Received: 17 May 2019 | Revised: 23 July 2019 | Accepted: 24 August 2019
DOI: 10.1002/cpe.5559

Check for updates

WILEY

RESEARCH ARTICLE

Big data analytics for large-scale UAV-MBN in quantum networks using efficient hybrid GKM

Mahaveerakannan R[1] | Suresh Gnana Dhas C[2]

[1]Information Technology, St. Peter's University, Chennai, India
[2]Vivekanada College of Engineering for Women, Namakkal, Elaiyampalayam, Tamil Nadu

Correspondence
Mahaveerakannan R, Information Technology, Information Technology, St Peters Institute of Higher Education and Research, Avadi, Chennai, Tamil Nadu, 600054.
Email: mahaveerakannan10@gmail.com

Summary

A primary important aspect of wireless network domain is known to be secured communication as the signals are emphatically available and broadcasted through the air. Quantum wireless networks are a hot topic of research in recent years that made researchers to avail new techniques in this field. Big data is one of the major aspects that support large-scale quantum network applications. As sensor nodes have resource constraints, it is more complex when using the traditional techniques of key establishment that only used for stable communication networks. Group-related applications are also one of the important aspects in wireless network for sending and receiving messages from multiple users. Unfortunately, maintenance of security for the group-oriented protocols is major issue due to the frequent changes in membership. In this paper, a hybrid GKM with re-keying procedure is proposed to obtain a secure communication for the remote system of unmanned autonomous vehicle (UAV) with mobile backbone network (MBN). Here, the group controller is selected based on the simplified hybrid energy efficient distributed (HEED) protocol and honey key encryption algorithm is used by the key management center (KMC) for generating and distribution of key for the group's controller. The secure communication is explored using the key exchange mechanism between the nodes. The joining and leaving of a node from the group are initiated by the re-keying process. The simulation results explain the improved performance of the proposed hybrid method when compared with other existing techniques in terms of privacy level, energy, memory, and time consumption.

KEYWORDS

group key management (GKM), hybrid energy efficient distributed (HEED), mobile backbone network (MBN), security, unmanned autonomous vehicle (UAV)

1 | INTRODUCTION

Wireless sensor network (WSN) has developed prominently in recent years due to its numerous applications based on control and surveillance. The controlling for access is the major aspect and security issue for the communication in a group environment. The traffic encryption key (TEK) or group key is circulated to all individual, which is used to encrypt the information passing over the network. The communication content can be disclosed to the individual who holds the key that is circulated by TEK or group key. The group keys' safety is responsible for the integrity and privacy of group's communication. Several receivers are included in a group communication and efficient regeneration, generation, and delivery of such key is a challenging and complicated task. The communication of the group would be active even if the member leaves the group and cannot force the departing node/member to forget the key. The updating of group key is much important as the communication information can be accessed by the previous members.[1-3]

Mobile ad-hoc network (MANET) is one type of the wireless ad-hoc networks, which has no fixed infrastructure and central administration. The auto configuration and routing problems are the major investigations of ad-hoc networks and also for the defense mechanism. The information is gathered and routed by sensor nodes to the base stations. The data messages are controlled and regulate the routing between the nodes using network routing protocols. The communication overhead is decreased and computation is localized by the practice of grouping in WSNs.[4] The

 © 2019 John Wiley & Sons, Ltd.

grouping of sensor nodes operation is to select the group controllers or heads among them. The communication and organization between the nodes are the responsibility of the group controller node. Several key management and routing protocols are proposed to analyze the concept of group controlling.[5] Normally, cluster contains the head node and group has controller node. The difference between the grouping and clustering is that group only concentrated on a small area, whereas the clustering is ubiquitous. A group will be union or a part of the several clusters. Re-keying management is the process of managing the group key, it mainly replaces the old lock pins and distributes the new one. Several protocols are used for re-keying management and such kinds are *n* node-one controller, GKMP, logical key hierarchy graph, and one-way functional tree.

The most important and reliable research domain in the area of WSN is security. The group keys' trusted transmission between the reasonable nodes in the group is responsible for the secured group communication. It consists the communication across the nodes, which are suitable to receive or send messages to the group. The group nodes only know the asymmetric group key that is used to encrypt the data traffic between the group users. The group key management system controls the access of the group key. The new users that are certified will be given group key by the GKM system and the re-keying process is performed when the nodes are joining or leaving the network.[6,7] Group key management (GKM) only focused on distribution and generation of keys among the group members. The group members participated mainly in creation, secure distribution, and revocation of keys. Two main entities are used for managing the communication of GKM and these are key server (KS) and group controller (GC). However, when big data is a major concern, then the GKM is not more efficient in using for large-scale applications.[8] Therefore, to overcome this issue, efficient GKM model is proposed with hybrid of HEED protocol.

In this research, we propose a hybrid GKM (HGKM) with re-keying protocol for UAV-MBN system based on MANET. The proposed technique is applicable for several other scenarios for the UAV-MBN network in the field of military environment. The strength and secrecy of the used group key are the main concept of security in group communication. The group data of the future communication cannot be accessed by the member who left the network that is known as forward secrecy and the past group data cannot be accessed by the new joined members, which ensured by backward secrecy. The re-keying mechanism helps in defending the security association. Organization of this paper is as follows. Section 2 will analyze the related works, Section 3 analyzes the proposed methodology, Section 4 evaluates the simulation results and discusses the impacts, and Section 5 discusses the conclusion and future scope of study.

