الجمهورية العربية السورية
المعهد العالي للعلوم التطبيقية والتكنولوجيا
قسم الاتصالات

التعمية المعتمدة على الشبكة واستخدامها في الشبكات اللاسلكية المخصصة النقالة

Lattice Based Cryptography for MANET

أعد هذا البحث لنيل شهادة الماجستير في نظم الاتصالات

الإعداد

م. علاء معلا

الإشراف

د. أميمة الدكاك د. محمد الجنيدي

تشرين الأول 2016

كـلـمـة شـكـر

جزيـل الشـكر وعظـيم الامتنـان للـدكتورة أميمـة الـدكاك، والـدكتور محمـد الجنيـدي. الـذين تفضـلا بالإشـراف علـى هـذا البحـث، ولـم يـبخلا بالنصـح والتوجيـه والإرشـاد طيلة فترة الإعداد.

الإهداء

إلى من سارت معي الدرب خطوة بخطوة،

رفيقة دربي وتوأم روحي

..... نداء

إلى شعلتي النور ، بسمة حياتي وشمعتي عمري

..... يزن وريان

إلى الكنز الذي سيبقى مابقيت الشمس تضيء

..... زكي

إلى من عرفت كيف أجدهم وعلموني ألا أضيعهم

..... أصدقائي

الفهرس

الملخص

مقدمة عامة 1

الفصل الأول: الحسابات الكمومية

1.1. الحسابات الكمومية 5

1.2. المسلّمات الأساسية في الفيزياء الكمومية 5

1.3. التشابك 7

1.4. خوارزميات الحسابات الكمومية 8

الفصل الثاني: التعمية بعد الكمومية

2.1. التعمية مابعد الكمومية 11

2.1.1. التوقيع المعتمد على توابع البصمة (Hash-based signatures) 12

2.1.2. التعمية باعتماد الترميز (Code based cryptography) 13

2.1.3. التعمية المتعددة المتحولات (Multivariate cryptography) 15

2.1.4. التعمية المعتمدة على الشبكة (Lattice based cryptography) 16

الفصل الثالث: التعمية المعتمدة على الشبكة

3.1. نظرية الشبكة 20

3.2. مسائل الشبكة 21

3.2.1. إيجاد الشعاع الأقصر SVP 21

3.2.2. إيجاد الشعاع الأقرب CVP 22

3.2.3. بعض الحلول المقترحة لحل مشاكل الشبكة 23

Gram-Schmidt Orthogonalization 23

LLL 23

BKZ 24

Babai's round off 24

3.3. خوارزميات التعمية بالمفتاح العام باستعمال الشبكة 24

GGH.3.3.1 24

NTRU.3.3.2 25

3.4. مقارنة أداء خوارزميات التعمية غير المتناظرة 30

الفصل الرابع : الشبكات اللاسلكية المخصصة النقالة

4.1. شبكات ad-hoc و MANET.....40

4.2. التسيير routing في شبكات MANET.....41

4.2.1 بروتوكولات التسيير الاستباقية proactive routing protocols.....42

4.2.2 بروتوكولات التسيير التفاعلية Reactive Routing Protocols.....43

4.2.3 بروتوكولات التسيير الهجينة Hybrid Routing Protocols.....44

4.3. المشاكل الأمنية في شبكات MANET.....44

4.3.1. البنية التحتية للمفتاح العام (PKI) Public Key Infrastructure.....45

4.4. الحلول المقترحة لإدارة الشهادات.....47

4.5. بعض الحلول المقترحة لإدارة المفتاح العام في شبكات MANET.....48

4.5.1. التنظيم الذاتي للمفتاح العام Self-Organized Public Key Management.....49

4.5.2 Providing Robust and Ubiquitous Security Support for MANET.....51

4.5.3 Self-Managed Heterogeneous Certification.....52

4.5.4 Trust and Clustering-Based Authentication.....52

4.6. إدارة الوثوقية باستخدام تقاسم السرية Secret Sharing.....53

4.6.1. تقاسم السرية في الشبكات قصيرة الأمد.....53

4.6.2. تقاسم السرية في الشبكات طويلة الأمد.....57

4.7. التحكم بالنفاذ Access Control.....60

4.8. التوثق وتعيين الهوية Authentication & Identification.....63

الفصل الخامس: الحل المقترح للتسيير في شبكات MANET

5.1. بروتوكول AODV.....68

5.1.1. المشكلات الأمنية في بروتوكول AODV:.....68

الهجوم باستخدام التعديل attacks using modification:.....69

الهجوم باستخدام التلفيق attacks using fabrication:.....70

الهجوم باستخدام الانتحال attacks using impersonation:.....70

هجوم الاندفاع Rushing attacks :.....70

5.1.2. بعض الحلول المطروحة لتأمين سرية بروتوكولات AODV.....71

- Secure AODV (SAODV).....71
- Security-Aware Ad hoc routing (SAR).....72
- Secure Routing Protocol (SRP).....72

• **Ariadne** 72
• **Authenticated Routing for Ad hoc Networks (ARAN)** 73
5.2. البروتوكول المقترح 74
5.2.1. مرحلة التسجيل والتعريف: 75
5.2.2. مرحلة بناء المسار واكتشافه: 76
5.2.3. مرحلة صيانة المسار: 79
5.3. دراسة أداء البروتوكول المقترح 80
الفصل السادس: الأداة **AVISPA** والنتائج العملية
6.1. الأداة **AVISPA** 84
6.2. سيناريو المحاكاة 87
6.2.1. الدور الأول (المرسل) **source role** : 88
6.2.2. الدور الثاني (عقد وسيطة) **intermediate role** : 90
6.2.3. الدور الثالث (الوجهة) **destination role** : 93
6.2.4. دور "الجلسة" **session role** 94
6.2.5. دور "البيئة" **environment role**: 94
6.3. نتائج تنفيذ البروتوكول: 95
7. الخاتمة والآفاق المستقبلية 103
8. المراجع 105

فهرس الأشكال

الشكل (1) تمثيل الشبكة في الفضاء ^{2} 21

الشكل (2) الشعاع u هو الأقصر بين أشعة الفضاء ^{2} 21

الشكل (3) الشعاع u هو الأقرب بين أشعة الفضاء ^{2} 22
الشكل (4.a) علاقة سرعة التعمية بطول المفتاح العام في NTRU,RSA 32
الشكل (4.b) علاقة سرعة فك التعمية بطول المفتاح العام في NTRU,RSA 33
الشكل (5) علاقة مقدار السرية مع سرعة توليد المفاتيح في NTRU,ECC 34
الشكل (6) علاقة حجم المفتاح بسرعة توليده في NTRU,ECC 35
الشكل (7.a) علاقة مقدار السرية مع سرعة عملية التعمية في NTRU,ECC 35
الشكل (7.b) علاقة مقدار السرية مع سرعة عملية فك التعمية في NTRU,ECC 36
الشكل (8.a) علاقة حجم المفتاح بسرعة تنفيذ التعمية في NTRU,ECC 36
الشكل (8.b) علاقة حجم المفتاح بسرعة تنفيذ فك التعمية في NTRU,ECC 37
الشكل (9) مثال يظهر البيئة غير المتجانسة في شبكات ad-hoc 40
الشكل (10) البيان المباشر للشهادة في شبكات ad-hoc 49
الشكل (11) الهجمات الممكنة ضد بروتوكولات التوجيه عند الطلب 71
الشكل (12) بنية الأداة AVISPA 85
الشكل (13) مثال عن طبولوجيا الشبكة والهجوم المفترض 87
الشكل (14) دور عقدة المرسل 89
الشكل (15) دور العقدة الوسيطة المجاورة 91
الشكل (16) دور العقدة الوسيطة البعيدة 92
الشكل (17) دور عقدة الهدف 93
الشكل (18) دور الجلسة 94
الشكل (19) دور البيئة 95
الشكل (20) واجهة المحاكاة في برنامج SPAN 96
الشكل (21) محاكاة اكتشاف المسار من a-8 إلى x-11 97
الشكل (22) محاكاة اكتشاف المسار من a-3 إلى x-11 97
الشكل (23) نموذج لتطفل العقدة I على الشبكة 98
الشكل (24) نتيجة تطبيق OFMC على البروتوكول المقترح 99
الشكل (25) نتيجة تطبيق CL-AtSe على البروتوكول المقترح 100
الشكل (26) نتيجة تطبيق OFMC على AODV التقليدي 101

فهرس الجداول

الجدول (1) مقارنة بين تقنيات التعمية بعد الكمومية..... 18

الجدول (2) درجة سرية نظام NTRU حسب معاملاته 27

الجدول (3) مقدار السرية في نظام NTRU مقابل معاملات الخوارزمية وطول المفتاح 30

الجدول (4) مقدار التعقيد في خوارزميتي NTRU, RSA 30

الجدول (5) مقارنة طول المفتاح العام في خوارزميات NTRU, RSA, ECC 31

الجدول (6) مقارنة سرعة توليد المفاتيح مع حجم المعطيات في خوارزميتي NTRU, RSA 31

الجدول (7) مقارنة سرعة توليد المفاتيح مع حجم المعطيات في خوارزميتي NTRU, ECC 34

الجدول (8) مقارنة خواص الآليات المقترحة لإدارة المفتاح العام 66

جدول بأهم المصطلحات

ACL	*Access Control List*
AODV	*Ad hoc On demand Distance Vector*
ARAN	*Authenticated Routing for Ad hoc Networks*
AVISPA	*Automated Validation of Internet Security Protocols and Applications*
BGP	*Border Gateway Protocol*
CA	*Certificate Authority*
CRL	*Certificate Revocation List*
CVP	*Closest Vector Problem*
DAC	*Discretionary Access Control*
DoS	*Denial of Service*
DSDV	*Destination Sequence Distance Vector*
DSR	*Dynamic Source Routing*
ECC	*Elliptic Curve Cryptography*
GGH	*Goldreich-Goldwasser-Halevi*
HLPSL	*High Level Protocol Specification Language*
IBC	*Identity Based Cryptography*
MAC	*Mandatory Access Control*
MANET	*Mobile Ad hoc Network*
NTRU	*N-th truncated ring polynomial*
OLSR	*Optimized Link State Routing*
OSPF	*Open Shortest Path First*
PKI	*Public Key Infrastructure*
RDP	*Route Discovery Packet*
REP	*Route Request Reply*
RREP	*Route Reply*
RREQ	*Route Request*
RSA	*Rivest-Shamir-Adleman*
SAR	*Security Aware ad hoc Routing*
SRP	*Secure Routing Protocol*
SVP	*Shortest Vector Problem*
TDE	*Trusted Decision Engine*
TTP	*Trusted Third Party*
WRP	*Wireless Routing Protocol*
ZRP	*Zone Routing Protocol*

Abstract

A Mobile Ad hoc Network (MANET) is a network of wireless mobile devices deployed without the aid of any pre-existing infrastructure or centralized administration. This technology is studied with a number of serious challenges that need to be well catered before its successful deployment. These challenges include security issues, such as key management, secure routing, node authentication, data privacy and communication reliability. An appreciable number of routing protocols used in a typical MANET have left the critical aspect of security out of consideration by assuming that all of its constituent nodes are trustworthy and non-malicious.

In our research, we will study the new algorithms for public key cryptography and focus on lattice based cryptography especially NTRU (N^{th}-TRUncated ring polynomial)and compare it with other traditional cryptography algorithms (RSA & ECC) to see that NTRU is the best nowadays and use it in MANET routing protocols. Then, we remind some of the major threats that MANETs are vulnerable to, because of these inherently insecure protocols. The focus is specifically on on-demand routing protocols. Further, we propose a solution to increase security for these protocols through authenticating nodes without the need of a trusted third party (TTP). This solution depends on a public key infrastructure (PKI) based on NTRU.

Generally, public key infrastructures are assumed to be unavailable in MANETs due to its non-centralized administration. So we propose a distributed nonhierarchical PKI model based on NTRU algorithm to overcome these challenges. The key element of our approach is to use Lattice based cryptography, specifically NTRU, and a distributed PKI model. We show that the proposed scheme is resistant to a wide range of security attacks and can scale easily to large-size networks.

الملخص

تعرف الـ MANET على أنها شبكة من الأجهزة المحمولة اللاسلكية، والتي تتخاطب فيما بينها دون الحاجة إلى إدارة مركزية. وتعتبر من التقنيات الواعدة جداً، لكنها تعاني بعض التحديات خاصة فيما يتعلق بالقضايا الأمنية. تتضمن هذه القضايا الإدارة المركزية، والتوجيه الآمن، وضمان توثيق عقدة ما، وموثوقية الاتصال بشكل عام. ولايمكن حل هذه القضايا باستخدام البروتوكولات التقليدية المستخدمة في الشبكات السلكية.

نقدم في الجزء الأول من بحثنا دراسة عامة عن خوارزميات جديدة للتعمية غير المتناظرة (التعمية بالمفتاح العام)، ونخص بالتفصيل خوارزميات التعمية المعتمدة على الشبكة التي تصنف من خوارزميات التعمية بعد الكمومية، وبصفة خاصة نقوم بدراسة وتطبيق لخوارزمية التعمية NTRU ونقارن أدائها مع الخوارزميات التقليدية (RSA,ECC) لبيان بأنها الأفضل حالياً بين الخوارزميات من حيث سرعة التنفيذ، والتعقيد الحسابي البسيط، والسرية العالية.

في الجزء الثاني سنقوم باستخدام هذه الخوارزمية الواعدة في بناء بروتوكول توجيه لشبكات الـ MANET. حيث سنقوم بعرض بعض التهديدات الرئيسية التي تتعرض لها تلك الشبكات نتيجة عدم سرية بروتوكولات التوجيه خاصتها، ونخص بدراستنا بروتوكولات التوجيه عند الطلب AODV. ومن ثم لزيادة الأمان لها سنستخدم تقنيات التوثيق بين العقد دون الحاجة لوجود طرف ثالث. يعتمد ذلك الحل على بناء نموذج PKI يعتمد خوارزمية NTRU.

إن بنية المفتاح العام PKI بشكلها الحالي لايمكن استخدامها في الشبكات اللاسلكية بسبب غياب الإدارة المركزية، لذلك سنقترح البنية الهرمية في بناء نموذج PKI الذي يعتمد خوارزمية NTRU للتغلب على جميع المشاكل السابقة. وسنرى أن النموذج المقترح مقاوم لطيف كبير من الهجمات مما يمكّننا من استخدامه حتى في الشبكات كبيرة الحجم.

مقدمة عامة

مقدمة عامة

إن إحدى أهم أهداف عمليات التعمية هو حماية المعلومات المنتقلة عبر القنوات غير الآمنة كاللاسلكية مثلاً. وقد قام Diffie and Hellman عام 1976 بتقديم مفهوم التعمية باستخدام المفتاح العام public key cryptography، والذي يعتمد على حل المسائل الرياضية المعقدة (اللوغاريتم المتقطع، تحليل كثيرات الحدود...). ومنذ ذلك الحين اعتُمدت هذه المسائل المعقدة كأساس لعملية التعمية باستخدام المفتاح العام، وقد أثبتت نجاحها في بعض المجالات بينما فشلت في مجالات أخرى.

اكتشف Ajtai في عام 1996 بعض المسائل الرياضية في مجال الشبكة Lattice التي تمتلك خواصاً ستكون مفيدة في عملية التعمية باستخدام المفتاح العام. أثبت Ajtai أن مسائل الشبكة الأساسية تساهم وبشكل كبير في بناء أنظمة تعمية ذات سرية عالية، وتلك الخواص هي مشكلة إيجاد الشعاع الأقصر SVP، ومشكلة إيجاد الشعاع الأقرب CVP. وصعوبة حل هذه المشاكل هي التي أعطت خوارزميات الشبكة مناعتها العالية ضد الهجمات التقليدية والكمومية. تكمن صعوبة الحل في أن تنفيذها يحتاج إلى حجوم هائلة وسرع عالية جداً.

ومنذ ذلك الوقت بدأ استخدام الشبكة لبناء نظم التعمية، لما له من إيجابيات عديدة سنأتي على ذكرها لاحقاً، ولعل أهمها السرية العالية في مقابل التعقيد البسيط، ومقاومة هذا النوع من التعمية للهجمات الكمومية التي من المتوقع أن تزدهر خلال الأعوام القليلة القادمة.

ومايهمنا في هذه التقنية الواعدة جداً هو توظيفها في مجال الشبكات وتحديداً اللاسلكية، نظراً لوجود نقطة ضعف مهمة في هذه الشبكات ألا وهي السرية.

لقد أخذت الشبكات اللاسلكية المخصصة ad hoc networks بالانتشار وبشكل كبير في العديد من التطبيقات العسكرية منها والمدنية، لما لها من طبيعة بسيطة تتمثل في اللامركزية في إدارة الشبكة، والتعاون الوثيق بين مختلف العقد لتحقيق عملية الاتصال، بالإضافة إلى البنية غير المتجانسة في الشبكة نتيجة التنوع الكبير في طبيعة العقد المشكلة للشبكة حيث يمكن لمختلف التجهيزات (حاسوب، هاتف نقال، حساس ...) أن تمثل عقداً.

ويمكن لهذه العقد أن تنضم أو تغادر الشبكة تبعاً لرغبتها، مما يعني التغير الدائم في بنية الشبكة. وأيضاً إمكانية الحركة لهذه العقد، وبالتالي الوصول إلى الشبكات اللاسلكية المخصصة النقالة Mobile Ad hoc Networks (MANET).

لكن هذه الطبيعة البسيطة أنشأت مجموعة من الإشكاليات التي يتطلب حلها. فغياب المركزية يتطلب ابتكار آليات جديدة لإدارة الشبكة وضبط عمليات التسيير، حيث لاتنفع الطرق التقليدية للشبكات في حل هذه المشاكل. كذلك من الناحية الأمنية لايمكن للأنظمة التقليدية أن تكون فعالة في حماية هذه الشبكات، نتيجة الحركية الدائمة للعقد، ومحدودية مواردها (سرعة، ذواكر، استطاعة ...)، وبالتالي نحتاج أنظمة خاصة لتغطية الحاجات الأمنية.

هذه الإشكاليات جعلت من انتشار شبكات MANET والاعتماد عليها محدوداً حتى الآن، وذهبت الدراسات والأبحاث باتجاه البحث عن نظام أمني فعال غير مركزي يسمح بالحفاظ على سرية المعلومات، والتحقق من هويات المستخدمين، ويضمن أداء عملية التسيير بشكل فعال. وهو ما سنعمل على بنائه في هذا البحث اعتماداً على خوارزميات التعمية المعتمدة على الشبكة Lattice based cryptography.

فهدف البحث هو بناء بروتوكول تسيير لشبكات MANET يحقق السرية كما في الشبكات التقليدية، ومقاوم للهجمات الممكنة. وجوهر بناء هذا البروتوكول هو في إدارة شهادات الوثوقية، وهو ما سنتخطاه من خلال تطبيق خوارزمية NTRU.

نقوم في الفصل الأول بتقديم عام لموضوع الحسابات الكمومية، والتعمية مابعد الكمومية. وفي الفصل الثاني سنقدم دراسة عامة وتفصيلية للتعمية المعتمدة على الشبكة، وسنهتم بدراسة خوارزمية NTRU، ومقارنتها مع خوارزميات التعمية التقليدية، لبيان ميزاتها العديدة التي سنستخدمها في بحثنا.

أما في الفصل الثالث سنتحدث عن شبكات MANETs ، وميزاتها، وخصائصها، ونقوم بدراسة شاملة للأنظمة الأمنية المقترحة سابقاً في هذا المجال، والطرق المقترحة في إدارة شهادات الوثوقية Certificate Authority (CA). وفي الفصل الرابع سنوظف خوارزمية NTRU في بناء بروتوكول تسيير يحقق متطلبات السرية دون خسارة في بنية الشبكة، ويضمن خواص النظام الأمني من حيث السرية confidently، والتوثق authentication، وسلامة المعطيات integrity، وعدم الإنكار non repudiation.

وفي الفصل الأخير سنستخدم الأداة AVISPA (أداة رسمية تستخدم في بناء البروتوكولات ودراسة الهجمات الممكنة عليها) للتحقق من هذا البروتوكول المقترح، وأدائه، وسريته، وممانعته ضد الهجمات الممكنة.

الحسابات الكمومية

1.1. الحسابات الكمومية

تتركز الحوسبة الكمومية على تطوير تقنيات الحوسبة باستخدام مبادئ نظرية الكم. وتطوير جهاز الحاسوب باستخدام هذه التقنية سيسمح بقفزة نوعية وكبيرة نحو الأمام في زيادة القدرة الحاسوبية من حيث زيادة الأداء بحيث تسمح بالقيام بمعالجات عددية هائلة في نفس الوقت، مع التوفير في الحجم والطاقة.

تعتمد الحسابات التقليدية على جبر بوليان، والذي يعمل عادة بمبدأ البوابات المنطقية. أي أن المعطيات تأخذ الشكل الثنائي فقط 0 أو 1 في لحظة واحدة، وهي البتات المعروفة الممثلة للمعطيات. بالتالي الوحدة الأساسية المسؤولة عن عملية الحسابات (الترانزستور أو المكثفة) في الحاسب تحتاج إلى زمن تبديل بين وضع العمل on والتوقف off. وهذا الزمن سيبقى موجوداً والعمليات ستبقى محدودة حتى وإن وصلت إلى بلايين العمليات في الثانية، أي أننا ومع التطور التكنولوجي الكبير قد وصلنا تقريباً إلى الحدود الفيزيائية لعمل هذه العناصر وإلى عتبة قوانين الفيزياء الكلاسيكية، لذلك بدأ التفكير بالاتجاه نحو الفيزياء الكمومية للوصول إلى عدد عمليات حسابية أكثر وزمن معالجة أقل.

أما في الحوسبة الكمومية فإن المعطيات يمكن لها أن تأخذ القيمة 0 و 1 في نفس اللحظة، أي أن القيمة الحالية الموجودة هي تراكب قيمتين للـ 0 وللـ 1 معاً، وهذا ما يمكن تمثيله بشعاع مكون من مركبتين ويسمى qubit، وبالتالي فإن عدد العمليات الحسابية المنجزة سيزداد بشكل كبير 2^n حيث n عدد الـ qubits، باعتبار أن كل حالة أصبحت تمثل عدداً كبيراً من القيم. وتزداد عمليات التخزين أيضاً فإذا كانت كل قيمة في الحسابات التقليدية تمثل بت واحد، فإن كل qubit تخزن قيمتين في نفس اللحظة.

ولفهم الحسابات الكمومية يجب فهم المسلمات الأربعة في الفيزياء الكمومية والتي تُعد القاعدة الأساسية في فهم آلية عمل هذه الحسابات.

1.2. المسلّمات الأساسية في الفيزياء الكمومية

- المسلمة الأولى: quantum bit

"في أي نظام فيزيائي معزول يوجد شعاع عقدي يمثل شعاع الحالة لهذا النظام، وهذا الشعاع يوصف النظام بشكل كامل ويمثل الشعاع الواحدي في فضاء حالة النظام" [phio7] .

ليكن لدينا qubit ممثل بشعاع ذي بعدين، و $|\phi_0\rangle,|\phi_1\rangle$ هي الأشعة الواحدية المتعامدة المولدة للفضاء واختصاراً عادة ما نكتب هذه الأشعة على الشكل $|0\rangle,|1\rangle$. عندئذ يمكن تمثيل الـ qubit :

$$|\psi\rangle = a\,|\phi_0\rangle + b\,|\phi_1\rangle$$

ويجب أن يكون الشعاع الممثل لل qubit واحدياً، تبعاً لقانون الاحتمالات، أي أن

$$\langle\psi|\psi\rangle = 1$$
$$a^2 + b^2 = 1 \qquad a,b \in \square$$

وتعتبر هذه الصيغة لتمثيل المعطيات تمديداً لفكرة التمثيل باستخدام البتات في الحوسبة التقليدية، بحيث يأخذ a,b القيمة 0 أو 1 فقط عند تمثيل أي بت في الحساب التقليدي.

- المسلمة الثانية : quantum systems

" إن تطور أي نظام كمومي مغلق يوصف بالتحويل الواحدي. أي أن الانتقال من الحالة $|\psi\rangle$ في اللحظة t_1 ، إلى الحالة $|\psi'\rangle$ في اللحظة t_2 يرتبط بالمعامل الواحدي U الذي يعتمد فقط على الفرق الزمني بين t_1,t_2" [phio7].

وكمثال على ذلك عندما $t_2 - t_1 = 1$:

ليكن الشعاع :

$$|\psi\rangle = 1\,|0\rangle + 0\,|1\rangle$$

$$U = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

عندئذ :

$$|\psi'\rangle = U\,|\psi\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}\begin{bmatrix} 1 \\ 0 \end{bmatrix} = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 \\ 1 \end{bmatrix}$$
$$= \frac{1}{\sqrt{2}}\,|0\rangle + \frac{1}{\sqrt{2}}\,|1\rangle$$

- المسلمة الثالثة : القياسات

" توصـف معاملات القياس الكمومية بالمجموعة $\{M_m\}$ وهي مجموعة المعاملات في فضـاء الحالة للنظام المراد قياسه، حيث m نتيجة القياس التي يمكن أن تحدث في التجربة. " [phio7] .

فإذا كانت حالة النظام قبل القياس مباشرة $|\psi\rangle$ فإن احتمال أن يكون القياس التالي هو m يساوي لـ

$$p(m)=\langle\psi|M_m^H M_m|\psi\rangle$$

بالتالي

$$\sum_m \langle\psi|M_m^H M_m|\psi\rangle=\sum_m p(m)=1$$

وتكون حالة النظام بعد القياس تماماً مساوية لـ :

$$\frac{M_m|\psi\rangle}{\sqrt{\langle\psi|M_m^H M_m|\psi\rangle}}$$

- المسلمة الرابعة : multi-qubit systems

" إن حالة النظام الكمومي المتعدد، تسـاوي جداء العزوم tensor product لحالات الأنظمة الكمومية المكونة له" [phio7] .

فإذا كان النظام الأول في الحالة $|\psi_1\rangle=a|0\rangle+b|1\rangle$ ، والنظام الثاني في الحالة $|\psi_2\rangle=c|0\rangle+d|1\rangle$

فإن النظام الكلي يكون في الحالة

$$|\psi\rangle=|\psi_1\rangle\otimes|\psi_2\rangle=|\psi_1\psi_2\rangle=a.c|0\rangle|0\rangle+a.d|0\rangle|1\rangle+b.c|1\rangle|0\rangle+b.d|1\rangle|1\rangle$$

$$=ac|00\rangle+ad|01\rangle+bc|10\rangle+bd|11\rangle$$

1.3. التشابك

ظاهرة التشابك Entanglement هي ظاهرة كمومية خالصة، وتحدث في أنظمة متعددة الحالات multi-qubit system . حيث تحتفظ الجزئيات بالاتصـال الموجود فيما بينها حتى بعد انتهاء عملية الاتصـال. وتتشـكل هذه الظاهرة بين كل زوجين من الـــ qubits، وتسـمى بالترابط correlation. وهذه الآلية الموجودة لم يستطع العلم تفسيرها نظرياً حتى الآن.

فعندما يدور أحد الجسيمين باتجاه ما فإن الجسيم الآخر المرافق سيدور بالاتجاه العكسي حتماً، ولا يمكن التنبؤ بطريقة دوران أحد الجسيمات لوحده دون قياس لأنه يمكن أن يدور بالاتجاهين معاً في نفس اللحظة. بالتالي لمعرفة قيمة qubit ما يجب أخذ قياس للـــ qubit الآخر. وهذه الخاصية الأساسية هي التي سنعتمد عليها لاحقاً في تحقيق عمليات التعمية باستخدام التشابك lattice based cryptography [Mico8].

1.4. خوارزميات الحسابات الكمومية

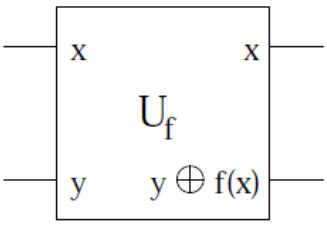
- Deutsch's Algorithm

هذه الخوارزمية هي خير مثال على إجراء الحسابات بالطريقة الكمومية. ويمكن توصيفها من خلال التبسيط التالي:

نريد تحديد فيما إذا كان التابع $f(x)$ ثابتاً أو متوازناً، أي أنه يعطي القيمة 0 أو 1 دائماً أياً كانت قيمة x، أو أنه يعطي من أجل نصف القيم لـ x القيمة 0 والنصف الآخر يعطي 1.

من خلال الطريقة التقليدية فإنه يلزمنا معرفة القيم من أجل x=0 و x=1. أي نحتاج إلى معلومتين لتحديد التابع f، بينما بالطريقة الكمومية يلزمنا فقط معلومة واحدة لتحديد التابع f.

ليكن التابع $f(x):\{0,1\}\rightarrow\{0,1\}$ في حاسوب كمومي و $|x,y\rangle\rightarrow|x,y\oplus f(x)\rangle$، ونستخدم بتين كموميين في الدخل للمحافظة على قيمة x بدون تغيير، وy لتخزين النتيجة، وU_f التحويل الواحدي الذي يحقق f كالتالي



في الحساب التقليدي إذا أردنا حساب $f(0)$ فيكون x=0,y=0 ونطبق التحويل U_f عندئذ نحصل في الخرج على $|0,0\oplus f(0)\rangle$

وكذلك بالنسبة لـ $f(1)$ نحصل على $|1,0\oplus f(1)\rangle$

أما بالنسبة للحساب الكمومي فإنه يمكن أن نضمن القيمتين لـ x في شعاع واحد $x=(|0\rangle+|1\rangle)/\sqrt{2}$ و y=0 عندئذ يكون الدخل هو الشعاع $|\psi_1\rangle=\frac{(|0,0\rangle+|1,0\rangle)}{\sqrt{2}}$ والخرج

$$|\psi_2\rangle=\frac{(|0,f\ (0)\rangle+|1,f\ (1)\rangle)}{\sqrt{2}}$$

نلاحظ أن التحويل U_f يطبق بنفس الوقت على القيمتين 0,1 وهو مبدأ الحوسبة الكمومية المتوازية، التي تسمح لنا بتحديد التابع f من خلال قيمة واحدة في الدخل [phio7].

- Deutsch-Jozsa Algorithm:

تعتبر هذه الخوارزمية تعميماً لخوارزمية Deutsch العادية. حيث يصبح تعريف التابع f على الشكل : $f\ (x):\{2^n\}\rightarrow\{0,1\}$ ويلزمنا في هذه الحالة أيضاً معلومة واحدة في الحوسبة الكمومية لتحديد التابع f بدل $2^n/2+1$ معلومة في الحساب التقليدي [phio7] .

- Shor's Algorithm :

تعتبر هذه الخوارزمية من الخوارزميات الأفضل في تحليل الأعداد إلى عوامل باستخدام الطريقة الكمومية، حيث تمتلك تعقيداً من رتبة $O\left(n^3\right)$ بالنسبة للعمليات الكمومية بينما تمتلك أفضل الخوارزميات التقليدية في تحليل الأعداد تعقيداً أسياً . وهذا التعقيد الأسي هو الذي سمح لخوارزميات التعمية التي تعتمد ذلك المبدأ أن تمتلك القوة الكافية لحمايتها ضد الاختراق كون الوقت اللازم لتحليل الأعداد كبير نسبياً، وبالتالي فإن تخفيف التعقيد في الحساب الكمومي يسمح بفتح آفاق جديدة في عالم خوارزميات التعمية من حيث الحماية ضد الاختراق والسرعة في الأداء [phio7].

نعلم أن رتبة أي عدد x بمفهوم باقي القسمة N $(x<N)$ هو أصغر عدد r يحقق $x^r \bmod N=1$

ولحساب هذه الرتبة اعتماداً على خوارزمية Shor يجب اتباع الخطوات التالية:

- اختيار عدد x أولي مع N .
- باستخدام الحساب الكمومي المتوازي نستطيع حساب x^r من أجل جميع قيم r معاً.
- مقابلة جميع القيم السابقة للحصول على المعلومة المطلوبة وهي قيمة التكرار.
- اعتماداً على قيم التكرار نستطيع الحصول على عوامل N.

التعمية بعد الكمومية

2.1. التعمية مابعد الكمومية

بدأ الحديث منذ 30 سنة تقريباً عن الحاسوب الكمومي، وتبعاً للتطورات التكنولوجية الحاصلة في العالم فإنه من المتوقع أن نصل إلى الحاسوب الكمومي خلال 10 سنوات على الأكثر (هناك حديث عن وجود بعض الحواسيب الكمومية حالياً لكنها لم تعرض تجارياً حتى الآن). فإذا افترضنا أن هذا الكلام سيتحقق قريباً عندئذ كل ما نعرفه عن الخوارزميات التقليدية في التعمية أنها ستكون قابلة للاختراق وبسهولة، ولسبب بسيط هو أن عدد العمليات الحسابية التي تستطيع تلك الحواسيب أن تقوم بها أكبر بكثير جداً من العمليات في الحواسيب التقليدية، وبالتالي فإن الزمن اللازم لاختراقها يصبح أقل بكثير. أي أن خوارزميات التعمية غير المتناظرة مثل خوارزميات RSA, ECC وغيرها ستصبح غير فعالة في حماية المعلومات المنتقلة عبر شبكة الانترنت، وتصبح الاتصالات مكشوفة تماماً بالنسبة لأي عنصر مهاجم، لأن الزمن هو العنصر الرئيسي في قوة هذه الخوارزميات. فكلما تعقدت الخوارزمية ازداد الزمن اللازم لاختراقها نتيجة زيادة عدد العمليات الحسابية وبالتالي أصبحت أكثر أمناً في المفهوم التقليدي [Dano9] .

إذن لابد من البحث عن خوارزميات وطرق أخرى لتحقيق عمليات التعمية بحيث تضمن الأمان والأداء في أنظمة الاتصال، وكان الحل المرشح لذلك هو الانتقال إلى التعمية الكمومية، لكن ذلك يقتضي تغييراً كاملاً في البنى التحتية لجميع الشبكات الموجودة بالإضافة إلى زيادة كبيرة في التكلفة للوصول إلى أداء مقبول ضمن شروط العمل.

لذلك، انتقلت الأبحاث إلى اتجاه آخر وهو البحث عن خوارزميات تنفذ في البنية التقليدية الموجودة، وتشابه في أدائها خوارزميات التعمية غير المتناظرة، وتكون مقاومة للهجوم الكمومي المحتمل، وقادرة على حماية المعلومات بشكل كامل عند الانتقال إلى الحواسيب الكمومية، واتخذت هذه الأبحاث مصطلح post quantum cryptography.

