International Journal of Aquatic Science
ISSN: 2008-8019
Vol 12, Issue 03, 2021

A Literature Study on Group Key Management using Huffman Key Tree

Parthasarathi. P[1], Shankar. S[2], Nivedha. S[3]

[1]Bannari Amman Institute of Technology, Erode, India [2]Hindusthan College of Engg. & Tech., Coimbatore, India [3]Sri Krishna College of Technology, Coimbatore, India

Sarathi.Pp@Gmail.Com, Shanx80@Gmail.Com, Nivedhasubramanian@Gmail.Com

Abstract: Recent trends and growth in Network and Internet Technology create unbelievable transaction in communication methodology. Distributed and Parallel Processing are the mile stones for network growth. Since technology has been developed, it is mandatory to take care of implementation difficulties. Installation Cost, Development Issues, Security Issues, Reliable Analysis and Resource Management are the major areas to do the research in implementation. Group Communication (GC) model is applied in most of the Distributed and Parallel Processing system. To provide security services, key based cryptography approaches are applied. Encryption key is dynamically changed in associate with the change in the group strength. Huffman code is used to regenerate the group key at minimum cost.
Keyword: Secure Group Communication, Key Management, Huffman Code.

1. INTRODUCTION

The growth of the network and Internet Technology plays the important role in the development of all the stream of Engineering. The industry process are turned development and simplified operation with the help of information technology. Internet and communication services are build the foundation for distributed and remote operation model. In distributed model, people are working together and collaborating with each other on the single application. To provide and monitor the services on the distributed system, clusters can be framed. Clusters are either group of people or resources involved in the functional operation. There are both one-to-one or one-to-many communications are happen. All the communications which are happed in the cluster is called as group communication (GC). Wireless Sensor Networks [10 is one of the examples group communication.

1.1 Security System

There are two model of security system are used to obtain the message confidentiality. They are steganography system and Cryptography System.

1.1.1 Steganography System

Steganography system is the basic model of security system. The cover media carry technique is used in the steganography system. The source message is added to the

cover media carrier. The source message and cover media carrier both are applied into the embedding process unit. The secret embedding process is worked for adding the source message into the cover media carrier. After adding the source message, the cover media carrier is transmitted to the receiver through the public channel. In the public channel, the cover media carrier only visible to the third party people who are accessing the public channel.

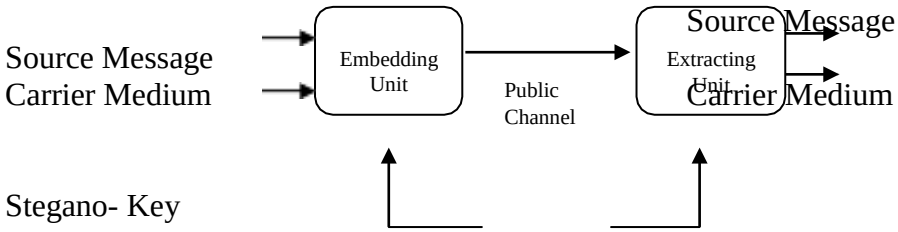


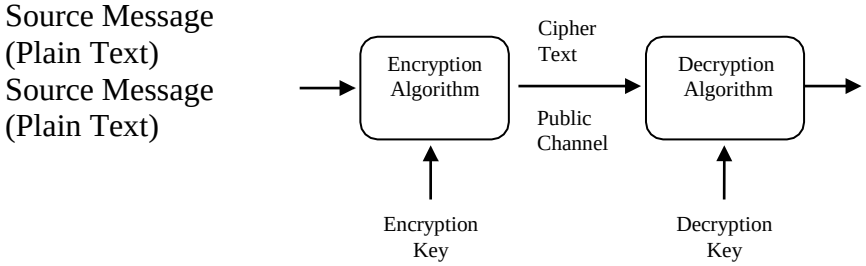
Fig. 1 Steganography System

At the receiving end, the extracting process unit is employed to determine the source message from the cover media carrier. Here also the secret extracting process unit is working to extract the source message from the carrier media. Based on the application, the secret entity called stegano-key is applied in the end to enhance the security to the next level. Figure 1 shows the steganography security system.

1.1.2 Cryptography System

Cryptography system [11][12] includes encryption operation and decryption operation. In cryptography system, key is the primary entity which is used in both encryption and decryption process. Based on the key, the cryptography system is again classified into two types. When there is only one key is used in both encryption and decryption process then the system is called as symmetric key cryptography. Suppose two different keys namely private key and public key are used in either encryption operation and decryption operation or both encryption function and decryption function then the system is called as asymmetric key cryptography.

