International Journal of Engineering Science Invention
ISSN (Online): 2319 – 6734, ISSN (Print): 2319 – 6726
www.ijesi.org ||Volume 4 Issue 5 || May 2015 || PP.59-70

Energy Efficient Key Management Analysis using AVL Trees in Wireless Sensor Network

Usham Robinchandra Singh[1], Kh. Manglem Singh[2], Sudipta Roy[3]
[1]*(Department of IT, Triguna school of Technology, Assam University, India)*
[2]*(Department of Computer Science & Engineering, NIT Manipur, India)*
[3]*(Department of IT, Triguna school of Technology, Assam University, India)*

ABSTRACT *: Wireless sensor networks (WSNs) are deployed in hostile environments in many applications. In a wireless sensor networks, such regular topology patterns as Square, Hexagonal and triangle can fully cover the area, provides accurate positioning for abnormal event, and achieve better network performance than random topology. In order to resist security threats, sensor nodes of WSNs often use pre-shared secret keys to encrypt and exchange confidential data. Accordingly, designing key management protocols that can securely distribute secret keys among sensor nodes becomes an important issue for WSNs. The proposed scheme analyses a novel key management protocol for hierarchical WSNs based on hexagonal topology using AVL tree. In the proposed protocol, a WSN is viewed as a Hexagonal model. That is, cluster head node is represented as a vertex and center of the cluster head is represented as a cluster coordinator which is the communicator to Base station. This paper also presents dynamic insert and remove protocols. The dynamic insert protocol allows newly deployed sensor nodes to join an existing WSN while the dynamic remove protocol can delete compromised sensor nodes from a WSN. We apply our proposed calculations only to the mobile nodes because Cluster head, Cluster Coordinator, Base station have strong key security. Nodes are mobiles in nature, physical damage and capturing of one node may totally affect whole network. In LEACH, there is minimization of the nodes that are directly communicating with the base station (i.e. sink) to save energy. In our model, there is no scalability problem.*

KEYWORDS -*Hexagonal Topology, AVL Tree, Cluster Head, Wireless Sensor Network, Key Management.*

I. INTRODUCTION

WSN is a wireless network which is constituted by a large number of randomly distributed sensor nodes through self-organization and multi-hop way. In single–hop sensor network, the sensor nodes use single hopping in order to reach cluster head]. In multi-hopping, the sensor nodes use multi-hopping in order to reach cluster head [1]. In the multi-hopping sensor network, because of the relaying operation of passing the information from the far away sensor nodes to the nodes that are very close to the cluster head more energy has to be spend. In fact, Sensor networks are collection of sensor nodes which co-operatively send sensed data to base station [2]. A sensor network is densely deployed either inside the location where the operation is being performed or very close to it [3]. According with the network topology, it can be divided in two classes: the static WSN and the dynamic WSN. However, because of the wireless sensor nodes are often placed in dangerous environment, coupled with their own characteristics, especially mobility, WSNs are more vulnerable to attack compared with the traditional network such as physical attack and so on. Therefore with the broaden application areas, WSN's security become even more important. The energy-constrained nature of the sensor networks makes the task of incorporating security, a challenging problem. Most of the well-known security mechanisms introduce significant overhead and requires a lot of computation and communication resources. Since the design of security protocols for sensor networks should be geared towards resource conservation, the level of security versus the consumption of energy, computation, and memory resources constitute a design trade-off. Such resource-constrained environment has motivated extensive research that addresses energy efficient and energy aware hardware and software design issues [4]. Because of these characteristics more care has to be taken by the developers to develop a particular sensor network [2]. Most of the research effort has concentrated on energy efficient communication protocols [5][6][7]. Generally security protocols would provide the network with two-party encryption, authentication, and key management. In WSNs security, the key management problem is one of the most important and the most fundamental aspects. To achieve security in wireless sensor networks, it is important to be able to encrypt and authentication messages among sensor nodes. Before doing so, keys for performing encryption and authentication must be agreed upon by the communication nodes. In the architecture of a generic Wireless Sensor Network [8] we can examine how the clustering phenomenon is an essential part of the organizational structure.

• Sensor Node: A sensor node is the core component of a WSN. Sensor nodes can take on multiple roles in a network, such as simple sensing; data storage; routing; and data processing.

• Clusters: Clusters are the organizational unit for WSNs. The dense nature of wireless sensor networks requires the need for them to be broken down into clusters to simplify tasks such as communication [12].

• Cluster heads: Cluster heads are the organization leader of a cluster. They often are required to organize activities in the cluster. These tasks include but are not limited to data-aggregation and organizing the communication schedule of a cluster.

Cluster Coordinator: Cluster head coordinator is the communication relay center of cluster heads as there is nearly equal distance from each cluster head. Only one node called cluster coordinator is able to communicate with the base station.

• Base Station: The base station is at the upper level of the hierarchical WSN. It provides the communication link between the sensor network and the end-user.

• End User: The data in a sensor network can be used for a wide-range of applications. [8] Therefore, a particular application may make use of the network data over the internet, using a PDA, or even a desktop computer. In a queried sensor network (where the required data is gathered from a query sent through the network). This query is generated by the end user.

