www.ijecs.in
International Journal Of Engineering And Computer Science ISSN: 2319-7242
Volume 5 Issues 7 July 2016, Page No. 17297-17305

Clustered Key Management Scheme to Maximize Life of Wireless Sensor Networks

K Vimal Kumar Stephen[1], Mathivanan V[2]

1. Research Scholar, Computer Science and Engineering Department
AMET University, Chennai, India,
nads74@yahoo.com
2. Research Supervisor, Computer Science and Engineering Department
AMET University, Chennai, India.
vmathivanan@yahoo.com

ABSTRACT - **A WSN typically has no infrastructure. It is composed of number of sensor nodes works together to monitor an environment to obtain data about it. Structured and unstructured are the two types of WSNs. An unstructured WSN contains a dense collection of sensor nodes. These sensors are small, computing resources, with limited processing and they are inexpensive. It can sense, measure, and gather information from the environment based on some local decision process; they can transmit the sensed data to the user. Security and lifetime of a sensor node in a network plays an important role.**

Keywords – Sensor Networks, mobile sink, clusters

I. INTRODUCTION

In sensor networks, the data are very crucial and to maintain secrecy in data communication is a toughest task. The process of establishing an authentication and secured communication could be achieved by a suitable key management scheme plays an important role in current scenario of security. A hierarchical sensor network consists of base station, cluster head and sensor nodes and it consists of three keys namely public and private key, cluster key and group key. In the research, Public-private key is employed for encryption and decryption, cluster key is for intra cluster communication and group key id for inter cluster communication should be shared among all members in the group in order to multicast information among a certain group securely.

Every data packages must be encrypted with a shared group key before transmitting. Only the users with the shared key can decrypt these packages and get the data. Then the illegitimate user can decrypt the package without the key. Designing any kind of secure key management scheme requires a secret to set up a trust relationship between two or more communicating parties. Hence, the communication among the members in the group can be said to be secure.

Network lifetime has become an important challenge for evaluating sensor network [1, 2, and 3]. Sensor coverage, connectivity and node coverage play a key role in deciding the lifetime of the sensor network. There are also several other factors that determine the lifetime of a sensor network like mobility, heterogeneity, quality of service and completeness. Many routing algorithms were proposed for energy efficiency to improve the lifetime of wireless sensor network (WSN). In the scenario of energy efficiency, wireless sensor network encounters loss of battery power during communication. Sensor node (SN) senses the data in the environment and transmits to the base station (BS) through the cluster head. Battery is drained when the data is sensed and also during transmission of sensed data. The battery is drained in cluster head during computation of keys and data transmission.

The issue present here is during data transmission from one sensor node to another sensor node, it takes more hops to reach cluster head/other sensor node/base station hence the energy is drained to the maximum. In order to retain the energy of the cluster head, energy efficient cluster based scalable key management technique has been proposed with mobile sinks to increase the lifetime of the cluster head which in turn increasing the lifetime of the network. Also routing path may differ when transmission of data takes place from sensor to BS. If the path is so long and large number of SN involved in transmitting the data and then this process repeats, it leads to energy depletion. The lifetime of the network increases when the route to transfer the data is optimal.

II. LITERATURE SURVEY

Efficient Group Key Management using Symmetric Key and Threshold Cryptography scheme [1] considers a hierarchical cluster structure of sensor network adopts the pair-wise group key management and keys are updated periodically. It prevents dangerous attacks from malicious nodes and mitigates the node compromise. The communication overhead is negligible for keys establishment with low memory overhead and energy savings. In this research, energy savings increase the network lifetime and achieves efficient security with low key storage overhead.

Weight-balanced 2-3 tree [2] is proposed to address the balance between security and limited resources is formed in every subgroup. Maximum Distance Separable (MDS) code technique is used to distribute the multicast key dynamically. The superior problem is to solve security. This method takes advantage of both centralized and distributed key group management method which is organized as irregular tree and every subgroup is organized as a weight-balanced 2-3 tree. This method shows superiority on security, scalability and performance.

Blind factor is used to compute group key in this method [4] that ensures an attacker will not be able to get the group key when the cluster head broadcasts the group key. MAC is used along with the partial keys to guarantee authentication. Group key is generated by using partial keys in this research. The energy consumption is very small compared to the total available energy for generating the partial keys and the group key.

Many efforts have been made for energy efficiency of WSNs [1, 6] and many researchers focused on next hop selection strategies such as one-hop neighboring nodes or multiple links for transmitting data [7–9]. Some researchers focused on scheduling the nodes. An efficient routing metric used in taking the selection of next hop. Recently, two categories of routing methodologies were attractive, Cluster based and Virtual backbone based. Cluster based protocols [4, 5, 6, 7] uses single-hop communication model, each sensor node sends packet to its cluster head directly in a single hop and the cluster head transfers the sensed data to the cesspool. The existing solution for clustering requires maintenance to reorganize the clusters due to mobility and node failures.

Virtual backbone can be produced by different algorithms [8, 9,10] to organize node in a better way. A backbone is a subset of active nodes that are able to perform a special task and serve nodes which are not in the backbone. A backbone reduces the operating cost involved in the communication between sink and other sensor nodes, decreases the overall energy consumption of each parcel and also increases the network lifetime in WSN.

