طريقة جديدة لتأمين اتصال المجموعة في الشبكات التطبيقية متعددة البث

د. مثنى القبيلي•

(تاريخ الإيداع 2 / 6 / 2020. قُبِل للنشر في 17/ 9 / 2020)

□ ملخّص □

ظهرت تقنية الإرسال المجموعاتي عندما تزايد استخدام الأنترنت بشكل كبير، بحيث أصبحت تقنية الإرسال وحيد الاتجاه غير فعالة في ذلك، فمع هذا النمو السريع في استخدام الأنترنت تزايدت الحاجة إلى التوسع في تطبيقاته لتشمل التلفزيون عبر الانترنت والتعليم عن بعد والفيديو كونفرنس وغيرها الكثير من التطبيقات التي تحتاج إلى عرض حزمة كبير.

ولكن في الواقع واجهت تقنية البث المجموعاتي جملة من التحديات التي حالت دون انتشارها كان منها التجارية والأمنية. لذلك تم اقتراح تقنية جديدة تدعى الشبكات التطبيقية متعددة البث والتي تعتمد على فكرة بناء شجرة تغطية من المستخدمين النهائيين كركيزة لإضافة خدمات شبكية جديدة ونشرها، أو لتوفير طوبولوجيا خاصة للتوجيه غير متوافرة في الشبكة الفيزيائية الأساسية. والهدف من ذلك سهولة إدارة مجموعاته وتنظيم العلاقات بين أعضاء هذه المجموعات، ومن ثم يصبح تحقيق الأمن أكثر سهولة مما هو عليه في البث المجموعاتي. وبما أن تحقيق سرية المعلومات يشكل تحدياً كبيراً، لذلك توجهت الكثير من الأبحاث نحو هذا الموضوع، واعتمدت بشكل أساسي على مفاتيح التشفير، لذا يتركز الموضوع على إدارة هذه المفاتيح ودراسة تأثيرها في حمل الشبكة.

يهدف هذا البحث إلى اقتراح طريقة جديدة لإدارة مفاتيح التشفير في الشبكات التطبيقية متعددة البث ومقارنته مع كل الطرائق الموجودة في هذه الشبكات. أظهرت نتائج المحاكاة فعالية الطريقة الجديدة من خلال دراسة تأثيرها في حمل الشبكة وعلى عدد عمليات تشفير/فك تشفير البيانات.

الكلمات المفتاحية : البث المجموعاتي، الشبكات التطبيقية متعددة البث، سرية البيانات، إدارة مفاتيح التشفير، حمل الشبكة الزائد.

• أستاذ مساعد، قسم هندسة الاتصالات والالكترونيات، كلية الهندسة الميكانيكية والكهربائية، جامعة تشرين، اللاذقية، سورية.
mothanna.alkubeily@gmail.com

A New Scheme to Secure Group Communication in Application-Level Multicast Networks

Dr. Mothanna Alkubeily*

(Received 2 / 6 / 2020. Accepted 17 / 9 / 2020)

□ ABSTRACT □

IP Multicast technology appeared when the use of the Internet increased dramatically, so that the one-way transmission technology became ineffective in that. With this rapid growth in the use of the Internet, the need for expansion in its applications increased to include TV via the Internet, distance education, video conferencing and many other applications that need a great bandwidth.

In reality, multicasting technology suffer from many challenges that prevented its spread, including commercial and security. Therefore, a new technology has been proposed called application-level multicast networks that rely on the idea of building an overlay tree from end users as a pillar to add and publish new network services, or to provide a special topology for routing that is not available in the basic physical network. The goal is to facilitate the management of its groups and regulate the relationships between members of these groups, and then achieving security becomes easier than it is in multicast. Since achieving information confidentiality is a major challenge, therefore, a lot of research has been directed towards this topic, and it relied mainly on encryption keys, so the topic focuses on managing these keys and studying their impact on network overhead.

This research aims to suggest a new scheme to manage encryption keys in application-level multicast and to compare them with all existed schemes in these networks. Simulation results demonstrated the effectiveness of the new method by examining its effect on network overhead and on the number of data encryption / decryption operations.

Keywords: IP Multicast, Application-Level Multicast Networks, Data Privacy, Key Management, Network Overhead.

* **Associate Professor, Department of Communication and Electronics, Factually of Mechanical and Electrical Engineering, Tishreen University, Lattakia, Syria.** mothanna.alkubeily @gmail.com

مقدّمة:

جاءت الشبكات التطبيقية متعددة البث Application-Level Multicast(ALM) or Overlay Multicast لتوجد حلولاً للتحديات التي واجهت تقنية الإرسال المجموعاتي، وقد ظهرت بقوة فعلاً نتيجة للمزايا التي تتمتع بها، إذ إنها تشكل شجرة تغطية (Overlay Tree) من المضيفات المشاركة في جلسة البث المجموعاتي، وتستخدم تقنية الإرسال وحيد الاتجاه (Unicast) بين كل زوج من المضيفات لتوزيع البيانات. نتج عن ذلك القدرة على استخدام بروتوكولات الطبقات السفلى لتحقيق الوثوقية والتحكم بالازدحام والتدفق فضلاً عن الأمن. وطبعاً يتم بناء شجرة الـ ALM وفق خوارزميات وبروتوكولات معينة تختلف باختلاف الخدمة التي تقدمها الشبكة [3-1].

تعتمد الـ ALM على مايسمى بمجموعات الاتصال (Group communication) بحيث يتم توزيع عقد شجرة التغطية على مجموعات يسهل إدارتها، تتمتع هذه المجموعات بديناميكيتها، بمعنى أنه يمكن بأية لحظة أن تنضم عقدة جديدة أو تغادر أخرى أو قد يحدث فشل في أحدها. تسبب ديناميكية هذه المجموعات مشاكل بالنسبة لطرائق الأمن المتبعة، وخاصة فيما يخص سرية المعلومات التي تعتمد على مفاتيح التشفير في تشفير البيانات لإرسالها بشكل آمن.

لذلك توجهت الأبحاث بشكل مكثف نحو موضوع الأمن وخاصة السرية، فضلاً عن كيفية إدارة مفاتيح التشفير لتحقيقها، خاصة أن أي حدث يطرأ على عضوية المجموعة يسبب إعادة توليد مفتاح تشفير جديد لمجموعة الاتصال، ولزيادة نسبة الأمن والحماية من هجمات تحليل التعمية (Cryptanalysis) فإنه يتم إعادة توليد مفتاح تشفير جديد عند مرور زمن دوري يتم تحديده تبعاً لمجموعة عوامل.

أهمية البحث وأهدافه:

تأتي أهمية هذا البحث من الاستخدام المتزايد للأنترنت وزيادة تطبيقاته التي تحتاج إلى عرض حزمة كبير، فضلاً عن التطبيق الفعلي لتقنية الـ ALM في عدد كبير من تطبيقات الأنترنت مثل التعليم عن بعد E-Learning والفيديو كونفرنس video Conferenceوالتلفزيون عبر الانترنت Internet TV ... الخ.

ومن جهة أخرى أصبح موضوع الأمن معقداً جداً كما أصبح السعي نحو الحفاظ على سرية البيانات المرسلة بين مجموعات الاتصال التي تشكل شجرة الـ ALM يشكل تحدياً رئيسياً. لذلك قام عدد من الباحثين بالتوجه نحو موضوع سرية البيانات وكان عدد كبير منها يسعى لإيجاد معادلة تحقق هذه السرية، وتوازناً بين ماتسببه إدارة مفتاح التشفير من حمل على الشبكة من جهة فضلاً عن ماتسببه من عدد مرات تشفير وفك تشفير البيانات. وعليه تمت المقارنة بين جميع الطرائق المقترحة في هذا المجال، وطبعاً كانت النتيجة أن هناك بعض الطرق التي تضحي تماماً بموضوع عدد عمليات تشفير/فك تشفير البيانات مقابل تخفيف الحمل على الشبكة بشكل كبير، في حين أن بعض الطرق كانت تسعى إلى تقليل عدد مرات تشفير/فك تشفير البيانات مقابل تضحيتها بحمل الشبكة ، وطبعاً هناك طرق قد خفضت كلا الأمرين ولكن ليس بنسبة كبيرة.