The clustering phenomenon as we can see, plays an important role in not just organization of the network, but can dramatically affect network performance. There are several key limitations in WSNs, that clustering schemes must consider. In order to enhance its security, many people proposed related authentication mechanisms and key management schemes, but these are usually for the fixed nodes. Solutions for the dynamic network efficient security options are less to be considered. Key management schemes are mechanisms used to establish and distribute various kinds of cryptographic keys in the network, such as individual keys, pair wise keys, and group keys. Key management protocols can be based on either symmetric or asymmetric management functions. But due to the scarcity of the resources, protocols based on public keys are inefficient. Hence, symmetric algorithm based key management schemes are favored in WSNs [9]. To achieve security in wireless sensor networks, it is important to be able to perform various cryptographic operations, including encryption, authentication, and so on. Keys for these cryptographic operations must be set up by communicating nodes before they can exchange information securely. Most security requirements, such as privacy, authenticity, and integrity, can be addressed by building on a solid key management framework. It actually helps in maintaining the confidentiality of secret information from unauthorized access. Furthermore, it is used for verifying the integrity of exchanged messages and authenticity of the sender. There are four types of key management schemes: trusted server, self-enforcing, key pre distribution and public key cryptography. When designing a key management scheme for WSNs, designers should take the following five major resource constraints of sensor nodes into consideration: (1) limited energy, (2) limited memory, (3) Limited computing power,(4) limited communication bandwidth, (5) limited communication range. The key management includes key generation, key distribution, and key storage. The enhanced key management in this version can perfectly eliminate the impacts of node compromise attacks on links between non-compromised nodes which most existing key management schemes have faced. Power consumed by the WSN is mainly due to network dynamics, node capabilities, data delivery model, energy consideration, data aggregation and network deployment [10]. Energy usage is an important issue in the design of WSNs which typically depends on portable energy sources like batteries for power [11]. Energy consumption in the clustering is measured as a fraction of total energy dissipated in the network [12]. The amount of power consumed by the SN depends on the nature of that application [3]. Clustering can be done in order to enhance the network life time. WSN are deployed in an Ad-Hoc manner and have large number of nodes [13]. Communication bandwidth can be conserved due to clustering; the size of the routing table can be reduced with the help of clustering. Topology maintenance can be cut because of clustering. The energy consumption can be reduced due to scheduling activities in the cluster, The battery life of the individual sensors and network can be extended due to clustering [14].The design attributes to be considered for clustering are number of clusters, intra-cluster communication, nodes and CH mobility, node types and roles, cluster head selection, multiple levels, overlapping [15].The issues in clustering the sensor networks are connectivity, rotating the role of cluster heads, MAC layer design, node duty cycle, optimal cluster size, node synchronization [13]. The collected data is fused each time when it travels from one node to another node [16]. The information gathered by the cluster head in the clustering is communicated to the data processing centre [17]. Two nodes are denoted as neighbors if they have a direct wireless link between each other. The number of neighbors of a node is denoted as its degree d [18]. The processing centre then analyses the information passed by the cluster head [17]. Several WSN applications require only an aggregate value to be reported to the observer. With the help of data aggregation, the life time of the WSN can be increased [15]. The consumption of power in a cluster depends on the distance between the two nodes. If the nodes are nearby, then less power is consumed.

But at the same time, if the distance between the nodes is large, then more power has to be consumed by the respective node. In order to overcome this drawback, individual nodes are requested to pass the information gathered by that node to the nearby node in a relay manner [19]. In this paper, we propose new model for wireless sensor network which can provide security authentication and dynamic key update in the initialization phase as well as network running phase, we can ensure the safety of the dynamic WSN. At the same time, this paper used AVL tree to achieve the key dynamic real-time update, while took advantage of the improved Hexagonal model using AVL tree to reduce the energy consumption of the network. The simulation results show that our scheme can ensure real-time network dynamic security in WSN, avoid conventional attacks such as replication attacks, and achieve the goal of energy efficiency. In this paper we only focus on the design of a low energy key management scheme using new network model for a sensor network. The rest of this paper is organized as follows. Section II summarizes related work. Section III demonstrates Key management in WSN. Section IV mention about clustering approach in key management in WSN. Section V discusses about role of binary tree called AVL tree. In section VI, we present network architecture and Assumption. Section VII evaluates the security of the proposed research work and a brief analysis is presented in Section VIII.

