ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 8, August 2015

Energy- Efficient Routing Protocol with Intrusion Detection System in Wireless Sensor Network

Sreeranjini Nandakumar, P.Krishna Kumaran Thampi

Final Year M. Tech, Dept. of Computer Science & Engineering, Sree Narayana Gurukulam College of Engineering, India

Associate Professor, Dept. of Computer Science & Engineering, Sree Narayana Gurukulam College of Engineering, India

ABSTRACT: Advances and progress in wireless communication made it possible to develop wireless sensor networks (WSN) which has emerged as an important computing platform in the recent few years. In WSN, battery is the only source for providing energy to the sensor nodes; which makes them to work in different environment. WSN consumes a lot of energy for sensing, processing, storing and communicating the data with the sink. Replacement of batteries that are drained or depleted of energy is undesirable in certain cases like surveillance applications or in military applications. Among different protocols so far developed, cluster-based communication protocols (LEECH, SEECH etc.) developed for hierarchical wireless sensor networks play a major role in energy saving. In such methods Cluster Head (CH) sends data directly to sink or via relay node. But it is inefficient if the distance between CH and sink or CH to relay/relay to sink is very large. This paper suggests a method which tries to improve the energy efficiency of WSN by combining Grid-based approach with Cluster-based approach. The network is divided in to grids and selects CH based on energy and distance per each grid. It guarantees uniform distribution of CHs and fixed number of clusters covering all the nodes. The proposed method selects next hop based on certain characteristics. As only CH gets rotated, there is no energy consumption for cluster updating. Since sensor nodes carries sensitive data and operated in hostile unattended environments it must be protected from attacks. But security in sensor networks poses great challenges due to computing and resource constraints. This paper also incorporate position based intrusion detection method to protect the sensor nodes from unauthorized attack and node compromising. Simulation result shows that our Energy-Efficient Routing Protocol with Intrusion Detection System (EERPIDS) can provide energy efficient and secure communication.

KEYWORDS: WSN, energy consumption, grid-based approach, cluster-based method, intrusion detection system

I. INTRODUCTION

Advancement in electronics field facilitated the designers to develop low cost, easily deployable, small sized sensors [1] which have emerged as an important computing technology for physical environment monitoring. Wireless sensor network which comprises of thousands of nodes equipped with sensing unit, transceiver, processing unit and power source with optional GPS, mobilizer and power generator, is not only a sensing network but also a processing, storage and communication network. It provides significant advantages in homeland security, structure, healthcare, and environment monitoring over traditional communication techniques. Sensor nodes senses the environment, collects the data and communicate it with other nodes or with base station (BS). Out of these tasks, communication requires large amount of battery power which makes it more costly in terms of energy consumption. It seems to be difficult to replace or recharge battery once it is depleted or drained-off. In several cases, both options can’t be applied, that is, it should be simply discarded. This means extending network lifetime and energy conservation is the key challenges in the design and implementation of WSNs. Thus our mission is to increase lifespan of sensor network by reducing energy consumption within the given memory and processing capabilities.

DOI: 10.15680/IJIRCCE.2015. 0308051

Different protocols and methodologies are developed so far to mitigate the energy consumption which differs from traditional distributed system. Various cluster based routing protocol [2] for hierarchical network have been proposed by many researchers and scholars. Here, sensor nodes which grouped in to different clusters send their sensed data to a node belong to their cluster called cluster head (CH) and then it aggregates the received data and forwards it to data sink. The cluster-based approach has the ability to enhance network longevity and stability by improving energy efficiency and balancing the energy consumption among the nodes during the network life time. They are classified with respect to the techniques adopted for selecting cluster heads and transmitting the aggregated data to the sink or BS [3].

Some protocols use single-hop communication for transmitting the collected data to the sink which consumes a large quantity of energy and deteriorates energy balancing of nodes. In our proposed method, multihop communication is used for forwarding the collected data to the BS. It uses a method that combines of grid-based approach with cluster based approach. In traditional methods like LEECH, data is sending to sink directly from the CH, which consumes more energy when it is located at a very large distance from sink. In SEECH, even though CH and relay is selected separately energy constraint still exists as the number of next hops from each CH to sink is maximum two.