A new algorithm called Connecting Dominating Set Augmentation (CDSA) [11] is proposed to construct a 2-connected virtual backbone which can resist the failure of one wireless node. CDSA has guaranteed quality by proving that the size of the CDSA constructed 2-connected backbone is within a constant factor of the optimal 2- connected virtual backbone size. Through extensive simulations, we demonstrate that in practice, CDSA can build a 2-connected virtual backbone with only small overhead.

The problem of constructing fault-tolerant CDS [12] in homogeneous wireless networks is investigated, which is abstracted as the minimum connected dominating set problems. A constant factor polynomial-time approximation algorithm is computed and this algorithm works for any abstract graph without the information of geometric coordinates of the input graphs. The property of UDG is used in the analysis part to get a constant approximation. Also investigated a constant factor approximation algorithm for k>=3 and m>=1 in a disk graph. Multipath transmission is proposed [13] enables fast transmission and coverage metric proved in this research yields maximum lifetime in the network**.**

III. ENERGY EFFICIENT AND CLUSTER BASED SCALABLE KEY MANAGEMENT TECHNIQUE TO IMPROVE THE LIFETIME

This section represents the proposed system architecture, features and implementation techniques. Considers a cluster structure of sensor network is illustrated in Figure 1.

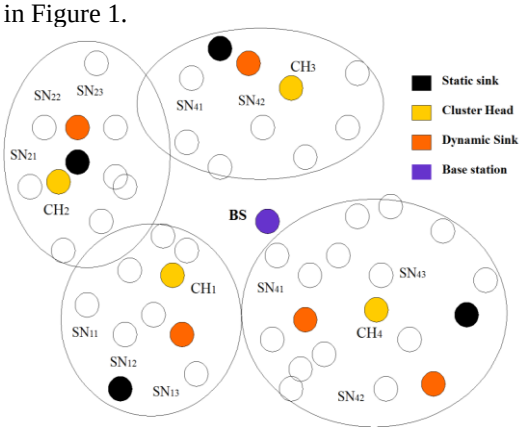

Figure 1 Proposed architecture

In figure 1, SN_{11},SN_{12}….SN_{ij} represents number of sensor nodes in the cluster(i represents cluster and j represents sensor nodes , CH_1,CH_2…..CH_n represents number of Cluster Heads (CH_i) in a network and base station is represented by BS. Clusters are formed based on the transmission range.

A. Trustworthy Base Station (BS) with unlimited resources is located in a safe place. BS has authentication system for any node in the network, a sensor node table of all nodes in the network and an intrusion detection system.
B. Cluster head (CH) is purely responsible for collecting sensed data within a cluster and sends to the BS.
C. Sensors node (SNs) senses the information of an environment and transmits to the CH.

Initially, sensor nodes are dynamic after deployment during the network operation. Cluster head is also dynamic which can be chosen by cluster head formation algorithm. Initially the cluster head is chosen among on sensor node which is having highest battery power. The new cluster head is selected by the algorithm only when the already exiting cluster head reaches the threshold value. Before sending the sensed data, the sensor node enters in to the network should be authenticated by the BS.

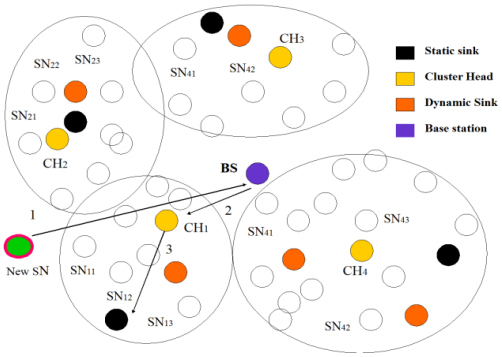

Figure 2: Joining of new sensor node

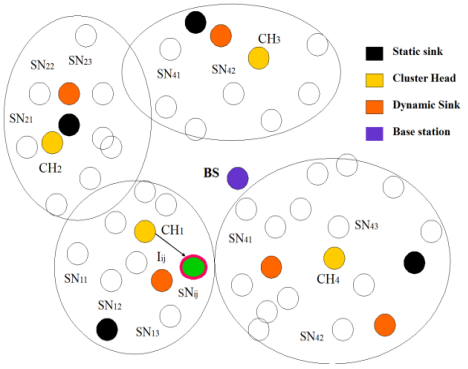

Figure 3: New sensor node receiving variable length identity

A. Key Generation

To ensure authenticity, identity for each sensor is assigned with the help of variable length Huffman coding algorithm by the CH. Identity I_{11} ,I_{12} …..I_{ij} is of variable length binary numbers such as 001, 00010, 100010, 100101, etc. The use of variable length coding is to avoid the illegitimate user in finding out guessing identities. Each sensor node is assigned with variable length so that no two nodes can have same identity i.e., each sensor node is provided with unique identity. This identity is used by the respective sensor nodes for further data transmission as well as for generating other keys.