وتنقسم هذه الأبحاث إلى أربعة أقسام رئيسية:

- Hash-based signatures
- Code-based cryptography
- Multivariate cryptography
- Lattice-based cryptography

2.1.1. التوقيع المعتمد على توابع البصمة (Hash-based signatures)

إن التوقيع الرقمي التقليدي يعتمد في تحقيق السـرية بأدائه على تعقيد عمليات التحليل إلى عوامل واللوغاريتم المتقطع، حيث تأخذ هاتان العمليتان زمناً كبيراً لتحقيقها بالتالي فإن التوقيع الرقمي يعتبر أميناً في الحسابات التقليدية. ولكن عند الهجوم الكمومي فإنه من السهولة الوصول إلى تحليل أي عدد كبير في زمن قصير نسبياً وبالتالي النجاح في اختراق خوارزميات التوقيع الرقمي. لذلك لابد من خوارزميات توقيع رقمي تكون ممانعة لهذه الهجومات، فكانت فكرة اعتماد التوقيع على توابع البصمة hash-based .

- تابع البصمة التقليدي:

يعتمد تابع البصمة التقليدي على ثلاث نظريات أساسية وهي:

- ليكن التابع $H:\{0,1\}^{*}\rightarrow\{0,1\}^{k}$ عندئذ أي رسالة m يمكن بناء بصمة خاصة لها h بحيث $H(m)=h$.
- هذا التابع غير عكسي. أي أنه لايمكن العودة إلى m من خلال التابع H.
- لايمكن إيجاد رسالتين مختلفتين لهما نفس البصمة. $m_1 \neq m_2 \Rightarrow h_1 = h_2$ وبالتالي نقول إن التابع H ممانع للتصادمات. وعلى نحو أدق لا يمكننا إنشاء رسالة m2 تكون لها نفس بصمة رسالة أخرى معلومة m1.

- التوقيع المعتمد على البصمة:

طرحت الفكرة أول مرة عن طريق [Lam79] Lamport-Diffie كالتالي:

1. نختار تابع بصمة g بحيث يحقق الخاصة الثالثة (ممانع للتصادمات). $g:\{0,1\}^{*}\rightarrow\{0,1\}^{n}$
2. نختار تابع بصمة آخر f باتجاه واحد $f:\{0,1\}^{n}\rightarrow\{0,1\}^{n}$
3. يتكون مفتاح التوقيع X من مجموعتين Xo, X1، كل منهما مكونة من n سلسلة عشوائية بتوزيع منتظم، أي كل منهما بطول n.

$$X=\{X_0,X_1\}$$
$$X_k=\{B_{k,1},B_{k,2},\ldots B_{k,n}\},\quad B_{k,i}\in\{0,1\}^{n}$$

4. مفتاح التحقق Y يبنى بنفس الطريقة، بحيث تكون السلاسل العشوائية هي نتيجة تطبيق التابع f على السلاسلB.

$$Y=\{Y_0,Y_1\}$$
$$Y_k=\{C_{k,1},C_{k,2},\ldots C_{k,n}\},\quad C_{k,i}=f(B_{k,i})$$

تجري عملية التوقيع كالتالي:

1. باستخدام التابع g نحسب قيمة بصمة الرسالة m . $d = g(m)$
2. يجري التوقيع S باستخدام إحدى السلاسل العشوائية من المفتاح X بطريقة تتابعية أي

$$S = \{S_0, S_1 ... S_n\}$$
$$S_i = B_{d(i),i}$$

حيث d(i) يمثل البت رقم i في السلسلة d.

أما عملية التحقق من التوقيع فتجري كما يلي:

1. باستخدام التابع g نحسب $d = g(m)$
2. كل سلسلة من S نحسب لها قيمة بصمة باستخدام f، ونقارنها مع Y.

$$f(S_i) \stackrel{?}{=} C_{d[i],i}$$

3. عند تطابق كل قيم السلاسل نقول إن التوقيع صحيح.

تعتمد هذه الطريقة على بناء المفاتيح بشـــكل دوري في كل مرة تجري فيها عملية التوقيع، لذلك فإن عملية إنتاج المفاتيح تحتاج إلى وقت طويل بالإضـــافة إلى موارد كثيرة. ما أدى إلى ظهور تقنية أخرى في عملية التوقيع الرقمي استخدمها [Mer89] Merkle لتخفيف أثر هذه المشكلة.

- إن الأداء الحسـابي لهذا التوقيع يعتبر ضـعيفاً نتيجة العمليات الحسـابية الكثيرة التي نحتاجها في بناء المفاتيح والتحقق منها، بالإضـافة إلى أن حجم التخزين المطلوب كبير جداً لهذه العملية. فكان الحل باستخدام سلاسل شبه عشوائية في توليد المفاتيح. ومن ناحية الأمان فإن الـ hash-based يعتبر من أكثر التواقيع أماناً، حيث توابع البصـمة المسـتخدمة تحقق الخواص الأسـاسـية في عدم وجود مقلوب لها وممانعتها للتصـادمات. ولتحقيق ممانعتها للهجوم الكمومي يمكن الاسـتعانة بتوابع بصـمة خاصـة مثل [Lyuo8] SWIFFT حيث نحصـل على أمان عالٍ باسـتخدام هذه التوابع في هذا النوع من التوقيع hash-based.

2.1.2. التعمية باعتماد الترميز (Code based cryptography)

نظرية الترميز لها تاريخ طويل في عالم المعلومات والاتصـالات كآلية لحذف المعلومات الإضـافية في الرسـالة (ترميز المنبع)، أو كآلية تستخدم للتقليل قدر الإمكان من الأخطاء أثناء النقل (ترميز القناة).

وفي الوقت الحالي أكثر ما يهمنا في عملية الترميز هي التراميز المصـححة للخطأ، التي تسـاهم بشـكل كبير في تقليل الأخطاء داخل القناة، وضـمان وصـول الرسـالة صـحيحة إلى المسـتقبل . وأهم التراميز الموجودة في هذا المجال هي التراميز الخطية الثنائية.

- **Binary linear codes**

إن أبسط طريقة لتصحيح الأخطاء هي إرسال الرمز أكثر من مرة، فيُرسل مرتين من أجل كشف الخطأ، وثلاث مرات من أجل تصحيحه. هذه الطريقة البسيطة طبعاً غير فعالة لأنها تحتاج إلى سرعات عالية جداً من أجل كمية قليلة من المعلومات المفيدة. لذلك يتجه التفكير نحو طرق أفضل وبفعالية أعلى وأهم هذه الطرق هي التراميز الخطية.

1. يعرف الترميز الكتلي C بمصفوفة التوليد $G \in \mathrm{F}_2^{k,n}$ ولها k سطر (k طول سلسلة الدخل)، و n عمود (n طول كلمة الترميز).
2. تحسب المصفوفة H وهي مصفوفة فحص الزوجية.

$$G = \left(I_k \,|P\right),\ H = \left(-P^T \,|I_{n-k}\right)$$

3. نعرف المسافة الصغرى لهامينغ $d \in \square$ للترميز C، وهي العدد الأصغري للبتات المختلفة بين أي كلمتي ترميز.
4. عندئذ يكون عدد البتات الممكن تصحيحها $t = \left\lfloor \frac{d-1}{2} \right\rfloor$.
5. تعرف مجموعة الـ syndrome بأنها مجموعة الأخطاء الممكنة (أقل أو تساوي t) مضروبة بالمصفوفة H. وذلك لتحديد الخطأ لاحقاً في عملية الاستقبال.

$$S = \left(e, He\right) : e \in \mathrm{F}_2^n,\ \sum_{i=0}^{n} e_i \le t$$

وتجري عملية الترميز من خلال توليد كلمات الترميز x وذلك عبر ضرب شعاع الدخل v بمصفوفة التوليد G. $x = vG$

أما عملية فك الترميز فتجري على الشكل التالي:

1. الرمز المستقبل z يعرف على أنه رمز مرسل x مع شعاع خطأ e. أي $z = x + e$
2. يعرف شعاع الـ syndrome من خلال العلاقة

$$s = Hz$$

$$s = H\left(x + e\right) = Hx + He = He$$

3. بمقارنة s مع المجموعة S نحصل على القيمة e. ونحذفها من الشعاع z للحصول على كلمة الترميز المرسلة x. أي $x = z - e$

نلاحظ مما سبق أن الاختلاف الوحيد في التراميز الخطية يكمن في طريقة اختيار مصفوفة التوليد G ، ومنه نستطيع اختيار الترميز المناسب في كل حالة.

- **McEliece cryptosystem**

نشـــر [Mce78] McEliece نظام تعمية جديد يعتمد على ترميز خطي ثنائي هو Goppa codes.
وحتى الآن لم تُكسر هذه الترامیز على الرغم من أن مثل هذه الترامیز الخطية قابلة للاختراق.
ويُبنى نظام McEliece بالشكل التالي:
لتوليد المفاتيح نقوم بتوليد المفتاح العام $G^{pub}=TGP$ اعتماداً على مصـــفوفة التوليد G، حيث T مصـفوفة عشـوائية ثنائية غير واحدية، و P مصـفوفة عشـوائية تبديلية. ويكون المفتاح الخاص لهذا النظام $\{T,D_c,P\}$، حيث Dc هي خوارزمية الفك للترميز C (مثلاً S في حالة فك الترميز باســـتخدام syndrome).
أما عملية التعمية فتجري على الشكل:

1. تُضرب الرسالة m بالمفتاح G^{pub} أي: $x=mG^{pub}$.
2. يضـــاف مقدار من الخطأ e على الشـــعاع x، وذلك لضـــمان عدم فك التعمية بســـهولة.

$$z=x+e$$

ولفك هذا التعمية :

1. نضرب الشعاع المستقبل بمقلوب المصفوفة P. $y=zP^{-1}$
2. بتطبيق المصفوفة Dc على الشعاع y نستطيع أن نحذف الخطأ e.
3. وبالضرب بمقلوب المصفوفة T نحصل على الرسالة الأصلية m.

- ونظراً لمقدار الحجم الكبير من الذاكرة المطلوبة في ترامیز Goppa Codes، فإن ترامیز أخرى قد طرحت بديلاً عنها في نظم McEliece لزيادة الأمان فيها مع ذاكرة أقل. وقد تتابعت الأبحاث في هذا المجال للوصـــول إلى نظام تعمية ســـري وفعال مضـــاد للهجوم الكمومي وذلك باســـتخدام توابع البصـــمة، والمولدات العشوائية pseudo random.

2.1.3. التعمية المتعددة المتحولات (Multivariate cryptography)

تعتبر نظم التعمية المتعددة المتحولات من النظم الواعدة في مجال النظم مابعد الكمومي، وذلك للســـرعة العالية في أدائها. وتبنى هذه الأنظمة على كثيرات الحدود P المتعددة المتحولات والتي تعرف بالشكل:

$$\mathrm{P}=\{p_1(x_1,\ldots,x_n),\ldots,p_m(x_1,\ldots,x_n)\},x_k\in \mathrm{F}_q$$

حيث يكتب كل كثير حدود بالشكل:

$$p_k(x_1,\ldots,x_m)=\sum_i p_{ik}x_i+\sum_i Q_{ik}x_i^2+\sum_{i>j}R_{ijk}x_ix_j$$

بشـــكل عام إن إيجاد شـــعاع دخل $X=(x_1,...,x_n)$، مكون من مجموعة كثيرات حدود متعددة المتحولات، عن طريق شـعاع الخرج فقط $C=\{p_1(X),...,p_m(X)\}$ هو أمر صـعب جداً. لذلك في نظم التعمية المتعددة المتحولات الثنائية لانختار مجموعة كثرات الحدود بشـكل عشـوائي، بل نختار كثيرات الحدود القابلة للقلب بسهولة.

ولبناء مثل هذه الأنظمة نقوم بتوليد المفاتيح بداية كالتالي:

1. نولد مجموعة كثيرات الحدود Q بحيث تكون قابلة للقلب بسهولة.
2. نولد المصفوفتين S,T . ونحسب المصفوفة $P=S\circ Q\circ T$.
3. المصفوفة P هي المفتاح العام في هذا النظام، بينما المجموعة $\{S,Q,T\}$ هي المفتاح الخاص.

ولتعمية الرسالة نعتبر شعاع الرسالة p دخلاً لكل كثير حدود في المجموعة P، بالتالي نحصل في الخرج على الشعاع c خرج كل تابع كثير حدود.

ولفك التعمية:

1. نحسب الشعاع u من شعاع الاستقبال c. $u=T^{-1}(c)$
2. نحسب الشعاع v من خلال $v=Q^{-1}(u)$
3. ونحصل في النهاية على الرسالة الأصلية p من خلال التطبيق العكسي لـ S.

$$p=S^{-1}(v)=S^{-1}\left(Q^{-1}\left(T^{-1}(c)\right)\right)$$

2.1.4. التعمية المعتمدة على الشبكة (Lattice based cryptography)

تعتبر ورقة البحث التي أصـدرها Ajtai " Generating hard instance of lattice problems" [Ajt96] النقطة التي انطلقت منها أبحاث التعمية باستخدام الشبكة، حيث أثبتت أنها نظام فعال وقابل للتطبيق، وبنسبة أمان عالية ضد الهجوم الكمومي، ما جعلها النظام الأكثر شـهرة في عالم التعمية مابعد الكمومي. وسنناقش الأمان في هذه الأنظمة لاحقاً.

- يعرف أساس الشبكة في نظام التعمية B على أنه مجموعة من الأشعة الخطية المستقلة في الفضاء $\mathbb{R}^n$. $B=\{b_1,...,b_n\}$
- أما الشـبكة $b_k\in\mathbb{R}^n$, $L_B=\mathbf{Z}b_1+...+\mathbf{Z}b_n$ فهي مجموعة التراكيب الخطية من هذا الأسـاس B. وبالتالي فإن هناك نوعان من الأسس في الشبكة النوع الجيد وهو الأساس الذي يمكن إيجاد التراكيب بسـهولة أما النوع السـيء هو الذي لايمكن إيجاد التراكيب بسـهولة. ولذلك فإن بناء الشبكة يمكن أن يكون باستخدام أحد النوعين من الأسس أو باستخدامهما معاً.

- اعتماداً على ورقة البحث لـــ Ajtai يمكن بناء نظام تعمية موثوق دائماً باستخدام توابع البصمة باتجاه واحد، حتى في الحالة الأســوأ. لكن هذه النظرية بقيت بعيدة عن التنفيذ العملي حتى قام Golreich, Goldwasser and Halevi بتطوير هذا النظام وجعله أقرب للتطبيق العملي عن طريق تنفيذه بنموذج مماثل لنموذج McEliece مع استخدام الشبكة بدل الرموز.

ولتوليد المفتاح في هذا النظام نقوم بتوليد أشعة أساس R جيدة، وباستخدام تحويل وحيد الاتجاه نقوم بتوليد أشعة أساس Q سيئة تكون هي المفتاح العام للنظام بينما R هي المفتاح الخاص.

ولتعمية رسالة ما نقوم باختيار شعاع عشوائي w باستخدام Q، ونجمعه إلى شعاع الرسالة p، ونرسل $c = p + w$ على أنها النص المعمى.

وفي الاستقبال نحسب الشعاع الأقرب لـــــ w باستخدام المفتاح الخاص R، وبطرح الشعاع المستقبل c نحصل على النص الأصلي للرسالة . $p = c - w$

- لقد أظهرت النتائج أن التعمية باســتخدام الشــبكة هو الحل الأفضــل في مجال مقاومة الهجوم الكمومي نظراً للأمان الذي يحققه مقارنة بطول المفتاح المســـتخدم، وللتعقيد الأقل مقارنةً مع التقنيات الأخرى. هذا جعله نظاماً واعداً جداً في مجال الأمان عند الوصـــول إلى الحواســـيب الكمومية [Mico8].

وفي الجدول التالي-1- نجد تلخيصاً للتقنيات الأربعة الموجودة حديثاً ومقارنة بينها من حيث درجة الأمان، وسرعة التنفيذ.

	Hash-based	Code-based	Multivariate-based	Lattice-based
الاستعمال	توقيع رقمي	توقيع رقمي تعمية بصمة hash	توقيع رقمي تعمية	توقيع رقمي تعمية- بصمة تعمية تشاكلية homomorphic تعمية تعتمد الهوية identity-based
نقاط القوة	ممانع للتصادمات	صعوبة عكس الترميز	صعوبة حل معادلات النظام المتعددة المتحولات	صعوبة إيجاد أساس جيد للشبكة
السرعة النظرية	تعتمد على تابع البصمة المستخدم	عالية عتادياً	عالية عتادياً	عالية برمجياً
السرعة العملية	سريعة جداً	عالية	لم تختبر	سريعة جداً (2014)
الميزات	سريعة جداً بأمان عالٍ	أمان جيد	سريعة حجم مفاتيح صغير	أمان عالٍ جداً
المساوئ	الأمان يعتمد على أمان تابع البصمة – الحاجة إلى ذواكر ضخمة	الحاجة إلى ذواكر ضخمة	وثوقية قليلة	حتى الآن لايوجد

الجدول (1) مقارنة بين تقنيات التعمية بعد الكمومية

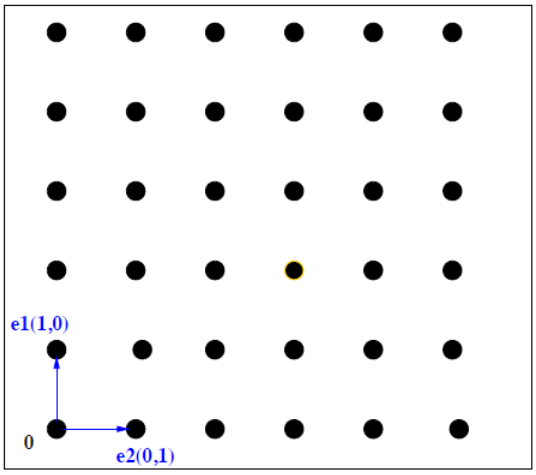
التعمية باستخدام الشبكة

3.1. نظرية الشبكة

الشبكة هي مجموعة من النقاط تأخذ شكلاً منتظماً في فضاء ذي n بعد. وبالتعريف الرياضي الدقيق الشبكة هي مجموعة الأشعة المولدة بمجموعة أشعة مستقلة وخطية، وتمثل هذه الأشعة v_i أساس الشبكة. الشكل -1- يوضح تمثيلاً لإحدى الشبكات في الفضاء $\mathbb{R}^2$ مع أشعة الأساس.

$$v_1, v_2, \ldots, v_n \in \mathbb{R}^n$$

$$L(v_1, v_2, \ldots, v_n) := \left\{ \sum_{i=1}^{n} \alpha_i v_i \mid \alpha_i \in \mathbf{Z} \right\}$$



الشكل (1) تمثيل الشبكة في الفضاء $\mathbb{R}^2$

تاريخياً تعود نظرية الشبكة إلى الرياضيين Lagrange, Gauss، وتقدمت بشكل متسارع لتصبح أداة حل للعديد من المشاكل الرياضية لاسيما في مجال التعمية. والسبب الرئيسي في الاعتماد على هذه النظرية هو حل مشاكل التعقيد بالنسبة للخوارزميات الأخرى. والتي أعطتها فيما بعد أهميتها في مجال السرية والأمان.

بداية الانطلاق هي ورقة البحث لـ Ajtai الذي وضع الشبكة كأداة في أنظمة التعمية [Ajt96]، حيث ربط بين مشاكل الشبكة التي سنراها لاحقاً والتعقيد الحسابي لها مما جعلها مناسبة جداً في عمليات التعمية. والأهمية الأخرى لطريقة Ajtai تتوضح في نسبة الأمان الذي نحصل عليه مقابل حل مشاكل الشبكة، حيث ترتبط نسبة الأمان في هذه الطريقة بمدى قابلية حل مشاكل الشبكة.

وهناك أسباب أخرى جعلت التعمية باستخدام الشبكة تأخذ أهميتها الكبيرة ومنها أن الحسابات التي تجري بسيطة جداً مقارنة بغيرها مما يجعلها فعالة جداً في الأجهزة المنخفضة الطاقة low-power.

وبما أن الحواسيب الكمومية ستصبح جاهزة للاستخدام خلال عدة سنوات (حسب بعض الشركات) فإنه من المهم جداً أن ننتقل إلى الخوارزميات الشـــبكية في التعمية، لأن الخوارزميات الكمومية الموجودة لتحليل الأعداد الكبيرة وحســـاب اللوغاريتم المتقطع (هذه التقنيات أســـاس قوة خوارزميات التعمية الحالية)، لم تستطع حتى الآن اختراق أو حل مشاكل الشبكة التي سنتحدث عنها.

3.2. مسائل الشبكة

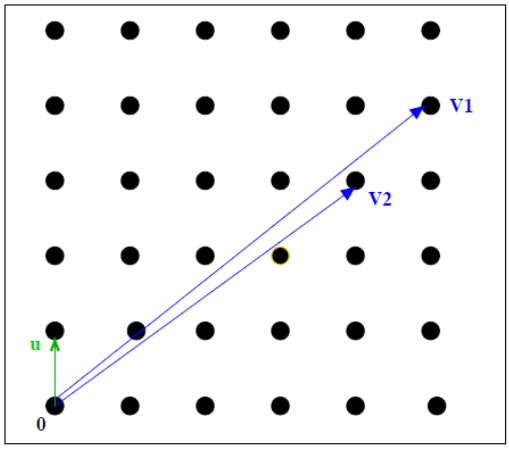
3.2.1. إيجاد الشعاع الأقصر SVP

إن المشكلة الأساسية في خوارزميات الشبكة هي إيجاد الشعاع الأقصر shortest vector problem SVP. وهي محاولة إيجاد الشعاع الأقصر غير الصفري في الشبكة، وبعبارة رياضية المشكلة هي إيجاد شعاع v غير الصفر بحيث يكون نظيمه أصغر من أي نظيم آخر في الشبكة بمعامل γ أي

$$\forall u \in L, \|v\| < \gamma \|u\|$$

$$\|u\| = \sqrt{\sum_{1}^{n} |u_i|^2}$$

الشكل التالي -2- يوضح ذلك حيث تمثل V1,V2 أشعة الأساس للشبكة، والشعاع u هو الشعاع الأقصر في هذه الشبكة.



الشكل (2) الشعاع u هو الأقصر بين أشعة الفضاء [2]

وهناك أيضاً مشاكل مثل SIVP وهي محاولة إيجاد مجموعة الأشعة المستقة الأقصر. وفي كلتا الحالتين المشكلة هي في إيجاد المسافة الأصغرية.

تكمن الصعوبة في هذا المجال بأنه يمكن أن يكون للشبكة أكثر من أساس، ويمكن لأشعة الأساس أن تكون أطول من الشعاع الأقصر، وقد كانت خوارزمية [Len82] LLL (خوارزمية كثيرات الحدود الزمنية

لحل مشاكل SVP) الأقرب في حل هذه المشكلة ولكن بزمن تنفيذ من رتبة $2^{O(n)}$ ، وقد قام Schnorr بتعميم هذه الخوارزمية للحصول على تقريب أفضل للمعاملات، ولكن بقيت المشكلة بأن رتبة التنفيذ الزمني من رتبة $2^{O(n)}$ ، وللتنفيذ العملي لهذه الخوارزمية نحتاج إلى حجوم كبيرة من المرتبة الأسية بالتالي بقيت هذه الخوارزمية نظرياً ولم تُنفذ.

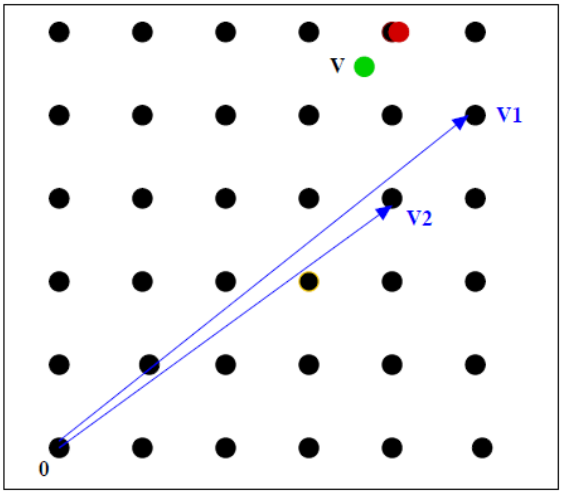
لذلك نستطيع القول إنه حتى الآن لا يوجد خوارزمية كثيرات حدود يمكنها حل المشكلة بزمن NP. وبالتالي فإن صعوبة حل هذه المشكلة هي التي أعطت خوارزميات التعمية باستخدام الشبكة الأمان الكبير ضد الهجمات التقليدية والكمومية.

3.2.2. إيجاد الشعاع الأقرب CVP

المشكلة الثانية في الشبكة هي إيجاد الشعاع الأقرب closest vector problem CVP وهي محاولة إيجاد الشعاع w الأقرب لشعاع معطى v. أي

$$\forall u \in L, \|w - v\| < \gamma \|u - v\|$$

في الشكل -3-، لدينا V1,V2 هي الاشعة الأساس في الشبكة، والنقطة v هي نقطة ما في الشبكة، فالهدف هو إيجاد أقرب نقطة في الشبكة للنقطة v.



الشكل (3) الشعاع u هو الأقرب بين أشعة الفضاء [2]

3.2.3. بعض الحلول المقترحة لحل مشاكل الشبكة

- **Gram-Schmidt Orthogonalization**

لتبسيط الحل يمكن تحديد أساس متعامد للشبكة. لذلك حاول Gram-Schmidt الوصول إلى أساس متعامد للشبكة باستعمال طريقة تكرارية اعتماداً على الأشعة الأساس الموجودة. حيث نختار شعاع b_1 وهو المرجع لباقي الأساس، ونحدد الشعاع b_2 مسقط b_1 على مستوي $(n-1)$ متعامد، ثم نختار b_3 مسقط b_1 على مستوي $(n-2)$ متعامد وهكذا حتى نحدد كل الأساسات في الشبكة.

$$b_i^* = b_i - \sum_{j=1}^{i-1} \mu_{i,j} b_j^*$$

وتكون عندئذ المجموعة هي مجموعة الأشعة المتعامدة الممثلة لأساس الشبكة.

$$\mu_{i,j} = \frac{\langle b_i, b_j^* \rangle}{\langle b_j^*, b_j^* \rangle}$$

ونحصل على شبكة جديدة B^* ربما تكون لا تساوي B، لكنها حتماً تمثل المسقط العمودي لـــ B على الفضاء المعرف.

- **LLL**

اقترح [Len82] Lenstra, Lenstra and Lovasz خوارزمية بزمن تنفيذ كثير حدودي للوصـــول إلى أساس متعامد في الشبكة B وبالتالي حل مشكلة SVP عن طريق حساب الأشعة الأقصر والأكثر اقتراباً من التعامد.

نعرف الأساس بحيث يحقق الشرطين:

$$\forall i, j \le n \quad |\mu_{i,j}| \le \frac{1}{2}$$

$$\forall k < n, \ \delta \|b_k^*\|^2 \le \|b_{k+1}^*\|^2 + |\mu_{k+1,k}|^2 \times \|b_k^*\|^2$$

وبالتالي بتمديد تعريف Gram-Schmidt نحصل على حل هذه الخوارزمية.

- **BKZ**

قام [Sch87] Korkine-Zolotarev بتعميم خوارزمية LLL وسميت Block KZ، حيث تقوم بحل مسألة SVP عن طريق تقسيم الأشعة الأساس إلى أجزاء blocks ومن ثم مقارنة هذه الأجزاء بطريقة مشابهة لـ LLL للوصول إلى الأساس المتعامد.

- **Babai's round off**

الحل الأبسط والأقل تعقيداً لمشكلة CVP هو اعتبار أن الأشعة الأساس خطية، وأن الشعاع الهدف هو عبارة عن تركيب خطي من هذا الأساس. فقام [Bab86] Babai بهذا التقريب وحاول الوصول إلى أساس خطي، وبالتالي الحصول على أساس متعامد، وتقريب المشكلة للحصول على أقرب شعاع ممكن للشعاع الهدف.

3.3. خوارزميات التعمية بالمفتاح العام باستعمال الشبكة

هناك العديد من خوارزميات التعمية بالمفتاح العام التي عمل العلماء على تطويرها اعتماداً على الشبكة وتعقيد الشبكة. بعض هذه الخوارزميات مازال نظرياً ولم يُطبَّق عملياً نتيجة التعقيد الكبير في الحسابات أو الذواكر الكبيرة المطلوبة لتنفيذه. ولكن الأمان الذي تعطينا إياه تلك الخوارزميات كبير جداً نتيجة مسائل الشبكة التي تحدثنا عنها وصعوبة حلها [lin11] .

3.3.1. GGH

اقترح [Gol97] Goldreich, Goldwasser, and Halevi خوارزمية جديدة للتعمية باستخدام الشبكة تعتمد عل نظام McEliece الذي يعتمد على فك التراميز الخطية. وتعمل هذه الخوارزمية كالتالي:

- المفتاح الخاص private H يصنف ضمن الأساس الجيد good basis للشبكة – أشعة قصيرة وتقريباً عمودية – حيث يمكن حل مشكلة CVP باستخدام هذا الأساس الجيد.
- المفتاح العام H هو أساس سيء لنفس الشبكة، وقد استخدم [Mic08] Micciancio النظيم الهرمتي للحصول على H.
- لإجراء عملية التعمية نحتاج إلى تعريف شعاع قصير r نعتبره شعاع ضجيج، يضاف إلى الرسالة التي تُعتبر نقطة في الشبكة v. وباستخدام النظيم الهرمتي نلاحظ أن $(r+v) \bmod H$ هو

تقريباً $r \bmod H$ بالتالي فإن أي مهاجم للقيمة $r \bmod H$ لن يستطيع الوصول إلى v باعتبار أن أي قيمة من الشبكة تعطي نفس القيمة بباقي القسمة على H .

- أما عملية فك التعمية فتقوم على إيجاد النقطة v من الشبكة والأقرب للقيمة المرسلة

$$c = r \bmod H = r + v$$

وبالتالي إيجاد شعاع الخطأ $r = c - v$

وباستخدام طريقة Babai's round off نستطيع الحصول على الشعاع v من خلال

$$v = B\left\lfloor B^{-1}(v + r)\right\rfloor$$

ولكن عملية التعمية محددة تماماً بالتالي لايمكن القول بأن السرية في هذه الخوارزمية عالية، ولزيادة السرية نختار إضافة حشو إلى الرسالة بشكل عشوائي.

وثمة نقطة ضعف أخرى في هذه الخوارزمية وهي عدم وجود طريقة محددة لاختيار المفتاح الخاص B، وشعاع الضجيج r .

3.3.2. NTRU

اقترح Hoffstein, Pipher and Silverman[Hof98] هذه الطريقة والتي تعتمد نموذجاً خاصاً من الشبكة وهو النموذج المعتمد على كثيرات الحدود الحلقية N-th TRUncated polynomial ring.

$$R = \mathbf{Z}[X]/(X^N - 1)$$
$$a(X) = a_0 + a_1 X + \ldots + a_{N-1} X^{N-1}$$

فالفكرة الأساسية في هذه الطريقة هي تبديل المصفوفات العامة إلى مصفوفات ذات صفات خاصة – مصفوفات دوارة – أي تحويل المصفوفة العشوائية $A \in \mathbf{Z}_q^{m \times n}$ إلى مجموعة مصفوفات أجزاء

$$A = [A^{(1)} | A^{(2)} | \ldots A^{(m/n)}]$$

وكل جزء هو عبارة عن مصفوفة دوارة أي:

$$A^{(i)} \in \mathbf{Z}_q^{n\times n}$$

$$A^{(i)} = \begin{bmatrix} a_1^{(i)} & a_n^{(i)} & \cdots & a_3^{(i)} & a_2^{(i)} \\ a_2^{(i)} & a_1^{(i)} & \cdots & a_4^{(i)} & a_3^{(i)} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ a_{n-1}^{(i)} & a_{n-2}^{(i)} & \cdots & a_1^{(i)} & a_n^{(i)} \\ a_n^{(i)} & a_{n-1}^{(i)} & \cdots & a_2^{(i)} & a_1^{(i)} \end{bmatrix}$$

$$a^{(i)} = \left(a_1^{(i)}, \ldots, a_n^{(i)}\right)$$

بمعنى أنها مصفوفة أعمدتها تنتج عن دوران العمود الأول أي:

$$A^{(i)} = \left[a^{(i)}, Ta^{(i)}, \ldots, T^{n-1}a^{(i)}\right]$$

$$T = \left[\begin{array}{c|c} 0^T & 1 \\ \hline I & 0 \end{array}\right]$$

وT هو التحويل الخطي الذي يحول إحداثيات شـــعاع الدخل إلى دورانية، عندئذ نعرف T*v على أنه المصفوفة الدوارة للشعاع v .

$$T*v = \left[v, Tv, \ldots, T^{n-1}v\right]$$

ويتعرف نظام التعمية NTRU بالمعاملات الثلاثة p,q,N بالإضـــافة إلى معامل الوزن d_f. حيث يمثل q معامل صـحيح – من الشـكل 2^n –، وp عدد صـحيح صـغير، والعددان p,q أوليان فيما بينهما، وN بعد الفضاء (عدد معاملات كثير الحدود).

وقد أشـار Silverman بأنه وحسـب قيمة هذه المعاملات يمكن تصـنيف درجة السـرية لهذا النظام. ويمثل الجدول التالي -2- توصيف درجة السرية حسب قيمة المعاملات:

	N	Q	P
Moderate Security	167	128	3
Standard Security	251	128	3
High Security	347	128	3
Highest Security	503	256	3

الجدول (2) درجة سرية نظام NTRU حسب معاملاته

ولتعمية رسالة معينة باستخدام هذه الطريقة:

- المفتاح الخاص : يتكون المفتاح الخاص من شعاعين $f, g \in \mathbf{Z}^{2n}$.

نختار f,g بحيث $\Lambda_q\left((T*f, T*g)^T\right)$ هي أصغر شبكة مترابطة تحوي f,g ، ويحققان الخواص التالية:

✓ المصفوفة T*f يجب أن تكون قلوبة بالمقاس q (mod q).

✓ نختار كثيري الحدود $\begin{matrix} f \in e_1 + \{p, 0, -p\}^n \\ g \in \{p, 0, -p\}^n \end{matrix}$ بحيث لدينا d_f+1 معاملات موجبة في كل من $f-e_1$ و g، و d_f معاملات سالبة والباقي أصفار.

✓ ويمكننا اختيار f من الشكل $f = 1 + pF$ حيث F كثير حدود عشوائي أيضاً، وذلك لتخفيف الحسابات والاكتفاء بعملية ضرب واحدة عند التنفيذ.

وبحسب Hoffestien فإن اختيار كثيرات الحدود f,g بهذه الطريقة يزيد من فعالية الأداء للنظام خلال عملية التعمية وفك التعمية. كما أن اختيار المصفوفة القلوبة والمعاملات {+p,0,-p} هي من أجل تسهيل حسابات المفتاح العام. ومن خلال هذا الشرط نلاحظ أيضاً أن f قلوب بالمقاس p أيضاً.

