Graduate Research in Engineering and Technology (GRET)

Volume 1 | Issue 1 Article 7

July 2013

LEVEL PARTITIONING OF NODES TO ENHANCE THE NETWORK LIFETIME DURING INTRUSION DETECTION IN WIRELESS SENSOR NETWORKS

A. BABU KARUPPIAH
Velammal College of Engineering and Technology, Madurai, India, a_babukaruppiah@gmail.com

LEVEL PARTITIONING OF NODES TO ENHANCE THE NETWORK LIFETIME DURING INTRUSION DETECTION IN WIRELESS SENSOR NETWORKS

A. BABU KARUPPIAH[1], KEERTHINATH[2], M. KUNDRU MALAI RAJAN[3], K.ASHIF ISMAIL SHERIFF[4] & S. RAJARAM[5]

[1,2,3,4]Velammal College of Engineering and Technology, Madurai, India
[5]Associate Professor, Thiagarajar College of Engineering, Madurai, India

Abstract- A Wireless Sensor Network (WSN) consists of many sensor nodes with low cost and power capability Based on the deployment, in the sensing coverage of a sensor node, typically more nodes are covered. A major challenge in constructing a WSN is to enhance the network life time. Nodes in a WSN are usually highly energy-constrained and expected to operate for long periods from limited on-board energy reserves. To permit this, nodes and the embedded software that they execute – must have energy-aware operation. Because of this, continued developments in energy-efficient operation are paramount, requiring major advances to be made in energy hardware, power management circuitry and energy aware algorithms znd protocols. During Intrusion Detection in sensor networks, some genuine nodes need to communicate with the Cluster Head to inform about the details of malicious nodes. For such applications in sensor networks, a large number of sensor nodes that are deployed densely in specific sensing environment share the same sensing tasks. Due to this, the individual nodes might waste their energy in sensing data that are not destined to it and as a result the drain in the energy of the node is more resulting in much reduced network life time. In this paper, a novel algorithm is developed to avoid redundancy in sensing the data thereby enhancing the life time of the network. The concept of Power Factor bit is proposed while a node communicates with the Cluster Head. The simulation results show that the network life time is greatly enhanced by the proposed method.

Keywords- *Wireless Sensor Networks, Intrusion Detection, Cluster Head, Network life time, Power Consumption.*

I. INTRODUCTION

A Wireless Sensor Network (WSN) is a specialized wireless network that is composed of a number of sensor nodes deployed in a specified area for monitoring environment conditions such as temperature, air pressure, humidity, light, motion or vibration, and can communicate with each other using a wireless radio device. WSNs are powerful in that they are amenable to support a lot of very different real-world applications; they are also a challenging research and engineering problem because of this very flexibility. Most sensor network protocols assume a high degree of trust between nodes in order to eliminate the overhead of authentication. This creates the risk of attackers introducing malicious nodes to the network, or manipulating the operation of existing nodes. Consequently, there is the potential for a wide variety of attacks on sensor networks. Inspection engines that can inspect network content for intrusion information are urgently required. After sensor nodes detect a target, they can collaboratively route data to a base station for analysis. The sensor nodes are usually programmed to monitor or collect data from surrounding environment and pass the information to the base station for remote user access through various communication technologies. During this complex process it becomes highly essential to maximize network lifetime in Wireless Sensor Networks (WSNs) and to do so the paths for data transfer to the base station are selected in such a way that the total energy consumed along the path is minimized. Efficient designing of a network in a way efficiently utilizes the energy of nodes to prolong the lifetime of the network. Since communication consume significant amount of battery power, sensor nodes should spend as little energy as possible when receiving and transmitting data [1-3]. To support high scalability and better data aggregation, sensor nodes are often grouped into disjoint, non overlapping subsets called clusters. Clusters create hierarchical WSNs which incorporate efficient utilization of limited resources of sensor nodes and thus extends network lifetime. Clustering schemes offer reduced communication overheads, and efficient resource allocations thus decreasing the overall energy consumption and reducing the interferences among sensor nodes. In this paper, a novel algorithm is developed to efficiently communicate the intrusion information to the Cluster Head with less usage of nodes resources thus extending the life time of the network. The rest of the paper is organized as follows: Section II discusses on the Security threats and limitations in the WSN. The work related to threats, clustering and energy consumption is elaborated under Section III.

