International Journal of Future Generation Communication and Networking
Vol. 9, No. 2 (2016), pp. 123-132
http://dx.doi.org/10.14257/ijfgcn.2016.9.2.13

Address Management in IPv6 Network

Dr. Subbulakshmi T[1] and Ankit Jain[2]

[1]*Prof. in Department of Computer Science and Engineering*
VIT University, Chennai,
Tamilnadu, India
[2]*Department of Computer Science and Engineering*
VIT University, Chennai,
Tamilnadu, India
[1]*research.subbulakshmi@gmail.com*, [2]*ankit.jain2014mcs1050@vit.ac.in*

Abstract

In this we tend to use a plan of Subnetting for sophistication 'C' address to scale back the address area. We tend to purposed "Aggregate Variable Length Subnet Masking exploitation IP4" with the assistance of fastened Length Subnet Masking, Variable Length Subnet Masking and combination fastened length Subnet Masking. scientific discipline Addresses are at a premium, therefore we tend to minimize the whole scientific discipline usages. Here, we tend to ar operating with the Cisco Packet Tracer and introduced the management of address area and key management in IPv6 network.

In unicast and multicast IPv6 networks key management is one among the key security problems. To realize secure communications in such networks reliable and competent key management theme ought to be obligatory and enforced, Whenever a brand new node is accepted to affix or leave the network, a brand new key ought to be generated and distributed to each nodes within the multicast group. Inadequately, this approach will increase the amount of keys transmitted (communication cost) of the key management, whereas variety of algorithms has been projected to handle this issue, most of them have severely affected the computation price (i.e., range of key coding, decryption, and derivation) of the key management. By concentrating on communication and computation prices, we tend to provide prominence to the chance of addressing the each prices while not having to sacrifice one for the sake of the opposite. during this paper, we tend to propose a light-weight key management theme for IPv6 networks, that is capable of reducing each communication and computation prices. The performance analysis demonstrates the potency of our projected methodology as compared with the present ones in reducing such prices, whereas at identical time maintaining each forward and backward securities.

Keywords: *Address Management, Multicast Securities, Group Communication, Multicast-Unicast IPv6 Network*

1. Introduction

The precipitate exposure of recent access technologies and web applications has affected the explosive growth within the variety of mobile and web users. due to this evergrowing variety of web users, a brand new suite of protocol known as web Protocol version vi (IPv6) has been originated to substitute the standard web Protocol version four (IPv4). IPv6 is ready to produce a bigger address house, that is ready to support the large variety of existing web users furthermore because the rising ones.

As the web moves forward into future century, it'll become AN data infrastructure for everybody, not only for scientists or professionals. This suggests that the next-generation web should win the following options.

ISSN: 2233-7857 IJFGCN

- Internet for everybody
- Internet for everything
- Internet all over
- Internet at any time
- Internet any means

IPv6 uses a 128-bit address, permitting 2128, or roughly three.4×1038 addresses, or quite seven.9×1028 times as several as IPv4, that uses 32-bit addresses and provides roughly four.3 billion addresses. The 2 protocols aren't designed to be practical.

In lightweight of this, this paper proposes a light-weight redistributed key management theme known as multicast-unicast key management technique (MUKM), This MUKM reduces the communication and computation prices of key change in IPv6 networks, whereas at constant time facilitating each forward and backward security to the key management[1] In such a redistributed theme, the key management method like key coding, decryption, and key update square measure handled by subgroup managers. with regard to knowledge transmission, the key tree of the planned MUKM technique is structured into 2 distinct levels, namely, multicast level and unicast level. Here, knowledge (or packets) square measure multicast from the foundation to the subgroup managers, whereas transmission of knowledge from these subgroup managers to the tip users is predicated on the unicast addressing technique. It ought to be noted that the key management problems square measure thought of during this paper, whereas the info transmission problems had been mentioned in this.