2 | RELATED WORKS

Several cryptographic techniques are proposed by many researchers for addressing the problem of group key management. In this segment, the review of contributory and centralized group key managements and the authentication efficiency for the re-keying messages are discussed. Sumathy and Kumar[9] proposed the secure mechanism of encryption and key exchange for the communication of groups in wireless ad-hoc network. A MAC address is used in this technique as an extra advantage for the encryption of message key and data transmission among the clients. Key management is the prime factor for proper and safe generation, distribution, and withdrawal of keys that is used to secure messages. For exchanging the keys, RSA algorithm is used for the secure channel after the encryption process is done.

Bawa et al[10] analyzed a scheme named random pre-key distribution for ensuring security, connectivity, and resilience in WSN. The keys are created and distributed by employing the binomial key pattern. The partition of network is processed as scattered nodes and implemented the authentication for the secure communication. The calculation and comparison are processed for traffic density and throughput. The performance of the proposed technique based on connectivity gives high reliability than the existing approaches. Zhang and Wang[5] secured the communication channel by updating the key using the proposed model named certificate-less effective key management (CL-EKM). The group-aligned key communication uses the keys presented by the CL-EKM and the node communication with pairwise is secured. The nodes simulation is done by adopting Manhattan mobility and random walk model. The static network in WSN is not suited by CL-EKM as like dynamic networks.

Wang et al[4] designed a proxy recryptography-based GKM strategy for near space network. The re-keying process uses the proxy recoding schema and failure of single level trouble is solved. The cipher text conversion from one group to other is done by proxy recryptography by permitting semitrusted proxy. In this model, the encrypted message by the group A can be decrypted by the group B members. Yao et al[11] proposed a GKM scheme with low power based on LKH++ for providing the security in WSNs. A secure tree is constructed for managing the networks group key. The construction of tree is explained by this scheme and keys are handled by this method. The survivability and security of the network are enhanced by the wireless LKH.

Jiang et al[12] analyzed scalable and secure GKM scheme based on hierarchal cluster (HRKT) that is used for dividing the group key into cluster-key and cluster-head-key. The route-key structure and logic-tree are important reasons to run this proposed scheme. The generation of route-key tree by the cluster head relies on the clusters route topology. The hybrid techniques that were proposed by Murugan and Devi[13-15] are the basic and important ideas behind the hybridization of algorithms that helps many researches to develop a new model by combing the key management models.

Zhao et al[16] analyzed the cluster WSN using hybrid key management technique. The clustered WSNs security is improved by a unique session-key that is produced between the cluster-heads. Doraipandian et al[17] focused the LU matrix that is based on group and node-to-node communication by developing a hybrid key management scheme. The security between the base station and CH is improved by using the public key encryption technique named ElGamal. The high node-to-node and resilience connectivity is achieved even when the base station and CH are disclosed to the attackers.

This paper (Raja and Pushpa[18]) has proposed a movie recommendation approach using integrated matrix factorization and temporal-aware clustering optimization (NOMINATE). This approach uses temporal information to update the rules that is used to derive personalized preferences of the users through probabilistic matrix factorization. K-Means and PSO-based clustering algorithm are used to group users with similar preferences. Personal preferences of the users are integrated through linked open data to select a set of optimal preferences of the users. Top-N recommendation list for the users is generated through ranking methods.

Geetha and Kannan[19] analyzed an integration of probabilistic key predistribution and polynomial pool-based scheme with hybrid key establishment for pairwise key generation to each pair of neighbors sensor nodes in WSN. The estimation of keys is utilized by the nodes having polynomial shares. The key pool is made by combining the estimated keys. The keys are preloaded to the balance sensor nodes, which are obtained by the key-pool. Three phases are composed in this proposed scheme and these are initialization phase, path-key establishment phase, and direct-key establishment path. Key distribution servers (KDSs) are used for deploying the initialization phase, the predistribution of polynomial share is processed in P-sensor, the key-pool is generated and applied for B-sensors, and at last, the key generated is predistributed. The metrics like memory consumption, connectivity, resilience, and communication overhead against attacks are used to analyze the proposed scheme performance.

Prakash et al[20] described the predictive re-keying mechanism with efficient key management protocol for dynamic networks. The re-keying helps in reducing the congestion that is used in this proposed method. The re-keying frequency, minimization of mobility, reduction of re-keying overhead, and improving scalability are processed by the novel predictive model that is used by the proposed mechanism. Rajamanickam and Veerappan[21] proposed a model for MANETs multicast security using re-keying technique and intercluster communication. This technique is addressed by using the centralized key manager by distributing the nodes private key shares. The performance of cluster re-keying is done for the joining of new member in the cluster.