The proposed work is dealt in Section IV followed by the simulation results in Section V. Finally,

concluding remarks are given in Section VI.

II. SECURITY ISSUES AND LIMITATIONS IN WSN

A Wireless Sensor Network (WSN) is a network of cheap and simple processing sensor nodes that are equipped with environmental sensors for temperature, humidity, etc. WSNs are deployed in large, open and unattended environments. The WSN nodes are tiny cheap devices and resource constrained in terms of their energy and processing capacity hence they are vulnerable to intrusions through variety of attacks. An intrusion is defined as a set of actions that compromises confidentiality, availability, and integrity of a system. Intrusion detection is a security technology that attempts to identify those who are trying to break into and misuse a system without authorization and those who have legitimate access to the system but are abusing their privileges. The system can be a host computer, network equipment, a firewall, a router, a corporate network, or any information system being monitored by an intrusion detection system

Denial of Service (DoS) attacks like jamming (by interfering with the radio frequency of the node), tampering the node and collision (disrupting key elements of the node by purposeful radio transmissions) can easily take place. An attacker may also disrupt the network by inducing repeated retransmission attempts. A node may be induced to transmit continually and eventually its energy may be exhausted. DoS attacks in detail can be found in [4]. WSN nodes are having limited memory and limited processing power hence the routing protocols developed for WSN are simple. Therefore these protocols are more vulnerable to attacks related to routing. Attacks on routing, well described and classified in [5] are Sinkhole, HELLO Flood, Sybil attack, Selective forwarding, Acknowledgement spoofing, Altering or replaying or spoofing routing information etc. Some more attacks like, Algorithmic Complexity Attack, worm hole, node replication attack are also real threats to the security of WSNs.

Variety of protection mechanisms for above attacks are available including some security protocols. Study of the solutions for WSN security threats reveal that different levels of protections are provided in individual manner. Moreover none of the solutions are capable enough to offer protection from both outside and inside intruders. A good example is protection using cryptographic mechanism. This mechanisms provide protection against some types of attacks from external nodes, however it will not protect against malicious inside nodes. Therefore, intrusion detection mechanisms are necessary to detect such nodes. Intrusion detection systems must be able to distinguish between normal and abnormal activities in order to discover malicious attempts in time and inform the cluster head about the Intruder which in turn will alert all the other sensor nodes about the intruder to make them alert. Typically, a sensor node is a small device that consists of four basic components 1) sensing subsystem for data gathering from its environment, 2) processing subsystem for data processing and data storing, 3) wireless communication subsystem for data transmission and 4) energy supply subsystem which is a power source for the sensor node. The challenges faced in designing sensor network systems and applications include:

- Limited hardware: Each node has limited processing, storage, and communication capabilities, and limited energy supply and bandwidth.
- Limited support for networking: The network is peer-to-peer, with a mesh topology and dynamic, mobile, and unreliable connectivity. There are no universal routing protocols or central registry services. Each node acts both as a router and as an application host.
- Limited support for software development: The tasks are typically real-time and massively distributed, involve dynamic Collaboration among nodes, and must handle multiple competing events. Global properties can be specified only via local instructions.

These limitations are typical characteristics of sensor nodes which affects, sensor networks life and the quality. For that reason, the protocols running on sensor networks must consume the re-sources of the nodes efficiently in order to achieve a longer network lifetime.

When power efficient communication is considered, it is important either to maximize the nodes lifetimes or reduce bandwidth requirements by using local collaboration among the nodes and tolerate node failures, besides delivering the data efficiently.

III. RELATED WORK

Many Clustering and power reduction algorithms that utilize energy in an efficient manner have been developed. Some of the basic concepts that are used to design the proposed algorithm are discussed here to know how nodes are clustered and levels are assigned for each node in a network. Vinay Kumar, Sanjeev Jain and Sudarshan Tiwari [6] have presented taxonomy of energy efficient clustering algorithms in WSNs which provides a survey of existing clustering algorithms. Among the existing methods the algorithm that interested is Linked Cluster Algorithm (LCA). In LCA each node has a unique ID number and selection of cluster heads is based on two factors: (i) Average of the Node that has the highest ID and (ii) Residual energy.

