Applied Research Frontiers

Ariviyal Publishing

Review Article

DOI: 10.36686/Ariviyal.ARF.2022.01.03.017

Appl. Res. Front., 2022, 1(3), 26-31.

A Review on Key Administration and Distribution in Secure Group Communications

B.T. Geetha,*[a] V. Perumal,[b] S. Hariharan[c] and A. Bhanuprasad[d]

[a]*Department of ECE-SIMATS, Saveetha School of Engineering, Chennai, India.*
[b]*Technical-Lead, GAD-A-GET Computers, Chennai, India.*
[c]*Professor, Vardhaman College of Engineering, India.*
[d]*Associate Professor, Vardhaman College of Engineering, India.*

***Corresponding author E-mail address**: dr.geetha.bt@gmail.com (B.T. Geetha)

ISSN: 2583-3065

Crossref

Publication details
Received: 22nd November 2022
Revised: 21st December 2022
Accepted: 21st December 2022
Published: 30th December 2022

Abstract: Group communication frameworks are utilized as a part of various web uses. In web, most cast has been utilized propitiously to offer a productive, greatest exertion output benefit from a source to a tremendous collection of recipients. Along these lines, accomplishing group communication (i.e., offering privacy, respectability and legitimacy of data conveyed between group individuals) will turn into a huge web planner issue. This paper introduces a broad summary of the literature relating the subject matter: prologue to key administration and distribution and describes the various discussions related to secure group communications also the disadvantages found in the current framework have been investigated and it can be represented with a procedure which is to be adopted during Key administration and distribution.

Keywords: MANET; Group Communication; Key Generation; key Distribution; key Administration

1. Introduction

Group communication (GC) has been progressively utilized as a dynamic communication approach for encouraging rising circumstances which needs packet transfer between one or many sources to numerous beneficiaries. The instable message path provides group key administration which is an essential basic unit for protecting bunch transmission, in the exceptional consideration.[1] Creation of group key administration and distribution in profoundly powerful situations especially in remote portable systems because of their innate attributes faces extra difficulties.

Necessities of Group key administration and Distribution:

A group key specialist requires meeting different conditions to accomplish security, proficiency,[2] and adaptability. These conditions are helpful also for looking at and contrasting different arrangements. Every model is recorded and briefly clarified as under

- Needs for Security includes Backward secrecy, Forward secrecy and Resistant to collusion.
- Needs for Efficiency includes Communication overhead, Computation overhead and Storage overhead.
- Quality of service requirements includes Service availability, Scalability and Dependability.[3]

A Mobile Ad hoc Network is a group of portable clients related by remote framework. A MANET is a parsimonious sorting out group of remote portable elements that build up an impermanent and changing remote system with no structure. MANETs are programmed arrangements with no focal specialist framework with determination obligations.[4] The entire versatile substance can have intra communication unequivocally, when in other's remote radio scope. They either communicate through one bounce or through a few jumps with the help of middle elements to enable providing information. An Ad-hoc hub should be some way or other, demoniacally find the element to which it can communicate exactly and how to approach the specific hub which it cannot reach. In such a system the station should have a specific end goal to allow a transmission. This sort of remote framework can be described as MANET.

Steering conventions in MANET commonly assume the hubs are honest and helpful. Be that as it may, an assailant might be going about as a switch during directing and disturbing the steering cycle. It can speak with any hub. The battery power can be depleted by a self-absorbed hub. Such inward attacks are more defenceless than outer attacks. Since MANET has no fixed framework and an exceptionally mind-boggling topology, observing of various assaults would be troublesome. In this way MANET is defenceless against attack.[5]

The remaining part of the paper is structured as follows. Key administration and distribution in GCs are discussed in Section 2. Secure Group communication is presented in Section 3. Finally, our proposed work and summarising the article in Sections 4 and 5 respectively.

2. Key Administration and Distribution

This segment depicts different procedures utilized in key administration and the distribution for a dynamic system, in the light of alternative points of view of value taken after by a talk that investigates the current approach and quality models.

2.1. Key Administration Protocol in Mobile Environments

Key administration protocol is the main security protocol which supports the group communication in mobile environment. The Key administration to protect Group Communications in Mobile environment.[29] KMGM accepts ASGK (a method which is decentralized with a free (TEK) Traffic Encryption Key)[6,7] as its most important grouping key administration method.

