ISSN: 2584-0495 Vol. 2, Issue 2, pp. 548-555

International Journal of Microsystems and IoT

ISSN: (Online) Journal homepage: https://www.ijmit.org

Group Key Management Schemes, Issues, challenges and opportunities: A Survey

Rohit Bathla, Priyanka Ahlawat

Cite as: Bathla, R., & Ahlawat, P. (2024). Group Key Management Schemes, Issues, challenges and opportunities: A Survey. In International Journal of Microsystems and IoT (Vol. 2, Number 2, pp. 548-555). https://doi.org/10.5281/zenodo.10792507

© 2024 The Author(s). Published by Indian Society for VLSI Education, Ranchi, India

Published online: 20 February 2024

Submit your article to this journal:

Article views:

View related articles:

View Crossmark data:

DOI: https://doi.org/10.5281/zenodo.10792507

Full Terms & Conditions of access and use can be found at https://ijmit.org/mission.php

International Journal of Microsystems and IoT
Vol. 2, Issue 2, pp. 548-555; DOI: https://doi.org/10.5281/zenodo.10792507

Group Key Management Schemes, Issues, challenges and opportunities: A Survey

Rohit Bathla[1], Priyanka Ahlawat[1]

[1]Department of Computer Science and Engineering, National Institute of Technology, Kurukshetra, India

ABSTRACT
With the growth and advancement in WSN, group communication's associated areas like teleconferencing, stock market, and distance education have also seen growth. Security in group communication- based applications needs to be maintained. This paper surveys various group key management schemes in WSNs. We explore key-based surveys in wireless networks and analyze multiple performance circumstances like storage, computation, and delivery costs during group communications join and leave operations. It is essential to ensure the safety of group keys and safe communication. It will enable them to make better decisions. For communication in WSNs, Key management and distribution is an essential security service. The key management scheme should signify security, robustness, and efficiency for reliable communication. The Paper further concentrates on the benefits, limitations, and security vulnerabilities of these protocols. That Paper includes the study of unique algorithms, including the four basic parameters: Computation Cost, Communication Cost, Rekeying cost, and key Storage cost.

KEYWORDS
Key management security, rekeying, Group controller, Security, Key Independence

1. INTRODUCTION

The key distribution and management is very important for secure communication inside WSN. Our main focus is to find feasible key distribution and management solutions for secure WSN. Establishing a secure communication is an open, difficult issue for WSN which involves key distribution and management. The solutions for key management use administrative keys i.e. key encryption key for safe efficient and complete distribution to generate safe channel. Session keys i.e data encryption keys for communication nodes. Session key are of pair wise key with in any two sensor nodes which are in a directly or indirectly communication or may be group wise key that shared by a group of nodes. Network keys whether it is administrative key or session keys require to be changed for secure and resiliency to attack, failure and network structure changed .The key management in WSN can be classified as static solutions and dynamic depends upon pre or post deployment of administrative keys. They are further classified as homogenous or heterogeneous depends upon the behavior of nodes inside WSN. Nodes in homogenous scheme perform the same function and in heterogeneous scheme are assigned different role. The information is encrypted with secure keys that give authentication for sender node is further responsible for safe communication Therefore, for the security of the whole network, nodes use more than one single key. The point of group-based communication, which includes any number of sensor nodes, can be quite experienced from the ongoing real- world applications, like online games, online education, mail system, Skype chat, Facebook and Twitter, etc. Group communication holds speedy growth in the networking background, and security continues a significant challenge. Besides the social networks, primary safe conditions similar to a military network, in which several unstable data is exchanged, forever require a private, safe environment for data transfer, group control, and key administration. Accordingly, the group information safety depends on the privacy and strength of the group key utilized. An additional and essential purpose is a rekeying scheme while the group grows in dynamic situations. Network independent and Network dependent oriented key management protocols usually are management protocols.

© 2024 The Author(s). Published by Indian Society for VLSI Education, Ranchi, India

2. RELATED WORK

The effective use of the LKH scheme to promote group key management by employing a hierarchical structure. A. Likely, it can involve all tree-like structures. The data needed during rekeying had reduced the comparison to GKMP. At the same time, the grade improvement, the group member's keys reduce because of a shorter tree power [1-2].

Inside OFT, a tree-based structure had used for the key generation. OFT uses the complementary tree formatting as LKH toward holding the keys. Beneath that scenario, the quantity of knowledge demanded rekeying declines to half the entire piece of data in rejection of the LKH approach [3].

NSGC transmits keys for nodes and delivers safety with minimal cost. The apiece nodes or the distinctive key were used to estimate the group transmission, called the stationary group key. To lower the transmission cost, during the encryption method particular self- invertible matrix must operate [4].