If a sensor SN_{12} is ready to send the sensed data to BS, it is done through by means of cluster head. Nodes need cluster key and Group key to transmit data to BS. The cluster key is calculated by the CH by getting partial keys P_j from all the nodes in it. The partial key is any random number generated by random number generation algorithm in SNs. After generating partial key P_j , the SN computes secret partial key called S_{ij}

$$S_{ij} = P_j \oplus I_{ij}.$$

Assume CH is going to compute its Cluster key (CKi), all the secret of S_{ij} is sent to the CH. In CH_1, it receives all the S_{ij} from the SNs and it computes CK (CKi) by computing its own partial key K_i as below

$$CK_i = h (S_{11} \oplus S_{12} \oplus S_{13} \oplus \ldots\ldots S_{ij} \oplus K_i)$$

h is the hash function. Equation 2 is invoked by all the CH and performs the computation. Similarly the Master Key (MK) is generated by getting partial keys of all CHs L_i and BS,s own partial key.

$$MK = h (K_1 \oplus K_2 \oplus K_3 \oplus \ldots\ldots K_i \oplus L_{BS})$$

MK is computed by BS when sensor nodes joins and leaves the cluster in the network in order to maintain secrecy (both forward and backward secrecy). Further this cluster key and master key is used for communication between the nodes, sinks, base station and the clusters. When new node connects to the existing network, it should be authenticated with identity, partial key should be generated, CKs and MK generation need to be done.

When any of the SNs leave the group, it is necessary to generate CK and MK to ensure secrecy. During each joins and leaves, the above computation needs to be done. Each time, computation such as identity generation and cluster key generation is being done by CH, drains the energy present in the short span of time.

To avoid this, two or more movable mobile sinks and one static mobile sink is placed in the network. This movable sink moves around the cluster and receives the sensed data and transmits directly to the CH/BS. If the SN is far away from the base station, it needs to transmit the data through multiple nodes. If it happens again and again hence there is a more chance of energy drain. If any of the SNs is ready to transmit the data when the sink is moving around the clusters, it gets the data and transmits to the BS. Hence loss of energy is reasonably avoided because sink gets the data directly from the SNs and move towards BS and delivers the data. This sink helps in saving battery power of CHs and all other SNs. The static sink is a trusted node deployed for computing the above mentioned key management system so that the computation overhead is reduced drastically in the CH. It acts as a proxy for CH in such a way that it prevents energy loss.

Both the variable length Huffman coding algorithm for generating random number identity and CK generation algorithm for generating cluster key are implemented in trusted third party static sink. This static sink computes identity and CK upon the request of CH about the join and leaves of SNs. This static sink concept helps to prolong the life of CH to the certain extent. The cluster head election algorithm is executed to select the new cluster head once the old one reaches the threshold level and also, the same is followed for sinks.

Once the sink reaches the energy level below threshold level, new sink is elected based on highest energy level among the SNs. The authenticity had been done efficiently using key management strategy. In order to ensure forward and backward secrecy, four scenarios such as single node join, multi node join, single node leave and multi node leave should be explored.

B. Single Node Join

In figure: node SN_{ij} connects under cluster CH_i , the SN_{ij} request to CH and it informs the BS about its join in the cluster. CH sends request to sink, it provides variable length identity to SN_{ij}. CH requests all the SN_{ij} to generate and send its secret partial key(S_{ij}). Upon receiving the S_{ij} of all the SNs and from CH, sink computes new CK_i and multicast it to the group. All the SNs in the cluster decrypt the new CK_i with the help of old CK_i. The old CK_i is dropped once new key is decrypted. Further, all the communication is done with the help of new CK_i. The SN does not have enough storage to store all the keys. Hence, the SNs should be automatically dropped the secret partial key once the CH acknowledges the Secret partial key.

SN is implemented to store its Identity and CK alone. The sink can store maximum of 20 cluster keys for a particular threshold time. When it reaches the threshold time, it should be automatically resetted. Nevertheless sink will not receive any new request. The table in the sink consists of CK with its time on request. Time taken to reset the sink table will in milliseconds. During each joins and leaves, Master Key can be generated as same as the cluster key generation by the BS and Multicast it. All the communication is done with the help of CK and MK.

DOI: 10.18535/ijecs/v5i7.21

C. Multi Node Join

In Figure.4, Multiple nodes SN_{45}, SN_{46} and SN_{47} connects under same cluster or under different cluster in a network, all the SN_{ij} request to CH and it informs the respective BS about its join. CH sends request to its corresponding static sink, it provides variable length identity to all the SN_{ij} under particular cluster. Then it requests all the SN_{ij} to generate and send secret partial key under the particular cluster. Upon receiving the S_{ij} of all the SNs, the process is same as discussed in single node join.

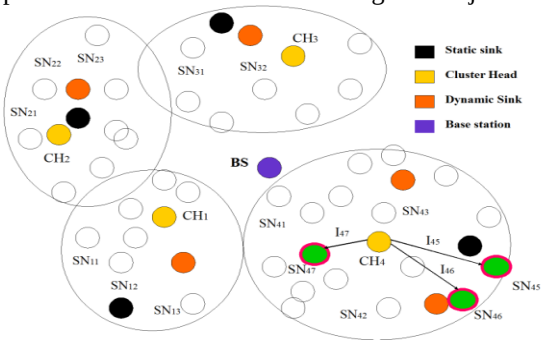

Figure 4: Multiple node join in cluster 4

D. Single Node Leave

In Figure 5, SN_{42} leaves from cluster CH_4 , the SN_{42} request to CH and informs the BS about its leave from the cluster. CH sends request to sink about SNs leave. Then CH requests all the remaining SNij to generate and send a new secret partial key. Upon receiving the Sij of all the SNs, the remaining operation is same as single node join.