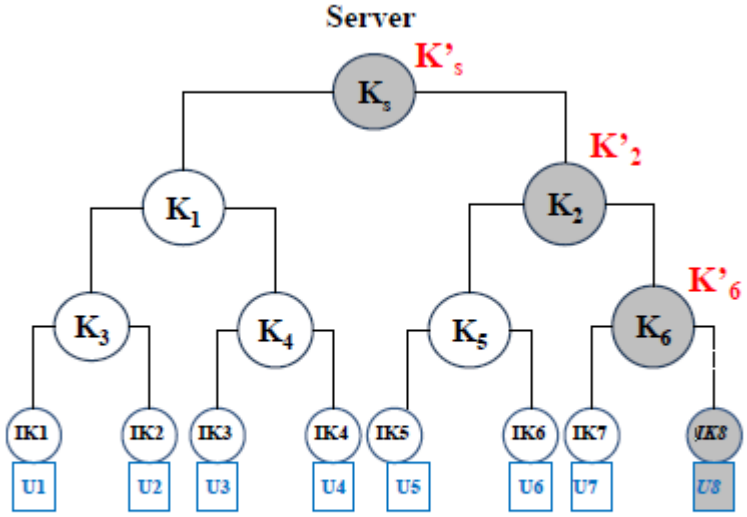


Fig. 1. A typical key tree.

The remainder of this paper is organized as follows. Section 2 places a stress on a typical re-keying procedure, then provides an outline of existing literature on key management theme, The theoretical framework of our projected MUKM is given in Section 3. Finally, the performance analysis of the projected theme is mentioned in Section IV, ending by some last remarks.

2. Management Scheme

A vast quantity of literature on key management has been reported , that falls below a centralized key management strategy. This section doesn't aim at addressing all connected works for the aforesaid strategy, however solely that that is very important and closely

associated with our work. First, a typical cluster rekeying procedure is given, Then a quick outline of 2 existing centralized key management schemes is given, namely, Logical Key Hierarchy (LKH) and unidirectional operate Trees (OFT).

A. Typical cluster Rekeying Procedure

In regards to typical cluster rekeying procedure, be part of and leave operations of nodes in IPv6 networks area unit mentioned supported the subsequent example of a key tree, as illustrated in Figure 1, allow us to assume that there area unit nine users (P1–P9) during a 4-tier key tree, wherever the basis (or server) possesses the server key (denoted as Rs) and intermediate youngsters nodes possess a alleged key coding keys, denoted as R1, R2, R3, R4, R5, R6 and R7. every user within the key tree is allotted a personal Key (IK) for decrypting these key coding keys. Suppose that a replacement user, say user nine (P9) desires to hitch the cluster. in step with a typical cluster rekeying procedure, all the keys on the trail from P9 to the basis should be modified, and also the new generated keys ought to be distributed to alternative members of the key tree. In light-weight of this, Rs, R2, and R6 area unit modified to the new keys R's, R'2, and R'6, respectively. The notation

$Q \rightarrow R(j)$

denotes server alphabetic character sends message j to user P and (R's,Rs) message means R's is encrypted with Rs. The image || is employed to denote concatenation of messages. The on top of mentioned be part of operation is delineated as follows.

1. P9 ! alphabetic character (join)
2. alphabetic character authenticates P9
3. alphabetic character ! P9 (IK8)
4. alphabetic character creates new arbitrarily key R's, R'2 and R'6
5. alphabetic character ! P1–P8 (R's,Rs)
6. alphabetic character ! P6–P9 (R'2,R2)
7. alphabetic character ! P8 (R'7,R7)
8. alphabetic character ! P9 (R'7,IK9) kk (R'2,R'6) kk (R's,R'2)

Whenever P9 is granted to hitch the cluster, the new keys R's, R'2 and R'6 area unit generated, then area unit distributed to alternative members supported the be part of operation explained on top of, lets assume that P9 is granted to go away the group, a collection of latest keys has got to be generated and distributed to alternative members.