CBHKDP protocol operates the ECC encryption method for efficient transmission and sufficient estimation cost. Either key server or associate supplies all the keys to minimize the number of rekeying messages. This protocol is adequate for dispersed conditions [5].

KMSGC is an enhanced protocol established on a collection system. Inside the cluster and illustrates various problems, e.g.,

decreased scalability, delivery period, and inferior operational commonness. In destiny, the method underestimates energy consumption by the individual node but grows WSN life [6-7]. The presented method was used to decrease the number of keys contained at the component's node. ECEGKM protocols induce the stationary group key to lowering estimation cost and complexness [8-9].

SKDPMC is a key allocation protocol that operates Euler's Totient process to improve safety components and limit estimation and transmission costs. Exponential procedures had used to calculate the group key [10].

Star topology-based multicast network had used to supply efficient and secured transmission. Secret keys are computed individually and uniquely in everyday practice and released with the node leaving strategy to lower rekeying costs [11-13].

3. GROUP KEY MANAGEMENT

3.1 Importance of Group key Management:

- According to the security framework it is a set of processes that always support key maintenance and establishment for keying relations within trusted parties.
- For group communication administration of group key is very important.
- For providing secure communication in WSN without any overhead.
- Dynamically set up and support a secure channel among communicating nodes.
- Provided low computation, communication and storage overheads.
- Support multicast, unicast and broadcast communication.

3.2 Role of Group Key Management:

- Confidentiality within Groups: Any node that are from outside not inside, need to decrypt all the data that we are transfer within groups.
- Integrity: Inhibit the incoming of illegal node from outside and only secure nodes within the system update the key.
- Scalability: Scalability is that feature that makes system capable to effectively address the some issues regarding change of group size.
- Access Control: Always gives some access control for all the members of group and prevent it against unauthorized access control inside group communication.
- Authentication: Authentication is very crucial term for the safety of the system over intruders
- Availability: Accessing information in a timely manner.

3.3 Applications Area of Group Key Distribution and Management in WSN:

- Smart Building: Group communication is the major requirement in smart city and buildings. For the consumption of low power and home and building security a secure key distribution and management is required.
- Health care and monitoring: For real monitoring of health signals and present further risk that may occur in its life.
- Vehicle Tracking: For presenting congestion in traffic, parking system and vehicle location.
- Agriculture: Sense the parameter like temperature, pressure and ensure accurate environment conditions.
- Security and Surveillance: For detection of the enemies early and tracking of the vehicle.

3.4 Steps for group key management:

- **Key generation:** The process of generating the all and unique group is called key generation phase that help key distributer center for distribution of the group key for each and every genuine user.
- **Key distribution**: Group members are geographical dispersed and easily move within WSN from one area to other. For efficiently delivery of group key to every genuine member is the most critical task.
- **Key updating**: For the modification inside the group, key must altered for every join and leave operation. Key updating is taking for assuring backward and forward secrecy.

3.5 Major research issues/requirements of Group key management:

Security issue:

- Forward secrecy: Whenever any group member tries to leaves own group then it must guaranteed that it should not get any further future group key.
- Backward secrecy: It always tends to prevent from any of new group member that being are able to decrypt any information that it has been communicating before joining within group.
- Collusion attacks freedom: Leaving members always have to operate with each other for presenting group key by taking the old key materials.
- Minimal Trust: Any third components inside Group key management schemes never be trusted.

QoS issue:

- Low bandwidth overhead: Rekey inside the group members should not influenced by very large number of transferring the messages.
- 1 Affect N: when a single membership changes join or leave process, so it applies various member within group.
- Minimal Delay: It deals with to the least transmission delay within the delivery of packets whenever the multicast operations are used.
- Availability of services: The complete multicast environment is not influenced by the failure of node.

Group member issue

- Low storage: Number of minimum keys required for communications that key server work fast and efficiently.
- Low Computation: Is to increase the efficiency with the response during of key within server for every group members.

4. CLASSIFICATION OF GROUP KEY MANAGEMENT

4.1 Centralized key management scheme:

Inside environment that schemes there is a centralized single entity that is Key Distribution Centre (KDC) that are responsible for all group activities. There is also a hierarchical structure of keys to facilitate key management during the process of key distribution, Key generation and key updating. The centralized scheme is one of the most utilized and best schemes.

