International Journal of Engineering Research and Development
***e**-ISSN: 2278-067X, **p**-ISSN: 2278-800X, www.ijerd.com*
Volume 2, Issue 9 (August 2012), PP. 41-45

SEECH: Secure and Energy Efficient Centralized Routing Protocol for Hierarchical WSN

Devendra Prasad[1] and Reema Goyal[2]
[1,2]Department of Computer Engineering, M.M University, Mullana, Ambala, Haryana, India

Abstract*—Wireless Sensor Networks (WSNs) differs from traditional wireless networks in several ways. One of them is energy constraints. Sensor nodes (SNs) are battery operated, with limited life and difficult to replace, if deployed in hostile environment. Therefore protocols in WSNs must be designed with minimum energy consumption to prolong the network life. In WSNs protocols are designed to minimize energy consumption and preserve the longevity of the network. In this paper, we have designed Secure and Energy Efficient Centralized Routing Protocol (SEECH) for hierarchical WSNs. In SEECH, the base station (BS) collects information about the logical structure of the network and residual energy of SN. With these information, BS does efficient clustering. Finally, SEECH is compared with LEACH-C protocol.

Keywords*—Wireless Sensor Networks (WSNs), sensor nodes (SNs), Base Station (BS), time division multiplexing access (TDMA) etc.

I. INTRODUCTION

Wireless sensor networks (WSNs) are built up of sensor nodes (SNs), which consist of sensing, computing, communication, actuation and power components that cooperatively perform the task of collecting relevant data and monitor its surrounding for some change or event to occur [1]. WSNs has its own features that not only differentiate it from other wireless networks but also craft the scope of wireless application to disaster relief, military surveillance, habitat monitoring, target tracking and in many civic, medical and security applications [2-5]. Extensive research is going on in almost all fields of sensor network, including sensor design, communication protocol stack design, operating system for sensors etc. The design goals of WSNs are application specific, but share some common attributes like scalability, robustness, network life time, fault tolerance, and data aggregation. Out of which, energy efficiency and security are most important.

Many Routing protocols exist in the W SNs. Depending on how the sender of a message gains a route to the receiver, routing protocols can be classified into three categories, namely, proactive, reactive and hybrid protocols. In proactive protocols, all routes are computed before they are really needed, while in reactive protocols, routes are computed on demand. Hybrid protocols use a combination of these two ideas. Since sensor nodes are resource poor, and the number of nodes in the network could be very large, SNs cannot afford the storage space for “huge” routing tables. Therefore reactive and hybrid routing protocols are attractive in sensor networks.

One of the most critical issues in WSNs is represented by the data confidentiality and limited availability of energy on SNs; thus, making good use of energy and security is necessary to increase network lifetime and confidentiality.

In hierarchical routing architecture, SNs self configures them for the formation of cluster heads. This protocol is BS assisted i.e. this protocol utilizes a high-energy BS to set up clusters and routing paths, perform randomized rotation of cluster heads, and carry out other energy-intensive tasks. Rest of the paper is organized as follows.

Rest of the paper is organized as follows. Section 2 presents the related works. In section 3 System Model is presented. SEECH Protocol description and Algorithm is given in Section 4. Simulation and performance analysis is presented in Section 5 and finally work done is concluded in Section 6.

II. RELATED WORKS

Hierarchical routing, are well-known techniques with special advantages related to scalability and efficient communication. Hierarchical routing is utilized to perform energy efficient routing in WSNs. In a hierarchical architecture, higher energy nodes can be used to process and send the information while low energy nodes can be used to perform the sensing in the proximity of the target. Hierarchical routing is an efficient way to lower energy consumption within a cluster and by performing data aggregation and fusion.

