Multicast Communication using Different Group Key Managements

Ranjan Kumar H S, Ganesh Aithal, Surendra Shetty

Abstract: The most appropriate communication mechanism for transfer of packets from one source to another is multicast IPv6 communication. Nowadays, multicast communication plays a major role in a large number of communication applications. In this multicast communication, the message privacy attains a highest position. The members of multicast are dynamic so they permit the host members to enter and depart the cluster without the permission of remaining group members and, it can't provide any transfer without the interference of host, this may reduce the performance. For security enhancement in multicast communication Group Key Management (GKM) was introduced. There are three different approaches in GKM and they were mainly involved to overcome the issues of host mobility in multicast communication. The challenges that are encountered by these GKM approaches their requirements and challenges was also discussed in this paper. Finally, some questions and their explanations were provided along with it. These GKM approaches will improve the privacy of multicast communication. So, the packets can deliver to the group members without any interference.

Index Terms*: *Multicast IPv6 communication, Security, GKM, Centralized, Decentralized, Distributed.

I. INTRODUCTION

The most important building block for secure group communication (SGC) system is GKM [1]. The rapid fluctuations that occurred in cluster membership was largely tolerated by this SGC method. In this communication field, the members are allowed to leave or join on their own will, also they can access the basic transmission structure (i.e., the multicast communication can be provided and revoked with less system overhead) [35, 37]. The confidentiality over the communication was ensured by GKM. It was achieved by creating a secret share key between the cluster members. Such secret key was referred as "traffic encryption key" (TEK) which was used for message encryption or decryption process [33]. The most important challenge is key generation and re-keying process without enhancing the communication overhead and storage [1, 34]. Recently, number of updated methods were developed for key generation and secure information sharing among various and within similar groups [1, 38]. A large quantity of network applications depends on client–server paradigm, but they include unicast for packet delivery. But, enormous upcoming applications depend on the group communication method. Normally, communication sector needs to transfer packet from a number of authorized transmitters to a large amount of permitted receivers [2]. The GKM performance was largely affected by resource constraints, largely spread mobile devices, and bandwidth limitation [23].

Due to, the rapid improvement in the field of technology and internet may affect the growth of both internet and mobile users. In order to compete with this growth an advanced IPv6 (Internet Protocol version 6) was introduced. The multicast communication was successfully developed in internet for best and efficient service delivery for large groups [9]. The performance of multicast communication in both the media or content suppliers/distributors and Internet Service Providers (ISPs) have gained a large popularity. The multicast communication in IPv6 perform efficiently for delivering services for group-oriented applications like video conferencing, video-on-demand (VoD), communicative group games, etc. from internet to various members [3, 10, 29]. The methods of key management concentrates in cryptographic key generation, maintenance and distribution [39].

The major role of multicast communication is to deliver a message from a single transmitter to a cluster of members. The task performed by both the group communication and group creation was found to be similar in the internet field. It performs more effectively than a unicast method. For each group, a leader was necessary for managing the group activities. But in various multicast communication systems, a key server (KS) or group centre (GC) plays a major role in group member interaction and management [4].

The important challenge for the designing process of Smart Grid (SG) was high level security. For secure communication, the message encryption and decryption was generally performed by the cryptographic keys. The key establishment among two parties includes various solutions, and these solutions were include as a section in the authentication process. The most popular solution for session key formation is Diffie-Hellman (D-H) algorithm [5].

Revised Manuscript Received on 30 July 2019.
***** Correspondence Author

Ranjan Kumar H S*, Department of Computer Science, NMAM Institute of Technology, Karnataka, India.

Dr. Ganesh Aithal, Dean (Research), Mangalore Institute of Technology and Engineering, Moodbidri, Karnataka, India.

Dr. Surendra Shetty, Professor and Head, NMAM Institute of Technology, Karnataka, India.

Retrieval Number B2701078219/19©BEIESP
DOI: 10.35940/ijrte.B2701.078219
Journal Website: www.ijrte.org

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

The scheme of key management also provide its service in health care system by providing facilities for sensor removal and addition from the Body area network (BANs), it also renew the group key if necessary [6]. The existing protocols of group key agreement (GKA) widely depends on the map-to-point hash computations and expensive bilinear pairing. But these schemes were not involved in the e-health application. The group session was safeguard by developing a secure scheme for GKM [12].

The securing scheme in group communication means providing authenticity, integrity, and confidentiality for the messages that are exchanged between the groups. It also avoid the interference of third party across the data path of multicast communication [7]. The most powerful element for the networking technologies of upcoming generation was IoT (Internet of Things).

Thus, the multicast communication provide efficient service by sending the multicast messages to a large number of receivers. But the unicast may consume large amount of energy for sending single packet to single receiver [8]. If the client needs to join the group, the authentication protocol provide a mutual authentication among both the server and client. After authentication, several member of the group has to share a key to the server which was normally designated as a member's individual key. In order to perform a group communication, the server needs to group key which was utilized by the entire members of the group. The high rate of security was provided by this newly developed group key [9]. The group key in symmetric was commonly referred as TEK, it was generally introduced in multicast communication to provide an access for control mechanism. This key was shared only the authorized members of the group. The new TEK was delivered by key server to the members of the existing group during the process of rekeying for old TEK invalidation [10, 34]. The GKM was mainly divided into three types they are decentralized, distributed, and centralized. Among these three, Centralized GKM includes existing algorithm of Group Diffie-Hellman key distribution or Diffie-Hellman (D-H) for cluster key generation [11, 40].

The outline for this overall review is as follows: the important objective of this entire review is described in Section.2. Some additional information about multicast IP was provided in Section.3 and the in Section.4 the details about GKM and its classes was included. The challenges of three classes and some methods that are involved in multicast communication was also reviewed in this section. Additional requirements like security, efficiency and service quality of GKM was reviewed in Section. 5, the challenges that are encountered by multicast communication was provided in Section. 6. The summary for this GKM approach was reviewed in Section. 7. Finally, some review queries and answers were provided in Section. 8 and the conclusion for this entire review was presented in Section. 9.

II. OVERVIEW OF MULTICAST IP

The huge amount of existing internet users and the emerging users obtain large support from IPv6. This IPv6 was introduced to provide an enormous address space. It contains wide advantage but some security defects were also identified in this IPv6 protocol. The biggest challenge of IPv6 is security for multicast communication. The confidentiality, data integrity, and authenticity are the main roles of security. This vision was achieved by proposing various protocols for key management and this proposed protocols provide huge support for data encryption by distributing, updating and generating the key. The defects of high bandwidth usage in unicast communication was entirely overcome by this multicast communication. In wireless networks, multicast plays a major role in various applications like lectures in school by e-learning, location-based military programs, video-conferencing, and distance learning [13]. In the multicast communication field, the common group key was used by symmetric algorithm for encrypting the actual process of data transfer. The computation of symmetric algorithm was found to be lighter so it was widely used in the IoT applications [32].