Such a leave operation is delineated as follows.
1. P9 ! alphabetic character (leave)
2. alphabetic character ! P9 (Accept)
3. S creates new arbitrarily key R's, R'2 and R'6
4. alphabetic character ! P1–P4 (R's,R1)
5. alphabetic character ! P5–P6 (R'2,R5) kk (R's,R'2)
6. alphabetic character ! P7 (R'6,IK8) kk (R'2,R'6) kk (R's,R'2)

B. Logical Key Hierarchy Protocol

Harney and more durable introduce the LKH protocol, that defines a Compromise Recovery (CR) theme for cluster key management. during this theme, a metal manager is that the high member of a key tree. The second tier of the key tree nodes area unit known as CR agents whereas the third tier is often occupied by the top users (or members). Specifically, an outsized cluster light-emitting diode by a metal manager is divided into many subgroups supported key tree hierarchy, once a replacement node arrives (*i.e.*, be part of operation), the key change operation affects solely the nodes on the trail from the basis (*i.e.*, metal manager) to the members, In such a situation, the metal manager creates a replacement key, and

afterward send a message to the actual metal agent along with the new generated key to update its domain. Note that similar description applies to a leave operation, within which a node departs from the cluster.

The number of keys transmitted by the metal manager depends on the peak (h) of the d-ary tree. during a d-ary tree, every node is connected to d youngsters, during this theme, once a node joins the cluster, the new generated key is disseminated to the present members and also the new node either by exploitation multicast or unicast, Hence, the quantity of needed key (*i.e.*, communication key) by multicast and unicast area unit adequate to 2h and h, severally. On the opposite hand, once a leave operation happens, d ∗ h variety of keys got to be generated by the metal manager and these new keys area unit sent to its members via multicast. With reference to computation price, we've got to think about the value for the metal manager and also the members. Here, every member needs solely h decipherment for be part of or leave operation, whereas the metal manager has got to perform coding and random key generation, that depends on the peak of the key tree, From these derivations, it is deduced that the LKH suffers from [1]high communication price. In LKH, whenever a node joins or leaves its cluster, all the cluster members has got to be updated. This situation can even be referred ICC'14 - W13: Workshop on Cooperative and psychological feature Mobile Networks 350 to as 1-affect-n drawback, wherever any action by one node can have a control to the complete member of the cluster.

C. Unidirectional operate Trees Protocol (OFT)

The ofttimes protocol may be a ascendible centralized bottom-up key management theme planned by Sherman and McGrew [14]. during this theme, the key generation and change method area unit enforced from very cheap of the key tree to the highest, in contrast with the LKH that may be a top-down key management theme, Moreover, the sort of tree is binary wherever every intermediate node has specifically 2 youngsters (d = 2), Since the key derivation is handled from members to the basis, the quantity of re-keying operations for n members is reduced to lg n. In general, 3 actions have to be compelled to be enforced to derive the new key,

(i) shared key institution
(ii) key tree creation
(iii) cluster key computation.

The shared-key institution happens between every member and also the server, whereas the ofttimes tree creation is entirely handled by the server, cluster key's then computed by the members rather than receiving it from the server. Whenever a node arrives to the cluster (or departs the group), the server has got to inform its members concerning the changes of the key tree. For this reason, the server sends a so called “change information” (in the shape of management message) to the actual affected members to update themselves and computes the new key whereas change itself.

Given its bottom-up paradigm, the communication price in ofttimes is a smaller amount than the LKH. specially, OFT’s communication price is adequate to the peak (h) of the tree. notwithstanding, so as to keep up its security level, ofttimes has got to increase its coding, decryption, and re-keying method, and thus suffers from an outsized computation price, In alternative words, by reducing the quantity of transmitted keys within the key management method, the complexness associate degreed computation time of an update area unit augmented throughout a be part of and leave operations. during a be part of operation, the new member performs decipherment of latest keys whereas the present members have to be compelled to implement each key decipherment and key derivation, Meanwhile, the server has got to perform key coding, key derivation, and random key generation throughout be part of operation, and has got to implement key coding and key derivation whenever leave operation happens.