Heinzelman, et. al. [6] introduced Low Energy Adaptive Clustering Hierarchy (LEACH). LEACH is a cluster-based protocol, which includes distributed cluster formation. LEACH randomly selects a few sensor nodes as clusterheads (CHs) and rotate this role to evenly distribute the energy load among the sensors in the network. In LEACH, the clusterhead (CH) nodes compress data arriving from nodes that belong to the respective cluster and send an aggregated packet to the base station in order to reduce the amount of information that must be transmitted to the base station. LEACH uses a TDMA/CDMA MAC to reduce inter-cluster and intra-cluster collisions. However, data collection is centralized and is performed periodically. Therefore, this protocol is most appropriate when there is a need for constant monitoring by the sensor network. A user may not need all the data immediately. Hence, periodic data transmissions are unnecessary which may drain the limited energy of the sensor nodes. After a given interval of time, a randomized rotation of the role of the CH is conducted so that uniform energy dissipation in the sensor network is obtained. The authors found that only 5% of the nodes need to act as cluster heads.

Although LEACH is able to increase the network lifetime, there are still a number of issues about the assumptions used in this protocol. LEACH assumes that all nodes can transmit with enough power to reach the BS if needed and that each node has computational power to support different MAC protocols. Therefore, it is not applicable to networks deployed in large regions. It also assumes that nodes always have data to send, and nodes located close to each other have correlated data. It is not obvious how the number of the predetermined CHs (p) is going to be uniformly distributed through the network. Therefore, there is the possibility that the elected CHs will be concentrated in one part of the network. Hence, some nodes will not have any CHs in their vicinity. Furthermore, the idea of dynamic clustering brings extra overhead, e.g. head changes, advertisements etc., which may diminish the gain in energy consumption. Finally, the protocol assumes that all nodes begin with the same amount of energy capacity in each election round, assuming that being a CH consumes approximately the same amount of energy for each node. The protocol should be extended to account for non-uniform energy nodes, i.e., use energy-based threshold.

Security is a big issue, when WSNs are deployed in a hostile environment. Secret keys should be used to encrypt the exchanged data between communicating parties. In the Internet or traditional wireless networks, such as, cellular networks, most security protocols are based on asymmetric cryptography, such as; RSA or Elliptic Curve Cryptography (ECC) [8] are not applicable, due to the high computational complexity, high-energy consumption and increased code storage requirements. Furthermore, due to unpredictable network topology and lack of infrastructure support, trusted-server based key distribution protocols are not suitable for WSNs either [7]. Research shows that key pre-distribution mechanism could be a practical method to solve the key distribution problem in WSNs. The basic idea of key pre-distribution scheme is preloading some secret keys into SNs, before they are deployed. After the deployment, the nodes discover shared keys for secure communications. It is divided into 3 phases; i.e. Key distribution, Shared key discovery and Path-key establishment.

During these phases, secret keys are generated, placed in sensor nodes, and each sensor node searches the area in its communication range, to find another node to communicate. A secure link is established, when two nodes discover one or more common keys (this differs in each scheme), and communication is done on that link between those two nodes. For this purpose, various keying techniques are being used. Some of the common key management schemes in [9], that we are focusing are as follows:

1. Single Network-wide Key Establishment
2. Pair-wise Key Establishment
3. Dynamic Key Management
4. Q-Composite Random Key Management

Each of the above WSN key management scheme consists of three main components [10]:

1. Key establishment (2) Key refreshment (3) Key revocation.

Key establishment is about creating a session key between the parties that need to communicate securely with each other. Key refreshment prolongs the effective lifetime of a cryptographic key, whereas, key revocation ensures that an evicted node is no longer to able to decipher the sensitive messages that are transmitted in the network.

III. SYSTEM MODEL:

The foundation of SEECH lies in the realization that the BS is a high energy node with a large amount of energy supply. Thus SEECH utilizes the BS to control the coordinated sensing task performed by the SNs. In SEECH the following assumptions are considered.

- A fixed BS is located far away from the deployment area.
- The SNs are energy constrained with a uniform initial energy allocation.
- The SNs are equipped with power control capabilities to vary their transmition range.
- Each SN senses the environment at a fixed interval and send the sensed data to the BS.
- All SNs are immobile.