Here in this paper, the network is divided in to grids and selects CH per each grid in such a way that they can communicate with each nodes in that grid. This approach guarantees uniform distribution of CHs and to form fixed number of cluster covering all the nodes. To improve the efficiency of network, CHs are selected based on energy and distance. Also the proposed solution selects the next hop based on certain characteristics: energy level of CH transmitter, distance between CH transmitter and next hop, distance between CH transmitter and BS. It uses multihop data transmission and suitable number of next hops for transmitting the data from each CH to sink. Another important feature is that there is no cluster updating; only CHs get rotated at the end of each round. So energy consumption for cluster updating can be saved. As communication is said to be success only when the data is reached safe and in right form, we incorporate a position-based approach to detect nodes that are compromised and unauthorized access to the network. Hence this paper ties to open eyes towards energy-efficiency with security.

This paper is organized as follows: Section II describes related works that motivates and leads to this work. Section III explains proposed energy efficient method and section IV illustrates intrusion detection of EERPIDS. In Section V, we evaluate our proposed method and shown simulation results. Section VI concludes the paper with future enhancements.

II. RELATED WORK

Several cluster-based hierarchical protocols have been proposed by researches and scholars to improve the efficiency of WSN. W. Heinzelman, et al; proposed LEACH [4] which was one of the earliest hierarchical clustering protocols developed in order to increase the lifespan of the network. Here, CHs communicate to BS and the non-cluster head node uses CHs as an intermediate node to communicate with the BS. It adopts randomized rotation of CHs to save battery in which each round consists of two phases, setup phase and steady state phase. Cluster formation, CH selection will be taken place in set up phase whereas communication is achieved in steady phase. The main disadvantage of this protocol is every node has the same probability to become the CH. So if node with low energy is selected as CH that node will die very early. X. H. Wu, et al; proposed LEACH-C [5] that differs from traditional LEACH during setup phase by adopting centralized approach. It dissipates extra energy in each round for sending node id, energy value, and position information and by making unnecessary comparison.

S. Lindsey, et al; proposed PEGASIS [6] requires a complete view of network topology for chain construction and suffers delays for forming single chain for distant nodes. It is a chain based routing mechanism and constructs chain instead of clusters. Here all nodes communicates with their closest neighbours and continues their communication until the aggregated data reaches the sink. The CCS [7] proposed by Jung et al. is a combination of both PEGASIS and cluster-based approach. It causes unbalanced distribution of nodes in each level and select leader randomly without considering residual energy. TL-LEACH introduced by Loscrì et al. [8] proposed a two-level hierarchy in which there is primary CH as well as secondary CH is present. A node that has elected as primary and secondary cluster-head has to advertise other nodes. It involves lots of message passing and doesn't bother remaining energy of nodes. A. Manjeshwar, et al; suggests TEEN [9] is not suitable for periodic reports applications since the user may get data only when attribute value reaches at threshold. APTEEN [10] introduced by Manjeshwar and Agrawal is had an additional complexity to implement the threshold functions and the count time with respect to TEEN. But it can be applied to both reactive and proactive scenarios.

LEACH with a mobility factor called LEACH-M [11] introduced by D. S. Kim, et.al; consider mobility of nodes during message passing with that of LEACH. It causes a large number of packet losses during CH movement before selecting a new CH for the next round. HPAR [12] proposed by Q. Li, et.al; is power aware routing protocol which will format the clustered zones and then decide how to route messages across other zones hierarchically for maximizing network lifetime. It uses max-min path for preserving energy of individual nodes. But it may result overhead to the network due to transmission and power estimation. Sleep/wake scheduling protocol [13] suggested by Wu, et al; conserves energy by keeping the radio to sleep during idle times and wake it up only on data transmission/reception suffers synchronization and scheduling overhead.

EECS proposed by Ye et al. [14] suited for periodical data gathering is a LEACH-like protocol, where the network is divided into several clusters. It performs single-hop communication between the CH and the BS and compete themselves to elevate it itself into CH for a given round. This competition involves broadcasting residual energy to neighboring candidates and determining a node with more residual energy to become CH. Also it requires more global knowledge about the distances between the CHs and the BS and results more control overhead complexity as all nodes compete for becoming CHs. HEED [15], introduced by Younis and Fahmy have more work load and generates hot spot in the network. Base-Station Controlled Dynamic Clustering Protocol (BCDCP), introduced by Muruganathan et al. [16], is a centralized clustering routing protocol with single-hop routing which is not appropriate for long-distance communications.