Kong et al[22] analyzed the security framework measurement for multi-level ad-hoc networks for the unmanned aerial vehicles (UAVs). Depending upon the networks infrastructure availability, the framework is designed by two modes and these are infrastrure-modes and infrastructure less-mode. The design of UAV relay networks with self-organizing paradigm is proposed by Orfanus et al[23] for tackling issues and to support military applications. Rhee et al[24] proposed a model by using key management approach with two layers and these are (1) group nodes consisted in cell groups and (2) cell group managers consisted in control groups. The membership change effect is restricted, which is the main motivation of this approach to the single group. Sahban et al[7] proposed a group communication management for UAV-MBN networks. The authors discussed the detailed survey regarding the group key communication and the challenges that made UAV-MBN more complicated. The security susceptibility, adverse circumstance, and influence are also focused.

3 | PROPOSED MODEL

Figure 1 shows the proposed efficient hybrid model with GKM for UAV-MBN network system in WSN. The process of this hybrid model collects several nodes in the network and uses the simplified HEED protocol to group the WSNs with one group-controller (GC) for each group. Based on this simplified HEED, the GC is selected for each group. The initial parameter is provided from the remaining energy and secondary parameter is exploited as distance to the neighbors. The keys are distributed and monitored to the group members by the group-controller. The secure key is generated using the dedicated key management center (KMC).

A key request is sent to KMC when the node is initiated for data communication. Based on the honey encryption algorithm (HEA), the keys are generated. The termination of node or alarm is accessed when compromise attack is sensed by the network. The re-keying process is initiated by the proposed model when the node is leaving or joining the network. The key-exchange Diffie-Hellman algorithm is used by the proposed method for securing communication among the group members. The framework process of this proposed model is shown in Figure 1.

Group Key Generation:

The relationship of key is established between the legitimate parties and assisted by the GKM. The group is formed by using the authorized parties. Furthermore, the access control is applied on the group by using it. Set of users are available in groups, which is named as group-members. The group-key-req is sent by the group-controller to the key management center (KMC). The group key and individual-key are present in the group-key-req that is generated and the secure-key is forwarded to its group-controller. The HEA-based keys are generated. The steps for the generation of group key are described as follows.

Group Key Generation Procedure:

Step 1: Two prime numbers distinctly chosen as a and b.

Step 2: Calculate $n = ab$.

Step 3: Calculate $\varphi(n) = \varphi(a)\varphi(b) = (a - 1)(b - 1)$.

Step 4: Integer T is chosen such that $1 < T < \varphi(n)$.

Step 5: GCD $(T, \varphi(n)) = 1$.

Step 6: Find G as $G^{-1} \equiv T(\text{mod } \varphi(n))$.

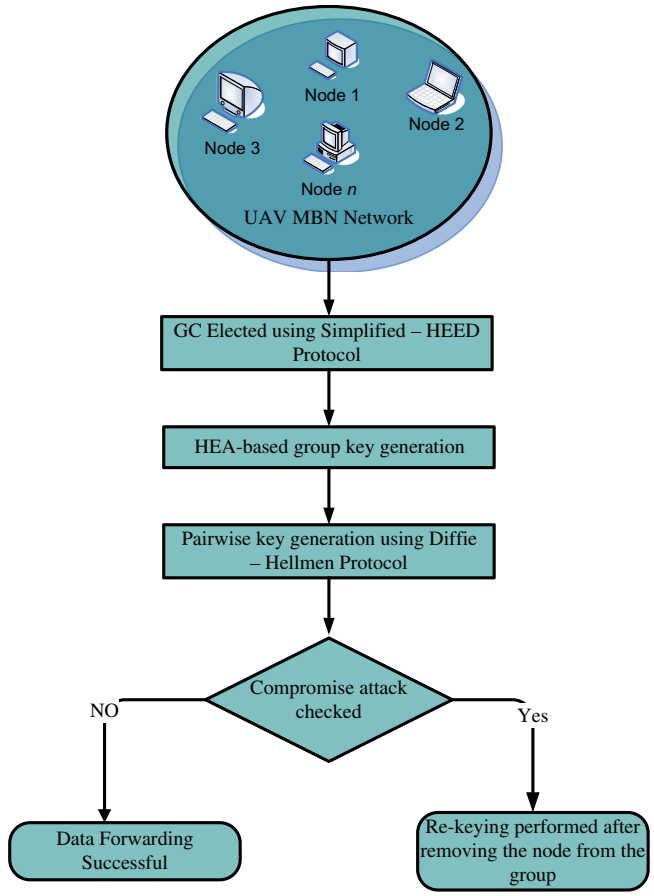


FIGURE 1 Framework process of proposed model

Step 7: Public encryption key is published as (T,n).
Step 8: Hold secret decryption-key: (G,n).
//Encryption
Step 9: $q \equiv s^T (\text{mod } n) 0 \leq s < n$.
//Decryption
Step 10: $s \equiv q^G (\text{mod } n)$.