The major challenges with the centralized scheme include:

- **Scalability overhead:** Scalability is the issue with centralized scheme this makes the scheme not suited for large and dynamic wireless applications. Inside this group communication total success totally depends upon the single centralized entity. Rekeying is becomes total overhead when group size change.
- **Storage overhead:** Total keys that are secured for a safe session. As the size is increases the storage becomes one major overhead. As the group users are increases, members are required to process larger rekeying data.
- **Forward and backward secrecy:** As a new user joins within the group and the old user wants to leaves such group.
- **Communication and computation inefficiency:** when we deal with multiple members there is communication inefficiency during rekeying process among the various groups.
- **Collusion independence:** Co-operation within members that are expelled, they work together, share their data and try to access group key.

Advantages:

- It is a straight forward scheme that easily calculates the cost of communication, cost of computation and storage cost
- Implementation is very easy.

Limitations:

- Scalability makes the system unsuitable for dynamic applications.
- Rekeying there are decay in communication within groups when there is memberships change.

Secure Lock approach:

This one is a centralized management in which single end-entity builds a rekey manner while a member goes inside a single broadcast manner. Chinese Remainder computation is done by the central entity that performs on each communication before forwarding it. Rekey connections is decreased. In this scheme, the central one that allots a definite positive number m_i and receives hidden value k_i among every group member. It creates random number i, whenever the central entity needs to transmit a data to every members within group.

LKH (Logical Key Hierarchy Protocol):

The approach was a systematic key management algorithm. The significant participation of LKH to promote group key management is to use a hierarchical arrangement. Probably, it can apply to all hierarchical tree structures. Due to the specific unique verification node services of a binary tree, we can apply a tree to illustrate LKH. In an LKH key tree, the root holds the TEK, the tree's internal nodes keep supporting keys Key Encryption Keys. A pair-wise KEK is held by group members correlated with each one leaf node.

One-way Function Tree Protocol:

It's essential against LKH because it permits all group members to compute key locally to reduce computation and delivery costs. Each group members include KEK, not the root entity that carries it out. OFT utilizes the corresponding tree composition as LKH for controlling these keys. Each group key does that root key that works a unique leaf node associates individually member easily and recognizes a collection of KEKs of its leaf node to every root. It is an expansion to the work of LKH, where the numbers of rekey messages are reduced to log2n.

Centralized Flat table Key Management:

In that process, to reduce this portion of keys maintained with these Key servers, the key server maintains a flat record rather than a hierarchical tree concerning keys. The central entity decreases the charge of managing keys by the CFKM system that works on flat records to collect the keys. One is connected with all reasonable states of single bit 0 or 1. Whenever a right member moves the group, the tool shall renew all keys reported to that departing licensed member with the control of forwarding secrecy.

4.2 Decentralized Group Key Management scheme:

The main focus of the decentralized scheme is to decrease KDC load. Key Distribution Center is the central entity. Group members are split into subgroups and every subgroup is controlled by own controller within subgroup. Single point failure problem is resolved by this scheme. The decentralized approach are membership driven protocols.

Challenges of decentralized scheme.

- For distribution of key messages to subgroup, how effectively that method work with many management of group key schemes.
- Trust relationship within the third parties.
- Authenticating the group members that are participating inside the session, that may be inside the same or different system

  .

Advantages:

- For large wireless networks applications, this scheme

provides a roadmap to address group key management.

- For address 1-affect-N phenomenon.

Limitations:

- For comprehensive solution, this scheme needs to correlate with all other management of group key approaches.
- It cannot work alone; always require third party trust relationship.

SMKD (Scalable Multicast Key Distribution):

In a multicast model, Protocols use a tree form and thus group all keys with group members. Architecture must be divided into two kernels: In the first kernel, the multicast tree is rooted, including in that secondary kernel that is used during validation. The developed kernel verifies these nodes they require to register the group. Therefore, the main kernel catches that authentication to spread the keys by including ACL, though some central focus is created. There is no explanation for corresponding security characteristics similar to forward secrecy in this system, unlike any recreation with a strange group externally leaving different group segments.

Lolus :

Lolus offered a composition for multicasting scalability with the reliability that utilizes an authority about subgroups that conduct group key control to address scalability. This extensive group is divided into different subgroups that make a tree-based arrangement. Each subset should possess a group intermediate security controller or a group security agent. There is GSC that handles GSI on every tree's highest level. Individually subgroup holds its subgroup key.

Dual Encryption Protocol:

A sub-group manager inside this protocol performs the group members' hierarchy, and controlling each sub-group is proposed. Each segment inside the sub-groups package decrypts that information and then, by decrypting the message, recovers DEK. Therefore, the DEK package does not signify re-calculation whenever a member understands both keys. Within that mechanism, this third function of supervision is involved in the design of SGM that constantly reliable individual key including an introduction to the group key (DEK).

