EAI Endorsed Transactions
on Mobile Communications and Applications
Research Article **ICST.ORG**

Multi-Service Group Key Management for High Speed Wireless Mobile Multicast Networks

Trust T. Mapoka[1], Simon J. Shepherd[1], Yousef A.S Dama[1,2], Haider M. Al Sabbagh[3], and Raed A. Abd-Alhameed[1,*]

[1]Electrical Engineering and Computer Science, University of Bradford, Bradford, BD7 1DP, United Kingdom
[2]Electrical Engineering, An-Najah National University, Nablus, Palestinian
[3]Electrical Engineering, Basra University, Basra, Iraq

Abstract

Recently there is a high demand from the Internet Service Providers to transmit multimedia services over high speed wireless networks. These networks are characterized by high mobility receivers which perform frequent handoffs across homogenous and heterogeneous access networks while maintaining seamless connectivity to the multimedia services. In order to ensure secure delivery of multimedia services to legitimate group members, the conventional cluster based group key management (GKM) schemes for securing group communication over wireless mobile multicast networks have been proposed. However, they lack efficiency in rekeying the group key in the presence of high mobility users which concurrently subscribe to multiple multicast services that co-exist in the same network. This paper proposes an efficient multi-service group key management scheme (SMGKM) suitable for high mobility users which perform frequent handoffs while participating seamlessly in multiple multicast services. The users are expected to drop subscriptions after multiple cluster visits hence inducing huge key management overhead due to rekeying the previously visited cluster keys. The already proposed multi-service SMGKM system with completely decentralised authentication and key management functions is adopted to meet the demands for high mobility environment with the same level of security. Through comparisons with existing GKM schemes and simulations, SMGKM shows resource economy in terms of reduced communication and less storage overheads in a high speed environment with multiple visits.

Keywords: mobile multicast communication, group key management, wireless networks, security.

Received on 07 February 2015; accepted on 17 July 2015; published on 11 August 2015

doi:10.4108/eai.11-8-2015.150093

1. Introduction

Multicast is an efficient communication technology for the provision of group-oriented services over the Internet. These include services such as VOD (Video on Demand) and video conferencing. The services could be deployed more comfortably in wireless mobile networks than in wired networks because the entire receiving nodes within the transmission range of the broadcast medium can receive the services in a single transmission. Thus, the multicast services are expected to be dominating services by considering the fact that the majority of the recent standards committees of wireless networks such as E-MBMS in LTE [1] have standardised them. However, to provide access control to the broadcasted multicast services, a symmetric group key, known as the Traffic Encryption Key (TEK), has been widely deployed to guarantee secure group communications among the subscribed group members. Thus the broadcasted services encrypted by the TEK at the Service Provider (SP) end are decrypted by the authorised group members holding the same valid TEK at the receivers end assuming multicast routing protocols are in place.

Although symmetric effort provide efficiency in achieving secure group communications than asymmetric effort with heavier computation effort, it causes some challenges in GKM because the TEK need to be updated to achieve both *forward* and *backward secrecy* [2] during group membership dynamics caused by joins, leaves and mobility. Conventional GKM schemes for secure wired and wireless multicast [3, 4] networks only target a single

*Corresponding author. Email: r.a.a.abd@bradford.ac.uk

multicast service subscribed by low mobility users. In addition to our multi-service group key management scheme known as SMGKM [5], dedicated to providing secure multi-group oriented services to mobile users who dynamically perform handoff while seamlessly participating in multiple multicast services, we now consider rekeying during dynamic movement of high mobility users in multi-service subscriptions who then leave subscriptions after multiple cluster visits. However, recently part of this paper has been presented in[6, 7].

The rest of the paper is organized as follows. Section 2 reviews the related work. Section 3 describes the scenario for high speed mobility environment with multi-leaves in SMGKM compared to the related work. Section 4 presents the performance analysis of SMGKM in terms of communication and storage overheads in high mobility environment compared to the concerned schemes. Section 5 shows the simulated results for the concerned schemes along with their performance discussions. Section 6 finally concludes the paper.

2. Related Work

It is expected that the conventional wireless GKM schemes such as are DeCleene *et al* [8], GKMF [9] and Kellil *et al* [10] may induce huge rekeying communication overheads in rekeying the TEK when the group becomes flooded with high mobility users which perform frequent handoffs while participating in diverse multicast services. In a wireless environment there is limited bandwidth and high error rate of packet loss. In order to preserve the available bandwidth it is vital to consider reducing the communication overheads while preserving secrecy of services in the conventional wireless GKM schemes [3, 4] during frequent handoffs, where rekeying and multiple authentication notifications may be triggered more frequently. In addition to this, in a wireless environment portable mobile user devices such as laptops, smartphones and IPads are power constrained by nature. In this case highly mobile users may be susceptible to frequent disconnections to the subscribed services before the subscription period elapses due to accelerated battery drainage. In order to preserve the power usage in user devices it is also crucial to reduce the huge computation and storage complexities the resource constrained mobile device cannot handle in the conventional wireless GKM schemes, especially the existence of multiple service subscriptions [11].

