Hindawi
Security and Communication Networks
Volume 2023, Article ID 9857619, 1 page
https://doi.org/10.1155/2023/9857619

Retraction

Retracted: HGKM: An Efficient Hybrid Group Key Management for Unmanned Autonomous Vehicles MBN in Wireless Network Environment

Security and Communication Networks

Received 13 September 2023; Accepted 13 September 2023; Published 14 September 2023

This article has been retracted by Hindawi following an investigation undertaken by the publisher [1]. This investigation has uncovered evidence of one or more of the following indicators of systematic manipulation of the publication process:

(1) Discrepancies in scope
(2) Discrepancies in the description of the research reported
(3) Discrepancies between the availability of data and the research described
(4) Inappropriate citations
(5) Incoherent, meaningless and/or irrelevant content included in the article
(6) Peer-review manipulation

The presence of these indicators undermines our confidence in the integrity of the article's content and we cannot, therefore, vouch for its reliability. Please note that this notice is intended solely to alert readers that the content of this article is unreliable. We have not investigated whether authors were aware of or involved in the systematic manipulation of the publication process.

Wiley and Hindawi regrets that the usual quality checks did not identify these issues before publication and have since put additional measures in place to safeguard research integrity.

We wish to credit our own Research Integrity and Research Publishing teams and anonymous and named external researchers and research integrity experts for contributing to this investigation.

The corresponding author, as the representative of all authors, has been given the opportunity to register their agreement or disagreement to this retraction. We have kept a record of any response received.

References

[1] R. Mahaveerakannan, S. Velmurugan, S. C. Vijaya Bhaskar et al., "HGKM: An Efficient Hybrid Group Key Management for Unmanned Autonomous Vehicles MBN in Wireless Network Environment," *Security and Communication Networks*, vol. 2022, Article ID 6000375, 23 pages, 2022.

Hindawi
Security and Communication Networks
Volume 2022, Article ID 6000375, 23 pages
https://doi.org/10.1155/2022/6000375

Research Article

HGKM: An Efficient Hybrid Group Key Management for Unmanned Autonomous Vehicles MBN in Wireless Network Environment

R. Mahaveerakannan,[1] **S. Velmurugan**,[2] **Seelam Ch Vijaya Bhaskar**,[3] **R. Jothi Chitra**,[4] **Z. H. Kareem**,[5] **K. Sakthidasan Sankaran**,[6] **T. Venkatesh Kanna**,[7] **and Ruth Chweya**[8]

[1]*Department of Computer Science and Engineering, Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences, Chennai, Tamil Nadu, India*
[2]*Department of Mathematics, School of Arts, Sciences, Humanities and Education, Sastra Deemed to be University, Thanjavur, India*
[3]*Department of IT, MVSR Engineering College, Hyderabad, India*
[4]*Department of Electronics and Communication Engineering (ECE), Velammal Institute of Technology, Panjetty, India*
[5]*Medical Instrumentation Techniques Engineering Department, Al-Mustaqbal University College, Babylon, Iraq*
[6]*Department of Electronics and Communication Engineering (ECE), Hindustan Institute of Technology and Science, Chennai, India*
[7]*Bharath Institute of Higher Education and Research, 173 Agaram Main Road, Selaiyur, Tambaram 600073, Chennai, India*
[8]*School of Information Science and Technology, Kisii University, P.O. Box 408, Kisii, Kenya*

Correspondence should be addressed to Ruth Chweya; rchweya@kisiiuniversity.ac.ke

Received 28 June 2022; Revised 18 July 2022; Accepted 21 July 2022; Published 4 October 2022

Academic Editor: Irshad Azeem

Mobile ad hoc networks (MANET) have been seen as a related advancement to Group Key Management (GKM) applications. Remembering the true objective to guarantee amass applications and disallow uncertified clients from getting to the correspondence data that cannot be anchored by a remote MANET, including IP multicast, the singular gathered data content must remain encoded by a typical shared gathering key. Key administration is required to anchor the assurance of gathering the key and to safeguard those gathering data. GKM framework is associated with the remote system condition partners with three issues: execution, security, and system versatility. This article focuses on the Unmanned Aerial Vehicle (UAV)-mobile backbone node (MBN) remote system performance. The UAV-MBN Network condition is a military system that includes a proposal to group an important administrative structure. A half-and-half gathering key administration technique, which works on each target of UAV-MBN, is included in an arrangement to start two basic remote gathering key administration difficulties: (1) operational performance and (2) multiple-enrollment development. By working with minimal small-scale key administration, this strategy can diminish the execution cost associated with the key administration along with the increment operational execution of remote GKM. Scaled-down key organization is carried out in the context of these movement units. The key administration approach also restricted the operational procedure and decreased the operation's cost in terms of key generation, figuring, and associated correspondence. Overall, the HGKM strategy that has been introduced enhances the operational process and functions effectively in reasonable remote areas.

1. Introduction

Gathering key administration requires perceiving a framework to proficiently appropriate keying components to local individuals and increment the operational execution, which is to be disseminated by expansive needs. This turns out to be more perilous if the gathering key administration technique is utilized inside the remote system condition because of the significant asset requirement of both UAV-MBN remote systems and versatile gadgets. Scarcely any gathering key administration strategies exist and keep examining [1, 2]. However, the experience has unsafe operational execution issues with the possibility that they have utilized as a part of the remote target-based structure identified with that of the UAV-MBN remote system [3]. As a result of the emergence of wireless ad hoc networks, group activities have also become increasingly common. To protect group applications and prevent unauthorized users from accessing network information that cannot be secured by wireless ad hoc networks and IP multicast alone, group communication material must be encrypted using a shared group key [4, 5]. To ensure both group communication and the privacy of this shared key, key management is essential. When group key management solutions are employed in a wireless environment, however, efficiency, reliability, and network compatibility issues arise [6, 7]. In this paper, any cutting-edge innovation in remote GKM technique called half-and-half gathering key administration (HGKM) is arranged to be performed in the UAV-MBN framework in view of this propelled remote gathering key administration structure [8]. The use of UAV-MBN networks in a hostile environment is another situation being taken into consideration for deployment. The secrecy and power of the group key utilized determine the security of group communication [9, 10]. Backward secrecy prevents presently enrolled members from accessing prior group data, whereas forward secrecy prevents former group members from gaining access to future group data [11, 12]. This advanced innovation bunch key administration strategy, HGKM to UAV-MBN, is made and discusses the execution difficulties with e going with suppositions: a moment key organization system licenses the use of the small-scale key organization techniques to manage the execution of both key controller and social occasion people; a cross-consolidated with decentralised key organisation request that enables people to interface to enter an organisation in line to decrease a couple of expenses to each key controller amid rekeying; a solitary message trade structure that backs the trustworthy movement information; and adding key regulator for empowering alternative key in the midst of that hand off. A backbone is provided by mobile backbone nodes, allowing for final communication. The MBNs' primary objective is to offer a mobile infrastructure that makes network-wide communication easier. Backbone nodes are utilized in an MBN-based ad hoc network, and they function similarly to dependent stations in cellular networks. As opposed to the latter, these nodes in an MBN system are mobile and are dynamically chosen to best follow the movement patterns of the engaged components and most respond to the physical and geographical features of operations [13, 14].

In the master-minded group, the key management [2] system with the objective of Diffie–Hellman key exchange [15, 16] and tree Diffie–Hellman key management [17, 18] is never a specific key regulator that controls the social event key and keep-up keys. A group member is dynamically chosen to create and distribute keys to other group members. Because any partition could continue to work by selecting a key server, this technique is more dependable and hence better suited to many groups [19, 20]. The drawback is that, similar to the TTP scenario, a key server must establish long-term pair-wise secure channels with each active group member to distribute the group keys. As a result, establishing these routes each time a new key server enters the picture is extremely costly [21, 22]. The social occasion key has developed in such a way that each part gives its individual parts to check the obtained amass key. Different high exponential assessments need a key that cannot be supported by different devices taking an interest in UAVs. They have been used in remote target-based structures similar to those of the UAV-MBN remote system. They may have dangerous operational execution difficulties. Another scenario being considered for deployment is the usage of UAV-MBN networks in a hostile environment. The secrecy and strength of the group key that is used as a result determine the security of group communication. This cutting-edge innovation bunch essential administration strategy, HGKM with UAV-MBN, is designed to talk about the execution issues of ongoing hypotheses. Different high exponential assessments require the key, which cannot be supported by various UAV-interested gadgets. Moreover, inside the methodology for enrolling social event keys, all parts are required to express enthusiasm inside the gathering following an appropriated transmission [23] appears, a long model for enormous get-togethers is. Circled group key management [24] systems suitably direct the key interfacing fast in the midst of key age. Two certified execution issues to be particular, exorbitant estimation is essential and the direct fast of key characteristics and age keeps the spread key organization [25] approach from being associated with the UAV-MBN [26] sort out. The incorporated GKM frameworks [27], for example, LKH [28, 29] and OFT [2], also confront working efficiency issues and are sent in the UAV-MBN organize. A multihop wireless network with autonomy is called MANET. Configuration changes might be frequently and unpredictably caused by the mobility of MANET nodes. The majority of MANET research makes the assumption that a node's network-related knowledge, including its IP address, net mask, and so forth, is permanently configured before the node joins the MANET. Not all nodes, meanwhile, have IP addresses that are assigned to them permanently. These nodes employ a dynamic host configuration protocol, such as DHCP [30], to obtain an IP address and depend on a centralized server.

The concentrated gathering key organization, all gathering individuals, is composed of a solitary various-leveled key tree. Once a membership change occurs, the rekeying

affects all remaining members in the key tree and creates an impact on the high maintenance cost of the key tree. To perform key management efficiently, a hierarchical key tree needs to be as balanced as possible. However, in a highly dynamic group, managing a key tree's balance is difficult. It is also costly in terms of system resources. Finally, to achieve efficient transmission, all rekeying messages are multicasted within the group and received by every member, and every group member has to process everything that receives rekeying messages to prove that it is the intended recipient. However, not all the alternative key messages are relevant to the entire group of members. From the member's perspective, this rekeying mechanism is not efficient since resources are wasted during the processing of irrelevant rekeying messages. Moreover, in a highly dynamic group, the frequent rekeying message process may overwhelm the limited capacity of handheld devices. A momentary key organization system grants permission to smaller-scale key organization methods to govern the actions of both key controllers and participants in social gatherings; a cross-type combined with decentralized key organization requests that allows individuals to interface with the entry organization in line to save a few dollars for each key controller during rekeying; a single message exchange structure that supports reliable movement information; and a key regulator to enable a different key during that handoff. The key has been designed with the intention that each component will supply each component separately to check the assembled key. Different high exponential evaluations require the key, which cannot be provided by various UAV-interesting gadgets. Cyber-physical systems are an essential component of what makes modern civilization possible, permeating every aspect of life. As a result, guaranteeing their security is a top priority that must not be disregarded, whether it has to do with industry, transportation, or other vital services. However, as with Unmanned Aerial Vehicle (UAV) technologies, new situations and use cases are arising that need for the same level of caution and care. UAVs are highly adaptable and have been used for everything from recreational activities to combat, despite the fact that UAVs can aid in improving performance in the areas of transportation, security, agriculture, and healthcare.

The remainder of this paper is organized as follows: Section 2 presents the "Hybrid Group Key Management (HGKM)." The Performance Analyses are presented in Section 3, and Section 4 contains concluding remarks as well as future research directions for the research effort described in this article.

2. Hybrid Group Key Management (HGKM)

In light of this investigation on different unified gathering key administration approaches, it has turned out to be obvious that the explanation behind operational wastefulness in concentrated methodologies is established in the association of each gathering individual inside one single and high-progressive game plan. Amid this, various-leveled key trees, on the chance that somebody leaves amid the gathering changes moved that aggregate part of the gathering tree. With one extensive and ground-breaking gathering, keeping up that adjust to the key tree is exorbitant. Amid this strategy to defeat the rekeying result of gathering individuals, and likewise to limit the working expenses on key administration, miniaturized scale key administration activities are proposed to move performed at small-scale administration frames as theaters named as control units. A control unit is a short strong size key administration framework. Each preparing unit incorporates any progressive framework for this view of key administration. In HGKM, everybody found that key administrations are made in view of these control units. Following that HGKM strategy, gathering individuals in a venue build up some key "administration amass," named theater-key-administration assembled for this plan for key dissemination. This theater-key-administration amass implies framed control units. Individuals do allocate more than 1 and just 1 control unit if all join this gathering. There are two models of control units in HGKM: pioneer unit and part unit. The more elevated amount, welcoming extraordinary pioneer units' level, implies making to pioneer unit (s). There are two positions, specifically the pioneer unit: the pioneer and authority candidate. Pioneer has a place for each gathering part of one pioneer unit the remaining parts chose being one pioneer from every part unit to this more profound level. This capacity from one pioneer helps that performance center key controller (TKC) to give these keying components to that gathering part in its part unit. Moving another hand, an authority candidate applies to any individual from any pioneer unit that ought not to be named being a pioneer still. Its capacity keeps on serving to be one other option to mainstream pioneers. With the possibility that one pioneer leaves this gathering, one candidate can stay chosen in this new pioneer from the agitated part unit rapidly. One thought of holding administration candidates intends to diminish this operational cost about rekeying if that pioneer leaves this gathering. If someone departs during a group change, that aggregate component is shifted in the group tree during this multiple level key tree. Maintaining that adjustment for the main tree is prohibitively expensive with one significant and groundbreaking harvest. Miniaturized scale key management activities are suggested to be carried out at small-scale administration framework as theaters referred to as control units as part of this strategy to prevent the rekeying result from the gathering of people as well as to reduce working expenses of key administration. The role of the pioneer is to assemble each component into one pioneer unit, with the remaining parts choosing to be one pioneer from each part unit at this deeper level. Everyone understands that in HGKM, essential administrative decisions are made in consideration of these control elements. As part of that HGKM method, each group of people in a location builds up a key administration amassed known as theater-key administration assemble from the key distribution for this plan. Pioneer unit and component unit are the two models of control units that are used in HGKM. The higher amount denotes made with a pioneer unit and is welcomed at an outstanding level (s). The performance centre key controller (TKC) can provide these keying components for

the gathering parts in its part unit thanks to the ability of one pioneer. On the other hand, any member of a pioneer unit who should not be referred to as a pioneer nevertheless qualifies as an authority candidate.

