GROUP KEY MANAGEMENT FOR MULTICAST COMMUNICATION IN WSN

A Thesis Submitted

IN PARTIAL FULFILLMENT OF THE REQUIREMENT

FOR THE DEGREE OF

DOCTOR OF PHILOSOPHY

IN

COMPUTER SCIENCE & ENGINEERING

By

GUNJAN SRIVASTAVA

[Admission No. 18SCSE3010009]

Supervisor

Dr. J. N. Singh
Professor

Co-Supervisor
Dr. Manisha Manjul
Assistant Professor

SCHOOL OF COMPUTING SCIENCES AND ENGINEERING
GALGOTIAS UNIVERSITY
UTTAR PRADESH

JANUARY 2024

GROUP KEY MANAGEMENT FOR MULTICAST COMMUNICATION IN WSN

A Thesis Submitted

IN PARTIAL FULFILLMENT OF THE REQUIREMENT

FOR THE DEGREE OF

DOCTOR OF PHILOSOPHY

IN

COMPUTER SCIENCE & ENGINEERING

By

GUNJAN SRIVASTAVA

[Admission No. 18SCSE3010009]

Supervisor

Dr. J. N. Singh
Professor

Co-Supervisor
Dr. Manisha Manjul
Assistant Professor

SCHOOL OF COMPUTING SCIENCES AND ENGINEERING
GALGOTIAS UNIVERSITY
UTTAR PRADESH

JANUARY 2024

Candidate's Declaration

I hereby certify that the work which is being presented in the thesis, entitled **"GROUP KEY MANAGEMENT FOR MULTICAST COMMUNICATION IN WSN"** in partial fulfillment of the requirements for the award of the degree of **Doctor of Philosophy in Computer Science and Engineering** and submitted in School of Computing Science and Engineering, Galgotias University, Greater Noida, Uttar Pradesh is an authentic record of my own work carried out during a period from September 2018 to December 2023 under the supervision of Dr. J. N. Singh, Professor-SCSE, Galgotias University and Dr. Manisha Manjul, Assistant Professor – CSE, G. B. Pant Government Engineering College, New Delhi.

The matter embodied in this thesis has not been submitted by me for the award of any other degree or from any other University/Institute.

GUNJAN SRIVASTAVA
18SCSE3010009

This is to certify that the above statement made by the candidate is correct to the best of our knowledge.

Dr. J. N. Singh — Supervisor

Dr. Manisha Manjul — Co-Supervisor

The Ph.D. Viva-Voice examination of GUNJAN SRIVASTAVA Research Scholar, has been held on _____.

Sign. of Supervisor Sign. of Co-Supervisor Sign. of External Examiner

Abstract

Wireless Sensor Network contains nodes with limited storage, energy and Computation power. WSN applications are spread in several areas etc. military, Agriculture Science3 and the environment Science. In WSN network, motes communicate with each other in secure mode and to achieve this the usual messages send to the other node after encryption. A major challenge in WSN is securing communication. Various algorithms have already been proposed in this regard by many researchers. WSN uses a variety of applications of various sizes in a range of environments. Secure communication that uses WSN by many applications, key management is essential to meet the security objectives by joint and leaving operations of the node. Information is broadcasted from one node in a cluster to another via the cluster head in multicast WSN, where information security is an important concern and cryptographic algorithms play a critical role. RSA and CRT are combined in a Dynamic Cluster-Based Group Key Management Scheme (DCGKMS) to provide hybrid security. Based on the evaluation parameters such as computing, communicating, and rekeying cost, the recommended DCGKMS is secure, effective, and cost-efficient. Simulated results are shown in comparison to LKH and OFT using NS2. There are several WSN applications used many areas like military applications, agriculture, and environmental monitoring. Sensors connected to wireless networks transmit sensitive data over insecure channels, exposing the data to several threats. In group communication, there are various challenges. Group key management has significant security requirements, as well as techniques for securing it. A comparison of the traditional systems that have been carried out and appraised is being done. The study finishes with open research talks on the best ways to reduce critical expenditures during leave and join operations.

Acknowledgment

I (Gunjan Srivastava) have been able to complete this research program with the support and active co-operation of concerned bodies, authorities, and several people. I owe my debt and would like to express deep feelings of gratitude to my supervisor, Dr. J. N. Singh, Professor, School of Computing Science and Engineering, Galgotias University for his valuable guidance at different stages of this research work. It would have been impossible to carry on the research work and make it into the final shape of a thesis without his able guidance and sympathetic encouragement.

I am intensely indebted to my associate supervisor Dr. Manisha Manjul, Assistant Professor, G. B. Pant Govt. Engineering College. New Delhi for her very useful guidance and counseling in overcoming various bottlenecks during the study and for her comments on the draft of my thesis. Her co-operation and assistance in the overall presentation and all her precautionary measures made the methodology of this thesis comprehensive. I appreciate her continuous encouragement.

My gratitude is also due to Dr. Karan Singh, Assistant Professor, School of Computer & Systems Sciences, Jawahar Lal Nehru University, New Delhi for his extraordinary support to the whole process of this research work. I was immensely befitted from his continuous assistance in finalizing the research methodology, pre-testing the cases, developing skills in interpretive approach, as well as his sincere guidance throughout the various stages of this study. I learned a lot from him about preparing a constructive research approach.

I must owe a special debt of gratitude to Hon'ble Chancellor Mr. Suneel Galgtotia, Mr. Dhruv Galgotia, CEO and Hon'ble Vice-Chancellor Dr. K. Mallikharjuna Babu, Registrar Dr. Nitin Kumar Gaur, Pro Vice-Chancellor Dr. Avadhesh Kumar, Dean of R & D Cell, Galgotias University for their valuable support throughout my research work.

I express my sincere thanks to Dean - School of Computing Science & Engineering and Research Coordinator SCSE for their guidance and moral support during my research work and all faculties of School of Computing Science & Engineering who helped me a lot in my course of research work and all those who stood behind me.

Nothing is possible without the constant support of my family, I am obliged to my husband Mr. Vikas Srivastava, who has been a source of incessant motivation and encouragement to me and who has always extended his profuse support to me in completing this research work. My daughter Arohi Srivastava also deserves special acknowledgement for willingly making the sacrifices necessary for me to enable me to work for realizing one of the major ambitions of my life.

In last, my heartiest gratitude to my Parents LATE Dr. S. M. Asthana and LATE Smt. Sushma Asthana and the ALMIGHTY GOD, who blessed and enabled me to complete my work.

GUNJAN SRIVASTAVA

List of contents

Contents

List of figures

List of tables

List of abbreviation

Abbreviations	Description
WSN	Wireless sensor network
BS	Base station
SN	Sensor node
SLAP	Safe and compact mutual authentication scheme
ROR	Real-or-Random
AVISPA	Automated verification of internet security protocols and applications
HEESR	Hybrid energy efficient static routing protocol
u-REST	Unadvertised round energy saving
BAN	Burrows-Abadi-Needham
IDS	Intrusion detection system
LEAP	Localized encryption and authentication protocol
COKE	Crypto-less over the air key establishment
ITS	Intelligent transportation system
VCS	Vehicular Communication Systems
SKC	session-key based convergent
CKS	convergent key sharing
CL-PKA	Certificate less-powerful key administration
ECC	Elliptic Curve Cryptography

MALSA	Multi-attribute location selection approach
MASF	Multi-attribute service fitness
STS	Secure Transmission Support
CPAS	Conditional privacy-preserving authentication
PBAS	proxy-based authentication scheme
RSU	Roadside unit
RFID	Radio frequency identification
DoS	Denial-of-Service
PDR	Packet Delivery Ratio
SEED	Sleep-awake energy efficient distributed
ECBK	Enhanced cluster based key
ISFC-BLS	Intelligent and Secured Fuzzy Clustering Algorithm with Balanced Load Sub-cluster Formation
CSDP	Cluster based secured data dissemination protocol

CHAPTER-1

INTRODUCTION

1.1 Wireless Sensor Network

Computer systems are lacking in capable to perceive the real environment. Hardware for sensor network aims to fill the space between the digital and physical world. A typical WSN is a distributed, dynamic network consisting of several small, inexpensive SNs that can sense, compute, and wirelessly communicate with base stations to manage a broad range of prospective a variety of uses, both military and civilian [1]. Figure 1.1 describes the systematic view of WSN. To increase data transfer faster WSNs are used recently. WSN means a connection between the SNs that covers with one another without the wire, which collects the information from the surroundings. In this the large number of data is collected by sensor nodes in one base station [2]. The sensor used in WSN is very small with limited computing and processing resources, compared to conventional sensors. Sensor nodes are positioned in inaccessible places and they have lean storage space, a radio for wireless transmission is employed to communicate the data from node to BSs. A sensor node's primary power source is a battery.

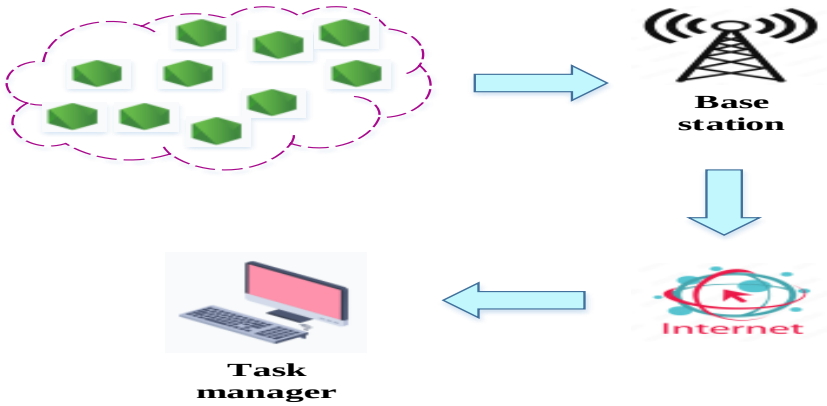


Figure 1.1 Components of WSN

WSN can be divided into two categories: infrastructure mode as well as ad hoc mode. In the infrastructure mode, BS connects mobile devices to wired networks and change BSs when a mobile device is handed off. In the ad hoc mode, no wired BSs are present, and nodes can only

transfer to other nodes within radio range. Instead, they organize into a network and only route traffic among themselves because of the infrastructure provided by the WSN. Figure 1.2 represents types of wireless sensor.

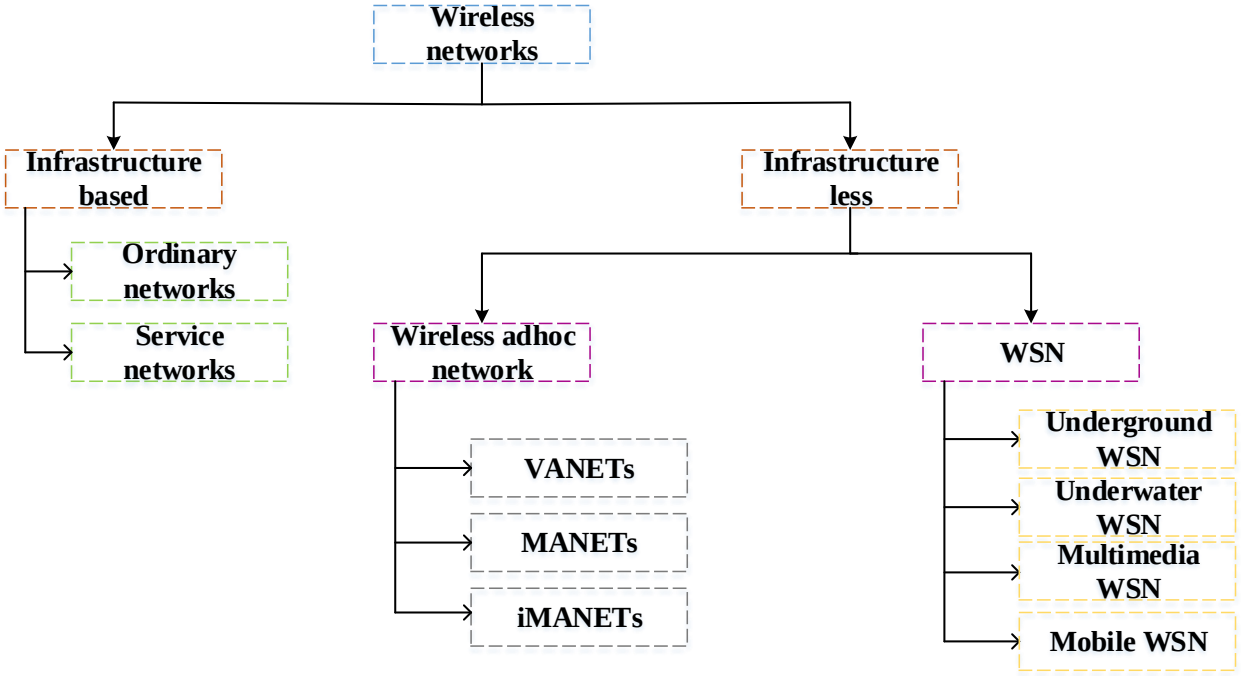


Figure 1.2 Types of Wireless networks

1.1.1 Various WSN Applications

WSN Application can be useful in military, civilian population and in addition of these areas WSN applications are also utilized in various other fields including medical health care, environment protection and monitoring, intelligent agriculture and in military field as shown in Figure 1.3.

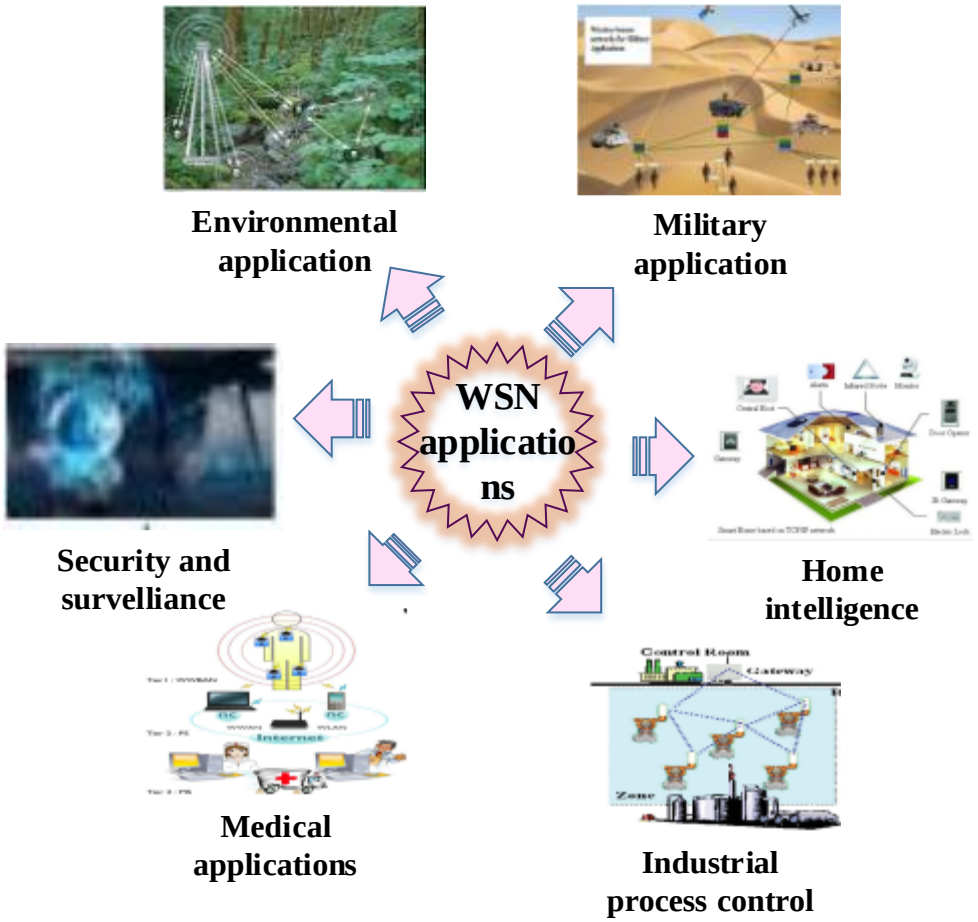


Figure 1.3 Application of WSN

Environmental applications

WSN in the environment is used to surveillance in forest, tracking animals, forecasting weather and detection of floods. The main advantage of using WSN is it is wireless, so it can sense the close objects and observe [3]. This can be used in understanding the number of animals and plants that live in the specified area.

Military applications

Military applications take advantage of the first WSN. Because SNs are low-cost, the loss of certain nodes by hostile activities on the battlefield may not have a significant impact on a military operation [4]. Military applications and wireless sensor networks are inextricably linked. WSNs are deployed in several fields from intelligence gathering to war field surveillance, adversary tracking, and target categorization.

- Battlefield monitoring: Sensors which are enabled in the battle field is to monitor the presence of vehicles and forces, and to monitor the opposite force surveillance and to track their movements.
- Object protection: For the protection purpose sensor nodes are enabled in strategic bridges, military headquarters, oil and communication centers, atomic plants and gas pipelines.
- Intelligent guiding: Sensors are used for robotic tanks, vehicles, fighter planes and missiles or torpedoed to direct them past obstacles and lead those to 14 cooperate with one another to achieve more effective assaults or defenses.
- Remote sensing: Sensor might be used to detect nuclear, chemical weapons and biological identify prospective terrorist attacks and conduct reconnaissance.

Health care applications

WSNs might be utilized to keep track of patients and the elderly for medical purposes, easing the severe staffing shortage in the medical field and bringing down costs [5].

- Behavior monitoring: Sensors shall be installed in a patient's house to detect the patient's activities. It can, for example, notify doctors if a person falls and requires rapid medical assistance. It may keep track of patients' movements with television or radios.
- Medical monitoring: A wireless body sensor network can have sensors to keep track of position, the surroundings, and bodily functions. Additionally, they offer long-term, non-invasive, and outpatient monitoring or the elderly, as well as prompt reporting of users health condition and real-time updates to their medical records. They also provide warnings to users in the event of an urgent to medical professionals in the case of emergency.

Industrial process control

WSNs can be utilized in industry to observe production methods or the status of industrial instruments. Wireless sensors, for example, can be integrated into production and assembly lines. As a result, they can monitor and regulate manufacturing operations. Sensors can be used by chemical plants or oil refineries to check the status of their kilometers of pipes [6]. Tiny sensors can be implanted in areas of a device that are out of reach to humans to monitor the machine's state and notify for any breakdown.

Security and surveillance

WSNs have a wide range of surveillance and security demands. Acoustic, visual, and other types of sensors, for example, can be installed in subways, airports, buildings, and other vital infrastructure [7]. Sensors can also be employed at communication centers or nuclear power plants to detect and monitor intruders, as well as to offer timely warning and security against prospective attacks.

Home intelligence

WSNs can be utilized to create more comfortable and smart living areas for humans.

- Smart home: An autonomous residual network can be created by installing wireless sensors throughout a home and connecting them. For instance, a smart microwave or stove linked to a smart refrigerator may cook a meal using the ingredients within the refrigerator. The smart stove or microwave oven receives the relevant cooking parameters and sets the necessary cooking temperature and time. It is possible to remotely monitor and change the programmes and contents of players for VCRs, TVs, CDs, and VCDs.
- Remote Metering: Service meters in a house, e.g. gas, electricity or water can be remotely read using wireless sensors, and the data can subsequently by wirelessly sent to a distant centre.

1.1.2Clustering in WSN

The majority of WSN applications require the network as a whole to be able to run unattended in severe settings where pure human access and monitoring is either impossible to schedule, manage well, or even be practical. The SNs are usually randomly dispersed as a part of significance by reasonably but not controllable (e.g., plunged by a helicopter) in many important WSN applications and they construct an ad hoc type network, based on this criticality.

Additionally, sensors in these settings have limited energy sources, and their batteries typically cannot be refilled [8]. Therefore, it follows that to maintain acceptable levels of network lifespan in such situations, specific energy-aware routing and information collection protocols with high scalability should be used. Naturally, the research community has embraced clustering sensor

nodes to meet the scaling target, achieve great energy efficiency, and extent lifetime network in large-scale WSN scenarios.

To enable data fusion and aggregation, which results in considerable energy savings, the relevant hierarchical routing and information collection protocols entail cluster-based structure of the SNs. Each cluster in the hierarchical network structure contains a leader, also known as the CH, who typically handles the specialized responsibilities (fusion and aggregation) mentioned above, as well as number of common SNs as members. The CH nodes represent the higher level of the two-level hierarchy that results from the cluster f

In Cluster formation process, a sensor node includes the below level. The relevant CH node receives data transmissions from the SNs on a regular basis.

The BS receives information from the CH nodes either correctly or incorrectly through intermediary connection with other CH nodes, therefore reducing the overall number of relayed packets [9]. However, the CH nodes inherently expended more energy since they transmit all time data over greater distances than the common (member) nodes. Re-electing new CHs on a regular basis in each cluster (cycling the CH role over time across all the nodes) is a typical method to balance the energy usage under all the network nodes. Figure 1.4 further exemplifies a typical instance of the inferred hierarchical information transmission inside a clustered network.

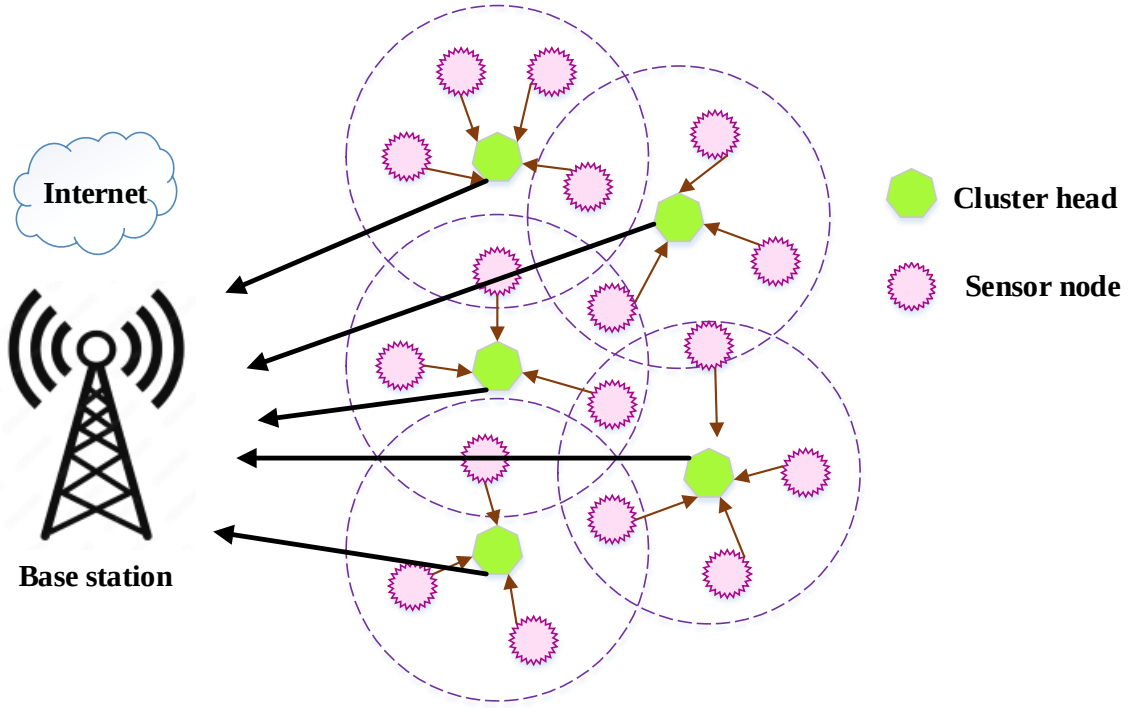


Figure 1.4 Clustering in WSN

Before information becomes available to the user , it is processed in BS. It is typically regarded as stationary and located far away from the SNs. CH node serves as gateways between the BS and SNs. Each CH's role is to bring all tasks that are common in all nodes of a cluster, such as aggregation data sending before it to Base Station, as was already explained. The Cluster head acts as a sink of sensor nodes and CHs send messages to BS. Additionally, this network produced by SNs, sink CH, and BS may be represented as often as necessary to produce (if desired) several levels of a hierarchical WSN.

1.1.3 Constrains in sensor network

A WSN is equipped with power sources, radio transceivers, and sensing and processing tools. The nodes of a WSN are inherently limited in terms of resources due to their constrained processing power, communication bandwidth, and storage capacity. Since SNs often get energy by batteries and energy utilization is the key factor to determine the sensor network life. In sensor networks, energy optimization can occasionally be more difficult because it involves not only cutting energy use but also maximizing network longevity [10]. Having knowledge of energy in

all facets of design and operation will allow for optimization. The energy awareness is included into the individual node, communication Sensor Network groups and overall network.

A sensor node contains of sub systems

- A computation subsystem: It subsystem has microprocessors to control the deployed sensors and implements connection protocols. To power management, MCUs often operate in a variety of modes. Given that different working modes require the use of electricity, energy utilization level of modes should be taken into account while evaluating battery life of each node.
- A communicating subsystem: It has a short-range signal that is using to connects with other nodes and the outer world. A radio can run in several modes. It is essential to completely switch off the ratio when it is not transmitting or receiving to conserve energy.
- A sensing subsystem: Using this subsystem nodes are connected to the outside world and is make collection of sensors and actuators. Minimum power components and sacrificing performance are not necessary to minimize energy usage.
- A power supply subsystem: The node is presented by a battery that is part of the device. It is important to keep an eye on how much power is being drawn from a battery because, even if it had lasted longer, a battery that is exposed to a high current for a lengthy period of time would ultimately expire. The minimal energy need is often smaller than the rated current capacity of a SNs battery. By considerably lowering its current or even by repeatedly shutting it off, a battery's lifespan can be increased.
- It is made comprised of a battery that powers the node. The amount of power being pulled from a battery should be monitored because if a battery is subjected to high current for an extended period, it will eventually die even if it might have lasted longer. Typically, a sensor node's battery's rated current capacity is less than the minimum energy need. A battery's lifespan can extend by reducing its frequently turn-off.

Several research work has been done to develop algorithms to reduce energy consumption by sensor nodes in WSN. In these studies researchers also considered about microprocessors, node's capabilities and hardware. This could encourage the development of a unique remedy for various

sensor node's designs. Sensor nodes deploy in several types of sensor networks. This could also influence the development of various cooperative algorithms for WSN.

1.1.4 Security challenges in WSN

- Resource constrains: WSN have a certain amount of battery life, computational power, and storage. The processing and communication requirements of all security methods are high [11].
- Standard activity: The majority of WSN routing protocols are known to the public and do not take possible security issues into account while they are being designed.
- Complex algorithms: The security techniques are computationally and commutatively intensive. They can't be used with WSN. For WSNs with limited resources, a lot of research has been done to lower the calculation and communication costs of security methods. Figure 1.5 denotes the challenges in WSN.

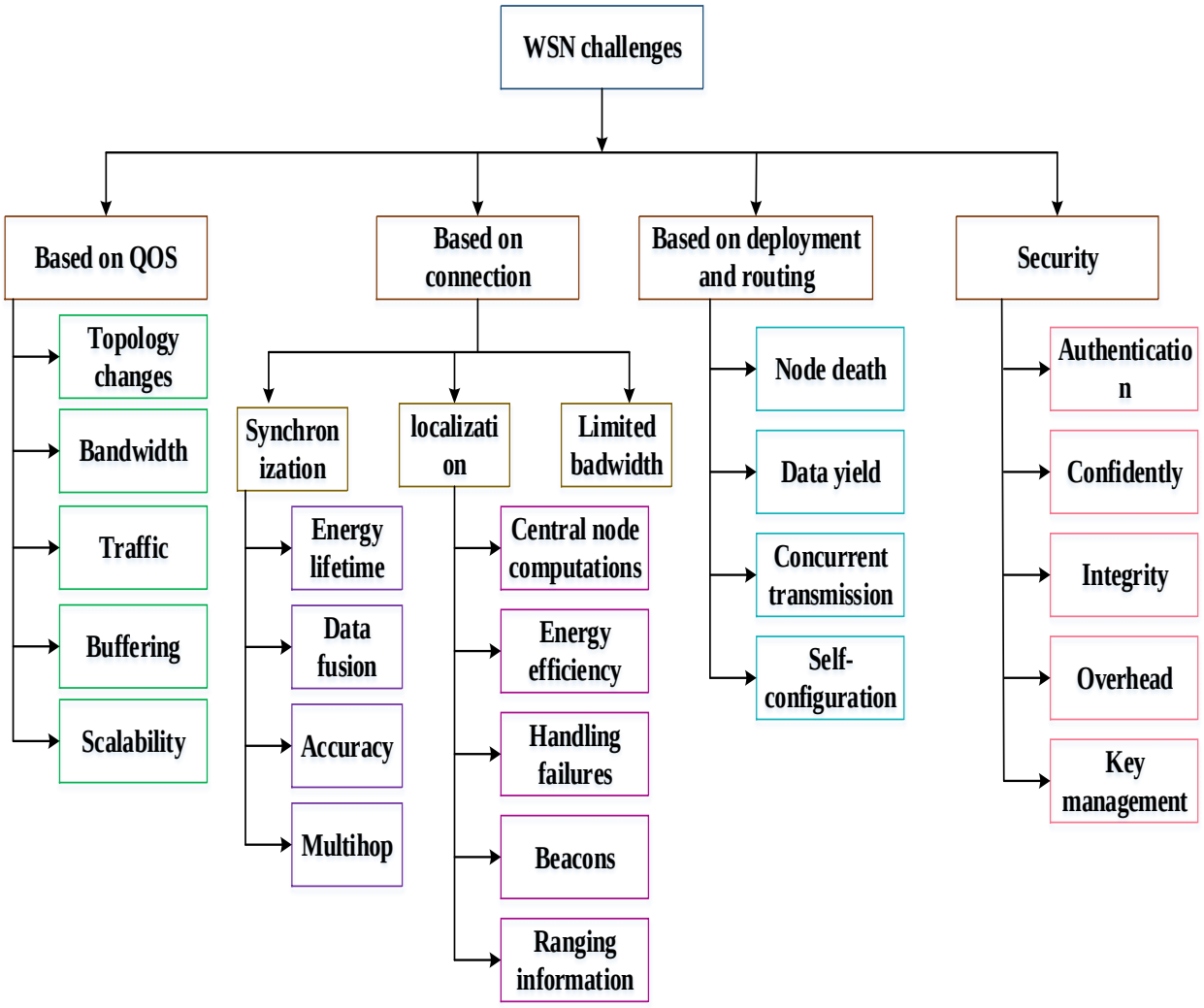


Figure 1.5 Challenges in WSN

1.1.4.1 Security requirements of WSN

The goal of secrecy is necessary in a sensor environment to prevent disclosure of data that is sent between SNs of a network or between sensors and BS. Each node and Base Station must be confirm about information sender because sender should be trustworthy. The clustering of SNs in WSN requires this authentication. After clustering, relay on the information given by the nodes in that group. Integrity checks must be put in place to guarantee that data won't be changed in any unanticipated ways [12]. The accuracy of the results is crucial for many sensor applications, including those that monitor pollutants and medical conditions. In a WSN, base stations, clustered nodes, and protocol layers all require secure management. Due to the necessity for safe

management of security concerns including key distribution to SNs for encryption and routing information. The following security standard apply to WSN

Node authentication

By identifying its source, node authentication protects the message's dependability. A mote must demonstrate its legitimacy to other network nodes and the base station. This stops the enemy from sending harmful into the network. The sensor mote's authenticity is verified by the base station.

Availability

Availability guarantees that network resources and sensor mote services are available whenever needed. This can be sustained by controlling a sensor mote's sleep cycle. Because of the WSN's availability, network services are still functional even when denial-of-service attacks are ongoing. The security protocols carry out data accessibility in the network with a fixation on low energy and storage with network code reuse. Depending on the available options, some techniques decide to modify the code in order to maximize code reuse and leverage additional communication in order to accomplish the same task.

Integrity

Integrity guarantees the accuracy of the information. It also ensures that a message hasn't been tempered, modified, or changed in the network.

Confidentiality

If one party's long-term private key is hacked, perfect forward secrecy guarantees that the session key generated by public and private keys cannot be shared with any node. Only authorized personnel are permitted access to the secret data. There shouldn't be any data leaking into nearby sensor networks. When a node delivers extremely private information to a recipient, numerous other nodes network participate in the transmission. Network protocols employ encryption techniques using a secret key to provide data security; the message is transmitted to the channel while being encrypted. Information should be encrypted to prevent attacks using traffic analysis.

Perfect forward secrecy

In order for the communication sent via a WSN to stay private, confidentiality guarantees that it is hidden from a passive attacker.

Network and data availability

In the presence of enemies, the network should guarantee that services and data are accessible to the application.

Authorization

Only allowed nodes should participate in supplying data to the application, according to the network. Since an enemy may simply insert messages, authenticity in WSN is crucial. The receiver node must ensure that any information utilized in a decision-making process comes from reliable sources. The purpose of data authenticity is to guarantee communication node identities. It is necessary for many administrative activities.

Non-repudiation

Any approved node should not be able to prevent the transfer of data from which they came, according to the network.

Data freshness

The network should guarantee that the data is current.

Robustness

No node in the network can be hacked, the WSN should guarantee that its services would be still being available.

Self-organization

By self-organizing to give service to the application, the network nodes should be adaptable. The WSN has several operational nodes spread over numerous fields and locations. All

nodes in the WSN are autonomous inside the network and lack infrastructure. It is an ad hoc network. This inherent quality poses a significant problem to wireless network and security.

Time synchronization

To deliver accurate data, the network must guarantee that the time is synchronized throughout all of its nodes. The WSN applications depend on synchronization of some kind. The nodes in the network can be in two stages: awake and asleep, and the radio can be turned on or left in sleep mode for a while. The sensor determines a packet's end-to-end delay.

Secure localization

WSN employ location-based data to pinpoint the locations of network nodes. A few attacks can be linked to sensor locations by looking into attacks. For this, the attackers are looking through the packet and data headers. An essential component of network security implementation is secure localization.

Flexibility

Because they change often, the scenarios for sensor networks vary and rely on the environments, risks, and mission. Sensors from established nodes in the network must regularly be lowered due to the constantly changing mission goals.

1.1.5 Attacks in WSN

WSNs are vulnerable to many attacks. Below mentioned categories are used for group attacks based on the security requirements [13]. Interference, interruption, and hijacking are the three main types of assaults against sensor network privacy. By keeping a record of the sensor node's sent messages, eavesdropping is used to determine the output of the sensor networks. There are primarily multi ways to learn about output data: by hiding from SNs, by contacting sensor nodes directly via queries, or by attacking sensor nodes directly via aggregation points or root nodes. The earlier method is known as passive eavesdropper, whereas the later method is known as aggressive eavesdropper. The WSN's authentication and confidentiality properties are also impacted by this attack as shown in figure 1.6.

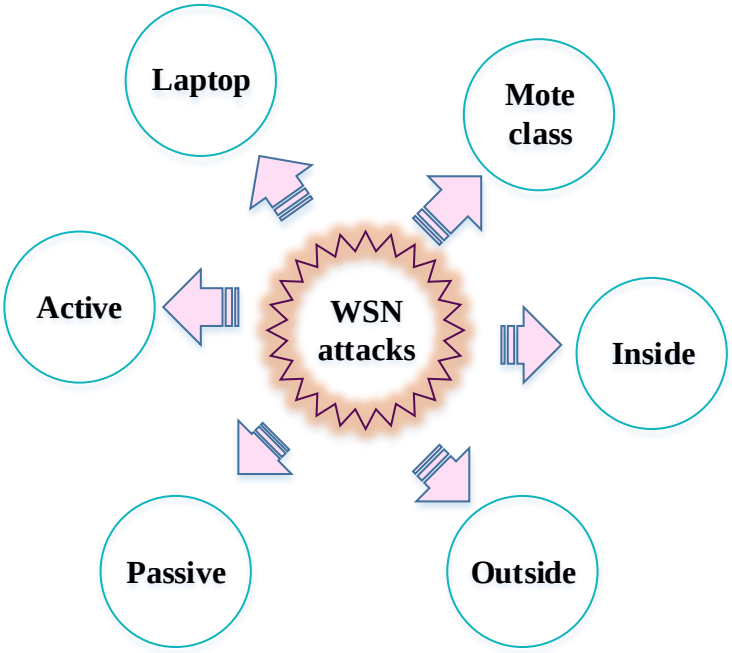


Figure 1.6 Attacks in WSN

Therefore, before broadcasting data, an appropriate encryption technique and message authentication code is required. The network's production is mostly impacted by the disruption. The aggregate data becomes distorted, unusable, and incomplete as a result of the semantic disruption, which injects corrupts data, messages, or modifies values. By physically altering the environment, physical disruption renders the sensor readings. The network sensor node, the hijacking process increases the effectiveness of listening in and disruption. Denial of service (DoS) is another significant WSN attack. DoS attack can occur at the transport, connection, and routing layers. Jamming networks is one of the denials of service attacks. That is only the WSN interface transmission frequency.

