BACK PROPAGATING TREE TO PRODUCE AN OPTIMAL PATH TO TRANSMIT DATA IN A WIRELESS SENSOR NETWORKS

K. Vimal Kumar Stephen and Mathivanan V.
Department of IT, AMET University, Chennai, India
E-Mail: nads74@yahoo.com

ABSTRACT

Wireless Sensor Networks (WSN) raises number of the challenges with regard to scalability and energy efficacy. Implemented of Huffman approaches one of the key variable length in the wireless sensor network is prolonging network lifetimes. To improve the lifetime of the sensor, static and movable mobile sinks are deployed. Movable sinks are used to receive sensed data from the sensor where it is located. Assigning prime number as the sensor node identity can be easily guessed by the intruder. Reusing the same identity in the cluster leads to compromising of nodes. The energy is retained when computation is reduced in cluster head thereby increases the life time of the particular cluster. Variable length gives variable length identity and avoids reusing of same identity hence it avoid network attacks such as random number length of nodes are not possible (No sensors are allowed inside the network without the knowledge of Cluster head).Increasing transmission range future will consume more battery power.

Keywords: wireless sensors, cluster head, base station, master Key.

INTRODUCTION

In sensor networks, data is very important and to maintain secure data communications is a toughest task. The process of establishing an authentication and secured communication could be achieved by a suitable key management scheme has a significant part to play 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 as well as group key. In the research, Public-private key is employed for encryption and decryption, cluster key is for intracluster communications and group key id for intercluster communications ought to be shared amongst every group member for multicasting data amongst a particular group in a secure manner.

Prior to transmission, all data packages ought to be encrypted with a common shared group key. Users who possess the shared group key are the only ones capable of decrypting the packages and receiving 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. Therefore, the communications amongst the group members could be considered secure [2].

In sensor networks, a generic huge-scale wireless sensor network comprises a minimum of one sink (base station) as well as several thousands of sensor nodes, which organize themselves into multi-hop wireless networks and deploy either arbitrarily or as per some pre-defined statistical distribution over a geographical locale. Sensor nodes by themselves are severely constrained in terms of resources like restricted amount of memory, battery, processing capability, computing ability, or even communication ability. Therefore, they can only sense a small area of their environments. 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. Therefore, the communications amongst the group members may be considered 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 [6, 7] were proposed for energy efficiency to improve the lifetime of wireless sensor network (WSN). Communication ranges: various general sensors possessing invariant communication range, some sensors' radio receivers are able to change their communication power in continuous steps for achieving various communication ranges. The actual communication range might also be impacted by several external factors like height of the sensors, or its surrounding entities

Literature Survey

Abdoulaye Diop [1]a various leveled cluster architecture of sensor networks received the pair-wise group key management and keys are updated intermittently. It prevents assaults from malicious nodes and mitigates the node trade off. The communication overhead is unimportant for key establishment with less memory overheads as well as energy conservation. In this research, energy conservation increases network lifetimes and attains effective security with minimal key storage overheads.

Lin Yao[2] proposed addressing the balance between security and restrictions formed in every subgroup. Maximum Distance Separable (MDS) code is utilized for distributing the multicast key randomly. The better problem is to solve security. This method takes strategy of both centralized and distributed key group management method which is organized as unpredictable tree and every subgroup is organized as a weight-balanced.

M. Shainika [3] security, scalability and performance are capable of proving the capacity to perform in an examination and then obtain the related credentials, with no presentation of identifying information. Else, one could have an interaction with a service through pseudonyms and want to obtain features related to the interaction without presenting their full identities.

Jyothi Metan [4] that ensures attackers will not be capable of getting the group keys when the CHs broadcast them. MAC is utilized along with the partial keys for guaranteeing authentication. Group keys are created through usage of partial keys in this research. The amount of power used is minimal in comparison to the overall energy present to generate the partial keys as well as the group key.

Yetgin, H [5] optimize the NL of WNS through analyzing the effect of the physical layer variables and signal processing power (SPP). The primary tradeoffs between the NL and bit error ratio (BER) performance for a pre-determined set of target signal-to-interference-plus-noise ratio values as well as for varying MCSs utilizing periodic transmit-time slot scheduling in interference-limited WSNs.