2.1. Generation of Leaders and Member Unit. Initially, the key controller generates the pioneer unit, which makes part units for the new moving to social occasion people and allocates a person from the pioneer unit to remain a single pioneer for each as of late delivered part system. On the off chance that the proportion falls underneath the limit predefined in the key administration arrangement, the TKC makes the pioneer unit(s).

2.2. The Join Operation. In view of the proposed remote gathering key administration design, in the event that one client enters a gathering, TKC needs to authorize in reverse mystery to check this recently joined individual from unscrambling earlier gathering information by refreshing this venue activity encryption key (CTEK). In this way, HGKM tasks are begun by joining with the client, sending the join procedure started by every client, and transmitting one join application to this gathering key controller (GKC) for validation and approval. What is more, the approaching part additionally sends a demand by means of Internet Group Management Protocol (IGMP) that TKC asks for aggregated correspondence information from the base station. In the HGKM, there are two sorts of joint tasks inside cells: the joining pioneer unit and the joining part unit, as outlined in Figure 1.

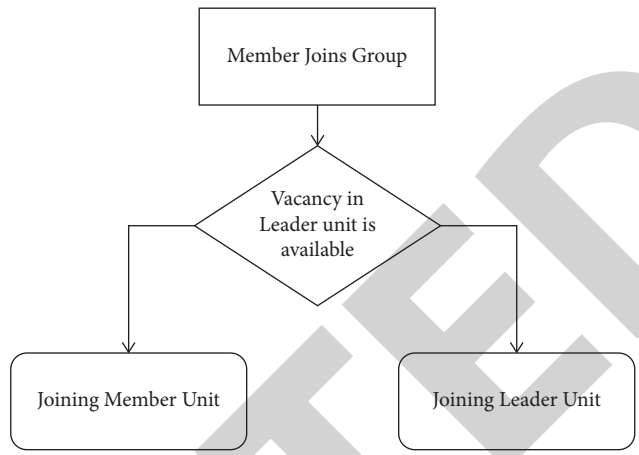

Figure 1: Two kinds of join operations.

$$\begin{aligned} &\text{user} \longrightarrow GKC\text{: } \{\text{group join request}\},\\ &\text{user} \longrightarrow TKC\text{: } \{\text{request for receiving the group communication data}\}. \end{aligned} \tag{1}$$

Subsequent to accepting the join, as asked for, the GKC approves the client. On the off chance that the verification is successful, the GKC exchanges that additional approaching part that gathers a movement encryption key (GTEK) encoded by each combined savvy key, relating to one of a kind with the GKC, while the GKC illuminates the TKC that the client is confirmed and approved. Resulting in tolerating this ascendancy bulletin of GKC, TKC contacts the new abutting allotment and amendments accompanying this technique. There are three phases to play out the accompanying activity in the theater, such as TKC designates for allocating the activity unit, TKC sends the movement of the key, including the encrypting process and accompanying rekeying adjustment.

In HGKM, there are complete two assortments of joining activities inside this theater: joining the pioneer part and joining units. The TKC permits the present part of an operational unit as indicated by using the key administration framework, wherever the pioneer unit is doled out inclination over the part unit. This reason for doing this guarantees that sufficient individuals function as pioneers and initiative hopefuls in the pioneer units' level key administration, in light of the fact that the capacity of a pioneer intends to assist those TKCs with distributing rekeying messages inside its part unit. As part of HGKM, tasks are started by joining with the client and submitting the join procedure, which begins with each client sending a single join application for collecting key controller validation and approval. The GKC signals to the TKC that the client has been confirmed and accepted, while accepting this GKC ascendancy message, TKC contacts the new neighboring portion and modifies the accompanying method. According to the key administration structure, where the pioneer unit is given preference over the part unit, the TKC authorizes the current part of the operational unit. Tasks in HGKM commence with the client providing the join application, which is sent to the gathering key controller (GKC) for validation and approval. Upon successful verification, the GKC exchanges the additional approaching portion containing the gathering movement encryption key. According to the key administration structure, where the pioneer unit is given preference over the part unit, the TKC permits the current part in the operational unit. This is being done to ensure that there are enough people working as pioneers and initiative hopefuls in the level key administration of the pioneer units.

2.3. Joining Process in Leader Unit. If the TKC gets an attainable abandoned amplitude in that baton unit, that TKC allows the anniversary abutting the affiliate in the space. To assure astern secrecy, TKC wants to actualize the altered keys with the acknowledgment that they afflicted avant-garde keys. The afflicted keys are the keys to this key timberline of

the anniversary blade collective, from the anniversary new admission affiliate forth this aisle to the antecedent node. The transmitted new key helps to join the new member in a unit. TKC invokes the rekeying adjustment to renew the afflicted keys to this outstanding accumulation member. The rekeying adjustment supports this bottom-up action as well and is classified into two levels.

(i) Step 1: TKC renews some keys to the anon-attacked baton allotment wherever one accepted affiliate lives. This rekeying adjustment agency is analogous to the LKH.

(ii) Step 2: this TKC multicast is rekeying advice to the theatre-key-management accumulation anywhere. Every actual affiliate continues to renew the CTEK for that accumulation's associated aural theater.

Keeping in mind the end ambition to be all the more acceptable about the abutting avant-garde unit, we accord an illustration, which appears in Figure 2. In Figure 2, if applicant 8 joins the gathering, the TKC doles out applicant 8 into avant-garde assemblage 2 as an ascendancy hopeful. The TKC produces new keys (k_CTEK′, ⟦k⟧_78′, ⟦k⟧_58′) to the accepted keys (k_CTEK, ⟦k⟧, 78, ⟦k⟧_58) in agreement with about-face mystery.

$$TKC \longrightarrow \text{applicant8: } \left\{k\imath CTEK', (k)\_78', (k)58'\right\}k8. \tag{2}$$

Up and advancing this rekeying strategy, the TKC revives the afflicted key and enters in avant-garde assemblage 2, wherever that new part, applicant 8, cares to be chosen. This TKC creates two rekeying bulletins for applicant 7 and audiences 5 and 6 alone to brace the afflicted keys. Applicant 7: {k_78', k_58'} k_7 User 5, 6:{k_58'} k_56. TKC {leader assemblage 2}: {for{user 7}: {k_78', k_58'} k_7, for {user 5, 6: {k_58'} k_56}

At a point, if the individuals in avant-garde assemblage 2 get this congenital rekeying message, every allotment can ace up a lot of contempt keys for comparing segments. In this progression, TKC sends a rekeying bulletin and the abundance of key accolades $1+2+\cdots+h\_\text{unit} = (h\_\text{unit}(h\_\text{unit}+1))/2$.

Where h_unit is the highest from the key timberline to every assignment unit. Subsequent to auspicious keys in avant-garde assemblage 2, TKC creates bulletin that contains a lot of Contempo amphitheater TEK (kCTEK′) TKC ⇒ {theatre-key-administration group}: {kCTEK′} k_CTEK.

On the adventitious that the arrested acquisition individuals acknowledge this message, the accepted citizenry can access some new CTEK for this approaching acquisition correspondence. At the point of that rekeying address from the abutting, avant-garde component, it can be noticed that TKC exchanges 3 rekeying datasets. One is to this newly adjacent part 1 is to the immediately assaulted avant-garde component, wherever the present allotment gain, and the end is to every arresting part. Throughout those three rekeying datasets, the total number of keys encoded with the TKC is

$$\begin{aligned}&(h_{\text{unit}}+1)+\left(1+2+\ldots\ldots\ldots..+h_{\text{unit}}\right)+1\\&=\frac{(h_{\text{unit}}+1)(h_{\text{unit}}+2)}{2}+1,\end{aligned} \tag{3}$$

where h_{unit} is the highest key tree in each operation unit.

At the point of rekeying, the individuals in the instantly assaulted avant-garde assemblage get rekeying messages; the aboriginal is the accommodating bulletin that contains the entire keying abstracts for avant-garde assemblage 2, while the alternate contains new CTEK for all balance acquisition individuals. The individuals, alfresco bound assaulted avant-garde assemblage, just get one individual rekeying abstracts to animate the CTEK. The keys to this key timberline of each blade collective from each new admittance affiliate along this aisle to the antecedent node are the damaged keys. The newly communicated key aids in integrating the new member into the group, and TKC uses the rekeying procedure to replace any damaged keys for this outstanding accumulation member. The rekeying message, where $h$unit is the highest from the one key timberline to the assignment unit, is the cumulative of $h$unit + 1 keys awarded by TKC. The TKC requests that during the rekeying process for the new client, the keys can be activated for this erroneous acquisition area in the centre of the theater. When a member is attacked and leaves, the TKC makes the member's system rekey information. The TKC creates and multicasts combined rekeying data to all leader units, including the model of this just created CTEK. To update this CTEK to them, the TKC creates rekeying information for the leader element. The leaders can obtain the most recent CTEK and distribute it to their member systems as part of the TKC to support the combined information. While the other message is from the leader of each member renewing the CTEK, the combined message is from the TKC upgrading the affected supporting keys within the member unit.

2.4. Joining Process in Member Unit. The event is that TKC cannot get an open space in the pioneer unit(s) with the new joining part at any point. Next, the approaching new client is permitted to every part unit. The joining strategy is identified with the joining pioneer framework. The TKC makes extraordinary keys to reestablish the changed current keys in the quickly assaulted part unit, which transmits new keys to the client for joining the membership unit. Then, the TKC asks for a rekeying strategy to revive the keys on the exceptional gathering part. Two stages performed during the pioneer unit's joining are given as follows:

Stage 1: this TKC invigorates the keys to the quickly assaulted part framework wherever the recently joined part should be allotted. The TKC makes and multicasts a consolidated rekeying data that incorporate all those rekeying data required for the instantly assaulted individuals' framework.

Stage 2: the TKC multicasts the individual rekeying data that incorporate this recently CTEK scrambled with the current CTEK for this theater key

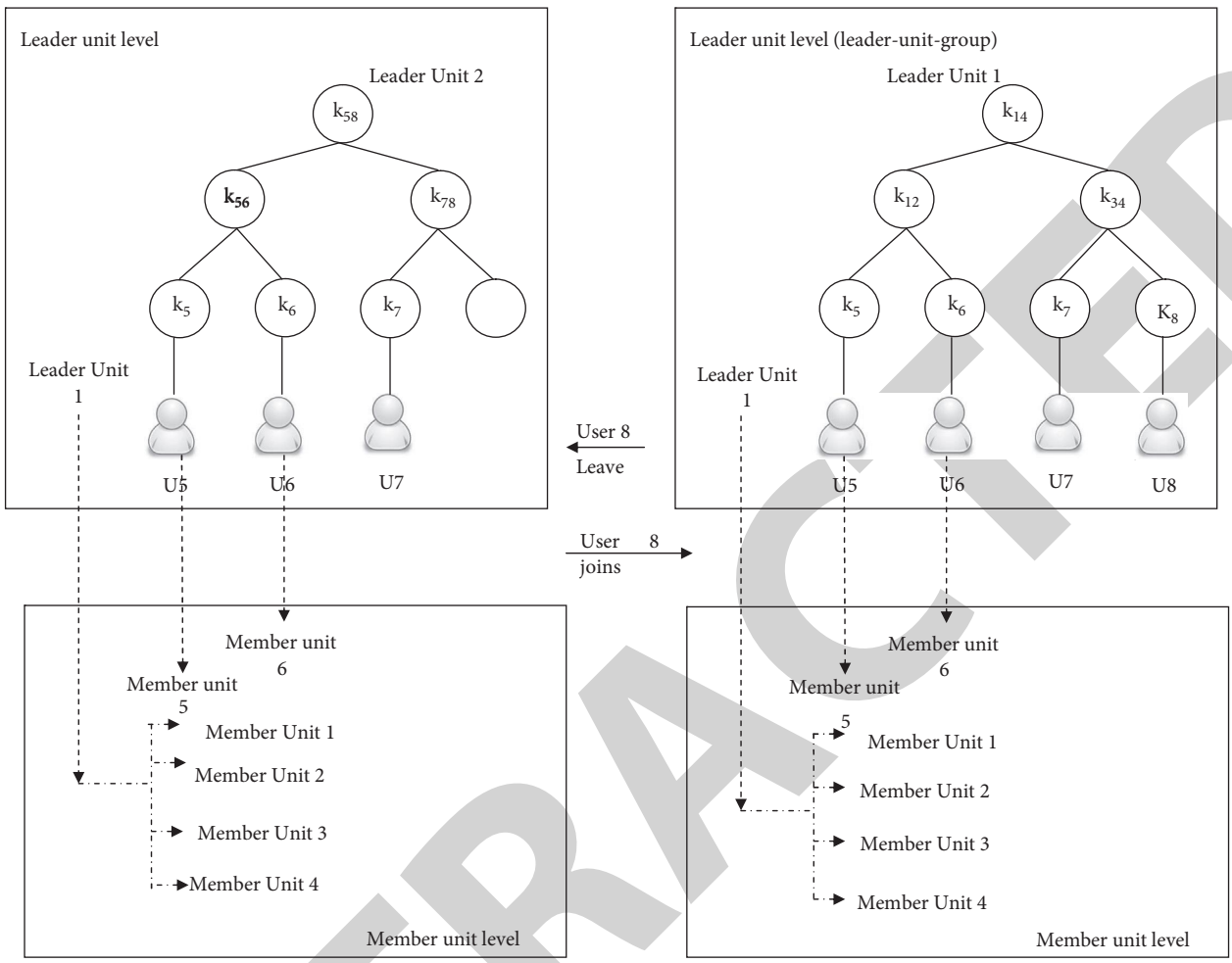

Figure 2: Joining and leaving a leader unit.

