FontSize', max(10, 14 - n), ...
```

```
                'FontWeight', 'bold', ...
                'Color', color, ...
                'Parent', ax);
        end
    end

    axis(ax, 'equal');
    axis(ax, 'tight');
    set(ax, 'XTick', 1:m, 'YTick', 1:n, ...
        'XAxisLocation', 'top', ...
        'GridLineStyle', '-', ...
        'GridColor', [0.8, 0.8, 0.8], ...
        'GridAlpha', 1);
    grid(ax, 'on');

  else
    % عرض بسيط، للمصفوفات الكبيرة
    imagesc(matrix, 'Parent', ax);
    colormap(ax, [1 1 1; 0 0 0]);
    colorbar(ax);
  end

  title(ax, titleStr, 'FontSize', 12, 'FontWeight', 'bold', 'Color', [0, 0.3, 0.6]);
 end
end

% دالة تحديث الحالة
function updateStatus(message, color)
 handles = getappdata(gcbf, 'handles');
 if isfield(handles, 'statusText') && ishandle(handles.statusText)
  set(handles.statusText, 'String', message, 'ForegroundColor', color);
  drawnow;
 end
end

% دالة التشفير
function runEncryption(~, ~)
 try
  updateStatus('   جاري معالجة البيانات...', [0, 0.5, 0]);

  % الحصول على المقابض
  handles = getappdata(gcbf, 'handles');

  if ~isfield(handles, 'binaryInput') || ~ishandle(handles.binaryInput)
   updateResults('خطأ: لم يتم العثور على عنصر إدخال السلسلة ');
   return;
```

```
        end

        % الحصول على المدخلات مباشرة من المقابض
        binaryStr = get(handles.binaryInput, 'String');
        keyStr = get(handles.keyInput, 'String');

        % التحقق من صحة السلسلة الثنائية
        if isempty(binaryStr)
            updateResults('خطأ: يجب إدخال سلسلة ثنائية ');
            updateStatus('خطأ في الإدخال', [1, 0, 0]);
            return;
        end

        if ~all(ismember(binaryStr, '01'))
            updateResults('خطأ: يجب أن تحتوي السلسلة على الأصفار والواحدات فقط ');
            updateStatus('خطأ في الإدخال', [1, 0, 0]);
            return;
        end

        n = length(binaryStr);

        % معالجة المفتاح
        if ~isempty(keyStr)
            try
                key = eval(keyStr);
                if length(key) ~= n
                    updateResults('خطأ: طول المفتاح يجب أن يساوي طول السلسلة ');
                    updateStatus('خطأ في المفتاح', [1, 0, 0]);
                    return;
                end
            catch
                updateResults('خطأ: تنسيق المفتاح غير صحيح ');
                updateStatus('خطأ في المفتاح', [1, 0, 0]);
                return;
            end
        else
            key = randperm(n);
        end

        % بدء التشفير

updateResults('═══════════════════════════════════════════════════════
═══════════');
        updateResults('    بدء عملية التشفير');
```

```
updateResults('═══════════════════════════════════════════════════════
═══════════');
        updateResults(sprintf('   السلسلة الأصلية: %s', binaryStr));
        updateResults(sprintf('   طول السلسلة: %d', n));
        updateResults(sprintf('   المفتاح: %s', mat2str(key)));
        updateResults('');

        % الخطوة 1: إنشاء المصفوفة
        updateResults('   الخطوة 1: إنشاء المصفوفة ووضع القطر الرئيسي');
        matrix = zeros(n, n);
        for i = 1:n
            matrix(i, i) = str2double(binaryStr(i));
        end

        % الخطوة 2: ملء المصفوفة
        updateResults('   الخطوة 2: ملء الخانات المتبقية');
        for i = 1:n
            for j = 1:n
                if i ~= j
                    if mod(i + j, 2) == 0
                        matrix(i, j) = matrix(i, i);
                    else
                        matrix(i, j) = 1 - matrix(i, i);
                    end
                end
            end
        end

        % الخطوة 3: تبديل الأعمدة
        updateResults('   الخطوة 3: تبديل الأعمدة');

        % فرز المفتاح تصاعدياً
        [sorted_key, indices] = sort(key);

        % إنشاء مصفوفة جديدة
        permuted_matrix = zeros(n, n);

        % تطبيق تبديل الأعمدة
        for i = 1:n
            for j = 1:n
                % نبحث عن موضع j في المفتاح الأصلي
                original_col_idx = find(key == sorted_key(j), 1);
                permuted_matrix(i, j) = matrix(i, original_col_idx);
            end
```