One of the most problems with ofttimes is that the transmission of the "change information". 1st of all, the broadcasting nature of the "change information" in ofttimes may be a crucial issue in IPv6 networks because it isn't supported by the latter, and thus it ought to get replaced by multicasting, therefore the computation price of members for be part of or leave operations is incredibly high, particularly once there's a high quality or frequent changes within the key tree, In fact, if the "change information" is lost, members don't seem to be ready to decipher the transmitted knowledge, and thus a major size of buffer is required to store the encrypted knowledge (*i.e.*, forward the "change information" are going to be received at later stage). Another issue that has to be thought-about is that the incorrect computation of latest cluster key thanks to the lost of "change information" update message, in addition as receiving out-of-sequence update message.

For the advantage of the readers, the whole derivation of the on top of mentioned communication and computation prices for each LKH and oft times area unit summarized in Table I.

3. Proposed Multicast and Unicast Scheme

MULTICAST – The unicast-based multicast emulation that's the overall resolution within the existing web setting might not be numerically ascendible for multicast capability. Multicasting, the transmission of a packet to multiple destinations in an exceedingly single send operation, is an element of the bottom specification in IPv6. In IPv4 this is often associate degree elective though normally enforced feature. IPv6 multicast addressing shares common options and protocols with IPv4 multicast, however additionally provides changes and enhancements by eliminating the necessity surely protocols. IPv6 doesn't implement ancient IP broadcast i.e. the transmission of a packet to all or any hosts on the connected link employing a special broadcast address, and so doesn't outline broadcast addresses. In IPv6, an equivalent result are often achieved by causing a packet to the link-local all nodes multicast cluster at address "ef02::1", that is analogous to IPv4 multicast to deal with "192.10.2.1". IPv6 additionally provides for brand new multicast implementations, as well as embedding rendezvous purpose addresses in associate degree IPv6 multicast cluster address, that simplifies the preparation of inter-domain solutions.

In IPv4 it's terribly troublesome for a corporation to urge even one globally routable multicast cluster assignment, and therefore the implementation of inter-domain solutions is esoteric. Unicast address assignments by a neighborhood web written record for IPv6 have a minimum of a 64-bit routing prefix, yielding the tiniest subnet size obtainable in IPv6 (also sixty four bits). With such associate degree assignment it's doable to introduce the unicast address prefix into the IPv6 multicast address format, whereas still providing a 32-bit block, the smallest amount vital bits of the address, or some four.2 billion multicast cluster identifiers. So every user of associate degree IPv6 subnet mechanically has obtainable a group of worldwide routable source-specific multicast teams for multicast applications.

Our projected multicast-unicast key management methodology (MUKM) disseminates its numerous key management processes, *i.e.*, encryption, decryption, key generation, and key update to network subgroups, in an exceedingly extremely dynamic setting, dividing a bunch into subgroups will considerably cut back the communication and computation prices of the rekeying method, in order that in such a localized approach, a bunch is split intoseveral subgroups that square measure administered by their several subgroup managers. This approach solves many issues experienced by the centralized one, like circumventing one purpose of vulnerability downside, also as avoiding the antecedently mentioned 1-affect-n issue. Moreover, this approach is ready to cut back each communication and computation prices of the key management of IPv6 networks. Specifically, whenever a be a part of or leave operation happens, as a result of its localized paradigm solely a subgroup are going to be affected.