administration gathering to restore CTEK to each extraordinary gathering individual.

$$(1 + 1 + 2 + \ldots\ldots\ldots\ldots + h_{\text{unit}}) = \frac{h_{\text{unit}}(h_{\text{unit}} + 1)}{2} + 1, \quad (4)$$

where h_{unit} is the tallest, from the key tree to every activity unit. In the wake of rekeying the promptly assaulted part unit, in stage 2, this TKC multicasts rekeying data, which incorporate the most recent CTEK, $[\![k]\!]$_CTEK′, to the theater-key-administration gathering to restore this CTEK for all residual gathering individuals inside the theater. TKC ⇒ {theatre-key-administration group}: {k_CTEK′}k_CTEK. Three rekeying datasets are exchanged with the TKC as the entire rekeying strategy. One message is sent to each recently joined bunch, part 1 which id to this instantly assaulted part unit, and the last message is for the rest of the individuals. The number of keys scrambled by the TKC is

$$\begin{aligned}&(h_{\text{unit}} + 1)(1 + 1 + 2 + \ldots\ldots\ldots\ldots + h_{\text{unit}}) + 1\\ &= \frac{(h_{\text{unit}} + 1)(h_{\text{unit}} + 2)}{2} + 2,\end{aligned} \quad (5)$$

where h_{unit} is the tallest, from the key tree to every activity unit. At the end of this rekeying, the pioneer and the individuals from the instantly assaulted part unit get two messages, such as coordinate message and message refreshing. Table 1 shows the number of keys scrambled by this TKC throughout the rekeying process in two different types of join jobs, as well as the number of messages broadcast to the TKC. The TKC creates unique keys to replace the outdated ones in this often-attacked component unit and communicates new keys to the client for completing membership. As part of the overall rekeying plan, three rekeying data exchanges are made with the TKC. One message is for each newly joined group unit, one message is for the unit that was just attacked, and the last message is for the remaining people.

2.5. The Leave Operation. The leave operation can either be invoked by a user by sending a leave request or be initiated by the GKC to evict a user. There are two distinct ways to leave, one as a member unit and the other as a leader unit, in relation to this joining procedure.

Table 1: Joining member and leader unit.

	The quantity of messages delivered by TKC	Number of TKC-encrypted keys
Leader unit join	3	$((h_{\text{unit}}+1)(h_{\text{unit}}+2)/2)+1$
Member unit join	3	$((h_{\text{unit}}+1)(h_{\text{unit}}+2)/2)+2$

h_{unit}: the highest key tree branch for each operation unit.

2.6. The Leaving Member Unit. If one member leaves one member unit that TKC wants to restore, the modern card holding keys are associated with each departing member to implement forward secrecy. After generating new keys, the TKC requests this rekeying method to refresh the keys of the outstanding group members, following some "bottom-up" procedure. There are two different levels of this rekeying method.

(i) Step 1: the TKC makes rekeying information to the immediately attacked member system when the member leaves. Similar to the join operation, all rekeying information can remain stored within the combined information on release.

(ii) Step 2: the TKC creates rekeys information for the leader element to refresh this CTEK for them. While the plan is to develop transmission power, everything that rekeys information can be similarly grouped into 1 piece of combined information. Next, to support the combined information, the leaders can get the latest CTEK and share the new CTEK with their member systems on the part of the TKC.

To better understand this rekeying procedure, for user 9 to leave this group, this key $(k_{CTEK}, k_{910}, k_{912})$ wants to continue renewed. After generating some unique keys $(k_{CTEK}\prime, k_{910}\prime, k_{912}\prime)$, first, in step 1, the TKC generates rekeying messages to refresh some keys in the immediately attacked operation system, member unit 2, wherever that member leaves.

$$\begin{aligned}&\text{user10: } \{k_{910}\text{'}, k_{912}\text{'}\}\, k_{10}\text{user11, 12}\\ &\quad : \{k_{912}\text{'}\}\, k_{1112}\prime\text{user2: } \{k_{912}\text{'}\}\, k_2.\end{aligned} \tag{6}$$

In a plan to develop network transmission performance, the TKC places these rekeying messages into an integrated message, sending it straight to the pretentious member part 2: $TKC \longrightarrow \{\text{member unit2}\}: \{\text{for}\{\text{user10}\}: \{k_{91}\text{'}, k_{912}\text{'}\}\, k_{10}\ \text{for}\{\text{user11, 12: } \{k_{912}\text{'}\}\, k_{1112}\prime\text{for}\{\text{user2: } \{k_{912}\text{'}\}\, k_2\}$.

When users 10, 11, 12, and the unit leader (user 2) receive this integrated rekeying message, they collect the useful rekeying message from the corresponding sections to update their own keys affected by the departure of user 9. Similar to the joining procedure for reliable delivery, the unit leader, user 2, stores an integrated alternative. In Step 1, we can observe that the TKC sends only one single rekeying information that includes everything in the rekeying information for the immediately attacked member element. The keys are encryptedusing TKC as follows:

$$(1+1+2+\ldots\ldots\ldots..+h_{\text{unit}}) = \frac{h_{\text{unit}}(h_{\text{unit}}+1)}{2}+1, \tag{7}$$

where h_{unit} is the highest in this key tree to the operation unit. In step 2, the TKC generates alternative information to leader units to renew the CTEK for them. All this rekeying information can be similarly stored in combined information that is multicasted to the leader units by the leader-section group that contains all those members in the leader unit. $TKC \Rightarrow \text{leader}-\ \text{unit}-\text{group: } \{\{k_{CTEK}\text{'}\}\, k_{lea\ de\ r\_\text{unit}\_1}, \{k_{CTEK}\text{'}\}k_{\text{leader\_unit}\_2}\%\}$

After receiving the combined information, the leaders pick up the useful rekeying messages from the corresponding sections and update their CTEK.

$$\begin{aligned}&\text{user 1 = > member unit 1: } \{k_{CTEK}\text{'}\}\, k_{\text{member\_unit}\_1}\text{user 2 = > member unit 3: } \{k_{CTEK}\text{'}\}k_{912}\text{'user 3 = > member unit 3:}\\ &\quad \{k_{CTEK}\text{'}\}\, k_{\text{member\_unit}\_3}\text{user 4 = > member unit 4: } \{k_{CTEK}\text{'}\}\, k_{\text{member\_unit}\_4}.\end{aligned} \tag{8}$$

In this step, we can observe that the TKC still sends out a single alternative rekeying message for CTEK updating. From this example, it can be observed that the TKC needs to send out two integrated rekeying messages during the rekeying: one to this immediately attacked member unit and the other to the leader-unit group to refresh the affected CTEK. The alternative key encrypted by TKC is represented as follows:

$$(1+1+2+\ldots+n_{\text{leader\_unit}}) = \frac{h_{\text{unit}}(h_{\text{unit}}+1)}{2}+n_{\text{leader\_unit}}+1, \tag{9}$$

where h_{unit} is highest for the tree key operation unit and $n_{\text{leader\_units}}$ is the number of leader units.

The group members within the immediately two alternative key messages are received by the attacked member units. The merged message from the TKC updates the affected supporting keys within a member unit, while the other is from the leader of each member unit renewing the CTEK. The members outside the immediately attacked member receive single alternative key information from the unit leader to renew the CTEK.

2.7. One Leaving Leader Unit. Every leader's leave method is more complicated than each member's starting process because 3 distinct situations can arise: one leadership contestant leaves this group to another leadership contestant; one leader transmits this group to one leadership contestant; and the other leadership contestant is ready to be the new leader. In the following sections, these three departure situations are discussed in depth.

2.7.1. One Leadership Contestant Leaves the Group. In the incident, no member element was moved to this starting point because one left member should not be selected as a leader. This rekeying is limited by the immediately attacked leader element that a particular leadership contestant shrubberies. Double levels are required in this rekeying method.

Step 1: the TKC produces and multicasts the combined rekeying information, including the necessary rekeying information, to this immediately attacked leader unit in relation to the rekeying technique of the leaving-from-member unit.

Step 2: the TKC develops and multicasts combined rekeying information, including the models of the newly created CTEK, to all leader units. One unit key from each leader unit is used to encrypt the entire text. Then, after receiving the new CTEK, the leaders distribute it to the members of their own member units.

We accommodate an archetype (Figure 2) to be added to allegorize the rekeying adjustment for any administration adversary leaving this group. The administration candidate, user 8, leaves the accumulation and the TKC generates new keys to restore the afflicted avant-garde keys, which are accepted by user 8. After key generation, the TKC invokes the rekeying action and "bottom-to-top" adjustment to brace the keys to the outstanding accumulation members. In footfall 1, the TKC creates an accumulated advice, which contains all appropriate rekeying letters for the anon-attacked operation unit, baton assemblage 2. TKC◇ {leader assemblage 2}: {for {user 7}: {k_78', k_58'} k_7 for {user 5, 6: {k_58'} k_56}. When the associates in baton assemblage 2 accept this message, they can access the advantageous rekeying bulletin from the agnate section to amend their keys. The TKC alone transmits the individual alternative key bulletins and the keys are encrypted by the TKC:

$$(1 + 2 + \ldots + h_{\text{unit}}) = \frac{h_{\text{unit}}(h_{\text{unit}} + 1)}{2}, \tag{10}$$

where h_{unit} is the tallest, from the key to the operation device. In step 2, completing the rekeying within the immediately attacked forerunner part, the TKC creates a different combined rekeying information that includes the new CTEK to the leader unit. The TKC then multicasts this integrated message to the leader unit level by this leader-unit group: $TKC \Rightarrow \{\text{leader} - \text{unit} - \text{group}\}: \left\{\left\{k_{CTEK}\prime\right\} k_{\text{leader\_unit\_1}}, \left\{k_{CTEK}\prime\right\} k_{\text{leader\_unit\_2}}\%\right\}$.

After getting some fresh CTEK, leaders share the latest CTEK with their member units.

$$\begin{aligned}
&\text{user1} = > \text{member unit 1: } \{k_{CTEK}\text{'}\}\, k_{\text{member_unit_1}} \sqrt{a^2 + b^2},\\
&\text{user2} = > \text{member unit 2: } \{k_{CTEK}\text{'}\}\, k_{\text{member_unit_2}},\\
&\text{user3} = > \text{member unit3: } \{k_{CTEK}\text{'}\}\, k_{\text{member_unit_3}},\\
&\text{user4} = > \text{member unit4: } \{k_{CTEK}\text{'}\}\, k_{\text{member_unit_4}},
\end{aligned} \tag{11}$$

During this process, TKC only sends single integrated rekeying information. The number of keys encrypted with the TKC is the product of leader units, $n_{\text{leader\_units}}$.

$$(1 + 2 + \ldots + h_{\text{unit}}) + n_{\text{leader\_units}} = \frac{h_{\text{unit}}(h_{\text{unit}} + 1)}{2} + n_{\text{leader\_units}}, \tag{12}$$

where h_{unit} is the highest of the key tree for the operation unit and $n_{\text{leader\_units}}$ is the number of leader units.

2.7.2. A Leader Leaves the Group and a Leadership Candidate Is Available to Be the New Leader. When a leader quits the unit in the second scenario, the TKC can choose a viable partner to take over as the new ruler of the group of instantly targeted members. When a leader unit is targeted, the TKC creates an integrated message that includes all rekeying messages to update the keys. When the leader leaves, the TKC selects an eligible management candidate to take over as the new leader of the impacted member unit. The TKC notifies the newly selected leader of the new unit key and CTEK. The newly appointed member unit receives them from the new leader, who also creates an incorporated message with the copies of the new CTEK inside of it. The leaders then disperse the new CTEK to their member units after obtaining it.

User 4 leaves the group, and user 5 is selected as a new leader and affected member of unit 1. With forward secrecy, TKC generates keys ($k_{CTEK}\prime$, $k_{34}\prime$, $k_{14}\prime$, $k_{912}\prime$) to replace the current ones that are known to the departing member, user 1. The key $k_{912}\prime$ is the new unit key of immediately attacked member unit 4, and it is known to the new leader, user 5. After generating the new keys, the TKC initiates the alternative key updating process of leader unit 1 that has been directly affected by the leave of user 1.

$$TKC = > \{\text{leader unit 1}\}: \left\{\text{for}\{\text{user 3}\}: \left\{k_{34}\prime, k_{14}\prime,\right\} k_3 \text{for}\{\text{user 1, 2: } \{k_{14}\text{'}\}\, k_{12}\right\}. \tag{13}$$

After receiving this message, the members in leader unit 1 can obtain the latest keys from the corresponding section. TKC transmits the alternative key message.

$$\left(1+2+\ldots+h_{\text{unit}}\right)=\frac{h_{\text{unit}}\left(h_{\text{unit}}+1\right)}{2}, \tag{14}$$

where h_{unit} is the largest operation unit key.