Clustering for Localization (CFL) algorithm closely resembles LCA in which the weight function is a combination of different parameters including: residual energy, number of neighbours and transmission power. S.V.Manisekaran, R.Venkatesan and G.Deivanai [7] have proposed Mobile Adaptive Distributed Clustering Algorithm (MADCA) that minimize energy consumption and also support mobile nodes. In this algorithm clustering of nodes is based on similarity of data. Thus reducing the burden on sink improves the lifetime of the network. Shilpa Mahajan and Jyoteesh Malhotra [8] have proposed an energy efficient technique based on graph theory that can be used to find out minimum path from source to the destination node. A sensor area is divided into number of levels based on the signal strength from base station. This technique gives the minimum path and alternate paths are also saved in case of node failure. In [9], a Cluster based algorithm is proposed that can present a flexible, adjustable and energy efficient scheme to identify redundant nodes for different requirements of network life time and low sensing coverage loss ratio.

The Cluster Head (CH) election procedure if done is based on two factors: 1.Node with large number of neighboring node and 2. Residual energy. In [10], H. Chan, A. Perrig discusses about Migration the process in which the candidate for being CH is selected. Each CH periodically checks the ability of its neighbors for being a CH and decides to step down if one of these neighbors has more followers than it does. A node that has the largest number of followers and the least overlap with existing clusters will be considered as the best candidate for CH. O. Younis, S. Fahmy proposed a Hybrid Energy-Efficient Distributed Clustering (HEED) in [11] which is a distributed algorithm which selects the CH based on both residual energy and communication cost.

Basically HEED was proposed to avoid the random selection of CHs. Energy Efficient Hierarchical Clustering (EEHC): EEHC [12] proposed by is a distributed, randomized clustering algorithm for WSNs, in which the CHs collect the information about the individual clusters and send the aggregated report to the base-station. In [13],

X. Co, H. Zhang, J. Shi, and G. Cui proposed a minimum spanning tree-PSO based clustering algorithm where election of cluster head is based on the energy available to nodes and Euclidean distance to its neighbor node in the optimal tree. A reliable clustering algorithm based on LEACH–D was proposed in [14]. An energy efficient clustering algorithm was proposed in [15] which is based on virtual area partition in heterogeneous networks environment where the maximal transmission power of each node may be different. Mehdi Saeidmanesh et al. [16] have discussed EDBC (Energy and Distance Based Clustering) that considers both the residual energy of sensor nodes and the distance of each node from the base station when selecting cluster head.

In [17], authors proposed a technique of clustering the sensors into groups that enables them to communicate with the cluster heads. Instead of collecting data from every node, the sink collects only from cluster heads.

IV. PROPOSED WORK

Our objective is to develop a Cluster Head Detection and communication mechanism with reduced processing and network power consumption and to prolong network lifetime by reducing network receiving power consumption. The detection and communication process involves three different phases:

1. Inter-node distance calculation
2. Neighbor node Discovery
3. Cluster Head Selection
4. Power Factor assignment using Level partitioning.

Inter-node distance calculation

A Cluster head is a sensor node in WSN which has the largest number of neighboring node and residual energy. In Cluster based algorithm the number of neighbors of each node is identified by sending and receiving of probe messages. Also every node calculates the weight of every other node in the network using the number of neighbors and residual energy of each node that is shared using probe messages.

In the existing algorithms energy consumption is mainly because of sending and receiving of probe messages. To reduce the network power consumption the number of probe messages have to be reduced. Also, each node reads the number of neighbours and residual energy of every other node and calculates the weight of every other node.

This makes the cluster head selection procedure more complex, inefficient, time and power consuming process. Hence, the use of a mobile node is suggested that is explicitly used for Cluster Head detection and does not do the work of a sensor node.

Probe messages are commonly used to know the number of neighbour and residual energy of each node in the WSN. To reduce the usage of probe messages the concept of Graph theory is used by which the neighbour node of each node is found by just reading the x and y coordinates of each node in a localised network. Once the coordinates of each node (x, y) are obtained, the inter distance between each node from every other node can be calculated using the two point distance formula given as in equation

(1),

$$D = \sqrt{(y_2 - y_1)^2 + (x_2 - x_1)^2} \qquad (1)$$

where 'D' is the distance, (x_1, y_1) and (x_2, y_2) are the coordinates of the nodes.

