تحقيق الحماية لبروتوكول التسيير الهجين للشبكات اللاسلكية العروية

م. مهند العاقل* الدكتور نوار العوا** الدكتور معتصم شفا عمري***

الملخص

تمثل الشبكات اللاسلكية العُرَوية Wireless Mesh Networks WMN فكرةً واعدةً لتوفير المتطلبات المستقبلية للشبكات، كتأمين بنية مرنة قابلة للتعديل ولإعادة التشكيل، فضلاً عن كونها تمثل حلاً اقتصادياً مناسباً لمزودي الخدمة، إذ تعدُّ الشبكات اللاسلكية العُرَوية حلاً جيداً للتزويد باتصال إنترنت لا سلكي ضمن مساحة جغرافية واسعة.

يعد التسيير Routing من أهم القضايا ضمن الشبكات اللاسلكية العروية، إذْ يجب تأمين بروتوكول تسيير آمن يستفيد من الخصائص الفريدة للشبكات اللاسلكية العروية.

هناك عدد كبير من الهجمات المعروفة على عملية التسيير، لذلك لا بد من تحقيق الحماية لعملية التسيير ضمن الشبكات اللاسلكية العروية.

نعرض في هذا البحث طريقة جديدة لتوفير الحماية للبروتوكول Hybrid Wireless Mesh Protocol HWMP (بروتوكول التسيير الافتراضي ضمن الشبكات العروية).

قمنا بالاستفادة من التوسعة الآمنة للبروتوكول Secure Ad-Hoc On-Demand Distance Vector SAODV لتحقيق الحماية للبروتوكول HWMP، مع إجراء التعديلات الضرورية.

كذلك قمنا بتطوير المحاكي الشبكي NS-3 لتحقيق البروتوكول الآمن الذي قمنا بتوصيفه، وقارنا النتائج مع أهم البروتوكولات الآمنة للشبكات العروية، وقد تبين أن البروتوكول SecHWMP يعطي أداء أفضل من باقي البروتوكولات في معظم الحالات.

الكلمات المفتاحية: الشبكات اللاسلكية العروية، بروتوكول التسيير الهجين للشبكات اللاسلكية العروية، بروتوكول التسيير الآمن للشبكات اللاسلكية العروية.

*أعد البحث في سياق رسالة الماجستير للمهندس مهند العاقل بإشراف الدكتور نوار العوا والدكتور معتصم شفا عمري
** أستاذ مساعد – قسم النظم والشبكات الحاسوبية كلية الهندسة المعلوماتية- جامعة دمشق
*** المعهد العالي للعلوم التطبيقية- دمشق

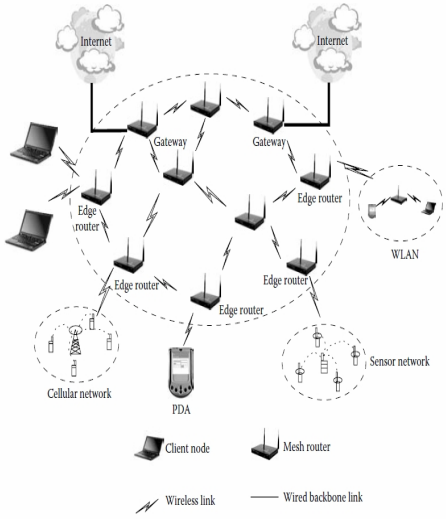
1. مقدمة

تعدّ الشبكات العروية من الشبكات اللاسلكية المتعددة القفزات multi-hop، تتألف هذه الشبكة من المسّيرات العروية والزبائن العروية Mesh clients، عادةً تكون سعة الحزمة في هذه الشبكات جيدة، وتكون كلفة تنفيذ الشبكة ومن ثم الصيانة اللاحقة غير كبيرة.

يتم اختيار بعض المسّيرات العروية لتكون العبّارات gateway routers، حيث يتم ربط هذه المسّيرات بالشبكة السلكية.

تؤمن هذه العبّارات للزبائن النقالين والشبكات التلاؤمية Ad Hoc وشبكات الحساسات sensor networks النفاذ إلى الإنترنت، كما هو موضح بالشكل 1.

يمكن للشبكات اللاسلكية العروية توفير مسار اتصال بين الزبائن النقالين فيما بينهم ومن ثمَّ تُستخدم كشبكة مجتمعية community network، أو توفر مساراً بين الزبائن النقالين والمسّيرات العبّارات وبذلك تحقق اتصال انترنت لاسلكياً عريض الحزمة broadband.



الشكل 1 بنية الشبكات اللاسلكية العروية

تُستَخدَمُ التقنيات الشبكية الموجودة مثل IEEE 802.11 و IEEE 802.15 لتنفيذ الشبكات اللاسلكية العروية.

تقوم مجموعة العمل IEEE Working group 802.11S بوضع المعايير الخاصة بالشبكات اللاسلكية العروية المحلية [1].

نعرض في هذا البحث البروتوكول الهجين للشبكات اللاسلكية العروية Hybrid wireless Mesh Protocol HWMP، ومن ثم نذكر بروتوكولات التسيير الآمنة ضمن الشبكات اللاسلكية العروية، يلي ذلك دراسة المتطلبات الأمنية لعملية التسيير، ثم بروتوكول التسيير الآمن للشبكات اللاسلكية العروية SecHWMP، ونحدد طريقة المحاكاة المتبعة، ومن ثم مقارنة أداء بروتوكولات التسيير الآمنة، و الدراسة التحليلية للبروتوكول SecHWMP.

2. برتوكول التسيير الهجين للشبكات اللاسلكية العروية Hybrid Wireless Mesh Protocol

و هو بروتوكول التسيير الافتراضي default في الشبكات اللاسلكية العروية، يجمع هذا البروتوكول مرونة بروتوكولات التسيير التفاعلية مع إمكانية بناء شجرة تمثل الشبكة بشكل استباقي.

يستخدم هذا البروتوكول الهجين العنوان الفيزيائي MAC address وليس العنوان الشبكي IP address لتوجيه الطرود، حيث يعمل هذا البروتوكول في الطبقة الثانية (طبقة ربط المعطيات data link).

يُعدُّ هذا البروتوكول تطويراً على بروتوكول Ad-Hoc On-demand Distance Vector AODV [3]، فضلاً عن استخدام كلفة مشتقة من جودة الإشارة اللاسلكية المستقبلة radio-aware link metrics واستخدام العنوان الفيزيائي، يتألف هذا البروتوكول

من مكونين، مكون تفاعلي on demand، ومكون استباقي proactive.

يستعمل الجزء التفاعلي آلية اكتشاف الطريق route discovery بشكل مشابه جداً لما هو متبع في البروتوكول AODV، في حين يمثل الجزء الاستباقي من هذا البروتوكول امتداداً لبناء شجرة توجيه استباقية باتجاه عقد خاصة يتم اختيارها لتؤدي دور الجذر.

إن أي عقدة عروية يتم إعدادها لتكون جذراً تقوم دورياً بنشر رسالة إعلان عن جذر root announcement [4]، بحيث تكون وظيفة هذه الرسائل بناء المسارات وصيانتها من جميع العقد العروية إلى الجذر.

