Efficient and Secure Routing Protocol for Wireless Sensor Networks through SNR Based Dynamic Clustering Mechanisms

Subramanian Ganesh and Ramachandran Amutha

Abstract: **Advances in wireless sensor network (WSN) technology have enabled small and low-cost sensors with the capability of sensing various types of physical and environmental conditions, data processing, and wireless communication. In the WSN, the sensor nodes have a limited transmission range and their processing and storage capabilities as well as their energy resources are limited. A triple umpiring system has already been proved for its better performance in WSNs. The clustering technique is effective in prolonging the lifetime of the WSN. In this study, we have modified the ad-hoc on demand distance vector routing by incorporating signal-to-noise ratio (SNR) based dynamic clustering. The proposed scheme, which is an efficient and secure routing protocol for wireless sensor networks through SNR-based dynamic clustering (ESRPSDC) mechanisms, can partition the nodes into clusters and select the cluster head (CH) among the nodes based on the energy, and non CH nodes join with a specific CH based on the SNR values. Error recovery has been implemented during the inter-cluster routing in order to avoid end-to-end error recovery. Security has been achieved by isolating the malicious nodes using sink-based routing pattern analysis. Extensive investigation studies using a global mobile simulator have shown that this hybrid ESRP significantly improves the energy efficiency and packet reception rate as compared with the SNR unaware routing algorithms such as the low energy aware adaptive clustering hierarchy and power efficient gathering in sensor information systems.**

Index Terms: **Dynamic clustering, intruder detection, routing protocol, signal-to-noise ratio (SNR), wireless sensor networks (WSN).**

I. INTRODUCTION

Wireless sensor network (WSN) is widely considered as one of the most important technologies of the twenty-first century. The sensing electronics measure the ambient conditions related to the environment surrounding the sensors and transform them in to an electrical signal. In many WSN applications, the deployment of sensor nodes is performed in an ad-hoc manner without careful planning and engineering. In the past few years, intensive research studies addressing the potential of collaboration among sensors in data gathering and processing and in the coordination and management of the sensing activities were conducted. However, the sensor nodes are constrained in energy supply and bandwidth.

Energy conservation is critical in WSNs. Replacing or recharging the batteries is not an option for the sensors deployed in hostile environments. Generally, the communication electronics in the sensor use most of the energy. Stability is one of the major concerns associated with the advancement of WSNs. A number of WSN applications require guaranteed sensing, coverage, and connectivity throughout its operational period. The death of the first node might cause instability in the network. Therefore, all of the sensor nodes in the network must be alive in order to achieve the goal during that period. One of the major obstacles to ensure these phenomena is the unbalanced energy consumption rate. Numerous techniques have been proposed to improve the energy consumption rate, such as clustering, efficient routing, and data aggregation.

In a typical WSN application, the sensor nodes are scattered in a region from where they collect data to achieve certain goals. Data collection may be a continuous, periodic, or event-based process. The WSN must be very stable in some of its applications such as security monitoring and motion tracking.

The death of only one sensor node may disrupt the coverage or connectivity and thus may reduce the stability in this type of applications. Therefore, all of the deployed sensor nodes in the WSN must be active during their operational lifetime. However, the sensor nodes are generally equipped with one-time batteries, and most of the batteries are of low-energy type. For this reason, each sensor node must efficiently use its available energy in order to improve the lifetime of the WSN. Different techniques are used for the efficient usage of this low available energy in a sensor node. Clustering is one of the most well known techniques.

Li *et al.* [1] have investigated the joint power allocation (PA) issue in a class of multiple input multiple output (MIMO) relay systems. By using the capacity and the mean-square error (MSE) as the optimization criteria, two joint PA optimization problems have been formulated. As the cost functions derived directly from the capacity and the MSE would lead to nonconvex optimization, two modified cost functions corresponding to a convex problem of the source and the relay power weighting coefficients have been developed. The key contribution of the proposed method lies in the discovery of a tight bound for the capacity and the MSE that simplifies the joint source and relay PA into a convex problem. A distinct feature of the new method is that the PA within the source and that within the relay are jointly optimal for any given power ratio of the two units.

It was studied in [2] that the joint PA problem for multicast systems can achieve a better data rate. The non convex optimization problem is dealt with by employing a high signal-to-noise

Manuscript received January 14, 2012; approved for publication by Hamid Sadjadpour, Division II Editor, May 16, 2013.

S. Ganesh is with the Electronics and Communication Engineering, Sathyabama University, Chennai, Tamil Nadu, India, email: ganesh8461@gmail.com.

R. Amutha is with the Electronics and Communication Engineering, SSN College of Engineering, Chennai, Tamil Nadu, India, email: amuthar@ssn.edu.in.

Digital Object Identifier 10.1109/JCN.2013.000073

ratio (SNR) approximation to modify the original cost function in order to obtain a convex minimization problem, where the approximation is shown to be asymptotically optimal in high-SNR regime. As an alternative, an iterative algorithm has been developed by using the convexity property of the cost function with respect to a part of the total power coefficients. By considering the low complexity of the physical layer network coding in the multi-cast system, a lattice-based network coding that uses the proposed joint PA schemes has been suggested.