في النهاية نسعى في هذا البحث إلى اقتراح طريقة جديدة لإدارة مفاتيح التشفير بحيث تخفض الحمل على الشبكة كما أنها تقلل عدد مرات تشفير/فك تشفير البيانات بنسبة عالية جداً وهذا هو الهدف الأساسي من الطريقة المقترحة. ولإثبات الطريقة المقترحة فقد تم مقارنتها مع سابقاتها من الطرائق المقترحة ضمن نفس المجال تبعاً لعدد من البارامترات التي سيتم شرحها تالياً.

طرائق البحث ومواده:

استخدمنا في بحثنا لغة البايثون، والتي اخترعها Guido van Rossum في عام 1990، وقد استقى هذه اللغة من عدة لغات سابقة من مثل: c و c++ و Modula و ABC و Icon، وتعد بايثون من اللغات النصية سهلة التعلم والمنظمة بشكل صارم مما أهلها أن تكون الخيار الأول في صنف اللغات الأكاديمية التي تعتمد في الجامعات ونلخص مميزات لغة بايثون بما يلي [4]:

- إدارة آلية للذاكرة.
- برمجه غرضية التوجه.
- البساطة والوضوح في قواعد الكتابة والتصميم.
- مفتوحة المصدر.
- دعم بروتوكولات الانترنت القياسية .
- كثرة المكتبات المضمنة لتسريع وتسهيل تطوير البرامج.
- تعمل على عدة منصات: الويندوز واللينكس والماكينتوش واليونكس بدون تغيير الكود.

1. الشبكات التطبيقية متعددة البث Application–Level Multicast Networks:

يتم تبادل البيانات عبر الانترنت [5] عموماً اعتماداً على الاتصال أحادي البث، لذا في حال وجود مليون مستخدم يحاولون مشاهدة حدث عالمي هام كمباراة رياضية مهمة، وبدلاً من بث المعلومات بثّاً عاماً لجميع المستخدمين فإنّ المصدر سيرسل نسخة من هذه المعلومات لكل مستخدم، أي يستمر المصدر بإرسال نفس الرزمة مليون مرة وهو مايقود لحركية زائدة في الشبكة وإلى ضياع إضافي للرزم.

في أواخر تسعينات القرن الماضي تم إيجاد البث المجموعاتي IP–multicast بحيث يُرسل المصدر المعلومات لمجموعة من المستخدمين، وتقوم الموجهات الوسطية بتكرار وإعادة توجيه الرزم باتجاههم. يتم تطبيق البث المجموعاتي على مستوى طبقة الشبكة، وقد قدّم هذا الصنف عدة تقنيات فعّالة لكنها لم تستخدم بشكل واسع لعدة أسباب أبرزها مستوى التعقيد العالي [6]. لذا تم إيجاد الشبكات التطبيقية متعددة البث كبديل فعّال عن البث المجموعاتي، وتم ذلك بالانتقال من طبقة الشبكة إلى طبقة التطبيقات، حيث تعمل هذه الشبكات في طبقة التطبيقات.

تميّزت الشبكات التطبيقية متعددة البث بسهولة انتشارها فهي لا تتطلب أي تغيير في طبقة الشبكة، حيث يتم إرسال البيانات في هذه الشبكة عبر شجرة التغطية المبنية باستخدام الاتصال أحادي البث بين العقد. تم اقتراح العديد من البروتوكولات خلال السنوات الماضية من أجل بناء شجرة تغطية فعّالة، ويمكن تصنيف هذه البروتوكولات إلى صنفين أساسيين [1,7] هما البروتوكولات المركزية Centralized Protocols والبروتوكولات الموزعة Distributed Protocols.

تستلزم البروتوكولات المركزية وجود عقدة مركزية تتحكم بالجلسة Rendez–vous Point (RP) والتي يمكن تعريفها كمخدّم، حيث تجمع هذه العقدة المعلومات المطلوبة لبناء الشجرة حسب البارامتر (التأخير، عرض الحزمة، الضياع ...) من جميع أعضاء الجلسة، ثم تقوم ببناء الشجرة المثالية بناءً على القياسات التي جمعتها. وبعد أن تتم عملية البناء تبدأ العقدة المركزية بإخبار كل عقدة عن تموضعها ضمن الشجرة وعن جيرانها. لكن تعاني هذه البروتوكولات من مشكلة نقطة واحدة للفشل.

أما البروتوكولات الموزعة فتستلزم أيضاً وجود عقدة متحكمة بالجلسة (RP) لكنّ مهامها تقل، حيث تقوم كل عقدة بإرسال معلوماتها نحو العقدة المركزية التي يكون لها دور تحكمي من خلال إخبار هذه العقدة الجديدة عن مجموعة الآباء

المحتملين لها، لكنّ عملية بناء الشجرة (قرار الانضمام للأب) فتتخذه العقدة الجديدة وليس العقدة المركزية، ويتم ذلك وفقاً للبروتوكول الذي سيتم اختياره لبناء الشجرة. ثم تُطلع العقدة الجديدة العقد الأخرى على موقعها بعدة طرق متاحة لذا نلاحظ بأنّ هذه الخوارزمية تعاني من حمل إضافي واضح.

1.1 خواص الشبكات التطبيقية متعددة البث:

يمكننا تلخيص خواص الشبكات التطبيقية متعددة البث [1,7,8] بما يلي:

1 . سهولة الانتشار: حيث أنها لا تتطلب أي تغيير في طبقة الشبكة بل تقوم ببناء شجرة منطقية بمستوى أعلى من الطبقة الفيزيائية، لذا فهي تعمل في مستوى المستخدمين حيث تتكون هذه الشجرة من العقد الطرفية بدلاً من الموجهات، أي يتم استخدام الطبولوجيا المنطقية لإخفاء الطبولوجيا الفيزيائية، لذلك فهي لا تتطلب أي دعم من الموجهات.

2 . غياب موجهات البث المجموعاتي: ينجز إرسال البيانات في هذه الشبكات عبر شجرة التغطية المبنية باستخدام الاتصال أحادي البث بين العقد، بحيث تصبح العقد هي المسؤولة عن الإرسال دون الحاجة إلى الدخول في تعقيدات الموجهات. كما تعمل هذه الشبكات في طبقة التطبيقات، لذا يتم الاستفادة من الخدمات المقدمة من الطبقات الأدنى حسب متطلبات الخدمة. مثل: دعم الوثوقية، ودعم الأمن، وتفادي الازدحام، فمثلاً إذا كانت الخدمة بحاجة إلى اتصال موثوق نستخدم بروتوكول التحكم بالنقل (TCP: Transport Control Protocol) وإذا كان العكس نستخدم بروتوكول التحكم بحزمة بيانات المستخدم (UDP: User Datagram control protocol).

2. أمن اتصال المجموعات (Group Communication Security):

من أجل تأمين اتصالات المجموعة، يتم استخدام تقنيات الأمن مثل: السرية، التحكم بالوصول، تكاملية البيانات والمصادقة. تعتمد أغلب هذه التقنيات عموماً على استخدام مفتاح أو عدة مفاتيح تشفير لحركة البيانات Traffic Encryption Keys (TEKs). تبني إدارة هذه المفاتيح مثل توليدها، توزيعها وتحديثها صندوقاً أساسياً لبناء اتصال مجموعة آمن [9,10].

2.1 سرية البيانات Data Confidentiality

تعتمد السرية على جعل البيانات غير متاحة ومغلقة على الأعضاء غير المسموح لهم الوصول إليها. يتم تأمين السرية باستخدام التشفير (Encryption) والذي يمثل عملية تحويل النص الواضح (Plain Text) إلى نص مشفر (Cipher Text) وذلك لجعل هذه البيانات كنموذج مبهم غير قابل للقراءة. أما عملية فك تشفير (Decryption) فهي تمثل عملية تحويل النص المشفر إلى شكله الأصلي الواضح. يمكن أن نميز بين طريقتين أساسيتين للتشفير: التشفير المتناظر والتشفير غير المتناظر.

2.1.1 التشفير المتناظر Symmetric-Key Encryption

في هذا النوع من التشفير، يوجد مفتاح سري Secret Key مشترك بين المنبع والمستقبل ويتم استخدامه من قبل المنبع لتشفير الرسالة قبل إرسالها ومن قبل المستقبل لفك تشفير الرسالة المستقبلة. هناك عدة أمثلة عن هذا النوع من التشفير مثل: DES, AES, IDEA. يعد هذا النوع من الخوارزميات فعالاً إلا أنه يستدعي استخدام طريقة آمنة لنقل المفتاح بين المرسل والمستقبل.