In STB :

In this scheme, committed routers are used only. These routers and receivers include public and private pairs of keys. Public key will produce from every public used key, that essential to identify one within public key of all used neighbors. Later getting data to a router must decrypts all the message by applying the DEK and re-encrypts further with applying the neighboring routers' DEK and public keys. Any intruder does not modify this encrypted data packet. Now more new packets are forwarded to different routers.

Kronos:

Within such protocol, group rekeying appears at a selected time, not for group revision. Kronos' composition is really extremely comparable over IGKMP, although there exist significant pair variations among them. One is, the DKD is obliquely included in the traffic key. Other, recurrent rekeying executes decoupling this repetition of rekeying of group scope and progressive development in society. Pair of circumstances require Kronos to operate flawlessly. All AKDs should offer the same transactions encryption key utilizing clock synchronization custom. The second part is that every AKDs requirement shares the corresponding key production algorithm. So, this identical key is created for each event. Kronos continuously produces a new group key that is based upon this former group key. Thus, for example, the key is declared, and then each keys notice is compromised. This is the bottleneck difficulty about Kronos.

Hydra:

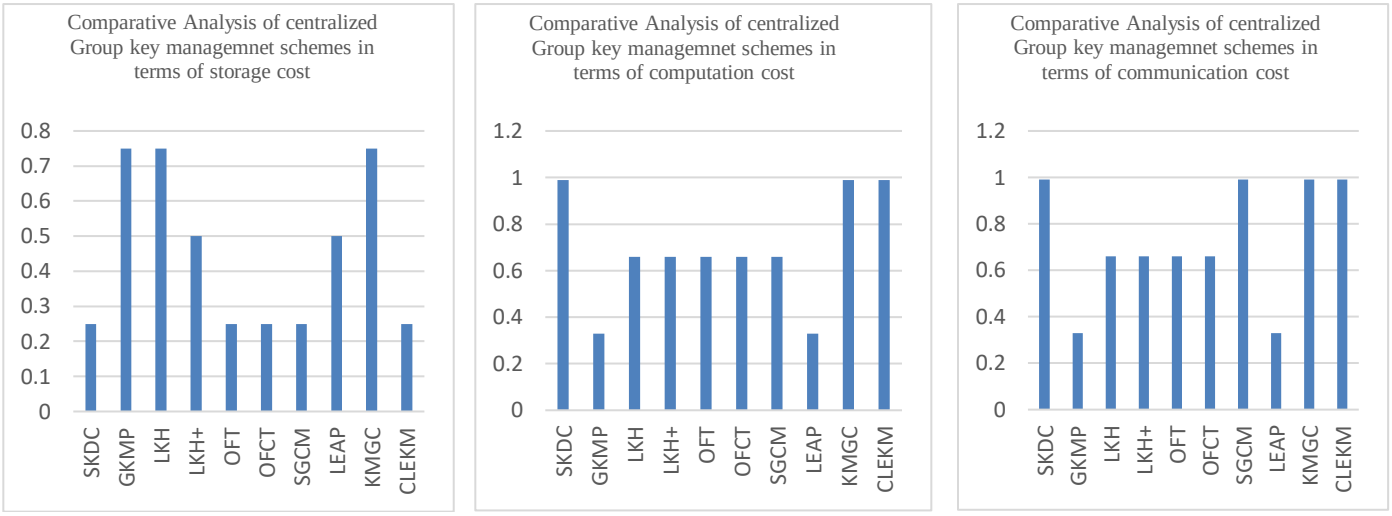
This top-level is linked among the Hydra Servers, including this bottom level denotes connected including the segments. Group the components receive a Group Key in every group to ensure group interaction. Everything the HSS forwards the Hydra Key toward interacting among the HS group. Hydra works on the bottleneck difficulty. Hydra does not handle the centralized controller during group key production; also, it can withdraw a unique time of defeat.

Table .1 Comparison analysis of centralized group key schemes

CGKM Schemes	Forward secrecy	Backward secrecy	Anti Collision	Integrity	Confidentiality	Authentication	Rekeying	Robustness	Independent
SKDC [16]	YES	YES	NO	NO	yes	NO	YES	NO	YES
GKMP [17]	NO	YES	NO	NO	no	NO	YES	NO	YES
LKH [18]	YES	YES	NO	NO	YES	NO	YES	NO	YES
LKH+ [19]	YES	YES	NO	NO	YES	NO	YES	NO	YES
OFT [20]	YES	YES	NO	NO	YES	NO	YES	NO	YES
OFCT [21]	YES	YES	YES	YES	YES	NO	YES	NO	YES
SGCM [22]	NO	NO	YES	YES	YES	NO	NO	NO	YES
LEAP [23]	YES	YES	NO	NO	YES	NO	NO	NO	YES
KMGC	YES	YES	NO	YES	YES	YES	YES	YES	YES
CLEKM	YES	YES	YES	YES	YES	YES	YES	YES	YES