For administration of versatility of clients, every AKM (Area Key Manager) keeps up two records. A rundown of current individuals dwelling inside the region is denoted as ListM and rundown of the old nodes which are officially transferred to alternate zones is denoted as ListO. A member or an element 'mi' that wishes to join as another part, sends its demand to join its AKMi, the region key trough verifies the part and thereafter produces an individual symmetric key called MEK (Member Encryption Key) and offers it with part mi. Key Derivation Function (KDF) that can be a Pseudo Random Function (PRF) is used for producing the MEK, where the PRF is a blend of one way hash functions (MD5, SHA1, HMAC,…). The seeds of the Key determination function are the session keys shared by the area key manager along with the public key of the recently joined members. In addition, AKMi incorporates the member to the present posting ListMi. At the point where an associate member goes to other dwelling region in the same group from the current region, this bypasses the move demand to the supervisor of the meeting zone. The AKMj checks the legitimacy of the guest originating from the past region. In the event of success of the verification, the new zone key administrator AKMj adds the guest to the present part list ListMj and the past AKMi adds the take-off to the old part list ListOi. The (Key Encryption Key) KEK and TEK of the new area are conveyed to the guest since these keys are unique in relation to withdrew the region. Amid the leaving occasion, the TEKs, KEKs of the regions are revitalized along with other keys. At the point when a member leaves a zone, the other regions are clued-up regarding the exiting associate. Now the information about fresh KEK and TEK are conveyed to other remaining individuals from the region with leaving occasion happened ensured by the MEK of every member. The AKM discharges the old member list ListO. In different regions where the leaving member is seen in ListOt, a secure unicast message is used to send the new KEK and TEK. In the rest of the regions, a fresh TEK is sent by a multicast communication protected under KEK to the individuals living inside the zone.

2.2. High Dimensional Quantum Key Distribution

This method negotiates the likelihood of expanded secure-key rate and expands photon-data productivity. In this paper key-generation stage utilizes 15% framework effectiveness for the recipients. Key generation is a vital criterion for security concerns. The utilization of moderate key administration technique is confined to sensor hubs due to the accessibility of the constrained assets in that system.[8]

2.3. Group Key Administration System in Wireless Mobiles

A technique which is decentralized using a typical TEK and projected a grouping key administration conspires that encourages versatility in remote portable conditions utilizing a rundown as a major aspect of convention. In the convention, group key chiefs including DKM and AKMs, keep up a rundown of versatile individuals who have officially moved out to different regions. This rundown alluded to as Mob List, and used for monitoring versatile clients and additionally stay away from visit rekeying in a zone which cause interruptions in the communication, and reminds the IDs of the part who moves from the group in which they connected.

2.4. Hierarchical Key Administration System

In MANET, the group communication is secured by utilizing this key organization framework. In this plan the rekeying cost is reduced by managing the individuals effectively. The two-layer structure arranges the key administration plot. The small group in stage 1 is involves all the subgroup hubs. In the Sub group1, by keeping the data area in mind the additional group established in stage 2 is sorted out. In every small group L1, the hub having high weight esteem is chosen as Stage 1 bunch head.[10] Thus, hub having the most weight an incentive in each Stage 2 is chosen as Stage 2 group lead. The L1 lead gets the whole data for the hubs; it frames the L1-small group key utilizing the RSA, then, the L1 lead conveys the same key to each hub in the small group. Since small group L1 is separated into various L2 small groups, the leader of each L2 small group produces a L2GK key which appropriates it to the hubs dwelling inside its small group. On the off chance of another part planning to join a small group, it sends solicitations to the neighbouring hubs. The adjacent hubs advise the L2 head. Along these lines, the L2 make a beeline for the new part. The GKL2 is refreshed and conveyed among the individuals from the small group. In the event that a hub leaves the small group, it notifies the L2 small group lead. L2 make a beeline for the departure hub and recovers another L2GK key. At the point where the leaders of a small group leave the small group, new choice for picking new head occurs.

2.5. Key Administration in Topology Matching

In this plan[28] the key administration hierarchy is coordinated with the topology of the system along with the goal of the transportation of keying materials being confined and subsequently a decrease in the communication costs. The network of cellular involves BS, portable clients, and SH. The TMKM tree includes three key administration sub-trees. The hosts inside a region prohibited by each BS can be dealt by a user sub tree. The admin host uses the BS sub tree to show case the arrangement of keying resources among the BSs and SH. In the long run, the supervisor of a group builds up a SH sub tree to administer the SHs. Every cell keeps up a WTBR record which holds the details of the clients who left the cell after officially after claiming an arrangement of substantial keys. This is done for monitoring the versatile host and the key refreshing procedure. The group administrator keeps up these WTBRs records. At the point

when a client shifts starting with one area then onto the next zone, the accompanying event occurs:

- The left client is expelled from the client sub tree of the previous cell, after updating its information in the WTBR of the previous cell.
- On the off chance of client having already gone by the new cell, it is situated on the division of the sub tree that it once in the past had a place with. From the WTBR the client's data is wiped out ell. If not, the user sub tree which is currently updated branch is located for the user.
- With the likelihood of the client joining after the season of the last key refreshed as a result of any take-off from the new cell, the client's key subset is refreshed by the client join technique portrayed by Wald Vogel.[11]

Apart from this, the keys no need to bother about updation. The explanation is focused in this methodology keeping a versatile part from approaching data earlier to its new joining group in the current cell. At the point where a part withdraws the session, the whole keys subset is handled by the part and refreshes the substantial. WTBR records of all the cells have the take-off data which are needed to refresh the subset of exiting part's key as per the strategy created.[11] Individuals who have the key comparable with take-off part should be expelled from the record of WTBR.

2.6. Cell-based Decentralized Key Management

In Cell-based Decentralized Key Management (CDKM),[12] the group key chief is in charge of dealing with occasions that involves entry or departure. Client portability and monitoring the clients in every cell is overseen by the BS. So with this reason, every BS deal with an IST key tree, for its related clients inside the cell and for this reason have no need to update the group key supervisor on the portability of a part. CDKM partitions a whole group into different cell-based sub- groups. To enable dealing with the versatility of group clients, a client is marked with the area of PIC or AIC in every cell. At the point where a part moves from its current location to the other location, in the small group key tree, the moving part is marked by the present location BS as AIC. In the fresh cell, the BS searches for the landing part in the small group key tree. In the event of the part having already gone by the current cell, the condition of the moving part is modified to PIC from AIC by the BS in its IST. Besides, the status of the moving part which is situated at a lower level of small group key tree is marked as PIC. On the off chance that a moving part exits from the cluster meeting, the cluster key administrator refreshes the TEK and inform to all the BSs about the leaving node. All the comparing BSs that keeps the condition of the exiting part in their IST must refresh the corresponding keying resources and prone all individuals with a condition of AIC from the small group key tree to maintain a strategic distance from the measure of the key tree from unreasonably expanding.

2.7. Group Key Administration in MANET

A decentralized model was taken up to set up a protected cluster communication in MANET.[13] The absence of a static foundation in MANET, which goes about as an area supervisor in the wired systems gave rise to the production of a weight-based plan with a specific goal to choose a zone chief for every region.

The weight factors for each node incorporate versatility, battery control level, and a topographical position. The plan has two stages; AKM choice, and the age and conveyance of the meeting key. A group that is managed by a station named the "group lead" is sorted out by the stations. The most extreme bounce between the group lead and the customary stations is one. A pioneer race algorithm is used to choose DKM, which also chooses an AKM with the most prominent cost. Rather than picking a DKM, a key understanding, for example, the one created is utilized by the AKMs keeping in mind the end goal to produce a typical traffic key. Group events incorporating joining and leaving in every region are overseen by the LKH inside every region, while hub versatility is taken care of by conventions, for example, SR, DR, or PR.

2.8. Key Tree in Mobile Multicast

In the KTMM technique,[14] the key administration tree is coordinated to the versatile IP organize topology. In this plan, the coherent key pecking order has a static degree at the transitional key hub level and a shifting degree at the client level. The most reduced level of the key tree relates to the association of BS with the portable individuals in the remote cell. In the key tree the least transitional key is linked with every BS. As it were, this most reduced key hub is the small group key which is collectively used by the BS and the portable individuals in every remote cell. At the point where a versatile part moves to another region, the BS of new zone confirms entry part where the checking of the part is effective, the subdivision key called transitional key in the key tree officially allocated to the current BS and it is shown to the portable part. In the interim, the key tree is changed by the group key administrator.

2.9. Wireless Subgroup in Mobile Multicast (WSMM)

The WSMM,[14] oversees isolate wired and remote regions. It sorts out the group individuals into various small groups that are overseen by BS in every remote cell. The BSs are in charge of producing and dealing with the entering materials in their remote cells. Keys of two sorts are utilized for information transmission with a wired cluster key and a remote subdivision key. This key is the foundation for the legitimate key order, where the BS is situated at the bottom level of the tree. The remote key in every small group is created by the corresponding BS, and communicated among the individuals from the subdivision. Subsequently every subdivision has its individual explicit remote key, the information transferred to all the cells are interpreted at the bottom level of every cell by the corresponding BS. Considering the portability, the WSMM take-off from the old region and join at the new region. Thus, whenever a dynamic host moved from one area to other area, the part confirmation succeeds the BS creates another unique key for the fresh zone. In this way BS in the old zone creates another small group key and spreads it to the rest of the individuals in its region.

