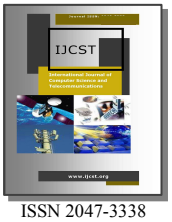

ISSN 2047-3338

Secured Data Transmission in Multinode Network (MN)

Ajay Kakkar[1], Dr. M. L. Singh[1] and Dr. P. K. Bansal[2]
[1]GNDU, Amritsar, India
[2]MIMIT, Malout, India

***Abstract*– Secured data transmission in a multinode network (MN) depends upon various factors; such as number of user, nodes, channel capacity, failure rate of keys and nodes, path allocation criteria and encryption methodology. In order to keep the routed thorough the various nodes continuous scanning and up gradation of nodes is essential. This paper includes the work done by the researchers in the field of data security in multi-node networks (MN). The flaws in various techniques are also highlighted in the work.**

***Index Terms*– Encryption, Keys, Multinode Network and Failure Rate**

I. INTRODUCTION

THERE are various ways to achieve the secured communication such as; passwords, multiple passwords, cryptography and biometrics. These techniques are used to keep the data secured from the hacker. *Passwords* are not treated as reliable for this task. It is easy to guess passwords due to its short range. The main difficulty in designing secure password mechanisms is that password space is usually small and much easier to attack with random efforts. The problem is coped up by using *multiple passwords* but remembering such amount of multiple passwords is not an easy task. Even in case of multiple passwords low entropy can exits which make the system unsecure. *Cryptography* is a technique used to protect the data from unauthorized access. It is the best method of saving the documents from the competitor in business. It consists of two components encryption algorithm and Keys. There are many algorithms available in the market for encrypting the data. Encryption is the process in which original data (plaintext) has been converted into the encoded format (cipher text) with the help of key. Key is any value or/and word used to encrypt and decrypt the data. If encryption algorithm consists of same key for encryption and decryption process then it is called as symmetrical or private key cryptography. On the other hand if different keys are used in the encryption and decryption then it is known as asymmetrical or public key cryptography. In both the algorithms key lengths and their characteristics has been designed on the basis of data length [1]. *Biometrics* is also used to provide the data security but there are few problems associated with the technique. In biometrics scanning of voice, thumb, finger, retina, etc have been considered and matched with the prefixed value. If matching of the inputs with prefixed values has been achieved to a certain level then access of the systems has been granted otherwise system remains in protected zone. The system accepts a fixed matched value and then responds therefore due to False Acceptance Ratio (FAR) and False Rejection Ratio (FRR) results in hazards. From the work done by various researchers it has been observed that scanning of voice, thumb, and finger techniques have many flaws. In case of sore throat, losing a hand in accidental conditions the matching of inputs does not take place, the system remains closed forever. The technique is costly and in case of retina scanning harmful rays enters in the body part of the human being. No one requires security at the cost of health therefore it has not been preferred over cryptography for data processing over web.

II. RELATED WORK

In 1970 the Data encryption Standard (DES) was developed by IBM but was later adopted by the US government as a National Standard [2]. It is one of the most widely accepted, publicly available cryptographic systems. Single key of 56 bits key has been used to encrypt the 64 bit block size data and algorithm undergoes 16 iterations. Padding techniques were used in case of mismatching of data and key lengths. The analysis of multiple key generation and their failures were not addressed in the standard.

Whitefield Diffie and Martin E. Hellman [3], [4] worked on exhaustive cryptanalysis of the national bureau of standards (NBS) for Data Encryption Standards in 1977. They suggest that the standards used for the encryption of data require to be changed after every 5 years due to the introduction of hacking software's. Their proposed standard was based on 64 bit plain text block operated by 56 bit key length which was same with DES. The system was designed in such a way that the key length can be extended up to 128 or 256 bits. The key length 128 bit key increases the estimated cost for a brute force from \$ 5000 to \$ $2 * 10^{25}$ at that time. They also considered chip size which includes 3000 gates in order to support high speed switching action. They showed that there is a tradeoff between in speed and power. The integrated chips used at that time were limited to 1 watt of power dissipation. The gate delay is around 4ns and 1 µsec search time for the key has been observed in the scheme and the equivalent gate operation per second is determined as $3000/(4* 10^{-9})$.

