مجلة جامعة تشرين للبحوث والدراسات العلمية _ سلسلة العلوم الهندسية المجلد (40) العدد (1) 2018
Tishreen University Journal for Research and Scientific Studies - Engineering Sciences Series Vol. (40) No. (1) 2018

Enhancement the Reliability of Communications in Multicast Networks using RE-KEYING Encryption keys

Dr. Mohammed Hijazieh*

(Received 7 / 1 / 2018. Accepted 19 / 2 / 2018)

□ ABSTRACT □

With the increasing demand for communications in Multicast networks and the rapid and changing evolution of these networks, it has been necessary to achieve high reliability of these connections, meaning that the members authorized to use this service are only able to access any content related to the communications of this group Therefore, the best solution was to encrypt the group broadcast data from the sender with the shared group key with all authorized members so that symmetric encryption prevents other users from accessing the content to achieve this goal, a technique called RE-KEYING was used in the research. This is done after each user has joined the group to prevent him from obtaining old information and after each user's departure to prevent him from accessing future information.

This research contributes to the development of the technique of using RE-KEYING encryption technology to ensure and improve the reliability of communications in multicast networks and to show how to distribute and exchange the key among the members of the group and then to indicate the meaning of confidentiality and reliability in these networks

Key Words: Traffic Encryption Key (TEK)- Group Key Management - Multicast - RE-KEYING- Key Server (KS)

*Associate Professor, Department of computer and automatic control Engineering, Faculty of Mechanical and electrical Engineering, Tishreen University, Latakia, Syria.
Email: mohammed.hejazieh2016@gmail.com

مجلة جامعة تشرين للبحوث والدراسات العلمية _ سلسلة العلوم الهندسية المجلد (40) العدد (1) 2018
Tishreen University Journal for Research and Scientific Studies - Engineering Sciences Series Vol. (40) No. (1) 2018

تحسين موثوقية الاتصالات في شبكات ال Multicast باستخدام تبديل مفاتيح التشفير

د. محمد حجازية*

(تاريخ الإيداع 7 / 1 / 2018. قُبِل للنشر في 19/ 2 / 2018)

□ ملخّص □

مع تزايد الطلب الكبير على الاتصالات في شبكات البث المجموعاتي Multicast إضافة إلى التطور المتسارع والمتغير في هيكلية تلك الشبكات، كان لابد من العمل على تحسين أمن هذا النوع من الاتصالات، بمعنى أن الأعضاء المخولين باستخدام خدمة ما يكون لهم فقط المقدرة على الوصول إلى أي محتوى يخص اتصالات تلك المجموعة ولذلك كان الحل الأمثل هو تشفير بيانات مجموعة الـ Multicast من المرسل بمفتاح المجموعة المشترك مع كل الأعضاء المخولين، وبالتالي يمنع ذلك المستخدمين الآخرين من الوصول إلى المحتوى. و لتحقيق الغاية المطلوبة تم في البحث استخدام تقنية تدعى بـ RE-KEYING ، أي تبديل المفتاح حيث يجب أن تُنجز هذه العملية بعد كل انضمام المستخدم الى المجموعة وذلك لمنعه من الحصول على معلومات قديمة وبعد كل مغادرة المستخدم وذلك لمنعه من الوصول إلى المعلومات المستقبلية[1,3]

هذا البحث يساهم في تطوير أسلوب استخدام تقنية تبديل المفتاح RE-KEYING لضمان وتحسين أمن الاتصالات في شبكات البث المجموعاتي الـ multicast مع تبيان كيفية توزيع وتبادل المفتاح بين أعضاء المجموعة.

الكلمات المفتاحية: البث المجموعاتي Multicast – تغيير المفتاح RE-KEYING – مفتاح تشفير الحركية – مخدم المفاتيح–إدارة مفتاح المجموعة

* أستاذ مساعد –قسم هندسة الحاسبات والتحكم الآلي–كلية الهندسة الميكانيكية والكهربائية–جامعة تشرين– اللاذقية– سورية.
الإيميل: mohammed.hejazieh2016@gmail.com

مقدمة:

إدارة مفاتيح المجموعة هي وظيفة هامة من أجل هيكلية البث المجموعاتي. وتدعى العملية بـRE-KEYING ويجب أن تُنجز بعد كل انضمام المستخدم الى المجموعة وذلك لمنعه من الحصول على معلومات قديمة وبعد كل مغادرة المستخدم وذلك لمنعه من الوصول إلى المعلومات المستقبلية.