No messages may be sent or received by a node in a WSN when there is continual jamming. So the network is completely jammed. Intermittent jamming involves the nodes exchanging messages at great risk. Sybil attack is yet another recent attack in WSN. The redundancy system, routing algorithms, resource allocation process, and data aggregation system are all being affected by this attack. An opponent may easily seize nodes, examine and replicate them, and then covertly implant the copies into the network in key areas. They may even enable the attacker to disconnect

important portions of the network or damage network data. This attack has the ability to alter the network's objective. Integrity and secrecy have been attacked.

- **Outside attacks:** The attack nodes are not a part of a WSN.
- **Inside attacks:** A WSN legitimate nodes act in an illicit manner.
- **Passive attacks:** The attacking nodes only observe the WSN's message exchanges. The data is not changed by them.
- **Active attacks:** Inside the WSN, the attacking nodes alter the data and occasionally provide fake data.
- **Mote class attacks:** Adversary node always pacts as similar nodes of sensor network.
- **Laptop class attacks:** Attackers being their attacks against the WSN using high configuration nodes.

The WSN has six layers: Physical, Data link, Network, Transport and Application. The following is a summary of the attacks made against the various levels of a WSN [14].

- **Application layer:** The application layer specifies the shared communications and interface mechanisms used by sites in a connection network. Both the Internet protocol suite and OSI model specify an application layer abstraction.

- **Transport Layer:** The data sent to the session layer and segregated into sections by the transport layer. The transport layer is responsible for debugging, which involves detecting. To control the flow if information was successfully received then request should not resend.

- **Data Link Layer:** This layer partitions a data packet into data and delivers data between two points. The LLC component of this layer, which recognizes performs error checking, network protocols, and synchronizes frames, and the MAC section, which merge devices and establishes allow for data transmission and reception utilize MAC address, make up this layer.

- **Physical Layer:** This layer is accountable for the wireless or wired node-to-node connectivity. It describes the connection between devices, whether it be a wired or

wireless connection and over-sees sending raw data, which consists just of a string of 0s and 1s. It also regulates bit rates.

- **Network layer:** A function of the communication protocol stack's network layer. A predictable deployment of a WSN's nodes allows for communication between them and the gateway might take place via established paths. Table 1.1 represents details about network and routing layer attacks.

Table 1.1Network and routing layer attacks

Attack	Details
Spoofed, altered or replay attacks	Spoofing is the process of hiding and secure the message to make it appear as though it is coming from an authentic source. Spoofing attacks are existed in a number of forms which are used during online frauds.
Hello flood attack	Network layer attack is commonly known as hello flood. A hostile node broadcasts hello packets with a strong transmission rate to be chosen as the CH by majority of other nodes in WSN.
Selective forwarding attacks	In this attack the adversary inserts itself into a targeted information flow channel. Certain packets may not be sent by the attacker. This attack can be modified by the adversary securely forwarding other packets while dropping just those coming from a particular source.
Sink hole attack	Sinkhole attacks usually function by making a node visible particularly desirable to neighboring nodes using an algorithm for routing. Because it is impossible to validate routing information provided by a node, sinkhole attacks are challenging to defend against.
Worm hole attack	These attacks are very common but critical in ad-hoc networks. In this type of attack data packets communicate between adversary nodes and defected data packets are then scattered.

Black hole attack	When an intruder router disconnects all the communications sources then its intuition is for black-hole attacks. A router can be set intentionally incorrect so that it provides a minimum cost path to every internet destination. so that all traffic can be routed to the intruder router as a result. The router fails because no equipment can withstand such a load.
Rushing attack	By transmitting route request packets more quickly than the legitimate node in the WSN, the attacker draws all of the packets from its nearby nodes. As an outcome, the attacker node is made to be one of the lawful nodes along the path to the target.
Vampire attack	This attack employs messages that violate protocols in an effort to gradually deplete the battery power. Attacks of this nature are challenging to recognize and avoid.
Sybil attack	This attack is significant and disruptive on a sensor network in which many real identifies together with fabricated identified are utilized to obtain unauthorized access to a network. In a WSN detecting the Sybil attack, sinkhole attack, and wormhole attack while multicasting is a huge attack.
Node replication attack	The attacker releases confidential data from the node that was physically taken. The secret information obtained from the legal nodes is then used to launch numerous other nodes.
Jamming attack	This attack works as an application to stop signal transmission of Jamming is an application of communication system's electromagnetic energy. Jamming application disturbs sensor nodes signals. Few jamming sensor nodes can affect many nodes. This becomes cause od DoS.
Physical attack	A WSN is constructed in layers, and these layers defend the sensors from different threats. Due to their limited computing

	capacity and power, sensor networks are vulnerable to attack because of these factors. The physical attacks employ various tactics and outcomes.
Tampering and capturing attack	The intersection, modification, and fabrication security class encompass this attack. The attack threat in this category is posted by the availability, integrity, and confidentiality. This form of attack can be detected by SN disconnection, node disconnection, node destruction, and noticing network node misbehavior. Applying common measures in the network and improving crypto processors are protective techniques. The network is further protected from these attacks by node physical protection and malicious node detection mechanisms.
DOS attack	The DOS attack is an all-purpose attack that affects levels like data link layer, transport layer, and network layer, among others. The attacker can insert fake broadcast packets in this technique to have the SN undertake pricey signature verification. The network's tiers and their functionality are impacted by the DoS attack. The availability, integrity, and authenticity are the major threats for this attack, which is classified as a disruption and intersection security attack.

1.2 Key management

An important component of security solutions is the usage of reliable and effective key management and distribution. To create and maintain secure channels, the key management is in charge of key maintenance, key distribution, and key generation across SNs. Key management ought to make it possible for sensor networks to scale to have many nodes. The following procedures make up the collection of key management stages. Unattended or ignored operation is the mode used by WSN [15]. To compromise the storing sensitive data and connecting keys on SNs, an attacker may physically seize them. Due to their cheap cost, wireless SNs are not attack-resistant therefore any attacker may seize a sensor node and quickly retrieve its saved encrypted

data. In WSN, key protection, updating, and revocation are given consideration. However, these techniques might not be used at all over the sensor lifespan. Additionally, their cost in processing and communication has increased. They expend more power. More messages must be transferred in the key update process of the present key management schemes [16]. Figure 1.7 denotes the stages of key management.

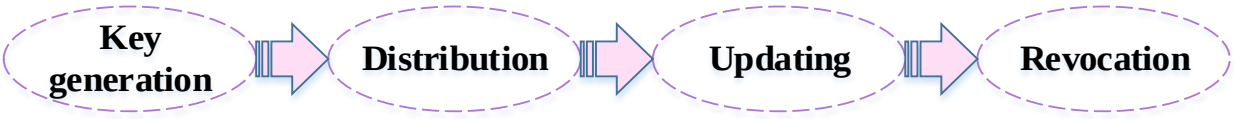


Figure 1.7 Key management

The following objectives must be met in order to design a key management protocol for any WSN. All SNs that must securely share data with one another must establish a key using the protocol. It must be ton add and remove nodes. It must function well in an unspecified deployment environment as well and prevent unwanted users from connecting to network nodes. The architecture of the nodes and the network places several limitations on how safe WSN can be and how a secure protocol may be developed. Node constraints: WSN nodes have limited processing power, memory, battery life, and transmission range. And WSN large packet size and ad-hoc nature, which limited the cryptography process, are network constraints.

The collection of methods and practices known as key management supports the development and upkeep of key connections between authorized parties. Handling with the creation, storage, trade, utilization, and replacement of keys is included in this. Asymmetric and symmetric keys are the two types of keys. To encrypt and decrypt the message the same symmatric key is used. It's important to pick, distribute, and keep symmetric keys safely. In contrast, asymmetric keys are two separate keys that are connected mathematically. They frequently converse with one another in this way. Three primary parts make up a WSN key management protocol as shown in figure 1.8. Key setup establishes a session key between parties that must securely interact with one another, key refreshment extends the useful lifetime of a key revocation, and cryptographic key prevents an expelled mote from deciphering the private communications send across the network.

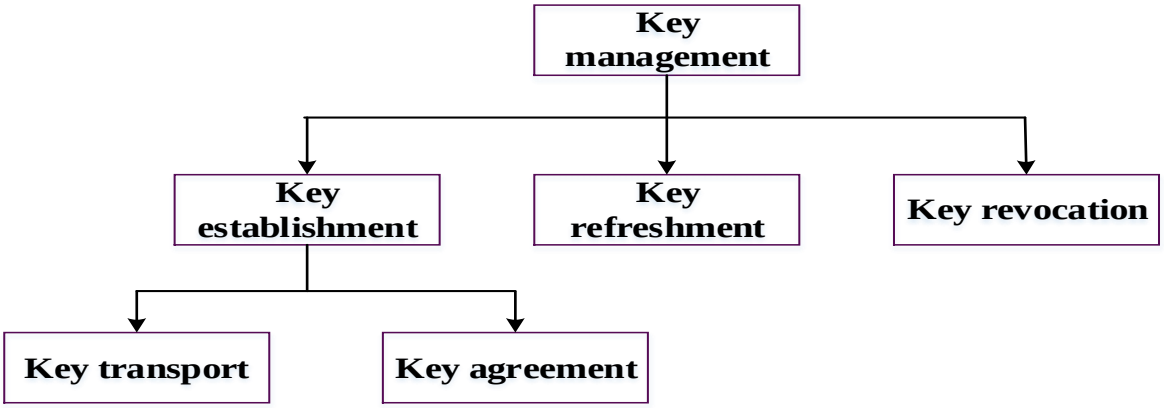


Figure 1.8 Key management protocol

Key establishment: A secret key shared is made available to more than two people through the procedure or protocol known as key setup for later cryptographic usage. Therefore, key setup entails the creation of a session key between two or more parties that require secure communication. Key establishment protocols come in two different categories.

- Key transport: A secret value is created or acquired by one party and safely send to the other side using key transit.
- Key agreement: In key agreement, two or more parties share a secret key for safe and secure communication. Three types of key establishment are:

    - The trusted-server scheme: This scheme is necessary for the trusted Communication.
    - The self-enforcing scheme: Using public keys for asymmetric cryptography is essential for the self-enforcing system. According to public key algorithms like RSA and DiffeHellman demand a lot of computational power.
    - The key pre-distribution scheme: This scheme involves embedding crucial information in the sensor motes prior to their deployment. A key pre-distribution technique is a key agreement mechanism in which the initial keying material totally determines the established that will be generated.
- **Key refreshment**: The confidentiality of the information is the primary objective of key management. Keys can also help with message integrity verification and genuine mote authentication. Adversaries attempt to figure out the secret keys and get access to private

data. Refreshing the secret keys at regular intervals is necessary to prevent adversaries from gaining access to private information. These intervals depend on the frequent communication and key usage. The effective lifetime of a cryptography key is extended through key refreshing.

- **Key revocation**: When keys are revoked, they are taken out of service before their initial expiration date for reasons like mote capture. Therefore, key revocation makes sure that communication between nodes are now secure for entire WSN.

1.2.1 Public key schemes for WSN

In WSN, nodes have less memory, Battery power, communication and processing power . For example, MICA2 mote with ATmega128 8-bit processor at 8 MHz, 128 KB programmer memory (flash), 512 KB additional data flash memory, 868/916 or 310 MHz multi-channel radio transceiver, 38.4 kpbs radio, and 500-1000 feet outdoor range (depending on versions) in a tiny 58 x 32 x (mm). Typically, it is powered by two AA batteries and runs on the TinyOS operating system. This setup prevents the device from supporting security measures the demand a lot of instructions to be executed [17].

Data privacy, data integrity, and data authenticity are the very basic criteria for any sort of secure communication. These might all be offered by employing powerful cryptography techniques. Again, WSN unattended nature makes them frequently susceptible to physical capture attacks. The attackers might obtain important key information from the nodes after physically seizing the sensors if they do. When considering this problem, the private key scheme works efficiently.

1.2.2 Key management schemes in WSN

Management of key schemes in pre-distribution, where the information key is disseminated across all SNs before to deployment, and in-situ management of key schemes, which do not need keying collected information prior to deployment, can be used to classify all key management systems [18]. Key pool, key space, random pair wise key, group, grid, deployment knowledge, polynomial, matrix based, tree, combinatorial design, hyper cube, id, energy, location, and other

factors may be used to categorize this pre distribution. There is other more probabilistic pre distribution in key systems in used in addition to this pre distribution in key categories.

1.2.2.1 Pre distribution management schemes

Prior to deployment, the unpredictable nature of the network topology must be accommodated by all important pre-distribution strategies. Thus, achieve a certain sharing of key probability across nearby sensor; a pre-distribution in key method needs additional keying collected information are pre-loaded. As a result, keying data might not be used over the network lifespan. Furthermore, this uncertainty could make it harder for important pre-distribution techniques to scale.

1.2.2.2 Key pool based pre distribution key management schemes

In these approaches, a sizable pool in key is calculated offline, and every sensor is already loaded with keys drawn at random from the pool in key without replenishment. A key in the sensor ring is made up of these keys. As long as two sensors key rings share almost one key, they can create a secure communication channel. In the absence of a shared key, a route key must be created with the aid of an intermediary node that has a key shared by both nodes in the pair.

1.2.2.3 Pair wise key based pre-distribution key management schemes

When a sensor node is hacked, this system provides a function to revoke its whole key ring. By having nearest nodes public votes opposed an identified misbehaving node, distributed node revocation is made feasible. Any node that notices more than a certain amount of public votes against another node cuts off contact with that node. The random pair wise technique supports node-based revocation, resists node replication, and is completely resilient to node capture threats.

1.2.2.4 Key space based pre-distribution key management schemes

Multiple bits in keying of data, each of which is specific different key in space, are preloaded onto sensors. If two sensors have access to the same key data in the uniform key space, they calculate a shared key. This scheme contains elements which are Subset assignment, polynomial share discovery, and path discovery are some of the examples. This plan permits dynamic join operations of sensors. This plan enables network expansion.

1.2.2.5 Group based probabilistic pre-distribution key management schemes

Depending on IDs, sensors are grouped, and pair-wise are keys are preloaded on nodes belong to some deploy group or cross group. Group-based methods drop the rigid topological premise they use. The cost of this flexibility is additional connection overhead incurred when two nearby sensors attempt to construct a route key.

1.2.2.6 Grid-based pre-distribution key management schemes

Any two nodes may establish keys using this approach, regardless of the network structure or node density. Because of this, it may be used in more deployment circumstances than random key pre distribution. For key setup, this technique benefits from a consistent communication pattern that is hard for an adversary to disrupt. This scheme's distributed design prevents an attackable single point of failure. Key establishment benefits from not being probabilistic since a bit of two nodes are assured of being able to establish a key.

1.2.2.7 Deployment knowledge-based pre-distribution key management schemes

This system's objective is to make it possible for SNs to discover a shared secret key with every nearest node after deployment. It has been demonstrated that pre-distribution in key with deployment knowledge can significantly increase a network's connection and resilience against node capture while also requiring less memory.

1.2.2.8 Tree based pre-distribution key management schemes

This scheme effectively defends the network against eaves dropping and compromised node assaults, is used to handle the complex security concerns of runtime WSN. Even if the attackers do crack the sensor network's keys, the re key process will continue to provide timely security for the whole network.

1.2.2.9 Energy-aware pre-distribution key management schemes

These sub-protocols make up the key management protocol, which uses symmetric keys. The method does not need the use of a sensor to create keys or to carry out any complex computations related to management of key. The expulsion of the compromised nodes is permitted under the protocol. Important revocation and renewal process are supported by this strategy.

1.2.3 Key management schemes Classification in WSN

WSNs are distinct from conventional networks in a number a way, including the restricted energy, computation, and memory capabilities of SNs. Moreover, before deployment, their location is typically unknown. Two nodes should share a secret key to connect and communicate securely. Such networks can make use of a variety of agreement strategies and key distribution is known as key management methods. Probabilistic deterministic matrix-based on the polynomial image [19]. Key management scheme classification in WSN takes into account the three primary management strategies that are most often classified: pre-distribution, self-enforcing, and trustworthy server as shown in Figure 1.9. In key pre-distribution scheme, there is most of the random deployment of nodes, the absence of trusted infrastructure, and resource restrictions.

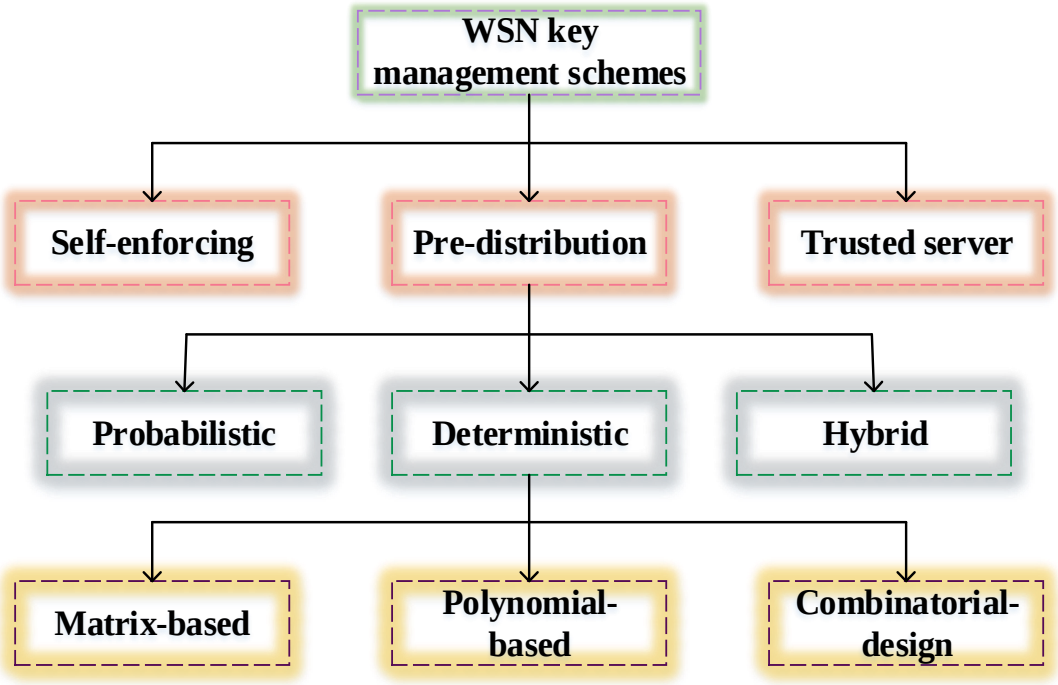


Figure 1.9 Classifications of key management schemes in WSN

In Key pre distribution scheme, a key-pool assigns key to each sensor nodes before their deployment. Each pair of nodes that must communicate with one another must have at least one shared key from their key chains and must be within radio range of one another. If communicating nodes do not have shared key they are not allowed to send information to each other.

Typical metrics Connectivity, robustness, scalability, and key chain size are used to assess a key pre-distribution scheme. Connectivity is the way of communication where two nodes will share a key. The sensor network stability against node capture attacks is referred to as resilience. These two criteria frequently clash. The capacity to sustain bigger network sizes is known as scalability. Key-chain size depends on amount of keys in a node's key-chain and is also associated with sensor node memory capacity.

1.2.4 Pairwise Key Management

Pairwise key calculation includes four stages [118]: Key Pre-distribution stage, Key Agreement stage, Key Revocation/Refresh stage. The Key Pre-distribution stage follows Blom's scheme [119] and it permits each pair of nodes in the network determine a pairwise secure key and it should be λ-secure. In this method, the ID of the node is utilized as seeds to construct the public matrix G. In the key agreement phase, if the node m wish to transmit secret information to node n then the data will be encrypted utilizing the key K_{mn}. The key K_{mn} can be generated by the node m as given as follows: (i) create the column of G matrix $Col_n(G)$ by considering node ID n as the seed (ii) Determine $\mathrm{K}_{mn} = Col_n(G).Row_m(A)$. Here, $Row_m(A)$ denotes the m th row of symmetric matrix A.

Key revocation and key refresh schemes play a significant role in all key management approach. When the key is not refreshed frequently, the network will be compromised easily. Furthermore, the key should be revoked after identifying the compromised node for continuing the regular network operation. In this pairwise key management scheme, the BS is worked to revoke the compromised node's key. Also, when a new node comes to join in the network, the base station will adds the seed value (i.e., node ID) and secure key shares in the memory of newly joined node. Consider the ID of new node as $N+1$ and this ID is used to determine the private secret shares for node $N+1$ as given below:

(i) Add a new column utilizing $N+1$ as the seed for extending the matrix G

(ii) for $m = 1$ to λ

for $n = 1$ to λ

$nr[m] = nr[m] + D[m][n] \cdot G[n][N+1]$

Where $nr[m]$ denotes the private secret share of node $N+1$. Figure 1.10 represents the new node addition mechanism.

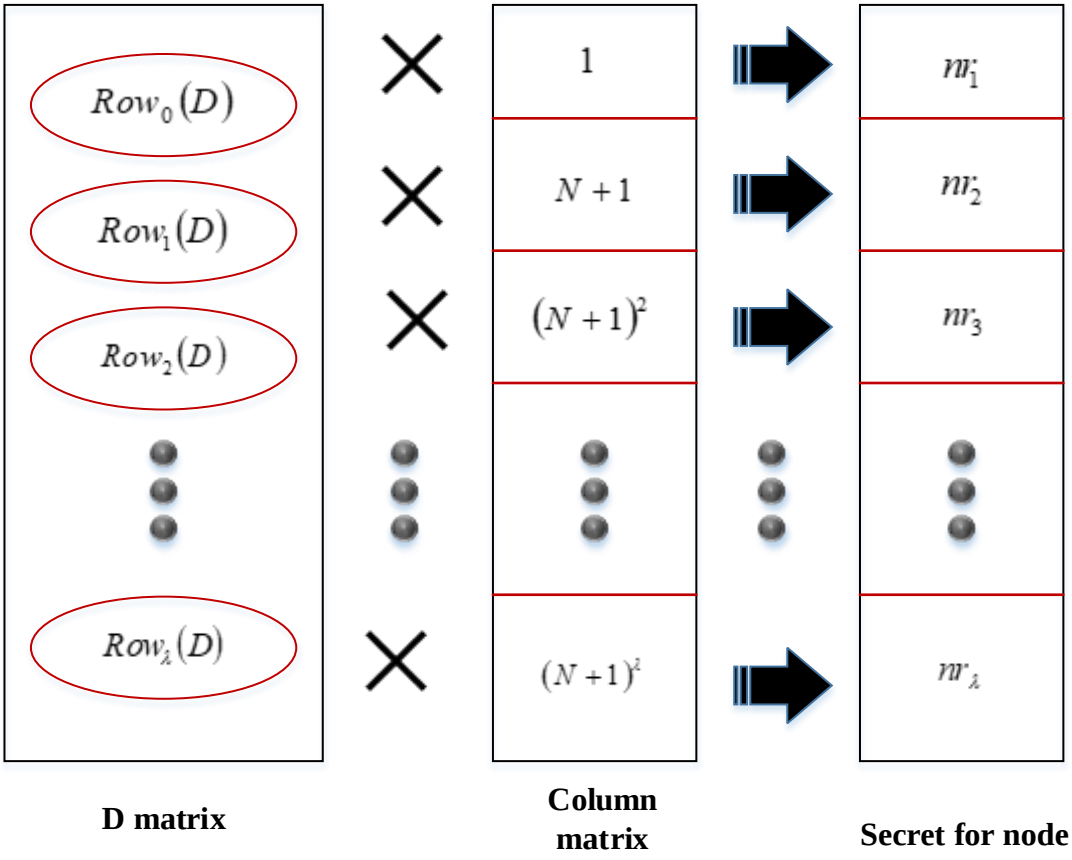


Figure 1.10 New node Join mechanism

1.2.5 Group key management protocols

For several WSN applications, e.g. networking and ecological control, forest fire warning, air quality, , etc., the data acquired at each node must be capable and pre-managed in the network. Pre-processing steps might involve filtering, compressing, or correlating data with relevant data. These applications may need temporary group nodes to work together and form a dynamic group. To meet this demand, a dynamic secure group might be created using protocol.

The following essential security requirements, notably group secrecy, should be followed by any system for maintaining group keys. The ability to communicate as a group will only be available to group members. Forward secrecy guarantees that a node can calculate future required session keys other than its identified key once it is connected to the wireless network, while backward secrecy ensures that a newly joined node entering the network cannot infer the past secure keys from present key. When a new node joins the network or a node's key then Group

keys should be updated. A group key may be changed by opting a newly calculated group key and broadcast it to group members.

1.2.6 Metrics to evaluate key management schemes

Key management includes a branch known as dynamic key management. The classical security standards of secrecy, authentication, freshness, integrity, and non-repudiation should be met by all key management methods. For dynamic key management methods, the same is true. Additionally, certain assessment metrics are emphasized in accordance with the characteristics and application environment of key management. Metrics are defined for assessing key management strategies in WSN. The limitations of sensor nodes and networking, evaluation criteria for pre-distribution key management are divided into safety, efficacy, and resistance categories. The fundamental needs and assessment metrics for key management based on the categorization and the unique quality of key management. It should be made clear that the metrics for forward and backward secrecy, collusion resistance, key connection and node revocation apply to key management systems. However, static key management systems may also be employed with the other metrics [20].

Security metrics

Only authorized nodes of the wireless network should be competent to safely distribute and /or update the keys inside the network, according to security metrics. Additionally, it needs to stop rogue nodes from taking part in important management procedures. Key management techniques must deliver cryptographic keys in a safe way, preventing rogue network nodes from carrying out their nefarious operations. A new secret key must be produced and disseminated to all related SNs, excluding the compromised one, when the compromised sensor node's secret key has been revoked. Furthermore, it is preferred that a dynamic key management system retains collusion resistance among the compromised nodes and the newly joined nodes in addition to backward and forward secrecy. Also required is robustness beside node detention and node duplication. These are the security metrics:

- Node authentication: Furthermore, the communicating nodes should mutually verify the authenticity during the key distribution or exchange. The feature makes it easier to spot the network's impostor nodes.
- Resilience: A node capture attack shouldn't be able to take down the WSN. If a legitimate sensor node is hacked, the node's secret data should be made confident. Resistance to node capture, in which an attacker physically assaults a SN and attempts to extract sensitive information from its memory, is referred to as resilience. It gauges how a single seized node affects the network as a whole. A key management system is resilient if an attacker cannot impact other nodes than the one they have taken. When a single node is taken over and the entire network is compromised, however, resilience is limited.
- Node revocation: To prevent the attacker from compromising the remaining legitimate nodes, key management should make it easier to revoke the compromised nodes from the network. An efficient solution should be able to quickly remove compromised SNs from the network once they are found. By injecting fake data or changing the data of trustworthy nodes, a hacked node cannot alter network behavior thanks to these techniques.
- Forward and backward secrecy: The reverse is backward secrecy, which is utilized to stop a mote with new key from moving back at time to decrypt earlier received messages encrypted with earlier keys. Node capture attempts may be prevented using both forward and backward secrecy.
- Collusion resistance: A network adversary might launch an assault by taking control of several network nodes, forcing them to cooperate and expose all system keys, and then seizing control of the whole network. A suitable dynamic key setup method must thwart collaboration between compromised and freshly joined nodes.

Efficiency metrics

The key management system should be able to create the keys by effectively leveraging the following resources. Rekeying message transmissions, many keys needed, and the number of procedures all need to keep minimum as possible. In addition, the length of three keys should be less. As a result, the network size is not controlled with energy and storage that each node has

access to. The key distribution itself must not significantly burden the sensor nodes' innately limited resources in terms of:

- Memory: The key management should be planned such that the network uses the least amount of memory possible to hold the node IDs and keying information.
- Bandwidth: Minimum data should sent among the nodes during key distribution. Data updating should also be minimum.
- Processing: Reduce the number of processing cycles for key establishment.
- Energy: A minimum amount of message exchanges between the nodes should be required to accomplish the key agreement procedure, directly reducing the energy usage.
- Key connectivity: The likelihood of the nodes creating and using the same shared keys should be increased.

Flexibility metrics

KMS should be flexible to handle many applications. The metrics are:

- Reduced prior deployment knowledge: The method of establishing the keys should be independent of deployment knowledge, such as the GPS coordinates of the node.
- Scalability: The network size expansion should be supported by the key management strategy without compromising security. There may be hundreds or even thousands of sensor nodes distributed in the sensing region. Furthermore, at any point of time node join and leave operation occurs in WSN. Dynamic key management solutions should be adaptable to various network size. When applied to bigger networks, efficiency and security must be considered for small networks.
- Mobility: Most network topologies presumptively consider sensor nodes to be inactive. However, mobility for base station, sensor nodes or both is required in some applications. Therefore, for relocated nodes to connect with their -new neighbors, the key establishment provides them with new keys. Key production and allocation to nodes are more difficult for dynamic nodes, in addition to bandwidth and energy, becomes a significant challenge.
- Key connectivity: Two or more nodes calculate and share keys after rekeying, is known as key connectivity. Local connectivity considers the connectivity between any two nearby

nodes. High key connection following each rekeying operation is necessary to maintain security.

The key establishment approaches created for WSN should take into account all the measures and limitations. Pair wise key management, key pre-distribution schemes, single network-wide key, public key schemes, hierarchical key management, and dynamic key management.

1.3Motivation

This study examines several algorithms based on four factors: cost of computing, communication, rekeying, and storage. Based on how well they perform in these four categories, various algorithms are compared. According to study, to maintain forward and backward anonymity, the rekey is calculated and communicated on each enter or exit a procedure. Any rekey computation requires a lot of storage space to retain a lot of keys for the least amount of money. As a result, a long-term objective is to provide a framework to change the WSN topology in order to minimize costs.

1.4 Problem formulation

As the sensors and cluster heads need acceptable shared keys to use security algorithms, key management schemes are crucial to achieving privacy and security goals. Based on encryption techniques, three categories for Key management protocols are: asymmetric, symmetric, and hybrid key management models as a result of the development of WSN technologies. For WSN device management and applications to be secure, key management is a crucial aspect. It seeks to distribute keys securely and reliably across nodes. Similar to this, the key management schemes needs to encourage node growth and renunciation inside the system. Using Neighbor node key and sub-cluster key to generate unique node key when a node joins or leaves the cluster, this approach lowers the computation complexity and expense. The group key is created initially in the first stage, then based on cluster group key, sub-group key generated, and the unique leaf node key generation. The idea behind a top-down strategy is to monitor the cluster creation process.

1.5 Research objective

- The research focuses on the creation of new keys for forwarding and preventing secrecy before moving on to the appropriate leave and join processes.
- A hybrid DCGKMS is proposed, which is cost-effective, efficient, and more secure on the evaluation parameters communication.
- Communication and rekeying cost for dynamic clusters and the obtained results are compared with LKH and OFT.
- To analyze the various key management schemes in WSN.

1.6 Thesis organization

Chapter-1 Introduction

This chapter explains the outline of WSN, clustering in WSN, constrains in WSN, application of WSN, security challenges in WSN, attacks in WSN, key management, its various classification, various schemes, and various metrics to evaluate key management schemes, motivation, problem formulation, and research objective.

Chapter-2 Literature survey

This chapter explains various techniques used, advantages and limitations of the security protocols for static homogeneous WSNs, key management techniques in static homogeneous WSN, dynamic key management techniques, group key management techniques, and key management schemes using clustering approach.

Chpater-3 Analysis of various key management schemes in wireless sensor networks

In this chapter the analysis of various key management methods in wireless sensor networks is discussed to provide the security of information by offering group key management techniques. Group communication needs effective group key management. Under this requirement, centralized and decentralized protocols are explained. Also, the distributed group key management protocols and comparative analysis is given the better result.

Chapter-4 DyClust – A Hybrid Key Management Scheme for Wireless Sensor Networks

This chapter discussed DyClust-a hybrid key management scheme for WSN. The suggested approach explains in step-by-step process. Finally, the chapter has concluded with a summary.

Chapter-5 Result and Discussion

This chapter summarizes the findings and conclusions of this research study. This chapter also includes information on the evaluation measures, comparison tables, and graphs. Different existing approaches are used to analyze the performance of the presented work.

Chapter-6 Conclusion

This chapter contains conclusion related to suggested work. The chapter also includes important results and carries future work in this section.

CHAPTER-2

LITERATURE SURVEY

2.1 Security protocols for static homogeneous WSNs

The usage of WSN was common to provide people practical services like healthcare and smart homes. In WSN settings, SNs gather and transform sensing data to the gateway in order to offer practical services. However, because vulnerable messages were sent across an unsecured route, it may experience significant security problems. Secure authentication techniques were therefore required to guard against WSN security issues. Kwon et al. [21] proposed a WSN-SLAP. WSN-SLAP offers full forward secrecy, mutual authentication, and resilience to a number of security flaws. BAN logic, the ROR model, and the AVISPA simulation were used to demonstrate the security of WSN-SLAP. WSN-performance SLAP's in comparison to already in use similar protocols

A motorist may acquire a variety of relevant information via WSN, such as congestion during traffic, collisions between vehicles, emergence, and speed. However, because such information was delivered over a public route, drivers and traffic managers may be subject to numerous assaults. As a result, safe mutual authentication had emerged as a crucial security concern, and several authentication systems had been put forth. Yu et al. [22] presented a safe authentication methodology for WSNs in vehicular connections. Authentication technique uses dynamic settings that were reset after each session to thwart various attacks and ensure safe mutual authentication and anonymity. The proposed protocol offers superior security features at a similar cost of computation in comparison to other relevant protocols. The proposed protocol may therefore be used for real-world, WSN-based vehicular communications.

In several fields, including surveillance, the smart grid, health care, and environmental monitoring, WSN were extensively employed. Due to the intrinsic qualities of wireless networks, several security protocols had been suggested and extensively researched. A potential authentication method that was sufficiently resistant to different assaults. However, it contains two significant security flaws that make it vulnerable to malevolent outsiders. Their plan can firstly result in user impersonation attacks. Second, their plan does not protect user anonymity. Ryu et al.

[23] investigated further depth about these flaws. Also suggest a different plan to counteract these shortcomings.

A region of interest was covered by a large count of nodes that were unevenly distributed in WSN. The nodes were equipped with wireless communication, processing, and sensing capabilities. On the other hand, nodes were limited by energy since they were powered by non-rechargeable batteries. Routing protocols address this problem by constructing the network to gather and transfer data while using less energy. Qabouche et al. [24] presented HEESR, which combines multi-hop routing with clustering, was introduced. The network was being into different layers by HEESR. It establishes the clusters for each round on which the collected data transmits through independent nodes and elect nodes by applying novel method.

The lifespan of WSN can expand in various ways while maintaining complete coverage of the sensed region. The majority protocols are used to save energy usage by turning off the sensors. These strategies must ensure that all nodes receive the most recent information about their neighbors in order to select which group the nodes to be turn-off, to avoid losing the entire coverage area. In a static WSN, the nodes level of energy was the sole crucial piece of information that had to be broadcast on a regular basis. One-hop messages were used to communicate this data between nodes within predetermined time windows. However, the energy required to conduct hundreds of transformations in a typical sensor was the same as that required to convey a single, little piece of information. Therefore, lowering communication between nodes increases energy savings. Menegazzo et al. [25] presented the u-REST to remove the level of energy of the advertising datasets and saves a substantial quantity of energy. u-REST made possible to enhance the energy savings by turned off the chosen group nodes while maintaining the complete coverage area without utilizing the energy of promoted messages. Mathematical arguments show how u-REST preserves energy while guaranteeing complete coverage of the interest region. In fact, it had been mathematically proven that u-worst REST's energy-saving scenario may save more energy than any synchronization-based method's best scenario.