Alagheb and, M.R [6] a lot of effort has been made in energy efficacy of WSN and several scholars have looked at subsequent hop selection schemes such as 1-hop neighbouring nodes or multiple links for the transmission of information.

Seo, S-H [7] some researchers focused on scheduling the nodes. An effective routing measure utilized in taking the selection of the next hop. Recently, two categories of routing methodologies were attractive; Cluster based as well as Virtual backbone based protocols.

J. Zhang [8] one-hop communication model, every single sensor node sends packet to its CH directly in a single hop and the cluster head transmits the sensed data to the sink. The existing solution for clustering needs maintenance for reorganizing the clusters because of mobility as well as node failures.

A Diop [9] a secure efficient hierarchical key management strategy (SEHKM) for WSNs is proposed where three kinds of keys for encrypting messages transmitted amongst sensor nodes. It fulfills various requisites of WSNs. The design of the strategy is influenced by the restrictions of sensor networks as well as high resource cost in conventional key management methods.

Y. Zhang [10] to structure nodes in an improved manner. Backbones are subsets of active nodes, which are capable of performing a special task, and serving nodes that are not in the backbone. A backbone reduces the operating cost of the communications between sink and the other sensor nodes, decreases the total power used by each parcel and also increases the network lifetime in WSN.

Harn L and Lin C [11] presented an authenticated key transfer protocol is suggested on the basis of a secret sharing strategy, in which key generation centre (KGC) can broadcast group key information to every group members at once and only those members who are authorized will be capable of recovering the group key, however, non-authorized members will not be able to recover the group key.

Klaoudatou, E [12] cluster-based Group Key Agreement (GKA) the complexity of every protocol as well as the energy costs added to the systems are computed. An evaluation of every discussed protocol is presented in a generalized manner ad can thus function as a reference for future evaluation as well as for designing novel, enhanced GKS protocols. The property of UDG is used in the analysis part to get a constant approximation. Also investigated a constant factor approximation protocol for k>=3 and m>=1 in a disk graph. Multipath transmission is proposed.

Kwang-JinPaek [13] the issue of building error-tolerant CDS in homogeneous WSNs is investigated that is abstracted as the minimum connected dominating set problems. A constant factor polynomial-time approximation protocol is computed and this protocol functions for all abstract graphs with no information of geometric coordinates of the input graph.

Fault tolerant virtual backbone tree model

Fault tolerant Virtual Backbone Tree (FTVBT) has been proposed in this work. It decreases the vitality utilization for an energy, builds system lifetime, doesn't deplete a specific hub rapidly furthermore keeps up N-of-N lifetime.

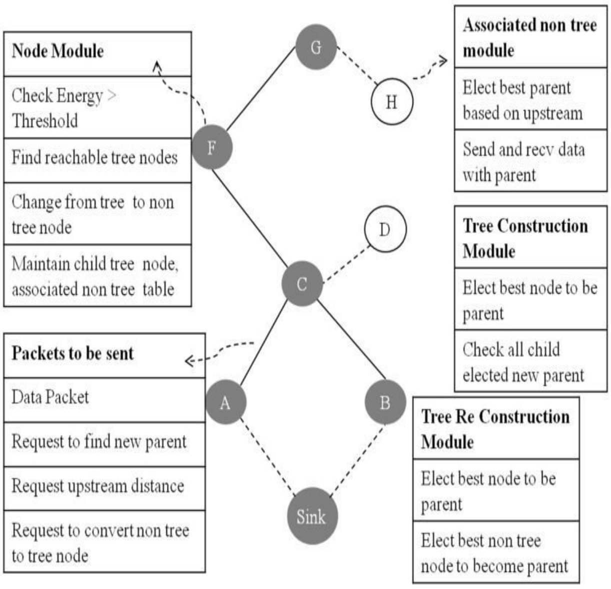
Node Module
Check Energy > Threshold
Find reachable tree nodes
Change from tree to non tree node
Maintain child tree node, associated non tree table
Packets to be sent
Data Packet
Request to find new parent
Request upstream distance
Request to convert non tree to tree node
G
H
F
D
C
A
B
Sink
Associated non tree module
Elect best parent based on upstream
Send and recv data with parent
Tree Construction Module
Elect best node to be parent
Check all child elected new parent
Tree Re Construction Module
Elect best node to be parent
Elect best non tree node to become parent

Figure-1. Backbone tree of the FTVBT system.