Table 1: Key size, number of operations and time required by the hacker to break the system [5]

Digits	**Number of operations**	**Time**
50	$1.4 * 10^{10}$	3.9 hours
75	$9.0 * 10^{12}$	104 days
100	$2.3 * 10^{15}$	74 years
200	$1.2 * 10^{23}$	$3.8* 10^{09}$ years
300	$1.5 * 10^{29}$	$4.9* 10^{15}$ years
500	$1.3 * 10^{39}$	$4.2* 10^{25}$ years

In 1980 R.L. Rivest et al. [5] proposed a method for obtaining digital signatures and public key cryptosystems. They assume that the receiver knows the deciphering function for the received message in order to obtain the original message. They claimed that if key size has been increased then hacker requires much large time to recover the data. The detailed about the time required to decrypt the data from with random keys is shown in Table 1.

By using powerful software's one can break the encryption key and get access of the cipher text within the minutes. The RSA algorithm and key combination was attacked by the hacker and side channel and internal attacks also put harm to the model.

In 1983, Selim G. Akl and Peter D. Tay [6] suggested a cryptographic solution to a problem of access control in a hierarchy based upon partially ordered set which sort out the problem of using randomly generated keys. The show a time versus storage trade off and suggest that more numbers of keys are used to encrypt bulk data. Before encryption different classes of data has been achieved and then these are encrypted by using randomly generated keys in a pipelined structure. Two large random integers (one even and one odd) were used of the generation of random keys having prime probability. They assume that each key has a length of at least 200 digits which becomes overheads in most of the cases. The work does not include any simulation results for the failure rates of key generation process.

In 1984 Andrew M. Odlyzko [7] provides fast signature scheme for the cryptanalytic attacks. They showed that the shamir's signature scheme can be cracked by random attacks made by hacker. The used first n prime numbers expressed in terms of polynomials and system requires the n4 operations to encrypt the data. The scheme was not efficient and reliable for multiple keys and does not able to handle the multinode networks.

In 1988, R.S. Sandhu [8] implemented a cryptographic tree hierarchy approach for the access control in different security levels. Each user has the power to store a single key of fixed size corresponding to the level of security. He also shows that one can create new security levels without altering the existing keys. For the new security levels; the sub keys have been designed from the existing keys. The two main limitations of the work are deriving new keys from existing key and fixed length of the keys. They were not succeeded to detect the faulty keys from the model.

In 1990 Lein Harn et. Al. [9], proposed a cryptographic key generation scheme used for multilevel data security. Their approach was based upon the bottom up key generation procedure by considering much smaller security classes. They assumed that the large value of data elements were associated with small number of security classes and always provides low security pattern. The insertion of new classes is still possible even in the case when all the keys were issued by CA. They failed to address the updating and distribution of keys in the presence of hacker. They were not able to provide any satisfactory solution of key management in case of class removal from the security level.

In 1991, Ohta, K et. Al. [10] proposed a membership authentication scheme for multi groups by using master key which was used to derive the sub keys. They consider efficiency, group isolation and hierarchy while implementing the membership authentication scheme with the help of smart cards. Cryptographic key assignment technique was not used for access control for multi user. Their scheme was based on centre key generation and distribution by using group administrator (GA). The responsibility of GA was to maintain the database for each user which becomes unreliable when users are increased.

In 1997 Chu-Hsing Li [11] provides a dynamic key management schemes for access control in a multinode network. The system was designed in such a way that users were authorized and classified into different privilege classes in order to access the data. They implement the dynamic operations such as updating a key, insertion of new class/users, deleting of existing classes and users were done efficiently. The key management technique was controlled by CA whose main responsibility was to create cryptographic functions between the group keys of different classes. The proposed scheme has the following assumptions; (i) the group keys can be selected randomly and independently by each class. (ii) any class can update its key without affecting other classes, (iii) A new class can be inserted into the system without affecting the keys of any existing class and (iv) A class can be cancelled from the system without affecting the key of existing classes. Li does not provide satisfactory the solution for contrary and collaborative attacks.