SEECH introduced by Mehdi Tarhani et.al [17] selects CHs and relays separately. This method differs from most of protocols in which high level energy nodes are chosen as cluster head and they are rotationally changed in each round. Even though CH and relay is selected separately energy constraint still exists as the number of next hops from each CH to sink is maximum two and hence it is not applicable in large networks.

To improve and overcome the performance of existing routing mechanism, we propose new method that considers different parameters for selecting CHs, and data transmission path to sink. To make it suitable in long distance communication, suitable numbers of hops are selected based on energy of CH transmitter, energy of CH receiver, distance from CHi to CHj, and distance from CH to BS. Also we add an additional functionality which will detect intruders that causes unauthorized access in the network. It uses simple methodology that will require only small amount of memory and computational capacity. But the IDS method describes in [18,19,20] involves high computational time and needs databases to store to store ontology information. Here we are trying to make a communication not only energy-efficient, but also secure to some extent.

III. ENERGY-EFFICIENT ROUTING IN EERPIDS

Wireless sensor nodes which are battery powered for sensing and collecting information are used in areas where there is very little scope to change or recharge batteries manually. It seems to be very difficult to change or charge batteries frequently as it requires continuous human effort, time and cost. Sensor nodes which collect the data from deployed environment will pass it towards the sink for further processing and analyzing. There is very large scope of research in implementing suitable routing/communication mechanism in WSN, because their function depends upon the type of network structure and type of application. For improving the performance, functionality and lifespan of WSN, we need to increase the lifetime of each sensor node by considering its energy consumption.

The proposed method tries to improve the energy efficiency of WSN by combining Grid-based approach with Cluster-based approach. Here, the network is divided in to grids and selects CH per each grid. Fig.1. illustrates the transmission model of EERPIDS.
Features of this approach:

- This approach guarantees uniform distribution of CHs

- Form fixed number of cluster covering all the nodes
- To improve the efficiency of network, CHs are selected based on energy and distance.
- Selects the next hop based on certain characteristics: energy level of CH transmitter, distance between CH transmitter and next hop, distance between CH transmitter and BS.
- It uses multihop data transmission and suitable number of next hops for transmitting the data from each CH to sink.
- No cluster updating; only CHs get rotated at the end of each round.

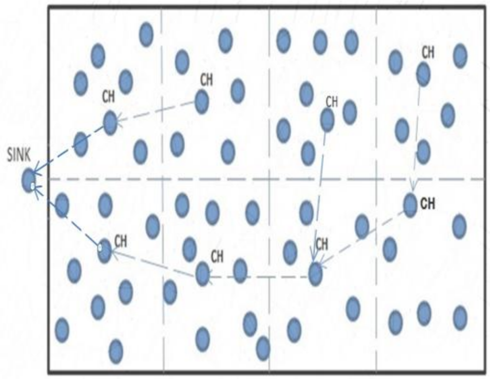


Fig.1. Transmission model in EERPIDS

Steps involved in this routing mechanism are given below:

1. Grid formation
2. CH selection per grid
3. Notification
4. CH collects the sensed data
5. Data transmission to sink
6. CH updating

A. Grid Formation

The area where sensor nodes are deployed should be divided in to ‘g’ number of grids.

$$\text{Number of grids, } g = x_1 * x_2, \text{ where}$$

$$x_1 = x/c$$

$$x_2 = y/c$$

‘x’ and ‘y’ are x-component and y-component of deployed area respectively. ‘c’ is a constant whose values can be set manually. It plays a major role in determining number of grids. We have to select the value of c in such a way that nodes in each grid can communicate with each other. This grid information is stored in GridInfo file for further communication. Here in the simulation, we take c as 400 and x and y as 1600 and 900 respectively. Therefore,

$$x_1 = 4$$

$$x_2 = 2$$

$$\text{Number of grids} = 8$$

B. Cluster Head Selection

The proposed method selects the cluster head by evaluating the residual energy and how closes it to the center of corresponding grid. That is paper tries to select the node which is almost center to the grid, so that other nodes in the grid can communicate with it using less transmission power.