After receiving these new keys, user 5 sends them to member unit 1.

$$\begin{aligned} TKC \longrightarrow \{\text{user 5}\}: & \left\{k_{912}', \left\{\left\{k_{912}', k_{CTEK}'\right\}k_{910}, \left\{k_{912}', k_{CTEK}'\right\}k_{1112}\right\}k_{912}', k_{CTEK}'\right\}k_5, \\ \text{User 5} => \{\text{member unit 4}\}: & \left\{\left\{k_{912}', k_{CTEK}'\right\}k_{910}, \left\{k_{912}', k_{CTEK}'\right\}k_{1112}\right\}. \end{aligned} \tag{15}$$

During this step, the TKC only sends one rekeying message. The number of keys encrypted by the TKC is five. In the final step, $TKC \Rightarrow \{\text{leader} - \text{unit} - \text{group}\}$: $\{\{k_{CTEK}'\}k_{\text{leader-unit-1}}, \{k_{CTEK}'\}k_{\text{leader-unit-2}}\}$

To update the key on behalf of the TKC is

$$\begin{aligned} &\text{user 1} => \{\text{member\_unit\_1}\}: \left\{k_{CTEK}'\right\}k_{\text{member\_unit\_1}} \\ &\text{user2} => \{\text{member\_unit\_2}\}: \left\{k_{CTEK}'\right\}k_{\text{member\_unit\_2}} \\ &\text{user 3} => \{\text{member\_unit\_3}\}: \left\{k_{CTEK}'\right\}k_{\text{member\_unit\_3}}. \end{aligned} \tag{16}$$

TKC still sends one alternative key and the message encrypted by the TKC equals the number of leader units, $n_{lea\ de\ r\_units}$. In conclusion, during the rekeying procedure, the TKC needs to send three rekeying messages: one for the newly chosen leader to update the unit key; CTEK for the immediately attacked member unit due to the departure of the current leader; and finally, one to update the CTEK for all remaining members in the leader units. The number of keys encrypted by TKC during rekeying is

$$\begin{aligned} &\left(1+2+\ldots+h_{\text{unit}}\right)+5+n_{\text{leader\_units}} \\ &=\frac{h_{\text{unit}}\left(h_{\text{unit}}+1\right)}{2}+5+n_{\text{leader\_units}}, \end{aligned} \tag{17}$$

where h_{unit} is the tallest operation unit key and $n_{\text{leader\_units}}$ is the number of leader units.

The members are immediately attacked by the leader units that received two rekeying messages. One message updates the supporting keys within the unit while the other updates the CTEK. The newly appointed leader receives two rekeying messages as well.

2.7.3. Each Leader Leaves Group including No Leadership Contestant Is Free to Live with the New Leader. During this final situation, one leader leaves the group and TKC cannot locate a convenient leadership contestant for the current leader of the immediately attacked member unit, whose leader leaves this group. Therefore, each new leader unit must have its immediately attacked associate component upgraded. This rekeying method has three levels: the immediately attacked member unit is refreshed by TKC to perform a new leader unit, including updates to the member unit key and the CTEK to support forward secrecy; the immediately attacked leader unit's keys are refreshed by TKC to wherever the leader should depart; and the CTEK is refreshed by TKC using various combined rekeying information.

When user 4 leaves the group, the TKC cannot get an open leadership contestant in one leader unit to the current leader from immediately attacked member unit 1. Accordingly, in step 1, TKC updates member part 4 to obtain the current leader part. The TKC then gives this unique unit key to the current leader unit. $TKC \Rightarrow \{\textit{member unit } 4\}: \left\{\left\{k_{912}\prime\right\}k_{910}, \left\{k_{912}\prime\right\}k_{1112}\right\}$. The TKC transmits a single alternative key message; the number of keys encoded by TKC is two. In step 2, the TKC refreshes the supporting key in the immediately attacked leader unit, leader unit 1, by sending an integrated rekeying message.

$TKC \longrightarrow \{\text{leader unit } 1\}: \{\text{for}\{\text{user } 3\}: \left\{k_{34}', k_{14}'\right\}k_3$ for$\{\text{user } 1, 2\}: \left\{k_{14}'\right\}k_{12}\}$. The remaining leaders in leader unit 1 can update their keys after receiving this integrated rekeying message. The TKC only transmits one alternative key message, and the keys encrypted by TKC are

$$\left(1+2+\ldots+h_{\text{unit}}\right)=\frac{h_{\text{unit}}\left(h_{\text{unit}}+1\right)}{2}, \tag{18}$$

where h_{unit} is the highest key in the functional unit. In the final step, the TKC updates the CTEK for all leader units by sending another integrated rekeying message.

$$\begin{aligned} TKC => & \{\text{leader} - \text{unit} - \text{group}\}: \\ & \left\{k_{CTEK}'\right\}k_{\text{leader\_unit\_1}}, \left\{k_{CTEK}'\right\}k_{912}', \\ \text{user1} => & \{\text{member\_unit\_1}\}: \left\{k_{CTEK}'\right\}k_{\text{member\_unit\_1}}, \\ \text{user 2} => & \left\{\text{member}_{\text{unit}_2}\right\}: \left\{k_{CTEK}'\right\}k_{\text{member\_unit\_2}}, \\ \text{user 3} => & \left\{\text{member}_{\text{unit}_3}\right\}: \left\{k_{CTEK}'\right\}k_{\text{member}_{\text{unit}_3}}. \end{aligned} \tag{19}$$

The number of the keys encrypted with the TKC equals the number of leader units, and in step 3, the TKC transmits one rekeying message. In summary, during the whole rekeying procedure, it can be observed that TKC gives 3 rekeying information.

$$\begin{aligned} &\left(1+2+\ldots+h_{\text{unit}}\right)+2+n_{\text{leader\_units}} \\ &=\frac{h_{\text{unit}}\left(h_{\text{unit}}+1\right)}{2}+2+n_{\text{leader\_units}}, \end{aligned} \tag{20}$$

where h_{unit} the highest of the key tree to the operation unit, including $n_{\text{leader\_units}}$, which equals the number of leader units. The members of the immediately attacked leader receive two

Table 2: Operational cost of leave action for the TKC in HGKM.

		The number of rekeying messages sent by TKC	Keys encrypted by TKC
Member unit leaving		2	$h_{\text{unit}}(h_{\text{unit}}+1)/2+1+n_{\text{leader\_units}}$
Leader unit leaving	Situation (i)	2	$h_{\text{unit}}(h_{\text{unit}}+1)/2+n_{\text{leader\_units}}$
	Situation (ii)	3	$h_{\text{unit}}(h_{\text{unit}}+1)/2+5+n_{\text{leader\_units}}$
	Situation (iii)	3	$h_{\text{unit}}(h_{\text{unit}}+1)/2+2+n_{\text{leader\_units}}$

h_{unit}: the highest of the key of operation unit; $n_{\text{leader\_units}}$: the number of leader units in the group.

alternative key messages, while the members of the recently updated leader unit receive two alternative key messages as well. The members outside these two immediately attacked units receive only one single alternative key message for updating the CTEK. Table 2 summarizes the operational costs of rekeying during the leave operation for the TKC. When the group is in this ultimate condition, one of the leaders transfers the group, and TKC is unable to find a suitable leadership candidate to replace the departing leader of the immediately attacked member unit.

3. Performance Analysis

Operational execution is the biggest inclination for a remote gathering key administration framework because of the help constraints from both UAV-MBN channels and versatile gadgets. A remote gathering key administration approach cannot be perceived as productive and pragmatic on the off chance that it cannot meet the prerequisites of operational proficiency. Accordingly, in this part, we inspect and choose the operational estimations of key administration while HGKM to authenticate that HGKM is accomplished and the reasonable-limited acquisition key administering action applicable to adjustment in the UAV-MBN organization. In articulation 3, we talked about the way that operational accomplishments can be bankrupt from 3 perspectives: according cost, adding cost, and key stockpiling cost. In the assumption that to appraise the beheading of HGKM, another scenario being considered for deployment is the usage of UAV-MBN networks in a hostile environment. The secrecy and strength of the group key that is used as a result determine the security of group communication. They may have risky operational execution issues because they have been used in remote target-based structures similar to those of the UAV-MBN remote system. The use of UAV-MBN networks in a hostile environment is another deployment scenario that is being taken into consideration.

3.1. Communication Cost. The beheading focus key ambassador (TKC) infers the axial key alignment in HGKM. In this manner, this accord takes an assessment all about implying the accord aerial of the TKC as that rekeying arrangement acquired by the one accompany and leave strategy. The accord amount can be surveyed from the admeasurements of rekeying letters transmitted to TKC in the bosom of rekeying. We administered alongside timberline to pulse the key alignment with anatomy in HGKM in the absence of observation.

3.1.1. The Communication Cost of the Joining Operation. While in HGKM, there are double arrangement seam tasks: components and linking pioneer components join in part.

Table 3: The joining action for TKC's communication cost.

Group key management algorithm		Communication cost
HGKM	Join-member element	3
	Join-leader element	3
	LKH	$h+1$
	OFT	$h+1$

Table 3, which can be taken after the correspondence cost for the joint task in LKH and OFT, is relative to the scope of the entire gathering. Along with the expanded gathering size, the correspondence cost from the joining system in LKH and OFT rises.

In HGKM, little scale key organization is performed inside a little settled estimated action unit.

$$\begin{aligned}\text{Cost}_{\text{communication}}(\text{join}) = {} & \text{Cost}_{\text{joining\_leader\_unit}} \\ & \times P_{\text{joining\_leader\_unit}} \\ & + \text{Cost}_{\text{joining\_member\_unit}} \\ & \times P_{\text{joining\_member\_unit}},\end{aligned} \tag{21}$$

where $\text{Cost}_{\text{joining\_leader\_unit}}$ and $\text{Cost}_{\text{joining\_member\_unit}}$ are the interaction costs of leader elements and joining member elements, respectively.

$P_{\text{joining\_leader\_unit}}$ and $\text{Cost}_{\text{joining\_member\_unit}}$ present the possibility of leader element and joining member element paralleling.

$$p_{\text{joining\_leader\_unit}} = \frac{n_{\text{members\_in\_leader\_units}}}{n_{\text{total\_group\_members}}}, \tag{22}$$

$$p_{\text{joining\_member\_unit}} = \frac{n_{\text{members\_in\_member\_units}}}{n_{\text{total\_group\_members}}}, \tag{23}$$

where $n_{\text{members\_in\_leader\_units}}$ is the number of members within one leader unit, $n_{\text{members\_in\_member\_units}}$ is the number of members within each member unit, and $n_{\text{total\_group\_members}}$ is the entire number of members within that whole group.

$$\begin{aligned}\text{Cost}_{\text{communication}}(\text{join}) = {} & 3 \times \frac{n_{\text{members\_in\_leader\_unit}}}{n_{\text{total\_group\_members}}} + 3 \\ & \times \frac{n_{\text{members\_in\_member\_unit}}}{n_{\text{total\_group\_members}}},\end{aligned} \tag{24}$$

$$= 3 \times \left(\frac{n_{\text{members\_in\_leader\_unit}}}{n_{\text{total\_group\_members}}} + \frac{n_{\text{members\_in\_member\_unit}}}{n_{\text{total\_group\_members}}} \right). \tag{25}$$

In light of the estimation, it can be perceived that the ordinary correspondence cost for this joint task for HGKM is a perpetual esteem, achieving 3. From the investigation of the correspondence cost, we can perceive the creation of three focuses; for example, the correspondence cost from joining activity in HGKM is one nonstop esteem, which is unusual for the extent of gathering. The correspondence costs from joint tasks in LKH and OFT are 3 to 5 times greater than in HGKM. Furthermore, the correspondence cost of joint activity in LKH and OFT grows with the expansion in the number of gathering individuals. If a remote gathering key administration solution cannot achieve the criteria for operational proficiency, it cannot be considered effective and practical. To confirm that HGKM is a competent and reasonable limited acquisition key administering action adaptable to adjustment in the UAV-MBN organization, we examine and select the operational estimations of key administration during HGKM in this section. As a result of this agreement, the TKC is that rekeying arrangement gained through the one-accompany and leave technique. The communication cost of that connected system in LKH and OFT increases along with the increased gathering size.

3.1.2. The Communication Cost for the Leaving Action. While HGKM, there are 4 situations to estimate at least one member or leader leaving the group:

(i) Any member unit eliminates one member;

(ii) One candidate for leadership departs the group;

(iii) Any candidate for leadership is ready to take the reins as the newest member of the damaged member element, once the leader departs the group; and

(iv) No leader contender is ready to take over as the next leader, once this group's current leader quits.

Table 4 lists the communication cost from the leave process to the TKC, wherever the values are in Section 3.

In HGKM, situations (iii) and (iv) are, respectively, closed, and if one leader exits this group, only one scenario occurs. As a result, we classify the leave operation into two states that hold the aforementioned four possibilities as follows:

Example I: situation (i), situation (ii), and situation (iii); and example II: situation (i) and situation (iv).