In 1998 Michael Luby and Jessica Staddon [12] presents a broadcast encryption system which allows a set of users to communicate securely over a broadcast channel. They showed that there was a gap between the number of keys generated and transmitted in a broadcasted encryption system called as resiliency. The difference between the two events must be minimized for an optimized model. The worked was focused to design a model in which only privileged users can be able to access the model by the help of authenticate keys. The model was only effective if a group of users can participate, with increase in the number of users the authenticity of user was not satisfactory.

In 2001 B. Pinkas [13] provides efficient state updates for key management in a dynamic network. The work was focused on the concept that all the parties must share a group key which was managed by a group controller (GC). They assume that the each party can share secret data by one to one channel by using different keys and the session was maintained by GC. They showed that in order to encrypt a

block size of 10, 00,000 bits with 128 bit key length the overheads bits were 25, 00,000 bits. The use of private key reduces the computational overheads due to its efficient cryptographic operations. The main limitation of the work was that the generation of unique keys for all the users in a dynamic scheme increases complexity. Such amount of keys also increases overhead bits which take more computation time. The scheme was not effective for public key cryptography.

In 2002, S .K. Lee et al. [14], they presented hierarchical approach to resolve multiple failures at the multi-node network (MN). In which various security levels have been proposed for different type of attacks and recovery mechanism can be selected on the basis of these security levels. Various security levels were discussed in their work but they were not able to provide any effective solution for the faulty nodes.

In 2002, V.R.L. Shen et al. [15], the authors present a cryptographic key assignment scheme to solve the dynamic access control problems in a partially ordered user hierarchy. They worked on the problem mentioned in the work of R.S. Sandhu (1988) and Hui-Min Tsai (1995) show that there is no need to consider the lower classes of security level in order to change the keys for the higher classes of any security level they were not able to reduce the complexity of the model. They also fail to address the key associated problems and not able to provide any analysis for the generation of multiple keys for the same classes with in the security level.

In 2002, Sheng Zhong [16] proposed a practical key management scheme for access control in a user hierarchy. They assumed that it desirable to allows the users of each security class to derive the keys from their subordinating classes. Their scheme was efficient from the work done by R.S. Sandhu in1998, but can be applied to a general hierarchy, where as earlier approaches were applicable on tree hierarchy. They provide the facility to the user to in each class to select and replace their keys without affecting the other keys. Their scheme was focused on the key selection; not on the key generation in the lower classes. It creates the need of the trusted party which causes the authentication related problems.

In 2003, W. Du [17], They developed two similar random key pre distribution techniques which uses the multi space key pool to improve network resilience and memory usage efficiency. Their work was focused on the optimization of memory in case of node failure. Their model was effective when multiple keys having same failure rates were used but not provide suitable results if the keys are having different failure rates. The reason of different failure rates are; i) if the length of the keys are of different order, ii) different polynomials are used for the encryption and iii) if data block size varies. As they were not able to determine the variable failure rates of the multiple keys therefore the key shifting problem still exists in their model.

In 2003 Hung-Yu Chien [18] proposed an efficient time bound hierarchical key assignment scheme in multinode network. The key assignment scheme used in the work improves the computational performance and reduces the implementation cost. Attack by an outsider and attack by a subordinate/Collusive attack by subordinates has been considered in the work. The encryption key used in the approach was time bounded which decreases the security level and does not provide the flexibility to the users to upgrade the private key.

In 2004, L. Hundessa et. Al. [19], they presented a protection mechanism packed up with multiple keys to handle multiple link/ node failures. A salient feature of the authentication protocol used in the mechanism is that it supports source authentication. Key sharing approach has the minimum storage costs and is very energy efficient solution in MN. It not requires any additional keys for establishing the network between the two nodes. The mechanism was not effective when it deals with various keys having different failure rates. It includes an efficient protocol for local broadcast authentication based on the use of single way key chains. Moreover, particular keying mechanisms may reduce the effectiveness of the network processing.