Steps:

For each grid,

1. Find midpoint of grid
2. Evaluate energy of each nodes and distance to midpoint of grid.
3. Select node having high energy and close to midpoint.

C. Notification, Data Collection and Cluster Head Updating

Node which is selected as CH will announce its status to other nodes in the corresponding grid by broadcasting CH-MSG message using GridInfo. They also send CH-Energy message to BS so that it can form CH-Energy list and send this information to every CH. On receiving CH-MSG, the nodes will send a JOIN-MSG message and became a member of that CH.

After joining under a CH, each member in the grid transmits the sensed data to their corresponding CH and thereafter it will forwards the packet towards sink via multiple hops. The hops are selected from CH list by considering certain characteristics: energy level of CH transmitter and receiver, distance between CH transmitter and next hop, distance between CH transmitter and BS. The node in the CH list whose energy greater than the average energy of the nodes in the CH list is taken as next hop. Also we compare distance from CH to next hop with that of distance from CH to sink. If dis(CH,next_hop) is less than dis(CH,sink) and energy is greater than average energy of nodes in CH list, then select it as next hop for data transmission. If distance to sink is lower than next hop, then data can send to it directly.

In each round, CH gets updated based on current residual energy and distance. That is grid doesn't change, only CH gets rotated and communication takes place.

IV. Intrusion Detection in EERPIDS

Communication is said to be success, only when the data is reached at the destination securely without any unauthorized access or manipulation. There are a lots of method used to identify intruder in traditional networks, but they can't be applied as such in WSN. Also there are papers [21, 22, 23] that illustrates IDS in WSN. But most of them adopt complex calculations and memory requirements. As we know, sensor nodes have limited memory and processing capacity, it seems to be difficult to implement such methods in practical situations. It produces high memory and time complexity which will affect the performance and functionality of network. Hence we incorporate a simple strategy (position-based method) to identify compromised nodes and to detect attack on CH by replicating a node in the grid. Here, we take two conditions for considering a node to be compromised,

- Node whose position gets changed (because we are handling static sensor network)
- Nodes which are trying to send data without providing position claim (PC) after reminding for the same.

The PC consists of node ID and position.

Steps for identifying node compromised:

```
1. Each node should send its PC to CH before sending the data.
2. If node sends PC,
    2.1 CH checks for change in position,
        2.1.1 If position is not changed, then send OK message.
        2.1.2 Else
        2.1.3 It detects node attack.
3. Else
    3.1 Inform node to send PC
    3.2 If node sends PC,
        3.2.1 Check whether it is correct
    3.3 Else
        3.3.1 Inform it again and if not send, detect it has compromised
```

Steps for identifying CH attack:

1. Attacker send malicious packet to CH
2. CH reject the packet and ask for PC
3. Attacker sends PC with ID of a valid node in that grid
4. CH rejects the packet by comparing positions in the PC. Even if ID is same, the position from it came is different. No node should have same ID with different position.
5. Alarm intrusion detection message.

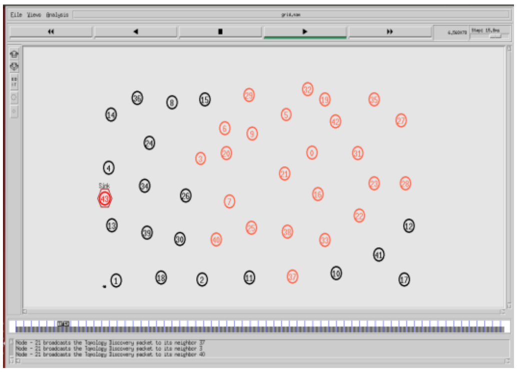
V. Simulation And Performance Results

The proposed system was implemented in NS2 to evaluate the performance and working. The main parameters to be initialized are summarized:

Table.1. Parameters

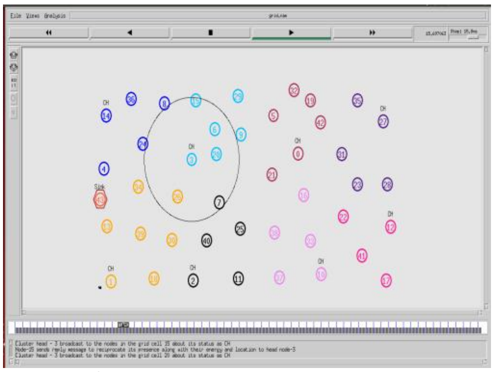
Parameters	Values
Number of nodes	45
Channel Type	Channel/Wireless Channel
Initial Energy	100 or 200
Packet size	128bits/packet

