A SECURE AND POWER EFFICIENT ROUTING IN WIRELESS SENSORE NETWORK

Dhruti N. Vashi[1] , Urmi Desai[2]
[1]P.G.Student, [2]Prof., CO Department,
Sarvajanik College of Engineering and Technology, Surat, India.
Email:[1]dhruti.vashi123@gmail.com,[2]urmi.desai@scet.ac.in

Abstract— Wireless sensor network (WSNs) is an incredible technology incredible technology which is to collect the information from the real world. With the limited battery power it consists of hundreds and thousands of nodes. The challenging task is how to route the information in secure manner to the base station with some pattern with power saving idea. In this paper we proposed a secure routing protocol called SAPER for the purpose of security data transfer. In this paper we have focused on energy efficient routing of information as well as data confidentiality. To fulfill this purpose minimum spanning tree is used for data routing purpose. Also for satisfy the security concern RC5 algorithm is used to keep the data secure from the intermediate node. Trade-off between energy constrains and security has been done in proposed technique.

Index Terms—Minimum spanning tree, RC5, TDMA, Wireless sensor network.

I. INTRODUCTION

An incredible technology called wireless sensor network (WSNs) have attained too much enthusiasm in today's world. Sensor network is the bridge between real physical world and virtual world. WSNs use nodes which have capabilities to sense, store, distribute and collect the information. Main motive of the sensor network is sense the data and pass it to the base station (BS). Data freshness and lifetime has to be focused when transfer the data to the base station. So selection of the path for routing has to be done more precisely.

In army field there may be some important as well as secrete information which has to be hide from the enemy. Encryption of the data gives the security from this kind of purpose. It is important that encryption takes less time as well as energy require for this purpose is also minimum. So lifetime of the network is not minimized.

The rest of the paper is ordered as follows: In Section 2, we initiate related work and problem with existing techniques. In section 3 we introduced problem definition. In section 4 we suggest our proposed scheme with radio model. Finally we present section 5 in which conclusion and future work.

II. RELATED WORK

Initial technique for routing was **direct transmission,** in which each node transmits its data directly to the base station. But it is not energy efficient. For moderate the numbers of nodes communicating straightly with the base station some techniques were proposed. **Cluster based routing** is one of them. In which nodes in entire network is separated by the clusters as shown in Fig 1. Each cluster elects one cluster head (CH) depending on different criteria. CH is responsible for transmit the data packet to the base station or sink. It is one kind of scalable and robust technique.

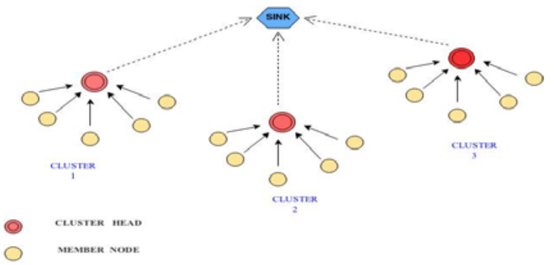

Fig 1: Cluster based routing

Chain based routing approach is one step ahead of cluster based approach then cluster based approach. As the name suggest there is a chain passing through all nodes where each node receive the data packets and transmit it to the nearest neighbor in the chain as in fig 2.

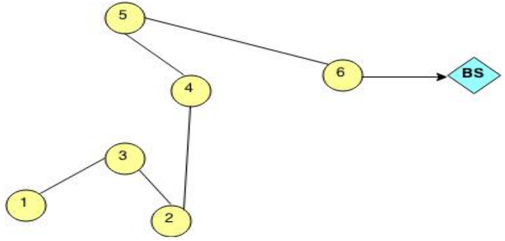

Fig 2: Chain based routing

Tree based routing approach is also used for power saving purpose. In which parent child relationship is maintained between nodes as in fig 3. Child route the data packet to its parent, this parent route to its parent and so on. This way routing process is move on. This technique maximizes the lifetime and reduced the total energy consumed in a round.