Figure-1 shows the system architecture of the suggested work. The system consists of a sink node as well as sensor nodes that are classified as tree as well as non-tree nodes.

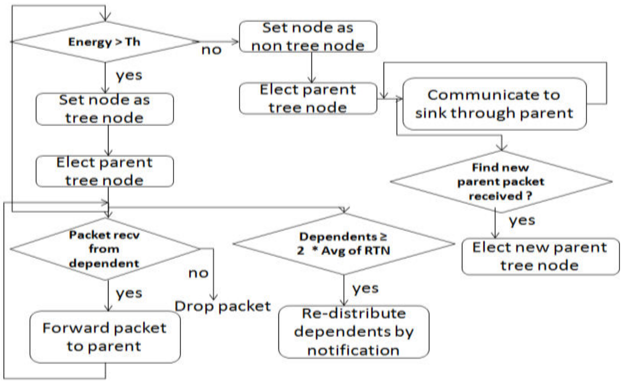
Energy > Th
no
Set node as non tree node
yes
Set node as tree node
Elect parent tree node
Communicate to sink through parent
Elect parent tree node
Find new parent packet received ?
yes
Elect new parent tree node
Packet recv from dependent
Dependents ≥ 2 * Avg of RTN
no
yes
yes
Drop packet
Forward packet to parent
Re-distribute dependents by notification

Figure-2. State diagram showing lifecycle of a node.

A tree node has similarity high throughput and it performs sensing, sending as well as receiving data. All data from the non-tree node to sink is required to be transferred with minimal energy as well as distance for a prolonged lifetime. While a non-tree node senses and transfers data Functions that a tree node performs include, finding all the reachable tree nodes. A tree hub turns into a non-tree hub when its vitality esteem falls underneath an edge. Packet to be sent includes data packets and request packet. Data packet holds data that is gathered by the sensor nodes, which is sent to the sink via the virtual backbone tree. Request packets include finding new parent and upstream distance. The lifecycle of the node is depicted in Figure.2 shows that the how tree and non-tree node elected.

Backbone construction methodology

In the sensor network, energy level of each node varies. At first, every nodes with energy levels higher than the threshold (T) are temporarily marked as tree nodes. A tree is built by the sink connecting all these nodes. If a tree node possesses too many dependents or reached its threshold value, it becomes a hotspot and will loses energy rapidly by transferring several packets through it. So one should concentrate on how a node comes to know whether it has many dependents. The methodology is to calculate the average quantity of dependents for all other reachable tree nodes which are in its detecting range. If the number of dependents of the present nodes is two times the normal dependents, it must try to reduce its number of dependents. It will ask its dependent branch tree node and associate non tree node to check if it can find a novel parent tree node. This node remains parent for only those nodes which do not find a novel 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 ought to decrease the quantity of its dependents considerably and possibly attempt to turn into 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 quantity of reachable tree nodes
Sum $\leftarrow$ 0
$\forall$ RTN
Sum+=RTN$\rightarrow$No.of.dependents
Avg=Sum/n
if RTN $\rightarrow$ No. of. dependents $\geq$ 2 x Avg ‖
$N_i$.Energy$\rightarrow$ T + $\varepsilon$   then
find a suitable parent
```

Finding an adequate parent for child tree nodes

One can finds all its reachable tree nodes of this child tree node which lie in its sensing range for all child tree nodes. When only one node in its range, then it is taken as parent node else node with greatest fitness factor and its other parameters like upstream distance and angle is chosen as its parent. 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 Ni remains as a tree node, so that the network sustains

Algorithm 2: Finding a parent for each of the child tree nodes.