Topology was created with given nodes as shown in Fig.2. Then the entire network is divided into grids and selects a node as CH per each grid. It announces its status to other nodes in the grid and ready to collect data (Fig.3).



```
Node - 21 broadcasts the Topology Discovery packet to its neighbor 37
Node - 21 broadcasts the Topology Discovery packet to its neighbor 3
Node - 21 broadcasts the Topology Discovery packet to its neighbor 40
```

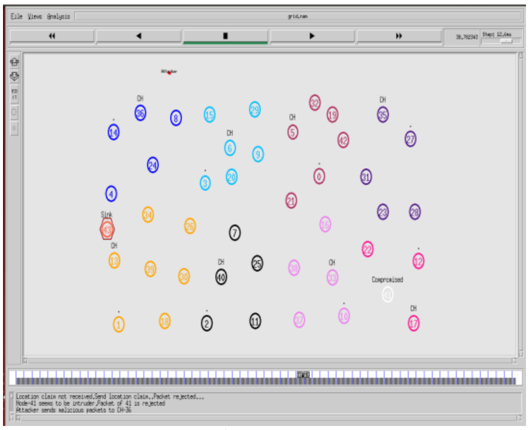
Fig.2.Initial topology



```
Cluster head - 3 broadcast to the nodes in the grid cell 35 about its status as CH
Node-35 sends reply message to reciprocate its presence along with their energy and location to head node-3
Cluster head - 3 broadcast to the nodes in the grid cell 20 about its status as CH
```

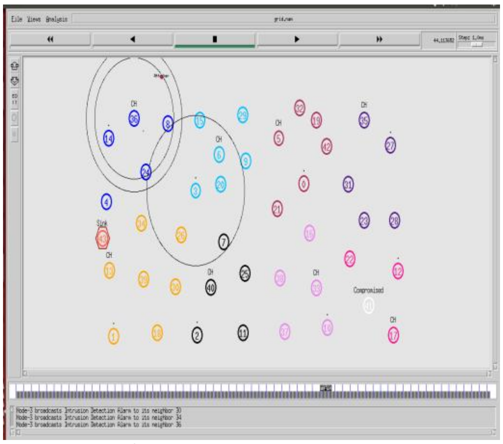
Fig.3.Grid formation, CH selection and announces status

To make it secure, CH will collect position claim from each node and detect whether the node is compromised or not. (Fig.4). Also it identifies intruder which tries to send malicious packet to CH by using position-based strategy. (Fig.5).



```
Location claim not received.Send location claim..Packet rejected...
Node-41 seems to be intruder.Packet of 41 is rejected
Attacker sends malicious packets to CH-36
```

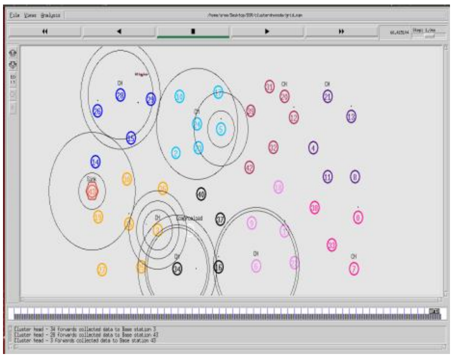
Fig.4.Identifying compromised node



```
Node-3 broadcasts Intrusion Detection Alarm to its neighbor 30
Node-3 broadcasts Intrusion Detection Alarm to its neighbor 34
Node-3 broadcasts Intrusion Detection Alarm to its neighbor 36
```

Fig.5.Identifying attacker node and alarm IDS message

Finally each CH will send data to sink via multiple hops selected based on energy and distance as parameters. (Fig.6). Periodically new set of CHs will be selected and the process will continues.



Cluster head - 34 forwards collected data to Base station 3
Cluster head - 28 forwards collected data to Base station 43
Cluster head - 3 Forwards collected data to Base station 43

Fig.6.Data transmission to sink

For evaluating performance, we took energy consumed in average (Fig.7), residual energy (Fig.8.) and throughput (Fig.9).

