INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY
WINGS TO YOUR THOUGHTS.....

Dynamic Cluster & Encrypted Data Routing Protocol For Hierarchical WSNs

Neha Gupta[1], Vinay Rana[2]

[1]M.Tech, IITB College,DCRUST Murthal, INDIA
[2]A.P., IITB College, DCRUST Murthal, INDIA
neha86gpta@gmail.com, vinay.rana237@gmail.com

Abstract: *Wireless sensor networks consist of hundreds or thousands of micro sensor nodes which are small battery powered devices with limited energy resources. Once deployed, the small sensor nodes are usually inaccessible to the user, and thus replacement of the energy source is not feasible. Hence, the energy efficiency is a first key design issue that needs to be enhanced in order to improve the life span of the network and the second one is secure transmission. There are several network layer protocols have been proposed to improve the effective lifetime of a network with a limited energy supply but all are ignoring the secure transmission implementation using minimum energy. In this paper we design a routing protocol named DCERH. This protocol is base station assisted i.e. this protocol utilizes a high-energy base station to set up clusters and routing paths, perform randomized rotation of cluster heads, and carry out other energy-intensive tasks. Encrypted data is sent to base station from lower level and upper level cluster heads. However using a central control algorithm to form the clusters produces better clusters by dispersing the cluster head nodes throughout the network. So, in terms of power it will be highly power efficient. It is centralized since in this protocol, rather than self-configuration, base station is used (that is centralized located in the sensor field). Lastly, the new protocol DCERH will be compared with Leach –C with and without security.*

Keywords: *Wireless sensor networks; Routing protocols; Energy efficiency; Hierarchical routing; Centralized routing: Scalability*

1. INTRODUCTION

Wireless Sensor Networks consist of tiny sensor nodes that, in turn, consist of sensors (temperature, light, humidity, radiation, etc.), microprocessor, memory, transceivers, and power supply. In order to realize the existing and potential application for WSNs, advanced and extremely efficient communication protocols are required [1]. In WSNs sensor nodes are densely deployed either inside the phenomenon or very close to it. The wireless sensor node, being a small device, can only be equipped with a limited power source. In some application it is impossible to replacement of power resources However, routing protocols for all Wireless Sensor networks, regardless of the application, must try to maximize the network life time and minimize the overall energy consumption in the network. Network lifetime is a critical concern in the design of WSNs. In many applications, replacing or recharging sensors is sometimes impossible [2]. Therefore, many protocols have been proposed to increase network lifetime. It is difficult to analyze network lifetime because it depends on many factors, like network architecture and protocols, data collection initiation, lifetime definition, channel characteristics, and the energy consumption model [3]. For all routing protocols, energy consumption during communication is a major energy depletion parameter; the number of transmissions must be reduced as much as possible to achieve extended battery life. For these reasons, the energy consumption parameter is a top priority [4]. The other important factor for WSNs is security, as sensor nodes communicate sensitive data, so it is necessary to ensure that any intruder or other neighboring network could not get confidential information intercepting the transmissions. One standard security method of providing data confidentiality is to encrypt data and use of shared key so that only intended receivers can get the sensitive data.

2. BACKGROUND

2.1 BCDCP:

A centralized routing protocol called BCDCP [5] which distributes the energy dissipation evenly among all sensor nodes to improve network lifetime and average energy savings. This protocol utilizes a high-energy base station to set up clusters and routing paths, perform randomized rotation of cluster heads, and carry out other energy-intensive tasks. BCDCP used to operates in *setup* and *data communication* phase.

2.2 SHPER:

A hierarchical scheme is used in SHPER [6] protocol. In SPHER the election of the cluster heads is not

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY
WINGS TO YOUR THOUGHTS.....

randomized rather it is based on the residual energy of the nodes. Cluster head selection is done by the base station itself. Base station asks each node to send their residual energy initially. And based on the energy of each node and the predefined percentage of cluster heads, base station selects the cluster head. The operation of SHPER [7] protocol works in two phases: Initialization phase, and Steady state phase.

Though BCDCP and SPHER are centralized based hierarchical protocols but few shortcomings are associated with them in terms of Security and Energy Dissipation. So, in this paper, we will present a new protocol named DCERH which combines the above two protocols. To make it more efficient, Security is also added while data communication is going on. Security is based on the scheme of Homomorphic Encryption.

