International Journal of Innovative
Computing, Information and Control
Volume **13**, Number **2**, April **2017**

ICIC International ©2017 ISSN 1349-4198
pp. 559–574

A STUDY OF KEY MANAGEMENT PROTOCOLS FOR MULTICAST ENCRYPTION

Jayaprakash Kar

Department of Computer Science and Engineering
The LNM Institute of Information Technology
Rupa ki Nangal, Post-Sumel, Via-Jamdoli, Jaipur-302031 (Rajasthan), India
jayaprakashkar@lnmiit.ac.in

Received May 2016; revised October 2016

Abstract. *Cryptographic key management requires the use of high levels of security when it is applied for generating, exchanging, storing, and re-keying of keys that are used for communication. In these scenarios, group key management is very crucial in controlling key generation, distribution and updates. However, the major problem that arises is the achievement of a scalable re-key technique triggered by membership change. The security of cryptosystems relies immensely on key management processes. In this paper, we have surveyed the key management protocols that are used for multicast encryption and presented the centralized scheme, decentralized scheme, distributed key management scheme, tree based scheme and cluster based scheme.*
Keywords: Group key, Multicast, Key management, Security, Re-keying, TEK

1. **Introduction.** Growth of the Internet has spurred the increased use of bandwidth in modern networks that have inspired the growth and development of new services with the ability to combine voice, text and video over IP. Despite the prominence of unicast communication over the last years, the demand of multicast communications immensely increased. Content providers are adopting the approach owing to its high service delivery approach. There is no doubt that multicasting is immensely used as a means of communication mechanism for the group based applications that include video conferencing, video on demand, interactive group games, e-learning, software updates, database replication and numerous other channels [1]. The security of these group communications is reliant on the protection of traffic encryption key (TEK). On this premise group key management is essential in controlling key generation, distribution and updates. However, the major problem that arises is the attainment of a scalable re-key technique triggered by membership change. In this survey, we have discussed bout the well-known group key management protocol in wired networks and classified them into three major groups: centralized, decentralized and distributed [2, 7]. Further, common and independent TEK denotes another form of classification of the key management protocols. In a bid to create an efficient key management protocol there is a need to adopt some miscellaneous requirements.

Key management protocol is a very essential cryptographic primitive for multi-cast encryption. In this survey, we have presented security challenges of key management protocols and discussed various protocols that are used for multi-cast encryption. For a secure communication, cryptographic key management requires the use of high levels of security when it is applied for generating, exchanging, storing, and re-keying of keys. In this context, group key management has the vital role to control the generation, distribution and modification of key. However, the major problem that arises is the achievement of a

scalable re-key technique triggered by membership change. The security of cryptosystems relies immensely on key management processes.

2. **Classification of Group Key Management Protocols.** The group key management protocols can be classified generally as network independent and network dependent based on the key management protocols. The independent key management is further broken into centralized, distributed and decentralized protocols. The network dependent key management protocol is also segmented into tree and cluster based key management protocols [2]. Figure 1 below shows an overview and the classifications of the group key management protocols, also listed some of existing protocols in each scheme. The centralized system offers a single entity the responsibilities of carrying out all the group communications. This entity is solely mandated with the tasks of key generation, distribution and management. The decentralized system was structured with a key idea of reducing the load on KDC, the central entity [3]. Decentralization is attained by splitting the group members into several manageable subgroups each managed by a controller. The decentralized system serves to solve the problems that hamper the centralized system [3]. The distributed system denotes the approach where the group members of a multi cast session cooperate with each other in order to generate the required group key. Distributed key management protocol category lacks controllers making it a more fault tolerant classification. The problem with this category is that whenever there is a change in membership the security protocols are compromised [4]. Unlike the group dependent key management protocols, the network independent cannot be applied to wireless communication networks [9]. The major challenge that arises from the network independent key management protocols is the problem of supporting mobile multicast where members move over the wireless network while receiving their multicast services [4].

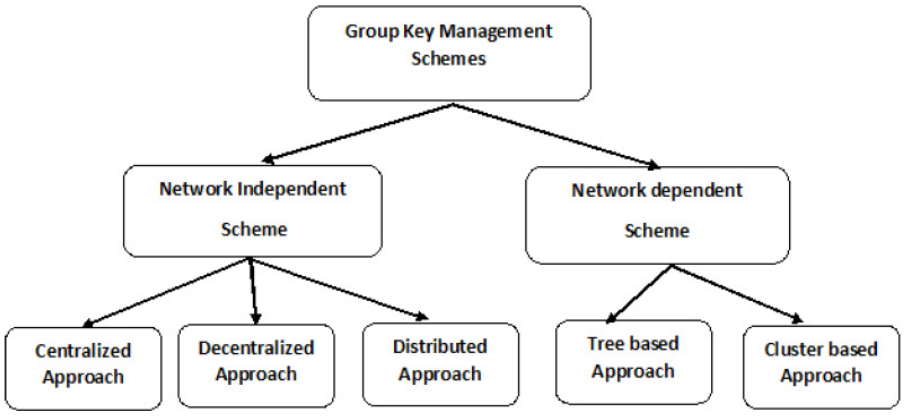

FIGURE 1. General classification of group key management scheme

3. **Group Key Establishment Protocols.** The essence of the key establishment protocols is to ensure that two or more networked parties are able to establish a secure communication framework. In order to establish a secure connection and use cryptography the parties must be able to share a key that is usually referred to as a session key. Further, a key establishment protocol is essential to have an existing infrastructure platform that will use an existing shared key, a public key infrastructure and a mutually trusted third party [5]. There are three main types of key establishment protocols namely:

- Two parties or group parties
- Key agreement or key transport
- Server based or server less