Extending the lifetime of WSN was crucial because of battery restriction. WSN energy-efficient routing strategies were crucial in achieving this. Yan et al. [26] described this issue and divide the two types of WSN routing protocols currently in use into homogeneous and

heterogeneous WSNs, respectively. They can also be divided into static and movable types. Finally, several unresolved challenges in the design of an WSN routing protocol with energy-efficient were highlighted.

To monitor safety in coal mines, WSN was required. This study aims to identify these requirements and security concerns and to create an authentication mechanism to ensure WSN security. By properly monitoring the equipment and subsurface conditions, the WSNs aid in decreasing risk and increasing output. The sensor's limited battery should be used effectively to compute the data collected. Kumari et al. [27] provide an authentication mechanism to address the security challenges in WSNs. To conserve the battery in sensors, protocol simply needs simple, low-cost message transmission operations.

Smys et al. [28] presented an energy-aware routing protocol that might address security concerns brought on by the massive data creation while still meeting QOS standards. To address difficulties with energy consumption, network lifetime management of security concerns, network latency, delay, and overhead problem, the node with large resources was chosen. To assess the network lifetime, power consumption, network latency, throughput, packet delivery ratio, the proposed method was additionally tested using NS2.

The embedded systems and WSN were used in more and more crucial application areas. Nearly every area of daily life, including industry, health care, education, vital infrastructure, and entertainment, now includes them. Due to the increasing count of merged devices and their inherent security flaws, there was also an increasing quantity of danger. However, with the development and implementation of WSN security standards, it was possible to reduce these dangers and foster a climate of trust in the technology. Lazrag et al. [29] presented a routing system that makes use of block chain technology to provide network nodes access to a shared memory. The simulation results demonstrated that this method may be relevant and that it may be able to address the problem mentioned above.

Multiple sensor nodes were deployed ad hoc to WSN, which were used to detect or monitor physical occurrences by gathering real-time data. These battery-powered sensor nodes had finite energy limitations that influence the network longevity. The design of a routing system that maximizes network longevity must take into account these nodes need for energy conservation.

By utilizing nodes along with various levels of energy, power, and computation, network heterogeneity plays a vital role in extending the network's lifespan. Naeem et al. [30] combines elements of direct transmission, distance-based protocol which is defined in a hybrid methodology called distance aware residual energy efficient stable election protocol. This protocol aims to offer an ideal transmission way from SNs to CHs, taking the dynamics of the network into account. To cut down on energy usage, multi-hop routing was employed between CHs and sink nodes.

Energy hole issues affect clustered routing methods with a static sink. As a conveyer for distant nodes, sensor nodes closest to the sink node quickly exhaust their energy, creating a hole of energy in the network. Utilizing the mobility of the sink node emerges as a highly effective strategy for addressing the energy hole challenge and optimizing the lifespan of Wireless Sensor Networks (WSN). A framework proposed by Sethi and Deepak et al. [31] integrates the concept of a mobile sink, directing a load of Sensor Nodes (SN) towards a nearby static or mobile sink. This framework incorporates 4- or 8-sojourn-location path patterns along with a centralized static sink, aiming to enhance the network's longevity. Furthermore, the framework's performance is compared to two network protocols, LEACH-C and DEEC, representing heterogeneous and homogeneous setups, respectively. Simulation results reveal that the introduced sink mobility architecture surpasses LEACH-C and DEEC in energy efficiency, significantly prolonging the network's lifespan.

Thirukrishna et al. [32] discussed about WSNs are frequently employed to keep an eye on the real world. Different environmental conditions can be detected using sensor nodes, which can also wirelessly connect with the sensed information. The SNs are equipped with batteries, and a decrease in power consumption may result in a longer expectation of a sensor node's lifetime. Sensor nodes were the subject of research to improve energy efficiency and improve lifetime. Routing methods that enable dependable and efficient communication between nodes are frequently utilized in WSNs. Energy conservation is a key goal of routing algorithms. In homogeneous WSNs, the clustering approach increases energy efficiency. The shortest path is found using the clustering technique, which is then utilized to choose the selection of cluster head. OREA is utilized to efficiently release energy. The PADSR clustering algorithm has been suggested to extend WSN network lifetime. QoS -based routing techniques balances energy use and data quality. The quality-of-service performance review is decided by PADSR.

Lazrag et al. [33] investigate the optimization of traffic load balancing, interference reduction, and security along the routing path in WSN and IoT. They conceptualize the nodes as coins, exchanged between source nodes and sink nodes. To facilitate real-time sharing of the network's status, all transactions are meticulously recorded in the blockchain. It introduces a cost function that considers load density and interference level at each node, aiding in the selection of the most optimal path. Furthermore, blockchain security measures are employed to safeguard the chosen network paths. Simulation results indicate the potential applicability of this method and its ability to effectively address the aforementioned challenges.

The most crucial problem in the study of WSNs is the effective utilize of energy. The network's sensor nodes are energy-constrained since the batteries that are fixed inside them are necessary for them to operate. Therefore, the requirement for the most appropriate means of sending sensed data from the network to the sink arises. By providing a new routing algorithm that improves network longevity and data packet delivery and adopts the concepts of cluster formation, cluster heads, and temporary cluster heads, Jangwan et al. [34] seeks to optimize the energy-related concerns. To compare the proposed protocol's outcomes to those of other protocols using related concepts, MATLAB simulation is used.

Mehra et al. [35] introduce the Stability Enhancement for LEACH (SE-LEACH) protocol, designed to augment the stability region of Wireless Sensor Networks (WSN). This protocol effectively balances the load across nodes, ensuring equitable power dissipation among all nodes. The selection criteria for the cluster head position take into account node density, distance to the base station, remaining energy, and power dissipation, as the optimal candidate for cluster head must meet these criteria to effectively fulfill its role. Additionally, nodes of non-cluster head choose their cluster head based on the cluster head's distance from them, node density, residual energy, and power output during the round. Two scenarios involving a base station kept at the network's center and a great distance away from it are simulated through testing. The enlargement of the stability region is confirmed by comparing simulation results with MODLEACH and LEACH, which also shows a load-balanced network for the proposed protocol. Table 2.1 denotes the security protocols for static homogeneous WSNs by mentioning the techniques used.

Table 2.1 Security protocols for static homogeneous WSNs

Sl no	Author name	Technique used	Observation	Advantage	Limitation
1.	Kwon et al. [21]	WSN-SLAP	WSN-SLAP was more suited and secure for WSN contexts than earlier methods.	Lightweight mutual authentication protocol for WSN environments.	_
2.	Yu et al. [22]	A safe authentication methodology for WSNs	The proposed protocol may therefore be used for real-world, WSN- based vehicular communications.	The protocol functionality and security features with those of other relevant protocols.	These were centralized management device, heterogeneity, routing protocols, and limited computational power.
3.	Ryu et al. [23]	Energy-aware routing protocol	The validation of the presented method was carried out in the simulator.	Increasing routing performance while consuming less energy is extremely difficult.	Extra packet flipping between nodes is necessary.

4.	Qabouche et al. [24]	Hybrid energy efficient static routing protocol	LEACH= 98% DEEC=40.5% HEESR=98.4%	The network to gather and transfer data while using less energy.	An increase in energy use, particularly for remote CHs, will lead to an uneven use of energy.
5.	Menegazzo et al. [25]	Unadvertised round energy saving	It had been mathematically proven that u-worst REST's energy-saving scenario may save more energy than any synchronization-based method's best scenario.	Removes the power level advertising messages and saves a significant quantity of energy.	In u-REST the worst-case scenario for energy savings was able to save most energy than that of the best-case scenario for all synchronization-based techniques combined.
6.	Yan et al. [26]	Energy-aware routing protocol	Several unresolved challenges in the design of an energy-efficient routing protocol for WSNs were highlighted.	Increasing routing performance while consuming less energy is really difficult.	Extra packet flipping between nodes was necessary.

7.	Kumari et al. [27]	An mechanism to address the security challenges in WSNs	Security protocols in internet and application tool was utilized for its formal security verification.	This method's benefit was an additional degree of protection that made it more difficult for hackers to access user's accounts.	Time may be an absolute metric, but it's also relative. Cost like time, cost was relative.
8.	Smys et al. [28]	Energy-aware routing protocol	The presented method was carried out in the network simulator.	Increasing routing performance while consuming less energy is really difficult.	Requires additional packet switching between nodes.
9.	Lazrag et al. [29]	Block chain technology	The simulation results had demonstrated that this method may be relevant and that it may be able to address the problem mentioned above.	The advantage of block chain technology was transparency, decentralized network, trusty chain, unalterable and indestructible technology.	The highly energetic dependence, challenging integration procedure, and expensive implementation of the block

					chain were its drawbacks.
10.	Naeem et al. [30]	Distance aware residual energy efficient stable election protocol	The results reveal a 10% gain in energy efficiency, extending the network life span.	These protocol aims to offer an ideal transmission path from sensor node to CHs, taking the dynamics of the network into account.	The receiving data from the network was critical.
11.	Sethi and Deepak et al. [31]	Homogeneous & Heterogeneous routing protocol using sink mobility	To extend the network's life as much as possible by sending a load of SN to a nearby mobile sink.	It improves the networks lifetime.	Moving around the forest to gather data and produce reports on a regular basis are the mobile sinks. It happens when the landscape makes navigating difficult.
12.	Thirukrishna et al. [32]	Homogeneous WSN using OREA and PADSR	OREA is used to dissipate energy efficiently & PADSR algorithm	Clustering algorithm improve efficiency of	Route finding method is initiated only

			used to improve the lifetime of network.	energy in homogeneous	when the route is not found.
13.	Lazrag et al. [33]	Block chain based method	A shared memory was made available between network nodes using this technique.	Decreased interference levels and improved traffic load balance	Every node has a maximum understanding of the network's classification, but it is impossible for it to know the status of the network at any one moment.
14.	Jangwan et al. [34]	Improve static clustering protocol for WSN	Protocol enhances the data packet delivery and networks lifetime.	Clustering protocol provides intelligent CH selection.	The position of every node in the network is unknown to the base station.
15.	Mehra et al. [35]	SE-LEACH protocol	It can equalize the load to ensure that every nodes to dissipate power same.	Stability period extended & balanced use of energy	The process of choosing a CH is dependent on randomization, therefore there is a risk that neither a CH nor an SN with low energy will be chosen.

2.2 Key Management Techniques in Static Homogeneous WSN

Jilna et al. [36] provides a key distribution strategy depend on the elliptic curve Diffie-hellman key exchange for static WSN. The proposed method solves the man-in-the-middle attack in the key exchange and depends on the transitory on key approach for key in secret formation. The strong resilience provided by the proposed method even if nodes were hacked during the startup phase was its main benefit over state-of-the-art systems. When compared to the elliptic curve-based system, the proposed method had significantly lower communication overhead, computational costs, and storage needs. Large networks may be supported by the proposed method without compromising security or effectiveness.

With the growth of WSN, mobile sinks will eventually replace conventional WSNs with static sink nodes in most application situations, necessitating a secure communication environment for the related application. The sensor networks security with MS receives less emphasis in current key management methods. Zhang et al. [37] presented a key management in hybrid method based on basic random pre-distribution and pool-based polynomial key pre-distribution. The strategy makes full use of these types of two techniques to increase the key systems breaking difficulty. It was also possible to greatly improve network resilience and storage effectiveness. The tree-based path key formation approach was presented to efficiently address the connectivity issue of communication links.

The overall network security was ensured by confirming security to each and every node that was part of the wireless network. The network had more than one SNs in the geographic fields. Due to WSN resource limitations and susceptible medium state, IDS or lightweight security were necessary. The carefully chosen watchdogs serve as IDS agents, keeping an eye on each network node's activity at the network level. The network needs adequate rate watchdogs in order to safeguard WSN. Rajasoundaran et al. [38] presented a system highlights the problems with the WSN watchdog-based IDS selection techniques. In order to boost watchdog availability ratio in WSN and defend against various sorts of attacks, suggests new secure watchdog selection process. Use a variety of low-cost, multi-layer security-providing techniques in the proposed method.

The most often used security method in WSN was symmetric encryption. Gandino et al. [39] presented a method that establishes keys using cryptography in public-key. The primary issue

with cryptography in public-key in a WSN was characterized by communication and processing overheads. A novel authentication approach based on authentication tables was proposed in order to lessen these needs. Analytical research demonstrates that the proposed strategy offered the best defense against a threat that compromised more than one nodes. Comparative study demonstrates that the proposed method may be the optimal one based on the size and density of the network. Additionally, a real-world network experimental investigation demonstrates that the proposed method may be successfully used with devices with little computing power.

Patel et al. [40] presented a key management efficient session technique for cluster based mobile sensor network, delivers a better session key by periodically updating inside the cluster and so avoiding various types of attacks from malicious nodes. This still had several drawbacks, such as the inability to scale and the static nature of the CHs in each round. As a result, this may enhance the proposed method by dynamically choosing CH for each round and cut down on energy use by sending messages via CH.

WSN employs a large number of specialized sensors for huge networks in order to record and monitor environmental variables. Routing, load balancing, network longevity, and other important issues were clarified by cluster based WSN. By restricting its resources or refusing to transfer the data to the other clusters, security poses a significant barrier in it. Different security techniques were applied by WSN to provide secure data transfer. To promote high information security, it was customary to encrypt records of information that were transported to other companies while using a limited number of systems. Such encoded data often relies on asymmetric or symmetric key sets, as does the recovery of unique data. Manikandan et al. [41] presented an ineffective or unapproved attempts had been made by various illegal outsiders to snoop on the transform information and keys as security had evolved. The constraints placed on the communication channel, sending, and receiving devices can occasionally degrade information security and prevent the completion of necessary task. As a result, WSN presents key management architecture and information security design. A reasonable integrated solution for secure information transfer and mystery keys to solve these limitations based on this audit and subsequent security flaws. Therefore, consistent, and secure clusters were necessary to ensure the operation.

Many applications that employ WSN for data collecting depend on these networks. WSN were more susceptible to attacks than traditional wireless networks because sensors had limited resources. The weak points of sensor must be consider into account while shaping a strong key management strategy for WSNs. To secure network data transmissions and increase the lifespan of WSN, Al-taha et al. [42] presented a strategy dubbed the symmetric key management scheme. For protecting homogeneous and heterogeneous hierarchical WSNs, the presented method uses symmetric key cryptography requires less processing. Simulation findings demonstrate that the proposed system offers security, conserves sensor energy, and had a little computational cost.

Mathew et al. [43] presented a key management system based on elliptic curve cryptography for use in WSN. Ellipse curve cryptography was used for key management by security-critical applications in WSN's because it increases security per key bit. As a result, the proposed implementation technique permits more phases of node insertion. The design was assessed in terms of hardware complexity and storage. The proposed method outperforms the current EC-based system in hardware efficiency by 23.76%. ModelSim PE 10.4 was used to model the GF (2163) design, Xilinx ISE 14.7 was used to synthesis it, and the Kintex-7 KC705 evaluation board was successfully used to implement it.

Jilnaet al. [44] presented a lightweight key setup method for WSN. The proposed method tackles the shortcomings of both approaches by combining two widely used key exchange protocols. LEAP and COKE. The system was protected against active attackers and node compromise, according to the security. The proposed method was more energy-efficient than COKE and assures the formation of a secret key with just one MAC computation.

Patil et al. [45] presented a brand-new fractal-based cryptography technique to the field of WSN. Due to its chaotic nature and complicated structure, fractal cryptography, which was subset of chaos cryptography, had excellent security properties and was thus preferable to the currently used cryptographic techniques. For heterogeneous mobile WSNs, a unique fractal PKC-based key management technique was put forward. Due to their great connection, the presented technique was more effective for WSNs with small key sizes than RSA and ECC. The proposed method was more effective than the current methods.

For networks of large scale, WSNs use a variety of specialized sensors to record and monitor environmental variables. Essential problems including load balancing, routing, network longevity, and other issues are clarified by C-based WSN. By restricting its resources or refusing to transfer the data to the other clusters, security in C-based WSNs poses a significant issue. WSN offer secure information transfer through the use of several security measures. To promote security for the high information, it is common to encrypt records of information that are transported to different companies while using a limited number of systems. Such encoded data typically relies on symmetric or asymmetric key sets, as does the recovery of unique data. Manikandan et al. [46] examines WSN's key management structure and information security design as of right now. It suggests a realistic integrated approach for safe information transmission and secret keys to overcome these restrictions based on this audit and recent security flaws. As a result, reliable and secure clusters are needed to ensure proper operation of CBWSNs.

Tian et al. [47] provided analytical equations for determining self-capacitance, leakage inductance, and ac resistance in TWAs, ranging from the typical non interleaved primary or secondary winding architecture to an interleaved, sectionalized, and bank folded architecture. For an RM8 transformer with a turn ratio of 10, the calculated results are examined experimentally and through finite-element simulations. The four TWAs for an EF25 transformer with a 20-turn ratio are examined and put into practice.

Hamsha and Nagaraja [48] noted how crucial secure sensor connection is to be preventing unauthorized activities. In self-organized, infrastructure-less networks with constrained amounts of computing power, energy, and other resources, security is a significant problem. To enhance network performance, the amount of overhead must be decreased. Performance of the network is also influenced by the of the secret key that must be transmitted among the SNs. The dimensions of the secret key that must be connected is decreased by the proposed LWKMS. It uses fewer network resources, distributes the secret throughout the network's sensor nodes, and offers effective security even if the keys are stolen by an attacking node. According to the simulation results, the suggested lightweight technique uses less energy and has less overhead than the current method, the GKM Scheme. Table 2.2 denotes the Key management techniques in static homogeneous WSN by mentioning the techniques used.

Table 2.2 Key Management Techniques in Static Homogeneous WSN

Sl no	Author name	Technique used	Observation	Advantage	Limitation
1.	Jilna et al. [36]	Elliptic curve Diffie-hellman key exchange for static WSN	When compared to the elliptic curve-based system, the proposed method had significantly lower communication overhead, computational costs, and storage needs.	Provides effective wireless security feature implementation, including secure web browsing and email.	This method was more complex and difficult to implement.
2.	Zhang et al. [37]	A hybrid key management method	The tree-based path key formation approach was presented to efficiently address the connectivity issue of connection links.	Secure network data transmissions and increase the lifespan of WSN.	With this, the issue of increased node capacity storage requirements and subpar connectivity in network

3.	Rajasoundaran et al. [38]	Watchdog-based IDS selection techniques	To boost watchdog availability ratio in WSN and defend against various sorts of attacks, suggests new secure watchdog selection process.	It was capable of detecting new or previously unrecognized attack kinds.	Every time transportation or activity results it was observed from the established regular traffic patterns or activity, an alarm is produced.
4.	Gandino et al. [39]	Public-key cryptography	A real-world network experimental investigation demonstrates that the proposed method may be successfully used with devices with little computing power.	The best defense against a threat that compromised one or more nodes.	The public key cryptography for encryption was speed.
5.	Patel et al. [40]	An efficient session key	The proposed method by	Delivers a better session key by	The inability to scale and the

		management technique	dynamically choosing CH for every round and cut down on energy use by sending messages via CH.	periodically updating inside the cluster and so avoiding various types of attacks from malicious nodes.	static nature of the CHs in each round
6.	Manikandan et al. [41]	Elliptic curve cryptography	A reasonable integrated solution for secure information transfer and mystery keys to solve these limitations based on this audit and subsequent security flaws.	Provides effective wireless security feature implementation, including secure opening as email.	This method was more complex and difficult to implement.
7.	Al-taha et al.[42]	A strategy dubbed the symmetric key management scheme	Simulation findings demonstrate that the proposed system offers security, conserves sensor energy,	Secure network data transmissions and increase the lifespan of WSN	The key must be communicated to the party with which you share data.

			and had a little computational cost.		
8.	Mathew et al. [43]	Elliptic curve cryptography	The proposed method outperforms the current EC-based system in hardware efficiency by 23.76%. ModelSim PE 10.4 was used to model the GF (2163) design, Xilinx ISE 14.7 was used to synthesis it, and the Kintex-7 KC705 evaluation board was successfully used to implement it.	Efficiently implements wireless security features, allowing for safe email and online browsing, for example.	This methodwas more complex and difficult to implement.
9.	Jilna et al. [44]	Lightweight key setup method for WSN	The presented method was more energy-efficient than	The easy design and effective operation make it attractive.	More energy requirements greatly restrict

			COKE and assures the formation of a secret key with just one MAC computation.		the network performance.
10.	Patil et al. [45]	Brand-new fractal-based cryptography technique	Due to their great connection, the presented technique was more effective for WSNs with small key sizes than RSA and ECC.	Had excellent security properties and was thus preferable to the currently used cryptographic techniques.	Even for a valid user, difficult to access at a critical decision making period.
11.	Manikandan et al. [46]	C based secured key management technique	By reducing the resources available to it or by refusing to send data to other clusters.	The flow explores gaps in the area of information security and key management problems of WSN circumstances are brought to light by the investigation.	In architecture of network, the CHs limit is higher in terms of calculation control and vitality than the part nodes.

12.	Tian et al. [47]	Analytical equations are used in the architecture of transformer windings.	For figuring out the ac resistance, self-capacitance, and leakage inductance in TWAs.	TWAs with the lowest self-capacitance are especially well suited for applications of HV charging.	In order to prevent high switching loss and other issues, it is crucial to forecast the self-capacitance during the design phase.
13.	Hamsha and Nagaraja [48]	Technique for lightweight key management based on threshold cryptography.	To make the secret key that needs to be shared smaller.	To ensure the authenticity and confidentiality of the message, the base station recovers all of the shared keys.	To increase network performance, network overhead must be decreased.

2.3 Dynamic key management techniques

People started to think that ITS would be possible since current vehicle and communication technology evolved quickly. ITS strives to increase traffic efficiency and road safety by integrating information technology into the infrastructure of transportation. However, in VCS, security continues to be a top priority. Secured group broadcast can be used to remedy this. Secure key management systems were therefore regarded as a crucial method for network security. Lei et al. [49] presented a safe key management in heterogeneous networks. By gathering data on encapsulating block to transport keys, vehicle departure, and then carrying out rekeying to vehicles inside the same security domain, the security managers play a crucial role in the system. A unique

network architecture built on a blockchain structure decentralized serves as the framework's first component. The blockchain idea was put out to make distributed key management in several VCS areas simpler. The dynamic transaction collection period was used in the framework's second section to further shorten the time required for important transfers during vehicle handover.

As broadcasting characteristics of WSN had high requirements for network security, they were typically employed in challenging contexts. The best defense against attackers attempting to intercept transmitted messages was encryption. Sun et al. [50] presented a topological structure of local dynamic scheme based on layer-cluster accomplishes the key management progress in WSN. By slowing down the negotiating process while maintaining network security, the technique saves more energy. According to this plan, the sensor nodes create a specific cluster based on their placement and choose the CH nodes using a self-election mechanism.

Yousefpoor et al. [51] presented a management key system uses both pre-distribution and post-deployment process for key distribution among the SNs, placing it in the category of hierarchical network-based methodologies. The proposed key management system's use of fuzzy logic improves decision-making precision and adds to its smartification. As a result, the network's energy use was decreased, and its lifetime was extended. According to simulation findings, the system was more effective than previous key management systems in terms of needed memory space, communication overload, and energy usage.

Secure communications was necessary for real-world WSN applications including border control, healthcare monitoring, and target tracking. As a result, one of the first steps in setting up a WSN was to give the keys to sensor nodes so they may utilize them to secure the messages sent between the sensors. The communication between a pair of nodes or a group of nodes was secured by the key management algorithms used in WSN. The sensor nodes low store capacity, however, make storage demand a crucial factor in evaluating key management strategies. Dave et al. [52] presented a key management scheme currently being considered for WSNs were categorized in to three groups: storage efficient, storage inefficient and very storage efficient key management schemes.

A sensor node may be physically attacked by an attacker, the safety key management approach offers extensive coverage for WSN issues. Various current key management techniques

propose operational requirements and security. The WSN had been employed in a variety of dynamic applications, including process monitoring, military surveillance, monitoring of areas and healthcare facilities, and dynamic sensor devices. Small sensor nodes with compute capability, limited energy, and memory make up wireless device network protocols for encryption used in communication and data security. Kamble et al. [53] presented a system that uses inefficient key management that differs by node flexibility in secure communication. When a new node joints a cluster, the method facilitates rapid key update and also offers key secrecy. This approach, which was successfully presented in a conflict with numerous multi hop wireless networks, had undergone security.

In recent years, WSN had grown due to their crucial function in monitoring environmental factors relevant to both civilian and military applications. Wearable technology can potentially incorporate sensors to monitor patient's vital signs for the healthcare industry. WSNs were dynamic because sensor device can move around to meet the needs of the application. Security was a difficult problem in crucial dynamic WSN applications. Many dynamic key management protocols and dynamic WSNs had been developed in the past to help accomplish this aim. Kuchipudi et al. [54] presented a dynamic key management in dynamic WSNs was insufficient. To serve as starting point for further in these networks provided the observations in a broad approach.

Data volume had been expanding significantly over the past several years due to the cyber physical social system increasing sensing and communication. Storage providers had shown a lot of interest in secure de duplication since it improves data management effectiveness while protecting data privacy. Adopt bilinear paring as the primary approach to resolve this issue. Bilinear paring, however had substantial implementation costs due to calculation costs. Wen et al. [55] presented a SKC key management system. In SKC, each data owner may specifically check the validity of the session key and dynamically modify it in response to data updates. Furthermore, a CKS was introduced to enable group combination and eliminate the need for a gateway. Security research shows that in the event dynamic updates, both SKC and CKS can preserve the privacy of the data and the convergent key. According to the simulation findings, SKC and CKS may greatly lessen communication complexity during the data uploading phase.

IoT security threats were on the increase and had serious repercussions. To prevent confidentiality attacks, data confidentiality was often built on a powerful symmetric-key method. For a variety of IoT system applications, a lightweight cyber scheme that was both effective and efficient must be developed. The dynamic key method was the foundation of a group of recent lightweight cryptographic algorithms that use a minimal number of rounds to reduce compute and resource overhead without sacrificing security. Noura et al. [56] presented this reasoning and offers a novel, adaptable, lightweight cyber that may operate in chaining or not, had a straightforward round function, and generates a unique dynamic key for each input message.

With physical items often moving between different locations, WSN was supplied for a variety of applications, including military identifying and following, industry status checking, and activity stream checking. Appropriate encryption key protocols were necessary for protecting data and correspondence. In the context of unique Wireless Sensor Networks (WSNs) characterized by node mobility, Kumar et al. [57] introduce the CL-PKA protocol, designed to facilitate secure communication. This protocol enables efficient key updates when a node joins or leaves a group and ensures the confidentiality of both forward and backward keys. A node breach has a limited impact on the security of other communication joints because to the protocol, which also supports effective key revocation. A security analysis of the strategy reveals that the convention was successful in defending against several threats. To determine the optimal time, energy, connectivity, and memory performance, CL-PKA was successfully in defending against several threats. To determine the optimal time, energy, connectivity, and memory performance, CL-PKA is implemented in Conic OS and tested using the Cooja test system.

One of the biggest issues facing WSN was network communication security. In contrast to heterogeneous WSN, the key distribution problem had received a lot of attention in traditional WSN. By inserting high resource capacity sensor node into the network, heterogeneous WSNs had maximized the network's capabilities and created new security prospects. Athmani et al. [58] presented a dynamic authentication and key management strategy for heterogeneous WSN. The major goal was to maximize security while offering a single, lightweight system for key establishment and authentication.

A network of linked devices that have been deployed to report sensitive environmental data makes up the WSN. Due to the constrained resource capacity of devices, key management in WSN continues to be a difficult problem. The majority of current systems place more of an emphasis on key storage and updating optimization than on mobility, which is more important in today's applications. An effective key management system with mobility support was suggested by Omar et al. [59]. In order to satisfy both the objectives for robustness and efficiency, the suggested technique is based on hybrid key establishment. The sensor nodes can move around, returning to their cluster or joining others. They incorporate simple methods for key update, departure, revocation, and integration of sensor nodes. By comparing it to other concurrent methods, where it performs best, its effectiveness is assessed.

The fundamental management tactics for such a future Internet rely mostly on a reliable third party, which necessitates complete KGC confidence. According to recent studies, we put too much faith in third parties, making it unlikely that centralized cloud centers can provide clients with appropriate services; as a result, these centers do not apply to user privacy-oriented situations. Ma et al. [60] proposed a distinctive solution to address latency reduction using a blockchain-based Decentralized Key Management Architecture (DKMA) integrated with fog computing. The approach incorporates multiple blockchains in the cloud to enable cross-domain access. To fulfill the needs of decentralization, fine-grained auditability, high scalability, and flexibility for hierarchical access control in the Internet of Things (IoT), the proposed method leverages blockchain technology. To enhance extensibility, the authors introduced techniques for system operations and included various authorization assignment types along with group access patterns.

The WSN, according to Bagavathipriya [61], is a perplexing area of study once security concerns are included. A crucial WSN design objective is to maintain the energy needed for communication to minimize packet loss or packet drops, rapid energy depletion, and node performance decline due to serious threats throughout the network that may cause packet delivery delays. The device nodes with limited resources use more energy and are more vulnerable to threats. Furthermore, robust cryptographic techniques are required for sensor nodes to offer improved lifetime and security services. It has been demonstrated that asymmetrical cryptosystems outperform symmetrical ones in terms of security achievement. Additionally, clustering is a crucial WSN approach that maximizes network longevity while lowering energy usage. Consequently, it

is suggested to identify the cluster heads and provide safe data transmission between the cluster head and sink nodes using a hybrid mix of a Neuro-Fuzzy based clustering technique and modified ECC based key management.

To demonstrate that existing group key management systems meet the requirements for forward and backward secrecy, the passive adversary model was taken into consideration. The active outsider adversary concept, in which the enemy compromises a legitimate group member, is a more realistic one. Because most techniques are insecure under the active adversary concept, their practicality of application is limited. The group key management systems based on proxy cryptography were examined by Patil et al. [62] for their security under the active outsider adversary scenario. The group key management scheme's security depends on the underlying proxy cryptosystem's ability to satisfy certain crucial features, including unidirectionality, non-transitivity, and resistance to collusion. They demonstrate the vulnerability of all proxy cryptography-based schemes to active outside adversaries as well as the shortcomings of the proxy re-encryption techniques they use. They underline that group key management techniques must be secure under the active external adversary model to be used in practice.

To safeguard against scan-based and memory attacks during manufacturing and in-field testing, Lee et al. [63] devised a secure scan architecture based on dynamic keys, working in conjunction with the intrinsic Physical Unclonable Function (PUF) of chips. This secure architecture ensures that only legal test patterns, when shifted into the scan chains, prompt the retrieval of genuine circuit responses. Notably, no test key is stored in memory, effectively preventing memory attacks. To enhance the security of chips, the PUF is utilized to differentiate legal test patterns for various manufactured chips. The analysis results indicate that this protective strategy achieves a robust security level without compromising system functionality, testability, or diagnosability. Table 2.3 denotes the dynamic key management techniques by mentioning the techniques used.

Table 2.3 Dynamic key management techniques

Sl no	Author name	Technique used	Observation	Advantage	Limitation
1.	Lei et al. [49]	A safe key management in heterogeneous networks	The block chain architecture outperforms the structure with a central manager in terms of key transfer time, while the dynamic scheme enables SMs to adapt flexibly to different traffic levels.	Increases security, improves energy efficiency, and uses less memory.	It cannot be used for high speed communication as it was designed for low speed applications.
2.	Sun et al. [50]	A local dynamic scheme based on layer-cluster topological architecture	The scheme's flexibility and extensibility allow it to better adapt to the network's dynamic changes.	Less energy consumption, load balancing, reusability of resources and improved network life time.	This scheme cannot be directly applied in WSN.
3.	Yousefpoor et al. [51]	Pre-distribution and post-	The system was more effective than previous	Fuzzy logic improves decision-	Even for a valid user, difficult to

		deployment process	key management systems in terms of needed memory space, communication overload, and energy usage.	making precision.	access at a critical decision-making period.
4.	Dave et al. [52]	Storage inefficient, storage efficient and very storage efficient key management schemes.	The connection along a pair of nodes or a group of nodes was secured by the key management algorithms used in WSN.	The sensor nodes low store capacity, however, make storage demand a crucial factor in evaluating key management strategies.	At a crucial juncture in a decision-making process, even a genuine user would find it difficult to access authentic, digitally signed content that had been highly encryoted.
5.	Kamble et al. [53]	Inefficient key management	This approach, which was successfully presented in a	The method facilitates rapid key update and	

			conflict with numerous multi hop wireless networks, had undergone security.	also offers key secrecy.	
6.	Kuchipudi et al. [54]	A dynamic key management in dynamic WSNs	To serve as starting point for further in these networks provided the observations in a broad approach.	Increases security, improves energy efficiency, and uses less memory.	It cannot be used for high speed communication as it was designed for low speed applications.
7.	Wen et al. [55]	Session-key based convergent	Security research shows that in the event dynamic updates, both SKC and CKS can preserve the privacy of the data and the convergent key.	Efficient and fast for large amount of data.	The necessary to keep key secret this can be especially challenging where decryption and encryption take place in different locations, requiring the key to be moved.

8.	Noura et al. [56]	A unique dynamic key for each input message	The dynamic key method was the foundation of a group of recent lightweight cryptographic algorithms that use a minimal number of rounds to reduce compute and resource overhead without sacrificing security	The proposed encryption scheme may be used to real-time applications and/ or low-resource devices like multimedia internet of things systems.	Even a legitimate user may find it challenging to obtain valid, digitally signed material that had been strongly encrypted.
9.	Kumar et al. [57]	Certificate less-powerful key administration	This inquiry concerns implementing CL-PKA in Conic OS and simulating it with the Cooja test system in order to assess the best time, energy, correspondence, and memory performance.	The efficiency with which it takes large amount of data and encrypts it quite rapidly.	The disadvantage of a private key encryption system was that it requires anyone new to gain access to the key.

10.	Athmani et al. [58]	A dynamic authentication and key management strategy for heterogeneous WSN	The key distribution technique relies on previously stored data to produce dynamic keys and does not need to secure channel or sharing phase	Increases security, improves energy efficiency, and uses less memory	It cannot be used for high speed communication as it was designed for low speed applications.
11.	Omar et al. [59]	Energy-aware and effective key management framework	A method that uses hybrid key establishment to satisfy the demands for robustness and efficiency.	Integrating an access control service is one of the elements that can enhance the suggested approach.	The only node in a cluster that updates key when a SNs enters or exits the cluster is the CH.
12.	Ma et al. [60]	Block chain based key management architecture	To reduce latency and several block chains operating in the cloud to achieve cross-domain access	Increase in network size, system performance increased	There were no cloud managers available to support the persistence of the blockchain-based IoT ecosphere.

13.	Bagavathipriya [61]	Modified ECC &neuro fuzzy clustering hybridization	To recognize the cluster heads and provide secured data transmission between the sink nodes and the cluster heads	High level security	delivery of packets is delayed

2.4 Group key management techniques

Yao et al. [64] presented a LKH++ based secure low-power key management scheme. A secure tree was built in this scheme to manage group keys. The scheme suggests using a key tree construction approach and a key holding mechanism to lessen the processing and storage requirements for each sensor node. Rekeying was also supported by WLKH to improve network security and node capture resistance. WLKH was extremely efficient in terms of security, computing, and key storage, according to a performance study.

