SCIENCE CHINA
Information Sciences

• HIGHLIGHT •

September 2017, Vol. 60 098104:1–098104:3
doi: 10.1007/s11432-016-9048-8

Area-based mobile multicast group key management scheme for secure mobile cooperative sensing

Jie CUI, Hong ZHONG*, Weiya LUO & Jing ZHANG

School of Computer Science and Technology, Anhui University, Hefei 230601*, China*

Received November 24, 2016; accepted January 21, 2017; published online August 2, 2017

Citation Cui J, Zhong H, Luo W Y, et al. Area-based mobile multicast group key management scheme for secure mobile cooperative sensing. Sci China Inf Sci, 2017, 60(9): 098104, doi: 10.1007/s11432-016-9048-8

In this study, we propose a novel key management model for localized mobile groups that employ multicasting. The service provisions will not be interrupted while users move among different wireless network areas, while each network provides the respective multicast services independently. All the mobile users in a given area form a cluster managed by an area key distributor (AKD) [1], and the AKD takes charge of the distribution of a key and updates the clusters accordingly. In our model, a special security coprocessor (SC) is embedded in the mobile client to facilitate the secure calculation of a group key. After receiving rekeying information, a mobile device calculates the group key entirely on the client side, which avoids the direct transmission of the key.

LKH [2] is one of the most commonly used methods in the group key management model. In LKH, the leaf nodes represent the users, which store the private key, the root node of LKH stores the group key, and the remaining nodes store the key encryption keys (KEK). The method proposed by Zhang et al. [3], which uses immediate rekeying (IR), meets the demand of both forward and backward secrecy. The single multicast servers are the only option in this model, resulting in a large number of rekeying requests each time users join or leave.

A few GKM strategies have successfully reduced the time required for rekeying; these include GKMF [4]. The method proposed by Kellil et al. [5] contends by means of delayed rekeying (DR). However, these methods may cause one-affect-n phenomenon. An SMGKM method was suggested by Mapoka et al. [6] that employs a list to distribute the keys contained in each session, and to update the keys to mitigate one-affect-n phenomenon. Nevertheless, methods of this category do not guarantee forward secrecy.

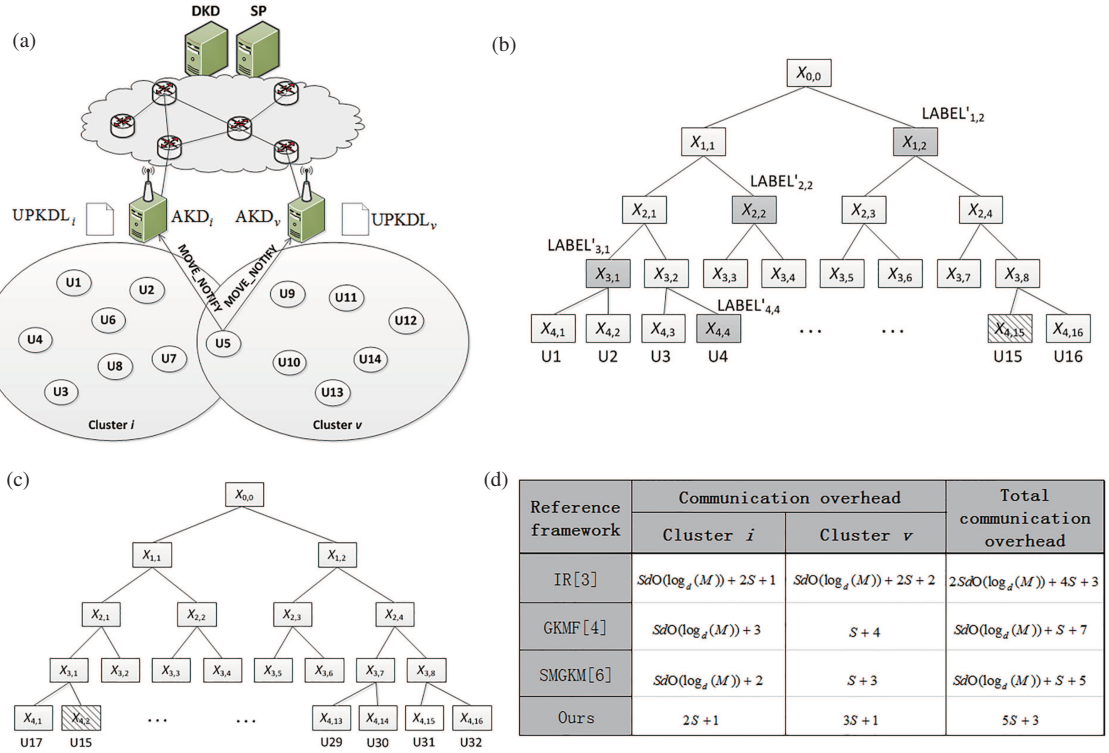
Algorithm overview. Our model is constructed in two layers, and the decentralized framework is illustrated in Figure 1(a). The first layer is the domain layer, which is the main wired component subject to the domain key distributor (DKD). The second layer is in charge of sequential AKD.