The conventional wireless GKM schemes are possible to cause storage complexities in the highly mobile users because the users maintain the local cluster keys (KEKs) for the previously visited clusters during frequent handoffs. Eventually when these users leave or drop the subscriptions after multiple visits, this triggers repeated rekeying of the entire keys (TEKs and local KEKs) held by the highly mobile users in all the previously visited clusters for *forward secrecy* hence causing extra rekeying signalling load in the network. Additionally, during frequent handoffs, the schemes also require synchronisation with the trusted Domain Key Distributor (DKD) for requesting the TEK during rekeying, user authentication as well as for tracking mobility hence the name key-request schemes [4, 12]. The DKD in key-request schemes controls the entire local cluster managers called the Area Key Distributors in a decentralised environment.

Moreover frequent handoffs constitute a huge number of notifications to the DKD which cannot be a negligible communication overhead anymore. This occurs especially in vehicle-related services, such as telematics services where high speed vehicles handover frequently, hence repeated rekeying and authentication notification requests. Also, if the entire key management and authentication functions of the TEK are concentrated on the DKD which is a single point of failure and maybe far from the serving AKD, the multicast services become vulnerable to service disruptions due to rekeying delivery and authentication delays. Therefore, the characteristics of the key-request schemes are unsuitable for high speed wireless networks with multiple services. This has motivated us to build an efficient multi-service GKM scheme suitable for high speed mobility users in this paper.

3. Scenario for High Mobility in SMGKM

By maintaining SMGKM network model assumptions in [5, 12], we further explore the performance of the SMGKM in the presence of high mobility users which perform frequent handoffs across multiple clusters. The users finally leave the target clusters after multiple cluster visits while participating in multiple subscriptions concurrently.

The SMGKM [5] is a two-tier cluster-based [13, 14] decentralized multi-service GKM scheme. It consists of the DKD for initial registration of subscribers, initial generation of cryptographic key parameters for authentication and key management. It also consists of cluster controllers called AKDs which operate under the jurisdiction of the DKD for securely establishing and distributing the group key management keys to valid mobile subscribers over a bandwidth limited wireless domain. The mobile users use portable devices like smartphones, Ipads, *etc.* to wirelessly access their subscribed multimedia services over the internet. Each AKD manages the TEK independently per cluster in order to localize group key management. Both the authentication [15] and group key management phases are delegated securely from the trusted DKD to the intermediate AKDs using a novel Session Key Distribution List (SKDL) [12] to offer DKD scalability, prevent bottlenecks and unnecessary delays during the system lifetime [5, 11] . The SMGKM utilises the multi-service rekeying strategy for efficient delivery of the $TEK_{i,,j}$ group-key-shares destined for mobile users belonging to the same service group [11].

Let us now consider a scenario where highly mobile users belong to the same service group G_K. The service group G_K determines users accessing exactly the same set of services (s_1, s_2,…, s_j) and this simplifies key management with multi-service subscriptions [5]. Suppose that users M_1, M_2, M_5 and M_9 in Figure 1 access three of the pay-tv

services concurrently such as sports (s_1), movie (s_2) and music (s_2) out of 8 services provided by the SP. The assumption is also that users can seamlessly access the subscribed services in a high mobility environment such as vehicular networks where frequent handoffs may occur hence making multiple visits possible before users leave/drop the subscriptions. The cellular clusters of the SMGKM scheme illustrated in Figure 1 consist of two types of subscribed users:

- Present in the cluster (PIC) users currently being served by the AKD_i. These are considered as low mobility users assuming they stay long in the service.
- Absent in the cluster (AIC) users who have visited multiple clusters served by the target AKD_v after frequent handoffs. These users are considered to have high mobility.

Clearly it can be observed from the AIC mobile users in SMGKM that M_1 and M_2 in G_K have previously visited AKD_0, AKD_1, AKD_2 and AKD_3 by performing frequent handoffs then finally stay at the target AKD_5 before dropping subscriptions. M_9 has previously visited AKD_5 and AKD_0 before leaving at AKD_2. Similarly, M_5 has previously visited AKD_4, AKD_3 and AKD_0 before leaving at AKD_1.