1.2 الجزء التفاعلي on demand routing

عندما تحتاج عقدة عروية Mesh Point طريقاً إلى عقدة عروية أخرى فإنها تقوم ببث رسالة طلب مسار Path Request (ولمّا كانت عملية التسيير تتم على مستوى الطبقة الثانية قامت IEEE وهي الجهة المسؤولة عن وضع المعيار باستبدال كلمة طريق route بكلمة مسار path)، تقوم العقد العروية الوسيطة بتعديل المسار باتجاه العقدة المصدر في حال كان هذا المسار أفضل، ثم تقوم بإعادة بث الرسالة، عندما تصل الرسالة إلى العقدة العروية الهدف فإنها تقوم بالرد باستخدام رسالة رد على المسار path reply.

العقد العروية الوسيطة تستطيع الرد على رسالة طلب المسار إذا كانت تمتلك مساراً صالحاً للعقدة الهدف، وإذا كانت راية العقد الهدف فقط Destination Only (DO flag) غير مفعلة، فضلاً عن ذلك تقوم العقدة الوسيطة بفحص راية جاوب وانشر Reply and Forward (RF) flag (لا توجد هذا الراية في البروتوكول AODV).

يوضح الشكل 2 بنية رسالة طلب المسار والراية الجديدة (RF)، بحيث إذا كانت قيمتها 1 تقوم العقدة بالرد على الطلب ولكن على خلاف AODV تقوم ببث الرسالة حيث تقوم بتعديل راية الهدف فقط لتصبح 1 (وذلك لتجنب إرسال المزيد من رسائل الرد على المسار)، عندما تستقبل العقدة الهدف الطلب، وفي حال وجود مسار أفضل، تقوم العقدة الهدف بإرسال رسالة رد على المسار عن طريق المسار الأفضل.

Octets: 1	1	1	1	1	4	6	4	4
Element ID	Length	Flags	Hop count N	TTL	RREQ ID	Originator Address	Originator Sequence Number	Path Metric value

1			6	4	....	1			6	4
Per Destination Flags			Destination Address #1	Destination Seq. Num.#1		Per Destination Flags			Destination Address #N	Destination Seq. Num.#N
DO #1	RF #1	Reserved				DO #N	RF #N	Reserved		

الشكل 2 بنية رسالة طلب الطريق في البروتوكول HWMP والراية الجديدة RF

إن الهدف من هذه الآلية السماح للعقدة بإيجاد المسار دون تأخير كبير بحيث تستطيع البدء بإرسال المعطيات، وعندما يتوافر مسار أفضل تقوم العقدة الهدف بالتغيير إلى المسار الجديد.

2.2 بناء الشجرة عن طريق رسالة الإعلان عن الجذر

تقوم العقدة الجذر دورياً بإرسال رسالة إعلان عن الجذر، تُستخدم المعلومات الموجودة في الرسالة لتقدير المسافة إلى العقدة الجذر.

ترسل كل عقدة تريد إنشاء المسار أو تحديثه إلى العقدة الجذر رسالة طلب مسار أحادية الوجهة unicast عن طريق العقدة العروية التي تسلمت الرسالة عن طريقها.

تعالج رسالة طلب المسار أحادية الوجهة بالقواعد نفسها لمعالجة رسالة طلب المسار التفاعلية.

تقوم العقدة الهدف بإرسال رسالة رد على المسار على كل رسالة طلب مسار تستقبلها.

تسمح رسالة طلب المسار أحادية الوجهة ببناء المسار العكسي من الجذر إلى العقدة العروية، في حين تتيح رسالة الرد على المسار بناء المسار المباشر من العقدة العروية إلى العقدة الجذر.

3.2 كلفة التسيير المعتمدة على الزمن اللازم لإرسال طرد Airtime Routing Metric

اقتُرِحَتْ هذه الكلفة لتكون كلفة افتراضية للأجهزة المشكلة للشبكة العروية (802.11s devices)، وذلك لتحقيق قابلية العمل البيني الأساسي basic interoperability بين العقد المصنعة من قبل شركات مختلفة.

تبرز هذه الكلفة الموارد المستهلكة من قناة راديوية حتى يتم إرسال إطار على وصلة محددة، بحيث يتم اختيار الطريق الذي يمثل أصغر مجموع للكلف الراديوية كأفضل طريق.

يتم حساب الكلفة الراديوية C_a على الشكل الآتي[1]:

$$C_a=[O_{ca}+O_p+\frac{B_t}{g}]\frac{1}{1-e_{pt}}$$

إذْ كلفة النفاذ إلى القناة الراديوية channel overhead O_{ca}، كلفة البروتوكول protocol overhead O_p، وB_t، هي ثوابت معرفة لكل تقنية إرسال IEEE a/b/g 802.11، حيث r المعدل بالميغابت في الثانية Mbit/s الذي سترسل به العقدة العروية إطار حجمه B_t، وذلك باعتبار الظروف الحالية للقناة بمعدل خطأ في الإرسال e_{pt} [1].

كما ذكرنا فإن الكلفة الراديوية هي الكلفة الافتراضية، ومن ثمَّ يستخدم HWMP هذه العلاقة لحساب كلفة كل وصلة وبالنتيجة حساب كلفة المسارات جميعها.

4.2 التعاون بين النمط التفاعلي والنمط الاستباقي

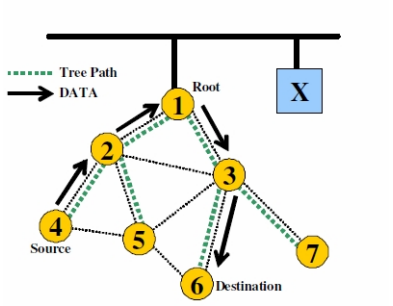
إذا لم يتم إعداد عقدة جذر في الشبكة اللاسلكية العروية، فإن العقد ستستخدم النمط التفاعلي لإيجاد المسارات إلى بعضها بعضاً.

ولكن في حال وجود عقدة جذر عندها يتم استخدام العقدة الجذر كوسيط لإيصال الطرود (لأنَّ معظم تدفق المعطيات في الشبكة باتجاه الشبكة السلكية أي عبر العقدة الجذر).

لا يعدُّ هذا الحل فعالاً efficient بالنسبة إلى العقد العروية ضمن الشبكة نفسها [5]، كما هو مبين في الشكل 3.

على سبيل المثال، إذا كانت العقدة 4 تملك معطيات تريد إيصالها إلى العقدة 6 عندها ستسلك المسار الموضح بالشكل وهو ←

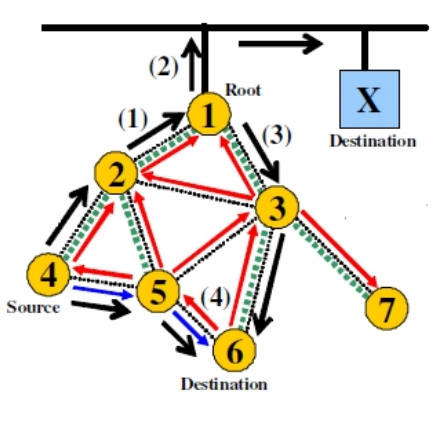
4 ← 2 ← 1 ← 3 ← 6، من الواضح أن هذا الطريق ليس أمثلياً (في حين الطريق أمثلي إلى العقدة الخارجية X).