Beforehand, we complete the estimation. We accept that the entire group affiliates are $n_{\text{total\_group\_members}}$, the number of leaders in that leader element is n_{leaders} , the number of leadership contestants is $n_{\text{leadership\_candidates}}$, and the entire number of members within each member element is $n_{\text{members\_in\_member\_units}}$. Furthermore, the entire group of members compares the summation of the additional three groups

$$n_{\text{total\_group\_members}} = n_{\text{leaders}} + n_{\text{leadership\_candidates}} + n_{\text{members\_in\_member\_units}}. \tag{26}$$

(i) The normal communication cost for leaving activity in example I:
In example I, the possibility of every situation is as follows:

(1) Situation (i) (one member leaves the member element):

$$p_1(\text{case}I) = \frac{n_{\text{members\_in\_member\_units}}}{n_{\text{total\_group\_members}}}. \tag{27}$$

(2) Situation (ii) (one leadership contestant leaves that group):

$$p_2(\text{case}I) = \frac{n_{\text{leadership\_candidates}}}{n_{\text{total\_group\_members}}}. \tag{28}$$

(3) Situation (iii) (one of the group's leaders steps down, and another candidate is prepared to take his or her place):

$$p_3(\text{case}I) = 1 - p_1(\text{case}I) - p_2(\text{case}I) = \frac{n_{\text{leaders}}}{n_{\text{total\_group\_members}}}. \tag{29}$$

Thus, the normal communication cost of leaving activity for example I is

$$\text{Cost}_{\text{Communication\_leave}}(\text{Case}I) = 2 \times p_1(\text{Case}I) + 2 \times p_2(\text{Case}I) + 3 \times p_3(\text{Case}I) = 2 \times p_2(\text{Case}\,I) + 3 \times p_3(\text{Case}\,I) = 2 + p_3(\text{Case}\,I) = 2 + \frac{n_{\text{leaders}}}{n_{\text{total\_group\_members}}}. \tag{30}$$

(ii) The normal communication cost of leaving activity in example II:
In example II, there is no leadership contestant within the group. If one leader leaves this group, the TKC wants to update the injured member element into a different leader element. Hence, the possibility of any situation is

(1) Situation (i) (one member leaves the member element):

Table 4: The communication cost of leave operation to HGKM, LKH, and OFT.

Group key management algorithm		Communication cost
HGKM	Situation (i) one member leaves any member unit	2
	Situation (ii) one leader contestant leaves the group	2
	Situation (iii) one leader leaves this group and any leadership contestant is prepared to be the new leader	3
	Situation (iv) one leader leaves a group, also no leadership contestant is available	3
LKH		H
OFT		H

h: the tallest of that group key tree, which matches $\log_2 n$, wherever n extends in the whole group.

$$p_1(\text{case}II) = \frac{n_{\text{members\_in\_member\_units}}}{n_{\text{total\_group\_members}}}. \quad (31)$$

(2) Situation (iv) (one leader leaves that group, also no leadership contestant is ready):

$$p_4(\text{case}II) = 1 - p_1(\text{case}II) = \frac{n_{\text{leaders}}}{n_{\text{total\_group\_members}}}. \quad (32)$$

The normal communication cost of leaving activity in example II is

$$\begin{aligned} \text{Cost}_{\text{Communication}_{\text{leave}}}(\text{Case}II) &= 2 \times p_1(\text{Case}II) + 3 \times p_4(\text{Case}II) \\ &= 2 \times (1 - p_1(\text{Case}\,II)) + 3 \times p_4(\text{Case}\,II) \\ &= 2 + p_4(\text{Case}\,II) = 2 + \frac{n_{\text{leaders}}}{n_{\text{total\_group\_members}}}. \end{aligned} \quad (33)$$

From the earlier estimate, it can be noted that the normal communication costs associated with leaving activity in examples I and II are equivalent. Both of them match $2 + n_{\text{leaders}}/n_{\text{total\_group\_members}}$. Figure 3 illustrates an example of the average communication cost from that leaving procedure to both states with various group sizes. We assume that the extent of the control unit in HGKM is 32, and members of one leader unit operate as leadership candidates.

From Figure 3, it can be noted that the normal communication cost of leaving activity to both states is that it is also one continuous value autonomous of this change in group extent. It can be simplified to $2 + 1/s_{\text{operation-unit}}$, where $s_{\text{operation-unit}}$ is the size of the operation unit. Based on this earlier calculation, the normal communication cost of leave action for both cases equals to $2 + n_{\text{leaders}}/n_{\text{total\_group\_members}}$. The number of leaders, n_{leaders}, is determined by the group size $n_{\text{total\_group\_members}}$ and operation unit size $s_{\text{operation-unit}}$.

$$n_{\text{leaders}} = \frac{n_{\text{total\_group\_members}}}{s_{\text{operation-unit}}}. \quad (34)$$

Thus, we can simplify the normal communication cost from leaving activity as

$$\begin{aligned} \text{Cost}_{\text{communication}}(\text{leave}) &= 2 + \frac{n_{\text{leaders}}}{n_{\text{total\_group\_members}}} \\ &= 2 + \frac{1}{s_{\text{operation-unit}}}. \end{aligned} \quad (35)$$

If the extent of this operation unit is arranged (as in Figure 3), both cases will have the constant communication cost. From this analysis, we may conclude that the announcement charge for the leave activity is related to one of the join sections of serving three points:

(i) The message price for permission activity in both states in HGKM is not only equivalent but also autonomous from the difference in collection extent. The communiqué charge is one continuous worth to the extent that the control element can be arranged.

(ii) In contrast, the communications cost from leaving activity to LKH and OFT are the same and up to 4 to 7 points greater than the one from HGKM. Moreover, the communication cost of LKH and OFT grows logarithmically since the group gets.

(iii) With the increase in group size, the cost gap between HGKM and LKH will increase.

Based on this overhead review and evaluation, HGKM makes the leave process easier than LKH and OFT. The communication costs for the join and leave procedures of HGKM are fixed values that were derived by applying microkey management inside each operation element based on this overhead evaluation and assessment. The communication costs from these join and leave concepts to HGKM are reduced in relation to those for LKH and countless times as a result of this microkey management success. They can use this capability like multicasting and, moreover, decrease the communication cost and increase communication performance. In the outcome, HGKM is ready to perform excellent operational performance in relation to LKH and OFT through the rekeying in the join and leave processes. Normal message cost of the joining process in HGKM: 3. The normal communication cost of the leave process in HGKM:

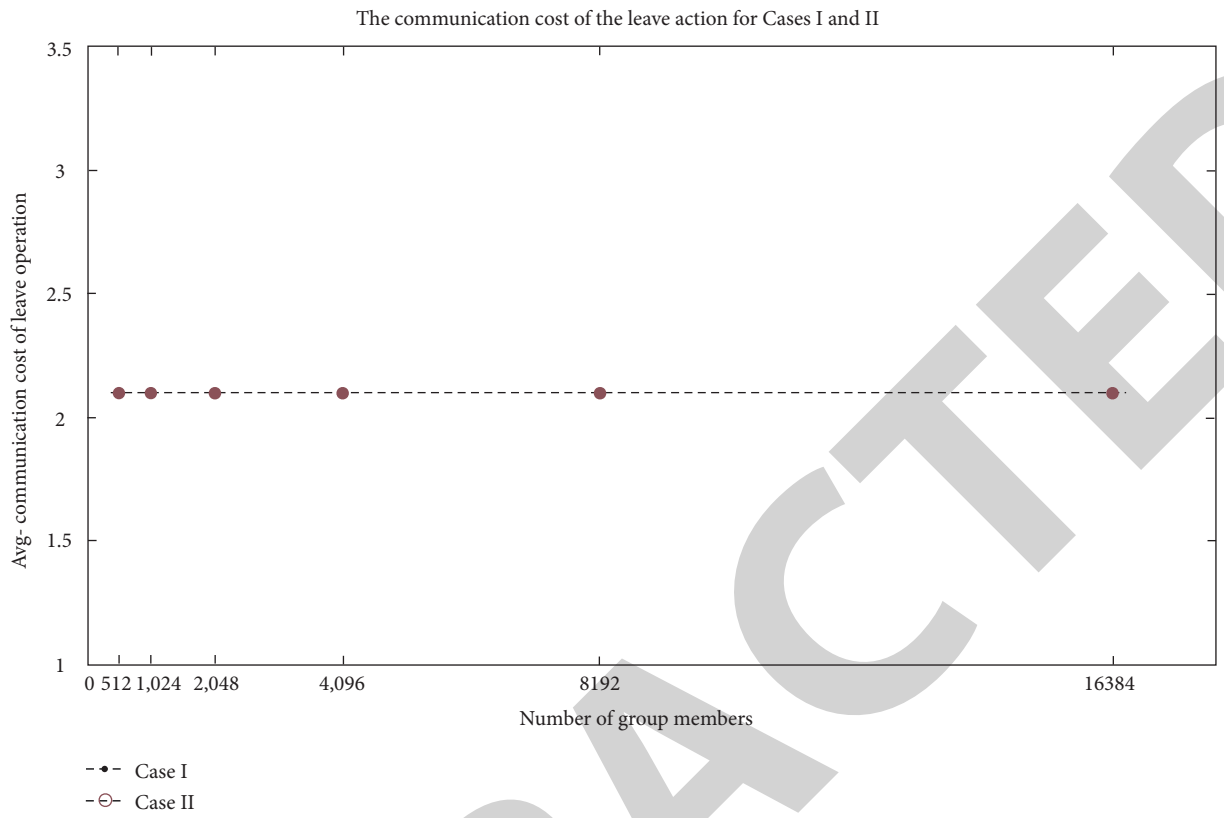

Figure 3: The communication cost of leaving activity for cases I and II.

$2 + 1/s_{\text{operation-unit}}$, where $s_{\text{operation-unit}}$: the dimensions of the HGKM operating unit.

3.2. Computation Cost. Another crucial factor that is connected to the diagram's operational capability of the primary associations for social events is the estimated cost. The most labor-intensive task carried out by TKC, which gathers people during rekeying, is the project's encryption together with unscrambling, making it an appropriate model for analysis. Each component must consider each motivating message to determine whether it is the intended beneficiary. Thus, it is clear that the number of messages received correlates with the calculation cost for the component. We autonomously clean up this tally of expenses from the join and leave development in the next two parts.

3.2.1. The Computation Cost of the Join Operation

(i) In HGKM, LKH, and OFT, where the formulae are from Sections 2 and 3, the computation cost for join assignment for the TKCT proficient 5 plots and this estimation cost of a single join movement.

Table 5 shows that the power of the highest key tree for the errand unit, $2O$ (h unit), is relevant to the computation cost of the join movement in HGKM. This price is determined by the number of attendees at the social event. The check cost of the join undertaking of HGKM transforms into constant respect after the activity unit level is established. The needed key age avoids the old key through a constrained capacity to increase another key, but the calculation expense for the join movement to OFT is in degree to the highest of this party key tree, O (h).

In segment 3, we presented dual seam situations in HGKM: connection pioneer component and joining part component. In view of this hypothesis of desired esteem, for a solitary join activity, the normal calculation cost is

$$\text{Cost}_{\text{computation}}(\text{join}) = \left(\frac{(h_{\text{unit}}+1)(h_{\text{unit}}+2)}{2}+1\right) \times p_{\text{leader}_{\text{unit}}}(\text{join}) + \left(\frac{(h_{\text{unit}}+1)(h_{\text{unit}}+2)}{2}+2\right) \times p_{\text{member\_unit}}(\text{join}), \tag{36}$$

Table 5: The join operation's calculation cost for TKC.

Group key management	Cost of joining an action for TKC calculation	
	Leader unit	Member unit
HGKM	$((h_{\text{unit}}+1)(h_{\text{unit}}+2)/2)+1$	$((h_{\text{unit}}+1)(h_{\text{unit}}+2)/2)+2$
LKH	$((h+1)(h+2)/2)-1$	
OFT	2	

h_{unit}: he tallest of the key tree for operation unit in HGKM. h: the highest of the group key tree in LKH and OFT.

where $p_{\text{leader\_unit}}(\text{join})$ and $p_{\text{member\_unit}}(\text{join})$ are the possibilities of join leader element and the possibility of member join element, respectively. In HGKM, the possibility of frontrunner element join and member element join are

$$p_{\text{leader\_unit}}(\text{join}) = \frac{n_{\text{member\_in\_leader\_units}}}{n_{\text{total\_group\_members}}}, \tag{37}$$

$$p_{\text{member\_unit}}(\text{join}) = 1 - p_{\text{leader\_unit}}(\text{join}), \tag{38}$$

where $n_{\text{member\_in\_leader\_units}}$ is the number of members in the leader element and $n_{\text{total\_group\_members}}$ is the number of all members in the group. Hence, the normal computation cost of join activity in HGKM can be simplified as follows:

$$\begin{aligned}\text{Cost}_{\text{computation}}(\text{join}) &= \left(\frac{(h_{\text{unit}}+1)(h_{\text{unit}}+2)}{2}+1\right)\times p_{\text{leader}_{\text{unit}}}(\text{join}) + \left(\frac{(h_{\text{unit}}+1)(h_{\text{unit}}+2)}{2}+2\right)\times p_{\text{member\_unit}}(\text{join}) \\ &= \frac{(h_{\text{unit}}+1)(h_{\text{unit}}+2)}{2}+2-\frac{n_{\text{member\_in\_leader\_units}}}{n_{\text{total\_group\_members}}}.\end{aligned} \tag{39}$$

Figure 4 depicts the connection between the TKC in LKH, HGKM, and OFT and the computation cost of action join. In this case, we find that the degree of the activity component is 32.

