EAI Endorsed Transactions
on Energy Web and Information Technologies
Research Article EAI.EU

Multicast Hybrid Group Key Management in Wireless Networks Environment

R. Mahaveerakannan[1,*], Dr. C. Suresh GnanaDhas[2] and R. Rama Devi[3]

[1]Research Scholar, Information Technology, St. Peter's University, Chennai, India
[2]Professor and Head, Department of CSE, Vivekananda College of Engineering for Women, sureshc.me@gmail.com
[3]PG Scholar, VLSI Design, Jansons Institute of Technology, Coimbatore, India, ramarengaraju@gmail.com

Abstract:

Multicasting may be a productive secure group communication components in UAV (Unmanned autonomous vehicles) – MBN (Mobile ad hoc networks) to distribute group key to a variety of recipients. During this paper, we have a tendency to propose a secure information group action and economical delivery of group key management theme, hybrid group key management (HGKM), for multicasting. This approach, contrasted with the Logical Key Hierarchy (LKH), Group Key Management Protocol (GKMP), and One-Way Function Tree (OFT) in multicast group key management approaches, we can improve the operation efficiency of wireless network Environment.

Keywords: Group Key Management, Logical Key Hierarchy, One-Way Function Tree, Unmanned autonomous vehicles, and Mobile ad-hoc networks

Received on 04 May 2018, accepted on 08 July 2018, published on 12 September 2018

3rd International Conference on Green, Intelligent Computing and Communication Systems - ICGICCS 2018, 18.5 - 19.5.2018, Hindusthan College of Engineering and Technology, India

doi: 10.4108/eai.12-9-2018.155560

*Corresponding author. Email:mahaveerakannan10@gmail.com

1. Introduction

Multicast is an efficient way of transmitting data simultaneously to a group of users [1, 2]. In a wireless network environment, multicasting is an efficient secure group communication mechanisms in UAV – MBN for the commercial and military services. However, wireless communication security must be ensured before we can enjoy the efficiency and convenience of wireless multicasting services. Security is an encryption and decryption can be achieved by using a secret key. In existing, how to maintain the secret key is the core issue of secure wireless multicast communication. In this paper, we propose a multicasting group key management approach for – Hybrid group Key Management (HGKM) to take the key management issue in the secure wireless multicast communication. We mainly focus a hybrid group key management approach for wireless networks environment. HGKM, the proposed improve the operation efficiency of the wireless network Environment.

2. Related Work

We call a centralized GKM protocol to an application on operational efficiency and protected information transaction in multicasting group key management (GKM). A GKM is one of the main advantages of our key combination and key update for secure group communication. A product of multicasting group key management methods has been suggested in the paper. In this proposes so as Group Key Management Protocol (GKMP)[2, 3], Logical Key

Hierarchy (LKH)[4, 5], Distributed Logical Key Hierarchy [6], and One-way Function Tree (OFT) [7].

Amongst them, the Logical Key Hierarchy (LKH) method introduced individually by Wallner et al. and Wong et al. are one of the most famous and effective group's key management algorithms. The initial improvement of LKH is to use a hierarchical formation, as shown in Figure 1, to promote key administration.

In an LKH key tree, leaders are associated with the leaf nodes of the tree hold supporting keys (key encryption keys (KEK)), Key Encryption Keys are used to encrypting the group key for key distribution to multicasting group members. When new member changes such as join and leave-taking place of Logical Key Hierarchy, the rekeying / group key procedure is invoked to update the group key and Individual Key along the path thereby ensuring security.

- Communication incompetence: As discussed above, in LKH key tree, group changes affect everyone in the association members, which guides to a quantity of rekeying information transferred with the key server. Yet, any information is added to the members, particularly in cellular systems, because the users in each group are not only logical friends in the key tree but more dynamic neighbours [6, 8].
- Storage incompetence: In that LKH algorithm, users must save a collection of keys. Since the extent of the group rises, so gives the number of keys collected by any user. This happens in storage incompetence of the small weight mobile plans due to the weakness of the storage area.