2.10. Subgroups Hierarchical Key Administration

SHKA[15] is a decentralized plan that practices the free TEK model where the small groups are prearranged into a various levelled

structure in a mixed manner. The necessities of group leads are more noticeable than those of the local customers and defined by the degree of positions where they join. Also, clients related to higher need associated groups are equipped for inferring the key of lower need subgroups. However, a contrary action is not performed. The sending substances in the multicast communiqué embrace the duty of subdivision administration. Meanwhile the sending elements have various levels; the antecedent elements can derive the traffic keys of the descendant substances. In this plan, the traffic key of every associated group is created inside the associated group in a random manner to the trusted with answer to CA which at that point figures a parameter for any two forerunner and descendant subgroups. This scheme adopts the FEDRP protocol to manage the user mobility. On the off chance of a part moving from the present associated group to the new associated group, the old chief does not do any instant play out a rekeying strategy.

In the event of the entering part having just gone to the new associated group, it gets the new associated group activity key via unicast information. Besides, another TEK is made by the associated group administrator and answer to the CA. In agreement to the gained data, then the CA re-evaluates the constraints. Every administrator saves a list of individuals that keeps the legitimate movement key while being external to the associated group. Then the list is rearranged during a part with the departure of a substantial TEK from the group or the lapse of the clock. Numerous specialists have talked about different issues and methodologies display in secure group communication.

3. Secure Group Communication

The following Table 1 describes the various discussions related to secure group communications.

Table 1. Various Discussions Related to Secure Group Communication

Author Name	Description of Discussion
Wang *et al*. (2013)[16]	The Wireless sensor systems (WSNs) are often conveyed in forceful circumstances making such systems amazingly helpless in raising the threat of assaults close to this sort of framework.
Yang & Vaidya (2004)[17]	Energy is a noteworthy factor in WSNs. Hence, most specialists are worried about routing protocols and the energy Effectiveness factor.
Das *et al*.(2010)[18]	At first, consideration in current conventions was more on Quality of Service (QoS), transfer speed, packet conveyance, and dependability Variables and thoughtfulness regarding the energy issue was less.
Rashmi Gupta et al (2015)[19]	In MANET hubs are worked through battery, as battery power or battery energy is constrained asset along these lines it requires uncommon thoughtfulness regarding limit energy utilization in MANET. For MANETs, advancing the power utilization has a massive effect as it straightforwardly influences the lifetime of systems.
Sukla Banerjee (2008)[20]	Proposed a process to deal with shielding the portable impromptu system from a grey hole and a black hole attack assault. They have provided a system to find collaborating vindictive hubs, which drop a huge portion of packets.
Sathiaseelan and Crowcroft (2012)[21]	There has been a lively advancement of remote communication and compact figuring gadgets emerging from significant mechanical enhancements for communication foundation, execution, and registering power. Moreover, Internet innovation has gotten the amazing advances amid the most recent couple of years.
Cisco Visual Networking Index (2013)[22]	Worldwide versatile information movement will achieve 1.4 zeta bytes for every year by 2017, which may give encouragement and enthusiasm to the improvement of new cluster base administrations and applications like intuitive group recreations, interactive media conferencing, Internet convention Tv (IP-Tv), broadcasting stock statements, video on request, and social group systems.
Martin and Haberman (2008)[23]	Individuals can have transparent and secret joining of the group because of the attributes of such communication. Along these lines, guaranteeing the protection of cluster base apps is no minor issues while the absence of protection in such apps, occurring in an open system over extensive way (i.e. Web) renders them more helpless to various assaults.
Sakarindr and Ansari (2010)[24]	Contingent upon application necessities, essential security administrations like information trustworthiness, confidentiality, and element validation should be up to guarantee reverse and forward secret, and also the honesty of group individuals and group operations. These administrations, more specifically in reverse and forward secret can be set up by sharing general keys. The TEK is then used to scramble all movement identified with a specific cluster and just individuals from the cluster who claim the TEK are fit for unscrambling the received messages.