الشكل 3 عدم استباقية التسيير الاستباقي في حال كانت العقدة الهدف داخل الشبكة

لحل هذه المشكلة التي تظهر عندما تجد العقدة الجذر أن كلاً من العقدة الهدف والمصدر تنتمي إلى الشبكة العروية، تقوم العقدة الجذر بتفعيل راية داخل الشبكة العروية interamesh flag (الموجودة في ترويسة التوسعة الخاصة بالشبكة العروية mesh extension header).

عندما تستقبل العقدة الهدف الطرد وتجد أن هذه الراية مفعلة، تقوم بإرسال رسالة طلب مسار إلى العقدة المصدر، كما هو موضح بالشكل 4.



الشكل 4 طريقة التعاون بين النمطين التفاعلي والاستباقي

بعد إتمام عملية اكتشاف الطريق تقوم العقد باستخدام المسار الأمثلي وهو المسار

4 ⟵ 5 ⟵ 6، أمَّا الطريق نحو العقدة الخارجية X فيبقى على حاله.

3. بروتوكولات التسيير الآمنة في الشبكات اللاسلكية العروية

على الرغم من إمكانية استخدام برتوكولات التسيير الخاصة بالشبكات التلاؤمية Ad Hoc في الشبكات اللاسلكية العروية، ولكن هذه البروتوكولات لا تعطي أداءً أمثلياً، ذلك لكون العقد في الشبكات اللاسلكية العروية ثابتة نسبياً، في حين تفترض بروتوكولات التسيير الخاصة بالشبكات التلاؤمية عكس ذلك.

يوجد عدد من بروتوكولات التسيير الخاصة بالشبكات التلاؤمية، والتي عُدِّلَتْ لكي تعمل في الشبكات اللاسلكية العروية، نذكر هنا أهم هذه البروتوكولات.

يوفر البروتوكول Secure Routing Protocol SRP [12]الحماية للبروتوكول Dynamic Source Routing DSR، وهو من بروتوكولات التسيير التفاعلية.

يفترض هذا البروتوكول وجود مفتاح مشترك بين كل زوج من العقد، إذْ يُستَخدَم المفتاح المشترك للتحقق من العقد الهدف والمصدر (لا توجد حاجة لوجود مفتاح مشترك مع العقد الوسيطة).
يستخدم هذا البروتوكول رقماً عشوائياً لكل طرد طلب مسار يقوم بإرساله، فضلاً عن عداد لرقم الطلب (فريد بين العقد الهدف والمصدر).

يتم استخدام رقم الطلب والعداد لحساب شفرة التحقق من الرسالة Message Authentication Code (في طرف العقدة المصدر)، ويتم التحقق منه في طرف العقدة الهدف [12].

يوفر هذا البروتوكول الحماية ضد عدد من الهجمات المعروفة على عملية التسيير، فضلاً عن استباقيية هذا البروتوكول، لكونه يستخدم المفاتيح التناظرية.

المشكلة في هذا البروتوكول أن التحقق يتم فقط في العقدة الهدف (لا تستطيع العقد الوسيطة التحقق من طرد طلب المسار أو الرد على المسار)، فضلاً عن عدم تحقيق الحماية للمعلومات القابلة للطفرة (قائمة العناوين الشبكية IP addresses) عند نشر الطرد ضمن الشبكة، مما يجعل هذا البروتوكول عرضة لهجوم انتحال الشخصية، و"هجوم سايبل".

البروتوكول Secure Multi-path Routing SecMR [13]، يخفف العبء الناتج عن تحقيق الحماية لعملية التسيير، وذلك من خلال تقسيم العمل إلى مرحلتين، أولاً التحقق المتبادل بين العقد المتجاورة، ومن ثم عملية التسيير.

الفكرة الرئيسية في هذا البروتوكول هي الاستفادة من تعدد المسارات بين العقد المصدر والهدف، ففي حال وجود N مسار غير متقاطع بين العقدة المصدر والهدف، يحتاج المهاجم N عقدة مخترقة لينفذ هجوم قطع الخدمة DoS (بشكل محدد أكثر يحتاج المهاجم عقدة مخترقة ضمن كل مسار).

يتألف هذا البروتوكول من مرحلتين، المرحلة الأولى هي التحقق من العقد المجاورة، يتم استخدام المفتاح العام للعقد لتقوم بالتحقق من بعضها (كل عقدة تمتلك شهادة موقعة من سلطة مانحة للشهادات الإلكترونية Certificate Authority CA) [13] .

المرحلة الثانية هي مرحلة اكتشاف المسار، حيث تقوم العقدة المصدر بإرسال طلب مسار في حال عدم وجود مسار للعقدة الهدف.

تقوم العقدة المصدر بتوليد مفتاح مشترك وتستخدم المفتاح العام للعقدة الهدف لتشفيره.

تعالج العقد الوسيطة في حال بروتوكولات التسيير التقليدية فقط أول نسخة من طرد طلب المسار، في حين تقوم العقد الوسيطة بمعالجة جميع الطرود القادمة من مسارات منفصلة في هذا البروتوكول (يحتوي كل طرد على قيمة تلبيد تُحسَبُ في كل خطوة).

عند استلام طرد طلب مسار أو رد على المسار، تقوم العقدة بالتحقق من كون العقدة السابقة (التي أرسلت الطرد) هي إحدى العقد المجاورة (الناتجة من المرحلة الأولى –التحقق من العقد المجاورة-).

يقوم هذا البروتوكول باكتشاف جميع المسارات غير المتقاطعة، وهو يعمل في أكثر من نمط.

في النمط الأول يقوم هذا البروتوكول باختيار أحد المسارات التي اكتُشِفَتْ، في حال حدوث خطأ في هذا المسار (نتيجة حركة العقد أو نتيجة فعل خبيث)، يتم اختيار مسار آخر.

إن هذا النمط هو الأقل كلفة والأقل أماناً، إِذْ إنَّ وجود عقدة مخترقة واحدة ضمن المسار الذي تم اختياره من الممكن أن يسبب قطع الخدمة (عملياً حتى يتم كشف العقدة المخترقة، أو حتى وصول تقرير من العقدة الهدف).

في النمط الثاني تُستَخدَمُ جميع المسارات التي اكتُشِفَتْ لإرسال طرود المعطيات.

إن هذا النمط هو الأكثر كلفةً كما أنه الأكثر أماناً، إذْ يتطلب وجود عقد خبيثة أو مخترقة بعدد المسارات، بحيث تقع كل عقدة ضمن مسار مختلف.

أمّا النمط الثالث فهو النمط الهجين، حيث يتم اختيار مجموعة من المسارات ليتم إرسال الطرود عبرها، وتستخدم العقدة المصدر التغذية الراجعة من العقدة الهدف لتغيير المسارات في حال وجود خطأ.

المشكلة في هذا البروتوكول هي الكلفة اللازمة لاكتشاف المسارات (زمن المعالجة).

يعمل البروتوكول Secure Multi-Path Hybrid Routing Protocol MHRP [14] على الشبكات العروية الهجينة (حيث يسهم الزبائن العروين في عملية التسيير)، بحيث يتألف هذا البروتوكول من مكون تفاعلي reactive يعمل ضمن الشبكة التلاؤمية المشّكلة من الزبائن العرويين، ومكون استباقي proactive يعمل ضمن البنية التحتية (المسيرات العروية).