```
end

% الخطوة 4: قلب البتات
updateResults('الخطوة 4: قلب البتات ');
flipped_matrix = 1 - permuted_matrix;

% الخطوة 5: القراءة العمودية
updateResults('الخطوة 5: القراءة العمودية ');
col_reading = [];
for j = 1:n
    current_col = flipped_matrix(:, j);  % الحصول على العمود j
    col_reading = [col_reading, current_col'];  % إضافة العمود (محول إلى صف)
end

encrypted_str = num2str(col_reading);
encrypted_str = encrypted_str(encrypted_str ~= ' ');
updateResults(sprintf('السلسلة المشفرة (عمودياً): %s', encrypted_str));

% الخطوة 6: ضغط RLE
updateResults('الخطوة 6: ضغط RLE');
[compressed_str, compression_ratio] = rle_compress(encrypted_str);
updateResults(sprintf('السلسلة المضغوطة: %s', compressed_str));
updateResults(sprintf('نسبة الضغط: %.2f%%', compression_ratio));

% حفظ البيانات
encryptionData = struct();
encryptionData.original = binaryStr;
encryptionData.key = key;
encryptionData.encrypted = encrypted_str;
encryptionData.compressed = compressed_str;
encryptionData.n = n;
encryptionData.matrix = matrix;
encryptionData.permuted_matrix = permuted_matrix;
encryptionData.flipped_matrix = flipped_matrix;
encryptionData.reading_mode = 'column';  % إضافة علامة للقراءة العمودية

setappdata(gcbf, 'encryptionData', encryptionData);

% عرض الملخص
updateResults('');
updateResults('□ ملخص التشفير');
updateResults('──────────────────────────────────────');
updateResults(sprintf('□ السلسلة الأصلية: %s', binaryStr));
updateResults(sprintf('المفتاح: %s', mat2str(key)));
updateResults(sprintf('السلسلة المشفرة: %s', encrypted_str));
```

```
        updateResults(sprintf('   السلسلة المضغوطة: %s', compressed_str));
        updateResults(sprintf('   2.% :نسبة الضغطf%%', compression_ratio));
        updateResults('');

        % تحديث المدخلات اليدوية
        if isfield(handles, 'manualEncryptedInput') && ishandle(handles.manualEncryptedInput)
            set(handles.manualEncryptedInput, 'String', encrypted_str);
        end
        if isfield(handles, 'manualKeyInput') && ishandle(handles.manualKeyInput)
            set(handles.manualKeyInput, 'String', mat2str(key));
        end

        % عرض النتائج رسومياً
        displayEncryptionResults(handles, matrix, permuted_matrix, flipped_matrix, flipped_matrix);

        updateStatus('✓ التشفير مكتمل بنجاح - يمكنك الآن تجربة فك التشفير', [0, 0.5, 0]);

    catch ME
        updateResults(sprintf('✗ خطأ أثناء التشفير: %s', ME.message));
        updateStatus('✗ خطأ في التشفير', [1, 0, 0]);
    end
end

% دالة العرض الرسومي للتشفير
function displayEncryptionResults(handles, matrix, permuted, flipped, final)
    if isfield(handles, 'ax1') && ishandle(handles.ax1)
        displayFormattedMatrix(handles.ax1, matrix, 'المصفوفة الأصلية');
    end
    if isfield(handles, 'ax2') && ishandle(handles.ax2)
        displayFormattedMatrix(handles.ax2, permuted, 'بعد تبديل الأعمدة');
    end
    if isfield(handles, 'ax3') && ishandle(handles.ax3)
        displayFormattedMatrix(handles.ax3, flipped, 'بعد قلب البتات');
    end
    if isfield(handles, 'ax4') && ishandle(handles.ax4)
        displayFormattedMatrix(handles.ax4, final, 'النتيجة النهائية');
    end
end

% دالة فك التشفير
function runDecryption(~, ~)
    try
        updateStatus('   جاري فك التشفير...', [0, 0.5, 0]);
```

```
        handles = getappdata(gcbf, 'handles');
        encryptionData = getappdata(gcbf, 'encryptionData');

        if isempty(encryptionData)
            if ~isfield(handles, 'manualEncryptedInput') || ~ishandle(handles.manualEncryptedInput)
                updateResults('خطأ: لم يتم العثور على عناصر الإدخال اليدوي');
                return;
            end

            encryptedStr = get(handles.manualEncryptedInput, 'String');
            keyStr = get(handles.manualKeyInput, 'String');