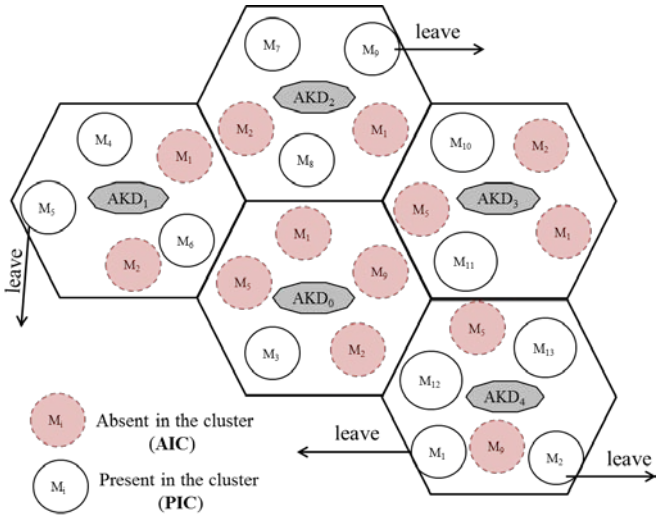

Figure 1. High mobility scenario with multiple visits

The assumption is that all M_i in G_K follow the same mobility pattern and SMGKM has already carried out the multi-service rekeying strategy based on Key Update Slots (KUS) [5, 11], to satisfy *backward secrecy* during frequent handoffs at the visited AKD_v and *forward secrecy* where M_1, M_2, M_5 and M_9 currently leave. The rekeying strategy detects the affected services during group dynamics so that the AKDs generate and securely deliver new TEK shares for the affected services to the PIC users where a join or leave occurs [11]. The assumption is that the Authentication phase of users is also performed at the target cluster during handoff using the Session Key Distribution List (SKDL) concept which tracks mobility at the AKD level without the DKD intervention hence DKD scalability [12].

3.1. Comparison of SMGKM with Key-Request Schemes for High Mobility

In this section, we summarise the characteristics of key-request schemes against SMGKM for suitability in high speed environments. As presented in Table 1, the key-request schemes adopt a two-tier decentralised framework with a common TEK approach. This approach allows highly mobile subscribers to maintain common TEK across the board, hence requiring the entire group members to commit to the new TEK whenever it changes due to group dynamics. The schemes also assume that the main DKD and the cluster managers which are the AKDs in this case have significant computation and storage resources to maintain and update the TEK and local cluster keys (KEK), respectively. Additionally, the introduced local KEKs maintained at the AKD level are used to safely distribute the TEK from the DKD to the users at the cluster level during rekeying, hence alleviating the need to renew the TEK during group dynamics. However, this enhances the rekeying performance of the key-request schemes by localising rekeying such that rekeying is only performed in the concerned cluster without affecting the neighbour clusters. The schemes also introduce the use of an unsecured mobility list to track user mobility such that only the target KEKs gets renewed while the TEK remains unchanged.

However, this causes huge storage complexity for high mobility users with resource-limited devices in situations of multi-subscriptions. Mostly, the key-request schemes rely on a single trusted centralised DKD for controlling all the AKDs as well as for TEK generation, TEK distribution and user authentication. Again, since the DKD controls the topological network reflecting all mobile user locations, it should be notified by all the AKDs whenever users undergo handoff and whenever existing mobile users leave the multicast services. However, this is not practical that a single entity controls the entire network consisting of millions of mobile users and huge AKDs. Additionally, frequent handoffs lead to a huge number of notifications with the DKD which cannot be a negligible communication overhead any more especially in vehicle-related services, such as telematics services where high speed vehicles handover frequently hence repeated rekeying. Also, if the entire key management functions of the TEK are concentrated on the DKD which is the single point of failure and maybe far from the serving AKD, the multicast services become vulnerable to service disruptions due to rekeying delivery and authentication delays.

In contrast, SMGKM offers qualitative benefits by decentralising some parts of the DKD tasks such as offloading the authentication and key management functions to the intermediate AKDs [5]. This was also inspired by the fact that each AKD has enough computing power capabilities to handle these phases independently to share the load across the entire network hence giving DKD scalability while alleviating the single point of failure problem.

Table 1. Comparison of SMGKM characteristics against Key-Request schemes for a high mobility situation

Evaluation criteria	DeCleene et al [8]	GKMF [9]	Kellil et al [10]	SMGKM [5]
Decentralised framework	Yes	Yes	Yes	Yes
Key independence	Yes	Yes	Yes	Yes
Number of layers	2	2	2	2
Forward secrecy on user handoff	No	No	No	No
Backward secrecy on user handoff	Yes	Yes	Yes	Yes
Rekey all visited clusters at leave	Yes	Yes	Yes	No
1-affect-n phenomenon	Yes	Yes	Yes	No
Localize rekeying at handoff	Yes	Yes	Yes	Yes
AKD to AKD communication	No	No	No	Yes
Support multi-group subscriptions	No	No	No	Yes
Single point of failure	Yes	Yes	Yes	No
DKD scalability	No	No	No	Yes
Use of list to manage mobility	Yes	Yes	Yes	Yes
Authentication at move	No	No	No	Yes
Suitability for high speed mobile users	No	No	No	Yes

Thus, authentication of highly mobile users during frequent handoffs and rekeying of the TEK for the affected services are both performed at the cluster level without involving the DKD. Each AKD keeps track of the users currently residing in its own cluster using the Secure Distribution List (SKDL) [12]. This enables independent generation and management of service keys locally during rekeying without affecting the neighbour clusters.

Additionally, handoff is not synchronised with the DKD, which significantly reduce the signalling load at SMGKM wireline [11]. Also, the control overhead of the DKD, such as maintaining and updating the trace history and the assigned keys for each highly mobile user is alleviated in SMGKM. This however has made SMGKM scheme very simple, but a practical and effective multi-group key management scheme for high speed networks.

4. Performance Analysis

This section investigates the performance of SMGKM scheme with comparisons to legacy key-request schemes by applying two types of rekeying approaches: *Pairwise* and *LKH tree based* [16] rekeying approaches. We also measure the storage complexity in highly mobile users with frequent handoffs.