- المفتاح العام: يعرف المفتاح العام من المفتاح الخاص بالشكل التالي

$$H = \begin{bmatrix} I & O \\ T*h & q.I \end{bmatrix}$$

حيث

$$h = [T*f]^{-1} g \pmod q$$
$$h \in \mathbf{Z}_q^n$$

- التعمية: نرمز بداية الرسالة بشعاع $m \in \{-1,0,+1\}^n$ مع وجود d_f+1 معامل موجب و d_f معامل سالب. يجمع بعدئذ الشعاع m مع شعاع عشوائي r يحقق الخواص السابقة لـــ m. ونلاحظ أن عدد المعاملات غير الصفرية في كثير الحدود يستخدم لتحديد الحد الأعظمي للخطأ في عملية فك التعمية. ونحصل على شعاع الخطأ (-r,m) (من الواضح أن إشارة الناقص لـ r ليس لها أهمية، فقط للحفاظ على نفس الشكل في التعريف الأساسي).

وبحساب هذا الشعاع بالمقاس H نجد :

$$\begin{bmatrix} -r \\ m \end{bmatrix} \bmod \begin{bmatrix} I & O \\ T*h & q.I \end{bmatrix} = \begin{bmatrix} 0 \\ \left(m+[T*h]r\right) \bmod q \end{bmatrix}$$

أي أن الرسالة المعماة التي حصلنا عليها هي

$$c = \left(m+[T*h]r\right) \bmod q$$

- فك التعمية: لفك تعمية الرسالة المعماة نبدأ بحساب جداء الرسالة المعماة c مع المصفوفة السرية T*f .

$$\begin{aligned} [T*f]c \bmod q &= [T*f]m + [T*f][T*h]r \bmod q \\ &= [T*f]m + [T*g]r \bmod q \end{aligned}$$

باعتبار أن العلاقة $[T*f][T*h] = \left[T*\left([T*f]h\right)\right]$ صحيحة دوماً لأي شعاع f,h.

نلاحظ أن المقدار السابق محدود دوماً بالقيمة q/2 بالتالي نحصل على القيمة الصحيحة $[T*f]m + [T*g]r$ دائماً.

وإذا حسبنا هذا المقدار بالمقاس p نجد:

$$[T*f]m + [T*g]r \bmod p = I.m + O.r = m$$

أي أننا نحصل على الرسالة الأصلية.

إذن لتحقيق نظام تعمية باستخدام NTRU نحتاج المواصفات التالية [Gau14]

Public Parameters	N	Prime (250<N<2500)
	Q	Large modulus (250<N<2500)
	P	Small modulus P=3, gcd (p,q)=1
Private Key	F	f=1+p**F** (**F** random $\{-1,0,+1\}^N$)
	G	g=p**G** (**G** random $\{-1,0,+1\}^N$)
Public Key	H	$h = f^{-1} * g \pmod q$
Encryption	M	Plaintext $\{-1,0,+1\}^N$
	R	random $\{-1,0,+1\}^N$
	C	$c = r * h + m \pmod q$
Decryption	A	$a = f * c \pmod q$
	M	$m = a \pmod p$

أما بالنسبة للسرية فحتى الآن لايوجد إثبات على مقدار السرية في هكذا أنظمة، ولكن تجريبياً أثبتت خوارزمية NTRU أن السرية فيها عالية بدرجة كافية ضد أي نوع من أنواع الهجمات الممكنة، وكما نعلم فإن أقوى هجوم حتى الآن موجود عالمياً هو هجوم [Gra07] Howgrave-Graham فهو يعتبر مقياس أمن لأي خوارزمية.

وبتطبيق هذا الهجوم على خوارزمية NTRU نحصل على الجدول التالي -3- الذي يمثل المقدار المطلوب من السرية مقدراً بالبت مقابل معاملات الخوارزمية .

حيث يعرف مقدار السرية مقدراً بالبت k-bits بأن الهجوم الأقوى على الخوارزمية يتطلب عدد عمليات 2^k عملية، وهو يكافئ سرية خوارزمية متناظرة [Lan14] [xin13] .

Estimated security (bits)	N	Q	d_f	Key size (bits)
80	257	1024	77	2570
80	449	256	24	3592
256	797	1024	84	7970
256	14303	256	26	114424

الجدول (3) مقدار السرية في نظام NTRU مقابل معاملات الخوارزمية وطول المفتاح

3.4. مقارنة أداء خوارزميات التعمية غير المتناظرة

نعلم أن الخوارزميات التقليدية في التعمية تحتاج إلى حجم مفتاح كبير للوصـــول إلى مقدار أعلى من السـرية، بالتالي لابد من خوارزميات أخرى أكثر تقدماً للحصـول على نفس السـرية بحجم مفاتيح أقل، وهو ما يميز خوارزمية NTRU حيث حجم المفتاح العام المســتخدم أقل من حجمه في RSA عند نفس السرية، كما أن درجة كثير الحدود أقل. وهذا يعود إلى استخدام كثيرات الحدود الحلقية بدل التحليل إلى العوامل الأولية وحساب اللوغاريتم المتقطع. لذلك فإن تعقيد خوارزمية NTRU عند توليد المفاتيح تقريباً من مرتبة $O(N)$ بينما نجد التعقيد في RSA من مرتبة $O(N^2)$. [Ali07]

والجدول التالي -4- يبين التعقيد في الخوارزميتين عند عملية توليد المفاتيح وعند التعمية وفك التعمية [Kum12].

	Encryption/Decryption	Key Generation
RSA	$O(N^3)$	$O(N^2)$
NTRU	$O(N \log N)$	$O(N)$

الجدول (4) مقدار التعقيد في خوارزميتي NTRU, RSA

- **حجم المفاتيح:**

في خوارزميات RSA و ECC يكون حجم المفتاح الخاص و العام تقريباً نفسه، بينما في NTRU يختلف طول المفتاح العام عن الخاص بنسبة تصل بين $\frac{n}{n-k}\log_p q$ و 1.

والجدول التالي -5- يوضح طول المفتاح العام المستخدم في الخوارزميات الثلاثة بالنسبة لمقدار السرية المطلوب [WEB07]

Security Level (bits)	NTRU (bits)	ECC (bits)	RSA (bits)
80	2008	160	1024
112	3033	224	2048
128	3501	256	3072
160	4383	320	4096
192	5193	384	7680
256	7690	521	15360

الجدول (5) مقارنة طول المفتاح العام في خوارزميات NTRU, RSA, ECC

نلاحظ من الجدول السابق أن طول المفتاح في ECC أصغر من باقي الخوارزميات، بالتالي توفر في حجم الذاكرة المستخدمة، كما نلاحظ أنه بزيادة السرية يصبح حجم المفتاح في NTRU أقل منه في RSA.

- **السرعة في توليد المفاتيح والتعمية وفك التعمية[1]**

نبدأ بمقارنة NTRU مع RSA في سرعة توليد المفاتيح، وحجم المعطيات المعالجة خلال ثانية واحدة .

هذه المقارنات تمت بعد برمجة الخوارزميات بلغة C في بيئة (.NET 4.5) VisualStudio 2012 في معالج intel core i3 @2.53 GHz. لنحصل على الجدول التالي -6-

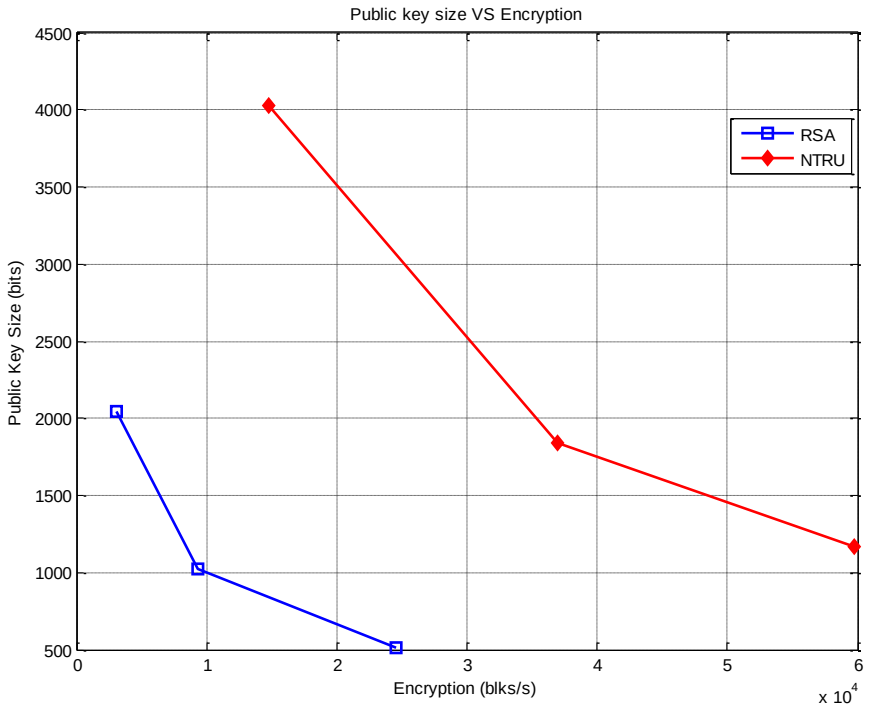
System	Security (MIPS-years)	Public Key Size(bits)	Key Generation (msec)	Encrypt (blks/s)	Decrypt (blks/s)
RSA 512	$3.98*10^{4}$	512	25.871	24532	1227
RSA 1024	$3.00*10^{11}$	1024	127.365	9366	221
RSA 2048	$2.99*10^{20}$	2048	417.418	3115	30
NTRU 167	$2.70*10^{5}$	1169	0.398	59706	28321
NTRU 263	$4.59*10^{13}$	1841	0.746	36943	16271
NTRU 503	$3.36*10^{34}$	4024	1.721	14783	6110

الجدول (6) مقارنة سرعة توليد المفاتيح مع حجم المعطيات في خوارزميتي NTRU, RSA[1]

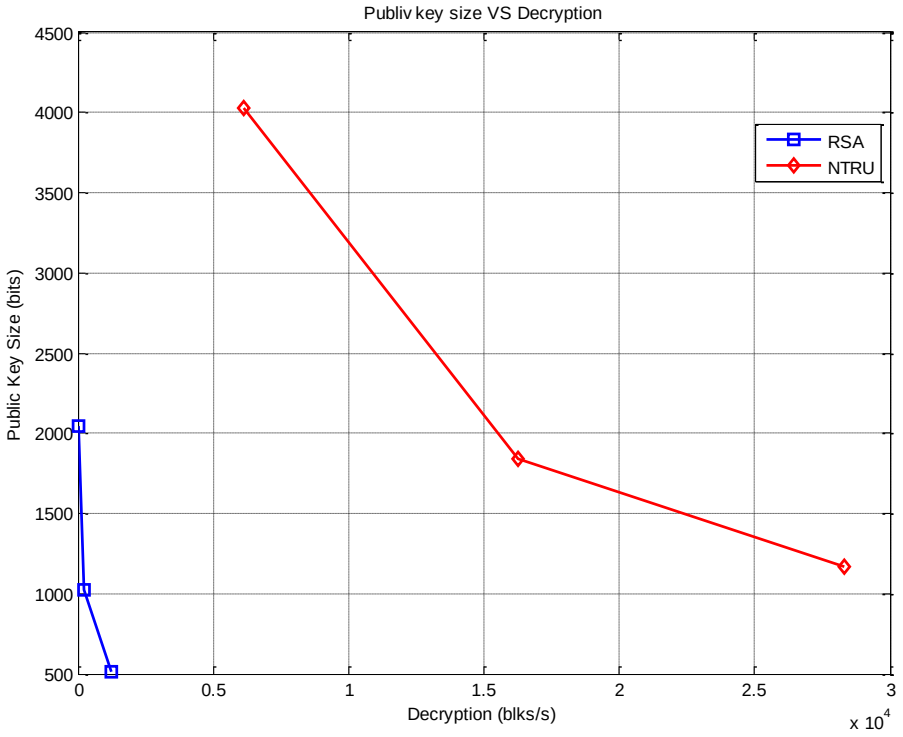
[1] http://www.certicom.com

نلاحظ من الجدول السابق أن NTRU تتقدم في أدائها على خوارزمية RSA من حيث السرعة في توليد المفاتيح ضمن نفس مجال السرية المطلوب.

نلاحظ أيضاً أن NTRU تقوم بتعمية عدد أكبر من الرسائل عند نفس حجم المفتاح والسرية. فإذا رسمنا المنحني الذي يربط سرعة التعمية/ فك التعمية بطول المفتاح، الشكل -4.a- والشكل -4.b-، نلاحظ أنه عند نفس الطول للمفتاح العام يمكننا تعمية عدد أكبر من الرسائل، وكذلك فك التعمية بسرعة أكبر.



الشكل (4.a) علاقة سرعة التعمية بطول المفتاح العام في NTRU,RSA



الشكل (4.b) علاقة سرعة فك التعمية بطول المفتاح العام في NTRU,RSA

- نقارن الآن خوارزمية NTRU مع ECC بالمحددات السابقة نفسها فنجد الجدول -7-.

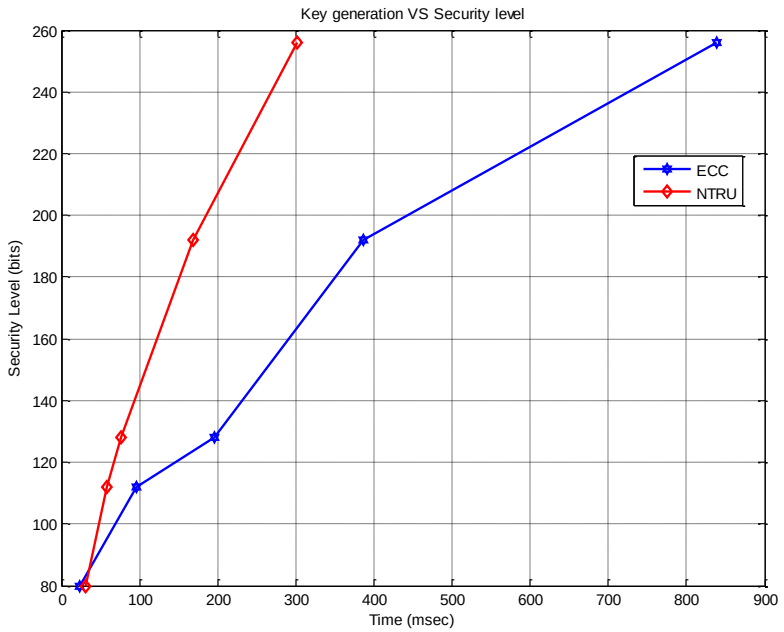
نلاحظ من الجدول -7- أن سرعة NTRU في التعمية/فك التعمية أفضل منها في ECC أي أنه يمكننا تعمية عدد أكبر من الرسائل عند نفس الحجم والسرية المطلوبة، وهذا يعود إلى بساطة العمليات المستخدمة في خوارزمية NTRU مقارنة بها في ECC.

أما بالنسبة لتوليد المفاتيح إذا رسمنا المنحني الذي يمثل سرعة توليد المفاتيح مع مقدار السرية، الشكل - 5 - ، نلاحظ أيضاً أن NTRU تعطي أداء أفضل من ECC كلما زادت نسبة السرية.

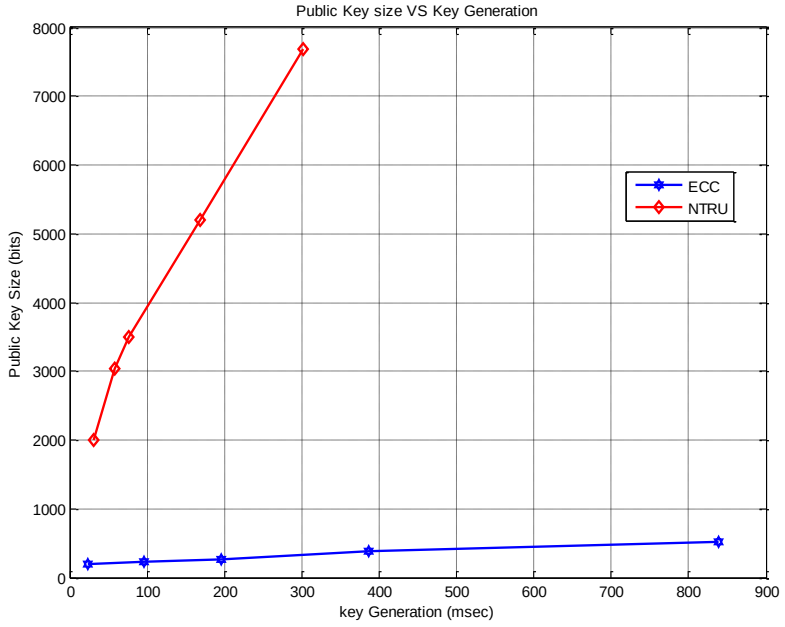
وبالمقارنة مع حجم المفتاح، الشكل -6-، نلاحظ أيضاً أن أداء NTRU يتفوق على ECC بسرعة توليد المفاتيح حتى مع الحجوم الكبيرة للمفتاح العام.

System	Security (bits)	Public Key Size(bits)	Key Generation (msec)	Encrypt (msec)	Decrypt (msec)
ECC 192	80	192	23.625	15.436	7.818
ECC 224	112	224	95.575	21.441	10.757
ECC 256	128	256	195.233	28.055	14.289
ECC 384	192	384	386.787	74.444	36.992
ECC 521	256	521	838.967	172.791	86.283
NTRU 251	80	2008	30.884	0.686	3.356
NTRU 347	112	3033	58.853	1.269	6.409
NTRU 397	128	3501	77.126	1.621	8.271
NTRU 587	192	5193	168.239	3.438	18.134
NTRU 787	256	7690	301.593	5.916	32.448

الجدول (7) مقارنة سرعة توليد المفاتيح مع حجم المعطيات في خوارزميتي NTRU, ECC

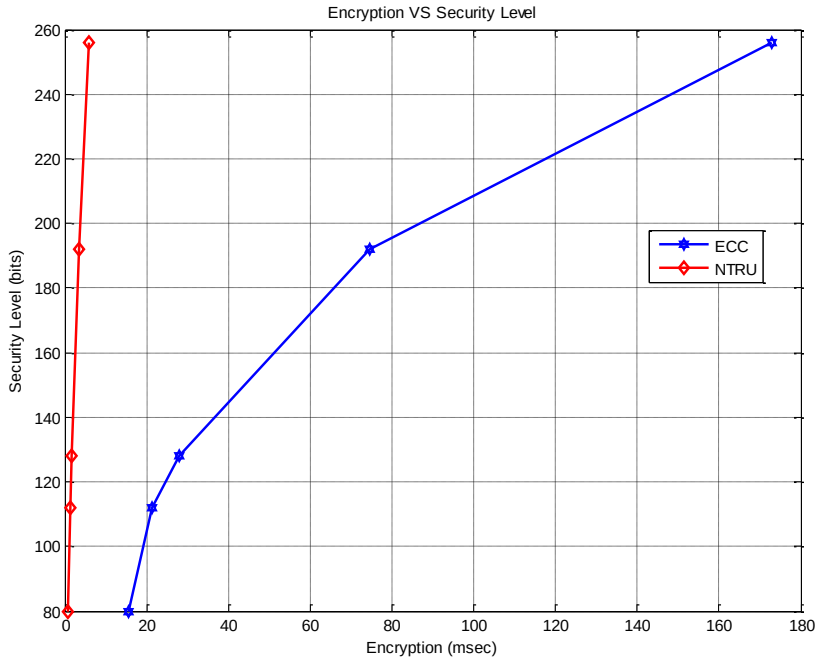


الشكل (5) علاقة مقدار السرية مع سرعة توليد المفاتيح في NTRU,ECC

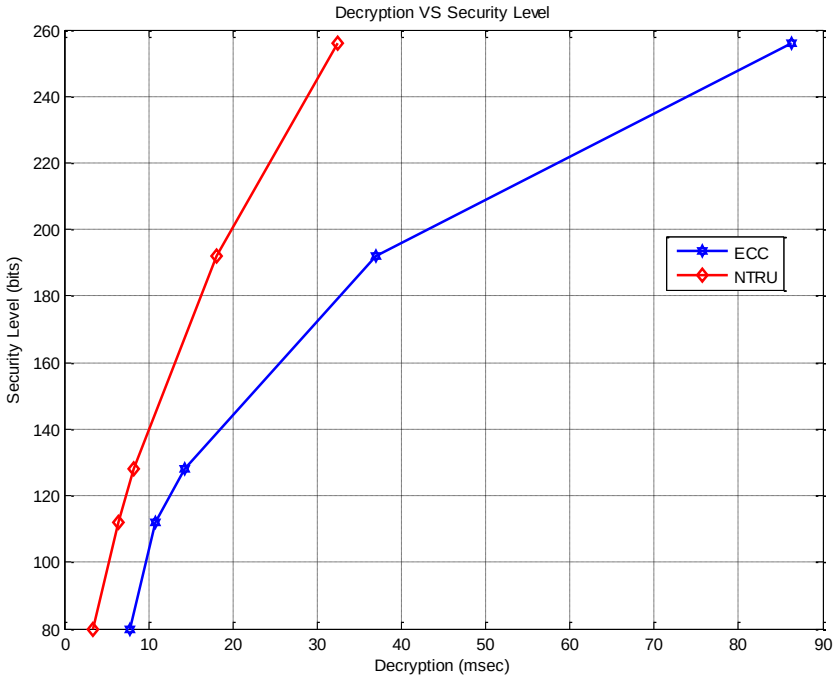


الشكل (6) علاقة حجم المفتاح بسرعة توليده في NTRU,ECC

أما بالنسبة لأداء التعمية/فك التعمية للوصول إلى مقدار السرية المطلوب نجد المنحنيات التالية، الشكل -7.a- والشكل -7.b- ويوضحان العلاقة بين المقدار المطلوب من السرية مع سرعة التعمية وفك التعمية.



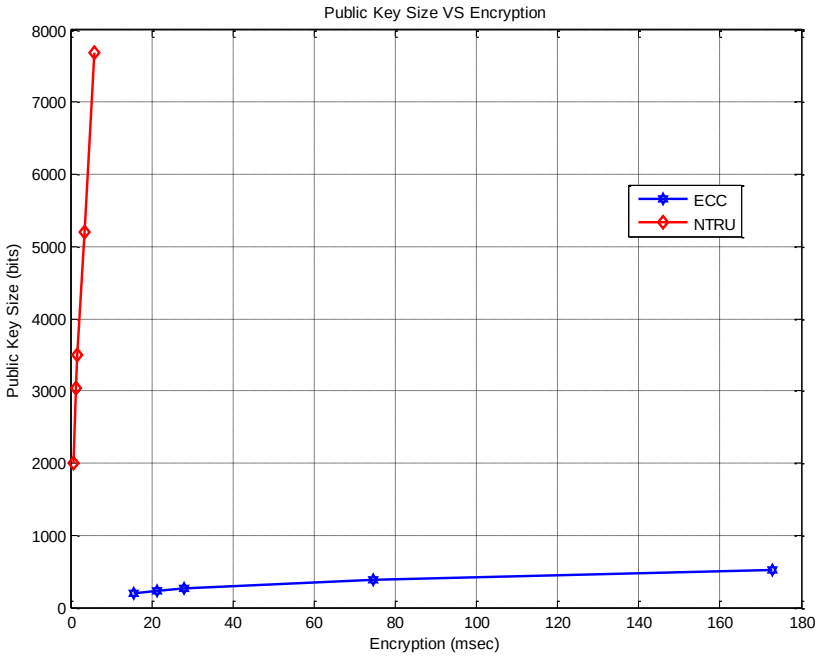
الشكل (7.a) علاقة مقدار السرية مع سرعة عملية التعمية في NTRU,ECC



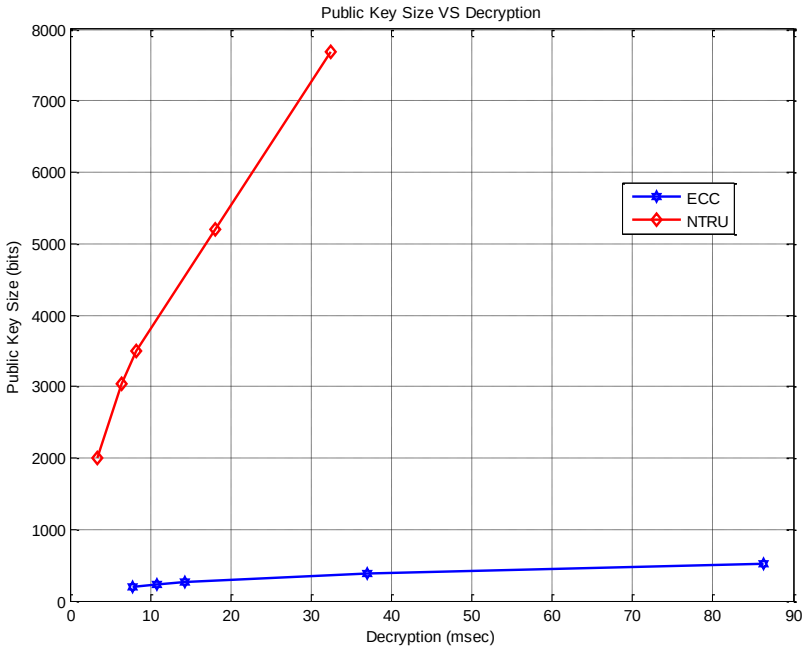
الشكل (7.b) علاقة مقدار السرية مع سرعة عملية فك التعمية في NTRU,ECC

نلاحظ الســـرعة العالية عند تنفيذ عمليات التعمية/فك التعمية بالنســـبة لخوارزمية NTRU مقارنة مع ECC.

وإذا رسمنا المنحني الذي يربط حجم المفتاح العام مع سرعة تنفيذ الخوارزميات، الشكل -8.a- والشكل -8.b-، نجد



الشكل (8.a) علاقة حجم المفتاح بسرعة تنفيذ التعمية في NTRU,ECC



الشكل (8.b) علاقة حجم المفتاح بسرعة تنفيذ فك التعمية في NTRU,ECC

نلاحظ مما سبق سرعة التنفيذ لخوارزمية NTRU مقارنة بـ ECC حتى عند الحجوم الكبيرة للمفتاح العام.

إذن للوصـــول إلى خوارزمية جيدة للتعمية يجب تحقيق التوازن بين طول المفتاح وســـرعة التنفيذ ومقدار الأمان الجيد، وهو ما تحقق في خوارزمية NTRU بالإضـــافة إلى فعاليتها في صـــد الهجمات الكمومية، بالتالي فإنها المستقبل الواعد وبقوة لنظم التعمية المتقدمة مهما تطورت الحواسيب والمعالجات الحسابية.

الشبكات اللاسلكية المخصصة النقالة

تتميز الشبكات المخصصة النقالة MANET بعدم وجود إدارة مركزية للشبكة، أي أن تشكيل الشبكة وانضمام عقد جديدة إليها أو انفصال عقد عنها يجري بشكل عشوائي، مما يعني تغير مستمر في طبولوجية الشبكة.

هذا التغير في طبولوجية الشبكة يؤدي إلى ظهور مشاكل في عملية التسيير routing، وكذلك فإن مسار المعطيات من المرسل إلى المستقبل يتغير باستمرار ولايمكن توقعه. لذلك لابد من وجود آلية لضمان خصوصية هذه المعطيات، وحمايتها من التلف أو السرقة أو التعديل، حيث لابد من وجود آلية للتوثق من هوية العقد في الشبكة لضمان عدم وصول المعطيات إلى جهات غير مرغوبة، وعدم إنكار المرسل للمعطيات التي أرسلها.

تكمن المشكلة الأساسية في شبكات MANET في إيجاد آلية مناسبة لإدارة شهادات الوثوقية Certificate Authority التي تعتبر الإشكالية الرئيسية في بناء الأنظمة الآمنة. وكما نعلم فإن النظام يعتبر آمناً إذا استطاع ضمان الخدمات الأمنية التالية:

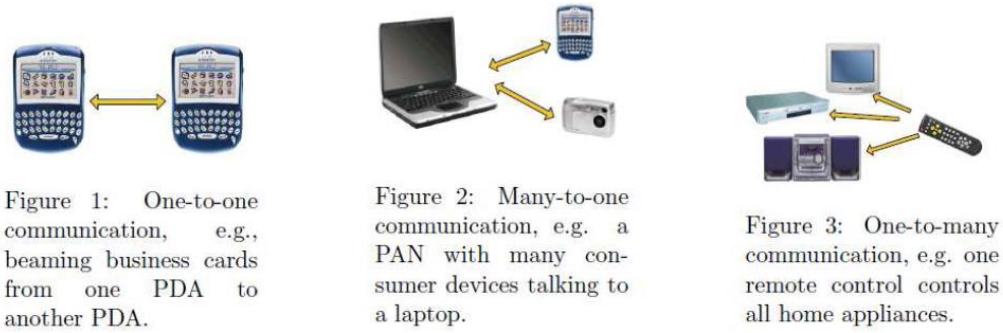
- الاستيقان Authentication.
- سلامة المعطيات Data Integrity.
- سرية المعلومات Data Confidentiality.
- عدم الإنكار non-Repudiation.

فالهدف الأساسي في بحثنا الآن هو بناء نظام لاسلكي آمن يؤمن آليات التوثق من عقد الشبكة، ونقل المعطيات بينها بشكل آمن وسري من خلال آلية مناسبة لإدارة شهادات الوثوقية CA.

4.1. شبكات ad-hoc وشبكات MANET

تتألف شـبكات ad hoc من مجموعة من العقد المتنوعة التي تتواصـل فيما بينها، حيث يمكن أن تكون هذه العقد أجهزة حاسوبية، أو أجهزة اتصال ثابتة أو متحركة، أوحتى مجموعة من الحساسات وغير ذلك الكثير...

هذا التنوع في العقد يجعل بنية شـبكة ad hoc غير متجانسـة heterogeneous structure كما في الشكل-9-.



الشكل (9) مثال يظهر البيئة غير المتجانسة في شبكات ad-hoc

من جهة ثانية تتميز شـبكات ad hoc باللامركزية في بناء الشـبكة وإدارتها وتأمين عمليات التسـيير بين العقد routing ، لأن العقد تتصـرف بشـكل عشـوائي في انضـمامها للشـبكة وانفصـالها عنها، كما أن عملية التسـيير تعتمد على تفاعل كل العقد مع بعضـها. كما يمكن لهذه العقد أن تتحرك بمعظمها مما يؤدي إلى تغيير مستمر في طبولوجية الشبكة، ويسمى هذا النوع من الشبكات بـشبكات ad-hoc النقالة، Mobile ad-hoc networks (MANET).

ويمكن تلخيص ميزات شبكات MANET بالنقاط التالية [Mar10] :

- سهولة الإنشاء وقلة التكاليف لعدم وجود بنية تحتية:

إن شـبكات ad hoc لا تسـتند إلى بنية تحتية ثابتة بل تعمل بشـكل مسـتقل و تتمتع بمتانة جيدة و تعتبر ذات تكلفة قليلة، لأنها لا تحتاج إلى تكاليف في التركيب و الصيانة.

- لايوجد إدارة مركزية للشبكة:

بحكم حركية العقد وعدم وجود مسـارات ثابتة فإنه لايمكن تحديد عقد مركزية ثابتة مسـؤولة عن إدارة الشبكة.

- عملية التسيير تعتمد على تفاعل كل العقد المشكلة للشبكة مع بعضها.

- حجم الشبكة قابل للزيادة بدون أي إعدادات إضافية.
- طبولوجية الشبكة تتغير بشكل ديناميكي تبعاً لانضمام عقد جديدة أو انفصال عقد موجودة.
- ضبط إعدادات الشبكة يجري بشكل ذاتي.

لذلك نلاحظ الانتشار الواسع لشبكات MANET في التطبيقات العسكرية، والمدنية كشبكات الهاتف الجوال والإسعاف وطواقم الإغاثة ....الخ

لكن هذه الميزات تقابلها خوارزميات معقدة لضمان عملية التسيير، كما يتطلب إيجاد حلول للمشاكل الأمنية التي تعاني منها هذه الشبكات –كما سنرى لاحقاً- حيث لاتنفع الطرق التقليدية في حماية الشبكات ذات البنية المحددة في هذا النوع من الشبكات.

كذلك فإن شبكات MANET تعاني من قلة الموارد في العقد المشكلة لها بسبب محدودية الاستطاعة المقدمة لها –تبعاً لحجم وموقع تلك العقد-، ومحدودية قدراتها الحسابية، وكذلك محدودية مساحة تخزينها. تتطلب هذه الموارد المحدودة إيجاد بروتوكولات عمل وأنظمة منخفضة التعقيد من أجل عمل فعال ضمن الشبكة.

وتساهم لامركزية الشبكة في زيادة العبء المحمل على العقد من خلال عمل العقدة كمرسل ومستقبل وموجه ومدير في آن معاً.

كما أن هذه الشبكات تحتاج إلى بناء أنظمة أمنية خاصة مناسبة تؤمن سرية المعلومات، وسلامتها، وضمان عدم وصولها إلى عقد أخرى غير موثوقة.

4.2. التسيير routing في شبكات MANET

تعتبر عملية التسيير من القضايا المهمة جداً، حيث ماتزال الأبحاث جارية لمحاولة إيجاد حلول فعالة تناسب تعقيد المسألة، والقدرات الحسابية للأجهزة المستخدمة التي غالباً ماتكون محدودة.

في الشبكات التقليدية يتولى عملية التسيير أجهزة هي الموجهات routers، تكون مسؤولة عن إيصال الرسالة من المنبع إلى الوجهة بإيجاد أفضل الطرق اعتماداً على خوارزميات التسيير التي تعتمد أساساً على نظرية البيان graph theory من خلال عدة بروتوكولات Routing Information Protocol(RIP),

Ad-hoc On-demand Distance Vector(AODV), Dynamic Source Routing(DSR), Open Shortest Path First(OSPF), Border Gatway Protocol(BGP) ... .

أما في شبكات ad hoc عموماً وشبكات MANET خصوصاً يقع عبء عملية التسيير على العقد نفسها المشكلة للشبكة. إذ تعتمد آلية التسيير على نقل الرسالة من المنبع إلى إحدى العقد الواقعة ضمن نطاق التغطية، والتي تعمل بدورها إلى نقل الرسالة إلى عقدة أخرى حتى الوصول إلى العقدة الوجهة. ومما يزيد الأمور تعقيداً أن طبولوجية الشبكة تتغير باستمرار نتيجة انضمام عقد جديدة وخروج عقد أخرى، وكذلك نتيجة حركية العقد نفسها مما يعني تغير مناطق تغطية كل عقدة باستمرار.