IP multicast performs the implementation process of point-to-multipoint communication. It was performed on the network infrastructure that were based on IP. The leave and join messages were provided by the destination nodes (i.e., to unsubscribe or subscribe from the data flow). The infrastructure of network was effectively used by IP multicast by sending the packets from source only once even if it includes numerous receivers. The packets were simply duplicated by network routers and provide it to various nodes. Most widely used communication in WSN was multicast IPv6 because it minimize the radio transmission and memory usage by increasing the energy efficiency. The multicast communication in Low power Multicast Protocol and Lossy Networks (MPL) was provided by the measured network-wide flooding which was normally directed by Trickle timers. Basically this governance was performed for providing a packet transmission for both data-plane and control packets [14, 15].

The energy usage and bandwidth was improved by the Multicast forwarding method in various applications. So this multicast method was widely demanded by this Low power and Lossy Networks (LLNs) because energy and bandwidth were found as a major critical factors in this LLN [15]. The bandwidth and scalability advantage of multicast provide accurate solution for traffic reduction in mobile network and also allow the users to share the limited volume and frequency bands [16]. In WSN, the important aspect of multicast communication is to increase the efficiency of communication and minimize the communication overhead. The entire IP communication was achieved by connecting the WSN with IPv6 network. It was performed due to the increasing demand of new WSN applications. This issue was mainly addressed by low-power Wireless Personal Area Network over IPv6 (6LoWPAN). In 6LoWPAN, the multicast communication was performed effectively in the absence of information regarding the node's location [17, 30]. Based on CRT (Chinese remainder theorem), the centralized GKM scheme distribute and update the GK of group members with reduced complexity in computation.

The minimum amount of computational complexity was obtained by CRT-based GK management (CRTGKM) algorithm but it slightly increase the KS storage space [4]. The IPv6 protocol was employed by the advanced metering infrastructure (AMI) [50] in a mesh-based topology. As this topology can easily expand the coverage area of network by performing multicast communication [5].

III. GKM FOR SECURE MULTICAST COMMUNICATION

The application of multicast is mandatory in the IoT field as its application was widely used by numerous healthcare, environmental monitoring, smart cities, and smart homes [8, 42]. In secure-key management, a common method was involved to maximize the capacity of transmitted packets encryption or decryption. In a highly dense network, frequent member leave or join operation may cause some problems in the encryption and decryption process of entire network [9]. The main objective of GKM is to maintain and set up the shared secret key between the entire group members [37].

When the alteration occurs in group membership, the high security was achieved by generating a new key and this key was provided to the entire members of the group. The backward security was emerged during the member 'join' process to prevent the new members from the incoming past data. Similarly, during member 'leave' the forward security was generated and forward to all the group members to stop the data access by the left member [9]. Multicast was identified as a bandwidth efficient method over the internet to deliver group-oriented applications [25]. The multicast and broadcast services were efficiently provided within the cell and core network by multimedia broadcast/multicast service (MBMS). The security attacks that are recorded in the broadcasted multicast services are Denial of service (DoS), eavesdropping opportunities, impersonation attacks, physical node capture attacks and others. These security attacks were happen in wireless networks due to open access [10].

The bandwidth efficiency and network performance obtained by this multicast was found to be better than the unicast transmission. So this multicast was widely implemented in IP (Internet Protocol). The entire group members were validated by transferring the data packets along with encrypted messages whereas the cryptographic key performs the message encryption. This common key was often referred in different names like group key (GK), session key or Traffic Encryption Key (TEK). A large number of methods were introduced in this multicast area to solve the problems that are obtained during key distribution. The quantum key distribution (QKD) was introduced by Bennett and Brassard to reduce the key management problems. The unrestricted security property was provided by QKD to protect the privacy and confidentiality of cryptosystem [11, 26].

The important goal of this review is to provide clear explanation for GKM architecture and classes. GKM was widely categorized into three types they are, Decentralized GKM, Distributed GKM, and Centralized GKM protocol. Here, the details regarding the GKM classes were reviewed thoroughly.

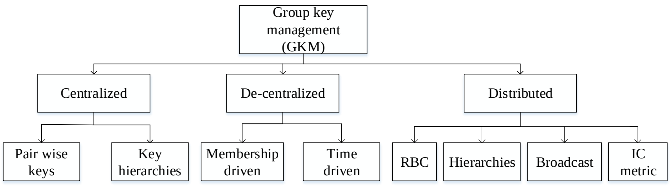

Figure 1: Group Key Management and its classes

In this, the review was performed in GKM and its classes were described properly along with its methods.

A. Centralized Group Key Management

Centralized approach makes the group member flexible by receiving the group communication from various groups, due to this it encounters huge scalability problem in wireless networks. The message required for key update get increased due to the unconditional increase in dispersed group members. A single key server was developed along with multitude request to avoid this additional message requirement from the entire group members. This single key server reduce the failure rate of GKM operation. In the meantime, the position of group member need to be tracked by introducing a base station as third party in cellular networks. In the entire wireless network domain, the keying material gets updated due to the group member movement [23]. Recently, various Centralized GKM approach introduce traditional algorithm of Group D-H key distribution or D-H for cluster key generation. This centralized approach encounters serious problems due to high communication and computation cost. This cost increase was due to the performance of some exponentiation operations like transmitting messages confidentiality and authentication between the multicast group members' and centralized server [11]. Some of the challenges that are encountered by this centralized GKM are lack of scalability, operational inefficiency, and Inability to support multiple membership change.

a) Lack of scalability: Wireless networks makes the group member flexible by receiving the group communication from various groups, due to this it encounters huge scalability problem in wireless networks. The dispersed members in wireless network get increased this significantly increases the amount of rekeying messages. In the highly dynamic group application, the capacity of single key server was widely overwhelmed by frequent rekeying in order to trigger the failure rate of GKM operation.

b) Operational inefficiency: The group members in the cellular network was dynamic, so the third party (BS) is necessary to track the member location. Due to this, the multicast messages enforces the rekeying messages into the entire wireless network.

c) Incompetence to support the multiple membership change: In centralized scheme, the structure of key management was found to be specific for multicast session. In each multicast session, a separate key tree was developed by this particular nature.

When the particular member was enforced to join in multiple session, this structure register the entire key management trees with this newly entered group members. For this, the member needs to store and handle large amount of keys. The group members and key trees get affected due the wide membership changes. This changes in wireless network also generates a huge rekeying messages [18].