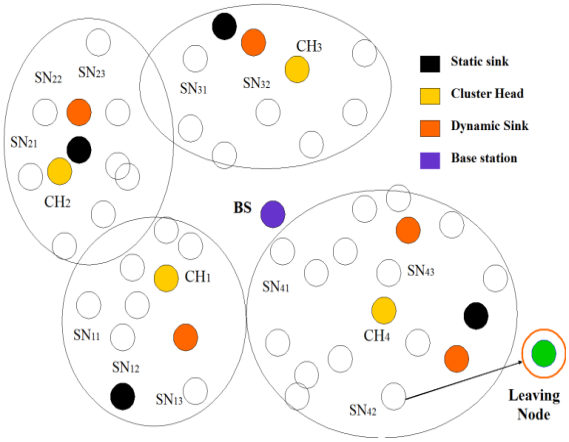

Figure 5: Single node leave from cluster 4

DOI: 10.18535/ijecs/v5i7.21

E. Multi Node Leave

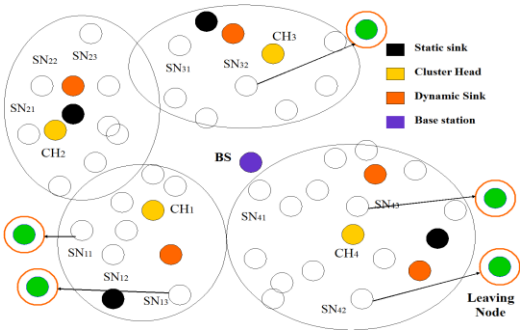

Figure 6: Multiple node leave from cluster 1, 3 and 4.

In Figure 6, multiple nodes SN_{11}, SN_{13}, SN_{32}, SN_{42}, SN_{43} leaves from the same cluster or from different cluster in a network, the SNij request to respective CH_i about its leaves. CH_i sends request to BS and sink about SNs leave. Then CH requests all the remaining SNij to generate and send a new secret partial key. Upon receiving the Sij of all the SNs by CH_i, all other operations are same as multi node join.

IV. Neural Feed Forward Fault Tolerant backbone tree construction

Initially, sensor nodes are dynamic after deployment during the network operation. Cluster head(CH) is also dynamic which can be chosen by cluster head formation algorithm. Initially the cluster head is chosen among on sensor node which is having highest battery power. The new cluster head is selected by the algorithm only when the already exiting cluster head reaches the threshold value.

The potential problem in the previous defined protocols is that once the optimal route is determined, sending data through the same path leads to energy depletion of all the nodes in the path may lead to network partition. It is done to have Multipath Data Transmission which consumes less energy and maximum coverage. These paths are chosen by means of a probability that depends on how low the energy consumption of each path is. Due to the probabilistic choice of routes, it continuously evaluates along different routes and optimal paths are chosen accordingly.

Let *Ni* , *N j* , *Ns* , *ND* are the intermediate, source and destination nodes, while *R _C* is the routing metric. Initially the value of routing cost *R _ C* is set to zero but it is updated as the data transmission takes place along the optimal path. Every intermediate node forwards the request only to the neighbors that are closer to the source node *NS* than itself and farther away from the destination node *ND* to maintain the coverage and connectivity. Routing cost of each path from source to destination and intermediate nodes is updated in the sink for further optimal path finding. The path having the high cost is discarded according to the defined metric. Each path is assigned the probability for successful transmission according to routing cost metric given below

$$R\_C = \left\lceil \frac{E_i^D}{E_t(S_i, S_j) + E_r(S_i, S_j)} * \frac{1}{R} \right\rceil$$

This multi path transmission is done with the help of Fault tolerant Virtual Backbone Tree (FTBT) to reduce the energy consumption for a packet, thereby increases network lifetime, doesn't drain any particular node quickly and also maintains N-of-N lifetime.

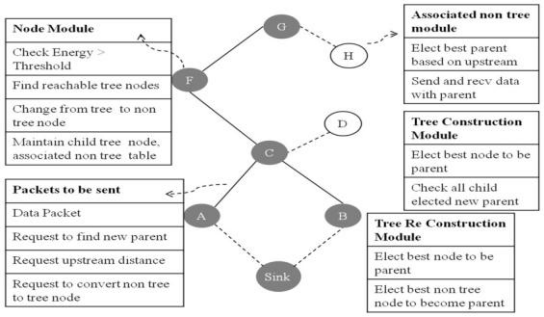

Figure 7. Feed Forward Backproagation Virtual Tree System

Virtual backbones provide an infrastructure for communicating efficiently to the sink node [14]. Nodes are elected as tree nodes and non tree nodes. All communication between particular sensor nodes to the sink node happens through the tree nodes. There are various strategies to elect the tree nodes. In EVBT [15], sink node transmits BCR (Broadcast Request Packet) packet to all nodes in its sensing range. The nodes on receiving this packet compute its fitness factor and time delay (t_d) are inversely proportional to each other. The node waits until t_d is expired. If the node has received one more BCR request in this interval, the node becomes non tree node and elects the nearest tree node as its upstream link. Else the node becomes a tree node and a part of virtual backbone. Electing the nearest tree node for the upstream link does not involve much computation, but it is not the shortest route to the sink. Here, Sink node and sensor nodes that are classified as tree and non-tree nodes.

A sensor has comparatively high energy and it performs sensing, sending and receiving data called tree node. All data from non-tree node to sink need to be transferred with minimum energy to prolong the lifetime of the sensor. Since each node periodically checks its energy, a tree node becomes a non-tree node when a node's energy reaches its threshold level. Two Packets to be sent includes data packets and request packet. Data packet holds data that is sensed by the sensor nodes, which is sent to the sink via the virtual backbone tree. Request packet is sent for finding new parent and upstream distance. How tree and non tree node elected depends on the lifecycle of the node.