يعطى هذا البحث هذا البحث مقدمة مختصرة عن شبكات البث المجموعاتي و يظهر معنى السرية والموثوقية في هذه الشبكات مع توضيح أهمية و كيفية توزيع وتبادل المفتاح بين أعضاء المجموعة .

أهمية البحث وأهدافه:

تكمن اهمية ذلك البحث في تحسين الموثوقية للاتصالات في شبكات البث المجموعاتي ال multicast مع استخدام تقنية re-keying رغم وجود مشكلة حرجة ناجمة عن التوسعية في الشبكات، أي أنه عند حدوث عملية الـ re-keying بعد كل تغير في علاقة أحد الأعضاء فإن عدد رسائل الـ TEK المُحدثة يكون مهماً في حالات عمليات الانضمام الى المجموعة والمغادرة منها، ولذلك تم اقتراح الحل المناسب وذلك بتنظيم المجموعة في مجموعات جزئية باستخدام TEKs محلية مُستقلة بما يقلل من تأثير الـ re-keying ولكن ذلك يتطلب تحويل البيانات على حالة المجموعات الجزئية [1,4] .

نستطيع تصنيف الحلول الموجودة وفق الوصولين:

- ✓ Common TEK
- ✓ TEK per subgroup

طرائق البحث ومواده:

إدارة مفتاح المجموعة هي وظيفة هامة جداً من أجل هيكلية البث المجموعاتي- Multicast. لذلك نتطرق في هذا البحث الى بعض بروتوكولات إدارة مفتاح المجموعة والمقارنة فيما بينها مع المقارنة بالأداء المعياري[1,2,3,11] .

شبكات البث المجموعاتي وموثوقية اتصالات المجموعة.

Multicast Networks and Group Communication Confidentiality

يوجد ثلاثة أنواع أساسية من العناوين وهي: (unicast, broadcast ,multicast)

- **العنوان من النوع unicast** (البث الأحادي): يصمم لكي ترسل الحزمة إلى وجهة واحدة فقط (IPV4 destination).
- **العنوان من النوع broadcast** (البث العام): يصمم لكي ترسل حزمة البيانات إلى كامل الشبكة الفرعية.
- **العنوان من النوع multicast** (البث المجموعاتي): يصمم لكي يمكن من تسليم رزم البيانات إلى مجموعة من الأجهزة التي تتم برمجتها لتكون أعضاء في مجموعة البث المجموعاتي وذلك ضمن شبكات فرعية متنوعة.

لماذا نستخدم البث المجموعاتي؟

يعتبر البث المجموعاتي مفيداً عندما يكون المطلب إرسال الرسالة إلى أكثر من جهاز واحد، وعادة فإن الزبون الذي يرسل رسالة البث المجموعاتي لا يعرف عدد المخدمات التي سوف تستقبل رسالته هذه، وبما أن البث المجموعاتي يعتمد على البروتوكول UDP ، لذلك يكون الإرسال غير موثوق.

إن ميزة استخدام البث المجموعاتي بدلاً من البث العام هو أنه في حالة البث المجموعاتي يتم استقبال الرسالة فقط من قبل المستخدمين الراغبيين بهذه الخدمة، كما أنه يتم إرسال الرسالة مرة واحدة فقط (وبذلك يتم توفير الكثير من عرض الحزمة).