There are three phases in the framework of Greatest Common Divisor (GCD) based centralized approach. The initial phase is Group Centre Initialization phase, in this multiple groups were developed at group centre. The Member Initial Join is the second phase in this approach, where the join request was send to the group centre by the member and receives the participation keys via secure channel. The "Member Leave" is the final phase, this phase handles the entire operations that are performed after the group member leaving process (providing forward secrecy). The computation time during this forward secrecy was found to be large so this framework highly focuses on this phase (i.e., Member Leave phase). The cost for this computation process was found as a major challenge in the multimedia based multicast communication [19, 36, and 37]. The two classification of this centralized GKM are pairwise keys and key hierarchies.

Pairwise keys

The separate secret key was shared by GKM for key material management among each group member. A secure channel was set up by this secret key among GKM and each group members. This channel establishment was to deliver a new TEK in a secure form during the changes that occur within the group membership. The multicast message was necessary to maintain the backward secrecy, whereas $O(n)$ rekeying message was assured in forward secrecy. Here 'n' represents the total number of cluster members. So, this solution was found to be not applicable for dynamic and large groups [20, 42]. The fusion of signalling load and rekeying messages between the core network and members introduce the communication overhead. The multicast and unicast messages were included in the rekeying transmission messages [43].

A separate secret key was distributed by the group initiator (Group Controller (GC)) to each member of the group. This corresponding key may generate a unicast secure channel among each member and GC. This key was referred as Key Encryption Key (KEK) by Wallner as it perform encryption process in multicast data. It was also designated as Traffic Encryption Key (TEK). A new TEK was generated by GC during member leave phase and send this generated key to each member through a secure channel [21].

Let us assume, the multicast group with 4 members and they were represented as m_1, m_2, m_3, m_4. In the initial phase, the private key was distributed by GC to each group members K_1, K_2, K_3, K_4 correspondingly. The TEK along with encrypted private key {TEK} Ki was provided to each group members. In the second step, the TEK gets updated after member leave phase and the generated TEK was transmitted to the entire group members. The transmitted messages that are required for rekeying changes from 'n' to (n−1) [21].

The GKM Protocol (GKMP) [35], in RFC 2094 and 2093. The Group Key Packet (GKP) was generated by the key server (KS) along with this GKMP. This generated GKP contains two keys they are Group KEK (GKEK) and Group TEK (GTEK). The new GKP distribution was secured by GKEK and the data traffic was encrypted by GTEK whenever required.

In this, the KS was supported by the initial member to join the group for GKP generation with GTEK and GKEK. A new GKP with novel GTEK for backward secrecy was generated by key server during the member joining phase. The generated key encrypted with KEK was then transfer safely to newly joined member and also transfer this key encrypted with old GTEK to the other cluster members. Finally, the GKP was refreshed periodically by the key server and GKEK distribute it to the other group members.

During the member leave phase, a new GKP was generated by key server and transfer it to the remaining members encrypted with shared KEK. In order to perform this, each leave phase of this GKMP requires re-key messages. Due to this reason, this solution was not scaled with the highly dynamic members of large group [21, 34, and 42].

Key hierarchies

The most popular method in this centralized GKM was logical key hierarchy (LKH) which is introduced by various study teams during the same time interval. The LKH tree was maintained by key server and this key tree includes user nodes and key nodes. The TEK key was involved in the root of the key tree. The individual keys were considered as leaves that are associated with each group members. The key server introduce KEK key also called as intermediate key to deliver the TEK securely to each group member. For this, each member should hold the key along their pathway to the root starting from leaf. For instance, an individual key {KEK1, KEK12, KEK1234, TEK} is included in member 1 [44, 48].

The messages required for update process was reduced by KEK, particularly when the member leave from the group. The alteration in group membership may reduce the key material update messages for this the entire method was scaled into the groups having large size. The failure at particular point was represented by single KS dependency to attain the bottleneck performance. Therefore, the rekeying message number is converted from $O(n)$ to $O(\log(n))$. At GC, the storage and computation cost were introduced by LKH. The required rekeying messages were further reduced by the One-way Key Derivation (OKD) method by performing local group key computation using the function of one-way hash. So, a new key was transfer by GC to the novel group member and then the total rekeying messages were compressed into a single message. This LKH is sub-divided into two driven rekeying categories they are user and server driven rekeying,

i. Server driven rekeying: The KS update the keying material along with KEK and TEK during the member leave and join phase, then it transmit the key to the remaining group members. One fine example for this method is, when the new member User7 enters the group, the multicast message generates the new key set {KEK7, KEK567, new TEK} and transmit the new TEK along with encrypted TEK to each group members. The communication overhead that maintain the backward secrecy was represented as, $\log_2 n+1$ and the messages that are required to provide forward secrecy is represented as, $2\log_2 n$,

ii. and 'n' represent the cluster members number.

iii. User driven rekeying: The KEK calculation was transferred by SKD, OFT, and ELK without including the key server to the group members. The required amount of ancestor KEKs (the entire KEKs throughout the route to reach the root from leaf) was calculated by each member by applying the key derivation function with respect to the pseudo random objectives. The important benefit of this process is to minimize the rekey message number from 2log2 n to log2 n [20].

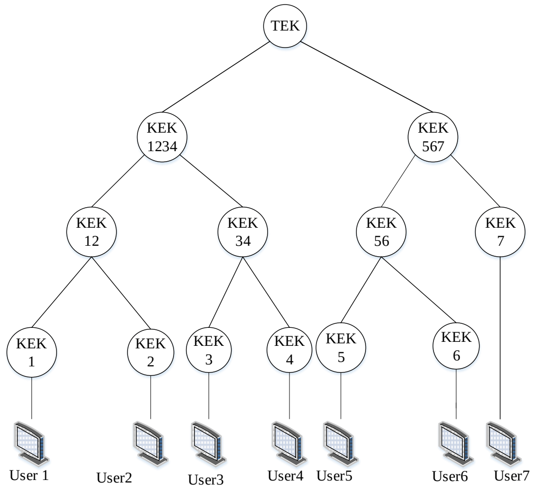

Figure 2: Logical Key Hierarchy

The LKH rekeying process was further secured by the Secure and Scalable Rekeying Protocol (S^2RP) method. The rekeying messages were validated to improve the security with a key-chain and a one-way-hash function. Its performance was found to be same as that of LKH. The main advantage is that it improves the efficiency of key authentication along with key distribution. When performing the key chain mechanism, only a hash function was required for key authentication, which makes the authentication process more efficient for computation purpose.

Table 2: Centralized GKM methods for multicast communication

Class	Method	Contribution
Centralized GKM	GKMP [21]	The Group Key Packet (GKP) was generated by the key server (KS) along with this GKMP. This generated GKP contains two keys they are Group KEK (GKEK) and Group TEK (GTEK). The new GKP distribution was secured by GKEK and the data traffic was encrypted by GTEK whenever required.
	LKH [20]	This method can be scaled to larger group size as the message count required for key material update was reduced on any group membership changes.
	S2RP [22]	It improves the efficiency of key authentication along with key distribution.
	LKH++ [23]	This method minimize the amount of multicast messages that are transmitted from the centre. The symmetric cryptography key was also applied by this scheme to reduce the length of computational effort and encryption key length that are essential for user device to perform message encryption and decryption, so that the battery can be saved.