```
$\forall$child tree node j
RTN $\leftarrow$ {($N_K$$\cap$ parent ( $N_K$) != $N_i$)$\cap$dist(k,j) <$S_k$ }
//k be the number of Reachable Tree Nodes
if  k == 1   parent [j] $\leftarrow$ RTN
elseif  k> 1
max $\leftarrow$ -1  ,  index $\leftarrow$ undefined
$\forall$ RTN t
If fitnessfactor( j , t ) > max
max $\leftarrow$ fitnessfactor( j , t ), index $\leftarrow$ t
parent[j] $\leftarrow$ index
if  max == -1
if parent Parent[sibling(j))]!= NULL &&
sibling(j)).isReachable()== TRUE
parent(j) = sibling(j)
flag $\leftarrow$ 1
$\forall$child tree node j
if Parent [ j ] == NULL ‖ parent [ j ] ==Ni
Ni $\leftarrow$ TN
flag $\leftarrow$ 0 ; break
```

Finding parent for associated non tree nodes

The reachable tree nodes which lie in its sensing range for every 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 Ni must check if its entire child nodes (tree and non-tree) are designated a new parent, then Ni becomes a non-tree node else the node remains as tree node. In short the parent for child tree nodes are chosen on the basis of maximal fitness value, and the parent for child non-tree node is chosen on the basis of minimum upstream distance.

Algorithm 3: Finding parent for each associated non-tree nodes.