It is necessary to eliminate the sensor which is having minimum energy below threshold value and retain the link between the nodes by constructing the virtual backbone tree. It is done using neural network back propagation feed forward algorithm. It retains the network structure and its link. The aim is to construct NNs with nearly minimum number of hidden neurons. It is intended to construct a NN where the input layer is fully connected to the hidden layer which is also fully connected to the output layer. The output o_j of the j_{th} neuron is given by

$$O_j = f\left(\sum_{i=0}^{k} w_{ij} O_i\right)$$

where w_{ij} is the synaptic weight corresponding to the connection from the i^{th} neuron in the previous layer to the j^{th} neuron, O_i is the output of the i^{th} neuron, K is the number of neurons that feeds the j^{th} neuron (which is equal to the number of neurons in the previous layer), **f** is the sigmoid

activation function given by **f(x)** = $1/(1 + e^{-x})$. The hidden neurons are added one by one, each receives a connection from each of the network's inputs. All the input-to-hidden and hidden-to-output weights are trained repeatedly, not only the hidden-to-output weights.

All the sinks initially trained with neural network back propagation feed forward algorithm which minimizes the link break probability in order to find its new optimal route to transmit the data instead of sending in the same route. It is generalized to train a pool of candidate neurons so that it can select the best neuron among the pool after training. Each candidate with different set of initial weights, is temporarily connected to the output of every input neuron, and its output is also temporarily connected to every neurons in a virtual output layer, where **a** virtual output layer is a temporal layer of the same size **as** the original output layer (i.e. they have the same number of neurons). Hence, each time a sink constructs path from the sensors where it is receiving data, if the path is not optimal and if there is maximum of non tree nodes then it back propagates thereby finds optimal path to destination.

A. Backbone Construction

In the sensor network, energy level of each node varies. Initially, all the nodes with an energy level greater than the threshold (T) are temporarily marked as tree nodes. A tree is constructed by the sink connecting all these nodes. If a tree node has too many dependents or reached its threshold value, it will become a hotspot and will lose energy quickly by transferring many packets through it. So one should concentrate on how a node comes to know whether it has many dependents. The approach is to calculate the average number of dependents for all other reachable tree nodes which are in its sensing range.

If the number of dependents of the present node is two times the average dependents, it must try to reduce its number of dependents. It will ask its dependent child tree node and associate non tree node to check if it can find a new parent tree node. This node remains parent for only those nodes which do not find a new parent. Though the backbone tree needs to be constructed from a minimum number of nodes covering the entire network, having more dependents for a particular tree node will have severe impact on its energy. Tree node whose energy is approaching threshold should reduce its number of dependents appreciably and possibly try to become a non tree node.

Algorithm 1:

N_i If N_i.Energy> T

$N_i \leftarrow$ TN // temporarily. Form a tree, root: sink and initiated by it

$\forall N_i$

RTN[ ] $\leftarrow$ { N_j==TN $\cap$ dist(i,j)<S_i }

// let n be the number of reachable tree nodes

Sum $\leftarrow$ 0

$\forall$ RTN

Sum+=RTN→No.of.dependents

Avg=Sum/n

if RTN → No. of.dependents ≥ 2 x Avg || N_i.Energy → T + ε **then**

find a suitable parent

B. Finding a suitable parent for child tree nodes

One can finds all its reachable tree nodes of this child tree node which lie within its sensing range for all child tree nodes. If there is only one node in its range, then it is chosen as its parent. The node with highest fitness factor is chosen as its parent if there is more than one tree node in its sensing range. If the parent is undefined, the child tree node waits so that any of its reachable sibling tree nodes of its earlier parent has chosen a new parent. Then the sibling is chosen as its parent. If it couldn't find a parent, then node N_i remains as a tree node, so that the network sustains.

C. Finding parent for associated non tree nodes

The reachable tree nodes which lie in its sensing range for each non tree child node are found. If the number of such nodes is just one, then it is chosen as its parent directly else compare the upstream distance for each tree node, assuming that as its parent, now node with least upstream distance is chosen as its new parent node. Node N_i must check if its entire child nodes (tree and non-tree) are assigned a new parent, then N_i becomes a non-tree node else the node remains as tree node. In short the parent for child tree nodes are chosen based on maximum fitness value, and the parent for child non-tree node is chosen based on minimum upstream distance.

D. Backbone Reconstruction

Reconstruction of a tree is needed when node fails due to hardware error or complete drain of energy. Tree nodes periodically check whether its energy falls below threshold energy. If so the node becomes a non-tree node. Let T be a tree node which fails, all its child tree nodes are assigned to a new parent. A child tree node finds all the tree nodes in its sensing range. If there is only one node, it is made as its parent, else a parent is chosen based on the highest fitness factor and its other parameters like upstream distance and angle. If there is no other tree node in its sensing range, it checks all non tree nodes, which are in its sensing range and selects the one with best fitness factor and minimum upstream distance and converts it from non tree to tree node. The pre-condition is the selected non tree must have energy greater than threshold. If a non-tree fails, then there is no breakage in the tree structure, hence that node is removed from the tree formed and considered to be dead.

V. Experimental Results

The system enhances security through variable length coding such as reduction of key management overhead in terms of reduction of key size and also large saving in complexity, execution time and storage space. Most-frequently occurring source symbols are provided with shortest bit lengths, hence, reduction in number of bits used for encryption and decryption is ensured. Illegitimate user cannot able to find the identity of another user by holding the UID of another user.