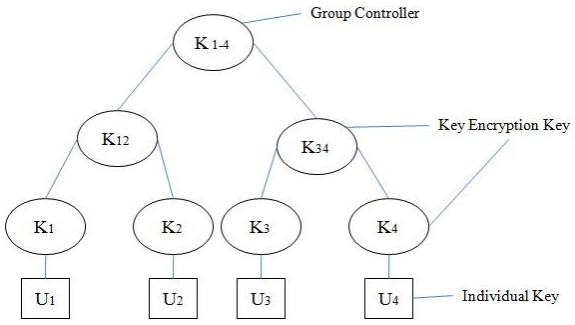

Figure 1: Structure of Logical Key Hierarchy

OFT [7] also does a practical key tree to decrease the communication price of rekeying method, but the character of the tree is double (i.e., each between node has correctly two kids). In opposition to another tree-based key management system which server controls the key source means, OFT recommended handling key source from the members to this root. In the process, the server receives key data with the members at the start of the session. Whenever a join or leave action occurs, the server notifies its members, and the group key is calculated by some members rather of getting it off the server. In those systems, the main problems that require to be examined are the large computation price and the wrong computation from the current key by the members. The OFT experiences from large computation value of these members for join or leaves services, particularly if there is a special movement or various modifications in the key tree.

3. Hybrid Group Key Management:

3.1 Group Key Management Protocol:

The Group Key Management to improve operational efficiency in key management, and multicasting key management in a wireless network environment. The operational efficiency is centralized and decentralized approaches: join and leave operations.

⇒ BKC: Bunch Key Controller
⇒ GKC: group key controller
⇒ {M} K: message M is encrypted by the key K
⇒ $A \rightarrow B$ {message}: User A sends a message to User B via unicast
⇒ $A \rightarrow B$ {message}: User A sends a message to User B via broadcast or multicast

3.2 The Join Operation:

In HGKM, when a new member joins a group, the member join activity begins with the client sending the join request to the BKC (Bunch Key Controller) for authentication.

$$new\ user \rightarrow BKC: \{group\ join\ request\}$$

$$user \rightarrow GKC: \{request\ for\ receiving\ the\ group\ communication\ data\}$$

After receiving the ask for, BKC approving the new client, the BKC sends the new approaching part the gathering key movement encryption key (GKTEK) scrambled with a pairwise key known just to the CKC and the client.

$$BKC \rightarrow new\ user: \{k_{GKTEK}\}k_{BKC} - user$$

$$GKC \rightarrow GKTKC: \{user\ is\ authenticated\}$$

There are two types of the operational efficiency: Joining the unit and leaving the unit.

3.3 Joining unit

Once the Bunch Key Controller finds an open free space in the Joining unit, the BKC relegates the joining part into accessible free that opening. Keeping in mind the end goal to authorize in backward secrecy (Guarantees), the BKC needs to start new keys to supplant the accessible current keys. This rekeying procedure takes after from the base to-top strategy and is isolated into two stages.

Step 1: the BKC refreshes the new keys for the specifically influenced pioneer unit where the new part lives. This rekeying technique is the same as that of LKH.

Step 2: the BKC (any-throws or) multicasts a rekeying message in the gathering key-administration where all outstanding gathering individuals dwell to refresh the GKTEK.

Step 3: The BKC produces and multicasts an incorporated rekeying message which contains all the rekeying messages required by the specifically influenced individuals unit where the new joining part has been doled out.

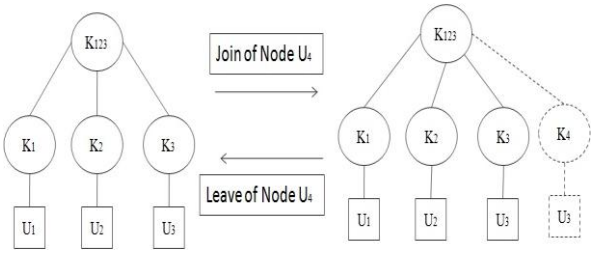

Figure 2: Hybrid group key management joining and leaving operations

Figure 2: hybrid group key management Joining and Leaving operations, the new user u_4 send a request message to BKC accept requisition new u_4 the BKC have to change the current GKTEK and new user forward the key known to the joining new user to ensure backward secrecy.

4. Leave Operation

At the point when a client u_4 leaves the gathering, the BKC need to change all keys known by the leaving client to guarantee forward secrecy to prevent the leaving client from getting to future gathering correspondence. As per our leaving procedure,

5. Leave unit

At the point when a client u_4 leaves the gathering, the BKC need to change the current GKTEK and client behind the keys known to the leaving client to guarantee forward secrecy. There are two stages for BKC summon this rekeying procedure for the rest of the gathering individuals following a "base to-top" approach.