لذلك جرى اقتراح عدة بروتوكولات تعالج عملية التسيير في شبكات MANET، ويمكن تقسيمها إلى مجموعتين رئيسيتين هي البروتوكولات الاستباقية proactive والبروتوكولات التفاعلية reactive. وهناك المجموعة الثالثة الهجينة hybrid وهي تضم المجموعتين السابقتين [Rau13] .

4.2.1 بروتوكولات التسيير الاستباقية proactive routing protocols

تسمى أيضاً table-driven routing protocols. كل عقدة تحوي جدولاً للتسيير routing table يحدد المسار لكل رسالة واردة من عقدة ما، ويجري بناء المسارات بشكل كامل قبل بدء عملية التسيير، ثم يُحدّث الجدول دورياً.

ومن أشهر البوروتوكولات التي تعتمد هذه الطريقة هي ... DSDV,OLSR,WRP

- Destination Sequence Distance Vector (DSDV): يعتمد على خوارزمية Distributed Bellman-Ford حيث تحتفظ كل عقدة بجدول تسيير يحوي عنوان العقدة التالية next hop، وعدد الخطوات اللازمة للوصول إلى الوجهة، ورقم الترتيب sequence number.
- Optimized Link State Routing (OLSR): حيث تعتمد كل عقدة على أحدث المعلومات في جدول التسيير لإرسال الرسالة. تحدد كل عقدة مجموعة من العقد تسمى MPR (Multi Point Relay) وتمتاز هذه العقد بأنها على مسافة خطوة واحدة ويمكن الوصول إلى أي عقدة في الشبكة من خلالها. بالتالي فإن العقدة تعتمد على مجموعة MPR خاصتها في إرسال أي رسالة مما يؤدي إلى تخفيف عبء التسيير.

- Wireless Routing Protocol (WRP): وهو تطوير لبروتوكول DSDV الذي يعاني عبئاً كبيراً بسبب كبر حجم جدول التسيير، لذلك يتم تجزئته إلى أربعة جداول: جدول التسيير، وجدول الكلفة، وجدول المسافات، ولائحة الرسائل المعاد إرسالها.

إن هذه المجموعة من البروتوكولات لاتعاني من مشكلة التأخير في إرسال الرسائل بسبب جهوزية جداول التسيير دوماً. غير أن هذه الميزة تسبب أعباءاً إضافية على العقد لتحديث الجداول بشكل دوري، أو عند حدوث تغيير في طبولوجية الشبكة. كما أنها تستهلك الكثير من الموارد – خصوصاً في الشبكات الكبيرة – وذلك لحفظ المسارات مع العلم أن الكثير من هذه المسارات لن يلزم لاحقاً.

4.2.2 بروتوكولات التسيير التفاعلية Reactive Routing Protocols

وتسمى أيضاً on-demand protocols. وهي الآلية التي تسمح ببناء المسار حين الحاجة إليه فقط. وتتميز بوجود طوري عمل:

- طور استكشاف الطريق Route Discovery: حيث تقوم العقدة المنبع بالبحث عن المسار الموصل إلى الوجهة في الخبيئة cache، وفي حال عدم وجوده يتم البحث عنه بالاستعانة بالعقدة المجاورة – ضمن مجال التغطية –. فتقوم العقدة المنبع بإرسال رسالة استكشاف تحوي عنوان العقدة المجاورة التي تحاول بدورها استكشاف الطريق بنفس الآلية. وعند الوصول إلى العقدة الوجهة يتم تخزين المسار عند المنبع من خلال معالجة رسائل acknowledgments وذلك للاستفادة منه مستقبلاً.
- طور الصيانة Route Maintenance: بسبب تغير طبولوجية الشبكة قد تصبح بعض المسارات غير صالحة للاستخدام، وهنا يتم إعادة إصلاح المسار بحيث يصل المرسل بالمستقبل إن أمكن ذلك طبعاً.

ومن أهم البروتوكولات التي تعمل بهذه الآلية DSR, AODV, TORA, LMR… [kau12] .

- Dynamic Source Routing (DSR): يعتمد هذا البروتوكول على خوارزمية link state، حيث يتم بناء المسار من المرسل إلى المستقبل عبر العقد الوسيطة، وتدرج كل عقدة وسيطة عنوانها ضمن المسار حتى الوصول إلى العقدة الهدف.

- Ad-hoc On-demand Distance Vector (AODV): ترسل العقدة المرسل طلباً route-req، وتعيد كل عقدة وسيطة إرسال الطلب إذا لم يكن المسار متوفراً عندها، وهكذا حتى الوصول إلى العقدة الوجهة التي ترسل الرسالة route-rep إلى المرسل.

وسنستخدم لاحقاً تعديلاً على هذا البروتوكول لتحقيق متطلبات الأمن التي تحدثنا عنها سابقاً.

إن هذه الآلية تحول دون استكشاف مسارات لاحاجة لها، مما يعني تخفيف العبء عن العقد. لكن بالمقابل فإن استخدام هذه البروتوكولات يسبب تأخيراً في إرسال ووصول الرسائل عبر الشبكة بسبب الوقت اللازم لاستكشاف المسار، والوقت اللازم لصيانته عند تغير طبولوجية الشبكة.

4.2.3 بروتوكولات التسيير الهجينة Hybrid Routing Protocols

تجمع هذه الآلية بين المجموعتين السابقتين، بحيث تقلل من التأخير في إرسال الرسائل الذي تعاني منه البروتوكولات التفاعلية، وتخفف العبء على العقد الذي تعاني منه البروتوكولات الاستباقية. ومن أشهر البروتوكولات الهجينة ZRP,SHRP .

- Zone Routing Protocol (ZRP): يتم تصنيف العقد في هذا البروتوكول إلى عقد داخلية وعقد محيطية، ولكل عقدة منطقةٌ تضم مجموعة من العقد التي لاتبعد عنها أكبر من مسافة محددة. ثم يتم استخدام بروتوكول استباقي للتسيير ضمن المنطقة، وبروتوكول تفاعلي للتسيير خارج المنطقة.

نلاحظ مماسبق اختلاف المعايير المحددة لعملية التسيير ضمن تلك البروتوكولات، لكن هذا الاختلاف يقابله مسألة موحدة لا يمكن تجاهلها، وهي أن اختيار العقد المشكلة للمسار يتم دوماً بشكل آلي. وهذا يؤدي إلى أن المعلومات المتبادلة قد تصل إلى عقد غير موثوقة الأمر الذي يؤثر على خصوصية وسلامة المعلومات. لذلك لا بد من إيجاد آليات تضمن سلامة المعلومات وخصوصيتها عند الانتقال من عقدة إلى أخرى، وهذا هو محورنا القادم.

4.3. المشاكل الأمنية في شبكات MANET

تعتبر المسائل الأمنية في شبكات MANET تحدياً كبيراً، وذلك بسبب حرية الحركة المفروضة للعقد، والطبولوجيا المتغيرة للشبكة، ومجال التغطية المحدود للعقد بالإضافة إلى أخطاء الإرسال المحتملة .

طالما أن جميع العقد في الشبكة تتعاون مع بعضها لإيصال الرسائل فإن قناة الاتصال اللاسلكية معرضة للهجمات active and passive attacks عن طريق العقد غير النظامية malicious nodes وأهم هذه الهجمات هي الاحتيال spoofing، والتنصت eavesdropping، ورفض الخدمة أو الإنكار Denial of Service (DoS).

وبالتالي فإن إجرائيات الأمن لها أولوية قصوى في هذه الشبكات.

ولبناء نظام أمني جيد يجب توافر مجموعة من الخدمات أهمها:

- الخصوصية confidentiality .
- سلامة المعطيات integrity.
- التحقق من الهوية authenticity .
- عدم الإنكار non-repudiability .
- المتاحية availability .

وتعتبر اللامركزية في إدارة شبكات ad-hoc و MANET أكبر عائق أمام إنشاء أنظمة أمنية جيدة تناسب هذه الشبكات، وذلك لأن الحلول الأمنية المعروفة تعتمد بشكل أساسي على وجود شهادة وثوقية certificate تصدر عن سلطة التوثيق CA والتي تتطلب وجود مخدمات مركزية تختص بهذا الشأن، أي يجب وجود طرف ثالث موثوق ومسؤول عن إصدار الشهادات.

وللبحث في هذه الإشكالية يجب التذكير بداية بمفهوم PKI.

4.3.1. البنية التحتية للمفتاح العام (PKI) Public Key Infrastructure

إن أنظمة الشركات الكبيرة والتجارة الالكترونية وغيرها تتطلب آليات موثوقة لحماية المعطيات الخاصة بها، وضمان نقلها عبر شبكة الانترنت بأمان. ولعل أكثر الحلول انتشاراً هي الحلول المبنية على PKI والتي تؤمن مجموعة الخدمات الأمنية باستعمال تقنيات التعمية بالمفتاح العام Public Key Cryptographyالتي تمكن المستخدمين من نقل المعطيات بشكل آمن.

يمكننا تعريف PKI على أنها بنية تضم مجموعة من الأشخاص مثلاً، والإجراءات، والسياسات الأمنية، والبروتوكولات، وعتاديات وبرمجيات لتوليد شهادات الوثوقية القائمة على المفتاح العام وتخزينها وإدارتها ومنحها ورفضها. [Weio1]

ويمكن تلخيص الوظائف الأساسية لل PKI فيمايلي:

1. التعمية بالمفتاح العام Public Key Cryptography: حيث تدعم PKI تقنيات التعمية بالمفتاح العام، وتقوم بتوليد أزواج المفاتيح عام/خاص وتوزيعها وإدارتها.

2. إصدار الشهادات Certificate Issuance: تتم عن طريق سلطات التوثيق CA بهدف توثيق المعلومات الشخصية أو الاعتمادية credentials لمستخدم أو جهة بمفتاحه العام، وتتم عملية التوثيق هذه من خلال توقيع الشهادة رقمياً بالمفتاح الخاص لـ CA ، وتعتبر عملية التحقق من شخصية المستخدم والمعلومات المراد توثيقها من المشكلات الكبيرة والحساسة.
3. التحقق من صلاحية الشهادات Certificate Validation:
   - التحقق من أن الشهادة صادرة عن جهات معروفة وموثوقة.
   - التحقق من سلامة المعطيات data integrity من خلال التحقق من التوقيع الرقمي لها.
   - التحقق من تاريخ الصلاحية.
   - التحقق من استخدام الشهادة بالتوافق مع القيود والمعايير المعرفة في سياسة الاستخدام.
4. رفض (إلغاء) الشهادات Certificate Revocation: قد تطرأ بعض الأمور التي تستوجب إلغاء الشهادة قبل انقضاء مدة صلاحيتها، مثل تسريب المفتاح الخاص إلى جهة غير مخولة. وعادة ما يتم نشر لوائح بالشهادات المرفوضة بشكل دوري عبر ما يسمى Certificate Revocation List (CRL) ، وتوجد أيضاً تقنيات أخرى تسمح بالاستعلام عن حالة الشهادة مثل Online Certificate Status Protocol (OCSP).

بالتالي يمكن من خلال منح شهادات الوثوقية التي تربط بين المستخدم ومفتاحه العام إنشاء قنوات اتصال آمنة لضمان سلامة المعلومات وسريتها وعدم إنكار تبعية المعطيات لمرسل معين، من خلال تعمية المعطيات والتوقيع الرقمي.

المشكلة في مثل هذه الآلية أنها غير مناسبة لطبيعة شبكات MANET ، إذ إن هذه التقنية تتطلب وجود جهة مركزية مخولة تحقق بنية PKI ، وعادة ما يكون هناك عدة جهات ترتبط فيما بينها بشكل هرمي، أو تنسق مع بعضها البعض من خلال سياسات policies تحكم العلاقة فيما بينها .من جهة أخرى يتطلب تحقيق بنية PKI على شبكة MANET وجود عقد بقدرات حسابية عالية تتولى مهمة إصدار الشهادات وإدارتها.

لذا، لابد من إيجاد آلية مناسبة لإدارة شهادات الوثوقية بحيث يمكن تحقيق الخدمات الأمنية في شبكات MANET والتي تتلخص في: التحقق من الهوية، سلامة المعطيات، سرية المعلومات وعدم الإنكار.

وللوصول إلى هذه الآلية نحن أمام خيارين: إما أن يكون توزيع الشهادات عشوائياً تماماً، وهذا الخيار حتى الآن لايمكن تحقيقه عملياً. أما الخيار الثاني وهو الاتجاه الوحيد الموجود حالياً ألا وهو بنية PKI الموزعة. ولكن هذا الخيار يفرض قيوداً جديدة على العقد المشكلة للشبكة، من خلال تقييد حركيتها،

وزيادة الموارد لبعض العقد لتصبح هي المسؤولة عن إدارة الشبكة فقط دون أن يكون لها دور في العمليات الأخرى. وهذا يؤدي طبعاً إلى الحد من أداء شبكة MANET .

نسعى في بحثنا الآن إلى بناء نظام أمني جيد لشبكات MANET باستخدام PKI دون فرض قيود إضافية عليها، وبالتالي الوصول إلى حل أمني لشبكة MANET يماثل في أدائه الحلول الأمنية للشبكات التقليدية.

لذلك لابد من دراسة متطلبات الإدارة الفعالة للشهادات ودراسة المقترحات الموجودة لتنجيزها.

4.4. الحلول المقترحة لإدارة الشهادات

من المسائل الهامة التي يجب أخذها بالاعتبار في بناء أي نظام مبني على الشهادات الموثقة هي التوزيع الآمن للمفاتيح العامة على كل العقد في الشبكة.

بغياب وجود بنية تحتية ثابتة أو إدارة مركزية إلى جانب التغير الديناميكي لطبولوجية الشبكة، وحالات فشل اتصال متكررة، هذه العوامل تؤدي إلى ظهور قضايا أخرى مثل ضرورة إعادة المصادقة على الشهادات واتخاذ أزمنة وأوقات مناسبة للتواصل مع مخدم الشهادات.

وللتغلب على هذه القيود والوصول إلى كامل المزايا من آلية المصادقة المستندة إلى الشهادات، تم اقتراح عدة آليات لإدارة المفتاح العام [Capo3] [Kono1] .

متطلبات المصادقة الفعالة المبنية على الشهادات:

لبناء أي نظام مصادقة تم تعريف خمس متطلبات ليكون فعالاً و آمناً [Sado5] :

1. نظام مصادقة موزّع authentication :

نظراً للمسائل المتعلقة بفشل الاتصال، حركية العقد و منطقة التغطية المحدودة للعقد فإنه ليس عملياً أن نقوم بتضمين سلطة توثيق CA ثابتة مركزية في الشبكة، بل أكثر من ذلك في مثل هذه الشبكات التي تتطلب إجرائيات أمنية كبيرة فإن وجود مخدم مركزي يجعل النظام خاضعاً له وبالتالي سينهار النظام عند انهيار هذا المخدم. لذلك يعتبر توزيع عملية المصادقة على مجموعة من العقد في الشبكة من المتطلبات الأساسية في نظام مبني على الشهادات.

2. مراعاة الموارد المتاحة Resources Awareness:

طالما أن العقد في شبكات MANET محدودة الاستطاعة، وكذلك محدودة القدرة الحسابية وسعة التخزين، فإن البروتوكولات المستخدمة يجب أن تراعي هذا الأمر. هذا يعني أن تعقيد الخوارزميات من حيث الحجم وزمن التنفيذ يجب أن يكون مقبولاً.

3. آلية فعالة لإدارة الشهادات:

لأنه وكما ذكرنا سابقاً فإن الشبكات التقليدية تمتلك إدارة توزيع مفاتيح فعالة [int99]، لكن في شبكات MANET فإن إدارة الشهادات مازالت تعتبر تحدياً كبيراً، والجميع في سباق للوصول إلى حل مثالي لها.

4. الشهادة غير المتجانسة:

كما في حالة الشبكات السلكية فإن سلطات التوثيق يجب أن تكون غير متجانسة في شبكات MANET، وهذا يعني أن اثنتين او أكثر من العقد تنتميان إلى نطاقين مختلفين (غير متجانستين) يمكن أن تحاولا التوثق من بعضهما البعض.

في مثل هذه الحالات يجب أن يكون هناك نوع من الثقة أو علاقة هرمية بين العقد التي تشكل سلطات التوثيق. وفي الشبكات السلكية هذا الأمر منجز من خلال سلسلة الشهاداتcertificate chaining.

5. آلية متينة للتوثيق المسبق:

قبل إنشاء الشهادة الفعلية وتوزيعها يجب بناء الثقة بين العقد باستخدام التوثيق المسبق. رغم أن هذا ليس جزءاً من مصادقة الشهادة نفسها، لكنه يبقى أمراً مهماً في شبكات MANET لأن تحقيق المطلب الأول يستوجب أن يكون هناك نوع من الثقة المسبقة بين العقد. وبدونها لن تكون عملية التوثيق المتبادل اللاحقة وتبادل الشهادات ممكنة.

ونموذج Duckling by Stajano and Anderson [Sta99] كان من الأوائل الذين ضمنوا الثقة بين العقدة والعقدة الأم عن طريق قناة جانبية (infrared) . أما Balfanz et al [Bal02] فناقش طريقة أكثر فاعلية وفائدة.

4.5. بعض الحلول المقترحة لإدارة المفتاح العام في شبكات MANET

إن شهادة الوثوقية هي عبارة عن بنية معطيات توثق ارتباط مفتاح عام بمعلومات معينة متعلقة بمستخدم ما، وعادة ما تتضمن معلومات شخصية عن المستخدم موقعة بالمفتاح الخاص لمصدر الشهادة. المشكلة في حالة شبكات MANET هو إيجاد آلية لإصدار وإدارة الشهادات في ظل غياب خدمات مركزية واحتمال حدوث تقسيم في الشبكة ناتج عن تغير مناطق التغطية للعقد [Capo3] .

تتألف عملية التوثيق المبنية على الشهادات من ثلاثة أطوار:

الطور الأول هو طور الثقة bootstrapping ويتم خلاله توليد شهادات للعقد وتوثيقها بوساطة سلطة موثوقة CA. تعتمد هذه السلطة على المعلومات الخاصة بكل عقدة (الاسم، المنظمة، المفتاح العام،

عنوان IP) في توليد الشهادات، وتحوي الشهادة أيضاً زمن التوثيق وهو الزمن الذي تم فيه المصادقة على الشهادة، ومدة صلاحيتها.

الطور الثاني وفيه يتم تجديد الشهادات تبعاً لتاريخ انتهاء صلاحيتها، أو عند حدوث تغيير في طبولوجية الشبكة.

أما الطور الثالث فهو يتضمن إلغاء الشهادات من قبل سلطة التوثيق CA.

كانت البدايات [Zho99] تتركز على إيجاد خدمة موزعة لإدارة المفتاح العام distributed public-key management service، لأن استخدام CA وحيدة ضمن الشبكة له عدة إشكالات، لعل أبرزها عدم قدرة عقدة من الحصول على المفتاح العام لبقية العقد إذا تعذر عليها الوصول إلى CA. تملك الخدمة service زوج مفاتيح عام Kp وسري Ks وجميع عقد الشبكة على معرفة بالمفتاح العام Kp وتثق بأي شهادة موقعة بالمفتاح Ks . ترسل العقد طلب استعلام query request للحصول على المفتاح العام لعقدة ما، كما يمكن أن ترسل طلب تحديث update query لتغَير مفتاحها العام.

ثم انتقلت الأبحاث لزيادة الوثوقية باستخدام تقاسم السرية مع النظم الموزعة ذاتها.

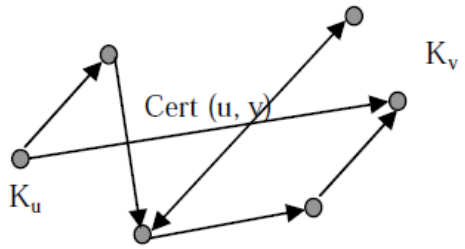
4.5.1. التنظيم الذاتي للمفتاح العام Self-Organized Public Key Management

اقترح هذه الطريقة Capkun, Buttyan and Hubaux [Capo3] والتي تقوم ببناء بيان graph للشهادات، والمبدأ الأساسي شبيه بشهادات PGP دون استخدام مخدم مركزي.

يعرف بيان الشهادة بالبيان المباشر G(V,E) حيث V,E هي مجموعة القمم والحواف vertices edges.

تمثل القمم المفاتيح العامة، والحواف تمثل الشهادات كما في الشكل -10-.

تمثل الوصلة u-v الشهادة الصادرة عن u والتي توثق امتلاك v للمفتاح العام K_v ، حيث تقوم u باستخدام المفتاح الخاص لتوقيع المفتاح العام لـ v. وبالتالي يمكن القول إن u تمثل CA لـ v. كما يحوي البيان G الشهادات غير منتهية الصلاحية للشبكة كلها.



الشكل (10) البيان المباشر للشهادة في شبكات ad-hoc

كل عقدة تحوي مستودعين للشهادات، الأول updated ويحوي الشهادات التي يتم تحديثها بشكل دوري، والآخر non-updated ويحوي الشهادات المنتهية الصلاحية. وقد ناقش capkun أن استخدام مستودعين للشهادات يعطي تقديراً جيداً للبيان و لعملية التحقق من الشهادات. عندما تريد العقدة u التحقق من المفتاح العام لعقدة أخرى v فإنها تحاول إيجاد مسار مباشر في البيان عن طريق خلط مستودعي الشهادات المحدّثة updated للعقدتين. وتستخدم سلسلة الشهادات على المسار بين العقدتين u,v للتحقق من v.

وإذا لم يتم اكتشاف أي مسار بين العقدتين عندئذٍ تسعى u عن طريق خلط مستودعي الشهادات المحدّثة وغير المحدّثة لإيجاد شهادات منتهية الصلاحية على المسار، وتقوم u بفحص صلاحيتها والتوثق منها.

يبدأ طور توليد الشهادات بأن تقوم كل عقدة بتوليد زوج المفاتيح الخاص بها. عندما تطلب عقدة جديدة شهادة من العقد المجاورة يقوم مصدر الشهادات بالتحقق من مصداقية المفتاح العام لها. ويفترض Capkun أن هذا محقق عن طريق تبادل مسبق للمفاتيح باستخدام قناة جانبية.

ومن أجل تحديث بيانات الشهادات الموجودة في المستودع المحدّث يبدأ طور تبادل الشهادات بعد تهشيرها hashing مع العقد المجاورة دورياً.

ومن أجل رفع كفاءة توليد الشهادات وتحديثها لمستودع الشهادات المحدّث اقترح Capkun et al خوارزميات مثل Maximum degree algorithm التي تقوم بإيجاد المسار في بيان الشهادات بأكبر عدد ممكن من الشهادات.لكنه لم يحدد أي إجرائية واضحة لتجديد الشهادات.

ولرفض الشهادات اقترح Capkun et al طريقتين: الأولى صريحة والأخرى ضمنية. في الطريقة الضمنية يتم رفض الشهادات اعتماداً على تاريخ صلاحيتها، أما في الطريقة الصريحة يصدر مصدّر الشهادة بيان إلغاء صريح يخص العقدة الهدف والتي يعتقد أن ارتباطها بالمفتاح العام لم يعد صالحاً. يُرسَل هذا البيان إلى العقد التي تطالب مصدّر الشهادة بتحديث الشهادة التي تخص العقدة الهدف.

تأتي فائدة هذه الآلية من أن عملية إدارة المفاتيح العامة تتم بشكل ذاتي التنظيم باستخدام الشهادات . أما مساوئها فتأتي من تكاليف الجداول و التي يتم الاحتفاظ بها من أجل مستودعات الشهادات، وفي كل مرة تتحرك فيها عقدة ما يجب عليها إعادة التفاوض مع بقية العقد و تحديث الجداول من جديد.

4.5.2. دعم أمن عام ومتين للشبكات المخصصة النقالة Providing Robust and Ubiquitous Security Support for MANET

اقترح [Kon01] Kong et al نظام شهادات موزع مبني على التعمية العتبية threshold cryptography وعلى وجود سر مشترك. إن الهدف الرئيسي من وجود السر المشترك في التعمية العتبية هو توزيع مفتاح سري k على مجتمع كبير من العقد باستخدام كثيرات الحدود. فعندما تكون درجة كثير الحدود k-1 هذا يعني أن أي مجموعة مكونة من k عقدة تستطيع الحصول على المفتاح السري، لكن أي مجموعة أقل من k لايمكنها اكتشاف هذ المفتاح [Zho99]. واستناداً إلى ذلك تتلقى العقدة مفتاحها العام من k عقدة مجاورة.

لتوليد الشهادات يجب أن تكون كل العقد في الشبكة موثقة بشهادات صادرة عن إدارة مركزية موثوقة. وعندما تريد عقدة جديدة الانضمام إلى الشبكة والحصول على شهادة، فإنها ترسل طلباً إلى k عقدة مجاورة من أجل الحصول على شهادات جزئية. إذا كانت العقد المجاورة تعتقد أن هذه العقدة جيدة تقوم بإصدار شهادات جزئية، ويتم تركيبها معاً في العقدة الجديدة لإصدار الشهادة الجديدة باستخدام توابع لاغرانج للاستيفاء.

ولتجديد الشهادات يتم تحديد زمن T_{renew}. وتقوم كل عقدة بإرسال شهادتها الصالحة مع زمن انتهاء صلاحيتها T إلى k عقدة مجاورة بحيث ($T < T_{renew}$ + Current Time) ، عندئذ تقوم العقد المجاورة بفحص لائحة رفض الشهادات لديها لتحديد إمكانية قبول الطلب أم لا.

أما رفض الشهادات فيتم بطريقتين: [Cap03] صريحة وضمنية. باستخدام الطريقة الضمنية، يتم رفض الشهادات إذا كان زمن انتهاء مدة الصلاحية أقل من تاريخ إصدار الشهادة مضافاً إليه T_{renew}. أما في الطريقة الصريحة، فكل عقدة تحتفظ بلائحة رفض للشهادات تحتوي على الشهادات التي لم تنتهِ مدة صلاحيتها بعد .تقوم كل عقدة بشكل دوري بتفقد هذه اللائحة و رفض الشهادات عند الضرورة.

تكمن الفائدة الرئيسية في هذه الطريقة في أنها لا تتطلب وجود سلطة مركزية موثوقة، ولكنها تفرض على كل عقدة وجود k عقدة مجاورة لإتمام عملية المصادقة. لكن عندما تكون k كبيرة تصبح هذه الطريقة غير فعالة بسبب حركية العقد. أيضاً لايمكن إصدار الشهادات للعقد التي تبعد أكثر من قفزة واحدة عن المصدّر. كما تتطلب هذه الطريقة وجود طور ثقة bootstrapping phase وذلك لتوزيع المفتاح الخاص على k عقدة أول مرة. وهذا يعني ضرورة إعادة تهيئة الشبكة عند الرغبة في ضم عقد جديدة غير معرفة مسبقاً، كما أن آلية إدارة طور الثقة غير معرفة .

اقتَرح [Sax05] آلية موزعة لإدارة شهادات الوثوقية تعتمد على تقاسم السرية باستخدام كثيرات الحدود الوحيدة المتغير uni-variate polynomial secret sharing، والتي تعتمد على تعمية العتبة،

بحيث تناسب شبكات ad-hoc القصيرة الأمد short-lived . من جهة أخرى قدم [Sax10] آلية شبيهة لإدارة الشهادات في الشبكات الطويلة الأمد long-lived تعتمد على تقاسم السرية باستخدام كثيرت الحدود الثنائية المتغير bi-variate polynomial secret sharing . ما يميز هذه الفكرة هو انخفاض الكلفة الحسابية وعدم الحاجة إلى التنسيق بين العقد لتوثيق عقدة جديدة .

4.5.3. التوثيق غير المتجانس الذاتي الإدارة Self-Managed Heterogeneous Certification

اقترح [Wan03] wang آلية مبتكرة يمكن أن يتواجد فيها سلطات موثوقة ذات نطاقات إدارية مختلفة غير متجانسة. واقترح أيضاً سلطة موزعة للشهادات باستخدام تقاسم السر اعتماداً على التعمية العتبية بشكل يماثل الطريقة المقترحة من قبل kong. للتعامل مع السلطات غير المتجانسة تم استخدام بيانات الثقة trust graphs. حيث نعتبر أن العقدة u تثق بـــ v بناء على الشهادة الرقمية للعقدة v الموقعة من قبل سلطة موثوقة تثق فيها u.

عندما تريد عقدة ما الحصول على شهادة يجب أن تجمع k جزءاً من السر المشترك من العقد المجاورة لها بقفزة واحدة لتبني المفتاح الخاص. وعندما ترغب u بالتحقق من العقدة v ترسل لها لائحة السلطات الموثوقة، وتقوم v بإرسال لائحة السلطات الموثوقة خاصتها. عندئذ تقوم u بمقارنة اللائحتين وفي حال وجود سلطات مشتركة ترسل لـ v شهادتها موثقة بهذه السلطات المشتركة، وكذلك تفعل v.

أما في حالة عدم وجود سلطات مشتركة تقوم كل عقدة بالبحث في نطاق قفزتين من خلال خوارزمية طلب توثيق موزع متعدد القفزات Distributed Multi-hop Certificate Request (DMCR).

وبالنسبة لتجديد الشهادات فهي مماثلة لخوارزمية DMCR. أما إلغاء الشهادات فلم تتم مناقشته.

تكمن الفائدة هنا أن هذه الطريقة تدعم عملية التوثيق غير المتجانس بين السلطات غير المتجانسة، وأنها تحدث على مستوى عدة قفزات.

4.5.4. الاستيقان المعتمد على الثقة والعنقدة Trust and Clustering-Based Authentication

تقوم هذه الطريقة كما عرفها [Nga04] Nagi على بناء نموذج للثقة ونموذج آخر للشبكة في سبيل دعم الأمن لشهادات المفتاح العام.

يُبنى نموذج الشبكة على تنظيم هرمي hierarchical أو عنقودي clustering للشبكة باستخدام خوارزميات العنقدة. حيث افترض أنه يتم تقسيم الشبكة إلى عناقيد لكل منها ID مميز.

أما نموذج الثقة فيبنى على نموذج web of trust المماثل لـ PGP [Bal02] ، والذي يمكن لأي مستخدم أن يلعب دور سلطة توثيق. وتعرف الثقة المباشرة direct trust بأنها علاقة ثقة بين عقدتين من عنقود واحد، أما الثقة بالتوصية recommendation trust فهي الثقة بين عقدتين من عنقودين مختلفين. بالتالي فإن إدارة المفتاح العام لم تعد مشكلة في العنقود الواحد، وبين عنقودين مختلفين يمكن للعقدة أن تتواصل مع عقد أخرى في العنقود الآخر.

أما فائدة هذه الطريقة فهي قدرتها على كشف وعزل نسبة كبيرة من العقد المتطفلة بالمقارنة مع طرق PGP. لكن سيئتها هي كمية الحسابات الكبيرة وحجم التخزين الكبير لقيم الثقة، بالإضافة إلى حركية العقد...

4.6. إدارة الوثوقية باستخدام تقاسم السرية Secret Sharing

تعتمد فكرة تقاسم السرية secret sharing على توزيع السر المشترك على مجموعة عبر كثير حدود من الدرجة (t – 1) [shm79] ، وكل عنصر في المجموعة يحوز على حصة من السر المشترك secret share. وتتطلب معرفة السر المشترك الحصول على t حصة على الأقل.

4.6.1. تقاسم السرية في الشبكات القصيرة الأمد

يستخدم كثير الحدود لتحصيص السر المشترك وتوزيع الحصص على أفراد المجموعة، وتلعب الحصص السرية دوراً أساسياً في تأمين قنوات الاتصال .تتلخص آلية [Sax05] في الخطوات التالية:

1. **التهيئة**: تتم من خلال مجموعة من العقد، أو من خلال عقدة وحيدة موثوقة trusted dealer (TD). يتم اختيار زوج مفاتيح سري/عام للمجموعة،و يتم تحصيص المفتاح السري وتوزيع الحصص secret share على العقد الأعضاء بطريقة آمنة.
2. **الإقرار بحق انضمام عقدة**: يجب أن تحصل العقدة M على حصة سرية secret share كي تتمكن من الانضمام إلى الشبكة. ترسل العقدة M طلباً JOIN_REQ إلى الشبكة .عندما تتلقى عقدة ما هذه الرسالة وتوافق على انضمام M إلى الشبكة فإنها ترسل إلى M عبر قناة آمنة حصة جزئية partial secret share مستخلصة من حصتها السرية .تقوم M بتشكيل حصتها السرية من الحصص الجزئية التي تلقتها من عقدة الشبكة شريطة أن تحصل على t حصة جزئية مختلفة على الأقل.

يمكن لعقدة معادية إفشال عملية الإقرار (DoS) من خلال إرسالها لحصة جزئية غير سليمة .لذلك يجب إيجاد آلية تمكن M من التحقق من سلامة حصتها السرية التي شكلتها من الحصص الجزئية قبل

استخدامها للتواصل مع الشبكة .وإذا أمكن تحديد الحصة الجزئية المعطوبة فإن هذا سيسهل إقصاء العقدة المعادية.

3. **تشكيل المفاتيح**: يمكن لأي عقدتين إنشاء مفتاح مشترك لتأمين قناة الاتصال بينهما من خلال حصصهما السريتين.

➢ تقاسم السرية باستخدام كثيرات حدود أحادية المتغير:

لتكن S سر المجموعة المشترك، يتم اختيار عدد أولي كبير q، وكثير حدود عشوائي f [Shm79] بحيث

$$f(x)=\sum_{i=0}^{t-1}a_i x^i \pmod q : f(0)=S$$

تقوم TD بحساب الحصة السرية لكل عقدة من خلال $ss_i = f(id_i) \bmod q$ وترسلها بشكل آمن إلى العقدة u_i .

وباستخدام استيفاء لاغرانج على القيم d_i, ss_i :

$$f(x)=\sum_{i=0}^{t-1}a_i x^i=\sum_{i=1}^{t}ss_i\,\lambda_i(x) \pmod q \;:\; \lambda_i(x)=\prod_{j=1,j\neq i}^{t}\frac{x-id_j}{id_i-id_j} \bmod q$$

من العلاقة السابقة نستنتج أن أي عقدة يمكنها استرجاع السر المشترك S باستخدام الحصص السرية ss_i، لأن $f(0)=S$.

ولإقرار انضمام عقدة جديدة v إلى الشبكة، ترسل u_i الحصة الجزئية pss_i:

$$pss_i = ss_i\,\lambda_i(id_v)$$

حيث

$$ss_v = f(id_v)=\sum_{i=0}^{t-1}a_i(id_v)^i=\sum_{i=1}^{t}ss_i\,\lambda_i(id_v)=\sum_{i=1}^{t}pss(v) \pmod q$$

وللتحقق من صلاحية الحصص السرية نختار عدداً أولياً p بحيث $p=m.q+1$ ، ونختار تابعاً مولداً $g\in \mathbf{Z}_p^*$ من الرتبة q. عندئذ تقوم TD بحساب القيم W_i – وتسمى الشاهد witness – بالشكل:

$$W_i = g^{a_i} \bmod p \;,\; i\in[0,t-1]$$

ومن ثم يتم نشر هذه القيم عبر شهادة وثوقية صادرة عن المجموعة.