In this paper, we have developed a hybrid efficient and secure routing protocol through SNR-based dynamic clustering mechanisms (ESRPSDC), which is a combination of SNR based dynamic clustering and routing pattern based security mechanisms. We have drawn a brief comparison of ESRPSDC with the low energy aware adaptive clustering hierarchy (LEACH) and power efficient gathering in sensor information systems (PEGASIS), two of the popular routing protocols. The rest of this paper is organized as follows. In Section II, the related work is briefly reviewed and discussed. Further, we describe our network model, the adversary model, and notations used throughout in this paper in Section III. The simulation results are presented in Section IV. We conclude this paper in Section V.

II. RELATED WORK

Several techniques have already been proposed to improve the network lifetime in a WSN. Among them, clustering is one of the widely accepted techniques. Clustering is also used in wireless ad-hoc networks and mobile ad-hoc networks, besides sensor networks. Several clustering techniques have already been introduced for partitioning nodes into areas.

Clustering is a technique in which the deployed sensor nodes are grouped into some clusters. Only one sensor node is solely responsible for communication with the base station (BS) in a cluster. This sensor node is called the cluster head (CH) and the remaining sensor nodes in the cluster are called followers.

The followers collect and transmit the data to their corresponding CHs. The CHs aggregate their own data with the data received from their followers. The aggregated data are transmitted to a sink to accomplish a specific goal. The CHs remain closer to their follower sensor nodes when compared with the sink. It takes less energy to transmit the data to a CH instead of the sink, which allows the sensor nodes to conserve more energy and live longer in the WSN.

There are different clustering techniques already established for ad-hoc networks. However, these techniques cannot be directly used in the WSN because of the fact that the WSN imposes strict requirements on the energy efficiency when compared with the ad-hoc networks. As a result, many techniques have been proposed for clustering in a WSN. Dynamic clustering techniques are more useful for the WSN because of the dynamic variation in the residual energies of the sensor nodes.

Some of the previously used clustering techniques include: Distributed clustering algorithm (DCA) [3], spanning tree (or breadth-first spanning tree) based clustering [4], clustering with on-demand routing [5], clustering based on degree or lowest identifier heuristics [6], distributed and energy-efficient clustering [7], adaptive power-aware clustering [8], PEGASIS, power efficient and adaptive clustering hierarchy (PEACH), optimal energy aware clustering algorithm for cluster establishment (ACE), and hybrid energy-efficient distributed clustering (HEED).

Lindsey *et al.* [9] introduced a near optimal chain-based protocol. Here, each node communicates only with a close neighbor and takes turns in transmitting to the BS, thus reducing the amount of energy spent per round. It assumes that all the nodes have global knowledge of the network and employ the greedy algorithm. It maps the problem of having close neighbors for all the nodes to the traveling salesman problem. PEGASIS is a greedy chain protocol that is near optimal for a data-gathering problem in sensor networks. The greedy approach considers the physical distance only, ignoring the capability of a prospective node on the chain. Thus, a node with a shorter distance and with less residual energy may be selected in the chain and may die quickly.

It was proposed in [10] that a routing algorithm, which combines the hierarchical and geographical routings, could perform well in greedy environments. The process of packet forwarding from the source nodes in the target region to the BS consists of two phases: Inter-cluster routing and intra-cluster routing. For inter-cluster routing, a greedy algorithm is adopted to forward the packets from the CHs of the target regions to the BS. For intra-cluster routing, a simple flooding is used to flood the packet inside the cluster when the number of intra-cluster nodes is less than the predetermined threshold. Otherwise, the recursive geographic forwarding approach is used to disseminate the packet inside the target cluster, that is, the CH divides the target cluster into some sub regions, creates the same number of new copies of the query packet, and disseminates these copies to a central node in each sub region.

PEACH [11] is a cluster formation technique based on the overheard information obtained from the sensor nodes. According to this approach, if a CH node becomes an intermediate node of a transmission, it first sets the sink node as its next hop. Further, it sets a timer to receive and aggregate multiple packets from the nodes in the cluster set for a pre-specified time. It checks whether the distance between this node and the original destination node is shorter than that between this node and the already selected next hop node. If the distance is shorter, this node joins the cluster of the original destination node and the next hop of this node is changed to the original destination node. PEACH is an adaptive clustering approach for multi-hop inter-cluster communication. However, it suffers from almost the same limitations as those of PEGASIS, owing to the selection of the physical propinquity.

The optimal energy aware clustering [12] solves the balanced k-clustering problem optimally, where k signifies the number of master nodes that can be present in the network. This algorithm is based on the minimum weight matching. It optimizes the sum of spatial distances between the member sensor nodes and the master nodes in the entire network. It effectively distributes the network load on all the master nodes and reduces the communication overhead and energy dissipation. However, this research work does not consider the residual energy level while selecting a node as the master node.