Independently, the group key (GK) is produced by the sub-group key (SGK) from this GKM scheme. The partial keys are used to generate this key that gathered from the members. Equation (1) shows the member that is present under SGC.

$$\begin{aligned} GK &= s^k 1^k 2^k 3^k GC \\ SGK0 &= s^l 1, 1^l 2, 1^l 3, 1^l 4, 1^l 5, 1^l 6, 1^l 7, 1^l 8, 1^k 1. \end{aligned} \tag{1}$$

The dynamic secret sharing scheme is used for generating keys that are assigned between group members. The individual key is combining with the generated GK of the nodes present in the cluster, which is known as auxiliary key.

Enhanced Simplified HEED Protocol:

The cluster head is selected using the enhance simplified HEED protocol based on the nodes' remaining energy. The application of Es-HEED protocol to the UAV-MBN network is choosing the energy nodes, which are lower rather than selecting the higher. The Es-HEED has a possibility of handling big data for large-scale applications in the quantum network. The proposed work is able to send efficient group key and can handle wireless networks. The existing algorithms such as GKM, CB-GKM, and HG-RMS have less competency of managing group key and control when compared with the proposed method. The steps processed in simplified enhanced HEED protocol are as follows.

Steps in Simplified Enhanced-HEED Protocol

Step 1: $X \leftarrow \{n : n \text{ defines cluster head}\} \neq \emptyset$.
Step 2: $GC \leftarrow \text{Lowest}_{\text{cost}}(X)$.
Step 3: If $(GC = \text{Node}_{ID})$.
Step 4: $GC_{\text{prob}} \leftarrow \text{maximum}\left(G_{\text{prob}} \times \frac{V_{\text{residual}}}{V_{\text{max}}}, d_{\text{min}}\right)$.

Step 5: If (GC_{prob} == 1).

Step 6: If (is − final − GC) ← True

Cluster − $head_{msg}$(Node − ID, final − GC, cost).

Else

Cluster − $head_{msg}$(Node − ID, tentative − GC, cost).

Step 7: Else if (CH_{prob} == 1) && (is − final − CH) ← True

Cluster − $head_{msg}$(Node − ID, final − GC, cost).

Step 8: Else if (Rand(0,1) ≤ GC_{prob})

Cluster − $head_{msg}$(Node − ID, tentative − GC, cost).

Step 9: $GC_{prev} \leftarrow GC_{prob}$.

Step 10: $Repeat_{Until} GC_{prev} = 1$.

The simplified HEED protocol is used for the clustering process in which rotation of nodes is regular as a group-controller. Each nodes' remaining energy is used for designation of the group-controller in simplified HEED. Higher probabilities will be consisted for the nodes that are having more remaining energy that is to choose as group-controller. The intra-group communication cost is the secondary clustering-factor present in simplified HEED when extra node within the group is present that claims to be group-controller. Moreover, the controller is joined by the controller-node, which is a non-group member having maximum communication cost. Two parameters are considered for performing the group formation and these are as follows:

(1) Residual energy of nodes
(2) Communication cost of intra-grouping

An energy efficient routing is provided by the multi-hop grouping algorithm of WSN named as simplified HEED. The percentage of GC in the simplified HEED among the nodes is known to be Gprob, which is a fixed and cannot be calculated apriority. Figure 2 shows the framework of the proposed work.

The probability of elected GC node is estimated as given in Equation (2)

$$GC_{prob} = \frac{GC_{prob} * V_{residual}}{V_{max}}. \tag{2}$$

Here, the current nodes computed energy is denoted as $V_{residual}$, and the maximum energy is defined as V_{max}. The threshold value of d_{min} should be always lower than the GC_{prob} value. Equation (3) is used for computing the threshold value.

$$d_{min} = \left(\frac{\text{Round} - \text{Duration}}{\text{No.of } GM \times \text{slot_size}}\right) * \text{avg of min and max of GM to that of GC.} \tag{3}$$

The time period for each round is consumed, which is denoted as round duration. The node deaths probability will be more when the d_{min} value is lesser. Threshold value that is selected is inversely proportional to V_{max}. Numerous iterations are processed by each node until the selection of the GC. The node itself is assigned to be GC when nothing is selected and messages are forwarded to the neighbor nodes. The potential period is taken for the non–group-controller node after the grouping and waits for countdown for the next transmission of data round. Two various statuses are broadcasted from sensor node to its neighbors: (1) Indefinite Status and (2) Last Status.

//Indefinite Status

$$\text{if } GC_{prob} < 1.$$

The status is changed as regular node when it becomes indefinite GC.

//Last Status

$$\text{if } GC_{prob} = 1.$$

Permanently, the node becomes GC002E.

Group Key Generation based on HEA:

The group-key-req is sent by the group-controller to the KMC. It is composed of group and individual key, then the secure-key is forwarded to the corresponding group-controller. The HEA is used to generate the keys.

Key Generation Steps using HEA:

//Encryption

Step 1: Initialize HEnc(K, N).

Step 2: $S \leftarrow \theta$ encode(N).

Step 3: $Q \leftarrow \theta \{0,1\}^k$.

Step 4: $S^1 \leftarrow H(R, K)$.

Step 5: $GC \leftarrow S^1 \oplus S$.