II. RELATED WORK

The distribution of symmetric keys is one of the main challenges in WSN. Many schemes were proposed in the literature. The simplest way is to let the network nodes share a single secret key. Unfortunately, the compromise of even a single node in a network would reveal the secret key and thus allow decryption of all network traffic. Yet another approach is the full pair wise scheme. This approach uses a shared unique symmetric key between each pair of nodes. This scheme is memory-intensive and does not scale up. Different key management protocols proposed on pair wise keying can be summarized as below [20]: 1) Eschenauer and Gligor [21] proposed a probabilistic key distribution scheme based on pair wise keying. Though it is robust and requires less storage it suffers from less authentication, low accessibility with no support to cluster operations [22]. . Moreover, Du et al. developed a pair wise key management scheme [23]. This scheme combines the random key pre-distribution scheme [24] and the Blom scheme [25] to substantially improve network resilience against node capture over existing schemes, without increasing the memory overhead. In order to find a scheme to support node mobility as well as reduce energy consumption, Chan, Perrig and Song [26] proposed a q-composite random key pre-distribution scheme. This scheme achieved security under small scale attack while trading off increased vulnerability in the face of a large scale physical attack on network nodes. Du, Dang, Han and Varshney [27] proposed a multi space key pre-distribution scheme where it used a number of private matrices instead of one and k key matrices in each node. In SPINS, proposed by Perrig et al, each sensor node shares a secret key with the base station. To establish a new key, two nodes use the base station as a trusted third party to set up the new key. The distribution of symmetric keys is one of the main challenges in WSN. Many schemes were proposed in the literature. The simplest way is to let the network nodes share a single secret key. Unfortunately, the compromise of even a single node in a network would reveal the secret key and thus allow decryption of all network traffic. Yet another approach is the full pair wise scheme. This approach uses a shared unique symmetric key between each pair of nodes. This scheme is memory-intensive and does not scale up. Kim proposed layer-based multiplex communication key management scheme in the literature [28], the program has reasonable routing load and lower mobile administrative overhead. A two-layer dynamic key management based on clustering supporting node mobility scheme is proposed by Chuang in wireless sensor networks [29]. Besides of that, a scheme proposed in the literature [30] supports node mobility based on polynomial key pre-distribution. The literature [31] proposed a method for authentication and key establishment real-time key generation scheme to reduce memory consumption and enhance the network fault tolerance. Camtepe and Yener proposed the combination design which is a key pre-distribution method [32]. Sanchez and Baldus improved the program [32], referred as the program [33] which can establish direct pair-wise key for a large number of physical connectivity independent sensor nodes in WSN. In order to reduce the memory load while supporting different network nodes mobility, Maerien [34] proposed a key management protocol in mobile wireless sensor network which is assigned to each node a symmetric key, and the key is just shared with its network back-end server, but the program needs to have a relationship of mutual trust between that nodes entered the network with its original network. Literature [35] proposed a mobile heterogeneous aware network key management scheme with high energy and memory utilization, reducing energy consumption and memory load during the network initialization phase, introducing a new common certification, ensuring network security and network connectivity as well as anti-aggressive, but sometimes the updates of keys do not in real-time. Our paper is not only taking the advantage with these schemes but also improving the security for the dynamic network while in the meantime reducing memory consumption. Blom's Scheme [36]: Blom presented a symmetric key generation system (SKGS) based on MD5. In a network of n users, where k users have to co-operate to get information, the public matrix P (n, k) over GF is known to all. The central authority chooses a symmetric secret matrix and computes the key and distribute to all users. Public matrix is constructed using linear Vandermonde matrix [37].

Reddy's scheme [37]: Instead of using Vandermonde matrix, [37] proposed to use a non–binary Hadamard's matrix as the public matrix. A Hadamard Matrix is a square matrix with values 1s and -1s. It reduces the complexity of calculating values of all the elements corresponding to the columns in Vandermonde matrix. Reddy used the same matrix by replacing the value of -1 with a large prime number p-1. However, one of the important mechanisms in sensor networks, in-network processing, is not considered in the previous schemes. So, hierarchical key management solutions are proposed as LEAP [38]. With the development of science and technology, cryptography has also been considerable development both in theory and in practice. For different applications, there are many different cryptography systems, such as the symmetric cryptography, public key cryptography and so on. All of these algorithms have the strengths and weaknesses in different applications, but we have not found that a theory which would be able to meet all application requirements in the WSNs. Security aspects of applications usually need to have better consideration more than the traditional network security. For example, how to deal with the relationship between the safety factor and energy consumption coefficient of various algorithms, how to choose a compromise to meet the needs of existing applications, all of these should be taken into consideration.

III. KEY MANAGEMENT IN WSN

Key is the most important component for most of the Cryptographic algorithms. Keys are generally numbers randomly selected from a large set of numbers. Management of these keys is very important in cryptography. Management of keys includes Key Generation which is the process in which a pool of key are generated by a central authority or by individual nodes and Key Establishment is the process by which right keys for right users can be determined and key rings for each user are sent to them accordingly. Key establishment can be done in many ways. Trusted Authority can help in sending the keys to each user through a secure channel. But this mechanism is a costly one and does not suit for sensor networks. So, in sensor networks Key Pre-distribution is used in which key rings are installed in the nodes before deployment of network in offline mode**.** [39] Key establishment process in Wireless sensor networks mainly consists of three phases.

(i)Key pre-distribution: Pre-loading keys in sensor nodes prior to deployment. The keys present in a sensor node constitute the key ring of the sensor. The key ring of each node, a random subset of m keys from the key pool is stored on the memory of each node before deployment.

(ii)Shared key discovery: After the nodes are deployed, a shared key discovery phase is performed, where two neighbor nodes find out their common key in their key rings and use it as a shared key. Each node broadcast key identities in its key to discover a common key with neighbor nodes.

(iii)Path key establishment: After a shared key discovery phase, if two nodes do not have a common key, then a path key establishment phase is performed between the two nodes [40].

If a common key does not exists, then a path has to be found between the communicating nodes. A path key is then established between the communicating nodes. In Key Pre-Distribution scheme, secret keys are placed in sensor nodes before deployment. When the nodes are deployed over the target area, the secret keys are used to create the network. Traditionally, key management protocols can be classified into three categories:

1. Symmetric key based key management protocol. The communication entities use a pre-shared symmetric key to negotiate a temporary session key. Then, they use this session key to encrypt messages and authenticate one another.
2. Asymmetric key based key management protocol. Each communication entity has its own public key and private key pairs. The communication entities may apply signature schemes (Rivest, Shamir, & Adleman, 1978) to authenticate each other and utilize the Diffie-Hellman key exchange scheme (Diffie & Hellman, 1976) to produce the session key for secure communications.
3. Trusted third party based key management protocol. Each communication entity shares a symmetric key with a trusted third party. Then, the communication entities can achieve mutual authentication and secure communication through the trusted third party's assistance.