DOI: 10.18535/ijecs/v5i7.21

Hash function used in this paper provides more security due to unique key generation. EX-OR operation used in generating cluster key and group key ensures accurate result i.e., no bit would be changed thereby error produced is negligible. The BS uses the partial keys received from each CH and also its own partial key to generate *CK*. Hence it takes *O(log C+1)* operations for MK generation. In the same way, CH uses partial keys of its SNs and also its own to generate CK. Hence it takes *O(log N+1)* operations for CK generation. During Node joins and leaves it takes computation cost O(1) for single and multiple joins and leaves.

Deployment of static and dynamic sink in the network helps to prevent sensor nodes and cluster head form energy drain in turn it increases the lifetime of the sensor network. This leads to negligible storage overhead and communication overhead thus it saves energy. The virtual backbone tree is very flexible, an energy efficient backbone tree and also maintains N – N lifetime and is virtually connected to the sink. All these benefits are simulated and represented in the form of graph given below.

All the sensor nodes are deployed randomly and simulated over 22 clusters where each having its own head that cover all nodes deployed in the region**.** The event detected containing information is sent to the movable sink. Time stamp is given to all packets to perform data aggregation. The parameters used for simulation are given below,

TABLE 1. Simulation Parameter

Parameters	Value
Network Area	500*500
No. of. sensor nodes	100
Radio range	60m
Transmitting Power	24.750mW
Receiving Power	13.500mW
Idle listening Power	13.500mW
Sleeping Power	0..015mW
Transmission Rate	100 bps
Transmitting radius	25m
No of mobile sinks	3
Sink1-Mobility model	Rectangular Mobility
Sink2-Mobility model	Circular Mobility
Sink3-Mobility model	Constant speed Mobility
Speed of mobile sinks	10 mps

Case 1: Without mobile sinks in the network:

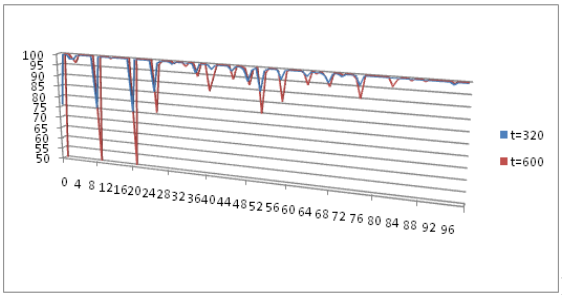

Figure 8: Comparison of energy levels of all nodes at t=320s and t=600s

The data collected by the cluster heads is to be forwarded to the movable sinks and to the base station. At time t= 320s and t= 600s, the energy draining is of 2J for event detection and 1J for forwarding the sensed data. The comparative analysis is given below,

Case 2: With Mobile sinks in the network

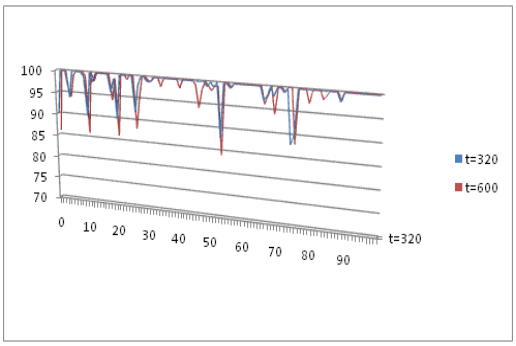

Figure 9: Comparison of energy levels of all nodes at t=320s and t=600s

From the above assumption at different times 320 seconds and 600 seconds, the draining of energy is 1J for sensing or detecting the event and 2J for transmitting the data. Mobile sinks are highly powered nodes and their energy also gets depleted which doesn't make a much difference. Even, we can come across that sensor packets are forwarded to the base station directly when no mobile sinks would be reachable during certain times in simulation. This situation occurs very rarely and energy depletion due to this reason is very low.

Next, the virtual backbone tree construction is proposed using neural network with adaptive learning. The neurons are assigned weight according to the residual energy of the nodes in the network. A coverage aware routing metric is also included to choose the best route from the available ones. Since it is multipath transmission, once the routes are decided and one of the routes is chosen from these routes, the data transmission is performed using the defined metric. The results obtained show that the proposed scheme is quite effective to deliver more than 95% of the packets to their destination with an increase in network coverage. Although with an increase in network coverage, the number of alive nodes decreases with respect to coverage and connectivity

Table 2. Simulation Parameters

Parameters	Value
Region radius under consideration	500 m*500 m
Nodes sensing range	60 m
Number of Nodes	100
Initial energy per node	5 J
Network bandwidth	2 Mbps/s
Power to run the transmitter/receiver circuitry	70 nJ/bit
Power for the transmit amplifier to achieve an acceptable SNR (Signal to Noise Ratio)	120 pJ/bit/m2
Size of a data packet	4096 bits
Size of a control packet	20 bits

Data transmission rate	4096 bits

Table 3: Transmission range, Average number of nodes vs Average number of dependents for each tree node

Transmission range in meter(m)	Average number of nodes	Average number of dependents for each tree node
20	0	3.6
25	20	5.66
30	40	7.94
35	60	10.44
40	80	13.06
45	100	16.49
50	120	18.52
60	140	21.09
70	160	24.14