مجموعات البث المجموعاتي Multicast Groups :

يمكن للأجهزة الأعضاء الانضمام إلى مجموعة البث المجموعاتي أو مغادرتها في أي وقت، ولا يوجد هناك أي قيود على الموقع الفيزيائي أو على عدد الأعضاء في مجموعة البث المجموعاتي. كما أن أي جهاز يمكن أن يكون عضواً في أكثر من مجموعة بث مجموعاتي واحدة في نفس الوقت، وليس من الضروري أن يكون الجهاز عضواً في مجموعة البث المجموعاتي كي يستطيع إرسال البيانات إلى هذه المجموعة.[2,3,4]

نشير هنا الى أن أهم ميزات شبكات البث المجموعاتي هي:

- استثمار عرض الحزمة بطريقة فعالة.
- منع حصول الازدحام في الشبكة.
- تخفيض الحمل عن المخدمات.
- منع وصول نسخ مكررة من المستخدمين.
- يمكن أن يتواجد عناصر المجموعة في أي مكان ضمن شبكة الإنترنت.
- يستطيع الأعضاء الانضمام إلى مجموعة ما أو تركها ويتم ذلك بإعلام الموجهات.
- هناك اختلاف بين المرسلين والمستقبلين وليس بالضرورة أن يكون المرسل عضواً في المجموعة.

common TEK approach :

حسب هذا الوصول جميع أعضاء المجموعة يشتركون بمفتاح تشفير مشترك TEK حيث يوجد ثلاثة أصناف لإدارة هذا المفتاح الوحيد هي Centralized المركزي، Decentralized اللامركزي، Distributed الموزع، في هذا البحث نبين باختصار إدارة هذا المفتاح الوحيد بالاعتماد على بروتوكولات مركزية centralized protocols.

البروتوكولات المركزية centralized protocols:

حسب هذا الوصول تنفذ وظيفة توزيع المفتاح بكيان وحيد والذي يكون مسؤولاً عن توليد وتوزيع مفتاح تشفير الحركية TEK عندما يكون ذلك مطلوباً.

تصنف هذه البروتوكولات في ثلاثة مستويات فرعية معتمدة على التقنية المستخدمة لتوزيع الـ TEKs ونبين فيما يلي كل مستوى فرعي:

Pair wise key: في هذا المستوى الفرعي للبروتوكولات مخدم المفتاح يشترك مع كل عضو بالمجموعة بمفتاح سري هذه المفاتيح تدعى عادة بمفاتيح تشفير المفتاح (KEKs) والتي تستخدم لإنشاء قنوات سرية بين ال KS وكل عضو من أجل إعادة توزيع الTEK الحالي بشكل سري كلما كان ذلك مطلوباً وفقاً للبرتوكولات الآتية[3,5,6] :

-**Group key management protocol (GKMP) [8-9,12]:** إن الـ KS يشترك مع كل عضو مخول من المجموعة بمفتاح سري (KEKS) في GKMP يولد الـ KS رزمة مفتاح المجموعة group key packet (GKP) والتي تحوي مفتاحين:

- **Group TEK (GTEK) يستخدم لتشفير الحركية**.يستخدم من أجل ضمان توزيع الـ GKP الجديدة بشكل آمن عندما يكون ذلك مطلوباً عندما ينضم عضو جديد للجلسة، ال KS يقوم بتوليد GKP جديدة (والتي تحوي الـ GTEK الجديد من أجل تحقيق backward and forward secrecy) ويرسله بشكل سري للعضو الجديد بعد تشفيره ب KEK المنشئ من أجل هذا العضو الجديد ويرسله الى بقية الأعضاء بعد تشفيره باستخدام ال GTEK القديم.

الـ KS يقوم بتحديث ال GKP بشكل دوري ويستخدم ال GKEK لتوزيعها الى أعضاء المجموعة. عندما يغادر عنصر من المجموعة ،ال KS يولد GKP جديدة ويرسلها إلى كل عضو موجود ضمن المجموعة مشفراً إياها باستخدام ال KEK المشترك مع كل عضو.

لذلك نلاحظ أنه لتحقيق الـ forward secrecy فإن الـ GKMP يتطلب رسائل re-keying هي O(n) لكل مغادرة من المجموعة.ولذلك هذا الحل لا يناسب المجموعات الكبيرة التي تتضمن تغيرات كثيرة في علاقات الأعضاء.

- **HAO-HUA CHUET AL protocol [8.11]:**

تم اقتراحه بحيث أن قائد المجموعة يشترك بـ KEK مع كل عضو للمجموعة.