In 2004 Sencun Zhu et. Al. [20] provides efficient security mechanisms for large scale distributed sensor networks (LEAP). LEAP supports the establishment of four types of keys for each sensor node. The detailed summary of the LEAP includes the individual key which has been shared by the base station and a pair wise key shared with another sensor node. A group key also introduced so that all the nodes in the network can share it for the data transmission. The major constrained of the system was energy budgets and the availability of the limited computational and communication capacities of sensor nodes in the network.

In 2005, Michael Backes et al. [21], they presented the relating symbolic and cryptographic secrecy technique for MN. A group key for encrypting a broadcast message has been preferable which using cluster keys. This group key has been used by all the nodes to share the information. They failed to discuss and provide better solution for key shifting time in MN.

In 2005 Mikhail J. Atallah et al. [22], proposed a dynamic and efficient key management for access hierarchies for various classes. They consider the space complexity of the public information and update of the private information at a class which consists of a single key. Security of access control model derived from their ability to deny access to unauthorized data. The main limitation of their approach was that it was based symmetrical key cryptography. The key generation and processing mechanism is very poor. The encryption algorithm is also very complex which leads to high probability of error.

In 2008 Syed Taha Ali et. Al. [23] proposed a key loss recovery scheme for secure broadcasts in wireless sensor networks (WSN). The work was focused to derive the keys slowly in a predetermined time period. Keys can also be varied from one packet to the next packet. Their approach was based upon the concept that the time varying keys offer more security in the broadcast network. The model which they present was too complex and bit error rate was very high.

In 2008, Huawei Huang et. Al. [24] present a generalized public key cryptosystem based on a new Diffie Hellman problem as a result one can achieve almost double the message expansion by using secret key length. The main feature of the work is that it does not require any additional computational cost. The main limitation of the work is that

the scheme it was based upon one way key exchange protocols. Higher classes of security level can derive their sub keys from the lower classes but the reverse of the same does not hold good. Although the Group Diffie-Hellman (GDH) approach has efficient protocols for group communication but they require member serialization. It indicates that the users must be serialized in some special way in order to achieve a common key.

In 2008, Elisa Bertino et al. [25], they discussed an efficient time bound hierarchical key management scheme for secure broadcasting. Members can distinguish the key updating process due to new user and that due to user departure alters the performance of the model. In such case key and group re sizing has been highly required. There is also need to recalculate the Key shifting, latency and processing time. They fail to address these issues in their work.

In 2009, Mikhail J. Atallah et al. [26] presents a dynamic and efficient key management for access hierarchies for multinode networks. The space complexity of the public information remains same as that of storing the hierarchy of the previous approaches. Single has been associated for each class and must be shared privately in session. Insertion and removal of classes between various security levels is possible and this scheme is more secured against collisions. A key management scheme was used which the multiple assigns keys to the access classes and distributes a subset of the keys to each user. Their scheme was bounded by the length of the path between the nodes which increases the propagation delay and provides more time to the hacker.

In 2011 Vijay Sivaraman et al. [27] proposed broadcast secrecy technique via key chain based encryption in single hop wireless sensor networks (WSN). Their approach is efficient and scalable means of delivering broadcast data secretly to a large number of low power sensor nodes. Their approach was based on key chain generation, bootstrapping and data transmission. Major drawback of using the key chain approach is that if a receiver misses one broadcast packet then it is excluded from all future broadcast messages. The reason for the above limitations is that the key contained in the missing packet is needed to decrypt the subsequent packet and in turn contains the key to the next packet. They also fail to cover the multi-hop networks where transit nodes are used.

The observations from the work done by the various researchers in the field of Multinode network are given as:

a) If numbers of nodes are increased then the data security tends to fall.
b) Increase in the number of nodes also causes a significant delay at the receiver section
c) The latency time also the function of number of nodes. It also varies with respect to number of nodes.
d) The short data streams have been preferred in a MN having large number of nodes.
e) The long data streams are suitable for only a MN having less number of nodes.