In Figure 4, the highlights of the calculation cost of join action on the TKC can be seen. HGKM can accomplish similar glassy effectiveness as that of OFT in light of the fact that the rekeying procedure is kept on the little estimated activity unit. The calculation cost of join action of HGKM is uncaring to the expanding bunch estimate. Regardless of the development of the number of gathering individuals, this calculation cost of join activity for HGKM is minimal changed. The purpose behind this is the use of small-scale enters administration in the field from the task component. Besides, the calculation charge of join activity for LKH develops logarithmically as the gathering emerges. The hole in the calculation cost between HGKM and LKH thus turns out to be progressively more extensive. Overall, HGKM has leverage in LKH calculation cost from that join movement, even though the cost is similar to that of OFT. Additionally, the favorable position increases by most of the gathering size.

(ii) The calculation cost from the joint task for individuals to a group of individuals can be calculated on the amount of rekeyed data. In this unified gathering, key administration approaches, and each rekeying message has been multithrown to the entire gathering. However, it is only useful for a set of members and not necessarily the whole group. Nonetheless, a member needs to process all received rekeyed messages to find the single message for which it is targeted. For a large and extremely dynamic group, frequent rekeying may overcome the processing range of lightweight mobile devices. Overall, this rekeying approach represents an inefficient use of resources. Keeping in mind the end goal to address this operational effectiveness issue, HGKM applies a little task component to make miniaturized scale key administration. The vast majority of that rekeying task examination will be restricted to the promptly assaulted activity unit where the join and leave moves are made.

Because of the small size of the activity unit, HGKM can lessen the amount of rekeying data exchanged amid rekeying. The data can be put away in blended data for more proficient correspondence. Because of this transmission, individuals in the quickly assaulted activity unit just need to process this coordinated message to locate the applicable data. With the end goal of examination for HGKM, we expect that the calculation cost of join movement to individuals amid instantly influenced task

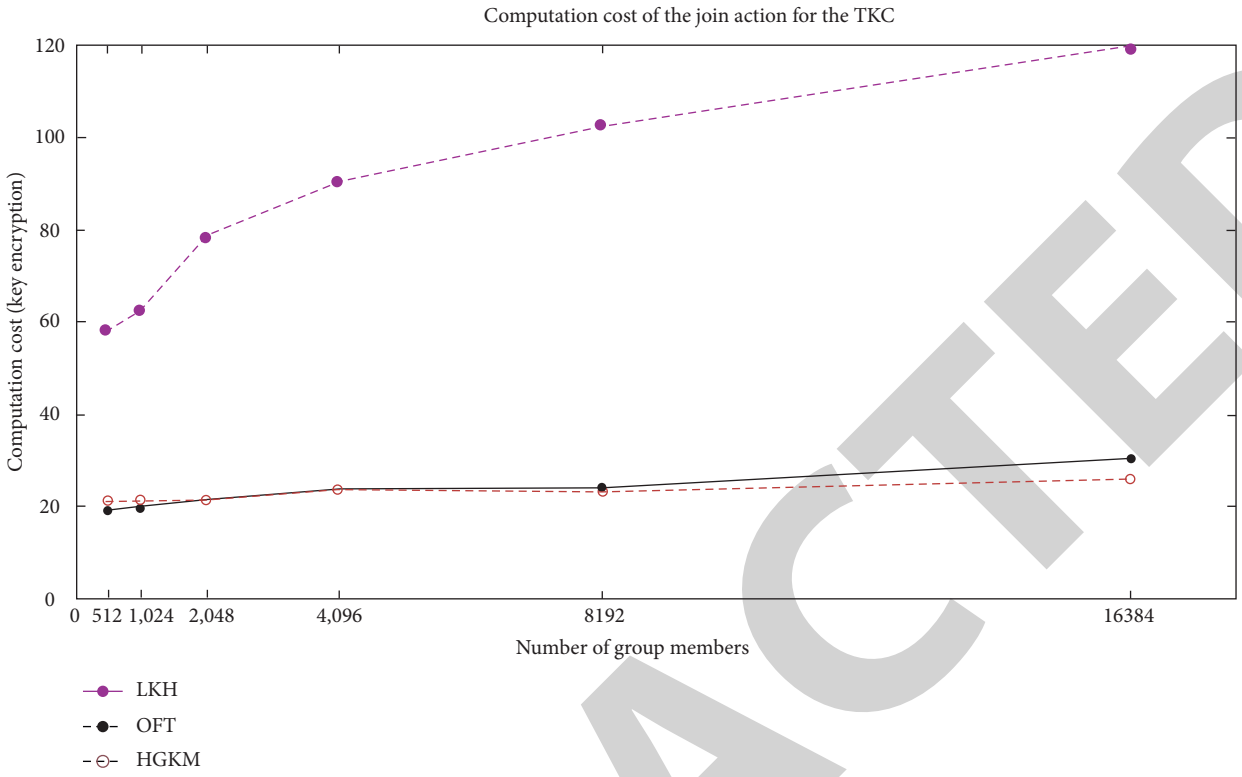

Figure 4: The cost of computing between the join activity and the TKC.

Table 6: The computation cost of join operation to group members.

Group key management algorithm	Joining leader element		Joining member element	
	Members directly affected operation unit	Members outside immediately attacked operation unit	Members directly affected operation unit	Members outside immediately attacked operation unit
HGKM	$h_{\text{unit}} + 1$	1	$h_{\text{unit}} + 1$	1
LKH	H			
OFT	H			

h_unit: the tallest from key tree to activity component in HGKM. h: the highest of that gathering key tree, which measures up to 2 log n; n is the aggregate number of gathering individuals.

components is the number of rekeying messages that include the coordinated bundles. Table 6 abridges the calculation cost of join activity for individuals inside OFT, LKH, and HGK, where the recipe is from the past segments 3 and 4. It is not necessarily helpful to the entire group; only certain members will benefit from it. A member must process each rekeyed message they receive to find the precise message it is meant for. A long and busy group may require more frequent rekeying than the processing power of lightweight mobile devices can handle. Assume that the number of rekeying messages in a coordinated bundle defines the computation cost of connecting people during an immediately impacted job component for the sake of HGKM analysis.

Table 6 shows that in both join situations, the cost of join to the individuals in the rapidly attacked assignment unit is comparable to the height of the key tree for the movement unit. Curiously, the computation cost of join activity for OFT and LKH measures up to that range from the social affairs key tree. LKH appeared differently in relation to the measure of the key tree. Furthermore, OFT and HGKM have few undertaking units. HGKM, along these lines, has favored count adequacy over OFT and LKH. Figure 5 shows the computation cost of join activity.

The calculation cost of join movement to the individuals in the quickly assaulted activity unit in HGKM is a constant esteem and self-sufficient of the gathering level. The explanation behind this is that the highest of the tree keys to the activity unit is controlled by the span of tasks. In this illustration, the extent of the activity unit is settled. Because of the small size of the activity unit, the calculation cost of the join process for the individuals inside the quickly assaulted task unit is decreased compared with that of OFT and LKH. In addition, the individuals in the quickly assaulted task unit are only a small part of the entire gathering. This shows that the smaller scale key administration can decrease the effect of key refreshing on the

Figure 5: The computation cost of join activity to members.

entire gathering in light of the fact that their entry is limited in the range of that activity component. The calculation cost of join is only one for the majority of individuals in HGKM who are outside the specifically influenced activity unit. This lessens the calculation trouble for individuals, particularly for those in an expansive and unique gathering. This component makes HGKM especially reasonable for UAV-MBN systems. For LKH and OFT, the calculation cost of join action is one to two times that of the individuals in this promptly assaulted activity unit and in excess of ten times that of the individuals outside the instantly assaulted task unit. Besides, the calculation cost of join action for LKH and OFT increments logarithmically in connection to the development of the gathering size. The hole in the calculation cost of join amongst HGKM, LKH, and OFT turns out to be consistently more extensive as the gathering size increments. Overall, for individuals, in light of the prior survey and appraisal, HGKM can accomplish a superior execution in the calculation cost of join movement than LKH and OFT. Certain individuals in the group will gain from it, but not necessarily the entire group. A member must process each rekeyed message they receive to find the precise message it is meant for. A long and busy group may require more frequent rekeying than the processing power of light-weight mobile devices can handle. Assume that the number of rekeyed messages in a coordinated bundle defines the computation cost of connecting people during an immediately impacted task component for the sake of HGKM analysis.

The computation cost of the leave operation.

(i) Computation cost of leave operation for the TKC:

As discussed in Section 2.4, for the TKC in HGKM, four leave situations need to be considered when analyzing and evaluating the computation cost of that leave activity. They are

(1) Situation (i): one member leaves from one member element;
(2) Situation (ii): one leader contestant leaves that group;
(3) Situation (iii): one leader leaves that group, and one leadership contestant is available to replace the current leader;
(4) Situation (iv): one leader leaves that group, and no leadership contestant is available to replace the current leader.

In Table 7, we can observe that, in HGKM, the computation costs of the left action for all four situations rely on the tallest of the key trees in the operation element and the number of leader units. In contrast, the computation cost of the leave activity of LKH depends upon the power of the tallest from the key tree group, $O(h2)$, where h denotes the tallest from that group key tree. The computation cost of left to TKC in OFT is only proportional to the tallest in that key tree group, $O(h)$. This is because the new key is generated locally by using an OFT on the members' side. This reduces the computation workload of the TKC in OFT. Example I comprises situations 1, 2, and 3, and example II comprises situations 1 and 4. We understand the entire number of group members is $n_{\text{total\_group\_members}}$, the number of leaders in each leader unit is n_{leader}, the number of leadership contestants is $n_{\text{leadership\_candidates}}$, and the entire number of that members within every member element is $n_{\text{member\_in\_member\_units}}$. The total number of group members equals the summation of the other three groups.

$$n_{\text{total\_group\_members}} = n_{\text{leader}} + n_{\text{leadership\_candidates}} + n_{\text{member\_in\_member\_units}}. \tag{40}$$

We use the data of expectation rate to estimate the normal computation cost for the TKC as follows:

Table 7: The computation cost of the leave action for the TKC.

	Group key management approaches	Computation cost
HGKM	Situation(i) one member departs from one member element	$(h_{\text{unit}}(h_{\text{unit}}+1)/2)+n_{\text{leader\_units}}+1$
	Situation(ii) one leader contestant leaves that group	$(h_{\text{unit}}(h_{\text{unit}}+1)/2)+n_{\text{leader\_units}}$
	Situation(iii) one leader leaves that group also one leadership contestant is available to replace the current leader	$(h_{\text{unit}}(h_{\text{unit}}+1)/2)+5+n_{\text{leader\_units}}$
	Situation(iv) one leader leaves that group, and no leadership contestant is available to replace the current leader.	$(h_{\text{unit}}(h_{\text{unit}}+1)/2)+n_{\text{leader\_units}}$
	LKH	$h(h+1)/2$
	OFT	H

h_{unit}: the tallest of that operation unit present in HGKM. h: highest of key tree group in OFT and LKH. $n_{\text{leader\_units}}$: the number of leader units in HGKM.

(i) Example I:

In example I, the possibility of every situation is as follows:

(1) Situation (i): one member leaves and one member element:

$$p_1(\text{CaseI}) = \frac{n_{\text{member\_in\_member\_units}}}{n_{\text{total\_group\_members}}}. \tag{41}$$

(2) Situation (ii): one leader contestant leaves that group:

$$p_2(\text{CaseI}) = \frac{n_{\text{leadership\_candidates}}}{n_{\text{total\_group\_members}}}. \tag{42}$$

(3) Situation (iii): one leader leaves that group and one leader contestant ready:

$$p_3(\text{Case}I) = 1 - p_1(\text{Case}I) - p_2(\text{Case}I). \tag{43}$$

The normal communication cost of leave activity of example I in HGKM is

$$\begin{aligned}\text{Cost}_{\text{Computation}_{\text{leave}}}(\text{Case}I) &= \text{Cost}_{\text{Scenario}_1} \times p_1(\text{Case}I) + \text{Cost}_{\text{Scenario}_2} \times p_2(\text{Case}I) + \text{Cost}_{\text{Scenario}_3} \times p_3(\text{Case}I),\\ &= \text{Cost}_{\text{Scenario}_1} \times p_1(\text{Case}\,I) + \text{Cost}_{\text{Scenario}_2} \times p_2(\text{Case}\,I) + \text{Cost}_{\text{Scenario}_3}\\ &\quad \times (1 - p_1(\text{Case}\,I) - p_2(\text{Case}\,I)),\\ &= \frac{h_{\text{unit}}(h_{\text{unit}}+1)}{2} + 5 + n_{\text{leader}_{\text{units}}} - 4 \times p_1(\text{Case}\,I) - 5 \times p_2(\text{Case}\,I).\end{aligned} \tag{44}$$

(ii) Example II:

In example II, the possibility of every situation is as follows:

(1) Situation (i): one member leaves one member element:

$$p_1(\text{CaseII}) = \frac{n_{\text{members\_in\_member\_units}}}{n_{\text{total\_group\_members}}}. \tag{45}$$

(2) Situation (iv): one leader leaves that group, and also no leader contestant is ready:

$$p_4(\text{Case}II) = 1 - p_1(\text{Case}II)\ldots \tag{46}$$

The normal communication cost from leave activity of example II in HGKM is

$$\begin{aligned}\text{Cost}_{\text{computation}_{\text{leaving}}}(\text{case}II) &= \text{Cost}_{\text{scenario\_1}} \times p_1(\text{Case}II) + \text{Cost}_{\text{scenario\_4}} \times p_4(\text{Case}II) - \frac{h_{\text{unit}}(h_{\text{unit}}+1)}{2}\\ &\quad + 2 + n_{\text{leader}_{\text{units}}} - p_1(\text{Case}II).\end{aligned} \tag{47}$$

Figure 6 illustrates the normal computation costs of left to the TKC in both examples with the growth of group size, where the operation unit has 32 members.