ACE [13] is a distributed clustering algorithm, which estab-

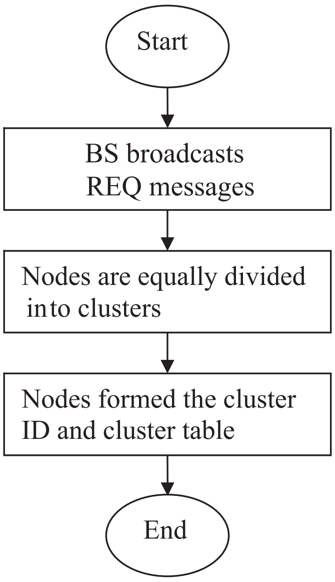
Start
BS broadcasts REQ messages
Nodes are equally divided into clusters
Nodes formed the cluster ID and cluster table
End

Fig. 1. Initialization phase.

lishes clusters into two phases spawning and migration. There are several iterations in each phase and the gap between two successive iterations follows a uniform distribution. During the spawning phase, new clusters are formed in a self-elective manner. When a node decides to become a CH, it broadcasts a message to its neighbors to become its followers. During the migration phase, existing clusters are maintained and rearranged, if required. The migration of an existing cluster is controlled by the country-region place CH. Each CH periodically polls all of its followers to determine the best candidate to be elected as a new leader for the cluster. The current CH promotes the best candidate as the new CH and abdicates itself from its position. ACE results in uniform cluster formation with a packing efficiency close to that of hexagonal close packing. However, ACE does not consider the residual energy of the nodes while selecting the CHs.

The distributed algorithms called HEED [14] incorporate the residual energy of the sensor nodes, which results in the formation of clusters by uniformly distributing the CHs across the network. It periodically selects the CHs according to a hybrid parameter, which consists of a primary parameter, the residual energy of a node, and a secondary parameter, such as propinquity of a node to its neighbors or node degree. HEED converges in 0 (1 iteration) using the low messaging overhead and achieves a uniform CH distribution across the network. However, it randomly selects the initial percentage of CHs. This random selection remains a severe limitation of this algorithm.

A number of research attempts have made to improve the network stability period by various techniques such as routing, scheduling, and aggregation. However, in this study, we attempt to improve the network stability period using clustering as it can serve as a better platform for upper layer functionality such as broadcasting and aggregation. Our approach ESRPSDC exploits the underlying method of the energy-efficient level based clustering routing protocol [15]. In our proposal, we have incorporated the security methods as specified in [16].

Table 1. Initial cluster.

Cluster ID	No. of active nodes	No. of sleep nodes	CH with its energy	Next CH
1	8	3	Null	Null
2	6	4	Null	Null

III. HYBRID SNR BASED DYNAMIC CLUSTERING MODEL

Grouping of the sensor nodes into clusters has been widely pursued by many of the research communities in order to estimate the network lifetime. Generally, the clustering methods can be categorized into static and dynamic clustering. The objective of static clustering is to minimize the total energy spent during the formation of clusters for a set of networks [17].

In this study, we assume a sensor network model with the following properties.

1. All the sensor nodes are heterogeneous with limited supply of energy.
2. Each node senses the data and transfers the information to the country-region place CH.
3. The BS is located at a distance away from the sensor nodes and is static.
4. Each node has a fixed number of transmission power levels.
5. The nodes are not equipped with global positioning system (GPS) unit.

The proposed system follows the SNR based dynamic clustering and its process is divided in to five different phases namely, initialization, energy based CH selection, SNR based CH selection by non CH (NCH) nodes, data forwarding through intercluster routing, and identifying the intruder.

A. Initialization

As shown Fig. 1, after the deployment of the nodes, the BS broadcasts a request (REQ) message to every node. When the nodes have received the REQ, they are equally divided into clusters depending on the number of nodes and their sensing range. Each cluster frames its own cluster identification (ID) and the cluster table (CT) as summarized in Table 1.

The CT maintains the CH node number along with its energy. The nodes, that are alive, are considered as the active nodes and those that are turned off are considered as the sleep nodes. Initially, during the creation of the CT, the CH node number and its energy are null.

On the initial deployment, the BS transmits a level-1 signal with minimum power level. All the nodes, which sense this message, set their level as 1. Further, the BS increases its signal power to attain the next level and transmits a level-2 signal. All the nodes that receive the massage but do not set the previous level set their level as 2.

This procedure continues until the BS transmits the corresponding massages to all the levels. The total number of messages of the levels is equivalent to the number of the distinct transmit signals that the BS can transmit. The BS broadcasts a hello massage, which contains the information of the upper limit and lower limit of each level.

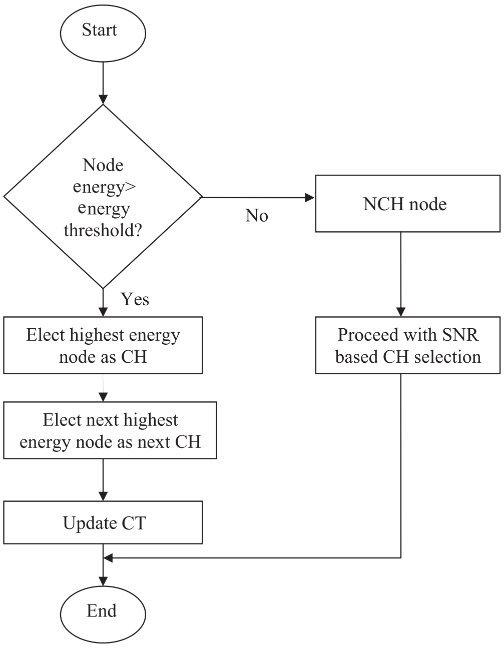
Start
Node energy> energy threshold?
No
NCH node
Yes
Elect highest energy node as CH
Proceed with SNR based CH selection
Elect next highest energy node as next CH
Update CT
End

Fig. 2. Energy based CH selection.