Another improvement of this LKH method was Topological Key Hierarchy (TKH), as in rekeying message it reduce the communication cost by performing the mapping function between the logical key tree and the physical topology. The advantage of this TKH method is that it reduce the key numbers that are required to store at the GC [22].

The performance of LKH was improved by LKH++ by exploring the features of user information and one way hash function property. These two properties were already involved in LKH method. Without performing any communication between the key server and user, the LKH with shared information set locally generates the new keys. Likewise, the keys were autonomously computed by the users from a particular point then move along the pathway to the LKH root after involving the one-way function. This method was found to be more suited for the wireless mobile network as a large keys were stored by each member similar to the logarithm number of group member. It also reduces the amount of multicast messages that are transmitted from the centre. The symmetric cryptography key was also applied by this scheme to reduce the length of computational effort and encryption key length that are essential for user device to perform message encryption and decryption, so that the battery can be saved. [23].

B. Decentralized Group Key Management

In decentralized GKM each group was divided into number of subgroups in which they are placed in hierarchical levels. The constituent level key management was achieved by each hierarchical level with more than one entity, it was obtained during the dependency maintenance on the higher level entity. It was distinguished into two major categories they are the independent TEK per each subgroup, and the common TEK per all subgroups [23]. In this method, the rekeying process was performed better than the centralized approach as it transmit the key for very few travel in order to reach its destination. The members roam over the entire wireless network and obtain the group communication content from the entire network. The GKM have to integrate authentication mechanism to verify the members before receiving the keying materials that are utilized in the target subgroup.

The interference of third party was considered as a major security threat, this entity then get compromise with the protocols security property. Thus, the trust impart level to these entities was consider by this GKM scheme.

Common TEK

In the common TEK method, a single entity performs TEK generation and distribution for entire group members through the subgroup managers. Each group member should accept with the new TEK for any membership changes to achieve backward and forward secrecy. The membership change may affect the entire members of the group, so this GKM approach has high 1-affect-n phenomenon problem.

TEK per each group

The effects of 1-affect-n phenomenon was lighten by introducing another approach where each subgroup contains independent TEK. Due to this, the membership change in subgroup does not disturb the whole members of the group. The important demerit of this method is that it affects the data path by translating the data to the edge of each subgroup when they are transferred from one subgroup to another. In figure 3, a single group was divided into five separate groups with own TEK for each subgroup. The challenges that are faced by this decentralized GKM are,

a) Co-operation with the key management protocol: In existing methods, this decentralized method propose a GKM framework without considering the concept of keying material distribution to the subgroup members. In order to overcome this, the decentralized approach have to combine with some other efficient GKM methods in wireless networks to develop an integrated solution.

b) Establishing trust relationship: The wireless GKM protocol have to consider the involvement of third party entity as a serious security concern in the decentralized approach. In order to maintain a trust level, the third party should maintain a form of security association.

c) Authentication integration with GKM: Decentralized GKM includes number of groups belonging to same or diverse networks. In order to make group member flexible to receive group contents, the authentication process should verify each members before receiving the keying materials that are involved in target subgroup. For multiple moves, an efficient mechanism for group authentication should be considered by the GKM protocol [18].

Examples: Baal, DEP (Dual Encryption Protocol), SMKD, IGKMP (Intra Domain GKM Protocol), MARKS, HYDRA, KRONOS, etc., [24]. Some of these examples were discussed below,

Figure 3. Decentralized group key management

Scalable Multicast Key Distribution

SMKD method was introduced to utilize the tree that was constructed by the routing protocol of multicast, Core Based Tree (CBT). SMKD was proposed with CBT for delivering the key to the multicast groups. The encryption and authentication tasks were delegated by SMKD to downstream the CBT routers.

SMKD depends on the CBT framework, where the multicast tree was rooted in the main core along with the secondary core set. This main core apprise the session key by generating the GTEK, access control list (ACL), and GKEK. The nodes and secondary cores that are joining the group after authentication was provided with ACL, GKEK, and GTEK. The SMKD perform forward secrecy only after recreating the new group without including the departed member. This method needs some modifications in IGMP and also consider that the CBT gets deployed. In CBT, intermediate routers directly deliver the packets to the group members while transferring the packets to the Routing Protocol (RP) [31]. This SMKD method depends on the fundamental multicast RP and believes the intermediate routers that every node receives similar key same as that of the group controller.

IOLUS system

The entire group gets affected due to the changes that occur in single membership. This limitation was addressed by the IOLUS system after including the subgroups that are locally maintained. The entire multicast groups were divided into number of subgroups along with individual security keys. In this each subgroup was considered as a real group, this subgroup includes own address and keying material and it was established with appropriate multicast routing protocols.

The session key needs to be replaced after performing member leave phase in the subgroup, so each member should maintain its own session key. In this IOLUS protocol, each group members were arranged in a hierarchy manner to form a virtual group. Two types of entities were introduced in the virtual group for various subgroups maintenance and connection they are GSIs (group security intermediaries) and GSC (group security controller). Among these two entities, GSC manages the subgroups that are in the top level whereas the GSIs is also described as group security agent (GSAs), one per subgroup.

This GSI update the local multicast keys and also manages the newly created subgroup. After the member leave phase, this GSI generates new local multicast key and transmit this generated key to the remaining subgroup members. [21].

M-IOLUS system

In this M-IOLUS system (Micro-grouped IOLUS), each GSA (subgroup manager) dynamically bring the entire micro group under its control. This control action was performed for the communication overhead reduction of keying materials that gets updated for any change. The members that are belonging to the same subgroup share the same micro key and this micro key secure the entire transmitted messages. When the member decides to leave from the subgroup then it have to inform its group manager regarding its shift from the old subgroup to new subgroup. If the member movement happens within the subgroup then the subgroup key was not altered by the subgroup manager. The timestamp regarding the mobility and micro key delivery to the mobile host should be taken into account by this GSA.

In this method, the mobile members who were already entered into the subgroup was maintained by GSA. When the mobile member travels from its subgroup to another group, the GSA of the new group receives a move message from this respective mobile member.

The manager of new subgroup authenticates this new member after receiving the request from the manager of old subgroup. After authenticating the new member, the new GSA connected with multicast group provides the group key to whole group and recently arrived members receive small group key and finally, update the member table. During leave phase, the entire subgroup GSA visited by this departed member should update their keying material in order to avoid forward secrecy [20].