            % التحقق من صحة الإدخال
            if isempty(encryptedStr)
                updateResults('خطأ: يجب إدخال السلسلة المشفرة');
                updateStatus('خطأ في الإدخال', [1, 0, 0]);
                return;
            end

            if isempty(keyStr)
                updateResults('خطأ: يجب إدخال المفتاح');
                updateStatus('خطأ في المفتاح', [1, 0, 0]);
                return;
            end

            % التحقق من أن السلسلة تحتوي على أرقام فقط
            if ~all(ismember(encryptedStr, '0123456789'))
                updateResults('خطأ: السلسلة المشفرة يجب أن تحتوي على أرقام فقط');
                updateStatus('خطأ في السلسلة', [1, 0, 0]);
                return;
            end

            try
                key = eval(keyStr);
                if ~isvector(key)
                    updateResults('خطأ: المفتاح يجب أن يكون مصفوفة أحادية');
                    updateStatus('خطأ في المفتاح', [1, 0, 0]);
                    return;
                end
            catch
                updateResults('خطأ: تنسيق المفتاح غير صحيح');
                updateStatus('خطأ في المفتاح', [1, 0, 0]);
                return;
```

```
        end

        % محاولة استخراج حجم المصفوفة
        n = sqrt(length(encryptedStr));
        if mod(n, 1) ~= 0
            % نحاول فك الضغط أولاً RLE قد تكون السلسلة مضغوطة ،
            updateResults('⚠ السلسلة قد تكون مضغوطة، جاري محاولة فك الضغط...');
            try
                decompressed_str = rle_decompress(encryptedStr);
                updateResults(sprintf('✓ تم فك الضغط: %s', decompressed_str));

                n = sqrt(length(decompressed_str));
                if mod(n, 1) ~= 0
                    updateResults('✗ خطأ: طول السلسلة غير مناسب لإنشاء مصفوفة مربعة');
                    updateStatus('خطأ في الطول', [1, 0, 0]);
                    return;
                end
                n = round(n);
                encrypted_str = decompressed_str;
                compressed_str = encryptedStr;
            catch
                updateResults('✗ خطأ: طول السلسلة غير مناسب لإنشاء مصفوفة مربعة');
                updateStatus('خطأ في الطول', [1, 0, 0]);
                return;
            end
        else
            n = round(n);
            encrypted_str = encryptedStr;
            compressed_str = '';
        end

        % التحقق من تطابق طول المفتاح مع حجم المصفوفة
        if length(key) ~= n
            updateResults(sprintf('✗ خطأ: طول المفتاح (%d) يجب أن يساوي حجم المصفوفة
(%d)', length(key), n));
            updateStatus('خطأ في المفتاح', [1, 0, 0]);
            return;
        end

        reading_mode = 'column';  % الافتراضي للقراءة العمودية

    else
        % استخدام بيانات التشفير السابقة
        encrypted_str = encryptionData.encrypted;
        compressed_str = encryptionData.compressed;
```

```
            key = encryptionData.key;
            n = encryptionData.n;
            reading_mode = 'column';  % تم التشفير بعمودياً
        end

        % بدء فك التشفير

updateResults('═══════════════════════════════════════════════════════
═══════════');
        updateResults('    بدء عملية فك التشفير');

updateResults('═══════════════════════════════════════════════════════
═══════════');
        updateResults(sprintf('    السلسلة المشفرة: %s', encrypted_str));
        updateResults(sprintf('    المفتاح: %s', mat2str(key)));
        updateResults(sprintf('    حجم المصفوفة: %dx%d', n, n));
        updateResults(sprintf('    نمط القراءة: %s', reading_mode));
        updateResults('');

        expected_length = n * n;
        if length(encrypted_str) ~= expected_length
            updateResults(sprintf('□ خطأ: طول السلسلة (%d) لا يتطابق مع الحجم المتوقع (%d = %dx%d)', ...
                length(encrypted_str), expected_length, n, n));
            updateStatus('خطأ في الطول', [1, 0, 0]);
            return;
        end

        if ~isempty(compressed_str) && length(compressed_str) < length(encrypted_str)
            updateResults('    الخطوة 1: فك ضغط RLE');
            decompressed_str = rle_decompress(compressed_str);
            updateResults(sprintf('    السلسلة بعد فك الضغط: %s', decompressed_str));

            if length(decompressed_str) ~= expected_length
                updateResults(sprintf('□ خطأ: طول السلسلة بعد فك الضغط (%d) لا يتطابق مع الحجم المتوقع (%d)', ...
                    length(decompressed_str), expected_length));
                updateStatus('خطأ في الطول', [1, 0, 0]);
                return;
            end

            working_str = decompressed_str;
        else
            working_str = encrypted_str;
```