Table .2 Cost Comparison of centralized group key schemes

CGKM Schemes	Computation cost	Communication cost	Storage cost	Key pupation	Cryptography used
SKDC	O(n)	O(n)	O(n)	Member driven	DH
GKMP	2E/2D	2K	2K	Member driven	DH,RSA
LKH	O(log n)	O(log n)	O(n)	Member driven	Symmetric
LKH+	O(log n)	O(log n)	O(n)	Member driven	Symmetric
OFT	O(log n)	O(log n)	O(n)	Member driven	Symmetric,Hash
OFCT	O(log n)	O(log n)	O(n)	Member driven	Symmetric,Hash
SGCM	O(b)	O(s)	O(n+s)	Time Driven	XOR,Hash
LEAP	O(a)	O(a)	O(a+s)	Time Driven	Symmetric,Tesla
KMGC	O(n)	O(n)	Pk/sk	Member driven	Asymmetric
CLEKM	O(n)	O(n)	Pk/sk	Member driven	Member driven



(a) Storage cost comparison (b) Computation cost comparison (c) Communication cost comparison

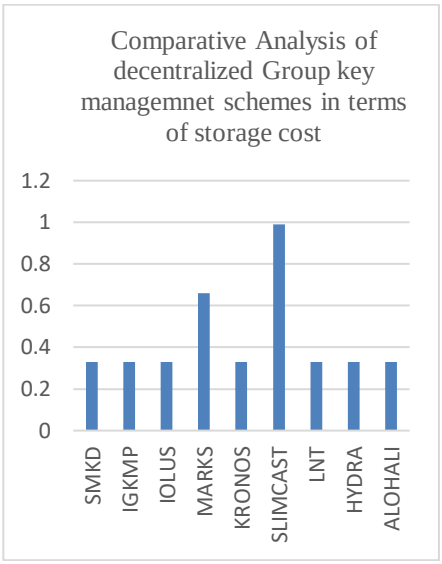
Fig. 1 (a): Storage cost, (b): computation cost, (c): communication cost comparison of centralized scheme

Table .3 Comparison analysis of decentralized group key schemes

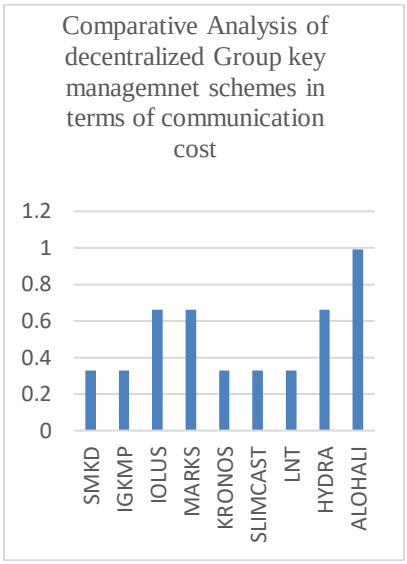
DEGKM Schemes	Forward secrecy	Backward secrecy	Anti Collision	Integrity	Confidentiality	Authentication	Rekeying	Robustness	Independent
SMKD	NO	YES	YES	NO	NO	YES	NO	NO	YES
IGKMP[24]	YES	YES	NO	NO	YES	YES	YES	NO	YES
IOLUS[25]	YES	YES	NO	NO	YES	NO	YES	NO	YES
MARKS[26]	NO	No	NO	NO	NO	NO	NO	NO	YES
KRONOS[27]	NO	YES	NO	NO	YES	YES	NO	NO	YES
SLIMCAST[28]	YES	YES	YES	YES	YES	YES	YES	NO	YES
LNT[29]	YES	YES	NO	YES	YES	YES	YES	NO	YES
HYDRA[30]	YES	YES	NO	NO	YES	YES	YES	NO	YES
ALOHALI[31]	YES	YES	YES	NO	YES	YES	YES	YES	YES