يعمل هذا البروتوكول ضمن الشبكات اللاسلكية العروية الهجينة، إذْ من الممكن أن تشكل الزبائن العروية شبكة تلاؤمية Ad Hoc، بحيث تعتمد العقد على بعضها للوصول إلى أقرب مسير عروي.

كما ذكرنا، يتألف هذا البروتوكول من عدة مكونات أهمها، المكون الاستباقي الذي يعمل ضمن البنية التحتية (وذلك لكون العقد ضمنها ثابتة)، ومكون تفاعلي يعمل ضمن الشبكة التلاؤمية [14].

يفترض هذا البروتوكول وجود سلطة موثوق بها مانحة للشهادات الإلكترونية Certificate Authority، بحيث تمتلك كل عقدة زوجاً من المفاتيح (مفتاح عام ومفتاح خاص) الموقعة من هذه السلطة، تُستَخدَمُ المفتاح الخاص للتحقق المتبادل بين العقد (الزبائن والمسيرات).

ثم يُحسَبُ مفتاح مشترك (عن طريق خوارزمية Diffie-Hellman).

كما يقوم المسير العروي بتوزيع مفاتيح محسوبة عن طريق سلاسل التلبيد Hash Chain للزبائن العروية، تُستَخدَمُ فيما بعد لاكتشاف المسارات.

يقوم هذا البروتوكول بتخزين المسارات المنفصلة، بحيث يتم اختيار أفضل مسار للاستخدام الحالي، وعند حدوث خطأ يتم اختيار مسار آخر.

يزيد هذا البروتوكول التغطية الكلية للشبكة العروية، إذْ لا يشترط أن يكون الزبون العروي ضمن مجال البث للمسير العروي، بل يكفي أن يقع الزبون العروي ضمن مجال البث لزبون آخر يستطيع النفاذ إلى الشبكة العروية.

كما رأينا يستخدم هذا البروتوكول بنية المفتاح العام للتحقق من كل من الزبائن والمسيرات العروية، لا يعدُّ ذلك مشكلة في طرف المسيرات (بوصفها غنية بالموارد)، أما الزبائن العروية فهي محدودة الموارد (وهنا تكمن المشكلة)، إذْ من الممكن أن يستغل المهاجم ذلك لشن هجوم قطع الخدمة على الزبون العروي.

فضلاً عن حدوث تأخير زمني عندما تكون العقدة الهدف والمصدر في شبكات تلاؤمية مختلفة.

يستخدم البروتوكول Secure Hybrid Wireless Mesh Protocol [15] بنية المفاتيح المعرفة ضمن المعيار IEEE 802.11S، ومن ثمَّ لا يضيف عبئاً على الشبكة لتوفير الحماية لعملية التسيير. يُستَخدَمُ مفتاح المجموعة Group Transient Key GTK لتوفير الحماية لطرود طلب المسار والإعلان عن الجذر، في حين يستخدم المفتاح المشترك مع العقدة المجاورة Pairwise Transient Key PTK لتحقيق الحماية لطرود الرد على المسار.

يحقق البروتوكول السابق الذكر الحماية من الهجمات التي تشنها العقد الخبيثة (التي لا تنتمي إلى الشبكة العروية)، بينما لا يوفر الحماية من العقد المخترقة compromised والتي تنتمي إلى الشبكة العروية (يمكن للمهاجم التغيير على برمجيات الموجه العروي، بسبب عدم وجود آمن فيزيائي للعقد المشكلة للشبكة العروية-توجد المسيرات العروية على أعمدة الإنارة ومن ثمَّ يستطيع المهاجم الوصول إليها).

4. المتطلبات الأمنية لعملية التسيير

في معظم التطبيقات الأمنية، الخدمة الأمنية الأهم هي مَن يملك السماحية authorization، وعملية التسيير ليست استثناءً، عملياً يجب أن يتخذ المسير قراراً بشأن نوعين من السماحيات.

النوع الأول: سماحية الاستيراد import authorization فعندما يستقبل المسير تحديثاتٍ خاصة بالتسيير routing updates من العالم الخارجي، يجب أن يقرر هل سيقوم بتعديل جدول التسيير وفقاً لذلك؟.

النوع الثاني: سماحية التصدير export authorization وذلك عندما يستقبل المسير طلباً لمعلومات التسيير.

الأهم بالنسبة إلينا بما يخص الشبكات العروية هو سماحيات الاستيراد.

يحتاج تحديد السماحيات إلى خدمات أمنية أخرى مثل الاستيقان authentication وسلامة المعطيات integrity، تُستخدم تقنيات مثل التوقيع الرقمي digital signature وشفرة استيقان الرسالة message authentication code لتحقيق هذه الخدمات، في حين لا تعدُّ السرية confidentiality وعدم النكران non-repudiation خدمات أمنية ضرورية.

ومن ثمَّ المتطلبات التالية هي الأهم [2]:

- **ü** سماحيات الاستيراد import authorization: لا يقصد بالسماحيات هنا المعنى الحرفي لها، فالمقصود بذلك أن المسؤول النهائي عن رسائل التسيير الخاصة بعقدة هدف ما هي العقدة نفسها، لذلك لا يتم وضع معلومات التسيير ضمن جدول التسيير إلا بعد التحقق من أن هذه المعلومات أُرسِلَتْ من قبل العقدة المعنية، في هذه الحالة إذا قامت العقدة الخبيثة بتزوير المعلومات المرسلة، تكون النتيجة عدم قدرة العقد الأخرى على توجيه المعطيات باتجاهها.
- **ü** استيقان المصدر :source authentication يجب أن تمتلك العقد القدرة على التحقق من أن العقدة التي تم وضعها كمصدر للرسالة هي نفسها العقدة التي أرسلت الرسالة.
- **ü** سلامة المعطيات: كذلك يجب أن تمتلك العقد القدرة على التحقق من أن رسائل التسيير وصلت دون أي تغيير.
- **ü** مزج آخر خدمتين أمنيتين يحقق وثوقية المعطيات، وهو شرط مشتق من سماحيات الاستيراد.

5. بروتوكول التسيير الأمن للشبكات اللاسلكية العروية *SecHWMP

كما ذكرنا، يعدُّ البروتوكول HWMP تطويراً على البروتوكول AODV، لذلك قمنا بتحقيق الحماية للبروتوكول HWMP، بتطوير الحل الأمني للبروتوكول AODV.

نستطيع من خلال توصيف البروتوكول SAODV [16]، الذي يعتمد على سلاسل التلبيد Hash Chain والتوقيع الرقمي Digital Signature، تحقيق الحماية لرسائل البروتوكول HWMP. ولكن يبقى لدينا تحقيق الحماية للإضافات التي تمت على البروتوكول AODV حتى نتج لدينا البروتوكول HWMP.

يفترض البروتوكول SHWMP [15] وجود ثقة بالعقد الوسيطة، فبمجرد امتلاك العقدة لمفتاح المجموعة GTK يسمح لها بفك تشفير رسالة طلب المسار، ثم إجراء التعديلات، ثم تشفير الرسالة ومن ثم إعادة بثها.

يعدُّ ذلك مشكلة لوجود نقص في الأمن الفيزيائي للموجهات العروية (وجود الموجهات العروية على أعمدة الإنارة).

بينما وجود التوقيع الرقمي في البروتوكول SecHWMP لا يفترض وجود ثقة في العقد الوسيطة، إذْ تستطيع هذا العقد تغيير الحقول المتغيرة فقط.