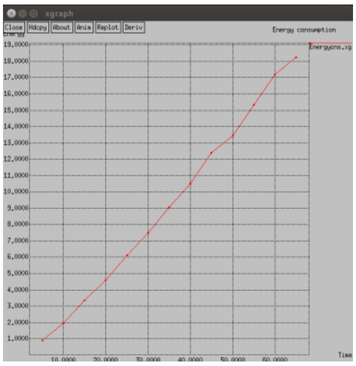


Fig.7.Energy consumption

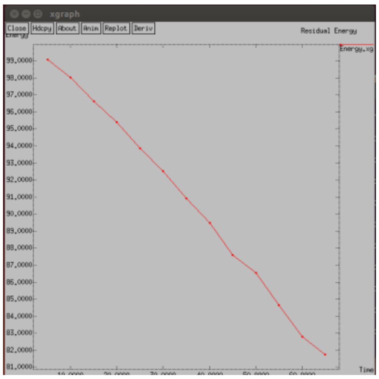


Fig.8.Residual Energy

The above figures show the average energy consumption and average residual energy of nodes in the given network. The amount of energy consumed is seems to be low for the given time interval. Residual energy is the amount of energy remained in the node even after communication.

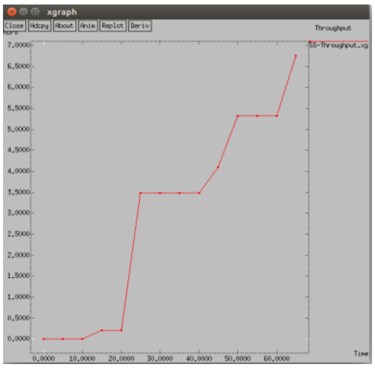


Fig.8.Throughput

The figure shows that our proposed method can provide desired energy efficiency with sufficient throughput.

VI. Conclusion and Future Work

This paper mainly focused on how to improve energy efficiency of WSN to enhance the lifespan of network. The proposed method uses grid-based approach with cluster-based strategy. It achieves the aim by selecting CH based on two parameters: energy and distance. Also it considers energy of CH transmitter and receiver, distance between CH and next hop, distance between CH and sink to select path to the BS. To make it more energy efficient, we just make CH to be rotated and no change in the grid once it is formed. The paper also specifies position based method to identify compromised nodes and attacker. Simulation results shows successful implementation of our proposed method and performance evaluation says that our method can achieve energy efficiency with lower energy consumption.

As future work, more attacking scenarios (sink-hole attack, worm attack etc.) can be included other than CH attack. Here we considered only CH attack assuming no attacks in other sensor nodes. We can also improve this method by incorporating methods to handle node failure by providing back-ups and alternate path