Table .4 Cost Comparison of centralized group key scheme

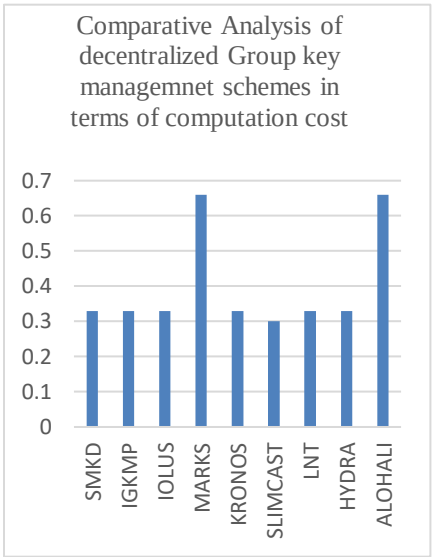
DEGKM Schemes	Computation cost	Communication cost	Storage cost	Key pupation	Cryptography used
SMKD	O(1)	O(1)	O(1)	Member driven	Symmetric
IGKMP	O(1)	O(m)	O(1)	Member driven	Symmetric
IOLUS	O(1)	O(m)	O(1)	Time driven	Symmetric
MARKS	O(log x)	O(log x)	O(log x)	Time driven	hash
KRONOS	O(1)	O(1)	O(1)	Time driven	Symmetric
SLIMCAST	O(1)	O(m)	O(n)	Member driven	Symmetric
LNT	O(1)	O(1)	(t+1)log q	Member driven	Symmetric
HYDRA	O(1)	O(m)	O(1)	Member driven	PK
ALOHALI	O(m)	O(n)	O(1)	Member driven	One way



(a) **Storage cost comparison**



(b) **Computation cost comparison**



(c) **Communication cost comparison**

Fig. 1 (a): Storage cost, (b): computation cost, (c): communication cost comparison of decentralized scheme

5 CHALLENGES FOR GROUP KEY MANAGEMENT IN IOT ENVIRONMENT

Group Key Management (GKM) in the context of the Internet of Things (IoT) faces several challenges due to the unique characteristics of IoT environments. Addressing these challenges is essential to ensure the security and efficiency of group communication. Here are some key challenges for Group Key Management in IoT:

***Scalability**:* As the number of IoT devices continues to grow, managing cryptographic keys for large-scale groups becomes increasingly complex. GKM solutions must be scalable to accommodate the dynamic nature and sheer volume of devices in IoT deployments.

***Dynamic Group Membership**:* IoT environments often involve devices joining or leaving groups dynamically. GKM systems must be able to handle frequent changes in group membership efficiently, ensuring secure communication even as group composition evolves.

***Resource Constraints**:* Many IoT devices have limited processing power, memory, and energy resources. GKM protocols need to be designed with a focus on resource efficiency to minimize the impact on resource-constrained devices.

Security Concern: Ensuring the security of group communication in the face of potential threats such as eavesdropping and unauthorized access. GKM solutions must employ robust cryptographic algorithms and protocols to resist various security threats.

Key distribution overhead: Distributing cryptographic keys to multiple devices can introduce communication overhead. Efficient key distribution mechanisms are required to minimize the impact on network resources and reduce latency.

***Efficiency**:* A good SGC has to achieve two conflicting objectives: efficiency and security. Indeed, better security often implies more computation which leads to lower efficiency. Nevertheless, most schemes can become more efficient if we can reduce the amount of data exchanged between sensor nodes.

6 APPLICATIONS OF GROUP KEY MANAGEMENT IN IOT ENVIRONMENT

Group Key Management (GKM) plays a crucial role in securing communication within groups or clusters of devices in various applications and use cases. In these diverse applications, Group Key Management is essential for establishing trust, ensuring confidentiality, and maintaining the integrity of communication within groups of interconnected devices. Its usage is critical for addressing the specific security requirements of each application and mitigating the risks associated with unauthorized access and data breaches in IoT ecosystems. Here are some key applications and usages of Group Key Management.

Table .5 Applications and usages of group key management

Application	Description	Usage of Group Key Management
Wireless Sensor Networks (WSNs)	WSNs consist of sensor nodes that collaborate to monitor and collect data from the environment.	GKM secures communication within WSNs, preventing unauthorized access to collected data and protecting against data tampering.
Smart Grids	Smart grids integrate digital communication and control technologies in the power grid infrastructure.	GKM is used to secure communication among smart meters, power devices, and control systems, ensuring the integrity of grid data.
Industrial Internet of Things (IIoT)	IIoT connects industrial devices and machinery to enable data exchange and automation in manufacturing and industrial processes.	GKM safeguards communication among connected industrial devices, ensuring the confidentiality and integrity of sensitive data.
Healthcare Systems	Healthcare IoT involves devices like medical sensors and wearable devices for patient monitoring.	GKM secures communication within healthcare systems, protecting patient data and ensuring the confidentiality of health information.
Smart Cities	Smart city initiatives use IoT to enhance urban services, such as transportation, energy management, and public safety.	GKM is crucial for securing communication in smart city networks, protecting data integrity, and ensuring the privacy of citizens.
Vehicular Ad-Hoc Networks (VANETs)	VANETs enable communication among vehicles for improving road safety and traffic efficiency.	GKM secures communication in VANETs, preventing unauthorized access to vehicle data, and ensuring the trustworthiness of communication.
Military and Defense Systems	Military IoT involves the use of connected devices for surveillance, communication, and intelligence.	GKM is employed to secure communication within military networks, protecting sensitive information and ensuring the confidentiality.
Smart Homes	Smart home IoT devices include connected appliances, security systems, and home automation devices.	GKM ensures the security of communication among smart home devices, protecting user privacy and preventing unauthorized access.
Collaborative Robotics (Cobots)	Cobots involve the collaboration between humans and robots in industrial settings.	GKM secures communication between collaborative robots, ensuring the integrity of control signals and preventing unauthorized access.
Supply Chain and Logistics	IoT is used in supply chain management for real-time tracking and monitoring of goods.	GKM ensures the security of communication in the supply chain, protecting logistics data and preventing tampering during transit.