لإرسال رسالة بث مجموعاتي سرية m، المرسل يقوم بتشفير m بمفتاح عشوائي k ثم يقوم بتشفير k باستخدام الـ KEK السري الذي يشترك به مع قائد المجموعة ويرسله إلى المجموعة مع الرسالة المشفرة.

المستقبلين في جهة الاستقبال، ليس بإمكانهم فك تشفير هذه الرسالة حيث أنهم لا يعرفون المفتاح العشوائي k.

عندما يستقبل قائد المجموعة الرسالة، فإنه يفك تشفير الـ k باستخدام المفتاح المشترك مع المصدر ويبني رسالة السماحية التي تحوي k المشفر بـ KEK الذي يشترك فيه قائد المجموعة مع كل عنصر مخول بالمجموعة (باستثناء الأعضاء المغادرين).

بالنسبة لاستقبال رسالة السماحية كل مستقبل يفك تشفير k مستخدما الـ KEK وبعد ذلك يفك تشفير ال m المشفرة باستخدام الـ k.

هذا البروتوكول يتطلب إرسال رسالة السماحية بالبث المجموعاتي بواسطة قائد المجموعة بعد كل مرة يرسل فيها المصدر رسالة إلى المجموعة مع حجم هو O(n) (حيث n هو عدد الأعضاء المخولين الحاليين).

Broad cast secrets:

طبقاً لهذا المستوى الفرعي من البروتوكولات فإن عملية الـ re-keying للمجموعة تعتمد على رسالة بث عام بدلاً من الإرسال السري الند للند.

- **Secure locks [7.10,12]:**

Chen and chiou اقترحا الـ secure locks كبروتوكول لإدارة المجموعة حيث أن ال KS يتطلب فقط بث عام وحيد لإنشاء مفتاح المجموعة أو من أجل re-keying بعد كل مغادرة من المجموعة .

وبالتالي هذا البروتوكول يقلل عدد رسائل الـ re-keying لكنه يزيد الحسابات عند المخدم بسبب حسابات النظرية المتبعة قبل إرسال كل رسالة إلى مجموعة.

فيما يلي سنقدم بعض البروتوكولات التي تستخدم هذه التقنية لـ re-keying:

- **Local key hierarchy (LKH) [8-11-13]:**

Wong etal and Wdlne etal اقترحوا بروتوكول الـ LKH وفيه الـ KS يحتفظ بشجرة من المفاتيح.

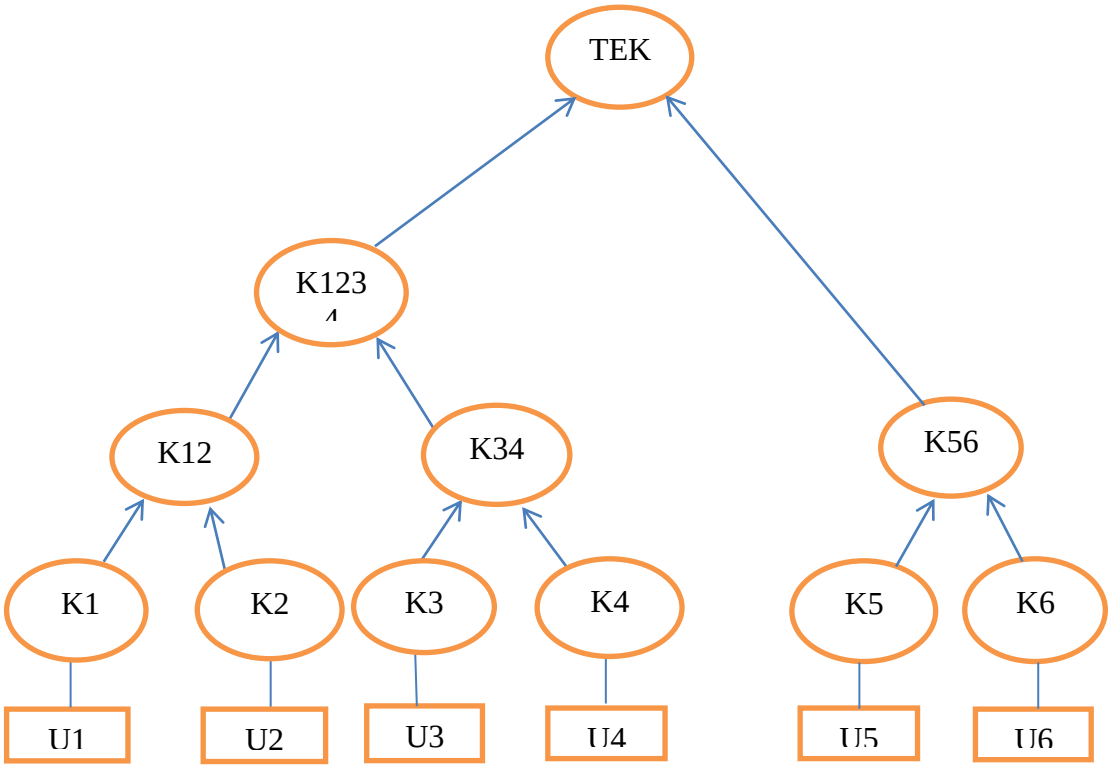
كل عضو يحتفظ بنسخة من ورقة مفتاحه السري وجميع الـ KEKs الموجودة على طول الطريق من ورقته إلى جذر الشجرة. المفتاح الذي يطابق جذر الشجرة هو الـ TEK. من أجل شجرة ثنائية متوازنة، كل عضو يحتفظ على الأكثر ب log2(n) + 1 مفتاح