Reviewing the above categories of key management protocol, symmetric key based key management protocols are more suitable for WSNs than the other categories. Due to the resource constraints of sensor nodes, asymmetric key based key management protocols are too complex and energy consuming for WSNs. This is because they require exponential computations. On the other hand, the sensor nodes are often spread in wide area so that many sensor nodes may be deployed too far away to communicate with the trusted third party. Therefore, trusted third party based key management protocols are also hard to implement in WSNs. The most common network architectures of WSNs are flat WSNs and hierarchical WSNs (Shen, Guo, & Leung, 2009). All senor nodes play the same role in a flat WSN. Under this architecture, a sensor node may randomly select a neighbor node to forward the data. Thus, the data transmission path may not be fixed. Nevertheless, a hierarchical WSN requires some special sensor nodes, called Cluster Head (CH). A CH is a data collection center of a small region in a WSN. Under this architecture, each sensor node can forward data to its local CH in a short distance, and then the CH forward collected data to the BS using a fixed path via other CHs. The manuscript (Cheng & Agrawal, 2007) showed that the communication of a hierarchical architecture is better than a flat architecture in WSNs. Therefore, several recent studies focus on designing key management protocols of hierarchical WSNs. Among all security issues, key management has become a challenging issue in the design and deployment of secure wireless sensor networks. Key management is a fundamental cryptographic primitive upon which other security primitives are built. It contains two parts: key distribution and key revocation. Key distribution refers to the task of distributing secret keys between communicating parties to provide secrecy and authentication. Key revocation refers to the task of securely removing compromised keys. By revoking all of the keys of a compromised sensor node, the node can be removed from the network. Compared to key distribution, key revocation has received very little attention. Therefore, designing secure key management protocols for WSNs is a desirable task that attracts many cryptographers. Some typical security requirement and goals for Key Management are

1. The scheme must work without prior knowledge of which nodes will come into communication range of each other after deployment.
2. Deployed nodes must be able to establish secure node-to-node communication.
3. Node addition / deletion should be supported.
4. Unauthorized nodes should not be allowed to establish communication with network nodes [41].
5. The protocol must establish a key between all sensor nodes that must exchange data securely
6. Additional legitimate nodes deployed at a later time can form secure connections with already deployed nodes.
7. Unauthorized nodes should not be able to take entry into the network or become members of the network.
8. Sensor nodes have limited resources so computational and storage requirements of the scheme must be low.
9. If a node becomes compromised, the key management scheme must be able to securely remove the compromised node from the network.

IV. CLUSTERING APPROACH IN KEY MANAGEMENT IN WSN

Energy efficient in the WSN can be achieved by considering energy conservation mechanism, power conservation mechanism, energy harvesting mechanism and energy efficient routing, and energy efficient key management mechanism. Clustering protocols improve the lifetime and energy consumption of the network. Since there is no addressing scheme for sensor network like IP- addresses, location information can be utilized in routing data in an energy efficient way. Single hop node transmits to the cluster head directly. By using efficient key management, we can minimized CH load when mobile nodes insertion or deletion of nodes. It means it is not necessary transmission of unnecessary data to cluster head. . Moreover, Power in each node will be depleted very quickly if each node in the cluster sends its data or information directly to the base station. Therefore, Cluster formation is important factor to save energy as well as reuse of resources. The purpose of the LEACH is to minimize the nodes that are directly communicating with the base station (i.e. sink). But in Power Efficient Gathering in Sensor information systems (PEGASIS), only one node can be able to communicate with the base station. That is, the cluster head coordinator only conveys the information to the base station. The cluster heads from various clusters convey the information to the cluster head coordinator in a chain manner [42]. The information collected from each and every node is combined by the other nodes and finally the Cluster head node only transmits the collected information to the base station. The information collected from each and every node is combined by the other nodes and finally the Cluster head node only transmits the collected information to the base station. Some of the advantages of PEGASIS are:

(i) The distance between the base station and CH has been reduced when compared to LEACH.
(ii) The messages conveyed to each node are 2 (at the maximum) when compared to LEACH.
(iii) The energy consumption is uniform in PEGASIS.
(iv) The number of transmitting and receiving information is limited.

The drawbacks of the PEGASIS are:-

(i) The energy level of the cluster head has not been considered
(ii) The data transmission to the base station may be redundant in nature, because the CH alone convey the message to the base station [43].

Energy efficient of LEACH is improved by two types of clustering algorithm. They are 1) LEACH-C 2) SECA. In SECA, the cluster head selection is based on the amount of residual energy present in the node.

V. ROLE OF SELF-BALANCING BINARY TREE—THE AVL TREE IN HEXAGONAL NETWORK TOPOLOGY

Nowadays, in the network system design, we often need to find relevant information in large amounts of data, such as determining whether an element is presented in the data set; accessing to the specified value lower bound and so on. Different search ways have various performances. Self-balancing binary search tree is a better relative performance search way. It has effectively insert operation tree appropriate treatment in order to control the height of the tree. The most common self-balancing binary search tree is the AVL tree and red-black tree. Red-black tree is more complex than the AVL tree. Our scheme is learned from the concept of AVL tree. The maximum difference height of any two different nodes in the two AVL sub trees is 1, so it is also called a high degree balanced tree. The average time for search, insert, and delete operations and the time of the worst case of the tree are O (log n). When execute the insert or delete operation, it may be necessary to re-adjust the angle of one or more sub trees. The balance factor of a node is the difference between the height of the right sub tree and the left sub tree. When a node of the balance factor of 1, 0 or -1, it is considered that the node is balanced, of course the node for other values is imbalanced which need to re-adjust the angle. Generally speaking, the balance factor can be directly stored in each node, or may be stored in the nodes in the sub-tree height calculated [44]. These balance factors can be used in our purpose Hexagonal topology of network using AVL tree. As the AVL tree node position can be adjusted dynamically, this feature can be applied to support dynamic data management mechanism. Due to the node addition and deletion or nature of distribution of nodes, structure of one cluster head may or may not equal storage of Balance factor. Therefore, In the program, during the network stable operation, the key real-time update takes the advantage of this concept, letting each cluster into a virtual self-balancing binary search tree, and then get the node's corresponding key in the tree, ensuring key real-time updates while reducing the energy consumption of the respective nodes.