The observations from the work done by the various researchers in the area of multiple key used for encryption of the data are given as:

a) Single key with fixed length does not able to provide to secured communication.
b) Single key with variable length provides little bit secured communication as compared to single key having fixed length. Such mechanism has been preferred for only short data streams in MN having less number of nodes.
c) Multiple keys having different failure rates can be achieved by varying the key length.
d) Multiple keys are always preferred for encrypting the data in MN having large number of nodes.

From the observations it has been comes into picture that for a secured model the following points should be considered in the design procedure of a secured model.

a) Reduce the time available for the hacker in which attempts are made to destroy the model.
b) Limit the processing time in the encryption process in case of multiple key systems. The processing time is the function of the hardware used and can it can be reduced by reducing the logical effort of a device.
c) Minimize the key shifting time (δ) from 1st key to 2nd key in case of multiple key encryption based system.

III. CONCLUSION AND FUTURE SCOPE

The related work indicates that there is a need to develop a model which provides the flexibility to select short and long data length sequences as per the requirement. The selection of keys and S- Boxes should be based upon the data sequence in order to reduce the hacking and processing times. Also, in case of node failure, the algorithm immediately generates new keys for corresponding node. It has been found that for efficient and reliable model; keys should be generated from the available data. Key recovery mechanisms should be available in the model in order to look after the failure situation. For a secured model there is a need to develop optimized efficient key management techniques in order to generate (i) random keys from the data by the algorithm. (ii) Determine failure rate of multiple keys used by various nodes and (iii) reduce the time available for the hacker in which attempts are made to destroy the model.

REFERENCES

[1] Ajay Kakkar, Dr. M. L. Singh, Dr. P. K. Bansal, "Efficient Key Mechanisms in Multinode Network for Secured Data Transmission", International Journal of Engineering Science and Technology, Vol. 2, Issue 5, 2010, pp.787-795.
[2] Davis, R, "The data encryption standard in perspective", Communications Society Magazine, IEEE, 2003, pp. 5 – 9.
[3] Diffiee, W., and Hellman, M., "New Directions in Cryptography", IEEE Transaction Information Theory IT-22, (Nov. 1976), pp. 644-654.
[4] Whitefield Diffie and Martin E. Hellman, "Exhaustive cryptanalysis of the NBS Data Encryption Standards", Computer Magazine, The Institute of Electrical and Electronics Engineers, California, 1977.
[5] R.L. Rivest, A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems", securespeech.cs.cmu.edu/reports/RSA.pdf,1980
[6] Akl Selim G., Taylor Peter D., 'Cryptographic solution to a problem of access

control in a hierarchy" ACM Transaction. Of Computer System, Vol.1, 1983, pp. 239–248.

[7] Andrew M. Odlyzko, "Cryptanalytic Attacks on the Multiplicative Knapsack Cryptosystem and on Shamir's Fast Signature Scheme" IEEE Transactions on Information Theory, Vol. IT-30, No. 4, July 1984.

[8] R.S. Sandhu, "Cryptographic Implementation of a Tree Hierarchy for Access Control," Information Processing Letters, Vol. 27, pp. 95-98, 1988.

[9] Lein Harn, Hung-Yu Lin, "A cryptographic key generation scheme for multilevel data security", Computers & Security Vol. 9, Issue 6, 1990, pp. 539-546.

[10] Ohta, K., Okamoto, T., and Koyama, K., "Membership Authentication for Hierarchical Multi groups Using the Extended Fiat-Shamir Scheme", in Proceedings of the Workshop on the Theory and Application of Cryptographic Techniques on Advances in Cryptology (EUROCRYPT'91), 1991, pp. 446–457.

[11] Chu-Hsing Lin, "Dynamic Key Management Schemes for Access Control in a Hierarchy", ELSEVIER Computer Communications Vol. 20, 1997, pp. 1381-1385.

