International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-10 Issue-6, March 2022

Implementation of Authenticated Group Key Management Scheme for Wireless Sensor Networks

A.V.V.S. Murthy, P. Vasudeva Reddy

Abstract*: The group key management technique is an important technique for cryptographic applications. In this paper, we implemented our proposed method [1] on a group key management protocol for group communication. The proposed protocol is authenticated group key distribution protocol is a mechanism for distributing a group key. We also discussed security analysis and attacks in active and passive adversary model. Also, it ensures semantic security as well as Key freshness of the group key. Along with this, they provide implicit and mutual authentication of the group key. Furthermore, the protocols provide key independence, provide Perfect Forward Secrecy and are resistant to Known Key Attack Implementation of proposed protocol in NS2 simulator.

Keywords*: Key Management, Group Key Management, Digital Short Signatures, Authentication, Wireless sensor networks.

I. INTRODUCTION

Key management [1,2] is an important cryptographic technique for sharing of either group secret key among parties or secret key between two parties. Many Key management techniques [2,5] have proposed for pairwise and group key management using several settings. As a result, the proposed key management protocol should not only support the creation of paired keys, but also cluster and group keys. A group key is a shared secret shared by all members of the same group, and it's mostly used to secure locally broadcast messages. A group key is a globally shared common key that the base station uses to encrypt communications sent throughout the whole network. The Group Key Management scheme [2,3,4] can be utilised in revocation encryption schemes, group encryptions, and threshold encryption schemes for security group communication. The group key security protocol should address issues such as group key production and regularity of group key updates. These important management strategies for groups can be classified into three categories: There are three types of group key agreement protocols: (i) centralised group key agreement protocols (CGKAP), (ii) decentralised group key management protocols with relaying (DeGKMP), and (iii) distributed group key agreement protocols (DGKAP)..

Manuscript received on January 20, 2022.
Revised Manuscript received on February 20, 2022.
Manuscript published on March 30, 2022.
* Correspondence Author
A.V.V.S. Murthy*, Department of Mathematics, Dr S.R.K. Govt. Arts College Yanam (U.T of Puducherry), India Email: murthyavvs@gmail.com
P. Vasudeva Reddy, Department of Engineering Mathematics, College of Engineering, Andhra University, Visakhapatnam. (A.P), India Email: vasucrypto@yahoo.com

II. LITERATURE SURVEY

This section extensively overviews the various key exchange protocols developed in years. In [7], The researchers propose a secure group communication technique based on the Chinese Remainder Theorem and Di e-Hellman. To generate the TEK, two rounds of broadcasts are required. It ensures that there is no single trusted authority and that computation is spread equitably among all users. The researchers of [8] suggest a two-round key agreement approach. Compared to CRTDH, this requires less message overhead. GKMPAN, a probabilistic approach to group key management, is proposed by the authors in [9. The authors presented a threshold cryptography-based decentralized key management scheme in [10]. [12] describes a number of topology-oriented group key management methods [13], [14], and [15]. The authors investigated fault-tolerance principles in MANET group key management protocols in [16],[17]. The researchers of [18] propose that the group be divided into sub-groups. Each sub-group is led by a leader, and the leaders of the sub-groups form a connected dominating set. GDH2 is a generalization of the two-party Diffe Hellman key agreement protocol [19]. In [20], the authors propose Secure Group communication Proto-col. In [21], the authors propose a cluster-based group key management protocol where clusters are geographically delimited regions. For hierarchical groups, the author provides a cluster-based group key management technique in [22]. Amir et al. [23] developed the first contributing GKA procedure that was resistant to any series of group modifications. Only a few known protocols, such as the Joux technique [24] and the BS protocol suggested by Boneh and Silverberg [25], are really one-round self-organizing and distributed protocols. Both of these, though, are unworkable. Wu [26, 27] has recently proposed some actual asymmetric group key agreement procedures. This protocol is classified as self-organizing, however it is only suitable for a static group [37] and is unauthenticated. The Chinese Remainder Theorem is used to create a novel approach to designing distributed group key agreement systems (CRT). The approach presented by Zheng [28] is a centralised CRT-based protocol.

III. PROPOSED MEHTOD IMPLEMENTATION

In [1], we presented our proposed method for group key management scheme for wireless sensor networks.

A. GKMP Algorithm Overview –

The entire network is divided into groups. Each group is having one Key Generation Center (KGC) and other participating clients. Group key management method executed within a group which is facilitating a common key among KGC and participating clients. The below random secret value generation algorithm generates distinct random parameters to each client and KGC. These parameters are used during the client's authentication with KGC and group key communication.