حيث n هو عدد عناصر المجموعة.

هذه البنية المتسلسلة للمفتاح تسمح بتخفيض عدد رسائل الـ re-keying إلى O(log2(n)) بدلاً من O(n) في الـ GKMP.

بفرض أنه لدينا مجموعة بث مجموعاتي عناصرها{u1,u2,...u6}

الـ KS يبني مراتب متسلسلة من المفاتيح(هرمية المفتاح) كما هو مبين في الشكل (1):



شكل (1) هرمية المفتاح

كل عضو يملك مفتاح سري والذي هو ورقة في الشجرة تماماً وكذلك المفاتيح على طول طريقه الى الجذر، الجذر يمثل ال TEK المشترك مع الأعضاء .

المفاتيح الأخرى تستخدم لتخفيض عدد رسائل ال re-keying المطلوبة ووفق الشكل(1) :.

U1 يملك { TEK ,K1234 ,K12 ,K1}

U2 يملك { TEK ,K1234 ,K12 ,K2}

[6,9,11]: One-way Function Tree(OFT) -

Sherman And McGrew وضعا وطورا الـ LKH باسم الـ OFT .

يسمح OFT بتخفيض عدد الرسائل لل re-keying من $(\log_2(n))$ 2 إلى $(\log_2(n))$

في الـ OFT يحسب الـ KEK من الأعضاء بدلاً من أن ينسب الى الـ KS بالإضافة لذلك فان كل KEK Ki يحسب باستخدام ال KEKs الابن له كما يلي :

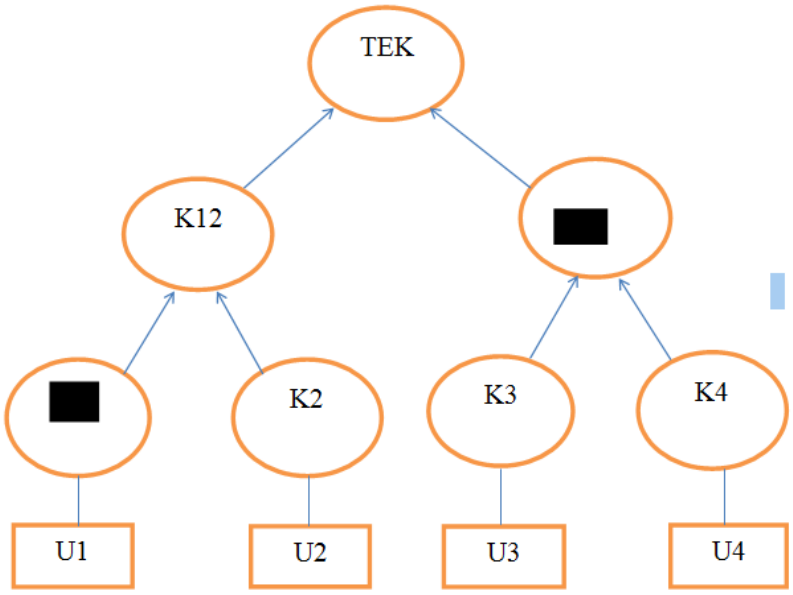
$$K_i=f(\ g(k_{left(i)})\ ,g(k_{right(i)})\ ) \qquad (1)$$