4.1. Communication Overheads

We focus on the extra rekeying communication overhead emanating from the unicast transmissions caused by delivering rekeying messages, under the assumption that this overhead is the most vital factor in wireless networks where radio resources are limited in the presence of high mobility users participating in multi-services. We also consider the communication overhead induced by the control messages emanating from the handoff and authentication requests at the wired network beyond each AKD.

In this network, let us assume that the various multicast services provided by the SP covers a huge area consisting of C clusters, and the number of mobile users M_i existing in each cluster is maintained at N. Let us define a random variable X as the number of clusters that M_i has visited before leaving the multicast services. Thus, the expected number of clusters previously visited, which represent the degree of user mobility, can be denoted as $E(X)$. Now let us contrast the rekeying communication overhead induced in SMGKM in contrast to the key-request schemes whenever multi-leaves caused by high mobility users occur after visiting multiple clusters. Stopping subscriptions may be due to various reasons such as subscription period elapse or battery failures.

4.1.1 Multi-leaves with Forward Secrecy in Key-Request Schemes

First assume that key-request schemes are used, not considering multi-services and multi-leaves in a wireless mobile network. The key-request schemes achieve more efficiency by limiting rekeying only to the clusters which have been visited by a leaving user. Thus, the rekeying communication overhead is mainly dependent on the number of clusters that a leaving user has visited. Since the leaving user maintains the local cluster keys for each of the visited clusters, each previously visited AKD_i should unicast $O(N)$ rekeying messages including the updated local cluster keys to PIC users of the visited clusters. After updating the local cluster keys, each AKD_i distributes the new TEK from the DKD. This induces rekeying communication overhead in the entire wireless network, $RO_{wireless}$, of

$$RO_{wireless} = E(X) \cdot O(N) + C. \quad (1)$$

Additionally, the key-request schemes require notifying the DKD about users' handoff as well as the TEK update. Though the notifications may be negligible in size, they cannot be overlooked in the presence of high mobility users and multi-services requiring TEK update in the network.

The notifications should be delivered to and from the DKD as a form of a control message in the wired network beyond the AKDs. Therefore, the total number of notifications at the wired network, N_w, on average gives

$$N_w = E(X) \cdot O(N) \cdot C \quad (2)$$

Let us now use a wireless weight denoted as α in [17] to demonstrate the importance of the wireless cost. Therefore, the total rekeying communication overhead for the key-request schemes, $RO_{KEY\text{-}REQUEST}$, induced at the wireline and wireless part of the network becomes

$$RO_{KEY-REQUEST} = \alpha \cdot RO_{wireless} + (1-\alpha) \cdot N_w \quad (3)$$

where $0 \le \alpha \le 1$.

However, in the presence of S-multi-services and x services requiring rekeying at user departure, the key-request schemes perform independent rekeying of the affected services whenever N-multi-leaves occur at the target cluster after visiting $E(X)$ clusters. Thus, equation (3) gives

$$RO_{KEY-REQUEST} = \alpha \cdot (x/S) \cdot RO_{wireless} + (1-\alpha) \cdot (x/S) N_w \quad (4)$$

4.1.2 Multi-leaves with Forward Secrecy in SMGKM

In contrast with the key-request schemes, SMGKM only performs rekeying at the target cluster where multiple departures occur regardless of the number of visited clusters. The DKD does not need to keep track of mobile subscribers because each AKD_i independently controls its own users due to cryptographically separate keys adopted per cluster in SMGKM. Thus, on every handoff, SMGKM provides access control mechanism which uses the SKDL concept [12] for authentication of highly mobile users before obtaining the new service group keys used for service access control at the target cluster. After a complete handoff of a mobile user, the cluster local keys for the previously visited clusters are automatically revoked under the assumption that the mobile users have the capability to store keys only for the target cluster. This is what differentiates SMGKM to the key-request schemes, hence less storage complexity at the mobile receiver [11]. This additionally lessens the number of rekeying communication overheads significantly.

Now let us consider M_1 and M_2 in G_K which finally stop x services after visiting $E(X)$ clusters. We first compute the number of AIC in the visited clusters at user departure. The assumption is that a handoff that occurs between two non-adjacent clusters can be possible, which is tolerable enough to make the performance comparison. Consider a certain cluster v whose AKD initially consists of N mobile users. Assume that N individual users move from one cluster to another at least $E(X)$ times, i.e., highly mobile user visits $E(X)$ clusters. Whenever the users finally drop the subscriptions at departure, only $E(X)$ of the initial N users remain in cluster v while $E(X)-1/E(X)$ of N users have left cluster v. Furthermore, let us also consider other users participating in the same set of services in G_K from other clusters with the exception of cluster v. A user of the other clusters can be considered to pick $(E(X) - 1)$ visiting clusters amongst $(C - 1)$ clusters. Therefore, the probability that the highly mobile user does not visit cluster v can be evaluated using k-permutations of n denoted as $P(n, k)$ or k-combinations of an n-set denoted as $C(n, k)$ in elementary combinatory contexts. Thus, the value of $P(n,k)$ over k factors is generally given by the product:

$$P(n,k) = \begin{cases} \dfrac{n!}{(n-k)!} & for\ k < n \\ 0 & otherwise \end{cases}. \quad (5)$$