B. Proposed GKMP

1. Initialization:

• Choose n, where n : group size, KGC: Key Generation centre, $c_i, 1 \leq i \leq n$: no. of participants.

• The KGC selects two large safe primes p and q

$(i.e\ p' = \frac{p-1}{2}\ and\ q' = \frac{q-1}{2}\ 1\ are\ also\ primes)$

and compute $n = pq;$

Then KGC runs **Setup** algorithm input for this algorithm is k (security parameter) and outputs params=(q, G_1, G_2, G_T, e).The message space is $Z/qZ.$ where G_1, G_2, G_T are cyclic groups of prime order q and $e : \{G_1 \times G_2 \longrightarrow G_T\}$. KGC also runs **Key generation** algorithm, the outputs public key and secret key pair, where KGC keeps the secret key with it and gives the public key to all users during user registration phase. Where public key is the tuple $\langle P_1, P_2, U, V, z \rangle$ and secret key is the tuple h $P_1, x, yi, U = xP_2 \in G_2$ (P_1 is a random generator from G_1) and $V = yP_2 \in G_2$ (P_2 is a random generator from G_2), $z = e(P_1, P_2) \in G_T$.

2. User Registration:

• Each user $U_i, i = 1, 2, \cdots, m,$ shares a long-term secret $(x_i, y_i) \in Z_n^* \times Z_n^*$ and public key $\langle P_1, P_2, U, V, z \rangle$with the KGC.

3. Round 1: User U_1:

• User send request to KGC: $U_1 \rightarrow$ KGC: $\{U_1, \ldots.., U_t\}$

4. Round 2: The KGC:

- Computes $m = h(U_1, \ldots.., U_t),$
- Let m be the message to sign and let $\langle P_1, x, y_i \rangle$be the secret key,
- Picks a random $r \in (Z/qZ) - \frac{x+m}{y}$,
- Compute $\sigma = (x + m + yr)^{-1} P_1 \in G_1$ (the inverse $(x + m + yr)^{-1}$ is computed module q),
- Broadcast $\langle \sigma, r \rangle$ to all users.

5. Round 3: Each user $U_i, i = 1, 2, \ldots., t:$

Each participant uses a pair $\langle \sigma, r \rangle$ and public keys $\langle P_1, P_2, U, V, z \rangle$ calculates as follows.

- Computes $m = h(U_1, \cdots, U_t)$
- Return valid if $e(\sigma, U + mP_2 + rV) = z,$ otherwise return invalid.
- Each user chooses a random integer R_i from Z_n^*.
- Sends $U_i \longrightarrow KGC : R_i$.

6. Round 4: KGC compute and broadcast

KGC transmits group secret key to each client $S = \{ID_1, ID_2, \cdots, ID_n\}$ then KGC calculate and send the commitments as follows:

• Randomly selects Group Key $K \in G_1$.

• Choose $R \in Z_p^*$ randomly and compute $HS = (C_1, C_2, C_3)$, where,

– $C_1 = K.\hat{e}(g, g)^R$

– $C_2 = U\,H(x_i, y_i)$

– $C_3 = g\,m.R$

• KGC broad cast commitments HS to each client ID_i .

7. Group Key $(\mathbb{K})$ Computation:

• Each client $ID_i \in S,$ Compute the common group key as follows:

– $K = \frac{C_1}{\hat{e}(C2.C3, g^{\sigma_i})}$

Successful computation of group key, each client ID_i use this for decryption of the cipher text.

8. Key Verification

• Each Participant S_i , compute $Auth^1 = H(K, S_1, S_2, \cdots, S_n, r_i);$

– $flag \leftarrow 1$

– $For\ i = 1, \ldots, n$

∗ If Auth = $Auth^1$, $flag = flag * 1$, else $flag = flag * 0$

– If $flag = 0$, return $\perp$

– Else, Return $\mathbb{K}$

B. Correctness

In this subsection, we present the correctness of the proposed Group Key Management Protocol.