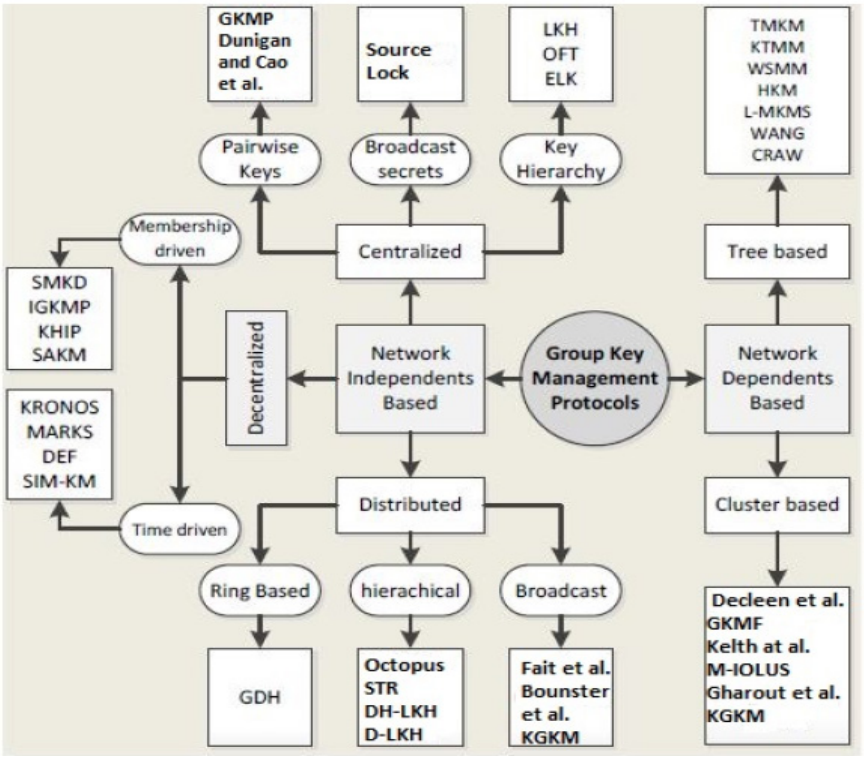

FIGURE 2. Overview of group key management protocols

3.1. **Two parties or group parties.** Two or more parties come together and agree on a specific key based on one or more party's knowledge. The protocol gives the involved parties the power to dictate their relationship as opposed to being controlled by a third party. The significance of this agreement is that an eavesdropper or middle man cannot be able to obtain information that will spur brute force guess on the passwords without interacting with the involved parties [7]. Thus, the protocol ensures strong security [4].

3.2. **Key agreement or key transport.** A key agreement protocol is where two or more parties agree on a specific key in such a way that they both influence the outcome of the key. This approach plays a crucial role of delineating any third parties who may force the use of a particular key [8]. A number of key exchange protocols are established on a premise where a single party generates the keys and sends them to other parties who play no role in the generation process. The use of a key agreement protocol avoids some of the problems associated with key distribution [10].

3.3. **Server based or server less.** The key management inter operability protocol (KMIP) is termed as a communication protocol that defines the format of messages which are used in the manipulation of cryptographic keys on the key management servers. Under the server based key establishment protocol the keys are created on a specific server and then retrieved or wrapped by other keys. The merit of this approach is that it supports both the symmetric and asymmetric keys. The goals of the key establishment protocols can be denoted as:

- Key authentication: the parties get to know who has the session key;
- Entity authentication: each party gets to know the active parties;
- Known-key security: the adversary may have obtained the security key from the other older channels [8];

- Forward secrecy: adversary may get to learn secrets of groups after the lapse of the sessions;
- Key compromise impersonation (KCI) security: the adversary may get to learn the security key of a single party before the session runs [11].

4. **Security Requirements of Key Management Protocols.** Key management protocols have many requirements in order to achieve the security needed. We have summarized these requirements as follows.

- **Forward secrecy**: Security is heightened by denying members who have left the group access to data or the ability to decrypt the data. This is an important strategy of guaranteeing that the overall security of the group and providing confidentiality and integrity. At the same time, the strategy is key in group management because some members may be evicted from the group and it is essential to ensure that they do not cause harm as payback. Instead of starting the whole process from scratch, their initial capabilities are disabled [7, 11].
- **Backward secrecy**: Here, previous keys are not accessible by any new members joining a group. The approach is essential in preventing the decryption of crucial data by new members. If these members are allowed to decrypt the data, then chances are that they would have also accessed the data without being members. Thus, strategy follows the principle of only members allowed [13].
- **Key independence**: The materials used ought to be independent from one another. This is a predominant approach of ensuring that if one key is compromised, the other keys remain protected and the damage that may be done may not be significant to the entire group [13].
- **Collusion freedom**: Any collusion from any departing members of fraudulent members is inhibited immensely. This is a security protocol undertaken by applying the old keying materials that are known to the evicted group members [13].
- **Trust relationship**: In this case, not all third parties or individuals are given full trust. This is essential in taking the necessary precautions in accepting fraudulent parties who may hamper the amicable relationships in a group [11].
- **Resilience**: A good key management protocol or security measure is one which is able to withstand the impact of an intrusion. Thus, it is mandatory to include a threat model when undertaking a security analysis and deployment of group key management protocols. In order to take consideration of the resilience of the group, such factors as network based attacks and service related attacks must be considered.

5. **Security Challenges of Key Management Protocols.** Most of key management protocols have many security challenges in both classified groups. Therefore, the key management security challenges are listed below. Many organizations have stuck to the use of wired networks despite their inflexibility. One of the most important aspects of wired networks is that they are easily controlled and reliable; this means that they are more secure than the wireless networks. However, as it is stipulated by different experts, no network is entirely secure. The use of wired networks requires the adoption of third party security protocols and firewall due to the absence of fully secure platforms. The use of such components exposes the wired networks to third parties who may inhibit their security stance. If not properly configured, the third party software of firewall may become entry points for hacking activities.

However, wired networks do not prevent social engineering. These are those activities that arise from within a given group. Some group members may be unscrupulous [12].

Thus, despite their controllability and reliability, wired networks are prone to security problems.