2.3 HOMOMORPHIC ENCRYPTION

A Homomorphic Encryption [8] scheme allows arithmetic operations on cipher texts. One example is a multiplicatively Homomorphic scheme, where the decryption of the efficient manipulation of two cipher texts yields the multiplication of the two corresponding plaintexts. Homomorphic encryption schemes are especially useful whenever some party not having the decryption key(s) needs to perform arithmetic operations on a set of cipher texts.

2.3.1 ENCRYPTION SCHEME USING RANDOM KEYS

The main idea is to replace the xor (exclusive-OR) operation typically found in stream ciphers with modular addition. The basic scheme is as follows:

Basic Additively Homomorphic [9] Encryption Scheme:-

Encryption:

(1) Represent message m an integer m Є [0, M -1] where M is the modulus.

(2) Let k be randomly generated key stream, where k Є [0, M - 1].

(3) Compute c = Enc k (m) = m+ k mod M.

Decryption:

(1) Deck(c) = c - k mod M.

Addition of Cipher texts:

(1) Let c1 = Enc k1 (m1)
and c2 = Enc k2 (m2).

Aggregated cipher text:

(2) cl = c1 + c2 mod M = Enc k (m1 + m2) Where k = k1 + k2 mod M.

The correctness of aggregation [3], [6] is assured if M is sufficiently large.

The reason is as follows:

c1 = m1 + k1 mod M and c2 = m2 + k2 mod M. Then cl = c1 + c2 mod M = (m1 + m2) + (k1 + k2) mod M = Enck1+k2 (m1 + m2).

For k = k1+k2, Dec k(cl) = cl -k mod M = (m1+m2)+(k1+k2)-(k1+k2) mod M = m1 +m2 mod M.

We assume that m < M. Note that, if n different ciphers ci are added, M must be larger than ni=1mi. Otherwise, correctness does not hold. In fact, if ni=1mi > M, decryption produces m < M. Note that this basic scheme is provided for illustration purposes only and does not represent the actual construction. Since the encryption key k, is assumed to be randomly chosen by each sensor node in very reporting session, a secure channel has to be maintained at all times between each sensor node and the sink. In the actual construction, such a secure channel is not required.

The security principles in WSNs are usually focused on cryptography. However, due to the constraints in WSNs, many already existing secure algorithms are not practical [7]. In this paper our goal is to achieve the Confidentiality of sensing data and Minimum Energy Consumption by combining the best features of BCDCP and SHPER protocol

3. PROPOSED ALGORITHM

The foundation of ***Dynamic Cluster & Encrypted Data Routing Protocol for Hierarchical WSN (DCERH)*** lies in the realization that the base station is a high-energy node with a large amount of energy supply. Thus, DCERH utilizes the base station to control the coordinated sensing task performed by the sensor nodes. In DCERH the following assumption are to be considered. A fixed base station is located far away from the sensor nodes.

- The sensor nodes are energy constrained with a uniform initial energy allocation.
- The nodes are equipped with power control capabilities to vary their transmitted power.
- Each node senses the environment at a fixed rate and always has data to send to the base station.
- All sensor nodes are immobile.

The radio channel is supposed to be symmetrical. Thus, the energy required to transmit a message from a source node to a destination node is the same as the energy required to transmit the same message from the destination node back to the source node for a given SNR (Signal to Noise Ratio). Moreover, it is assumed that the communication environment is contention and error free. Hence, there is no need for retransmission. Each node has the ability of monitoring its residual energy. The initial energy of nodes is selected to be the same for all nodes and set to 2J.

The two key elements considered in the design of DCERH are the sensor nodes and base station. The sensor nodes are geographically grouped into clusters[10] and

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY
WINGS TO YOUR THOUGHTS.....

capable of operating in two basic modes, the cluster head mode and the sensing mode.

In the sensing mode, the nodes perform sensing tasks and transmit the sensed data to the cluster head. In cluster head mode, a node gathers data from the other nodes within its cluster, performs data fusion, and routes the data to the base station through other cluster head nodes. The base station in turn performs the key tasks of cluster formation, randomized cluster head selection, and CH-to-CH routing path construction. DCERH is a wireless sensor routing protocol with the base station being an essential component with complex computational abilities, thus making the sensor nodes very simple and cost effective. DCERH operates in two major phases: *setup* and *data communication* phase.