The value of $P(n, k)$ is well defined without the assumption that n is a non-negative integer. However the convention of permutation is closely related to combination. Thus, a k-element combination of an n-set S is a k-element subset of S, the elements of which are unordered. For example, by taking all the k element subsets of S and ordering them individually in all conceivable ways, we obtain all the k-permutations of S. Therefore the number of k-combinations of an n-set, $C(n, k)$, relate to the value of $P(n, k)$ by:

$$C(n,k) = \frac{P(n,k)}{P(k,k)} = \frac{n!}{(n-k)!k!} \quad (6)$$

Note that the values in equation (5) and (6) are known as binomial coefficients and can be represented as $\binom{n}{k}$. By using this representation, where n denote the cluster variations of C and k denote factors of the visited clusters $E(X)$, as the highly mobile user handoffs, we can evaluate the probability P_{PIC}, that the highly mobile user does not visit the target cluster v as:

$$P_{PIC} = \binom{C-2}{E(X)-1} / \binom{C-1}{E(X)-1} \quad (7)$$

Therefore, by using the relation in equation (7), we can obtain the number of highly mobile users that has visited the target cluster v from other clusters as:

$$P_{AIC} = 1 - N \cdot P_{PIC}. \quad (8)$$

Likewise, only $1/E(X)$ of the N users remain in cluster v while $E(X)-1/E(X)$ of the N users have left. Consequently, the number of AICs in the visited clusters, denoted by L, can be calculated as:

$$L = E(X) - 1/E(X)[N + (C-1)P_{AIC}] \quad (9)$$

In contrast to the key-request schemes, since SMGKM independently manages its own TEK per cluster, the visited AKDs do not undergo rekeying except the target cluster where multi-leaves currently occur under the assumption that leaves occur concurrently while participating in multi-services. It should be noted that it is possible for multi-leaves to occur at various locations visited (i.e., $E(X)$) in SMGKM as shown in Figure 1. Therefore, in order to guarantee *forward secrecy* at the concerned cluster, SMGKM needs to unicast O(N+L) rekeying messages to the PIC user of the concerned clusters in order to deliver the updated TEK shares for the services affected by multi-leaves. Additionally, SMGKM does not need to notify the DKD about the user mobility since AKD_i automatically revokes the rows for the corresponding departures from $SKDL_i$. However, the notification of the updated TEK shares at the concerned AKD_i to the SP is absolutely necessary at the wired part of SMGKM. The notification/control message uses the KUS notifier which is negligible in size and dependent on the number of affected services x, assuming that the SP also has prior knowledge of the KUS operation to update the service keys. This on average gives the total number of notifications, N_n, beyond the concerned clusters as:

$$N_n = E(X) \cdot O(x/S). \quad (10)$$

Therefore, in the presence of S-multi-services and x services requires rekeying if L-users departure, SMGKM induces total rekeying communication overhead of

$$RO_{SMGKM} = \alpha\{E(X) \cdot O(N+L)\} + (1-\alpha)N_n. \quad (11)$$

If we apply the LKH rekeying approach to equation (4) and (11), we employ the well-known fact that rekeying of a balanced tree of degree d accommodating N users requires $d \log_d N$ rekeying messages for a leaving user. This equivalently reduces the rekeying communication overheads logarithmically with the number of leaving users. Thus, equations (4) and (11) respectively become:

$$RO_{KEY-REQUEST} = \alpha \cdot (x/S) \cdot O(d \log_d(N) + (1-\alpha) \cdot (x/S) N_w \quad (12)$$

and

$$RO_{SMGKM} = \alpha\{E(X) \cdot O(d \log_d(N+L))\} + (1-\alpha)N_n \quad (13)$$

4.2. Storage Overheads

High mobility users maintain the local cluster key management keys for the previously visited clusters in the key-request schemes as they perform frequent handoffs. This may reasonably add storage complexity to the resource constraint mobile devices, the AKD and the DKD, hence slow execution and slow accessibility to the stored keys in the underlying system. This section measures the number of keys held by the participating network entities at each network level. Assume that N high mobility individual users perform frequent handoff by visiting at least $E(X)$ clusters of the available C clusters while participating in x of the total S available multicast services in the underlying system. The expected storage complexity in key-request schemes and SMGKM after N high mobility users' participating in x of the S services visit $E(X)$ clusters out of C total clusters is summarised in Table 2. The simulation scenarios presenting the storage complexity of the underlying system in the presence of high speed users is presented in section 5.

Table 2. Comparison of storage complexity during high mobility

Storage overhead	KEY-REQUEST SCHEMES			SMGKM
	DeCleene et al [8]	GKMF [9]	Kellil et al [10]	
At the user	(x/S+2)E(X)	(x/S+3)E(X)	(x/S+3)E(X)	(x/S)+2
At the AKD	(N+1)E(X)	(N+4)E(X)	(N+2)E(X)	N+1
At the DKD	(x/S) E(X)	(x/S+2)E(X)	(x/S) E(X)	N

5. Simulation Results and Discussion

To compare the performances of the above schemes, we consider S-multicast services covering a huge cellular cluster decentralised topology containing 1000 clusters under the assumption that each cluster has a total of 400 mobile users subscribed to these services from various locations. The expectation is that each user is likely to visit $E(X)$ clusters on average before leaving the subscribed multicast services simultaneously, where $E(X)$ varies from 10 to 60.