Baugher *et al*. (2005)[25]	Group key administration is a major dispute seen in outlining a solid and secure cluster communication plot. The augmentation of cluster communication to the remote versatile condition stays troublesome and complex in key administration conventions.
Shin *et al*. (2013)[26]	Remote gadgets regularly experience the ill effects of such essential imperatives as data transfer capacity constraints, low algorithm power, and low stockpiling limit. Moreover, such gadgets can move start moving with one region of a system then onto the next one, henceforth part versatility are taken into account as an extra constraint in the outline of protected data transfer.
Koodli (2009)[27]	Client versatility muddles aggregate key administration in portable conditions because of this administration deals with active group enrolments and dynamic part areas.

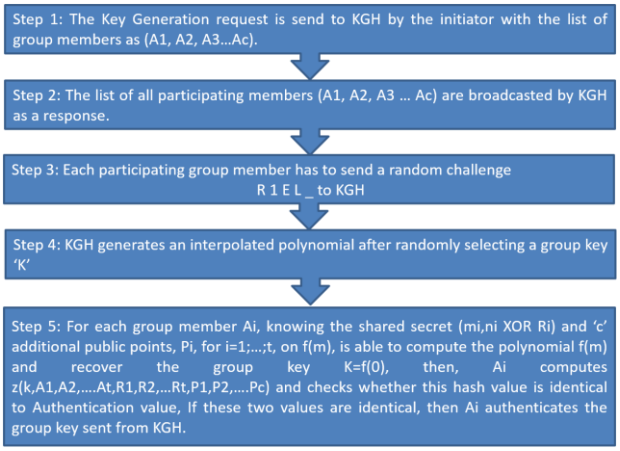

Fig. 1. Procedure for generating the key and distribution

4. Proposed Work

The survey of relevant literature discussed above displays the issues in the data broadcasting in wireless systems condition. The audit talked about in insight with respect to the different procedures utilized as a part of key administration and distribution in secure group communication.

The disadvantages found in the current framework have been investigated to enable getting answers for the same and it can be depicted as Key administration and distribution and the information encryption process. The key generation portrays the initialization of KGH, node registration process and the process of key distribution and encryption. Information encryption process portrays the skills of the current technology and its issues. The sequence of steps involved in the proposed key generation and distribution process are represented in the below Fig. 1.

5. Conclusions

The survey of relevant literature displays the issues in the data broadcasting in wireless systems condition. The audit talked about in insight with respect to the different procedures utilized as a part of key administration and encryption among broadcasting. Diverse key administration methods have been examined. At last different research tables are given in this section in light of various methodologies.

Conflicts of Interest

The authors declare no conflict of interest.

References

1 Daghighi B.; Kiah M.L.M.; Shamshirband S.; Rehman M.H.U. toward Secure Group Communication in Wireless Mobile Environments: Issues, Solutions, and Challenges. *J. Netw. Comput. Appl*., 2015, **50**, 1-14. [CrossRef]
2 Sakarindr P.; Ansari N. Survey of Security Services on Group Communications. *IET Inf. Secur*., 2010, **4**, 258-272. [CrossRef]
3 Geetha B.T.; Srinath M.V. August. A Study on Various Cryptographic Key Management and Distribution System in Secure Multicast Communications. In 2012 *International Conference on Advances in Mobile Network, Communication and Its Applications*. IEEE, 2012, 64-69. [CrossRef]
4 Wang N.C.; Fang S.Z. A Hierarchical Key Management Scheme for Secure Group Communications in Mobile ad hoc Networks. *J. Syst. Softw*., 2007, **80**, 1667-1677. [CrossRef]
5 Sekar S. Key Management Schemes in MANET-A Detailed Review. 2020, **8**, 62-67. [Link]
6 Gharout S.; Bouabdallah A.; Challal Y.; Achemlal M. Adaptive Group Key Management Protocol for Wireless Communications. *J. Univers. Comput. Sci*., 2012, **18**, 874-899. [Link]
7 Challal Y.; Gharout S.; Bouabdallah A.; Bettahar H. Adaptive Clustering for Scalable Key Management in Dynamic Group Communications. *Int. J. Secur. Netw*., 2008, **3**, 133-146. [CrossRef]
8 Chen C.Y.; Chao H.C. A Survey of Key Distribution in Wireless Sensor Networks. *Secur. Commun. Netw*., 2014, **7**, 2495-2508. [CrossRef]
9 Kiah M.L.M.; Martin K.M. December. Host Mobility Protocol for Secure Group Communication in Wireless Mobile Environments. *Future Gener. Commun. Netw*., (*FGCN 2007*). IEEE, 2007, **1**, 100-107. [CrossRef]
10 Dhurandher S.K.; Singh G.V. January. Weight based Adaptive Clustering in Wireless Ad hoc Networks. In *2005 IEEE International Conference on Personal Wireless Communications*, 2005. ICPWC 2005. IEEE, 2005, 95-100. [CrossRef]
11 Waldvogel M.; Caronni G.; Sun D.; Weiler N.; Plattner B. The VersaKey Framework: Versatile Group Key Management. *IEEE J. Sel. Areas Commun*., 1999, **17**, 1614-1631. [CrossRef]
12 Park M.H.; Park Y.H.; Seo S.W. May. A Cell-Based Decentralized Key Management Scheme for Secure Multicast in Mobile Cellular Networks. In *2010 IEEE 71st Vehicular Technology Conference*. IEEE, 2010, 1-6. [CrossRef]
13 Hernandez-Serrano J.; Pegueroles J.; Soriano M. May. GKM over large MANET. In *Sixth International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing and First ACIS International Workshop on Self-Assembling Wireless Network*. IEEE, 2005, 484-490. [CrossRef]
14 Roh J.H.; Lee K.H. Key Management Scheme for Providing the Confidentiality in Mobile Multicast. In *2006 8th International Conference Advanced Communication Technology*. IEEE, 2006, **2**. [CrossRef]
15 Cao J.; Liao L.; Wang G. Scalable Key Management for Secure Multicast Communication in the Mobile Environment. *Pervasive Mob. Comput*., 2006, **2**, 187-203. [CrossRef]