يعدُّ النمط التفاعلي الموصف للبروتوكول* HWMP هو نفسه توصيف البروتوكول AODV مع بعض الإضافات:

1. يوجد حقل ضمن كل من رسالة طلب المسار، ورسالة الرد على المسار، يدل على الكلفة التراكمية للمسار، يجب تحقيق الحماية لهذا الحقل على اعتبار أنه قابل للتغيير mutable.
2. يسمح البروتوكول HWMP أن تحتوي رسالة طلب المسار على أكثر من عقدة هدف (العقد التي نبحث عن مسار باتجاهها)، بحيث إنَّه عندما تقوم العقدة بالرد على طلب المسار لعقدة معينة (إما العقدة الهدف أو عقدة وسيطة تمتلك المسار للعقدة الهدف) تقوم بحذف عنوان العقدة الهدف الموافقة من قائمة العقد التي نبحث عن مسار باتجاهها.
3. يمثل ذلك مشكلة لدينا إذْ إنَّ حذف أأي جزء من الرسالة سيؤدي إلى تغير التوقيع الرقمي للرسالة (لا يحق للعقد الوسيطة تغيير الرسالة، سماحيات الاستيراد كما توضح ذلك الفقرة 4).
4. يجب تأمين الحماية للرايات الخاصة بكل عقدة هدف per destination flags مع الأخذ بالحسبان أن قيمة هذه الحقول متغيرة.
5. لمّا كانت كلفة المسار أصبحت كلفة التسيير الراديوية Airtime Routing Metric، وليس عدد القفزات Hop count، كما هو الحال في البروتوكول AODV، فيجب أيضاً تأمين الحماية لعملية حساب الكلفة، بحيث لا يقوم المهاجم بالتلاعب بها.

قمنا خلال البحث بدراسة الحل الأمني لكل من الإضافات السابقة:

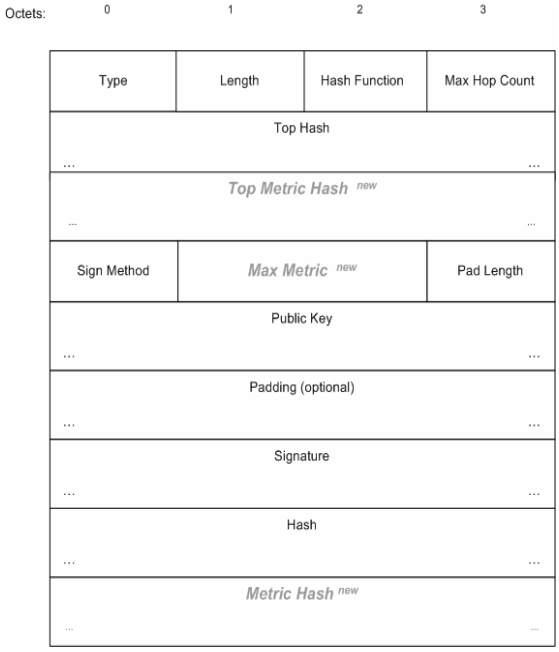
* البروتوكول Secure Hybrid Wireless Mesh Protocol SHWMP [15]، مختلف تماماً عن البروتوكول الذي قمنا بتوصيفه

- يمكن تحقيق الحماية للحقل الدال على قيمة الكلفة بطريقة تحقيق الحماية نفسها لعدد القفزات (سلاسل التلبيد)، ولكن المشكلة أن قيمة الكلفة كبيرة، ومن ثمَّ سيكون عدد مرات
- التلبيد اللازم لحساب القيمة العليا للتلبيد كبيراً، يمكننا أخذ الناتج الصحيح للقسمة على ثابت (دراستنا التجريبية على المحاكي دلت أن القيمة 100 تعطي نتائج جيدة).
- بالنسبة إلى عملية حذف العقدة بعد إرسال رسالة الرد على المسار، فيوجد حلان لهذه المشكلة، الحل الأول يكمن في أن نقوم بتوقيع الرسالة ككل، وعندها لا تستطيع العقد الوسيطة إجراء أي تغيير (تتوقف عملية البحث عندما تصل الرسالة إلى كل العقد في الشبكة)، أمَّا الحل الثاني فيكمن بإضافة أكثر من توقيع إلى الرسالة (توقيع لكل عقدة هدف) عندها تستطيع العقدة التي تقوم بإرسال رسالة رد على المسار حذف العقدة الهدف من قائمة العقد التي نبحث عن مسار باتجاهها، بالطبع هذا الحل يتطلب العديد من عمليات التوقيع (التي تعدُّ مكلفة حسابياً).
- يمكن تأمين الحماية للرايات الخاصة بكل عقدة هدف باستخدام التوقيع الرقمي.
- بالنسبة إلى تحقيق الحماية لحساب الكلفة، يمكن الاعتماد على عملية الحماية المعرفة في المعيار IEEE 802.11S (يتم التحقق من العقد المتجاورة، وتوليد المفاتيح المشتركة باستخدام IEEE 802.11i).

بالنسبة إلى لنمط الاستباقي، قمنا بتمييز الشهادة الرقمية للعقدة الجذر، ومن ثمَّ لن تتمكن أي عقدة مهاجمة من انتحال هوية العقدة الجذر.

كذلك قمنا بتحقيق الحماية لرسالة الإعلان عن الجذر root announcement بطريقة تحقيق الحماية نفسها لرسالة طلب المسار.

يوضح الشكل 5 الحقول التي قمنا بإضافتها إلى رسالة طلب المسار من البروتوكول SAODV، وهي القيمة العليا لتلبيد الكلفة Top Metric Hash، القيمة العظمى للكلفة Max Metric، وقيمة تلبيد الكلفة Metric Hash.



الشكل 5 الحقول التي قمنا بإضافتها إلى رسالة طلب المسار من البروتوكول SAODV

6. المحاكاة

على الرغم من أن المحاكي الشبكي Network NS-2 Simulator 2 [7] ذو شهرة واسعة، فهو لا يحتوي على دعم للشبكات اللاسلكية العروية.

في البداية قمنا بإضافة توسعة extension إلى المحاكي NS-2 توفر الدعم للشبكات اللاسلكية العروية [13]، فضلاً عن دعم استخدام أكثر من بطاقة شبكة

واحدة، بحيث تعمل هذه البطاقات على أقنية راديوية مختلفة [9].

المشكلة في هذه المكتبة المضافة أنها لا تحتوي على تنجيز لبروتوكول التسيير الهجين للشبكات اللاسلكية العروية HWMP، كما أن التسيير يتم على مستوى الطبقة الثالثة (طبقة الشبكة)، خلافاً لتوصيف هذا البروتوكول، حيث يتم التسيير على مستوى الطبقة الثانية، كما ذكرنا سابقاً.

لذلك قمنا باستخدام المحاكي الشبكي Network Simulator 3 NS-3 [6]، الذي يحتوي على دعم كامل للشبكات اللاسلكية العروية (يدعم وجود أكثر من بطاقة شبكة واحدة، كما يحتوي على تنجيز للبروتوكول الهجين للشبكات اللاسلكية العروية).

يعدُّ NS-3 محاكياً منفصل الأحداث discrete-event لأنظمة الانترنت، وهو موجه بشكل رئيسي للبحوث والاستخدام الأكاديمي.