Step 1: the CKC produces rekeying messages for the specifically influenced part unit the part clears out. One coordinated message is required for this progression.

Step 2: the CKC creates rekeying messages for the pioneer units to refresh the CTEK. So as to enhance correspondence effectiveness, all the rekeying messages can likewise be set in one incorporated message. Subsequent to accepting this coordinated

Performance Analysis

Hybrid group key administration to enhance operational productivity is the elite in a remote system condition, multicasting bunch key administration frameworks because of the asset confinements of both UAV – MBN systems and cell phones. In this area, we break down and enhance the operational proficiency of correspondence cost.

So as to assess, the Bunch key controller (BKC) is the predominantly authorize on crossover assemble key administration, the correspondence cost can be estimated with various rekeying messages to transmitted by the BKC amid the join and leave the activity.

A. Communication cost joining and leaving operation

We apply the hypothesis of desire esteem [10, 11] to figure the normal correspondence cost of a join activity in HGKM.

B. Communication cost joining the unit

In HGKM, when another part joins the current gathering part, the correspondence cost is

$$Cost_{communication}(join)$$

$= Cost_{joining\_unit} \times P_{joining\_unit}$ is the quantity of clients in the joining unit. Likewise, BKS creates a rekeying message for the new part to refresh the gathering key for the influenced part unit.

$P_{joining\_unit} \rightarrow$ *Presents the probability of joining member unit*

In HGKM, the probabilities of joining part unit join are:

$$p_{joining\_unit} = \frac{n_{members\_units}}{n_{total\_group\_members}}$$

where $n_{members\_units}$ is the number of members in the units

C. Communication cost leaving the unit

In HGKM, when a part leaves the present gathering, there are leaving part in our proposition: part takeoff from part unit. The part leaving the part unit, the correspondence cost is, the aggregate number of gathering individual's members is $n_{total\_group\_members}$,

The communication cost of the leave action

$$p_{leaving\_unit} = \frac{n_{members\_units}}{n_{total\_group\_members}}$$

The correspondence cost of the Joining and leaving activities in HGKM is that the same and is independent of the assortment of gathering size. The correspondence esteem could be a consistent cost once the measurements of the activity unit might be resolved.

6. Key storage cost

Key stockpiling cost estimates the assortment of keys put away for both the TKC and individuals in the UAV-MBN hubs. In HGKM, because of applying miniaturized scale key administration, a part is appointed to a little agent component where a progressive key tree is worked for key administration. An individual from the task unit subsequently needs to keep a position of keys structure from its leaf hub along the way to the source hub. The quantity of put away keys is h_{unit}+1, where h_{unit} is the tallest from that key tree to the operation unit. Next to these keys, the part likewise needs to store the gathering activity encryption key (GTEK) and the auditorium movement encryption key (CTEK) for taking an interest in the gathering application.

Along these lines, the whole number of keys a part needs to spare is $h_{unit} + 3$. In the event that a part is assigned as a pioneer, it needs to store an additional key - the unit key of the relating part unit. In this way, the whole of keys spared by a pioneer is $h_{unit} + 4$.

As far as LKH and OFT, when these two methodologies are connected in the remote theater, a part likewise needs to spare a gathering of keys from its leaf hub along this way to the source hub, in addition to the GTEK and CTEK. Accordingly, the whole number of spared keys is $h + 2$ (the key for the root node can be served as CTEK), where h is the tallest from that group key tree for LKH and OFT.

On the TKC side, in HGKM, all operation units have the same fixed size, for the entire number of keys saved is: $n_{unit} \times n_{keys\_in\_unit}$

Where n_{unit} is the number of operation units and $n_{keys\_in\_unit}$ is the number of keys stored in the operation unit. If a binary tree is applied within the operational element, the variety of keys saved in the operation unit is:

$$n_{keys_{in_{unit}}} = 1 + 2 + 4 + 8 + \cdots + s_{operation_{unit}}$$

$$= 2s_{operation\_unit} - 1$$

Where $S_{operation\_unit}$ is the size of the operation element

Therefore, the entire number of keys saved on the TKC is:

$$n_{unit} \times n_{keys\_in\_unit} = \frac{s}{S_{operation\_unit}} \times (2s_{operation_{unit}} - 1)$$

In LKH and OFT (assuming the binary tree is also applied), the number of keys saved by the TKC is $1 + 2 + 4 + 8 + \ldots + n = 2s - 1$, where s is the size of the group. Table 10, table the key storage cost for HGKM, LKH, and OFT.