B. Energy Based CH Selection

Each cluster group can elect its own CH based on its energy. Among all the nodes in the cluster, the node, that has the highest energy, is selected as CH [18]. The next highest energy node is selected as the next CH, therefore, during the next iteration, if the CH losses its energy, the next CH becomes the current country-region place CH. The flow chart is shown in Fig. 2. The threshold is defined in (1).

$$T_i(n) = \frac{(\mathrm{P} \times \mathrm{C})(U_i - d(n, \mathrm{BS}))}{(1 - \mathrm{P})(r \bmod 1/\mathrm{P})(U_i - L_i)} \left[\frac{E_{\mathrm{cur}}(n)}{E_{\min}(n)}\right]^K \tag{1}$$

where P is the desired percentage of the CHs. r is the current round and Z is the set of nodes, which have not been CHs in the last 1/P rounds. C is the constant factor whose value is between 0 and 1. U_i is the upper limit of level-i and L_i is the lower limit of level-i. $d(n, \mathrm{BS})$ is the distance between node n and the BS. $E_{\mathrm{cur}}(n)$ is defined as the current energy of node n. $E_{\min}(n)$ is the initial energy of node n and the value of K is between 0 to 3.

The updated CT is summarized in Table 2.

C. SNR Based CH Selection by NCH Nodes

In many cases, those nodes, that are distributed in the sparse regions [19] or at the edge of a network, cannot directly communicate with the CHs owing to the limitation on their radio ranges. There are tradeoffs among connectivity, energy usage, and communication latency. In our work, communication between a CH and a node beyond the radio range of the CH has been achieved through the intermediate nodes (one-hop member nodes) which provide relaying service based on their SNR value as shown in Fig. 3. When a normal node will receives a CH state message from the CH node not belonging to any other cluster, it transmits a confirm message to the CH node. Now, the normal node becomes a one-hop node. It will create its own ID and transmits a state message to its neighbors within their region. When an NCH node receives a state message from a one-hop member node, it declares itself as a two-hop member node. The two-hop member node also selects its own ID, which is an m-byte random integer added at the end of the selected one-hop member node's ID.

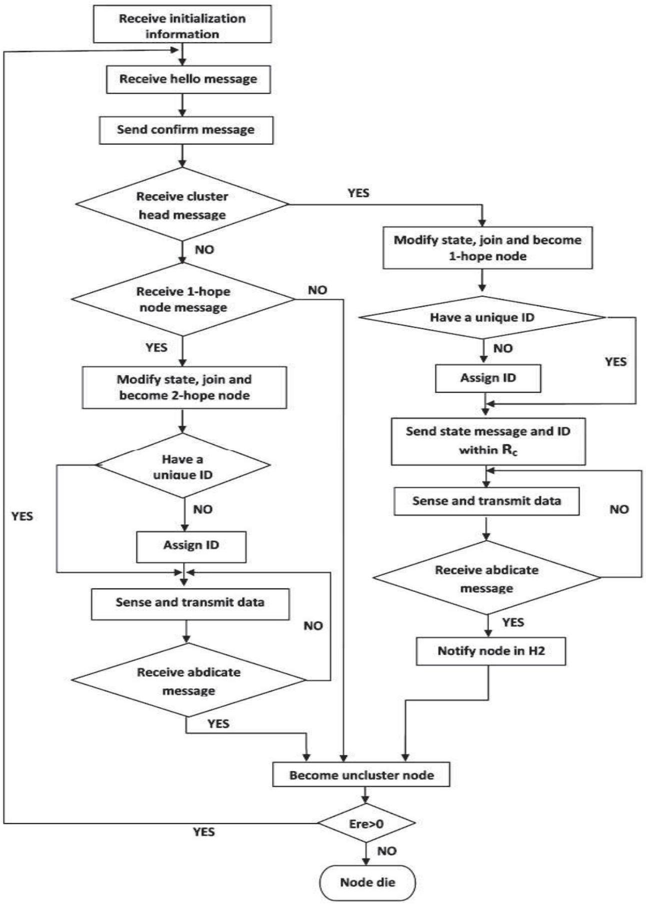

Fig. 3. SNR based CH selection by NCH nodes.

It may rarely occur that two sensor nodes within the same cluster select the same random number. This conflict can be solved through the CH by assigning one of the nodes a different ID. Thus, at the end of this phase, each node has its locally unique ID and knows the cluster to which it belongs. The abdicate message is transmitted by each CH to notify its member nodes of its unwillingness to serve as the CH in the next round, because of their lower energy levels.

D. Data Forwarding through Inter-Cluster Routing

Further, each CH creates [20] a time division multiple access (TDMA) schedule for its cluster members. This information is broadcast back to the nodes in the cluster. Once the clusters are created and the TDMA schedule is derived, data transmission can begin. Each cluster member can be turned off until the node's allocated time. Each node transmits data to its CHs with a minimal transmission power. This power is estimated by

Table 2. Updated cluster.