ونلاحظ أنه:

$$g^{ss_i}=g^{\sum_{k=0}^{t-1}a_k(id_i)^k}=\prod_{k=0}^{t-1}g^{a_k(id_i)^k}=\prod_{k=0}^{t-1}W_k^{(id_i)^k} \bmod p$$

وبالتالي فإن أي حصة سرية لاتحقق العلاقة السابقة تعتبر غير صالحة.

إن حســـاب ثوابت لاغرانج يتطلب من كل عقدة معرفة id الخاص بكل عقدة مشـــاركة في عملية إقرار انضـــمام العقدة v إلى الشـــبكة، وهذا يتطلب التنســـيق بين t عقدة على الأقل، كما يتطلب وجود آلية للتحقق من امتلاك عقدة u_i لـ id_i كي لاتتمكن من سرقة الحصة السرية لعقدة أخرى.

ومن جهة أخرى تستطيع v معرفة الحصة السرية ss_i للعقدة u_i من خلال الحصة الجزئية pss_i حيث

$$ss_i = \frac{pss_j(v)}{\lambda_i(id_v)} = \frac{pss_j(v)}{\prod_{k=1,k\neq i}^{t} \frac{id_v - id_k}{id_i - id_k}}$$

ولمنع ذلك يجب تغيير الســـر المشـــترك بشـــكل دوري، إلا أن هذا الاقتراح يبدو صـــعب التحقيق عملياً. لذلك يمكن تحديث الحصـــص الســـرية بشـــكل دوري لمنع أي مهاجم من تجميع معلومات كافية عن الســـر المشترك كمايلي [Her95] :

1. تولد كل عقدة u_i مشاركة في عملية إقرار انضمام العقدة v مجموعة قيم عشوائية $\{r_{i,j}\} \in \mathbf{Z}_q^*,\ j \in \{1,\dots,t\}$ وتولد كثير الحدود العشوائي $\delta_i(z) = \sum_{j=1}^{t} r_{i,j} z^j$.
2. ترسل u_i وبشكل سري إلى كل عقدة u_j المقدار $u_{i,j} = \delta_i(id_j) \bmod q$.
3. تحســـب العقـــدة u_i حصـــتهـــا الســـريـــة خلال الـــدور τ من خلال العلاقـــة $ss_i^{(\tau)} = ss_i^{(\tau)} + \sum_{j=1}^{T} u_{j,i} \bmod q$.

وبالتالي يلزم لإقرار انضمام v مشاركة T عقدة حيث T>t.

المشكلة هنا تكمن في تبادل إرسال القيم $u_{i,j}$ بين العقد وهذا يتطلب قنوات اتصال آمنة، بالإضافة إلى أن أي عقدة معادية يمكنها شل هذه الطريقة من خلال إرسال قيم عشوائية غير متجانسة – غير مولدة بكثير الحدود العشوائي.

ولحل ذلك قام [Her95] باســـتخدام التوقيع الرقمي للتحقق من صـــحة القيم العشـــوائية المرســـلة، لكن ذلك يتطلب حصـــول كل عقدة على تأكيد بأن القيم المتبادلة بين كل العقد ســـليمة، وهذا يؤدي إلى زيادة التنسيق بين العقد، وبالتالي لايمكن تنفيذ هذا الاقتراح عملياً.

هذه الدراسة تؤدي إلى القول بأن طريقة تقاسم السرية باستخدام كثيرات الحدود الوحيدة المتغير لايمكن تطبيقها عملياً لأن:

- القيم id بحاجة إلى نشر بين كل العقد وهذا يعني التنسيق الكبير بين العقد.
- يجب وجود آلية لتوثيق امتلاك العقدة u لقيمة id وذلك لمنع سرقة الحصص السرية.
- آلية تحديث الحصـــص الســـرية دورياً وبشـــكل آمن معقدة جداً لأنها تتطلب التنســـيق الكامل بين العقد، وتستهلك الكثير من الموارد كونها تستخدم التوقيع الرقمي.

➢ تقاسم السرية باستخدام كثيرات الحدود ثنائية المتغيرات

ليكن S هو سر المجموعة المشترك، يتم اختيار عدد أولي كبير q، وكثير حدود عشوائي f بحيث

$$f(x,y)=\sum_{i=0}^{t-1}\sum_{j=0}^{t-1}a_{ij}x^i y^j \mod q : a_{ij}=a_{ji} , f(0,0)=S$$

من أجل كل عقدة u_i تقوم TD بحساب كثير حدود وحيد المتغير من الدرجة t-1 من خلال

$$f_{u_i}(x)=f(x,id_i) \mod q$$

وترسله بشكل آمن إلى u_i. ويمكن الاستغناء عن TD بعد تهيئة t عقدة. [Sax05]

وللتحقق من صلاحية كثير الحدود، يختار TD عدداً أولياً p بحيث $p=m.q+1$ وتابعاً مولداً $g\in \mathbf{Z}_p^*$ من الرتبة q، وينشر الثوابت $W_{i,j}$ عبر شهادة الوثوقية حيث $W_{i,j}=g^{a_{i,j}} \mod p$.

وإقرار انضمام عقدة v إلى الشبكة، تقوم u_i بإرسال $b_v(id_i)$ حيث :

$$b_v(id_i)=b_i(id_v)=f(id_v,id_i)$$

ثم تقوم v بحساب $f(id_v,x)$ باستخدام طريقة Standard Gaussian Elimination .

نلاحظ أن $b_v(x)=f(x,id_v)=f(id_v,x)$ ، وبالتالي يجب إيجاد مجموعة من الثوابت $\{A_i\}$ بحيث $b_v(x)=\sum_{i=0}^{t-1}A_i x^i$ ، وذلك عن طريق استيفاء القيم $\{b_i(id_v)\}$.

عندئذ تؤول المسألة إلى تعيين المصفوفة A بحيث $X.A=B$.

$$\begin{bmatrix} (id_1)^0 & (id_1)^1 & \cdots & (id_1)^{t-1} \\ (id_2)^0 & (id_2)^1 & \cdots & (id_2)^{t-1} \\ \vdots & \vdots & \vdots & \vdots \\ (id_t)^0 & (id_t)^1 & \cdots & (id_t)^{t-1} \end{bmatrix} \begin{bmatrix} A_0 \\ A_1 \\ \vdots \\ A_{t-1} \end{bmatrix} = \begin{bmatrix} b_v(id_1) \\ b_v(id_2) \\ \vdots \\ b_v(id_t) \end{bmatrix}$$

وبما أن المصفوفة X عكوسة، فإن جملة المعادلات السابقة تعطي حلاً وحيداً. ويجب أن تتحقق v من أن الثوابت A تحقق العلاقة $A_i=\sum_{j=0}^{t-1}a_{ij}(id_v)^j$:

$$g^{A_i}=g^{\sum_{j=0}^{t-1}a_{ij}(id_v)^j}=\prod_{j=0}^{t-1}\left(g^{a_{i,j}}\right)^{(id_v)^j}=\prod_{j=0}^{t-1}\left(W_{i,j}\right)^{(id_v)^j} \mod p$$

وعند عدم صلاحية إحدى القيم A_i يتم التحقق من $b_v(id_k)=b_k(id_v)$ لتحديد العقدة المسببة للخطأ واستبعادها.

ويمكن لأي عقدتين إنشاء مفتاح مشترك كالتالي:

$$k_{ij}=b_i(id_j)=f(id_j,id_i)=f(id_i,id_j)=b_j(id_i)=k_{ji} \mod q$$

تزيد هذه الآلية من العبء الحسابي، إلا أنها تقلل من التنسيق بين العقد مقارنة مع الآلية السابقة. ولكن تبقى مشكلتان، الأولى هي إيجاد آلية للتحقق من id لكل عقدة بحيث نمنع تسرب كثير الحدود إلى العقد المعادية، والأخرى هي تعميم الفكرة على الشبكات الطويلة الأمد.

4.6.2. تقاسم السرية في الشبكات الطويلة الأمد

تعتمد الفكرة [Sax10] على صعوبة اللوغاريتم المتقطع Discrete Logarithm في المنحنيات القطعية Elliptic Curves .

- التهيئة Bootstrapping : تتم عملية التهيئة في الشبكة بطريقة موزعة عبر استخدام مجموعة من العقد، أو من خلال عقدة مركزية trust dealer (TD). حيث يتم تحديد معاملات القطع (p, F_p, a, b, P, q)، ونختار $G_1 = G$ زمرة دوارة من الرتبة q مولدة بـ p نقطة. ثم نختار زمرة جزئية G_2 منتهية من $F^*_{p^2}$ من الرتبة q.

  تابع البصمة المعرف $H_1 : \{0,1\} \to G_1$ الذي يحول سلسلة ثنائية إلى نقاط من G_1. نختار H الذي يستخدم إحدى خوارزميات التوقيع المشهورة ... SHA, MD5 ومن ثم يتم نشر المعلومات.

  ليكن S السر المشترك للشبكة. تقوم TD بتوليد كثير حدود ثنائي المتغيرات ومتناظر بحيث:

$$f(x,y) = \sum_{i=0}^{t-1}\sum_{j=0}^{t-1} a_{ij} x^i y^j \mod q \ : a_{ij} = a_{ji}, f(0,0) = S$$

  ومن ثم تحسب قيم الشهود $W_{i,j} = a_{ij} P$.

  ولكل عقدة u_k تولد TD كثير حدود تشاركي $p_k(z) = f(z, id_k)$ ، ومفردة ارتباط T_k Membership token : $T_k = S.H_1(id_k, PK_k)$ بحيث PK_k المفتاح العام الذي تولده TD، والمفتاح السري هو SK_k . ثم يتم إرسال $p_k(x), T_k, SK_k$ بشكل آمن إلى العقدة u_k.

- الإدارة الذاتية للشهادات Self Certification: عندما تريد عقدة جديدة u_m الانضمام إلى الشبكة، لابد أن تحصل على t قيمة تشاركية و t مفردة ارتباط جزئية على الأقل وذلك عبر قنوات آمنة. لذلك ترسل العقدة u_m رسالة m موقعة بالمفتاح الخاص SK_m تتضمن طلب الانضمام join_req والمفتاح العام PK_m و id_m.

  كل عقدة u_k توافق على انضمام العقدة الجديدة تقوم بتوليد $x_k = p_k(id_m) = f(id_m, id_k)$، إضافة إلى القيمة الجزئية لمفردة الارتباط $T_m^k = p_k(0) H_1(m)$، وتكون الرسالة m' التي تتضمن الجواب join_rep و x_k, T_m^k, id_k ثم توقعها وترسلها.

  ثم تشكل العقدة u_m كثير الحدود التشاركي $p_m(z)$ باستخدام طريقة Standard Gaussian Elimination، فتؤول المسألة إلى جملة المعادلات:

$$\begin{bmatrix} (id_1)^0 & (id_1)^1 & \cdots & (id_1)^{t-1} \\ (id_2)^0 & (id_2)^1 & \cdots & (id_2)^{t-1} \\ \vdots & \vdots & \vdots & \vdots \\ (id_t)^0 & (id_t)^1 & \cdots & (id_t)^{t-1} \end{bmatrix} \begin{bmatrix} A_0 \\ A_1 \\ \vdots \\ A_{t-1} \end{bmatrix} = \begin{bmatrix} p_m(id_1) \\ p_m(id_2) \\ \vdots \\ p_m(id_t) \end{bmatrix}$$

نلاحظ أن $p_m(id_k) = f(id_k, id_m) = f(id_m, id_k) = p_k(id_m)$.

بعد تعيين الثوابت A_i يصبح لدينا $p_m(z) = \sum_{i=0}^{t-1} A_i x^i$ ، ويمكن للعقدة u_m أن تحصل على مفردة الارتباط الخاصة بها من خلال:

$$T_m = \sum_{j=1}^{t} T_m^j \lambda_j(0) \bmod q : \ \lambda_j(x) = \prod_{k=1, k\neq j}^{t} \frac{x - id_k}{id_j - id_k} \bmod q$$

وكذلك:

$$T_m = \sum_{j=1}^{t} \left(p_j(0)\, \lambda_j(0)\right) H_1(m) = \left(\sum_{j=1}^{t} p_j(0)\, \lambda_j(0)\right) H_1(m) \bmod q$$

وإذا عرفنا التابع $g(x) = f(0, x)$ فإنه وحسب استيفاء لاغرانج:

$$g(x) = \sum_{i=1}^{t} a_i \lambda_i(x) \ : \ a_i = g(x_i), \ \lambda_i(x) = \prod_{k=1, k\neq i}^{t} \frac{x - x_k}{x_i - x_k} \bmod q$$

نلاحظ أن : $p_j(0) = f(0, id_j) = g(id_j)$ ، إذن:

$$T_m = \left(\sum_{j=1}^{t} g(id_j)\, \lambda_j(0)\right) H_1(m) = \left(\sum_{j=1}^{t} a_j\, \lambda_j(0)\right) H_1(m) = g(0) H_1(m)$$

$$= f(0,0) H_1(m) = S.H_1(m)$$

- التحقق Verification: لابد للعقدة u_m من التحقق من صحة القيم التي استقبلتها، بالتالي:

$$p_m(x) = f(x, id_m) = \sum_{i=0}^{t-1} A_i x^i$$

$$= \sum_{i=0}^{t-1} \sum_{j=0}^{t-1} a_{ij}\, x^i (id_m)^j = \sum_{i=0}^{t-1} \left(\sum_{j=0}^{t-1} a_{ij} (id_m)^j\right) x^i$$

أي أن: $A_i = \sum_{j=0}^{t-1} a_{ij} (id_m)^j$

لكن: $W_{i,j} = a_{ij} P$ ، إذن:

$$\sum_{j=0}^{t-1} (id_m)^j W_{i,j} = \sum_{j=0}^{t-1} a_{ij} (id_m)^j P = \left(\sum_{j=0}^{t-1} a_{ij} (id_m)^j\right) P$$

ونستنتج أن الثوابت A_i تحقق العلاقة:

$$A_i P = \sum_{j=0}^{t-1} (id_m)^j W_{i,j}$$

كما يمكن التحقق من العقدة التي قدمت معلومات خاطئة وتعقبها من خلال التثبت من صحة العلاقة:

$$p_m(id_m)P = \sum_{i=0}^{t-1}\sum_{j=0}^{t-1} (id_m)^i (id_k)^j W_{i,j}$$

وذلك لأن:

$$\sum_{i=0}^{t-1}\sum_{j=0}^{t-1} (id_m)^i (id_k)^j W_{i,j} = \sum_{j=0}^{t-1}\left(\sum_{i=0}^{t-1} (id_m)^i W_{i,j}\right)(id_k)^j$$

$$= \sum_{j=0}^{t-1} (id_k)^j \left(\sum_{i=0}^{t-1} a_{ij} (id_m)^i\right) P$$

$$= \sum_{i=0}^{t-1}\sum_{j=0}^{t-1} a_{ij} (id_m)^i (id_k)^j P = \left(\sum_{i=0}^{t-1}\sum_{j=0}^{t-1} a_{ij} (id_m)^i (id_k)^j\right) P$$

$$= p_k(id_m)P$$

وللتحقق من صحة مفردة الارتباط يجب أن تتحقق العلاقة

$$e(P, T_m) = e(Q, H_1(m)) \quad : Q = S.P$$

وe هو التطبيق الخطي الثنائي المعرف $e: G_1 \times G_1 \to G_2$. ويمكن أيضاً تعقب العقدة التي أرسلت معلومات خاطئة من خلال معرفة المعطيات التي لاتحقق العلاقة:

$$e(P, T_m^i) = e\left(\sum_{j=0}^{t-1} (id_i)^j W_{0,j}, H_1(m)\right)$$

- تشكيل المفاتيح: يمكن لأي عقدتين إنشاء مفتاح تعمية مشترك $K_{m,n}$ لتأمين قناة الاتصال بينهما، حيث $K_{m,n} = f(id_m, id_n) = f(id_n, id_m) = K_{n,m}$.

- نلاحظ في هذه الآلية عدم الحاجة إلى أي تنسيق بين العقد لإقرار انضمام عقدة جديدة إلى الشبكة . ومن ناحية أخرى، تتمتع الآلية بسرية جيدة نتيجة صعوبة اللوغاريتم المتقطع في المنحيات القطعية، ولزيادة السرية نستخدم خوارزميتنا NTRU ، وذلك لتخفيف العبء الحسابي وزيادة الأمان، وبالتالي منع أي من الهجمات الكمومية الممكنة أيضاً لسرقة الشبكة. بالتالي حتى لو تمكن المهاجم من اختراق t-1 عقدة، فإنه لن يحصل على أية معلومة عن السر المشترك S .

  كما أن كثير الحدود التشاركي الذي تنشئه العقدة بعد انضمامها إلى الشبكة لا يعطي أية معلومات عن السر S، أو عن كثير الحدود التشاركي لأية عقدة أخرى، كما لا يسمح بمعرفة المفتاح التشاركي الذي تستخدمه عقدتان أخريتان لتأمين قناة الاتصال فيما بينهما.

- **من ناحية أخرى** يجب التفكير بآلية للتحقق من id_k، كي نمنع تسرب المعلومات إلى عقد مهاجمة تنتحل شخصيات مزورة، ولمنع امتلاك العقدة لعدة شخصيات، لأن هذا قد يساعد على تفكيك السر المشترك S . ولحل هذه الإشكالية يمكننا الاعتماد على خوارزمية NTRU في التوقيع الرقمي لضمان عدم تزوير id_k كما يجب تحديد آلية إنشاء القناة الآمنة في طور معالجة انضمام عقدة جديدة إلى الشبكة وهو محقق في اختيار بروتوكول التخاطب السري المقترح كما سنرى لاحقاً.

4.7. التحكم بالنفاذ Access Control

لا تعتبر مسألة التحقق من الهوية المشكلة الوحيدة في فضاء الشبكات اللاسلكية عموماً، وشبكات MANETخصوصاً، حيث إن معالجة التخويل Authorization والتحكم بالنفاذ Access Control للموارد من القضايا الحساسة والبالغة الأهمية، والحلول المقترحة لمعالجة هذه القضايا يجب أن تتناسب مع الطبيعة الخاصة لشبكات MANET.

تستخدم آليات التحكم بالنفاذ لضمان استخدام المعلومات من قبل المستخدمين المخولين وفق السياسة الأمنية ذات الصلة، وبالتالي فإن هذه الآليات تضمن سرية المعلومات confidentiality أو سلامة المعلومات integrity ، أو كليهما معاً [Cru05]. ولتحقيق ذلك أنشئت عدة نماذجmodels ، تربط بين الفاعل subject ، الذي يمثل أي كينونة تتعامل مع المعلومات(مثل المستخدم)، والغرض الذي يحوي المعلومات التي يرغب الفاعل بتطبيق فعل action عليها.

يعتبر النموذج Mandatory Access Control (MAC) من أقدم النماذج المطروحة للتحكم بالنفاذ، ويقوم بفرض السياسة الأمنية بشكل مستقل عن العملية التي ينفذها المستخدم وهذا ما كان يستخدم

غالباً في التطبيقات العسكرية. يعتبر النموذجان Bell-LaPadula و Biba من النماذج التي تستخدم مفهوم MAC (أي فرض السياسية الأمنية بمعزل عن عملية المستخدم).

يضمن Bell-LaPadula سرية المعلومات confidentaility ، إذا يقوم بتصنيف الفاعلين والأغراض باستخدام وسوم أمنية security labels مرتبة، ويطبق الخاصتين التاليتين لضمان سرية المعلومات [Cru05]:

الخاصة الأولى simple security property : لايمكن قراءة غرض ذي سمة أمنية أعلى.

الخاصة الثانية property : لا يمكن الكتابة على غرض ذي سمة أمنية أدنى.

أما Biba فيضمن سلامة المعلومات integrity ، إذ يتم تصنيف الفاعلين والأغراض بوسوم مرتبة من الأدنى إلى الأعلى. ويمكن للفاعل قراءة غرض ذي سمة أعلى، ولايمكنه الكتابة إلا على غرض ذي سمة أدنى (على عكس Bell-LaPadula).

على غرار MAC ، يعتبر النموذج Discretionary Access Control (DAC) من أقدم النماذج التي استخدمت في التطبيقات التجارية والأكاديمية، يستخدم لتمثيل النموذج مصفوفة ثلاثية الأبعاد، تمثل الأسطر الفاعلين على حين تمثل الأعمدة الأغراض، أما البعد الثالث فيمثل صلاحيات الفاعل على الغرض. ولكن معظم المستخدمين لا يملكون صلاحيات على معظم الأغراض مما يجعل المصفوفة مبعثرة، لذلك عادة ما تستخدم بنى معطيات أخرى لترشيد حجم التخزين، مثل اللوائح Lists [Cru05] كما هو الحال في Access Control List (ACL) .

غير أن أكثر النماذج مرونة هو Role-Based Access Control (RBAC) [Cru05]، إذ يبدو MAC و DAC كحالتين خاصتين من هذا النموذج، وبالتالي فهو يؤمن سلامة وسرية المعلومات. يتم منح الصلاحيات لأدوار roles وليس لأشخاص من قبل مدير النظام وفقاً للسياسة الأمنية.

بغض النظر عن النموذج المستخدم، ينبغي الأخذ بعين الاعتبار الطبيعة الخاصة لشبكات MANET عن بناء نظام لمعالجة التحكم بالنفاذ. بشكل عام، تم اقتراح مجموعة من الحلول، يعتمد بعضها على استخدام شهادات وثوقية Certificates للموارد وأخرى للمستخدمين، على حين قدم [Doo96] تصميماً وتنجيزاً لأغراض شبكية آمنة Secure Network Objects تؤمن مجموعة من الوظائف الأمنية في مجال التخويل والتحكم بالنفاذ، إذ اعتمد على المزاوجة بين لائحة التحكم بالنفاذ Access Control List (ACL) ومفهوم الإمكانات capabilities . توصف الإمكانية العمليات المسموح تنفيذها على غرض معين object . حيث يتم توصيف المعطيات ضمن الشبكة على شكل أغراض objects تتضمن مجموعة من الطرائق methods . يتم استدعاء الطرائق من قبل العقد الزبائن clients عن بعد remotely ، بحيث تتولى العقدة المالكة owner للغرض مهمة تنفيذ الطرائق

المستدعاة وإرسال النتائج إلى العقد الزبائن. يعرف المالك مجموعة من الإمكانات المتعلقة بغرض معين، ويمكن للزبون تنفيذ العمليات المصرح عنها في الإمكانات التي يمتلكها على هذا الغرض. بجميع الأحوال، يتطلب استخدام ACL وجود إدارة مركزية موثوقة من قبل جميع المستخدمين [Thm99] وتصبح الأمور أكثر تعقيدا في البيئة الموزعة، حيث تتعدد سياسات الاستخدام وتتعقد الآليات اللازمة لإجراء عمليات التحقق من هويات المستخدمين. لذلك كانت فكرة [Thm99] في استخدام شهادات التوثيق certificate لضبط عملية التحكم في النفاذ. تستخدم الشهادة لإثبات شخصية المستخدم وامتلاكه للمفتاح السري وتتضمن الواصفات attributes التي يملكها، أما المخدم(مالك المورد) فيصدر شهادة use-condition certificate يثبت فيها الشروط الواجب توافرها في المستخدم ليتمكن من النفاذ إلى المورد. وهذه الآلية تتطلب وجود CA للتحقق من صلاحية الشهادات المستخدمة.

ومع الانتشار الكبير للغة XML واستخدامها في نقل المعطيات عبر الانترنت، قدم [Hadoo] توصيفاً للغة XML Access Control Language (XACL) من أجل إتاحة الإمكانية لإضافة قواعد الاستخدام ضمن وثائق XML ، حيث يمكن كتابة سياسة الاستخدام ضمن وثيقة XML . يقوم المستخدم بإرسال طلب النفاذ إلى المخدم، يتضمن الطلب هوية المستخدم وعنوان المورد(الوثيقة) بالإضافة إلى العملية المراد تنفيذها على المورد. يتم معالجة الطلب من خلال مراجعة سياسة الاستخدام لهذه الوثيقة وإرجاع النتيجة حسب ما تسمح به سياسة الاستخدام.

ضمن نفس السياق، قدم [Damoo] نظاماً يسمح بالتحكم بالنفاذ إلى وثائق XML ، يتم تدوين عبارة التحكم بالنفاذ ضمن ملف خاص XML Access Sheet (XAS) ، يتم معالجة طلب الزبون من قبل المخدم الذي يعيد المعلومات المسموح بها بناء على هوية الزبون وعلى عبارات التحكم بالنفاذ المعرف ضمن ملف XAS الخاص بالوثيقة.

كما هو مبين أعلاه، فإن قرارات التحكم بالنفاذ تتم عبر مخدم موثوق يقرر السماح أو عدم السماح بالنفاذ إلى مورد معين. وعند السماح بالنفاذ إلى وثيقة معينة يتم تمرير هذه الوثيقة إلى الزبون الذي قد يخزن الوثيقة بطريقة غير آمنة على غرار المخدم الذي لا يأخذ بعين الاعتبار آليات لتخزين الموارد بطريقة آمنة. كما لايمكن فرض آليات التحكم بالنفاذ إلا بين الزبون والمخدم، حيث يمكن للزبائن تبادل الوثائق بين بعضهم البعض عند الحصول عليها [Moro5] .

قدم [Moro5] فكرة تقوم على تغليف الرسالة عبر تعميتها بمفتاح تعمية تناظري K ، ويرفق بالرسالة المفتاح التناظري بعد تعميته بالمفتاح العام للمستقبل PK (يمكن أن يكون هناك أكثر من مستقبل).

يمكن تعميم الفكرة بحيث يتم تضـمين أكثر من وثيقة مع أكثر من مسـتخدم. يتم تعمية كل وثيقة بمفتاح تناظري، وتعطى الصلاحية للمستخدمين بالوصول إلى المفتاح التناظري تبعاً لسياسة الاستخدام. يتضـمن C_i الرسـالة المعماة بمفتاح تناظري K_i بالإضـافة إلى توقيع الرسـالة، على حين يتضـمن R_j مجموعة مفاتيح التعمية التناظرية $\{ K_i \}$ المتاحة للمسـتقبل j معماة بمفتاحه العام .وبهذا يمكن توزيع الوثيقة على مجموعة من المسـتخدمين مع ضـمان حجب المسـتخدمين عن الأجزاء غير المخول لهم الوصول إليها.

من جهة أخرى، قدم [Moro5] توصيفاً لنظام اتخاذ قرار الثقة Trusted Decision Engine (TDE) لتطبيق سياسة استخدام معقدة لإدارة الموارد، تقوم الفكرة على دمج نظام TDE ضمن نظام تشغيل التجهيزة (من الممكن وضعه ضمن جهاز مستقل كالبطاقة الذكية smart card أو ضمن i-button). تملك كل أنظمة TDE (نظام ضـمن تجهيزة كل مسـتخدم) نفس زوج مفاتيح التعمية غير المتناظرة (مفتاح عام/سـري). تتلقى هذه الأنظمة الطلبات من المسـتخدمين (والتي تتضـمن معلومات اعتماد المستخدمين credentials المضمنة ضمن شهادة الوثوقية) وتعالجها بناء على سياسة استخدام معينة، وتعيد للمسـتخدم المفاتيح التناظرية المسـتخدمة في حماية أجزاء المعلومات المخول له بالوصـول إليها بما يتناسب مع الآلية التي سبق عرضها.

تمكن [Moro5] (عبر توزيع أنظمة TDE على المسـتخدمين) من إنشـاء نظام موزع لمعالجة التحكم بالنفاذ، المشكلة أن قوة النظام تعتمد على تنجيزه ضمن عتاد منفصل (smart card, i-button)، لأن تنجيزه على شـكل برمجيات تلحق بنظام التشـغيل يشـكل ضـعفاً من الناحية الأمنية، لوجود إمكانية لكسـر المفتاح السـري الخاص المشـترَك بين أنظمة TDE . ينبغي الإشـارة إلى أن كل الأفكار المطروحة تهدف إلى ضـبط العمليات التي يمكن للفاعل القيام بها على غرض معين، وهنا تبرز مشـكلة أخرى يتوجب إيجاد حلول لها تناسب شبكات MANET ، وهي تحديد الهوية identification .

4.8. التوثق وتعيين الهوية Authentication & Identification

إن تعيين الهوية مسألة غاية في الأهمية في شبكات MANET ، غير أن هذا المفهوم يرتبط بأمرين اثنين: تعيين هوية العقد (التجهيزات)، بحيث لا يمكن لعقدة أن تنتحل هوية ليسـت لها أو أن تزيف امتلاكها لعدة هويات لتظهر على أنها أكثر من عقدة Sybil attack ، وتعيين هوية المستخدمين.

نسـتخدم الاسـتيقان authentication للتحقق من أن ادعاء عقدة، مسـتخدم أو إجراء بامتلاكه لما يصـرح عنه صـحيحاً أم لا. ويفيد ذلك في إنشـاء علاقة ثقة بين الطرفين. تعتبر الآلية The

Resurrecting Duckling من بواكير الأفكار المطروحة في هذا الصدد، حيث تتم عملية الاستقيان عبر اتصال فيزيائي مباشر يتم خلاله تبادل مفتاح متناظر [Sta99] . غير أن هذه الآلية لا تناسب إلا عمليات الاتصال التي تتم عبر قفزة واحدة، كما يصعب استخدامها عند ازدياد حجم الشبكة.

من جهة ثانية، يمكن استخدام التعمية غير المتناظرة لإجراء عملية الاستقيان، والتي تتلخص في التثبت من صحة العلاقة بين المفتاح العام والهوية عن طريق طرف ثالث CA. وقد بينا سابقاً الإشكالات المتعددة في استخدام CA مركزية أو موزعة في شبكات MANET ، ولعل أهمها هي كيفية تحديد العقد التي ستلعب دور CA ، وما هي المعايير والآليات التي تضبط عملية إصدار الشهادات وتجديدها، وأيضاً الحاجة إلى طرف ثالث لتهيئة عقد CA عند إقلاع الشبكة.

من الأفكار المطروحة أيضاً في هذا الصدد، استخدام مفهوم Web of Trust، حيث لا يمكن لمستخدم Aالقيام بعملية توقيع لـ (B, kB) باستخدام مفتاحه الخاص k'_A إذا كان على يقين أن المفتاح العام k_Bيعود لـــ B ، وبهذا يتم ربط المفتاح العام لمستخدم بهويته اعتماداً على شهادة مستخدم آخر. فإذا كان المستخدم C يثق ب A فهذا سيمكنه من التحقق من هوية B ومفتاحه العام.

المشاكل الأساسية التي تواجه استخدام هذا المفهوم هي:

- كيفية تخزين وإدارة المفاتيح. في أحد الطرق المقترحة [Capo3] تقوم كل عقدة بتخزين جزء من المفاتيح، ومن ثم تستخدم خوارزميات (Shortcut Hunter or Maximum Degree) لتحديد واسترداد المفتاح المطلوب.
- كيفية إنشاء علاقة ثقة بين العقد في مرحلة إقلاع الشبكة.
- غموض الآليات الواجب استخدامها لاتخاذ القرار بمنح الثقة لمستخدم معين.

استخدم [Bobo3] مفهوم الهوية المعتمدة على التعمية Crypto-Based Identity (CBI) ومفهوم العنوان المعتمد على التعمية Crypto-Based Address (CBA) [Mono2] وذلك لتوليد الهوية (قد يكون عبارة عن id) أو العنوان ، إذ يتم تطبيق تابع البصمة hash على المفتاح العام للعقدة، ليصبح بمقدور بقية العقد التحقق من كون الهوية أو العنوان يتوافق مع المفتاح العام المصرح عنه. تحول هذه الآلية دون انتحال العقدة لهويات مزيفة ولا تتطلب وجود طرف ثالث، غير أنها لا تزود العقد بمعلومات ذات معنى تفيد في تعيين الهوية (أسماء، صلاحيات)... سوى ربط زوج مفاتيح تعمية غير متناظرة بعقدة عبر توليد عنوان مشتق من المفتاح العام. كما أنه من السهل على عقدة أن تولد عدة أزواج من المفاتيح لتنضم إلى الشبكة بأكثر من هوية.

يعتمد مفهوم Identity-Based Cryptography (IBC) على اشتقاق المفتاح العام لعقدة من التمثيل الثنائي لهويتها، ليتم بعد ذلك توليد المفتاح السري، وبذلك يمكن لبقية العقد التحقق من موافقة الهوية

للمفتاح العام، غير أن معرفة الهوية يودي إلى معرفة المفتاح السري بسهولة، لذلك يتم اللجوء إلى طرف ثالث Private Key Generation Service (PKGS) [Boneh03] لتوليد المفاتيح السرية، وهذا الأمر يشابه استخدام CA.

اقترح [Karo6] استخدام CA لتوليد زوج مفاتيح عام/سري يمنح لكل عقدة ترغب بالانضمام إلى الشبكة، وتقتصر مهمة CA على توليد زوج المفاتيح وتوقيعه لضمان سلامة استخدامه، أي أنها لا تجري أية عمليات تثبت من الهوية كما جرت عليه العادة. يستخدم المفتاح العام لتعيين هوية العقدة، على حين يطبق تابع البصمة على المفتاح العام لتوليد عنوان للعقدة (وفقاً لمفهوم CBA) يستخدم في عملية التسيير. تحتاج العقد لإثبات هويتها إلى إبراز قيمة V_i بالإضافة إلى شهادة الوثوقية، تعبر هذه القيمة عن استمرار صلاحية الشهادة خلال الشريحة الزمنية i من زمن صلاحية الشهادة، أي أن الشهادة لم يتم رفضها بعد وهي ما تزال صالحة للاستخدام. يتم الحصول على هذه القيمة من CA بشكل دوري. نلاحظ أن [Karo6] ما زال يعتمد على CA ، إلا أنه حاول التخفيف قدر المستطاع من تواصل العقد معها عبر استخدام تقنية [Elw96] لرفض الشهادات، إلا أن هذه التقنية تتطلب وجود اتصال بشبكة الانترنت لأن CA لاتعمل محلياً ضمن الشبكة، كما تتطلب نوعا من التزامن بين العقد لضبط الشرائح الزمنية. ما تزال إمكانية انتحال عدة شخصيات أمراً قائما لأن CA لا تقوم بأية إجراءات ذات صلة بتعيين الهوية.

إذن لازالت الصعوبة موجودة في إيجاد آلية عامة لتعيين هوية المستخدمين أو العقد، تضمن تحديد العقد بشكل وحيد وتحدد هوية المستخدم لمعرفة الصلاحيات المرتبطة به، إذ إن كل الآليات المقترحة تعاني من بعض السلبيات التي ينبغي أخذها بعين الاعتبار والتي غالباً ما تكون مرتبطة بسياق معين، كافتراض وجود CA مركزية أو مخدم مركزي لتوليد المفاتيح الخاصة أو نوع من التزامن بين العقد.