Step 1: Initial key distribution. After the generation of a key that is used over a long period of time (sk) by the DKD, which is then shared with all other AKDs, sk, the serious task. Then, the data of the service sent from the aforementioned DKD to every AKD are encoded. In addition, the data derived between each two AKDs are coded with sk as well.

AKD generates a pair of keys (e, d), where d represents the private key kept by AKD and e represents the public key that is distributed to the users in a given cluster. For each multicast service, AKD establishes a corresponding LKH to manage keys, respectively. As shown in Figure 1(b), the LKH is a complete binary tree, and all the nodes in the tree have a LABEL

* Corresponding author (email: zhongh@ahu.edu.cn)

The authors declare that they have no conflict of interest.



(d)

Reference framework	Communication overhead		Total communication overhead
	Cluster i	Cluster v	
IR[3]	$Sd\mathrm{O}(\log_d(M))+2S+1$	$Sd\mathrm{O}(\log_d(M))+2S+2$	$2Sd\mathrm{O}(\log_d(M))+4S+3$
GKMF[4]	$Sd\mathrm{O}(\log_d(M))+3$	$S+4$	$Sd\mathrm{O}(\log_d(M))+S+7$
SMGKM[6]	$Sd\mathrm{O}(\log_d(M))+2$	$S+3$	$Sd\mathrm{O}(\log_d(M))+S+5$
Ours	$2S+1$	$3S+1$	$5S+3$

Figure 1 Illustration of scheme and analysis results. (a) Reference framework; (b) updated LKH of cluster i after U15 left; (c) updated LKH of cluster v after U15 joined; (d) comparison of communication overhead.

whose value remains constant. The root node has $\mathrm{LABEL}_{0,0}$, which is generated by AKD. Other nodes' LABELs in LKH are generated by their parents through the pseudo-random sequence generator G, such as $\mathrm{LABEL}_{2,2} = G_R(\mathrm{LABEL}_{1,1}) = G_R(G_L(\mathrm{LABEL}_{0,0}))$. The leaf nodes are then distributed among mobile users. The number of users is less than the total number of leaf nodes to meet the demand of users' dynamic changes, which means that the LKH needs to set up some redundant left nodes according to the actual situation. When a user joins the group, the first left leaf node will be assigned to that user.

After the mobile user Ui registers with and subscribes to one or several multicast services, the DKD makes the first attempt in generating lk_j, a private key. The generation of safe key distribution that is privately used by a customer serves for corresponding AKD_i, and every row stores the profile of a user who signed in within the cluster area i. The UPKDL_i includes both the private key that only belongs to a mobile user and his or her service ID that is subscribed. UPKDL_i rows are coded by the DKD with sk and sent to AKD_i, and AKD_i keeps its corresponding UPKDL_i.