Cluster ID	No. of active nodes	No. of sleep nodes	CH with its energy (Joules)	Next CH with its energy (Joules)
1	8	3	N6/5	N8/4.5
2	6	4	N4/6.5	N5/6

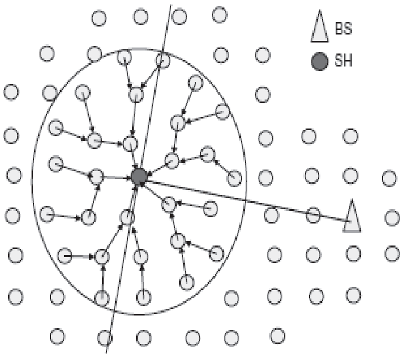

Fig. 4. Pattern of the attacked area.

Table 3. Simulation parameters.

Area of sensing field	1000 m × 1000 m
Number of sensor nodes	1000
Simulation time	600 s
Frequency	2.4 GHz
Bandwidth	2 Mbps
Traffic type	Variable bit rate (VBR)
Payload size	30 to 70 bytes
Number of loads	200 packets
Number of nodes	500 nodes
Propagation limit (dBm)	−111
Path loss model	Two ray model
Location of the BS	(50, 75)
Number of clusters	20
Initial energy of nodes	0.5 J
Antenna type	Omni directional
Channel bandwidth	20 Kbps
MAC layer protocol	IEEE 802.11

the received signal strength of the advertisement message, therefore, data transmission uses a minimal amount of energy. When all the data have been received from the cluster members, then CH node perform the data aggregation function to compress the data into a single signal. After a certain amount of time the next round, begin. After the cluster formation, the CHs broadcast the aggregate data to the next level. At the next level, the node aggregates their data and transmits to their CHs. In this manner, the CHs at the last level transmit the final information to the BS.

E. Identifying the Intruder

Generally, the attacked area may contain many nodes and the intruder nodes are not necessarily located at the center of the area [21] in a multi-hop sensor network. Therefore, it is necessary to further locate the exact intruders and isolate them from the network. This can be achieved by analyzing the routing pattern in the affected area. We now demonstrate a method for collecting the network flow information, which facilitates the routing pattern analysis. First, the BS transmits a request message to the network. The message contains the IDs of the affected nodes, and is flooded hop by hop. For each node receiving the request, if its ID is present, it should respond to the BS with a message, which includes its own ID, the ID of the next-hop node, and the cost for routing, for example, hop-count to the BS. It is noted that the next-hop and the cost could already be affected by the attack; therefore, the response message should be transmitted along the reverse path in the flooding, which corresponds to the original route with no intruder.

The BS can further visualize the routing pattern by constructing a tree using the collected next-hop information. It is noted that the area invaded by a sinkhole (SH) attack has a specific routing pattern, where all the network traffic flows toward the same destination, that is, the intruder SH. As shown in Fig. 4, once the tree is constructed, the BS can easily identify the SH, which is exactly the root of the tree in this single malicious node case.

IV. SIMULATION RESULTS

We have used a simulation model based on global mobile simulator (GloMoSim)-2.03 [22] in our evaluation. Our performance evaluations are based on the simulations of 500 wireless sensor nodes that form a WSN over a rectangular (1000 m × 1000 m) flat space. The medium access control (MAC) layer protocol used in the simulations was the distributed coordination function (DCF) of IEEE 802.11. The performance setting parameters are listed Table 3.

We set the distance between the source and the sink to be 350 meters. The other 498 nodes are deployed between the source-sink pair. The performance setting parameters are listed in Table 3.

We make the following assumptions about the WSN and the malicious node.

1. WSN nodes are deployed uniformly at random in a planar square region. All the nodes have the same wireless communication range, following the unit disk model.
2. All the nodes are implemented with the ESRPSDC routing algorithm, and have loosely synchronized clocks.
3. Each node transmits one data packet at a random time during a specified send interval *S*. The payload of each packet indicates the originator of the data. No encryption mechanism has been deployed within the network.
4. A single malicious node is present when the WSN is first deployed. The malicious node may be a compromised node or an implanted node. It has the same basic capabilities as the legitimate sensor nodes.
5. The malicious node participates in the network activities, however, it may provide false information in its link quality advertisements. The malicious node may also drop, modify,

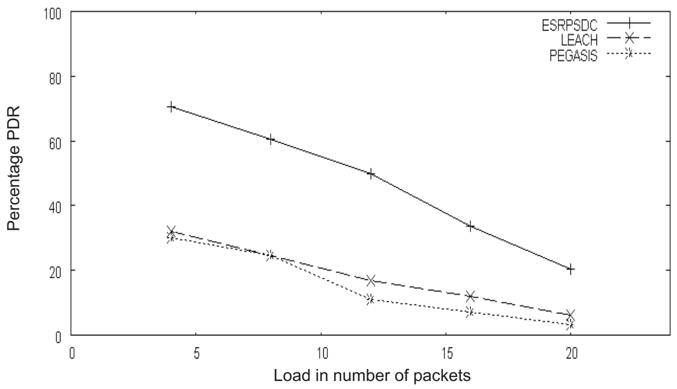

Fig. 5. Comparison of load versus percentage of PDR between ESRPSDC, LEACH, and PEGASIS.