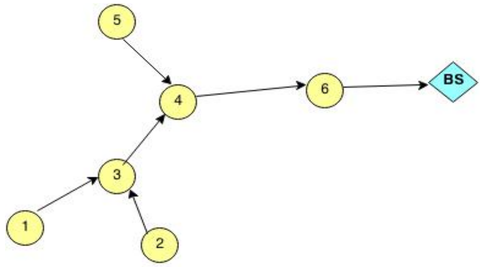

Fig 3: Tree based routing

Variety of routing schemes were proposed among which LEACH [9], PEDAP [1], BATR [3], CMST-DC [4], LC-MST [5], TRP [6], EESS [7], Reliable Multipath WSN routing protocol [8] are the hierarchical protocols which provide the fruitful solution for power efficient routing, which maximize the lifetime of the network also.

LEACH [9] divides the network into the cluster. There are cluster head for each cluster which can decide on some criteria which is predefined. CH is responsible to receive data from the other node in the cluster and aggregate them. There are two phase setup phase and steady-state phase in LEACH protocol. It used TDMA scheduling for the number of nodes in the network. LEACH has some drawbacks among them one is it does not give priority to the residual energy.

In PEDAP [1] prim's algorithm is used to build a minimum spanning tree for the routing purpose. BS is act as the root. In every iteration minimum weighted edge is selected which is not in the tree and added to tree. After some round base station will check all nodes were alive or not. Also it will check the energy level of each node in the tree.

In DMSTRP [2] nodes are divided into the clusters. All nodes in the cluster are connected by a minimum spanning tree, this MST also include cluster head. One another MST is used for connecting the CHs. There are four states in which lifetime of the process are divided. And they are -1 as routed state, 0 as initial state, 1 as candidate state, and 2 as prepare state.

In BATR [3] for finding the optimal path balanced tree has been made. In this balanced tree all nodes have almost same number of child. BS knows the position of all nodes by using GPS. Path construction process is starts form BS. After every iteration minimum weighted edge is selected as per the decided child. The number of child nodes, denoted by μ, is given as an operational parameter whose value can be calculated by:

$$\mu(R) = \frac{N * \Pi * R2}{A} \text{ [3]} \qquad (1)$$

Where, N is number of scattered sensor nodes in region and A, R is either range of a particular sensor or radio transmission range. This process repeats until all nodes are added to the tree. After certain number of round BS further computes the routing information.

In CMST-DC [4] there exists two phases. In the first phase cluster formation is done. CH is selected just as in LEACH algorithm. Then all nodes within the cluster make a tree using greedy algorithm. Then by connecting all cluster head higher level tree is made. Only one cluster head sends information to the base station. Minimum spanning tree is used to connect the nodes. The cluster head node is also act as starting node. This node broadcast a find-nearest –neighbor (FNN) message for finding nearest live node among all nodes in the cluster. This way connection is done in the tree. After cluster formation phase data transmission phase take place. In these sensors starts data collection operation. Each cluster head gathered data of its own cluster nodes.

In LC-MST [5] for making the weighted graph G (V, E) distance matrix D= $[dij]_{nxn}$ is used. For all i,j, least cost element is fined in every column j and other element is set as 0. And by using this preferred link matrix (PLM) is constructed. By using PLM node set matrix (NSM) is built. In NSM each element holds the node pairs that correspond to the favored link in PLM. Then by combining the node pair candidate spanning tree is constructed. If there are duplicate set of nodes or any set of node pairs which make a cycle or any pairs have largest cost then it has been removed.

In TRP [6] it is assumed that sensor nodes are circulate in a circle field. For recognize the distance sensor node used Receive Signal Strength Indication (RSSI). First network is deployed and then sink broadcast a sink_ADV message to the network. Then each node estimate relative distance between itself and sink using RSSI, which is called d_sink. For creating a tree all nodes broadcasts HELLO (ID, d_sink, En). When nodes receives this message they computes relative distance d form neighbor. After that each node creates table which is neighbor information table. From this table each node decides about their neighbor and also about their parent. If sink node is in the range of communication then it kept as the next hope, and if not then the node which is closer to sink and has minimum cost is kept as neighbor node. This way tree is made. And sink is kept as root.

In EESS [7] problem of TDMA is solved in which because of more quantity of packets sensor node have to wait until all other sensors complete their activity. In this approach entire network is divided into different groups which contain parent and child nodes. Parent node delivers the data to the sink which is collected from the child nodes. For preventing interference between nodes sensors were deployed as the spacing between them is kept as it is greater than or equal to the interference range. For each group load is calculated. Groups were scheduled as the decreasing order of the load. For scheduling strategy if two sensors of different groups are in the interference range of each other than they are not scheduled concurrently for transmission purpose.