هذا المحاكي مفتوح المصدر open source، وهو مرخص ضمن الترخيص العام GNU General Public License.

يستخدم المحاكي الشبكي NS-3 لغة البرمجة C++ كلغة للتطوير، خلافاً للمحاكي NS-2 الذي يستخدم TCL كلغة للتخاطب (scripting) مع الأغراض الناتجة من لغة التطوير C++، يستخدم المحاكي NS-3 لغة البرمجة C++ نفسها للتخاطب مع الأغراض.

قمنا بمكاملة integration المكتبة Libgcrypt [10] مع المحاكي الشبكي NS3، هذه المكتبة أيضاً مفتوحة المصدر، وهي مرخصة للاستخدام ضمن شروط الترخيص العام GNU، ويمكن الحصول على تفصيلات ذلك في المرجع [11].

تحتوي هذه المكتبة على توابع التشفير غير المتناظر public key or asymmetric cryptography (RSA, Elgamal, ECC) (بالتأكيد يتضمن ذلك التوقيع الرقمي digital signature)، والتشفير المتناظر symmetric cryptography (AES, 3DES, IDEA ..etc)، فضلاً عن توابع التلبيد Hash (SHA1, SHA256, MD5, MD4 ..Etc).

7. مقارنة أداء بروتوكولات التسيير الآمنة

قمنا بمقارنة أداء بروتوكول التسيير الآمن الهجين للشبكات اللاسلكية العروية، وكل من بروتوكولات التسيير الآمنة SRP [12]، SecMR [13]، MHRP [14].

فالبروتوكول SRP يوفر الحماية للبروتوكول DSR، والأخير يعدُّ من أشهر بروتوكولات التسيير في الشبكات التلاؤمية، فضلاً عن كونه مستخدماً في الشبكات اللاسلكية العروية.

البروتوكول SecMR يستفيد من تعدد المسارات غير المتقاطعة في الشبكات اللاسلكية العروية، ومن ثمَّ يحقق مستوى عالي من الحماية عندما يعمل في النمط الثاني.

أما البروتوكول MHRP فهو مصمم خصّيصى للشبكات اللاسلكية العروية، وهو يزيد التغطية الكلية للشبكات اللاسلكية العروية.

قمنا بإجراء المحاكاة على بيئة اختبار افتراضية تتكون من 16 موجهاً عروياً، 49 زبوناً عروياً متحركاً.

تم توزيع الزبائن العروية بشكل عشوائي ضمن مساحة 1000*1000 متر مربع، كل زبون عروي مزود ببطاقة شبكة مجال الإرسال الخاص بها 150 متراً، وسعة الوصلة 2 Mbps، زمن المحاكاة 900 ثانية.

كما ذكرنا يتحرك الزبائن العرويون، بسرعة 20mps، أو قد يكونون ثابتين (السرعة =0mps).

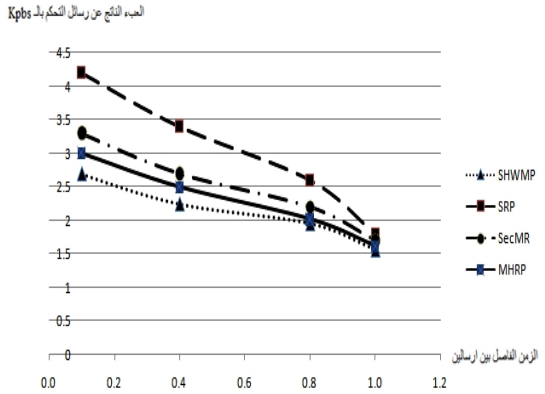
قمنا باختيار 16 من الزبائن العرويين حتى يقوموا بإرسال المعطيات، حجم طرد المعطيات 512 بايت، استخدمنا معدل تدفق ثابت Constant Bit Rate CBR، وقمنا بتغيير الزمن الفاصل بين إرسالين متتاليين packet inter-arrival time.

قمنا بحساب العبء باعتبار عدد طرود طلب المسار، والرد على المسار، وخطأ في إذْ إنَّ أن طول كل من هذه الطرود معروف، ثم قمنا بحساب الوسطي بالنسبة إلى جميع العقد.

$$\text{Throughput}=\frac{\sum_{k=0}^{16} 512*8*NoPackets_k}{16}$$

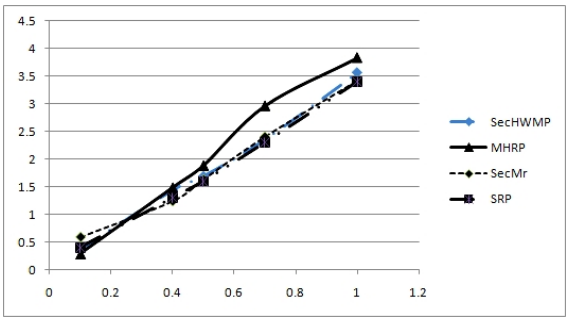
إذْ $NoPackets_k$ هو عدد الطرود التي استُقبِلَتْ عند العقدة المصب k، لحساب المردودية حُسِبَ الوسطي لعدد الطرود المستقبلة عند جميع العقد المصب بعد أخذ ناتج الضرب بالقيمة 512 التي تمثل طول الطرد بالبايت والضرب بالقيمة 8 لتحويل إلى بت.

يوضح الشكلان 6 و 7 نتائج المحاكاة.



الشكل 6 مقارنة العبء الناتج عن بروتوكولات التسيير بالنسبة إلى الزمن الفاصل بين إرسالين

يمثل الشكل 6 مقارنة للعبء الناتج عن بروتوكولات التسيير المختلفة، نلاحظ من الشكل أن العبء الناتج عن هذه البروتوكولات متقارب، على الرغم من كون العبء الناتج عن البروتوكول SecHWMP هو الأقل، ذلك لكون هذا البروتوكول تفاعلياً، فضلاً عن عدم وجود قائمة بالعقد الوسيطة (كما هو الحال في البروتوكول SRP، فهو بروتوكول تفاعلي ولكن رسالة طلب المسار تحتوي قائمة بالعقد الوسيطة مما يؤدي إلى زيادة العبء).



الشكل 7 مقارنة مردودية الشبكة بالنسبة إلى كل من بروتوكولات التسيير بالنسبة إلى الزمن الفاصل بين إرسالين

يمثل الشكل 7 مقارنة لأداء بروتوكولات التسيير (المردودية)، نجد أن أداء البروتوكولات متقارب، حيث يكون أداء البروتوكولات نفسه تقريباً عندما

يكون حمل الشبكة خفيفاً، ويصبح أداء البروتوكول MHRP الأفضل عندما يزداد حمل الشبكة.

يتميز البروتوكول SecHWMP بكون العقد الوسيطة قادرة على التحقق من العقدة المصدر، في حين لا يمكن للعقد الوسيطة في البروتوكول SRP التحقق من العقدة المصدر، مما يسمح بعدد من الهجمات مثل هجوم انتحال الشخصية، وهجوم "سايبل".

على الرغم من كون العقد الوسيطة غير قادرة على التحقق من العقدة المصدر في البروتوكول SecMR، ولكن وجود آلية للتحقق من العقد المجاورة يسمح بتخفيف أثر المشكلة السابقة.