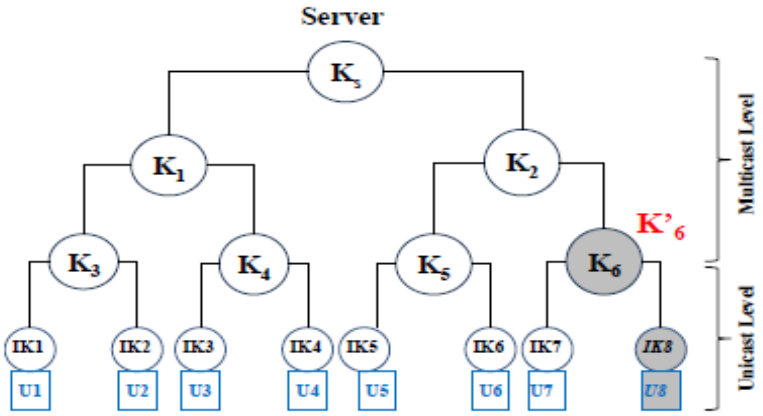


Fig. 2. Join and leave operations of the proposed MUKM.

In our planned theme, the key update method (*i.e.*, because of be part of and leave operations) is explained supported the key tree illustrated in Figure 2. during this example, Rs is that the root with six intermediate nodes. User nine (P9) requests to affix and so leave the cluster connected to the R6 subgroup, R6 is accountable to assign a brand new key to P9. It re-encrypts the multicast packets, *i.e.*, antecedently received from the basis, and so forwards them as unicast packet to the mack address of its members. the choice of mack address rather than information science address is especially for achieving the end-to-end multicasting, By bypassing the process of layer three and on top of, packets forwarded to finish users supported their mack address is transmitted quicker than the conventional forwarding multicast packet.

The be part of operation of our planned MUKM is delineated as follows.
1. P9 ! R6 ! Q (join)
2. R6 keeps the P9 be part of record
3. Q authenticates UP9
4. Q informs R6
5. R6 updates routing table by adding P9 mack address
6. R6 ! P9 (IK9) //via mack address
7. R6 ! P8–P9 (R'6, IK8–IK9) //via mack

Assuming that P9 sends asking to affix the cluster, and R'6 is that the new traffic coding key, Note that P9 doesn't have access to Rs, R2, R6, so this theme is ready to attain backward security then R6 re-encrypts the information science packets and sends them to any or all members within the subgroup supported their mack address. Similar description applies to a leave operation. the subsequent codes represent the leave operation of our planned MUKM.
1. P9 ! R6 ! Q (leave)
2. R6 keeps the P9 leave record
3. Q ! R6 ! P9 (accept)
4. R6 updates routing table by deleting P9 mack address
5. R6 ! P8 (R'6,IK8)

In leave operation, P9 sends a leave request to R6, that is accountable to forward the request to Q, Whenever a leave operation is granted by a network user, the R6 updates its routing table, and so generates a brand new R'6 key for the prevailing members, during this leave operation, P9 doesn't have access to the R'6 any longer, so the planned theme achieves forward security. so as to make sure the forward security, R6 should not be used for future

sessions. Besides achieving each backward and forward security, the planned MUKM can also address the mounted interest rate downside in IPv6 networks.

In comparison with the prevailing schemes mentioned in Section II, the amount of coding and secret writing, and also the range of keys for change its cluster members square measure considerably reduced, Since the network is split into 2 distinct levels, the machine complexness and communication prices square measure confined to individual subgroups rather than the complete network. As a signal of thought, we tend to compare our planned MUKM with 2 existing key management schemes, LKH and OFT, within the next section.

4. Performance Evaluation

In this section, we have a tendency to value and validate the effectiveness of the planned MUKM theme supported 2 overhead parameters, namely, communication value and computation value, The communication value is remarked because the variety of keys transmitted by a node to perform key update operation, On the opposite hand, the computation value is outlined because the variety of key secret writing, decryption, derivation, and random generation within the key management procedure.

Assuming that E, D, F, and R ar the price of secret writing, decryption, key derivation and random key generation, severally, allow us to denote B because the key length in bits, h because the height of tree, and n because the variety of users, As shown in Table I, the communication value of a be part of operation for MUKM is B notwithstanding its key delivery technique, i.e., whether or not the new key's multicast or unicast to the members. In our theme solely one key's needed to be sent to the new member.

