Secured Dynamic Routing Strategy in Wireless Sensor Networks

A.Ramakrisha , P.VijayaBharathi

Abstract-Recent years usage of wireless sensor networks (WSNs) are increased. These are used in many applications, including environmental monitoring and military field surveillance .In Wireless sensor networks network topology, routing and security place the major role for communication. Generally Dynamic Clustering is an efficient topology management approach for sensor networks. But routing in cluster is difficult due to the dynamic nature of the nodes. Another biggest problem in WSNs is that they are very defenseless to security threats because of less memory and processing capability. In this paper we proposed strategies to improve the energy efficiency for data transmission based on clustering hybrid routing algorithm to finding best route and we also proposed CA (certificate authority) security strategy to increases the security level in cluster based communication.

Index Terms: bound list, certification authority, cluster, cluster list, reliability, transmission range, and region

1. INTRODUCTION

Wireless technology has propagated the use of sensor networks in many applications. Recent years have witnessed an increasing interest in using wireless sensor networks (WSNs) in many applications, including environmental monitoring and military field surveillance. In these applications, tiny sensors are deployed and left unattended to continuously report parameters such as temperature, pressure, humidity, light, and chemical activity[1]. Reports transmitted by these sensors are collected by observers (e.g., base stations).The dense deployment and unattended nature of WSNs makes it quite difficult to recharge node batteries. Therefore, energy efficiency is a major design goal in these networksSensor networks joins small sized sensors and actuators with general purpose computing components. Such networks comprise of hundreds and sometimes thousands of self-functioning, low power, inexpensive wireless nodes to observe and influence the surroundings.

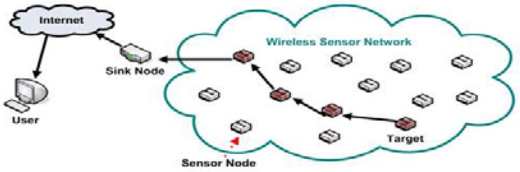


Figure: 1 sample wireless sensor network

Wireless sensor networks usually consist of a single or multiple base stations acting as points of centralized control, whereby they provide access to other networks. These networks are unique in their dynamic network topologies [2]. A network topology is usually selected depending on the type of application the sensors are used for or where it is situated.

The types of topologies used for sensor networks include star, mesh, star-mesh etc. In Wireless sensor networks there are two kinds of wireless nodes: sensor and base station nodes [1]. The main function of the base station (also referred to as sinks) relies on managing the actions executed to provide reliable and efficient sensing support. It provides a gateway to other networks or acts as a data storage processing data in a powerful way.

It even acts as an access point to human interface for human interaction, and is capable of broadcasting control data in the network or removes data from it. The base station node will calculate and send the even source, its position and a timestamp to the analysis centre. If an alert is received by the base station regarding a target, an identity of the target will be allocated allowing all related alerts getting appropriate management. Every sensor within the network primarily consists of a certain amount of power and a base station that provides entrance to other networks or to the centre analysis. It is important to know that base stations have significant features over other nodes in the network. They comprise of adequate battery power to exceed the existence time of all sensor nodes, and have the capacity to save cryptographic

- *A.Ramakrishna ,Asst.Professor,Department of CSE
Vignan's Institute of Engineering for women
Visakhapatnam ,INDIA 530046 email:arknrpm@gmail.com*
- *P VijayaBharathi ,Asst.Professor,Department of CSE
Vignan's Institute of Engineering for women
Visakhapatnam ,INDIA 530046 .*

keys, well-built processors and resources to commune with external networks. In contrast to the base stations, in a sensor network a large number of sensor nodes are connected together with radio frequency communication links, giving much significance to broadcasting in the network.

The main functions associated with sensor nodes include: collecting information on the target with consideration to their nature and positioning, which involves the communication from nodes to base stations regarding for example sensor readings and particular alerts. Nodes should be capable of producing real-time events on detected targets using the base station node to forward an even transmission to a centre for the event to be analyzed. Base stations may request updates from sensor nodes, resulting in base station to node communication. Finally the generated events will be relayed to the base station from the sensor nodes. In this part of the communication architecture, base stations contact all of the nodes it is assigned for purposes such as routing beacons or reprogramming of the complete network.

2. Problem Statement

2.1 Network Model

Considering a set of nodes and a sink deployed in a sensing area, we assume the sensor network has the following properties [2]:
1) The mission of the sensor network is gathering sensor data from sensor nodes to sink, such that the destination of every sensing data is the sink.
2) The network is organized into clusters. The cluster member sends sensing data to its cluster head directly and the cluster head transmits the data to its next hop cluster head for relaying data to the sink.
3) Each node has a maximum transmission range noted as TR. This motivates the need for keeping connectivity with the limitation.
4) The critical transmitting range is less than TR.