VI. NETWORK ARCHITECTURE AND ASSUMPTIONS

In our paper we are going to present a security scheme for wireless sensor networks based on public key cryptography as a tool for managing mutual authentication between sensors and the base station. Public key cryptography is used in our proposed scheme to guaranty the authentication of the base station since only the base station has a pair of asymmetric keys (private, public), the public key is preloaded for each sensor over the network before deployment, this key is used by sensors to authenticate the base station and secure the handshake, which guaranties the integrity and the confidentiality of all dialogues with the base station, since only the base station has the valid private key for decryption. The network model of this proposed scheme is mainly consisted with four types of nodes which randomly distributed in the network. In this network architecture, Cluster based network approach is used. Nodes are divided as Base station, cluster head coordinator, Cluster head and member nodes. Every cluster head knows its members. Base station has all information about network. The level of authentication responsibility is like member nodes are verified by respective cluster heads and cluster head is verified by base station via Cluster coordinator.

In order to implement this security scheme we assume that:

1. The base station have more computational and energy power compared to sensors.
2. Only one node called cluster coordinator is able to communicate with the base station.
3. The base station has a pair of keys (private and public key).
4. Cluster head coordinator is taken at the center of the hexagonal AVL network model.
5. Cluster coordinators have same distance with all the Cluster head.
6. Each sensor is capable to use:
    a. Asymmetric Cryptography: To provide authentication of the base station.

    b. Symmetric Cryptography: To ensure the confidentiality of traffic across the network.
7. MAC (message authentication code) to ensure data integrity.
8. Each sensor has the capacity to save at least the public key of the base station and one or more symmetric keys used for data encryption.
9. Each sensor receives the public key of the base station by an off-line dealer.

VII. THE PROPOSED RESEARCH WORK INVOLVES

Based upon number of nodes and number of clusters heads a network model is formed and further Verification of Common pair nodes will be carried out on this network itself. For Ex we consider network model as,

a. Network Model for explanation.
b. Finding secure parameter t=6 and prime number (q) =31 based on number of node and Connectivity matrix.
c. Calculation of common key pair.

We can develop sparse Hexagonal Matrix using AVL tree model for easy efficient key management process in the Energy saving wireless sensor network. The research work includes the model of wireless sensor network. The clustering approach of network is used here. Cluster head using Hexagonal topology can be applied using AVL tree where each vertex represent cluster head nodes. So we need to arrange those balance factors according to the purpose model given below. The network is divided into base station, cluster coordinator, cluster heads and member nodes. Base station is powerful and has information of total network. The network is divided into clusters. Each cluster has limited nodes. Each cluster has one cluster head. There is only cluster coordinator for this Hexagonal type of topology. Each cluster head communicates with the Cluster coordinator. All the information is sent to the base station by Cluster coordinator. The verification (authentication) of any sensor node of particular cluster is done by respective cluster head. Verification of cluster coordinator will be done by Base station. Each node knows its immediate neighbours. If certain attack occurs on the network, base station will alert to network especially to particular Cluster coordinator. Cluster coordinator then carries verification for that cluster head and don't allow it to enter the network. Thus network will be secured. We make a matrix from each cluster head node of hexagonal type of topology where each cluster head node represent parent of the AVL tree. Therefore possible Balance factor of each cluster head are 0, 1 and -1 according to type of distributed nodes attach to the corresponding Cluster head. In a distributed network, nodes are distributed unequal hop distances between the nodes. Therefore it is not comfortable to use complete Binary tree. Arrangement of matrix elements can be in many ways, but we make matrix elements according to our purpose diagram. If we modify Hadmard Matrix using balance factor in such a fashion that 0, 1, -1 are distributed alternately. Cluster head are making in a manner of hexagonal network topology where each vertex of hexagonal cell represent cluster head so that maximum suitable cluster node are at least six. Sparse matrix with greater number of zeroes has lesser computation. Distribution of zeroes in each vertex of Hexagonal shape network contributes good network as well as energy efficiency in the key management process. Using inter cluster communication is very effective than nodes to nodes communication. We take cluster coordinator in the middle of hexagonal network because it has nearly equal hop from every cluster node. Cluster coordinator will contact Base station to give all the detail information of clusters. Cluster coordinator will not take any responsible of the distributed tree network. Energy efficient key management is depending upon the efficient network arrangement, special distribution of sensor nodes, cluster node, coordinator cluster nodes.

Let n be the value of cluster head node in the proposed work, so that value of balance factor f(n) may be 1,-1,and 0 according to type of member nodes attach to each cluster head.

$$f(n) = \begin{cases} 1 & \text{if balance factor is } 1 \\ -1 & \text{if balance factor is } -1 \\ 0 & \text{if balance factor is } 0 \end{cases}$$

In our Proposed Scheme, the public matrix as chosen by taking t (secure parameter) rows from an N x N Hadamard matrix which contains 1 and -1, we convert it into a sparse Hadamard matrix H, with the following modification:

1. The matrix elements that is 1 and -1 given in the Hadamard are added by one of the balance factor that by 1, -1 and 0.