16 Diop A.; Qi Y.; Wang Q.; Hussain S. An Advanced Survey on Secure Energy-Efficient Hierarchical Routing Protocols in Wireless Sensor Networks. *arXiv preprint arXiv:1306.4595*, 2013. [CrossRef]
17 Yang X.; Vaidya N.H. A Wakeup Scheme for Sensor Networks: Achieving Balance between Energy Saving and End-to-End Delay. In *Proceedings. RTAS 2004. 10th IEEE Real-Time and Embedded Technology and Applications Symposium*, 2004, 19-26. [CrossRef]
18 Das B.; Das S.; Das C. Efficacy of Multiband OFDM Approach in High Data Rate Ultra Wideband WPAN Physical Layer Standard using Realistic Channel Models. *Int. J. Comput. Appl*., 2010, **2**, 81-87. [CrossRef]
19 Velayutham R. A Survey on Routing Protocols of MANET in Wireless Sensor Network. *Int. J. Res. Soc. Sci*., 2017, **7**, 539-561. [Link]
20 Banerjee S. October. Detection/Removal of Cooperative Black and Gray Hole Attack in Mobile Ad-Hoc Networks. In *proceedings of the world congress on engineering and computer science*. 2008. [Link]
21 Sathiaseelan A.; Crowcroft J. Internet on the Move: Challenges and Solutions. *ACM SIGCOMM Comput. Commun. Rev*., 2012, **43**, 51-55. [CrossRef]
22 Cisco Visual Networking Index. The Zettabyte Era—Trends and Analysis. *White paper*. 2020.
23 Haberman B.; Martin J. *Internet Group Management Protocol Version 3 (IGMPv3)/Multicast Listener Discovery Version 2 (MLDv2) and Multicast Routing Protocol Interaction* (No. rfc5186). 2008. [Link]
24 Sakarindr P.; Ansari N. Security Services in Group Communications over Wireless Infrastructure, Mobile Ad Hoc, and Wireless Sensor Networks. *IEEE Wireless Commun*., 2007, **14**, 8-20. [CrossRef]
25 Baugher M.; Canetti R.; Dondeti L.; Lindholm F. *Multicast Security (MSEC) Group Key Management Architecture* (No. rfc4046). 2005. [Link]
26 Shin Y.; Choi M.; Koo J.; Choi S. Video Multicast over WLANs: Power Saving and Reliability Perspectives. *IEEE Netw.*, 2013, **27**, 40-46. [CrossRef]
27 Koodli R. *Mobile IPv6 Fast Handovers* (No. rfc5568). 2009. [Link]
28 Sun Y.; Trappe W.; Liu K.R. A Scalable Multicast Key Management Scheme for Heterogeneous Wireless Networks. *IEEE/ACM Trans. Netw*., 2004, **12**, 653-666. [CrossRef]
29 Bouassida M.S.; Chrisment I.; Festor O. Group Key Management in MANETs. *Int. J. Netw. Secur*., 2008, **6**, 67-79. [Link]