حيث right(i), left (i) تعني الابن اليساري واليميني للعقدة i و g هي تابع لمتحول وحيد.

نتيجة تطبيق g على المفتاح Kهي g(K) وتدعى بنسخة المفتاح المحجوب K .

وفقاً لهذا البروتوكول يحتفظ كل عضو بورقة مفتاحه السرية وبمفتاح الأخ له المحجوب ومجموعة من KEKs للأخوة المحجوبة للأجداد الأعلى.

الشكل (2) يوضح الأجداد الأعلى ومفاتيح الأخوة المقابلة للعضو u2:



الشكل (2): مفاتيح الأجداد الأعلى والأخوة المقابلة ل u2

كل عضو بإمكانه حساب ال KEKs المطلوبة للأجداد: (KEKs على العقد على الطريق من الورقة السرية إلى الجذر). عملياً في النموذج الأصلي (LKH) عندما يولد KEK جديد فإنه يشفر باستخدام ال KEKs للأبناء.

أما في الـ OFT عندما يتغير المفتاح المحجوب في العقدة فإنه يجب أن يشفر فقط بمفتاح العقدة الأخت له.

بعد ذلك فإن عدد رسائل ال re-keying المطلوبة سينخفض إلى النصف.

- **Canetti [2,1]:**

اقترحا وصول مشابه يسمى النموذج المقترح بـ one-way function chaintree باستخدام مولد عشوائي لتوليد ال KEKsالجديدة.

- **Perrig etal [2,1] :**

اقترح بروتوكول مشابه آخر يدعى ب Efficient Large Key Distribution ELK والذي استخدم الوظائف العشوائية الزائفة لتوليد ال KEKs الجديدة.

- **Centralized Flat Table Key Management(CFKM):**

البنية الهرمية للمفتاح المشترك في هذا الوصول استبدلت بجدول من أجل تقليل عدد المفاتيح التي يحتفظ بها الـ KS .

الجدول (1): يبين مقارنة بروتوكولات إدارة مفتاح المجموعة المركزية

protocol	1.affect.n	Re-Key overhead			Storage overhead	
		Join		leave	Key server	member
		multicast	unicast			
GKMP	Yes	2	2	2n	N+2	3
LKH	Yes	$Log_2(n)-1$	$Log_2(n)-1$	$2log_2(n)$	2n-1	$Log_2(n)+1$
OFT	Yes	$Log_2(n)+1$	$Log_2(n)+1$	$Log_2(n)+1$	2N-1	$Log_2(n)+1$
CFKM	Yes	2I	I+1	2I	2I+1	I+1
Secure lock	No	0	2	0	2N	2

حيث:

1- 1. affect.n : البروتوكول يعاني من ظاهرة 1.affect.n إذا تغيرت علاقة عضو واحد من المجموعة فإنها ستؤثر على كل أعضاء المجموعة الآخرين.

2- Storage at key server : عدد المفاتيح التي يجب ان يحتفظ بها ال KS.

3- Storage at member: عدد المفاتيح التي يجب ان يحتفظ بها العضو في المجموعة.

4- Join re-key overhead: عدد رسائل ال re-key المرسلة من ال KS لتوزيع ال TEK بعد الانضمام.

5- LEAVE RE-KYE overhead: عدد رسائل ال re-key المرسلة من ال KS لتوزيع ال TEK بعد المغادرة.