Wireless networks have been denoted to offering flexibility and immense convenience in connecting various devices. Wireless networks are also cost effective and generally easier to use as opposed to the wired networks. However, from a security perspective, wireless networks are more susceptible. The threats of malware and viruses intruding the networks are real. Wireless networks may have rogue access. Unknown and unmanaged devices in the network become open back doors providing an easy route for the entry of malware and information to leave the network. Another problem with wireless networks is that mis-configuration of switches and access points impacts the security of the networks. Wireless networks cannot be fully controlled like the wired networks. As people use their devices to connect to wireless networks, they open gates for possible attacks. Hackers are a major menace of the wireless network as far as security is concerned. Hackers intrude the networks easily stealing the crucial information [14].

6. **Centralized Schemes.** The centralized key management scheme (CKM) denotes a single entity responsible for the overall communication processes in a group. The entity carries out key generation, management and distribution. The keys created only with secured dedicated server. Figure 3 below shows overview of centralized key management system. In the following figure, the single entity is the group manager, i.e., key server (KS) which is centralized.

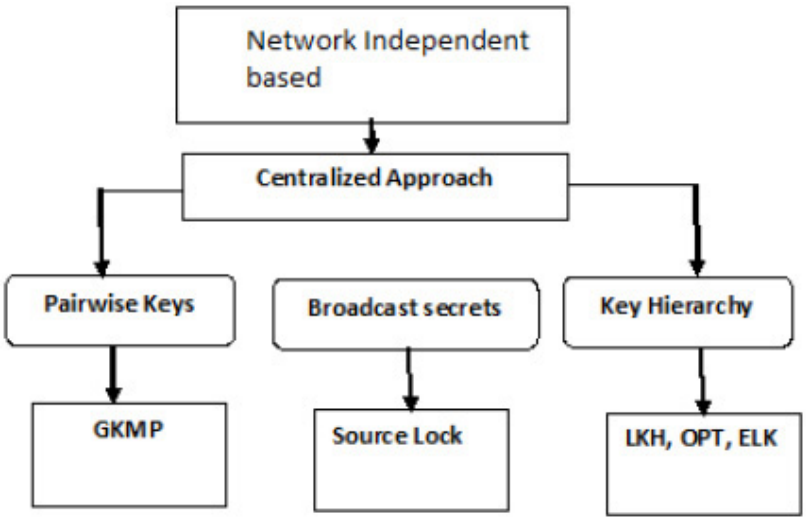

FIGURE 3. Centralized key management schemes

KS gathers and saves information about the members of the group and then it takes n KEK, i.e., key encryption keys. Also each encryption key is participating with a single member of a group. KEK is the stealthy key and the basic purpose for which it is used is the TEK.

Centralized system faces multiple challenges that include scalability overhead, storage overhead, single failure point, and maintenance of backward and forward secrecy, collusion independence. The different centralized key management schemes with some proposed protocols are as illustrated in Figure 4. In pairwise scheme the KS shares with all group members the secret key KEK. The key purpose is to launch the secured channel for the transfer of TEK securely between the member of the group and the KS whenever there is a need of key. In this article, it has reviewed four group key management protocol

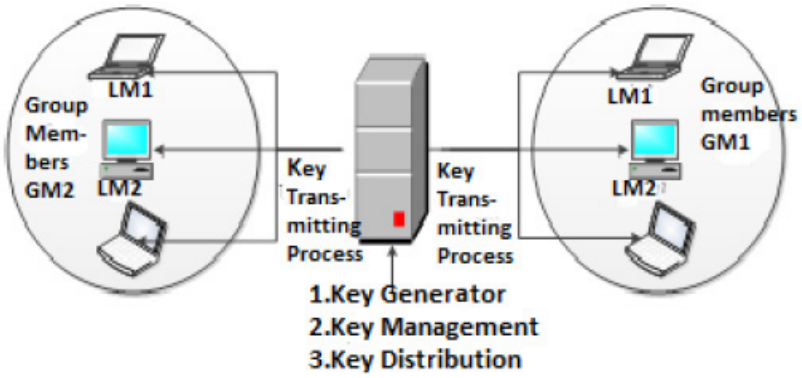

FIGURE 4. Centralized key management system

(GKMP) which are under pairwise scheme. A group key is generated by the key server which contains group KEK and group TEK keys. While, if we look on the functionality of TEK and KEK group, GTEK is functioned to encode the data while group KEK is functioned to shelter the new GKP whenever there is a need. Though, whenever a session is joined by a new member then a new GKP is generated by the server key which covers a new GTEK to ensure the maximum retrograde secrecy and then forwards it to the new associate safely which is encoded with the KEK, i.e., recognized with the new associate and also forward it to the already existing associates which are encoded with the older GTEK. GKP is re-invigorated sporadically by the key server and then forwards it to the other members of the group which are encrypted with KEK, i.e., shared with every member of the group. To carry out this procedure, $\nvdash(n)$ re-key messages are required by GKMP for every leave from the group. So, this is the keen reason that problem of particular solution does not gage to a group of extremely vibrant associates.

Chu et al. [15] proposed their own protocol which is Chu et Protocol, where a furtive key encryption key is shared by a group leader with every member of the group. In order to send a secret message, it is encrypted with an unsystematic key by the dispatcher and then the key is encrypted by the sender with the help of secret KEK which has been shared with the leader of the group and after this, it is forwarded accompanied by the encoded message to the other associates of the group. When the posts are received by the receiver, then it can be decrypted because the sender does not have the key which was sent on the sender end protected with a random number. When the message is received by the leader, then it is decrypted with the help of key and then group leader constructs a substantiation message which have the encrypted data with every KEK which is then further pooled with every associate of the group except the leaving members. When the validation message being received, then it is further decrypted by every receiver with the help of KEK and hereafter decrypt the message which was firstly encrypted with communication of the authentication messages being required by the leader of the group every time whenever a message is sent to the group which is the drawback of this protocol.

Logical key hierarchy (LKH) protocol is proposed by Wallner et al. [16, 17]. In this protocol, origin of the tree is KS and a hierarchy of keys is maintained by it. In this protocol, as a maximum $1 + \log_2(n)$ re-key communication is stored by each node. The limitation of this solution is the number of messages which are required to apprise key is the order of $\mathbb{O}(n)$.