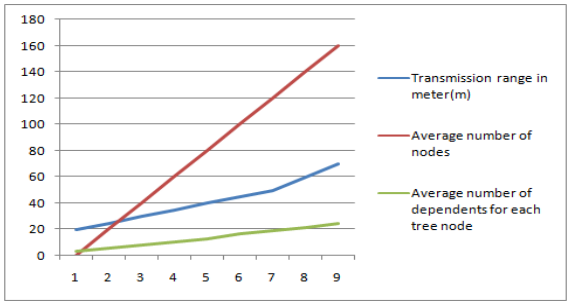

Figure 10. Analysis of Transmission range, Average number of nodes vs Average number of dependents for each tree node

The energy consumption for delivering the data for 100 and 200 nodes for EVBT[29,31], ViTAMin[30] and FTBT are also simulated as above and are depicted. Increasing transmission range further will consume more battery power.

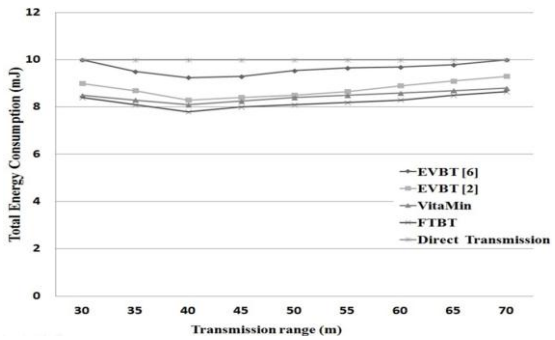

Figure 11: Energy consumption during delivery of data (No. of nodes = 100)

VI. CONCLUSION

A good key management strategy speaks about secure transmission of data. Long distance data transmission by sensor nodes is not energy efficient, since it is energy consumption. Deployment of static and dynamic sink in the network helps to prevent sensor nodes and cluster head form energy drain in turn it increases the lifetime of the sensor network. This leads to negligible storage overhead and communication overhead thus it saves energy. Also, a proposed fault tolerant Feed Forward back propagation network algorithm emphasizes the lifetime maximization. This virtual backbone tree is flexible and duration of the network for a longer period of time is maintained, hence, N – N lifetime is achieved through virtually connected sink. Multipath transmission is enabled to improve the performance of the network and fast data transmission. Hash function and Ex-OR operation in random partial keys provides us better result to ensure authenticity of a node. Variable code identity prevents attackers from acquiring the identity of the sensor node hence; compromising of sensor node is not possible. This paper achieves efficient security with low key storage overhead. Results proved that the proposed method gives better performance and achieved the major challenges in wireless sensor networks.

VII. REFERENCES

[1] Abdoulaye Diop, Yue Qi and Qin Wang , Efficient Group Key Management using Symmetric Key and Threshold Cryptography for Cluster based Wireless Sensor Networks, I.J. Computer Network and Information Security, 2014, 8, 9-18

[2] Lin Yao, Bing Liu, Feng Xia, Guo-Wei Wu and Qiang Lin, A Group Key Management Protocol Based on Weight-Balanced 2-3 Tree for Wireless Sensor Networks,

[3] M.Shainika and Mrs.C.Hema, Cluster Based Mobile Key Management Scheme to Improve Scalability and Mobility in Wireless Sensor Networks, National Conference on Research Advances in Communication, Computation, Electrical Science and Structures (NCRACCESS-2015) , 22-26.

[4] Jyothi Metan and K N Narasimha Murthy, Group Key Management Technique based on Logic- Key Tree in the Field of Wireless Sensor Network, International Journal of Computer Applications, Volume 117 – No.12, May 2015, pp.0975 – 8887.

[5] Yetgin, H., Cheung, K.T.K., El-Hajjar, M., Hanzo, L.2014. Cross-layer network lifetime optimization considering transmit and signal processing power wireless sensor networks. Wireless Sensor Systems, IET , Vol.4, No.4, pp.176-182

[6] Alagheband, M.R., Aref, M.R.2012. Dynamic and secure key management model for hierarchical heterogeneous sensor networks. Information Security, IET, Vol.6, No.4, pp.271-280

[7] Seo, S-H., Won, J., Sultana, S., Bertino, E.2015. Effective Key Management in Dynamic Wireless Sensor Networks. Information Forensics and Security, IEEE Transactions, Vol.10, No.2, pp.371-383

[8] J. Zhang, V. Varadharajan, "Wireless sensor network key management survey and taxonomy," Journal of Network and Computer Applications, vol. 33, no. 2, 2010, pp. 63-75.

[9] A Diop, Y. Qi, Q. Wang "An Improved Key Management Scheme for Hierarchical Wireless Sensors Networks," in TELKOMNIKA Indonesian Journal of Electrical Engineering Science, vol. 12, 2014, pp 3969-3978.

[10] Y. Zhang, C. Wu, J. Cao and X. Li "A Secret Sharing-Based Key Management in Hierarchical Wireless Sensor Network", Hindawi Publishing Corporation International Journal of Distributed Sensor Networks, vol. 2013, pp. 1-7.

[11] Harn L, Lin C," Authenticated group key transfer protocol based on secret sharing", In Proceedings IEEE Trans. Comput, 2010, vol. 59 (6), pp, 842–846.

[12] Klaoudatou, E., Konstantinou, E., Kambourakis, G. and Gritzalis, S., A Survey on Cluster-Based Group Key Agreement Protocols for WSNs. IEEE Communications Surveys & Tutorials, PP (2010), 1-14.