```
∀ associated non tree node j,
RTN ← { $N_K$==TN ∩ parent( $N_K$) != $N_i$ ∩dist(k,j) <$S_k$ }
k ← ( sizeof(RTN) / sizeof(RTN[0] )
if k == 1     parent [j] ← RTN
else if k> 1
min ← INFINITY  index ← NULL
∀ RTN t
ifustream(t) + distance( j , t ) < min
min ← ustream(t) + distance( j , t )
index ← t
parent[j] ← index
∀ associated non tree node j
if Parent [ j ] == NULL‖ parent [ j ] ==$N_i$
Ni ← TN
flag ← 0
if flag == 1
$N_i$ ←NTN
```

Backbone reconstruction

Reconstruction of a tree is needed when node fails due to hardware error or complete drain of energy. Tree nodes periodically monitor whether its energy goes below threshold energy. If the energy falls below threshold than the node turns into a non-tree node. Let T be a tree node which fails, every child tree nodes is designated to a new parent. As seen before in finding adequate parent step, the child tree node discovers every tree node in its sensing range and chooses its parent. In case if there is no other tree node within the sensing range, every non-tree node which are within the sensing range is checked and the one with best fitness factor as well as minimum upstream distance and converts it from non-tree to tree node is selected. The pre-condition is the chosen non tree must have energy higher than threshold. If a non-tree fails, then there is no breakage in the tree architecture, hence that node is removed from the tree formed and considered to be dead.

RESULT AND DISCUSSIONS

The system enhances security improves through variable length coding such as reduction of key management overhead in terms of decrease of key management overheads with regard to decrease of key size as well as huge savings in complexity, execution time, as well as storage space. Frequently occurring source symbols are given with shortest bit lengths, hence, decrease in the quantity of bits utilized for encryption as well as decryption is guaranteed. Illegitimate user cannot able to find the identity of another user by holding the UID of another user. Hash function used in this paper provides more security due to extraordinary key generation. EX-OR operation used in utilized cluster key and group key ensures accurate result i.e., no bit would be changed thereby error produced is negligible. The BS utilizes the partial keys obtained from every CH as well as its own partial key for generating CK. Therefore, it takes O(log C+1) operations for MK generation. Similarly, CH utilizes partial keys of its SNs as well as also its own for generating CK. Therefore, 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 structure 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 diagram given below.

All the sensor nodes are deployed randomly and simulated over 22 clusters where each having its own head that cover every node deployed in the area. The event detected containing information is sent to the movable sink. Time stamp is given to all packets for performing data aggregation. The variables utilized for simulation are provided below.

Table-1. Simulation parameter.

Parameters	Value
Total Network Area	500 m by 500 m
Number of. sensor nodes	100 nodes
Radio range & transmitting radius	60m, 25m
Transmitting & Receiving Power	24.750mW, 13.500mW
Idle listening & Sleep Power	13.500mW, 0..015mW
Transmission Rate	100 bps
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:

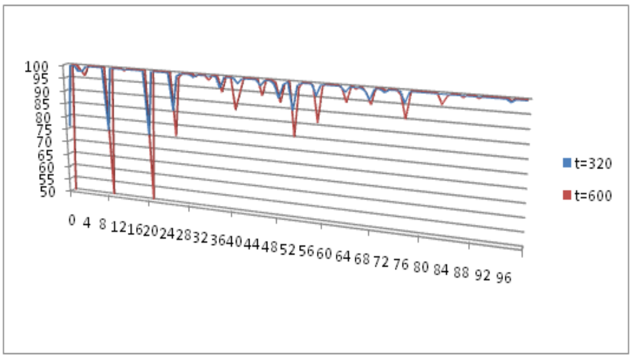

Figure-3. Comparison of energy levels of all nodes at t=320s and t=600s.

The data gathered by the CHs is to be transmitted to the movable sinks and to the base station. At time t= 320s and t= 600s, the energy draining is of 2J for events detection and 1J for transmitting the sensed informion. The comparative analysis is given below.

Case 2: With mobile sinks in the network

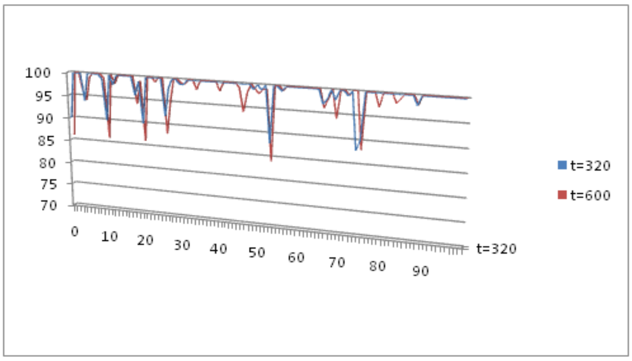

Figure-4. Comparison of energy levels of all nodes at t=320s and t=600s.

From the above assumption at various times 320 seconds as well as 600 seconds, the draining of energy is 1J for sensing or the detection of event and 2J for information transmission. Though mobile sinks have more power, its energy also becomes depleted that does not make a lot of difference. Even, we can come across that sensor packets are forwarded to the base station directly when no mobile sinks can be reached during certain times in simulation. This situation occurs rarely and energy gets depleted because of this reason is extremely less.