7 CONCLUSION

In the wireless system, for group applications, group key management is essential for ensuring safety and giving secure connection within the group of keys. That paper analyzes several key management clarifications for performance and the security queries correlated with the group describes applications within WSN. Different algorithms are analyzed using cost of computation, cost of complexity, cost of rekeying, and storage cost. For preventing forward and backward secrecy, rekey is determined and communicated on each join or leave operation. The joint research purpose is to produce a mechanism for change in WSN tree structure that decreases these overheads.

REFERENCES

1. Pande, A. S., & Thool, R. C. (2016, September). Survey on logical key hierarchy for secure group communication. In 2016 International Conference on Automatic Control and Dynamic Optimization Techniques (ICACDOT) (pp. 1131-1136). IEEE.
2. Wallner, D., Harder, E., & Agee, R. (1999). Key management for multicast: Issues and architectures. RFC 2627.
3. Sherman, A. T., & McGrew, D. A. (2003). Key establishment in large dynamic groups using one-way function trees. IEEE transactions on Software Engineering, 29(5), 444-458.
4. Kumar, N. S., & Lavanya, S. (2015). A novel scheme for secure group communication in multicast network. International Journal of Security and Networks, 10(2), 65-75.
5. Kumar, N. S., Purusothaman, T., & Lavanya, S. (2013). A Performance Analysis on Cluster Based Group Key Management Schemes in Multicast Network. Archives Des Sciences, 66(2).
6. Bao, X., Liu, J., She, L., & Zhang, S. (2014, June). A key management scheme based on grouping within cluster. In Proceeding of the 11th World Congress on Intelligent Control and Automation (pp. 3455- 3460). IEEE.
7. Vijayakumar, P., Bose, S., Kannan, A., & Subramanian, S. S. (2011, February). A secure key distribution protocol for multicast communication. In International Conference on Logic, Information, Control and Computation (pp. 249-257). Springer, Berlin, Heidelberg.
8. Begum, S. J., & Purusothaman, T. (2011). A new scalable and reliable cost effective key agreement protocol for secure group communication. In Journal of Computer Science.
9. Muthusamy, S. K., Thiyagarajan, P., & Selvaraj, L. (2013). An enhanced and cost effective group key management scheme for multicast network.
10. Vijayakumar, P., Bose, S., Kannan, A., & Jegatha Deborah, L. (2013). Computation and Communication Efficient Key Distribution Protocol for Secure Multicast Communication. KSII Transactions on Internet & Information Systems, 7(4)
11. Kumar, S., PurusothamanT, N. M., & Lavanya, S. (2013). Design and performance analysis of scalable and efficient group key Management scheme [SEGKMS] for group communication in multicast networks. Life Science Journal, 10(2).
12. Saravanan, K., & Purusothaman, T. (2012). Efficient star topology based multicast key management algorithm. Journal of Computer Science, 8(6), 951.
13. Albakri, A., Harn, L., & Song, S. (2019). Hierarchical key management scheme with probabilistic security in a wireless sensor network (WSN). Security and Communication Networks, 2019.
14. Prantl, T., Zeck, T., Bauer, A., Ten, P., Prantl, D., Yahya, A. E. B., & Kounev, S. (2022). A survey on secure group communication schemes with focus on iot communication. *IEEE Access*.
15. Samiullah, F., Gan, M. L., Akleylek, S., & Aun, Y. (2023). Group Key Management in Internet of Things: A Systematic Literature Review. *IEEE Access*.
16. Li, S. Q., & Wu, Y. (2010, July). A survey on key management for multicast. In *2010 Second International Conference on Information Technology and Computer Science* (pp. 309-312). IEEE.
17. Harney, H., & Muckenhirn, C. (1997). *Group key management protocol (GKMP) architecture* (No. rfc2094).
18. Waldvogel, M., Caronni, G., Sun, D., Weiler, N., & Plattner, B. (1999). The VersaKey framework: Versatile group key management. *IEEE Journal on selected areas in communications*, *17*(9), 1614-1631.
19. Wong, C. K., Gouda, M., & Lam, S. S. (2000). Secure group communications using key graphs. *IEEE/ACM transactions on networking*, *8*(1), 16-30.
20. Sherman, A. T., & McGrew, D. A. (2003). Key establishment in large dynamic groups using one-way function trees. *IEEE transactions on Software Engineering*, *29*(5), 444-458.
21. Canetti, R., Garay, J., Itkis, G., Micciancio, D., Naor, M., & Pinkas, B. (1999, March). Multicast security: A taxonomy and some efficient constructions. In *IEEE INFOCOM'99. Conference on Computer Communications. Proceedings. Eighteenth Annual Joint Conference of the IEEE Computer and Communications Societies. The Future is Now (Cat. No. 99CH36320)* (Vol. 2, pp. 708-716). IEEE.
22. Kausar, F., Hussain, S., Park, J. H., & Masood, A. (2007). Secure group communication with self-healing and rekeying in wireless sensor networks. In *Mobile Ad-Hoc and Sensor Networks: Third International Conference, MSN 2007 Beijing, China, December 12-14, 2007 Proceedings 3* (pp. 737-748). Springer Berlin Heidelberg.
23. Zhu, S., Setia, S., & Jajodia, S. (2006). LEAP+ Efficient security