مراحل الاختبار العملي

- لاختبار سرية (موثوقية) اتصالات المجموعة تم فرض أن هناك مصدر يقوم بإرسال البيانات على مجموعة مستقبلين في جلسة بث مجموعاتي فإن أمن هذه المجموعة يكون مقاداً من مخدم المفاتيح المتحكم بالمجموعة

- للتأكيد على السرية خلال جلسة البث المجموعاتي ، يشارك المرسل جميع أعضاء المجموعة الشرعيين بمفتاح سري متماثل والذي يدعى بمفتاح تشفير الحركية Traffic Encryption Key(TEK) .

- من أجل البث المجموعاتي لرسالة معماة فإن المصدر يرمز تلك الرسالة بـ TEK باستخدام خوارزمية تشفير متناظر.

– أما في جهة الاستقبال لرسالة البث المجموعاتي المشفرة بالـ TEK فإن كل عضو شرعي يعرف الـTEK يستطيع فك تشفير الرسالة بالـ TEK ويكشف الرسالة الأصلية . وبذلك فإن العضو الذي يغادر من المجموعة بإمكانه فك تشفير رسالة البث المجموعاتي المعماة ولتجنب ذلك فإن الـ KS يجب أن يولد TEK جديد ويوزعه بشكل سري لجميع أعضاء المجموعة غير المغادرين . وتدعى هذه العملية re–keying وإن الـ KS يشترك مع كل عضو من المجموعة بمفتاح يدعى مفتاح تشفير المفتاحKey Encryptions Key (KEKI) (لا يكون ال KEKI مع العضو المغادر) .

بحيث أنه في ال rekey يقوم ال KS بتوليد TEK جديد وليكن TEK' ويرسله إلى كل عضو mi (عدا العضو المغادر) ويرمز ال TEK' باستخدام ال KEKI .

ونتيجة لذلك ليس بإمكان العضو المغادر معرفة ال TEK الجديد ومن تلك اللحظة لن يكون بإمكانه فك تشفير رسائل البث المجموعاتي في هذه الجلسة .

أما في حالة انضمام عنصر جديد إلى الجلسة ، فإن ال KS يقوم بعملية re–keying وذلك لمنع العضو الجديد من فك تشفير الرسائل المتبادلة السابقة باستخدام المفتاح الحالي .

وبذلك ال KS يولد TEK جديد TEK' و يرمزه باستخدام ال TEK القديمTEK ((TEK ويرسله إلى أعضاء المجموعة وبذلك يكون بإمكان الأعضاء القدامى معرفة ال TEK الجديد TEK' .

ثم يرمز ال KS ال TEK' ب KEKj سري الذي يشترك فيه مع العنصر الجديد mj ويرسله له ليكتشف ال TEK' المطلوب لفك تشفير رسائل البث المجموعاتي .

إن عملية توزيع المفاتيح و المحافظة عليها المتضمنة في ال re–keying والتشفير تدعى بشكل شائع بإدارة مفتاح المجموعة Group Key Management .

إن عملية ال re–keying تحدث رسائل O(n) rekeyبعد كل مغادرة من المجموعة

حيث أن n : عدد أعضاء عناصر المجموعة.

والـ re–keying تحدث أيضاً تخزين ل O(n) مفتاح (TEK + n KEKi 1)في الـ KS خلال كامل جلسة البث المجموعاتي السرية.

حيث أن تغيير علاقة أي عنصر بالمجموعة يتطلب re–keying ويمكن أن تكون المجموعة متغيرة بشكل كبير .

والأمر الأساسي في إدارة مفتاح المجموعة هو:

كيف يمكن تأمين عملية الـ re–keying باستخدام أقل عرض حزمة ممكن من دون فائض في التخزين.