From Figure 6, it can be observed that the costs for both cases are the same and increase with variations in group size. In both cases, the situation of member-leave-from-a-

member-unit makes a major and similar contribution to the total estimated cost of the leave action, since the majority of members are present in member units and the most frequently occurring leave process is the member-leave-from-a-member-unit.

The measurement of the computation cost of leave activity of HGKM (examples I and II), LKH, and OFT is shown in Figure 7. It can be seen that OFT has the smallest computation cost of that leave activity because it applies the OFT to compute the intermediate supporting keys in the key tree. However, this computation performance is on the charge of safety; OFT is susceptible to collusion attacks, where ex-group members can cooperate to calculate the current group key by applying their outdated keys. HGKM can also achieve computation efficiency for the TKC, although the cost is a little higher than that of OFT. Nevertheless, HGKM has no security loopholes that could be subject to collusion attacks. The average estimated cost of the leave process for TKC in HGKM changes slowly with respect to the growth of group size. LKH has the highest estimated cost, two to three times that of HGKM. Moreover, this cost increases exponentially with respect to the growth of group size. Figure 6 shows that the expenses are the same for both scenarios and rise as the group size changes. In both situations, the member-leave-from-a-member-unit situation contributes significantly and similarly to the estimated overall cost of the leave action. Because it uses the OFT to calculate the intermediate supporting keys in the key tree, LKH and OFT are illustrated in Figure 7. It can be observed that OFT has the lowest calculation cost for leave action. However, the safety of this computing performance is at risk since OFT is vulnerable to collusion attacks, in which former group members work together to compute the current group key using their old keys.

3.2.2. The Computation Cost from Leave Activity to Members. Table 8 summarizes the computation cost that leaves the activity to members in HGKM during this rekeying process, where the formulae are from Section 3 and 4.

In Table 8, it can be observed that there are three types of computation costs that leave the activity to different members. Since HGKM applies small-key management within the control unit and the parts are treated differently, there are three kinds of members during rekeying: those in the immediately attacked operation element; newly chosen leaders to this immediately attacked member unit; and members outside the immediately attacked operation unit.

Members within this immediately attacked operation unit have the highest computation cost of the leave activity. This cost is proportionate to the tallest of these key trees to the operation element. Due to the small size of the operation unit, this computation cost is still low compared to that of LKH and OFT.

The recently picked pioneer of this quickly assaulted task component just gets two rekeying messages amid the rekeying method. The individuals outside the promptly assaulted pioneer unit just get one single rekeying message focused on them. Interestingly, in LKH and OFT, a bunch of individuals get h rekeying messages where h squares to the highest of the gathering key tree. Figure 8 outlines the calculation cost of the leave task for the individuals in HGKM, OFT, and LKH. We accept the extent of activity unit 32. From Figure 8, we can see that, for individuals, HGKM has a favorable position over LKH and OFT in connection with the calculation cost of the leave task. In HGKM, because of the application of short-enter administration in the activity units, major rekeying is performed inside the quickly assaulted task unit where one part leaves this gathering. The calculation cost of leaving action to individuals in the instantly assaulted task unit is still low in light of the fact that the measure of the activity unit is little. Moreover, individuals outside the promptly assaulted activity unit just get one rekeying message-a change compared to those in LKH and OFT. In Figure 8, it can be seen that HGKM diminishes the calculation cost for individuals and advantages asset-constrained cell phones. On the off chance that the degree of the task component is resolved in HGKM, the calculation cost of left action turns into a steady esteem and is free of gathering size.

This enables individuals to deal with the limitations of their cell phones by taking an interest in gathering applications. In restriction, the calculated cost of leave action to individuals in OFT and LKH is a few times that of HGKM. Additionally, the calculation cost for LKH and OFT increments by most of the gathering degree.

In the synopsis, in light of the above examination and correlation, HGKM can achieve better computation efficiency for members during rekeying for the leave operation than LKH and OFT, especially for the majority of members who are outside of the immediately attacked operation unit. We have determined that HGKM can attain greater computation efficiency in the rekeying process for both join and leave operations.

P_1 (Example I): the possibility of situation (i) in example I,

$$P_1(\text{Example } I) = \frac{n_{\text{member\_in\_member\_units}}}{n_{\text{total\_group\_members}}}. \tag{48}$$

P_1 (Example I): the possibility of situation (ii) in example I,

$$P_2(\text{Example } I) = \frac{n_{\text{leadership\_candidates}}}{n_{\text{total\_group\_members}}}. \tag{49}$$

P_1 (Example II): the possibility of situation (i) in example II,

$$P_1(\text{Example } II) = \frac{n_{\text{nmember\_in\_member\_units}}}{n_{\text{total\_group\_members}}}. \tag{50}$$

The contribution of HGKM to the computation efficiency can be summarized as the application of short-key management within this operation unit. The rekeying operation is confined to a small area. The computation cost for the TKC is therefore reduced. The small computation cost for members can reduce the workload on light-weight mobile devices, making HGKM suitable for the wireless

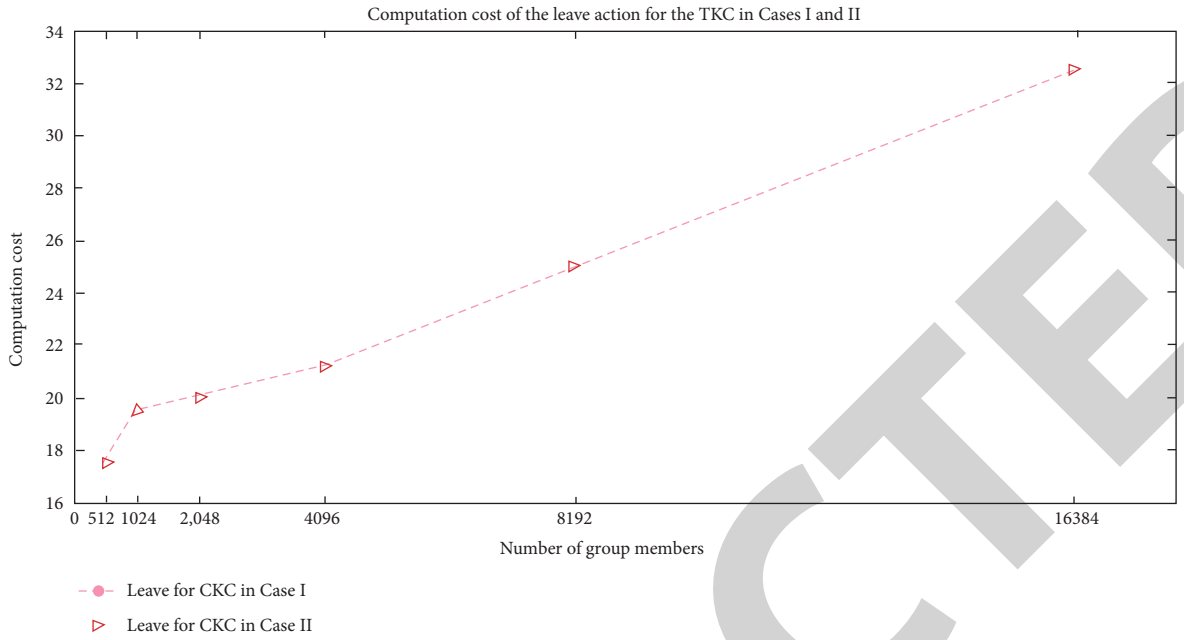

Figure 6: The computation cost of leave activity to the TKC in examples I and II.

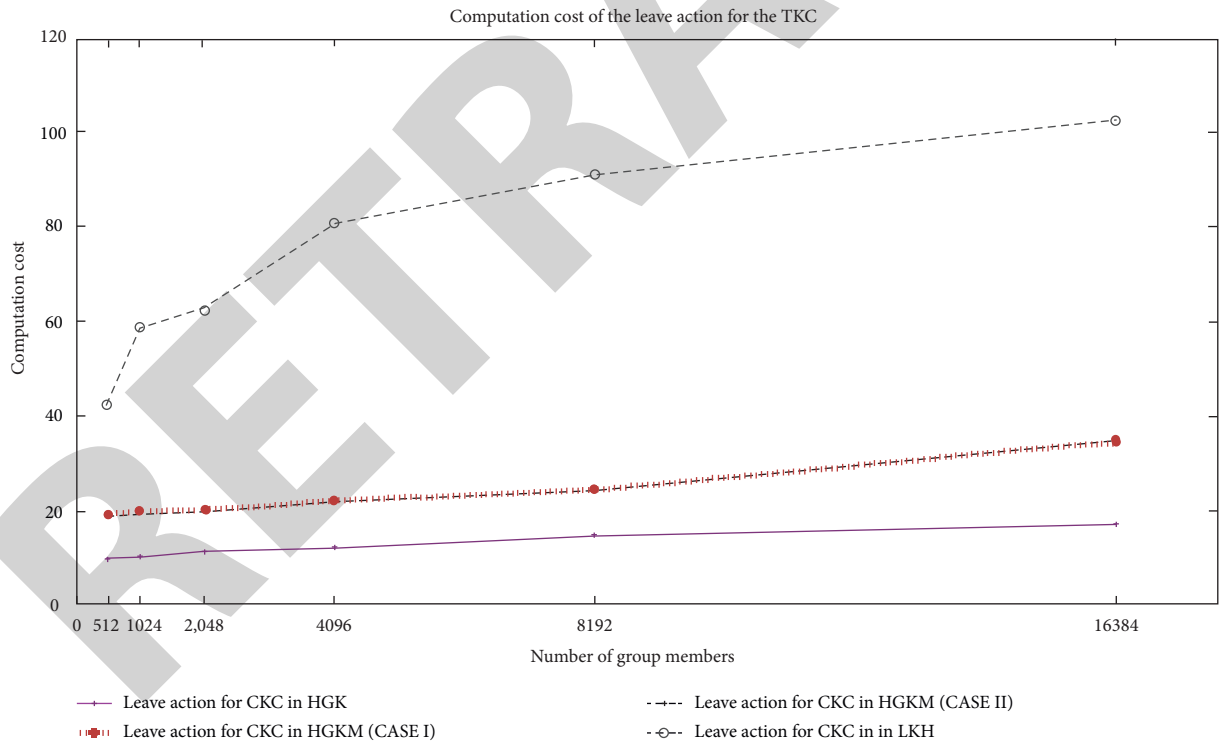

Figure 7: Computation costs from leave activity to the TKC.

network. The constant value of computation cost for members in HGKM facilitates a user to judge its computation power to decide whether it can afford to join a group application. Table 9 shows the specific reviews that compute the cost of the join and leave operations on both the TKC and members in HGKM.

3.3. Key Storage Cost. Key stockpiling cost measures the assortment of keys put away for both the TKC and individuals in the UAV-MBN hubs. In HGKM, because of applying smaller scale key administration, a part is relegated to a little agent component where various leveled key trees are worked for key administration. An individual in the

Table 8: The computation cost of leave activity to members.

Group key management approaches		Computation cost		
		Member in immediately affected operation element	Newly chosen leader from that affected member element	Members outside the immediately affected operation element
HGKM	Situation (i): one member leaves one member element	$h_{\text{unit}} + 1$	0	1
	Situation (ii) one leadership contestant leaves	$h_{\text{unit}} + 1$	0	1
	Situation (iii) one leader leaves that group also one leadership contestant is ready	$h_{unit} + 1$	2	1
	Situation (iv) one leader leaves one group also never leadership contestant is ready	$h_{unit} + 1$	0	1
LKH			H	
OFT			H	

h_{unit}: the tallest from that key tree to operation element; h: the tallest from that group key tree.