Hur et al. [65] presented a unique key management strategy. It had a feature that makes it possible for authorized receivers to retrieve the most recent group key, even if they Misskey update messages during prolonged sessions. The technique makes use of member computation and brief hint messages. Performance research reveals that the proposed method was superior to earlier trustworthy group key distribution schemes in terms of scalability and effective key rekeying. The conditional access system in a media broadcast that lacks a feedback route from viewers to the broadcasting station was the focus of the proposed key management method.

Group key management was a crucial technique for protecting IoT data privacy. The current group key management approach, which was primarily reliant on central authentication and adheres to a hierarchical structure, cannot be adjusted to the scattered internet of things environment. Block chain was a good option for enhancing the security of group key management in the internet of things since it was transparent, unchangeable, and traceable. Ma et al. [66] presented a block chain IoT group key management. Blocks of the user's activity and key update

may be logged in this fashion, making it simple for other domain administrators to retrieve and audit the information.

Manikandan et al. [67] proposed a polynomial equation-powered pairing-based cryptography protocol. First, before uploading to the cloud, the document was just minimally complexly encrypted once to save computational cost during group communication. The security concludes by demonstrating that all potential attacks-including man-in-the-middle, message notification, and collusion attacks can be prevented by managing user security parameters carefully. The results of the implementation show how well this work can handle secure group conversations in cloud storage.

Selecting the most effective service among the available services was a significant job while using VANETs, which offer comparable services at different service locations. Similar to that, using services for exchanging time-sensitive messages necessitates secure protocols. Ramamoorthy et al. [68] presented an effective group-based dual mode key management (G-DMKM) system to effective service and secure access method to the service. The base stations were grouped in G-DMKM for each session based on localization in a time window manner, which limits the key and group lifetime. Each group receives a unique group key that was produced using the time-domain randomization process and was utilized by all stations and vehicles. Using group and private keys, vehicles communication was authenticated. The base station that the car was parked beneath generates the private key. To choose the best service from the available services, the MALSA in G-DMKM computes the MASF for each service. Additionally, the way with the greatest STS support was chosen for secure access to the service and data transfer. STS evaluates the STS value for each path found towards the service point.

Every developing country had been concentrating on smart cities for past decades. The people of a smart city will receive all required services, such as efficient water, waste, traffic, and health management. VANET, a novel paradigm in smart cars, was capable of forming a network. The RSU was wirelessly equipped so that drivers of vehicles may efficiently communicate crucial traffic data and make informed judgments while operating their vehicles. Each roadside device was equipped to control a select number of automobiles, which may gather together. In the VANET group, there were other data transmission systems, although they were not as secure.

Pulagara et al. [69] presented an elliptic curve cryptographic-based intelligent conditional privacy-preserving strategy for automotive ad hoc networks. The proposed method was clever, effective, and simple to implement, according to the security.

Mohammadi et al. [70] presented a group distributed key management strategies for WSN. To safeguard the group keys from being utilized against a network opponent had acquired access, a lot of emphasis on forward secrecy and backward secrecy. Unfortunately, when a certain number of nodes were hacked or some group keys were disclosed, the majority of distributed systems for group key management do not ensure forward and backward secrecy. A brand-new, locally collaborative, dynamic distributed group key management technique that offers both forward and backward secrecy.

Due to their extensive use, MANETs had generated a lot of issues. Wireless nodes in MANETs typically self-organize into groups to carry out cooperative tasks and communicate with one another over open channels that were subject to intrusions. In MANETs, Group key management was typically used to provide secure group communication. However, the majority of current group key management techniques for MANETs still had several drawbacks, such as receiver limitation, reliance on a reliable dealer, and high overheads for certificates. Han et al. [71] a group key management strategy for MANETs based on the identity-based authenticated dynamic contributory broadcast encryption protocol, which expands on prior work to solve these problems. Certificate management and eliminates the requirement for a reliable dealer to provide each node with a secret key. The secret keys can be negotiated by a group of wireless nodes in a single round. Additionally, because the scheme was receiver-unrestricted, each sender can freely choose any advantageous nodes in a group as the receivers. Additionally, plan simultaneously meets the requirements for authentication, message secrecy, known security, forward security, and backward security. Analysis of plan's performance demonstrates its effectiveness.

Mahaveerakannan et al. [72] introduced a group key management architecture tailored for the UAV-MBN, a military network. To address specific challenges in wireless group key management, namely operational efficiency and accommodating multiple membership changes, they proposed a hybrid group key management technique designed to operate within each theatre of the UAV-MBN. This approach aims to enhance the operational efficiency of wireless group key

management while reducing associated operational costs through micro-key management. Additionally, the issue of multiple-membership changes is addressed through a membership-oriented group key management approach, enabling more effective handling of such changes compared to traditional application-oriented group key management methods.

Security for WSN was becoming more and more crucial, especially for sensitive applications. Key management was one of the most crucial security procedures. Key management was one of the most crucial security procedures. Hussain et al. [73] presented a pair wise and group key management scheme for WSN. To save time and space, the public matrix of Blom's scheme was generated using an ID-based circular matrix rather than a vandermonde matrix for the pair wise key establishment. To reduce the burden on the group head and other nodes and to allow each member to independently confirm the validity of the group key, the group key establishment enables everyone in the group to participate in the group key management.

The two most prominent wireless technologies for building a comprehensive smart environment for the IoT are RFID and WSN. Since both RFID and WSN are devices with limited resources, we must choose lightweight cryptography for security. One of the main challenges for mobile sensing devices under resource restrictions is key management. This work builds on the work done by Chugh et al. [74] employing limit of agreement for anomaly score and efficient error prediction. Through the use of an outlier detection mechanism, this study ensures the availability of cryptographic properties in an integrated RFID-WSN network with 50 to 5000 nodes. A system's resistance to outliers is measured using detection ratios and anomaly scores. For defense against DoS attack, the suggested outlier detection system recognizes the inliers and outliers by anomaly score. Intruders can be found in a matter of milliseconds without interfering with access permissions. The proposed protocol outperforms Kumar et al. by a minimum of 6.2% and a maximum of 219.9% in terms of throughput. In comparison to Kumar et al. protocol, the suggested protocol shows a minimum increase of 8.9% and a maximum improvement of 19.5% in terms of PDR.

WSN is made up of numerous sensor nodes that are battery-powered and have a limited amount of memory and computing capability. Since the safety of the sensors inside is under multiple threats, secure communication requires some sort of cryptographic system. Key management in WSNs is an active area of study. A Lightweight Matrix-based key management system for WSN

was proposed by Kamal et al. [75]. Our suggested key management solution makes use of encryption to increase storage capacity, make nodes lighter, and improve connection between nodes. They evaluated our plan, and the results showed that it would improve network connectivity and storage capacity. Table 2.4 denotes the group key management techniques by mentioning the techniques used.

Table 2.4 Group key management techniques

Sl no	Author name	Technique used	Observation	Advantage	Limitation
1.	Yao et al. [62]	LKH++ based secure low-power key management scheme	WLKH was extremely efficient in terms of security, computing, and key storage.	Rekeying was also supported by WLKH to improve network security and node capture resistance.	It cannot be used for high speed communication as it was designed for low speed applications.
2.	Hur et al. [63]	A unique key management strategy	The conditional access system in a media broadcast that lacks a feedback route from viewers to the broadcasting station was the focus of the	The technique makes use of member computation and brief hint messages.	Even for a valid user, difficult to access at a critical decision making period.

			proposed key management method.		
3.	Ma et al. [64]	Block chain technology	Blocks of the user's activity and key update may be logged in this fashion, making it simple for other domain administrators to retrieve and audit the information.	Block chain technology was used in this plan to increase the effectiveness of group key updates for dynamic group members.	Block chain were high energy dependence, the difficult process of integration and the implementation high costs.
4.	Manikandan et al. [65]	Polynomial equation-powered pairing-based cryptography protocol	Blocks of the user's activity and key update may be logged in this fashion, making it simple for other domain administrators to retrieve and audit the information.	The re-encryption of documents in the cloud was prevented on the group manager side	Expensive double encryptions, the requirements for re-encryption after each user exit procedure, and vulnerability to attacks.
5.	Ramamoorthy et al.[66]	An effective group-based	Simulation results reveal	Using group and private	When encryption and

		dual mode key management	that the inclusion of an STS-supported route increases G-DMKM efficiency in all aspects	keys, vehicles communication was authenticated.	decryption occur in separate places and the key needs to be transported, maintaining key secrecy can be very difficult.
6.	Pulagara et al. [67]	An elliptic curve cryptographic-based intelligent conditional privacy-preserving	The proposed method was clever, effective, and simple to implement, according to the security.	Encryption/ decryption were much faster than the other methods.	Too complex to understand.
7.	Mohammadi et al. [68]	A group distributed key management strategies	Comparing with two related schemes both analytically simulations to verify its efficiency on storage and communication overhead.	Fast and efficient for large amount of data.	The majority of distributed systems for group key management do not ensure forward and backward secrecy

8.	Han et al. [69]	The identity-based authenticated dynamic contributory broadcast encryption protocol	Additionally, plan simultaneously meets the requirements for authentication, message secrecy, known security, forward security, and backward security.	Certificate management and eliminates the requirement for a reliable dealer to provide each node with a secret key.	The disadvantage of a private key encryption system was that it requires anyone new to gain access to the key.
9.	Mahaveerakannan et al. [70]	Group key management architecture for the UAV-MBN	The performance issue of multiple-membership changes was targeted by a membership-oriented group key management approach.	This strategy can increase the operational effectiveness of wireless group key management while lowering the operational costs related to key management through the use of micro-key management.	It lacks authentication process and does not clearly define any process for recoking or refreshing keys.

10.	Hussain et al. [71]	A pair wise and group key management schemes	To reduce the burden on the group head and other nodes and to allow each member to independently confirm the validity of the group key, the group key establishment enables everyone in the group to participate in the group key management.	It offers robustness against node compromise at a reasonable scalability cost.	The complexity of the protocol increases overhead costs.

2.5 Key management schemes using clustering approach

Now a days, data mining and packet transfer between various sensor nodes in a WSN were the key security issues that arise. Borkar et al. [76] introduced an efficient clustering method known as the adaptive chicken swarm optimization algorithm to address these issues, specifically targeting the role of the cluster head. The adoption of this adaptive approach not only increased the network's lifespan and scalability but also significantly reduced time consumption. Furthermore, an acknowledgment-based method was employed to identify malicious sensor nodes using an adaptive Support Vector Machine (SVM) classification, a supervised learning technique integrated with Intrusion Detection Systems (IDS). This two-stage classification methodology effectively detected various attacks, including Denial of Service (DOS), probing, User to Root (U2R), and Remote to Local (R2L), which were then integrated with the IDS. Upon intrusion

detection, other sensor nodes were granted access to a high-level security mechanism and an intrusion response, ensuring secure packet transfer across diverse sensor nodes. The proposed approach, executed in the Python platform, demonstrated superior results compared to existing methods through a comprehensive comparison.

The numerous security vulnerabilities that the wireless communication medium faces secured communication through the WSN were one of the main issues. To establish secure communication within the clustered Wireless Sensor Network (WSN), Saraswathi et al. [77] introduced a key management protocol named multistage key management. The protocol is structured into three phases: pre-deployment, key creation, and key authentication and verification. In the initial step, nodes are assigned their identities, while the second stage employs the homomorphic encryption model for generating the communication key. A mathematical model, including a hashing function among other components, is constructed. The MSKM protocol ensures secure communication over the WSN by authenticating the involved entities. The entire protocol was evaluated using various criteria and compared against several state-of-the-art methodologies. The communication overhead, detection accuracy, key memory storage, and energy values for the proposed MSKM protocol were 0.122 kb, 0.929 kb, 2.332 kb, and 14.586 joules, respectively.

Within Wireless Sensor Networks (WSN), the hierarchical clustering method serves as a valuable tool for topology control, effectively prolonging the network's lifespan by reducing the volume of broadcasts directed towards the base station. Ahmed et al. [78] introduced the SEED clustering algorithm as a routing protocol, where direct communication between cluster heads and the base station divides the network sensing area into three energy zones. The cluster heads in the high-energy region communicate with the base station over a greater distance and at a higher energy cost. To minimize broadcasts to the base station, sensor nodes from the same application form sub-clusters. In each round, one node from these sub-clusters awakens to transmit data, while others remain dormant to conserve resources. The effectiveness of the algorithm is assessed using six criteria, and simulation results indicate that SEED outperforms existing clustering techniques in terms of network lifetime and overall performance.

To monitor conditions at various places, WSN are made up of several tiny nodes with distributing equipment. In a sensor field, which groups certain locations, wireless sensor nodes are often dispersed. In order to ensure safe data transport based on clustering mechanisms, Robinson et al. [79] presented the ECBK management protocol. The cluster coordinator node, which is utilized to coordinate the members and provide protective communication among the sensor nodes to increase dependability, is given additional weight in this protocol. Two different types of nodes were deployed in enhanced cluster-based key management. To facilitate the routing process without interruption, the high power nodes group together with nearby nodes to create clusters. The ECBK protocol, which distributes load evenly among clusters, achieves high throughput, reduces end-to-end delay, lowers routing cost, and increases network lifespan. According to the simulation results, the existence of high transmission nodes improves throughput by 45% when compared to other similar systems and lowers latency, load balancing, and overhead associated with routing.

Numerous small sensor nodes are used in WSNs, which have a wide range of applications, to analyze and send detected data to the base station. The two main issues for extending the WSN's lifespan are security and energy efficiency. WSNs are vulnerable to a number of dangers because of their broadcast nature, which has to be addressed. These security risks may be avoided, and an efficient clustering strategy can increase the network's energy efficiency and lifespan. The ISFC-BLS routing protocol is suggested as a safe and effective solution for WSNs, and relevant maintenance procedures and routing algorithms are constructed. Bhushan et al. [80] presented a solution employing a fuzzy-based clustering technique, facilitating cooperative communication, and forming balanced load sub-clusters within the network. This approach assists in the selection of nodes joining the cluster. The best route to the goal is found via ant colony optimization. Experimental results and performance analysis reveal that ISFC-BLS surpasses energy-efficient heterogeneous ring clustering and other existing clustering techniques in terms of extending network lifetimes and enhancing energy efficiency. This superiority is demonstrated by the reduction in the number of control messages and node energy consumption, highlighting the efficiency and security of ISFC-BLS.

A significant barrier in WSN is securing the data against intrusion and lengthening network lifespan. The quantity of energy used by each node affects how long the network will last. Selvi et

al. [81] presented a security-based clustering approach to lengthen network lifetime and safeguard data. As the cluster head gathers and aggregates data from the cluster members, it builds the cluster to save energy among the sensor nodes.An unique node data from the cluster head are gathered and aggregated by MDC before being sent to the base station. By authenticating the cluster head by MDC using the shared secret key and the digital signature, the data are shielded from hackers. The outcomes of the experiment shows that the proposed method secures data more effectively and uses less energy than the time stamp protocol and polynomial points sharing protocol.

Santhosh Kumar et al. [82] introduced a Secure and Energy-Efficient Data Distribution Protocol (CSDP) that operates in a distributed manner, encompassing route discovery, cluster formation, cluster head selection, cluster-based routing, and security considerations. The protocol incorporates a novel authentication algorithm based on digital signatures, trust-based security enhancement, and encryption techniques to efficiently manage keys. The primary contributions of this work include the formulation of algorithms for generating public and private keys using cryptography, the development of methods for calculating trust scores and identifying malicious nodes, and the effective detection and elimination of malicious behavior to enhance network security. Simulation results demonstrate that the proposed protocol enhances security by introducing a time-efficient encryption and decryption algorithm, leading to increased packet delivery ratio and network throughput. Additionally, the protocol reduces energy consumption and data dissemination delay.

A specific network compared of tiny sensor nodes is known as WSN. The sensor nodes have distinguishing qualities. Thus, it has the ability to perceive and interpret data in WSN. WSN offers a wide range of incredible uses. Despite WSN's importance, this type of network has a number of problems. Security and energy usage are the two greatest issues that WSN is facing today. For WSN applications to function, robust security development is required. Cryptography approaches are highly advantageous for WSN security needs. The fundamental issue in implementing any security mechanism, though, is WSN's resource constraints. Mehmood et al. [83] introduced a secure hybrid session key management system that simplifies the main steps of public key cryptography, emphasizing a substantial reliance on symmetric key cryptography. This approach leads to a significant reduction in the energy consumption of Wireless Sensor Networks (WSN) while ensuring optimal security. The proposed method is implemented and analyzed

against benchmark schemes using various metrics. The results demonstrate that the proposed method outperforms other approaches in terms of energy efficiency, providing a robust framework for secure key management and agreement within the context of WSNs.

A large number of cheap, power-constrained wireless sensor nodes make up WSNs, which use self-organization to detect and track environmental physical characteristics. In WSNs, network management and data aggregation are frequently implemented using clustering techniques to create hierarchical network architecture. Liao et al. [84] presented a load-clustering approach for WSNs based on their distance and density distribution, which is fundamentally different from the prior clustering algorithms. The residual energy of nodes follows the random distribution. Simulated experiments show that the new technique can improve the network life cycle and create more balanced clustering structures.

Many civic and military users of WSN necessitate security, such as target monitoring in dangerous circumstances. Typical sensors are not able to apply very resource-intensive security techniques since they have limited computing, energy, and memory capabilities. Jolly et al. [85] presented a IBSK-based cryptographic key management system for the pre-deployment of two symmetric keys to each sensor. The expulsion of the compromised nodes is permitted under the protocol. Because only sensor-to-gateway secure sessions are permitted, the multi-tier network design demonstrates that key management is extremely cheap. Simulation also yields orders-of-magnitude improvements in energy savings when compared to the original IBSK system and Kerberos-like schemes. Table 2.5 denotes the key management schemes using clustering approach by mentioning the techniques used.

Table 2.5 Key management schemes using clustering approach

Sl no	Author name	Technique used	Observation	Advantage	Disadvantage
1.	Borkar et al. [76]	Adaptive chicken swarm optimization algorithm	The suggested approach was implemented in the Python platform, and a comparison with current methods shows that it produces better results.	Simple concept, easy implementation, robustness to control parameters, and computational efficiency.	Global search over the entire search space with faster convergence speed.
2.	Saraswathiet al. [77]	Multi stage key management	The communication overhead, detection accuracy, key memory storage, and energy values for the proposed MSKM protocol were 0.122 kb, 0.929 kb, 2.332 kb, and 14.586	The entire piece was assessed using a variety of criteria and compared to several state-of-the-art methodologies.	It cannot be used for high speed communication as it was designed for low speed applications.

			joules, respectively.		
3.	Ahmed et al. [78]	Sleep-awake energy efficient distributed (SEED) clustering algorithm	The simulation findings demonstrate that SEED outperforms the currently used clustering techniques in terms of network lifetime and performance.	Thus gives the flexibility to express that data points can belong to more than one cluster.	Minimizing the utilization of energies and for extending the lifespan of the network, but poses a limitation, which is regarding the irregular size of clusters.
4.	Robinson et al. [79]	Enhanced cluster based key (ECBK) management protocol	The existence of high transmission nodes improves throughput by 45% when compared to other similar systems and lowers latency, load balancing, and overhead associated with routing.	Coordinate the members and provide protective communication among the sensor nodes to increase dependability, is given additional weight in this protocol.	Too complex to understand.

5.	Bhushan et al. [80]	Fuzzy based clustering technique	That ISFC-BLS is more efficient and secure than energy-efficient heterogeneous ring clustering and other existing clustering techniques.	Thus gives the flexibility to express that data points can belong to more than one cluster.	Clustering are complexity and in ability to recover from database corruption.
6.	Selvi et al. [81]	A security-based clustering approach	The outcomes of the experiment shows that the proposed method secures data more effectively and uses less energy than the time stamp protocol and polynomial points sharing protocol.	As the cluster head gathers and aggregates data from the cluster members, it builds the cluster to save energy among the sensor nodes.	Disadvantage of clustering are complexity and inability to recover from database corruption.

7.	Santhosh Kumar et al. [82]	Cluster based secured data dissemination protocol	The development of methods for calculating trust scores and identifying malicious nodes and finally the effective detection and elimination of malicious behavior for enhancing network security.	Reducing energy consumption and data dissemination delay.	The majority of distributed systems for group key management do not ensure forward and backward secrecy.
8.	Mehmood et al. [83]	A secure hybrid session key management system	Result showing that the proposed method is more energy efficient than the other methods and it offers a powerful framework for secure key management	Advantage is that it is sometimes easier to construct secure than the direct construction of public-key encryption shemes.	The disadvantage of secret key encryption is that a single key is used for both encryption and decryption.

			and agreement in the context of WSNs.		
9.	Liao et al. [84]	A load-clustering approach	Simulated experiments show that the new technique can improve the network life cycle and create more balanced clustering structures.	Clustered solution is automatic recovery from failure.	Clustering are complexity and in ability to recover from database corruption.
10.	Jolly et al. [85]	IBSK-based cryptographic key management system	Simulation also yields orders-of-magnitude improvements in energy savings when compared to the original IBSK system and Kerberos-like schemes.	Many civic and military users of WSN necessitate security, such as target monitoring in dangerous circumstances.	Single key is used for both encryption and decryption.

2.6 Summary

Due to information transfer and communication, it is extremely difficult to maintain data privacy throughout the network. Sensors run on batteries and have limited computer power. Therefore, the traditional cryptography method won't be implemented in WSN. Various securities for data secrecy had been proposed by numerous researchers for the WSN environment. Both multicast and unicast communication are possible in a WSN. Multicast communication dominates group communication. In contrast to unicast communication, which distributes vital information to each member independently via unicast messages, this technique prefers to convey messages via a tree-based design.

It is preferred to manage authentication, access control concerns, and message confidentiality while transmitting the message to the receiver. A node in a WSN system has to securely connect and communicate with a number of other nodes. This is only feasible with group key management. To communicate securely through multicast, group key is essential. Members of the group can communicate using this symmetric key in a multicast situation. Group key management is a need for all forms of security architecture used for group communication. The previous method has various advantages and certain limitations to overcome these limitations new method is required.

CHAPTER 3

Analysis of various key management schemes in wireless sensor networks

3.1 Introduction

Sensors which continuously transfer data to its base station, in WSN. It is a challenge to keep data secure on the network, undertaking because of transmission of the information. Different security techniques were presented by several researchers to offer data secrecy in the WSN context. Wireless networks of a WSN are composed of the devices of distributed autonomous, using the conjoin sensors to evaluate environmental conditions, like pressure, vibration of sound, pollutants & temperature at various locations. In WSN each node has a transceiver or other wireless device, typically a battery. Additionally, military applications like battlefield monitoring served as the initial motivation for the creation of WSNs. Healthcare, homeland security, target tracking and environmental monitoring are just a few of the military [86] and commercial applications that WSNs are expected to find widespread use.

However, because of their ease of flexibility, simplicity, deployment and maintenance, WSN are increasingly employed in a number of civil application fields, such as home automation, traffic management and monitoring of the environment and habitat. Security is a major concern as compared to wired or other wireless competitors, even though WSN can be fast and expensive for applications of healthcare as required. Numerous inside and outside passive and aggressive security assaults can be launched by compromised nodes or attacker nodes. Therefore, techniques of Key management must be developed effectively among CH, SN and BS before a WSN may transmit data securely. Examine the applicability of current mechanisms, like pre-shared keys for nodes of sensor in IoT context and public key cryptography, as well as the the use of connection layer-oriented system of key management, the basic intention is to produce the shared keys for SN which comes under same type of WSN in [87]. Both unicast and multicast communication is possible in WSN. Unicast communication, in other way, sends the critical data via unicast messages to each member separately. Multicast communication predominates group communication and typically chooses to transmit the message in a tree based design. The material of key is transmitted to every member separately using messages as unicast in the unicast method, and using a multicast strategy that combines Lagrange interpolation and a multicast packet [88].

In addition to message secrecy, other issues like authentication, access control, etc, must be addressed when a message is sent to a recipient.

In the system of WSN, a node must connect securely with numerous sensor nodes. The only way to accomplish this is through the GKM. A WSN technique of key management that is effective and supports both pairwise & GKM [89]. A crucial idea in safe multicast group communication is the group key. Members of the group can communicate using this symmetric key in a multicast environment. Any security of the structure for the communication group includes GKM. Three methods like decentralized, centralized and distributed are used to distinguish it.

The group key communication has several issues e.g. security, speed, bandwidth management etc. It will efficiently use in bandwidth if communication is well structured and handled. Group communication messages need be to securely transmitted. Of all its security issues, GKM is the most crucial. A productive technique that helps communication of group is multicast. It aids in improved network resource use. To guarantee the privacy of group communications, the group key must be distributed to all members and kept secure and up to date. This aids in ensuring that the group key is only accessible to authorized users. Before transmission, each message must be encrypted using the group key. Even when they receive the encrypted message, others or intruders are unable to understand the messages. The network needs to be scalable and dynamic in any real-world application. These networks may experience changes in frequent membership. The four basic rules of the key management are forward security, backward security, group confidentiality, and collusion freedom. This must be followed with each change in membership, therefore key management operations must be carried out. Secure group communication depends on effective GKM.

3.2 GKM techniques

The protocols are categorized into three groups depending on "how" the management of key activities are carried out: decentralized, centralized & distributed. For centralized GKM protocols, a central group key server is used and it is exclusively in charge of maintaining and transmitting the group keys.

Despite the simplicity of this solution, a system bottleneck is caused using a single key server. The entire group is divided into separate subgroups in the systems of decentralized GKM, and each

group has a controller of the subgroup. The controller of the subgroup is in charge of the operation of key management. This executes message relaying tasks concurrently with message delivery, which causes transmission delays. Each of the group members consists of an equal portion to contributed to the group key while using contributory or distributed GKM. The issue of single point failure and centralized trust is avoided in this way.

Techniques of key management can be differentiated into 3 methods depend on "when" the group key is updated: message driven, membership driven and time driven. For time-driven approaches, the group key is given on a regular basis. This increases system security and lowers the frequency operations of rekeying in highly adaptable groups. With the protocols of message driven management of key, rekeying occurs concurrently with every message sent. This helps in ensuring the safety of both forward and backward.

When a member joins or leaves a cluster, the group key is updated according to the protocols of membership driven GKM. The below discussion explains about the requirements of GKM in the next section. Some of the examples of decentralized and centralized protocols of GKM are explained. It focus more on several distributed key management approaches and its analysis of performance in the coming sections.

3.2.1 GKM requirements

The expanding use of WSN has raised serious concerns about security technology now a day. The sensors are the foundation of many real-time applications. Existing methods are not able to address all types of threats in security, which affect data reliability and security. Four classes of the threats in security for the network were explained below: interception, fabrication, interruption and modification.

Nodes that are unavailable during interruptions include message corruption, node capture, etc. Interception denoted that in anode capture attack, an attacker accesses a network and gains unauthorized access to a data or node. Modification is when an attacker accesses data and makes changes, like DoS. Fabrication involves the attacker intentionally changing the information and adding false data.

a) Security prerequisites

Nodes are unstable by nature & are free to join or leave any group at any moment without risk to their privacy. However, in the dynamic WSN context, they always maintain the forward and backward secrecy.

Secrecy of the group key: The privacy of this kind which stops any attacker from obtaining one of the key nodes for the group. Rekeying must be a reliable process that only uses random numbers and mathematical operations [90].

Forward secrecy: By employing this strategy, the node will be prevented from obtaining the group key in the event that the member leaves from the group.

Backward secrecy: A node's backward secrecy makes sure that group joining will not be permitted to view already existed information [91].

Protection against collusion: It should be prohibited for an unauthorized user to join the group while carrying a public encryption key that is already in use [92].

b) QoS requirements

A crucial component of QoS is service availability, and group communication processes must be supported even in the event of a single unit failure [93]. The system must have sufficient scalability to manage various keys for maintaining group keys.

c) Efficiency needs

The rapid rate of movement of the node and generation of rekey in dynamic WSN groups produces a large number of messages. Thus, creating a key and distributing it further both entail a lot of work at the user levels and control manager. All communication entities must securely keep and manage the keys. The communication functional cost, calculation, storage and rekeying must be reduced by taking into account all efficiency parameters.

d) Join and leaves nodes

A node informs the CH when it needs to join a cluster. For every node in the WSN network, CH generates a special identification key that must be transmitted to all of the nodes. As a new cluster

member, the recently joined's information is updated by CH. On the departure of the members of active group from the cluster of WSN, CH should receive a leaving message. When a node joins, CH either deletes its keys and data or transfers them to the new node [94].

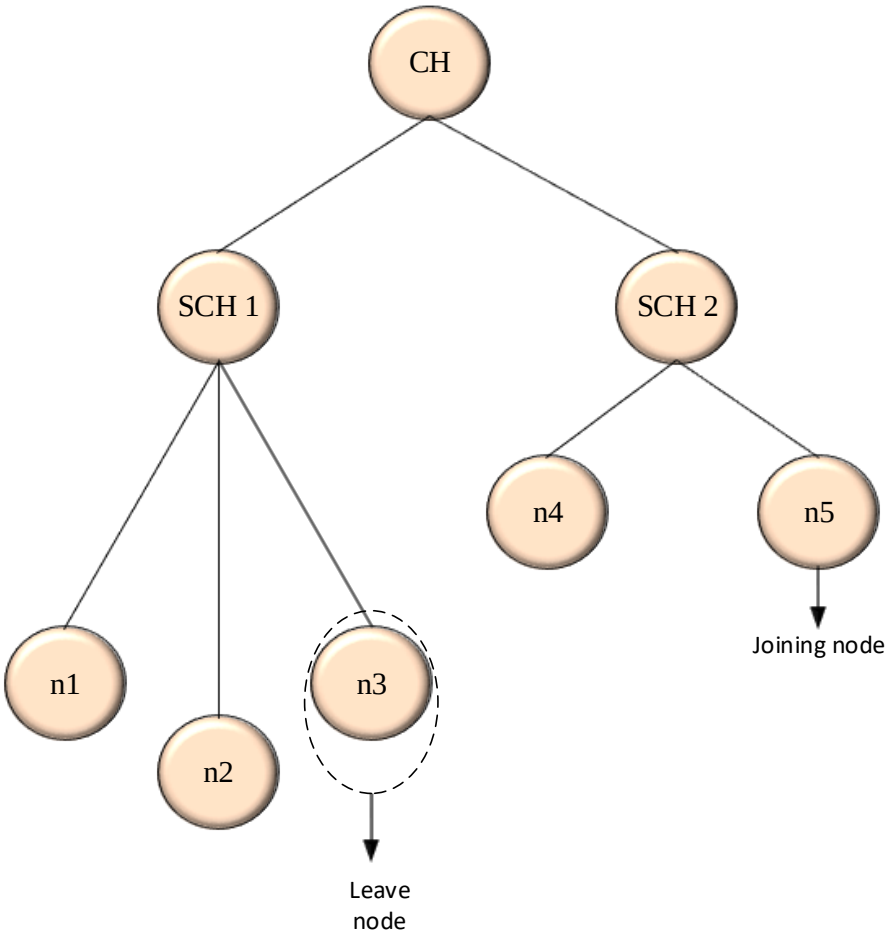


Figure 3.1Join node and leave node

The management of the cluster network, together with its connected nodes and subclusters, is shown in Figure 3.1. Any node can join/leave the network. As a result, cost-effective security measures can be taken into consideration.

3.2.2 Centralized protocols

The entire re-keying procedure will be handled by the key server. Each participant has a KEK that is shared with the key server. As a result, there will be n-keys for a n-members group, & the server which keeps a list of the member group's & group keys. Each time the server generates a latest group key, it encrypts with n KEKs before sending the packets to the appropriate group member.

To minimize the dissipation of average energy & deliver boost packet ratio, centralized energy-efficient routing strategy for dynamic nodes is given in [95]. To accomplish the majority of energy-intensive operations, in [96] it suggested a media access control centralized routing protocol that uses advanced BS.

The group key is then retrieved after each member uses their KEK to decrypt the packets. As a result, each member gets the same key of new group. To maintain forward security & security in backward, the server of key which distributes & generates new group keys each time a member node joins or leaves a group. It is extremely difficult for the server of key to produce, distribute and encrypt n keys in a timely manner in the event of a group of large dynamic. The use of bandwidth is significantly increased by sending n encrypted packets. The following is a description of a few centralized key management strategies.

a) Hao-Hua Chu's protocol

It represents a message driven protocol. A member generates new TEK & message gets encrypted before transferring it when it wants to multicast the message. Additionally, it transmit the TEK to the server of group encrypted using the KEK known only to the group and the member. Server encrypts each message using KEK in between the corresponding member & the server, by using KEK it decrypts the TEK, & after that it unicasts the TEK to the balance group members.

The members then use the key to message decryption from the original member of group after first decrypting the message is from the server & retrieving the new TEK. The server of key also produce new distributes & TEK it to every member after every change in membership. But this increases the server's workload. Next time within the permitted time, assured authorized ping-pong users will be given the most recent TEK, avoiding the key generation process described in [97].

b) GKM protocol (GKMP)

It represents a member driven protocol, each participant and the server share the secret key. With this technique, the server creates a GKP that includes a GTEK and a GKEK. A new participant joins the group, the server creates GKP of new & securely sends to the new participant by KEK encryption created with the new participant. It transmits the new GKP to existing members by encrypting it using the old GTEK. The server produces new GKP when a member quits and

delivers it to remaining members by encryption it with KEKs that are distributed to every member. Backward and security in forward is ensured in this way. However, because each re-keying in this method requires on messages, it is not appropriate for the groups of large dynamic. In WSN, technical management of a hierarchical group key utilizing threshold cryptography is proposed in [98].

c) Protocol of logical hierarchical key (LHK)

It represents membership driven protocol. The logical hierarchical key tree structure serves as the method's foundation. The server will maintain this tree structure. The group key serves as the key tree's root. The secret key used by both the server and each individual user is stored on the leaf node. New group keys are distributed via intermediate keys. The member only utilizes the keys that are located on the way leading them to the server out of all of these keys. Therefore, the impacted path keys must be updated & redistributed after each membership change. The server of key creates new group keys & keys of intermediate in the impacted path when a member enters or quits a group. The LHK technique creates a tree of KEKs to decrease the amount of rekeying messages to O (log N) in [99].

The keys are then safely distributed to the appropriate group members. Compared to previous unicast-based methods, this one is more scalable. The cost of communication for an N-member group with a d-degree key tree is O (log (d N)). However, it is O (n) for the aforementioned unicast techniques. All of the drawbacks of centralized approaches will apply to this strategy as well because it is likewise centralized.

d) Code for key calculation (CKC)

The logical key hierarchy is another foundation for this approach. The intermediate node keys, in contrast to LHK, are determined by individual users. The server provides group key to members when a member joins or leaves a group. Members calculate other keys by utilizing this key, a one-way hash function and node codes. This method's privacy is mostly predicated on the hash function's one-wayness and strength. This technique minimizes both the message size and server overhead. In CKC, some keys should be updated after every member change, same like in LKH-depended methods. Instead of being distributed by the server of key, the keys which are updated

are calculated by group of members. Members use the node codes of the key tree associated with each middle node for this purpose in [100].

3.2.3 Decentralized protocol

The entire group is categorized into multiple divisions by using decentralized approaches. Every group members shares the group key, & every member of a subgroup shares the subgroup key. For each subgroup, there will be a subgroup key server in addition to the central key server. Here are a few instances of this technique. Adaptive decentralized re-clustering protocol was introduced in [101], it explained about the remaining every node of energy & the average cluster energy are utilized to pick the next heads and CH.

a) Iolus

This approach depends on a secure tree distribution, where each group split into number of smaller groups, each of which is hierarchically organized to create a secure group. A user locates appointed GSA & sends a JOIN stable when they want to join a multicast group. The GSA determines to deny or approve the request after receiving it. When a suggestion is authorized, a secret key that is used only by the new member & GSA is generated, & the key is safely transmitted to the member of new.