أمَّا بالنسبة إلى لبروتوكول MHRP، فمردوديته أفضل من SecMR و SRP، ولكن استخدام المفتاح العام للتحقق من الزبائن، والتأخير الزمني عندما تكون العقد في شبكات تلاؤمية مختلفة، يخلق بعض المشاكل ضمن هذا البروتوكول.

بالنتيجة فإن بروتوكول التسيير الآمن الهجين يحقق حماية ضد العديد من الهجمات (كما سنرى لاحقاً)، كما لا يسبب عبئاً كبيراً في الشبكة، فضلاً عن كون مردودية الشبكة جيدة مقارنة ببروتوكولات التسيير الأخرى.

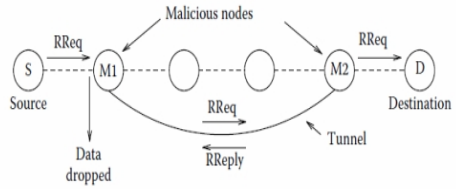
بالطبع استخدام التشفير غير المتناظر يسبب بعض التأخير الزمني (عمليات التشفير غير المتناظر مكلفة زمنياً)، ولكن يقتصر استخدام التشفير غبر المتناظر على الموجهات العروية (وهي غنية بالموارد).

8. الدراسة التحليلية للبروتوكول الهجين الآمن للشبكات اللاسلكية العروية

يتعرض التسيير لعديد من الهجمات أشهرها:

1. هجوم الممر الدودي wormhole يعتمد على فكرة وصل بين جسمين غير متصلين أساساً.

خلال هذا الهجوم تقوم عقدتان أو أكثر بالتآمر سوياً من خلال تأسيس قناة باستخدام وسيط اتصال عالي الفاعلية (اتصال سلكي أو اتصال لا سلكي مرتفع السرعة) كما هو موضح في الشكل 8، في أثناء مرحلة اكتشاف الطريق في بروتوكولات التسيير التفاعلية، تُمرَّرُ رسالة طلب الطريق بين العقدتين الخبيثتين باستخدام القناة السريعة التي تم إنشاؤها، لذلك فإن أول رسالة طلب طريق تصل إلى العقدة الهدف تكون الرسالة التي أُرسِلَتْ من قبل العقد المهاجمة، بالنتيجة فقد تم إضافة العقد المهاجمة في الطريق الواصل بين العقدة الهدف والمصدر، بعدها إما أن تقوم العقد المهاجمة برمي جميع الطرود مما يسبب بقطع كامل للخدمة، أو أن تقوم برمي الطرود انتقائياً كي لا يتم اكتشافها [2].

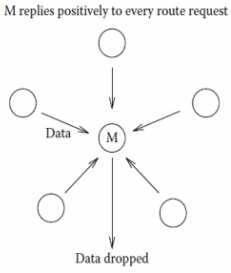


الشكل 8 هجوم الممر الجحري يتم شن هذا الهجوم من قبل العقدتين M1 و M2، تستخدم هاتان العقدتان قناة اتصال سريعة لنقل طرود التحكم، في حين يتم رمي طرود المعطيات.

2. هجوم الثقب الأسود black hole (أو هجوم المصب sink attack) هو هجوم يؤدي إلى قطع الخدمة في الشبكات اللاسلكية العروية، فضلاً عن أنه يستغل آلية اكتشاف الطريق في بروتوكولات

التسيير التفاعلية، ففي هذا الهجوم تقوم العقدة المهاجمة بالإجابة دائماً عن رسالة طلب الطريق على الرغم من أنها لا تمتلك طريقاً صالحاً باتجاه العقدة الهدف.

3. نظراً إلى أنَّ العقدة المهاجمة لا تفحص جدول التسيير الخاص بها، فستكون دائماً العقدة الأولى التي ترد على رسالة طلب الطريق، بالنتيجة فإن معظم الطرود الخاصة بالعقد المجاورة للعقدة المهاجمة سيتم تسييرها إلى العقدة المهاجمة، والتي تقوم برمي الطرود مما يؤدي إلى قطع الخدمة، يوضح الشكل 9 تأثير هجوم الثقب الأسود على العقد المجاورة للعقدة المهاجمة، حيث يتم تسيير معظم الطرود الخاصة بالعقد المجاورة للعقدة المهاجمة.



الشكل 9 تقوم العقدة المهاجمة M بالرد دائماً على رسائل طلب الطريق، بالنتيجة كل الطرود يتم تسييرها إلى هذه العقدة، التي تقوم لاحقاً برميها

4. هناك شكل أكثر تعقيداً لهذا الهجوم، حيث تتآمر مجموعة من العقد مع بعضها، مما يؤدي إلى تشويه كامل لعملية التسيير وتوجيه الطرود في الشبكة [2].
5. يعدُّ هجوم الثقب الرمادي grey hole attack شكلاً آخرَ لهجوم الثقب الأسود، فبدلاً من رمي جميع الطرود، تقوم العقدة المهاجمة برمي الطرود اختيارياً.
6. يؤدي ذلك إلى قطع الخدمة بشكل جزئي، ولكن المهاجم يتفادى أن يتم اكتشافه، إذْ إنَّ رمي الطرود بشكل اختياري يمكن أن يعدُّ اختناقاً في الشبكة، ومن ثمَّ يتفادى المهاجم الاكتشاف مدة أطول [2].

تمنع سلاسل التلبيد المهاجم من التلاعب بكل من عدد القفزات، وقيمة الكلفة.

بالطبع يستطيع المهاجم زيادة قيمة هذه الحقول، ولكن لا يعدُّ ذلك مشكلة لأنه من الأفضل بالنسبة إلى العقد السلمية أن لا يعبر المسار من العقدة الخبيثة malicious node.

لا يستطيع المهاجم إنقاص عدد القفزات أو قيمة الكلفة (كون ذلك يتطلب حساب القيمة العكسية للتلبيد reverse hash)، ومن ثمَّ لا يستطيع المهاجم إجبار عملية اكتشاف المسار لتعبر من خلاله.

الهجمات المعروفة على هذا البروتوكول هي، أولاً من الممكن أن يقوم المهاجم بإعادة بث طرد طلب المسار أو طرد الرد على المسار دون أن يقوم بزيادة عدد الخطوات والكلفة.

يتطلب كشف هذا الهجوم نظام كشف عن الاختراقات Intrusion Detection System IDS (يجب أن تقوم العقدة بالتصنت عند إرسال طرد طلب المسار، في حال قامت إحدى العقد المجاورة بإعادة بث الطرد دون زيادة عدد القفزات والكلفة فهي عقدة خبيثة).

الهجوم الثاني يتمثل في هجوم الممر الجحري worm hole، وهجوم النفق tunnel attack، يتطلب كشف كل من هاتين الهجمتين أيضاً نظام كشف عن الاختراقات.

يمنع التوقيع الرقمي العقد الخبيثة من تزوير أو انتحال شخصية العقد السليمة، ومن ثمَّ يمنع هجمات الثقب الأسود والثقب الرمادي، إذْ يجب أن تمتلك العقدة المهاجمة المفتاح الخاص للعقدة الهدف حتى تتمكن من تزوير الرسالة.

أمَّا رسائل الخطأ فكل عقدة تولد أو تقوم بإعادة بث رسالة الخطأ، توقع الرسالة ككل، ومن ثمَّ تستطيع العقد المستقبلة التحقق من هوية المرسل، في حال كانت العقدة المرسلة هي القفزة التالية على المسار، تقوم العقدة الحالية بتعليم المسار على أنه غير صالح.