2. After taking 2 modulo in the result of addition, we get one matrix of the form given below

$$\begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 1 & 0 \end{bmatrix}$$

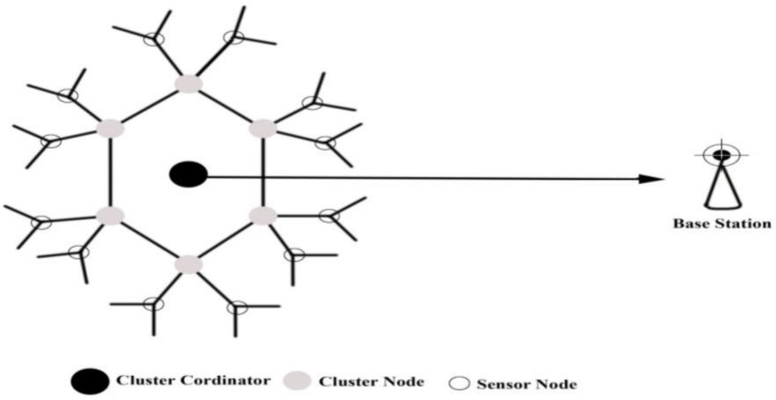

Figure 1: Existing model for explanation.

Example: The following example shows the working of our scheme - the sparse Hadamard matrix. Let the number of nodes in the network be 8, secure parameter t = 6.

Hadamard Matrix:

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \\ 1 & 1 & 1 & 1 & 1 & -1 & 1 & -1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\ 1 & 1 & -1 & -1 & -1 & -1 & -1 & 1 \\ 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 \end{bmatrix}$$

Modified Hadamard Matrix (by Reddy):

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 30 & 1 & 30 & 1 & 30 & 1 & 30 \\ 1 & 1 & 30 & 30 & 1 & 1 & 30 & 30 \\ 1 & 30 & 30 & 1 & 1 & 30 & 30 & 1 \\ 1 & 1 & 1 & 1 & 1 & 30 & 1 & 30 \\ 1 & 30 & 1 & 30 & 30 & 1 & 30 & 1 \\ 1 & 1 & 30 & 30 & 30 & 30 & 30 & 1 \\ 1 & 30 & 30 & 1 & 30 & 1 & 1 & 30 \end{bmatrix}$$

Sparse Hadamard Matrix (Proposed):

$$\begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 1 & 0 \end{bmatrix}$$

$$\text{Public Matrix (P)} = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 1 & 0 \end{bmatrix}$$

Let the secret matrix (S) be:-

$$S = \begin{bmatrix} 3 & 11 & 15 & 28 & 7 & 5 \\ 11 & 30 & 4 & 1 & 2 & 8 \\ 15 & 4 & 6 & 14 & 18 & 21 \\ 28 & 1 & 14 & 17 & 25 & 6 \\ 7 & 2 & 18 & 25 & 27 & 9 \\ 5 & 8 & 21 & 6 & 9 & 8 \end{bmatrix}$$

$$P = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 1 & 0 \end{bmatrix}$$

$A = (S.P)^T$

$$S.P = \begin{bmatrix} 59 & 10 & 5 & 66 & 33 & 46 \\ 43 & 13 & 8 & 45 & 9 & 16 \\ 45 & 33 & 21 & 63 & 35 & 35 \\ 38 & 53 & 6 & 63 & 23 & 59 \\ 54 & 34 & 9 & 81 & 34 & 50 \\ 43 & 14 & 8 & 52 & 14 & 32 \end{bmatrix} \quad \text{mod } 31$$

$$A = (S.P)^T = \begin{bmatrix} 59 & 43 & 45 & 38 & 54 & 43 \\ 10 & 13 & 33 & 53 & 34 & 14 \\ 5 & 8 & 21 & 6 & 9 & 8 \\ 66 & 45 & 63 & 63 & 81 & 52 \\ 33 & 9 & 35 & 23 & 34 & 14 \\ 46 & 16 & 35 & 59 & 50 & 32 \end{bmatrix}$$

The rest of whole Blom's scheme and its modified version by Reddy remain same as described by [37]. Now, suppose node 3 and 4 want to communicate, then the key used by both will be

$$K1 = A3 * P4$$

$$A3=\begin{bmatrix}5 & 8 & 21 & 6 & 9 & 8\end{bmatrix}\begin{bmatrix}0\\1\\1\\1\\1\\1\end{bmatrix}$$

=52 mod 31=21

K2= A4 *P3

$$K2=\begin{bmatrix}66 & 45 & 63 & 63 & 81 & 52\end{bmatrix}\begin{bmatrix}0\\0\\0\\0\\0\\1\end{bmatrix}$$

= 52 mod 31=21

Thus we observe that both the nodes generate a common pair-wise key that will be use for communication. Now if we compare our scheme with that of Blom's, we observe that we can reduce computation time by eliminating operations on zero elements. Also if we follow the steps of Blom's scheme to pre allocate each of the columns of public matrix (Hadamard matrix) to different nodes according to their index then we can reduce space requirements by taking advantage of the properties of sparse matrix. In Blom's scheme, we require a space proportional to t to save the column of the public matrix in the node where as in our scheme; we require the space proportional to the number of non-zero elements in that column. If we compare our scheme to that of Reddy's that favors to generate the public matrix at the node itself rather than storing it in advance, then too our scheme takes the advantage by reducing computation time by eliminating operations on zero elements.