2.1.2 التشفير غير المتجانس (التشفير بالمفتاح العام) Asymmetric-Key Encryption (Public Key)

في هذا النوع من التشفير، يتم استخدام زوج من المفاتيح: مفتاح عام Public Key ومفتاح خاص Private Key. يتم نشر المفتاح العام بينما يبقى المفتاح الخاص المطابق له سرياً لدى المنبع، يمكن تشفير البيانات من قبل أي واحد باستخدام المفتاح العام بينما يتم فك تشفير البيانات من قبل مالك المفتاح الخاص المطابق. الخوارزميات الأكثر استخداماً ضمن هذا النمط هي: Diffie&Hellman, RSA, ElGamal. يعتمد أمان هذه الخوارزميات على صعوبة استخلاص المفتاح الخاص من المفتاح العام وبالتالي صعوبة استخلاص النص الواضح من النص المرمز.

2.2 سرية اتصال المجموعة

في أي جلسة ALM سرية، يستطيع الأعضاء الفعالون (المخّول لهم) فقط الحصول على المعلومات المرسلة ضمن شجرة التغطية، فمثلاً ضمن الخدمات المدفوعة، يستطيع المستخدمون الذين دفعوا من أجل الخدمة الحصول على هذه الخدمة من أجل فترة توافق المبلغ الذي دفعوه [10].

يعتمد أي حل لضمان أمن المعلومات في الشبكات التطبيقية متعددة البث بشكل ضروري على نظام إدارة مفاتيح (Key management) فعّال. في نظام إدارة المفاتيح ومن أجل مجموعة ALM، فإن تجديد مفتاح تشفير نقل المعطيات TEK(Traffic Encryption Key) ضروري من أجل الحفاظ على سرية المعطيات المتبادلة عند وجود أي حدث انضمام أو مغادرة لعقدة خلال الجلسة. في الحقيقة، يجب أن يتم منع أي عضو جديد من الوصول إلى الرسائل المتبادلة قبل انضمامه، وهذا مايسمى **بالسرية الماضية** (أو الرجعية) (Backward Secrecy). وبنفس الطريقة أيضاً، يجب منع أي عضو مغادر من المجموعة من الوصول إلى المعلومات المتبادلة بعد مغادرته، وهو ماندعوه **بالسرية المُسبّقة** (Forward Secrecy). **من أجل ضمان السرية الماضية،** يجب توليد مفتاح TEK جديد وإرساله إلى جميع أعضاء المجموعة مشفراً باستخدام المفتاح TEK السابق. يستقبل العضو الجديد المفتاح TEK الجديد في رسالة مستقلة مشفراً باستخدام المفتاح العام لهذا العضو الجديد. **في حالة السرية المُسبّقة،** يُرسل المفتاح TEK الجديد بشكل مستقل إلى كل عضو باقي في المجموعة مشفراً باستخدام المفتاح العام لكل عضو. تعاني هذه العملية لإعادة توليد المفتاح TEK مايسمى بظاهرة 1− affects−n، بمعنى آخر أن كل تغير في المجموعة (انضمام/مغادرة) سيؤثر على كل أعضاء المجموعة.

كما يجب **إعادة توليد المفتاح الدورية** (Periodic Rekeying): حيث يتم إعادة توليد مفتاح التشفير المستخدم في المجموعة بشكل دوري بحيث يتم اختيار هذه المدة تبعاً للخدمة المقدمة، أو تبعاً لأزمنة ورود أو مغادرة العقد من المجموعة وذلك لتفادي مشكلة كسر التعمية (Cryptanalysis).

وأخيراً يجب ألا تتمكن أي عقدة ليست داخل مجموعة الإرسال المتعدد من الوصول إلى أي مفتاح يمكّنها من فك تشفير الرزم المرسلة إلى عقد هذه المجموعة.

2.2.1 التواطؤ الحر (Collusion Freedom):

وهو عدم قدرة مجموعة من العقد (من خارج المجموعة) التي تتواطأ مع بعضها بعضاً للحصول على المفتاح (TEK). ولتحقيق الخواص السابقة لابد من تجديد المفتاح (توليد مفتاح جديد أو مجموعة مفاتيح) عند كل حدث يطرأ على الشجرة (كانضمام عقدة أو مغادرتها). ولكن ينشأ عن عملية التحديث هذه مشكلة حرجة كبيرة وهي التوسعية (Scalability)، فمثلاً يتوقف مدى استخدام عرض الحزمة في نظام ALM خلال عملية الـ Rekeying على طول رسالة الـ Rekeying

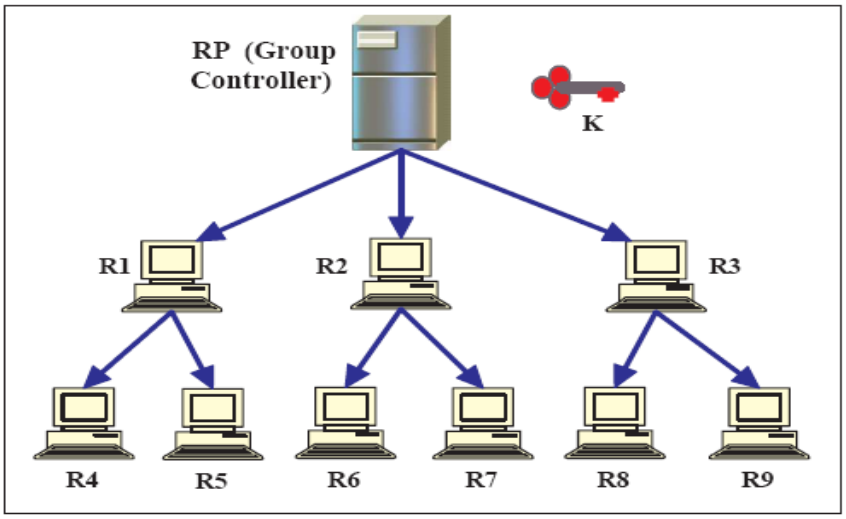
نفسها وعدد أعضاء المجموعة، فكلما كان عدد الأعضاء كبيراً وكلما كانت المجموعة تتمتع بديناميكية عالية عندئذ سيكون عرض الحزمة المطلوب لإعادة توليد مفتاح جديد وتوزيعة ضمن المجموعة كبيراً جداً.

إذاً لتطبيق السرية في بيئة ALM يجب بشكل رئيسي إدارة المفتاح TEK ليكون فعالاً في عملية التشفير بحيث لايزيد من حمل الشبكة عند إعادة توليده كما لايسبب زيادة في عدد عمليات تشفير/فك تشفير رسائل البيانات.

3. طرق إدارة مفاتيح التشفير في الشبكات التطبيقية متعددة البث

3.1 طريقة مفتاح المجموعة GKS: Group Key Scheme

حيث يتم استخدام مفتاح TEK واحد مشترك بين جميع أعضاء المجموعة كما هو موضح بالشكل 1 [11]. تعاني هذه الطريقة من مشكلة الظاهرة 1–affects–n الموضحة سابقاً. ولكن بنفس الوقت ليس هناك أي حاجة لأي عملية تشفير/فك تشفير وسطية للمعطيات على اعتبار أن هذه الطريقة تستخدم مفتاحاً واحداً حيث أن متحكم الجلسة RP يشفر البيانات باستخدام هذا المفتاح ويتم فك التشفير عند الأعضاء باستخدام نفس المفتاح.