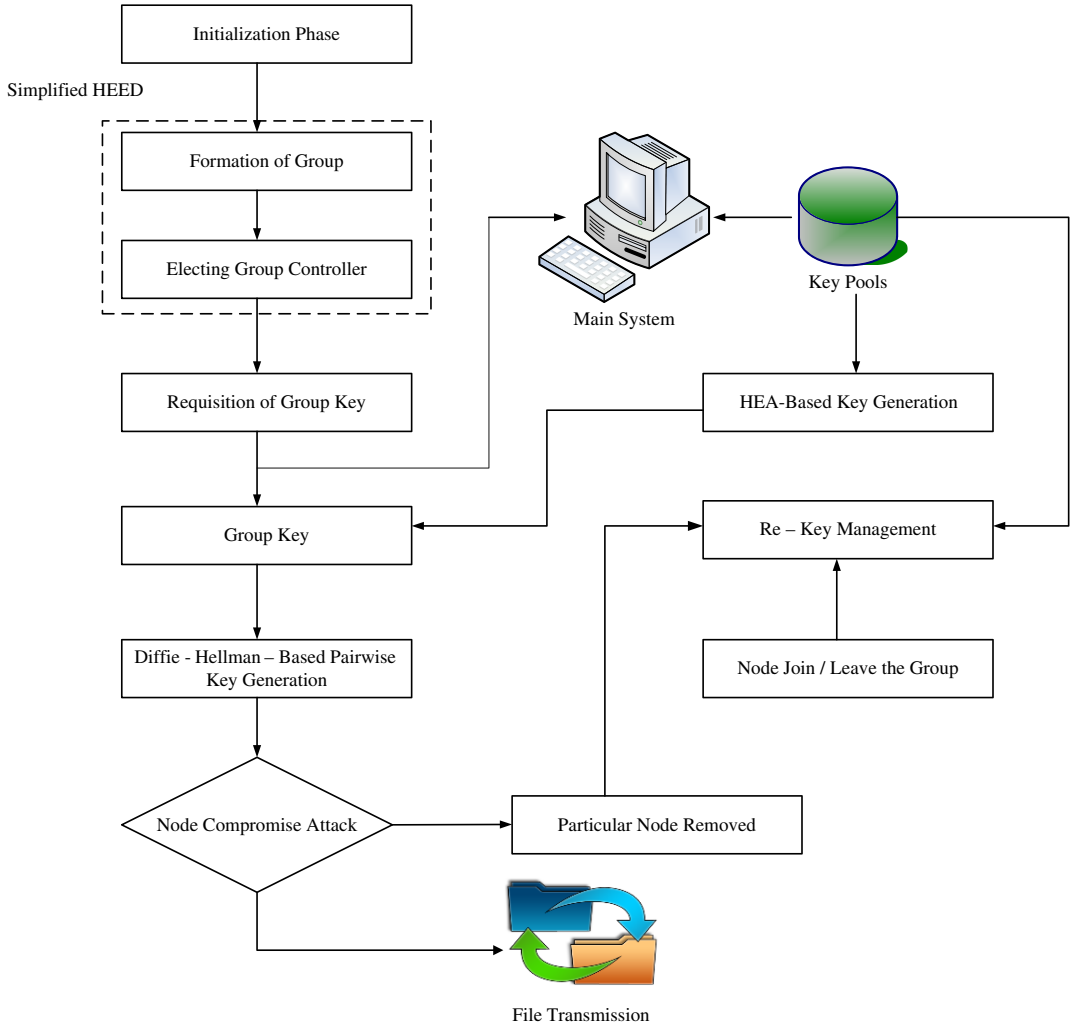


FIGURE 2 Framework of hybrid GKM scheme

Step 6: Return (*R*, *GC*).

//Decryption

Step 1: Initialize HDnc(*K*, (*R*, *GC*)).
Step 2: $S^1 \leftarrow H(R,K)$.
Step 3: $S \leftarrow GC \oplus S^1$.
Step 4: $N \leftarrow$ decode (*S*).
Step 5: Return (*N*).

The keys are generated based on the steps provided by the HEA and it is sent to the group-controllers. Keys are distributed by the group-controllers for the particular group-members. The exchanging and validation of keys are done by using Diffie-Hellman algorithm in the proposed scheme. It automatically checks for the authentication of two participated nodes. The re-keying process uses three main segments of information and these are as follows. (1) A personal secret K_n will be handled by each sensor node. (2) The GC should not use and reveal the re-keying information for estimating the broadcast message. (3) The new group key is calculated by GC by using K_n and broadcast message. A new key is generated when adding a new-member or deleting the existing-member from the group for the prevention of future communication and securing the past-communication.

4 | SIMULATION RESULTS

This segment analyzes the performance and comparison of the proposed scheme with the existing approaches. The parameters for simulation used for the proposed method are shown in Table 1.