mechanisms for large-scale distributed sensor networks. *ACM Transactions on Sensor Networks (TOSN)*, *2*(4), 500-528.
24. Bao, X., Liu, J., She, L., & Zhang, S. (2014, June). A key management scheme based on grouping within cluster. In *Proceeding of the 11th World Congress on Intelligent Control and Automation* (pp. 3455-3460). IEEE.
25. Mittra, S. (1997). Iolus: A framework for scalable secure multicasting. *ACM SIGCOMM Computer Communication Review*, *27*(4), 277-288.
26. Briscoe, B. (1999, November). MARKS: Zero side effect multicast key management using arbitrarily revealed key sequences. In *International Workshop on Networked Group Communication* (pp. 301-320). Berlin, Heidelberg: Springer Berlin Heidelberg.
27. Setia, S., Koussih, S., Jajodia, S., & Harder, E. (2000, May). Kronos: A scalable group re-keying approach for secure multicast. In *Proceeding 2000 IEEE Symposium on Security and Privacy. S&P 2000* (pp. 215-228). IEEE.
28. Huang, J. H., Buckingham, J., & Han, R. (2005, September). A level key infrastructure for secure and efficient group communication in wireless sensor network. In *First International Conference on Security and Privacy for Emerging Areas in Communications Networks (SECURECOMM'05)* (pp. 249-260). IEEE.
29. Cheikhrouhou, O., Koubaa, A., Dini, G., Alzaid, H., & Abid, M. (2012). LNT: A logical neighbor tree secure group communication scheme for wireless sensor networks. *Ad Hoc Networks*, *10*(7), 1419-1444.
30. Rafaeli, S., & Hutchison, D. (2002, June). Hydra: A decentralised group key management. In *Proceedings. Eleventh IEEE international workshops on enabling technologies: infrastructure for collaborative enterprises* (pp. 62-67). IEEE.
31. Alohali, B. A., Vassilakis, V. G., Moscholios, I. D., & Logothetis, M. D. (2018, July). A secure scheme for group communication of wireless IoT devices. In *2018 11th International Symposium on Communication Systems, Networks & Digital Signal Processing (CSNDSP)* (pp. 1-6). IEEE.

AUTHORS

Priyanka Ahlawat received B.Tech, M.Tech in Computer Science and Engineering from M.D.U, Rohtak and Guru Jambheshwar University of Science and Technology, Hisar (India). She is Assistant Professor in Computer Engineering Department NIT Kurukshetra Haryana, India. She is working towards her Ph.D. in Wireless Sensor Network Security from the Department of Computer Engineering, National Institute of Technology Kurukshetra, and India. Her interest areas are Cryptography, Key management, Wireless Sensor Networks Security.
E-mail: priyankaahlawat@nitkkr.ac.in

Rohit Bathla received B.Tech, in Computer Science and Engineering from JMIT, Radaur and M.Tech from KUK University (India). She is Assistant Professor in Computer Engineering Department MRIIRS, Faridabad Haryana, India. She is working towards his Ph.D. in Wireless Sensor Network Security from the Department of Computer Engineering, National Institute of Technology Kurukshetra, and India. Her interest areas are Cryptography, Key management, Wireless Sensor Networks Security.

E-mail: Rohitbathla2005@gmail.com

.