A higher $E(X)$ means that a user has the higher mobility. Also, the assumption is that the wireless cost of the network is much greater than wire line cost. Hence, we set the wireless weight to be 0.999 in order to weight wireless links much more than wired links. To summarize, we set the hypothetical parameters as x=3 to be the number of affected services requiring rekeying out of S=8 total multicast services provided by the SP, C=1000, N=400, α=0.999, respectively. We use the MATLAB simulation tool to represent the simulated results in the next section.

5.1. Communication Overheads

From the simulation results in Figure 2, we compare the communication overheads emanating from employing a *pairwise* [18] rekeying approach including the handover control messages at both the wireless and wireline parts of the SMGKM framework. It can be seen from Figure 2 that by employing *pairwise* rekeying approach, the performances of both schemes degrade with high user mobility and multi-leaves participating in multi-services.

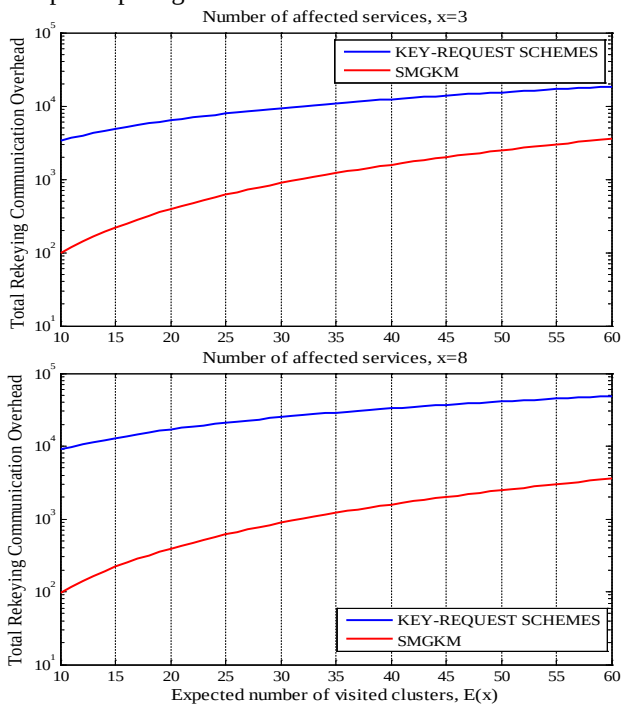

Figure 2. Communication overheads emanating from pairwise rekeying and control messages

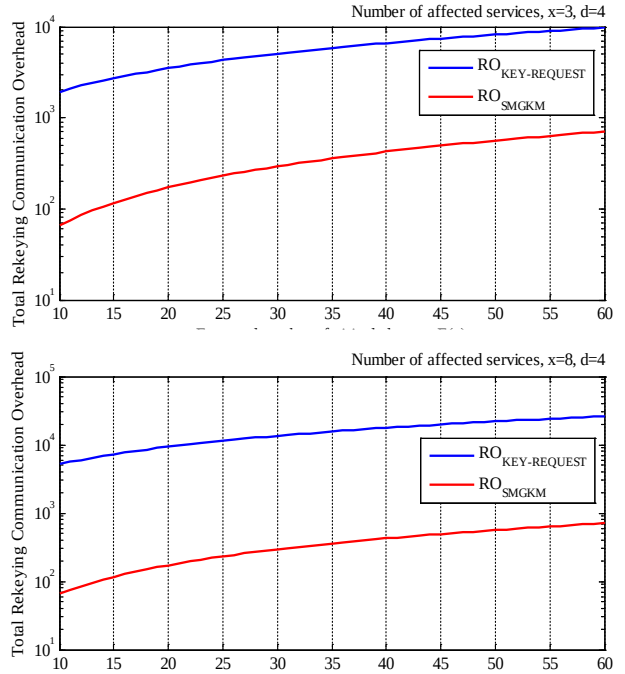

Figure 3. Communication overheads emanating from LKH rekeying and control messages

However, the SMGKM overhead outperforms that of the key-request schemes because high mobility users in key-request schemes maintain the key management keys for the local $E(X)$ clusters. This requires rekeying that incurs substantial rekeying communication overhead. In contrast, SMGKM only rekeys the concerned clusters where user departure occurs hence reducing communication overheads significantly.

If we employ the *LKH tree* rekeying approach with a balanced tree of degree d =4 at the affected clusters, the communication overheads reduces logarithmically with the number of leaving users for both the schemes, as shown in Figure 3. Some tree based rekeying approaches such as the TMKM-based scheme [17] can be used in the underlying system to achieve more efficient rekeying than the LKH scheme by limiting the users who should be updated to only the users in the cells which have been visited by the leaving users.