BALADE system

BALADE is a type of protocol in decentralized scheme which contains common TEK, it dynamically separates the entire group into a number of clusters. The local manager was included in this group to manage each member and the common key was shared by the particular group member and manager. The source performs two types of functions they are, it was considered as a group manager as it generates the TEK, it also act as a sender to the members for transmitting the multicast flow that are encrypted. The KEK (session key) is responsible for securely transfer the TEK to the cluster managers, so this KEK was commonly distributed among the group manager and source. The TEK was protected by group key and it was safely delivered to group members by group managers. Based on the application, the TEK was updated at each data semantic.

In case of member mobility from one subgroup to another, then re-authentication process needs to be perform before it enters into the multicast group. The re-authentication ticket was included in each member with password encrypted TEK, this encryption help the group manager to verify the new member easily before joining the member into the group [20].

Table 3: Decentralized methods in multicast communication network

Class	Method	Contribution
Decentralized GKM	SMKD	SMKD method was introduced to utilize the tree that was constructed by the routing protocol of multicast, Core Based Tree (CBT). SMKD was proposed with CBT for delivering the key to the multicast groups. The encryption and authentication tasks were delegated by SMKD to downstream the CBT routers.
	IOLUS	In this virtual group two types of entities were introduced for various subgroups maintenance and connection they are GSIs (group security intermediaries) and GSC (group security controller).
	M-IOLUS	In this method, the mobile members who were already entered into the subgroup was maintained by GSA. During leave phase, the entire subgroup GSA visited by this departed member should update their keying material in order to avoid forward secrecy
	BALADE	BALADE is a type of protocol in decentralized scheme which contains common TEK, it dynamically separates the entire group into a large number of subgroups. The local manager was included in this group to manage each member and the common key was shared by the particular group member and manager.

C. Distributed Group Key Management

In distributed scheme, the features of fault tolerance losses its operational efficiency due to the effects of computation overhead and communication cost. This schemes performs TEK computation by involving the asymmetric algorithm for cryptography key in specific D-H key exchange protocol. This was fond to be expensive due to the performance of multiple exponentiation process. These exponentiation increases the time required for the contributing members to reach the common TEK and its computation cost was significantly increased by this introduced asymmetric cryptography algorithm.

The group key generation was contributed by the cluster members without the influence of central KS. The workload was equally shared by the entire members of the group, so the rekeying process was found to be rapid than the other two management approaches. Some of the examples for this GKM method are Octopus, Distributed Logical Key Hierarchy (DLKH), Conference Key Hierarchy (CKA), Tree based Group D-H (TGDH), Distributed One-Way Function (DOFT), Group D-H (GDH Key exchange), and Distributed Flat Table (DFT).

The GDH method was involved for session group key. The cluster head and core members contribute to generate a TEK. The Two Round key agreement Protocol (TRP) was used for the purpose of intra-cluster communication. The inter cluster keys were used instead of global key for nearby cluster communication [24]. One of the most important challenge encountered by this Distributed GKM is,

a) Operational inefficiency: In distributed scheme, the features of fault tolerance sacrifices its operational efficiency due to the effects of computation overhead and communication cost. In this scheme, the involvement of D-H key exchange protocol increase the computational cost of TEK with respect to its exponentiation. In addition to this, it takes large time for entire collaborating members to extent the TEK. The group size increment may linearly increase the conjunction time required for key generation. [18].

Ring based

Ring based method develops the virtual ring from the group member contribution for TEK generation. The algorithm of Diffie–Hellman (DH) key exchange was used among two parties in order to agree with the common key and extend it to the entire group having 'n' members [27]. The intermediary values were calculated in a distributed manner as well as the group agrees with the pair of primes (p and α). The initial values were generated and transfer to the subsequent members by this starting group members. The cardinal value and TEK were extracted by the last member was transmit to other members for TEK extraction. The most primitive method in this category was GDH and number of studies were performed for GDH advancement. The main aspect of this approach is to treat the entire group members equally and if any one of the group member does not finish the setup, then it won't affect the entire group member performance. The key computation requires strict synchronization and it was estimated serially in multiple rounds [20].

Hierarchical based

The two party DH key exchange method was used by the group for logical hierarchy tree formation that should agree with the TEK. The results of LKH was held by group members for key number reduction. For instance, the popularly known method in this hierarchical based method is TGDH, in this each parent node receive their secret key from its one child and then obtain the blind key from another child by applying the DH key exchange protocol [28, 47]. Number of schemes have been presented in this category. The group member interaction for TEK computation does not depends on the member quantity or reduced as low as $\log_2 n$. The delay in the computation of parent key from the two children key may cause some interruption in the key agreement process, so the group member needs to be synchronized in a proper way [20]. Likewise, the leader dependence during the setup time cause some failure at single point. The cluster keys were computed by the individual key trees and generates two types of key trees. In the first stage, the group controller was considered as a root whereas the cluster heads were considered as group members. In the second stage, the group member was designated as subgroup member and the cluster head was referred as root. In hierarchical distributed GKM, the steps that are used for cluster key generation was shown below,

1) After performing the cluster formation and CH selection the two arbitrary private keys $(a, a0)$ and blinded keys $(ba, ba0)$ was send by CH to its cluster members.
2) In the meantime, individual private numbers $(PN_1, ..., PN_N)$ were generated by each member. The blinded keys were calculated by each member using Equation. 1.

$$bK_{PN} = g^{PN} \bmod P \tag{1}$$

Where P and g are limits. The cluster member's unicast the blinded keys to CH.

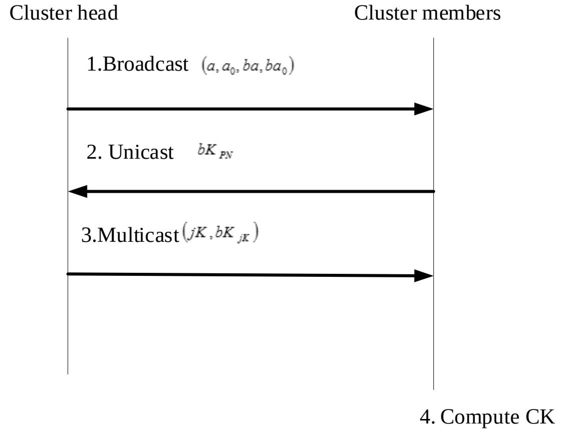

Figure 4: Timing figure for creating cluster key (CK)

3) The intermediate keys bK^{jK} and jK were computed by CH along with blinded keys and multicast these keys to all the members of the cluster, where

$$\begin{aligned} &jK_1 = bK^{a}{}_{PN1} \bmod P, ik_2 = bK^{jK1}_{PN2} \bmod P \\ &bK_{jK} = g^{jK} \end{aligned} \tag{2}$$

4) The CK was calculated by members using the following equation,

$$CK = ba_0^{jKN} \bmod P \tag{3}$$

In this way, the cluster key was generated and contributed by the cluster members. This similar process was followed by inter-cluster and intra-cluster communication for key generation. The rekeying prevent the backward and forward secrecy were by performing the membership movement [46]. The normal data transfer process begins after performing the group key distribution and cluster generation between the cluster members [24].