REFERENCES

1. Zheng., Jamalipour., "Wireless sensor networks a networking perspective", IEEE book, John Wiley & Sons, 2009
2. Shankar, Dr Rajashree; "Survey on Energy-Efficient Secure Routing In Wireless Sensor Networks"; International Journal of Computational Engineering Research, pp. 7-11, July 2013
3. O. Boyinbode, H. Le, A. Mbogho, Takizawa, and Poliah, "A survey on clustering algorithms for wireless sensor networks," in Proc. 13th Int. Conf. Netw.-Based Inf. Syst., Sep. 2010, pp. 358–364.
4. Heinzelman, A. Chandrakasan, Balakrishnan, "Energy-Efficient Communication Protocol for Wireless Microsensor Networks," In Proc.33rd Hawaii International Conference on System Sciences, HI, USA, Vol. 8, pp. 110,2000.
5. Wu, S. Wang, "Performance comparison of LEACH and LEACH-C protocols by NS2," In Proceedings of 9th International Symposium on Distributed Computing and Applications to Business, Engineering and Science. Hong Kong, China, pp. 254-258, 2010
6. Lindsey, C.Raghavendra, "PEGASIS: Power-Efficient Gathering in Sensor Information Systems," In Proc. IEEE Aerospace Conference, USA, Montana, Vol. 3, pp. 1125-1130, 2002.
7. Jung, S.; Han, Y.. "The Concentric Clustering Scheme for Efficient EnergyConsumption in the PEGASIS"; In Proceedings of the 9th International Conference on AdvancedCommunication Technology, Gangwon-Do, Kore ; pp. 260–265, February 2007.
8. Loscri, V.; Morabito, G.; Marano, S.; "A Two-Level Hierarchy for Low-Energy Adaptive Clustering Hierarchy"; In Proceedings of the 2nd IEEE Semiannual Vehicular TechnologyConference, Dallas, TX, USA; pp. 1809–1813; September 2005.
9. Manjeshwar, D. Agrawal, "TEEN: A Routing Protocol for Enhanced Efficiency in Wireless Sensor Networks," In Proc. 15th InternationalParallel and Distributed Processing Symposium (IPDPS'01) Workshops, USA, California, 2001, pp. 2009-2015.
10. Manjeshwar,.; Agrawal, D. P. "APTEEN: A Hybrid Protocol for Efficient Routing and Comprehensive Information Retrieval in Wireless Sensor Networks." In Proceedings of the 2nd International Workshop on Parallel and Distributed Computing Issues in Wireless Networks and Mobile computing, Lauderdale, FL, USA, 15–19 April 2002; pp. 195–202.
11. Kim and Y. J. Chung, "Self-organization routing protocol supporting mobile nodes for wireless sensor network," in Proc.First International Multi-Symposiums on Computer and Computational Sciences, Hangzhou, China, 2006.
12. Q. Li, J. Aslam, D. Rus, "Hierarchical Power-aware Routing in Sensor Networks," In Proc. DIMACS Workshop on Pervasive Networking, California, 2001, pp. 25-27.
13. Wu, S. Fahmy, N. Shroff, "Energy Efficient Sleep/Wake Scheduling for Multi-Hop Sensor Networks: non-Convexity and Approximation Algorithm," In Proc. 26th Annual IEEE Conference on ComputerCommunications, Anchorage, Alaska pp. 1568-1576, 2007.
14. Ye, M.; Li, C.; Chen, G.; Wu, J. "*An energy efficient clustering scheme in wireless sensor networks*". Ad Hoc Sens. Wirel. Netw. 2006, 3, 99–119.
15. Younis, O.; Fahmy, S. "HEED: A hybrid, energy-efficient, distributed clustering approach for ad- hoc sensor networks". IEEE Trans. Mobile Comput. 2004, 3, 366–379.
16. Murugunathan, S.D.; Ma, D.C.F.; Bhasin, R.I.; Fapajuwo, A.O. "A Centralized Energy-Efficient Routing Protocol for Wireless Sensor Networks". IEEE Radio Commun. 2005, 43, S8–S13.
17. Tarhani, Yousef S. Kavian, and Saman Siavoshi. "SEECH: Scalable Energy Efficient Clustering Hierarchy Protocol in Wireless Sensor Networks". IEEE Sensors Journal, Vol. 14, No. 11, November 2014, pp 3944-3954
18. Yuxin Mao, "A Semantic-based Intrusion Detection Framework for Wireless Sensor Network",Networked Computing (INC), 6th International Conference, Gyeongju, Korea ,pp.26-32, 2010
19. Mohammad Saiful Islam Mamun, A.F.M. Sultanul Kabir, "Hierarchical Design Based Intrusion Detection System For Wireless Ad Hoc Sensor Network", International Journal of Network Security &Its Applications (IJNSA), Vol.2, No.3 , pp. 102-117, July 2010
20. K.Q. Yan, S.C. Wang,. Liu, "A Hybrid Intrusion Detection System of Cluster-based Wireless Sensor Networks", Proceedings of the International MultiConference of Engineers and Computer Scientists , Vol II ,Hong Kong March 2009
21. Garth V. Crosby, Lance Hester, and Niki Pissinou, "Location-aware, Trust-based Detection and Isolation of Compromised Nodes in Wireless Sensor Networks", International Journal of Network Security, Vol.12, No.2, PP.107- 117; March 2011
22. Rung-Ching Chen, Chia-Fen Hsieh and Yung-Fa Huang, "An Isolation Intrusion Detection System for Hierarchical Wireless Sensor Network", Journal of Networks, Vol. 5, pp. 335-342, March 2010
23. Gupta, S.; Rong Zheng ; Cheng, A.M.K., "ANDES: an Anomaly Detection System for Wireless Sensor Networks", IEEE International Conference on Mobile Adhoc and Sensor Systems, pp 1-9, 2007