The radio channel is supposed to be symmetrical. Moreover, it is assumed that the communication environment is contention and error free. Each SN has the ability to monitor its residual energy. The SN are geographically grouped into clusters and capable of operating in two basic modes:

- The cluster head mode
- The sensing mode

In the sensing mode, the SNs perform sensing tasks and transmit the sensed data to the CH. In CH mode, a SN gathers data from the other SNs within its cluster, performs data fusion and routes the data to the BS through other CH nodes. The BS in turn performs the key tasks of cluster formation, randomized CH selection, and CH-to-CH routing path construction.

IV. SEECH PROTOCOL

SEECH operates in two major phases: setup phase and data communication phase.

A. Set up Phase

In this phase, cluster formation, cluster head selection and CH to CH routing path is established. The steps involved in this phase are as follows:

Step 1: Initially, BS broadcast a START message in the field to acquire information about the SN's residual energy and their neighbors list.

Step 2: After receiving the start "START" message, each SN broadcasts the "HELLO" message in the field.

Step 3: Each SN receiving "HELLO" message, sends "REPLY" message containing its ID.

Step 4: When a SN gets "REPLY" message, it maintains the ID of the SN sending the "REPLY" message. In this way each SN have their individual neighbor list.

Step 5: After receiving the information about neighbors, the SNs sends a STATUS message, containing it's own ID, Neighbor list and Energy level to the BS, if the BS is within its range.

Step 6: BS sends an acknowledge message ACK to all those SNs from where it receives STATUS message.

Step 7: After acquiring acknowledge ACK, the SNs set their level to one which was initially zero and broadcasts a gateway advertisement message GW_ADV to all its neighbors.

Step 8: SNs receiving GW_ADV will check their level. If SN's level is zero (i.e. SN has not sent their status yet), it sends their STATUS to the SN advertising gateway message. In this case, a SN can receive a GW_ADV from many SNs but it will reply only to that SN from where it has received GW_ADV message first.

Step 9: 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 BS directly (if directly connected).

Steps 7 to 9 are continuously replayed until all the SNs send their STATUS to the BS, directly or via gateway. At this time BS has acquired all the information about logical structure of the sensor field. This can be shown in table consisting 10*10 cells for 10 SNs in the field. This information is stored in status array of [10] [10] size as shown in Table 1.

Node No	0	1	2	3	4	5	6	7	8	9
0	0	1	1	0	0	0	0	0	0	0
1	1	0	1	1	0	0	0	0	0	0
2	1	1	0	0	0	0	0	0	0	0
3	0	1	0	0	0	1	0	0	0	1
4	0	0	0	0	0	1	0	0	0	0
5	0	0	0	1	1	0	1	0	0	0
6	0	0	0	0	0	1	0	1	0	0
7	0	0	0	0	0	0	1	0	1	1
8	0	0	0	0	0	0	0	1	0	0
9	0	0	0	1	0	0	0	1	0	0

Table 1: Neighbor Information of each SN

A value in cell status[i] [j] represents whether a SN i is within the range of j or not. If it is, then its value is 1 otherwise 0. The BS has information (in the energy table) about the residual energy status of the each SN in the field as shown in Table 2.

Node	0	1	2	3	4	5	6	7	8	9
Energy	0.5	0.7	0.4	0.5	0.7	0.6	0.65	0.8	0.4	0.7

Table 2: Energy Information about each node

Step 10: Since the SNs, for which the BS 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 11: BS computes the average energy level avgE for those nodes (let it be called set X) that have not been declared as cluster head themselves yet, but have been associated with cluster head having their neighbors' count greater than zero.

Step 12: Out of X nodes, select N number of nodes as a cluster head, whose energy is greater than avgE and has maximum number of neighbors.

Step 13: Nodes selected in step 12 is set as cluster head to the rest of unassigned neighbors.

Step 14: Repeat the steps 11 to 13 until X is greater than zero.