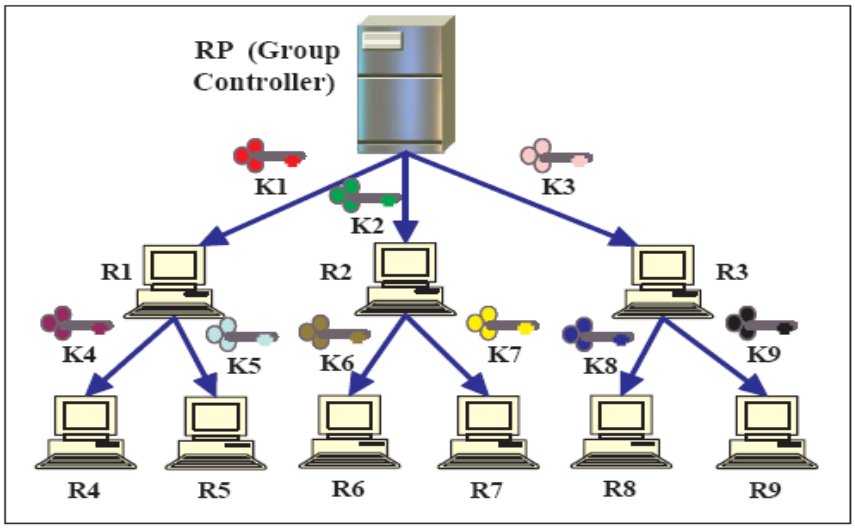
الشكل 1: طريقة مفتاح المجموعة

2.3 طريقة مفتاح الجيران NKS: Neighbors Key Scheme

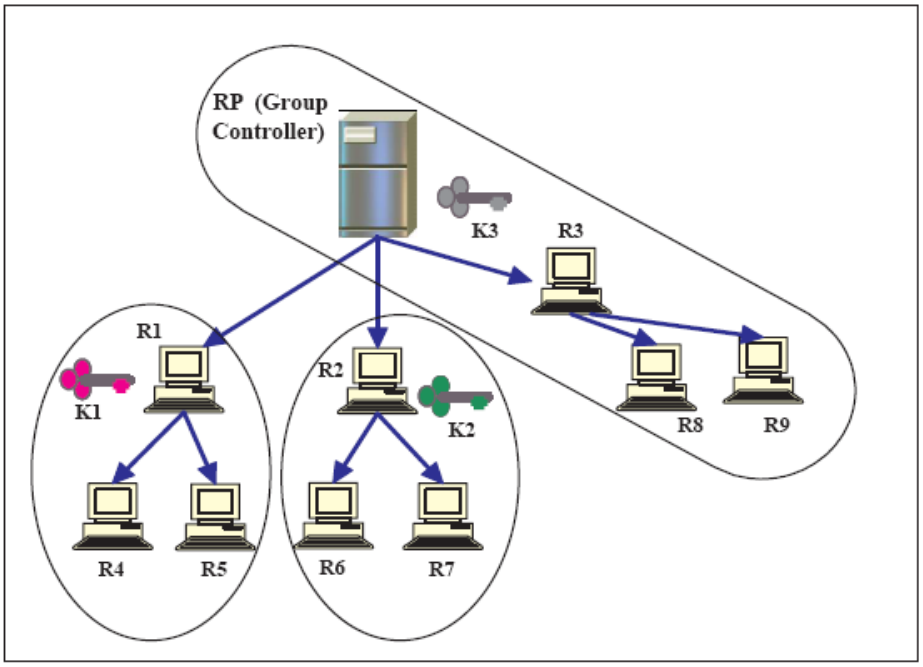
حيث يتم استخدام مفتاح TEK واحد بين كل عقدتين من المجموعة كما هو موضح بالشكل 2 [12].لاتحتاج هذه الطريقة إلى إعادة تغيير المفتاح بعد كل انضمام/مغادرة، ولذلك فهي لاتعاني من مشكلة 1–affects–n، ولكن تكمن سيئة هذه الطريقة بأنه يجب تشفير/فك تشفير البيانات عند كل عقدة في الشجرة، لذا سيزيد هذا من زمن التأخير والذي يكون حساساً في تطبيقات البث المباشر.

3.3 طريقة مفتاح العنقود CKS: Cluster Key Scheme

تعد هذه الطريقة حلاً وسطياً ما بين الطريقتين السابقتين حيث يتم تقسيم المجموعة الكلية لعدة عناقيد ويتم استخدام مفتاح مستقل لكل عنقود كما هو موضح بالشكل 3 [13]. يتم في هذه الطريقة تغيير المفتاح ضمن كل عنقود بعد كل انضمام/مغادرة، لذلك فهي تحل مشكلة 1–affects–n، كما يتم تشفير البيانات مرة عند المصدر وسيتم فك تشفيرها و إعادة تشفيرها من قبل قائد كل عنقود.



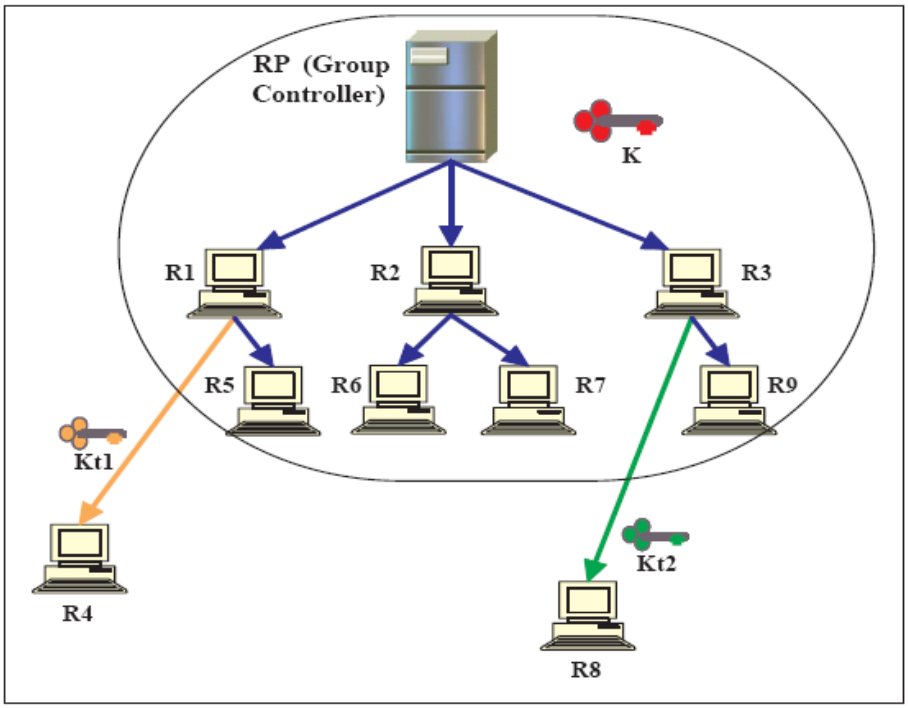
الشكل 2: طريقة مفتاح الجيران



الشكل 3: طريقة مفتاح العنقود

4.3 طريقة المفتاح الانتقالي TKS: Transition Key Scheme

في TKS، تم اقتراح استخدام مفتاح TEK وحيد من أجل المجموعة. يتم تجديد هذا المفتاح دورياً كما هو الحال في كل بروتوكولات إدارة المفاتيح وذلك لحماية الجلسة من هجومات تحليل التعمية. خلال فترة TEK، إذا انضم عضو جديد إلى المجموعة، سيضع في الخدمة قناة آمنة مع الأب الذي سيتم اختياره باستخدام مفتاح مستقل، يدعى بالمفتاح المؤقت كما هي حالة المستقبلين R4 و R8 في الشكل 4 [14].



الشكل 4: طريقة المفتاح الانتقالي

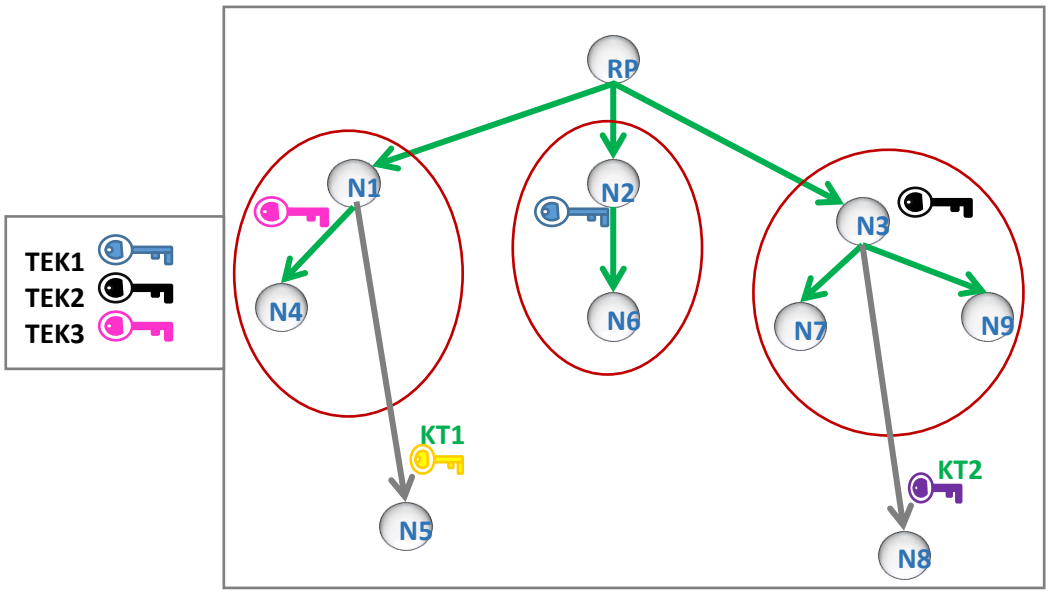
سيتم استخدام هذا المفتاح المؤقت من قبل الأب لتشفير معطيات المجموعة وإرسالها إلى هذا العضو الجديد. باستخدام هذه الطريقة، ليس من الضروري تجديد مفتاح المجموعة TEK للأعضاء الآخرين. سيبقى العضو الجديد في الحالة المؤقتة حتى موعد فترة التجديد الدوري للمفتاح TEK، حيث سيستقبل بالتالي المفتاح TEK الجديد ولن يستخدم بعد ذلك القناة الآمنة.