McGraw and Sherman proposed one-way function tree (OFT) protocol [18] a big enhancement over the LKH. KEK of the nodes is deliberated by members of the group rather than accredited by the KS. Blended sibling keys are maintained by each node and

the blinded secret KEK of its ancestors is also maintained by the leaf secret key in this protocol. In this approach the number of re-keying the required message is reduced to half in contrast with LKH.

The centralized flat table key management (CFKM) was proposed by Waldvogel et al. [19]. The flat table concept is used in this protocol so as to minimize the strength of keys that are upheld by the KS. It is comprised of one TEK and $2w$ records for KEKs, and in it, identifier of a member uses w number of bits. Wong et al.'s procedure is the lee way of the LKH procedure. Binary tree for key dissemination is used by the LKH while Wong et al. practice the k-array tree.

Source lock was proposed in [20]. The deciphering group session key is locked with this protocol and therefore it is used. Each encrypted message is encrypted along with the single lock. The session key can be "unlocked" by the members of the secure group. The principle on which the secure lock works is the mathematics of the Chinese Remainder Theorem (CRT). This method is more flexible towards the lively addition and also in the deletion of group members. The strength of re-key messages is minimized with this protocol. Though, the drawback increases due to the reckoning at the server because of the implementation of Chinese Remainder calculations theorem before transferring each communication to the members of the group.

7. **Decentralized Schemes.** Groups under the decentralized system are split into subgroups that enable the overall management of key protocols. Decentralized approach is also broken down into protocols which are membership driven and also the time driven protocols. The membership driven protocol culminates such protocols as scalable multicast key distribution (SMKD), hydra fall and intra-domain group key management protocol (IGKMP). Kronos, MARKS and dual-encryption protocol fall under the time driven protocols. The main challenges of this approach include the issues of trust and efficiency. A group key dissemination technique which is built on the core based tree (CBT) multicast routing protocol is proposed by Ballardie's scalable multicast key distribution (SMKD) protocol. If we look the architecture of CBT, main core is rooted by the multicast. The network is split into managerially scoped areas in intra domain group key management (IGKMP) [21], area key distributor (AKD) and domain key distributor (DKD) is contained by this protocol. Group TEK is created by the DKD and it is the responsibility

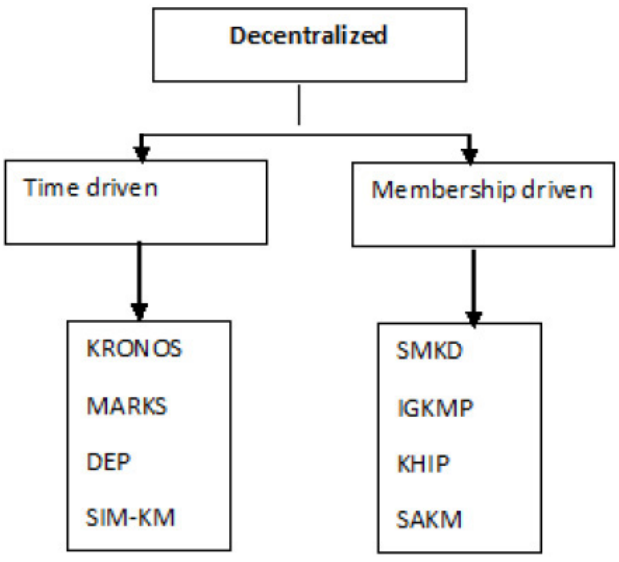

FIGURE 5. Decentralized key management schemes

and it is propagated to the members through AKD. Both of them belong to the multicast cluster called All-KD-Group.

The group is systematized into further sub groups in Hydra protocol [22]. Every sub group has its own server which is called Hydra server and its keen responsibility is to regulate the sub cons. The BAAL procedure contains three entities: one of them is the group controller (GC) which is responsible to maintain the participant list (PL) and to create and distribute the collection key TEK to other members with the help of local controller. Another is the local controller (LC) which is accountable to accomplish the keys in sub-sectors, obtains the new TEK and allocates it to the associates which are further linked to the sub-sectors. The last one is the group associate. The context of a grading of the multicast subsections is to establish cybernetic group protocol by the IOLUS [23]. Security agent (GSA) manages every group and it is accountable for handling the key inside the sub sectors and groups.

Planned context for multicast safety is cipher sequences [24], which is founded on revocable cipher sequence. Roots of the multicast tree are at basis and the leaves of the tree are termed as group associates. Scalable adaptive key managing structure (SAKM) procedure is presented in [3]. The scalability problem is managed by this protocol. SAKM challenges the scalability by arranging the groups into further groups.

A time driven scalable tactic known as Kronos is defined by Setia et al [25]. The cluster is denoted with a birth and death method archetypical by Setia in this protocol and has discussed the model in two cases which are independent subscriber and correlation subscriber behavior. Kronos is functioned in similarity with IGKMP and the functionality is the same. The cluster is alienated hierarchically into further collections in dual encryption protocol (DEP), and sub-cluster manager (SGM) manages the further sub groups. The multicast cluster is systematized into a bundle of sub groups and every sub-zone is accomplished by KS in Yang et al. [26] protocol approach. It is the responsibility of the KS responsible to re-key the members in the subgroups sporadically. The proxy encryption is used by the ascendable substructure for multicast key management (SIM-KM). The proxy function is used by SIM-KM which further changes the cipher text for one key and then into the cipher for another key. The table below shows the performance of the decentralized group key management schemes. The different protocols are compared by the use of parameters that include independence, re-keying among the subgroups and central re-keying [25].