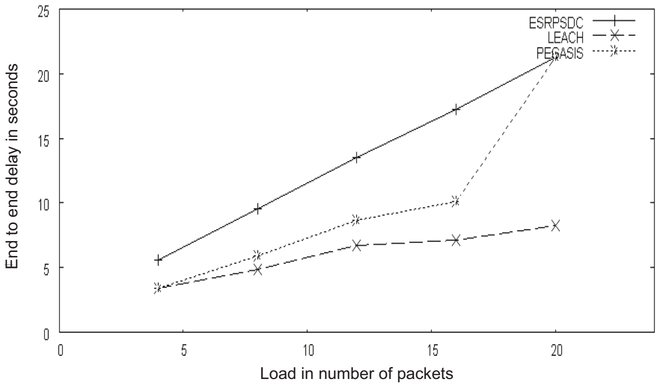

Fig. 7. Comparison of load versus end to end delay between ESRPSDC, LEACH, and PEGASIS.

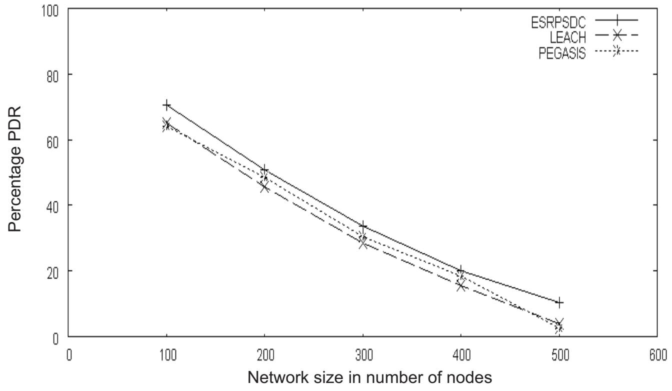

Fig. 6. Comparison of network size versus percentage of PDR between ESRPSDC, LEACH, and PEGASIS.

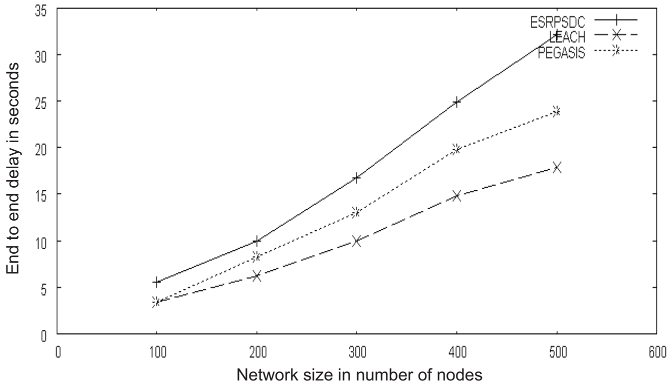

Fig. 8. Comparison of network size versus end to end delay between ESRPSDC, LEACH, and PEGASIS.

or divert the traffic that traverses it.

We have compared our ESRPSDC with LEACH and PEGASIS, based on the following three parameters.

1. Packet delivery ratio (PDR): It is the ratio of the successfully delivered data packets to the destinations to those generated by the VBR sources.

$$\mathrm{PDR} = \frac{\mathrm{N}_r}{\mathrm{N}_t}. \tag{2}$$

2. End-to-end delay (seconds): It indicates the time taken for the message to reach from the source to the destination.
3. Energy consumption in milliwatt hour (mWh).

A. Investigation-I

Investigation-I focuses the attention on comparing the PDR when the load and network size are varied in the presence of 30% of the malicious nodes. The observations are as follows.

In general, the PDR decreases as the number of load and network size are increased as shown in the Figs. 5 and 6. On the average, PDR drops from 70.41% to 20.18% for ESRPSDC. For LEACH, the PDR has a steep fall from 32.07% to 6.08%, and in the case of PEGASIS, the PDR drops from 30.37% to 3.03%. Clearly, ESRPSDC delivers more packets than LEACH and PEGASIS.

B. Investigations-II

Investigation-II focuses the attention on comparing the end-to-end delay in seconds, when the load and network size are varied in the presence of 30% of the malicious nodes. The observations are as follows.

As shown in Figs. 7 and 8, the end-to-end delay increases with the amount of load and network size. The average increase in the case of ESRPSDC is from 5 s to 32 s. For LEACH, the delay increases from 3 s to 17 s and for PEGASIS the increase is from 3 s to 23 s.

The adverse increase in the end-to-end delay can be observed in Fig. 8 as compared with Fig. 7, when the network size increases. The increased delay in ESRPSDC can be attributed to the increased level security mechanisms used in it. LEACH and PEGASIS were performed well, when there were a minimum number of malicious nodes. However, as shown in Fig. 9, ESRPSDC performs better than LEACH and PEGASIS when the percentage of malicious nodes increases. This proves the efficiency of the ESRPSDC security mechanism, because most of the malicious nodes are identified and isolated before the actual data transmission. During the data transmission, they are trapped and misdirected.