في حال كان العضو المغادر موجوداً في الحالة المؤقتة، فهو بحاجة فقط لإعلام والده بأنه يريد المغادرة باستخدام الرسالة leave-request، والتي تؤدي إلى إغلاق القناة الآمنة بينهما. في هذه الحالة الخاصة، لسنا بحاجة إلى تجديد (إعادة توليد) المفتاح TEK للمجموعة على اعتبار أن الأمن المُسبّق هو دوماً مؤمن مع المفتاح TEK الحالي. أما إذا كان ضمن المجموعة، فإن تجديد مفتاح المجموعة TEK ضروري دائماً من أجل تأمين السرية المسبّقة.

5.3 طريقة المفتاح العنقودي/الانتقالي TCKS: Cluster-Transition Key Scheme

تجمع هذه الطريقة كلاً من طريقتي TKS و CKS، كما يبين الشكل 5 [15] إذ افترض الباحث تقسيم الشجرة إلى عناقيد بحيث يوجد مفتاح تشفير TEK لكل عنقود يتم تحديثه بشكل دوري، كما افترض وجود نوعين من الـ RP أحدهما رئيسي يتحكم بالشجرة ككل ويدعى Main RP(MRP)، والثاني فرعي بحيث يوجد لكل عنقود RP خاص به ويتبع للـ MRP يدعى Cluster RP(CRP). يتحكم الـ MRP بكل الـ CRPs التي بدورها تدير عمليات إدارة المفاتيح ضمن العناقيد، ويكون كلُ منها مسؤولاً عن عنقوده.

يحتفظ الـ MRP بالمفاتيح العامة للـ CRPs وبالمفاتيح العامة لكل العقد في الشجرة. ومن أجل إنشاء جلسة إرسال متعدد آمنة يقوم الـ MRP بتوليد مفتاح TEK يرسله إلى كل الـ CRPs. يقوم كل من الـ CRPs بإعادة توليد المفتاح TEK وإرساله إلى العقد التابعة لعنقوده.



الشكل 5: طريقة المفتاح العنقودي الانتقالي

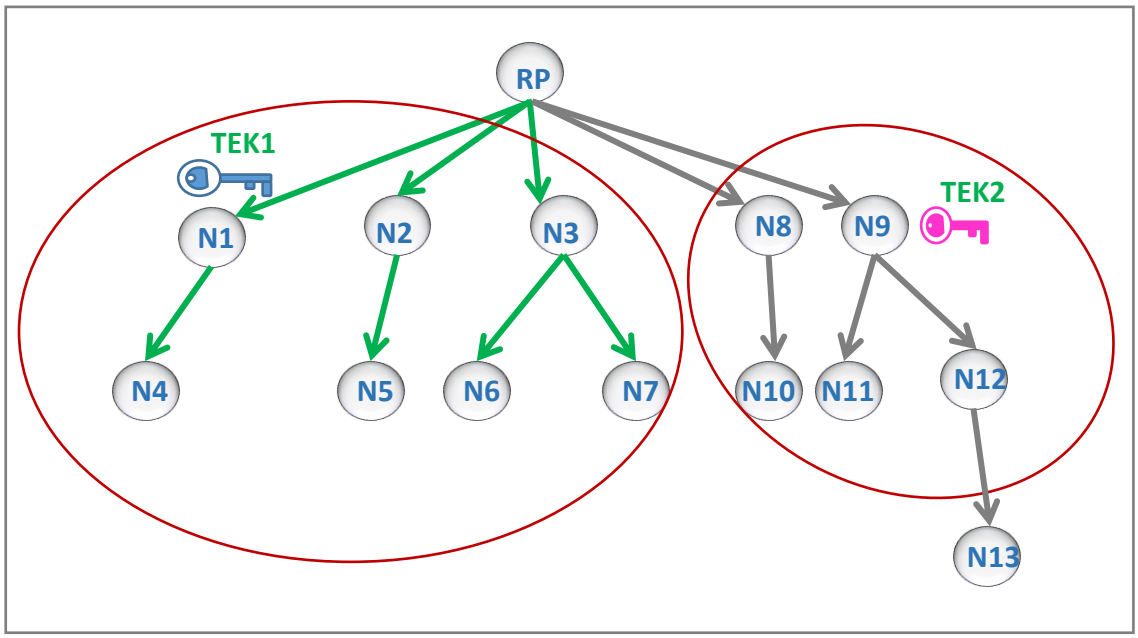
عندما تريد عقدة ما الانضمام فإنها ترسل رسالة طلب إلى الـ MRP، عندها يرسل لها قائمة بجميع الـ CRPs الموجودين. وهنا على العقدة الجديدة أن تقيّم كلفة الاتصال بينها وبين كل الـ CRPs لتختار الأقرب وترسل إليه رسالة طلب انضمام إلى العنقود الذي يتحكم به. ثم يقوم الـ CRP الأقرب بربطها بالعنقود الأقرب. ثم ترسل العقدة طلبها من جديد إلى العقدة المجاورة لها والتي اختارها لها الـ CRP، ثم يتم تأسيس مفتاح انتقالي بينهما يدعى Transition key(TK) لتشفير البيانات المتناقلة بينهما. وتبقى هذه العقدة في حالتها الانتقالية حتى عملية الـ Rekeying الدورية، بحيث تتم هذه العملية بالشكل الذي لايجعل العقد الانتقالية تنتظر طويلاً.

أما في حالة المغادرة، ترسل العقدة التي تريد المغادرة رسالة تنبيه إلى الـ CRP الذي يتحكم بعنقودها وتنتظر، في هذه الأثناء يرسل الـ CRP رسالة الطلب هذه إلى الـ MRP عندها يمكن للعقدة المغادرة أن تترك الجلسة عندما تأتيها الموافقة بذلك، وهنا يتم تنفيذ عملية توليد مفتاح TEK جديد ضمن العنقود.

أما إذا كانت العقدة لاتزال بحالتها الانتقالية فإن الأمر مشابه لطريقة TKS حيث يتم إلغاء قناة الاتصال بينهما، وإلغاء المفتاح الانتقالي بينهما.

4. الطريقة المقترحة: طريقة مفتاح المجموعة الانتقالي Group-Transition Key Scheme(GTKS)

تدمج هذه الطريقة طريقتي الـ TKS و الـ GKS. نفترض في هذه الطريقة وجود شجرتين إحداهما انتقالية والأخرى شبه ستاتيكية كما يبين الشكل 5، بحيث يكون لكل شجرة مفتاح مشترك بين عقدها، بمعنى أنه يوجد مفتاحان TEK يتم توليدهما من قبل الـ RP. وعندما يحين موعد الـ rekeying الدوري يتم دمج الشجرتين بشجرة واحدة لتفرغ الشجرة الانتقالية من العقد ويعاد بناؤها فيما بعد من العقد المنضمة حديثاً.



الشكل 5: الطريقة المقترحة

في طريقتنا المقترحة يتم بناء كل من الشجرة الأصلية والانتقالية بالطريقة نفسها سواء أكان البروتوكول المستخدم مركزياً أو موزعاً، كما يتم دمجهما على الأساس نفسه.

عندما تريد عقدة ما الانضمام فإنها ترسل طلبها إلى الـ RP، الذي يعطيها بدوره موقعاً مناسباً في الشجرة الانتقالية، وطبعاً تأخذ العقدة الجديدة موقعها في الشجرة الانتقالية حسب البروتوكولات والخوارزميات المتبعة في بناء هذه الشجرة، فإذا كانت هي أول عقدة تنضم إلى الشجرة الانتقالية فإنها تأخذ موقع الجذر فيها. وإلا فإنها ترتبط مع مجاوريها في الشجرة لتحصل على المفتاح المشترك TEK في الشجرة الانتقالية الذي يعاد توليده من جديد من جراء انضمام هذه العقدة وذلك لضمان السرية الماضية.