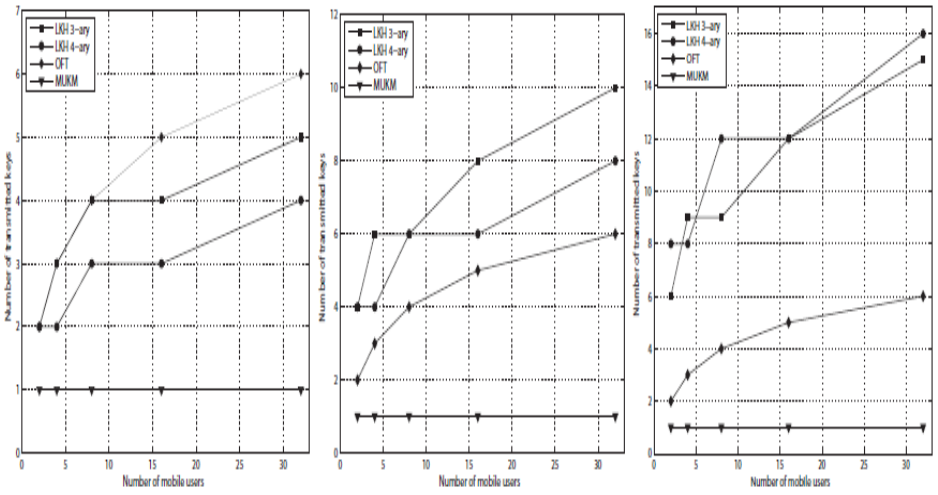
Therefore, it achieves a superior performance in terms of communication value because it reduces the quantity of transmitted keys compared to LKH and frequently schemes, Regarding the computation value at the server, one key secret writing and one key decipherment ar required for a be part of operation. Meanwhile, upon receiving the new key from the server, the prevailing members and also the new member need to perform solely one decipherment method to scan (or decrypt) the key, on the opposite hand, for LKH and frequently, the computation value depends on each the peak of the tree (*i.e.*, h) in addition because the variety of youngsters at intermediate nodes, denoted by this paper as d, here we have a tendency to contemplate a binary tree (*i.e.*, d = 2) for frequently and d-ary tree for LKH (d = three and d = 4), moreover, the frequently conjointly has got to contemplate the computation value of key derivation method, therefore, it's obvious that the OFT has the worst performance in terms of computation value.

As are often seen in Table I, the communication and computation value of be part of and leave operations ar considerably reduced in MUKM as compared to LKH and frequently, supported these derivations, we have a tendency to perform AN analytical analysis to demonstrate the superiority of the planned MUKM theme over each LKH and frequently here, h is adequate to ⌈logd n⌉. In our performance analysis, a most variety of 32 members is taken into account for each theme. will be} chiefly as a result of a typical access purpose can solely handle regarding thirty mobile users at a selected times.

Figures 3(a) and 3(b) illustrate the communication value of be part of operation for LKH, frequently and MUKM for each unicast and multicast approaches, severally. As are often seen, notwithstanding the addressing approach, MUKM has rock bottom communication value as compared to each LKH and frequently, for frequently and MUKM, the quantity of transmitted keys is comparable for each multicast and unicast, yet, for LKH the price of the multicast is beyond the unicast, and also the 4-ary tree includes a lower communication value compared to the 3-ary tree. As the number of users will increase, the communication value for each LKH and frequently conjointly will increase, whereas the communication overhead for MUKM isn't stricken by the quantity of users, similarly, the communication value of leave operation for each

TABLE I
COMPARISON OF COMMUNICATION AND COMPUTATION COSTS FOR JOIN OPERATION.

	Parameter		LKH	OFT	MUKM
JOIN	Communication Cost	Multicast	$2hB$	hB	B
		Unicast	hB	hB	B
	Computation Cost	Server	$h(2E+R)$	$h(2E+2F)+2R$	$E+R$
		Old member	hD	$h(D+F)$	D
		New member	hD	hD	D
	Parameter		LKH	OFT	MUKM
LEAVE	Communication Cost	Multicast	dhB	hB	B
	Computation Cost	Server	$h(dE+R)$	$h(E+2F)$	$E+R$
		Member	hD	$h(D+F)$	D



(a) Join operation - unicast approach. (b) Join operation - multicast approach. (c) Leave operation - multicast approach.