ALGORITHM 1: Inter Node Distance Calculation

1: **if** *Distance of node i from node i* **then**
2: *Distance* ⟵ *0*
3: **else** *Distance of node i from node j*
4: *calculate the distance using the formula*
5: **end if**

The Algorithm 1 explains the steps in calculating the distances from all other nodes from each node.

Neighborhood Discovery

Algorithm 2 gives the steps in which the neighbors are estimated.The number of neighbors is determined from the Internode distance calculation. If this distance is less than the sensing radii of the sensor node then both the nodes are said to be neighboring nodes. The residual energy of each node is periodically updated which could be read by the Mobile node during Cluster head detection.

ALGORITHM 2: Neighbourhood Discovery

1: **if** *two nodes taken are not the same*
2: **if** *Distance of node i from node j is less than 50m*
3: *Node j is a neighbour of Node i*
4: **end if**
5: **end if**

Cluster Head Detection

The Inter-node distance calculation and the neighborhood discovery form the basis for finding the Cluster Head in the network. The Cluster Head is selected based on the number of neighbor nodes and residual energy. Using the information of the number of neighbor nodes and their residual energies the weight of each node can be calculated. It is done so by using equation (2),

$$W_v = w_1 * N_v + w_2 * E_v \qquad (2)$$

where w1 and w2 are the weight parameters Nv and Ev are the number of neighboring nodes and residual energy respectively. The Mobile node calculates the weights of all nodes and assigns the node with highest weight as the Cluster Head node. After this the mobile node becomes inactive for a particular timeout. After a particular time out this Cluster head detection procedure is again run by the mobile node. Hence his algorithm is stored and run only by the Cluster head node and not in any other sensor node, thus economically utilizing the memory energy level of the sensor nodes. Fig.3 is the flow chart that explains the process of Cluster Head Selection.

ALGORITHM 3: Cluster Head Detection

1: **for** *all nodes in the network*
2: **if** *Weight of Node i less than Weight of Node j*
3: *swap the weight of the nodes*
4: **end if**
5: **end for**
6: **if** *Weight of node 1 equals original copy of weight of node i*
8: Cluster Head equals i
9: **End if**

Power Factor Assignment

Generally in a WSN communication between sensor nodes and Sink node is by broadcasting. Thus all sensor nodes transmit their message with maximum power irrespective of its distance from the sink node. Thus to prolong the network lifetime we vary the transmitting power of each sensor node in accordance to its distance from the Cluster Head which acts as the Sink node of the network. The Power factor assignment algorithm is stored in all the sensor nodes but is run only once by the sensor node which has been chosen as the Cluster Head by the Mobile node. To make the Cluster Head or Sink node unique from all other sensor nodes it is assigned with a unique Power Factor 0.

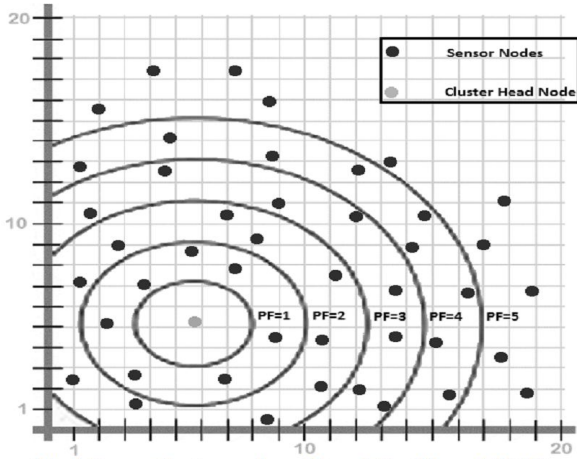

Fig.4 Power Factor assigned Level Partitioned WSN

Fig. 1 shows the network area where the sensing radii of the Cluster head node are divided into concentric rings of different sensing radii. The node in the region between each concentric ring is given with a particular Power Factor. Power Factors are real natural numbers. Each sensor node is given with a basic transmitting power (say 10mW). The Cluster head assigns Power Factor to its sensor nodes through probe messages. First it transmits a probe message with a Power Factor bit of 1, the transmitting power of which is give by the product of basic transmitting power and Power Factor (10mW).