Set up phase:

Set up phase includes the cluster set up, cluster head selection and Cluster head to cluster head routing path Here main activities include to identify the number of cluster head nodes and to group other nodes into cluster so that overall energy consumption is minimized . The steps involved in this phase are as follows:

Step 1: Initially, base station is centralized and all the nodes in the network have energy equal to 2 J. Now Base station sends an START message to all the nodes in the sensor field, to gather information about the node's residual energy and their neighbor list.

Step 2: After receiving the "START" message, each node broadcasts the "HELLO" message. After receiving "HELLO" message each node sends "REPLY" message containing its Node ID.

Step 3: When a node gets reply, it will note down the Node ID of the node from where the reply has been acknowledged. In this way each node will have their individual neighbor list.

Step 4: After receiving the information about their neighbors the nodes, for which the base station is within their range, sends a STATUS message to the base station. This STATUS includes ID, Neighbor list, and Energy of the node as shown in figure 1.

Step 5: Base station sends an acknowledge (ACK) to all sending nodes.

Step 6: When nodes are acknowledged, ACK, the nodes set their level to one which was initially zero and broadcasts a gateway advertisement GW_ADV to all its neighbors.

Step 7: Nodes receiving GW_ADV will check their level. If a node's level is zero (i.e. a node has not sent their status yet) it sends their STATUS to the node advertising gateway. In this case, a node can receive a GW_ADV from many of the nodes but it will reply only to that node from where it has received GW_ADV message first.

Step 8: After receiving the STATUS, gateway sends an ACK to the nodes, from where it has received the STATUS, and forwards this STATUS to the other gateway or to the base station directly (if directly connected).

Steps 6 to 8 are continuously replayed until all the nodes send their STATUS to the base station, directly or via gateway. At this time base station has acquired all the information about logical structure of the sensor field.

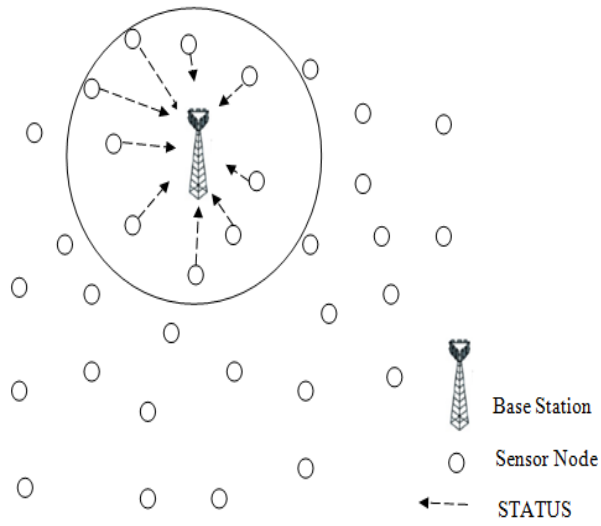

Figure 1: Sensor Nodes Sends their STATUS to Base Station

Step 9: Since the nodes, for which the base station is within the range, can send their data directly to it. For such types of nodes the base station is assigned as their cluster head.

Step 10: Base station computes the average energy level avgE for those nodes (let it be Z) that have not been declared as cluster head themselves yet, but have been assigned with cluster head having their neighbors' count greater than zero.

Step 11: Out of Z nodes, select a node N as a cluster head CH, whose energy is greater than avg. E and has maximum number of neighbors.

Step 12: Assign selected CH as cluster head to the rest of unassigned neighbors as shown in Figure 1.6. We will repeat the steps from 11 to 13 until Z is greater than zero.

Data transmission phase:

Step 13: Base station broadcasts cluster information that includes the ID's of the cluster head, along with the set of (Z-N) numbers of keys, non-cluster head nodes belongs to which cluster head in addition to hard and soft thresholds values.

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY
WINGS TO YOUR THOUGHTS.....