5.2. Communication Overheads Ratio

Additionally, in Figure 4 we further compare the ratio of the communication overheads for the concerned schemes.

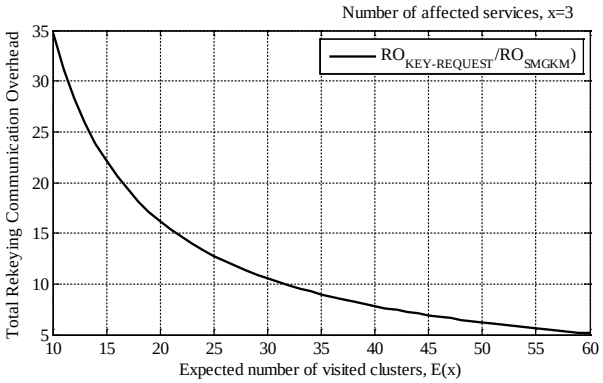

Figure 4. Relative communication overhead (the ratio $RO_{Key\_request}$ to that of RO_{SMGKM})

It can be observed in Figure 4 that when $E(X)$ =30, the key-request schemes incur 10.6 times communication overheads as much as that of the SMGKM scheme. Therefore, the SMGKM obtains quantitative advantage of less communication overheads and qualitative advantage of distributing some parts of the DKD functions to the AKDs.

5.2. Storage Overheads

In order to compare the storage complexity caused by high mobility users for the concerned schemes, we set the same parameters for simulation. From the simulation scenarios in Figure 5, it can be observed that the key-request schemes add high storage complexity to the resource constraint highly mobile user M_i by introducing additional local cluster keys for localising rekeying. Thus, as the number of visited clusters E(X) increases, a highly mobile user device may lose connection to other subscriptions due to lack of storage space requirement. In contrast to

SMGKM, extra storage requirement is not necessary because high mobility users only maintain the key management keys for the cluster where they currently reside, hence incurring less storage complexity at the communicating entities. This is also advantageous because repeated rekeying becomes unnecessary in SMGKM, hence reduced rekeying signalling overheads. The compromise to the keys held by the local users in SMGKM is limited to the currently serving AKD without affecting the neighbour clusters.

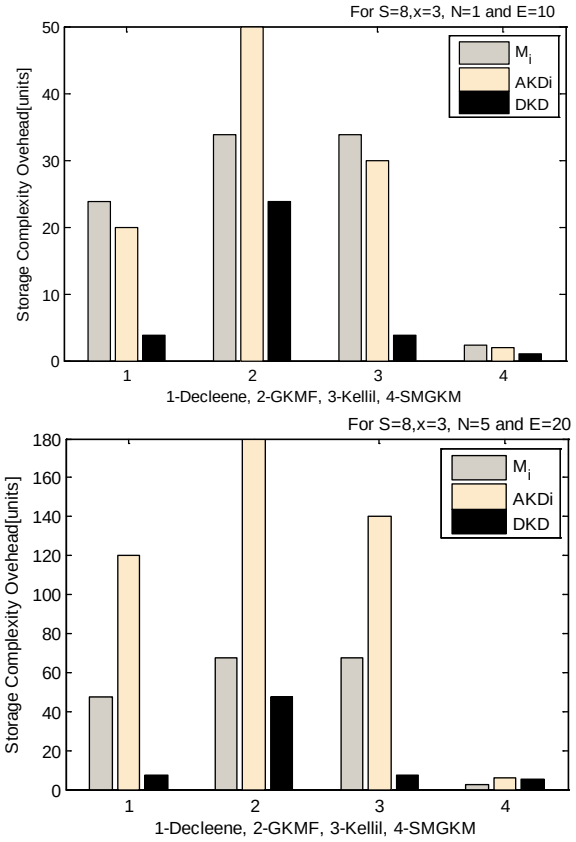

Figure 5. Storage complexity in high mobility situation

It can also be observed that some key-request schemes such as GKMF and Kellil et al. induce high storage overhead at the limited resource mobile users by introducing more encryption keys as E(X) and x variables increase. This may accelerate more power drainage, hence high likelihood of service disruptions. However, both the schemes increase the storage complexity at the intermediate keys AKDs because AKDs are assumed to have sufficient space and power to process the key management keys. It can also be observed that SMGKM gives the DKD storage scalability to accommodate more high mobility users, assuming M_i stays longer in the system without dropping subscriptions.

6. Conclusion

This paper has addressed the inefficiency of existing key-request GKM schemes for secure multicast in high mobility wireless networks by proposing an efficient and practical solution. The core of the proposed scheme is to decentralise the DKD key management and authentication functions. While the DKD only does the initial setup phase of the entire group membership, each AKD keeps track of users during handoff and manages the group TEK shares for multiple services independently per cluster to guarantee both *backward* and *forward secrecy* when frequent handoffs and multi-leaves participating in multi-services occur respectively. The proposed scheme also achieves high efficiency with significant reduction in the system communication overheads as well as reduced storage complexity in the communicating agents while preserving secrecy of services. The SMGKM also reduce the overburden of the DKD by distributing it to the intermediate AKDs in high mobility environments. Therefore, it is expected that the proposed protocol can be a practical solution for securing group communication with multi-services in high speed wireless networks.