LKH and frequently is additionally severely tormented by the amount of users, as shown in Figure 3(c), frequently incorporates a lower communication value of leave operation compared to each 3-ary and 4-ary LKH, Again, the projected MUKM retains its superiority over the opposite 2 schemes in terms of the communication value of leave operation. This can be principally owing to the 2 separate levels of delivery technique, *i.e.*, multicast and unicast. it's quite fascinating to visualize that the communication value for the LKH 3-ary is above LKH four-ary once there ar 4 users within the system, recall that the communication value for leave operation is d ∗ h[1] For LKH three-ary the d = three and h = 3 whereas for LKH four-ary the d = four and h = two This explains why the communication value of LKH 3-ary is above LKH 4-ary once there ar 4 users within the system.

In regards to the computation value, our analysis utilizes the execution time (seconds/1,000,000 computations) of E, D, R, and F that ar derived by sculpturer *et. al.*, in. These values ar zero.516, 0.797, 1.656 and 1.140, severally. Here, the key length is 128 bits and therefore the height of a tree is computed supported varied range of users, *i.e.*, two to thirty two users.

Figure four illustrates the computation value of LKH, OFT, and MUKM for the server, recent members and therefore the new member for a be part of operation, during this figure, it will be discovered that frequently suffers from the worst computation value owing to its

oneway key derivation, whereas our projected MUKM offers the smallest amount computation value, at the server, for a leave operation frequently incorporates a considerably high computation value since most of the computation like key encoding, decryption, etc., ar handled by the server. In fact, frequently suffers from the best computation value for members because the members ar concerned in key derivation method, as shown in Figure 5. For a leave operation, MUKM offers rock bottom computation value compared to the opposite 2 ways for each server and member, In general, owing to the subgroup key change, MUKM provides a more robust performance in terms of communication and computation value, and aren't tormented by the amount of users. Therefore, whenever a node desires to affix or leave the cluster, it's not necessary to update the complete cluster.

5. Conclusion

In this paper, a light-weight key management theme for multicast IPv6 networks is planned. The planned key management theme referred to as multicast-unicast key management methodology (MUKM) facilitates a suburbanised key management wherever the IPv6 network is split into many subgroups (*i.e.*, is managed by subgroup manager), The planned MUKM distributes freshly generated cluster keys by separating associate IPv6 network into 2 distinct levels, namely, multicast level (*i.e.*, from root to subgroup managers) and unicast level (*i.e.*, among subgroup members), every subgroup manager re-encrypts multicast packets and later on sends them to the multicast members via unicast transmission methodology, supported the waterproof address of every members. During this state of affairs, whenever a be part of or leave operation occur, solely members therein explicit subgroup ought to be updated. The obtained results show that MUKM is effective and capable of reducing each communication and computation prices, and is superior to the prevailing schemes, given the promising results of the planned theme, we are going to judge the theme on associate IPv6 test-bed, further on analyze its potency in terms of storage value and delay.