فالحل المقترح هو محاولة إيجاد آلية لتعيين هوية العقد دون الحاجة إلى طرف ثالث، أو على الأقل عند وجود الطرف الثالث يكون موثوقاً، ولا يستخدم إلا عند بداية إنشاء الشبكة أو دخول عقدة جديدة. وهو ما سنحاول بناءه اعتماداً على خوارزمية NTRU .

❖ مقارنة بين الآليات المقترحة:

يبين الجدول التالي -8- بعض الخواص لكل آلية اقترحت لإدارة المفتاح العام في شبكات MANET

الاستيقان المعتمد على الثقة والعنقدة	التوثيق غير المتجانس الذاتي الإدارة	دعم أمن عام ومتين لشبكات MANET	التنظيم الذاتي للمفتاح العام	
طريقة موزعة بشكل كامل، ومنظمة ذاتياً، كل عقدة تتصرف كسلطة موثوقة	طريقة موزعة بشكل كامل، وتتصرف بشكل جيد مع تغيير حجم الشبكة وازديادها	طريقة موزعة بشكل كامل، وتتصرف بشكل جيد مع تغيير حجم الشبكة وازديادها	طريقة موزعة بشكل كامل، كل عقدة تتصرف كسلطة موثوقة	Distributed Authentication استيقان موزع
الاحتفاظ بجداول الثقة و الأجزاء الخاصة بالمراقبة و الادارة تستهلك من القدرة التخزينية	كل عقدة تحتفظ فقط بلائحة بالسلطات الموثوقة.	توليد المفاتيح العامة وتوزيعها باستخدام كثيرات الحدود العقدية يعتبر مستهلكاً للزمن و للموارد بشكل كبير	كل عقدة تحتفظ بمستودعي شهادات الأمر الذي يفرض حملاً زائداً على الشبكة	Resource Awareness إعلام بالموارد
توليد الشهادات مبني على قيم الثقة. وجود introduce nodes قد لايكون موجوداً دائماً	يماثل آلية k-threshold	تتطلب على الأقل k عقدة مجاورة، بالتالي قد تخنق الشبكة bottleneck	الشهادات موقعة ذاتياً و بالتالي يعتبر النظام أكثر متانة من أنظمة تقاسم السر المشترك.	Creation الإنشاء
لم تناقش	مطبقة من خلال DMCR	تماثل إصدار الشهادات	لايوجد آلية صريحة	Renewal التجديد
لم تناقش	لم تناقش	يتم تخزين لائحة رفض الشهادات في كل عقدة	تسبب تأخيراً في العقد البعيدة عن بعضها	Revocation الرفض
غير مطبق	مطبق باستخدام بيانات الثقة	غير مطبق	غير مطبق	Heterogeneous Certification توثيق هجين

الجدول (8) مقارنة خواص الآليات المقترحة لإدارة المفتاح العام

الحل المقترح للتسيير في شبكات MANET

5.1. بروتوكول AODV

بروتوكول توجيه الموجهات عند الطلب في الشبكات العشوائية AODV [Aodoo] هو بروتوكول فعّال، يستخدم جدولاً للمسارات يتم فيه الاحتفاظ بمعلومات عن المسارات الحديثة التي استخدمتها العقدة مؤخراً، فهو بذلك يراعي حالة الطاقة المحدودة للعقد. يتلخص عمل البروتوكول في وظيفتين أساسيتين: وظيفة اكتشاف المسار بين المصدر والوجهة، ووظيفة صيانة المسار وتسليم الحزم المرسلة بشكل سليم وصحيح للوجهة.

- اكتشاف المسار: عندما تحتاج عقدة ما (المصدر) لمسار حديث لعقدة أخرى (الوجهة)، ولا يكون هذا المسار موجوداً في جدول التسيير الخاص بها (لم يستخدم سابقاً، أو انتهت فترة صلاحيته)، فإنها تقوم ببث رسالة Route Request(RREQ) إلى بقية العقد المجاورة لها في الشبكة. عندما تصل الرسالة إلى العقدة التالية تبحث في جدول التسيير الخاص بها، فإذا وجدت المسار أعادت إلى المصدر رسالة Route Reply(RREP) تتضمن المسار نحو الهدف، وإلا فإنها تقوم بإعادة بث الرسالة الاصلية إلى العقد المجاورة لها، وتسجل في جدول التسيير المسار الذي جاء منه الطلب وذلك للحفاظ على طريق الرجوع إلى العقدة المصدر. وهكذا حتى الوصول إلى العقدة الهدف. وعند الوصول إلى الهدف تقوم تلك العقدة بإرسال رسالة RREP إلى المصدر عبر العقد الوسيطة التي مررت الطلب.
- صيانة المسار: عندما تكتشف العقدة أن هناك مساراً لإحدى العقد المجاورة لم يعد صالحاً، فإنها تقوم بحذف ذلك المسار من جدول التسيير لديها، ومن ثم تبث إعلاناً بعدم صلاحية هذا المسار لكل العقد المجاورة. وكل عقدة تصلها الرسالة تعيد بثها إلى أن تصل الرسالة إلى المصدر الذي يستخدم ذلك المسار.

5.1.1. المشكلات الأمنية في بروتوكول AODV:

إن أهم متطلبات السرية في شبكات MANET مثلها كأي شبكات سلكية أو لاسلكية أخرى يمكن تلخيصها في المتطلبات الأساسية التالية [sha14]:

1. السرية confidentiality: طالما أن الوسط متاح للجميع في الشبكات اللاسلكية العشوائية فإنه يمكن لأي أحد أن يطلع على المعلومات المتبادلة ضمن الشبكة، لذلك يجب أن تبقى هذه المعلومات سرية، لايمكن لغير المصرح لهم بالاطلاع عليها.

2. التوثق أو الاستيقان authentication : وهو التحقق من هوية العقد المشاركة في الشبكة. أي أنه يجب التحقق في كل عملية إرسال واستقبال من هوية العقد المشاركة في العملية ضماناً لعدم دخول أي غريب إلى الشبكة وسرقة المعلومات أو مقاطعة أي عملية.
3. التكاملية integrity : وهو ضمان الرسالة من التعديل بشكل غير قانوني من قبل مستخدمين غير مخولين.
4. عدم الإنكار non repudiation : وهو التأكد من أن الرسالة المرسلة قد تم بالفعل إرسالها من قبل المصدر نفسه ولايستطيع إنكار ذلك، بالتالي يستطيع الهدف التأكد من مرسلها.

وهناك أيضاً متطلبات أخرى نتيجة الحركة العشوائية للعقد ضمن الشبكة. ويمكن أن نقسم الهجمات المحتملة في شبكات الـ MANETs إلى مجموعتين رئيسيتين [kum13]:

- الهجمات الفعالة active attacks: وهي الهجمات التي تحاول مقاطعة العمليات ضمن الشبكة من خلال قراءة وتغيير محتويات الرزم المتبادلة كتغيير معلومات التسيير وبالتالي تغيير المسار.
- الهجمات غير الفعالة passive attacks: وهي الهجمات التي تحاول سرقة المعلومات المتبادلة، كهجمات التنصت.

كما يمكن تصنيف الهجمات في بروتوكلات التوجيه عند الطلب في شبكات الـ MANETs إلى أربع مجموعات كالتالي:[Tom10]

1. **الهجوم باستخدام التعديل attacks using modification**:

يمكن للمهاجم أن يغير رسائل التسيير. ويتضمن هذا الهجوم:

- إعادة التوجيه عبر تغيير الرقم التسلسلي sequence number: كما نعلم فإن العقدة تختار المسار الأمثلي من خلال القياس المتري (الرقم التسلسلي، عدد القفزات hop count، التأخير الزمني)، وأصغر قيمة هي التي تعطي المسار الأمثل. لذلك يقوم المهاجم بتغيير قيمة sequence number إلى قيمة أصغر تمكنه من فرض المسار الأمثل على العقد الأخرى.
- إعادة التوجيه عبر تغيير عدد القفزات hop count: كما في الحالة السابقة، سيعمد المهاجم إلى تغيير قيمة الـ hop count لتغيير المسار الأمثل لباقي العقد.
- حجب الخدمة عبر تحويل مسار المصدر Denial of Service by altering source route: حجب الخدمة هدفه القضاء على خدمة التسيير routing من خلال تعديل وجهة الرسالة، أو مصدرها بحيث يتسبب بضغط كبير على الشبكة يؤدي إلى خروجها عن الخدمة.

- Tunneling: حيث تتفق عقدتان أو أكثر، وتتبادلان المعلومات فيما بينها عبر المســـار الطبيعي. وهذا يؤدي إلى سيطرة هذه العقد على المسار والتحكم به.

2. الهجوم باستخدام التلفيق attacks using fabrication:

- رسائل الخطأ المزورة: في الحالات الطبيعية تقوم العقدة بإرسال رسالة لصيانة المسار نتيجة خروج عقدة مجاورة. أما في هذا النوع من الهجوم يقوم المهاجم بإرسال هذه الرسائل لعزل إحدى العقد الموجودة أصلاً.
- تغيير جداول التسيير: يقوم المهاجم بتغيير معلومات التسيير في الرزم المتبادلة، مما يؤدي إلى تغيير جداول التسيير في العقد المجاورة.
- Routing table overflow إغراق جدول التســـيير: حيث يقوم المهاجم بخلق مســـارات غير موجودة، وذلك لزيادة الأعباء في جدول التســـيير، بالتالي لايمكنه تخزين المســـارات الجديدة الطبيعية.

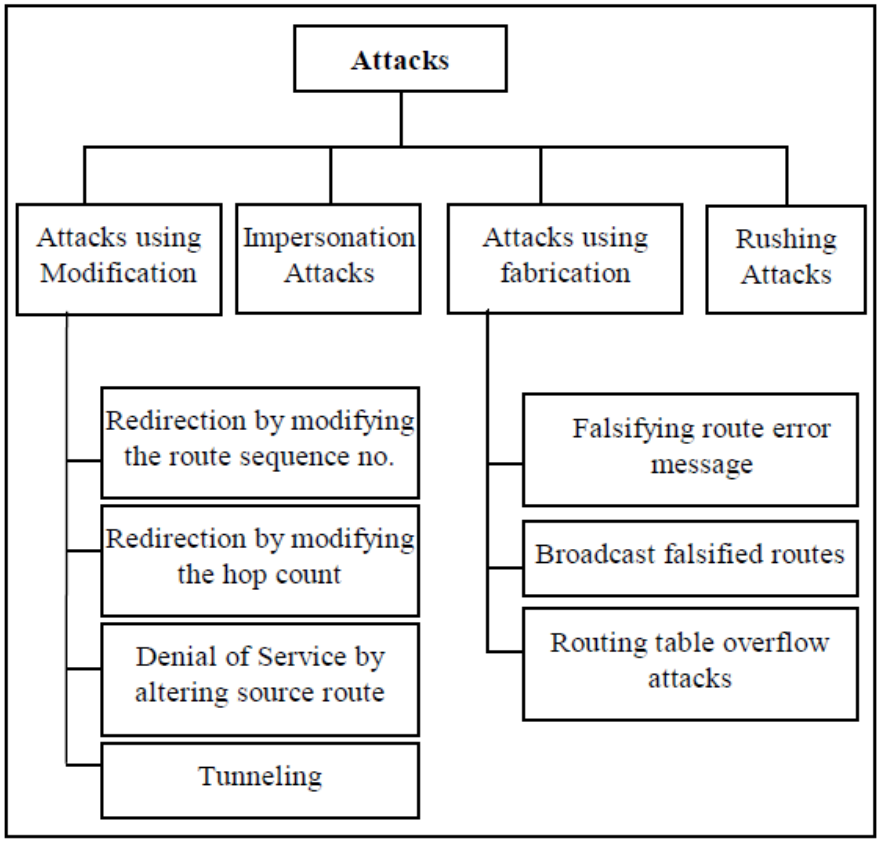
3. الهجوم باستخدام الانتحال attacks using impersonation:

وهي الهجمات التي تعرف أيضاً بالهجمات الخدّاعة spoofing attacks. وفيها يقوم المهاجم بتغيير عنوانه المنطقي IP أو الفيزيائي MAC، ووضع عنوان أي عقدة أخرى سليمة في الطرود المتبادلة، ويستطيع بذلك التحكم بطبولوجية الشبكة، وعزل عقد موجودة.

4. هجوم الاندفاع Rushing attacks :

يعتمد هذا الهجوم على خاصية بروتوكول AODV المتمثلة ببث رسائل RREQ لاكتشاف المسار، فتقوم العقدة المهاجمة ببث RREQ بشكل كبير مما يؤدي إلى دخولها في المسار المكتشف.

والشكل التالي -11- يلخص الهجمات المحتملة ضد بروتوكولات التوجيه عند الطلب.



الشكل (11) الهجمات الممكنة ضد بروتوكولات التوجيه عند الطلب

عملياً لايوجد حل عام لهذه التهديدات الأمنية، نتيجة اختلاف متطلبات السرية حسب التطبيق. لذلك اقُترحت العديد من الحلول التي تؤمن سرية بعض الأجزاء وسنناقش أهمها في الفقرة التالية [kle11]

5.1.2. بعض الحلول المطروحة لتأمين سرية بروتوكولات AODV

ندرس في الفقرات التالية أهم المقترحات التي ناقشت سرية بروتوكولات AODV، والآليات التي استخدمتها لتأمين هذه السرية.

- **Secure AODV (SAODV)**

اقترح هذا البروتوكول من قبل [zap02] Manel Gerrero Zapta and N.Askon. مهمته الرئيسية توفير السرية في بروتوكول AODV اعتماداً على التوثيق لمعظم حقول RREQ/RREP. توقع العقدة المرسلة رسائل التوجيه باستخدام مفتاحها الخاص، وتستخدم العقدة المستقبلة مفتاحها العام للتحقق من صحة التوقيع، لكنها لاتستطيع توقيع قيمة حقل عدد القفزات باعتبار أنه يزداد في كل قفزة [sha14][cer08] ، فيستخدم البروتوكول خوارزمية hash chain للتحقق من حقل عدد القفزات،

حيث تضيف كل عقدة توقيعها الخاص لسلسلة التوقيع h_i . وبالتالي فإن كل عقدة يجب عليها التحقق من توقيع كل العقد السابقة.

يعاني هذا البروتوكول SAODV من انخفاض الأداء نتيجة التعقيد الحسابي الكبير عند استخدام التعمية غير المتناظرة لأن كل عقدة يجب عليها توليد التوقيع أو التحقق منه، في كل مرة تصلها رسالة توجيه أو ترسل هي رسالة توجيه.

- **Security-Aware Ad hoc routing (SAR)**

هو محاولة لتنفيذ طريقة أكثر عمومية في توفير الأمان لبروتوكولات التوجيه من خلال إضافة مقياس سرية لبنية البروتوكول الأساسية [nal01].

يمكن لهذا البروتوكول منع بعض أنواع الهجوم كالـــ spoofing وهجوم الثقب الأسود، لكنه ضعيف أمام هجمات حجب الخدمة DoS ، وهجوم الثقوب [per03].

- **Secure Routing Protocol (SRP)**

تم تطوير هذا البروتوكول من قبل [pap02] papadimitratos، حيث يجب على كل عقدتين تريدان التواصل فيما بينهما أن يكون لهما مفتاح مشترك من أجل الاتصال والتوثق. وهذا يؤدي إلى ضمان دقة المعلومات الطبوغرافية للشبكة، ولذلك فإنه من السهل على العقدة المرسلة اكتشاف العقد المزيفة أو المتطفلة من خلال معلوماتها الطبوغرافية.

هذا البروتوكول يسمح بمقاومة هجوم الثقب الأسود، لكنه ضعيف أمام هجوم DoS، وهجوم العقد غير المرئية [mar03].

- **Ariadne**

اقترح هذا البروتوكول [Huy02] Hu et al لزيادة سرية التوجيه. للحصول على قائمة التوثيق الخاصة بالعقدة يستخدم هذا البروتوكول طريقة [per01] TESLA لنشر توثيق العقد المشاركة. كما يستخدم تقنية one way hash بواسطة message authentication code (MAC) الذي يستخدم مفتاح خاص مشترك للتوثق بين المرسل والمستقبل.

يعتبر هذا البروتوكول ضعيفاً أمام هجمات العقد غير المرئية [ram04] ، وهجوم الثقوب وهجوم حجب الخدمة.

• Authenticated Routing for Ad hoc Networks (ARAN)

تم اقتراح البروتوكول من قبل Dahill et al [dah02]، ويعتمد على التعمية بالمفتاح الخاص والعام في عمليات التحقق والتوثيق، ويوجد مخدم توثيق للشهادات يصدر شهادة توثيق لكل عقدة.

يتكون هذا البروتوكول من مرحلتين:

- تجهيز المسار: حيث تبث العقدة المرسل رسالة لاكتشاف المسار RREQ تحوي شهادتها الموثقة والموقعة بمفتاحها الخاص. ثم تقوم كل عقدة وسيطة بالتحقق من التوقيع السابق باستخدام الشهادة المرفقة، وتقوم بوضع شهادتها الموثقة والموقعة بمفتاحها الخاص وتعيد بث الرسالة بعد إزالة التوقيع السابق. وعند وصول الرسالة إلى العقدة الهدف تتحقق من توقيع العقدة المرسلة مع شهادتها الملحقة، وتقوم بإنشاء الرد RREP وتوقعه ثم ترسله مباشرة إلى العقدة المرسلة عبر المسار المكتشف، وأي عقدة وسيطة يصلها هذا الرد تقوم بنفس العمليات السابقة حيث تتحقق من التوقيع السابق، وتضيف توقيعها وشهادتها بعد حذف التوقيع السابق.
- اكتشاف أقصر مسار بين العقدة المرسلة والهدف: حيث يستخدم لهذه الغاية عدة خوارزميات لتحديد أقصر الطرق بين العقدتين.

يستخدم بروتوكول ARAN تقنية التوثق من قبل طرف ثالث بين عقدتين لتحقيق الأمان في شبكات Adhoc [meh10]، حيث نفترض وجود طرف ثالث لإعطاء الشهادات، موثوق دوماً هو Certificate Authority (CA) وهي العقدة المسؤولة عن توزيع الشهادات على العقد المشاركة في الشبكة. وبالتالي هي العقدة الرئيسية في الشبكة. فقبل البدء بأي عملية ضمن الشبكة تقوم هذه العقدة بتوزيع الشهادات الموثقة والموقعة على العقد المشاركة، ثم تبدأ عملية اكتشاف المسار بين العقد.

نقوم العقدة الأولى وتسمى initiator ببث رسالة طلب اكتشاف المسار RREQ، تتضمن عنوان العقدة المرسل وعنوان العقدة الهدف، وأيضاً الشهادة الموثقة والموقعة للعقدة المرسل. عند وصول الرسالة إلى العقدة التالية تقوم بالتحقق من التوقيع المرفق ثم تزيل الشهادة الأولى وتضع شهادتها الموثقة والموقعة، وتعيد بث الرسالة ... وهكذا حتى الوصول إلى العقدة الهدف. عند الوصول إلى الهدف تقوم العقدة بوضع شهادتها الموثقة والموقعة وترسل رسالة RREP حسب المسار المكتشف إلى العقدة المرسل.

نلاحظ أن بروتوكول ARAN يستخدم التوثق دائماً بين كل عقدتين وبالتالي فإن هجوم الانتحال impersonation يمكن تفاديه بسهولة، وهي إحدى الميزات الرئيسية لهذا البروتوكول، لكنه يستخدم التعمية غير المتناظرة مما يؤدي إلى انخفاض الأداء بشكل عام من حيث السرعة، كما أن هجوم DoS لايمكن مقاومته باستخدام ARAN.

- تبعاً لما سبق من مقترحات لزيادة أمان ووثوقية بروتوكولات التوجيه عند الطلب نلاحظ أن البروتوكولات التي تستخدم المفتاح العام في التعمية توفر خدمات أوسع في السرية، لكنها مكلفة حسابياً إذا ماتم تنفيذها في الشبكات اللاسلكية، وذلك لأنها تتطلب عبئاً حسابياً كبيراً عند المعالجة في العقد الوسيطة وبالتالي من الصعب تطبيقها عملياً في هذه الشبكات.

كما نلاحظ أن مقترحات Ariadne تتطلب آلية تزامن بين العقد وهي أيضاً مكلفة جداً وتجعل الشبكة أكثر عرضة للهجمات.

والملاحظة العامة لكل البروتوكولات التي تم اقتراحها من أجل توفير الأمان والسرية لبروتوكول AODV هي وجود سلطة توثيق مركزية لإدارة وتوزيع المفاتيح. تعتبر السلطة CA نقطة الضعف في هذه الشبكات لأنه لايوجد سرية لهذه السلطة وبالتالي معرضة بسهولة للاختراق، وبالتالي للحصول على مستوى سرية مقبول يجب التخفيف من شروط الشبكة اللاسلكية النقالة العشوائية.

لذلك كان التفكير بطريقة أخرى تساهم في زيادة الأمان للشبكة دون التخفيف من شروطها، فكانت النتيجة محاولة تطبيق خوارزمية NTRU لبروتوكول توجيه موثق ومعمى من أجل الحصول على بروتوكول توجيه يساهم في زيادة السرية والأمان لبروتوكول AODV مع المحافظة على عشوائية وحركية الشبكة اللاسلكية.

إن تطبيق خوارزمية NTRU يحسن من الأداء بشكل جيد لأنها قليلة التعقيد الحسابي وبالتالي لن تكلف الكثير كخوارزميات التعمية. وأيضاً والأهم من ذلك أن الحاجة إلى وجود سلطة مركزية موثقة ستختفي وبالتالي ستحل مشاكل الأمان المتعلقة بهذه الشبكات.

5.2. البروتوكول المقترح

نحتاج لطريقة تجعل بروتوكول AODV آمناً، والحل الأمثل هو وجود طرف ثالث Trusted Third Party (TTP) يقوم بالتوثيق بين كل عقدتين متصلتين. بشكل عام فإن وجود طرف ثالث سيعرض الشبكة لمزيد من الهجمات كهجوم man in the middle و brute force. لذلك الهدف الرئيسي من الطريقة المقترحة هو أن نلغي الحاجة لوجود ذلك الطرف الثالث باستخدام خوارزمية التعمية NTRU، ونعتمد فقط على العقد المتصلة للتوثق من أي عقدة أخرى تود الانضمام إلى الشبكة أو موجودة بالفعل ضمنها. وهذا يعني أن الشكل الهرمي المتبع في تقنيات المفتاح العام التقليدية لم يعد موجوداً، ولاداعي لوجود CA مركزية .

لحل مشـــكلة وجود الطرف الثالث الموثق قام Huei Lu [hue13] بتمديد النماذج المعرفة من قبل Shamir [sha84], Okamoto [oka89] وذلك لتطبيق التوثق الثنائي وتبادل المفاتيح في شـــبكات MANET. ســـنقوم بتعريف هذه الطريقة في بروتوكولات AODV لنتخلص من الحاجة إلى الســـلطة المركزية CA. وسنستخدم بروتوكول توجيه موثق كما في حالة بروتوكول ARAN .

يتألف البروتوكول المقترح من ثلاث مراحل أساسية هي:

- مرحلة التسجيل والتعريف.
- مرحلة بناء المسار واكتشافه.
- مرحلة صيانة المسار.

5.2.1. مرحلة التسجيل والتعريف:

نســتخدم لهذه الغاية عقدة خاصــة نســميها " مولد المفاتيح KG "، وهي العقدة التي تشــبه في عملها عقدة "dealer" في التعمية العتبية threshold cryptography. وهي أيضــاً التي تمثل الســلطة المركزية CA في الشـــبكة. نحتاج هذه العقدة في اقتراحنا فقط من أجل التحقق من العقد الموجودة في البداية، ولتوليد المفاتيح المطلوبة خلال هذه المرحلة، ثم يمكننا الاستغناء عن KG ووضعها خارج الشبكة.

خلال مرحلة التســجيل تقوم العقدة KG باختيار كثيري حدود بشــكل عشــوائي $f \in L_f$, $g \in L_g$ ثم تقوم بحساب المفتاح العام بالشكل:

$$K_{ca+} = f_q^{-1} \times g \pmod q$$

تستخدم العقدة A رقماً مميزاً يمثل الرقم التعريفي لها ID_A للتسجيل عند العقدة KG.

الآن تقوم KG بحساب المفتاح العام والخاص على التتالي للعقدة A بالشكل:

$$K_{A+} = f_{A,q}^{-1} \times g \pmod q$$

$$K_{A-} = \left(f_A, f_{A,q}^{-1}, f_{A,p}^{-1}, g\right)$$

ومن ثم تختار كثير حدود عشوائي $k_A \in L_k$ وتقوم بحساب القيم التالية (وهي القيم المميزة لكل عقدة):

$$X_A = k_A \times K_{ca+} \pmod q$$

$$HID_A = H\left(K_{A+} \| ID_A\right)$$

$$S_A = HID_A \times K_{A+} + k_A \pmod q$$

حيث يمثل التابع H تابع التهشير و || هي علاقة الضم بين المتحولات.

- عند ورود عقدة جديدة تريد الانضمام إلى الشبكة، نستخدم التعمية العتبية دون الحاجة إلى وجود العقدة KG. حيث تقوم مجموعة من العقد الموجودة بتجميع المفتاح وإعطائه للعقدة الجديدة بعد التحقق منها.

5.2.2. مرحلة بناء المسار واكتشافه:

قبل البدء بعملية اكتشاف وتحديد المسار يجب على العقد المشاركة في الشبكة أن تتحقق من بعضها البعض. لذلك تقوم العقدة A بطلب الشهادة الموثقة من العقدة KG، فترسل لها الشهادة المفصلة التالية:

$$CA \rightarrow A : cert_A = [IP_A, K_{A+}, t, e] K_{CA-}$$

والموقعة بالمفتاح الخاص للعقدة KG.

تحوي هذه الشهادة عنوان العقدة A وهو IP الخاص بها، والمفتاح العام لها، وقيمة زمنية تمثل تاريخ صدور الشهادة وتاريخ نهايتها.

بعد نهاية مرحلة التسجيل تكون كل العقد قد عرفت المفتاح العام للعقدة KG، والمفاتيح الخاصة بها، والقيم المميزة لها X_M, HID_M, S_M . عندئذ تكون مهمة KG قد انتهت، ولاداعي لوجودها بعد الآن في الشبكة.

- من أجل اكتشاف مسار ما، يجب على كل عقدة التحقق من العقد الأخرى المجاورة، ولتحقيق ذلك نحتاج إلى المرور بمرحلتين : حساب مفتاح الغلاف، وتحقيق التوثق المتبادل.

➢ **حساب مفتاح الغلاف (مفتاح جلسة التوثق):**

يجب على كل عقدة A تحقيق الاتصال بشكل سري مع العقدة المجاورة B، لذلك يجب عليهما توليد مفتاح مشترك. وقبل توليد هذا المفتاح يجب على العقدتين أن تتحققا من بعضهما، أي يجب على العقدتين A,B أن تتحققا من قيم المتحولات $(ID_A, H(X_A), S_A, K_{A+})$, $(ID_B, H(X_B), S_B, K_{B+})$ على التوالي.

ولضمان ذلك:

i. ترسل العقدة A مجموعة القيم $(ID_A, H(X_A), S_A, K_{A+})$ إلى العقدة B.

ii. ترسل العقدة B مجموعة القيم $(ID_B, H(X_B), S_B, K_{B+})$ إلى العقدة A.

iii. تقوم A بحساب:

$$\overline{HID_B} = H(K_{B+} \| ID_B)$$

$$\hat{X}_B = k_B \times K_{ca+} (\bmod q) = \left(S_B - \overline{HID_B} \times K_{B+}\right) \times K_{ca+} (\bmod q)$$

فإذا كانت $H(\hat{X}_B) = H(X_B)$ تكون A قد تحققت من B.

iv. تقوم B بحساب:

$$\overline{HID_A} = H\left(K_{A+} \| ID_A\right)$$

$$\hat{X}_A = k_A \times K_{ca+} \left(\bmod q\right) = \left(S_A - \overline{HID_A} \times K_{A+}\right) \times K_{ca+} \left(\bmod q\right)$$

فإذا كانت $H\left(\hat{X}_A\right) = H\left(X_A\right)$ تكون B قد تحققت من A.

وعندئذ يمكن لهاتين العقدتين توليد المفتاح المشترك للغلاف، وهو مفتاح جلسة التوثق

$$K_{AB} = f_A^{-1} \times K_{B+} \left(\bmod q\right) = f_B^{-1} \times K_{A+} \left(\bmod q\right)$$

➢ تحقيق التوثق المتبادل:

بعد أن تتشـــارك العقدتان A,B المفتاح K_{AB} نســـتخدم برتوتوكول challenge response لتحقيق التوثق كالتالي:

i. تولد العقدة A كثير حدود عشوائي $t_A \in L_k$ وتحسب:

$$T_A = t_A \times K_{ca+} \left(\bmod\ q\right)$$

$$V_A = K_{AB} + T_A \left(\bmod q\right)$$

ثم ترسل $\left(ID_A, V_A\right)$ إلى B.

ii. تولد العقدة B كثير حدود عشوائي $t_B \in L_k$ وتحسب:

$$T_B = t_B \times K_{ca+} \left(\bmod\ q\right)$$

$$V_B = K_{AB} + T_B \left(\bmod q\right)$$

$$\hat{T}_A = V_A - K_{AB}$$

وحيث أن العقدة B صحيحة فإنه يجب أن نحصل على $\hat{T}_A = T_A$.

للتحقق من ذلك تقوم B بحساب:

$$W_B = T_B \times \hat{T}_A \left(\bmod q\right)$$

$$I\left(B\right) = H\left(ID_A \| ID_B \| W_B\right)$$

$$Z_B = W_B + K_{AB}$$

$$I\left(A\right)^* = H\left(ID_A \| ID_B \| Z_B\right)$$

وترسل $\left(ID_B, V_B, I\left(B\right)\right)$ إلى A.

iii. بعد استقبال هذه المعلومات من قبل A، تقوم بحساب:

$$\hat{T}_B = V_B - K_{AB}$$

$$\hat{W}_B = \hat{T}_B \times T_A \left(\bmod q\right)$$

$$I\left(B\right)^* = H\left(ID_A \| ID_B \| \hat{W}_B\right)$$

فإذا كانت $I(B)^{*} = I(B)$ تكون A قد توثقت من B.

ومن ثم تقوم A بحساب :

$$Z_A = \widehat{W}_B + K_{AB}$$
$$I(A) = H(ID_A \| ID_B \| Z_A)$$

وترسل $I(A)$ إلى B.

iv. تقوم العقدة B بالتحقق من $I(A) = I(A)^{*}$ وتكون قد توثقت من A.

- والآن بعد تحقيق التوثق المتبادل تقوم العقدتان بحساب المفتاح المشترك من أجل تعمية المعلومات المتبادلة.

$$SK_A = H\left(ID_A \| ID_B \| T_A \| \widehat{T}_B \| \widehat{W}_B\right)$$
$$SK_B = H\left(ID_A \| ID_B \| \widehat{T}_A \| T_B \| W_B\right)$$

➢ اكتشاف المسار :

بعد التأكد من كل العقد الموجودة في الشبكة، تبدأ العقدة مرحلة اكتشاف المسار من خلال بث رسالة RDP (Route Discovery Packet) إلى العقد المجاورة.

$$A \rightarrow brdcst\left[RDP, IP_X, N_A\right]K_{A-}, Cert_A$$

تتكون هذه الرسالة من:

- الترويسة RDP.
- عنوان العقدة الهدف X وهو الـ IP الخاص بها.
- الشهادة الخاصة بالعقدة A.
- عدد خاص N_A ويسمى nonce، وهو للتعريف بكل رسالة طلب اكتشاف من قبل العقدة A. ويزداد في كل مرة تقوم A ببث رسالة طلب اكتشاف مسار جديد RDP.

تجمع هذه المعلومات وتُوَقع باستخدام المفتاح الخاص للعقدة A.

تقوم كل عقدة بالتحقق من التوقيع والشهادة، وتعدل جدول التسيير الخاص بها اعتماداً على رسالة RDP، ثم تعيد بث الرسالة بعد أن تحذف الشهادة والتوقيع للعقدة الوسيطة السابقة، وتضيف شهادتها ثم توقع الرسالة بمفتاحها الخاص. ولكن تبقى شهادة وتوقيع العقدة الأساسية المرسلة.

لتكن B العقدة المجاورة لـــ A، عندئذ بعد استقبال رسالة البث RDP من A ، تتحقق منها وتضيف شهادتها ثم توقع بمفتاحها الخاص، وتعيد بثها إلى جيرانها.

$$B \rightarrow brdcst : \left[\left[RDP, IP_X, N_A\right]K_{A-}\right]K_{B-}, Cert_A, Cert_B$$

تصـــل الرســـالة إلى العقدة المجاورة C، فتتحقق من العقدة المرســـلة A، والعقدة المجاورة B، ثم تزيل توقيع وشهادة B، وتضيف شهادتها، ثم توقع كل الرسالة بمفتاحها الخاص، وتعيد بث الرسالة.

$$C \rightarrow brdcst : \left[\left[RDP, IP_X, N_A\right]K_{A-}\right]K_{C-}, Cert_A, Cert_C$$

وهكذا حتى تصل الرسالة إلى العقدة الهدف X.

بعد ذلك تقوم العقدة X بإرســـال رســـالة جواب REP (route request reply) إلى العقدة المرســـلة A مباشـرة عبر المسـار الذي تم تخزينه، وتحوي هذه الرسـالة العدد الخاص nonce المرسـل من قبل A. ولتكن D هي آخر عقدة في المسار المكتشف قبل الهدف X.

$$X \rightarrow D : \left[REP, IP_A, N_A\right]K_{X-}, Cert_X$$

تحوي رسـالة الجواب المعرف REP، وعنوان العقدة المرسـلة A، والعدد الخاص N_A المميز لرسـالة الطلب، وترسل موقعة بالمفتاح الخاص.

بعدها تصل الرسالة إلى العقدة التالية في المسار وهي C مثلاً (السابقة في ترتيب اكتشاف المسار). فتقوم C بنفس العمليات في الاتجاه المباشر (اكتشاف المسار)، حتى تصل الرسالة إلى العقدة المرسلة A.

$$D \rightarrow C : \left[\left[REP, IP_A, N_A\right]K_{X-}\right]K_{D-}, Cert_X, Cert_D$$

$$C \rightarrow B : \left[\left[REP, IP_A, N_A\right]K_{X-}\right]K_{C-}, Cert_X, Cert_C$$

كل عقدة تقوم بالتحقق من العدد N_A، وتوقيع العقدة الســـابقة، وشـــهادتها. ثم تزيل الشـــهادة والتوقيع للعقدة السابقة وتضيف شهادتها وتوقيعها بمفتاحها الخاص.