TABLE 1. Decentralized key management protocols

Protocol	Key independence	1-affect-n	Local re-ky	Re-key	Fault tolerant
SKMD	Yes	Yes	No	No	No
IGKMP	Yes	Yes	No	Yes	No
Hydra	Yes	Yes	No	Yes	Yes
Kronos	No	No	No	No	Yes
MARKS	No	No	No	No	Yes
DEP	Yes	Yes	No	No	No

8. **Distributed Key Management Schemes.** A distributed key management scheme does not involve the role of a controller. Under this approach the group members cooperate with each other to generate the required keys. The problem with the distributed mechanism is that when there is a change in membership the security is compromised. The procession time and communication overhead also tends to increase when the group

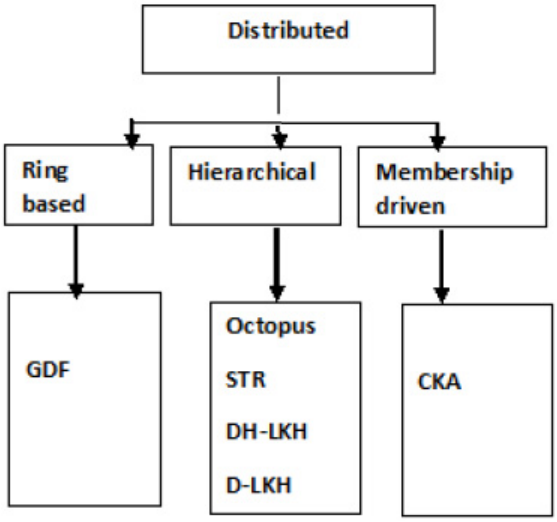

FIGURE 6. Distributed key management schemes

size increases. Each group member is required to keep track of all other members to enhance communication. The system is sub-categorized into ring based, hierarchy based and broadcast based cooperation. The number of rounds required in communication, message numbers and computational costs affect the distributed system [1]. Every group member is organized into a cybernetic ring by Ingemarson et al. procedure [27], and for the cluster key generation, the group Diffie-Hellman (GDH) procedure uses the leeway of Diffie Hellman algorithm. The limitation of GDH protocol is that it is not appropriate for every dynamic group because after the change of every membership it entails the implementation of the whole procedure. The whole group is alienated into other four sub zones in OCTOPUS. The spearhead member of the sub-zone is accountable for amassing the midway sub-zone standards and computes the transitional DH assessment. Every associate of the group is accomplished of scheming the cluster key in this protocol. Group associates are the leaves and are associated with it and every leaf is recognized by its position. This protocol persuades a $\mathbb{O}(n)$ key cunning so as to create the cluster key linked to the origin of the tree due to its unique linear structure. Besides, every associate should stock and uphold all the free keys which are allied to every lump of the tree. The tree is recreated thus and henceforth every associate apprises the cluster key which is new key allied to the main origin of the tree in case of a membership change. The binary tree is built from ground to top. The concept of sub-trees, like minded on a shared key is used by the distributed logical key hierarchy (D-LKH) protocol. Logical key order is used in the distributed one-way function tree (D-OFT) method in a disseminated fashion and it was planned by Dondeti et al. [28], which practices the single way function tree proposed by McGrew and Sherman. Group associate is trustworthy with admittance switch and key peer group. Every member transmits a sole message to other members so as to settle on a mutual clandestine in Fiat and Naor procedure [29]. In this protocol, by dissemination of the clandestine messages and issuing additions among the group associates, group key is produced. The weakness of this protocol is that it is not robust against collusions and has the problem that it requires an unfailing third party. A three round protocol is Burmester and Desmedt protocol [30] with associate group, dissemination and cluster key calculations. Conference key agreement (CKA) protocol [31] is proposed by Boyd and all the group associates are subsidized in order to create the group key the limitation with this protocol is the security as every member of the group can decrypt and generate key on condition that the member owns the public key.

TABLE 2. Distributed key management scheme

Protocol	Rounds	Multi-cast message	DH Key	Leader requirement
Ingemarson et al.	$n-1$	–	Yes	No
DFM	N	n	Yes	No
Octopus	$2\frac{(n-1)}{(4+2)}$	–	Yes	Yes
STR	N	n	Yes	No
D-LKH	3	n	No	Yes
D-OFT	$\log_2 n$	–	No	No
D-FT	N	–	Yes	Yes
Fiat-Naor	2	n	Yes	Yes
BD	3	$2n$	No	No
CKA	3	n	No	Yes

Table 2 shows the requirements of the distributed key exchange schemes. The number of rounds, multi-cast messages, required leaders and DH keys are used to show the different exchange keys [1].

9. **Tree Based Schemes.** The different protocols under the tree based scheme include:
   - Topology matching key management tree (TMKM)
   - A hybrid key management scheme (HKM)
   - WANG approach
   - Combination of rekeying and authentication in wireless networks (CRAW)
   - Multicast key management scheme (MKMS)

The TMKM protocol adapts the traditional key tree (LKH key tree) to the cellular wireless system model and matches the key management tree to a three-level topological assembly. It consists of network entities such as the base stations (BS), mobile users and a manager host commonly termed as (SH). The base stations perform key management inside its scope and then multicast the useful keying to its members and they operate under the jurisdiction of the SH having low communication overheads by broadcasting re-key messages to the useful member unlike network independent centralized group key management approaches that need to broadcast re-keying messages within the whole wireless domain. The drawback of TMKM is the 1-affect-n phenomenon since it uses common TEK approach; hence re-keying affects the entire group. In the user sub tree, the BS needs to multicast all rekeying messages to the members within the cell to achieve key updating. TMKM lacks trust relationship because both the BSs and SHs are provided by a third party hybrid key management (HKM) proposed by [32]. HKM tree suitable for cellular IP environments with topology corresponding (TM) sub trees and topology autonomous (TI) sub trees similar to TMKM [33]. HKM is a network dependent protocol which is enthused by the methodology of tiered cellular systems. HKM tries to solve the problem of TKMM by making sure the corporeal setting of an itinerant user does not affect the user's site on the key supervision tree. It adopts the amalgamation of benefit of together TIKM trees and TMKM trees to achieve both low motion users and also high motion users. Bandwidth is not wasted in HKM because it is able to trace the transfer of re-keying messages for low agility users. However, bandwidth is wasteful for high mobility users because HKM broadcasts the re-keying messages to all the BSs. Even though re-keying messages are reduced in HKM, it uses joint TEK method, which agonizes from

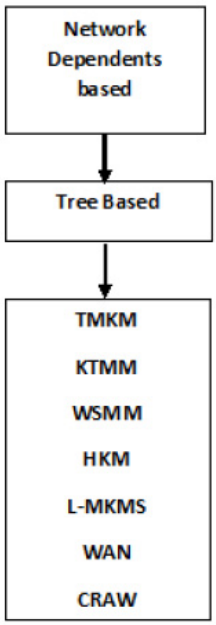

FIGURE 7. Tree key management schemes

1-affect-n spectacle. Update of the group key Ks affects both the TI sub tree and TM sub tree for low mobility and high mobility respectively; hence the protocol cannot handle highly dynamic environment with multiple membership change. This would induce more signaling messages which cannot be handled by the central GM which is a single point of failure.