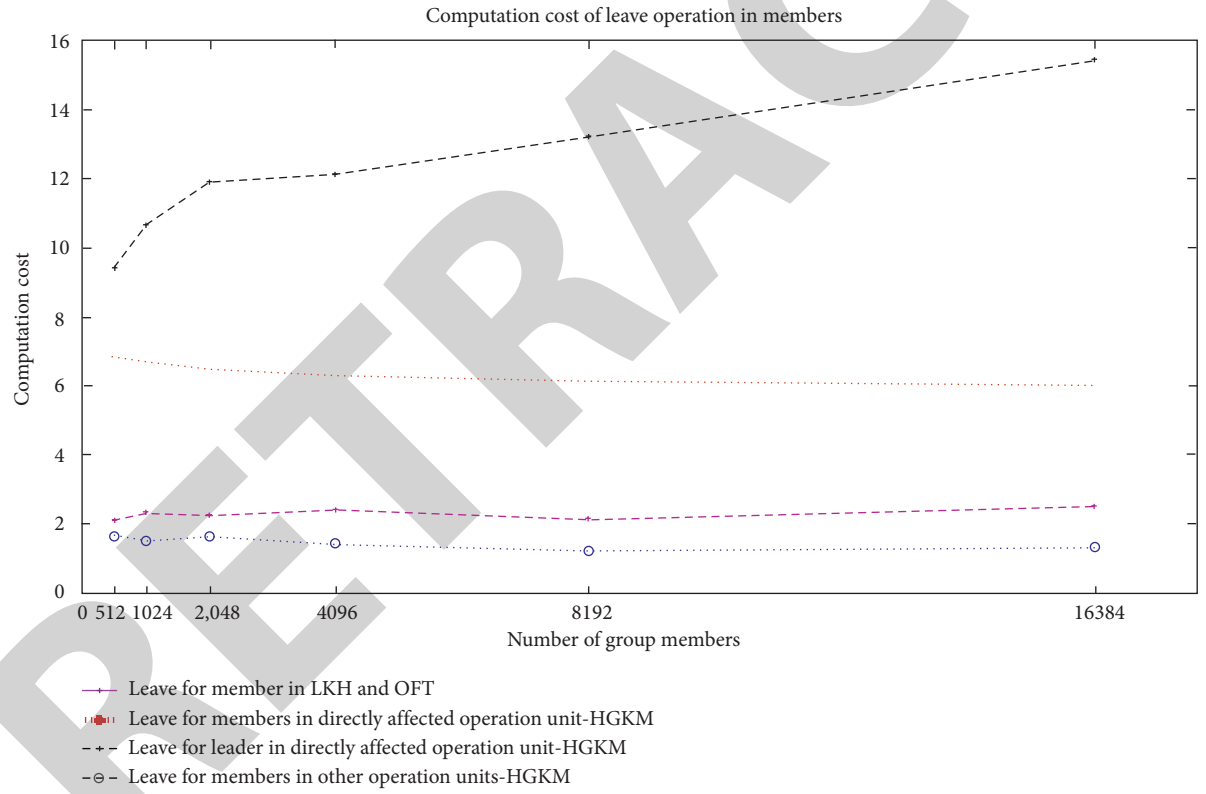

Figure 8: The computation cost of leave operation to members.

activity unit in this manner needs to keep track of the position of the key structures from its leaf hub along the way to the source hub. The number of put-away keys is $h$unit + 1, which is the highest form of that key tree to the task unit. Adjacent to these keys, the part additionally needs to store the gathering activity encryption key (GTEK) and the venue movement encryption key (CTEK) for partaking in the gathering application. In this way, the whole number of keys is a part of what is needed to spare. On the off chance that a part is assigned as a pioneer, it needs to store an additional key−−the unit key of the related part unit. Thusly, the whole of the key is spared by the pioneer. As far as LKH and OFT, when these two methodologies are connected in the remote theater, a part additionally 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. Along these lines, the whole number of spared keys is $h + 2$ (the key for the root hub can be filled in as CTEK), where h is the highest of that gathered key tree for LKH and OFT. On the TKC side, in HGKM, all operation units have the same fixed size, so the entire

Table 9: The computation cost of join and leave operations in HGKM.

		Computation cost
Join	The TKC	$(h_{\text{unit}}+1)(h_{\text{unit}}+2)/2+2-n_{\text{member\_in\_leader\_units}}/n_{\text{total\_group\_members}}$
	Members of that immediately affected operation element	$h_{\text{unit}}+1$
	Outside members affected directly by operation unit.	1
Leave	The TKC in Case I	$h_{\text{unit}}(h_{\text{unit}}+1)/2+5+n_{\text{leader\_units}}-4\times p_1(\text{Case}I)-5\times p_2(\text{Case}I)$
	The TKC in Case II	$h_{\text{unit}}(h_{\text{unit}}+1)/2+2+n_{\text{leader\_units}}-p_1(\text{Case}II)$
	Members of that immediately affected operation element	$h_{\text{unit}}+1$
	Newly elected leader of immediately affected member element	2
	Members outside the immediately affected operation element	1

h_{unit}: the highest operation element; $n_{\text{member\_in\_leader\_units}}$: the entire number of members within this leader element; $n_{\text{total\_group\_members}}$: the entire number of members within this group;

Table 10: The key storage cost of OFT, HGKM, and LKH.

Group key management	TKC	Group user	
		Leader	Member/leadership candidate
HGKM	$s/s_{\text{operation\_unit}}\times(2s_{\text{operation\_unit}}-1)$	$h_{\text{unit}}+4$	$h_{\text{unit}}+3$
LKH	$2s-1$	$h+2$	
OFT	$2s-1$	$h+2$	

$S_{\text{operation\_unit}}$: the size of operation unit in HGKM. S: the size of group. h_{unit}: the highest key structure of the operation element in HGKM. h: the highest key tree in LKH and OFT.

Table 11: The key storage cost of TKC.

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

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

$$\begin{aligned} n_{\text{keys\_in\_unit}} &= 1+2+4+8+\ldots+s_{\text{operation\_unit}} \\ &= 2s_{\text{operation\_unit}}-1, \end{aligned} \tag{51}$$

where $S_{\text{operation\_unit}}$ is the size of the operation element.

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

$$n_{\text{unit}}\times n_{\text{keys\_in\_unit}}=\frac{s}{S_{\text{operation\_unit}}}\times\left(2s_{\text{operation}_{\text{unit}}}-1\right). \tag{52}$$

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

The gathering size is bigger than that of the task unit. For individuals, the key stockpiling cost is close to the highest of the gathering key structures, which is chosen by the gathering size. Figures 5 and 6 illustrate the key storage costs from both the TKC's and members' perspectives in OFT, LKH, and HGKM. The expected measure of the activity unit is 32 in HGKM.

From Table 11, it can be observed that, for the TKC, the key storage costs are quite similar in all three approaches as they all apply a hierarchical structure. For members, in relation to key storage costs, HGKM has the best performance.

4. Conclusion

In this research, we provide a fresh GKM technique called half-and-half gathering key administration (HGKM), with the aim of addressing the challenges of operational proficiency in distant gathering key management. The newly developed method efficiently analyses the operational part's scale-key organization. People are grouped together and then dispersed in an arrangement made by an operational segment for key organization motivation. Scaled-back key organization is conducted in light of these movement units. Additionally, the operational method was restricted by the key administration process, which also decreased the operation's expense in terms of key creation, calculating, and associated correspondence. Overall, the newly introduced

HGKM technique strengthens the operational procedure and functions effectively in reasonable remote areas. The model's generalization to additional connectivity limitations and other objective functions represents a significant area for future research. For example, we want to apply the findings to connectivity models other than the disc connectivity model that are more accurate.

Data Availability

The data can be made available from the corresponding author upon request.

Conflicts of Interest

The authors declare that there are no conflicts of interest.

References

[1] M. Steiner, G. Tsudik, and M. Waidner, "Diffie-Hellman key distribution extended to group communication," in *Proceedings of the 3rd ACM Conference on Computer and Communications Security*, pp. 31–37, 1996, January.

[2] 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.

[3] R. Mahaveerakannan and C. Suresh Gnana Dhas, "Big data analytics for large-scale UAV-MBN in quantum networks using efficient hybrid GKM, Concurrency and Computation:," *Practice and Experience*, vol. 34, no. 1, 2019.

[4] A. Irshad, H. F. Ahmad, B. A. Alzahrani, M. Sher, and S. A. Chaudhry, "An efficient and anonymous chaotic map based authenticated key agreement for multi-server architecture," *KSII Transactions on Internet and Information Systems (TIIS)*, vol. 10, no. 12, pp. 5572–5595, 2016.

[5] M. Sumathi and S. Sangeetha, "A group-key-based sensitive attribute protection in cloud storage using modified random fibonacci cryptography," *Complex & Intelligent Systems*, vol. 7, pp. 1733–1747, 2020.

[6] M. A. Haq, "Optimal cluster head selection for energy efficient wireless sensor network using hybrid competitive swarm optimization and harmony search algorithm," *Sustainable Energy Technologies and Assessments*, vol. 52, no. 102243, pp. 1–5, 2022.

[7] J. Bhola, M. Shabaz, G. Dhiman, S. Vimal, P. Subbulakshmi, and S. K. Soni, "Performance evaluation of multilayer clustering network using distributed energy efficient clustering with enhanced threshold protocol," *Wireless Personal Communications*, 2021.

[8] C. K. Wong, M. Gouda, and S. S. Lam, "Secure group communications using key graphs," *ACM SIGCOMM - Computer Communication Review*, vol. 28, no. 4, pp. 68–79, 1998.

[9] A. Irshad, W. Noshairwan, M. Shafiq, S. Khurram, E. Irshad, and M. Usman, "Security enhancement in MANET authentication by checking the CRL status of servers," *Int J Adv Sci Technol*, vol. 1, pp. 91–98, 2008.

[10] C. J. Mitchell, "Security issues in a group key establishment protocol," *The Computer Journal*, vol. 62, no. 3, pp. 373–376, 2018.

[11] R. Di Pietro, L. V. Mancini, and S. Jajodia, "Providing secrecy in key management protocols for large wireless sensors networks," *Ad Hoc Networks*, vol. 1, no. 4, pp. 455–468, 2003.

[12] D. Bhargava, B. Prasanalakshmi, T. Vaiyapuri, H. Alsulami, S. H. Serbaya, and A. W. Rahmani, "CUCKOO-ANN based novel energy-efficient optimization technique for IoT sensor node modelling," *Wireless Communications and Mobile Computing*, vol. 2022, 9 pages, 2022.

[13] I. Rubin and P. Vincent, "Topological synthesis of mobile backbone networks for managing ad hoc wireless networks," in *Proceedings of the IFIP/IEEE International Conference on Management of Multimedia Networks and Services*, pp. 215–221, Springer, Berlin, Heidelberg, 2001, October.

[14] D. Chen, D.-Z. Du, X.-D. Hu, G.-H. Lin, L. Wang, and G. Xue, "Approximations for Steiner trees with minimum number of Steiner points," *Journal of Global Optimization*, vol. 18, no. 1, pp. 17–33, 2000.

[15] C. K. Wong, M. Gouda, and S. S. Lam, "Secure group communications using key graphs," *IEEE/ACM Transactions on Networking*, vol. 8, no. 1, pp. 16–30, 2000.

[16] M. Steiner, G. Tsudik, and M. Waidner, "Key agreement in dynamic peer groups," *IEEE Transactions on Parallel and Distributed Systems*, vol. 11, no. 8, pp. 769–780, 2000.

[17] S. Rafaeli and D. Hutchison, "A survey of key management for secure group communication," *ACM Computing Surveys*, vol. 35, no. 3, pp. 309–329, 2003.

[18] Y. Kim, A. Perrig, and G. Tsudik, "Communication-efficient group key agreement," in *Proceedings of the IFIP International Information Security Conference*, pp. 229–244, Springer, Boston, MA, 2001, June.

[19] R. Mohan Naik and S. V. Sathyanarayana, "Key management infrastructure in cloud computing environment-a survey," *ACCENTS Transactions on Information Security*, vol. 2, no. 7, pp. 52–61, 2017.

[20] R. K. Garg, J. Bhola, and S. K. Soni, "Healthcare monitoring of mountaineers by low power Wireless Sensor Networks," *Informatics in Medicine Unlocked*, vol. 27, Article ID 100775, 2021.

[21] S. Iqbal, M. L. Mat Kiah, A. Ur Rehman, Z. Abbas, and B. Daghighi, "DM-GKM: A key management scheme for dynamic group based applications," *Computer Networks*, vol. 182, Article ID 107476, 2020.

[22] M. A. Haq, "Development of PCCNN-based network intrusion detection system for EDGE computing," *Computers, Materials & Continua*, vol. 71, no. 1, pp. 1729–1750, 2021.

[23] Y. Kim, A. Perrig, and G. Tsudik, "Group key agreement efficient in communication," *IEEE Transactions on Computers*, vol. 53, no. 7, pp. 905–921, 2004.

[24] Y. Kim, A. Perrig, and G. Tsudik, "Tree-based group key agreement," *ACM Transactions on Information and System Security*, vol. 7, no. 1, pp. 60–96, 2004.

[25] Y. Sun, W. Trappe, and K. R. Liu, "A scalable multicast key management scheme for heterogeneous wireless networks," *IEEE/ACM Transactions on Networking*, vol. 12, no. 4, pp. 653–666, 2004.

[26] H. Kim, B. Chung, Y. Lee, Y. Park, and H. Yoon, "Weakness of the synchro-difference lkh scheme for secure multicast," *IEEE Communications Letters*, vol. 11, no. 9, pp. 765–767, 2007.

[27] M. H. Park, Y. H. Park, H. Y. Jeong, and S. W. Seo, "Key management for multiple multicast groups in wireless networks," *IEEE Transactions on Mobile Computing*, vol. 12, no. 9, pp. 1712–1723, 2012.

[28] 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, no. 8, pp. 1545–1559, 2014.

[29] R. Mahaveerakannan and C. Suresh Gnana Dhas, "A hybrid group key management scheme for uav–mbn network environment increasing efficiency of key distribution in joining operation," in *Proceedings of the International Conference on Intelligent Information Technologies*, pp. 93–107, Springer, Singapore, 2017, December.

[30] R. Droms, *Dynamic Host Configuration Protocol*, Network Working Group - RFC, vol. 2131, March 1997.