The new member's relevant details are then saved by GSA in its safe, private database. Then it securely distributes a group key message update to each of the current members. It securely transmits the subgroup key to new join member across a secure medium and contains new subgroup key that has been encrypted with the old subgroup key.

b) Kronos

It is a scalable strategy. The frequency of rekeying is time-driven, so it doesn't matter how big or dynamic the group is. The key management architecture Igkmp is the foundation of Kronos. With the main exception that Kronos uses a period-based rekeying approach, the working is very similar to Igkmp.

Decentralized group key management strategies include others like hydra, safecast, and marks. The fundamental disadvantage of these systems is that the key server must create ongoing secure communications with each group member. This raises the price of adding a new key server.

3.3 Distributed group key management protocols

Techniques in different distributed key management schemes including EDKAS by using one way function trees, DGKD, DHSA and TGDH will be covered. The two main operations that need attention are member join and member leaves because all four of the protocols are membership driven. Below is detailed how all four of the aforementioned approaches member join and leave procedures work.

i) EDKAS

In terms of key structure, EDKAS and one-way function trees are quite similar. A secret key & its given blinded key are linked to every node. Utilizing a predetermined one way function, the blindfolded keys are calculated. Each participant uses a generator safe pseudo random number to create a special secret key for themselves in [102]. The idea of distributed one-way function trees serves as the foundation for this approach. This approach to group rekeying is period-based. In order to ensure authenticity, this system makes the presumption that all members have already been through some admissions screening procedures. This approach assigns one ID to each leaf node and ID as 0 to the root node. The child node of any parent node with the ID it have IDs (2v+1) & (2v+2) respectively. The members are represented by each leaf node. Each participant possesses a key with secret & a blinded key. By utilizing mixing function (KV=f (Bk2v+1, Bk2v+2)), one can determine a node secret key from child node blinded keys. The secret key of the root nodes, often referred to as the group key, is given to all the members in this fashion. Each participant has a unique secret key. Additionally, it stores all of the blinded keys for all the nodes which are siblings of those in its key route, starting with the leaf node with which it is related and ending with the tree's root node. A node that has members in the rooted of the tree at its nodes of sibling is also connected to a responsible member set, or RM. In figure 3.2, the member join procedure is described, 6 represent the insertion node, and the sponsor denotes U5 and U7 desires to join the group. The U7 sends the blinded key Bk14 to U5. U5 regenerates its blinded key Bk13,

its secret key k13, and it’s two other keys like Bk6 and Bk2. Then BK6 and BK2 are sent by U5 to U4, U1, U2, and U3 respectively. Additionally, it sends to U7 the tree structure of distributed one way function, BK13, BK5 & BK1. At this point, each member has the knowledge necessary to produce group key K0. The circumstance of a leaving member is identical to that of a member joining in that a sibling node serves as sponsor & is elevated to the place of the leaving node's parent. The sponsor then starts the re-keying activities, as was mentioned in figure 3.3.

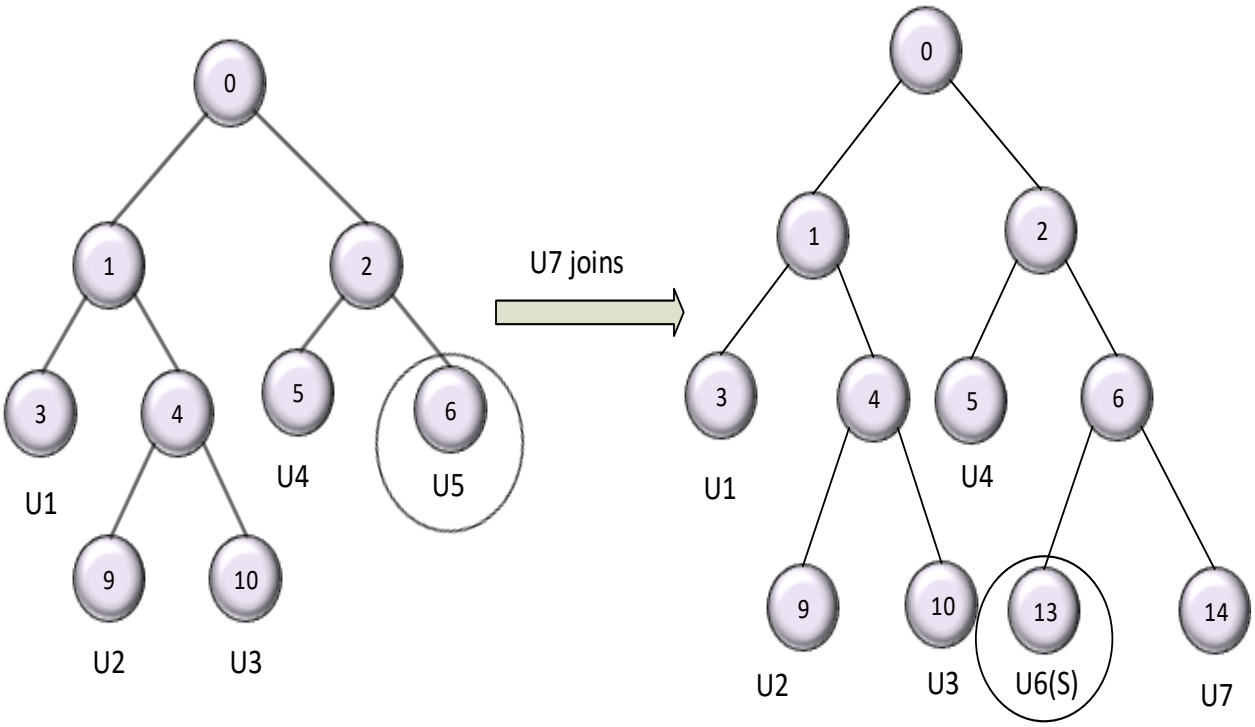


Figure 3.2Join operation of EDKAS

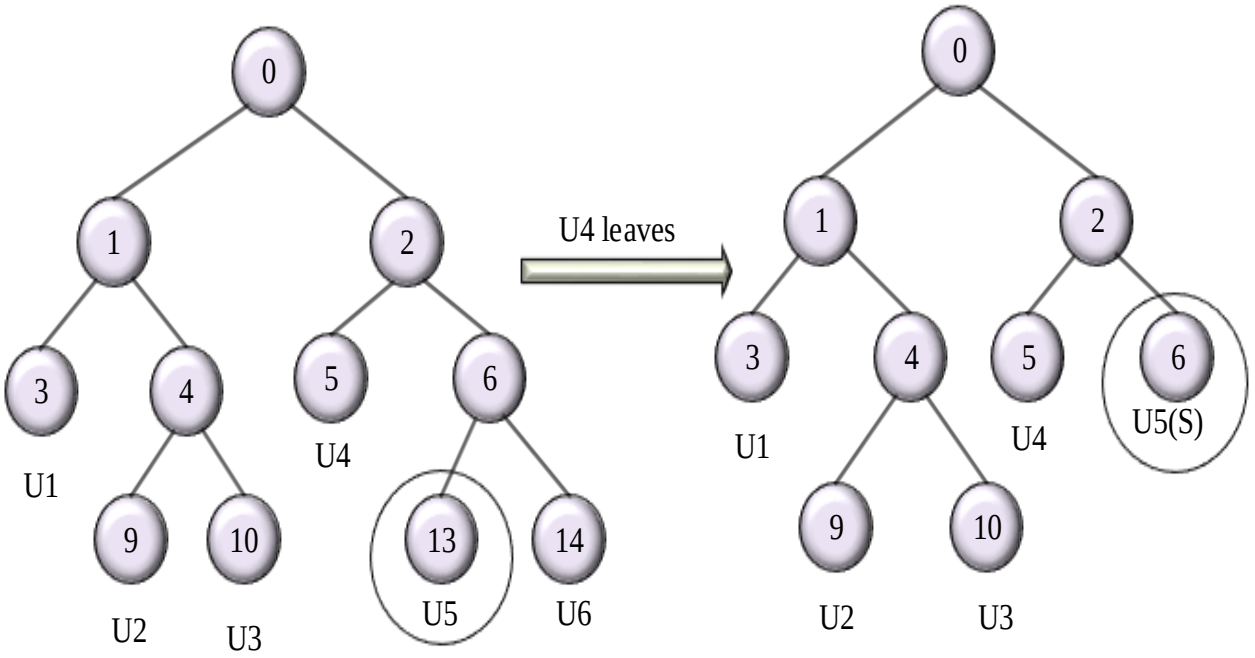


Figure 3.3 Leave operation of EDKAS

Actually, this strategy is based on periods. As a result, the join of the single node case discussed above is expanded to a join batch, & a structure of temporary level of key tree is created and set

aside for each join. The temporary tree is combined with the structure of actual tree at the start of each period. This method separates the frequency of key replacement from the group's membership and size because it is period-based. As a result, this plan can readily be expanded to include dynamic collaborative groups. Although this approach is effective in theory, it is expensive to use in practice.

ii) TGDH

The TGDH approach makes use of the multi-party Diffie-Hellman and hierarchical key tree concepts. Users are represented by the key tree's leaves. Operations of the two rounds are necessary in this strategy for new node join. A join request of the brand-new node broadcasts with its unique blinded key inside. By performing a procedure of the modular exponentiation on its secret key, the blinded key is evaluated. The insertion position is determined by each node when it receives this message. To avoid increasing the tree's height, a new sensor node should be added to the branch that is the shallowest.

At the insertion node, the sponsor will be the leaf with the rightmost root. A new node of intermediate is generated by each member, with the sponsor and new node as its children. All of the members will get banned after this stage, with the exception of sponsor node. The sponsor calculates its blinded keys and creates a secret key. It can determine the new key group because it has all of the other nodes' blinded keys. Sponsor then broadcasts every key that has been blinded. The new key group can then be calculated by the new member and all the existing members.

The protocol for leaving is comparable to joining. In the rooted sub tree at the sibling of leaving nodes, sponsor is the leaf node on right. By removing the departing node and elevating its sibling to the leaving node's parent position, all members update their tree structures. Like join, the sponsor updates the blindfolded keys and new key and broadcasts it to other members. The new group key is calculated by the members. The expense of exponentiation with modules slows down the full system because this protocol necessitates rekey initiation with the change of the each membership. The communication overhead for TGDH, DGKD, & DHSA is the same during depart, but DHSA's message size is less because just the new key group is sent to the balance members which represents in [103].

iii) DGKD

DGKD method makes use of the sponsors and co-distributors concepts and this approach depends on a hierarchical tree structure. The sponsor generates a new key group upon joining or leaving and starts the key distribution process. With the assistance of co-distributors, the new key gets distributed by the sponsors. All members of group are commonly applicable and trustworthy because this strategy is distributed. Any group member may have a prospective sponsor depends on the proximity of join or leave node member.

Every member has a field of sponsor, which, if it is on the path of joining members, will be modified. If new node's sponsor id value is higher than the old node's sponsor key, then it will changed with new node's sponsor id. This approach, the co-distributor oversees producing the keys for the damaged intermediate nodes. The co-distributor assists in key distribution to the nodes of other individuals since sponsor may not has the keys combine with other branches.

In order to join, the new node, mn+1, transmitts its own public key to other nodes, m1,...,mn. After authenticating this node, the member on the right responds to it. It broadcasts and decides the new node's insertion location. Virtual key tree and list of additional nodes' public key are then sent to the new joined nodes. Then sponsor node member is chosen. The sponsor is changed to the new node's sibling member node. If there are no sibling nodes then new member node itself takes the role of sponsor. New keys are distributed and generated by the sponsor node all the way to the root. If necessary, members must also change the sponsor ID.

As shown in Figure 3.4, New keys K'4-5, K'4-7 and K'0-7 are generated by M4 and ts the encrypted keys using co distributers public keys. The messages will then be distributed to the other members by co-distributors when the keys and intermediary node keys have been decrypted. The messages will be {K0-7} K0-3 by M3 and M7 messages will be {K4-7} K6-7 and {K'0-7} K4-7. M4 also encrypts and sends the key to M5: {K'4-5, K'4-7, and K'0-7} PK5.

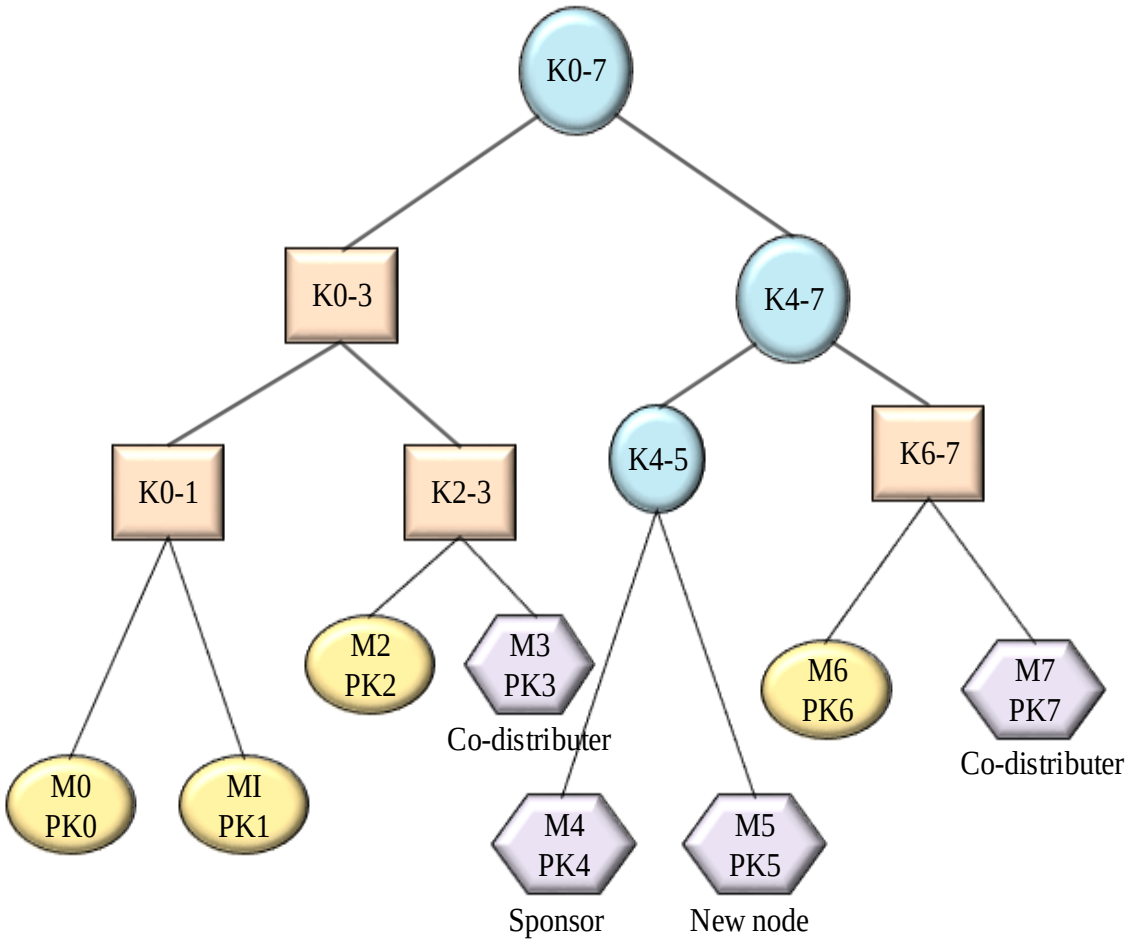


Figure 3.4Join operation of DGKD

In the operation of the member leave, M4 distributes the new keys K'4-5, K'4-7 and K'0-7; sibling like as sponsor, M4 distributes the encrypted keys utilizing the public keys of co-distributors such as {K4-7, K0-7} PK7 and {K0-7} PK3. The messages will then be distributed to the other members by co-distributors when the keys and intermediary node keys have been decrypted. The messages will be {K0-7} K0-3 by M3 and M7 messages will be {K4-7} K6-7 and {K'0-7} K4-7. As a result, in figure 3.5, all the members will receive new keys.

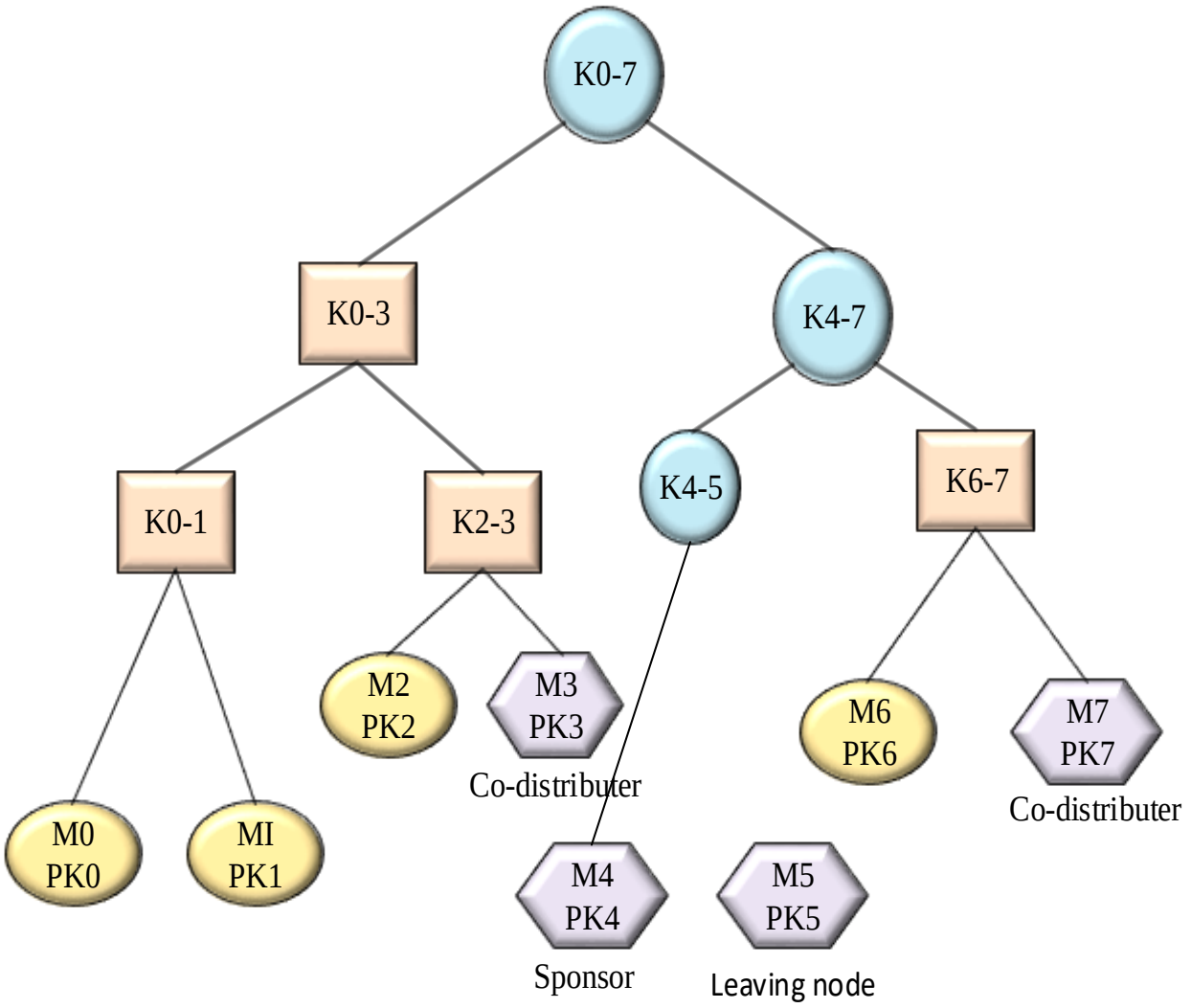


Figure 3.5 Leave operation of DGKD

This approach makes use of unique authentication techniques. Two components make up the packet that m4 sends to m3 when it transmits new keys. One is an m4 private key and k0-7 signed k0-7. So that m3 can decrypt the message and confirm its authenticity.

For each member to confirm that the message comes from the node m4, m3 preserves the signed k0-7 along with the message while sending it to other members. The fundamental problems with this approach are two. The sponsor member must generate each of the impacted intermediate keys, adding to the sponsor's workload. Additionally, this method makes use of asymmetric cryptography, which is slower than symmetric cryptography.

iv) DHSA

As the name suggests, this distributed GKM strategy combines the idea of a logical hierarchical key tree with the symmetric algorithm and Diffie-Hellman. Each member's public key is kept in a leaf of the key tree structure, and symmetric keys are kept in the intermediate nodes. This approach employs decimal code and binary code, two different sorts of codes. The calculation of intermediate node keys uses decimal code, while binary code is employed to identify a member's position. All group members share a list known as the member list that contains the public keys and binary codes of each member. If any change occurs in membership then list will be updated. The group key will be with root node. The formulas listed below are used to calculate the intermediate node key.

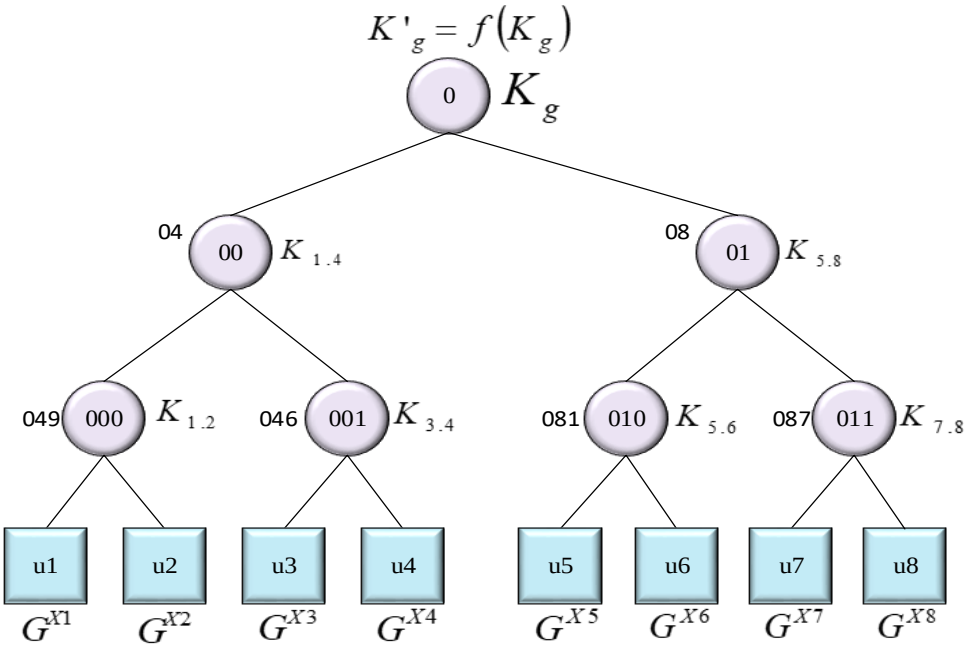
$$Key_{IN} = f\left(Key_G \ \ XOR \ Code_{IN}\right)$$

$$Code_{CN} = \left(Code_{PN} \| \ Random \ digit\right)$$

Where, IN represents intermediate node, G represents group, CN represents child node, PN represents parent node, Key_{IN} represents key of the intermediate node, Key_G represents key of group, $Code_{IN}$ represents code of the intermediate node, $Code_{CN}$ represents code of the child node, $Code_{PN}$ represents code of the parent node. Figure 3.6 displays an illustration of a hierarchical key tree structure. A join request message is sent to all groups whenever a new member wishes to join. That node will respond if it has no siblings. Node with the lowest value of parent binary code which responds to join the request if there are several nodes with no siblings. Upon receiving this join request, each member checks its value of the binary code to see whether it is the smallest; if it is, that node will be in charge of this join's key management procedures.

Consider a group with U4 joining node and 7 members in figure 3.7. All seven members receive a join request broadcast by U4. Since U3 lacks a sibling node, U3 will serve as U4's sponsor. It confirms U4 is real. Both the keys of U3 and U4 exchanges their public keys and it establishes a shared keys using the scheme of Diffie-Hellman key arrangement, i.e., $G^{x3x4} \bmod p$, here $x3$ denotes private key for U3 and $x4$ denotes private key for U4. U3 shifts its position to makes area for U4. Additionally, U3 determines the key and codes of intermediate node for new nodes. The

member list table is updated with the modified binary code for U3 and the position with new and public key for U4. Currently, every other node calculates a new group key using the hash value of the already available group key. Then U3 sends the newly created group key to U4 after encrypting it with the Diffie-Hellman shared key. The affected path members will then use the updated group key and decimal code to determine the intermediate node keys.



$$K_{1,4} = f(K_g \oplus 04) \qquad K_{5,8} = f(K_g \oplus 08)$$
$$K_{1,2} = f(K_g \oplus 049) \qquad K_{5,6} = f(K_g \oplus 081)$$
$$K_{3,4} = f(K_g \oplus 046) \qquad K_{7,8} = f(K_g \oplus 087)$$

Figure 3.6 Hierarchical key tree structure of DHSA

A member's sibling node will act as its sponsor when they want to leave a message. The shared member list of table will be updated with the new parent code of binary when all entries related to the departing member have been removed and the sibling member has moved up in the key tree. All other members now stop their transmission for a short period of time and listen to the sponsor of sibling node for the new key group. Now, the node of sponsor uses the algorithm of symmetric, one time pad, to calculate the new group key. The key group is transformed in a certain order to

minimize key packet transmission in figure 3.8. All group is categorized into (log n -1) groups ({u1, u2, u3, u4}, {u5, u6}) and from each group one member is selected randomly. The sponsor member then used their shared keys to encrypt the group key before uncasting it to those nodes. The new group key will then be broadcast to the other members by the representative members (U1 and U5) using their shared intermediate node's key (in this case, nodes U1-4 and U5-6).

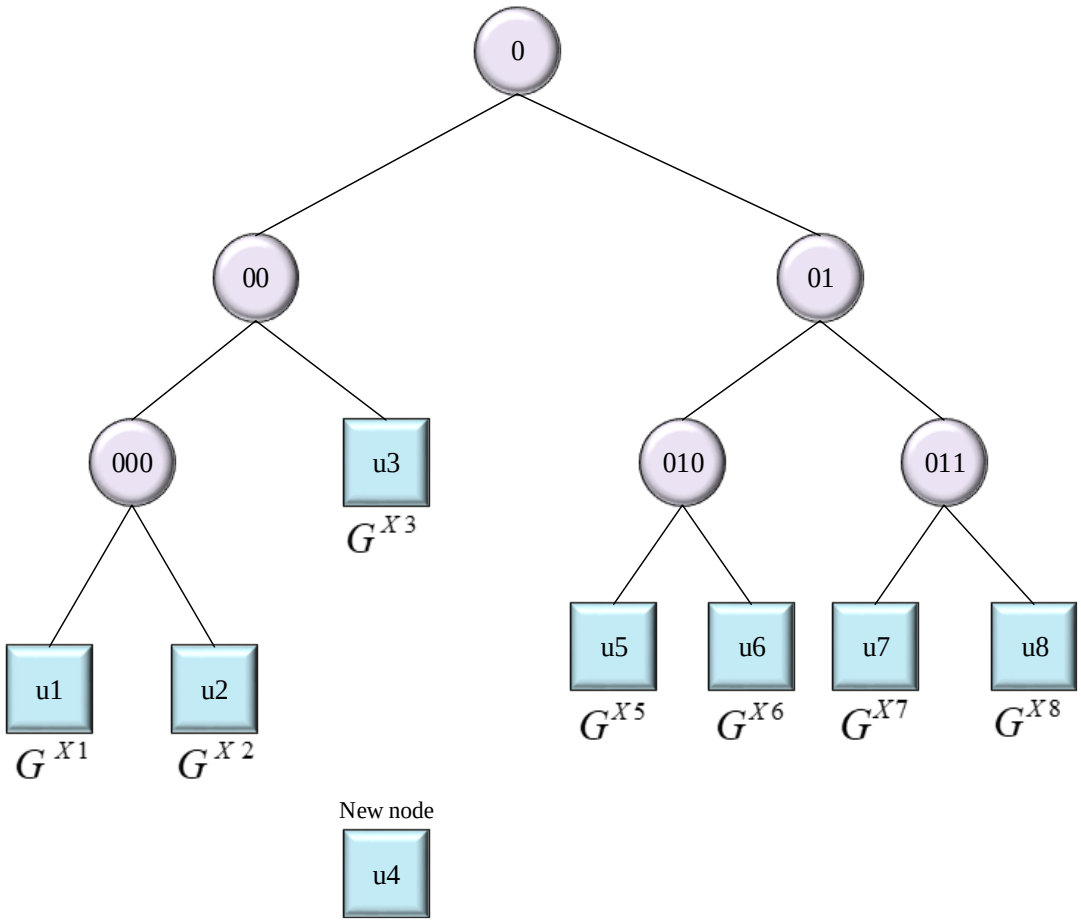


Figure 3.7 DHSA join

This method's benefit is in the join operation rekeying. The group key is only ever sent between the new node and the sponsor in a join operation message.

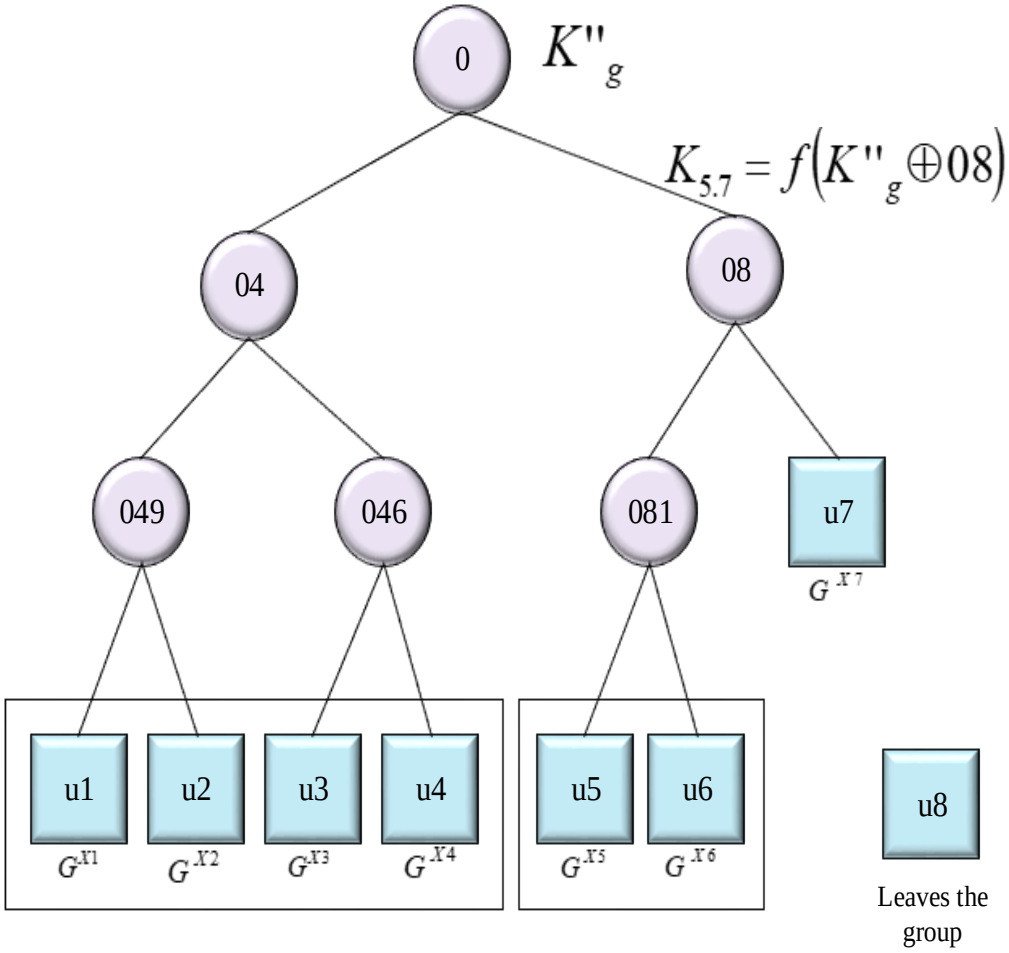


Figure 3.8 DHSA member leave

In ECDHSA, as in DHSA, only the key group is created by the member of sibling of the new member, & the various needed keys are calculated by the members. It minimizes the key number creation at join & leave operations to 1 for every change in membership. This feature makes managing group keys for a group with dynamic leave & join more effective. The method has a overhead of lower key generation than EDKAS at join.

3.3 Comparative Analysis

Four of the different distributed key management strategies are discussed here. Also, their major generating overhead and overhead key communications performance analysis is discussed. The amount of keys that the sponsor member generates is known as key generation overhead. Overhead of the key communication is the total messages needed to transmit the group key.

Table 3.1Key generation overhead formula

Protocols	**Join**	**Leave**
EDKAS	$2\log_2 n$	$2\log_2 n - 2$
TGDH	$2\log_2 n - 2$	$\frac{1}{4^n}$
DGKD	$\log_2 n + 1$	$\log_2 n$
DHSA	l	l

Table 3.1 displays the overhead of key generation for join & operations of leave. With DHSA, only the key group is created by the member sibling of a new member, & the other required keys are calculated by the members, reducing the key generation number operations at join & leave to 1. With this capability, GKM is more effective for a group that has dynamic join & leave rates. Although TGDH operation is slower because it requires modular exponentiation to construct a new intermediate key node, the overhead of key creation in EDKAS, DGKD & TGDH at join is practically identical.

For DGKD and EDKAS, the overhead of the key generation is essentially the same. For DHSA, the generation of key overhead is minimal & constant. Because only one key group is created by the sponsor node for DHSA. The key group is calculated by all other nodes using the hash value of the existing. The calculation of the overhead of key generation for joins & leave operation was explained in table 3.2.

Table 3.2 Evaluation of the overhead of key generation for join & leave operations

Count of node	Number of generated keys					
	Member join			Member leave		
	DGKD	DHSA	EDKAS	DGKD	DHSA	EDKAS
6	3	1	4	2	1	2
7	3	1	4	2	1	2
10	4	1	6	3	1	4
11	4	1	6	3	1	4
12	4	1	6	3	1	4
23	5	1	8	4	1	6
24	5	1	8	4	1	6
25	5	1	8	4	1	6
27	5	1	8	4	1	6
28	5	1	8	4	1	6
30	5	1	8	4	1	6

The overhead of communication associated with joining and leaving are shown in Table 3.3. This communication for DHSA during the join operation is 1, as the sibling member of the new one it only interacts with that member during the join operation to deliver the group key, & the members with other it compute the new key group by applying a one-way hash functions to the previous key group. The sponsor node must contact with every node in order to supply the required keys, making EDKAS' join/leave communication overhead higher than that of the others. The communication overhead for TGDH, DGKD, and DHSA is the same during leave, but DHSA just needs to provide the new group key to the balance members, hence its message size is less.

Table 3.3 Key communication overhead formula

Protocols	**Join**	**Leave**
EDKAS	$n-1$	$n-2$
TGDH	$\log_2 n$	$2\log_2 n-2$
DGKD	$2\log_2 n-1$	$2\log_2 n-2$
DHSA	l	$2\log_2 n-2$

DHSA has a communication overhead of 1 for join operation. Because the sponsor transmits group key only to new member. The existing members and sponsor do not exchange group keys. The EDKAS has the highest communication overhead because the sponsor provides the keys to each participant separately. The communication overhead during member leave is the same for DHSA and DGKD. DHSA, however, has the smallest message size because it only includes the group key. Table 3.4 represent the evaluation of the overhead key communication for join & leave the operations.