In Multiple Wireless Sensor Network Routing Protocol scheme [8] network is divided into the cluster. Each member of the cluster was arranged into the single hope network topology. And cluster is again arranged in a tree structure, in which cluster head is connected. Each node has store the identity of the cluster head. Root node has the maximum number of child node. And as the level is increasing the number of child node is decreasing by $n/2^i$. Where n represent the number of child node of the parent node, i represent the level of the tree. Sink node randomly select one node in the cluster for the sensing purpose, which sense the data, store it and transfer it to the neighbor node. Neighbor node aggregates that data. This way all nodes in the cluster sense data and aggregate it until most of the cluster member has the identical value. Then randomly one of the nodes is selected for transfer the stored data to the cluster head. Cluster head is responsible for transfer this data to the sink node.

III. PROBLEM DEFINITION

In case of wireless sensor network power efficient routing is becoming more important in issue that has to be focused. There are several amazing schemes available for efficient routing in WSN, but each having their own powerful and risky feature. So a new efficient approach can be developed by improving security and power saving idea. Another primary concern is confidentiality of data that is security of the information which were route to the base station. Compulsory we have to do trade-off between these two features but by saving some energy in the routing we can maximize the lifetime of the nodes. We are doing the same in our proposed algorithm. For routing purpose we use the minimum spanning tree which uses residual energy for making tree. And for confidentiality we use RC5 algorithm which is symmetric key algorithm. RC5 provide confidentiality to the data as well as take care about the freshness of data and also consumes less energy for encryption purpose.

IV. PROPOSED ALGORITHM

In proposed algorithm secure and power efficient routing we used first order radio model used in [1]. It is assumed that radio channel is symmetric so the cost of trasmitting packet from A to B and B to A is same. For distance d transmit k-bit packet energy required is:

$$E_{Tx}(k , d) = E_{elec} * k + E_{amp} * d^{2} \text{ [1]} \tag{2}$$

To receive that packet energy required is:

$$E_{Rx}(k) = E_{elec} * k \text{ [1]} \tag{3}$$

So, the cost of one transmission of the k bit packet from node i to j with distance d is:

$$C_{ij}(k) = 2*E_{elect} * k + E_{amp} * k * d^{2}_{ij} \text{ [1]} \tag{4}$$

The cost of one transmission of the k bit packet from node i to base station with distance d is:

$$C'_{i}(k) = E_{elect} * k + E_{amp} * k * d^{2}_{ib} \text{ [1]} \tag{5}$$

In proposed algorithm SAPER We assume that location of the sensor node is fixed. At the time of deployment of the network the symmetric key value is provided to the nodes. This value is also known by the base station. Nodes only aware with their own key value, another node's key value do not known by them. In initial state base station (BS) send the route request to the nodes in the network. Nodes reply with the route reply (RREP) packet. On the bases of the time require to receive the RREP packet base station get to know about the location of the nodes. By using this information base station calculate the minimum spanning tree (MST) and send the path to the nodes. Also base station gives the time schedule by using TDMA scheduling technique to the node. So with this information nodes send the sensed data to the base station. At the scheduled time if node do not have the data for the base station then the nodes of that entire path were put in the sleep mode. If node have some information to route then it first encrypt the data with help of the key which is distributed at the time of deployment with RC5 algorithm. Then it will route to the base station. So data confidentiality is provided to the data. Any intermediate node is also note able to read the data. If this data is stolen by any attacker then also it will not able to read or decrypt that data because of missing key value. After certain number of rounds the MST is further calculated. The residual energy is also used to build the MST. Nodes having the less energy get fewer loads. This way nodes energy will used efficiently. And nodes do not earlier. Figure 4 shows the flowchart of the SAPER. By using MST data will send with the minimum delay, so data freshness is present. In SAPER nodes were put in the sleep mode if they have no data to send so this way other nodes do not have to wait more for their turn and the time and energy both utilize extremely well.