لن تقوم العقدة المهاجمة بتزوير طرد خطأ في الطريق (من مصلحة العقدة المهاجمة أن تسيطر على أكبر قدر ممكن من المسارات، حتى تقوم بمراقبة الطرود أو قطع الخدمة عن العقد الضحية).

بالنسبة إلى النمط الترقبي من البروتوكول HWMP، فهو يستخدم طرد طلب مسار استباقي (وهو نفسه طرد طلب المسار العادي مع راية flag تدل على كونه استباقياً proactive)، ومن ثمَّ يتم تحقيق الحماية لهذا الطرد بطريقة تحقيق الحماية نفسهاغ للطرد طلب المسار العادي، لكن من الضروري أن تستطيع العقد في الشبكة تمييز المفتاح العام للعقدة الجذر، ومن ثمَّ لا تتمكن العقدة المهاجمة من انتحال هوية العقدة الجذر.

الخلاصة:

يعدُّ التسيير حجر الزاوية في الشبكات اللاسلكية العروية، فباعتبار حقيقة أن العقد تعتمد على بعضها بعضاً لتشكيل البنية التحتية للشبكة، يجب أن تقوم العقد بالتعاون والتنسيق فيما بينها لضمان استمرارية الشبكة.

من الممكن لمهاجم واحد فقط أن يقوم بقطع الخدمة عن جزء كبير من الشبكة بتغيير على بروتوكول التسيير ضمن المسيّر العروي (وهو موجود فيزيائياً لدى المهاجم في حالة الشبكات المجتمعية أو يمكن للمهاجم الوصول إليه بوصفه غير محمي فيزيائياً، ومن ثمَّ يعدُّ تغيير سلوك المسيّر العروي أمراً غير معقدً).

هنا تظهر الحاجة إلى بروتوكول تسيير آمن، إذْ إنَّ بروتوكول التسيير الآمن الهجين للشبكات العروية SecHWMP الذي قمنا بتنجيزه يحقق الحماية ضد الهجمات السابقة الذكر.

يمنع التحقق الرقمي المهاجم من تزوير الرسائل، فضلاً عن سلاسل التلبيد التي تمنع المهاجم من التلاعب بكلفة التسيير، ومن ثمَّ تمنع المهاجم من السيطرة على معطيات الزبائن ومراقبتها (أي تحتوي معظم المسارات بين عقد الشبكة العقدة المهاجمة كعقدة وسيطة).

كما أن أداء هذا البروتوكول أفضل من باقي البروتوكولات الآمنة ضمن الشبكات اللاسلكية العروية عندما يكون الحمل كبيراً.

و بالطبع يُعدّ بروتوكول التسيير الآمن خطوة مهمة لتحقيق الحماية للشبكة اللاسلكية العروية، ولكن ذلك لا يشمل التحقق من سماحية الزبائن العرويين (التحقق من حق الزبون العروي بالنفاذ إلى الشبكة العروية)، فضلاً عن منع هجوم حقن طرود وهمية مكررة.

نجد مما سبق أن تحقيق الحماية لرسائل التسيير أمر ضروري لضمان ديمومة الشبكة اللاسلكية العروية، وهذا شرط أساسي للحصول على شبكة منيعة ضد الهجمات، وقادرة على إعادة البرمجة الذاتية.

الآفاق المستقبلية

قمنا بتنجيز التوسعة الآمنة المفردة Single Security Extension، ولم نقم بتنجيز التوسعة الآمنة المزدوجة Double Security Extension، التي تسمح للعقد الوسيطة بالرد على رسالة طلب المسار.

كما رأينا تمنع التوسعة الآمنة عدداً لا بأس به من الهجمات الممكنة على عملية التسيير، ولكنها لا تحقق الحماية من الهجمات الناتجة عن التعاون بين العقد الخبيثة. لذلك من الضروري دراسة نظام كشف الاختراقات IDS، بحيث يصبح من الممكن كشف العقد الخبيثة، وتنبيه مدير الشبكة Administrator.

كذلك لا بد من وجود آلية لاكتشاف الطرود المكررة والوهمية، حيث تعدُّ العقد الوسيطة هذه الطرود حقيقية وتقوم بتسييرها حتى تصل إلى لعقدة الهدف.

بالطبع، تمتلك العقدة الهدف القدرة على التحقق من كون الطرد مكرراً، ولكن المشكلة تمكن في الموارد التي استهلكتها العقد الوسيطة حتى قامت بتسيير هذا الطرود.

المراجع

[1] Y. Zhang, J. Luo, and H. Hu, "Wireless Mesh Networking: Architectures, Protocols and Standards", Auerbach Publications, 2007.

[2] Y. Zhang, J. Zheng, and H. Hu, "Security in Wireless Mesh Networks", CRC Press, 2008.

[3] C. E. Perkins and E. M. Royer, "Ad Hoc On-Demand Distance Vector Routing", Proceedings of IEEE Workshop on Mobile Computing Systems and Applications, pp. 90–100, February 1999.

[4] IEEE P802.11s/D2.0-Draft STANDARD for Local and Metropolitan Area Networks – Specific Requirements- Amendment to Part 11: Mesh Networking, November 2006.

[5] Won-Ju Yoon, Sang-Hwa Chung, and Seong-Joon Lee, "An Efficient Cooperation of On-demand and Proactive Modes in Hybrid Wireless Mesh Protocol", IEEE LCN 2008.

[6] Network Simulator 3 NS-3,

http://www.nsnam.org, accessed Jan 2010

[7] Network Simulator 2 NS-2,

http://www.isi.edu/nsnam/ns/, accessed Nov 2009.

[8] Extensions to ns-2,

http://www.q2s.ntnu.no/~paquerea/ns.php, accessed Dec 2009.

[9] Laurent Paquereau," Extensions to ns-2 Notes and Documentation", July, 2009.

[10] Werner Koch, Moritz Schulte, "The Libgcrypt Reference Manual",

accessed Feb 2010.

[11] Libgcrypt, basic cryptographic library, http://www.gnupg.org/download/, accessed Feb 2010.

[12] P. Papadimitratos and Z. Haas, "Secure routing for mobile ad hoc networks", In Proceedings of the SCS Conference (CNDS) (TX, San Antonio), January 2002.

[13] P. Kotzanikolaou, R. Mavropodi, and C. Douligeris, "Secure multipath routing for mobile ad hoc networks", Proceedings of the WONSS05 Conference (St. Moritz, Switzerland) IEEE, January 19-21 2005.

[14] M. Siddiqui, S. Amin, "MHRP: A Secure Multi-Path Hybrid Routing Protocol for Wireless Mesh Network", IEEE MILCOM, Oct. 2007.

[15] Md. Islam, Y. Yoon, Md. Hamid, and C. Hong, "A Secure Hybrid Wireless Mesh Protocol for 802.11s Mesh Network", Springer-Verlag Berlin Heidelberg, 2008.

[16] M. Guerrero Zapata. "Secure ad hoc on-demand distance vector (SAODV) routing", work in progress. —INTERNET-DRAFT draft-guerrero-manet-saodv-06.txt, Sept 2006.

تاريخ ورود البحث إلى مجلة جامعة دمشق 2010/6/17