$$\frac{C_1}{\hat{e}(C2.C3, g^{\sigma_i})} = \frac{C_1}{\hat{e}(g^{H(x_i,y_i).R}.g^{m.R}, g^{(H(x_i,y_i).R+m)^{-1}})}$$

$$= \frac{C_1}{\hat{e}(g^{H(x_i,y_i)+m).R}, \frac{1}{g^{(H(x_i,y_i)+m}})}$$

$$= \frac{K.\hat{e}(g,g)\,R}{\hat{e}(g,g)R} = K \qquad (4.1)$$

IV. RESULT AND DISCUSSION

The findings of the suggested GKMP Method on the NS2 simulator are presented in this section. Different network topologies were selected in our experiment to simulate key management (KM) in the NS2 simulator. The routing protocol is used to mimic a cluster of 70 nodes in a topography. The nodes in the topology of the network are picked at random.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

Simulation procedure: We used tcl (Tool command language) for the front end and C++ for the back end in the NS2 simulator. - is the primary file; dsdv.cc - is the routing protocol; clust - is the file that deals with node location and cluster colours. It also determines the coverage range. - is the network animator; God - is the general operating director, which monitors each node within the cluster; pairkey - is in charge of pairwise key generation; clus1 - is in charge of adding the agent for each node (TCP agent is required for data transmission); - bloom filter is in charge of node authentication. It is used to keep adversaries at bay while communicating.

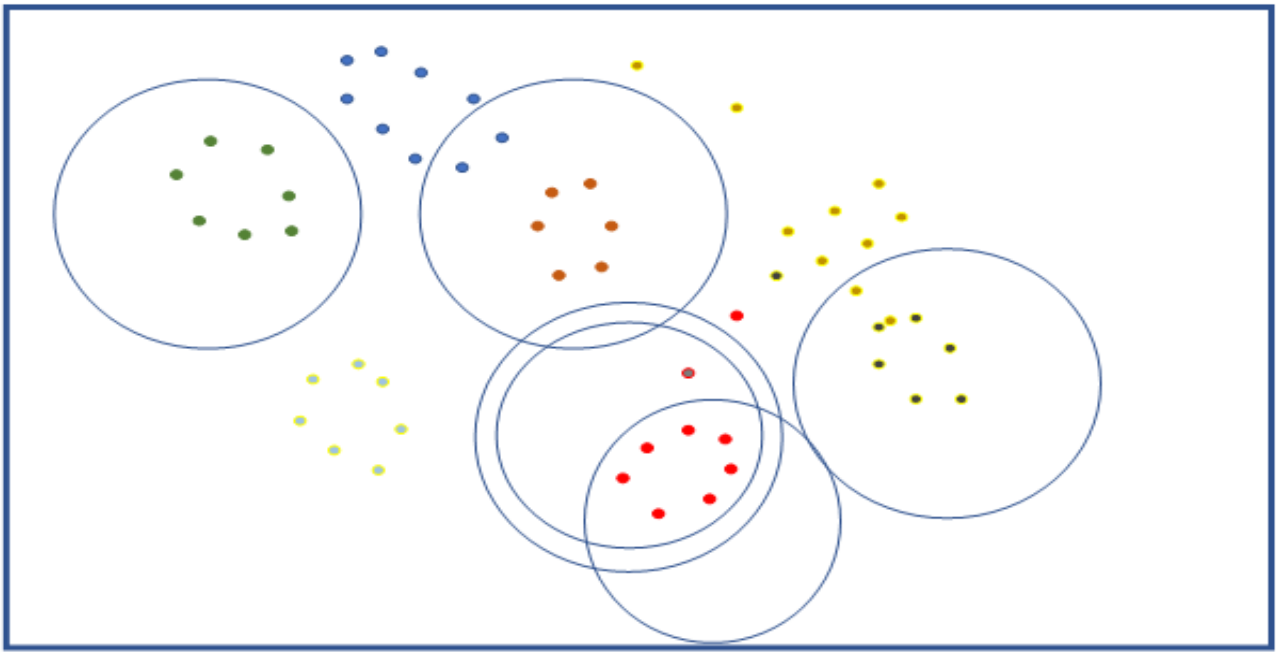


Fig 1: Sensor node deployment

Sensor node deployment - Figure 1 depicts the deployment of sensor nodes. The sensor nodes are first installed in the network area in this step. The topology also specifies the total number of nodes. Path-Key Establishment Among Nodes - The path key between sensor nodes is established in this step. Figure 1 shows an example of this process (c).