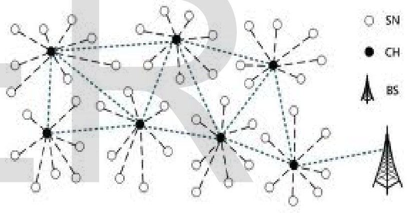
2.2 Clustering and Routing Problem

In this paper, the special clustering is referred to the change of the status. Every node begins with the status of IDLE. When there is data needed to be transmitted, the node becomes candidate (CND). The clustering algorithm is run to make the decision about whether to be cluster head (CH) or cluster member (CM) that belongs to a cluster. Then it could transmit its data to the sink through the routes built by the routing algorithm. When the mission is completed, the node could return to IDLE status. Our goal is to design a special hybrid clustering, routing protocol and secured communication with joint consideration of cluster head selection and routing discovery. Specifically, the design goals are given as follows:
1) The clustering and routing discovery are hybrid. At the end of the protocol, each node is either a CH or a CM, and has selected a node as its next-hop relay.
2) The network is ensured to be connected, i.e. every node could transmit its data to the sink using limited Transmission range bounded by TR.
3) Every head node need prove their authorization based certificate authority model to other head.
4) Cluster heads are well-distributed over the sensor field to achieve the energy efficiency.

3. Cluster Description

3.1. Cluster in wireless sensor networks:

Clustering a wireless sensor network means partitioning its nodes into clusters, each one with a cluster head and some ordinary nodes as its members. The task of being a cluster head is rotated among sensors in each round to distribute the energy consumption across the network. Clusters closer to the base station have smaller cluster sizes, thus they will consume less energy during the intra-cluster data processing, and can conserve some more energy for the inter-cluster relay traffic. Ordinary nodes become tentative cluster heads.



SN-sensor node CH-cluster head BS-base station
Figure-2 relationship between cluster heads

3.2. Cluster Formation

Routing from one node to another will consist of routing inside a cluster and routing from cluster to cluster. A change in the dynamic network may or may not result in a change in the cluster compositions. We have identified four different possible types of changes in the dynamic network graph in the Occurrence of a single event. We assume that each cluster has a unique indenters, id. Each node maintains a list of its neighbors, a list of clusters (Cluster List) in the network, and a list of boundary nodes (Bound List) in the network.

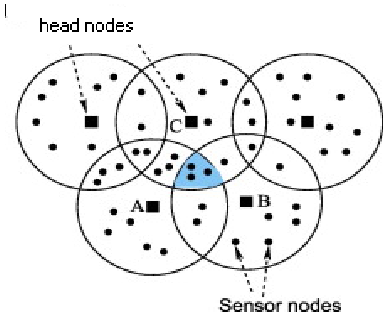


Figure-3 sample overlapping cluster

There can be multiple boundary nodes between overlapping clusters. If there are multiple boundary nodes between clusters, the one can also be used with the biggest cluster set is chosen to be the boundary node and is maintained in the Bound List. Note that a node can be a boundary node for more than two overlapping clusters. In a connected network, Cluster List is the same in all the nodes. It is not true in a partitioned network. This is because nodes in a partitioned network may not be aware of all the clusters in the network. Clustering in WSNs involves grouping nodes into clusters and electing a CH such that the members of a cluster can communicate with their CH directly and a CH can forward the aggregated data to the central base station through other CHs.

4. Routing Protocol

A routing protocol can be divided into two phases, namely, route construction and route maintenance.

1. During the route construction phase, routes are constructed between all pairs of nodes.
2. The route maintenance phase takes care of maintaining loop-free routes in the face of unpredictable topological changes.

4.1 Route Construction Phase

The protocols to maintain clusters in the face of various network events have been explained earlier. Upon receipt of new cluster information, a boundary node stores the new cluster list in its Cluster List, the new boundary list in its Bound List, and then rebroadcasts the information. A boundary node has to forward the new information only once. Nodes other than the boundary nodes listen to this information and just update their tables. In this manner, the information about each network event is distributed to all the nodes. Each node now has the topology information of the whole network. For a connected network, the boundary nodes also form a connected network.