Fig. 2 Cryptography System



In cryptography system, the source message is called as plain text which is applied to the encryption process. During the encryption process, the source message is converted into another form of representation[17]. This encrypted message is called as cipher text. The cipher text message is transmitted in the public medium to the destination. During the message transmission in the public channel, there may be a chance for third party attack. Since the source message is encrypted, it is not readable and understandable[18]. At the destination point, the cipher text is transformed to plain text with the help of decryption process. The entire process of cryptography system is shown in figure 2.

1.3 Key Management System

Cryptography system is commonly used security system for various applications. In this system, key is the primary entity which is owned by the owner. To maintain the security features, the key also kept in the secured manner. To provide the security for key, there are some systemic procedure followed. Key management is the process of key creating, key sharing among the system users, key storing, key updating and properly removing the existing key from the system. The key management system is categorised based on the key location or the key server.

1.3.1 Centralized Key Management Architecture

The key creation process task is performed in single system or key server. Whenever the key is required then that system will generate the key. Since there is a single system for the entire application, the key generation reliability is the major problem. If that system turns failure then the entire system need to wait for failure recovery. This is the main drawback in the centralized key management system.

1.3.2 Decentralized Key Management Architecture

The key creation task is performed in multiple system or key server. Whenever the key is required then any system will generate the key. Since there are multiple systems, the key generation reliability is achieved. If any one of system turns failure then the remaining system will take responsibility. This is the main benefit in the decentralized key management system.

1.3.3 Contributory Key Management Architecture

The key creation task is performed by all the system or key server. Whenever the key is required then all system will participate in the key generation process. Since all the systems are participating in the key generation process, the key security is increased.
Based on the application requirement for the security, any one of the above model will be executed in secure group communication.

1.4 Secure Group Communication

The security services are implemented in the cluster communication model to attain the secured communication is called as Secure Group Communication (SGC) [9][13][14][15][16][19]. Because of multicast communication in the cluster, the cryptography security model is most used in the cluster communication. In cryptography security system,keys are playing the important role in implementing security. In cluster communication, each member are having their self-key is referred as individual key and a mutual key which is common to every member is referred as cluster key.

The art of key management [2] is the measurable process, it deals the entire communication cost in the cluster communication. When there is a change in the member count in the cluster, then new cluster key is created and existing key is replaced with new key. This process is continuously performed to achieve the backward secrecy and forward secrecy.

The cost of the key generation process is deals with communicational and computational cost. The new key generation process is tried in minimum cost with implementing various key generation process which considering operation involved and parameter shared among the cluster members. There are list of procedures followed to handle member join and leave to reduce the key generation process. The cluster member and their roles are referenced using any one of the data structures using either list or tree. The tree based represent is mostly used because the cluster members are scatted over the network.

1.5 Huffman Tree

The optimal tree method is used as Huffman tree which will reduce the avg. code length under prefix condition. Huffman tree is the structure free tree since there are number of combinations of sub-tree for the same input frequency. The tree developer may select any combination of node from the frequency list. The condition beyond to construct the sub-tree is one that both the leaf values are might be closed to each other. The new sub-tree may be constructed with both the case i.e leaf with leaf and leaf with root of the sub-tree. The identical member are placed at the leaf of the Huffman tree. Each Huffman leaf are assigned with unique representation in binary code. This binary code is constructed from the root to its corresponding places. This binary code is called as Huffman code.

1.6 Huffman Code

Huffman code is one of the most simplified techniques applied in the tree based member representation in the cluster communication. Huffman code for each character is framed from the Huffman tree and the structure of the Huffman tree is free to the user. A user may construct more than one Huffman tree for the given character frequency. Since Huffman is user selected code for each character, it creates more confidentiality on the user data when it is used in message communication over the both public and private network. So Huffman code is not only used for message compression, also used for message security. In the upcoming sessions, different model of Huffman code used in secure group communication are discussed.

The upcoming portion of the paper is arranged as follows. The session 2 deals with literature Survey. There are 30 papers are taken for the literature survey. All the 30 papers are picked in the domain related to secure group communication with Huffman key tree. Form the 30 papers, selected 7 papers are descripted here in detail. In session 3, the conclusion of the survey study is discussed.