Wang et al. protocol is proposed by [34]. It is a distributed network dependent group key managing protocol which splits group members into leader elements and general member units. The network entities involved are: group key server (GKS) in the first level which creates group key and distributes it by multicasting it to controller units in the secondary level, independent cell key servers (CKS) per cell in the secondary level which obtains the group key from the GKS and further allocates it to the other associates in its wireless cell. Distributed two tier logical structure is not matched to the cellular network topology which makes the WANG scheme not suitable for wireless implementation. Moreover, it is complicated to select the leader when member evicts at the lead unit. The vast number of keys stock piled by the mobile device which is resource constrained device can affect the operational performance of the mobile device [6]. The protocol does not consider the huge number of messages that can overwhelm the server which is also a single point of failure when multiple membership change occurs. This protocol cannot support highly mobile users who require fast re-keying due authentication delay caused by contacting the previous area server every time a member moves. Increased number of level in WANG scheme complicates key management and delays packet delivery. In order to achieve an efficient re-keying method the authors of [34] proposed this protocol which operates by combining member authentication procedure with group key management. They use simple and password authentication protocol (SAS) [35] for member authentication and use an efficient network independent key managing protocol known as code for key calculation [36] for group key management in wireless networks. This combination provides a simple and secure mechanism while mobile members join/leave a group or move inter-area.

The CRAW scheme adopts a decentralized cellular wireless network framework with the main server which distributes the multicast content to individual area wireless server

(AWS). Main server maintains the main list which contains member information regarding join/leave and movement. AWS which performs member authentication process generates, sends the area group key, and forwards the content to the mobile members. CRAW protocol collaborates with CKC which is more efficient than LKH to manage re-keying in each subgroup. CKC is an improved version of logical key hierarchy (LKH). It reduces the workload from the server by enabling members to compute necessary u-node and k-node keys of the tree using node encryptions and one-way muddle purpose after receiving the updated group key after membership change. The safety of the keys in CKC relies on single way hash function. CRAW procedure is partitioned into two phases: authentication phase when the member first joins the group and when the member moves, and the group key management phase which enables the update of group key and area group key on membership change due to join/leave and update of the area keys only when a member moves.

TABLE 3. Tree based scheme

Protocol	Key dependence	1-affect-n	Multiple membership changes support	Scalability	Security services	Fault tolerant	Re-key overhead
TMKM	Yes	Yes	No	No	No	No	No
HKM	Yes	Yes	No	Yes	No	No	No
WANG	Yes	Yes	Yes	Yes	Yes	Yes	Yes
CRAW	No	Yes	No	Yes	Yes	No	No
MKMS	Yes	Yes	No	Yes	Yes	No	No

Table 3 above shows the comparison of tree based network dependent protocols taking consideration of key dependence, 1-affect-n phenomenon, scalability, fault tolerance, re-key overhead, membership changes, and support of security services [4]. The Wang scheme operates in heterogeneous as opposed to the other protocols in wireless networks. topology matching key management tree (TMKM) and a hybrid key management scheme (HKM) suffer from a single point or failure [39]. Additionally, the number of tree levels affects the overall performance when more hand offs are established.

10. **Cluster Based Schemes.** Kellil et al. [40] proposed a decentralized approach that was termed as the Kellil et al. protocol. The protocol addresses the mobility of the members in using the mobile multicast communication process. In this case the members use a specific key called visitor encryption key (VEK) [37]. The group key management framework (GKMF) is another protocol whose aim is to provide a safe cluster communique in wireless mobile settings. Gharout et al. protocol was proposed as a new key managing protocol to avail a safe cluster communique in cellular networks by using a null re-keying cost. Key managing to secure cluster communications in mobile environments (KMGM) was meant to improve the performance of adaptive clustering in scalable key management communication protocols by the addition of mobility support for the multi-cast members in mobile based networks [38]. The authors of [32, 33] propose a network dependent based group key managing protocol which discourse the subject of member mobility protocol for safe cluster communique in wireless mobile settings. The protocol also introduces the use of lists to simplify mobility management of members. Provisions of other security services for example message authentication and data integrity are indirectly assumed in GKMF. In GKMF, the knots of a network are logically or physically categorized to main units and also the settlement of things, so that all knots are alienated to two levels:

area level and domain level. The entities involved are the DKM which is termed as domain key manager, the main key administrator of sphere i which generates, distributes, stores, and deletes all the key material which may be required at the dominion level and the AKM which is termed as area key manager and the key administrator of the zone j inside a sphere which performs key management in its area and manages group members be located in its area. Both the entities maintain a list so-called Mob List to keep trajectory of mobile associates. Every time there is a member hand off, the protocol records the information such as the IDs of mobile member, multicast cluster G linked by the associate, area that an associate is mobile from, ID of target zone that an associate is poignant to. The GKMF relies on the Mob List to keep track of mobile members and can easily determine whether re-keying is necessary in the visited areas. In GKMF the trustworthy relationship between the communicating entities is ensured by introducing secure association at different levels using shared symmetric keys which are fast to process. However, the biggest disadvantage of this procedure is the large number of keys which are used and then it results in storage complexity at the resource constraint mobile devices. The protocol does not address how leave re-keying is performed in the previous area since there is no re-keying while moving hence forward secrecy is violated. The use of common TEK gives rise to the 1-affect-n phenomenon. A member moving with backward secrecy can suffer join latencies due to rekey of both area key and TEK which are done independently. A member leaving after rapidly moving between the areas requires update of both the area key and the traffic in all the areas that a member had visited. The authors [35] propose a new key management protocol considering node mobility which secures group communications in mobile setting with an insignificant re-keying rate. The procedure follows the concept of sovereign TEK per subgroup to avoid 1-affect-n spectacle. The entities involved are the DKD which are domain key distributors and which manages all the area key distributors (AKDs) under it and AKDs which limit key management procedure only to its area. Each cluster is controlled by one DKD at the domain level and at least one AKD at the area level. AKDs belonging to the same DKD use common TEK; hence no re-keying is required when an associate moves from one place to another within the same cluster. The area levels consist of member nodes which are either dynamic or moving from one area to another. Each AKDi preserves two lists and these lists are a list of associates which is signified by LMi and it comprises individually of current zone i associates; and also an inventory of old associates which is signified by LOi and it also comprises identities of previous members. This protocol has an advantage of optimizing re-keying messages by avoiding renewing the TEK when the member intra cluster moves across areas belonging to the same DKD. This violates the forward and backward secrecy required by any group key management protocol. It reduces the workload from the DKD by allowing the mobile members to be authenticated by the AKDs. Though it introduces null re-keying intra-move, it has a drawback of storage overheads at the member because a moving member participating in multiple sessions needs to store multiple MEKs. The protocol does not address inter cluster movement which may cause data transformation problem the same as in Iolus [36]. A moving member can experience join latency due to data transformation processing delays when it inter moves. The authors of [37] propose an adaptive group key managing protocol for wireless communications known as KMGM which introduces mobility support to adaptive bunching for scalable key managing in active group communications protocol (ASGK) in [38]. The scheme is improved by introducing both the intra-cluster mobility and inter-cluster area mobility then categorizing the AKDs belonging to the same cluster as passive agents or active agents using the heuristic described in [36]. Verification steps of moving members on the target AKD is performed similar to [37]. KGKM forms a hybrid scheme

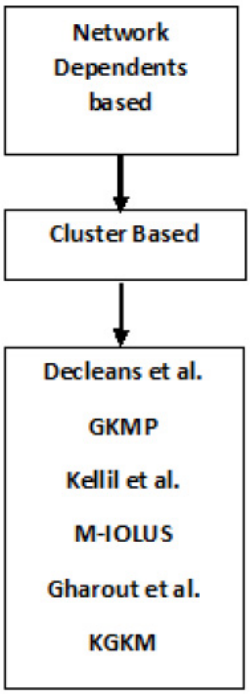

FIGURE 8. Clustering based key management schemes

TABLE 4. Cluster based key management protocol

Protocol	Key dependence	1-affect-n	Multiple membership changes support	Capability	Security services	Fault tolerant	Re-key overhead
Kellil et al.	Yes	Yes	No	No	No	No	Yes
GKMF	Yes	Yes	No	Yes	No	No	Yes
Gharout et al.	Yes	Yes	No	Yes	Yes	Yes	No
KMGM	Yes	Yes	No	Yes	Yes	Yes	No

which takes advantage of both the common TEK and autonomous TEK per sub-category methods. KGKM adopts a decentralized framework whereby a group is partitioned into a hierarchy of administrative areas managed by an area key distributors (AKDs). The internal AKDs of a cluster which are considered passive receive and forward the messages to their respective area members with no data transformation. The operation of KMGM is partially based on the same protocol proposed in [34]; therefore, it inherits some strengths and drawbacks of the protocol. Introducing more micro-groups like in M-Iolus [30] within the cluster add number of encryption areas which may delay the packet delivery to the members. The following table summarizes the cluster based network protocols based on the characteristics of the keys. It is crucial to note that Kellil et al. [40] protocol and GKMF suffer from single point failure. From the above survey, we observed that, group key management is one of the most important cryptographic primitives which is essential in controlling key generation, distribution and alteration. However, the drawback is the attainment of a scalable re-key technique triggered by membership change. The surveys brief the well-known group key management protocol in wired networks. This has been classified in three foremost groups: centralized, decentralized and distributed.

11. **Conclusion.** We have discussed here, the various group key management protocols for encryption in multicast communication. The survey shows that each protocol encompasses a unique set of features that differentiates it from the rest. The different protocols are based on centralized, decentralized and distributed frameworks. The decentralized approach was found to offer scalability by providing the subdivision of individual groups into subgroups. The distributed framework allows each group to participate in key management processes. Further, in this survey, we have shown that, the success of multi cast communication is reliant on the security of the used TEK. A secure channel is required in group management to construe key generation, development and distribution [4]. In order to develop or propose a secure and efficient key management protocol such characteristics as delay, storage overhead, re-key overhead, cost of computation and 1-affect-n phenomenon must be taken into consideration.

REFERENCES

[1] M. Abdalla, Y. Shavitt and A. Wool, Key management for restricted multicast using broadcast encryption, *IEEE/ACM Trans. Networking*, vol.8, no.4, pp.443-454, 2000.

[2] H. Bettahar, M. Alkubeily and A. Bouabdallah, TKS: A transition key management scheme for secure application level multicast, *International Journal of Security and Networks*, vol.4, no.4, p.210, 2009.

[3] D. Gollmann, F. Omara, S. Zaki and M. A. El Soud, Ancestors protocol for scalable key management, *Egyptian Informatics Journal*, vol.11, pp.11-17, 2010.

[4] K. Kumar, J. Begum and V. Sumathy, A novel approach towards cost effective region-based group key agreement protocol for ad hoc networks using elliptic curve cryptography, *IJCNS*, vol.3, no.4, pp.369-379, 2010.

[5] D. Macedonio and M. Merro, A semantic analysis of key management protocols for wireless sensor networks, *Science of Computer Programming*, vol.81, pp.53-78, 2014.

[6] J. Kar, Deniable authentication protocol based on integer factorization and discrete logarithm problems, *ICIC Express Letters*, vol.7, no.7, pp.2061-2067, 2013.