References

[1] A. Mehdizadeh and F. Hashim, "Multicast-Unicast Key Management Scheme in IPv6 Networks", ICC'14 - W13: Workshop on Cooperative and Cognitive Mobile Networks.
[2] H. Soliman, "Mobile IPv6. Mobility in a wireless Internet", Addison-Wesley Professional, **(2004)**.
[3] C. E. Caicedo, J. B. D. Joshi and S. R. Tuladhar, "IPv6 security challenges", IEEE Computer, vol. 42, **(2009)**, pp. 36–42.
[4] Y. Piao, J. Kim, U. Tariq and M. Hong, "Polynomial-based key management for secure intra-group and inter-group communication", Computers & Mathematics with Applications, doi:10.1016/j.camwa.2012.02.008, **(2012)**.
[5] A. Mehdizadeh, R. Abdullah, F. Hashim, B. Ali, M. Othman and S. Khatun, "Reliable Key Management and Data Delivery Method in Multicast Over Wireless IPv6 Networks", Wireless Personal Communications, vol. 73, **(2013)**, pp. 967-991.
[6] M. Baugher, R. Canetti, L. Dondeti and F. Lindholm, "Multicast security (MSEC) group key management architecture", Internet Engineering Task Force, RFC, **(2005)**, vol. 4046.
[7] H. Ragab Hassen, H. Bettahar, A. Bouadbdallah and Y. Challal, "An efficient key management scheme for content access control for linear hierarchies", Computer Networks, vol. 56, **(2012)**, pp. 2107-2118.
[8] X. Lv, H. Li and B. Wang, "Group key agreement for secure group communication in dynamic peer systems", Journal of Parallel and Distributed Computing, vol. 72, **(2012)**, pp. 1195-1200.
[9] M. Eltoweissy, M. H. Heydari, L. Morales and I. H. Sudborough, "Combinatorial optimization of group key management," Journal of Network and Systems Management, vol. 12, **(2004)**, pp. 33-50.
[10] C. Wong, M. Gouda and S. Lam, "Secure group communications using key graphs", IEEE/ACM Transactions on Networking, vol. 8, no. 1, **(2002)**, pp. 16-30.
[11] J.-C. Lin, K.-H. Huang, F. Lai, and H.-C. Lee, "Secure and efficient group key management with shared key derivation," Computer Standards & Interfaces, vol. 31, no. 1, **(2009)**, pp. 192-208.
[12] W. Trappe, S. Jie, R. Poovendran, and K. J. R. Liu, "Key management and distribution for secure multimedia multicast", IEEE Transactions on Multimedia, vol. 5, no. 4, **(2003)**, pp. 544-557.
[13] H. Harney and E. Harder, "Logical key hierarchy protocol", draft-harneysparta- lkhp-sec-00. txt, IETF Internet Draft (work in progress), **(1999)**.
[14] A. Sherman and D. McGrew, "Key establishment in large dynamic groups using one-way function trees", IEEE Transactions on Software Engineering, **(2003)**, pp. 444-458.

[15] X. Gu, Y. Zhao and J. Yang, "Reducing rekeying time using an integrated group key agreement scheme", Journal of Communications and Networks, vol. 14, no. 4 pp. 418-428, **(2012)**.
[16] D.-H. Je, J.-S. Lee, Y. Park and S.-W. Seo, "Computation-and-storageefficient key tree management protocol for secure multicast communications", Computer Communications, vol. 33, no. 2, **(2010)**, pp. 136-148.
[17] R. Srinivasan, V. Vaidehi, R. Rajaraman, S. Kanagaraj, R. Kalimuthu and R. Dharmaraj, "Secure group key management scheme for multicast networks", International Journal of Network Security, vol. 11, no. 1, pp. 30-34, **(2010)**.
[18] A. Mehdizadeh, F. Hashim, R. S. A. Raja Abdullah, B. Mohd ali and M. Othman, "Quality-improved and secure multicast delivery method in mobile IPv6 networks", The 16th IEEE symposium on Computers and Communications (IEEE-ISCC), **(2011)** June 28–July 1.
[19] A. Mehdizadeh, F. Hashim, R. S. A. R. Abdullah, B. M. Ali, M. Othman and S. Khatun, "Multicast-Unicast Data Delivery Method in Wireless IPv6 Networks", Journal of Network and Systems Management, **(2013)**, pp. 1-26.
[20] Q. Wu, B. Qin, L. Zhang, J. Domingo-Ferrer and J. A. Manjn, "Fast Transmission to Remote Cooperative Groups: A New Key Management Paradigm", IEEE/ACM Transactions on Networking, vol. 21, no. 2, **(2013)**.