Acknowledgements.

This work was supported partially by TSB UK under grant application KTP008734, MoESD-DTEF (Ministry of Education Skills & Development Planning, Department of Tertiary Education & Financing) and BIUST (Botswana International University of Science & Technology, Gaborone, Botswana.

References

[1] J. F. Monserrat, J. Calabuig, A. Fernandez-Aguilella, and D. Gomez-Barquero, "Joint Delivery of Unicast and E-MBMS Services in LTE Networks," *IEEE Transactions on Broadcasting*, vol. 58, pp. 157-167, 2012.

[2] Y. Challal and H. Seba, "Group Key Management Protocols: A Novel Taxonomy," *Enformatika, International Journal of Information technology*, vol. 2, 2005.

[3] T. T. Mapoka, "Group Key Management Protocols for Secure Mobile Multicast Communication: A Comprehensive Survey," *International Journal of Computer Applications*, vol. 84, 2013.

[4] B. Daghighi, M. L. M. Kiah, S. Shamshirband, and M. H. U. Rehman, "Toward secure group communication in wireless mobile environments: Issues, solutions, and challenges," *Journal of Network and Computer Applications*, vol. 50, pp. 1-14, 2015.

[5] T. T. Mapoka, S. J. Shepherd, and R. A. Abd-Alhameed, "A New Multiple Service Key Management Scheme for Secure Wireless Mobile Multicast,"*IEEE Transactions on Mobile Computing*, vol. 14, pp. 1545-1559, 2015.

[6] T. T. Mapoka, H. M. AlSabbagh, Y. A. Dama, S. J. Shepherd, R. Abd-Alhameed, M. Bin-Melha, *et al.*, "A Multi-service Cluster-Based Decentralized Group Key Management Scheme for High Mobility Users," in *Wireless Internet*, ed: Springer, 2015, pp. 305-312.

[7] T. T. Mapoka, H. M. AlSabbagh, Y. A. Dama, M. Bin-Melha, and K. O. Anoh, "A Multi-service Cluster-Based Decentralized Group Key Management Scheme for High Mobility Users," in *Wireless Internet: 8th International Conference, WICON 2014, Lisbon, Portugal, November 13-14, 2014, Revised Selected Papers*, 2015, p. 305.

[8] B. DeCleene, L. Dondeti, S. Griffin, T. Hardjono, D. Kiwior, J. Kurose, *et al.*, "Secure group communications for wireless networks," in *Military Communications Conference, 2001.*

MILCOM 2001. Communications for Network-Centric Operations: Creating the Information Force. IEEE, 2001, pp. 113-117 vol.1.

[9] M. L. M. Kiah and K. M. Martin., "Host Mobility Protocol for Secure Group Communication in Wireless Mobile Environments," *International Journal of Security and its Applications*, vol. 2, pp. 39-52, January 2008.

[10] M. Kellil, Olivereau, J. C. A., and P. Janneteau, "Rekeying in secure mobile multicast communications," *United States Patent Application Publications*, US 2007/ 0143600 A1 2007.

[11] T. T. Mapoka, S. Shepherd, R. Abd-Alhameed, and K. O. O. Anoh, "Novel rekeying approach for secure multiple multicast groups over wireless mobile networks," in *International Wireless Communications and Mobile Computing Conference (IWCMC)*, 2014, pp. 839-844.

[12] T. T. Mapoka, S. J. Shepherd, R. Abd-Alhameed, and K. O. O. Anoh, "Efficient authenticated multi-service group key management for secure wireless mobile multicast," in *Third International Conference on Future Generation Communication Technology (FGCT)*, 2014, pp. 66-71.

[13] Y. Challal, H. Bettahar, and A. Bouabdallah, "SAKM: a scalable and adaptive key management approach for multicast communications," *SIGCOMM Comput. Commun. Rev.*, vol. 34, pp. 55-70, 2004.

[14] Y. Challal, S. Gharout, A. Bouabdallah, and H. Bettahar, "Adaptive clustering for scalable key management in dynamic group communications," *Int. J. Secur. Netw.*, vol. 3, pp. 133-146, 2008.

[15] T. T. Mapoka, S. J. Shepherd, R. Abd-Alhameed, and K. O. Anoh, "Handover Optimised Authentication Scheme for High Mobility Wireless Multicast." in 15th *International Conference on Computer Modelling and Simulation (UKSim2015)*, 2015,

[16] W. Chung Kei, M. Gouda, and S. S. Lam, "Secure group communications using key graphs," *Networking, IEEE/ACM Transactions on*, vol. 8, pp. 16-30, 2000.

[17] S. Yan, W. Trappe, and K. J. R. Liu, "Topology-aware key management schemes for wireless multicast," in *Global Telecommunications Conference, 2003. GLOBECOM '03. IEEE*, 2003, pp. 1471-1475 vol.3.

[18] L. R. Dondeti, S. Mukherjee, and A. Samal, "Scalable secure one-to-many group communication using dual encryption," *Computer Communications*, vol. 23, pp. 1681-1701, 11/1/ 2000.