لقد تم في البحث اجراء اختبار عملي وفقاً لبرنامج تم كتابته بلغة الجافا للحالات التالية:

– **الحالة الاولى:** لا يوجد أي عضو في المجموعة

– **الحالة الثانية:** يتم إدخال الشخص الأول من قبل مخدم المفاتيح حيث سيرسل له مفتاح تشفير المفتاح(الذي تمت تسميت هنا المفتاح الخاص) ومفتاح تشفير الحركية (الذي تمت تسميته المفتاح العام) كما تم الشرح سابقاً

– **الحالة الثالثة:** حالة أنه يوجد لدينا مجموعة (مثلا 8 أعضاء):

النتائج والمناقشة:

بعد الدراسة النظرية والتحليلية ووفقاً للاختبارات العملية للبروتوكولات السابقة في البحث تبين أن:

- بروتوكول GKMP يحقق نتيجة ممتازة من ناحية التخزين عند العضو، لكن من دون وجود حل من أجل الـ re-keying بعد مغادرة العضو للمجموعة والتي تحدث o(n) رسالة re-key فائضة حيث n عدد الأعضاء الباقيين .

- Secure Lock: يحقق نتيجة ممتازة من ناحية فائض الاتصالات والتخزين لـ KS والأعضاء أيضاً.

لكنه يتطلب حسابات زائدة عند الـ KS بسبب الاعتماد على نظرية ال Chinese reminder

- تظهر النتائج أن استخدام البنية الهرمية الشجرية للـ KEKs يعطي أداءً أفضل لإدارة مفتاح المجموعة بشكل واضح.

المقترحات والتوصيات المستقبلية:

يمكن اعتماد مجموعات فرعية بحيث أن كل مجموعة فرعية هي مجموعة مستقلة ومسؤول عنها مخدم مفاتيح وفي هذه الحالة عندما يحدث تغير في علاقة عضو من المجموعة الجزئية تحدث عملية إعادة توليد المفتاح فقط ضمن المجموعة الجزئية التي ينتمي لها هذا العضو وعند فشل إحدى المخدمات لن يؤدي ذلك إلى فشل الشبكة ككل وإنما فقط الجزء الذي تم تضرره.

نورد فيما يلي جدول بالمصطلحات الأساسية في البحث

متحكم المجموعة	Group Controller (GC)
مخدم المفاتيح	Key Server (KS)
مفتاح تشفير الحركية	Traffic Encryption Key (TEK)
مفتاح تشفير المفتاح	Key Encryptions Key (KEKI)
إدارة مفتاح المجموعة	Group Key Management
إعادة توليد المفتاح	re-keying
الأمن المسبق	Forward Secrecy
الأمن الماضي	Backward Secrecy
البروتوكولات المركزية	Centralized protocols
بروتوكول إدارة مفتاح المجموعة	Group key management protocol (GKMP)
بروتوكول هرمية المفتاح المحلي	Local key hierarchy (LKH)
شجرة تابع حل وحيد الاتجاه	One-way Function Tree(OFT)

المراجع:

[1] د. رياض ضاهر ،*أمن المعلومات*، منشورات جامعة تشرين 2014 – 2015 م.

[2] د. سائد محمود الناظر، *التعمية وأمن الشبكات* ، شعاع 2012.

[3] fedral information processing standards publication .data encryption standard(DES) (12/2015).

[4] fedral information processing standards publication. advanced encryption standard(AES) (12/2015). cryptosystems.communication of the ACM (1/2016).

[5] r.canetti,j.garay,g.itkis,d.micciancio,m.naor,and b.pinkas : A taxonomy and efficient constructions 2015

[6] g.h.chiou and w.t.chen.secure broadcast using secure lock . ieee transactions onsaftware engineering 2015.

[7] h.h.chu,l.qiao, and k.nahrstedt. a secure multicast protocol with copyright protection. 2016.

[8] h. Harney and c.muckenhirn. group key management protocol (gkmp) architecture (2/2016).

[9] d.a.mcgrew and a.t.sherman. key establishment in large dynamic groups using One-way function trees 2016.

[10] a. perrig,d.song,and j.d.tygar.elk,a new protocol for efficient large-group key distribution 2016.

[11] d.wallner, e.harder,and r.agree. key management for multicast: issues and architecture. National security agency (4/2016).

Web Sites

[12] https://www.3lom4all.com/vb/showthread.php?t=10753 (7-2017)

[13] https://www.rwaq.org/courses/introduction-to-encryption (11-2017)

[14] http://www.marefa.org/sources/index.php (1-2016)

[15] https://www.google.com/webhp?sourceid=chrome-instant&ion=1&espv=2&ie=UTF (3-2016)