Table 1. The key storage cost for HGKM, LKH, and OFT

GKM	TKC	Group User	
		Leader	Member / Leadership candidate

HGKM	$\frac{s}{s_{operation_{unit}}} \times \left(2s_{operation\_unit} - 1\right)$	$h_{unit} + 4$	$h_{unit} + 3$
LKH	*2s-1*	*h+2*	
OFT	*2s-1*	*h+2*	

$S_{operation\_unit}$: The size of the operation unit in HGKM

S: The size of the group

h_{unit}: The tallest from key structure to the operation element in HGKM

h: The tallest from key tree to LKH and OFT

The gathering size is bigger than that of the task unit. For individuals, the key stockpiling - cost is relative to the tallest of the gathering key structure, which is chosen by the gathering size.

Fig 5 and 6 outline the key stockpiling costs from both the TKC's and individuals point of view in HGKM, LKH, and OFT. We expect the extent of the activity unit is 32 in HGKM.

Table 2. The key storage cost for the TKC and members in HGKM, LKH, and OFT

Size of Group	Number of keys (TKC)		Number of keys (members)	
	LKH & OFT	HGKM	LKH & OFT	HGKM
512	1000	1000	10	8
1024	3100	3100	11	8
2048	4750	4750	12	8
4096	9800	9800	13.5	8
8192	16200	16200	14	8
16384	33900	33900	15.2	8

From table 11, it tends to be seen that, for the TKC, the key stockpiling costs are very comparable in every one of the three methodologies as they all apply a various leveled structure. For individuals, in connection to key stockpiling cost, HGKM has the best execution. In Fig 6, when the length of the operational component is settled, the key stockpiling cost for HGKM turns into a settled cost and private from the gathering size. This advantages clients to deal with the key stockpiling cost on cell phones. Conversely, the key stockpiling cost for individuals from LKH and OFT logarithmically increments with gather estimate development.

7. Conclusion

Wireless network environment in multicasting creates great challenges to the security. In this paper, we tend to project a group key management approach for the wireless network environment in multicasting. Contrasted with the Logical key hierarchy (LKH), our proposals UAV – MBN network reduces the communication cost throughout to boost the operational potency. To provide is a more efficient solution for group key management, the secure multicast in wireless networks.

Reference

[1] Wittmann, R., & Zitterbart,M. (2000). Multicast communication: Protocols and applications. Los Altos: Morgan Kaufmann Pub.
[2] Hardjono, T., & Dondeti, L. R. (2003). Multicast and group security. Artech House Publishers.
[3] H. Harney and C. Muckenhirn, “Group Key Management Protocol (GKMP) Architecture,” RFC 2094, 1997.
[4] H. Harney and C. Muckenhirn, “Group Key Management Protocol (GKMP) Specification,” RFC 2093, 1997.
[5] C.K. Wong, M. Gouda, and S.S. Lam, “Secure group communications using key graphs,” in Proc. ACM SIGCOMM' 98, pp. 68-79,1998
[6] D. Wallner, E. Harder, and R. Agee, “Key Management for Multicast: Issues and Architectures,” RFC 2627, 1999.
[7] O. Rodeh, K.P. Birman, and D. Dolev, “Optimized Group Rekey for Group Communication Systems,” in Proc. Network and Distributed System Security, pp. 39-48,2000
[8] A.T. Sherman and D.A. McGrew, “Key Establishment in Large Dynamic Groups Using One-Way Function Trees,” IEEE Transactions on Software Engineering, vol. 29, no. 5, pp. 444-458, 2003.
[9] K.Brown and S.Singh, "RelM: Reliable multicast for mobile networks," Computer Communication, vol. 21, no.16, pp. 1379-1400, June 1996.
[10] Y.Sun, W.Trappe, and K. J. R. Liu, "An Efficient Key Management Scheme for Secure Wireless

Multicast," presented at IEEE International Conference on Communication, pp 1236-1240, May, 2002
[11] Sherman, A., & McGrew, D. (2003), "Key establishment in large dynamic groups using one-way function trees" IEEE Transactions on Software Engineering, pp. 444–458.
[12] C.M. Grinstead and S.J. Laurie, Introduction to Probability (2nd Edition): American Mathematical Society, 1991.
[13] R.A. Roberts, An Introduction to Applied Probability: Addison-Wesley Publishing Company, 1992.