Step 14: Every cluster head informs each one of its cluster nodes when it can transmit, according to the TDMA schedule which is broadcasted back to the nodes in the cluster. Nodes sends the sensed data along with its key value, in its TDMA slot to their respective cluster heads, that will be selected according to the minimum distance of a particular node from cluster heads and energy consumption will be calculated. In a way similar to that proposed in TEEN protocol hard and soft thresholds are used in DCERH too.

Step 15: Each cluster head receives the data from its cluster nodes. When all the data have been received, each cluster head performs signal processing functions to aggregate the data it has received along with its own data into a single composite message. This composite signal also contains the ids of the nodes. After each cluster head has created its aggregate message, it waits until its own time slot in order to transmit it to the base station, either directly or via intermediate upper level cluster heads. The appropriate route selected to send data from lower level cluster heads to higher level cluster heads takes into consideration both the residual energy of nodes and the energy consumption for all possible paths.

Step 16: The base station collects all the encrypted messages transmitted to it. New cluster heads are determined by the base station by using the data of the received message. More precisely, the node having the highest residual energy and maximum number of neighbors, in each cluster, is elected to be the new cluster head. Additionally, the new soft and thresholds are defined.

Step 17: The base station gets the decrypted messages by subtracting the sum of values of set Q. BS decrypts the received data by subtracting all the key values, to get the original message or data.

4. PARAMETERS AND RESULTS

In this work the performance is measured by quantities matrices of average energy dissipation, system lifetime and number of nodes that are alive. Throughout the simulation, network node configuration is considered with 100 nodes where, each node is assigned an initial energy of 2 Joules. Figure 2 shows the average energy dissipation over the number of rounds of operation. This plot clearly shows that DCERH (without security) has a much more desirable energy expenditure curve than that of LEACH-C [11]. DCERH by having only multi-hop cluster head nodes to forward the data to the base station. This in turn decreases the communication energy cost for those DCERH nodes that have close neighbors

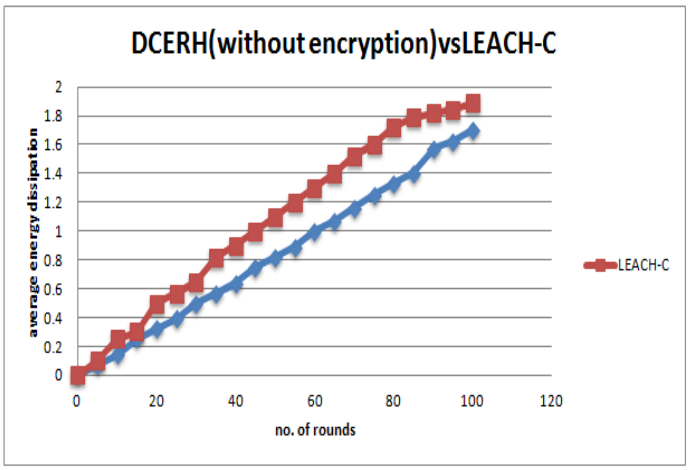

Figure 2: A Comparison of DCERH's Avg. Energy Dissipation

The improvement gained through DCERH is further exemplified by the comparison graph in Figure 3. This plot shows the energy dissipation over the number of rounds of activity for the 100 m × 100 m network scenario. On average, DCERH consumes 10 percent extra energy to achieve encryption.

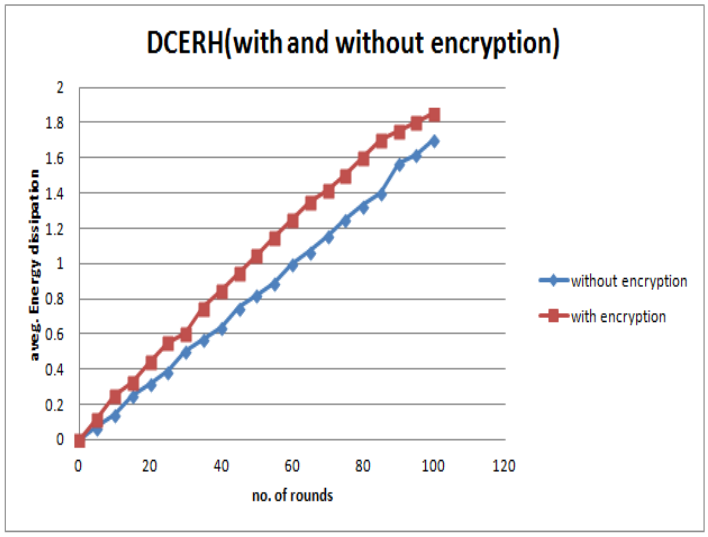

Figure 3: DCERH (with and without encryption)