Table 3.4 Evaluation of the key communication overhead for join and leave operations

Count of node	**Number of messages send**					
	Member join			**Member leave**		
	DGKD	**DHSA**	**EDKAS**	**DGKD**	**DHSA**	**EDKAS**
6	3	1	5	2	2	4
7	3	1	6	2	2	5
8	5	1	7	4	2	6
9	5	1	8	4	4	7
10	5	1	9	4	4	8
24	7	1	23	6	6	22

25	7	1	24	6	6	23
27	7	1	26	6	6	25
28	7	1	27	6	6	26

3.4 Conclusion

Management of key for WSN is a basic problem that has been given by numerous suggested solutions that are displayed in various studies. WSN is utilized in a various settings, have a various applications, and come in different sizes. Secure communication is necessary for many WSN applications. To achieve the security goals in WSN, key management is crucial during the joining & leaving node operations. The range of applications in the modern period relies on sensor-based technologies such as IOT, etc., which by their very nature use WSN and discovered security issues. The document details all these security risks. In this study, many methods are investigated. The procedures depends on 4 factors: computation cost, communication, complexity, & storage cost of rekeying. It focuses on creating new keys for forwarding and preventing secrecy before moving on to the appropriate leave and join procedures. To collect a large key number at a reasonable cost requires a significant quantity of storage space, which is a difficult task. A goal of future research work is to develop a method of changing the topology of tree WSN to reduce overheads by using a top-down method because the methods used a bottom-up method & implied a significant overhead key for complex computing.

Here the discussion is about many categories of GKM approaches. It focused more on EDKAS, TGDH, DGKD, and DHSA, four different distributed key management strategies. According to the performance analysis of the four approaches, DHSA has the lowest generation of key, key encryption & overheads of communication for the case of new member joins. This indicates that DHSA is scalable than other methods.

CHAPTER-4

DyClust – A Hybrid Key Management Scheme for Wireless Sensor Networks

4.1. Overview:

WSN is the self-organized active topology with the group of active sensor nodes. The radio networking method used in wireless sensor networks for its organization, hence it doesn't have any cables [104]. The security of knowledge and information is slightly severe and vital difficulties in several areas, nodes and networks are very significant considerations for connecting between continual communication and nodes. The applications of WSN are detection of fire, controlling wildlife, monitoring, and recording patient details, traffic observation, detecting floods, smart environments etc. [105].

The WSN is used broadly in variety of application including armed forces, personal tracking, and mission critical. Sensor nodes computation is typically limited in terms of, power resources, communication, and memory. In an unattended area, the sensor nodes are placed; the risk of physical attacks is greater, and sensor network security is a challenging one because of its disadvantages of resource constrained devices [106]. The key management (KM) method is a good solution for resource constrained devices. For communication security in WSN, the key exchange is safely before information exchange. Several KM methods are used in the WSN.

WSNs are a controlled type of network, comprised of sensor nodes with small capabilities and a large gateway node including high capability. Sensor nodes are the hardest constraint consisting of limited energy and memory. So, light-weight as well as efficient energy security methods are required in networks [107]. The WSN, is used to a set of sensor nodes, transmit serious data, such as military, airport, etc. for this reason, requirement of security is the extra feature of WSN, that consist of some main terms like authenticity, confidentiality, quality of service, and integrity.

Confidentiality:

An illegal user on the network is not permitted to access the messages on the network.

Authentication:

The secret message authentication code is shared among the network nodes order to achieve safe network communication and provide high-quality data communication from origin to end.

Integrity:

The illegal user on the network is not allowed to transform the messages being transferred on the network.

Quality of service:

In WSN, security deals with correct data packet and timing to avoid the loss of data. WSN are commonly restricted in low processing set of devices commutation, low bandwidth memory and battery power. Because of these limitations, several security technologies are used in other networks, and it should not be misused in this environment. For the hybrid approach to manage both the transparent cluster's interconnectivity and the KM method's regime group, should not be treated for node key control group tampering issues. Simulations that validate the viability of this approach show that performance of cluster connectivity shouldn't be hampered by network node improvements [108].

The small sensor nodes have only restricted amount of energy and memory, and routing protocols, which is possible decrease the routing difficulty are desirable. This method is achieved by various conventional flat topologies and provide the routing tasks to few nodes and rotate this periodically. The base station has some power to send straightly to the sensor nodes, transferring to straight way for the down link. The sensor nodes have limited power supply and that tends to asymmetric communication [109]. This energy constraint takes hierarchical clustering is the best model for WSN. WSN is the combination of a greater number of nodes which are commonly arranged in several region geographical to obtain data of interest that be obtained from source of nodes to base station via multi-hop transmission.

The dense deployment sensor nodes that are sensing ranges of sensor nodes are highly overlapped. Transporting all data to base station that tends high energy consumption, that cause the reduction of lifetime of the sensor nodes. The data aggregation is improved by data collection of energy efficiency when the data is sensed are aggregated by other nodes. The data aggregation used in many applications because it has more advantages such as energy efficiency. For security reasons, the highly trivial issues, especially WSN are commonly arranged in the unattended even in critical environment.

Security reasons, it is required to distribute the secret keys among sensor nodes correctly. Constructing secure communication between nodes through secret keys has been main issue in recent years. This problem is called as KM problem. This KM method is used in more WSNs. The sensor nodes use only a limited number of resources [110].

To confirm the correct functionality improvement of WSN to permit the proper service, like a network must obey basic safety requirements like integrity, verification, confidentiality, availability, and it mainly depends on the usage. The extremely controlled capability, battery power, communication bandwidth, and memory of network. Node must be arranged closely to physical source of events, and its simple to access that are not commonly temper- resistant because of cost restrictions. Next, external, or internal devices can access the data interchange due to the public communication channel. WSN should face several threats, which delay its functionality and reverse the advantages of using its service [111]. The features of WSN make it the recognized method among other types of networks. Communication security against attackers increases the data amount, which wants to send the extra operations wants to be calculated by each communication.

The resource constrained sensors that are in the reserved fields are danger to node capture attacks. The opponent describes nodes and steals the personal keying data from them in such attacks. As a result, safe contact with the adversary in reality is extremely difficult in WSN defense [112]. The key management method is very significant attaining security and privacy objectives as the sensors and the cluster heads are necessary to use the security algorithms. The KM procedures are split into three groups based on the encryption methods, such as hybrid key management modals, asymmetric and symmetric [113].

The KM is a serious feature for certifying security in wireless sensor network device usage and management. The main goal is to allocate keys between nodes securely and safely. In the same way, the KM scheme should stimulate node improvement and disallowance in the structure [114].

4.2. KM schemes:

The KM method is used in WSN, must support certain features. The strength of the KM method for WSN is based on how many features are present in that method. Consider that the security level means that KM must provide confidentiality, integrity, flexibility, and scalability. Aside from security, maintaining the integrity of secret key is critical. If the number of nodes varies in WSN and in several cases it increases significantly, the KM method must be accessible to provide for this situation [115]. Lastly, WSNs are dynamic in nature. Nodes that have with time no energy die down, and a new node can be included at any time. The KM method for WSN must be flexible enough to provide for such a situation.

The KM method is the necessary part for security reasons. It includes distributing and computing secrets which can serve improves integrity and confidentiality of communication among the sensor nodes. KM is not simple to reach WSN because;

- Sensor nodes dispersed only unattended in environments and must perform in hostile conditions for several applications.

For dense deployment determinations and cheapness, the sensor is not tampering resistant devices.

4.3. Requirements of WSN in KM:

The KM method should provide security and work efficiency due to the power limitation, communication, and computation in WSN. The KM method must have various requirements depending on the function and security of WSN as exposed in table 4.1.

Table 4.1Shows requirements of WSN in KM

Requirements	Details
Security	Robustness, freshness, data integrity, confidentiality, and authentication.
Efficiency	Power consumption, computation, storage, and reasonable communication.
operation	Accessibility, scalability, and flexibility.

4.4. Objectives of KM:

In WSN, the KM system reaches the objects as follows:

- Low memory: limited storage capacity of WSN, the key stored into the nodes achieve low message as available.
- Energy consumption is low: based on data communication, energy consumed. In order to achieve low energy consumption, communication is being reduced.
- Enhanced anti attack capability: WSN nodes are visible, that can tend to node capturing. The KM method must make sure that information sent among the nodes are should not take by adversary. Node is captured, it is key message about remaining nodes must not be leaked.
- Storage network connectivity: the connection between the two neighboring nodes. The messages should be sent securely between the neighboring nodes.
- Scalability: the KM method must confirm that the participated network saves the high degree of connectivity after removal or addition of nodes.

When each different key has node, it is more challenging manage whole keys since they consist large number of nodes [116]. When a node has low number keys that will generate issue in network connection, and that will provide a high number of keys to each node that will reduce the resiliency of the network. In public key cryptography commonly have some limitations. The following are the basic requirements of key:

i. Public key be inefficient (power consumption is higher)
ii. One limitation of symmetric key method is compromising one node tends to compromise whole network.

iii. The pre distribution method that organizes the nodes in the target area. This method, each pair has a shared key, but that is not used in large networks.

iv. Several different probabilistic of numbers of methods cover some probability of connectivity. This method, a group of keys is organized from a large pool of keys each node, and probability of two nodes is shared; the general key used as secret key between nodes. Finding a compromise between the amounts of keys allotted to each node and the overall number of keys in the pool key can be challenging for big networks.

v. One main difficulty in KM is the sensor new node that connects network, which challenging in key pre distribution event. Connect the network, after the key creation phase, and repeat the process.

4.5. Classification of KM method:

In WSN, KM method divided into several categories, as shown in the following figure 4.1. Commonly, WSN is divided into two categories: distributed and hierarchical structures. Hierarchical WSN, data flow is categorized into 3 parts; group-wise in the cluster of sensor nodes; network-wise from base station to sensor nodes; pair-wise between pairs of sensor nodes to the base station and sensor nodes [117]. The distributed WSN data flow is the same as the hierarchical WSN data flow, difference with that network-wise information transfer by each sensor node is prohibited.

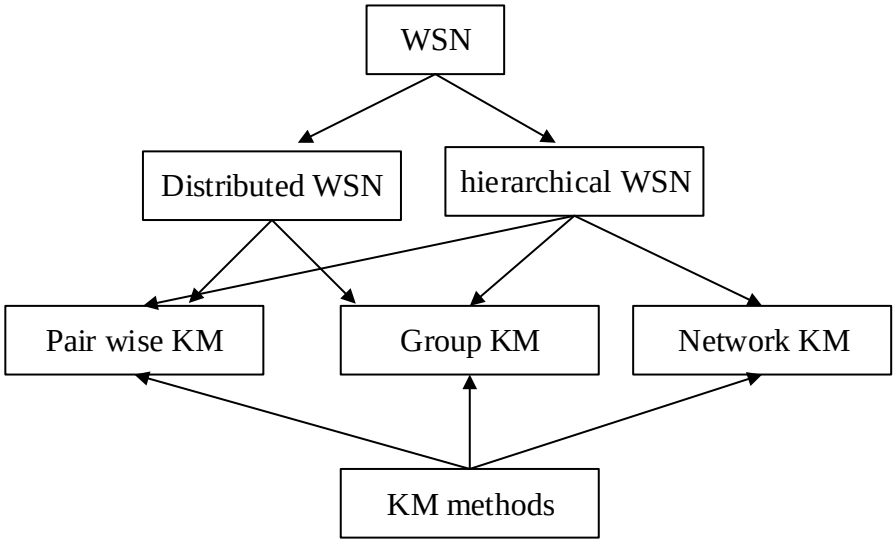


Figure 4.1 Classification of KM methods

The key distribution is the main issue for security as it applied in WSN. KM is defined as techniques and procedures for preserving, distributing, and forming the private key among the communication events. KM consists of updating or refreshing keys of compromised nodes. The KM method must fulfil the three metrics groups as follows:

- Efficiency
- Security
- Flexibility

Other than security level, the KM method planned for WSN must provide for restrictions related to sensor nodes. Computation capabilities, memory and limited bandwidth, sensor nodes should not have knowledge based on positioning. Limited range of transmission and low battery life is the main reason for KM method.

4.5.1. Group key management (GKM) for WSN:

The GK is used for safe group communication that in WSN states to the situation which sensor in group is receive and send information from group members, likewise outcasts are not able to collect the message, that are able to divert the information. GKM is very difficult while considering the dynamic problem in WSN. Various GKM schemes for WSN is used. The logical key tree-based method that will decrease the cost of rekeying radically by constructing the tree of

encryption keys, is best method. The nodes allocated the equal key encryption keys because the cost of rekeying is reduced.

4.5.1.1. Secure group of communication scheme:

The communication group system includes four general steps that are followed:

- Initiative
- Leave
- Partition
- merge

The group is created initial members. Next, various members join the group when the original members leave it. This process is known as dynamic membership. Large number of membership changes, desire the specific protocol without design degrading the performance group. In some cases, the group is partitioned into several subgroups or joined the big group. This is known as the membership bulk change since the transitions between the groups are experienced overhead. The dynamic membership aspect wants the group communication system to rekey session keys to maintain secrecy key. In WSN, dynamic membership should not require since keys are predetermined previously to the creation.

Sensor nodes in group communication methods cooperate for equal tasks and are typically arranged in the same group. Various groups already exist in the various WSNs. Connectivity among the sensor nodes, which are members of the group is common, when the connections among the members of different groups are rare compared to each other. The connections between various groups include the nodes at the high hierarchy levels. The various applications, in the combination of several groups, overlapped based on arbitrary topology. The nodes are grouped based on the requirements, and applications can take advantage of the node.

The main security service n secure group communication is the facility of shared key of GK. Shared GK is used for encode the group information, sign the information, and verify the information and members and access to group and traffic resources. Therefore, secure group communication strength is mainly dependent on cryptographic strength of keys and KM method.

GKM organized in the secure group communication method must satisfy the requirements as follows:

- key creation is secure
- the GK must be computationally or infeasible is challenging one
- the GK is securely spread and collect the GK
- cancellation of GK in each membership change must immediate
- Each membership should result in rekeying of connected keys.
- Rekeying of key must be secured one.

Various sensor nodes in WSN data are collected from surrounding and sent it to centralized node sink. The reporting or sensing action of sensor nodes are controlled by the control signal broadcasted from the centralized sink node.

For security, the encryption KM method for dynamic WSN is based on symmetric key encryption. This encryption method is suitable when sensor nodes contain limited energy and limited ability. So, large communication overhead and wants to high memory space to stock the collected pairwise keys. This isn't resilient and not scalable against compromising and not able to support mobility node. So that is not suitable for symmetric key encryption dynamic WSN.

The asymmetric KM method shows intense mathematical calculations and gain sensor nodes from more energy. Meanwhile, transmit sensor nodes up to a small distance. Various sensor network data collection methods are employed in the network processing.

The good KM method is defined by its capability to effectively survive attacks on resource challenged sensor networks. In the KM method, a sensor node can be divided into two groups.

- Static KM method
- Dynamic KM method.

4.5.2. Static KM method:

The static KM method assumes that the administrative keys are pre-arranged in the nodes that should not change. The administrative keys are created according to the arrangements and are assigned to the nodes either commonly or depending on the arrangement information and node

distribution. In the communication process, the static KM method uses overlapping administrative keys to find adjacent eligibility node to create the direct pairwise key. The communication keys are used to join other nodes. To create and distribute the communication key among the non-adjacent nodes and set of nodes, the key is broadcast one joint at a time using prior recognized direct communication keys.

4.5.3. Dynamic KM method:

The dynamic KM method changes periodically in administrative key based on the discovery of the capturing of nodes. The main benefit of the dynamic KM method is improved network survivability because several captured keys are exchanged periodically. This process is called rekeying. Give good support for expansion of network; based on addition of new nodes, chance of network capture improvement is arrested. The disadvantage of the dynamic KM method has to construct the secure rekeying mechanism.

Depend on the encryption methods the KM method is divided into three categories:

- Symmetric KM
- Asymmetric KM
- Hybrid KM method.

KM is a necessary component network of security. Symmetric key want keys for protection. The WSN has computational and energy constraints, so it wants to preserve balance to those constraints' security level with respect.

4.5.3.1. Symmetric KM:

In this KM method, both the receiver and share sender the common key for encryption and decryption. This symmetric KM method is rapid and reliable one, connectivity and scalability. The important receiver and sender must exchange the key securely.

4.5.3.2. Asymmetric KM:

In this KM method are used two different types of keys. The key that encryption is used for public key.

4.5.3.3. Hybrid KM method:

This method is a combination of symmetric and public key cryptography methods. Several traditional cryptography methods should not be used because of their high energy consumption and more memory usage. This issue can be solved by combining the asymmetric key pre distribution with symmetric key creation by using WSN.

Safely allocating keys for sub networks generated actions in sensor network is a non-trivial issue because subnetworks may cover several arbitrary sets of neighboring nodes. These nodes should be able to safely communicate with one another to assign subnetwork key to all subnetwork members. Following are the limitations of KM procedures:

Improve security:

Decrease the mathematical equations that consume low computational power, which causes cooperating on network security.

Improve mobility:

Mobility is improved by decreasing the calculation procedures, and nodes get more mobility. Mobility is closely monitored for security reasons.

Decrease key handling time:

If mobility is increased, means the key handling time increases, the quality of the whole network and verification is sensibly handled.

Decrease the power:

In many applications, the network nodes are battery operated. Power consumption dynamically increases stability of the whole network.

The KM method generally used sensor nodes for safe communication in its range. The KM method is categorized into 3 phases:

- pre key distribution
- discovery shared key

- establishment key

4.5.3.1. Key pre distribution:

In key pre distribution method, keys allocated to every node before placement sensor nodes. In WSN**,** it's not necessary that keys be recognized between each pair sensor nodes. In WSN process, every sensor node develops enough bandwidth and adjacent nodes when information is sent to base station via different ways. In pre distribution random key method, GK is shared among the nodes and the base station. To cancel the compromised sensor node, utilizing GK to sign the list also broadcasts it into the network by other nodes. After getting the list, whole nodes delete keys that be identified with compromised mode from memory. One disadvantage of this method is that node cancellation leads to more links that use one of deleted keys to break.

Each pair of nodes want to communicate with every node and it should share at least a common key. Key pre distribution method includes two phases:

- establishment direct key
- establishment indirect key

4.5.3.1.1 Direct key establishment:

After placement sensor nodes, requires pairwise key, in case of 2 sensor nodes wants to communicate. First identify vicariate polynomials. After finding this, the common pairwise key is created directly by polynomial based key creation.

4.5.3.2.2. Indirect key establishment:

If direct creation key fails, two sensor nodes determine intermediate adjacent node using shared pair wise key with an indirect key. Intermediate sensor node was broadcast this information continuously till finds the sensor node that share the pairwise key with two sensor nodes.

Before node arrangement, keys pre-distributed into the sensor nodes. After nodes are placed, every node wants to find the shared key in its communication range. In the 2nd phase, nearby sensor nodes form shared key safe communication.

4.5.4Shared key discovery:

Whole nodes are organized; key shared discovery stage created. Stage in every sensor node challenges to find out with its adjacent it shares the common key. Whole keys commonly selected from same key pool, since the 2 nodes contain the overlapped keys in their memory. If key already exists, next it can used for communication security among 2 nodes.

4.5.5 Key establishment:

In the shared key stage, 2 sensor nodes not share common key, every node should discover the intermediary adjacent node to shares the pairwise key among the path keys. Then sensor node intermediate will broadcast, this information continuously till find the sensor node, which share pairwise key with two sensor nodes respectively. Path can recognize between two nodes. Key establishment reduces network resilience against node it captures attack.

There are two KM methods for both subnetwork and group-wide KM. In the first method, manage both individual and group-wide keys. For non-critical messages broadcast among the nodes, the group wide key is used. The individual key is used for communicating security between nodes generating setting sub network key. The next KM method is generating and allocating the keys for dynamically generated subnetworks.

4.5.6 Individual and group-wide keys:

4.5.6.1 The individual key:

This key is the single key which shares every sensor node and base station. Base station is used as the individual key to send the information to every node in the network.

4.5.6.2 GK:

The base station shared GK with all the sensor nodes in network to send information to them. The GK uses rekeying mechanism an efficient for updating the keys where the opponent captures, and node is compromised.

This procedure starts with the distribution of the network. Before distribution, 3 values should be stored in every node. The first value in the group wide key, which is used for communication group wide among the nodes, shouldn't be involved sub network. The 2nd value is used to interchange keys pairwise among adjoining nodes that are removed past some time. The

third value is ideal for every node is covered on both the node and base station. This key is used to send encrypted messages between the base station and the node.

4.5.7 Subnetwork KM:

The subnetwork section of KM starts with the generation of subnetworks in WSN. Initially, CH determines the energy average remaining for full nodes in cluster. The network is the predetermined partial keys number, which is enough generate the sub network key was estimated previously.

4.5.8 Dynamic cluster KM algorithm:

The network calculates the cluster, which will generate partial keys and passing that to head CH, the different dynamic group KM method used create sub network keys. This method leaves start method by partial key casually creating. This key is parent of leaf node passed.

4.6. Issues in KM methods:

The WSN is the type of network that has several disadvantages compared to ordinary networks. Because of these constraints is challenging to straightly employ security methods to area WSN. So that to improve the application in security mechanisms when the ideas are borrowed from the recent security methods. Typical KM issues are discussed as follows,

- Complexity
- Heterogeneity
- A poor KM system can do damage.
- The privacy of the information that they safeguard depends on the security of the encryption keys.
- Availability
- Governance

4.7. Problem Preparation:

In this work, the main aim is computational overhead aided with security and efficiency in the KM process. DCGKMS depends on the top-down method for dynamic clusters when sensors

are in motion as per their necessities. Calculate all keys in wireless sensor networks, using bottom-up method. The DCGKMS gives the following three security levels:

- Cluster head level
- Sub-clusters level
- Node level.

4.7.1 Cluster head level:

Several applications sensors want to identify events and subsequently transmit data to reserved base station for purpose of estimating parameters that define these events. The transmitting cost is high compared to the calculation and it is helpful to arrange sensors into clusters. Clustered situation, data is collected sensors and communicated to base station through CH. The base station finds last calculation parameters by using data communicated by CH. The sensors are communicating information through a small distance in clustered situation. The energy consumed in network is lower compared to energy consumed when each communicates sensor directly to base station.

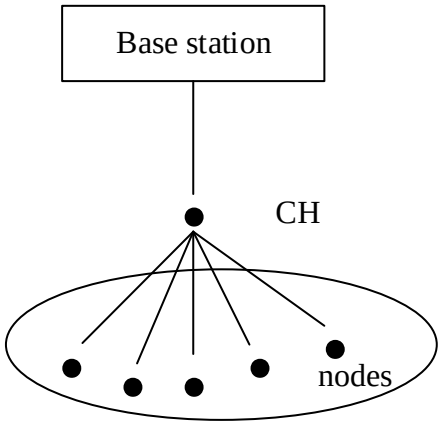


Figure 4.2WSN structure

The ideal WSN network is shown in the above figure 4.2. Here the nodes send information to the corresponding CH that compresses information and transmits it to the base station. The following assumptions are made in WSN structure:

- The base station positioned a distance from sensor nodes, and it fixed.
- Whole nodes in the network are energy-reserved and homogeneous.

- Nodes have position data that is sent to the base station with energy steps through the set up phase respectively.
- Symmetrical propagation channel.
- Base station included in CH selection.
- Nodes have low flexibility.

The nearby sensor nodes commonly have information about events, so they gather events in the exact area. When every node separately conveys the collected information to every sink node, more energy is wasted to convey the same information to every sink node. Then sensor nodes arranged into proper number clusters in proper order to reduce the wastage of energy. Cluster-based methods are used decrease wastage of energy and increase the resource allocation, which increase the lifetime of network. Every cluster is controlled and observed by node that is known as the CH. This CH directly communicates with the base station. The information is identified from environment sent to this CH by the remaining nodes. After cluster formation, optimal CH selection is an important issue in the application of sensor networks, and severely disturbs network communication energy dissipation.

4.7.1.1. Cluster formation:

In WSN, after the arrangement of nodes in a physical environment, information is first sent to base station, next network stars to choose CH. Based on the selection of CH, every node choose if it can serve as the CH based on the following selection roles:

- Communication capabilities are extensive.
- High processing capacity
- High energy resources.

After formation of cluster, the new nodes join network shown in the figure 4.3. Whole nodes communicate through the bidirectional wireless network. If the first node sends message to third node through second node, then the first node can receive if the second node forwards that message to the third node at the end node. In the key distribution, every node has three keys:

- Cluster key
- Master key

- Pairwise key.

Cluster key:

This key is shared between adjacent nodes and nodes. By using cluster key, the node selects that information transfers so that will decrease the communication loads of the system. A cluster key shared with every cluster. Every cluster has a different cluster key.

Master key:

A shared master key is each node and enables by the base station broadcast.

Pairwise key:

This pairwise key is a single key that shared between adjacent nodes and every sensor node in the network. Each node uses this pairwise key for transferring and sending the information to the CH. The pairwise key permits node-to-node communication.

The key pair wise is shared by 2 nodes. base station has pairwise key with full CH, and base station shares key with secondary node in every cluster. The CH has the pairwise keys with whole nodes in cluster, and secondary node has the pairwise key that is shared with whole normal nodes in the cluster. Key generation, the pair wise for secrecy and can be removed later. The pairwise key secures the information that can used for certification. Figure 4.3 denotes the clusters in WSN.

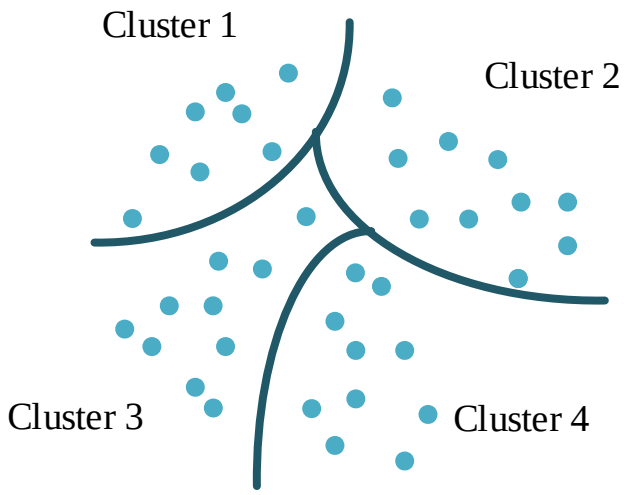


Figure 4.3 Clusters in WSN

CH:

Neighbors of sink node have to forward a large amount information compare to the remaining nodes. While increasing the network size decreases lifetime. Split the big network into a number of clusters, that includes number of sensor nodes and CH improves network lifetime. In this system, CH is sensor nodes that have significantly more resources, such as large memory, long range antenna, and powerful batteries. CH is used to merge and collect the messages from the neighboring sensor nodes in cluster, combine the received messages, and forward result to sink.

Sensor nodes:

Sensor nodes are essential components of a WSN, they are naturally small electronic devices that have limited capability and are inexpensive. Every node has controlled storage capacity, data processing capability, power, and transmission range. They are in charge of gathering data from the transferring and surrounding environment it to CH, whether via multiple or single path.

The first node transmitting sensed data to CH, as shown in the following figure 4.4. When the first node transmits, the remaining nodes in cluster are listening. Each node has received the transmission of remaining nodes in their broadcast collection that they describe as their neighborhood. The area of the first and second nodes is shown by large circles around nearby

nodes. The third node is next to the first and second nodes. So that the third node will observe the whole transmissions of the first and second nodes. Transmit information from first node to CH through second node. The third node is able to create parameters for second node through calculations. Measure the second node's reliability in forwarding message from first node to end, the CH. If the first node is performed in immoral mode, it will be able to create its own parameters with respect to second node depending on the observation. In the same way, every node can monitor the performance of remaining nodes in its area. It tends to maintain local separate trust tables of every node. Figure 4.4 denotes the communication occurs from node to CH.

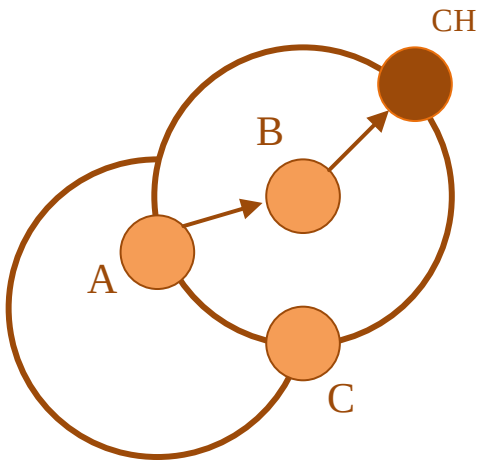


Figure 4.4 Communications from node to CH

In this method, where the novel node leaves or joins the cluster, single node key is estimated by using sub cluster keys and neighbor keys to decrease the computation difficulty and cost. GK is generated in the first step, and depending on GK, sub group key (SGK) is formed and, depending on dub group key (DGK), single node key of the leaf node is formed. After cluster formation, the top-down method is used. So this method is used for dynamic wireless network systems.

The DCGKMS method for GKM with various groups. The communal is formed by sensing nodes, and y groups want to be recognized. The nodes are labelled by using the numbers N1, N2, N3…., N_x and groups are labelled by the numbers M1, M2, M3…., M_y.

Where j=1, 2…y, a logical tree is constructed in every group M_j. The tree height in group M_j is determined by number of sensing nodes in the group, and log2t is the tree covers t nodes.

The following figure 4.5 shows that the GK is positioned on the tree root, and it is used to connect with additional members in the group securely.

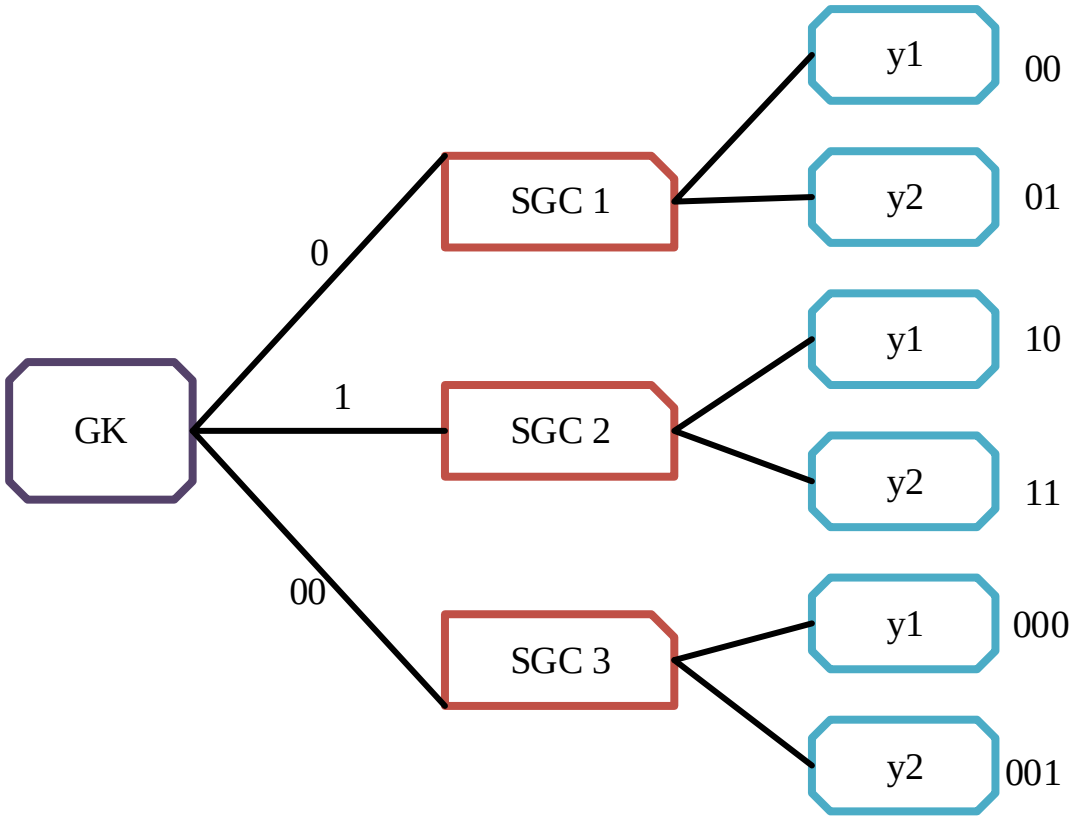


Figure 4.5 Generation of UNK

The tree is maintained by the root node. In every group, that generates various key trees as illustrated in figure 4.6. For every sub group collector (SGC) and sensing node, a session key is to be shared for communication security.

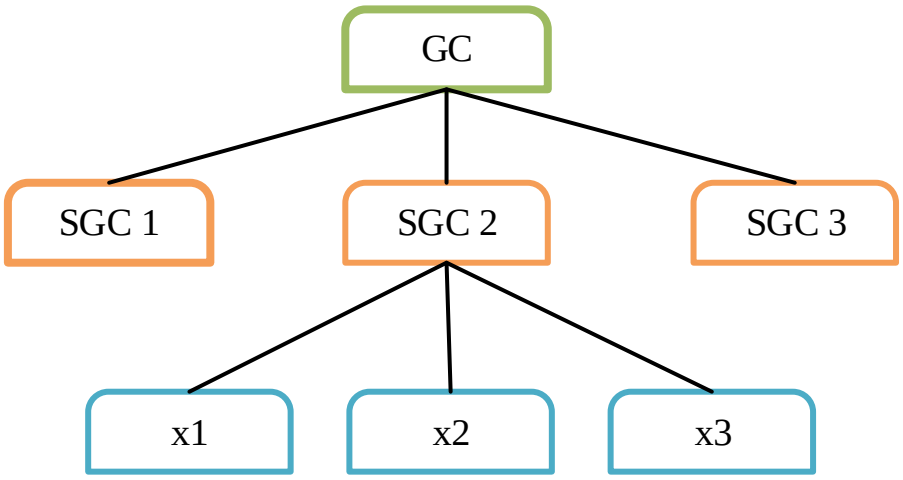


Figure 4.6 Key creation tree

The internal node aids its children nodes procedures as a sub group and full nodes are joined with their parent or other node by using a key. Based on either one or more than one node, the keys are known as tjk, where $k = 1, 2, ...y \; or \; tp - 1, \; for \; k = 1, 2, ...y.$ Assume the key is the subtree root, with the rightmost child Nk and leftmost child Nj, which is called tjk, whether the root of the subtree related to a single child node, then it is known as $tp - 1$ (either right or left). Whether rightmost or leftmost child is tp, and corresponding level number is 1.

Group generation and rekeying operations are manipulated by using the root node. That gives the exclusive id (UNK) to every sensing node. The group controller (GC) is used to create GK, the partial keys are taken by every SGC and its partial key. In the same way, SGC creates SGK by partial keys of its members and also its individuals.

The GK is calculated by Rivest-Shamir-Adelman (RSA) and the Chinese remainder theorem (CRT). The SGC1 and SGK1 were taken by partial GK with CRT and RSA. SGK3 can be calculated by using partial SGK2 with CRT and RSK. Likewise, the UNK for node x1 is computed using partial SGK1 with CRT and RSA. By using partial UNK1 with RSA and CRT, x2 will be calculated and so on.

4.8. RSA algorithm:

The RSA algorithm is used for security, and full node public and private keys are generated in every node. Both private and public keys of whole nodes are allocated in a key table and placed in the node that is known as the base station. The RSA method is the security method and the public key encryption algorithm that uses public key and private key to decrypt and encrypt messages. There are 2 keys in public crypto methods: private key is unique that is retained secret, the public key is released openly therefore anybody can determine it. The private key used decryption, and public key is used for encryption. It is hard to determine that private key is used for public key.

RSA is more effective in CRT mode than in direct mode. It holds the data with part of the RSA modulus size. RSA with CRT is ideally about four times quicker and it is well suitable for WSN. Figure 4.7 denotes the flow chart diagram of RSA.

The encryption of the information in RSA is done by public key, and information decryption is done by private key. The RSA method has some disadvantages and limitations for WSN. RSA is not the best selection for data security data communication in networks such as WSN.

Depend on RSA that is not able to bring faultless user un-tractability and privacy in WSN. It is specified that the RSA- dependent methods are more vulnerable to offline attacks such as the guessing of passwords that results in cooperating various keys in the network.