```
end

updateResults('الخطوة 2: إعادة بناء المصفوفة من القراءة العمودية');
matrix_after_flip = zeros(n, n);

if strcmp(reading_mode, 'column')
    % القراءة كانت عمودية
    for j = 1:n
        start_idx = (j-1)*n + 1;
        end_idx = j*n;
        col_str = working_str(start_idx:end_idx);
        for i = 1:n
            matrix_after_flip(i, j) = str2double(col_str(i));
        end
    end
else
    for i = 1:n
        start_idx = (i-1)*n + 1;
        end_idx = i*n;
        row_str = working_str(start_idx:end_idx);
        for j = 1:n
            matrix_after_flip(i, j) = str2double(row_str(j));
        end
    end
end

updateResults('الخطوة 3: إعادة قلب البتات');
matrix_after_permute = 1 - matrix_after_flip;

updateResults('الخطوة 4: إعادة ترتيب الأعمدة');

[sorted_key, ~] = sort(key);

original_matrix = zeros(n, n);

for i = 1:n
    for j = 1:n
        original_col_idx = find(key == sorted_key(j), 1);
        original_matrix(i, original_col_idx) = matrix_after_permute(i, j);
    end
end

updateResults('الخطوة 5: استخراج السلسلة الأصلية');
original_binary = '';
for i = 1:n
    original_binary = [original_binary, num2str(original_matrix(i, i))];
```

```
        end
        updateResults(sprintf('□ السلسلة المستخرجة: %s', original_binary));

        if ~isempty(encryptionData)
            updateResults('');
            updateResults('    التحقق من النتائج');
            updateResults('═══════════════════════════════════════');
            updateResults(sprintf('    السلسلة الأصلية: %s', encryptionData.original));
            updateResults(sprintf('    السلسلة المستخرجة: %s', original_binary));

            if strcmp(original_binary, encryptionData.original)
                updateResults('    فك التشفير ناجح!');
                updateStatus('□ فك التشفير ناجح - تم استعادة السلسلة الأصلية', [0, 0.5, 0]);
            else
                updateResults('□ فك التشفير فاشل!');
                updateStatus('□ فك التشفير فاشل', [1, 0, 0]);
            end
        else
            updateResults(sprintf('□ تم استخراج السلسلة: %s', original_binary));
            updateStatus('□ فك التشفير مكتمل', [0, 0.5, 0]);
        end

        displayDecryptionResults(handles, matrix_after_flip, matrix_after_permute,
original_matrix, original_matrix);

    catch ME
        updateResults(sprintf('□ خطأ أثناء فك التشفير: %s', ME.message));
        updateResults(sprintf('    تفاصيل الخطأ: في السطر %d', ME.stack(1).line));
        updateStatus('□ خطأ في فك التشفير', [1, 0, 0]);
    end
end

function displayDecryptionResults(handles, after_flip, after_permute, original,
final)
    if isfield(handles, 'ax1') && ishandle(handles.ax1)
        displayFormattedMatrix(handles.ax1, after_flip, 'بعد القراءة العمودية');
    end
    if isfield(handles, 'ax2') && ishandle(handles.ax2)
        displayFormattedMatrix(handles.ax2, after_permute, 'بعد إعادة القلب');
    end
    if isfield(handles, 'ax3') && ishandle(handles.ax3)
        displayFormattedMatrix(handles.ax3, original, 'بعد إعادة الترتيب');
    end
    if isfield(handles, 'ax4') && ishandle(handles.ax4)
```

```
        displayFormattedMatrix(handles.ax4, final, 'المصفوفة المستعادة');
    end
end

function updateResults(newText)
    handles = getappdata(gcbf, 'handles');
    if isfield(handles, 'resultsText') && ishandle(handles.resultsText)
        currentText = get(handles.resultsText, 'String');

        if ischar(currentText)
            currentText = {currentText};
        end

        if ischar(newText)
            newText = {newText};
        end

        set(handles.resultsText, 'String', [currentText; newText]);
        drawnow;

        try
            allText = get(handles.resultsText, 'String');
            if iscell(allText)
                set(handles.resultsText, 'ListboxTop', length(allText));
            end
        catch
        end
    end
end

function clearResults(~, ~)
    handles = getappdata(gcbf, 'handles');

    if isfield(handles, 'resultsText') && ishandle(handles.resultsText)
        set(handles.resultsText, 'String', { ...
            '   نظام التشفير وفك التشفير باستخدام المصفوفات الثنائية'; ...
            '});
    end

    if isfield(handles, 'ax1') && ishandle(handles.ax1)
        initializeAxes(handles);
    end

    setappdata(gcbf, 'encryptionData', []);
  if isfield(handles,'manualEncryptedInput')&&
ishandle(handles.manualEncryptedInput)
```