If a cluster has multiple boundary nodes, the nodes in that cluster will choose the boundary node with the shortest path for a destination as the next hop node for the destination. The next hop node and the number of hops for each destination are maintained in the Routing Table. Each message packet contains the identifier of the destination node in its header. When a node receives a message packet, it looks up the Routing Table to determine the next hop node for the packet's destination. The node then forwards the message packet to the next hop node. This process of forwarding continues till the packet reaches its destination.

4.2 Route maintenance Phase

Hybrid routing algorithm is combination properties of Hierarchical Routing and link state routing. In this algorithm each cluster assumed as region .In each region header node routing table contains all its neighbors' information and its own sensor nodes information. This information is updated based on link state routing algorithm. Every CH update their routing information based on link state routing algorithm .Due to dynamic nature of the WSN every time there is the possibility of changing of nodes and clusters so that every time CH requires update their information for the faster communication. This purpose we are using link state routing properties. Each CH must do the following:

1. Discover its neighbors (CH).
2. Measure the cost to each of its neighbors.
3. Send updated information to all other CH.
4. Compute the shortest path to every other CH using Dijkstra's algorithm.

Finally each CH maintain routing table that contains information about all other nodes. Initially each CH identifies their neighbors based on distance (cost) and collect the other clusters information from neighbors. Based on the collected information it's creating a message i.e forwarded to the all other nodes in the network. Then each node in the network knows others nodes information. Hybrid algorithm useful to identify be best routes based on neighbor's information.

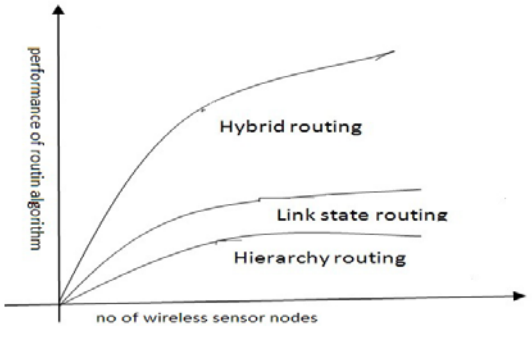
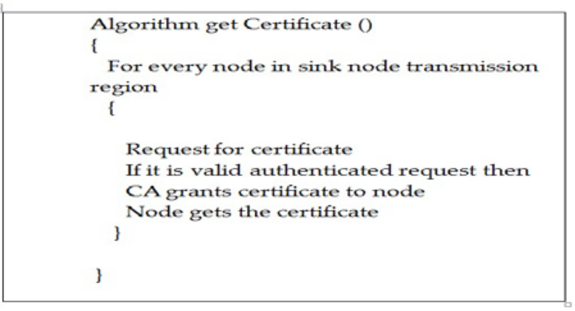


Figure 4 .performance of Hybrid routing algorithm

5. Security in clusters communication

Many researchers have been carried out in the field of wireless sensor networks since a long time. The issues that make this research more challenging are the wireless nature of these sensor nodes [8]. Wireless sensor networks are difficult to secure as, the limited memory resources rule out the pre distribution of keys or certificates, and manual device configuration in the field is not feasible due to the dynamic and ad-hoc nature of wireless sensor networks.

The issue of securing a wireless sensor network is further challenging due to the fact that WSN nodes are not tamper resistant and operate over an unsecure wireless medium. Public key encryption methods are useful to protect the communicated information .but in cluster communication we use CA for validating cluster nodes to other cluster nodes.



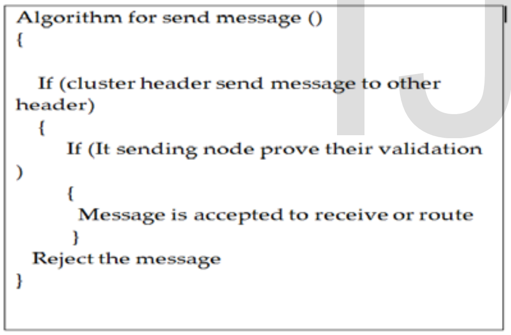
```
Algorithm get Certificate ()
{
  For every node in sink node transmission
region
  {

    Request for certificate
    If it is valid authenticated request then
    CA grants certificate to node
    Node gets the certificate
  }

}
```

Figure 5. Algorithm represents get certificate

Using this algorithm every node in sink transmission range need to ask the permission i.e. certificate from CA to communicate other nodes within its transmission range. The sink node check their authentication if it is valid it grants a certificate to the node otherwise rejected.



```
Algorithm for send message ()
{

  If (cluster header send message to other
header)
  {
    If (It sending node prove their validation
)
    {
     Message is accepted to receive or route
    }
  Reject the message
}
```

Figure 6. Algorithm for send message

If any node or header node want to send some information to other header node in the cluster they need to prove their validation based on certificate. If certificate is valid the message is accepted to route or receive. The LEAP is useful for protecting information in cluster communication.