[7] M. R. Mishra, J. Kar and B. Majhi, Practical deployment of one-pass key establishment protocol on wireless sensor networks, *International Journal of Pure and Applied Mathematics*, vol.100, no.4, pp.531-542, 2015.

[8] P. Nose, Security weaknesses of a signature scheme and authenticated key agreement protocols, *Information Processing Letters*, vol.114, no.3, pp.107-115, 2014.

[9] J. Kar, ID-based deniable authentication protocol based on Diffie Hellman problem on elliptic curve, *International Journal of Network Security*, vol.15, no.5, pp.347-354, 2013.

[10] E. Makri and E. Konstantinou, Constant round group key agreement protocols: A comparative study, *Computers & Security*, vol.30, no.8, pp.643-678, 2011.

[11] R. Siva, D. Bhaskari and D. Avadhani, Current trends in group key management, *International Journal of Advanced Computer Science and Applications*, vol.2, no.11, 2011.

[12] H. Sun, B. He, C. Chen, T. Wu, C. Lin and H. Wang, A provable authenticated group key agreement protocol for mobile environment, *Information Sciences*, vol.321, pp.224-237, 2015.

[13] R. Seetha and R. Saravanan, A survey on group key management schemes, *Cybernetics and Information Technologies*, vol.15, no.3, 2015.

[14] R. Varalakshmi and V. Uthariaraj, Huddle hierarchy based group key management protocol using gray code, *Wireless Netw.*, vol.20, no.4, pp.695-704, 2013.

[15] H. H. Chu, L. Qiao and K. Nahrstedt, A secure multicast protocol with copyright protection, *ACM SIGCOMM Computer Communications Review*, vol.32, no.2, pp.42-60, 2002.

[16] D. M. Wallner, E. J. Harder and R. C. Agee, Key management for multicast: Issues and architectures, *Internet Draft*, Network Working Group, 1998.

[17] C. K. Wong, M. Gouda and S. S. Lam, Secure group communications using key graphs, *Proc. of ACM SIGCOMM*, 1998.

[18] D. A. McGrew and A. T. Sherman, Key establishment in large dynamic groups using one-way function trees, *Technical Report TR-0755*, World Academy of Science Engineering and Technology, 1998.

[19] M. Waldvogel, G. Caronni, D. Sun, N. Weiler and B. Plattner, The VersaKey framework: Versatile group key management, *IEEE Journal on Selected Areas in Communications (Special Issues on Middleware)*, vol.17, no.8, pp.1614-1631, 1999.
[20] G. H. Chiou and W. T. Chen, Secure broadcast using secure lock, *IEEE Trans. Software Engineering*, vol.15, no.8, pp.929-934, 1989.
[21] T. Hardjono, B. Cain and L. Monga, Intra-domain group key management for multicast security, *IETF Internet Draft*, 2000.
[22] S. Rafaeli and D. Hutchison, Hydra: A decentralized group key management, *The 11th IEEE International WETICE: Enterprise Security Workshop*, 2002.
[23] S. Mittra, Iolus: A framework for scalable secure multicasting, *Proc. of ACM SIGCOMM*, 1997.
[24] R. Molva and Pannetrat, Scalable multicast security in dynamic groups, *Proc. of the 6th ACM Conference on Computer and Communications Security*, Singapore, pp.101-112, 1999.
[25] S. Setia, S. Koussih, S. Jaodia and E. Harder, Kronos: A scalable group re-keying approach for secure multicast, *Proc. of IEEE Symposium on Security and Privacy*, 2000.
[26] Y. R. Yang, X. S. Li, X. B. Zhang and S. S. Lam, Reliable group re-keying: A performance analysis, *TR-01-21*, 2001.
[27] I. Ingemarson, D. Tang and C. Wong, A conference key distribution system, *IEEE Trans. Information Theory*, no.5, pp.714-720, 1982.
[28] L. Dondeti, S. Mukherjee and A. Samal, A distributed group key management scheme for secure many-to-many communication, *Technical Report PINTL-TR-207-99*, 1999.
[29] A. Fiat and M. Naor, Broadcast encryption, *CRYPTO'93, LNCS*, vol.773, pp.480-491, 1993.
[30] M. Burmester and Y. G. Desmedt, A secure and efficient conference key distribution system, *EUROCRYP'94, LNCS*, vol.950, pp.275-286, 1994.
[31] C. Boyd, On key agreement and conference key agreement, *Australasian Conference on Information Security and Privacy, LNCS*, pp.294-302, 1997.
[32] L. Lin, X. Li and Y. Cheng, HKM: A hybrid key management scheme for secure mobile multicast, *Proc. of Networking, Architecture, and Storage*, pp.109-114, 2007.
[33] S. Yan, W. Trappe and K. J. R. Liu, Topology-aware key management schemes for wireless multicast, *Proc. of IEEE Global Telecommunications Conference*, vol.3, pp.1471-1475, 2003.
[34] Y. Wang, P. D. Le and B. Srinivasan, Hybrid group key management scheme for secure wireless multicast, *Proc. of the 6th IEEE/ACIS International Conference on Computer and Information Science*, pp.346-351, 2007.
[35] M. Sandirigama, S. Akihiro and M. Noda, Simple and secure password authentication protocol, *IEICE Trans. Com.*, vol.E83-B, pp.1363-1365, 2000.
[36] M. Hajyvahabzadeh, E. Eidkhani, S. A. Mortazavi and A. N. Pour, A new group key management protocol using code for key calculation: CKC, *Proc. of Information Science and Applications (ICISA)*, pp.1-6, 2010.
[37] T. Hardjono and L. R. Dondeti, *Multicast and Group Security: Artech House*, 2003.
[38] C. Perkins, RFC3344: IP mobility support for IPv4, *IETF RFC*, 2002.
[39] L. M. Kiah and K. M. Martin, Host mobility protocol for secure group communication in wireless mobile environments, *Future Generation Communication and Networking (FGCN 2007)*, pp.100-107, 2007.
[40] M. Kellil, J. C. A. Olivereau and P. Janneteau, Rekeying in secure mobile multicast communications, *United States Patent Application Publications, US 2007/0143600 A1*, 2007.