5. CONCLUSION & FUTURE SCOPE

In this paper, we look at routing protocols, which can have a significant impact on the overall reliability and energy dissipation of these networks. In this paper, we proposed "**Dynamic Cluster & Encrypted Data Routing Protocol for Hierarchical WSNs**. In non-centralized hierarchical routing, sensor nodes self configured for the formation of cluster head. While self

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY

WINGS TO YOUR THOUGHTS.....

configuring, the nodes are unaware about the logical structure of the network. But in DCERH the base station first collects information about the logical structure of the network and residual energy of each node. So, with the global information about the network, base station does cluster formation better in the sense that it has information about the residual energy of each node and in terms of security we have confidentiality, integrity and availability. Out of these characteristics we implemented, data confidentiality by using Homomorphic Encryption scheme. Finally, DCERH is compared with LEACH-C protocol.

In WSN, nodes sense the data and send this sensed data to the cluster head (in case of hierarchical routing) or directly to the base station according to the TDMA (time division multiplexing access) given by cluster head or base station resp. But this TDMA schedule will be failed if there will no synchronization of the clocks of all the nodes. So this can be another research area where this can be considered. So in future, time synchronization can be applied to DCERH. In terms of security, data integrity and availability are also open research area

REFERENCES

[1] F. Akyildiz and M. C. Vuran, "Wireless Sensor Networks," 1st Edition, John Wiley & Sons, Ltd, Chichester, 2010.

[2] S. Bandyopadhyay and E. Coyle, "An Energy Efficient Hierarchical Clustering Algorithm for Wireless Sensor Networks," Proceedings of the 22nd Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM 2003), San Francisco, 30 March-3 April 2003, pp. 1713-1723.

[3] Y. Chen and Q. Zhao, "On the Lifetime of Wireless Sensor Networks," IEEE Communications Letters, Vol. 9, No. 11, 2005, pp. 976-978.

[4] Norouzi and A. Sertbas, "An Integrated Survey in Efficient Energy Management for WSN Using Architecture Approach," International Journal of Advanced Net-working and Applications, Vol. 3, No. 1, 2011, pp. 968- 977

[5] S.D. Muruganathan, D.C.F. Ma, R.I. Bhasin, A.O. Fapojuwo, "A Centralized Energy efficient Routing Protocol for Wireless Sensor Networks", IEEE Radio Communications, University of Calgary, March 2005, pp. S8 –S13

[6] D. Kandris, P. Tsioumas, A. Tzes, N. Pantazis, and L. D. Vergados, "Hierarchical Energy Efficient Routing in Wireless Sensor Networks", 16th Mediterranean Conf. on Control and Automation Congress Centre, Ajaccio, France, June 25- 27, 2008.

[7] E. Shi and A. Perrig. Designing secure sensor networks. In Wireless Communications, IEE, volume 11, December 2004.

[8] Claude Castelluccia, Inra Aldar, C-F. Chan Einar Mykletun and Gene Tsudik, "Efficient and Provably Secure Aggregation of Encrypted Data in Wireless Sensor Networks", ACM Transactions on Sensor Networks, Vol. 5, No. 3, Article 20, Publication date: May 2009.

[9] W. Heinzelman, J. Kulik, and H. Balakrishnan, "Negotiation-based Protocols for Disseminating Information in Wireless Sensor Networks", in Proc. of the 5th Annual ACM/IEEE Int. Conf. on Mobile Computing and Networking, 1999.

[10] Minh Tuan Nguyen and Nazanin Rahnavard, "Cluster-Based Energy-Efficient Data Collection in Wireless Sensor Networks utilizing Compressive Sensing", IEEE Military Communications Conference, January 2013

[11] Wendi B. Heinzelman,, Anantha P. Chandrakasan, and Hari Balakrishnan, "An Application-Specific Protocol Architecture for Wireless Microsensor Networks", IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, VOL. 1, NO. 4, OCTOBER 2002.