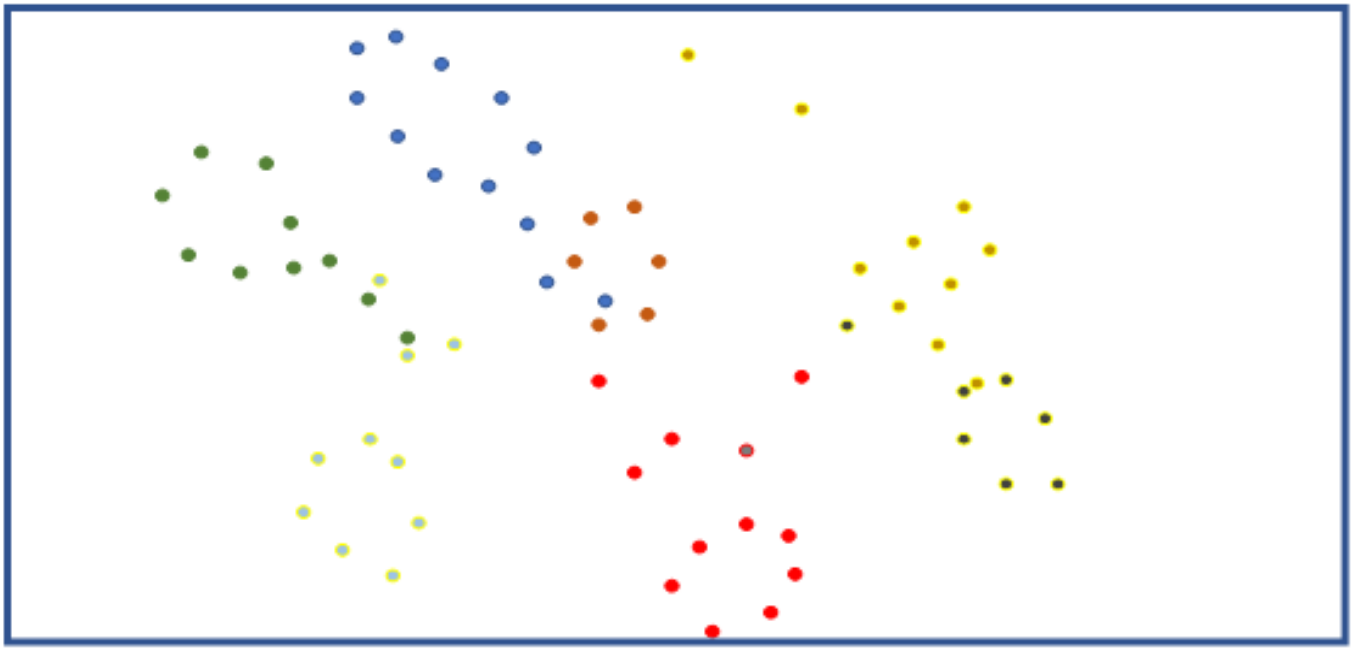


Fig 2: Cluster formation

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

Data transmission - After key establishment, data transmission in a secure manner will happen inside network.