This message will be received by all the nodes within the first concentric ring. Now second probe message is transmitted with Power Factor bit as 2, which will be received by nodes in between the first and second concentric ring. Thus probe messages of varying power are transmitted by the Cluster Head and the entire sensor node just stores the Power Factor bit present in the probe message. Now when a sensor node senses any change in physical quantity and needs to communicate it to the Cluster head, then is broadcasts the message with a transmitting power given as in equation (3),

TX Power = (Basic TX power * Power Factor of that sensor node.) (3)

Also this message will not be processed by all the nodes that receive the broadcasted message. Once the message is received, it gets processed only if the Power Factor of the receiving node is 0 i.e., if the receiving node is the sink node then the message is sensed and processed. Else on any other case if the Power Factor of receiving node is non-zero or equal the message is dropped immediately after being sensed without processing and thus utilizing the Energy of a node economically.

V. EXPERIMENTAL RESULTS AND COMPARISONS

It is assumed that the network setup is static, meaning that the location of the sensor nodes does not change. It is also assumed that the sensor nodes have the same transmitting power. Suppose a node in level 2 wants to communicate with the Cluster Head to inform about intrusion in the network, it sends a message with Power Factor 2 with a transmitting power of 69mW. The nodes in level 1 will also receive the message since it is within the coverage range of level 2 nodes.

When those nodes receive the packet, they only sense the Power Factor bit to do the match. If it matches with its PF bit, they process the message else they drop it without processing. By evading processing, the nodes conserve considerable amount of energy thereby enhancing the network life time.

Table 1 shows the assumed simulation parameters taken into consideration for analyzing the proposed algorithm.

Table 1 Simulation parameters

S.No	Parameter	Value
1.	Transmitting Power	69mW
2.	Receiving Power	42mW
3.	Idle Power	9.3mW
4.	Inactive Power	16.2mW
5.	Energy per Individual node	50J
6.	Weighting Parameters W_1 and W_2	0.2, 0.8

Table 2 shows the simulated result of the level partitioned WSN where it is inferred that the Energy consumption is greatly reduced when the concept of Power Factor assignment is taken into consideration.

Table 2 Simulation results of Power Consumption by the WSN

No of Nodes	Tx Node	X	Y
10	5	360	175
20	10	760	325
30	15	1160	475
40	20	1560	625
50	25	1960	775
60	30	2360	925
70	35	2760	1075
80	40	3160	1225

X - Power Consumption of the network without Power Factor in mW
Y - Power Consumption of the network with Power Factor in mW

Fig. 2 shows the comparison between the power the consumed by the network with Power Factor and without it, where it is inferred that as the number of nodes in the WSN increases a great amount of energy can be conserved by reducing the power consumption using the Power Factor bit assignment combined with level partitioning of the network. As the energy of the sensor nodes are conserved so do the life time of the network.

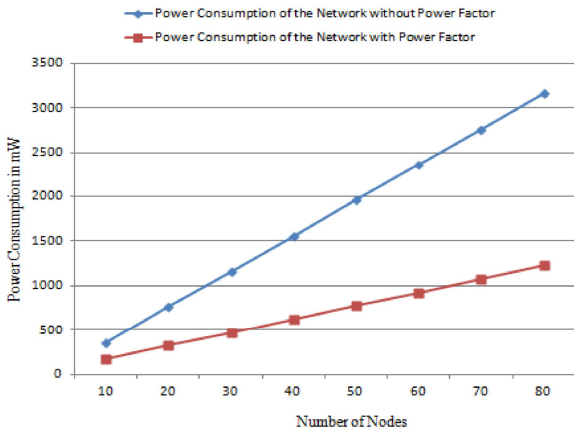

Fig. 2 Comparison of Power Consumption with and without Power Factor.

VI. CONCLUSION

A Novel algorithm combining Level partitioning of the WSN and Power Factor assignment for Intrusion detection is proposed here. This novelty aims at enhancing the network life time of the WSN. Conventionally, the Wireless Sensor nodes sense and process the data. Here in the proposed method, the processing of information is avoided if the Power Factor bit sent is not matching with the receiver‟ s Power Factor bit. It is inferred that quite a large amount of energy can be saved by shirking the processing of information and the life time of the

network can be extended by employing this proposed method. The results show that the conservation of the energy will be huge if the proposed method is implemented for a dense WSN where the nodes are abundant in the network.