أما في حالة المغادرة فيوجد حالتان:

- الأولى إذا كانت العقدة المغادرة من الشجرة الأصلية فإنه يتم تنفيذ عملية الـ Rekeying لهذه الشجرة ليتم توليد مفتاح TEK جديد للعقد الموجودة في الشجرة الأصلية –وذلك بعد ضم عقد الشجرة الانتقالية إليها– لضمان السرية المسبّقة.
- أما إذا كانت العقدة المغادرة من الشجرة الانتقالية فيتم تنفيذ عملية الـ Rekeying لهذه الشجرة ويتم توليد مفتاح TEK جديد يوزع على عقدها وذلك أيضاً لضمان السرية المسبّقة.

عندما يحين موعد **إعادة توليد المفتاح الدورية** يتنبه الـ RP للأمر. فيقوم بضم عقد الشجرة الانتقالية إلى الشجرة الأصلية وفق الطريقة المتبعة في بناءالشجرة. وكما ذكرنا مسبقاً تتم إضافة العقد من الشجرة الانتقالية واحدة تلو الأخرى بدءاً من الأوراق وانتهاء بالجذر، وهكذا تفرغ الشجرة الانتقالية من العقد بعد كل Periodic Rekeying. بعد ذلك يعيد الـ RP توليد مفتاح جديد TEK يقوم بتوزيعه على جميع العقد في الشجرة الأصلية. نلاحظ أن عملية الـ Periodic Rekeying تسبب حملاً كبيراً على الشبكة، ويتم تحديد زمن حدوث هذه العملية بحسب اعتبارات معينة متعلقة بأزمنة ورود أو مغادرة العقد أو بطبيعة الخدمة التي تقدمها الشبكة ومن ثمّ حجم الشبكة. طبعاً إن تخفيض حمل هذه العملية يتناسب طرداً مع تخفيض زمن الـ Periodic Rekeying، لذلك لابد من إيجاد معادلة توازن بين زمن الـ Rekeying ومعدل عدد العقد في الشجرة

الانتقالية، مع الأخذ بالحسبان تردد تغير العضوية في الشجرة ككل (الانتقالية والأصلية) بمعنى دخول عقد جديدة ومغادرة أخرى أو انهيار عقدة ما.

بعد التعرف على الطريقة المقترحة سوف نجري مقارنة بينها وبين الطرائق السابقة من حيث تأثير إدارة المفتاح وعدد عمليات تشفير/فك تشفير الرسائل على حمل الشبكة خلال جلسة إرسال المتعدد . كما يشير إليها الجدول (1.4). وذلك بفرض لدينا المتحولات الآتية:

- N: تشير إلى عدد العقد الكلي في المجموعة.
- D: تشير إلى مدة جلسة الإرسال المتعدد.
- R_m: تشير إلى عدد الرسائل خلال الجلسة.
- C: تشير إلى عدد العناقيد في الشجرة.
- N_C: تشير إلى عدد العقد في العنقود الواحد.
- N_{New}: تشير إلى عدد العقد الجديدة.
- N_{trans}: تشير إلى عدد العقد في الشجرة الانتقالية.
- N_{static}: تشير إلى عدد العقد في الشجرة الأصلية قبل دمج الشجرة الانتقالية معها هذا يعني أن: $N > N_{static}$.

الجدول 1: مقارنة بين الطريقة المقترحة والطرائق الأخرى من حيث حمل الشبكة وحمل تشفير/فك تشفير البيانات

Scheme	Key Management Overhead			Data Encryption / Decryption Overhead
	Join	Leave	Rekeying Periodic	
GKS	N	N	N	$1*R_m*D$
NKS	1	0	N-1	$(N-1)* R_m *D$
CKS	N_C	N_C	N	$C* R_m *D$
TKS	1	N or 0	N	$(1+ N_{New})* R_m*D$
CTKS	1	N_C or 0	N	$(C+ N_{New})* R_m*D$
GTKS	N_{trans}	N or N_{trans}	N	$2* R_m*D$

5. المحاكاة وإظهار النتائج:

5.1 إعدادات المحاكاة:

من أجل قياس الحمل الإضافي لعمليات التعمية، استعملنا مكتبة OpenSSL 0.9.8[1] على جهاز سونترينو Centrino 1.4 GHz. استخدمنا RSA-1024 من أجل التشفير/فك التشفير غير المتجانس، و DES-CBC-64 من أجل العمليات المتجانسة. وفيمايلي خرج سطر الأوامر لـOpenssl Speed لهاتين الخوارزميتين:

```
>> openssl speed rsa1024
Sign          verify          sign/s          verify/s
0.005000s     0.000254s       200.0           3942.8
>> openssl speed des-cbc
The 'numbers' are in mega bytes per second processed. type
16 bytes      64 bytes        256 bytes       1024 bytes
des cbc: 28.54239      29.54255        29.97002        30023.65
```

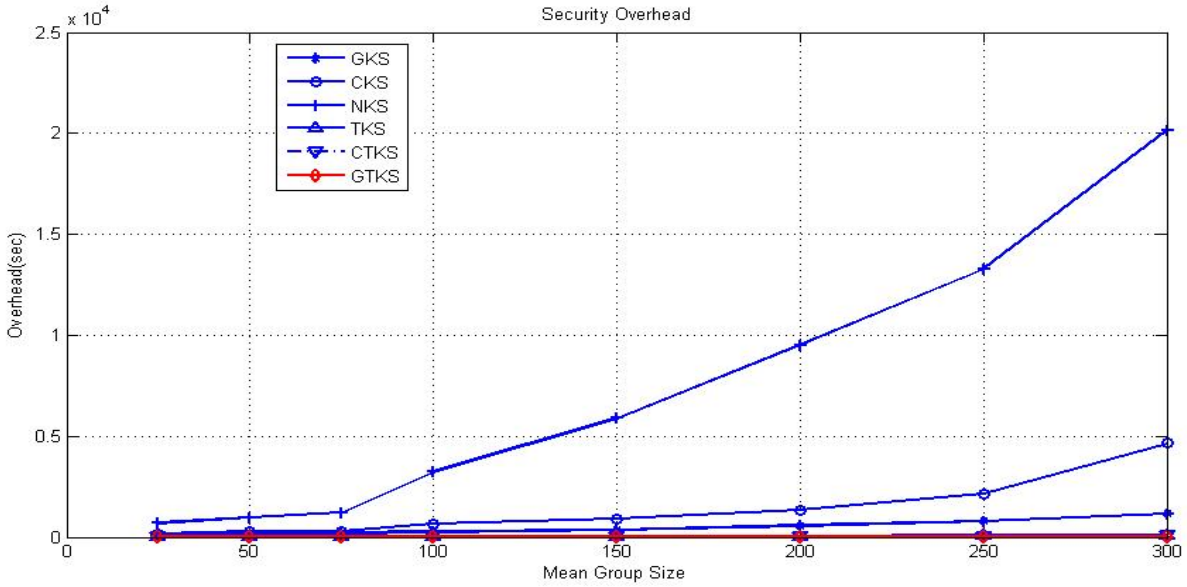
تم تهيئة المحاكاة باستخدام مخططات مستوية عشوائية Random flat graph وباستخدام نسخة معدلة من خوارزمية واكسمان Waxman مكتوبة باستخدام مكتبة الشبكات في بايثون Networks Python library. تبني هذه التقنية