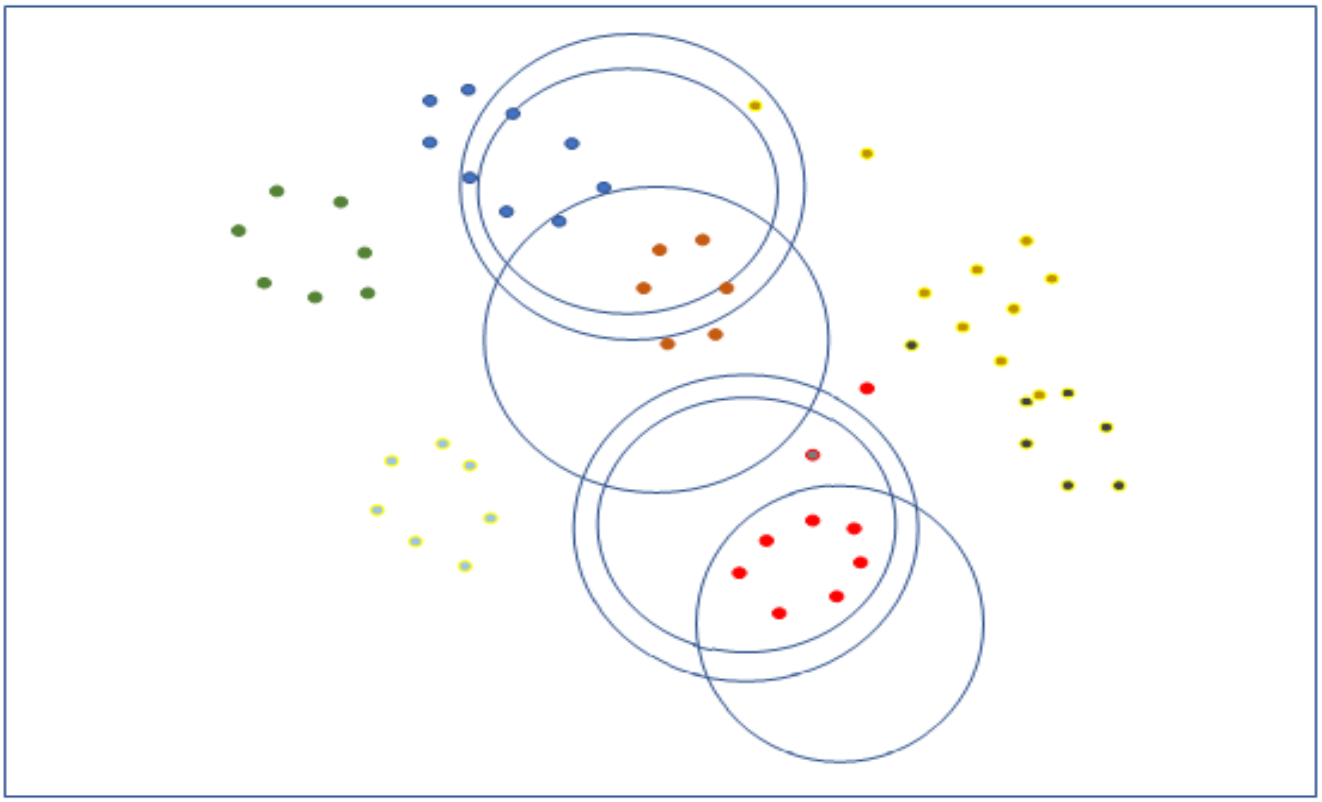


Fig 3: Path Key Establishment

Node/Member Added in a network chunk - This step deals with the new node addition in the network.