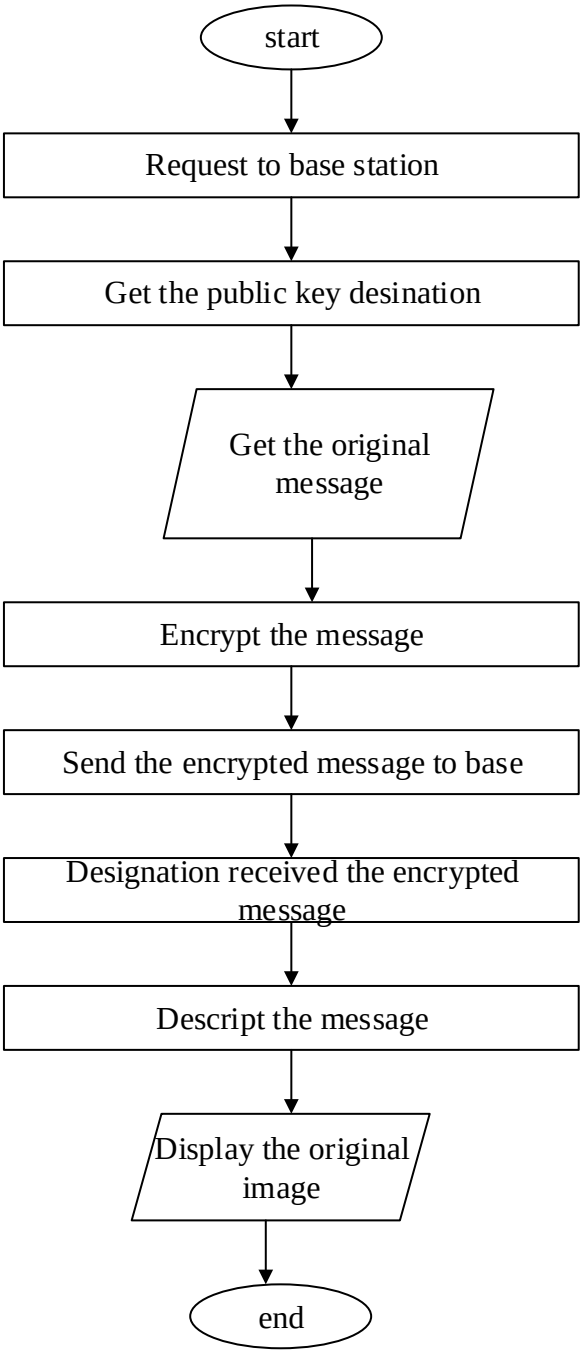


Figure 4.7 Flow chart of RSA

Thus, the base station includes the routing table and has the location of all the remaining nodes. Depending on the routing table, the base station gives two extra nodes that are near the base station as CH. Finally, the remaining two nodes are given as the designation node and source node casually with respect to all other usages.

4.9. CRT

Algorithm:

The CRT method is also called cryptography, signal processing, channel coding, and number theory. The sensors are battery operated with diverse types and capabilities are permitted with low data processing devices. These sensors are typically change to assist the requirement of single or multiple command nodes. These command nodes are either stable or moveable.

Two centralized GKM methods depend on CRT. By transferring heavy computation load into the key server, number of key storages, user side key computation, and number of rekey broadcast information are optimized. This CRT method wants high computation power from key server.

The CRT depends on a static key tree structure for allotting GK to members of group, then that changes membership. The CRT deals with the situation of pre-defined static prospective user group and includes full potential duties of multicast services and focuses on the stateless receiver side. It will decrease computation difficulty of the key server for every GK distribution. It will improve the workload of key server by permitting key server to determine the general group by using CRT for n number of equations.

GKM based on CRT typically decreases computation complexity of key server. Computation complexity is decreased by minimizing the group members by operating one modulo division operation where user leaves or joins the multicast group.

4.10. Top-down KMS:

The GK for GC is computed with CRT and RSA. Until, designated, RSA decryption is slow compared to encryption. It is altered by using an algorithm that is unique to the regular one or by generating an algorithm that is similar to the existing one. The CRT is another approach to RSA decryption and it is used to increase the process speed. The RSA decryption, single modular exponentiation is used. In CRT and RSA two modular exponentiation are used. When the CRT is used, the RSA decryption speed is increased by four times. The exponent size and smaller modulus reduce the resource consumption and calculation time. The KMS works has following steps figure 4.8.

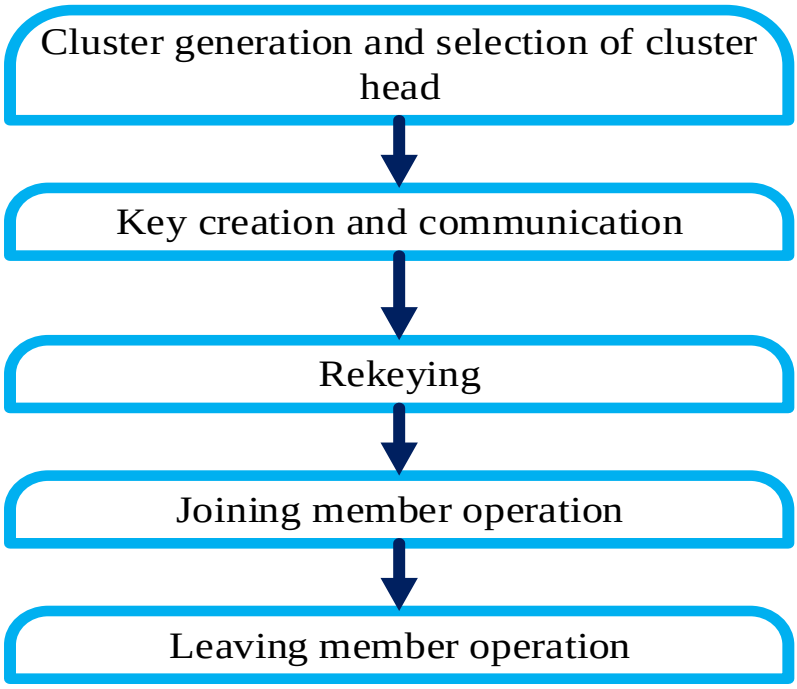


Figure 4.8 Steps of KMS work

4.10.1. Cluster generation and selection of cluster head:

Generation of cluster started the root node; a single SN or BS sends the transmission saying it needs to create a cluster. The cluster coverage is calculated by either the forward broadcast through a single or multi-hop cluster. After selecting the root node, various additional child cluster heads from the subset nodes nearer the cluster boundary after getting acknowledgement from the neighbors. The child cluster head is picked from nodes beyond the cluster boundary and overlapped among the clusters is reduced. The outside node is detected by forwarding the broadcast beyond the boundary and restricting the distance. The root node broadcasts a unicast message to selected child cluster heads, requesting that their cluster be created. The procedure continues where the cluster head generates and selects another batch of child cluster heads. Every cluster head retains track parent cluster head child cluster head to build the cluster tree. This approach is repeated until whole potential clusters are generated.

Clustering is the current routing approach for reducing the dissipation of energy of nodes, remaining energy consumption among nodes, and extending lifetime of network. In clustering approach, nodes are categorized into groups known as clusters. Every cluster has a head node called CH, and the remaining nodes are known as member nodes. The member nodes transmit the

information to the corresponding CH after gathering the received information, corresponding information, and transmitting it to base station. Base station has infinite energy and communicates with last user through satellite, internet, and communication media. CH performs gateway between the sensor nodes and the base station. Ideal cluster formation and CH selection play a significant role in reduction of energy consumption.

One of energy management characteristics in WSN is clustering, which divides network into several clusters and a node is selected as CH in every cluster. Base station decreases by combining the information from every node and then transmitting it into the base stations. That leads to energy consumption of resource constrained WSN as base station obtain information from fewer nodes. The benefits of CH are as follows:

- Collected information is allowed at CH to avoid unwanted information that saves the sensor node energy.
- CH has to continue the local route setup; routing is maintained simply and small routing data is wanted; that improves the network scalability.
- Sensor nodes communicate with corresponding CH, communication bandwidth is preserved, thus avoiding the redundant information exchange within themselves.

Clustering algorithm aids in energy consumption reduction in WSN. Clustering performs in rounds and there are 2 phases:

1. Setup phase
2. Steady phase

Nodes are organized into separate clusters. Every cluster has CH that is selected. Sensed information is transmitted to sink through CH. CH collects information from sensed nodes to cluster. Various information aggregation methods are used to achieve significant data clustering. The data is transmitted and collected to the base station. Clustering algorithms maintain energy efficiency, and the CH plays an important role. The location of selected CH cluster finds the inter-cluster communication distance (ICCD), where distance between clusters finds ICCD. The cluster that has the ICCD consumed a high amount of energy compared with the remaining cluster.

4.10.2. Key creation and communication:

The key distribution and creation are very difficult and are computed by using RSA and CRT. Table 4.2 represents key formation, UNK1 for the starting connected node is estimated by SGK1 and GK. By using SGK1 and UNK1, the UNK2 is estimated. By using UNK2 and SGK1, the UNK3 is estimated. In the process of key distribution, every node performs key calculation and rekeying operations on every node. Table 4.3 depicts the process of key distribution in each node, as well as the computation of rekeying and key operations on each node.

Table 4.2 Algorithms for key formation

For key formation

Initialization: GK, SGK, N (leaf node)

GK creation

GK K_{CRT} -K_{RSA}
SGK formation
SGK 1
For i in range (2, n);

SGKi

UNK formation
UNK 1
For I in range (2,n);
+
N(leaf node) formation
N1
For I in range (2,n);
+

where, GK represents group key

- K represents key
- SGK represents sub group key
- CRT represents Chinese remainder theorem
- RSA represents Rivest-Shamir-Adelman
- UNK represents unique id
- SGKi represents height of a tree for sub group key
- I, i represents iteration

Table 4.3 Algorithm key distribution process

Key distribution process

Key distribution – cluster (clusters, x1, x2)

{ // no of clusters

// x1, x2, x3 are nodes

// key generation

GK -> compute RSA + CRT

SGK -> f(GK) + RSA +CRT

UNK -> f(SGK) + RSA + CRT

// Key generation process for nodes

x1--> SGK1+GK (only for first node)

x2--> SGK1 + UNK1

x3--> SGK1 + UNK2

// communication between nodes

Session key -> x1, x2

Temp = x1->x2 // node link

}

where,

- GK represents group key
- SGK represents sub group key
- UNK represents unique id
- RSA represents Rivest-Shamir-Adelman
- CRT represents Chinese remainder theorem
- x1, x2, x3 represents nodes
- Temp represents variable

4.10.3. Rekeying:

The rekeying process is used to improve the protection of the overall system regularly changing the security keys. It is required when a node is compromised and wishes to be removed from the system and replaced by new cluster in key distribution assignment session, rekeying after the session has ended and forming the new cluster are the same. The key allotted in the prior session is used for secure transmission in the new session when it is not compromised.

Capturing the node by adversaries, then restoring the captured key in a timely manner is called rekeying. Each CH wants to change the sensor node key in its cluster. So that the rekeying includes redistribution of keys and reconstruction of clusters. The renewal of keys requires high amount of energy because of the large exchanging of messages. This process is not sufficient for WSN since its cost for communication is high.

Joining or leaving a member will cause a change in the number of members in sub group. The proposed method confirms both forward and backward confidentiality by permitting the large number of leavers and joins to happen at once. While joins and leaves happen, the GK is changed after it is generated. The only variable that will change is the cluster key. The current members will obtain the current id, public private key pair, and signature. Moreover, the count of members in the current group finds difficulties and overheads.

4.10.4. Joining member operation:

If the new member joins group, GC confirms the membership, creates new member key, and adds node to key tree. Next, send key to current member by secure unicast channel through GC. To certify backward security, the GC issues rekeying updates and messages entire keys through the key route of each member in the logical key ladder. The current member y10 needs to join, the GC creates the equivalent private key k10 after the identification process, and then updates whole keys on route from k10 parent node to root node (k1-9 becomes k1-10, k789 becomes k7-10) before rekeying message sending.

When {k1-10} k1-9 denotes k1-10 converted with k1-9. The prior GK k1-9 should not be computed by using the new GK k1-10, keeping the safety of the multicast transmission content is called backward security, where k represents key.

4.10.5. Leaving member operation:

The group members need to leave; the GC cancels the suitable leaf node in the key tree, modifies whole keys on route from parent node to root node to certify forward security, and sends the rekeying message. When group member y10 wants to leave, the GC removes nodes t10 from the key tree that update t1-10 and t7-10 to t1-9 and t789, respectively, before rekeying message

sending. Next create the new key, the GC strongly sent the key to essential group members through key distribution.

4.10.6. Flow chart:

Figure 4.9 represents the Dyclust flow chart diagram with the step-by-step procedure.

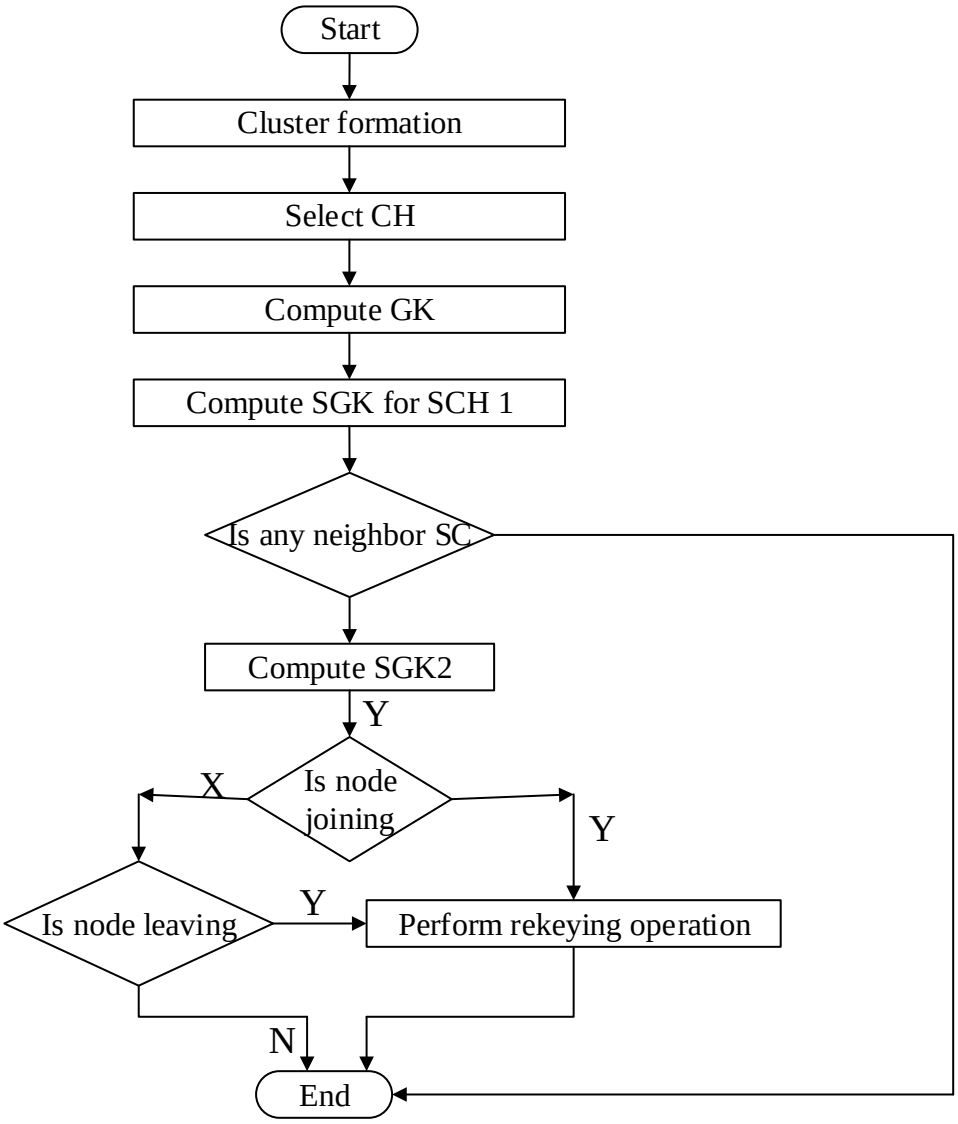


Figure 4.9 Dyclust flow chart

4.11 Summary

In a hybrid KM scheme for wireless sensor networks KM schemes, WSN requirements in KM, classification of KM methods is discussed. This classification includes subdivisions like GKM for WSN, static, dynamic, key discovery, key establishment, individual and group keys, subnetwork of KM are explained in detail manner. Issues in KM, RSA algorithm was discussed it is used for security and full node public and private keys are generated in each node. Top down KMS includes cluster generation and selection of cluster head, Key creation and communication, Rekeying, joining member operation, leaving member operation was discussed.

CHAPTER-5

Results and discussion

The emergence of WSN has been made possible by advancements in device technology, radio transceiver designs, & integrated circuits, as well as effective network protocols. These new applications include habitat, monitoring the soil quality, hazardous chemicals detection and forest fires detection, seismic activity, military surveillance, and more. Such a network gathers data from the sensor nodes for extended time periods and is made up of numerous sensor nodes dispersed over a vast area. Traditional WSN are seen as a particular extension & application of pure ad-hoc networks, with their distinctive features being a dense dispersion of SN & transmission of multi-hop over the entire network. Even though numerous illustrious studies have been conducted, some performance indicators still have intrinsic drawbacks, such as inadequate scalability, a poor energy balance, and short network lifetimes.

In recent years, a promising study area has been exploiting hybrid architecture in wireless sensor networks. A hybrid wireless sensor network typically consists of a variety of heterogeneous devices that primarily serve as sinks for data collection and transmission from underlying sensor nodes. Some of them have abundant energy or are rechargeable, while others have improved communication capabilities and mobility. These qualities can not only increase the network's throughput, reliability, and scalability as well as its energy efficiency, but they can also broaden its possible applications and simplify commercial deployment.

In recent years, innovative portable technologies like mobile phones, PDAs, and laptops have become more and more popular. Due to their strong computational and communication capacities, they are also appropriate for hybrid WSN. With the analysis, that a mobile phone is the best solution because it is both widely used and has extensive cellular infrastructure support. Clustering the network and employing a hierarchical structure are typical of large-scale WSN. Each cluster consists of a cluster head and several cluster members; the bottom cluster is a high-level member, and this caused the top cluster head nodes to communicate with the base station, creating a clustered WSN. This plan separates the network into numerous clusters made up of every connected region. The further distant the cluster head is from the base station, the more probable

it is that nodes in the same area will choose to join the same cluster as its members. Symmetric key methods require less computation time than other methods; the majority of WSNs utilize them. It can divide these methods into six categories depends on distribution of key, key establishment and key discovery in them: entity-based methods, polynomial based methods, pure probabilistic methods, tree based pre distribution of the key methods and matrix based methods and exclusion basis methods. The multicast key distribution method using logical key trees has been expanded to include WSN in the already used system. The centralized GKM protocol includes this method. For WSN, centralized solutions are frequently not ideal. However, such a method does have some value in that it enables an efficient base station to offload some of the computations from the weaker sensor nodes. Cluster deployment of nodes within a network is a typical approach for WSN. Assume from time to time that sensors located in the same partition are more likely to be neighbors or nearby. For solving the key management problem, the construction of a binary tree for each node is the method of choice. Effective key management is possible in this approach.

This study examines several algorithms based on four factors: the cost of computation, the cost of communication, the cost of rekeying and the cost of storage. Based on how well they perform in these four categories, various algorithms are compared. According to a study, to ensure forward and backward anonymity, the rekey is calculated and communicated on each join or leave procedure. Any rekey computation requires a lot of storage space to hold a lot of keys. The computational burden as well as the effectiveness and security of the key management process are the main areas of focus. This work described a top down DCGKMS method for dynamic clusters of sensors that move in accordance with their needs. The bottom-up method is used for determining all the keys in the static WSNs. The hybrid key management scheme for WSN method is applied and tested in a wireless channel with an $800 \times 800 m2$ simulation area and nodes of 100 mobiles in the ns2 environment. For this network, the AODV routing protocol is employed.

Table 5.1 Simulation table

Input parameter	Description	Input type
Set val(prop)	Two ray ground/propagation	Radio-propagation model
set val(ll)	LL	Link layer type
set val(ifqlen)	50	Max packet in ifq
set val(mac)	mac/802_ 11	MAC type
set val(x)	800	X length
set val(finish)	100	Finish time
set val(chan)	Channel/wireless channel	Channel type
set val(ant)	Antenna/Omni Antenna	Antenna type
set val(ifq)	Queue/Drop Tail/Pri-Queue	Interface queue type
set val(netif)	phy/wireless phy	Network interface type
set val(rp)	AODV	Routing protocol
set val(y)	800	Y length
set val(nn)	10	Number of mobile nodes

The input parameters and its type are shown in simulation Table 5.1. The results of the communication, computation and rekeying operations are calculated as follows, communication costs explain that there is a change in database that is altered to the sub-group controller once for each change whenever a member joins or leaves. Therefore, any modification in the network can be made with just one message. Cost of communication at joins and leaves of DCGKMS can be compared with OFT, LKH to number of messages and size of group.

The length of time required to execute a particular task. Even if there are numerous computer resources like power supply, memory, etc., that contribute to computational cost, it usually refers to calculation time. Cost of computation at joins and leaves of DCGKMS can be compared with OFT, LKH with respect to the number of messages and group size. Making a new key for the system is known as rekeying. Encryption must be enabled on the system in order to generate a new key; nevertheless, whether or not encrypted items are present, the rekey process still functions. Rekeying is mostly done to regain key control. Rekeying at joins and leaves of DCGKMS can be compared with OFT, LKH with respect to the number of messages and group size.

5.1 Analysis

This section offers a comparative examination of the outcomes obtained following the use of the approach.

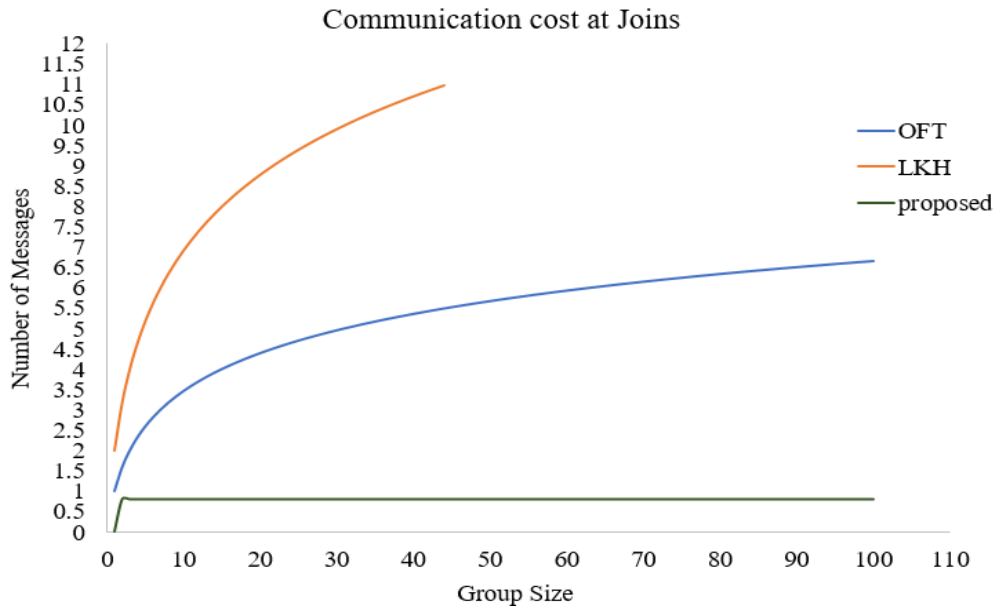


Figure 5.1 Cost of communication at joins

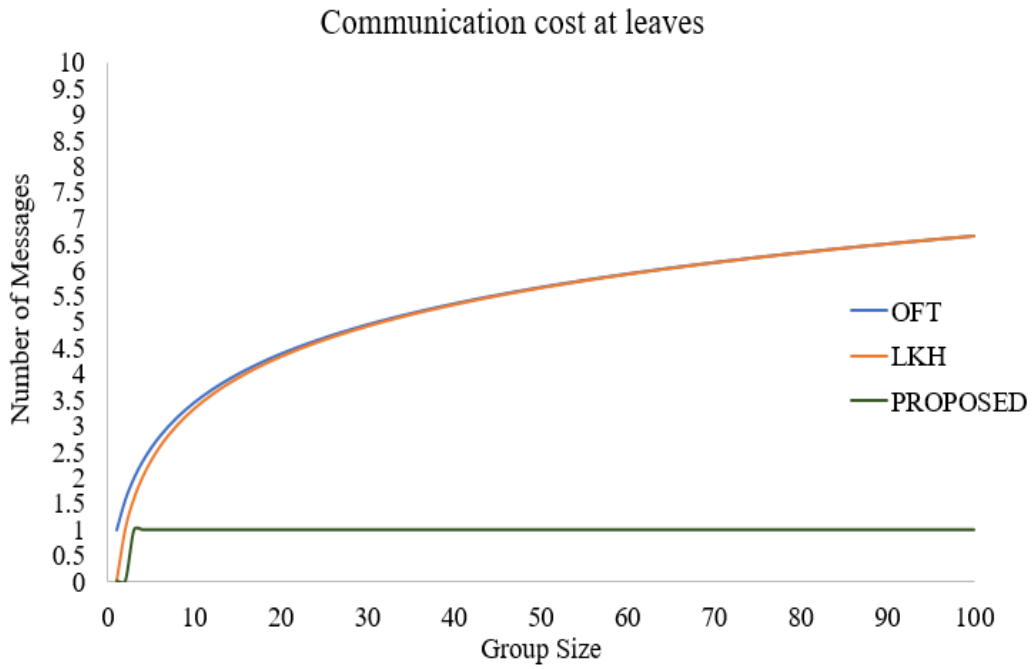


Figure 5.2 Cost of communication at leaves

Figures 5.1 and 5.2 display the statistical representation of the analytical measurements along with the communication costs at joints and the communication cost at leaves. The database changes when a member joins or leaves, and the sub-group controller is notified once for each change. As a result, only one message is needed for each network adjustment.

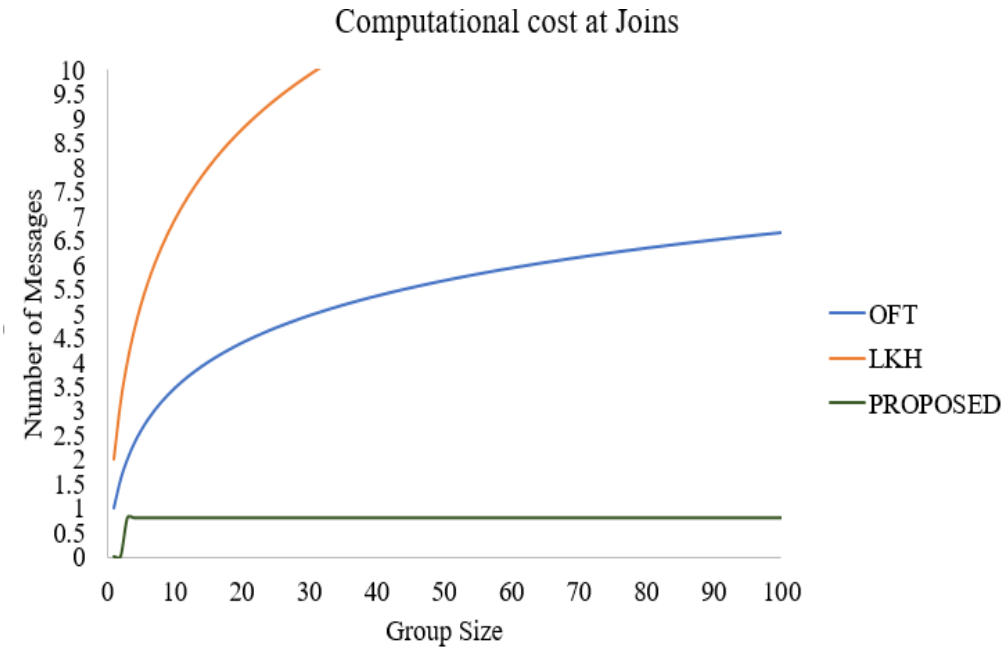


Figure 5.3 Cost of computation at joins

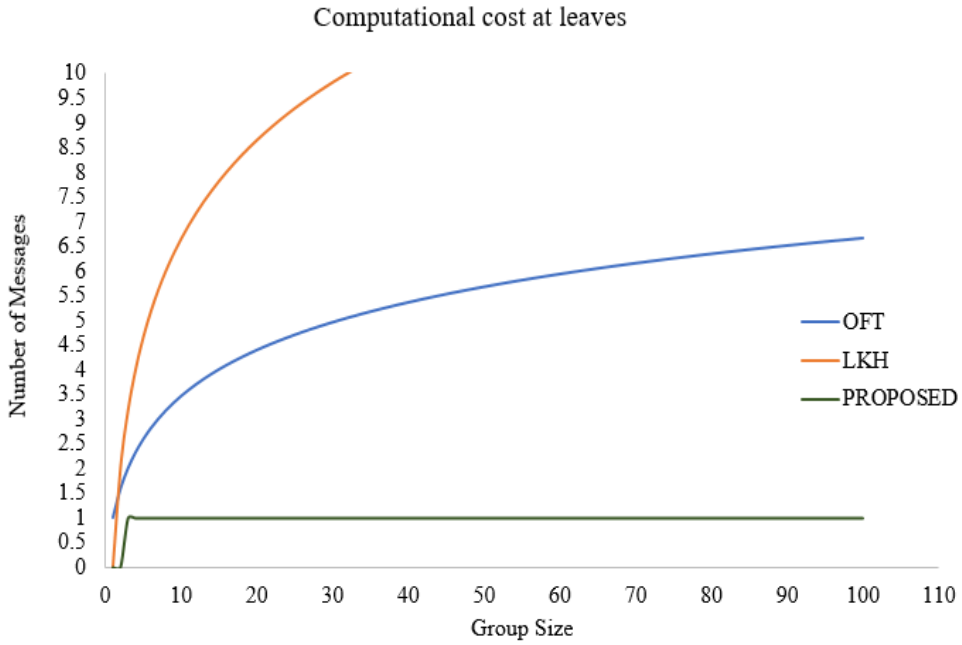


Figure 5.4 Cost of computation at leaves

That example, O (1) represents the communication cost for a key management system that is more effective. As a result, the join and depart node operations using the suggested method exhibit better results in a dynamic environment when compared to OFT and LKH. The statistical comparisons

of the computation costs at join and leave operations over a node between the suggested method and the existing algorithm (OFT and LKH) are shown in Figures 5.3 and 5.4. Although there is a rekeying method in the upgraded and cost-effective KMS, the group key remains the same for any change in the number of members while maintaining security standards.

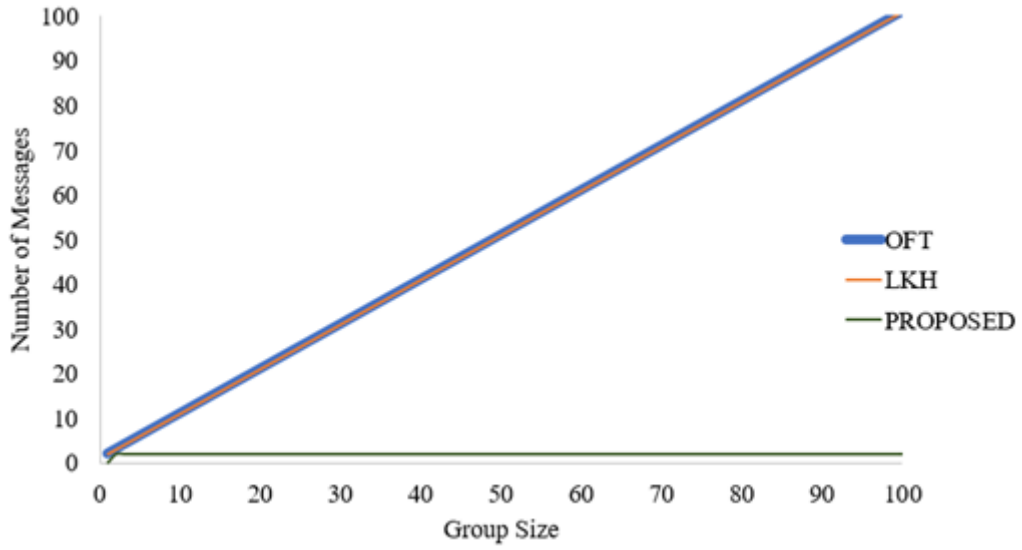


Figure 5.5 Rekeying is necessary at joins

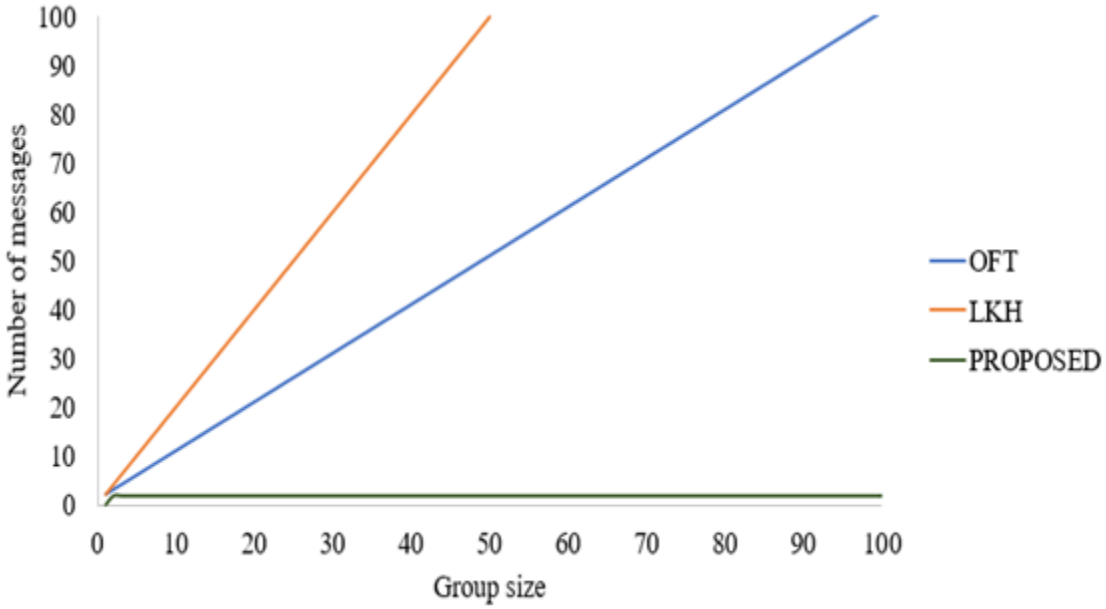


Figure 5.6 Rekeying is necessary at leaves

Figures 5.5 and 5.6 illustrate how the quantity of messages required for rekeying at joints and leaves varied from one another. Any change in the number of members in a sub-group could be the result of a member-leave or member-join. As a result, the proposed strategy produced improved rekeying operations results.