VIII. ANALYSIS

Converting the public matrix to a sparse matrix by replacing nearly half of its elements with **0** serves the following purposes:-

1. Using sparse matrix to store data that contains a large number of zero-valued elements can both save a significant amount of memory and speed up the processing of that data.

2. Store only the nonzero elements of the matrix, together with their indices. Thus, Number of bytes of memory stored is much less in sparse matrix**.**

3. In this case, we require even more reduced space proportional to non-zero elements in that column.

4. Reduce computation time by eliminating operations on zero elements.

IX. CONCLUSION

Our scheme enhances Blom's scheme by minimizing the storage required by using a modified sparse Hadamard matrix & eliminates the run time generation of public matrix to save the computational time & computational energy of the energy scarce sensor nodes. The wireless communication cost is decreased by the reduction of the data packets, and the clustering protocols improve the lifetime and the energy consumption of the networks by data aggregation in wireless sensor networks. However, we have only taken the dynamic WSNs in the consideration. In this paper, we proposed a novel key management scheme for dynamic WSNs security using balance factor in hexagonal network topology. Simultaneously, during the node dynamic update stage, we add the idea of the self-balanced binary search tree to ensure the dynamic security of the network while reduce the entire cluster node energy consumption.

REFERENCES

[1] Vivek Mhatre, Catherine Rosenberg, “Homogeneous vs Heterogeneous Clustered Sensor Networks: A Comparative Study”,

[2] Nandini. S. Patil, Prof. P. R. Patil, “Data Aggregation in Wireless Sensor Network”, 2010 IEEE International Conference on Computational Intelligence and Computing Research.

[3] I.F. Akyildiz, W. Su*, Y. Sankarasubramaniam, E. Cayirci, “ Wireless sensor networks: a survey”, Computer Networks 38 (2002) 393–422,

[4] S. Hollar, ―COTS Dust,‖ Master's thesis, Electrical Engineering and Computer Science Department, UC Berkeley, 2000.

[5] M. Younis, M. Youssef, and K. Arisha, ―Energy-Aware Routing in Cluster-Based Sensor Networks,‖ in Proceedings of the 10th IEEE/ACM International Symposium on Modeling, Analysis and Simulation of Computer and Telecommunication Systems (MASCOTS2002), (Forth Worth, TX), October 2002.

[6] V. Raghunathan, C. Schurgers, S. Park, and M. B. Srivastava, ―Energy Aware Wireless Microsensor Networks,‖ IEEE Signal Processing Magazine, March 2002.

[7] E. Shih, B. Calhoun, S.-H. Cho, and A. Chandrakasan, ―Energy-Efficient Link Layer for Wireless Microsensor Networks,‖ in Proceedings of the Workshop on VLSI 2001 (WVLSI '01), (Orlando, Florida), April 2001.

[8] I. F. Akyildiz,W. Su, Y. Sankarasubramaniam, and E. Cayirci, “A Survey on Sensor Netowrks,” IEEE Communications Magazine, vol. 40, no. 8, pp. 102–114, Aug 2002.

[9] G.J. Pottie, W. J. Kaiser, “Wireless Integrated Network Sensors”, in communications of the ACM, 2000, vol 43(5) pages 51-58.

[10] Maytham Safar, Hasan Al-Hamadi, Dariush Ebrahimi, “PECA:Power Efficient Clustering Algorithm for Wireless Sensor Networks”, International Journal of Information Technology and Web Engineering, 6(1January-March 2011, pages 49 -58.

[11] Vinay Kumar, Sanjeev Jain and Sudarshan Tiwari, “Energy Efficient clustering Algorithms in Wireless Sensor Networks: A Survey, IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 5, No 2, September 2011, pages – 259 – 268.

[12] D. J. Dechene, A. El Jardali, M. Luccini, and A. Sauer, “A Survey of Clustering Algorithms for Wireless Sensor Networks”,

[13] Ossama Younis, Marwan Krunz, and Srinivasan Ramasubramanian, University of Arizona, “Node Clustering in Wireless Sensor Networks: Recent Developments and Deployment Challenges, IEEE Network • May/June 2006, pages 20-25.

[14] Vivek Katiyar, Narottam Chand, Surender Soni, , “A survey on Clustering Algorithms for heterogeneous wireless sensor Networks” , Int. J. Advanced Networking and applications Volume: 02, Issue: 04, Pages: 745-754 (2011)

[15] Srie Vidhya Janani. E, Ganeshkumar.P, Vasantha Suganthi.G, Sultan.M, Kaleeswaran. D, “A Survey on Algorithms for Cluster Head Selection in WSN”, International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 2, No 5, May 2013.

[16] Huseyin O¨ zgu¨r Tan and I˙brahim Ko¨rpeogˇlu, “Power Efficient Data Gathering and Aggregation in Wireless Sensor Networks”

[17] C.E.Nishimura and D.M.Conlon, “IUSS dual use: Monitoring of whales and earthquakes using SOSUS,” Mar. Technol. Soc. J., vol. 27, no. 4, 1994.

[18] Bettstetter, C., "The cluster density of a distributed clustering algorithm in ad hoc networks," Communications, 2004 IEEE International Conference on , vol.7, no., pp.4336,4340 Vol.7, 20-24 June 2004.

[19] Jong-Shin Chen,Zeng-Wei Hong ,Neng-Chung Wang, “Efficient Cluster Head Selection Methods for Wireless Sensor Networks”, JOURNAL OF NETWORKS, VOL. 5, NO. 8, August 2010, pages 964-970.