B. Data transmission phase

Step 15: Base station broadcasts cluster information that includes the ID's of the cluster head, along with the set of (X-N) numbers of keys, non-cluster head nodes belongs to which cluster head in addition to hard and soft thresholds values similar to the way in TEEN and APTEEN.

Step 16: 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.

Step 17: Each node, during its allocated transmission time add the key value to the data, sends to the cluster head quantitative data concerning the sensed events. In a way similar to that proposed in TEEN protocol hard and soft thresholds are used in SEECH too.

Step 18: 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 (if this is possible) or via intermediate upper level cluster heads.

Step 19: The base station collects all the encrypted messages transmitted to it. The base station determines the new cluster heads 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 20: The base station gets the decrypted messages by subtracting the sum of values of set Q.

V. PERFORMANCE ANALYSYS

A. Simulation Parameters

The sole criterion for evaluation is the energy consumption of the model simulated. To measure the energy used we have defined three metrics.

- First Node Dead (FND) – It is the number of rounds that have elapsed before first node of the network runs out of power. It gives an indication of network lifetime but is not a very useful measure of lifetime.
- Half Node Dead (HND) – It is the number of rounds that have elapsed before half of the nodes run out of power. It is a very useful measure of network lifetime since 'death' of half the nodes signals a serious degradation of network performance.
- Last Node Dead (LND) – It is the number of rounds that have elapsed before Last node in the network runs out of power. It is the effective lifetime of the network.

Throughout the simulations we consider network node configuration with 100 nodes where, each node is assigned an initial energy of 2 Joules.

B. Average energy dissipation

Figure 1 shows the average energy dissipation of the protocols under study over the number of rounds of operation. This plot clearly shows that SEECH (without security) has a much more desirable energy expenditure curve than that of LEACH-C. SEECH uses multi-hop cluster head nodes to forward the data to the base station, this in turn decreases the communication energy cost for those SEECH nodes that have close neighbors

The improvement gained through SEECH is further exemplified by the comparison graph in Figure 2. This plot shows the energy dissipation over the number of rounds of activity for the 100 m × 100 m network scenario. On average, SEECH consumes 10 percent extra energy to achieve encryption.