```
        set(handles.manualEncryptedInput, 'String', '');
    end
    if isfield(handles, 'manualKeyInput') && ishandle(handles.manualKeyInput)
        set(handles.manualKeyInput, 'String', '');
    end

    updateStatus('جاهز... أدخل سلسلة ثنائية جديدة', [0, 0.5, 0]);
end

% دوال الضغط وفك الضغط (نسخة بديلة أكثر قوة)
function [compressed, ratio] = rle_compress(input_str)
    try
        if isempty(input_str)
            compressed = '';
            ratio = 0;
            return;
        end

        compressed = '';
        count = 1;
        current_char = input_str(1);

        for i = 2:length(input_str)
            if input_str(i) == current_char
                count = count + 1;
            else
                % Format: (count space char)
                compressed = [compressed, sprintf('(%d %c)', count, current_char)];
                current_char = input_str(i);
                count = 1;
            end
        end

        % Add the last sequence
        compressed = [compressed, sprintf('(%d %c)', count, current_char)];
        ratio = (length(compressed) / length(input_str)) * 100;

    catch ME
        compressed = input_str;
        ratio = 100;
        fprintf('خطأ في الضغط: %s\n', ME.message);
    end
end

function decompressed = rle_decompress(compressed_str)
    decompressed = '';
```

```
    % Find all patterns matching (number space 0/1)
    tokens = regexp(compressed_str, '\((\d+)\s+([01])\)', 'tokens');

    for k = 1:length(tokens)
        token = tokens{k};
        count = str2double(token{1});
        char_val = token{2};
        decompressed = [decompressed, repmat(char_val, 1, count)];
    end

    % Fallback if regex doesn't work
    if isempty(decompressed) && ~isempty(compressed_str)
        decompressed = manual_decompress(compressed_str);
    end
end

function decompressed = manual_decompress(compressed_str)
    decompressed = '';
    i = 1;
    len = length(compressed_str);

    while i <= len
        % Find opening parenthesis
        if compressed_str(i) == '('
            % Find closing parenthesis
            j = find(compressed_str(i:end) == ')', 1);
            if isempty(j)
                break;
            end
            j = i + j - 1;

            % Extract content between parentheses
            content = compressed_str(i+1:j-1);

            % Split by space
            parts = strsplit(strtrim(content), ' ');

            if length(parts) >= 2
                count = str2double(parts{1});
                char_val = parts{2};

                if ~isnan(count) && (char_val == '0' || char_val == '1')
                    decompressed = [decompressed, repmat(char_val, 1, count)];
                end
            end
```

```
            i = j + 1;
        else
            i = i + 1;
        end
    end
end
    end

% تشغيل الواجهة
encryption_decryption_gui();
```

Abstract

Wireless sensor networks are critical systems deployed across various fields. Ensuring their continuous operation despite node failures is essential. Random deployment in challenging environments increases vulnerability to faults. This thesis develops a mathematical-algorithmic model for fault tolerance in randomly deployed, heterogeneous wireless sensor networks using random geometric graph theory. The research aims to enhance network robustness and lifespan through improved energy management and automated fault handling. A hierarchical multi-level model is proposed, featuring energy-aware mechanisms and the formation of a fault-tolerant giant component. A graph-based encryption algorithm is also introduced. Simulations in MATLAB confirm the model's effectiveness in reducing energy consumption, extending network lifetime, and maintaining connectivity during faults, with acceptable time complexity.

Keywords: Wireless Sensor Networks, Fault Tolerance, Graph Theory, Random Geometric Graph, Network Modeling, Energy Management, Giant Component, Mathematical Simulation.

Syrian Arab Republic

Damascus University

Faculty of Science

Department of Mathematics

Graph Theory and Its Applications in Mitigating Wireless Sensor Network Problems

A dissertation submitted in partial fulfillment of the requirements for the degree of PhD in Mathematics

by

Alaa Hassan SALAMEH

Supervisor

Dr.Samir Jafar

Associate professor at the Department of Mathematics - Faculty of Science

(2025-2026)