[13] Kwang-Jin Paek, Jongwan Kim Chong-Sun Hwang And Sangkeun Lee, Group-Based Key Management Protocol For Energy Efficiency In Long-Lived And Large-Scale Distributed Sensor Networks, Computing And Informatics, Vol. 27, 2008, 743–756

[14] Jae-Hwan Chang and Leandros Tassiulas," Maximum Lifetime Routing in Wireless Sensor Networks",IEEE/ ACM Transactions on Networking, VOL. 12, NO. 4, AUGUST 2004,DOI:10.1109/TNET.2004.833122

[15] Md Nafees Rahman, M A Matin,Md Nafees Rahman, "Efficient Algorithm for Prolonging Network Lifetime of Wireless Sensor Networks", Tsinghua Science and Technology , December 2011, Volume 16, Number 6,pp561-568
[16] YoungSang Yun, Ye Xia, Behnam Behdani, and J. Cole Smith," Distributed Algorithm for Lifetime Maximization in a Delay-Tolerant Wireless Sensor Network with a Mobile Sink", IEEE Transactions on Mobile Computing, VOL. 12, NO. 10, OCTOBER 2013, DOI: no. 10.1109/TMC.2012.152.
[17] A. Manjeshwar and D. P. Agarwal, "TEEN: a Routing Pro-tocol for Enhanced Efficiency in Wireless Sensor Networks,"1st International Workshop on Parallel and Distrib. Computing, 2001, DOI: 10.1109/IPDPS.2001.925197.
[18] A. Manjeshwar and D. P. Agarwal , "APTEEN: A Hybrid Protocol for Efficient Routing and Comprehensive Infor-mation Retrieval in Wireless Sensor Networks," Parallel and Distributed Process. Proc. Symp, pp. 195–202, 2002 ,DOI: 10.1109/IPDPS.2002.1016600.
[19] Deng.S , "Mobility-based clustering protocol for wireless sensor networks with mobile nodes," IET Wireless Sensor Systems, Vol.1, Iss. 1, pp. 39-47, 2011.
[20] J.Akbar Torkestain,M.R.Meybodi, "An intelligent backbone formation algorithm for wireless as networks based on distributed learning automate,"Computer Networks,Vol 54, pp.826-843,2010, DOI: 10.1016/j.comnet.2009.10.007.
[21] K.M.Alzoubi,"New Distributed algorithm Connected Dominating Set in Wireless Ad Hoc Networks," Proceedings of the 35th Annual Hawaii International conference on System Sciences(HICSS'02), Vol.9.pp.297,2002.
[22] R. Xie,D.Qil , " A novel distributed MCDS approximation algorithm for wireless sensor networks,"Mobile & Wireless Communication,Vol.9,Issue 3, pp.427-437,2009.
[23] I.FAkyildiz , "A Survey on Sensor Networks," IEEE Communication Magazine, vol. 40, pp. 102-114,2002 DOI: 10.1002/wcm.547.
[24] Feng Wang, Member, IEEE, My T. Thai, Member, IEEE, and Ding-Zhu Du, "On the Construction of 2-Connected Virtual Backbone in Wireless Networks", IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, VOL. 8, NO. 3, MARCH 2009.
[25] Wei Wang, Donghyun Kim, Min Kyung An, Wei Gao, Xianyue Li, Zhao Zhang, and Weili Wu," On Construction of Quality Fault-Tolerant Virtual Backbone in Wireless Networks", IEEE/ACM TRANSACTIONS ON NETWORKING, VOL. 21, NO. 5, OCTOBER 2013.
[26] Neeraj Kumar, Manoj Kumar and R.B. Patel, "Coverage and Connectivity Aware Neural Network Based Energy Efficient Routing in Wireless Sensor Networks", Journal on Applications of Graph Theory in Wireless Ad hoc Networks and Sensor Networks, Vol.2,No.1, March 2010.
[27] Bosheng Zhou,"An energy-aware virtual backbone tree for wireless sensor networks,"IEEE Global Telecommunications Conference, pp. 1212-1215,2005 DOI: 10.1109/GLOCOM. 2005.1577373.
[28] Kim, Jaekwang and Lee Jee-Hyongng, "ViTAMin: A Virtual Backbone Tree Algorithm for Minimal energy consumption in wireless sensor network routing," International Conference on Information Networking (ICOIN), pp.144, 149,2012 DOI: 10.1109/ICOIN.2012.6164366.
[29] Md Nafees Rahman, M A Matin,Md Nafees Rahman, "Efficient Algorithm for Prolonging Network Lifetime of Wireless Sensor Networks", Tsinghua Science and Technology , December 2011, Volume 16, Number 6,pp561-568.
[30] YoungSang Yun, Ye Xia, Behnam Behdani, and J. Cole Smith," Distributed Algorithm for Lifetime Maximization in a Delay-Tolerant Wireless Sensor Network with a Mobile Sink", IEEE Transactions on Mobile Computing, VOL. 12, NO. 10, OCTOBER 2013, DOI: no. 10.1109/TMC.2012.152.
[31] A. Manjeshwar and D. P. Agarwal , "APTEEN: A Hybrid Protocol for Efficient Routing and Comprehensive Infor-mation Retrieval in Wireless Sensor Networks," Parallel and Distributed Process. Proc. Symp, pp. 195–202, 2002 ,DOI: 10.1109/IPDPS.2002.1016600.