Each UPKDL_i row contains the personal information of a mobile user, which is encrypted with sk. When AKD_i receives the UPKDL_i rows from DKD, AKD_i distributes the corresponding LKH leaf nodes to the new user according to the user's subscription. Then AKD_i assigns brother nodes' LABEL of all the nodes on the path, from the root node to the corresponding leaf node to the user through a secure channel. Assuming that the user Ui is in the group, AKD will distribute the free leaf node $X_{3,2}$ to Ui, AKD assigns a short-term private key and LABEL information $(\mathrm{LABEL}'_{3,1}, \mathrm{LABEL}'_{2,2}, \mathrm{LABEL}'_{1,2})$ to Ui, where $\mathrm{LABEL}'_{i,j} = E_{ki}(\mathrm{LABEL}_{i,j})$, the encryption algorithm E cannot be broken into polynomial time. It can be known that the user does not know the LABELs in LKH, because LABEL$'$ is encrypted through his short-term private key. In addition, encryption algorithm E is stored in SC and the user cannot access it. Therefore, all users will get different LABEL$'$s even for the same node of LKH. Each time a user joins the cluster, AKD will reassign a new short-term private key to him. Therefore, even if a user frequently leaves and joins a group, he/she will obtain different LABEL$'$ every time.

Step 2: Rekeying when a user leaves. When mobile users move from the cluster i to the target cluster v, AKD_i must update the keys of cluster i to ensure forward security. Similarly, in order to ensure backward security and continuity of services, AKD_v must update the affected keys.

Assume that U15 has subscribed to multicast

service 1 and multicast service 2, where the multicast service 1 represents LKH as shown in Figure 1(b). Group key of service 1 is K_i, leaf node of U15 is $X_{4,15}$ and short-term private key is k_{15}. When U15 moves from cluster i to the target cluster v, AKD_i transmits the UPKDL_i row of U15 to the target AKDv and then update the UPKDL_i by deleting the corresponding row. To satisfy forward security criterion, AKD_i needs to update the keys of service 1 in this cluster. AKD_i first generates a random number r and then broadcasts rekeying information $\{\{X_{0,0}, X_{1,2}, X_{2,4}, X_{3,8}, X_{4,15}, r\}_{K_i}\}_{d_i}$, where $\{A\}_B$ means A is encrypted by B and d_i is the private key of AKD. After receiving the rekeying information, users first verify the legitimacy of the information through AKD_i's public key e_i. Only the users who subscribe to multicast service 1 could decrypt the ciphertext and get the rekeying information, and then users can calculate the new group key by themselves.

Every user has one of the LABEL′s about nodes $\{X_{0,0}, X_{1,2}, X_{2,4}, X_{3,8}\}$ except for U15 and U16. For example, as shown in Figure 1(b), U3 has $\{\mathrm{LABEL}'_{4,4}, \mathrm{LABEL}'_{3,1}, \mathrm{LABEL}'_{2,2}, \mathrm{LABEL}'_{1,2}\}$. U3 can calculate $\mathrm{LABEL}'_{2,4}$ and $\mathrm{LABEL}'_{3,8}$ through SC and his private key k_3 according to $\mathrm{LABEL}'_{1,2}$, and then input $\mathrm{LABEL}'_{3,8}$, k_3 and random r in SC, U3 can get new group key $K'_i = E_r\left(G_L(D_{k3}(\mathrm{LABEL}'_{3,8}))\right) = E_r(\mathrm{LABEL}_{4,15})$. U15 and U16 have no LABEL′ about $\{X_{0,0}, X_{1,2}, X_{2,4}, X_{3,8}\}$, so that they cannot calculate the $\mathrm{LABEL}'_{3,8}$ as well as the new group key K'_i. As for U16, ADK_i would unicast the rekeying information $\{K'_i\}_{\mathrm{lk}_{16}}$ to the user, where lk_{16} is the long-term private key of U16. Therefore, every user can receive the new group key K'_i except for U15.