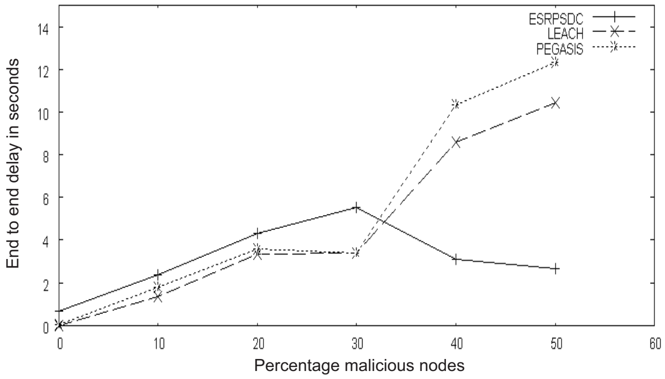

Fig. 9. Comparison of percentage of malicious nodes versus end-to-end delay between ESRPSDC, LEACH, and PEGASIS.

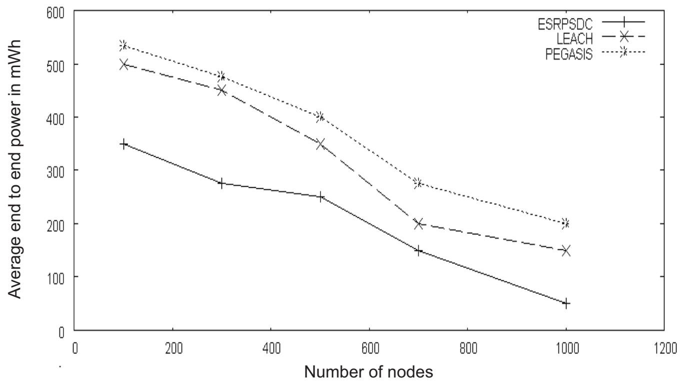

Fig. 10. Comparison of power consumption in mWh between ESRPSDC, LEACH, and PEGASIS.

C. Investigations-III

Investigation-III focuses on comparing the average power consumption in mWh, when the network size is varied in the presence of 30% of the malicious nodes. The power consumption is reduced in all the three protocols, which shows their clustering strength, however, nearly over 50% more reductions could be observed in ESRPSDC as compared with LEACH and PEGASIS as shown in Fig. 10.

V. CONCLUSIONS

The energy efficiency of a candidate route is critically dependent on the packet error rate of the underlying links, because they directly affect the energy wasted in retransmissions. The analysis of the interplay between the error rates, number of hops, and transmission power levels reveals several key results. It has been shown in [23] that for reliable energy-efficient communication, the routing algorithm must consider both the distance and the quality (e.g., in terms of the link error rate) of each link. Thus, the cost of selecting a particular link should be the overall transmission energy (including possible retransmissions) needed to ensure eventual error-free delivery, and not just basic transmission power. This is particularly important in practical multi-hop wireless environments, where the packet loss rates could be high [24].

In this paper, routing protocols for energy-efficient data collection through SNR-based dynamic clustering have been proposed. A network model based on the power levels has been developed along with deriving the mathematical formulae for selecting the country-region place CH. The developed model is simulated using GloMoSim. We have studied in detail about the simulation results of the energy consumption of CHs, percentage of PDR and end-to-end delay.

Our future research will focus on the optimization of our algorithm for effective energy consumption among all the nodes and for improving the network lifetime. We shall extend our algorithm to heterogeneous WSNs.

The process of isolating the intruder or the compromised node could increase the number of hop count, which would further increase the delay in data delivery. Therefore, the node replacements strategies have to be analyzed carefully. In addition, we need to calculate the amount of overhead involved in our proposed scheme.

REFERENCES

[1] C. Li, X. Wang, L. Yang, and W. P. Zhu, "A joint source and relay power allocation scheme for a class of MIMO relay systems," *IEEE Trans. Signal Process.*, vol. 57, no. 12, pp. 4852–4860, Dec. 2009.

[2] C. Li, S. He, L. Yang, and W. P. Zhu, "Joint power allocation for multicast systems with physical-layer network coding," *EURASIP J. Wireless Commun. Netw.*, pp. 1–9, July 2010.

[3] S. Basagni, "Distributed clustering algorithm for ad-hoc networks," in *Proc. I-SPAN*, Dec. 1999, pp. 310–315.

[4] S. Banerjee and S. Khuller, "A clustering scheme for hierarchical control in multi-hop wireless networks," in *Proc. IEEE INFOCOM*, Anchorage, Apr. 2001, pp. 1028–1037.

[5] M. Gerla, T. J. Kwon, and G. Pei, "On demand routing in large ad-hoc wireless networks with passive clustering," in *Proc. IEEE WCNC*, vol. 1, Mar. 2000, pp. 100–105.

[6] C. R. Lin and M. Gerla, "Adaptive clustering for mobile wireless networks," *IEEE J. Sel. Areas Commun.*, vol. 15, no. 7, pp. 1265–1275, Apr. 1997.

[7] J. Kamimura, N. Wakamiya, and M. Murata, "Energy-efficient clustering method for data gathering in sensor networks," in *Proc. BASENETS*, vol. 103, Apr. 2004, pp. 31–36.

[8] J. Leu, M. H. Tesai, T. C. Chiang, and H. Y. M. Huang, "Adaptive power aware clustering and multicasting protocol for mobile ad-hoc networks," *LNCS*, vol. 4159, pp. 331–340, June 2004.