[1] **www.openssl.org**

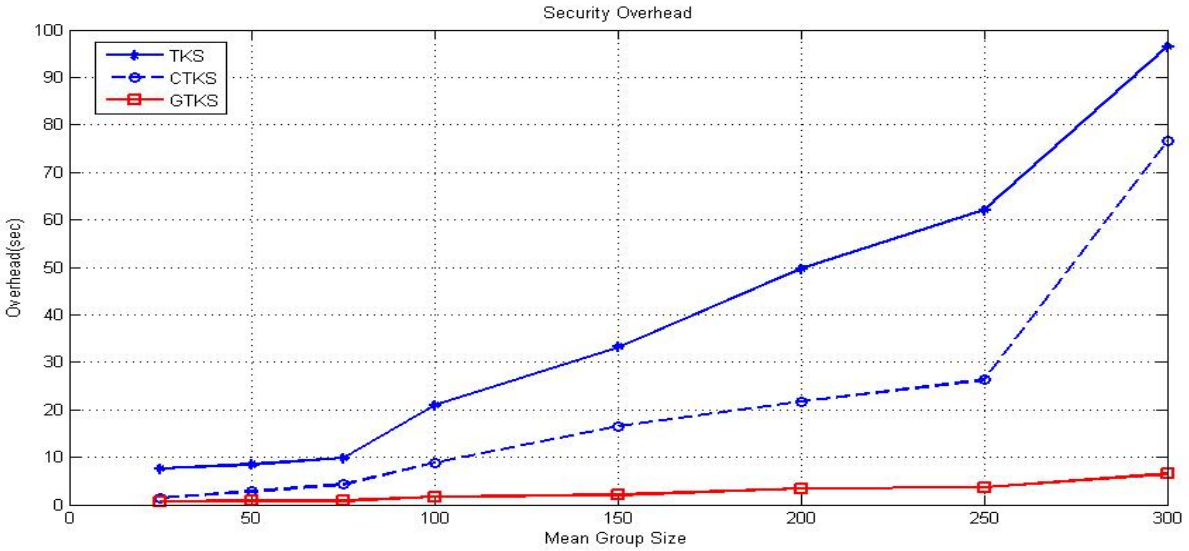
مخططات تملك خصائص مشابهة لشبكات الانترنت، يتم إضافة الوصلات بين العقد باستخدام النموذج الاحتمالي Probabilistic model. من أجل محاكاتنا، تم استخدام مخططات بـ 500 عقدة ومع درجة عقدة متوسطة مكافئة لـ 3. كانت قيم تأخير الوصلة منتظمة التوزيع بين 1 و 5 ميلي ثانية. قمنا باستخدام نموذج الميروث–عمار الموضح في [16,17] من أجل توليد جلسات شبكة تطبيقية متعدد البث حقيقية. أخذنا بالحسبان تطبيق ALM بمعدل نقل مقداره 256 رزمة في الثانية، مع حجم رزمة قدره 1kbyte. هذا مايعطي معدل نقل مقداره 256kbytes/sec. تم تثبيت زمن تجديد المفتاح الدوري إلى 80 ثانية وعدد العناقيد في حالة CKS إلى 5.

النتائج والمناقشة:

قارنا أداء GTKS مع الطرق الخمسة الأخرى الأخرى لإدارة المفاتيح GKS، CKS، NKS، TKS و CTKS. يبين الشكل 6 الحمل الكلي للأمن للطرائق الستة المدروسة (كلفة تجديد المفتاح+كلفة تشفير/فك تشفير البيانات)، ولزيادة الإيضاح يوضح الشكل 7 الحمل الكلي للطرائق الثلاثة المستندة إلى المفتاح الانتقالي وكل ذلك استناداً للجدول رقم 1. كماهو متوقع، يمكن أن نلاحظ أن بروتوكولنا المقترح GTKS يعطي أفضل النتائج وهو البروتوكول ذو الأداء الأفضل. بينما تعطي الطريقة NKS أسوء أداء وذلك على الرغم من أنها لاتقوم بعملية تجديد لمفتاح المجموعة بعد كل عملية انضمام أو مغادرة، ولكن يجب أن يُفك تشفير رزم البيانات وإعادة تشفيرها عند كل عقدة في شجرة التغطية. مثلاً من أجل مجموعة مؤلفة من 300 عقدة، يخفض GTKS الحمل الكلي للأمن حتى 99% بالمقارنة مع NKS، 94% بالمقارنة مع CKS ، 91% بالمقارنة مع GKS، 78% بالمقارنة مع TKS ، و 69% بالمقارنة مع CTKS.

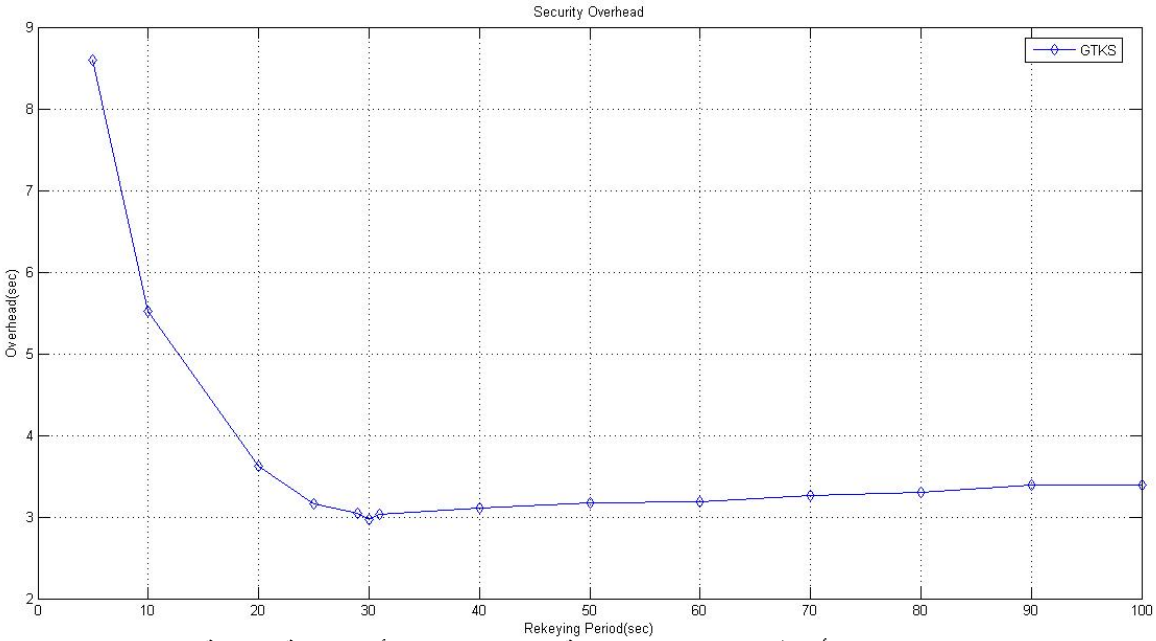


الشكل (6): الحمل الكلي للأمن للطرائق الستة



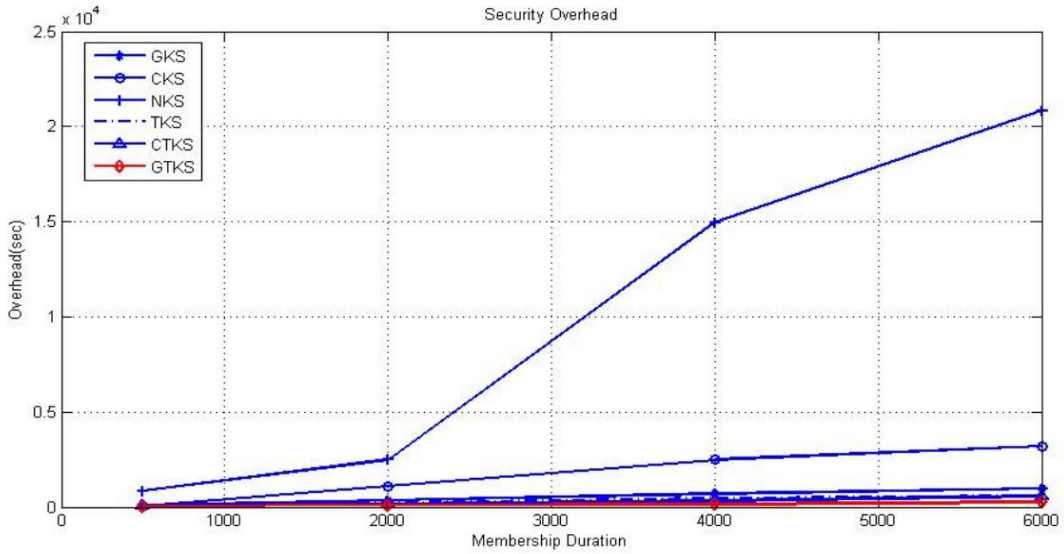
الشكل (7): الحمل الكلي للأمن لطرائق المفاتيح الانتقالية الثلاث

في الشكل 8، درسنا تأثير زمن فترة التجديد على الحمل الكلي للأمن من أجل بروتوكولنا المقترح من أجل مجموعة مؤلفة من 100 مستخدم. قمنا بتغيير زمن فترة تجديد المفتاح TEK من 5 إلى 100 ثانية. يمكن أن نلاحظ أنه من أجل هذه الجلسة الخاصة فإن الفترة المثالية لعملية تجديد المفتاح هي 30 ثانية والتي تعطي أقل حمل إضافي على الشبكة.