Framework	Values
Number_of_Nodes	10,20,30, … ,200
Time for simulation	180 seconds
Area	100 x 100 meters
Packet_Size	512 bytes
Packet_Rate	8 packets/s
Maximum_Number_of_Connections	10,20,30,40,50
Bandwidth	20 Mbps
Delay	10 ms

TABLE 1 Framework used for the proposed model

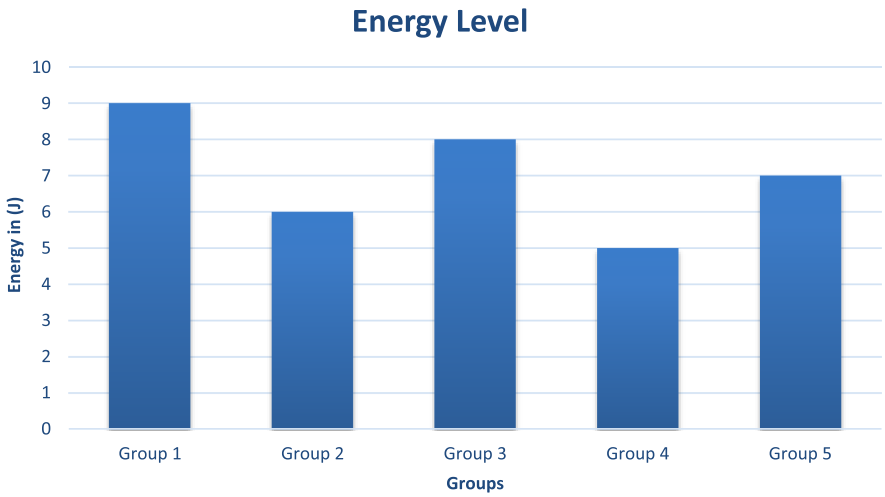


FIGURE 3 Utilization of energy in groups for HGMK-RMS

The performance metrics used for the simulation testing are as follows:

- Energy-consumption
- Privacy-level analysis
- Key-accuracy level
- Memory-consumption analysis
- Time-analysis

Energy-Consumption:

Figure 3 shows the utilization of energy for different groups. The residual energy is exploited as the major constraint, which is used to elect the group-controller. The proposed hybrid GKM model with re-keying process for the UAV-MBN system using simplified HEED protocol is used for the group-formation and group-controller election, which helps in reducing the energy consumption. The energy of each group is divided as shown in Figure 3.

Privacy-Level Analysis:

The group key is shared securely by the proposed scheme to the respective group-members through the group-controller when the node is joining or leaving the group. Based on the performance analysis, the proposed scheme gives better security level when compared with other existing approaches. The privacy-level analysis is shown in Figure 4.

Key-Accuracy Level:

The key-accuracy level of the proposed system and the comparison with the existing approaches are shown in Figure 5. The proposed HGKM-RMS uses the Diffie-Hellman protocol for key exchanging between the nodes. The performance of accuracy-level is higher for the proposed method when compared with other works.

Memory-Consumption:

The memory-consumption for the proposed method is compared with the previous works, shown in Figure 6.

Each cluster is elected with cluster-head (CH) using the proposed approach HGKM with re-keying; the information is not maintained by the cluster members about the various nodes present in the cluster. The information is obtained by simply contacting the CH. Therefore, the proposed method consumes the memory in a less amount when compared with existing CB-GKM and HG-RMS.