[9] S. Lindsey and C. S. Raghavendra, "PEGASIS: Power efficient gathering in sensor information systems," in *Proc. IEEE Aerosp. Conf.*, vol. 3, June 2002, pp. 1125–1130.

[10] L. Li, S. Dong, and X. Wen, "An energy efficient clustering routing algorithm for wireless sensor networks," *J. China Univ. Posts Telecommun.*, vol. 3, no. 13, pp. 71–75, June 2006.

[11] S. Yi, J. Heo, Y. Chon, and J. Hong, "PEACH: Power-efficient and adaptive clustering hierarchy protocol for wireless sensor networks," *Comput. Commun.*, vol. 30, no. 14–15, pp. 2842–2852, Apr. 2007.

[12] S. Ghiasi, A. Srivastava, X. Yang, and M. Sarrafzadeh, "Optimal energy aware clustering in sensor networks," *Sensors*, vol. 2, no. 7, pp. 258–269, June 2002.

[13] H. Chan and A. Perrig, "ACE: An emergent algorithm for highly uniform cluster formation," *LNCS*, vol. 2920, pp. 160–171, Feb. 2004.

[14] O. Younis and S. Fahmy, "Distributed clustering in ad-hoc sensor networks: A hybrid, energy-efficient approach," in *Proc. IEEE INFOCOM*, vol. 1, Apr. 2004, pp. 629–640.

[15] M. Diwakar and S. Kumar, "An energy efficient level based clustering routing protocol for WSN," *IJASSN*, vol. 2, no. 2, pp. 55–65, Apr. 2012.

[16] S. Ganesh and R. Amutha, "Efficient and secure routing protocol for wireless sensor networks through two level intrusion detection mechanism," *WULFENI*, vol. 19, pp. 388–406, Dec. 2012.

[17] J. Y. Cheng, S. J. Ruan, and R. G. Chenghsu, "PADCP: Power aware dynamic clustering protocol for wireless sensor network," in *Proc. IFIP WOCN*, Apr. 2006, pp. 1–6.

[18] R. V. Kulkarni and A. Forester, "Computational intelligence in wireless sensor networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 13, no. 1, pp. 68–96, Apr. 2011.

[19] S. Mohammadi, R. A. Ebrahimi, and H. Jadidoleslamy, "A comparison of routing attacks on wireless sensor networks," *Int. J. Inf. Assurance Security*, vol. 6, no. 3, pp. 195–215, July 2011.

[20] K. Sharma and M. K. Ghose, "Wireless sensor networks: An overview on security threats," *Int. J. Comput. Appl.*, vol. 1, pp. 42–45, Mar. 2010.

[21] K. Kant and N. Gupta, "Application based study on wireless sensor network," *Int. J. Comput. Appl.*, vol. 21, Mar. 2011.

[22] A.-I. A. Wang, P. Reiher, R. Bagrodia, and G. Popek, "A simulation evaluation of optimistic replicated filing in a mobile environment," in *Proc. IEEE IPCCC*, Feb. 1999.

[23] S. Ganesh and R. Amutha, "Network security in wireless sensor networks using triple umpiring system," *European J. Sci. Research*, vol. 64, no. 1, pp. 128–145, June 2011.

[24] S. Ganesh and R. Amutha, "Efficient and secure routing protocol for wireless sensor networks through optimal power control and optimal handoff-based recovery mechanism," *J. Comput. Netw. Commun.*, vol. 2012, July 2012.

Subramanian Ganesh received the B.E. degree in Electronics and Communications Engineering from Bharadidasan University Trichy, Tamilnadu, India and M.E. degree in Applied Electronics from Anna University, Chennai, Tamilnadu, India, in 1998 and 2008, respectively. He is working towards his Ph.D. degree in the area of "efficient and secure routing protocol for wireless sensor networks" as a part-time candidate in, Sathyabama University, Chennai, Tamilnadu, India. He is working as an Associate Professor in the Department of Electronics and Communication Engineering at Panimalar Institute of Technology, Chennai. He has contributed and presented papers at IEEE international conferences in Kerala, Allahabad, China, Korea, and in Thailand. He had published his research works in various reputed international and national journals. Recently, the teams led by him have participated in international ROBOSUB competition held at Sandiego, CA, USA during the month of July 2012 under the sponsorship of Indian Government. He has completed fourteen years in the field of teaching.

Ramachandran Amutha received the B.E. degree in Electronics and Communications Engineering from Madurai Kamaraj University, Tamilnadu, India and M.E. degree in Applied Electronics from PSG College of Technology, Coimbatore, Bharathiar University Tamilnadu, India, in 1987 and 1991, respectively, and Ph.D. degree in Communication Networks from Anna University, Chennai, India in 2006. She is presently working as a Professor in Electronics and Communication Engineering, Sri Venkateswara College of Engineering, Sriperumbudur, Tamilnadu, India. She served as a Lecturer from June 1988 to May 1993 in the Dept. of ECE, PSG College of Technology, Coimbatore, India. She has presented papers at IEEE international conferences several times. She has published papers in international journals such as international journal on information sciences and international journal on electronics and telecommunication research. Presently, she is coordinating the central government sponsored research project titled "artificial intelligence based tsunami". She has completed twenty three years in the field of teaching.