REFERENCES

[1] J. M. Kahn, R. H. Katz, and K. S. J. Pister, "Next century challenges: Mobile networking for smart dust," in Proceedings of ACM/IEEE International Conference on Mobile Computing Networks, pp. 271–278, August 1999.

[2] I. F. Akyildiz, S. Weilian, Y. Sankarasubramania and E. Cayirci, "A survey on sensor networks," IEEE Communications Magazine, vol. 40, no. 8,pp. 102–114, August 2002.

[3] Z. Q. C. Yunxia, "On the lifetime of wireless sensor networks," Vol. 9, pp. 976–978, 2005.

[4] A.D. Wood, J.A. Stankovic, "A Taxonomy for Denial-of-Service Attacks in Wireless Sensor Networks", Handbook of Sensor Networks: Compact Wireless and Wired Sensing Systems, CRC Press,2004.

[5] Chris Karlof and David Wagner. Secure routing in wireless sensor networks: Attacks and countermeasures. In First IEEE International Workshop on Sensor Network Protocols and Applications, 2003.

[6] Vinay Kumar, Sanjeev Jain and Sudarshan Tiwari "Energy Efficient Clustering Algorithms in Wireless Sensor Networks: A Survey" IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 5, No 2, September 2011

[7] S.V.Manisekaran, R.Venkatesan, G.Deivanai "Mobile Adaptive Distributed Clustering Algorithm for Wireless Sensor Networks", International Journal of Computer Applications (0975 – 8887),Volume 20– No.7, April 2011.

[8] Shilpa Mahajan1, Jyoteesh Malhotra2 "Energy Efficient Path Determination in Wireless Sensor Network Using BFS Approach " Received September 9, 2011; revised October 10, 2011; accepted October 20, 2011

[9] Li-Liann Lu, Jean-Lien C. Wu, San-Hao Chen, "A Cluster-Based Algorithm for Redundant Nodes Discovery in Dense Sensor Networks", International Journal of Sensor Networks, 2011 Vol.10, No.1/2, pp.59 - 72

[10] H. Chan, A. Perrig, An emergent algorithm for highly uniform cluster formation, in: Proceedings of the 1st European Workshop on Sensor Networks (EWSN), Berlin, Germany, January 2004.

[11] O.Younis, S.Fahmy, A hybrid energy-efficient distributed clustering approach for Ad Hoc sensor networks, IEEE Transactions on mobile computing 3(4) (2004) 366-379.

[12] S.Bandyopadhyay, E.Coyle, An energy efficient hierarchical clustering algorithm for wireless sensor networks, in: Proceedings of the 22nd Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM 2003), San Francisco, California, April 2003.

[13] Y. Liu, Z. Lo, K. Xu and L. Chen; "A reliable clustering algorithm base on LEACH protocol in wireless mobile sensor networks" 2nd International Conference on Mechanical and Electrical Technology (ICMET), 2010, pp 692 – 696.

[14] X. Co, H. Zhang, J. Shi, and G.Cui "Cluster heads election analysis for multi-hop wireless sensor networks based on weighted graph and particle swarm optimization", in IEEE fourth International Conference on computing, 7, 599–603.

[15] R. Wang, L. Guozhi, and C. Zheng " A clustering algorithm based on virtual area partition for heterogeneous wireless sensor networks", in International Conference on Mechatronics and Automation, 372–376.

[16] Mehdi Saeidmanesh, Mojtaba Hajimohammadi, and AliMovaghar, "Energy and Distance Based Clustering: An Energy Efficient Clustering Method for Wireless Sensor Networks", World Academy of Science, Engineering and Technology, vol. 55, p.p 555-559, 2009.

[17] Stanislava, S. and Wendi, B. H. 2005. Prolonging the Lifetime of Wireless Sensor Networks via Unequal Clustering. In Proceedings of the 19th IEEE International Parallel and Distributed Processing Symposium, p.p 8-16.

[18] H.Chan, M.Luk, A.Perrig, Using clustering information for sensor network localization, in: Proceedings of the International Conference on Distributed Computing in Sensor Systems (DCOSS˝ 05), Marina Del Rey, CA, USA, June 2005.