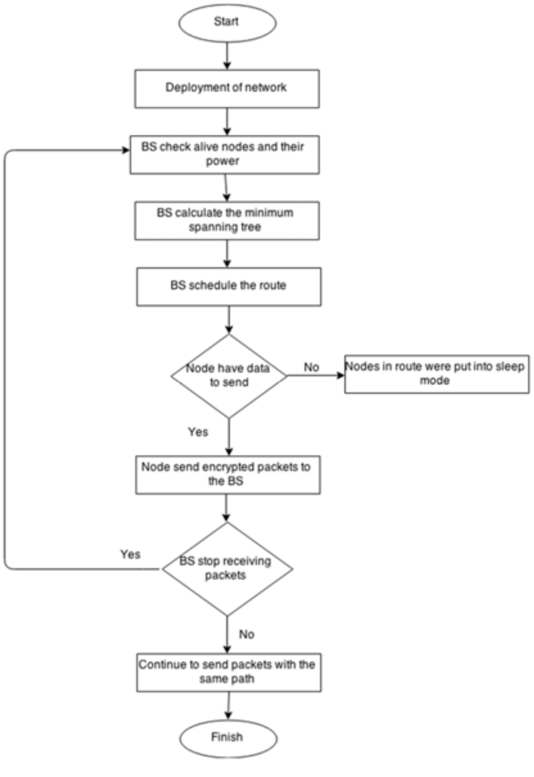
Start
Deployment of network
BS check alive nodes and their power
BS calculate the minimum spanning tree
BS schedule the route
Node have data to send
No
Nodes in route were put into sleep mode
Yes
Node send encrypted packets to the BS
Yes
BS stop receiving packets
No
Continue to send packets with the same path
Finish

Fig 4: Flowchart of SAPER

SAPER uses RC5 which is symmetric key encryption algorithm which keep the data safe. Also the encryption-decryption time taken by RC5 is less than any asymmetric encryption. There are numerous methods exist for the confidentiality purpose. Asymmetric encryption is one of them but it is not affordable to use that in sensor network. The reason is it takes more time for encryption purpose so the freshness of data has compromised. Also energy consumption done by the asymmetric encryption is more so node get die very earlier and it is unacceptable. Primary concern of the sensor network is energy consumption reduction for longer lifetime so by using RC5 as compare to the asymmetric encryption we reduce the power consumption.

V. Conclusion

In this paper we explored SAPER algorithm by doing tread-off between power consumption and security. By using minimum spanning tree we save the energy of node as well as improved the lifetime of the network. RC5 provide the confidentiality by compromising some power. In future we will try some another technique for security purpose to reduce the power consumption with same level of security.

References

[1]. H. Tan, I. Korpeoglu, “Power Efficient Data Gathering and Aggregation in Wireless Sensor Networks” ACM SIGMOD Record, pages 66-71, 2003 ACM.

[2]. G. Huang, X. Li, and J. He, “Dynamic Minimal Spanning Tree Routing Protocol for Large Wireless Sensor Networks”, 2006 IEEE.

[3]. H. Kim, K. Han, “A Power Efficient Routing Protocol Based on Balanced Tree in Wireless Sensor Networks” 1st International Conference on Distributed Frameworks for Multimedia Applications, 2005 IEEE.

[4]. C. Liang, Y. Huang and J. Lin “An Energy Efficient Routing Scheme in Wireless Sensor Networks” 22nd International Conference on Advanced Information Networking and Applications, 2008 IEEE.

[5]. M. Hassan, “An efficient method to solve least-cost minimum spanning tree (LC-MST) problem” Journal of King Saud University – Computer and Information Sciences, pages 101-105, 2011 Elsevier.

[6]. B. Gong, T Jiang, “A Tree-Based Routing Protocol in Wireless Sensor Networks”, 2011 IEEE.

[7]. P. Shrivastava, B. Pokle, “An Energy Efficient Scheduling Strategy for Data Collection in Wireless Sensor Network” International Conference on Electronic Systems, Signal Processing and Computing Technologies, 2014 IEEE.

[8]. A. Chatterjee, D. Mukherjee, “Reliable Multiple Wireless Sensor Network Routing Protocol scheme for Network Lifetime Maximization” 2nd International Conference on Business and Information Management (ICBIM), 2014 IEEE.

[9]. W. R. Heinzelman, A. Chandrakasan, and H. Balakrishnan,“Energy efficient communication protocol for wireless microsensor networks,”33rd Annual Hawaii International Conference on System Sciences,2000.

[10]. S. Othman, A. Trad, H. Youssef, “Performance Evaluation Of Encryption Algorithm For Wireless Sensor Networks” International Conference on Information Technology and e-Services, 2012 IEEE.