Table 4: Methods of GKM classes in multicast communication

Class	Method	Contribution
Distributed GKM	Ring based	The contributions of group members were developed as a virtual ring for TEK generation. The cardinal value and TEK were extracted by the last member was transmit to other members for TEK extraction.
	Hierarchical based	The popularly known method in this hierarchical based method is TGDH, in this each parent node receive their secret key from one of its child and also obtain the additional blind key from another child by applying the DH key exchange protocol.

IV. GROUP KEY MANAGEMENT REQUIREMENT

Some of the miscellaneous criteria were encountered by this GKM to achieve efficiency, scalability and security.

This miscellaneous criteria were very much useful for various solutions comparison and examination. These criterions were listed and explained briefly as follows.

A. GKM security requirement

Backward secrecy: The members that are wishing to join the cluster should not receive any past keying materials [41, 45].

Forward secrecy: The members who were leaving from the group should not receive any future messages [41, 45].

Resistant to collusion: The present TEK was not deduce and collude by some other set of fraudulent users.

B. Efficiency requirements

Communication overhead: The key material update regarding the group membership change does not induce enormous messages, particularly for dynamic group members.

Computation overhead: The process of intensive computation was not induced by the distribution and generation of traffic cryptographic key at the user and control manager levels.

Storage overhead: Minimum number of keys were stored and handled securely by the overall communication entities.

C. Requirement of Service quality

Service availability: The single entity failure in the architecture of key management should cease the process of group communication.

Scalability: This solution should have the capacity to scale the GKM scope to a largely distributed groups [45].

Reliability: It is vital for the keying material to make sure that the entire cluster members have obtained the keys in a suitable manner [23, 45].

V. CHALLENGES OF MULTICAST COMMUNICATION

This section provides some challenges that outline the direction for future investigation on multicast communication with GKM in wireless environment. They are discussed below:

A. Key manager mobility

The member mobility was tracked at the area manager level to mitigate the mobility effects. The key managers contains stable network infrastructure and this corresponding structures were made available only during the session of overall group members. The GKM design was found to be complex as the group members enter inside the network and at the same time the group managers are also assumed as a mobile entity. In this, manager mobility performs two mechanism they are, firstly it relocate the security service from previous manager to novel manager and secondly, it selects the manager for particular areas where the old group manager left out.

B. Based on communication overhead optimize the group performance

For efficient operation, the performance of group needs to be optimized in terms of both computation and communication costs. This optimization mainly occurs during the sudden visit and leave within the group by mobile member. The key material update from the overall visited areas during the identical time intervals acquires significant overhead, so the unicast messages in secure form is used by this manager for new key deliver.

C. Member's congestion in some areas

The same pattern was not followed by the member's mobility to reach next destination. Due to this, the subgroup size increases and also increases the overhead of key management than the subgroup with few members. In order to attain high efficiency, it requires an adaptive method to separate the large subgroup into numerous small subgroups. Otherwise it combines the adjacent subgroups into single group for reducing the impacts of both computation and communication cost [23].

D. IoT as a developing Information based global internet architecture

The IoT offers infrastructure for dynamic global network by joining the day-to-day objects and also by inserting intelligence into the environment. In GKM the future works were carried out to support the wireless networks heterogeneity. [20].

VI. SUGGESTION FOR FURTHER STUDY

The summary for GKM classes and its future scope were provided in this part. To compare GKM classes various criteria's were discussed, they are presented below.

Recovery: A perfect GKM needs to be recover from the failures without reinitializing the whole group. This condition was widely satisfied by the decentralized GKM and distributed GKM and high range of availability was achieved by this two GKM in system failures and network. Because in these two schemes similar group key was computed by the entire members. In this, the member failure was ignored as it does not affect any other members in the group, and the overall members were treated equally. In the same way, if any member failure, does not disturb the whole group. However, the centralized scheme does not perform this recovery because it depends on single group controller.

Key independence: If the developed key does not co-operate with further keys, then the presented protocol is said to be key independent.

Scalability: The centralized method was scaled to huge amount of group members and large sparse groups. It can also adapt highly dynamic membership, and frequent key re-distribution was generally provided by these features. But, these features were widely end up by both distributed and decentralized GKM methods [45].

Keys storage: Tree based scheme same as centralized requires members for storing huge amount of other host keys. But, in both distributed and decentralized methods the members can store only its own key.

Dynamic membership: These security service use only the registered senders and receivers for packet transmission and reception. The leave and join processes were found to be frequent and dynamic in multicast communication. The GKM approach was included with this multicast to make sure that the past messages were not applicable to the new members and also to ensure that the members left from the group does not receive any future or current messages. Particularly, distributed approach improves the efficiency of key update by not frequently updating the keys on the members who were left from the group.

Table 5: Comparison between three approaches of GKM

Evaluation properties	Centralized	Decentralized	Distributed
Bottleneck	present	absent	Absent
Key management	Single key	Multiple keys	contributory
Handling capacity	Easy to handle	Easy to handle	Difficult
Key structure	Pairwise or LKH	Pairwise or LKH	Ring based, hierarchical
Server computational cost	High	Moderate	unpredictable
Client computational cost	Low	Low	High
Group size Scalability	Moderate	High	Low
Reliability	No	Yes	Yes
Key type	symmetric/ Asymmetric	symmetric/ Asymmetric	Asymmetric
Central entity dependence	Dependent	Independent	Independent

Signalling message: This method was also compared with numerous messages for key update during member join/leave, network failure, etc. In order to minimize these messages various methods based on multicast communication for key distribution was developed. The group controller contact each group member for membership validity verification, this process increase the bandwidth requirement of centralized GKM [21].

Future scope: The requirement of GKM has increased a lot due to its merits in encryption and decryption process. But in recent days, enormous advancement in technology demand for advanced methods in GKM to perform multicast communication in encrypted way without any interference. So, the researchers were working efficiently in this field to improve the security of messages in multicast communication. In this review, a large number of GKM methods were reviewed for multicast communication. Our future scope is to present a new efficient method in GKM for providing secure communication among clusters. So, that the packets can be deliver to client without any third party intrusion in the multicast network.

VII. QUESTIONS AND ANSWERS BASED ON THE STUDY

a. Whether the centralized approach has sufficient scalability?
b. Why the distributed approach offers the fault tolerance in multicast communication?
c. Why the computational cost of distributed GKM is high?
d. What are the challenges that affect the performance of GKM approaches?
e. Why separate authentication scheme required for decentralized GKM?
f. What are the advantages of using ring based approach in distributed GKM?
g. What are the merits of KEK in LKH?