2. LITERATURE SURVEY

2.1 Huffman-based Join-Exit-Tree scheme

In tree based cluster communication model, there are three tree scheme is used. They are Main tree, Join tree and Exit tree. The list of active participants are represented by the main tree. The list of new participants who are want to join in the tree are grouped and new sub-tree is framed which is called as Join Tree. Similarly the list of participants who want to leave the cluster communication are identified, the new sub- tree is framed with

the leaving member. This sub-tree is called as Exit Tree. Xiaozhuo Gu et al., [1] proposed Huffman based JET method to reduce the common key generation time and also reduce the new key generation cost during new member join and existing member leave with minimized computational cost and communicational cost.
In HJET scheme, members are splitted into number of subgroups based on their location to cut the communication cost. Join tree and leave tree are constructed based on Huffman code to reduce the communicational cost and computational cost. In H- JET scheme, Join tree and Exit tree are considered and worked as temporary buffer to both the joining and leaving operation. The total cost of each member join includes the cost of member joining in the join tree and cost of relocation. These two functions joining into join tree and relocation is same for each member. So, the author considered the constant cost for all the members. With implement of this scheme, the average join tree cost minimized to O(1). The same kind of process is applied in the leave operation. Because the total cost of each member leave includes the cost of relocation from main tree to exit tree and the cost spent for leave from exit tree. Similar to join operation, the average exit tree cost also minimized to O(1).

2.2 Huffman Tree for Group Rekeying

The performance of the cluster communication is easily monitored and managed using tree data structure based member arrangement. In general, different types of binary key tree is used to handle the issues created due to invariant join and leave operation. The Huffman key tree is also proposed [1] to solve the member join and leave problem. In Huffman key tree, the leaf nodes represent the member of the cluster. The position of the member is determined based on the probability of leave. Sometimes, they are based on the frequency of the member join and leaves. Each and every member in the Huffman key tree are having their own member's length. The member's length are the binary string constructed from the root to leaf. The number of bit in the binary string represents the number of edges presents in between leaf to root. The cost of the rekeying is directly proportional to the member's length.
The leaving probability of the node is defined by the frequency of the member leaving during a period of time. The frequency of the member leaving is also dependent on member's service in the cluster. The Huffman key tree is statically established. If the Huffman key tree is dynamically established then the entire Huffman key tree need to change. It also leads some challenges and it's communication cost and computational cost is high.

Xie Hai-taoand and Wang Chun-zhi [3] proposed adaptive Huffman key tree. In this scheme, Huffman key tree structure is adjusted adaptively according to the frequency of member join and leave operation in the cluster communication. Due the member join and leave probability, the frequency is changed. So, the Huffman key tree is dynamically reconstructed. During this reconstruction, to avoid the increased rekeying cost, adaptive adjusted scheme is appended with Huffman key tree. This adjustment in the frequency will reduce the communicational cost and computational cost because of limited space between the members. The rekeying process is done with limited changes. It also provide the security of multicast rekeying and minimal average cost of new key generation.

2.3 Generating Strong Keys Using Huffman Tree

The Cryptography is the technic which is used to encrypt the message into another representation by means of applying transposition or substitution operation. There are

many number of encryption algorithms are available. All the encryption algorithms are accepting message with one secret entity which is called as key. Key is the primary input which owned by user, along with original message key is applied in the encryption algorithm. The key is securely handle by the both sender and receiver. Since key is the primary component, encryption algorithms are selecting different featured key to strengthen its performance. But it is possible to hack the key information when the fixed size like 16 bits, 32 bits, 64 bits, 128 bits and 256 bits are used in encryption algorithm.
The author Presanna Venkatesan et al., [4] proposed to use Huffman Key Tree to generate new variable length key. The traditional key is selected for the encryption algorithm, then Huffman Key Tree is constructed based on the traditional key. Huffman tree is structure free tree, user can construct different Huffman tree for the same input frequency. So, the third party can't predict the structure of the Huffman tree of the original input key. From the constructed Huffman Key Tree, Huffman code is framed for each leaf in the Huffman tree. This Huffman code is applied as key in the encryption algorithm. In the [4] proposed method, the Blowfish Encryption Algorithm is used to generate the cipher text of the original message. Since the Huffman code is used, the key strength is increased with variable size. When the key is becomes unbreakable then the sender ensure that the confidentiality of the message is highly secured.

2.4 Huffman Key Tree

In Secure Group Communication, the key management is the art to implement security service such as confidentiality and authentication. There are two different keys are used namely group key and member key. Group key is used to encrypt and decrypt the message, through which the message confidentiality is achieved. Suppose a person wants to leave from the group then the new group key is generated in order to obtain the forward secrecy, similarly new group key is generated for each join operation to ensure the backward secrecy. To efficiently ensure these key management process, the entire group is divided into subgroups. For each subgroup, a subgroup key is maintained which is common to all in the same group.