[20] Rohithi Singh Reddy, “Key management in wireless sensor networks using a modified Blom scheme”, arXiv:1103.5712.

[21] L. Eschenauer, V. Gligor, “A key management scheme for distributed sensor networks”, in ACM CCS2002, Washington D.C 2002.

[22] J.C. Lee, V.C.M. Leung, K.H. Wong, J. Cao, H.C.B. Chan, “ Key Management Issues In Wireless Sensor Networks: Current Proposals And Future Developments”,in IEEE Wireless Communications, October 2007.

[23] W. Du, J. Deng, Y. S. Han, and P. K. Varshney, “A pairwise key predistribution scheme for wireless sensor networks”, in Proceedings of the 10th ACM Conference on Computer and Communications Security (CCS), Washington DC, USA, 2003, pp. 42–51.

[24] L. Eschenauer, V.D. Gligor, “A key management scheme for distributed sensor networks”, in: Proceedings of the 9th ACM Conference on Computer and Communication Security. November 2002, pp. 41–47.

[25] R. Blom, “An optimal class of symmetric key generation systems,” Advances in Cryptology: Proceedings of EUROCRYPT 84, Lecture Notes in Computer Science, Springer-Verlag, 1985, 209:335–338.

[26] H. Chan, A. Perrig, D. Song, “ Random key pre-distribution schemes for sensor networks”, in proceedings of the 2003 IEEE Symposium on Security and Privacy, May 11-14, 2003, p. l97.

[27] W. Du, J. Deng, Y. S. Han, S. Chen, P. K. Varshney, “ A keymanagement scheme for wireless sensor networks using deployment knowledge” , in IEEE INFOCOM 2004, Hong Kong,March 2004.

[28] K. T. Kim, R. S. Ramakrishna, “A Level-based Key Management for both In-Network Processing and Mobility in WSNs”, IEEE Internatonal Conference on Mobile Adhoc and Sensor Systems, MASS 2007, (2007) October 8-11, pp. 1-8.

[29] I. -H. Chuang, W. -T. Su, C. -Y. Wu, J. -P. Hsu and Y. -H. Kuo, “Two-Layered Dynamic Key Management in Mobile and Long-Lived Cluster-Based Wireless Sensor Networks”, Wireless Communications and Networking Conference, WCNC 2007, IEEE, (2007) March 11-15, pp. 4145-4150.

[30] C. Blundo, A. De Santis, A. Herzberg, S. Kutten, U. Vaccaro and M. Yung, “Perfectly Secure Key Distribution for Dynamic Conferences”, (1992) pp. 471–486.

[31] S. U. Khan, L. Lavagno, C. Pastrone and M. Spirito, “An effective key management scheme for mobile heterogeneous sensor networks”, 2011 International Conference on Information Society (i-Society), (2011) June 27-29, pp. 98-103.

[32] S. A. Camtepe and B. Yener, “Combinatorial Design of Key Distribution Mechanisms for Wireless Sensor Networks”, Networking, IEEE/ACM Trans. on, vol. 15, no. 2, (2007) April, pp. 346-358.

[33] D. S. Sanchez and H. Baldus, “A Deterministic Pairwise Key Pre-distribution Scheme for Mobile Sensor Networks”, SecureComm 2005, First International Conference on Security and Privacy for Emerging Areas in Communications Networks, (2005) September 5-9, pp. 277- 288.

[34] J. Maerien, S. Michiels, C. Huygens and W. Joosen, “MASY: MAnagement of Secret keYs for federated mobile wireless sensor networks”, Wireless and Mobile Computing, Networking and Communications (WiMob), (2010) October 11-13, pp. 121-128.

[35] S. U. Khan, C. Pastrone, L. Lavagno and M. A. Spirito, “An Energy and Memory-Efficient Key Management Scheme for Mobile Heterogeneous Sensor Networks”, 2011 6th International Conference on Risks and Security of Internet and Systems (CRiSIS), (2011).

[36] R. Blom, “ An optimal class of symmetric key generation systems”, in: Proc. Of EUROCRYPT '84, pages 335-338.

[37] Rohithi Singh Reddy, “Key management in wireless sensor networks using a modified Blom scheme”, arXiv:1103.5712.

[38] S. Zhu, S. Setia, and S. Jajodia, “LEAP: Efficient security mechanisms for large-scale distributed sensor networks”, In ACM CCS 2003, October 2003, pp. 62–72.

[39] Ubuntu Operating System,http://www.paulcolmer.co.za/index_files/page0006.htm.

[40] http://blog.millennialnet.com/2011/06/30/good-wireless-sensor-network/, "Good Wireless Sensor Network".

[41] Chiara Buratti ,et.al. "An Overview on Wireless Sensor Networks Technology and Evolution" ,WiLAB, DEIS at University of Bologna, Bologna, Italy.

[42] Jong-Shin Chen,Zeng-Wei Hong ,Neng-Chung Wang, “Efficient Cluster Head Selection Methods for Wireless Sensor Networks”, JOURNAL OF NETWORKS, VOL. 5, NO. 8, August 2010, pages 964-970.

[43] S. U. Khan, L. Lavagno, C. Pastrone and M. Spirito, “An effective key management scheme for mobile heterogeneous sensor networks”, 2011 International Conference on Information Society (i-Society), (2011) June 27-29, pp. 98-103.

[44] D. E. Knuth, “Sorting and Searching”, vol. 3 of The Art of Computer Programming, section 6.2.2, Reading, Massachusetts: Addison-Wesley, second ed., (1997), pp. 430–31.