وعند وصول الجواب إلى A تقوم بالتحقق من توقيع العقدة X وشهادتها، والعدد المميز N_A. ويصبح المسار جاهزاً للاستخدام بين العقدتين A و X.

5.2.3. مرحلة صيانة المسار:

عندما لايســـتخدم مســـار ما في جدول التســـيير الخاص بعقدة من العقد، يصـــبح غير فعال ويخرج من الخدمة. لذلك عند ورود معلومات عبر هذا المسـار تقوم العقدة بتوليد رسـالة خطأ ERR، تحوي عنوان العقدة المرسل وعنوان العقدة الهدف. وتقوم بإرسالها إلى العقدة التالية.

$$B \rightarrow C : \left[ERR, IP_A, IP_X, N_B\right]K_{B-}, Cert_B$$

ويمكن أن تولد العقدة رسالة خطأ عند استخدام مسار فعال، وذلك عند حركة إحدى العقد وتغيير هذا المسار.

تقوم العقدة B بتوليد رســـالة الخطأ التي تحوي عنوان المرســـل A، وعنوان الهدف X، والرقم المميز N_A لضـمان أن الرسـالة لن تبقى في الشـبكة دائماً. ثم تضـيف شـهادتها وتوقع بمفتاحها الخاص، وترسـلها إلى

العقدة المجاورة C التي تقوم بإعادة إرسال الرسالة عبر المسار نفسه دون تعديل فيها، حتى تعمم على كل عقد المسار، فتقوم عندئذ بحذفه من جداول التسيير والبحث عن غيره.

من الواضح أنه من الصعب تحديد فيما إذا كانت رسالة الخطأ صحيحة أو خاطئة تهدف إلى تغيير في جداول التسيير، لذلك فإن إضافة التوقيع الخاص للعقدة يضمن عدم انتحال الشخصية. وبالنظر إلى العدد المميز N_A يمكن التأكد من عدم تكرار الرسالة دائماً.

وبشكل عام فإن العقدة التي تقوم بإرسال عدد كبير من رسائل الخطأ يفضل دائماً تجنبها حتى وإن كانت الرسائل صحيحة لضمان استمرارية الأداء والسرعة في الشبكة.

5.3. دراسة أداء البروتوكول المقترح

سنقوم بدراسة أداء البروتوكول المقترح من خلال دراسة سريته وأمانه، كوننا درسنا في الفصل السابق الأداء من خلال السرعة والتعقيد باستخدام خوارزمية NTRU، ومن ثم ننتقل في الفصل التالي لدراسة أدائه عملياً باستخدام أداة المحاكاة AVISPA.

ولدراسة سرية البروتوكول ندرس أداءه ضد بعض أنواع الهجمات:

- Brute force attack

عندما يحاول المهاجم معرفة المفتاح الخاص للعقدة KG عند العقدة A، فإنه يجب أن يحدد كل كثيرات الحدود f, f_A حيث $f_A \times K_{A+} = g \pmod q$ and $f \times K_{ca+} = g \pmod q$. وأيضاً عليه أن يحدد كل القيم الممكنة لكثير الحدود g، وبالتالي يصبح تعقيد هذا الهجوم $\frac{1}{d_g!}\sqrt{\frac{N!}{(N-2d_g)!}}$ حيث d_g عدد المعاملات غير الصفرية في g، و N درجة الخوارزمية. وكما نلاحظ فإن قيمة هذا التعقيد كبيرة جداً [Hof98].

- Common session key attack

للحصول على المفتاح المشترك K_{AB} يجب أن يحدد المهاجم كل القيم الممكنة لـ :

f_A and f_B

$f_A \times K_{A+} = g \pmod q, f_B \times K_{B+} = g \pmod q$

ومن الواضح أن التعقيد أيضاً كبير جداً $\frac{1}{d_g!}\sqrt{\frac{N!}{(N-2d_g)!}}$ ، والهجوم فاشل أيضاً.

- Man in the middle attack

يجب على المهاجم تحديد القيم (ID_A, X_A, S_A, K_{A+}) للحصـــول على هوية عقدة A مشـــاركة في الشبكة، لكن لايمكنه ذلك لأنه في مرحلة التوثق تكون ID_A محمية بتابع تهشير وبالتالي لايمكن للمهاجم حساب $\widehat{X}_A = X_A$ بشكل صحيح. أيضاً لايمكنه حساب المفتاح K_A لأنه في خوارزمية NTRU لتحديد التشكيلة L_f, L_g, L_k نحتاج إلى 2^{160} عملية حتى في متطلبات السرية الضعيفة.

فمثلاً كما رأينا في الفصل السابق $(N, p, q) = (167, 3, 128) \rightarrow key\ security \approx 2^{80}$

- Attack using modification

جميع حقول RDP و REP تبقى ثابتة دون تغيير بين المرســل والمســتقبل في هذا البروتوكول، وكلها توقع من المرسل، لذلك أي تغيير فيها سيتم اكتشافه مباشرة، وستهمل الرسالة المعدلة. لذلك هجوم التعديل فاشـــل أيضـــاً، وكذلك هجوم التعديل على عدد القفزات لأن عدد القفزات لايهمنا أصـــلاً في هذا البروتوكول، ولايرسل في أي رسالة.

- Attack using impersonation

طالما أن الرســائل المرســلة من قبل المرســل موقعة بالمفتاح الخاص مع الشــهادة الموثقة، وكذلك الرســائل المرسلة من قبل المستقبل موقعة بمفتاحه الخاص مع شهادته الموثقة، فإنه لايمكن أن يتم انتحال شخصية أي منهما حتى لو تجسس المهاجم عليهما.

- Attack using fabrication

إن شــهادة المرســل الموثقة، وتوقيعه باســتخدام المفتاح الخاص في خوارزمية NTRU تمنع عدم الإنكار، وأيضاً التنصت، والدخول غير المصرح به في أي مرحلة من مراحل التوجيه.

والعقدة التي تقوم بتكرار الرسائل الخاطئة تستبعد من الشبكة لذلك فإن هذه الهجمات فاشلة أيضاً.

نســتنتج أن التقنية المقترحة أكثر فاعلية من التقنيات التقليدية المســتخدمة في تأمين ســرية بروتوكولات التوجيه عند الطلب في الشبكات اللاسلكية، كون التعقيد المستخدم بسيط نتيجة استخدام NTRU والتي تستخدم فقط عمليات الجمع والضرب. وأيضاً أكثر أماناً كون المهاجم لن يستطيع تحمل الوقت المصـــروف لاختراق أي معلومة في كثيرات الحدود الحلقية. والنقطة الأهم في هذا البروتوكول هو عدم

حاجته إلى طرف ثالث لتوثيق أي عقدة في الشـــبكة، أو توزيع المفاتيح، وبالتالي نســـتطيع الوصـــول إلى مســتويات عالية من الســرية مع المحافظة على بنية الشـبكات اللاسـلكية العشـوائية وهي العقبة الأهم في تطوير وانتشار هذا النوع من الشبكات.

النتائج العملية و

AVISPA

6.1. الأداة AVISPA

في العقد الماضي بدأ الحديث عن تقنيات جديدة لدراسة وقياس مقدار سرية البروتوكولات المستخدمة. وقد اقترح العديد منها [Arm02][Bla01][Bod05][Bor02]. ولما كانت البروتوكولات متنوعة جداً ومتعددة، كان لكل نوع منها أداة لدراسة سريتها وتحليلها ، ولكن الأداة AVISPA هي التي غطت جميع التقنيات السابقة، باعتبارها تصلح لدراسة وتحليل جميع أنواع البروتوكولات.

مشروع AVISPA وهو اختصار لـــ " Automated Validation of Internet Security Protocols and Applications" [Avi04] تم تطويره من قبل أربعة فرق هي:

- The research team led by A. Armando at the University of Genova, Italy.
- The team led by M. Rusinowitch at INRIA-Lorraine, Nancy, France.
- The team led by D. Basin at the ETH Zurich, Switzerland.
- The team led by J. Cuellar at SIEMENS AG, Munich, Germany.

وهي التقنية المستخدمة في تحليل ودراسة سرية البروتوكولات المختلفة من خلال:

- توفير لغة رسمية موحدة لتحديد مستويات أمن البروتوكولات وخصائصها. وهي لغة HLPSL "High Level Protocol Specification Language".
- دمج مختلف تقنيات التحليل من أجل بناء هجمات مفترضة على البروتوكول وتحديد أدائه، واكتشاف الثغرات المحتملة خلال عدد كبير من مرات التنفيذ.

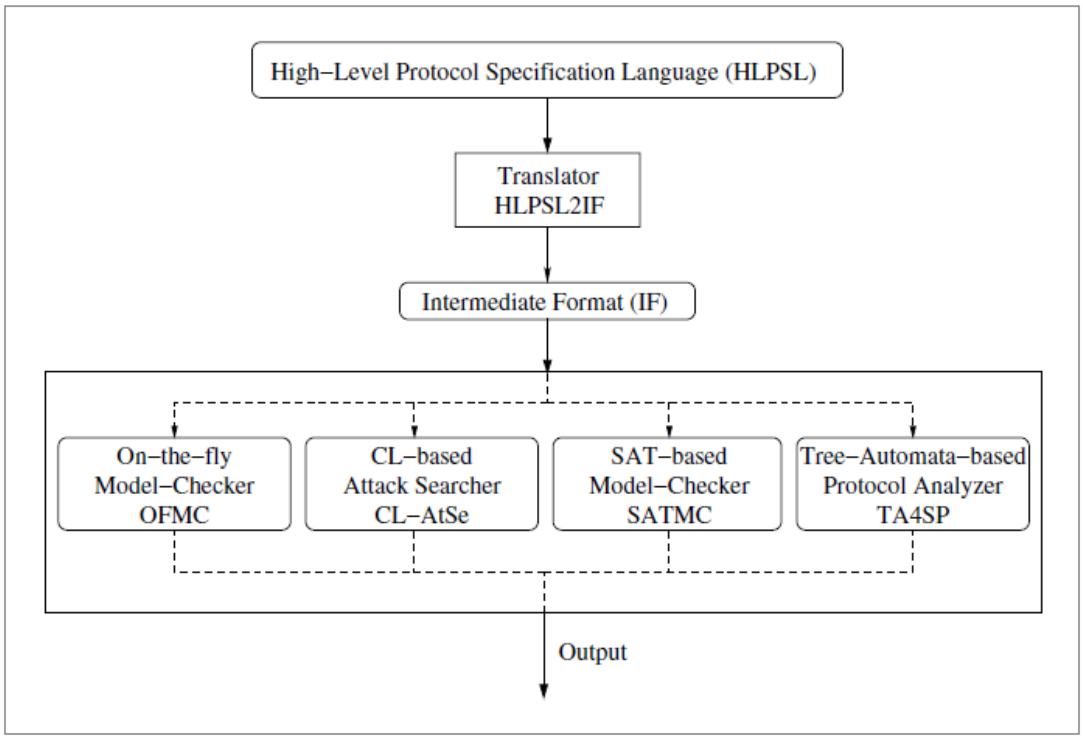
يوضح الشكل التالي -12- بنية الأداة AVISPA حيث تتحدد لغة التخاطب بين المستخدم والأداة باستخدام لغة HLPSL. تعرف لغة HLPSL على أنها لغة تعبيرية رسمية تحدد المواصفات العامة للبروتوكول من قيم التدفق، بنية المعلومات، نوع وطريقة التعمية المتبعة، المواصفات الجبرية، وكذلك مواصفات السرية.

بعد كتابة البروتوكول والمواصفات المطلوبة بلغة HLPSL تقوم AVISPA بتحويل هذا الرماز إلى شكل آخرمن المعلومات—وسيط- هو "Intermediate Format" IF عبر المترجم "HLPSL2IF". في لغة IF يتوصف نظام الحالة للبروتوكول، وتتحدد طرق الانتقال بين الحالات، وبالتالي يتوصف البروتوكول بشكل كامل. وتتوصف حالات الهجوم المحتملة ضد البروتوكول أو بعض مواصفاته.

خرج المترجم هو دخل لإحدى التطبيقات في AVISPA. توجد حالياً أربعة أنواع من التطبيقات هي:

- On-the-Fly-Model-Checker OFMC
- Constraint-Logic-based Attack Searcher CL-AtSe
- SAT-based Model Checker SATMC

- Tree automata for analysis Security Protocol TA4SP protocol analyzer



الشكل (12) بنية الأداة AVISPA

1. OFMC: [Bas04] يقوم هذا التطبيق بتنفيذ نسخة عن البروتوكول، وذلك عبر نظام التحويل الذي ولده المترجم، وتنفيذ عدد من التقنيات في سبيل تحقيقه. يدعم هذا التطبيق الأنواع المعروفة من المتحولات الجبرية، وخوارزميات التعمية، كما يمكنه تعرف المتحولات الجديدة التي تم بناؤها بلغة HLPSL.
2. CL-AtSe: [Che02] يقوم بتطبيق الشروط الموصفة في البروتوكول، مع بعض تقنيات التبسيط والتكرار، وقد بني هذا التطبيق بشكل يسمح بتطويره في حال ظهور أنماط وأنواع جديدة من خوارزميات التعمية.
3. SATMC: [Arm04] يقوم هذا التطبيق ببناء النموذج المقترح في نظام الحالة في IF، مع إضافة الخواص الأمنية المطلوبة في كل حالة. وتمرير هذا النموذج إلى SAT solver حيث يعتبر التطبيق أن أي نموذج لايفهمه هو بمثابة هجوم.
4. TA4SP: [Boi04] يقوم بتقدير معرفة المتطفل intruder في الشبكة، ومن ثم –وحسب مواصفات السرية المطلوبة– يتم تقدير فيما إذا كان البروتوكول آمناً بالنسبة لتلك المعلومات أم

لا.يستخدم التطبيق لهذا الغرض نموذج Dolev-Yao [Dol83] والذي يضمن للمتطفل تحكماً كاملاً بالشبكة.

إذن نحصل في النهاية بعد تنفيذ التطبيقات الأربعة على تمثيل ومحاكاة لتنفيذ البروتوكول، وتحديد أنواع الهجوم المحتملة ضده، ونقدّر كذلك فيما إذا كان قادراً على منع تلك الهجمات أو لا. وبالتالي تحديد فيما إذا كان البروتوكول آمناً ضمن الشروط المحددة مسبقاً.

قمنا بكتابة البروتوكول المقترح بلغة HLPSL وتنفيذه باستخدام AVISPA لتقييم أدائه الأمني ضد الهجمات المحتملة (انظر الشكل -15-)، والإجابة عن السؤال الأهم: هل يمكن اعتباره آمناً وبالتالي نكون قد حققنا الهدف المنشود حيث وصلنا إلى بروتوكول توجيه ضمن الشبكات اللاسلكية العشوائية سري وآمن دون الحاجة إلى طرف توثيق ثالث، وبدون الحاجة إلى تقييد الشروط على الشبكة أو على البروتوكول نفسه.

نمذجة البروتوكول المقترح باستخدام لغة HLPSL:

للتحقق من أداء البروتوكول باستخدام AVISPA، يجب بداية نمذجة هذا البروتوكول باستخدام لغة HLPSL.

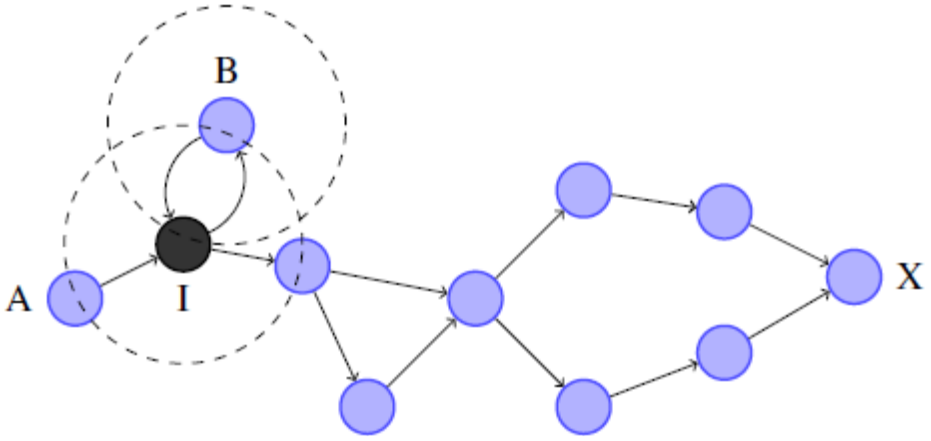
كل العقد في الشبكة التي تتصرف بنفس الأداء تُجمع فيما يسمى بالأدوار الأساسية basic roles. يُعرف الدور على أنه نموذج module يحوي المعلومات الأولية عن العقدة وهي متحولات هذا الدور، ويحوي أيضاً الحالة الابتدائية للعقدة، وطرق الانتقال بين الحالات.

فإذا أخذنا هذا التعريف في تطبيقنا نجد أن العقد في البروتوكول المقترح تُجمع في ثلاثة أدوار أساسية: المرسل source، والهدف destination، والعقد الوسيطة intermediate. وهناك الدور الرابع والذي يتمثل في بناء الشبكة والتواصل بين العقد session، والدور الخامس environment والذي يحدد طريقة بناء طبولوجية الشبكة.

تبدأ العقدة المرسل عملية اكتشاف المسار ببث رسالة RDP، وتمر عبر العقد الوسيطة للوصول إلى العقدة الهدف. وبعدها تقوم العقدة الهدف بتوليد رسالة REP وإرسالها إلى المرسل عبر المسار المكتشف. وللتحقق من خواص الأمان والسرية في هذه المرحلة من البروتوكول (مرحلة اكتشاف المسار) علينا بناء وتعريف هذه الأدوار الثلاثة، اعتماداً على طبولوجية معينة للشبكة .

6.2. سيناريو المحاكاة

لتكن الشبكة ممثلة بالشكل التقليدي التالي -13-



الشكل (13) مثال عن طبولوجيا الشبكة والهجوم المفترض

لدينا العقدة المرسلة A، والعقدة الهدف X، والعقدة الوسيطة B ، والعقدة المتجسسة I (المهاجم) intruder.

العقدة I ستتظاهر بأنها عقدة وسيطة في الشبكة وبالتالي ستكون الرسائل المتبادلة كالتالي:

$$A \rightarrow I : \{RDP, X, N_A\}_{K_{A-}}, cert_A$$

$$I \rightarrow B : \{RDP, X, N_A\}_{K_{A-}}, cert_A$$

$$B \rightarrow I : \left\{\{RDP, X, N_A\}_{K_{A-}}\right\}_{K_{B-}}, cert_A, cert_B$$

عندما تتحرك B خارج نطاق الشبكة، تأخذ العقدة المهاجمة I موقعها بين العقدتين A,B. تبث A رسالة RDP، تصل إلى العقدة I، لكن I لاتستطيع الرد لأنها لاتمتلك المفتاح الخاص لـ B فتعيد إرسال الرسالة إلى B على أنها المرسل A. وترد B إلى I على أنها A أيضاً. لنحصل في النهاية على مسار خاطئ يحوي العقدة المتجسسة I.

- سلوك العقد في الشبكة كإرسال الرسائل واستقبالها يمثل بلغة HLPSL بأحداث events. هذه الأحداث تمثل المعلومات في كل عقدة موثوقة وهناك أيضاً الأحداث المساعدة auxiliary events، والتي تمثل المعلومات المتبادلة بين العقد. باستخدام هذه الأحداث يمكننا تعريف الهدف من تنفيذ البروتوكول وبالتالي تحديد مواصفات السرية المطلوبة في تلك الشبكة.

فمن أجل التوثق مثلاً authentication لدينا الحدثان الشـــاهد witness و الطلب request اللذان يُســتخدمان في التحقق من أن العقدة الموثقة تتصــرف بشــكل صــحيح من حيث الوصــول إلى الحالة الصحيحة وإرسال واستقبال القيم الصحيحة غير المزيفة.

وهناك أيضــاً الحدث wrequest والذي يســتخدم في التوثق بين عقدتين دون الحاجة لوجود طرف ثالث weak authentication، وهو ما يهمنا في دراستنا.

- Witness (A,B,v,M) : تعني أن العقدة A شـــاهد على موثوقية العقدة B، وذلك عبر التحقق من القيمة M باستخدام البروتوكول v.
- Wrequest (B,A,v,M) : وتعني أن العقـدة B تطلـب التوثق من خلال القيمـة M، باعتبار أن العقدة A شاهد على هذه القيمة في وقت ما سابقاً، باستخدام البروتوكول v.

وتمثل هذه الأحداث في لغة HLPSL الهدف المطلوب الوصـــول إليه، بالتالي متطلبات الســـرية في البروتوكول تُمثَّل بوساطة هذه الأحداث.

- متطلبات السرية في البروتوكول المقترح:

تحوي العقدة المرســـلة A الحدث witness مع العقدة B والرقم المميز N_A في مرحلة اكتشـــاف المســـار request phase. وتحوي الحدث wrequest في مرحلة الرد reply phase أيضـــاً مع العقدة B والرقم المميز N_a.

وتحوي العقدة المجاورة الوسـيطة B الحدثين witness, wrequest مع العقدة السـابقة A، والعقدة المجاورة C. وكذلك باقي العقد حتى العقدة الهدف X، التي تتضمن نفس الحدثين.

6.2.1. الدور الأول (المرسل) source role :

تقوم عقدة المرسل بعملين رئيسيين، ترسل رسالة RDP إلى الهدف، وتستقبل رسالة REP منه. ويمكن لهذه العقدة أن تستقبل من الهدف مباشرة، أو عبر العقد الوسيطة. ويُعبّر عن هذا باستخدام HLPSL كالتالي، الشكل -14-:

متحولات المعرفة الابتدائية للعقدة:

- العقدة المرسل A، وباقي العقد الوسيطة B,C، والعقدة الهدف X.
- المفتاح العام للعقدة المرسلة K_a ، والعقد الوسيطة Kb,Kc، والعقدة الهدف K_x.

- متحولات القناة للإرسال SND، والاستقبال RCV.

```
role source_node(
      A,B,C,X : agent,
      Ka, Kb, Kc, Kx : public_key,
      RCV, SND : channel(dy))
played_by A def=
      local
            RDP,REP : protocol_id,
            State   : nat,%{not assigned}
            NA      : text %identifier
      const
            a_b_IPa, a_b_IPx, a_a_Na : protocol_id
      init State := 0
      transition
            step1.
                  State = 0 /\ RCV(start)  %state=0  and starting command
                  =|>
                  State' := 4 /\ Na'  := new() % updated values needs  '
                              /\ SND({RDP.X.Na' }_inv(Ka))
                              /\ witness(A,B,a_b_IPx,X) /\ witness(A,B,a_a_Na,Na' )
            step2.
                  State = 4   /\ RCV({{REP.A' .Na' }_inv(Kx)}_inv(Kb))
                  =|>
                  State' := 8 /\ wrequest(A,B,a_b_IPa,A' )
                              /\ wrequest(A,B,a_a_Na,Na' )
end role
```

الشكل (14) دور عقدة المرسل

تبدأ العقدة المرسل A بإرسال رسالة RDP في الحالة الابتدائية (state = 0). وتقوم بتغيير الحالة إلى حالة انتظار الجواب REP.

عند الانتقال من الحالة الابتدائية تأخذ N_a قيمة جديدة، وتقوم A بإرسال RDP تحوي عنوان العقدة الهدف X، والرقم المميز N_A باستخدام المفتاح K_a. وتكون أيضاً شاهداً على الثنائية (X, N_A) للعقدة المجاورة B، من أجل اختبار سريتها.

أما عند الانتقال من حالة استقبال رسالة الرد REP، فإن العقدة A تطلب اختبار سرية الثنائية (A,N_A) القادمة إليها من B.

6.2.2. الدور الثاني (عقد وسيطة) intermediate role :

تقوم العقد الوسيطة بمهمتين هما : إعادة بث رسائل RDP بعد المصادقة عليها، وإعادة إرسال رسائل REP أيضاً بعد المصادقة عليها. ولدينا حالتان إما تكون الرسائل قادمة مباشرة من المرسل أو المستقبل، أو عبر العقد الوسيطة الأخرى، لذلك يمكننا تمييز حالتين من العقد الوسيطة تحديداً في مرحلة الاكتشاف request phase. أولهما هي حالة العقد التي تجاور المرسل A، وفيها يتم التحقق من توقيع العقدة A وشهادتها، بينما الثانية هي العقد الأبعد لأنها سوف تتحقق من التوقيعين سوية (للمرسل وللعقدة المجاورة) والشهادتين المرسلتين أيضاً. بينما في مرحلة الرد reply phase ستقوم العقد الوسيطة بنفس المهمة ولاحاجة للتمييز بينها.

يمثل هذا بلغة HLPSL كالتالي، الشكل -15- :

عند استلام رسالة RDP، ستبحث العقدة الوسيطة في ذاكرتها عن الثنائية (N_A,A) فإذا وجدتها فهذا يعني أن الطلب قد مرّ سابقاً وتمت معالجته، فتهمل الرسالة. أما عندما لا تجد الثنائية السابقة فإنها تعالج هذا الطلب، وتقوم بتخزين الثنائية التي حصلت عليها (N_A,A) من أجل الطلبات اللاحقة.

ولمعالجة الطلب تقوم B بالانتقال إلى حالة إرسال الرسالة RDP بعد إضافة توقيعها، وتكون شاهداً على الثنائية (X,N_A) المرسلة إلى العقدة المجاورة C، وبنفس الوقت تطلب الاختبار على الثنائية (X,N_A) من العقدة A.

أما في حالة إرسال الرد REP، فإن B ترسل رسالة الجواب إلى A، بعد التحقق من التوقيع X، وإضافة توقيعها. كما تكون شاهداً للثنائية (A,N_A) المرسلة إلى A، وتطلب أيضاً الاختبار من العقدة C على تلك الثنائية.

```
role intermediate_node1(
A,B,C,X : agent,
Memory : (text.text.agent) set,
Ka, Kb, Kc, Kx : public_key,
RCV,SND : channel(dy))
played_by B def=
local
RDP,REP : protocol_id,
State : nat,
Na: text
const
a_b_IPa, a_b_IPx, a_a_Na : protocol_id
init State := 1
transition
step1.
State = 1 /\ RCV({RDP.X'.Na'}_inv(Ka)) /\ not(in(RDP.Na'.X', Memory))
=|>
State' := 5 /\ SND({{RDP.X'.Na'}_inv(Ka)}_inv(Kb).
/\ wrequest(B,A,a_b_IPx,X') /\ wrequest(B,A,a_a_Na,Na')
/\ witness(B,C,a_b_IPx,X') /\ witness(B,C,a_a_Na,Na')
step2.
State = 5 /\ RCV({{REP.A'.Na'}_inv(Kx)}_inv(Kc) /\ not(in(RDP.Na'.X', Memory))
=|>
State' := 9 /\ SND({{REP.A'.Na'}_inv(Kx)}_inv(Kb).
/\ wrequest(B,C,a_b_IPa,A') /\ wrequest(B,C,a_a_Na,Na')
/\ witness(B,A,a_b_IPa,A') /\ witness(B,A,a_a_Na,Na')
end role
```

الشكل (15) دور العقدة الوسيطة المجاورة

في الحالة الأخرى من العقد الوسيطة (غير مجاورة للمرسل) فثمة فرق بسيط وهو أن التحقق من التوقيع سيكون للمرسل وللعقدة المجاورة. وتكتب بلغة HLPSL كالتالي، الشكل -16-:

```
role intermediate_node2(
A,B,C,X : agent,
Memory : (text.text.agent) set,
Ka, Kb, Kc, Kx : public_key,
RCV,SND : channel(dy))
played_by C def=
local
RDP,REP : protocol_id,
State : nat,
Na : text
const
a_b_IPa, a_b_IPx, a_a_Na : protocol_id
init State := 2
transition
step1.
State = 2 /\ RCV({{RDP.X' .Na' }_inv(Ka)}_inv(Kb) /\ not(in(RDP.Na'.X', Memory))
=|>
State'  := 6 /\ SND({{RDP.X' .Na' }_inv(Ka)}_inv(Kc). % two verification processes
/\ wrequest(C,B,a_b_IPx,X' ) /\ wrequest(C,B,a_a_Na,Na' )
/\ witness(C,X,a_b_IPx,X' ) /\ witness(C,X,a_a_Na,Na' )
step2.
State = 6 /\ RCV({REP.A' .Na' }_inv(Kx)) /\ not(in(RDP.Na'.X', Memory))
=|>
State' := 10 /\ SND({{REP.A' .Na' }_inv(Kx)}_inv(Kc).
/\ wrequest(C,X,a_b_IPa,A' ) /\ wrequest(C,X,a_a_Na,Na' )
/\ witness(C,B,a_b_IPa,A' ) /\ witness(C,B,a_a_Na,Na' )
end role
```

الشكل (16) دور العقدة الوسيطة البعيدة

6.2.3. الدور الثالث (الوجهة) destination role :

تقوم العقدة الهدف (الوجهة) بمهمة واحدة هي الرد على رسالة RDP. ولدينا أيضاً حالتان إما أن تصل الرسالة من المرسل مباشرة، أو عبر العقد الوسيطة. ويكتب هذا بلغة HLPSL بالشكل -17-:

```
role destination_node(
A,B,C,X : agent,
Memory : (text.text.agent) set,
Ka, Kb, Kc, Kx : public_key,
RCV,SND : channel(dy))
played_by X def=
local
RDP,REP : protocol_id,
State : nat,
Na : text
const
a_b_IPa, a_b_IPx, a_a_Na : protocol_id
init State := 3
transition
step1.
State = 3 /\ RCV({{RDP.X' .Na' }_inv(Ka)}_inv(Kc) /\ not(in(RDP.Na'.A', Memory))
=|>
State' := 7 /\ SND({REP.A' .Na' }_inv(Kx)
/\ wrequest(X,C,a_b_IPx,X' ) /\ wrequest(X,C,a_a_Na,Na' )
/\ witness(X,C,a_b_IPa,A' ) /\ witness(X,C,a_a_Na,Na' )
end role
```

الشكل (17) دور عقدة الهدف

وكما في حالة العقد الوسيطة فإن العقدة الهدف تقوم بداية بالتحقق من أن الرسالة قد عولجت سابقاً أم لا من خلال الثنائية (N_A, A). ثم ترسل رسالة الرد المتضمنة عنوان العقدة المرسلة، والرقم المميز N_A، ومعماة باستخدام K_x. وتكون العقدة X شاهداً للعقدة C من أجل عنوان العقدة المرسلة والرقم المميز، كما تطلب التحقق من C أيضاً من أجل العنوان X والرقم المميز N_A.

6.2.4. دور "الجلسة" session role

يقوم هذا الدور بتوصيف بنية الشبكة، وكما تحدثنا سابقاً سنفترض الحالة التقليدية للشبكة أي لدينا مرسل ومستقبل وعقدتان وسيطتان. ونقوم باستدعاء القواعد السابقة كلها عند المتحولات الصحيحة كالتالي، الشكل -18-:

```
role session(
A,B,C,X : agent,
Ka, Kb, Kc, Kx : public_key)
def=
local
Mem1,Mem2,Mem3 : (text.text.agent) set,
RCV1,SND1,RCV2,SND2,RCV3,SND3,RCV4,SND4 : channel(dy)
Init Mem1:= {} /\ Mem2:= {} /\ Mem3:= {}
composition
source_node(A,B,C,X,Ka,Kb,Kc,Kx,RCV1,SND1)
/\ intermediate_node1(A,B,C,X,Mem1,Ka,Kb,Kc,Kx,RCV2,SND2)
/\ intermediate_node2(A,B,C,X,Mem2,Ka,Kb,Kc,Kx,RCV3,SND3)
/\ destination_node(A,B,C,X,Mem3,Ka,Kb,Kc,Kx,RCV4,SND4)
end role
```

الشكل (18) دور الجلسة

6.2.5. دور "البيئة" environment role:

وفيه يتم تحديد طريقة بناء طبولوجية الشبكة، وكمية المعرفة بالنسبة للعقدة المهاجمة. لدينا إذن العديد من الخيارات لاختبارها، من حيث عدد العقد المشاركة في الشبكة وموقع العقدة المتطفلة.وقد قمنا بتجربة معظم هذه الخيارات لتحديد أداء البروتوكول المقترح.

فمثلاً يمكننا بناء الشبكة بمرسلين ومستقبلين وأربع عقد وسيطة، كما في الرماز التالي، الشكل -19-

```
role environment()
def=
const
a_b_IPa, a_b_IPx, a_a_Na : protocol_id,
a, b, c, x : agent,
ka, kb, kc, kt, kx : public_key
intruder_knowledge ={a, b, c, x, ka, kb, kc, kx}
composition
session(a, b, c, x, ka, kb, kc, kx)
/\ session(a, i, c, x, ka, kb, kc, kx)
end role
```

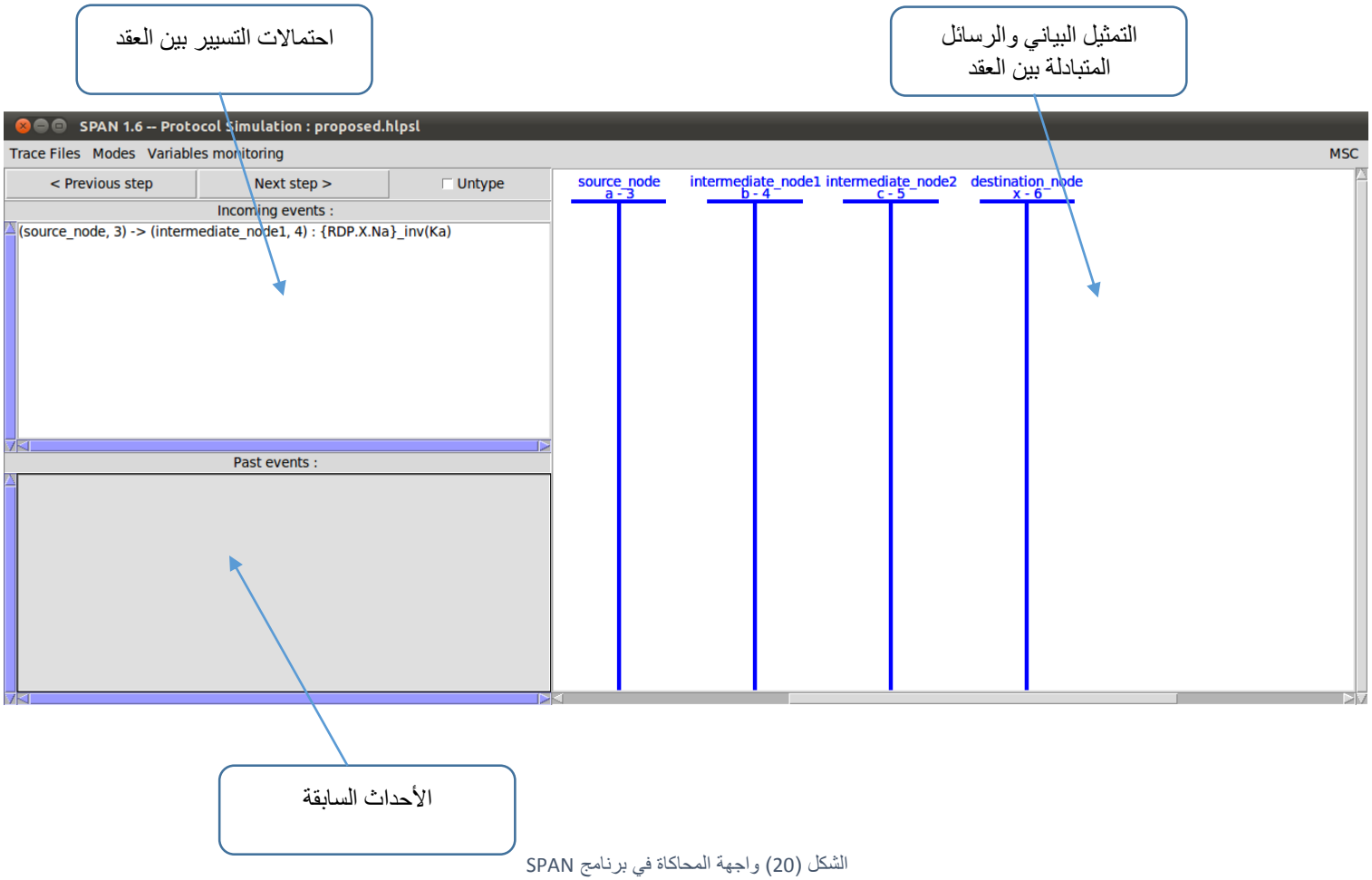
الشكل (19) دور البيئة

والعقدة المتطفلة i يمكنها أن تكون بديلة لأي عقدة في هذا المخطط. في المثال الســـابق اخترنا العقدة المتطفلة بديلة عن العقدة الوسيطة B.