[12] Michael Luby and Jessica Staddon, 'Combinatorial Bounds for Broadcast Encryption", EUROCRYPT '98, LNCS 1403, 1998, pp. 512-526.

[13] B. Pinkas, "Efficient State Updates for Key Management," Proceedings of ACM Workshop on Security and Privacy in Digital Rights Management, Nov. 2001, pp. 910 - 917.

[14] S. K. Lee and D. Griffith, "Hierarchical Restoration Scheme for Multiple Failures in GMPLS Networks," Proc. 31st International Conference on Parallel Processing Workshops (ICPPW '02), Aug., 2002, pp. 177-182.

[15] V. R. L. Shen and T. S. Chen, "A Novel Key Management Scheme Based on Discrete Logarithms and Polynomial Interpolations", Computers & Security, Vol. 21, No. 2, 2002, pp. 164–171.

[16] Sheng Zhong, "A Practical Key Management Scheme for Access Control in a User Hierarchy, Computers & Security, Elsevier Science Ltd., Vol. 21, No 8, 2002, pp. 750-759.

[17] W. Du, J. Deng, Y. S. Han, and P.K. Varshney, "A Pair wise Key Pre distribution Scheme for Wireless Sensor Networks," Proceedings of 10th ACM Conference on Computer and Communication Security (CCS '03), 2003, pp. 42-51.

[18] Hung-Yu Chien, "Efficient Time-Bound Hierarchical Key Assignment Scheme", IEEE Transactions on Knowledge and Data Engineering, Vol. 16, No. 10, October 2004, pp. 1301-1304.

[19] L. Hundessa and J. Domingo-Pascual, "Optimal and Guaranteed Alternative LSP for Multiple Failures," Proceedings of 13th IEEE International Conference on Computer Communication and Networks (IC3N '04), 2004, pp. 59-64.

[20] Sencun Zhu, Sanjeev Setia, Sushil Jajodia, "LEAP: Efficient Security Mechanisms for Large Scale Distributed Sensor Networks", 2004 ACM, pp. 514–528.

[21] Michael Backes, and Birgit Pfitzmann, "Relating Symbolic and Cryptographic Secrecy", IEEE Transactions on Dependable and Secure Computing, Vol. 2, No. 2, 2005, pp. 109-123.

[22] Mikhail J. Atallah, Keith B. Frikken, and Marina Blanton, "Dynamic and Efficient Key Management for Access Hierarchies", Proceedings of ACM CCS'05, Alexandria, Virginia, USA, November 7–11, 2005, pp.1-12.

[23] Syed Taha Ali, Vijay Sivaraman, Ashay Dhamdhere, Diethelm Ostry, 'A Key Loss Recovery Scheme for Secure Broadcasts in Wireless Sensor Networks", IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC), 2008, pp. 1-5.

[24] Huawei Huang, Bo Yang, Shenglin Zhu, Guozhen Xiao, "Generalized ElGamal Public Key Cryptosystem Based on a New Diffie-Hellman Problem" , Proceedings of the 2nd International Conference on Provable Security, 2008, pp. 1-21.

[25] Elisa Bertino, Ning Shang, and Samuel S. Wagstaff Jr., "An Efficient Time-Bound Hierarchical Key Management Scheme for Secure Broadcasting", IEEE Transactions on Dependable and Secure Computing, Vol. 5, No. 3, 2008, pp. 65-70.

[26] Mikhail J. Atallah, Marina Blanton, Nelly Fazio and Keith B. Frikken, "Dynamic and Efficient Key Management for Access Hierarchies", ACM Transactions on Information and System Security, Vol. 12, No. 3, 2009, pp. 1-43.

[27] Vijay Sivaraman,1,2 Diethelm Ostry,2 Jaleel Shaheen,1,2 Antoni Junior Hianto,1 and Sanjay Jha1,2 "Broadcast Secrecy via Key-Chain-Based Encryption in Single-Hop Wireless Sensor Networks", EURASIP Journal on Wireless Communications and Networking Volume 2011, pp. 1-12.