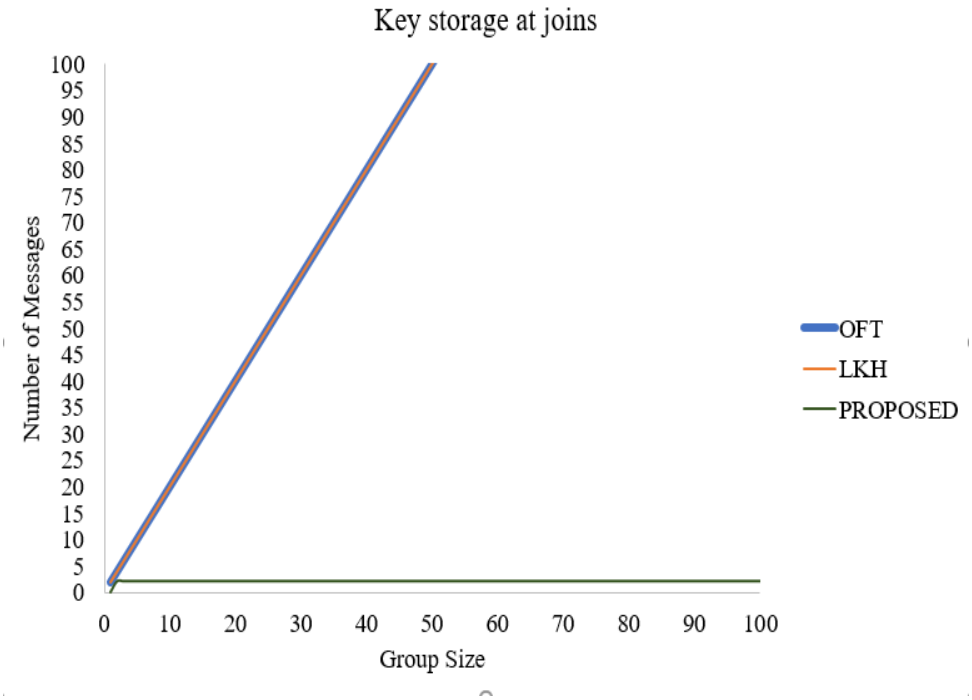


Figure 5.7 Key storage at joins

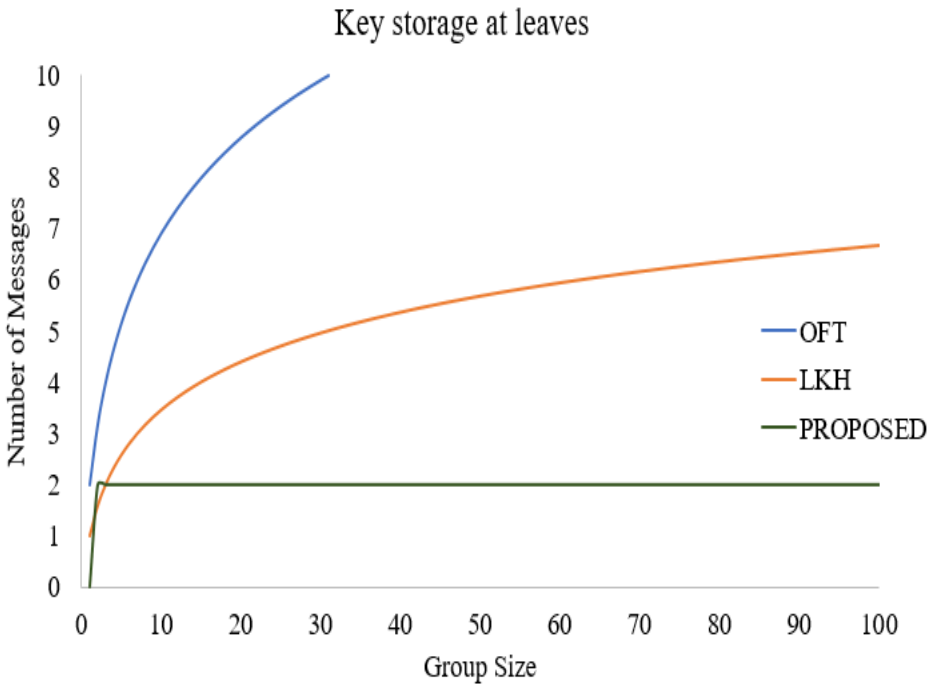


Figure 5.8 Key storage at leaves

In contrast, OFT and LKH are shown to be more expensive when used as key storage for dynamic WSN, as shown in Figures 5.7 and 5.8. In a better and more economical KMS, databases are

utilized to keep track of both present members and outgoing members. The simulation results comparison which is based on various factors is shown in Table 5.2, which demonstrates the effectiveness of the suggested methodology in comparison to the techniques now in use. Traditional algorithms are built from the bottom up, but the suggested method is built from the top down.

Table 5.2 Comparison results

Parameter	LKH/OFT (approximate value)	Proposed technique (approximate value)
Cost of communication at joins	From 0 to 1	From 0 to 0.8
Cost of communication at leaves	From 0 to 1	From 0 to 1
Rekeying is necessary at joins	From 0 to 4	From 0 to 2
Rekeying is necessary at leaves	From 0 to 4	From 0 to 2
Cost of computation at joins	From 0 to 1	From 0 to 0.8
Cost of computation at leaves	From 0 to 1	From 0 to 1
Key storage at joins	From 0 to 4	From 0 to 2
Key storage at leaves	From 0 to 3	From 0 to 2

5.2 Summary

Result and discussion section explains a comparative examination of the outcomes obtained following the use of the approach. Communication costs at joins and leaves, computational costs at joins and leaves, rekeying at joins and leaves, key storage at joins and leaves are resulted by comparing with the existing and proposed methodology. The simulation results comparison which is based on various factors and its approximate value is given.

Chapter 6

Conclusion and Future scope

6.1Conclusion

Numerous proposed solutions that are displayed in various studies address a basic problem that has been addressed by numerous key managers. WSN is available in a variety of sizes and has a variety of applications. Secure communication is necessary for many applications. During the joining and leaving operations of nodes, key management is crucial to achieving the security goal in WSN. Sensor-based technologies of applications in the modern period, such as IOT, etc., WSN, and discover security issues by their very nature of use. All these security risks are detailed in the paper. Many methods are covered by this study. The computation, storage costs, and communication, of rekeying based on four factors by the procedures. Group key management approaches are about many categories in the discussion. Four different distributed key management strategies were focused more on EDKAS, TGDH, DHSA, and DGKD. In the case of new member joins, DHSA has key encryption, lowest key generation, and communication overheads by the performance analysis of four approaches.

That accomplishes safe transmission among participants of a group-based network was improved and cost-effective KMS by this paper discussed and illustrated. This scheme and it's static are created only once by the group key. Participants leaving or joining, any shift in the networks, such as a result. This paper presents improved and cost-effective key management systems in terms of coordination overhead and computing costs. The key generation and data sharing employ the most dependable approaches revealed by the suggested key management system. Moreover, the party or members themselves are unaffected by the number of participants being rank. Rapidly evolving classes are presented for minor to moderate-sized by two unified, quick, and effective CRT-centered community key management sets of rules. A large range of protected group transmission applications can be implemented using protocol's simplicity and limited re-keying. Key recovery protocols should be developed based on the proposed scheme's key generation and refreshment functionality.

With its results on 4 parameter computations are analyzed different algorithm by this paper on 4 parameter computation, rekeying storage cost, complexity and communication, and cost. Throughout the study, it was found that calculated rekey and communicated on leave operation each join and to prevent forward and backward secrecy. Whenever a computation rekey is performed, a large storage amount capacity is needed store large number of keys at low cost.

6.2 Future scope

- It is also possible to disseminate unique credentials to trusted users online through the presence of a trustworthy third party (for example, mutual keys, Blom key pairs, polynomial shares).
- Potential work in this field will be taken into account by such possibilities.
- For forwarding and preventing secrecy on creating new keys by focusing before moving on to the appropriate leave and join procedures.
- A reasonable cost requires a significant quantity of storage space, a large number of keys at a reasonable cost, which is a difficult task.
- To reduce overheads using a top-down approach is to develop method used on behalf of changing tree WSN topology by a future research goal because the aforementioned techniques employ a significant overhead key and a bottom-up approach for complex computing.

Chapter 7

References

1. Karray, Fatma, Mohamed W. Jmal, Alberto Garcia-Ortiz, Mohamed Abid, and Abdulfattah M. Obeid. "A comprehensive survey on wireless sensor node hardware platforms." *Computer Networks* 144 (2018): 89-110.
2. Rashid, Bushra, and Mubashir Husain Rehmani. "Applications of wireless sensor networks for urban areas: A survey." *Journal of network and computer applications* 60 (2016): 192-219.
3. Kassim MR, Harun AN. Applications of WSN in agricultural environment monitoring systems. In2016 international conference on information and communication technology convergence (ICTC) 2016 Oct 19 (pp. 344-349). IEEE.
4. Elhoseny M, Hassanien AE. Secure data transmission in WSN: an overview. Dynamic wireless sensor networks. 2019:115-43.
5. David DS, Jeyachandran A. A comprehensive survey of security mechanisms in healthcare applications. In2016 international conference on communication and electronics systems (ICCES) 2016 Oct 21 (pp. 1-6). IEEE.
6. Wang Q, Jiang J. Comparative examination on architecture and protocol of industrial wireless sensor network standards. IEEE Communications Surveys & Tutorials. 2016 Apr 6;18(3):2197-219.
7. Kaiwen C, Kumar A, Xavier N, Panda SK. An intelligent home appliance control-based on WSN for smart buildings. In2016 IEEE International Conference on Sustainable Energy Technologies (ICSET) 2016 Nov 14 (pp. 282-287). IEEE.
8. Gaber T, Abdelwahab S, Elhoseny M, Hassanien AE. Trust-based secure clustering in WSN-based intelligent transportation systems. Computer Networks. 2018 Dec 9;146:151-8.
9. Shahraki A, Taherkordi A, Haugen Ø, Eliassen F. A survey and future directions on clustering: From WSNs to IoT and modern networking paradigms. IEEE Transactions on Network and Service Management. 2020 Nov 2;18(2):2242-74.
10. Kovásznai, Gergely, KrisztiánGajdár, and Laura Kovács. "Portfolio SAT and SMT solving of cardinality constraints in sensor network optimization." In *2019 21st*

International Symposium on Symbolic and Numeric Algorithms for Scientific Computing (SYNASC), pp. 85-91. IEEE, 2019.

11. Wani, Anwaar Ahmad, Razeef Mohammad, and Idrees Ahmad Bhat. "An Advanced Security Framework Scheme Based on SCSR for Hierarchical Wireless Sensor Network." In *Proceedings of Second International Conference in Mechanical and Energy Technology*, pp. 571-578. Springer, Singapore, 2023.
12. Grover, Jitender, and Shikha Sharma. "Security issues in wireless sensor network—a review." In *2016 5th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions)(ICRITO)*, pp. 397-404. IEEE, 2016.
13. Maheswari, S. Uma, N. S. Usha, EA Mary Anita, and K. Ramaya Devi. "A novel robust routing protocol RAEED to avoid DoS attacks in WSN." In *2016 International Conference on Information Communication and Embedded Systems (ICICES)*, pp. 1-5. IEEE, 2016.
14. Iala, Imad, MouradOuadou, DrissAboutajdine, and OuadoudiZytoune. "Energy based collision avoidance at the mac layer for wireless sensor network." In *2017 International Conference on Advanced Technologies for Signal and Image Processing (ATSIP)*, pp. 1-5. IEEE, 2017.
15. Iwendi, Celestine, Zhiyong Zhang, and Xin Du. "ACO based key management routing mechanism for WSN security and data collection." In *2018 IEEE international conference on industrial technology (ICIT)*, pp. 1935-1939. IEEE, 2018.
16. Gautam, Amit Kumar, and Rakesh Kumar. "A comparative study of recently proposed key management schemes in wireless sensor network." In *2018 International Conference on Computing, Power and Communication Technologies (GUCON)*, pp. 512-517. IEEE, 2018.
17. Boudia, Omar RafikMerad, Sidi Mohammed Senouci, and Mohammed Feham. "A novel secure aggregation scheme for wireless sensor networks using stateful public key cryptography." *Ad Hoc Networks* 32 (2015): 98-113.
18. Yao, Wenbin, Si Han, and Xiaoyong Li. "LKH++ based group key management scheme for wireless sensor network." *Wireless Personal Communications* 83, no. 4 (2015): 3057-3073.

19. Messai, Mohamed-Lamine, and HamidaSeba. "A survey of key management schemes in multi-phase wireless sensor networks." *Computer Networks* 105 (2016): 60-74.
20. Bentaleb, Abdelhak, Bayan Taani, Ali C. Begen, Christian Timmerer, and Roger Zimmermann. "A survey on bitrate adaptation schemes for streaming media over HTTP." *IEEE Communications Surveys & Tutorials* 21, no. 1 (2018): 562-585.
21. Kwon, DeokKyu, Sung Jin Yu, Joon Young Lee, Seung Hwan Son, and Young Ho Park. "WSN-SLAP: Secure and lightweight mutual authentication protocol for wireless sensor networks." *Sensors* 21, no. 3 (2021): 936.
22. Yu, SungJin, JoonYoung Lee, KyungKeun Lee, KiSung Park, and YoungHo Park. "Secure authentication protocol for wireless sensor networks in vehicular communications." *Sensors* 18, no. 10 (2018): 3191.
23. Ryu, Jihyeon, Hakjun Lee, Hyoungshick Kim, and Dongho Won. "Secure and efficient three-factor protocol for wireless sensor networks." *Sensors* 18, no. 12 (2018): 4481.
24. Qabouche, Hicham, Aïcha Sahel, and AbdelmajidBadri. "Hybrid energy efficient static routing protocol for homogeneous and heterogeneous large scale WSN." *Wireless Networks* 27, no. 1 (2021): 575-587.
25. Menegazzo, Cinara, and Luiz Carlos Pessoa Albini. "Unadvertised energy saving method for static and homogeneous wireless sensor networks." *IET Wireless Sensor Systems* 4, no. 3 (2014): 105-111.
26. Yan, Jingjing, Mengchu Zhou, and Zhijun Ding. "Recent advances in energy-efficient routing protocols for wireless sensor networks: A review." *IEEE Access* 4 (2016): 5673-5686.
27. Kumari, Shipra, and HariOm. "Authentication protocol for wireless sensor networks applications like safety monitoring in coal mines." *Computer Networks* 104 (2016): 137-154.
28. Smys, S. "Energy-aware security routing protocol for WSN in big-data applications." *Journal of ISMAC* 1, no. 01 (2019): 38-55.
29. Lazrag, Hilmi, AbdellahChehri, RachidSaadane, and MoulayDrissRahmani. "Efficient and secure routing protocol based on Blockchain approach for wireless sensor networks." *Concurrency and Computation: Practice and Experience* 33, no. 22 (2021): e6144.

30. Naeem, Afia, Abdul RehmanJaved, Muhammad Rizwan, Sidra Abbas, Jerry Chun-Wei Lin, and Thippa Reddy Gadekallu. "DARE-SEP: A hybrid approach of distance aware residual energy-efficient SEP for WSN." *IEEE transactions on green communications and networking* 5, no. 2 (2021): 611-621.
31. Sethi, Deepak. "An approach to optimize homogeneous and heterogeneous routing protocols in WSN using sink mobility." *MAPAN* 35, no. 2 (2020): 241-250.
32. Thirukrishna, J. T., S. Karthik, and V. P. Arunachalam. "Revamp energy efficiency in homogeneous wireless sensor networks using optimized radio energy algorithm (OREA) and power-aware distance source routing protocol." *Future Generation Computer Systems* 81 (2018): 331-339.
33. Lazrag, Hilmi, AbdellahChehri, RachidSaadane, and MoulayDrissRahmani. "A blockchain-based approach for optimal and secure routing in wireless sensor networks and IoT." In *2019 15th International Conference on Signal-Image Technology & Internet-Based Systems (SITIS)*, pp. 411-415. IEEE, 2019.
34. Jangwan, Harendra S., and Ashish Negi. "Enhanced Energy-Efficient Static Clustering Protocol for WSNs." *International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)* 7, no. 8 (2018).
35. Mehra, Pawan, M. Doja, and Bashir Alam. "Stability enhancement in LEACH (SE-LEACH) for homogeneous WSN." *EAI Endorsed Transactions on Scalable Information Systems* 6, no. 20 (2019).
36. Jilna, Payingat, and Deepthi P. Pattathil. "A key management technique based on elliptic curves for static wireless sensor networks." *Security and Communication Networks* 8, no. 18 (2015): 3726-3738.
37. Zhang, Ying, Jixing Liang, BingxinZheng, and Wei Chen. "A hybrid key management scheme for WSNs based on PPBR and a tree-based path key establishment method." *Sensors* 16, no. 4 (2016): 509.
38. Rajasoundaran, S., A. V. Prabu, J. B. V. Subrahmanyam, RakeshRajendran, G. Sateesh Kumar, SiripuriKiran, and Osamah Ibrahim Khalaf. "Secure watchdog selection using intelligent key management in wireless sensor networks." *Materials Today: Proceedings* (2021).

39. Gandino, Filippo, CesareCelozzi, and Maurizio Rebaudengo. "A key management scheme for mobile wireless sensor networks." *Applied Sciences* 7, no. 5 (2017): 490.
40. Patel, Vaishali, and JaydeepGheewala. "An efficient session key management scheme for cluster based wireless sensor networks." In *2015 IEEE International Advance Computing Conference (IACC)*, pp. 963-967. IEEE, 2015.
41. Manikandan, G., K. Suresh, and L. SherlyPuspha Annabel. "Performance Analysis of Cluster based Secured Key Management Schemes in WSN." In *2019 International Conference on Smart Systems and Inventive Technology (ICSSIT)*, pp. 944-948. IEEE, 2019.
42. Al-taha, Mohammed A. "Symmetric Key Management Scheme for Hierarchical Wireless Sensor Networks." *International Journal of Network Security & Its Applications (IJNSA) Vol* 10 (2018).
43. Mathew, Priya, P. Jilna, and P. P. Deepthi. "Efficient implementation of EC based key management scheme on FPGA for WSN." In *2015 9th International Conference on Telecommunication Systems Services and Applications (TSSA)*, pp. 1-6. IEEE, 2015.
44. Jilna, Payingat, and P. P. Deepthi. "Light Weight Key Establishment Scheme for Wireless Sensor Networks." In *International Conference on Security, Privacy, and Applied Cryptography Engineering*, pp. 124-137. Springer, Cham, 2016.
45. Patil, Shantala Devi, B. P. Vijayakumar, and KiranKumariPatil. "Fractal PKC-based key management scheme for wireless sensor networks." In *Recent Developments in Intelligent Computing, Communication and Devices*, pp. 121-128. Springer, Singapore, 2017.
46. Manikandan, G., K. Suresh, and L. SherlyPuspha Annabel. "Performance Analysis of Cluster based Secured Key Management Schemes in WSN." In *2019 International Conference on Smart Systems and Inventive Technology (ICSSIT)*, pp. 944-948. IEEE, 2019.
47. Tian, Youliang, Zuan Wang, JinboXiong, and Jianfeng Ma. "A blockchain-based secure key management scheme with trustworthiness in DWSNs." *IEEE Transactions on Industrial Informatics* 16, no. 9 (2020): 6193-6202.
48. Hamsha, K., and G. S. Nagaraja. "Threshold cryptography based light weight key management technique for hierarchical WSNs." In *International conference on ubiquitous communications and network computing*, pp. 188-197. Springer, Cham, 2019.

49. Lei, Ao, Haitham Cruickshank, Yue Cao, Philip Asuquo, Chibueze P. AnyigorOgah, and Zhili Sun. "Blockchain-based dynamic key management for heterogeneous intelligent transportation systems." *IEEE Internet of Things Journal* 4, no. 6 (2017): 1832-1843.
50. Sun, Bowen, Qi Li, and Bin Tian. "Local dynamic key management scheme based on layer-cluster topology in WSN." *Wireless Personal Communications* 103, no. 1 (2018): 699-714.
51. Yousefpoor, Mohammad Sadegh, and Hamid Barati. "DSKMS: a dynamic smart key management system based on fuzzy logic in wireless sensor networks." *Wireless Networks* 26, no. 4 (2020): 2515-2535.
52. Dave, Mayank. "Storage as a parameter for classifying dynamic key management schemes proposed for WSNs." In *2016 International Conference on Computational Techniques in Information and Communication Technologies (ICCTICT)*, pp. 51-56. IEEE, 2016.
53. Kamble, Swapnil B., and Vivek V. Jog. "Efficient key management for dynamic wireless sensor network." In *2017 2nd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT)*, pp. 583-586. IEEE, 2017.
54. Kuchipudi, Ramu, Ahmed Abdul MoizQyser, and VVSS S. Balaram. "Latest developments on dynamic key management for dynamic wireless sensor networks." In *2016 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT)*, pp. 1119-1124. IEEE, 2016.
55. Wen, Mi, Kaoru Ota, He Li, Jingsheng Lei, ChunhuaGu, and Zhou Su. "Secure data deduplication with reliable key management for dynamic updates in CPSS." *IEEE transactions on computational social systems* 2, no. 4 (2015): 137-147.
56. Noura, Hassan, Ali Chehab, and Raphael Couturier. "Lightweight dynamic key-dependent and flexible cipher scheme for IoT devices." In *2019 IEEE Wireless Communications and Networking Conference (WCNC)*, pp. 1-8. IEEE, 2019.
57. Kumar, Vinod, Om Pal, Vinay Thakur, and Kamendra Kumar. "SCGKM: a secure and cost-effective group key management scheme for multicast communication in large dynamic groups." *International Journal of Information Technology* 14, no. 2 (2022): 781-788.

58. Athmani, Samir, AzeddineBilami, and DjallelEddineBoubiche. "EDAK: An efficient dynamic authentication and key management mechanism for heterogeneous WSNs." *Future Generation Computer Systems* 92 (2019): 789-799.
59. Omar, Mawloud, ImeneBelalouache, SamiaAmrane, and BournaneAbbache. "Efficient and energy-aware key management framework for dynamic sensor networks." *Computers & Electrical Engineering* 72 (2018): 990-1005.
60. Ma, Mingxin, Guozhen Shi, and Fenghua Li. "Privacy-oriented blockchain-based distributed key management architecture for hierarchical access control in the IoT scenario." *IEEE access* 7 (2019): 34045-34059.
61. Bagavathipriya, S. "Hybrid Neuro-Fuzzy Clustering and Modified ECC Based Dynamic Key Management in WSN." (2019).
62. Patil, Shravani Mahesh, and Purushothama BR. "Security Analysis of Proxy Cryptography Based Group Key Management Schemes for Dynamic and Wireless Networks Under Active Outsider Attack Model." *Journal of Information Assurance & Security* 14, no. 2 (2019).
63. Lee, Kuen-Jong, Ching-An Liu, and Chia-Chi Wu. "A dynamic-key based secure scan architecture for manufacturing and in-field IC testing." *IEEE Transactions on Emerging Topics in Computing* (2020).
64. Yao, Wenbin, Si Han, and Xiaoyong Li. "LKH++ based group key management scheme for wireless sensor network." *Wireless Personal Communications* 83, no. 4 (2015): 3057-3073.
65. Hur, Junbeom, and Younho Lee. "A reliable group key management scheme for broadcast encryption." *Journal of Communications and Networks* 18, no. 2 (2016): 246-260.
66. Ma, Haiying, and Guorong Sun. "Blockchain-based group key management scheme in IoT." In *International Conference on Intelligent Computing*, pp. 445-457. Springer, Cham, 2020.
67. Manikandan, S. Periasamy, and Shanmugam Milton Ganesh. "SPPGKM: A secure polynomial function powered group key management scheme for dynamic user environments in cloud." *Concurrency and Computation: Practice and Experience* (2022): e7053.

68. Ramamoorthy, Raghu, and MenakadeviThangavelu. "Group based dual mode key management scheme for secure communication in vehicular ad hoc networks." *Wireless Personal Communications* 120, no. 2 (2021): 949-973.
69. Pulagara, SeshuBabu, and P. J. A. Alphonse. "An intelligent and robust conditional privacy preserving authentication and group-key management scheme for vehicular ad hoc networks using elliptic curve cryptosystem." *Concurrency and Computation: Practice and Experience* 33, no. 3 (2021): e5153.
70. Mohammadi, Mojtaba, and AlirezaKeshavarz-Haddad. "A new distributed group key management scheme for wireless sensor networks." In *2017 14th International ISC (Iranian Society of Cryptology) Conference on Information Security and Cryptology (ISCISC)*, pp. 37-41. IEEE, 2017.
71. Han, Wendie, Rui Zhang, Lei Zhang, and Lulu Wang. "A Secure and Receiver-Unrestricted Group Key Management Scheme for Mobile Ad-hoc Networks." In *2022 IEEE Wireless Communications and Networking Conference (WCNC)*, pp. 986-991. IEEE, 2022.
72. Mahaveerakannan, R., and C. Suresh GnanaDhas. "A hybrid group key management scheme for uav–mbn network environment increasing efficiency of key distribution in joining operation." In *International Conference on Intelligent Information Technologies*, pp. 93-107. Springer, Singapore, 2017.
73. Hussain, Abdalkahik W., and Mahmood K. Ibrahem. "An efficient pairwise and group key management scheme for wireless sensor network." *Int. J. Enhanc. Res. Sci. Technol. Eng* 1, no. 4 (2015): 25-31.
74. Chugh, Neeraj, Adarsh Kumar, and Alok Aggarwal. "Availability aspects through optimization techniques based outlier detection mechanism in wireless and mobile networks." *International Journal of Computer Networks & Communications (IJCNC) Vol* 10 (2018).
75. Kamal, Rishabh, and PriyankaAhlawat. "Improved matrix based key management scheme for wireless sensor network security." In *2019 international conference on issues and challenges in intelligent computing techniques (ICICT)*, vol. 1, pp. 1-5. IEEE, 2019.

76. Borkar, Gautam M., Leena H. Patil, DilipDalgade, and AnkushHutke. "A novel clustering approach and adaptive SVM classifier for intrusion detection in WSN: A data mining concept." *Sustainable Computing: Informatics and Systems* 23 (2019): 120-135.
77. Saraswathi, R. Vijaya, L. Padma Sree, and K. Anuradha. "Multi-stage key management scheme for cluster based WSN." *International Journal of Communication Networks and Information Security* 10, no. 3 (2018): 552.
78. Ahmed, Gulnaz, JianhuaZou, Mian Muhammad SadiqFareed, and Muhammad Zeeshan. "Sleep-awake energy efficient distributed clustering algorithm for wireless sensor networks." *Computers & Electrical Engineering* 56 (2016): 385-398.
79. Robinson, Y. Harold, S. Balaji, and M. Rajaram. "ECBK: enhanced cluster based key management scheme for achieving quality of service." *Circuits and Systems* 7, no. 08 (2016): 2014.
80. Bhushan, Bharat, and GadadharSahoo. "ISFC-BLS (intelligent and secured fuzzy clustering algorithm using balanced load sub-cluster formation) in WSN environment." *Wireless Personal Communications* 111, no. 3 (2020): 1667-1694.
81. Selvi, G. Vennira, and R. Balasubramanian. "Secure based Clustering Algorithm for Wireless Sensor Networks." *International Journal of Computer Applications* 117, no. 1 (2015).
82. Santhosh Kumar, S. V. N., YogeshPalanichamy, MunuswamySelvi, SannasiGanapathy, ArputharajKannan, and SankarPariserumPerumal. "Energy efficient secured K means based unequal fuzzy clustering algorithm for efficient reprogramming in wireless sensor networks." *Wireless Networks* 27, no. 6 (2021): 3873-3894.
83. Mehmood, Gulzar, Muhammad Sohail Khan, Abdul Waheed, Mahdi Zareei, Muhammad Fayaz, Tariq Sadad, Nazri Kama, and AzriAzmi. "An efficient and secure session key management scheme in wireless sensor network." *Complexity* 2021 (2021).
84. Liao, Ying, Huan Qi, and Weiqun Li. "Load-balanced clustering algorithm with distributed self-organization for wireless sensor networks." *IEEE sensors journal* 13, no. 5 (2012): 1498-1506.
85. Jolly, Gaurav, Mustafa C. Kusçu, PallaviKokate, and Mohamed Younis. "A low-energy key management protocol for wireless sensor networks." In *Proceedings of the Eighth*

IEEE Symposium on Computers and Communications. ISCC 2003, pp. 335-340. IEEE, 2003.

86. Đurišić, MilicaPejanović, ZhilbertTafa, GoranDimić, and VeljkoMilutinović. "A survey of military applications of wireless sensor networks." In *2012 Mediterranean conference on embedded computing (MECO)*, pp. 196-199. IEEE, 2012.
87. Roman, Rodrigo, Cristina Alcaraz, Javier Lopez, and Nicolas Sklavos. "Key management systems for sensor networks in the context of the Internet of Things." *Computers & Electrical Engineering* 37, no. 2 (2011): 147-159.
88. Carlier, Matthias, Kris Steenhaut, and AnBraeken. "Symmetric-key-based security for multicast communication in wireless sensor networks." *Computers* 8, no. 1 (2019): 27.
89. Rahman, Musfiq, and SrinivasSampalli. "An efficient pairwise and group key management protocol for wireless sensor network." *Wireless Personal Communications* 84, no. 3 (2015): 2035-2053.
90. Dohare I, Singh K. Green communication in sensor enabled IoT: integrated physics inspired meta-heuristic optimization based approach. *Wireless Networks*. 2020 Jul;26(5), pp.3331-48.
91. Rao RV, Selvamani K, Elakkiya R. A secure key transfer protocol for group communication. arXiv preprint arXiv:1212.2720. 2012 Dec 12.
92. Balen J, Zagar D, Martinovic G. Quality of service in wireless sensor networks: a survey and related patents. *Recent Patents on Computer Science*. 2011 Sep 1;4(3),pp.188-202.
93. Kumar, N. S., &Lavanya, S. A novel scheme for secure group communication in multicast network. *International Journal of Security and Networks*, 2015, 10(2), pp. 65-75.
94. Zhang, Jingxia, and Ruqiang Yan. "Centralized energy-efficient clustering routing protocol for mobile nodes in wireless sensor networks." *IEEE Communications Letters* 23, no. 7 (2019): 1215-1218.
95. Ahutu, OhidaRufai, and Hosam El-Ocla. "Centralized routing protocol for detecting wormhole attacks in wireless sensor networks." *IEEE Access* 8 (2020): 63270-63282.
96. Sridevi, B., and S. Rajaram. "Dynamic Inter Arrival Time Based Seamless Handoff for Mobile WIMAX Ping-Pong Calls Bypassing PKMv2 EAP Authentication." *International Journal of Computer Network & Information Security* 4, no. 6 (2012).

97. Singh, Kamaljit, and Lalit Sharma. "Hierarchical group key management using threshold cryptography in wireless sensor networks." *International Journal of Computer Applications* 63, no. 4 (2013).

98. Son, Ju-Hyung, Jun-Sik Lee, and Seung-Woo Seo. "Topological key hierarchy for energy-efficient group key management in wireless sensor networks." *Wireless personal communications* 52, no. 2 (2010): 359-382.

99. Hajyvahabzadeh, Melisa, ElinaEidkhani, SeyedehAnahitaMortazavi, and AlirezaNemaney Pour. "An efficient group key management protocol using code for key calculation: CKC." *Telecommunication Systems* 51, no. 2 (2012): 115-123.

100. Bajaber, Fuad, and IrfanAwan. "Adaptive decentralized re-clustering protocol for wireless sensor networks." *Journal of Computer and System Sciences* 77, no. 2 (2011): 282-292.

101. Sharma, Shikha, and C. Rama Krishna. "An efficient distributed group key management using hierarchical approach with elliptic curve cryptography." In *2015 IEEE International Conference on Computational Intelligence & Communication Technology*, pp. 687-693. IEEE, 2015.

102. Mortazavi, S. Anahita, AlirezaNemaney Pour, and Toshihiko Kato. "An efficient distributed group key management using hierarchical approach with Diffie-Hellman and Symmetric Algorithm: DHSA." In *2011 international symposium on computer networks and distributed systems (CNDS)*, pp. 49-54. IEEE, 2011.

103. Singh, UdayPratap, and Rajkumar Singh Rathore. "An efficient distributed group key management using hierarchical approach with ECDH and symmetric algorithm." *J. Comput. Eng. Intel. Syst* 3, no. 7 (2012): 32-41.

104. Ketshabetswe, Lucia Keleadile, AdamuMurtalaZungeru, MmolokiMangwala, Joseph M. Chuma, and Boyce Sigweni. "Communication protocols for wireless sensor networks: A survey and comparison." *Heliyon* 5, no. 5 (2019): e01591.

105. Ahlawat, Priyanka, and Mayank Dave. "An attack model based highly secure key management scheme for wireless sensor networks." *Procedia Computer Science* 125 (2018): 201-207.

106. Jose, Joel Mathew, Jovel Varghese Jose, and ChaitanyaVijaykumarMahamuni. "Multi-Biosensor based Wireless Body Area Networks (WBAN) for Critical Health

Monitoring of Patients in Mental Health Care Centers: An Interdisciplinary Study." *International Journal of Research in Engineering, Science and Management* 3 (2020).

107. Kuo, Yaw-Wen, Cho-Long Li, Jheng-Han Jhang, and Sam Lin. "Design of a wireless sensor network-based IoT platform for wide area and heterogeneous applications." *IEEE Sensors Journal* 18, no. 12 (2018): 5187-5197.

108. Guerrero-Sanchez, Alma E., Edgar A. Rivas-Araiza, Jose Luis Gonzalez-Cordoba, Manuel Toledano-Ayala, and AndrasTakacs. "Blockchain mechanism and symmetric encryption in a wireless sensor network." *Sensors* 20, no. 10 (2020): 2798.

109. Mukase, Sandrine, Kewen Xia, and Abubakar Umar. "Optimal Base Station Location for Network Lifetime Maximization in Wireless Sensor Network." *Electronics* 10, no. 22 (2021): 2760.

110. Modieginyane, Kgotlaetsile Mathews, Babedi Betty Letswamotse, Reza Malekian, and Adnan M. Abu-Mahfouz. "Software defined wireless sensor networks application opportunities for efficient network management: A survey." *Computers & Electrical Engineering* 66 (2018): 274-287.

111. Bhushan, Bharat, and GadadharSahoo. "Recent advances in attacks, technical challenges, vulnerabilities and their countermeasures in wireless sensor networks." *Wireless Personal Communications* 98, no. 2 (2018): 2037-2077.

112. Boubiche, DjallelEddine, Samir Athmani, Sabrina Boubiche, and HomeroToral-Cruz. "Cybersecurity issues in wireless sensor networks: current challenges and solutions." *Wireless Personal Communications* 117, no. 1 (2021): 177-213.

113. Bajpai, Pranshu, Aditya K. Sood, and Richard Enbody. "A key-management-based taxonomy for ransomware." In *2018 APWG Symposium on Electronic Crime Research (eCrime)*, pp. 1-12. IEEE, 2018.

114. Liu, Jianming, Ziyan Zhao, Jerry Ji, and Miaolong Hu. "Research and application of wireless sensor network technology in power transmission and distribution system." *Intelligent and Converged Networks* 1, no. 2 (2020): 199-220.

115. Alappatt, Valanto, and PM Joe Prathap. "Hybrid cryptographic algorithm based key management scheme in MANET." *Materials Today: Proceedings* (2020).

116. Kumar, Vipin, Navneet Malik, Gaurav Dhiman, and Tarun Kumar Lohani. "Scalable and storage efficient dynamic key management scheme for wireless sensor network." *Wireless Communications and Mobile Computing* 2021 (2021).

117. Patel, Harshita, Dharmendra Singh Rajput, G. Thippa Reddy, Celestine Iwendi, Ali Kashif Bashir, and Ohyun Jo. "A review on classification of imbalanced data for wireless sensor networks." *International Journal of Distributed Sensor Networks* 16, no. 4 (2020): 1550147720916404.

118. Rahman, Musfiq, and SrinivasSampalli. "An efficient pairwise and group key management protocol for wireless sensor network." Wireless Personal Communications 84, no. 3 (2015): 2035-2053.

119. Blom, R. (1985). An optimal class of symmetric key generation systems. In Proceedings of the EUROCRYPT 84 workshop on advances in cryptology: Theory and application of cryptographic techniques (pp. 335–338). New York, NY, USA: Springer-Verlag New York Inc.

Publications

1. Srivastava, G., Singh, J. N., & Manjul, M. (2021). Group key management: Issues and opportunities. Journal of Discrete Mathematical Sciences and Cryptography, 24(3), 787-795.

https://doi.org/10.1080/09720529.2020.1794518

2. Srivastava, G., Singh, J. N., & Manjul, M. (2022, April). A Critical Review On Cost Reduction Schemes in Hetregeneous Network. In 2022 2nd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE) (pp. 627-631). IEEE. ISBN (Online): 978-1-6654-3789-9

3. Srivastava, G., Singh, J. N., & Manjul, M. (2024). DyClust – A Hybrid Key Management Scheme for Wireless Sensor Network, SN Computer Science, DOI : 10.1007/s42979-023-02584-5.