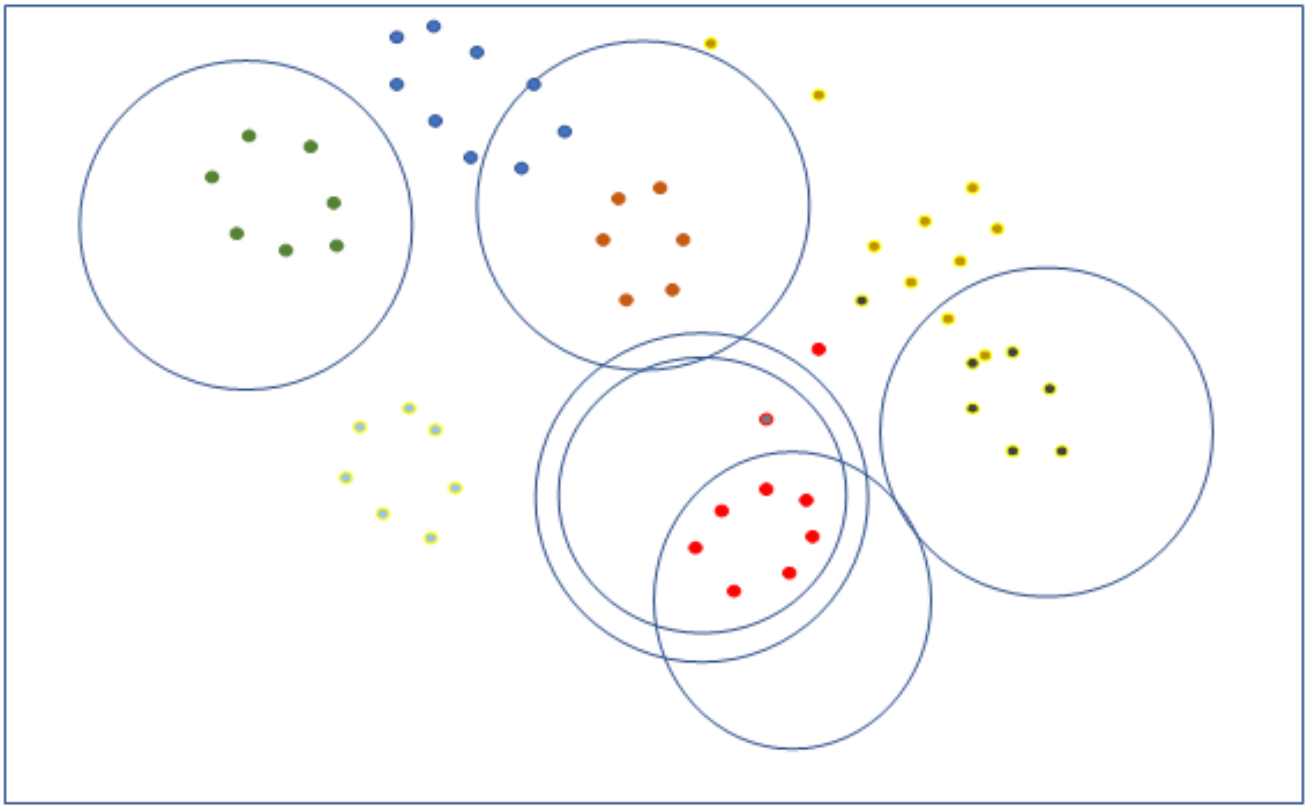


Fig 4: Node Add/Leave Operation

Retrieval Number: 100.1/ijrte.E67780110522
DOI: 10.35940/ijrte.E6778.0310622
Journal Website: www.ijrte.org

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

graph presented in fig. (5) is - Total utilization of bandwidth in network cluster.

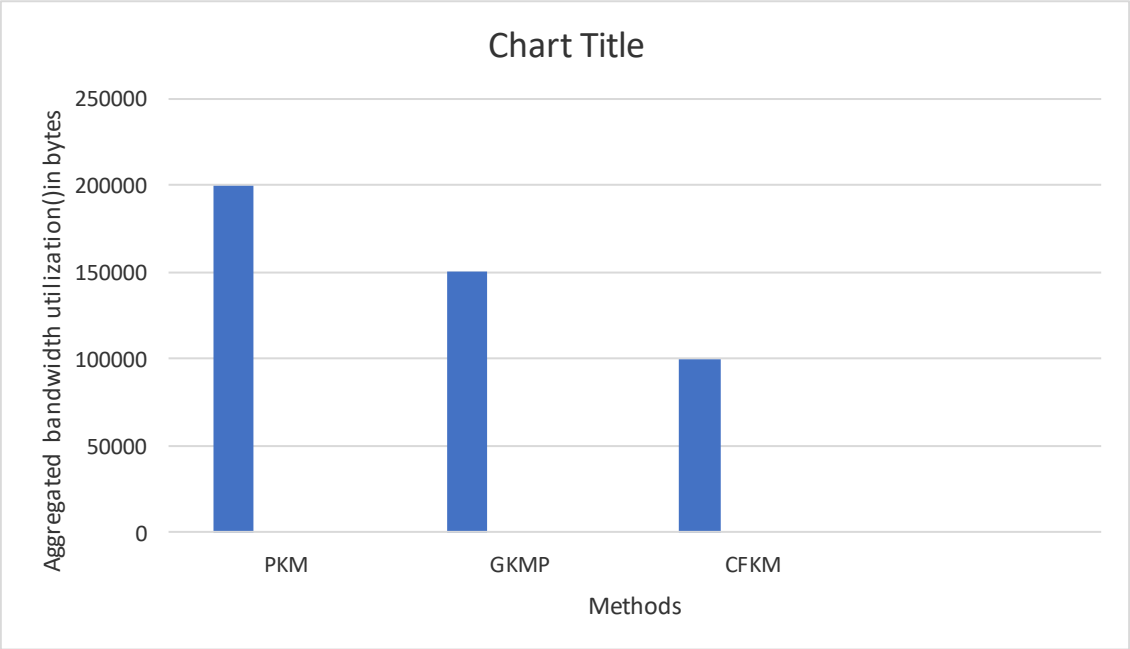
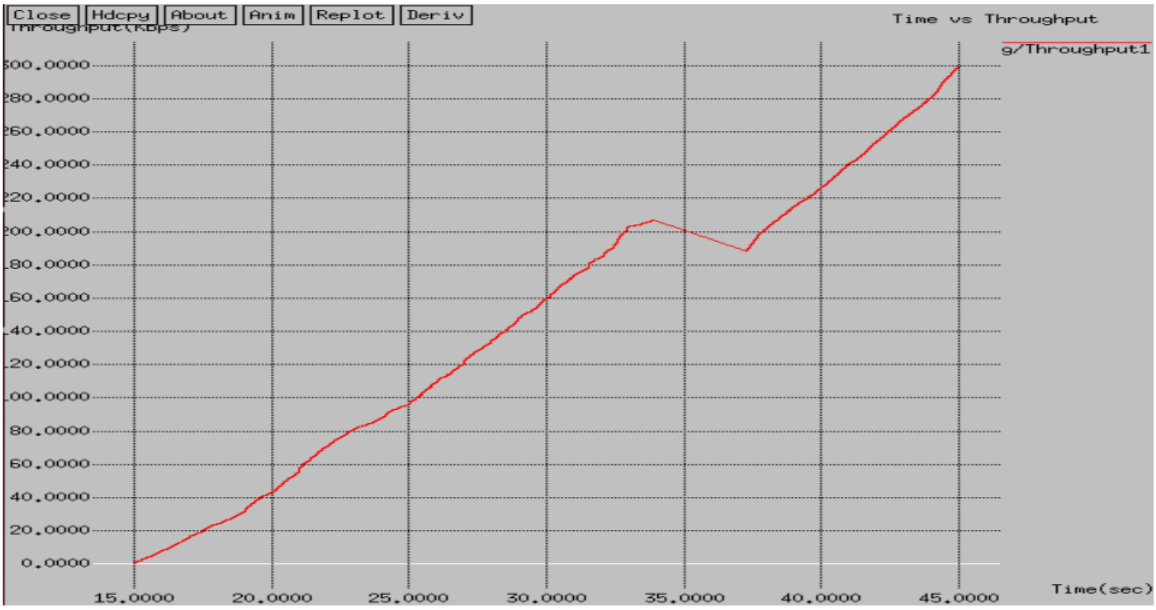