Answers for review questions:

h. Centralized approach makes the group member flexible by receiving the group communication from various groups, due to this reason, it encounters huge scalability problem in wireless networks.
i. In distributed scheme fault tolerance was involved and the features of fault tolerance sacrifices its operational efficiency due to the effects of computation overhead and communication cost.
j. The involvement of D-H key exchange protocol in distributed GKM increases the computational cost of TEK with respect to its exponentiation. In addition to this, it takes large time for entire collaborating members to extent the TEK. The group size increment may linearly increase the conjunction time required for key generation.
k. The performance of GKM methods was largely affected by some factors they are, resource constraints, widely dispersed mobile devices, and bandwidth limitation.
l. In this decentralized method, the rekeying process was performed better than the centralized approach as it transmit the key for very less hops in order to attain its destination. The members roam over the entire wireless network and obtain the group communication content from the entire network. The GKM have to integrate authentication mechanism to verify the members before receiving the keying materials that are utilized in the target subgroup.
m. The significant advantage of this method is that, it treat the entire group members equally and if any one of the group member deteriorate to finish the setup, it won't degrade the entire group member performance. The key computation requires strict synchronization and it was estimated serially in multiple rounds.
n. The messages required for update process was reduced by KEK, particularly when the member leave from the group. The alteration in group membership may reduce the key material update messages for this the entire method was scaled into the groups having large size. The failure at particular point was represented by single KS dependency to attain the bottleneck performance.

VIII. CONCLUSION

The issues of multicast communication and some of the GKM approaches to overcome this issues were reviewed. The security mechanism is largely needed for multicast IPv6 network to provide a confidential communication among group members. GKM place its wide footprint in the multicast communication field by improving the communication security. GKM includes three types; centralized, decentralized, and distributed. These three types further more improve the privacy of multicast communication. In this review, number of methods that belongs to these three GKM classes were also reviewed. Some of the challenges that are faced by this multicast communication was also reviewed and provided literally. The requirements of these GKM classes was also reviewed. Finally some of the review questions and their answers were also provided in this work. These details were very much useful to obtain a clear details regarding the performance of GKM in multicast communication. In recent years, number of experiments were performed in this multicast IPv6 network for secure communication. The high range of security was achieved after implementing the GKM classes.

REFERENCE

1. Piao, Y., Kim, J., Tariq, U. and Hong, M., 2013. Polynomial-based key management for secure intra-group and inter-group communication. Computers & Mathematics with Applications, 65(9), pp.1300-1309.
2. Wong, C.K., Gouda, M. and Lam, S.S., 1998, October. Secure group communications using key graphs. In ACM SIGCOMM Computer Communication Review (Vol. 28, No. 4, pp. 68-79). ACM.
3. Mapoka, T.T., 2013. Group key management protocols for secure mobile multicast communication: A comprehensive survey. International Journal of Computer Applications, 84(12).
4. Vijayakumar, P., Bose, S. and Kannan, A., 2014. Chinese remainder theorem based centralised group key management for secure multicast communication. IET information Security, 8(3), pp.179-187.
5. Nicanfar, H., Jokar, P., Beznosov, K. and Leung, V.C., 2014. Efficient authentication and key management mechanisms for smart grid communications. IEEE systems journal, 8(2), pp.629-640.
6. Shen, J., Tan, H., Moh, S., Chung, I., Liu, Q. and Sun, X., 2015. Enhanced secure sensor association and key management in wireless body area networks. Journal of Communications and Networks, 17(5), pp.453-462.
7. Veltri, L., Cirani, S., Busanelli, S. and Ferrari, G., 2013. A novel batch-based group key management protocol applied to the internet of things. Ad Hoc Networks, 11(8), pp.2724-2737.
8. Porambage, P., Braeken, A., Schmitt, C., Gurtov, A., Ylianttila, M. and Stiller, B., 2015. Group key establishment for enabling secure multicast communication in wireless sensor networks deployed for IoT applications. IEEE Access, 3, pp.1503-1511.
9. Karthick, S. 2018. TDP: A Novel Secure and Energy Aware Routing Protocol for Wireless Sensor Networks. In International Journal of Intelligent Engineering and Systems, 11(2), pp. 76-84..
10. Sathish, T., Periyasamy, P., Chandramohan, D., Nagabhooshanam, N.., 2018. Modelling K-nearest neighbour technique for the parameter prediction of cryogenic treated tool in surface roughness minimization. International Journal of Mechanical and Production Engineering Research and Development, 2018(special), pp.705-710.
11. Metwaly, A.F., Rashad, M.Z., Omara, F.A. and Megahed, A.A., 2014. Architecture of multicast centralized key management scheme using quantum key distribution and classical symmetric encryption. The European Physical Journal Special Topics, 223(8), pp.1711-1728.
12. Yang, Y., Zheng, X., Liu, X., Zhong, S. and Chang, V., 2018. Cross-domain dynamic anonymous authenticated group key management with symptom-matching for e-health social system. Future Generation Computer Systems, 84, pp.160-176.
13. Mehdizadeh, A., Hashim, F., Abdullah, R.S.A.R., Ali, B.M., Othman, M. and Khatun, S., 2014. Multicast-unicast data delivery method in wireless IPv6 networks. Journal of network and systems management, 22(4), pp.583-608.
14. Lorente, G.G., Lemmens, B., Carlier, M., Braeken, A. and Steenhaut, K., 2017. BMRF: Bidirectional multicast RPL forwarding. Ad Hoc Networks, 54, pp.69-84.
15. Abdel Fadeel, K.Q. and El Sayed, K., 2015, May. ESMRF: enhanced stateless multicast RPL forwarding for IPv6-based low-Power and lossy networks. In Proceedings of the 2015 Workshop on IoT challenges in Mobile and Industrial Systems (pp. 19-24). ACM.
16. Nguyen, T.T. and Bonnet, C., 2014. Considerations of IP multicast for load balancing in Proxy Mobile IPv6 networks. Computer Networks, 72, pp.113-126.
17. Wang, X., 2015. Multicast for 6LoWPAN wireless sensor networks. IEEE Sensors Journal, 15(5), pp.3076-3083.
18. Mapoka, T.T., 2013. Group key management protocols for secure mobile multicast communication: A comprehensive survey. International Journal of Computer Applications, 84(12).
19. Vijayakumar, P., Bose, S. and Kannan, A., 2013. Centralized key distribution protocol using the greatest common divisor method. Computers & Mathematics with Applications, 65(9), pp.1360-1368.
20. Daghighi, B., Kiah, M.L.M., Shamshirband, S. and Rehman, M.H.U., 2015. Toward secure group communication in wireless mobile environments: Issues, solutions, and challenges. Journal of Network and Computer Applications, 50, pp.1-14.
21. Baddi, Y. and El Kettani, M.D.E.C., 2013, April. Key management for secure multicast communication: A survey. In 2013 National Security Days (JNS3) (pp. 1-6). IEEE.
22. Cheikhrouhou, O., 2016. Secure group communication in wireless sensor networks: a survey. Journal of Network and Computer Applications, 61, pp.115-132.
23. Daghighi, B., Kiah, M.L.M., Iqbal, S., Rehman, M.H.U. and Martin, K., 2017. Host mobility key management in dynamic secure group communication. Wireless Networks, pp.1-19.
24. Gomathi, K., Parvathavarthini, B. and Saravanakumar, C., 2017. An efficient secure group communication in MANET using fuzzy trust based clustering and hierarchical distributed group key management. Wireless Personal Communications, 94(4), pp.2149-2162.
25. Baddi, Y. and El Kettani, M.D.E.C., 2018, October. Optimal Shared Multicast Tree Based Solution for Group Key Management in Mobile IPv6. In 2018 IEEE 5th International Congress on Information Science and Technology (CiSt) (pp. 567-572). IEEE.
26. Pourbabak, H., Chen, T. and Su, W., 2019. Emerging data encryption methods applicable to Energy Internet. In The Energy Internet (pp. 181-199). Woodhead Publishing.
27. Harn, L., Hsu, C.F. and Li, B., 2018. Centralized group key establishment protocol without a mutually trusted third party. Mobile Networks and Applications, 23(5), pp.1132-1140.
28. Cohn-Gordon, K., Cremers, C., Garratt, L., Millican, J. and Milner, K., 2018, October. On ends-to-ends encryption: Asynchronous group messaging with strong security guarantees. In Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security (pp. 1802-1819). ACM.
29. Baddi, Y. and Ech-cherif El Kettani, M.D., 2018, May. OSM-GKM Optimal Shared Multicast-Based Solution for Group Key Management in Mobile IPv6. In International Conference on Networked Systems (pp. 255-269). Springer, Cham.
30. Khan, M.A. and Salah, K., 2018. IoT security: Review, blockchain solutions, and open challenges. Future Generation Computer Systems, 82, pp.395-411.
31. Islam, S., Muslim, N. and Atwood, J.W., 2018. A survey on multicasting in software-defined networking. IEEE Communications Surveys & Tutorials, 20(1), pp.355-387.
32. Basu, S.S. and Tripathy, S., 2019. Securing Multicast Group Communication in IoT-Enabled Systems. IETE Technical Review, 36(1), pp.83-93.
33. Ali, M. and Salim, B.M., 2019. An Efficient Group Key Management Using Clustering Algorithm for Mobile Ad Hoc Networks. In Third International Congress on Information and Communication Technology (pp. 107-118). Springer, Singapore.
34. Rafaeli, S. and Hutchison, D., 2003. A survey of key management for secure group communication. ACM Computing Surveys (CSUR), 35(3), pp.309-329.