5.1 Overview of LEAP

LEAP (Localized Encryption and Authentication Protocol), is a key management protocol intended for large-scale wireless sensor networks where the nodes have limited power, processing, and memory resources. In order to support the in-network processing necessary for most applications of these networks while at the same time providing security properties, such as security and authentication, similar to those of pair wise symmetric keys, LEAP species four types of keys: individual keys, pair wise shared keys, cluster keys and group keys. Individual keys are symmetric keys shared between the base station and each of the nodes. For example, a node might use the individual key to notify the base station of a suspicious neighbor. Pair wise shared keys are symmetric keys shared between a node and each of its neighbors. While pair wise shared keys are used to establish cluster keys, they prevent passive participation which is desirable for in-network processing. Cluster keys are symmetric keys shared between a node and all of its neighbors. These cluster keys can be used for locally broadcast messages such as a routing protocol might use and are also used for updating the group key. The group key, a symmetric key shared between the base station and all of the nodes, allows encrypted and authenticated messages to broadcast through the whole network. LEAP's goal is to satisfy the security properties of authentication (which they do not define) and confidentiality in a wireless environment where the intruder may eavesdrop, inject packets, and replay messages.

5. Conclusion

In this paper we proposed cluster topology approach to reduce the communication overhead and exploit data aggregation in sensor networks. We have focused on security issues on distributed clustering approaches, which are more suitable for large-scale sensor networks. We are proposed dynamic routing strategy for improvement of communication speed and also surmise that the LEAP based security and intra clustering problems. Finally this paper specifies efficient usage of energy in sensor nodes and secured communication clustered based wireless sensor networks.

6. Acknowledgment

We are thankful to IJSER members for their suggestions and also thankful to our principal vignan's Institute Engineering for women for supporting and encouraging innovative ideas.

7. REFERENCES

[1] I. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A survey on sensor networks," *IEEE Commun. Mag.*, vol. 40, no. 8, pp. 102–105,2002.

[2] O. Younis and S. Fahmy, "Heed: A hybrid, energy-efficient, distributed clustering approach for ad hoc sensor networks," *IEEE Trans. Mobile Comput.*, vol. 3, no. 4, pp. 366–379, 2004.

[3] S. Fang, S. Berber, and A. Swain, "An overhead free clustering algorithm for wireless sensor networks," in *Global Telecommunications Conference, 2007. GLOBECOM '07. IEEE*, Nov. 2007, pp. 1144–1148.

[4] S. Soro and W. B. Heinzelman, "Cluster head election techniques for coverage preservation in wireless sensor networks," *Ad Hoc Networks*, vol. 7, no. 5, pp. 955–972, 2009.

[5] M. Younis and K. Akkaya, "Strategies and techniques for node placement in wireless sensor networks: A survey," *Ad Hoc Networks*, vol. 6,no. 4, pp. 621–655, 2008.

[6] A. Perrig, J. A. Stankovic, and D. Wagner, .Security in wireless sensor networks,. *Commun. ACM*, vol. 47, no. 6, pp. 53.57, 2004.

[7] S. Zhu, S. Setia, and S. Jajodia, .Leap+: Ef_cient security mechanisms for large-scale distributed sensor networks,. *TOSN*, vol. 2,no. 4, pp. 500.528, 2006.

[8] S. Zhu, S. Setia, and S. Jajodia, .Leap: efficient security mechanisms for large-scale distributed sensor networks,. in *ACM Conference on Computer and Communications Security*, 2003, pp. 62.72.

[9] J. K. Millen and V. Shmatikov, .Constraint solving for bounded-process cryptographic protocol analysis,. in *ACM Conference on Computer and Communications Security*, 2001, pp. 166.175.

[10] J. C. Mitchell, M. Mitchell, and U. Stern, .Automated analysis of cryptographic protocols using mur-phi,. in *IEEE Symposium on Security and Privacy*, 1997, pp. 141.151.

[11] D. Dolev and A. C.-C. Yao, .On the security of public key protocols,. *IEEE Transactions on Information Theory*, vol. 29, no. 2, pp. 198.207, 1983.

[12] L. Tobarra, D. Cazorla, F. Cuartero, and G. Diaz, .Analysis of security protocol MiniSec for Wireless Sensor Networks,. in *Proc. Of the IV Congreso Iberoamericano de Seguridad Informatica (CIBSI'07)*, November 2007, pp. 1.13.