6.3. نتائج تنفيذ البروتوكول :

نبدأ عملية المحاكاة بتحديد بيئة العمل، فنفترض كما في المثال السابق شبكة مكونة من 8 عقد سليمة، عقدتين مرسلتين، وعقدتين مستقبلتين، وأربع عقد وسيطة. تتضمن المحاكاة تحديد المسارات بين العقد المكونة للشبكة، وتحديد قيم المتحولات عند كل عقدة، وكيفية تغيير هذه القيم تبعاً للمسار المحدث.

الشكل التالي -20- يمثل واجهة المحاكاة في برنامج SPAN المرافق لـــ AVISPA من أجل بناء واجهات المحاكاة للبروتوكولات المختبرة، وتفاصيل هذه الواجهة. حيث لدينا عقدة مرسل a-3 وعقدتان وسيطتان b-4 و c-5 وعقدة وجهة x-6. أما قيمة الصفر فتُحجز للعقدة المتطفلة، والقيم 1 و 2 لأغراض أخرى.

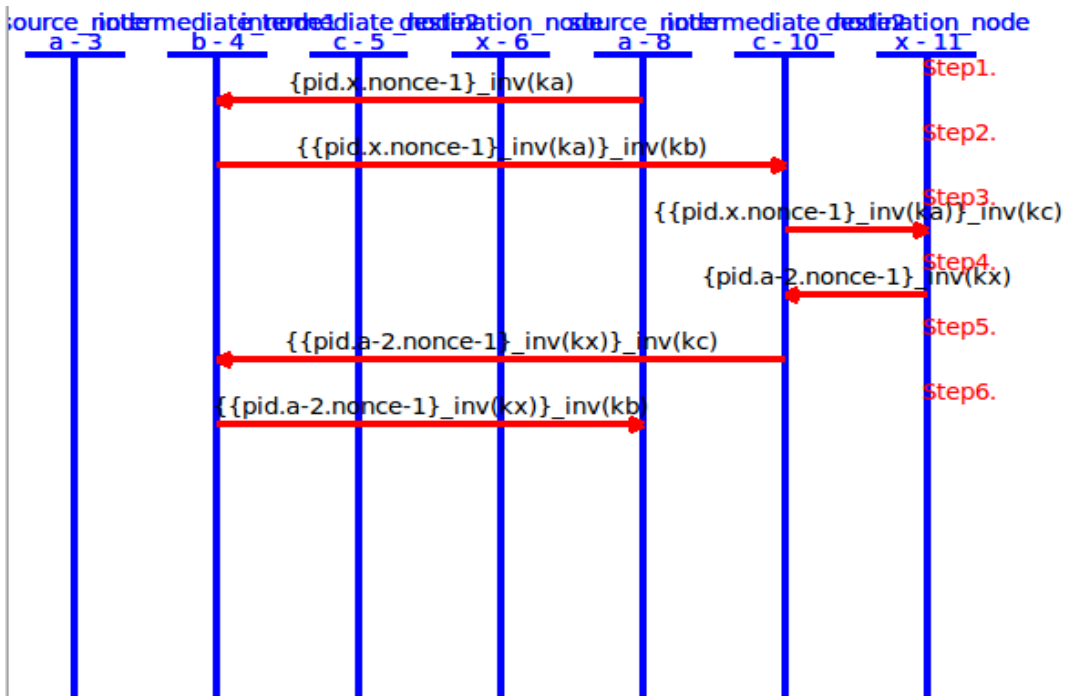


الشكل (20) واجهة المحاكاة في برنامج SPAN

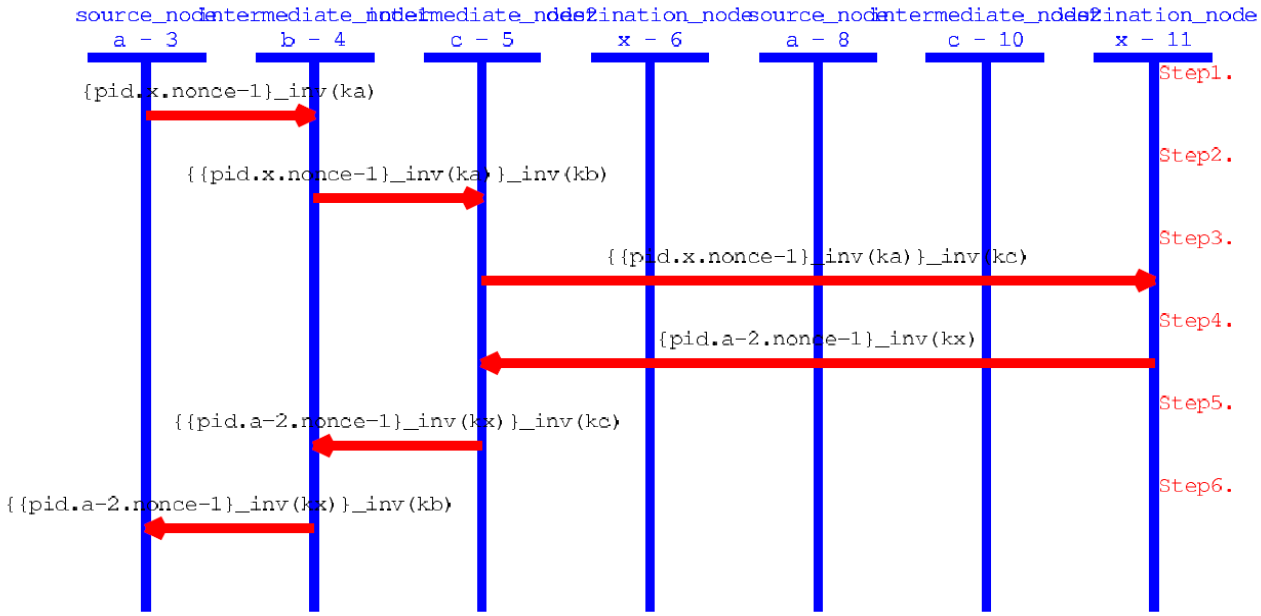
عند محاكاة البروتوكول، يأخذ البرنامج بالاعتبار كل مسارات التوجيه الممكنة. وفي مثالنا لدينا المرسلان a-3, a-8 والوجهتان x-6, x-11 ومجموعة العقد الوسيطة b-4, c-5, c-10. ويتوضح جزء من هذه المسارات في الأشكال التالية :

❖ الشكل الأول -21- لدينا رسالة اكتشاف المسار مرسلة من العقدة a-8، وتتضمن هذه الرسالة البادئة RDP وعنوان الوجهة x، والرقم المميز nonce-1، وتوقع هذه المتحولات باستخدام المفتاح K_a. تصل هذه الرسالة إلى الوجهة x-11 عبر العقدة b-4 التي تضيف مفتاحها K_b، ثم العقدة c-10 التي تزيل التوقيع b وتضيف توقيعها باستخدام K_c.

وبعد الوصول إلى الوجهة ترسل x-11 رسالة الجواب REP إلى المرسل a-8 عبر نفس المسار السابق متضمنة عنوان المرسل والرقم المميز وموقعة باستخدام المفتاح K_x.

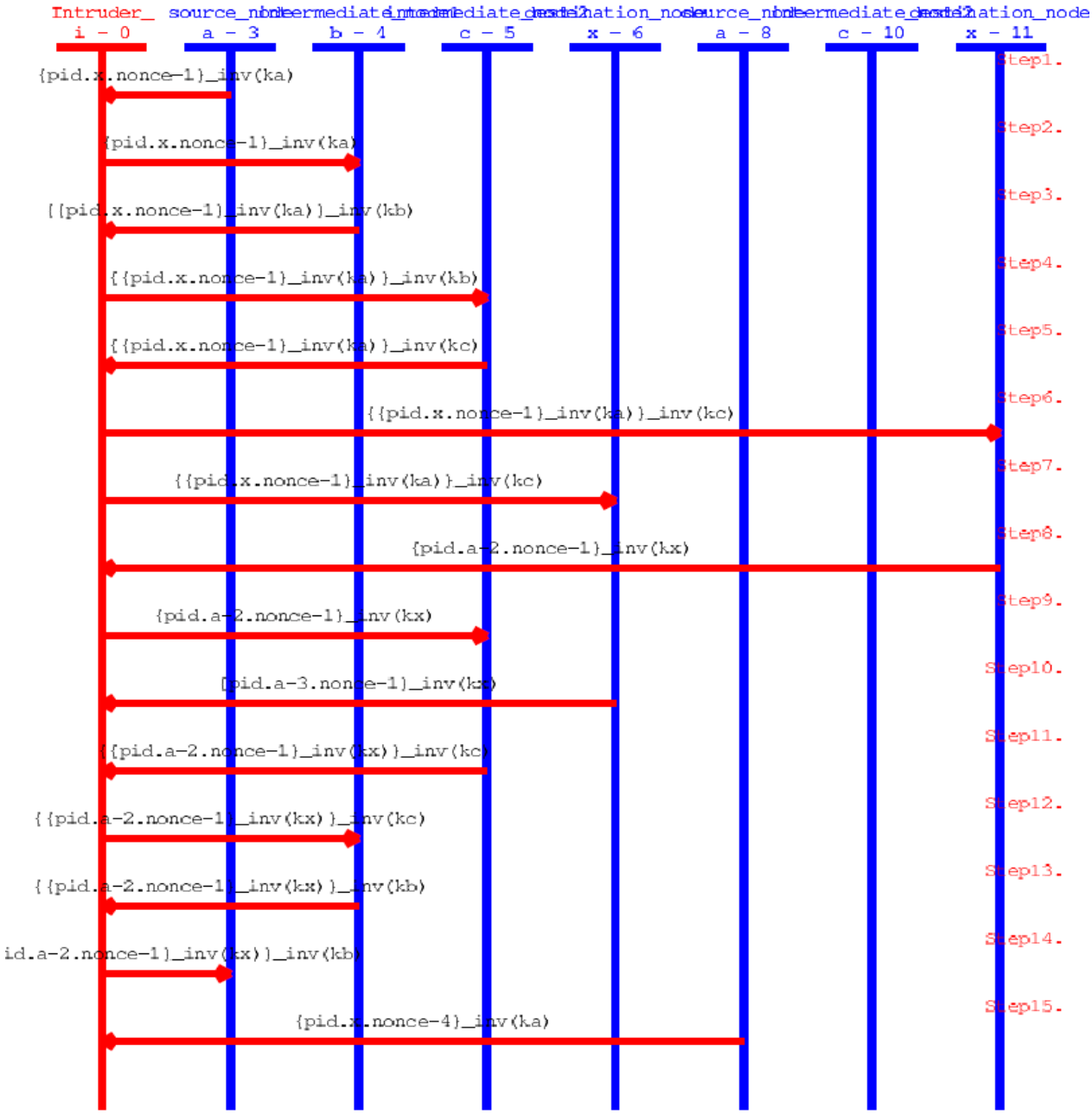


الشكل (21) محاكاة اكتشاف المسار من a-8 إلى x-11



الشكل (22) محاكاة اكتشاف المسار من a-3 إلى x-11

❖ الشكل الثاني -22- يمثل المسار من المرسل a-3 إلى الوجهة x-11 عبر العقدتين b-4, c-5. تتضمن رسالة الاكتشاف عنوان الوجهة، والرقم المميز، وموقعة بالمفتاح K_a . وتمر عبر العقدتين الوسيطيتين b-4, c-5 إلى الوجهة x-6 . والتي بدورها ترسل رسالة الرد REP عبر نفس المسار.



الشكل (23) نموذج لتطفل العقدة I على الشبكة

تدخل الآن عقدة متطفلة I تريد الحصـــول على معلومات الشـــبكة، فتقوم بأخذ مكان عقدة ســـليمة، وتستقبل الرسائل ثم ترسلها على أنها عقدة سليمة. ويبين الشكل التالي -23- نموذجاً لهذا الهجوم.

حيث تقوم العقدة المهاجمة بمخاطبة جميع العقد ومحاولة الحصـــول على المفتاح الخاص بكل منها. وهنا يظهر دور خوارزمية التعمية NTRU التي لن تسـمح لهذه العقدة بالحصـول على أي من المفاتيح الخاصـة في الشـبكة. بالتالي العقدة المهاجمة لن تحصـل على أي من المعلومات الخاصـة بالشـبكة حتى لو وضـعت نفسـها داخل الشـبكة وقامت بإرسـال واسـتقبال الرسـائل كعقدة سـليمة، لأن العقد الأخرى لن تتواصـل معها باعتبار أن عملية التوثق لن تكتمل، فتصنف على أنها عقدة غير سليمة.

وللتحقق من خواص السـرية المتوقعة، نمرر هذا الرماز على تطبيق OFMC، للـــتأكد من سـريته فتكون النتيجة كالتالي، الشكل -24-:

```
% OFMC
% Version of 2006/02/13
SUMMARY
  SAFE
DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
  /home/span/span/testsuite/results/proposed.if
GOAL
  as_specified
BACKEND
  OFMC
COMMENTS
STATISTICS
  parseTime: 0.00s
  searchTime: 0.53s
  visitedNodes: 68 nodes
  depth: 9 plies
```

الشكل (24) نتيجة تنفيذ OFMC على البروتوكول المقترح

نلاحظ أن OFMC يعطينا نتيجة أن هذا البروتوكول آمن، ولم يستطع إيجاد ثغرة للهجوم عليه.

كذلك باستخدام تطبيق ATSE نجد أن البروتوكول المقترح آمن، ولايمكن إيجاد هجوم لاختراقه، الشـكل -25-.

```
SUMMARY
  SAFE

DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
  TYPED_MODEL

PROTOCOL
  /home/span/span/testsuite/results/proposed.if

GOAL
  As Specified

BACKEND
  CL-AtSe

STATISTICS

  Analysed    : 49 states
  Reachable   : 17 states
  Translation: 0.06 seconds
  Computation: 0.00 seconds
```

الشكل (25) نتيجة تنفيذ CL-AtSe على البروتوكول المقترح

والجدير ذكره أنه عند تنفيذ برتوكول AODV التقليدي بدون التعديلات التي أضفناها باستخدام أداة AVISPA، أعطى تنفيذ التطبيق OFMC نتيجة سلبية كما في الشكل -26-، فهو يخبرنا أن ذلك البروتوكول غير آمن، وقابل للاختراق.

```
% OFMC
% Version of 2006/02/13
SUMMARY
  UNSAFE
DETAILS
  ATTACK_FOUND
PROTOCOL
  /home/span/span/testsuite/results/test.if
GOAL
  as_specified
BACKEND
  OFMC
COMMENTS
STATISTICS
  parseTime: 0.00s
  searchTime: 0.06s
  visitedNodes: 2 nodes
  depth: 1 plies
ATTACK_TRACE
   i -> (a,8): start
   (a,8) -> i: {dummy_pid.x.Na(1)}_inv(ka).{a.ka.dummy_nonce.dummy_nonce}_inv(kt)
   i -> (b,3): {dummy_pid.x.Na(1)}_inv(ka).{a.ka.dummy_nonce.dummy_nonce}_inv(kt)
   (b,3) -> i:
{dummy_pid.x.Na(1)}_inv(ka)}_inv(kb).{a.ka.dummy_nonce.dummy_nonce}_inv(kt).{b.kb.dummy_nonce.
dummy_nonce}_inv(kt)
```

الشكل (26) نتيجة تنفيذ OFMC على البروتوكول التقليدي AODV

الخاتمة والآفاق المستقبلية

الخاتمة والآفاق المستقبلية

قدمنا في هذه الدراسة عرضاً لخوارزميات التعمية بعد الكمومية، وقمنا بدراسة عامة لخوارزمية NTRU، ومن ثم مقارنة أدائها بخوارزميات التعمية التقليدية مثل RSA,ECC من حيث سرعة التنفيذ، والتعقيد الحسابي، وقابلية اختراقها. ولاحظنا أن خوارزمية NTRU هي الخوارزمية الأمثل في الوقت الحاضر لعمليات التعمية حيث تتميز بسرعة أدائها وتعقيدها الحسابي البسيط وصغر طول المفتاح مقابل سرية عالية تماثل الخوارزميات الأخرى.

وانتقلنا في هذه الدراسة لاستعراض التقنيات المطروحة حالياً لبناء نظام أمني في شبكات MANET. والتفكير بتوظيف خوارزمية NTRU في بناء نظام أمني يلبي الاحتياجات في هذه الشبكات.

كما نعلم أن بروتوكولات التوجيه في شبكات MANET لاتحوي سرية عالية وبالتالي فإن اختراقها بشكل عام يعتبر سهلاً. لذلك اقترحنا آلية جديدة في زيادة سرية بروتوكولات التوجيه وتحديداً بروتوكولات التوجيه عند الطلب AODV تعتمد على خوارزمية NTRU في تحقيق عملية التوثق بين العقد دون الحاجة إلى وجود طرف ثالث موثوق. أي نستطيع التوثق من جميع العقد في الشبكة باستخدام الطريقة التقليدية في إدارة الشهادات الموزعة دون الحاجة لوجود إدارة مركزية، وبالتالي الوصول إلى سرية عالية في شبكات MANET دون الخسارة في شروط الشبكة من حيث الاستطاعة المطلوبة، والتوزع الجغرافي للعقد.

تمتلك هذه الآلية عدداً من الإيجابيات يمكن تلخيصها فيمايلي:

- سهولة إجرائية التوثق بين العقد.
- سهولة التحقق من شهادات العقد.
- مناعة عالية للاختراق، بسبب مناعة خوارزمية NTRU.
- تؤمن الخدمات الأمنية كلها : التوثق، وسلامة المعطيات، وسريتها، وعدم الإنكار.
- تؤمن مسار آمن بين أي عقدتين باستخدام الخوارزمية NTRU.

وللتحقق من هذا المقترح استخدمنا أداة AVISPA وهي الأداة الرسمية في اختبار سرية بروتوكولات الشبكات، واختبارها ضد الهجمات المحتملة. وقد أثبتت AVISPA أن هذه الآلية المقترحة آمنة تماماً، ومنيعة ضد الاختراقات.

وفي المستقبل يمكن العمل على خوارزمية لضمان عملية التوثق بين العقد باعتماد مبدأ التشاركية، حيث تحمل كل عقدة جزءاً من السر، تُجمع هذه الأجزاء لتستخدم عندما تريد عقدة جديدة الانضمام إلى الشبكة، وذلك باستخدام خوارزمية NTRU أيضاً. وبالتالي بناء نظام أمني متكامل يمتلك السرية العالية في شبكات MANET من حيث توليد الشهادات وتوزيعها واختبار صلاحيتها دون الحاجة إلى الحد من طبيعة الشبكة.

المراجع

[Ajt96]	*M.Ajtai, "Generating hard instances of Lattice problems". IBM research center, 1996.*
[Ali07]	*A.Mersin, "the comparative performance analysis of lattice based ntru cryptosystem with other asymmetrical cryptosystems". Master of Science Thesis, Izmir Institute of technology,2007*
[Aod00]	*"Ad hoc On-Demand Distance Vector (AODV) Routing" RFC3561*
[Arm02]	*A. Armando, D. Basin, M. Bouallagui, Y. Chevalier, L. Compagna, S. Modersheim, M. Rusinowitch, M. Turuani, L. Vigano, and L. Vigneron, "The AVISS Security Protocol Analysis Tool". Springer, 2002.*
[Arm04]	*A. Armando and L. Compagna, "SATMC: a SAT-based Model Checker for Security Protocols". Springer, 2004.*
[Avi04]	*The AVISPA Project. URL: www.avispa-project.org.*
[Bab86]	*L.Babai, "On Lovasz Lattice Reduction and the nearst lattice point problem". Combinatorica 6, 1986.*
[Bal02]	*D.Balfanz, D. K. Smetters, P.Stewart and H. Chi Wong, "Talking To Strangers: Authentication in Ad-Hoc Wireless Networks". Xerox Palo Alto Research Center, 2002.*
[Bas04]	*D. Basin, S. Modersheim, L. Vigano, "OFMC: A Symbolic Model-Checker for Security Protocols". International Journal of Information Security, 2004.*
[Bla01]	*B. Blanchet. "An efficient cryptographic protocol verifier based on prolog rules". CSFW'01, IEEE Computer Society Press, 2001.*
[Bob03]	*B.Bobba, L.Eschenauer, V.D.Gligor, W.Arbaugh," Bootstrapping Security Associations for Routing in Mobile Ad- Hoc Networks". TECHNICAL RESEARCH REPORT, University of Maryland, 2003.*
[Bod05]	*C. Bodei, M. Buchholtz, P. Degano, F. Nielson, and H. Riis Nielson. "Static validation of security protocols". Journal of Computer Security, Vo. 13, 2005.*
[Boi04]	*Y. Boichut, P. Heam, O. Kouchnarenko, F. Oehl. "Improvements on the Genet and Klay Technique to Automatically Verify Security Protocols". AVIS'04, 2004.*
[Bon03]	*D.Boneh and M.Frankliny, "Identity-Based Encryption from the Weil Pairing". SIAM J. of Computing, Vol. 32, No. 3, 2003.*
[Bor02]	*M. Boreale and M. G. Buscemi. "A framework for the analysis of security protocols". LNCS 2421, Springer, 2002.*
[Cap03]	*S.Capkun, L.Buttyan, and J.Hubaux, "Self-Organized Public-Key Management for Mobile Ad Hoc Networks". IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 2, NO. 1, JANUARY-MARCH 2003.*
[Cer08]	*D. Cerri, A. Ghioni, SecuringAODV: The A-SAODV Secure Routing Prototype, IEEE Communication Magazine, 2008, pp 120-125*
[Che02]	*Y. Chevalier and L. Vigneron. "Automated Unbounded Verification of Security Protocols". CAV'02, LNCS 2404. Springer, 2002.*
[Cru05]	*R.Crues, "Methods for Access Control: Advances and Limitations". Harvey Mudd College, Claremont, California. 2005.*
[Dah02]	*B. Dahill, K. Sanzgiri, B.N. Levine, E.M. Belding-Royer, A secure routing protocol for ad hoc networks, in Proceedings of the 10th IEEE International Conference on Network Protocols (ICNP), Paris, France, p.78-89, 2002.*
[Dam00]	*E.Damiani S.Capitani, V.Stefano P.Samarati, "Design and Implementation of an Access Control Processor for XML Documents". Computer Networks 33(1):59-75 · 2000*
[Dan09]	*D.Bernstein, J.Buchmann and E.Dahmen, "Post-Quantum Cryptography". Springer, 2009.*
[Dol83]	*D. Dolev and A. Yao. "On the Security of Public-Key Protocols". IEEE Transactions on Information Theory, 2(29), 1983.*

[Doo96]	*L.Doorn, M.Abadi, M.Burrows and E.Wobber, "Secure Network Objects". SP'96, IEEE conference on Security and privacy, 1996.*
[Elw96]	*F.Elwailly, C.Gentry, and Z.Ramzan, "QuasiModo: Eficient Certificate Validation and Revocation". DoCoMo Communications Laboratories USA, Inc. 2004.*
[Gau14]	*P.Gauravaram, H.Narumanchi, N.Emmadi, "Analytical study of Implementation issues of NTRU". International Conference on Advances in Computing, Communications and Informatics, IEEE, New Delhi, India, pp. 700-707, 2014*
[Gol97]	*O.Goldreich, S.Goldwasser, S.Halevi, "Public-Key Cryptosystems from Lattice Reduction Problems". MIT, Laboratory for Computer Science, 1997.*
[Gra07]	*N.H.Graham, "A Hybrid Lattice-Reduction and Meet-in-the- Middle Attack Against NTRU". NTRU Cryptosystems, Inc. 2007.*
[Had00]	*S.Hada and M.Kudo, "XML Access Control Language: Provisional Authorization for XML Documents". Tokyo Research Laboratory, IBM Research. 2000.*
[Her95]	*A.Herzberg, S.Jarecki, H.Krawczyk, M.Yung, "Proactive Secret Sharing or: How to cope with Perpetual Leakage". IBM T.J. Watson Research Center, Yorktown Height, NY. 1995.*
[Hof98]	*J.Hoffstein, J.Pipher, J.H.Silverman, "NTRU: A Ring-Based Public Key cryptosystem". NTRU Cryptosystems, Inc. 1998.*
[Hue13]	*E-Huei Lu, HK.Chang, SH.Liaw and PC.Su "A Security and Efficiency of Authenticated Key Exchange Protocol for Wireless Mobile Ad Hoc Networks". Applied Mechanics and Materials, Switzerland, Vols. 284-287, 2013.*
[Huy02]	*Y.C. Hu, P. Adrian, and B. David,"Ariadne: A secure on-demand routing protocol for ad hoc networks". MobiCom 2002, Atlanta, Georgia, USA, 2002.*
[Kar06]	*F.Kargl, S.Schlott, M.Weber, "Identification in Ad hoc Networks". Media Informatics Department, Ulm University, Germany. 2006*
[Kau12]	*R.Kaur & M.Kumar Rai, "A Novel Review on Routing Protocols in MANETs". Department of Electronics and Engineering, Lovely Professional University, Punjab, India. 2012.*
[Kle11]	*L.KleinBerndt, "A Quick Guide to AODV Routing, National Institute of Standards and Techhnology", US Department of Commerce, USA. 2011.*
[Kon01]	*J.Kong, P.Zerfos, H.Luo, S.Lu, L.Zhang, "Providing Robust and Ubiquitous Security support for Mobile ad-hoc Networks". University of California, Los Angeles. 2001.*
[Kum12]	*R.Kumar and V.Saraswat, "Comparative Analysis for Performance acceleration of Modern Asymmetric Crypto Systems". J. of Comp. and I.T. Vol. 3(1&2), 2012.*
[Kum13]	*M. Kumar, M. Faisal, A. Ahmed, "Attacks in MANET". International Journal of Research in Engineering and Technology. Volume 02- Issue 10, 2013.*
[Lam79]	*L.Lamport," Constructing Digital Signatures from a One Way Function". Computer Science Laboratory, SRI International. 1979.*
[Lan14]	*A.Langlois, "Lattice-Based Cryptography: Security Foundations and Constructions". PHD thesis in Lyon University, France. 2014.*
[Len82]	*A.K.Lenstra, H.W.Lenstra, L.Lovasz, "Factoring Polynomials with Rational Coefficients". Math. Ann. 261, S15-534. 1982.*
[lin11]	*R.Lindner, "Towards E_cient Lattice-Based Cryptography". PHD Thesis in Darmstadt university, Germany. 2011.*
[Lyu08]	*V. Lyubashevsky, D. Micciancio, C. Peikert, and A. Rosen. Swifft: "A modest Proposal for fft hashing". In FSE, 2008.*
[Mar03]	*J. Marshall,"An Analysis of the Secure Routing Protocol for mobile ad hoc network route discovery: using intuitive reasoning and formal verification to identify flaws", Master's Thesis, Department of Computer Science. Florida State University, Tallahassee, May 2003.*
[Mar10]	*M.Dipobagio, "An Overview on Ad Hoc Networks". Institute of Computer Science (ICS), Freie Universität Berlin. 2010.*

[Mce78]	*R. McEliece. "A public key cryptosystem based on algebraic coding theory". DSN Progress report, 1978.*
[Meh10]	*S.Mehla, B.Gupta and P.Nagrath,"Analyzing security of Authenticated Routing Protocol (ARAN)". International Journal on Computer Science and Engineering Vol. 02, No. 03, 2010.*
[Mer89]	*R. C. Merkle. "A certified digital signature. In Proceedings of Advances in Cryptology". CRYPTO'89, Springer, 1989.*
[Mic08]	*D.Micciancio, O.Regev, "Lattice-based Cryptography". pp. 147-191, Springer, 2009.*
[Mon02]	*G.Montenegro, C.Castelluccia, "Statistically Unique and Cryptographically Verifiable (SUCV) Identifiers and Addresses". SUNLabs, Meylan, France. 2002.*
[Mor05]	*M. C. Morogan, "Security System for Ad-hoc Wireless Networks based on Generic Secure Objects". Ph.D. Thesis, Kungliga Tekniska Högskolan, 2005.*
[Nal01]	*S. Yi, P. Naldurg, and R. Kravets, "Security-Aware Ad hoc Routing for Wireless Networks", ACM international symposium on Mobile ad hoc Networking & Computing, Long Beach, CA, USA, 2001.*
[Nga04]	*C.H. Ngai, and M.R. Lyu, "Trust- and Clustering-Based Authentication Services in Mobile Ad Hoc Networks". Department of Computer Science & Engineering, The Chinese University, Hong Kong, 2004.*
[Oka89]	*E. Okamoto, K. Tanaka, "Identity-based Information Security Management System for Personal Computer Networks," IEEE J. Areas Communication. vol. 7, 1989.*
[Pap02]	*P. Papadimitratos, and Z. Haas, "Secure routing for mobile ad hoc networks, in Proceedings of the SCS communication Networks and Distributed Systems". Modeling and Simulation Conference, San Antonio, TX, 2002*
[Per01]	*A. Perrig, R. Canetti, D. Song, and J.D. Tygar. "Efficient and secure source authentication for multicast". Network and Distributed System Security symposium, pp. 35-46, 2001.*
[Per03]	*A.Perrig, Y.Hu, and D.Johnson, "Rushing attacks and defense in wireless ad hoc network routing protocols". ACM workshop on WIreless SEcurity WISE 2003, San Diego, CA, USA, 2003.*
[Phi07]	*Ph.Kaye, R.Laflamme, M.Mosca, "An introduction to quantum computing". Oxford 2007.*
[Ram04]	*P. Ramachandran and A. Yasinsac, "Limitations of On Demand Secure Routing Protocols", IEEE Information Assurance Workshop 2004, pp. 52-59, 2004.*
[Rau13]	*S.Raut, H.Ambulgekar, "Proactive and Reactive Routing Protocols in Multihop Mobile Ad hoc Network". International Journal of Advanced Research in Computer Science and Software Engineering.Volume 3, Issue 4, 2013.*
[Sad05]	*K.Sadasivam, "Performance and Security in Mobile Ad hoc Networks". Master of Science Thesis in University of Houston-Clear Lake, USA. 2005.*
[Sax05]	*N.Saxena, G.Tsudik, J.Yi, "Eficient Node Admission for Short-lived Mobile Ad Hoc Networks". IEEE International Conference on Network Protocols. 2005.*
[Sax10]	*N.Saxena, J.Yi, "Non-Interactive Self-Certification for Long-Lived Mobile Ad Hoc Networks". IEEE Transactions on Information Forensics and Security 4(4), 2010.*
[Sha14]	*R. Shaktawat, D. Singh, N. Choudhary, "An Efficient Secure Routing Protocol in MANET Security - Enhanced AODV (SE-AODV)". International Journal of Computer Applications. Volume 97– No.8, 2014.*
[Sha84]	*A. Shamir, "Identity-based Cryptosystems and Signature Schemes". Crypto-84, Santa Barbara, CA, 1984*
[Shm79]	*A.Shamir, "How to Share a Secret". ACM, MIT. 1979.*
[Sch87]	*C.Schnorr, "A hierarchy of polynomial time basis reduction algorithms". Goethe-Universität Frankfurt, Germany. 1987.*
[Sta99]	*F.Stajano and R.Anderson, "The Resurrecting Duckling: Security Issues for Ad-hoc Wireless Networks". Springer-Verlag Berlin Heidelberg 1999.*

[Thm99]	*M.Thompson, W.Johnston, S.Mudumbai, G.Hoo, K.Jackson, A.Essiari, "Certificate-based Access Control for Widely Distributed Resources". Ernest Orlando Lawrence Berkeley National Laboratory, Berkeley, CA. 1999.*
[Tom10]	*P. Tomar, P. Suri, M. Soni, "A Comparative Study for Secure Routing in MANET". International Journal of Computer Applications. Volume 4 – No.5, 2010.*
[Wan03]	*W.Wang, Y.Zhu, B. Li, "Self-Managed Heterogeneous Certification in Mobile Ad Hoc Networks". University of Toronto 2003.*
[Web07]	*"The Case for Elliptic Curve Cryptography",* http://www.nsa.gov/ia/industry/crypto_elliptic_curve.cfm
[Wei01]	*J.Weise, "Public Key InfrastructureOverview". Sun Microsystems, Inc. 2001.*
[Xin13]	*X.Zhan, R.Zhang, Z.Xiong, Z.Zheng, Z. Liu, "Efficient Implementations of NTRU in Wireless Network". Communications and Network, Vo.5, 485-492, 2013.*
[Zap02]	*M. Guerrero Zapata and N. Asokan, "Securing Ad hoc Routing Protocols", ACM workshop on Wireless security, Atlanta, GA, USA, Sep 2002.*
[Zho99]	*L.Zhou, Z.Haas, "Securing Ad Hoc Networks". IEEE network, special issue on network security, 1999.*