The author senthamil Illango et al., [5] propose Boolean Function Minimization Technique, where user have set of keys namely auxiliary keys along with session key. Each member in the group have Unique ID (UID). Based on the UID, the set of keys are finalized. Suppose UID is 3 bit then there are three auxiliary keys are used. The Modified Huffman tree is used to generate the UID. Since there are variable length bits, the auxiliary keys are generated. Finally the security of the system is increased.
[5] is also proposed Petrick's function of Boolean method minimization. It is used to determine all minimum sum of product solutions. It also increase the number of variable in the prime implicant chart. It also increasing the complexity of solving them.

2.5 Huffman Tree Structure for Group Rekeying

Secure Group Communication (SGC) is the common communication model for one to many secure message sharing. In SGC, data confidentiality and key management are consider as primary process. The common key is frequently changed for each member join and leave operation. The new common key generation and sharing the common key information with existing member are the complex process. The author Hemanth Tumbare et al., [6] is proposing Huffman tree based process for generating new common key. Since Huffman tree is not a dynamic tree structure, the adaptive Huffman tree is proposed. The new member joining probability and existing member leaving probability are taken as frequency set for constructing Huffman tree. So it is ease to rekey the

common key and secure then the existing key distributed method.

2.6 LKH Technique with Huffman Algorithm

In Secure Group Communication, there are two keys namely group key and member key plays an important role to achieve Data Confidentiality and Resource Access Control in the distributed and collaborated environment. In group dynamic conditions, the group key is frequently updated suppose there is any modification in the group member count. During the group key update, communication cost and computation cost are considered. The tree based member representation techniques are used to reduce both the same cost. In general, Logical Key Hierarchy (LKH) method is followed to construct key tree. The author Takahito et al.,[7] proposed to Huffman Algorithm to build LKH. The Huffman tree is the structure free data structure. i.e any number of the key trees are construct for same frequency set. In Huffman tree, all the leaf nodes are tried to connect to the root with minimum length edges. The user will get option to build more than one key tree for live member count in the group. From the collects, the minimal cost tree is taken to build new group key with minimized cost.

2.7 Conference Key Generation Using Huffman Tree

In secure Group Communication, the group key is frequently changed to achieve the high security on data during the group dynamic condition. Whenever there is a change in group member count, the group is updated. If there is case of joining set of user to the user as new member then they are group and a separate external tree is constructed called as Join Tree. Similar to the bulk join, there are set of existing user may want to leave from the group, then they are identified and separate tree called Exit Tree is constructed. The join tree and exit tree are consider as buffered tree data structure for set of new member join and leave operation. The member joining in the join tree cost includes both the cost of member join to the joining tree and cost relocation. In this process, the member relocation cost is common to all the member.

The author Xiaozhuo et al, [8] introduced HJET Scheme. In HJET Scheme, Huffman tree for member join in the join tree at the rate of constant cost for all the user. Similar to Join Tree, the Exit Tree is also built for the set of user leave operation. It includes the cost of relocation and the cost for user leave from the exit tree. In HJET scheme, the member join in the join tree is constant for all the member in the group. The constant cost of the member join is nearly reduced to O(1). It is same to the leave operations. The cost for member leave from the group is O(1) in average. The HJET scheme is relatively increasing the key strength as well as reduce the key generation cost compare than other tradition tree based techniques.

3. CONCLUSION

The Huffman tree method is more secure in the key management because the Huffman tree structure is unpredictable. There are many number of Huffman tree is constructed for the given data frequency. Since it is having variable length for the each node in each tree. In ASCII code representation, there are 8 bit for each character. So there may be an opportunity to predict the actual key value. But in Huffman code, each and each character has been assigned with different number of bit combination. So, it is not possible to identify the key's bit string. The strength of the key is most powerful than other formation. Also, the cost of the building Huffman Key Tree is O(1), which is relatively chipper than the Logical Key Hierarchy.

4. REFERENCE

[1] Jianzu Yang et al.: Huffman-based Join-Exit-Tree scheme for contributory key management. Computers and Security, Volume 28, Issues 1, pp 29-39, (2009).

[2] P.Parthasarathi, Dr.S.Shankar, S.Nivedha: A Survey on dynamic key Management system in Secure Group Communication. Proceedings of 2020 6th International Conference of Advanced Computing & Communication Systems (ICACCS), pp 1440-1443, (2020).