Next, the virtual backbone tree construction is suggested utilizing NN with adaptive learning. The neurons are designated weight as per the remaining energy of the network nodes. Coverage aware routing measure is included for choosing the best path from the ones present. Since it is multipath transmission, when the paths are determined and one of the paths is selected from the paths, information transmission is carried out utilizing the defined measure. Outcomes got prove that the suggested method is adept in delivering more than 95% of the packets to their destinations with increase in network coverage. Though with increase in network coverage, the quantity of alive nodes decreases with respect to coverage and connectivity.

Table-2. Simulation parameters.

Parameters	Value
Region radius under consideration	500 m*500 m
Node sensing range	60 m
Quantity 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 transmit amplifier to attain an adequate 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**	**Averagenumber 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

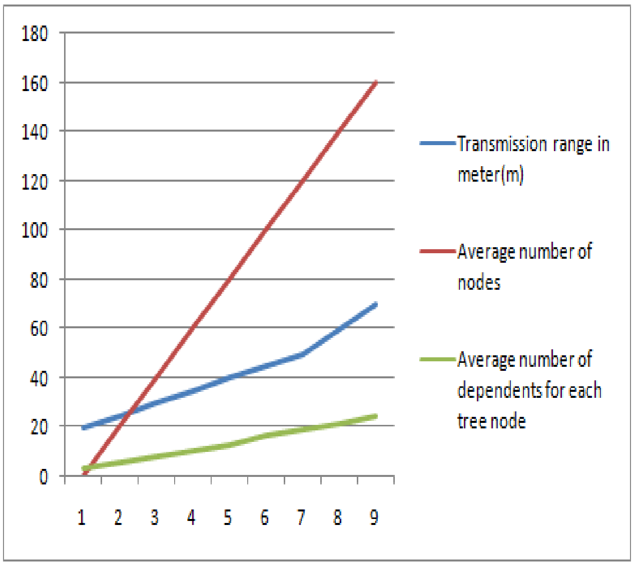

Figure-5. Analysis of transmission range, Average number of nodes vs Average number of dependents for each tree node.

Comparative analysis of the proposed method

The research done sounds well only if it is proved to be better than existing technique. Implementation of Huffman provides better result compared to other approaches in wireless network.

a) Assigning prime number as the sensor node identity can be easily guessed by the intruder. Reusing the same identity in the cluster leads to compromising of nodes.
b) Assigning random number as the sensor node identity can be easily identified by the random number generation algorithm if the intruder knows two sensors identity who left after the group
c) Variable length gives variable length identity and avoids reusing of same identity hence it avoid network attacks such as Birthday attack (since Sensor ID is variable length), Guessing attack (uses partial keys) and Compromising of nodes are not possible (No sensors are allowed inside the network without the knowledge of Cluster head)

Then, implementation of mobile sinks and construction of virtual backbone tree reduces energy consumption there by improves the lifetime of the sensor networks.

a) The assumption at different times 320 seconds and 600 seconds leads to the energy drain of 2J for sensing or detecting the event and 1.5J for transmitting the data in the absence of mobile sink
b) The assumption at various times 320 seconds and 600 seconds leads to the energy drain of 1J for sensing or detection of the event and 1J for information transmission with the help of mobile sink
c) Jamming attack referred as Denial of service is also not possible since frequency of identity cannot be identified (because it is unique) and the sinks are trusted party. Path is secret and virtual for every sensor and it is tracked by sink hence no choice for attacker to compromise sink
d) Wormhole attack is not possible because sink is the only source of proving virtual routing path and any node in the network will not receive any other path routing data from other nodes

The power used for data delivery for 100 and 200 nodes for EVBT, ViTAMin and FTBT are also simulated as above and are depicted. Increasing communication range further will deplete the battery further.

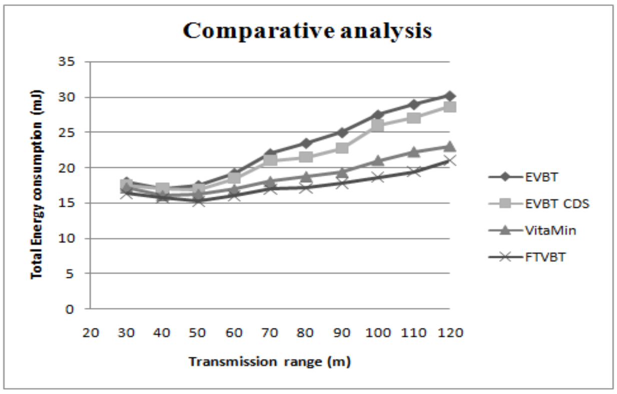

Figure-6. Energy consumption during delivery of data (No. of nodes = 200).

CONCLUSIONS

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 is maintained for longer, 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 attains effective security with less key storage overheads. Results proved that the proposed method gives better performance and achieved the major challenges in wireless sensor networks.

REFERENCES

[1] Abdoulaye Diop, Yue Qi and Qin Wang. 2014. Efficient Group Key Management using Symmetric Key and Threshold Cryptography for Cluster based Wireless Sensor Networks. I.J. Computer Network and Information Security. 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. 2015. 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. 2015. Group Key Management Technique based on Logic-Key Tree in the Field of Wireless Sensor Network. International Journal of Computer Applications. 117(12): 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. 4(4): 176-182

[6] Alagheband M.R., Aref M.R.2012. Dynamic and secure key management model for hierarchical heterogeneous sensor networks. Information Security. IET. 6(4): 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. 10(2); 371-383 .

[8] J. Zhang, V. Varadharajan. 2010. Wireless sensor network key management survey and taxonomy. Journal of Network and Computer Applications. 33(2): 63-75.

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

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

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

[12] Klaoudatou E., Konstantinou E., Kambourakis G. and Gritzalis S. A Survey on Cluster-Based Group Key Agreement Protocol.

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