Fig 5: Total Utilization of Bandwidth



The above graph presented in fig. (6) is - time vs throughput in pairwise key management.

Fig 6: Time vs Throughput

V. CONCLUSION

A Group Key Management procedure or method allows a group of people to create a shared secret across an open network. The protocol enables group members to generate a common encryption key, as well as providing key security and unknown key share characteristics. The suggested scheme's security is also explored. The proposed protocol was tested in the NS2 simulator, and the results are presented.

REFERENCES

1. A.V.V.S. Murthy and P. Vasudeva Reddy, An Efficient Group Key Management based on Bilinear Pairings, Journal of Computational Information Systems, Volume15, Issue2, pp 1-10, 2019.
2. S. Rafaeli and D. Hutchison, A survey of key management for secure group communication," ACM Computing Surveys, Volume 35 Issue 3, Sept. 2003.
3. Q. Zhang and Y. Wang. A centralized key management scheme for hierarchi-cal access control. In IEEE Global Telecommunications Conference (Globe-com'04), volume 4, pages 2067-2071, 2004.
4. H. Harney, C. Muckenhirn, and T. Rivers, Group key management protocol architecture," IETF, RFC2093, 1997.
5. H. Harney and E. Harder, Logical key hierarchy protocol," draft-harneysparta-lkhp-sec-00.txt, IETF Internet Draft, 1999.
6. G. Horng, Cryptanalysis of a key management scheme for secure multicast communications" IEICE Trans. Commun., vol. E85-B, no. 5, pp. 1050{1051, 2002.