Step 3: Rekeying when a user joins. After receiving the UPKDL_i rows sent by AKD_i, AKD_v can obtain the newly-joining mobile user's personal private key as well as the subscribed service ID. When users arrive at the target cluster, AKD_v verifies their identity first. If users are authorized, they are assigned with LKH leaf nodes of the corresponding multicast service according to their service subscription. In order to ensure the continuity of service and backward security, AKD_v needs to update the affected keys and UPKDL_v.

The LKH of multicast service 1 in cluster v is shown as Figure 1(c). When U15 joins the cluster v, AKD_v retrieves all the leaf nodes to find a free node. Assume that the first free leaf node is $X_{4,2}$ selected to be assigned to U15, AKD_v generates a short-term private key k_{15} for U15 and calculates a set of LABEL′s as $\{\mathrm{LABEL}'_{4,1}, \mathrm{LABEL}'_{3,2}, \mathrm{LABEL}'_{2,2}, \mathrm{LABEL}'_{1,2}\}$ through k_{15}. AKD_v unicasts $\{\mathrm{LABEL}'_{4,1}, \mathrm{LABEL}'_{3,2}, \mathrm{LABEL}'_{2,2}, \mathrm{LABEL}'_{1,2}, k_{15}, K'_v\}_{\mathrm{lk}_{15}}$ to U15, where K'_v indicates the new group key. AKD_v generates a random number r' and broadcasts rekeying information $\{\{K'_v\}_{K_v}\}_{d_v}$, where $K'_v = E_{r'}(\mathrm{LABEL}_{4,2})$. Therefore, all the users subscribed to multicast service 1 are able to obtain the updated group key. For the rekeying of multicast service 2, a similar method can be used.

Performance analysis. Suppose that the number of services affected is S when a mobile user moves from one cluster to another. The degree of LKH is d. The transmission overhead of communication contained in our model is summarized in Figure 1(d).

Conclusion. This area-based, decentralized, bilevel model improves the self-management of each individual cluster and further ameliorates network load. Unlike some other approaches, backward and forward security criteria are both satisfied. Moreover, our model supports the addition and removal of users and is suitable for practical applications with large groups of users such as VANETs.

Acknowledgements This work was supported by National Natural Science Foundation of China (Grant Nos. 61572001, 61502008), and Natural Science Foundation of Anhui Province (Grant No. 1508085QF132).

Supporting information Appendixes A–D. The supporting information is available online at info.scichina.com and link.springer.com. The supporting materials are published as submitted, without typesetting or editing. The responsibility for scientific accuracy and content remains entirely with the authors.

References

1 Park M H, Park Y H, Jeong H Y, et al. Key management for multiple multicast groups in wireless networks. IEEE Trans Moble Comput, 2013, 12: 1712–1723
2 Wong C K, Gouda M, Lam S S. Secure group communications using key graphs. IEEE ACM Trans Netw, 2000, 8: 16–30
3 Zhang C, de Cleene B, Kurose J, et al. Comparison of inter-area rekeying algorithms for secure wireless group communications. Perform Eval, 2002, 49: 1–20
4 Kiah M L M, Martin K M. Host mobility protocol for secure group communication in wireless mobile environments. In: Proceedings of Future Generation Communication and Networking (FGCN 2007). Washington: IEEE Computer Society, 2007. 100–107
5 Kellil M, Olivereau A, Janneteau C. Rekeying in secure mobile multicast communications. U.S. Patent Application, 10/596786, 2004-12-22
6 Mapoka T T, Shepherd S J, Abd-Alhameed R A. A new multiple service key management scheme for secure wireless mobile multicast. IEEE Trans Mobile Comput, 2015, 14: 1545–1559