35. Rafaeli, S. and Hutchison, D., 2002. Hydra: A decentralised group key management. In Proceedings. Eleventh IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises (pp. 62-67). IEEE.
36. Zhang, Q. and Wang, Y., 2004, December. A centralized key management scheme for hierarchical access control. In IEEE Global Telecommunications Conference, 2004. GLOBECOM'04. (Vol. 4, pp. 2067-2071). IEEE.
37. Eltoweissy, M., Heydari, M.H., Morales, L. and Sudborough, I.H., 2004. Combinatorial optimization of group key management. Journal of Network and Systems Management, 12(1), pp.33-50.
38. Ali, S., Rauf, A., Islam, N., Farman, H., Jan, B., Khan, M. and Ahmad, A., 2018. SGKMP: A scalable group key management protocol. Sustainable Cities and Society, 39, pp.37-42.
39. Vijayakumar, P., Chang, V., Deborah, L.J. and Kshatriya, B.S.R., 2018. Key management and key distribution for secure group communication in mobile and cloud network.
40. Jaiswal, P. and Tripathi, S., 2018. Cryptanalysis of olimid’s group key transfer protocol based on secret sharing. Journal of Information and Optimization Sciences, 39(5), pp.1129-1137.
41. Islam, S.H., Obaidat, M.S., Vijayakumar, P., Abdulhay, E., Li, F. and Reddy, M.K.C., 2018. A robust and efficient password-based conditional privacy preserving authentication and group-key agreement protocol for VANETs. Future Generation Computer Systems, 84, pp.216-227.
42. Abdmeziem, M.R. and Charoy, F., 2018. Fault-tolerant and Scalable Key Management Protocol for IoT-based Collaborative Groups. In Security and Privacy in Communication Networks: SecureComm 2017 International Workshops, ATCS and SePrIoT, Niagara Falls, ON, Canada, October 22–25, 2017, Proceedings 13 (pp. 320-338). Springer International Publishing.
43. Iqbal, S., Kiah, M.L.M., Zaidan, A.A., Zaidan, B.B., Albahri, O.S., Albahri, A.S. and Alsalem, M.A., 2019. Real-time-based E-health systems: Design and implementation of a lightweight key management protocol for securing sensitive information of patients. Health and Technology, 9(2), pp.93-111.
44. Pareek, G. and Purushothama, B.R., 2018. Provably secure group key management scheme based on proxy re-encryption with constant public bulletin size and key derivation time. Sādhanā, 43(9), p.137.
45. Yousefpoor, M.S. and Barati, H., 2018. Dynamic key management algorithms in wireless sensor networks: A survey. Computer Communications.
46. Janani, V.S. and Manikandan, M.S.K., 2019. A Genetic-Based Distributed Stateless Group Key Management Scheme in Mobile Ad Hoc Networks. In Integrated Intelligent Computing, Communication and Security (pp. 233-241). Springer, Singapore.
47. Ali, M. and Salim, B.M., 2019. An Efficient Group Key Management Using Clustering Algorithm for Mobile Ad Hoc Networks. In Third International Congress on Information and Communication Technology (pp. 107-118). Springer, Singapore.
48. Kung, Y.H. and Hsiao, H.C., 2018. GroupIt: Lightweight Group Key Management for Dynamic IoT Environments. IEEE Internet of Things Journal, 5(6), pp.5155-5165.
49. Athmani, S., Bilami, A. and Boubiche, D.E., 2019. EDAK: An Efficient Dynamic Authentication and Key Management Mechanism for heterogeneous WSNs. Future Generation Computer Systems, 92, pp.789-799.5.
50. Benmalek, M., Challal, Y., Derhab, A. and Bouabdallah, A., 2018. VerSAMI: Versatile and Scalable key management for Smart Grid AMI systems. Computer Networks, 132, pp.161-179.