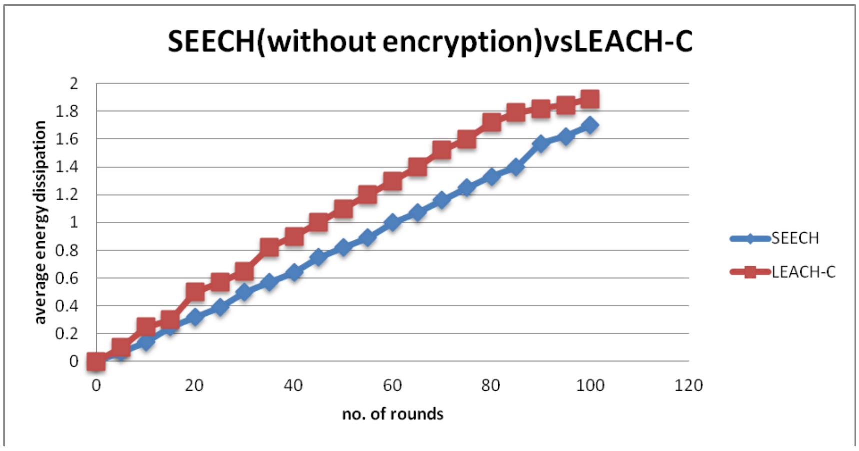

Figure 1: Comparison of Avg. Energy Dissipation between LEACH-C and SEECH

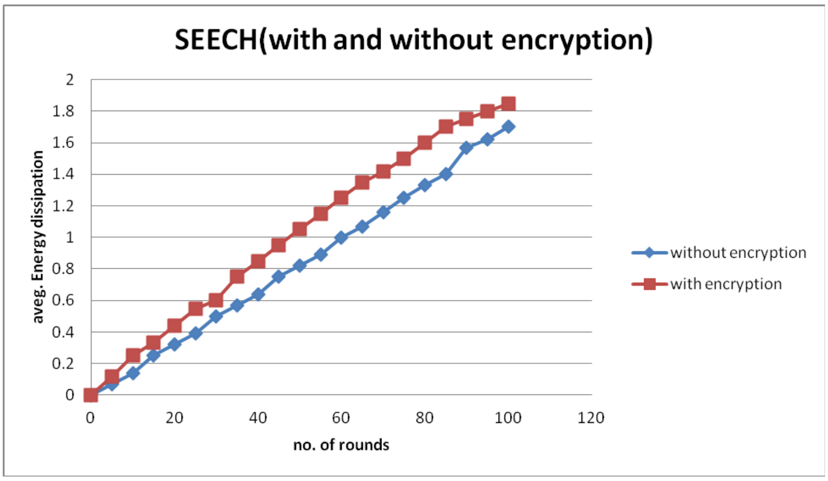

Figure 2: Performance of SEECH protocol.

VI. CONCLUSION AND FUTURE SCOPE

In WSNs protocols are designed to minimize energy consumption and preserve the longevity of the network. In this paper, we have presented a Secure and Energy Efficient Centralized Routing Protocol (SEECH) for hierarchical WSNs. In non-centralized hierarchical routing, sensor nodes self configured for the formation of cluster head. While self configuring, the nodes are unaware about the logical structure of the network. But in SEECH, the base station first collects information about the logical structure of the network and residual energy of each node. With this global information BS does cluster formation better in better way.

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 respectively. 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 SEECH.

REFERENCES

[1]. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, “Wireless sensor networks: A survey”, Computer Networks Journal, Elsevier Science, Vol. 38(4):393-422, No. 4 pp 393–422, March 2002.

[2]. Matt Welsh, Dan Myung, Mark Gaynor, and Steve Moulton. “Resuscitation monitoring with a wireless sensor network”. In Supplement to Circulation: Journal of the American Heart Association, October 2003.

[3]. G.L. Duckworth, D.C. Gilbert, and J.E. Barger. “Acoustic counter-sniper system”, In SPIE International Symposium on Enabling Technologies for Law Enforcement and Security, 1996.

[4]. Alan Mainwaring, Joseph Polastre, Robert Szewczyk, and David Culler. “Wireless sensor networks for habitat monitoring”, In First ACM International Workshop on Wireless Sensor Networks and Applications, 2002.

[5]. Robert Szewczyk, Joseph Polastre, Alan Mainwaring, and David Culler. “Lessons from a sensor network expedition”, In First European Workshop on Wireless Sensor Networks (EWSN'04), January 2004.

[6]. W. Heinzelman, A. Chandrakasan and H. Balakrishnan, "Energy-Efficient Communication Protocol for Wireless Mi-crosensor Networks," Proceedings of the 33rd Hawaii International Conference on System Sciences (HICSS '00), January 2000.

[7]. S. A. Camtepe and B. Yener, “Key distribution mechanisms for wireless sensor networks: a survey,” Department of Computer Science, Rensselaer Polytechnic Institute, Tech. Rep. TR-05-07, March 23 2005.

[8]. J.-P.Kaps, “Cryptography for ultra-low power devices”, Ph. D. thesis, at Worcester Polytechnic Institute, 2006.

[9]. A Survey of Key Management Schemes in Wireless Sensor Networks.Yang Xiao, Venkata Krishna Rayi, Bo Sun, Xiaojiang Du, Fei Hu, and Michael Galloway; Computer Communications, Special Issue On Security On Wireless Ad Hoc and Sensor Networks.

[10]. Key Management Building Blocks for Wireless Sensor Networks; Yee Wei Law, Jeroen Doumen and Marimuthu Palaniswami: The University of Melbourne, Australia, University of Twente, The Netherlands.