[3] Xie Hai-tao, Wang Chun-zhi: A Novel Huffman Tree Scheme for Group Rekeying. Proceedings of 2010 Second Int. Workshop on Intelligent Systems and Applications (IWISA), (2010).

[4] PrasannaVenkatesan. S, Nooka Saikumar, Srividhya. S, Manikandan. G: Generating Strong Keys Using Modified Huffman Tree Approach Proceedings of 2016 International Conference on Circuit, Power and Computing Technologies [ICCPCT], (2016).

[5] Senthamil Ilango, Johnson Thomas: Group Key Management utilizing Huffman and Petrick based approaches Proceedings of the International Conference on Information Technology: Coding and Computing (ITCC'04), (2004).

[6] Hemanth Tumbare, Raghu Venkat. P, Prasad Chaure, Usha Devi. G: Huffman Tree Structure for Multicast Group Rekeying. Proceedings of 2012 2nd IEEE International Conference on Parallel, Distributed and Grid Computing (ICPDGC), pp 779-17823. (2012).

[7] Takahito Sakamoto, Takashi Tsuji, Yuichi Kaji: Group Key Rekeying Using the LKH Technique and the Huffman Algorithm. Proceedings of International Symposium on Information Theory and its Applications (ISITA2008), (2008).

[8] Xiaozhuo Gu, Jianzu Yang, Xiangjie Ma, Julong Lan: An Efficient Conference Key Updating Scheme with the Knowledge of Group Dynamics. Proceedings of 2008 Global Telecommunications Conference (GLOBECOM), pp 1-6, (2008).

[9] Parthasarathi.P, Jayasmruthi A, Sathishkumar: A Survival Study of Security Attacks, Mechanisms and Security Challenges in Network Security. Advanced in Natural and Applied Sciences (ANAS), Issue 11(5), pp 58-66, (2017).

[10] Parthasarathi. P, Nivedha S: Energy-Efficient and Coverage based Data Collection in Sparse Wireless Sensor and Actor Networks. International Journal of Computer Engineering and Applications, Volume 12, Special Issue, pp 48-58, (2018).

[11] Parthasarathi.P, Radhini.M.P: Secure Sharing of Medical Records Using Cryptographic Methods in Cloud. International Journal of Computer Science and Mobile Computing, Volume No.3, Issue No.4, pp 514-521, (2014).

[12] Parthasarathi P, Radhini M P, Ananthaprabha P: Security Mechanism for Group Communication in Cloud. International Journal of Research in Computer Applications & Information Technology, Volume No.2, Issue No.1, pp 17-22, (2014).

[13] Xiaozhuo Gu, Zhenhuan Cao, Jianzu Yang and Julong Lan: Dynamic Contributory Key Management Based on Weighted-Join-Exit-Tree. IEEE Military Communications Conference, pp 1-7, (2008).

[14] Chang Xu, Rongxing Lu, Huaxiong Wang, Liehuang Zhu and Cheng Huang, "TJET: Ternary Join-Exit-Tree Based Dynamic Key Management for Vehicle Platooning, Special Section on Security and Privacy for Vehicular Networks" IEEE Access, Volume 5, Pages 26973-26989, (2017).

[15] Vijayakumar. P, Bose. S, Kannan. A: Centralized Key Distribution Protocol using the Greatest Common Divisor Method, Computers and Mathematics with

Applications. Elsevier Publication, Volume No: 65, Issue No: 9, pp 1360-1368, (2013).

[16] Mao. Y, Sun. Y, Wu, Liu KJR: JET: Dynamic Join-Exit-Tree Amortization and Scheduling for Cotributory Key Management. IEEE/ACM Transaction on Network, Volume No: 14, Issue No: 5, pp 1128-1140, (2006).

[17] Classification and prediction of social attributes By K-Nearest Neighbor Algorithm with Socially-aware wireless networking-A study To cite this article: Sujatha Krishanmoorthy et al 2020 IOP Conf. Ser.: Mater. Sci. Eng. 937 01205

[18] Amin Salih Mohammed, Saravana Balaji B, Saleem Basha M S, Asha P N, Venkatachalam K(2020),FCO — Fuzzy constraints applied Cluster Optimization technique for Wireless AdHoc Networks,Computer Communications, Volume 154,Pages 501-508.

[19] K. Venkatachalam, A. Devipriya, J. Maniraj, M. Sivaram, A. Ambikapathy, and S. A. Iraj, "A novel method of motor imagery classification using eeg signal," *Artificial intelligence in medicine*, vol. 103, p. 101787, 2020.