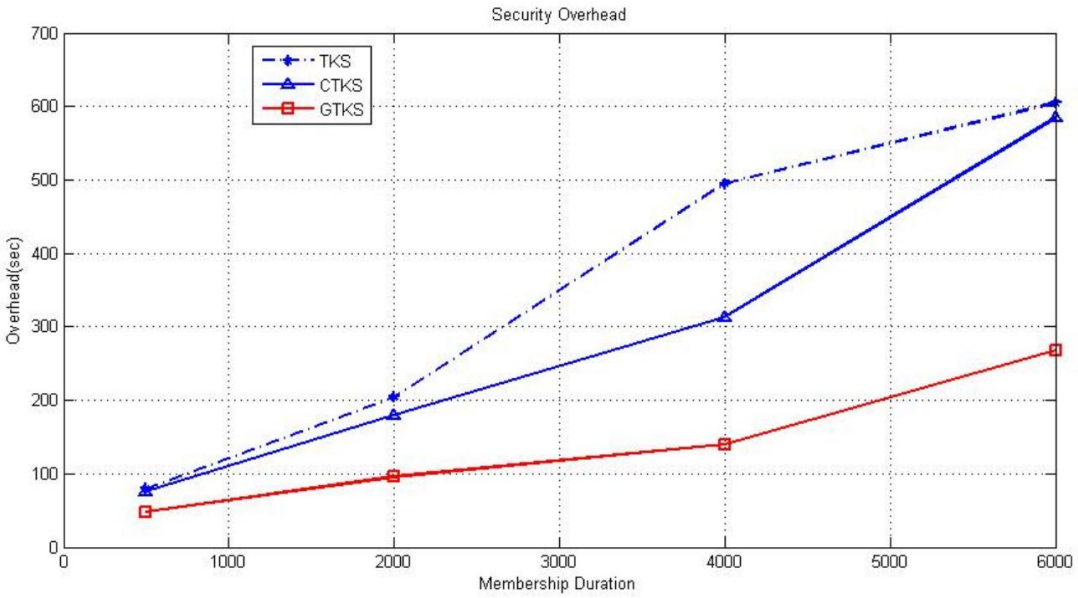


الشكل (8): تأثير فترة تجديد المفتاح الدورية على الحمل الكلي للأمن للطريقة المقترحة

كما درسنا في الشكلين 9 و10 تأثير ديناميكية المجموعة على جلسة ALM. أخذنا بالحسبان 4 نماذج للجلسات من خلال تغيير زمن الإقامة في الجلسة (MMD): جلسة شديدة الديناميكية (MMD=500)، جلسة عالية الديناميكية (MMD=2000)، جلسة ديناميكية (MMD=4000)، جلسة ضعيفة الديناميكية (MMD=6000). حيث يمكن أن نلاحظ بأنه كلما كانت الجلسة أكثر ديناميكية كلما ازداد الحمل الكلي للأمن.



الشكل (9): تأثير ديناميكية المجموعة على الحمل الكلي للأمن للطرائق الستة



الشكل (10): تأثير ديناميكية المجموعة على الحمل الكلي للأمن لطرائق المفاتيح الانتثالية الثلاث

الاستنتاجات والتوصيات:

اقترحنا في هذا البحث بروتوكول إدارة مفاتيح فعال، يدعى GTKS (Group–Transition Key Scheme)، والذي يخفض الحمل الإضافي لإدارة المفاتيح في حالة الجلسات عالية الديناميكية. لفعل ذلك، نفترض في هذه الطريقة وجود شجرتين إحداهما انتقالية والأخرى شبه ستاتيكية، بحيث يكون لكل شجرة مفتاح مشترك بين عقدها، بمعنى أنه يوجد مفتاحان TEK يتم توليدهما من قبل الـ RP. وعندما يحين موعد الـ rekeying الدوري يتم دمج الشجرتين بشجرة واحدة لتفرغ الشجرة الانتقالية من العقد ويعاد بناؤها فيما بعد من العقد المنضمة حديثاً. أظهرت نتائج المحاكاة بأن بروتوكولنا المقترح يخفض بشكل واضح الحمل الكلي للأمن مقارنة مع البروتوكولات الأخرى.

نرغب بالعمل على استخدام ALM في الشبكات الخليوية وشبكات الـ Ad– Hoc، في الحقيقة قاد التطور الحديث في الاتصالات اللاسلكية إلى انتشار عدد كبير من التطبيقات والخدمات التي تحوي الصوت، الفيديو، والنص عبر الأجهزة اللاسلكية المجهزة بمعالجات ذات قدرة عالية. من أجل إشباع حاجات المستخدمين، تعمل مخدمات الخليوي على توجيه الكثير من الخدمات والتطبيقات لهؤلاء المستخدمين. نتيجة لسهولة تطبيقها وتكيفها واستقرارها، يمكن أن تكون الشبكات التطبيقية متعددة البث حلاً مناسباً جداً للانتشار السريع لتطبيقات المجموعة وللخدمات في MANETS (بيئات الخليوي).

References:

[1] M. Alkubeily, H. Bettahar, and A. Bouabdallah; "*A New Application-Level Multicast Technique for Stable, Robust and Efficient Overlay Tree Construction*", In Computer Networks (ELSEVIER),55: 3332-3350, 2011.

[2] K. Xu, J. Liu, L. Fu, and C. Liu, "*On the Stability of Application-Layer Multicast Tree*," in Proceedings of The 21st International Symposium on Computer and Information Sciences(ISCIS'06, LNCS 4263), Istanbul, Turkey, November (2006), pp. 401-412.

[3] Krzysztof Stachowiak, Tytus Pawlak and Maceij Piechowiak, "*Performance Evaluation of Multicast Overlay Routing Protocols*", Image Processing & Communication, 17(1-2): 19-32, January (2013).

[4] https://www.python.org/, last visit Mai, 2020.

[5] B. Levine, B. Lyles, H. Kassem, D. Balensiefen and C. Diot, "*Deployment issues for the IP multicast service and architecture*," *Network, IEEE,* vol. 14, no. 1, pp. 78-88, Jan/Feb 2000.

[6] S. Fahmy and M. Kwon. "*Characterizing Overlay Multicast Networks*". In Proccedings ofthe IEEE International Conference On Network Protocols (ICNP), pages 61–70, Atlanta,Georgia, USA, November 2003.

[7] S. Banerjee, S. Lee, B. Bhattacharjee, and A. Srinivasan. "*Resilient Multicast using Over-lays*". InACM Sigmetrics'03, san Diego, CA, June 2003.

[8] Y. Chu, S. Rao, S. Seshan and H. Zhang, "*A case for end system multicast*," Selected Areas in Communications, vol. 20, no. 8, pp. 1456- 1471, Oct 2002.

[9] Francesca Palombini, "*Application Layer Security for the Internet of Things*", Ericsson Research, 2019

[10] Ranjan Kumar, Ganesh Aithal, and Surendra Shetty, "*Multicast Communication Using Different Group Key Managements*", International Journal of Recent Technology and Engineering (IJRTE)ISSN: 2277-3878, Vol.8, Issue.2, July2019.

[11] C. Abad, I. Gupta and W. Yurcik, "*Adding confidentiality to application-level multicast by leveraging Multicast overlay*," in international conference on communications(IEEE ICDCSW'05), June 2005.

[12] J. Liebeher and G. Dong, "*An overlay approach to data security in ad-hoc networks*," Ad Hoc Networks, vol. 5, no. 7, pp. 1055-1072, Sept 2007.

[13] W. P. Yiu and S. H. Chan, "*SOT: secure overlay tree for application layer multicast*," in IEEE International Conference Communications, June 2004.

[14] M. Alkubeily, A. Bouabdallah and H. Bettahar, " *TKS: A Transition Key Management Scheme for Secure Application Level Multicast*," International Journal of Security and Networks, Vol. 4, No. 4, 2009, pp. 210-222

[15] A. El-Sayed, "*Advanced Transition/Cluster Key Management Scheme for End-System Multicast Protocol*," Computer Science & Communications, vol. 5, no. 5, pp. 286-297, May 2012.

[16] K. Almeroth and M. Ammar. " *Collecting and Modelling the Join/Leave behaviour of Multi-cast Group Members in the MBone*". In5th International Symposium on High PerformanceDistributed Computing (HPDC'96), pages 209–216, Syracuse, NY, USA, August 1996

[17] K. Almeroth and M. Ammar. " *Multicast group behaviour in the internet's multicast backbone(Mbone)* ".IEEE communications Magazine, 35:124–129, June 1997.