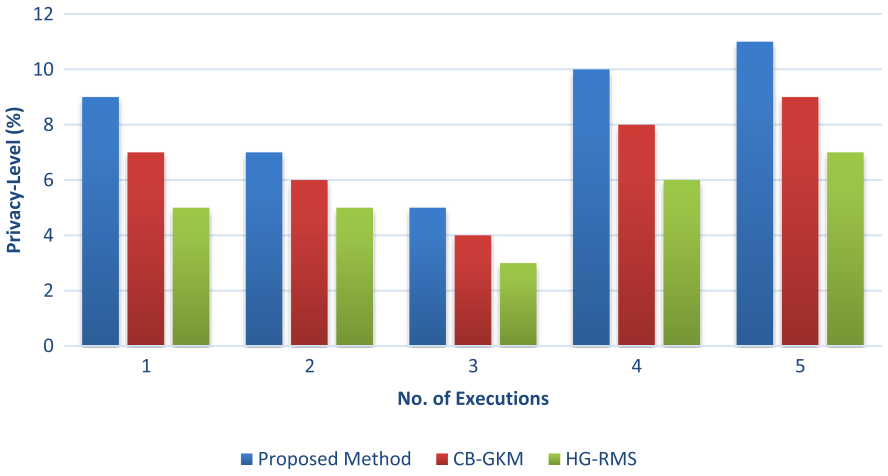


FIGURE 4 Privacy-level analysis using proposed method vs existing approaches

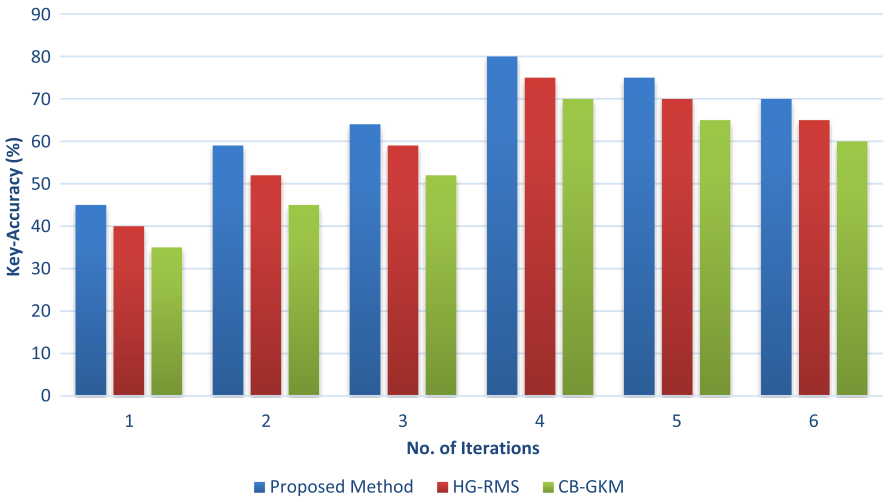


FIGURE 5 Key-accuracy analysis

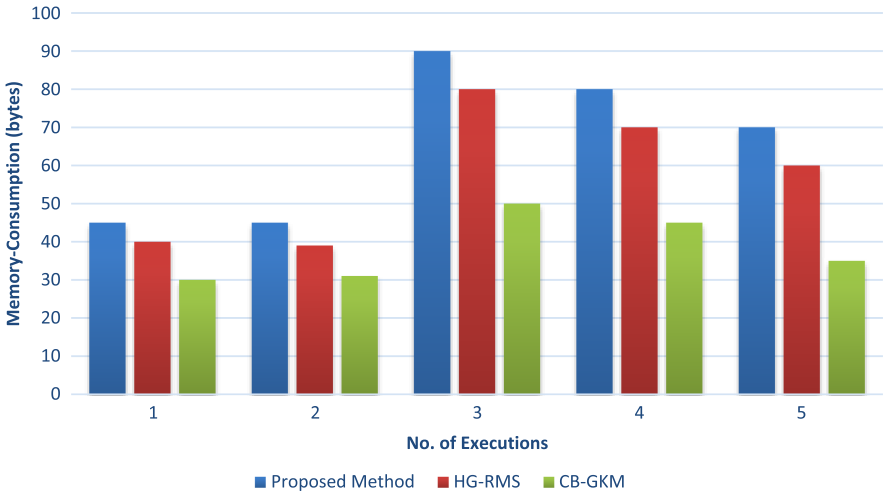


FIGURE 6 Memory-consumption analysis

Time-Analysis:

The average time-consumption of the proposed method is compared with HG-RMS and CB-GKM, which is shown in Figure 7. The CH is elected by the proposed HGKM with re-keying approach for the maintenance of information regarding all the clusters. The CH is contacted directly by the node when it is needed to access the information. The time-consumption is reduced when preventing the information search from the neighboring nodes and the performance is better than the other existing approaches. The proposed method obtained a time analysis of 88 ms when compared to other existing techniques in which HG-RMS obtained 40 ms to 70 ms for six executions and CB-GKM obtains 35 ms for first execution and 55 ms for six executions.

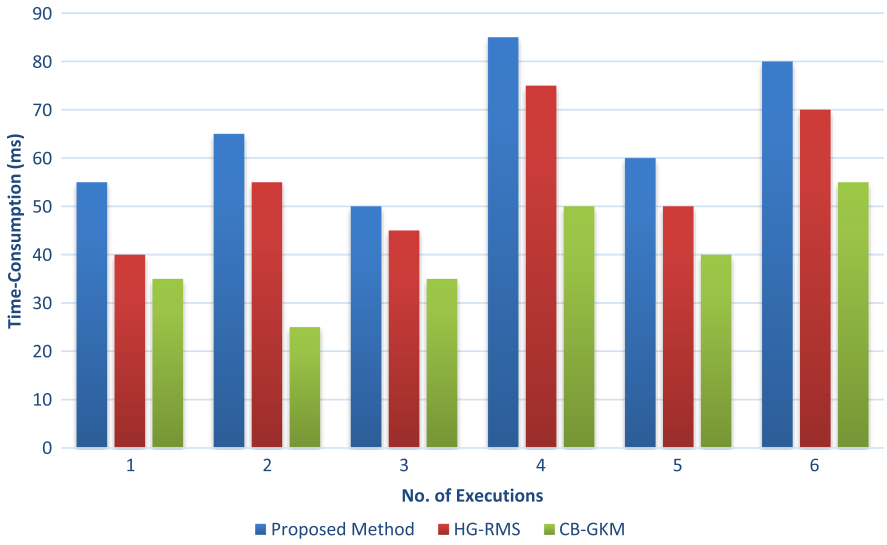


FIGURE 7 Time-analysis

5 | CONCLUSION

In this research work, we proposed a hybrid GKM with re-keying process for assigning a secure communication in the UAV-MBN network. Initially, each group is elected with a group-controller (GC), which helps in managing the group-members. The simplified HEED protocol is used to elect the GC and the keys are generated using honey encryption algorithm (HEA). The performance of the proposed HGKM with re-keying process gives better results when compared with CB-GKM and HG-RMS based on the metrics such as privacy-level, energy consumption for multiple groups, time-analysis, key-accuracy, and memory-consumption. The simulation results show that the proposed model obtains the optimal result for the given metrics than the previous works. Furthermore, future work includes in finding different attacks for the node compromise and minimization of memory-consumption could be improved.