7. D. McGrew, A. David, T. Alan, and A. Sherman, \Key establishment in large dynamic groups using one-way function trees," TIS Report no.0755, TIS Labs at Network Associates, Inc., Glenwood, MD, 1998.
8. B. Zhou, S. Li, Q. Li, X. Suna, X. Wang, An e cient and scalable pairwise key pre-distribution scheme for sensor networks using deployment knowl-edge, Computer and Communication 32 (2009) 124-133.
9. Y. Zhang, W. Yang, K. Kim, M. Park, An AVL Tree-Based Dynamic Key Management in Hierarchical Wireless Sensor Network, in: International Con-ference on Intelligent Information Hiding and Multimedia Signal Processing, 2008.
10. R.K. Balachandran, B. Ramamurthy, Z. Xukai, N.V. Vinodchandran, CRTDH: an e cient key agreement scheme for secure group communications in wire-less ad hoc networks, in: IEEE International Conference on Communications, (ICC 2005), vol. 2, May 2005, pp. 1123-1127.
11. R. Bhaskar, D. Augot, V. Issarny, D. Sacchetti, An e cient group key agree-ment protocol for ad hoc networks, in: IEEE Workshop on Trust, Security and Privacy in Ubiquitous Computing, Taormina, Italy, 12-16 June 2005.
12. S. Zhu, S. Setia, S. Xu, S. Jajodia, GKMPAN, An e cient group rekey-ing scheme for secure multicast in ad-hoc networks, in: MobiQuitous, IEEE Computer Society, 2004, pp. 42-51.
13. Xiaobing He, Michael Niedermeier, Hermann de Meer," Dynamic Key Manage- ment in Wireless Sensor Networks: A Survey". Journal of Network and Computer Applications, December 28, 2012.
14. X. Zheng, C.T. Huang, M. Matthews, Chinese remainder theorem-based group key management, in: Proc. of the 45th ACM Southeast Regional Conference, 2007.
15. G.-H. Chiou, W.-T. Chen, Secure broadcasting using the secure lock, IEEE Transactions on Software Engineering, 15 (8) (1989) 929-934.
16. K. Drira, H. Seba, H. Kheddouci, ECGK: An efficient clustering scheme for group key management in MANETs, Computer Communications 33 (2010) 1094-1107.
17. Xixiang Lv, Hui Li, Baocang Wang, Group key agreement for secure group communication in dynamic peer systems, J. Parallel Distrib. Comput. 72 (2012) 1195-1200.
18. Yang Yang, Yupu Hu, Chunhui Sun, Chao Lv, Leyou Zhang, An Efficient Group Key Agreement Scheme for Mobile Ad-Hoc Networks, International Arab Journal of Information Technology, Vol. 10, No. 1, January 2013.
19. Chingfang Hsu, Bing Zeng, Guohua Cui, Liang Chen, A New Secure Authenticated Group Key Transfer Protocol, Wireless Pers Commun (2014) 74:457-467.
20. Ramzi Bellazreg and Noureddine Boudriga, DynTunKey: a dynamic distributed group key tunneling management protocol for heterogeneous wireless sensor networks, EURASIP Journal on Wireless Communications and Networking 2014, 2014:9.
21. Ruxandra F. Olimid, On the Security of an Authenticated Group Key Transfer Protocol Based on Secret Sharing, ICT-EurAsia 2013, LNCS 7804, pp. 399-408.
22. Cheng Guo and Chin-Chen Chang, An authenticated group key distribution protocol based on the generalized Chinese remainder theorem, Int. J. Commun. Syst. 2014; 27:126-134.
23. T. Elgamal, A public key cryptosystem and a signature protocol based on discrete logarithms, pp. 469-472, 31, IEEE Transactions on Information Theory, 1985.
24. Hayotjon Aliev, HyungWon Kim, Proceedings of Symposium of the Korean Institute of communications and Information Sciences, , 2018, 664-665
25. Esfahani, A., Mantas, G., Rodriguez, J., Neves, J.: An efficient homomorphic MACbased scheme against data and tag pollution attacks in network coding-enabled wireless networks. Int. J. Inf. Secur. 16(6), 627–639 (2017).
26. R. Vijaya Saraswathi, L. Padma Sree, K. Anuradha. "Dynamic group key management scheme for clustered wireless sensor networks" , International Journal of Grid and Utility Computing, 2020.
27. B Murali Krishna1, B.T. Krishna2, K Babulu, Hardware Implementation of Stockwell Transform and Smoothed Pseudo Wigner Ville Distribution Transform on FPGA using CORDIC Algorithm, International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878 (Online), Volume-10 Issue-5, January 2022.
28. Wannarisuk Nongbsap , Madan Mohan Singh, A Cryptographic Application of the M-Injectivity of $Mn(Zp)$ Over Itself, International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878 (Online), Volume-10 Issue-4, November 2021.

AUTHORS PROFILE

A. V. V. S. Murthy, M.Sc., M. Phil., M. Tech., Working as an Assistant Professor in the Department of Mathematics, Dr.S. R.K. Govt. Arts College, Yanam (Affiliated to Pondicherry University). Presently Pursuing Ph.D,in the Department of Mathematics, Jawaharlal Nehru Technological University, Kakinada. His area of interest and research is Croptography. He had 19 years of experience in teaching. He has published six research articles in international journals /Books and presented five papers in international and national Conferences/Seminars.

P. Vasudeva Reddy, received the M.Sc. and Ph.D. degrees from S. V. University, Tirupati, India, and the M. Tech. degree in CST-networks from Andhra University, Visakhapatnam, India. He is currently a Professor with the Department of Engineering Mathematics, Andhra University. He has several publications in reputed national and international journals. His current research interests include cryptography, information security, algebra, and number theory applications. Dr. Reddy is a reviewer and an advisory board member for several journals. He is a Life Member of the Indian Mathematical Society and the Cryptology Research Society of India.