ORCID

Mahaveerakannan R https://orcid.org/0000-0003-4458-0783

REFERENCES

1. Barskar R, Chawla M. A survey on efficient group key management schemes in wireless networks. *Indian J Sci Technol*. 2016;9(14).
2. Karuturi NN, Gopalakrishnan R, Srinivasan R, Rangan CP. Foundations of group key management-framework, security model and a generic construction. *IACR Cryptol EPrint Arch*. 2008;2008:295.
3. Kumari VV, NagaRaju DV, Soumya K, Raju KVSVN. Secure group key distribution using hybrid cryptosystem. Paper presented at: 2010 Second International Conference on Machine Learning and Computing; 2010; Bangalore, India.
4. Wang Z, Du X, Sun Y. Group key management scheme based on proxy re-cryptography for near-space network. Paper presented at: 2011 International Conference on Network Computing and Information Security; 2011; Guilin, China.
5. Zhang X, Wang J. An efficient key management scheme in hierarchical wireless sensor networks. Paper presented at: 2015 International Conference on Computing, Communication and Security (ICCCS); 2015; Pamplemousses, Mauritius.
6. Chu-yuan W. A hybrid group key management architecture for heterogeneous MANET. Paper presented at: 2010 Second International Conference on Networks Security, Wireless Communications and Trusted Computing; 2010; Wuhan, China.
7. Sahban S, Manu MR, Mon FA, Suthendran K. Group communication management in UAV-MBN networks. *Int J Pure Appl Math*. 2018;118(7):349-355.
8. Velumadhava Rao R, Selvamani K, Kanimozhi S, Kannan A. Hierarchical group key management for secure data sharing in a cloud-based environment. *Concurrency Computat Pract Exper*. 2019:e4866.
9. Sumathy S, Kumar BU. Secure key exchange and encryption mechanism for group communication in wireless ad hoc networks. 2010. arXiv preprint arXiv:1003.3564.
10. Bawa H, Singh P, Kumar R. An efficient novel key management scheme for enhancing user authentication in a WSN. *Int J Comput Netw Inf Secur*. 2013;5(1):56.
11. Yao W, Han S, Li X. LKH++ based group key management scheme for wireless sensor network. *Wirel Pers Commun*. 2015;83(4):3057-3073.
12. Jiang R, Luo J, Wang X. HRKT: a hierarchical route key tree based group key management for wireless sensor networks. *KSII Trans Internet Inf Syst*. 2013;7(8).
13. Murugan NS, Devi GU. Detecting streaming of Twitter spam using hybrid method. *Wirel Pers Commun*. 2018;103(2):1353-1374.
14. Murugan NS, Devi GU. Feature extraction using LR-PCA hybridization on Twitter data and classification accuracy using machine learning algorithms. *Cluster Computing*. 2018:1-10.
15. Murugan NS, Devi GU. Classifying streaming of Twitter data based on sentiment analysis using hybridization. *Neural Comput Appl*. 2018;31(5):1425-1433.

16. Zhao P, Xu Y, Nan M. A hybrid key management scheme based on clustered wireless sensor networks. *Wirel Sens Netw*. 2012;4(08):197.
17. Doraipandian M, Rajapackiyam E, Neelamegam P, Rai AK. An efficient and hybrid key management scheme for three tier wireless sensor networks using LU matrix. In: *Advances in Computing and Communications: First International Conference, ACC 2011, Kochi, India, July 22-24, 2011, Proceedings, Part III*. Berlin, Germany: Springer; 2011:111-121.
18. Raja K, Pushpa S. Novelty-driven recommendation by using integrated matrix factorization and temporal-aware clustering optimization. *Int J Commun Syst*. 2018.
19. Geetha R, Kannan E. A hybrid key management approach for secure communication in wireless sensor networks. *Indian J Sci Technol*. 2015;8(5):1-8.
20. Prakash AJ, Uthariaraj VR, Elizabeth BL. Efficient key management protocol with predictive rekeying for dynamic networks. Paper presented at: 2016 2nd International Conference on Green High Performance Computing (ICGHPC); 2016; Nagercoil, India.
21. Rajamanickam V, Veerappan D. Inter cluster communication and rekeying technique for multicast security in mobile ad hoc networks. *IET Inf Secur*. 2014;8(4):234-239.
22. Kong J, Luo H, Xu K, Gu DL, Gerla M, Lu S. Adaptive security for multilevel ad hoc networks. *Wirel Commun Mob Comput*. 2002;2(5):533-547.
23. Orfanus D, de Freitas EP, Eliassen F. Self-organization as a supporting paradigm for military UAV relay networks. *IEEE Commun Lett*. 2016;20(4):804-807.
24. Rhee KH, Park YH, Tsudik G. An architecture for key management in hierarchical mobile ad-hoc networks. *J Commun Netw*. 2004;6(2):156-162.

How to cite this article: R M, C SGD. Big data analytics for large-scale UAV-MBN in quantum networks using efficient hybrid GKM. *Concurrency Computat Pract Exper*. 2019;e5559. https://doi.org/10.1002/cpe.5559